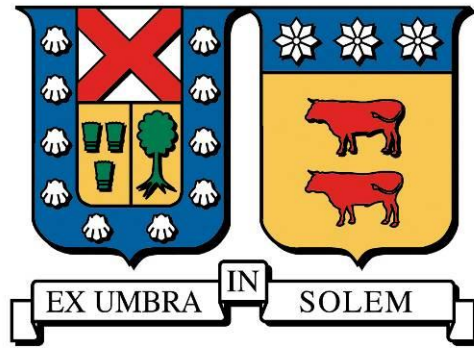




**UNIVERSIDAD TECNICA FEDERICO SANTA MARIA
DEPARTAMENTO DE INGENIERÍA MECÁNICA**

**“Evaluación técnica, regulatoria y económica de la
Ley Marco de Ciberseguridad (Ley N.º 21.663) en el
sector de generación eléctrica chileno”**

Franklin Sánchez Gómez

MAGÍSTER EN ECONOMÍA ENERGÉTICA

2026



CONSTANCIA DE VALIDACIÓN Y CONFIDENCIALIDAD DE MONOGRAFÍA A REPOSITORIO ACADÉMICO

1.- IDENTIFICACIÓN DEL TRABAJO ACADÉMICO

Tipo de monografía (marcar una opción): ☐ Memoria o trabajo de título ☒ Tesis de Postgrado

Título del trabajo: Evaluación Técnica Regulatoria y económica de la Ley Marco de Ciberseguridad (Ley 21.663) en el sector de generación eléctrica chileno

Nombre del candidato(a): Franklin Sanchez

Carrera / Grado: Magíster en Economía Energética

Campus: Vitacura

Departamento: Ingeniería Mecánica

2.- VALIDACIÓN DEL PROFESOR GUÍA/DIRECTOR DE TESIS

Yo, Juan Carlos Olmedo Hidalgo, en mi calidad de profesor(a) guía/director(a) del trabajo académico mencionado anteriormente **DEJO CONSTANCIA** que:

- He revisado esta versión del documento y corresponde a la versión final aprobada del trabajo.
- El trabajo cumple con los requisitos académicos y de formato establecidos por la institución.

3.- EVALUACIÓN DE CONFIDENCIALIDAD POR PROPIEDAD INDUSTRIAL (marcar una opción)

☒ El trabajo **NO contiene** información que amerite confidencialidad y puede ser publicado de inmediato en repositorio con acceso abierto.

☐ El trabajo **CONTIENE** información con potenciales implicancias de propiedad industrial o intelectual y requiere un periodo de confidencialidad (**embargo**) por (**marcar una opción**):

☐ 6 meses ☐ 12 meses ☐ 2 años ☐ 3 años ☐ 5 años ☐ 10 años

Fundamentación de la necesidad de confidencialidad (obligatorio si se solicita embargo):

4.- FIRMAS

Profesor(a) guía o director(a) de memoria o tesis:

Fecha: _____ Firma: _____

JUAN
CARLOS
OLMEDO

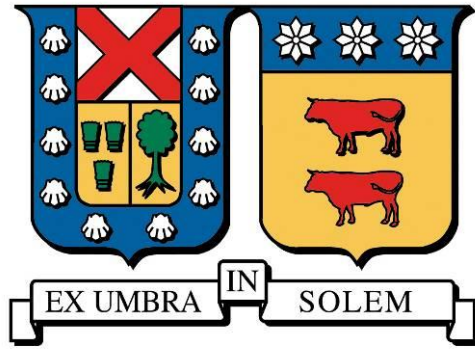
Firmado digitalmente
por JUAN CARLOS
OLMEDO
Fecha: 2026.10.19
21:35:33 -03'00'

Estudiante o Candidato(a):

Fecha: 18/10/2026 Firma: _____


F. Sanchez

Este formulario debe ser insertado como página 2 de la memoria o tesis, completado y firmado por estudiante y profesor(a) antes de la entrega en portal PRISMA de Biblioteca USM.



**UNIVERSIDAD TECNICA FEDERICO SANTA MARIA
DEPARTAMENTO DE INGENIERÍA MECÁNICA**

**“Evaluación técnica, regulatoria y económica de la
Ley Marco de Ciberseguridad (Ley N.º 21.663) en el
sector de generación eléctrica chileno”**

Tesina de grado presentada por

Franklin Sánchez Gómez

como requisito parcial para optar al grado de

Magíster en Economía Energética

Profesor Guía
Juan Carlos Olmedo

Profesor Correferente
Marco Mancilla

Profesor Correferente externo
Patricio Leyton

Julio 2026

TITULO DE LA TESINA:

Evaluación técnica, regulatoria y económica de la Ley Marco de Ciberseguridad (Ley N.º 21.663) en el sector de generación eléctrica chileno

AUTOR:

FRANKLIN SÁNCHEZ GÓMEZ

TRABAJO DE TESINA, presentado en cumplimiento parcial de los requisitos para el Grado de Magíster en Economía Energética del Departamento de Ingeniería Mecánica de la Universidad Técnica Federico Santa María.

Nombre Profesor: Juan Carlos Olmedo

Nombre Profesor: Marco Mancilla

Nombre Profesor: Patricio Leyton

Julio de 2026, Santiago, Chile.

ÍNDICE

Índice.....	5
Resumen.....	8
Abstract.....	9
Glosario.....	10
1. Introducción y Marco de Contexto	13
2. Objetivos.....	15
2.1 Objetivo General.....	15
2.2 Objetivos Específicos.....	15
3. Estado del arte.....	17
3.1 Ciberseguridad en infraestructuras críticas del sector eléctrico.....	17
3.2 Enfoques regulatorios internacionales en ciberseguridad eléctrica	17
3.3 Evolución del marco normativo de ciberseguridad en Chile	18
3.4 Convergencia entre ciberseguridad y gestión de activos.....	21
3.5 Dimensión económica de la ciberseguridad en el sector eléctrico.....	21
3.6 Vacíos de conocimiento y oportunidad de investigación.....	21
3.7 Síntesis del estado del arte.....	22
4. El sistema Eléctrico Nacional como infraestructura crítica: Fundamento técnico del estudio.....	23
4.1 Estructura y escala del Sistema Eléctrico Nacional	23
4.2 Criticidad Sistémica y consecuencias de una disrupción.....	25
4.3 Agrupación tecnológica para el análisis metodológico.....	27
4.4 De la digitalización a la exposición: por qué surge la vulnerabilidad.....	29
4.5 Vulnerabilidades técnicas y vectores de ataques en entornos OT.....	30
4.6 Casos documentados de ciberataques a infraestructura crítica.....	31
4.7 Síntesis: de la exposición técnica a la necesidad regulatoria	32
5. Marco Regulatorio e integración con la gestión de activos	34
5.1 Criterios de análisis regulatorio.....	34
5.2 Análisis de la Ley 21.663 según dimensiones	35

5.3 Obligaciones de Cumplimiento y Matriz Regulatoria (Ley N° 21.663).....	40
5.4 Habilitación sectorial y Estándar de Ciberseguridad del CEN	43
5.5 Convergencia normativa: control técnico integrado Ley 21.663 y Estándar CEN	48
5.6 Marco Normativo en desarrollo: Reglamento de Auditoría y Norma Técnica CNE	52
5.7 Integración de la ciberseguridad en la gestión de activos (OE2)	53
5.8 Síntesis del Capítulo	57
6. Evaluación Comparada y Matriz de Brechas	59
6.1 Propósito y método	59
6.2 Eje legal: Ley 21.663, NIS2 y ANEEL RN 964	61
6.3 Eje técnico: Estándar CEN, NERC-CIP e IEC 62443	64
6.4 Análisis de Brechas (Gap Analysis)	68
6.5 Matriz de Brechas	69
6.6 Síntesis del Capítulo	71
7. Modelo de Estimación de Costo Anualizado de Cumplimiento (OE5)	72
7.1 Fundamento y Justificación del modelo	72
7.2 Enfoque metodológico general	75
7.3 Arquitectura del modelo: Grupo A/B/C y unidad de análisis	77
7.4 Drivers de costo: Identificación y correspondencia normativa	82
7.5 Fuentes de Costos y Calibración (Min/Med/Max)	93
7.6 Formulación matemática del modelo CAC.....	98
7.7 Arquitectura computacional del modelo Excel	101
7.8 Alcances y limitaciones del modelo	103
7.9 Resultados del modelo: Comparación entre tipologías.....	105
7.10 Estructura CAPEX/OPEX y dominancia operativa	106
7.11 La paradoja de la proporcionalidad	108
7.12 Análisis de Sensibilidad	110
7.13 Dispersión de mercado (rangos Min-Max)	113

7.14	Síntesis del modelo y cierre del Objetivo Específico 5.....	114
8.	Discusión de los resultados finales	116
8.1	Dimensión técnica.....	116
8.2	Dimensión regulatoria	117
8.3	Dimensión económica.....	118
9.	Conclusiones y Recomendaciones	120
9.1	Conclusiones por objetivo específico.....	120
9.2	Conclusión General	121
9.3	Recomendaciones	122
10.	Anexos	124
10.1	ANEXO A: Metodología	124
10.1.1	Enfoque metodológico general	124
10.1.2	Estructura general del estudio	124
10.1.3	Etapas de desarrollo y entregables.....	124
10.2	ANEXO B: Carta Gantt.....	129
11.	Referencias.....	131

RESUMEN

El sector de generación eléctrica chileno opera sobre una infraestructura crecientemente digitalizada en la que sistemas de control industrial (OT) gestionan en tiempo real la inyección de energía al Sistema Eléctrico Nacional. La Ley Marco de Ciberseguridad (Ley N.º 21.663, marzo de 2024) y el Estándar de Ciberseguridad del Coordinador Eléctrico Nacional establecen obligaciones permanentes para los Operadores de Importancia Vital del sector. Estas obligaciones tienen un costo concreto cuya magnitud y estructura no ha sido cuantificada: los marcos regulatorios prescriben qué debe cumplirse, pero no cuánto cuesta hacerlo. Esa es la pregunta que esta investigación responde, con foco exclusivo en el sector de generación.

El trabajo se estructura como un recorrido que avanza desde el sistema hacia su costo. Primero caracteriza el Sistema Eléctrico Nacional como infraestructura crítica ciberfísica y como activo estratégico de seguridad nacional, documentando con casos reales —Ucrania 2015 y 2016, entre otros— la transición de la amenaza desde el plano informático hacia el daño físico, y proponiendo una clasificación que agrupa las centrales en tres tipologías según su arquitectura de control OT. Sobre esa base, se desarrollan los cinco objetivos específicos de la investigación. El primero analiza el marco normativo y de gobernanza, sistematizando las obligaciones de la Ley 21.663 y el Estándar CEN en una matriz de convergencia. El segundo examina su integración en la gestión de activos eléctricos, articulando los deberes de ciberseguridad con los indicadores de integridad del SGIIE supervisado por la SEC. El tercero contrasta el marco chileno con estándares internacionales mediante un doble eje legal (NIS2, ANEEL RN 964) y técnico (NERC-CIP, IEC 62443), evaluando su coherencia conceptual. El cuarto diagnostica las brechas que condicionan la viabilidad de implementación del marco, distinguiendo vacíos normativos, brechas técnicas y solapamientos regulatorios, y asignando a cada hallazgo su vía de resolución. El quinto desarrolla el modelo de Costo Anualizado de Cumplimiento (CAC) como aporte metodológico original que integra CAPEX anualizado y OPEX recurrente, a partir de diecisiete drivers derivados de las obligaciones regulatorias, y normaliza los resultados sobre el Valor de Inversión de cada central para producir indicadores comparables con la regulación sectorial del RPTD N.º 17.

Los resultados muestran que el marco chileno presenta coherencia conceptual con los estándares internacionales analizados, con divergencias puntuales en el mecanismo de designación de entidades obligadas y en el alcance de la detección técnica. El CAC aplicado a una central de 100 MW en escenario base arroja costos anualizados entre USD 615.480 (Solar FV) y USD 724.816 (Térmica Gas), equivalentes a entre 0,141% y 0,761% del Valor de Inversión según tipología, con el OPEX representando cerca del 69% del total y un solo driver —el monitoreo SIEM industrial— concentrando hasta un tercio del costo. El estudio concluye que el cumplimiento normativo constituye una carga económica estructural y permanente, dominada por el gasto operativo, diferenciada por arquitectura de control y no neutra en términos de proporcionalidad regulatoria entre tecnologías, sin que ello permita, por sí solo, evaluar la suficiencia del marco frente al riesgo cibernético que busca mitigar.

ABSTRACT

The Chilean electricity generation sector operates on an increasingly digitalized infrastructure in which industrial control systems (OT) manage real-time energy injection into the National Electric System. The Cybersecurity Framework Act (Law No. 21,663, March 2024) and the Cybersecurity Standard of the National Electric Coordinator establish permanent obligations for Vital Importance Operators in the sector. These obligations carry a concrete economic cost whose magnitude and structure has not been quantified: regulatory frameworks prescribe what must be complied with, but not how much it costs to do so. That is the question this research answers, with focus on the generation sector.

The work is structured as a journey that advances from the system toward its cost. It first characterizes the National Electric System as a cyber-physical critical infrastructure and as a strategic national security asset, documenting with real cases —Ukraine 2015 and 2016, among others— the transition of the threat from the informational domain toward physical damage, and proposing a classification that groups power plants into three typologies according to their OT control architecture. On that basis, the five specific objectives are developed. The first analyzes the regulatory and governance framework, systematizing the obligations of Law 21,663 and the CEN Standard into a convergence matrix that demonstrates both instruments resolve into an integrated set of technical controls without duplication. The second examines the integration into electric asset management, linking cybersecurity duties with the integrity indicators of the SGIIE supervised by the SEC. The third contrasts the Chilean framework with international standards through a dual legal axis (NIS2, ANEEL RN 964) and technical axis (NERC-CIP, IEC 62443), evaluating its coherence. The fourth diagnoses the gaps that condition the effective implementation of the framework, distinguishing regulatory voids, technical gaps by typology and regulatory overlaps, and assigning each finding its resolution path. The fifth develops the Annualized Compliance Cost model (CAC) as an original contribution: a parametric tool that integrates annualized CAPEX and recurring OPEX, based on seventeen drivers derived from regulatory obligations, and normalizes results against each plant's Investment Value to produce indicators compatible with the existing sector regulation under RPTD No. 17.

Results show that the Chilean framework presents conceptual coherence with the analyzed international standards, with specific divergences in the mechanism for designating obligated entities and in the scope of technical detection. The CAC applied to a 100 MW plant under the base scenario yields annualized compliance costs ranging from USD 615,480 (Solar PV) to USD 724,816 (Gas Thermal), equivalent to between 0.141% and 0.761% of the Investment Value by typology, with OPEX representing approximately 69% of the total and a single driver —industrial SIEM monitoring— accounting for up to one-third of the cost. The study concludes that regulatory compliance constitutes a structural and permanent economic burden, dominated by operating expenditure, differentiated by control architecture and non-neutral in terms of regulatory proportionality across technologies, without this alone allowing an assessment of the framework's sufficiency against the cybersecurity risk it seeks to mitigate.

Glosario

Término / Sigla	Definición
ANCI	Agencia Nacional de Ciberseguridad: Organismo rector creado por la Ley 21.663, encargado de coordinar, supervisar y fiscalizar las acciones de ciberseguridad nacional.
CAC	Costo Anualizado de Cumplimiento: Modelo metodológico propuesto en esta tesis para estimar el esfuerzo económico anual requerido para cumplir con la normativa de ciberseguridad.
CAPEX	Capital Expenditure: Inversiones de capital destinadas a la adquisición de tecnología y activos fijos para la protección de la infraestructura.
CEN	Coordinador Eléctrico Nacional: Organismo técnico independiente encargado de la coordinación de la operación del Sistema Eléctrico Nacional (SEN).
CSIRT	Computer Security Incident Response Team: Equipos de respuesta ante incidentes de seguridad informática encargados de la gestión operativa de crisis.
DCS	Distributed Control System: Arquitectura de control industrial utilizada en procesos continuos complejos como los ciclos termodinámicos de centrales térmicas.
DS 285	Decreto Supremo N.º 285: Reglamento que define el procedimiento administrativo para la calificación de los Operadores de Importancia Vital (OIV).
DS 295	Decreto Supremo N.º 295: Reglamento que establece las reglas de notificación y estándares para el reporte de incidentes de ciberseguridad.
HFORg	Indisponibilidad Forzada de Generación: Métrica definida en la NTSyCS que cuantifica las salidas de servicio no programadas de las unidades de generación.
HPROg	Indisponibilidad Programada de Generación: Métrica de la NTSyCS que registra las salidas de servicio planificadas y coordinadas para

	mantenimiento.
ICS/OT	Industrial Control Systems / Operational Technology: Hardware y software dedicado a monitorizar y controlar procesos físicos mediante el control directo de dispositivos industriales.
IEC 62443	Serie de estándares internacionales para la ciberseguridad en sistemas de automatización y control industrial (IACS).
ISO 55001	Norma internacional que especifica los requisitos para un sistema de gestión de activos físicos.
Ley 21.663	Ley Marco de Ciberseguridad: Normativa chilena de 2024 que establece la institucionalidad y obligaciones para la protección de infraestructuras críticas.
NERC-CIP	Critical Infrastructure Protection Standards: Estándares de seguridad obligatorios para sistemas eléctricos en Norteamérica, base técnica del estándar del CEN.
NIS2	Directiva (UE) 2022/2555: Marco regulatorio de la Unión Europea que establece un elevado nivel común de ciberseguridad en sectores estratégicos como energía.
NIST CSF	Cybersecurity Framework: Marco de gestión de riesgos desarrollado por el NIST de EE. UU. basado en identificar, proteger, detectar, responder y recuperar.
NTSyCS	Norma Técnica de Seguridad y Calidad de Servicio: Marco regulatorio que establece las exigencias mínimas para la operación segura del sistema eléctrico.
OIV	Operador de Importancia Vital: Entidades calificadas por la ANCI que requieren un régimen de supervisión reforzada por su impacto sistémico.
OPEX	Operational Expenditure: Gastos operativos y de mantenimiento continuo, incluyendo licenciamientos y servicios de monitoreo (SOC).
PLC	Programmable Logic Controller: Computadora digital industrial que ejecuta la lógica de control local sobre los procesos físicos.

RPTD N° 17	Pliego Técnico Normativo N° 17: Normativa de la SEC que regula la gestión de integridad de las instalaciones eléctricas (SGIIE).
SCADA	Supervisory Control and Data Acquisition: Sistemas informáticos para el control y supervisión a distancia de procesos industriales en tiempo real.
SEC	Superintendencia de Electricidad y Combustibles: Organismo fiscalizador de la seguridad y calidad del suministro de energía y combustibles en Chile.
SGIIE	Sistema de Gestión de Integridad de Instalaciones Eléctricas: Conjunto de actividades sistemáticas para controlar riesgos de accidentes e incidentes en activos eléctricos.
SGSI	Sistema de Gestión de Seguridad de la Información: Marco organizacional para gestionar los riesgos cibernéticos, mandatado por el Art. 8 de la Ley 21.663.
SOC	Security Operations Center: Centro responsable de la monitorización continua y la defensa activa de la infraestructura lógica.
XX-CAPV	Relación CAPEX / Valorización: Indicador económico del SGIIE que mide la inversión anual efectiva en renovación y mejora de activos.
XX-CIAC	Cantidad de Incidentes de Activos Críticos: Métrica del SGIIE que cuantifica averías e incidentes lógicos en activos esenciales.
XX-CPMP	Cumplimiento del Plan de Mantenimiento Preventivo: Relación entre HH ejecutadas vs planificadas, integrando tareas de <i>hardening</i> y parcheo.
XX-OPEV	Relación OPEX / Valorización: Indicador económico del SGIIE que refleja el gasto operacional real incurrido para mantener la integridad.
XX-TICB	Tasa de Investigación de Causas Basales: Proporción de incidentes sometidos a análisis de causa raíz (RCA) según el estándar IEC 62740.

1. INTRODUCCIÓN Y MARCO DE CONTEXTO

El suministro eléctrico constituye el pilar fundamental sobre el cual se sustenta el desarrollo económico y social de la nación, actuando como la “**infraestructura de infraestructuras**” de la que dependen otros sectores vitales como las telecomunicaciones, el transporte, la salud y el abastecimiento de agua potable. Debido a esta interdependencia funcional, cualquier perturbación significativa en el sistema eléctrico nacional tiene el potencial de desencadenar efectos en cascada que podrían paralizar la actividad productiva y comprometer la seguridad nacional. En este escenario, la progresiva integración de tecnologías digitales, sistemas de control remoto y redes inteligentes ha incrementado la eficiencia operativa, pero simultáneamente ha generado nuevas vulnerabilidades frente a amenazas cibernéticas.

A nivel internacional, distintos incidentes han demostrado que los ciberataques a infraestructuras energéticas no constituyen un riesgo teórico, sino una amenaza real con consecuencias materiales. Los ataques al sistema eléctrico de Ucrania (2015–2016) [1] y el caso del ataque de *ransomware* a **Colonial Pipeline** [2] en Estados Unidos (2021) evidenciaron que un incidente digital puede suspender operaciones críticas y forzar una respuesta de emergencia estatal. Estos eventos marcaron un punto de inflexión en la forma en que los Estados y los reguladores abordan la protección de infraestructuras críticas, impulsando un endurecimiento de los marcos regulatorios y de los requerimientos de seguridad para operadores del sector energético.

En América Latina, el contexto resulta igualmente desafiante. Informes de **Fortinet** [3] y **Check Point Research** [4], identifican a la región entre las más afectadas por el aumento de ataques cibernéticos al sector energético, en un escenario de convergencia IT/OT y brechas de madurez en ciberseguridad industrial. Además de lo anterior, el aumento de la dependencia tecnológica en todos los sectores productivos de la economía ha impulsado la necesidad de una regulación robusta en materia de ciberseguridad. En Chile, esta respuesta regulatoria se ha construido en etapas: ya en 2018 y 2019 la Superintendencia de Electricidad y Combustibles (SEC) mandató al Coordinador Eléctrico Nacional (CEN) a establecer requisitos mínimos de ciberseguridad para el sistema eléctrico, dando origen al Estándar de Ciberseguridad del CEN [5]. Este avance normativo en materia de ciberseguridad se consolidó posteriormente en abril de 2024 con la promulgación de la **Ley Marco de Ciberseguridad (Ley N.º 21.663)** [6], la cual establece los principios, organismos e instrumentos para proteger las infraestructuras críticas de información, y se complementará con una tercera iniciativa aún en desarrollo: la Norma Técnica de Ciberseguridad de la Comisión Nacional de Energía (CNE).

Sin embargo, al tratarse de una ley reciente, aún existen **desafíos importantes en**

su implementación. Parte de la normativa técnica complementaria está en desarrollo, y no se dispone de una metodología establecida que permita estimar el esfuerzo económico que su cumplimiento impone a los operadores. En el sector eléctrico, la diversidad tecnológica plantea diferencias en cuanto a exposición a riesgos y costos de cumplimiento, lo que genera incertidumbre sobre la proporcionalidad económica de las medidas exigidas por la ley – incertidumbre que, a la fecha, no cuenta con una herramienta cuantitativa que permita dimensionarla.

Desde la perspectiva de la **economía energética**, la ciberseguridad constituye una exigencia normativa con implicancias económicas concretas y permanentes: la implementación de controles técnicos OT genera inversiones de capital (CAPEX) y gastos operativos (OPEX) que se incorporan estructuralmente al costo de operación de las instalaciones. Cuantificar ese esfuerzo económico de forma comparable entre tecnologías y tipologías de central es el problema que esta investigación aborda.

A partir de este contexto, la presente investigación busca proponer un marco metodológico cuantitativo orientado a estimar el esfuerzo económico que impone el cumplimiento de la Ley 21.663, sus reglamentos y otros instrumentos sectoriales como el Estándar de Ciberseguridad CEN sobre los operadores del sector de generación eléctrica, diferenciando ese esfuerzo por tipología de central y expresándolo en métricas comparables con los indicadores de gestión de activos del sector. Este enfoque permitirá avanzar hacia una comprensión más integral del impacto de la ley, fortaleciendo la discusión sobre la sostenibilidad regulatoria y la gobernanza de la ciberseguridad en el sistema eléctrico nacional.

En síntesis, la investigación se plantea como un estudio que une la **economía energética** con la **gestión de riesgos tecnológicos**, contribuyendo a responder una pregunta central: **¿Cuál es el impacto económico que el cumplimiento de la Ley 21.663 impone sobre los operadores del sector de generación eléctrica chileno, y es ese impacto proporcional y consistente entre las distintas tipologías de central que componen el parque generador nacional?**

Para responder esta pregunta, el presente trabajo avanza desde la caracterización del SEN como infraestructura crítica (Cap. 4), pasando por el marco regulatorio y su integración con la gestión de activos (Cap. 5, OE1–OE2), su contraste con estándares internacionales e identificación de brechas (Cap. 6, OE3–OE4), para finalizar en la contribución principal de esta investigación, presentando el modelo de Costo Anualizado de Cumplimiento, instrumento metodológico que traduce las obligaciones regulatorias en drivers de costo trazables, diferenciados por tipología de central (Cap. 7, OE5), que sustentan la discusión y las conclusiones finales (Cap. 8 y 9).

2. OBJETIVOS

2.1 Objetivo General

Evaluar la coherencia regulatoria y el impacto económico de la Ley Marco de Ciberseguridad (Ley N° 21.663) en su aplicación al sector de generación eléctrica chileno, mediante un análisis enfocado en la protección de la infraestructura crítica física, integrando un estudio normativo comparado y la formulación de un marco metodológico para la estimación de los costos de cumplimiento regulatorio.

2.2 Objetivos Específicos

2.2.1 Analizar el marco normativo de la Ley Marco de Ciberseguridad (Ley 21.663) y sus reglamentos complementarios

Desglosar las exigencias que la Ley 21.663 impone a los operadores del sector de generación eléctrico en materia de gobernanza, gestión de incidentes, reportabilidad, continuidad operativa y protección de infraestructura crítica; identificando las competencias de las entidades responsables (ANCI, CSIRT, ministerios sectoriales). Este análisis buscará establecer una base conceptual sobre la cual se caracterizará el alcance regulatorio del marco y su coherencia con las políticas públicas existentes.

2.2.2 Analizar cómo los requerimientos de ciberseguridad establecidos en la Ley 21.663 se integran en los sistemas de gestión de activos del sector generación eléctrica

Analizar cómo los requerimientos de ciberseguridad de la Ley 21.663 se articulan con el Sistema de Gestión de Integridad de Instalaciones Eléctricas (Decreto Supremo 109/2017, Pliego Técnico Normativo RPTD N° 17), contrastando los requisitos de integridad, mantenimiento y confiabilidad del RPTD N° 17 con las obligaciones de protección, detección, monitoreo, reporte y respuesta ante incidentes previstas en la Ley, con el objetivo de identificar convergencias, tensiones, y brechas normativas que puedan limitar una implementación coherente de ambos marcos sobre los Ciber Sistemas SEN de generación.

2.2.3 Comparar la Ley 21.663 con los principales estándares internacionales de ciberseguridad industrial y marcos jurídicos equivalentes

Realizar un análisis comparativo detallado entre el marco regulatorio chileno de ciberseguridad aplicable al sector de generación eléctrica y los marcos internacionales de naturaleza equivalente, adoptando un enfoque metodológico

dual: en el eje legal, mediante la comparación con la Directiva NIS2 de la Unión Europea y la Resolución Normativa ANEEL N°964 de Brasil; en el eje técnico, mediante el contraste del Estándar de Ciberseguridad del Coordinador Eléctrico Nacional (Estándar CEN) con las normas NERC-CIP (su fuente directa) y la serie IEC 62443 como referente OT alternativo de alcance multisectorial. El objetivo es determinar el grado de coherencia del marco chileno respecto de las mejores prácticas internacionales en los dominios críticos de seguridad OT.

2.2.4 Identificar y clasificar brechas regulatorias y técnicas que puedan limitar la efectividad de la ley en el contexto del sector de generación eléctrica

Construir una matriz de correspondencia normativa (Gap Analysis) que relacione los requerimientos del marco regulatorio chileno de ciberseguridad — compuesto por la Ley N.º 21.663 y el Estándar de Ciberseguridad del Coordinador Eléctrico Nacional — con los controles específicos de los estándares internacionales de referencia, diferenciando las brechas según las particularidades tecnológicas y operativas de las distintas fuentes de generación. Las brechas se clasifican según impacto operativo y su criticidad de implementación; el resultado será la identificación de vacíos normativos, solapamientos y posibles áreas de mejora en la implementación nacional.

2.2.5 Desarrollar un modelo de estimación de costos de cumplimiento normativo.

Elaborar un modelo económico que cuantifique los esfuerzos requeridos para cumplir con las obligaciones regulatorias de ciberseguridad derivadas de la Ley 21.663 y el Estándar CEN, que contemple tanto inversiones iniciales (CAPEX) como costos operativos (OPEX) derivados de la adopción, mantenimiento y monitoreo de los sistemas de ciberseguridad. Este modelo buscará establecer el Costo Anualizado de Cumplimiento (CAC), desagregado por tipo de central generadora, considerando factores como nivel de automatización y criticidad de los procesos.

El objetivo es proporcionar una estimación comparativa, y sus rangos de sensibilidad, del esfuerzo económico requerido para cumplir y mantener los niveles de seguridad exigidos por la normativa.

3. ESTADO DEL ARTE

3.1 Ciberseguridad en infraestructuras críticas del sector eléctrico

La operación de los sistemas eléctricos modernos depende de forma estructural de infraestructuras digitales de control, supervisión y comunicación, tales como sistemas SCADA, DCS, sistemas de protección, telecomunicaciones operativas y plataformas de despacho. Esta dependencia convierte al sistema eléctrico en una infraestructura crítica de naturaleza ciberfísica, donde los incidentes de ciberseguridad pueden materializarse en impactos físicos, económicos y sociales significativos.

La literatura especializada coincide en que la ciberseguridad en infraestructuras críticas ha evolucionado desde un enfoque voluntario basado en buenas prácticas hacia regímenes regulatorios obligatorios, particularmente en sectores energéticos considerados estratégicos para la seguridad nacional y la continuidad del suministro. En este contexto, la ciberseguridad deja de ser un problema exclusivamente tecnológico y se consolida como un problema regulatorio y organizacional. No obstante, esta convergencia normativa no ha ido acompañada, en la misma medida, por el desarrollo de metodologías económicas estandarizadas que permitan estimar de manera estructurada el costo del cumplimiento regulatorio.

3.2 Enfoques regulatorios internacionales en ciberseguridad eléctrica

3.2.1 Norteamérica: el estándar NERC-CIP

En Estados Unidos y Canadá, la ciberseguridad del sistema eléctrico se regula mediante los Critical Infrastructure Protection Standards (NERC-CIP), desarrollados por la North American Electric Reliability Corporation y aprobados por la Federal Energy Regulatory Commission. Este conjunto de estándares constituye el marco sectorial más específico y prescriptivo existente a nivel internacional para la protección cibernética del sistema eléctrico. Su particularidad es incorporar de forma explícita requisitos de protección física además de ciberseguridad —a diferencia de NIS2, IEC 62443 o NIST CSF, que tratan la seguridad física solo como principio general—, clasificando los activos según su impacto potencial sobre la confiabilidad del sistema y definiendo controles proporcionales a ese impacto.

3.2.2 Unión Europea: la Directiva NIS2

En la Unión Europea, la evolución regulatoria culmina con la promulgación de la Directiva (UE) 2022/2555 (NIS2), que amplía significativamente el alcance de la Directiva NIS original. NIS2 incorpora explícitamente al sector energía —incluida la

generación eléctrica— dentro del conjunto de sectores esenciales, sujetos a obligaciones reforzadas de gestión de riesgos y reporte de incidentes.

Uno de los aportes conceptuales más relevantes de NIS2 es la introducción explícita del principio de proporcionalidad, estableciendo que las medidas de ciberseguridad deben ser adecuadas considerando el nivel de riesgo, el tamaño de la entidad y el costo de implementación. No obstante, la directiva no define métricas operativas para materializar esta proporcionalidad, delegando su aplicación a los Estados miembros.

El Informe ENISA – NIS Investments 2024, que analiza la inversión en ciberseguridad de 1.350 organizaciones europeas, indica que la ciberseguridad representa aproximadamente el 9 % del presupuesto total de TI (Ilustración 1), sin desagregar entre entornos IT y OT ni distinguir al subsector de generación eléctrica.

Figure 19: Information security spending by NIS 2 sector

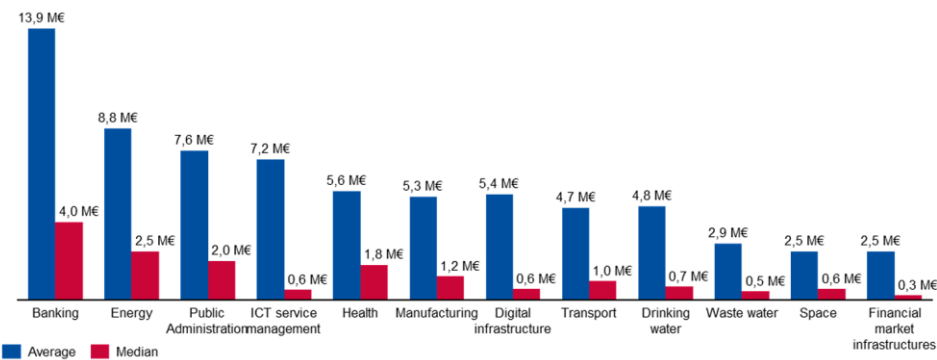


Ilustración 1. Evolución del gasto en ciberseguridad como % del presupuesto TI en sectores críticos europeos [7]

3.2.3 América Latina: el caso de Brasil como referente sectorial

En América Latina, Brasil constituye el caso más avanzado y estructurado en materia de regulación de ciberseguridad aplicada específicamente al sector eléctrico. La Resolução ANEEL n.º 964/2021, establece las directrices y el contenido mínimo de las políticas de seguridad cibernética para los agentes del sector eléctrico, complementada por la Rotina Operacional RO-CB.BR.01 del Operadora Nacional do Sistema Eléctrico (ONS).

3.3 Evolución del marco normativo de ciberseguridad en Chile

La arquitectura legal de la ciberseguridad en Chile no surgió de forma aislada, sino que es el resultado de un proceso de maduración institucional que transitó desde la voluntad política hacia la exigencia técnica sectorial, culminando en la actual gobernanza nacional consolidada.

3.3.1 Antecedente de gobernanza y sensibilización institucional

La génesis de la política pública en esta materia se remonta a 2015, con el Decreto 533 [8], que creó el primer Comité Interministerial sobre Ciberseguridad. Dentro de esta etapa de preparación, se sitúa la Ley N.º 21.113, promulgada en 2018, que declara el mes de octubre como el Mes Nacional de la Ciberseguridad. Esta ley no constituye un hito regulatorio, dado que carece de facultades mandatorias o regímenes sancionatorios, su valor es más de concientización, al reconocer la relevancia estratégica de la ciberseguridad y promover actividades de sensibilización y ejercicios nacionales [9].

3.3.2 Primer hito regulatorio sectorial: Estándar de Ciberseguridad del Coordinador Eléctrico Nacional

Un hito relevante a nivel sectorial es la publicación del Estándar de Ciberseguridad del Coordinador Eléctrico Nacional (CEN), vigente desde 2022, que establece exigencias técnicas obligatorias de ciberseguridad para los agentes del sistema eléctrico chileno, como adaptación del marco internacional NERC-CIP a instrucción de la Superintendencia de Electricidad y Combustibles (SEC, Oficios N.º 3.377 de 2018 y N.º 11.508 de 2019). Su diseño responde a una adaptación estratégica del marco internacional NERC-CIP, desarrollada con el apoyo técnico especializado de CAISO (California Independent System Operator) para armonizar las mejores prácticas globales con la arquitectura operativa e institucional del Sistema Eléctrico Nacional (SEN). El desarrollo de sus criterios de categorización de impacto, controles técnicos y mecanismos de auditoría se abordará en el capítulo de marco regulatorio.

3.3.3 Consolidación normativa: Ley Marco de Ciberseguridad

La promulgación de la Ley N.º 21.663, en 2024, marca el punto de inflexión en la gobernanza de la ciberseguridad en Chile. Esta ley establece la institucionalidad nacional, crea la Agencia Nacional de Ciberseguridad (ANCI) y define obligaciones generales para prestadores de servicios esenciales y Operadores de Importancia Vital (OIV), categoría en la que puede clasificarse la generación eléctrica.

La ley introduce obligaciones reforzadas de gestión de riesgos, continuidad operacional, reporte de incidentes y auditorías, junto con un régimen sancionatorio significativo.

La evolución normativa y los principales hitos que estructuran este marco regulatorio se sintetizan en la Tabla 1.

Tabla 1. Principales hitos normativos de ciberseguridad en Chile (Fuente: Elaboración Propia)

Año	Instrumento	Alcance
2015	Decreto N° 533	Génesis de gobernanza política: Creación del primer comité interministerial sobre ciberseguridad, sentando las bases para la Política Nacional
2018	Ley N° 21.113	Antecedente de sensibilización: Declaración del Mes Nacional de la Ciberseguridad; hito de carácter simbólico y cultural sin facultades mandatorias
2022	Estándar CEN	Primer hito regulatorio sectorial: Establecimiento de exigencias técnicas obligatorias basadas en la adaptación estratégica del marco NERC-CIP
2024	Ley N° 21.663	Consolidación normativa Nacional: Ley marco que crea la Agencia Nacional de Ciberseguridad (ANCI) y el régimen de responsabilidad pública reforzada.

3.3.4 Desarrollos normativos en curso en el sector eléctrico chileno

Adicionalmente al Estándar de Ciberseguridad del Coordinador Eléctrico Nacional y a la promulgación de la Ley Marco de Ciberseguridad (Ley N.º 21.663), la Comisión Nacional de Energía se encuentra desarrollando una Norma Técnica de Ciberseguridad y Seguridad de la Información para entornos OT.

Esta Norma Técnica se encuentra actualmente en proceso de elaboración conforme al Plan Normativo Anual de la CNE (ver Ilustración 2).



Estado de Procedimientos Normativos del Plan Normativo Anual

Nº	Procedimiento Normativo Plan Normativo Anual 2026 (Res. Exta. N°779 de 15/12/2025)	Resolución de inicio	Comité Consultivo	Elaboración de Proyecto de Norma	Consulta Pública	Elaboración Informe consolidado de respuestas y Norma Técnica	Fijación Norma Técnica
1	Elaboración Norma Técnica de Coordinación y Operación del Sistema Eléctrico Nacional, Capítulo Funciones de Control y Despacho.						
2	Modificación Norma Técnica de Seguridad y Calidad de Servicio.						
3	Modificación Norma Técnica de Seguridad y Calidad de Servicio: Incorporación de elementos que contribuyen a la fortaleza de la red.				(1)		(1)
4	Modificación Norma Técnica de Seguridad y Calidad de Servicio - Anexo Técnico de Información Técnica de Activos en Transmisión						
5	Modificación Norma Técnica de Conexión y Operación de PMGD				(2)		(2)
6	Norma Técnica de Ciberseguridad y Seguridad de la Información.						
7	Modificación Norma Técnica de Calidad de Servicio para Sistemas de Distribución	(3)					

Ilustración 2. Estado de Procedimiento Normativo - 6 Norma técnica de ciberseguridad y seguridad de la información (Fuente: CNE [10])

A la fecha del presente estudio, la referida Norma Técnica no ha sido sometida a consulta pública ni dictada, y por tanto no forma parte del marco regulatorio vigente, constituyendo un desarrollo normativo en curso.

3.4 Convergencia entre ciberseguridad y gestión de activos

Una tendencia relevante identificada en la literatura es la convergencia entre ciberseguridad industrial y gestión de activos físicos, particularmente bajo los principios de la norma ISO 55001 y a nivel nacional el pliego técnico RPTD N°17. En sistemas eléctricos, la indisponibilidad o manipulación de sistemas OT puede generar daños físicos, reducción de vida útil y pérdidas económicas significativas, lo que posiciona a la ciberseguridad como un componente del mantenimiento preventivo. Sin embargo, esta convergencia conceptual aún no se traduce en modelos operativos que integren de forma sistemática ciberseguridad, criticidad del activo y análisis económico, lo que constituye una oportunidad de análisis y estudio relevante.

3.5 Dimensión económica de la ciberseguridad en el sector eléctrico

Desde la perspectiva económica, la ciberseguridad en infraestructuras eléctricas puede conceptualizarse como un costo necesario para la preservación de la continuidad operativa y del valor de los activos físicos. La evidencia empírica internacional muestra que el gasto en ciberseguridad en sectores críticos es creciente y estructural, impulsado por la digitalización, la convergencia IT/OT y el aumento de amenazas dirigidas.

El informe ENISA 2024 [7] constituye una importante referencia cuantitativa, indicando que la ciberseguridad representa en promedio cerca del 9 % del presupuesto de TI en sectores críticos europeos. No obstante, no existen datos públicos que permitan cuantificar el costo específico de la ciberseguridad OT, ni desagregar estos costos por tipo de tecnología de generación o criticidad del activo.

De manera similar, ni en Estados Unidos ni en Brasil existen publicaciones oficiales que cuantifiquen el costo anualizado de cumplimiento de los estándares sectoriales. La regulación se limita a definir obligaciones técnicas y organizacionales, dejando en manos de los operadores la internalización de los costos asociados.

3.6 Vacíos de conocimiento y oportunidad de investigación

El análisis de la literatura permite identificar vacíos de conocimiento relevantes que justifican la pertinencia del presente estudio:

- Ausencia, en literatura especializada, de indicadores económicos aplicables a la ciberseguridad del sistema eléctrico chileno.
- Falta de evidencia empírica sobre los costos reales de cumplimiento para las empresas generadoras, tanto en inversión (CAPEX) como en mantenimiento (OPEX).
- Necesidad de metodologías replicables que permitan medir y comparar el impacto económico del cumplimiento normativo en el sector generación.

La presente tesis busca contribuir a llenar estos vacíos de conocimiento, respondiendo cuánto cuesta cumplir la Ley 21.663 y el Estándar CEN en el sector de generación eléctrica chileno —para lo cual desarrolla una metodología de estimación de costos que complementa el análisis normativo y técnico ya existente. Esta respuesta se limita al costo del cumplimiento; no evalúa el valor del riesgo cibernético que ese cumplimiento mitiga, comparación que requeriría datos de siniestralidad no disponibles públicamente en Chile a la fecha de este estudio.

3.7 Síntesis del estado del arte

La revisión del estado del arte permite concluir que existe un consenso técnico y regulatorio sobre la necesidad de fortalecer la ciberseguridad en el sector eléctrico, con marcos obligatorios en Norteamérica, Europa y Brasil. No obstante, también se identifica un vacío de conocimiento: la ausencia de metodologías que permitan evaluar el costo económico del cumplimiento. Este vacío es especialmente relevante en el contexto chileno, donde la coexistencia del Estándar de Ciberseguridad del Coordinador Eléctrico Nacional y la Ley 21.663 introduce nuevas exigencias técnicas cuyo costo de implementación aún no ha sido estimado en la literatura. Cerrar ese vacío de conocimiento es el propósito de la presente investigación.

4. EL SISTEMA ELÉCTRICO NACIONAL COMO INFRAESTRUCTURA CRÍTICA: FUNDAMENTO TÉCNICO DEL ESTUDIO

El presente capítulo construye el marco conceptual y técnico que sustenta el análisis que se desarrollará en los capítulos posteriores, siguiendo una secuencia que avanza desde la descripción del sistema hacia la justificación de su regulación obligatoria.

Se parte por caracterizar el sistema eléctrico chileno en su estructura, composición tecnológica y escala, describiendo los segmentos que lo conforman y los riesgos cibernéticos propios de cada uno (Sección 4.1). A continuación, se examina la criticidad sistémica del SEN y las consecuencias de una disrupción: su rol como infraestructura crítica de la información, su condición de activo estratégico, las vulnerabilidades y el apagón de 2025 (Sección 4.2).

Con ese contexto establecido, se propone una taxonomía que agrupa las instalaciones de generación en tres grupos según su arquitectura de control OT y su perfil de exposición al riesgo cibernético (Sección 4.3). Sobre esta base, se describe la evolución desde la generación analógica hacia el control digital integrado, explicando por qué esa transformación amplía la superficie de exposición (Sección 4.4), y se identifican las vulnerabilidades técnicas y vectores de ataque propios de los entornos OT, organizados en cuatro categorías (Sección 4.5).

El capítulo cierra con dos secciones. La primera presenta casos documentados de ciberataques a infraestructuras críticas tanto internacionales como nacionales, así como el caso reciente de Qilin – que demuestra que la amenaza no es hipotética sino verificable (Sección 4.6). La segunda sintetiza el argumento técnico del capítulo para fundamentar por qué la naturaleza ciberfísica del sistema eléctrico justifica la existencia de un marco regulatorio obligatorio (Sección 4.7).

4.1 Estructura y escala del Sistema Eléctrico Nacional

El Sistema Eléctrico Nacional (SEN) es la infraestructura que abastece de electricidad a aproximadamente el 99% de la población del país. Nacido en 2017 de la unificación de los antiguos Sistema Interconectado del Norte Grande (SING) y Sistema Interconectado Central (SIC), constituye un sistema único por su geografía: se extiende a lo largo de más de 3.100 kilómetros entre Arica y la Isla de Chiloé, abarcando casi la totalidad del territorio nacional [11]. Su operación se articula en cuatro segmentos funcionales encadenados, cada uno con una función técnica diferenciada y un perfil de riesgo cibernético propio.

La generación es el segmento donde la energía eléctrica se produce a partir de fuentes primarias. A inicios de 2026 el parque generador del SEN comprendía 1.164 centrales en operación y una capacidad instalada bruta superior a 39.000 MW (Ilustración 3), con un fuerte predominio de unidades solares fotovoltaicas en número (31,6% del total), seguidas por centrales termoeléctricas (30,1%), hidroeléctricas (19,8%) y parques eólicos (15,7%) [12]. Este segmento es el objeto de estudio del presente trabajo y se caracteriza por una superficie de ataque distribuida: el riesgo no se concentra en pocos activos de alto impacto, sino que se reparte en un parque numeroso y tecnológicamente heterogéneo, en el que la creciente digitalización de las centrales renovables —inversores, controladores y plataformas de monitoreo remoto— amplía la exposición agregada del sistema.

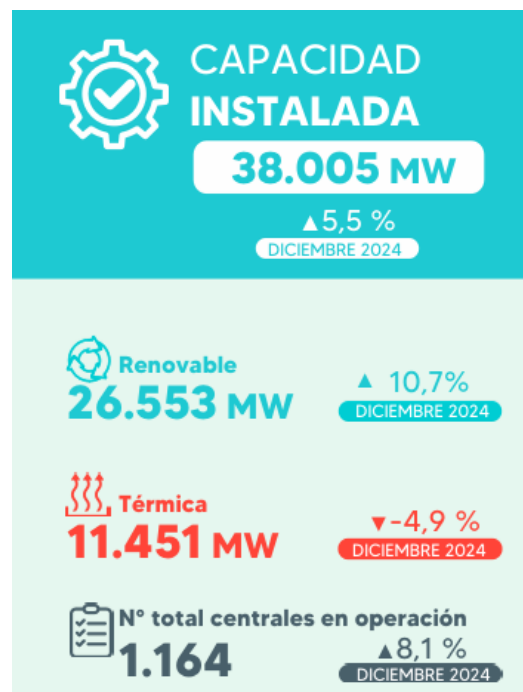


Ilustración 3. Capacidad instalada en Chile y Total de Centrales (Ene 2026) (Fuente: Generadora.cl)

La transmisión transporta la energía desde los centros de generación hasta los de consumo mediante líneas de alta tensión. El sistema de transmisión del SEN comprende más de 38.000km [13] y 1.256 subestaciones [14], siendo el nivel de 220 kV el de mayor extensión acumulada, complementado por un eje troncal en 500 kV que vertebra el sistema en sentido norte-sur [15]. Aunque la transmisión queda fuera del alcance metodológico de este estudio, su mención es indispensable: por su topología longitudinal con redundancia limitada en varios tramos, este segmento concentra el riesgo sistémico del SEN lo que permite dimensionar la escala completa del sistema.

La distribución entrega la energía al consumidor final, reduciendo la tensión a niveles de media y baja tensión mediante subestaciones de transición y redes locales. A 2023, las empresas distribuidoras del país concentraban más de 7,3 millones de clientes regulados – el 97% de los usuarios regulados del país – y operaban 182.000 kilómetros de redes de distribución [16]. Es el segmento con mayor número de puntos de conexión y, por tanto, con la mayor superficie de exposición en términos de dispositivos, aunque el impacto individual de cada uno es acotado. Este segmento queda fuera del alcance de este estudio.

Los grandes consumos corresponden a clientes industriales y mineros conectados directamente a la red de alta tensión, sin intermediación de empresas distribuidoras.

En Chile, la minería del cobre representa una fracción significativa de la demanda eléctrica total, lo que convierte la continuidad del suministro en un factor crítico no solo para los hogares sino para la principal actividad exportadora del país.

Esta cadena opera de forma interdependiente y coordinada en tiempo real por el Coordinador Eléctrico Nacional. La Tabla 2 resume esta estructura y el alcance de cada segmento en el presente estudio.

Tabla 2. Segmentos del SEN: función y perfil de riesgo cibernético (Fuente: Elaboración Propia)

Segmento	Función técnica	Escala (2025)	Perfil de riesgo cibernético	Alcance en este estudio
Generación	Producción de energía	1.164 centrales; 39.000 MW	Superficie distribuida; digitalización creciente en ERV	Objeto de estudio
Transmisión	Transporte en alta tensión	38.000 km, 1256 subestaciones	Riesgo sistémico concentrado; topología longitudinal	Fuera de alcance (se menciona)
Distribución	Entrega a tensión media/baja	7,3 millones de clientes regulados, 182.000km de redes	Mayor número de puntos; impacto individual acotado	Fuera de alcance
Grandes consumos	Demanda industrial/minera directa	Minería ≈ alta fracción de demanda	Dependencia crítica de continuidad	Fuera de alcance

4.2 Criticidad Sistémica y consecuencias de una interrupción

El concepto de infraestructura crítica ha adquirido una creciente relevancia en el contexto de la seguridad nacional y la resiliencia de los sistemas modernos, particularmente en aquellos sectores cuya operación resulta esencial para el funcionamiento de la sociedad. En términos generales, la infraestructura crítica se define como el conjunto de instalaciones, sistemas y activos cuya interrupción o destrucción tendría un impacto significativo en la seguridad, la economía, la salud pública o el bienestar de la población [17]. El sector eléctrico chileno adopta este concepto de forma operacional a través del Estándar de Ciberseguridad del CEN, cuyo desarrollo y criterios de clasificación se abordarán más adelante.

Dentro de las diversas verticales de infraestructuras críticas (telecomunicaciones, transporte, agua potable, salud, entre otras), el sistema eléctrico ocupa una posición singular: a diferencia de otros sectores que dependen entre sí de manera parcial o indirecta, el suministro eléctrico es condición necesaria para la operación de prácticamente todos los demás sectores estratégicos, de modo que una

perturbación significativa en el sistema eléctrico desencadena efectos en cascada que se propagan simultáneamente por múltiples sectores, amplificando el impacto inicial del evento [18]. Por esta interdependencia funcional, el SEN constituye la “infraestructura de infraestructuras”, condición que sitúa su protección más allá del ámbito sectorial e inscribe su continuidad operativa directamente en la política de seguridad del Estado.

4.2.1 La transición hacia la infraestructura crítica de la información

Históricamente, la protección de la infraestructura eléctrica se centraba en la seguridad física (perímetros, subestaciones, torres). Sin embargo, la digitalización ha transformado al SEN en una Infraestructura Crítica de la Información (ICI). Esta interdependencia entre componentes físicos y digitales configura al sistema eléctrico como una infraestructura de carácter ciberfísico, cuya seguridad requiere un enfoque integral.

4.2.2 El SEN como activo estratégico

El reconocimiento jurídico de esta condición estratégica quedó formalizado con la Ley N.º 21.663, cuyo procedimiento de calificación de Operadores de Importancia Vital (OIV) culminó su primera etapa con la Resolución Exenta N.º 87 de la Agencia Nacional de Ciberseguridad, publicada el 17 de diciembre de 2025. De las 915 instituciones calificadas como OIV en esta primera etapa, 147 corresponden a empresas del sector eléctrico, el grupo sectorial más numeroso de la nómina [19]. La generación distribuye el riesgo en un parque numeroso y tecnológicamente heterogéneo: la criticidad individual de cada central es menor que la de un activo de transmisión, pero la superficie de ataque agregada es mayor y diversa.

4.2.3 Vulnerabilidades estructurales y geopolíticas

Además de su condición de infraestructura crítica, el SEN presenta cuatro características estructurales relevantes para su perfil de exposición.

La **primera** es la geografía longitudinal y la concentración de la transmisión. El SEN se extiende por más de 3.100 kilómetros entre Arica y Chiloé, articulado sobre ejes troncales en 500 kV y 220 kV que recorren el país en sentido norte-sur con redundancia limitada en varios tramos [15]. Esta topología implica que la desconexión de un número reducido de elementos puede separar el sistema en islas eléctricas, como quedó demostrado empíricamente el 25 de febrero de 2025 (ver sección 4.2.4). La **segunda** es la concentración geográfica de la generación por tecnología. La generación solar fotovoltaica se concentra en el Norte Grande y el Norte Chico; la hidroeléctrica de embalse, en la zona centro-sur. Esta especialización geográfica, eficiente desde la lógica de mercado, implica que una disrupción regional compromete la diversificación de la matriz como mecanismo de

resiliencia. La **tercera** es la dependencia de combustibles importados. La generación térmica, depende de gas natural licuado y carbón importados por vía marítima. En un escenario de disrupción de las cadenas logísticas internacionales, la capacidad de respaldo del sistema queda condicionada por la seguridad de las rutas marítimas y los terminales de regasificación. La **cuarta** es la digitalización acelerada del parque generador. La transición hacia una matriz dominada por energías renovables variables —con la consecuente multiplicación de inversores, controladores y plataformas de monitoreo remoto, frecuentemente gestionadas por proveedores externos— amplía la superficie de ataque cibernético precisamente en el segmento de mayor crecimiento del sistema.

Estas cuatro características configuran el perfil de exposición que la institucionalidad de ciberseguridad busca mitigar.

4.2.4 El apagón del 25 de febrero de 2025

El 25 de febrero de 2025, el SEN experimentó el apagón más extenso de su historia reciente. Aunque su origen no fue un ciberataque, el evento sirve para dimensionar las consecuencias de una disrupción sistémica y la relevancia operacional de los sistemas de protecciones, SCADA y comunicaciones durante la recuperación.

El Estudio de Análisis de Falla (EAF) remitido por el CEN a la SEC en marzo de 2025 reveló que el evento se originó por una intervención no informada ni autorizada sobre un sistema de protecciones de una subestación [20], lo que provocó e n segundos la separación del sistema en islas eléctricas que no lograron mantener su estabilidad y colapsaron en un apagón total.

Un elemento del EAF es directamente relevante para este estudio, el proceso de recuperación del servicio enfrentó dificultades por fallas en los sistemas SCADA y de comunicaciones, lo que evidencia que la dependencia de los sistemas de telecontrol condiciona no solo la operación normal sino también la capacidad de recuperación tras una contingencia. El apagón del 25F sirve para dimensionar las consecuencias sistémicas que puede tener la manipulación no autorizada de los elementos de control de un sistema.

4.3 Agrupación tecnológica para el análisis metodológico

La diversidad tecnológica presente en la infraestructura de generación eléctrica no solo se manifiesta a nivel de los activos físicos de potencia, sino también en las arquitecturas de control y supervisión. Estas arquitecturas responden a las características dinámicas del proceso, al tipo de tecnología empleada y a los requerimientos de integración con el sistema eléctrico, dando lugar a configuraciones de control sustancialmente distintas entre sí.

Con el objetivo de estructurar el análisis y facilitar la identificación de patrones

comunes, resulta pertinente agrupar las instalaciones de generación en **familias de arquitectura de control**, atendiendo a criterios técnicos tales como el grado de inercia del proceso, el nivel de centralización del control, la dependencia de electrónica de potencia y el rol de la instalación en la interfaz con el sistema eléctrico. En este marco, se propone la siguiente taxonomía técnica.

4.3.1 Grupo A: Electrónica de potencia distribuida (Solar PV, Eólica)

Este grupo corresponde a instalaciones cuya operación se basa fundamentalmente en **electrónica de potencia distribuida**, sin acoplamiento directo a máquinas síncronas tradicionales. La conversión y control de la energía se realiza mediante **inversores**, los cuales permiten regular de forma rápida y precisa la potencia activa y reactiva inyectada al sistema.

Este grupo se caracteriza por la fragmentación del activo de potencia en cientos o miles de unidades menores (inversores o aerogeneradores) coordinadas digitalmente por un único PPC (Power Plant Controller), así como por el uso de protocolos abiertos estandarizados como Modbus, TCP, DNP3, entre otros.

4.3.2 Grupo B: Procesos de Alta Inercia y DCS Propietario (Centrales térmicas e hidroeléctricas)

El segundo grupo agrupa instalaciones basadas en **procesos físicos de alta inercia**, con ciclos termodinámicos o hidráulicos cerrados y máquinas rotatorias de gran escala. En este caso, la dinámica del proceso está dominada por fenómenos mecánicos y energéticos de mayor constante de tiempo, lo que se traduce en esquemas de control más centralizados y fuertemente acoplados al proceso físico. Son plantas que operan con máquinas rotatorias sincrónicas de gran tamaño, donde la estabilidad física depende de un control milimétrico de variables termodinámicas y mecánicas. Las arquitecturas de control típicas de este grupo se apoyan en **Sistemas de Control Distribuido (DCS)** o en sistemas de control centralizado, los cuales integran la regulación de variables del proceso con la supervisión operativa y las funciones de protección.

4.3.3 Grupo C: Infraestructura de interconexión (Subestaciones y SMMC)

El tercer grupo corresponde a las arquitecturas de control asociadas a la **interfaz entre la generación y el sistema eléctrico**, incluyendo subestaciones elevadoras, patios de maniobra, sistemas de protección, control y medición comercial. Si bien estos activos no generan energía propiamente tal, su operación resulta indispensable para la inyección segura y confiable de la potencia generada al sistema.

El grupo de taxonomía propuesta plantea que las diferencias entre grupos no son solo tecnológicas sino que determinan perfiles de riesgo cibernético diferenciadas. Para ilustrar esta taxonomía en adelante se ocuparan los grupos A/B/C como se muestran en la Tabla 3.

Tabla 3. Tabla Síntesis de la taxonomía técnica por grupo: arquitectura, perfil de riesgo y cumplimiento (Fuente: Elaboración Propia)

Grupo	Tipo de tecnología	Arquitectura de control	Perfil de riesgo cibernético	Dependencia OT
A	Solar, eólica	Electrónica de potencia distribuida	Alta granularidad, protocolos abiertos, riesgo concentrado en PPC	Muy alta
B	Térmica, hidráulica	Procesos físicos de mayor inercia, Control Distribuido	DCS propietario, ciclos de parcheo lentos, riesgo cinético en TCS	Media
C	Subestaciones, SMMC, Interconexión	Protección e interconexión	IED con decisiones físicas inmediatas, mayor impacto sistémico	Alta

4.4 De la digitalización a la exposición: por qué surge la vulnerabilidad

Las secciones anteriores establecieron qué se protege (el SEN como sistema y como activo estratégico) y por qué importa (su criticidad para la seguridad nacional). Esta sección y la siguiente abordan la pregunta complementaria: ¿contra qué se protege? El punto de partida es que la superficie de ataque cibernético del sistema eléctrico no es una condición preexistente, sino el resultado directo de su evolución tecnológica. La progresiva digitalización del control de la generación —que aporta eficiencia, monitoreo remoto y coordinación en tiempo real— es exactamente el mismo proceso que introduce los vectores de riesgo que no existían en la generación analógica. Comprender esa evolución es, por tanto, el requisito para comprender la amenaza.

Históricamente, estas instalaciones operaban de manera predominantemente analógica y manual: los operadores supervisaban el proceso físico in situ y ejecutaban acciones de control mediante instrumentación local. Esta condición los hacía robustos frente a amenazas externas, pero también imponía restricciones operativas significativas.

Hoy en día se puede afirmar que toda tecnología de generación actual opera bajo controles digitales, impulsada por la necesidad de integración operativa, control

remoto, reporte de datos de proceso a niveles gerenciales, entre otras necesidades. Esta misma digitalización ha introducido una superficie de ataque que no existía en la generación analógica.

Lo que hace a estos sistemas relevantes para esta investigación no es su descripción técnica, sino su consecuencia operacional: una señal digital errónea — ya sea por falla o por manipulación deliberada — puede traducirse en una acción física sobre la infraestructura. Esta naturaleza ciberfísica es la que convierte a los sistemas OT en vectores de riesgo con consecuencias materiales.

La Cybersecurity and Infrastructure Security Agency (CISA) [21] señala que los sistemas de control industrial fueron históricamente diseñados con un enfoque en la disponibilidad y seguridad operativa, pero no necesariamente en la ciberseguridad. Esta brecha de diseño – combinada con la convergencia IT/OT – configura la superficie de exposición que se organiza a continuación.

4.5 Vulnerabilidades técnicas y vectores de ataques en entornos OT

La arquitectura de control descrita en la sección anterior introduce vulnerabilidades técnicas que los atacantes pueden explotar. Esta sección organiza esas vulnerabilidades en cuatro categorías que agrupan los vectores de ataque documentados contra infraestructura eléctrica según su naturaleza.

- **Acceso y Conectividad:** La convergencia IT/OT eliminó el aislamiento físico que históricamente protegía a los sistemas de control, habilitando accesos remotos para mantenimiento y conexiones desde la red corporativa hacia la red de control. El movimiento lateral desde la red IT comprometida hacia la red OT constituye el patrón más recurrente en los incidentes documentados: el atacante rara vez ingresa directamente al sistema de control, sino que escala desde un punto de entrada corporativo de menor protección.
- **Cadena de suministro tecnológica:** Los entornos OT dependen de un número reducido de fabricantes de sistemas de control, lo que concentra el riesgo: un componente, firmware o actualización comprometido en origen puede afectar simultáneamente a múltiples instalaciones que comparten el mismo proveedor. Esta categoría es particularmente relevante en Chile, dada la alta concentración de proveedores de inversores en la generación solar y eólica.
- **Factor humano e ingeniería social:** El componente humano es, de forma transversal, el vector de entrada más explotado: phishing dirigido, suplantación de identidad, ofertas laborales falsas, y el uso de medios removibles permiten obtener credenciales o accesos legítimos sin necesidad de vulnerar el sistema por la fuerza, lo que además dificulta su detección posterior.
- **Arquitectura heredada y protocolos expuestos:** Muchos sistemas OT

fueron diseñados para operar en entornos aislados y carecen de mecanismos nativos de autenticación o cifrado. Los protocolos industriales de uso extendido (Modbus, DNP3, IEC 60870-5-104, IEC 61850) transmiten comandos sin verificación de origen ni integridad, lo que permite a un atacante con acceso a la red inyectar instrucciones que el sistema ejecutará como legítimas. A esto se suma el ciclo de vida prolongado de los activos OT, que mantiene en operación equipos con vulnerabilidades conocidas durante años.

Estas cuatro categorías no son hipótesis teóricas: cada una ha sido explotada en ataques reales contra infraestructura eléctrica. La sección siguiente examina los casos documentados que materializaron estos vectores y demuestran su capacidad de producir consecuencias físicas.

4.6 Casos documentados de ciberataques a infraestructura crítica

Las vulnerabilidades descritas en las secciones anteriores no son hipótesis teóricas: han sido explotadas en ataques reales con consecuencias físicas verificables. Esta sección examina algunos casos documentados con atribución pública documentada.

4.6.1 Ucrania 2015 y 2016: materialización del riesgo ciberfísico en el sector eléctrico

El 23 de diciembre de 2015, tres empresas de distribución eléctrica ucranianas sufrieron un ataque coordinado que dejó sin suministro a aproximadamente 230.000 personas durante un período de una a seis horas. Constituye el primer corte de suministro eléctrico causado por un ciberataque reconocido públicamente [22]. Los atacantes comprometieron las redes corporativas de las distribuidoras al menos seis meses antes del evento, mediante una campaña de spear-phishing con documentos de Microsoft Office que contenían el malware **BlackEnergy**. Desde ese punto de apoyo escalaron hacia las redes de control, obtuvieron credenciales legítimas y, el día del ataque, tomaron control remoto de los sistemas SCADA para abrir manualmente los interruptores de aproximadamente 30 subestaciones. El ataque incluyó tres componentes coordinados: el acceso remoto a los SCADA, un ataque de denegación de servicio a los centros de atención telefónica para impedir que los clientes reportaran los cortes, y el malware **KillDisk**, que borró los discos de los servidores para retrasar la recuperación [22].

Un año después, el 17 de diciembre de 2016, la subestación de transmisión Pivnichna, operada por Ukrenergo al norte de Kiev, sufrió un corte que dejó sin suministro a aproximadamente una quinta parte de la ciudad durante alrededor de

una hora. Aunque la interrupción fue más breve que la de 2015, su importancia técnica es mayor: fue ejecutada mediante el primer malware diseñado específicamente para manipular de forma autónoma los protocolos de comunicación de subestaciones eléctricas [23]. A diferencia del ataque de 2015, que requirió operadores humanos manipulando los SCADA, Industroyer incorpora de forma nativa protocolos industriales lo que le permitió controlar directamente interruptores y relés sin intervención humana directa.

Ambos casos, atribuidos al grupo Sandworm, muestran una progresión relevante: del acceso por factor humano y manipulación manual de SCADA (2015), a un malware capaz de interactuar de forma autónoma con protocolos industriales (2016).

4.6.2 Antecedentes chilenos y regionales en sectores críticos no eléctricos

Si bien Chile no registra a la fecha ciberataques que hayan provocado cortes de suministro eléctrico, sí existen antecedentes documentados en otros sectores críticos. En mayo 2018, el un ataque al **Banco de Chile**, atacantes del grupo **Lazarus** sustrajeron aproximadamente USD 10 millones a través de la manipulación del sistema de transferencias internacionales SWIFT, utilizando un malware destructivo (KillIMBR) como distracción para encubrir las transferencias fraudulentas.

En septiembre de 2022, el grupo de hacktivismo **Guacamaya** comprometió sistemas del Estado Mayor Conjunto de la Defensa Nacional, filtrando aproximadamente 400.000 correos electrónicos, en una operación que afectó simultáneamente a instituciones militares de otros cuatro países de la región [24].

4.6.3 Qilin y ransomware reciente contra entidades estratégicas en Chile

El antecedente más reciente es de enero de 2026: el CSIRT Nacional de la ANCI emitió la Alerta de Incidente en Curso AIC26-00002, advirtiendo un incidente de efecto significativo en una entidad estratégica del país perteneciente a la nómina de Operadores de Importancia Vital (OIV) o Prestadores de Servicios Esenciales (PSE), sin especificar la entidad afectada. El CSIRT atribuyó tempranamente el ataque al grupo de ransomware Qilin, señalando que el acceso inicial se logró mediante fuerza bruta contra un firewall perimetral sin autenticación multifactor configurada [Nivel4/CSIRT Nacional, 2026]. Este antecedente muestra de que la amenaza de ransomware contra entidades estratégicas chilenas es actual y vigente, no un riesgo hipotético o exclusivamente extranjero [25].

4.7 Síntesis: de la exposición técnica a la necesidad regulatoria

El recorrido desarrollado en este capítulo permite arribar a una conclusión técnica

con implicancias regulatorias directas: el sistema eléctrico chileno ha alcanzado un nivel de integración ciberfísica tal que la ciberseguridad ya no es una capa opcional de protección, sino una condición estructural de la operación segura y confiable del sistema. Los sistemas OT fueron diseñados sin considerar amenazas cibernéticas deliberadas, que la convergencia IT/OT ha eliminado el aislamiento que históricamente los protegía, y que las vulnerabilidades identificadas tienen consecuencias físicas medibles, como demuestran los casos revisados.

La seguridad de suministro ha sido tradicionalmente abordada desde la confiabilidad técnica —disponibilidad de unidades, redundancia de equipos y respuesta ante contingencias—. La incorporación de sistemas ICS/OT introduce, sin embargo, una categoría de riesgo cualitativamente distinta: las fallas ya no provienen solo de mecanismos físicos, sino de eventos intencionados cuya simultaneidad, coordinación y velocidad de propagación no tienen equivalente en la ingeniería de confiabilidad convencional. La protección de la infraestructura eléctrica no puede, por tanto, limitarse a la integridad física de los equipos: debe incorporar la dimensión digital como elemento crítico de la continuidad operativa.

Dado el carácter crítico de la infraestructura eléctrica y su exposición documentada a amenazas cibernéticas, es evidente que resulta necesario establecer marcos regulatorios que aseguren niveles mínimos de protección. Los casos documentados en la sección 4.6—en particular los ataques a Ucrania de 2015 y 2016— demuestran que esta necesidad no es preventiva en abstracto, sino la respuesta a una amenaza ya materializada.

En Chile, la **Ley Marco de Ciberseguridad**, y en el caso del sector eléctrico el **Estándar de Ciberseguridad del Coordinador Eléctrico Nacional** responden a la necesidad, reconociendo que la ciberseguridad es un componente de la **seguridad nacional**, las infraestructuras eléctricas críticas requieren estándares específicos de protección y que la gestión del riesgo debe ser sistemática y continua.

5. MARCO REGULATORIO E INTEGRACIÓN CON LA GESTIÓN DE ACTIVOS

En el presente capítulo se desarrollan los Objetivos Específicos 1 y 2 de esta investigación, correspondientes a la dimensión regulatoria del análisis: qué exige el marco normativo chileno de ciberseguridad al sector de generación eléctrica, y cómo esas exigencias se integran con la gestión de activos del sistema eléctrico. Las dimensiones técnica (comparación internacional y diagnóstico de brechas) y económica (estimación del costo de cumplimiento) se desarrollan en los capítulos siguientes.

El capítulo se organiza en ocho secciones. Se parte por establecer los criterios metodológicos que estructuran el análisis regulatorio (5.1) y aplicarlos a la Ley N.º 21.663 (5.2), sistematizando sus obligaciones en una matriz de cumplimiento (5.3). A continuación se examina el Estándar de Ciberseguridad del CEN, su habilitación sectorial y su matriz de obligaciones (5.4), y la matriz que sistematiza la convergencia entre ambos instrumentos (5.5), dando cumplimiento al Objetivo Específico 1.

Se aborda además el estado del marco normativo aún en desarrollo —Reglamento de Auditoría y Norma Técnica de la CNE (5.6)— y se examina cómo estas obligaciones se integran operativamente en la gestión de activos eléctricos, vinculando los deberes de ciberseguridad con los indicadores de integridad del Pliego Técnico RPTD N.º 17 (5.7), dando cumplimiento al Objetivo Específico 2.

Los resultados de este capítulo, la línea base regulatoria de la Ley 21.663 y el Estándar CEN, y su integración con la gestión de activos, constituyen el punto de partida para la comparación internacional y el diagnóstico de brechas (Cap. 6) y para la estimación del costo de cumplimiento (Cap. 7).

5.1 Criterios de análisis regulatorio

El análisis del marco normativo de ciberseguridad aplicable al sector de generación eléctrica chileno se organiza en torno a seis dimensiones de análisis. Estas dimensiones no constituyen una clasificación arbitraria: corresponden a los ejes bajo los cuales es posible caracterizar de forma comparable cualquier instrumento regulatorio de ciberseguridad, con independencia de su origen legal o técnico, y son las mismas que se utilizarán en el Capítulo 6 para contrastar el marco chileno con otros marcos normativos y regulatorios de naturaleza similar.

Las seis dimensiones son:

- **Naturaleza y fuerza obligatoria del instrumento:** Si se trata de una ley, un reglamento, un estándar técnico sectorial o un instrumento de adhesión voluntaria, y qué grado de exigibilidad jurídica tiene cada uno.
- **Gobernanza institucional y actores responsables:** Qué organismos

administran, fiscalizan y hacen cumplir el instrumento, y cómo se articulan entre sí cuando existe más de una autoridad con competencia.

- **Alcance, sujetos obligados y mecanismo de designación:** A qué entidades aplica el instrumento, bajo qué criterios se determina esa aplicabilidad, y qué procedimiento formal designa a un operador como sujeto obligado.
- **Principio de proporcionalidad:** Si el instrumento diferencia las obligaciones exigidas según el tamaño, impacto o complejidad del sujeto obligado, y bajo qué mecanismo formaliza esa diferenciación.
- **Gestión de riesgos y exigencia de un Sistema de Gestión de Seguridad de la Información (SGSI):** Qué obligaciones sustantivas de identificación, evaluación y mitigación de riesgos impone el instrumento a los sujetos obligados.
- **Reporte de incidentes y plazos de notificación:** Qué eventos deben reportarse, a quién, y bajo qué plazos y formatos.
- **Exigibilidad, régimen de infracciones y sanciones:** Qué mecanismos de verificación de cumplimiento existen y qué consecuencias jurídicas y económicas enfrenta un sujeto obligado que incumple.

Estas dimensiones así como el análisis de las obligaciones regulatorias proporcionan la estructura de análisis de la Ley 21.663, alineando así el cumplimiento del Objetivo Específico 1 de este trabajo.

5.2 Análisis de la Ley 21.663 según dimensiones

5.2.1 Naturaleza y fuerza obligatoria del instrumento

La naturaleza acelerada de las ciberamenazas exige que el marco legal sea capaz de adaptarse sin necesidad de reformas legislativas constantes. Por ello, la Ley N.º 21.663 se estructura como una "ley marco", estableciendo principios y obligaciones generales, y delega las especificaciones técnicas y los procedimientos operativos a la potestad reglamentaria del Ejecutivo y a las atribuciones normativas de la Agencia.

El detalle de las obligaciones de los Operadores de Importancia Vital (OIV) se determina mediante reglamentos expedidos por el Ministerio del Interior y Seguridad Pública —como el DS 285 y el DS 295—, mientras que la ANCI, según el Artículo 11°, letra b), posee la atribución de dictar protocolos, estándares e instrucciones generales de cumplimiento obligatorio. El marco de cumplimiento es, en consecuencia, bidimensional: una reglamentación de base (procedimientos, plazos, criterios de calificación) y una normativa técnica operativa que la ANCI puede actualizar periódicamente sin necesidad de modificar la ley.

Esta flexibilidad es particularmente relevante para el sector eléctrico: las plantas

generadoras operan con sistemas de control industrial de ciclo de vida larga (15-20 años) frente a amenazas digitales de frecuencia diaria, por lo que la ley permite dictar normas específicas para sistemas industriales sin necesidad de reforma legal, en línea con el Principio de Racionalidad del Artículo 3°, número 7.

Para el generador eléctrico, esto implica que el cumplimiento debe gestionarse como un proceso de adaptación continua a la normativa derivada, y no como un evento único.

5.2.2 Gobernanza institucional y actores responsables

Para comprender el impacto de la Ley N.º 21.663 en el sector generación, es preciso analizar la transición desde un modelo de gobernanza fragmentado hacia uno centralizado y reticular. Con anterioridad a esta ley, la ciberseguridad en el Sistema Eléctrico Nacional (SEN) operaba bajo una estructura de responsabilidades compartidas donde el **Coordinador Eléctrico Nacional (CEN)** definía estándares técnicos operativos, mientras que la facultad fiscalizadora recaía de manera indirecta en la **Superintendencia de Electricidad y Combustibles (SEC)** bajo el prisma de la continuidad y calidad del suministro eléctrico.

5.2.2.1 El Surgimiento de la ANCI como Autoridad Rectora

La Ley N.º 21.663 resuelve esta atomización mediante la creación de la **Agencia Nacional de Ciberseguridad (ANCI)** a través de su **Artículo 10**, definiéndola como un servicio público técnico y especializado con personalidad jurídica y patrimonio propio. Sus facultades, consagradas primordialmente en el **Artículo 11**, dotan a la Agencia de potestad normativa, potestad fiscalizadora y potestad sancionatoria.

5.2.2.2 El Ecosistema de Competencias Institucionales

La nueva normativa no deroga las facultades sectoriales preexistentes, sino que superpone una capa de autoridad técnica nacional sobre tres pilares: la ANCI y el CSIRT de Energía; la SEC, que mantiene su potestad sobre la seguridad de las instalaciones bajo el RPTD N.º 17; y el CEN, que aplica su propio Estándar de Ciberseguridad y conserva, por el Art. 72-1 del DFL 4, la facultad de segregar áreas del sistema ante ataques lógicos que amenacen su estabilidad. Esta multiplicidad de actores se articula mediante el Principio de Coordinación (Art. 3 N.º 3) y un sistema de "ventanilla única" (Art. 9) que unifica el reporte dentro del ecosistema ANCI —CSIRT Nacional y CSIRT sectoriales—, sin sustituir la obligación de reporte técnico independiente que la generadora mantiene con el CEN (Art. 72-2 DFL 4), tal como se desarrolla en la sección 5.2.6 y se identifica como solapamiento en el Cap. 6.5.

La eficacia de este modelo depende de la armonización de estándares del Artículo 26, que hace prevalecer a la autoridad sectorial cuando sus normas tienen efectos

equivalentes. Esta arquitectura se precisó operativamente en 2025 mediante las Instrucciones Generales N.º 1 (procedimiento de inscripción en la plataforma de reporte de incidentes) y N.º 3 (designación del Delegado de Ciberseguridad, exigida a los OIV, con requisitos de perfil e independencia funcional).

5.2.3 Alcance, sujetos obligados y mecanismos de designación

5.2.3.1 Definición de Servicios Esenciales y Operadores de Importancia Vital

El Artículo 4º de la Ley 21.663 define como prestadores de servicios esenciales (PSE) aquellos cuya interrupción puede causar un grave daño a la vida, integridad física o salud de la población, o afectar el normal funcionamiento de la sociedad, y clasifica taxativamente a la generación eléctrica dentro de esa categoría. Sobre esa base, el Artículo 5º faculta a la ANCI para calificar como Operadores de Importancia Vital (OIV) a aquellas instituciones privadas que, prestando servicios esenciales, reúnan requisitos de impacto significativo en la seguridad y el orden público debido a su dependencia de sistemas informáticos - calificación que, para una generadora, incorpora sus activos a la Infraestructura Crítica de la Información (ICI) de la nación.

5.2.3.2 Criterios Legales de Calificación

La calificación como OIV se acredita bajo tres criterios: **Dependencia Tecnológica**, cuando la provisión del servicio dependa críticamente de redes y sistemas de control industrial, tales como el SCADA y el DCS, **Impacto Significativo o Sistémico**: cuando la afectación o interrupción del servicio produce un impacto significativo en la seguridad nacional o en la provisión regular de otros servicios esenciales. Para determinar esta magnitud, el Artículo 4º del DS 285 mandata considerar factores como el número de afectados, la extensión geográfica de la falla y la monoprovisión del servicio en ciertas zonas. **Relevancia Estratégica e Interdependencia**: Se evalúa la interconexión de la planta con otros servicios esenciales y el efecto en la cadena de suministro que su indisponibilidad generaría sobre el sistema económico.

5.2.3.3 Etapas del Procedimiento Administrativo

El procedimiento de designación consta de cuatro etapas: **Informe Técnico Sectorial**, donde antes de calificar, la Agencia debe requerir un informe fundado a los organismos con competencia técnica, tales como la **SEC** o el **CEN**, quienes disponen de 30 días para elaborarlo, luego la **Elaboración de Nómina Preliminar**: donde la ANCI, con los antecedentes recabados elabora una nómina preliminar de potenciales OIV, luego una **Consulta Pública y Notificación** de 30 días, con notificación electrónica a las empresas afectadas, y finalmente la **Resolución de Calificación Final**, donde tras ponderar las observaciones, el Director Nacional de la ANCI dicta una **resolución fundada** declarando a la institución como OIV e

inscribiéndola en el Registro correspondiente. Esta calificación debe revisarse y actualizarse al menos cada tres años.

5.2.3.4 Implicancias y Carga Pública del Estatus OIV

La dictación de la resolución definitiva altera el estatus regulatorio del generador, transformándolo en un garante de la resiliencia del ciberespacio nacional. La calificación bajo el DS 285 activa de forma inmediata los deberes específicos del Artículo 8° de la Ley 21.663, obligando a la empresa a implementar un Sistema de Gestión de Seguridad de la Información (SGSI), certificar planes de continuidad operacional cada dos años y someterse a auditorías externas obligatorias. Esta "carga pública" desplaza la ciberseguridad desde el ámbito de la gestión de riesgos corporativos voluntarios hacia un régimen de responsabilidad legal auditable y sancionable.

5.2.4 Principio de Proporcionalidad

La Ley 21.663 incorpora el principio de proporcionalidad de forma explícita, estableciendo que las obligaciones deben ser adecuadas a la naturaleza, tamaño y complejidad del operador, diferenciando entre Infraestructura Crítica de la Información (ICI) y Operadores de Importancia Vital (OIV) —estos últimos sujetos al régimen reforzado del Art. 8°. Sin embargo, a diferencia de otros marcos internacionales que formalizan esta diferenciación mediante categorías objetivas de tamaño o impacto, el desarrollo reglamentario específico del principio de proporcionalidad en la Ley 21.663 se encuentra pendiente a la fecha de corte de este estudio.

5.2.5 Gestión de riesgos y exigencia de un Sistema de Gestión de Seguridad de la Información (SGSI)

Una vez que una empresa de generación eléctrica es calificada como Operador de Importancia Vital (OIV), queda sujeta a un régimen de obligaciones reforzadas que se sustenta en los Artículos 8° y 9° de la Ley N° 21.663. Estas obligaciones no constituyen un esfuerzo puntual sino una carga pública permanente.

El Artículo 8° establece un catálogo de deberes específicos que las generadoras OIV deben implementar de manera permanente, entre estos deberes se encuentra implementar un Sistema de Gestión de Seguridad de la Información (SGSI) (Art. 8, letra a), llevar Registro de Acciones (Art. 8, letra b), tener Planes de Continuidad Operacional y Ciberseguridad (Art. 8, letra c), los cuales deben certificarse bajo el Artículo 28 y revisarse obligatoriamente cada dos años, realizar Ejercicios y Simulacros (Art. 8, letra d), aplicar Medidas de Mitigación Inmediata (Art. 8, letra e), Informar a Potenciales Afectados (Art. 8, letra g), mantener programas de Capacitación y Ciberhigiene (Art. 8, letra h), y la Designación de un Delegado de

Ciberseguridad (Art. 8, letra i) con facultades ejecutivas para implementar políticas de seguridad, y con reporte directo a la alta dirección.

Adicionalmente, la normativa impulsa la formalización de políticas de control de acceso, gestión de vulnerabilidades y seguridad en la cadena de suministro, las cuales deben ser contractualmente exigibles a terceros y contratistas que operen en las instalaciones de generación.

Este deber de mitigación (letra e) se precisó operativamente mediante la Instrucción General N.º 4 de la ANCI, que eleva el estándar desde la planificación hacia la ejecución inmediata, estableciendo medidas mínimas de carácter obligatorio: restricción de accesos y aislamiento de sistemas comprometidos, suspensión de servicios expuestos a internet, deshabilitación de accesos remotos, cambio inmediato de contraseñas administrativas, eliminación de cuentas genéricas, y segmentación de redes para evitar el desplazamiento lateral.

5.2.6 Reporte de incidentes y plazos de notificación

La Ley 21.663 y el DS 295 clasifican los eventos reportables por impacto: un Incidente de Efecto Significativo (Art. 3º DS 295) es aquel capaz de interrumpir el servicio esencial, afectar la integridad física de las personas o comprometer activos informáticos críticos; un Ciberataque (Art. 2º letra c) es el intento de destruir, exponer, alterar o exfiltrar un activo informático. En una generadora, esto activa los planes de continuidad operacional del Art. 8º letra c).

El Art. 9º, desarrollado por el DS 295, exige a las generadoras OIV una cronología estricta: Alerta Temprana (3 horas desde el conocimiento del incidente), Reporte de Impacto (24 horas para OIV, plazo reducido del general de 72 horas), Plan de Acción (7 días corridos) e Informe Final (15 días corridos, con causas, vulnerabilidades y medidas correctivas).

Los reportes se realizan a través de la plataforma ANCI, operativa 24/7 como ventanilla única para notificar simultáneamente a otras autoridades sectoriales cuando corresponda (Art. 9º inciso penúltimo). Esta reportabilidad es independiente y complementaria a la obligación técnica que la generadora mantiene con el CEN por contingencias operativas (Art. 72-2 DFL 4): mientras el CEN gestiona la recuperación del balance potencia-demanda, la ANCI y el CSIRT Nacional se enfocan en neutralizar la amenaza digital. Un mismo incidente puede activar ambos canales sin que uno sustituya al otro.

5.2.7 Exigibilidad, régimen de infracciones y sanciones (desde 5.1.5.3)

El incumplimiento de estos deberes no solo compromete la seguridad sistémica, sino que activa un régimen sancionatorio severo. El Artículo 39 clasifica específicamente las infracciones de los OIV en tres niveles:

- **Infracciones Leves (Art 39, num. 1 y 3):** Como no mantener el registro de las acciones de seguridad, o no contar con programas de capacitación.
- **Infracciones Graves (Art. 39, num. 1 y 2):** Como no implementar el SGSI o los planes de continuidad operacional.
- **Infracciones Gravísimas (Art. 39, num. 1):** No adoptar medidas de mitigación inmediatas (Art. 8 letra e) ante incidentes de impacto significativo.

Estas faltas se sancionan según el Artículo 40, el cual establece multas de entre 5.000, 10.000 y 20.000 UTM para los PSE, y para los OIV multas de 10.000, 20.000 y hasta 40.000 Unidades Tributarias Mensuales (UTM) por infracciones gravísimas.

La ley reconoce la complejidad del sector eléctrico mediante el Artículo 37, que regula la concurrencia de facultades sancionadoras entre la ANCI y la SEC. Si un incumplimiento afecta normas sectoriales dictadas por la SEC —como el RPTD 17— con efectos equivalentes a los de la Agencia, será la autoridad sectorial quien instruya el proceso. En caso contrario, la ANCI retiene la potestad exclusiva, evitando la duplicidad de sanciones por un mismo hecho.

Las empresas sancionadas tienen garantizado el derecho a la defensa mediante procedimiento administrativo reglado, pudiendo interponer recursos de reposición o ejercer una reclamación judicial de ilegalidad ante la Corte de Apelaciones respectiva dentro de los quince días hábiles siguientes a la notificación (Art. 42 al 46).

5.3 Obligaciones de Cumplimiento y Matriz Regulatoria (Ley N° 21.663)

Las obligaciones desarrolladas en la sección precedente configuran un conjunto de deberes específicos, permanentes y auditables que la Ley N.º 21.663 impone a las empresas de generación calificadas como OIV.

Las seis dimensiones desarrolladas en la sección 5.2 caracterizan el marco normativo de la Ley 21.663 en su lógica jurídica e institucional. Esta sección sistematiza ese mismo marco en su dimensión de cumplimiento operativo. La Tabla 4 organiza cada deber legal en función de su artículo de origen, el aspecto regulatorio que aborda, la exigencia concreta que impone, la forma de implementación requerida, el componente técnico asociado y su perfil económico en términos de CAPEX y OPEX.

Esta matriz constituye el primer instrumento de análisis del OE1 y será complementada en las secciones siguientes por una tabla equivalente para el Estándar de Ciberseguridad del CEN (Tabla 5, sección 5.4) y por una tabla de convergencia que demuestra cómo ambos marcos normativos se articulan en controles técnicos integrados (Tabla 6, sección 5.5), evitando la duplicación de costos de cumplimiento.

Tabla 4. Matriz de cumplimiento para Ley 21.663 (Fuente: Elaboración Propia)

N°	Reglamento	Artículo / Norma	Aspecto Regulatorio	Exigencia	Implementación (Qué hacer)	Componente Técnico (Cómo)	Naturaleza	Relación con Ciber-Sistema	Perfil Económico (OPEX/CAPEX)	Justificación Económica
1	Ley 21.663	Art. 8°, letra a)	Gobernanza de Riesgos	Implementar un SGSI continuo para determinar riesgos que afecten la seguridad de las redes, sistemas y la continuidad operacional, evaluando probabilidad e impacto de los incidentes.	Clasificación y gestión de inventario de Ciber-Sistemas SEN. Asesorías de riesgo (Risk Assessments) para evaluar probabilidad e impacto sobre los Ciber-Sistemas.	Herramientas de Asset Inventory para OT y cálculo de indicadores de disponibilidad de activos críticos.	Organizacional / Técnica	Asegura disponibilidad al identificar vulnerabilidades antes de la falla.	Ambos (CAPEX + OPEX)	El SGSI requiere software de gestión (CAPEX) y personal/licencias continuas (OPEX).
2	Ley 21.663	Art. 8°, letra b)	Trazabilidad Legal	Mantener registro íntegro y auditable de todas las acciones que componen el SGSI.	Bitácora auditable de mantenimientos, accesos y cambios en sistemas de control OT.	Implementación de SIEM industrial con almacenamiento de logs inmutables. El plazo mínimo de retención de logs para investigación de incidentes (90 días) se establece en el DS 295 Art. 9°.	Procedimental / Técnica	Reduce probabilidad de falla mediante análisis de logs de comportamiento en redes OT.	Ambos (CAPEX + OPEX)	SIEM industrial: hardware/licencia inicial (CAPEX) + gestión de logs y almacenamiento (OPEX).
3	Ley 21.663	Art. 8°, letra c)	Resiliencia Operativa	Elaborar e implementar planes de continuidad operacional y ciberseguridad. Certificar dichos planes cada dos años conforme al Art. 28°.	Protocolos de operación en modo degradado y recuperación ante desastres (DRP). Coordinación con la ANCI, CEN y CSIRT Nacional.	Planes de continuidad, respaldo y recuperación. Sitios de respaldo, redundancia de enlaces de comunicación y sistemas tolerantes a fallas.	Operacional / Técnica	Asegura disponibilidad del activo crítico ante ataques destructivos o pérdidas de control.	CAPEX	Redundancia física y sitios de respaldo (DRP) exigen inversiones en infraestructura. La certificación bienal es OPEX.
4	Ley 21.663	Art. 8°, letra c) y Art. 28°	Certificación y auditoría externa	Someter los planes de continuidad y ciberseguridad a auditorías externas periódicas obligatorias, realizadas por entidades acreditadas ante la ANCI conforme al Art. 28°.	Gestionar procesos de auditoría externa periódica para verificar la 'debida diligencia' en la implementación del SGSI y los planes de continuidad.	Auditorías técnicas de cumplimiento por terceros acreditados, basadas en el Estándar del CEN. La acreditación de auditores la define la ANCI mediante normativa técnica.	Documental / Procedimental	Asegura integridad al validar que los controles técnicos son suficientes. Obliga a revisión permanente.	OPEX	Las auditorías externas periódicas son gastos operativos recurrentes (Art. 28° obliga de forma permanente).
5	Ley 21.663	Art. 8°, letra d)	Detección, pruebas y comunicación de resultados	Realizar revisiones y simulacros periódicos para detectar programas o acciones maliciosas en sistemas OT. Comunicar los resultados de los ejercicios al CSIRT Nacional. Aplica a todos los OIV sin excepción.	Ejecutar pruebas periódicas sobre sistemas OT críticos y reportar resultados formalmente al CSIRT Nacional (coordinación externa obligatoria).	Pentesting OT, ejercicios tabletop y simulacros de respuesta a incidentes. Protocolo de reporte de resultados al CSIRT Nacional. Monitoreo de intrusiones en redes industriales (IDS/SIEM).	Técnica / Procedimental	Directa: prueba la resiliencia de los Ciber-Sistemas e identifica vulnerabilidades antes de que sean explotadas.	OPEX	Pentesting y simulacros son OPEX por evento o anualidad. El reporte al CSIRT Nacional implica horas-hombre adicionales de coordinación externa.
6	Ley 21.663	Art. 8°, letra e)	Defensa en Profundidad	Adoptar de forma oportuna medidas para reducir el impacto y propagación de incidentes, incluyendo la restricción de acceso a sistemas informáticos si fuere necesario.	Protección lógica de los sistemas de control industrial (SCADA/DCS). Implementación de controles de segmentación y contención. Control de acceso físico a sala de control. Evaluación de riesgo físico de la instalación por tercero acordado con el CEN.	Diodos de datos, firewalls OT (IPS/IDS), segmentación de red (PSE), hardening de sistemas. Protocolo de aislamiento de emergencia. Control de acceso físico (lectoras, CCTV interior, bitácora). Evaluación de riesgo físico.	Técnica	Protección directa a Ciber-Sistema mediante aislamiento de comandos maliciosos y contención de incidentes.	CAPEX (principal) + OPEX (evaluación física)	Controles técnicos distintos: firewall industrial y diodo de datos, control de acceso físico sala OT, evaluación de riesgo físico instalación.
7	Ley 21.663	Art. 8°, letra h)	Capacitación y ciberhigiene	Contar con programas de capacitación continua y campañas de ciberhigiene para trabajadores y colaboradores con acceso a sistemas críticos.	Implementar formación continua para personal técnico y operativo con acceso a sistemas OT.	Programas de capacitación OT, talleres presenciales y campañas internas de ciberhigiene. Registros de completación auditables.	Organizacional	Reduce el riesgo humano (error no intencional e insider threat) sobre los Ciber-Sistemas.	OPEX	Formación y campañas de ciberhigiene son gastos recurrentes en recursos humanos y cultura organizacional.

N°	Reglamento	Artículo / Norma	Aspecto Regulatorio	Exigencia	Implementación (Qué hacer)	Componente Técnico (Cómo)	Naturaleza	Relación con Ciber-Sistema	Perfil Económico (OPEX/CAPEX)	Justificación Económica
8	Ley 21.663	Art. 8°, letra i)	Responsabilidad Jerárquica	Designar formalmente a un Delegado de Ciberseguridad que informe directamente a los directores, gerentes o ejecutivos principales de la empresa.	Estructura de mando interna con línea directa a la alta dirección. El Delegado debe tener autoridad para ejecutar presupuestos de crisis y acceso irrestricto a la plana ejecutiva.	Rol organizacional formalizado con capacidades ejecutivas y técnicas. Acceso directo a directores y CEO/gerente general (requisito explícito del Art. 8°(i)).	Organizacional	Gobernanza estratégica: asegura que las decisiones de ciberseguridad lleguen a la alta dirección sin intermediarios.	OPEX	Sueldo y estructura del Delegado son costos operacionales puros. Mayor especialización requerida en centrales con DCS propietario.
9	Ley 21.663 / DS 295	Art. 9° / DS 295 Arts. 2–12	Gestión de Crisis y Reportabilidad	Notificar incidentes significativos cumpliendo los cuatro hitos del DS 295: (1) Alerta inicial: máx. 3 horas. (2) Reporte detallado OIV: máx. 24 horas. (3) Plan de acción: máx. 7 días corridos. (4) Informe final: máx. 15 días corridos.	Protocolos de respuesta rápida para cada hito de reporte. Integración SOC→CSIRT Nacional. Análisis forense y recopilación de evidencias para el Informe Final.	SOC 24/7 con monitoreo de redes industriales (detección en < 3h). Plataforma SIEM para trazabilidad. Protocolo documentado de reporte por hito. Análisis forense OT para Informe Final.	Operacional / Técnica	Minimiza daño sistémico, limita propagación en el SEN y asegura aprendizaje institucional post-incidente.	Ambos (CAPEX + OPEX)	SOC 24/7 requiere tecnología y servicios de monitoreo constante. El Informe Final implica OPEX de análisis forense por evento.
10	DS 295	DS 295 Art. 2°	Clasificación y reporte de incidentes	Reportar obligatoriamente todo incidente con impacto significativo conforme a la taxonomía del DS 295 Art. 3°.	Definir y mantener protocolo interno de clasificación de incidentes con criterios de impacto operacional para determinar si aplica reporte obligatorio.	SIEM/SOC + matriz de criticidad de incidentes (BIA). Procedimiento documentado de clasificación y decisión de reporte.	Técnica / Procedimental	Asegura que todo evento con potencial de afectar Ciber-Sistema sea evaluado y reportado oportunamente.	OPEX	Definir y mantener protocolos de clasificación es esfuerzo procedimental (horas-hombre). El SIEM que soporta la clasificación es compartido con otros controles.
11	DS 295	DS 295 Art. 3°	Definición de impacto significativo	Identificar y documentar los criterios que califican un incidente como de impacto significativo conforme a la taxonomía del DS 295.	Implementar matriz de criticidad que clasifique eventos según impacto operacional, número de afectados y extensión geográfica.	Análisis de impacto operacional (BIA) específico para sistemas OT. Matriz de criticidad documentada y aprobada.	Analítica / Organizacional	Priorización correcta de Ciber-Sistemas SEN según criticidad sistémica.	OPEX	El BIA es una consultoría o tarea analítica recurrente (revisión anual recomendada). Costo predecible e independiente de otros controles.
12	Ley 21.663	Art. 28°	Validación externa periódica	Obtener certificaciones y someterse a auditorías externas periódicas realizadas por entidades acreditadas ante la ANCI para verificar la debida diligencia en ciberseguridad.	Contratación periódica de auditorías técnicas externas acreditadas para verificar la implementación del SGSI y los controles OT.	VIGENTE: auditorías técnicas basadas en el Estándar del CEN (NERC-CIP adaptado al SEN). PROYECTADO: el reglamento técnico ANCI en desarrollo proyecta alineamiento con IEC 62443, pero aún no está vigente a mayo 2026.	Procedimental	Asegura integridad al validar que los controles físicos y lógicos son técnica y legalmente suficientes.	OPEX	Auditorías externas por terceros acreditados son gastos operativos recurrentes. Frecuencia mínima bianual (Art. 8°c).
13	Ley 21.663	Art. 7° y Art. 26°	Integración sectorial	Cumplir obligaciones de la Ley 21.663 en forma coherente con la regulación eléctrica vigente. El Art. 26° establece que prevalece la normativa sectorial del CEN cuando su efecto es equivalente o superior.	Integrar el SGSI con el Estándar del CEN y la NTSyCS. Mantener matriz de integración normativa que evite conflictos regulatorios.	Matriz de integración normativa Ley 21.663 ↔ Estándar CEN ↔ NTSyCS. Revisión ante cada actualización normativa.	Técnica y documental	Directa: asegura que la protección de los Ciber-Sistemas cumple simultáneamente con la regulación de ciberseguridad y la eléctrica.	OPEX	Mantenimiento de la matriz de integración es labor de cumplimiento administrativo (horas-hombre). Costo marginal absorbido en el rol del Delegado.
14	Ley 21.663	Art. 11°, letra b)	Adaptación dinámica a instrucciones ANCI	Cumplir las instrucciones técnicas, protocolos y estándares de aplicación general que dicte la ANCI en ejercicio de su potestad normativa, en la medida en que sean aplicables al sector eléctrico y no contradigan normativa sectorial equivalente (Art. 26°).	Monitorear permanentemente la normativa técnica ANCI y actualizar los controles OT y procedimientos del SGSI conforme a nuevas instrucciones obligatorias.	Actualización continua de controles OT ante nuevas instrucciones ANCI. Proceso interno de seguimiento normativo y gestión del cambio regulatorio.	Regulatoria / Organizacional	Ajuste continuo de la protección de activos ante amenazas emergentes y nuevas exigencias regulatorias.	OPEX	La adaptación continua a normativa dinámica es gestión operativa (horas-hombre de compliance). Costo marginal absorbido en el rol del Delegado. Puede implicar CAPEX puntual si la instrucción exige nuevo hardware.

5.4 Habilitación sectorial y Estándar de Ciberseguridad del CEN

El análisis del marco regulatorio de ciberseguridad para el sector de generación eléctrica no puede limitarse a la Ley N.º 21.663 y sus reglamentos operativos. Existe un segundo cuerpo normativo de igual fuerza vinculante que preexiste a la ley, que la complementa y que, en virtud del principio de especialidad sectorial, puede incluso prevalecerse sobre ella: el Estándar de Ciberseguridad del Coordinador Eléctrico Nacional [5].

La ciberseguridad ya formaba parte de las exigencias operativas del sector eléctrico antes de la promulgación de la Ley 21.663. La Norma Técnica de Seguridad y Calidad de Servicio (NTSyCS) [26], instrumento regulatorio superior del sistema eléctrico chileno, establece que la seguridad del servicio y la eficiencia económica son principios irrenunciables de la operación del SEN bajo el Artículo 72°-1 del DFL N°4. Bajo ese marco, cualquier incidente digital que degrade los niveles de estabilidad o recuperación definidos en la NTSyCS constituye una vulneración de los estándares eléctricos sectoriales. La Ley 21.663 no reemplaza este ecosistema, lo jerarquiza bajo el principio de especialidad sectorial del Art. 26.

5.4.1 El Art. 26 como habilitación sectorial

La Ley N.º 21.663 reconoce expresamente esta realidad en su Artículo 26, que establece que cuando las autoridades sectoriales dicten normas técnicas de ciberseguridad con efectos equivalentes o superiores a los de la ANCI, prevalecerán las disposiciones de la autoridad sectorial. Esta disposición no es una excepción a la ley — es su mecanismo de implementación técnica para sectores con regulación especializada preexistente. En el caso del sector eléctrico, el Art. 26 activa una cadena normativa precisa:

Ley 21.663 → Art. 26 (habilitación sectorial) → Estándar CEN (norma técnica sectorial) → controles específicos por nivel de impacto

Esta cadena tiene una consecuencia metodológica directa para la presente investigación: las obligaciones del Estándar CEN no son adicionales a las de la Ley 21.663, sino su operacionalización técnica sectorial. Por tanto, cualquier análisis del costo de cumplimiento que ignore el Estándar CEN subestimaría sistemáticamente el esfuerzo real que el marco regulatorio impone a los operadores de generación.

5.4.2 Génesis del Estándar CEN: una adaptación, no una copia

El Estándar de Ciberseguridad del CEN no surge de manera espontánea. Su origen se remonta a la Política Nacional de Ciberseguridad de 2017 [27]. En ese marco, la SEC instruyó al CEN mediante los Oficios N°3377 (2018) y N°11508 (2019) [28] para desarrollar un estándar sectorial específico. Con apoyo técnico del California

Independent System Operator (CAISO), el CEN analizó los marcos internacionales disponibles y adoptó NERC-CIP como referencia técnica, publicando el estándar en julio de 2020 y actualizándolo en octubre de 2022.

La decisión del CEN no fue replicar NERC-CIP en su versión norteamericana, sino adaptarlo a las condiciones específicas del SEN chileno. Esa adaptación implicó modificaciones sustanciales en varias dimensiones del estándar. Por un lado, los umbrales de clasificación de impacto fueron redefinidos para el SEN: el umbral de Impacto Medio para generación se fijó en 300 MW agregados por planta, frente a los 1.500 MW del estándar norteamericano, lo que amplía significativamente el universo de instalaciones obligadas en Chile. En segundo lugar, el mecanismo de verificación de antecedentes de personal (CIP-004) fue adaptado para permitir el cumplimiento mediante Declaración Jurada, reconociendo la ausencia en Chile de un sistema centralizado equivalente al norteamericano. En tercer lugar, la identificación de instalaciones críticas bajo CIP-014 fue asignada al CEN con criterios propios adaptados al SEN, en lugar de los umbrales objetivos de transmisión del estándar original.

A estas tres modificaciones de contenido se suman dos diferencias de carácter estructural, por un lado el Estándar CEN no incorpora un mecanismo equivalente a la Technical Feasibility Exception (TFE), que en Estados Unidos permite a un operador documentar la inviabilidad técnica de cumplir un control específico y acordar medidas compensatorias, lo que reduce la flexibilidad frente a limitaciones tecnológicas. Y finalmente, el marco chileno no cuenta aún con guías de implementación (RSAW, Reliability Standard Audit Worksheets) que orientan tanto al operador como al auditor, lo que introduce un margen de interpretación en la fiscalización.

En conjunto, estas cinco diferencias —tres de contenido y dos estructurales— ejemplifican el trabajo de adaptación del estándar a la realidad nacional.

5.4.3 Alcance y arquitectura de cumplimiento

El Estándar CEN es de aplicación obligatoria tanto para el propio Coordinador como para todas las Empresas Coordinadas, denominadas "Entidades Responsables". Su aplicabilidad específica está determinada por la clasificación de impacto de las instalaciones: Impacto Alto, Medio o Bajo, definidos en las secciones 6.1, 6.2 y 6.3 del estándar respectivamente. El estándar incorpora trece bloques CIP — desde CIP-002 hasta CIP-014 — cada uno con requerimientos, medidas de control y plazos de implementación diferenciados por nivel de impacto.

Las Entidades Responsables están obligadas a informar anualmente al CEN — durante el primer trimestre de cada año — el nivel de cumplimiento de las medidas de control para cada requerimiento, firmado por el Encargado CIP. El CEN puede

instruir auditorías de cumplimiento y certificaciones por terceros especializados. Los registros de evidencias deben mantenerse por un período mínimo de tres años.

5.4.4 Implicancias para el modelo de costos

El cumplimiento del Estándar CEN genera obligaciones técnicas concretas que determinan drivers de costo directos. Cada bloque CIP exige implementar controles específicos — inventarios de activos, firewalls industriales, gestión de parches, planes de recuperación, evaluaciones de vulnerabilidades — que implican tanto inversiones de capital (CAPEX) como gastos operativos recurrentes (OPEX). Estos controles no son opcionales ni graduables: su incumplimiento activa el régimen sancionatorio de la SEC y complementa el de la ANCI en virtud del Art. 37 de la Ley 21.663.

La Tabla 5 de la sección 5.4.5 sistematiza estas obligaciones bloque por bloque, con el mismo formato de la Tabla 4 de la Ley 21.663, permitiendo visualizar el esfuerzo de cumplimiento sectorial en la misma lógica analítica que el marco legal general. La Tabla 6 de la sección 5.5 demuestra que ambos instrumentos no generan cargas independientes sino que se articulan en controles técnicos integrados, lo que constituye el fundamento metodológico del modelo económico que será desarrollado en el Capítulo 7 .

5.4.5 Matriz de cumplimiento – Estándar de Ciberseguridad del CEN

La sección 5.3 sistematizó las obligaciones que la Ley N.º 21.663 impone directamente a los operadores calificados como OIV. Sin embargo, como se estableció en la sección 5.4, el marco regulatorio aplicable al sector de generación eléctrica no se agota en ese instrumento: el Estándar de Ciberseguridad del CEN, habilitado por el Art. 26 de la ley, constituye el instrumento técnico sectorial que operacionaliza esas obligaciones y agrega controles específicos para la protección de los Ciber Sistemas SEN. Su cumplimiento es igualmente obligatorio para todas las Empresas Coordinadas y genera drivers de costo directos sobre los operadores.

La Tabla 5 presenta la matriz de cumplimiento del Estándar CEN, organizada bloque por bloque siguiendo la misma estructura analítica de la Tabla 4, lo que permite comparar directamente el esfuerzo de cumplimiento exigido por cada instrumento normativo. Cada fila corresponde a un bloque CIP incorporado por el estándar, describiendo su propósito, la exigencia concreta que impone a los operadores de generación, la forma de implementación requerida, el componente técnico asociado y su perfil económico en términos de CAPEX y OPEX.

Tabla 5. Matriz de cumplimiento – Estándar de Ciberseguridad del CEN (Fuente: Elaboración Propia)

N°	Reglamento	Artículo / Norma	Aspecto Regulatorio	Exigencia	Implementación (Qué hacer)	Componente Técnico (Cómo)	Naturaleza	Relación con Ciber-Sistema	Perfil Económico	Justificación Económica
1	Estándar CEN (NERC-CIP)	CIP-002 Clasificación de activos BES	Identificación y clasificación de activos críticos del SEN	Identificar y clasificar todos los ciberactivos que afectan la confiabilidad del SEN por nivel de impacto (alto, medio, bajo). Revisión anual obligatoria.	Inventario de sistemas OT (SCADA, DCS, PLC, PPC, IED, RTU) con clasificación de impacto asignada.	Herramienta de Asset Inventory OT. Lista documentada de Ciber Sistemas SEN con nivel de impacto y revisión anual.	Técnica / Organizacional	Directa: define qué activos requieren controles reforzados y en qué nivel de protección.	Ambos (CAPEX + OPEX)	Software de inventario OT (CAPEX) + horas-analista de revisión anual (OPEX).
2	Estándar CEN (NERC-CIP)	CIP-003 Controles de gestión de seguridad	Gobernanza: liderazgo y responsabilidad organizacional	Implementar políticas de ciberseguridad aprobadas por el Encargado CIP. Designar un Encargado CIP con acceso a la dirección.	Política de ciberseguridad OT documentada y aprobada. Encargado CIP con rol senior y línea directa a la dirección.	Documento de política CIP aprobado. Rol formal del Encargado CIP con responsabilidades definidas para activos de cada nivel de impacto.	Organizacional	Gobernanza estratégica: asegura responsabilidad ejecutiva sobre la protección de los Ciber Sistemas SEN.	OPEX	Sueldo del Encargado CIP. Mayor especialización requerida en centrales con DCS propietario.
3	Estándar CEN (NERC-CIP)	CIP-004 Personal y capacitación	Capacitación obligatoria del personal con acceso a ciberactivos OT	Todo el personal con acceso a Ciber Sistemas SEN debe completar formación en ciberseguridad OT. Verificación de antecedentes periódica (admite Declaración Jurada en el contexto chileno).	Programa de capacitación anual en ciberseguridad OT. Registro de completación por persona. Verificación de antecedentes al ingreso y periódica.	Programa de capacitación CIP. Plataforma e-learning OT. Registros auditable. Proceso de verificación de antecedentes.	Organizacional / Procedimental	Reduce riesgo humano (insider threat y error no intencional) sobre los Ciber Sistemas SEN.	OPEX	Costo de capacitación anual por persona + plataforma e-learning.
4	Estándar CEN (NERC-CIP)	CIP-005 Perímetro de Seguridad Electrónica (PSE)	Segmentación de red y control de acceso al entorno OT	Definir y proteger el PSE de cada activo de alto y medio impacto. Controlar y documentar todos los accesos remotos interactivos (ARI).	Segmentación IT/OT con firewall industrial. Control de accesos remotos mediante Sistema Intermedio y autenticación multifactor. Revisión de reglas de firewall.	Firewall OT ruggedizado. Diodo de datos para zonas críticas. Sistema Intermedio para ARI. Detección de comunicaciones maliciosas en CDCs y CCs.	Técnica	Protección directa: impide acceso no autorizado a Ciber Sistemas SEN desde redes externas.	CAPEX	Firewall industrial y diodo de datos son CAPEX. Gestión de acceso remoto (PAM/MFA): OPEX menor.
5	Estándar CEN (NERC-CIP)	CIP-006 Seguridad física de Ciber Sistemas SEN	Control de acceso físico a instalaciones con activos OT críticos	Implementar Perímetro de Seguridad Física (PSF) para activos de alto y medio impacto. Controlar, registrar y revisar todos los accesos físicos. Alarma ante acceso no autorizado dentro de 15 minutos.	Control de acceso físico a sala de control, cuarto de servidores OT y celdas de protección. Registro de accesos. Sistema de alarma ante intrusión.	Lectoras de tarjeta / badge + controlador de acceso. CCTV interior en zonas OT. Bitácora digital de accesos físicos. Sistema de Control de Acceso Físico (SCAF) para impacto alto.	Técnica / Procedimental	Protección directa: impide manipulación física de Ciber Sistemas SEN desde el interior del recinto OT.	CAPEX	Componentes: lectoras de tarjeta + controlador de acceso, CCTV interior sala OT, bitácora digital de accesos. Inversión puntual y no recurrente.
6	Estándar CEN (NERC-CIP)	CIP-007 Gestión de seguridad de sistemas	Hardening, parcheo y gestión de cuentas en sistemas OT	Deshabilitar puertos innecesarios. Evaluar parches cada 35 días y aplicar o documentar controles compensatorios. Gestionar cuentas y contraseñas OT. Monitorear eventos de seguridad.	Script de hardening por tipo de sistema OT. Ciclo de evaluación + aplicación de parches con registro. Gestor de credenciales OT. Log de eventos de seguridad.	Registro de evaluación de parches. Herramienta de gestión de parches OT. Política de contraseñas OT y renovación periódica. Sistema de log de eventos.	Técnica	Directa: reduce superficie de ataque de cada Ciber Sistema SEN.	Ambos (CAPEX + OPEX)	Herramienta gestión parches OT (CAPEX) + horas-técnico ciclo de parcheo (OPEX recurrente).
7	Estándar CEN (NERC-CIP)	CIP-008 Reporte de incidentes y planes de respuesta	Plan de Respuesta a Incidentes OT con ejercicios periódicos	Implementar y mantener Plan IR para Ciber Sistemas SEN. Ejercicios periódicos. Revisar y actualizar tras cada ejercicio o Incidente de Ciberseguridad Reportable (ICR).	Plan IR con roles, responsabilidades y procedimientos OT. Ejercicio al menos una vez cada 36 meses. Revisión post-incidente documentada.	Documento Plan IR aprobado por Encargado CIP. Registro de ejercicios. Notificación de ICR al Coordinador, SEC y autoridades que defina la SEC.	Procedimental / Organizacional	Reduce tiempo de recuperación del Ciber Sistema SEN ante incidente; limita daño operacional y sistémico.	OPEX	Plan IR + ejercicios: horas-hombre (consultoría o personal interno). Coordinación con Ley 21.663: plazos DS 295 se superponen a los del Estándar CEN.

N°	Reglamento	Artículo / Norma	Aspecto Regulatorio	Exigencia	Implementación (Qué hacer)	Componente Técnico (Cómo)	Naturaleza	Relación con Ciber-Sistema	Perfil Económico	Justificación Económica
8	Estándar CEN (NERC-CIP)	CIP-009 Planes de recuperación de Ciber Sistemas SEN	Planes de continuidad y recuperación operacional post-incidente cibernético	Desarrollar, probar y actualizar planes de recuperación de Ciber Sistemas SEN. Ejercicios de recuperación al menos cada 15 meses. Respaldo configuraciones críticas.	Plan de Recuperación documentado y probado. Respaldos de configuraciones OT en sitio seguro fuera de línea. Ejercicio de restauración periódico.	Infraestructura de backup de configuraciones OT. Procedimiento de restauración validado. Servidor DRP para DCS en activos Gr.B.	Operacional / Técnica	Asegura retorno controlado a operación segura del Ciber Sistema SEN; reduce tiempo de indisponibilidad forzada.	CAPEX	Infraestructura de respaldo de configuraciones OT (CAPEX). Ejercicios de recuperación: OPEX. Mayor impacto en Gr.B.
9	Estándar CEN (NERC-CIP)	CIP-010 Gestión de configuración y evaluación de vulnerabilidades	Baseline de configuración OT y evaluación periódica de vulnerabilidades	Establecer baseline de configuración por Ciber Sistema SEN. Autorizar y documentar cambios. Evaluación de vulnerabilidades OT cada 15 meses con herramienta pasiva.	Baseline documentado por sistema OT. Change management formal para OT. Evaluación de vulnerabilidades con herramienta pasiva (sin interrupción del proceso).	Plataforma de monitoreo OT pasivo (Claroty / Nozomi / Dragos). Detecta cambios no autorizados y evalúa vulnerabilidades sin afectar operación. Nota: esta plataforma integra en un mismo producto las funciones de Asset Inventory (CIP-002) y monitoreo pasivo (CIP-010).	Técnica	Directa: detecta cambios no autorizados en Ciber Sistemas SEN y evalúa vulnerabilidades sin afectar operación.	Ambos (CAPEX + OPEX)	Plataforma OT de monitoreo pasivo: mayor componente CAPEX del modelo. Licencias anuales OPEX.
10	Estándar CEN (NERC-CIP)	CIP-011 Protección de información de Ciber Sistemas SEN	Clasificación y protección de información sensible de sistemas OT	Identificar y proteger información de Ciber Sistemas SEN: planos de red, configuraciones, credenciales. Procedimiento de destrucción segura de dispositivos retirados.	Política de clasificación de información OT. Almacenamiento cifrado de configuraciones. Procedimiento de borrado seguro de dispositivos retirados.	Política documentada. Almacenamiento cifrado (servidor o nube privada). Sanitización de dispositivos OT (NIST SP 800-88).	Procedimental / Técnica	Protege la información que permitiría a un atacante conocer arquitectura y vulnerabilidades del Ciber Sistema SEN.	OPEX	Principalmente horas-hombre para clasificación y procedimientos. Responsabilidad del Encargado CIP / Delegado. Almacenamiento cifrado: costo marginal bajo.
11	Estándar CEN (NERC-CIP)	CIP-012 Comunicaciones entre Centros de Control	Seguridad de comunicaciones entre Centros de Control del SEN	Proteger la confidencialidad e integridad de los datos de evaluación y monitoreo en tiempo real transmitidos entre Centros de Control. Implementar plan documentado de protección.	Plan documentado de protección de comunicaciones entre CCs con: identificación de protecciones, ubicación de aplicación y responsabilidades entre entidades.	Encriptación de enlaces entre Centros de Control. Controles de integridad sobre datos SCADA en tránsito. Documentación de arquitectura de comunicaciones inter-CC.	Técnica	Protege la integridad de los datos de operación en tiempo real transmitidos entre el CDC del Coordinador y los CCs de las Coordinadas.	Ambos (CAPEX + OPEX)	Aplica al Coordinador y a Empresas Coordinadas que operen un Centro de Control propio (SCADA ≥2 instalaciones). Implementación de encriptación en enlaces inter-CC (CAPEX).
12	Estándar CEN (NERC-CIP)	CIP-013 Gestión de riesgo en la cadena de suministro OT	Evaluación de ciberseguridad de proveedores y supply chain OT	Implementar plan de gestión de riesgo de supply chain para software y hardware OT. Incluir cláusulas de ciberseguridad en contratos con proveedores OT.	Plan de gestión de proveedores OT. Evaluación de ciberseguridad en adquisición de equipos. Cláusulas contractuales de ciberseguridad.	Cláusulas estándar en contratos OT. Cuestionario de evaluación de proveedores. Registro de software y firmware autorizado por fabricante.	Procedimental / Organizacional	Previene compromiso de Ciber Sistemas SEN mediante actualizaciones de firmware malicioso introducido por proveedores.	OPEX	Esfuerzo administrativo: revisión de contratos y evaluación de proveedores (horas-hombre). Sin CAPEX significativo.
13	Estándar CEN (NERC-CIP)	CIP-014 Seguridad física de instalaciones críticas	Protección física de instalaciones cuya pérdida afecta la estabilidad del SEN	Identificar instalaciones críticas para la estabilidad del SEN según criterios del Coordinador. Evaluación de riesgo físico por tercero acordado con el CEN. Implementar plan de seguridad física resultante.	Evaluación de riesgo físico por evaluador acordado con el CEN. Plan de seguridad física aprobado. Revisión periódica del plan.	Evaluación de riesgo físico (consultoría acordada con CEN). Medidas físicas según hallazgos: CCTV perimetral, perímetro reforzado, iluminación de seguridad, sensores de intrusión, alarmas.	Técnica / Procedimental	Directa: protege la infraestructura física del Ciber Sistema SEN y su interfaz con el SEN contra amenazas físicas deliberadas.	OPEX (evaluación) + CAPEX variable (medidas no modelables)	Solo la evaluación de riesgo físico por tercero acordado con el CEN es un costo predecible y modelable (OPEX consultoría por evento). Ver nota 1.

Nota1: El control CIP-014 se ha modelado exclusivamente en su componente de evaluación de riesgo físico por tercero (OPEX de consultoría), al ser este el único costo predecible y universalmente exigible. Se excluye la valorización genérica de las medidas de mitigación resultantes (tales como refuerzos perimetrales, CCTV, sensores de intrusión o iluminación de seguridad) debido a que su necesidad, diseño y costo dependen de los hallazgos específicos de cada emplazamiento y la topografía propia de la instalación. Incluir una estimación monetaria genérica para estas obras civiles e instalaciones de seguridad física introduciría una imprecisión metodológica mayor que declarar la limitación de alcance del modelo.

5.5 Convergencia normativa: control técnico integrado Ley 21.663 y Estándar CEN

Las dos matrices precedentes — Tabla 4 para la Ley 21.663 y Tabla 5 para el Estándar CEN — describen los marcos normativos de forma independiente. Sin embargo, desde la perspectiva del operador de generación que debe cumplir ambos instrumentos simultáneamente, la pregunta relevante no es cuántas obligaciones existen en cada marco, sino cuántos controles técnicos distintos debe efectivamente implementar. La respuesta a esa pregunta determina el costo real de cumplimiento.

La Tabla 6 sistematiza la convergencia entre ambos instrumentos, identificando los controles técnicos OT que satisfacen simultáneamente obligaciones de la Ley 21.663 y requerimientos del Estándar CEN.

Esta convergencia no es casual — es el resultado directo del Art. 26, que diseñó el marco normativo para que ambos instrumentos se articulen sin duplicar exigencias. Un mismo firewall industrial satisface el Art. 8°(e) y el CIP-005. Un mismo SOC MDR-OT satisface los plazos de notificación del DS 295 y el monitoreo de eventos del CIP-007. Un mismo Encargado CIP satisface el Delegado de Ciberseguridad del Art. 8°(i) y el rol CIP senior del CIP-003.

Esto denota que el costo de cumplimiento efectivo no es la suma aritmética del costo de cumplir la ley más el costo de cumplir el estándar sectorial, sino el costo de implementar los controles técnicos integrados que satisfacen ambos marcos de forma simultánea. La Tabla 6 es el puente metodológico entre el análisis normativo del OE1 y el modelo económico del OE5.

La convergencia sistematizada en la Tabla 6 permite extraer tres conclusiones que sintetizan el análisis normativo del OE1.

- Primero, el marco regulatorio chileno de ciberseguridad para el sector de generación eléctrica es arquitectónicamente coherente: la Ley 21.663 establece las obligaciones de alto nivel y el Estándar CEN las operacionaliza técnicamente, sin contradicciones ni duplicaciones relevantes.
- Segundo, la articulación entre ambos instrumentos — habilitada por el Art. 26 — produce una reducción del costo de cumplimiento respecto de lo que implicaría cumplir cada marco de forma independiente.
- Por último, los deberes de la ley y los controles CIP se resuelven en un conjunto de controles técnicos integrados y esos controles constituyen los drivers estructurales del modelo económico que será analizado más adelante.

Tabla 6. Convergencia Normativa – Ley N° 21.663 y Estándar CEN (Fuente: Elaboración Propia)

N°	Control técnico OT	Descripción del control integrado	Satisface Ley 21.663 (Artículo)	Satisface Estándar CEN (Bloque CIP)	Nivel de impacto CEN aplicable	Perfil Económico	Justificación Económica
1	Inventario y clasificación de Ciber Sistemas SEN	Un único inventario de activos OT satisface la obligación de SGSI de la ley y la clasificación de impacto de CIP-002. El mismo registro sirve como base del SGSI mandatado por la ley y como lista de Ciber Sistemas SEN exigida por el estándar.	Art. 8°(a) – SGSI + inventario de activos ICI	CIP-002 – Categorización de Ciber Sistemas SEN	Todos los niveles	CAPEX + OPEX	Plataforma de gestión certificable; base del SGSI mandatado. Licencia inicial (CAPEX) y renovación anual (OPEX).
2	Software SGSI — plataforma de gestión ISO 27001	El software de gestión del SGSI exigido por Art. 8°(a) materializa la política de ciberseguridad OT requerida por CIP-003. Un mismo sistema documenta, gestiona y certifica el SGSI para ambas obligaciones.	Art. 8°(a) – SGSI política de seguridad	CIP-003 – Controles de Gestión de la Seguridad	Todos los niveles	CAPEX	Plataforma certificable ISO 27001 (CAPEX implementación). Costo independiente del rol del Delegado.
3	Designación del Encargado CIP / Delegado de Ciberseguridad	El Delegado exigido por Art. 8°(i) cumple el rol de Encargado CIP requerido por CIP-003. La política de ciberseguridad OT exigida por CIP-003 forma parte del SGSI del Art. 8°(a). Un mismo rol y un mismo documento cubren ambas obligaciones.	Art. 8°(i) – Delegado con acceso a alta dirección Art. 8°(a) – SGSI política de seguridad	CIP-003 – Controles de Gestión de la Seguridad	Todos los niveles	OPEX	Responsabilidad jerárquica mandatada por ley. Sueldo del Delegado / Encargado CIP es OPEX puro. Mayor especialización en centrales con DCS propietario.
4	Programa de capacitación y verificación de antecedentes	El programa de capacitación OT para Art. 8°(h) satisface los requisitos de formación y registro de CIP-004. Los mismos módulos y registros de completación cubren ambas obligaciones. En Chile, CIP-004 admite Declaración Jurada para verificación de antecedentes.	Art. 8°(h) – capacitación y ciberhigiene	CIP-004 – Personal y Capacitación	Impacto Alto y Medio	OPEX	Reducción del riesgo humano. Costo recurrente por persona con acceso a Ciber Sistemas SEN.
5	Firewall OT ruggedizado — Perímetro de Seguridad Electrónica (PSE)	El firewall industrial implementado para CIP-005 satisface simultáneamente el deber de defensa en profundidad del Art. 8°(e). Control técnico único, doble cumplimiento normativo.	Art. 8°(e) – defensa en profundidad + restricción de acceso	CIP-005 – Perímetro de Seguridad Electrónica (PSE)	Impacto Alto y Medio	CAPEX	Segmentación red OT/IT. Inversión en activo fijo de infraestructura industrial.
6	Diodo de datos — aislamiento unidireccional zona crítica	Para zonas con Ciber Sistemas SEN de mayor criticidad, el diodo de datos proporciona aislamiento unidireccional que elimina la posibilidad de acceso bidireccional. Complementa el firewall donde se requiere aislamiento total.	Art. 8°(e) – defensa en profundidad zona crítica	CIP-005 – PSE zona crítica (complemento al firewall)	Impacto Alto y Medio (según evaluación de riesgo)	CAPEX	Aislamiento unidireccional red crítica. Costo complementario al firewall OT.
7	Control de acceso remoto seguro — PAM / MFA / Sistema Intermedio	La solución PAM/MFA implementada para el ARI de CIP-005 R2 satisface el control de accesos del Art. 8°(a) y la gestión de cuentas de CIP-007. El Sistema Intermedio es el mecanismo específico exigido por el Estándar CEN para ARI.	Art. 8°(e) – reducción de impacto Art. 8°(a) – SGSI gestión de accesos	CIP-005 R2 – Acceso Remoto Interactivo (ARI)	Impacto Alto y Medio	OPEX	Acceso remoto seguro para proveedores y mantenimiento. Licencias anuales PAM/MFA.
8	Control de acceso físico a sala de control y cuarto de servidores OT (PSF)	CIP-006 exige controlar físicamente el acceso al recinto donde se alojan los Ciber Sistemas SEN: sala de control, cuarto de servidores OT, celdas de protección. Incluye lectoras de tarjeta/badge, cerradura electrónica, CCTV interior y bitácora de accesos. Distinto de CIP-014: aplica al recinto interior OT, no a la instalación completa.	Art. 8°(e) – defensa en profundidad (dimensión física sala OT)	CIP-006 – Seguridad Física de Ciber Sistemas SEN (PSF)	Impacto Alto y Medio	CAPEX	Costo acotado y predecible (CAPEX). Aplica principalmente a Grupo B y C; con menor intensidad en Grupo A por menor complejidad del recinto de control. Componentes: lectoras de tarjeta/badge, cerradura electrónica, CCTV interior sala OT, bitácora digital de accesos.
9	Hardening OT — configuración segura de sistemas	El hardening de sistemas OT (deshabilitar puertos innecesarios, configuración segura) satisface simultáneamente el deber de reducción de impacto del Art. 8°(e) y el requisito de gestión de puertos y servicios de CIP-007 R1.	Art. 8°(e) – reducción de superficie de ataque	CIP-007 R1 – Gestión de puertos y servicios	Impacto Alto y Medio	CAPEX	Reducción de superficie de ataque mediante configuración segura inicial. Inversión de implementación única con revisiones periódicas.
10	Gestión de parches OT — ciclo de evaluación y aplicación	Los ciclos de evaluación y aplicación de parches OT satisfacen el SGSI continuo del Art. 8°(a) y el requisito de gestión de parches de CIP-007 R2. Las mismas horas-técnico cubren ambas obligaciones normativas.	Art. 8°(e) – reducción de riesgos continua Art. 8°(a) – SGSI gestión de riesgos	CIP-007 R2 – Gestión de parches (evaluación cada 35 días)	Impacto Alto y Medio	OPEX	Horas-técnico recurrentes para ciclos de evaluación y aplicación de parches OT. Ciclo trimestral efectivo.

N°	Control técnico OT	Descripción del control integrado	Satisface Ley 21.663 (Artículo)	Satisface Estándar CEN (Bloque CIP)	Nivel de impacto CEN aplicable	Perfil Económico	Justificación Económica
11	SIEM industrial + monitoreo de eventos de seguridad OT	El SIEM industrial cubre: trazabilidad legal del Art. 8°(b), capacidad de detección para plazos DS 295, monitoreo de eventos de CIP-007 R4/R5 y base para evaluación de vulnerabilidades de CIP-010 R3. Un sistema, cuatro obligaciones simultáneas.	Art. 8°(b) – registro auditable SGSI Art. 9°/DS 295 – trazabilidad para reportes	CIP-007 R4/R5 – Monitoreo de eventos de seguridad CIP-010 R3 – Evaluación de vulnerabilidades	Impacto Alto y Medio	CAPEX + OPEX	Trazabilidad legal obligatoria; retención de logs mínimo 90 días (DS 295 Art. 9°). Plataforma requiere licencia inicial (CAPEX) y gestión continua (OPEX).
12	SOC MDR-OT 24/7 — monitoreo continuo externalizado	El SOC MDR-OT cubre: detección en menos de 3h para DS 295, monitoreo de eventos CIP-007 R4, evaluación pasiva de vulnerabilidades CIP-010 R3, coordinación de respuesta CIP-008 R2, y comunicación al CSIRT del Art. 8°(d). Un servicio, cinco obligaciones normativas simultáneas.	Art. 9°/DS 295 – notificación 3h/24h/7d/15d Art. 8°(d) – detección y comunicación al CSIRT	CIP-007 R4 – Monitoreo de eventos CIP-008 R2 – Coordinación de respuesta CIP-010 R3 – Evaluación pasiva vulnerabilidades	Impacto Alto y Medio	OPEX	Monitoreo continuo 24/7 con especialización OT. Mayor driver de costo por cobertura multifuncional.
13	Plan de Continuidad + Infraestructura DRP + Plan IR	Plan de Continuidad (ley), Plan IR (CIP-008) y Plan de Recuperación (CIP-009) se fusionan en un instrumento único. La infraestructura DRP incluye: servidor de respaldo DCS, NAS externo para configuraciones, software de backup OT y medios fuera de línea.	Art. 8°(c) – planes de continuidad bienales Art. 8°(d) – simulacros periódicos	CIP-008 R1-R3 – Plan IR CIP-009 R1-R3 – Plan de recuperación OT	Impacto Alto y Medio	CAPEX + OPEX	Resiliencia operacional; certificación bianual Art. 28°. Infraestructura DRP es CAPEX. Ejercicios de recuperación son OPEX anual.
14	Pentesting OT y simulacros de respuesta a incidentes	El pentesting OT y los ejercicios tabletop son el mecanismo técnico con que se ejecuta el Art. 8°(d) sobre sistemas OT. CIP-008 R1-R3 exige ejercicios periódicos del Plan IR. Los resultados se reportan al CSIRT Nacional conforme al Art. 8°(d).	Art. 8°(d) – revisiones, simulacros y comunicación al CSIRT	CIP-008 R1-R3 – Ejercicios del Plan IR	Impacto Alto y Medio	OPEX	Costo anual por ejercicio de pentesting OT. Separado del DRP porque tiene diferente frecuencia y proveedor.
15	Análisis de Impacto de Negocio (BIA) — matriz de criticidad de incidentes	El BIA produce la matriz de criticidad de incidentes exigida por el DS 295 Art. 3° para determinar qué eventos califican como de impacto significativo. Es un entregable independiente del SGSI general: requiere una consultoría o análisis específico para sistemas OT.	DS 295 Art. 3° – criterios de impacto significativo Art. 8°(a) – SGSI gestión de riesgos	CIP-008 – soporte metodológico Plan IR	Impacto Alto y Medio	OPEX	Consultoría o análisis específico recurrente (revisión anual recomendada). Costo predecible e independiente de otros controles.
16	Auditorías externas integradas — Art. 28° y Estándar CEN	La auditoría externa exigida por Art. 28° puede cubrir simultáneamente: verificación de controles del SGSI, verificación de vulnerabilidades OT (CIP-010 R3), revisión de gestión de proveedores (CIP-013) y verificación de evaluación de riesgo físico (CIP-014 R2). Una auditoría integrada reemplaza evaluaciones independientes.	Art. 28° – certificaciones y auditorías periódicas Art. 8°(a) – SGSI y gestión de riesgos	CIP-010 R3 – Verificación vulnerabilidades CIP-013 – Verificación supply chain CIP-014 R2 – Verificación evaluación riesgo físico	Impacto Alto y Medio (Art. 28° aplica a todos los OIV)	OPEX	Validación independiente del SGSI; costo recurrente bianual (Art. 28°). Integración reduce costo vs auditorías separadas por instrumento normativo.
—	Baseline de configuración + plataforma monitoreo OT pasivo	El baseline de configuración de CIP-010 R1 y el change management de R2 satisfacen la gestión de riesgos continua del Art. 8°(a). La evaluación de vulnerabilidades de CIP-010 R3 se ejecuta mediante la plataforma de monitoreo OT pasivo, que integra también la función de Asset Inventory (CIP-002). Nota: Claroty/Nozomi/Dracos integran Asset Inventory (CIP-002) + monitoreo pasivo (CIP-010) en una sola plataforma.	Art. 8°(a) – SGSI gestión de riesgos continua Art. 8°(e) – reducción de impacto	CIP-010 R1 – Baseline de configuración CIP-010 R2 – Gestión de cambios CIP-010 R3 – Evaluación de vulnerabilidades (cada 15 meses)	Impacto Alto y Medio	CAPEX + OPEX	Plataforma de monitoreo OT pasivo (Claroty / Nozomi / Dracos). Licencia inicial (CAPEX) y suscripción anual (OPEX). La misma plataforma cubre CIP-002 (control 1) y CIP-010 (este control). * Nota2 *
—	Protección de información OT — responsabilidad del Delegado	CIP-011 exige proteger la información de los Ciber Sistemas SEN (configuraciones, planos, credenciales). Esta responsabilidad recae sobre el Delegado / Encargado CIP — el mismo rol del control 3. No genera un control técnico adicional: es una política administrada por el mismo rol.	Art. 8°(a) – SGSI protección de datos Art. 8°(b) – registro íntegro y auditable	CIP-011 R1-R2 – Protección de información de Ciber Sistemas SEN	Todos los niveles	OPEX (marginal)	Costo marginal absorbido en el rol del Delegado / Encargado CIP. Sin tecnología adicional. * Nota2 *
—	Integración normativa Ley 21.663 ↔ Estándar CEN ↔ NTSyCS	El Art. 26° de la Ley 21.663 establece que prevalece la normativa sectorial del CEN cuando su efecto es equivalente o superior. El operador debe mantener una matriz de integración normativa que asegure coherencia entre los tres instrumentos y se actualice ante cada modificación regulatoria.	Art. 7° y Art. 26° – integración sectorial y prevalencia normativa CEN	Estándar CEN general – coherencia normativa entre instrumentos	Todos los niveles	OPEX (marginal)	Labor de cumplimiento administrativo (horas-hombre). Costo marginal absorbido en el rol del Delegado. * Nota2 *

N°	Control técnico OT	Descripción del control integrado	Satisface Ley 21.663 (Artículo)	Satisface Estándar CEN (Bloque CIP)	Nivel de impacto CEN aplicable	Perfil Económico	Justificación Económica
—	Monitoreo y adaptación a instrucciones técnicas ANCI	El Art. 11°(b) obliga a los OIV a cumplir las instrucciones técnicas que dicte la ANCI en ejercicio de su potestad normativa, en la medida en que sean aplicables al sector eléctrico y no contradigan normativa sectorial equivalente (Art. 26°). Requiere seguimiento permanente de la normativa ANCI.	Art. 11°(b) – instrucciones técnicas ANCI	Sin CIP equivalente directo — obligación legal transversal	Todos los niveles	OPEX (marginal)	Gestión operativa continua (horas-hombre de compliance). Costo marginal absorbido en el rol del Delegado. Puede implicar CAPEX puntual si la instrucción exige nuevo hardware. * Nota2 *
—	Reporte de incidentes DS 295 — protocolo cuatro hitos	El DS 295 exige notificar incidentes significativos en cuatro hitos: alerta inicial (3h), reporte detallado OIV (24h), plan de acción (7 días) y informe final (15 días). El costo del reporte en sí es marginal: es una tarea ejecutada por el Delegado y el SOC que ya están modelados como controles independientes.	Art. 9° / DS 295 Arts. 2–12 – protocolo de reportabilidad	CIP-008 – Notificación de Incidente de Ciberseguridad Reportable (ICR)	Todos los OIV	OPEX (marginal — absorbido en SOC y Delegado)	Costo marginal absorbido en los roles del Delegado de Ciberseguridad y el SOC MDR-OT ya modelados. No genera un costo adicional independiente. * Nota2 *
—	Gestión de riesgos en la cadena de suministro OT	CIP-013 exige un plan de gestión de riesgos de supply chain para software y hardware OT, con cláusulas de ciberseguridad en contratos con proveedores y registro de software/firmware autorizado por fabricante.	Art. 8°(a) – SGSI y gestión de riesgos Art. 8°(e) – integridad de componentes OT	CIP-013 – Gestión de Riesgos en la Cadena de Suministros	Impacto Alto y Medio	OPEX	Esfuerzo administrativo: revisión de contratos y evaluación de proveedores OT. Sin CAPEX significativo. * Nota2 *
X	Seguridad de comunicaciones entre Centros de Control	CIP-012 exige proteger la confidencialidad e integridad de datos de evaluación en tiempo real entre Centros de Control. Aplica al Coordinador y a Empresas Coordinadas que operen un Centro de Control propio (SCADA ≥2 instalaciones). No aplica a generadoras sin CC propio: costo variable según arquitectura.	Art. 8°(a) – SGSI integridad de datos Art. 8°(e) – protección de comunicaciones críticas	CIP-012 – Comunicaciones entre Centros de Control	Entidades con Centro de Control propio (SCADA ≥2 instalaciones)	CAPEX + OPEX	Encriptación de enlaces inter-CC (CAPEX). Mantenimiento plan de protección (OPEX). Costo variable según arquitectura de comunicaciones. No aplica a generadoras sin CC propio. * Nota3 *
⚠	Evaluación de riesgo físico de instalación crítica — por tercero	CIP-014 exige una evaluación de riesgo físico de la instalación completa frente a amenazas deliberadas, realizada por tercero acordado con el CEN. Solo el costo de la evaluación es predecible y modelable. Las medidas resultantes (CCTV perimetral, cercado, iluminación, sensores perimetrales) presentan variabilidad indeterminada y no se modelan en un CAC genérico por razones metodológicas explícitas.	Art. 8°(e) – defensa en profundidad (amenazas físicas deliberadas a la instalación completa)	CIP-014 – Seguridad Física de instalaciones críticas del SEN	Instalaciones identificadas por el CEN como críticas para estabilidad del SEN	OPEX (evaluación) + CAPEX variable (medidas no modelables)	Solo la evaluación de riesgo físico por tercero acordado con el CEN es un costo predecible y modelable como driver del CAC. Las medidas resultantes de la evaluación (CCTV perimetral, cercado, iluminación, sensores de intrusión, refuerzo de perímetro) no se modelan en el CAC genérico: su variabilidad por instalación es prácticamente inmodelable y modelar un costo genérico introduciría una imprecisión mayor que declarar la limitación explícitamente. * Nota4 *

Nota2: Varios controles técnicos se solapan entre ellos, lo que se reflejará en el Modelo CAC y en el Capítulo 7

Nota3: La protección de comunicaciones en tránsito (CIP-012) varía críticamente según la arquitectura y propiedad de los enlaces de cada operador, haciéndola no modelable como un driver genérico sectorial. No obstante, desde el punto de vista del CAC, sus componentes técnicos de mitigación ya se encuentran absorbidos en los drivers core de infraestructura perimétrica: (1) Firewalls OT y Diodos de datos, los cuales ya proveen el aislamiento perimétrico, segmentación y tunelización segura (VPN) requerida para los canales de comunicación hacia el Coordinador (CDC) u otros centros de control, evitando la doble contabilidad de activos de red.

Nota4: Solo la evaluación de riesgo físico por tercero acordado con el CEN es un costo predecible y modelable (OPEX consultoría). Las medidas resultantes se EXCLUYEN del modelo CAC genérico por tres razones: (1) dependen completamente de los hallazgos específicos de cada instalación; (2) la variabilidad entre instalaciones es prácticamente inmodelable; (3) incluir un costo genérico introduciría una imprecisión mayor que declarar la limitación. La evaluación sí debe tener su propio driver de costo en el modelo CAC.

5.6 Marco Normativo en desarrollo: Reglamento de Auditoría y Norma Técnica CNE

Dos instrumentos normativos adicionales previstos en la arquitectura de la Ley 21.663 se encuentran, a la fecha de este informe en proceso de elaboración: el Reglamento sobre Estándares de Ciberseguridad y Auditorías, y la Norma Técnica de Ciberseguridad de la Comisión Nacional de Energía (CNE).

La CNE se encuentra desarrollando una Norma Técnica de Ciberseguridad específica para el sector eléctrico, en ejercicio de sus atribuciones normativas sectoriales. Esta norma está llamada a complementar el Estándar del CEN y la Ley 21.663, estableciendo requisitos técnicos adicionales orientados a la operación segura del Sistema Eléctrico Nacional.

Si bien su texto definitivo no ha sido publicado, los contenidos preliminares de la norma fueron presentados por el jefe del Subdepartamento de Normativa de la CNE, Félix Canales, en la I Conferencia Internacional de Ciberseguridad e Infraestructura Crítica Eléctrica [29]. Según la cobertura periodística de esa conferencia, la norma estaría estructurada en siete bloques temáticos: Disposiciones Generales, CSIRT Sectorial, Sistema de Gestión de Seguridad de la Información (SGSI), Ciberseguridad Industrial, Gestión de Riesgo, Comunicación de Incidentes y Disposiciones Temporales [30]. El capítulo de SGSI se basaría en ISO 27001, mientras que el de Ciberseguridad Industrial adoptaría el Estándar CEN como referente técnico prescriptivo, confirmando la naturaleza híbrida de la norma — que integra una dimensión de gestión de riesgos y una dimensión técnica OT en un solo instrumento sectorial. Dado que estos contenidos provienen de cobertura periodística de una conferencia y no de un documento oficial de la CNE, deben considerarse como preliminares y sujetos a modificación en el texto definitivo.

Por su parte, el reglamento de Auditorías es el encargado de materializar las exigencias del Artículo 28, definiendo los controles técnicos específicos y los protocolos de verificación a los que deberán someterse los Operadores de Importancia Vital (OIV) para dar cumplimiento a los deberes de certificación previstos en el Artículo 8°, letras c) y f).

La ausencia de ambos instrumentos al momento de este análisis genera una serie de riesgos y desafíos que impactan tanto al sector industrial como al desarrollo metodológico de este trabajo. Para el operador, genera incertidumbre en la planificación de inversiones y en los criterios de auditoría aplicables; para este análisis, implica que la Norma Técnica CNE no puede incorporarse aún a las matrices de cumplimiento. En conclusión, el marco vigente a analizar para este trabajo será únicamente la Ley 21.663 y Estándar CEN.

5.7 Integración de la ciberseguridad en la gestión de activos (OE2)

5.7.1 Marco Conceptual de Convergencia

El Pliego Técnico Normativo RPTD N.º 17, que regula el Sistema de Gestión de Integridad de Instalaciones Eléctricas (SGIIE), define la integridad como la aptitud de una instalación para desarrollar su función requerida de manera eficaz y segura, durante todo su ciclo de vida, en cumplimiento de la normativa aplicable. Esta definición, alineada con los principios de la gestión de activos físicos (ISO 55001), incorpora explícitamente el desempeño funcional, la continuidad operacional y el enfoque de ciclo de vida como elementos centrales de la seguridad eléctrica.

Esa aptitud funcional no es una propiedad exclusiva del activo físico: depende estructuralmente de la integridad de la capa de control OT. En centrales modernas, la capacidad de una turbina, un generador, un inversor o una subestación para cumplir su función requerida está condicionada por la disponibilidad, confiabilidad e integridad lógica de sistemas tales como SCADA, DCS, PLC, PPC, TCS e IEDs.

En este contexto, la ciberseguridad deja de constituir un dominio externo o complementario y pasa a ser un **atributo constitutivo de la integridad de la instalación**. La degradación de la capa OT —ya sea por fallas técnicas, errores operativos o incidentes de ciberseguridad— puede impedir que el activo físico opere dentro de condiciones seguras, aun cuando su estado mecánico o eléctrico sea nominal.

Bajo el marco del RPTD N.º 17, la pérdida de control lógico equivale a una pérdida de integridad funcional. La Ley 21.663 introduce la categoría de Infraestructura Crítica de la Información (ICI); el Estándar CEN utiliza el término Ciber Sistema SEN para referirse a la agrupación de Ciber Activos esenciales para la operación confiable del sistema eléctrico —constituyendo la ICI específica del entorno OT en generación.

En consecuencia, un incidente que compromete un sistema SCADA, un controlador de turbina, un PPC o un sistema de protección digital debe ser interpretado, por definición, como un ataque a la integridad del ICI o del Ciber-Sistema, aun cuando no se materialice inmediatamente un daño físico. Esta lectura resulta coherente con la tipificación de incidentes de efecto significativo establecida en el Decreto 295, donde se reconoce que el compromiso de activos informáticos críticos constituye un evento relevante incluso en ausencia de una interrupción efectiva del suministro. La Ilustración 4 representa esta convergencia entre la gestión de integridad física y la gestión de seguridad de información.



Ilustración 4. Diagrama de Convergencia Normativa SGIIE-SGSI. (Fuente: Propia generada con IA)

5.7.2 Integración de la ciberseguridad en ciclo de vida del activo

La ciberseguridad, bajo el marco normativo vigente, no constituye un sistema de gestión autónomo, sino que debe integrarse operativamente en los sistemas existentes de gestión de integridad de las instalaciones eléctricas. En el sector generación, este rol lo cumple el **Sistema de Gestión de Integridad de Instalaciones Eléctricas (SGIIE)** definido por el **Pliego Técnico Normativo RPTD N.º 17** [31], el cual adopta un enfoque de ciclo de vida conforme a los principios de la gestión de activos físicos (ISO 55001).

Desde esta perspectiva, los deberes mandatorios del Artículo 8º de la Ley N.º 21.663 [6] deben ser interpretados como requisitos transversales que se insertan en cada una de las etapas del ciclo de vida del activo eléctrico, reforzando su integridad funcional y su resiliencia operacional.

A continuación, se describen las fases del ciclo de vida del activo y cómo la Ley y el Estandar CEN se complementa con cada fase:

- En planificación y diseño, la Ley introduce el principio de seguridad por diseño (Art. 3º, N.º 8), operacionalizado mediante la definición temprana de Perímetros de Seguridad Electrónica exigidos por el CIP-005.
- En adquisición, el deber de gestión de riesgos (Art. 8º, letra a) se traduce en cláusulas contractuales de ciberseguridad hacia proveedores de sistemas de control, alineadas con el CIP-013 (gestión de cadena de suministro).
- En construcción y puesta en servicio, se valida la implementación efectiva de los controles de diseño y adquisición (CIP-005/CIP-007) antes de la energización.

- En operación, el SGSI de la ANCI y el SGIIE de la SEC convergen explícitamente, apoyados en los controles de monitoreo (CIP-007) y respuesta a incidentes (CIP-008).
- En mantenimiento, la gestión de parches y hardening del CIP-007 se integra a los planes de mantenimiento preventivo (CPMP) auditados por la SEC.
- En retiro, los controles de gestión de accesos (CIP-004) y protección de información (CIP-011) controlan los riesgos residuales de credenciales y configuraciones persistentes. La Tabla 9 sintetiza esta correspondencia por fase.

Esta articulación no es una opción metodológica sino una exigencia legal: el Artículo 26° establece que, ante normas sectoriales con efectos equivalentes o superiores, prevalecen las disposiciones de la autoridad sectorial.

El SGSI de la ANCI es, en consecuencia, el complemento lógico del SGIIE de la SEC: uno protege la capa digital, el otro preserva la integridad física del activo.

5.7.3 Mapeo de indicadores

El **Sistema de Gestión de Seguridad de la Información (SGSI)** exigido por la ANCI debe entenderse como un **subsistema generador de eventos, registros y datos técnicos**, los cuales alimentan directamente los indicadores de desempeño del Anexo Técnico del RPTD N° 17. La ciberseguridad no crea un sistema paralelo de evaluación, sino que provee insumos críticos que deben reflejarse en los indicadores de integridad auditados por la autoridad sectorial.

Sobre la base de esta interacción, los principales indicadores del Anexo Técnico del RPTD-17 reciben insumos directos de la gestión de ciberseguridad se muestran en la Tabla 7.

Tabla 7. Mapeo de indicadores SGIIE afectados por obligaciones de ciberseguridad OT (Fuente: Elaboración Propia)

Indicador RPTD N.º 17	Nombre completo	Fuente en Marco CiberOT	Mecanismo de integración
XX-CIAC	Cantidad de Incidentes de Activos Críticos	Ley 21.663 — DS 295 (reporte de incidentes)	Los incidentes reportados bajo el DS 295 que involucran sistemas OT se incorporan a su cómputo, evitando su sub-declaración desde la óptica de integridad.
XX-TICB	Tasa de Investigación de Causas Basales	Ley 21.663 — DS 295 (Informe Final de Incidente)	El Informe Final de Incidente exigido por el mismo decreto constituye el análisis de causa basal que lo alimenta.

XX-CPMP	Cumplimiento del Plan de Mantenimiento Preventivo	Estándar CEN — CIP-007 (gestión de parches, hardening y cambios)	Las actividades exigidas por el CIP-007 se integran formalmente al Plan de Mantenimiento Preventivo.
----------------	---	--	--

5.7.4 Tensiones operativas

Esta integración no está exenta de tensión. La Norma Técnica de Seguridad y Calidad de Servicio (NTSyCS) establece exigencias explícitas de disponibilidad física para las instalaciones de generación, las cuales son monitoreadas y sancionadas por el Coordinador Eléctrico Nacional (CEN). En particular, el Artículo 5-54 define límites máximos para la Indisponibilidad Forzada de Generación (HFORg) y la Indisponibilidad Programada de Generación (HPROg) [26]. La lógica regulatoria es inequívoca: las salidas de servicio no programadas son penalizadas, mientras que las indisponibilidades programadas deben ser previamente coordinadas y justificadas ante el sistema.

En sistemas OT, las actividades de parcheo y hardening exigidas por el CIP-007 no siempre pueden ejecutarse en caliente: su aplicación puede requerir el reinicio de estaciones o controladores, generando pérdida temporal de control y de visibilidad para el CEN.

El operador enfrenta así un dilema: postergar el parcheo y asumir el riesgo de un incidente XX-CIAC, o ejecutarlo y asumir el riesgo de afectar los índices HFORg/HPROg. La evidencia operacional muestra que una vulnerabilidad no mitigada puede derivar en una indisponibilidad forzada de impacto económico y regulatorio superior al de una ventana coordinada.

La Ley 21.663, al calificar a las generadoras como OIV, eleva estas actividades a obligación de seguridad pública: el desafío no es optar entre disponibilidad y ciberseguridad, sino coordinarlas operativamente con el CEN.

5.7.5 Dimensión económica

El Anexo Técnico del Pliego Técnico Normativo RPTD N.º 17 incorpora, dentro de los indicadores de desempeño del Sistema de Gestión de Integridad de Instalaciones Eléctricas (SGIIE), métricas de carácter económico destinadas a evaluar la coherencia entre el esfuerzo financiero realizado por el operador y el valor de los activos eléctricos gestionados. En este contexto, los indicadores XX-CAPV y XX-OPEV permiten capturar cómo las decisiones de inversión y gasto operacional inciden directamente en la preservación de la integridad de los Ciber-Sistemas SEN.

Las medidas exigidas por el Artículo 8º —diodos de datos, firewalls industriales,

segmentación OT, redundancia de centros de control— califican como CAPEX de renovación bajo el SGIIE, elevando el indicador XX-CAPV. Este incremento es económicamente justificable: mitiga el riesgo de pérdida de valor del activo por incidentes ciberfísicos o indisponibilidades forzadas prolongadas.

El cumplimiento sostenido genera además un OPEX estructural: monitoreo continuo 24/7 (SOC), auditorías del Art. 28°, licencias de software y horas-hombre especializadas.

Este aumento del OPEV no constituye una ineficiencia, es marginal frente a los pasivos evitados que pueden tener órdenes de magnitud superiores al costo normal de operación de una central. En la Tabla 8 algunos ejemplos del componente OPEX vs los riesgos mitigados

Tabla 8. Descomposición del OPEX asociado a ciberseguridad dentro del O&M del activo (Fuente: Elaboración Propia)

Componente OPEX	de	Ejemplos típicos	Función económica	Riesgo mitigado
Vigilancia monitoreo	y	SOC 24/7, correlación de eventos	Detección temprana	Impacto de incidentes
Cumplimiento regulatorio		Auditorías, certificaciones	Evitar sanciones	Multas (UTM)
O&M lógico del activo		Licencias, parches, hardening	Preservar función requerida	CIAC / indisponibilidad
Preparación respuesta	y	Planes, simulacros	Limitar daño máximo	Racionamiento / pérdida de valor

La caracterización de la ciberseguridad como componente diferenciado del CAPEX y del OPEX del activo constituye el fundamento conceptual sobre el que se construye el análisis cuantitativo de esta investigación.

5.8 Síntesis del Capítulo

El recorrido desarrollado en las secciones precedentes permite concluir que el marco regulatorio de ciberseguridad aplicable al sector de generación eléctrica chileno está compuesto por dos instrumentos complementarios —la Ley N.º 21.663 y el Estándar CEN— cuya articulación no es redundante sino funcional: la ley establece la gobernanza, los deberes generales y el régimen de responsabilidad; el Estándar CEN operacionaliza esas obligaciones en controles técnicos específicos para el entorno OT del sector eléctrico, habilitado expresamente por el Art. 26° de

la misma ley.

Este marco se encuentra en plena implementación: 147 empresas del sector eléctrico han sido calificadas como OIV mediante la Resolución Exenta N.º 87, y las Instrucciones Generales N.º 1, 3 y 4 de la ANCI precisaron durante 2025 los deberes del Delegado de Ciberseguridad y las medidas mínimas de contención de incidentes.

La sistematización de ambos marcos en la matriz de convergencia normativa (sección 5.5) demuestra que el cumplimiento simultáneo de la Ley y el Estándar CEN se resuelve en 17 controles técnicos integrados, lo que reduce la duplicación de costos: un mismo control satisface obligaciones de ambos instrumentos.

El marco conserva, sin embargo, una naturaleza parcialmente incompleta: el Reglamento de Auditoría del Art. 28º y la Norma Técnica de la CNE —desarrollados en la sección 5.6— aún no han sido publicados, lo que introduce incertidumbre en la planificación del cumplimiento para los operadores del sector.

Con esto se da por desarrollado el Objetivo Específico 1: el análisis regulatorio del marco de ciberseguridad aplicable al sector de generación eléctrica chileno, identificando las obligaciones vigentes, su instrumento de origen y su perfil cualitativo de costo.

El análisis desarrollado en la sección 5.7 muestra que la ciberseguridad industrial no es un componente periférico, sino una dimensión estructural de la integridad física de las instalaciones eléctricas. El estudio de la interacción entre la Ley N.º 21.663 y el RPTD N.º 17 permite identificar tres resultados: el SGSI exigido por el Artículo 8º y el SGIIE fiscalizado por la SEC se articulan de forma complementaria, proveyendo el primero la visibilidad lógica necesaria para preservar la función requerida del activo; los incidentes de ciberseguridad reportados bajo el DS 295 se integran en los indicadores XX-CIAC y XX-TICB, y el hardening y parcheo del CIP-007 califica como mantenimiento preventivo (XX-CPMP); y el cumplimiento normativo impacta los indicadores XX-CAPV y XX-OPEV como inversión en preservación de valor del activo, no como gasto accesorio, frente a pasivos como los costos de racionamiento del DFL N.º 4 o multas de hasta 40.000 UTM.

Con esto se da por desarrollado el Objetivo Específico 2: la integración de las exigencias de ciberseguridad de la Ley 21.663 y el Estándar CEN con el Sistema de Gestión de Integridad de Instalaciones Eléctricas fiscalizado por la SEC.

Los resultados normativos y técnicos sistematizados en este capítulo constituyen la línea base sobre la cual se desarrollan los objetivos siguientes: la comparación con estándares internacionales y el diagnóstico de brechas (Cap. 6), y la estimación del costo de cumplimiento (Cap. 7).

6. EVALUACIÓN COMPARADA Y MATRIZ DE BRECHAS

El presente Capítulo desarrolla el Objetivo Específico 3 y 4: el análisis comparativo del marco regulatorio chileno con estándares internacionales relevantes de ciberseguridad industrial (OE3), y la identificación de brechas que condicionan su implementación efectiva en el sector de generación eléctrica (OE4).

El análisis opera mediante un doble eje metodológico. El eje legal contrasta la Ley N.º 21.663 con la Directiva NIS2 de la Unión Europea y la Resolución ANEEL RN 964 de Brasil, evaluando la coherencia en términos de naturaleza del instrumento, gobernanza institucional, sujetos obligados y mecanismo de designación, gestión de riesgos, reportabilidad y régimen sancionatorio. El eje técnico contrasta el Estándar CEN con NERC-CIP —su fuente directa— y con IEC 62443, evaluando los cinco dominios de ciberseguridad OT: identificación de activos, protección, detección, respuesta y recuperación. El NIST CSF se utiliza como referencia conceptual de fondo, no como benchmark directo de comparación.

El capítulo se organiza en siete secciones: tras precisar el propósito y método (6.1), se desarrolla el eje legal (6.2) y el eje técnico (6.3) del OE3. A continuación se establece el método del Gap Analysis (6.4), la matriz de brechas resultante y su priorización por responsable (6.5) dando cumplimiento al OE4. El capítulo cierra con una síntesis única (6.6) que integra ambos objetivos.

6.1 Propósito y método

El OE3 busca determinar si los principios, enfoques y dominios técnicos de la normativa chilena se alinean conceptualmente con las mejores prácticas internacionales aplicables a sistemas de control industrial (OT), particularmente en la protección de la infraestructura OT y la continuidad operacional. El análisis se desarrolla desde un enfoque funcional, centrado en la comparación de dominios técnicos y objetivos de control, y no mediante una revisión literal o artículo-a-artículo de los cuerpos normativos considerados. Para ello, el análisis adopta un enfoque metodológico dual: un eje legal, que compara la Ley N.º 21.663 con marcos jurídicos de naturaleza equivalente de otras jurisdicciones, y un eje técnico, que contrasta el Estándar CEN con sus referentes internacionales en materia de sistemas de control industrial (OT). Este criterio responde a una exigencia metodológica básica: la comparación es válida cuando se realiza entre instrumentos de naturaleza homogénea.

En este sentido, lo que se compara es, en el eje legal, el grado de correspondencia entre la Ley 21.663 y marcos jurídicos equivalentes en términos de alcance, gobernanza y gestión de riesgos; y en el eje técnico, la cobertura de dominios OT, el nivel de prescripción técnica y la aplicabilidad al sector eléctrico entre el Estándar CEN y sus referentes internacionales. Por el contrario, no se comparan mecanismos

específicos de implementación, arquitecturas tecnológicas particulares, ni niveles reales de adopción por parte de empresas u operadores individuales.

Es importante delimitar explícitamente que el análisis desarrollado en esta sección no constituye una auditoría de cumplimiento normativo, no persigue fines de certificación, ni corresponde a una evaluación de madurez en ciberseguridad. El foco del OE3 se restringe deliberadamente a una evaluación de coherencia técnica y regulatoria, entendida como la consistencia conceptual entre marcos normativos, y no como una medición de desempeño, eficacia o nivel de seguridad alcanzado en la práctica.

El OE3 cumple un rol habilitador dentro de la metodología general: sus resultados constituyen el insumo para el diagnóstico de brechas del OE4, desarrollado en las secciones 6.4 a 6.6.

El eje legal se guía por la pregunta: *¿La Ley 21.663 recoge, a nivel de diseño jurídico, los estándares de gobernanza y gestión de riesgos que marcos equivalentes de otras jurisdicciones consideran mínimos para infraestructuras críticas?*, por su parte el eje técnico se organiza en torno a cinco dominios técnicos de ciberseguridad OT, entendidos como conjuntos coherentes de funciones críticas que permiten preservar la operación segura y continua de los sistemas industriales. Bajo esta lógica, la pregunta metodológica central del eje técnico es: *¿El Estándar CEN cubre, a nivel de dominios técnicos OT, los mismos ámbitos críticos que sus referentes internacionales directos?*

Para operacionalizar la comparación se definen dos conjuntos de criterios. Para el **eje legal** se utilizan las mismas siete dimensiones definidas en el Cap. 5 (sección 5.1) para el análisis de la Ley 21.663: naturaleza y fuerza obligatoria del instrumento, alcance y sujetos obligados, gobernanza institucional, gestión de riesgos y SGSI, reporte de incidentes y plazos, infracciones y sanciones, y principio de proporcionalidad. El uso de estas mismas dimensiones permite comparar el marco chileno con sus referentes internacionales bajo el mismo criterio con que se caracterizó la Ley 21.663 en el Cap. 5. Para el **eje técnico** se utilizan los cinco dominios técnicos de ciberseguridad OT definidos en la sección 6.3: identificación, protección, detección, respuesta y recuperación, y cada dominio se evalúa conforme a criterios de Orientación OT, Nivel de prescripción técnica y aplicabilidad al sector de generación eléctrica.

A partir de lo anterior, la correspondencia entre los marcos analizados en cada eje se evalúa utilizando una escala cualitativa de cuatro niveles, empleada de forma homogénea en todo el capítulo:

- Convergencia: el dominio o dimensión es abordado de forma equivalente, tanto en objetivo como en enfoque técnico.
- Convergencia parcial: el dominio o dimensión es abordado, pero con menor

nivel de profundidad, prescripción o especificidad OT.

- Divergencia: el dominio o dimensión existe en el marco de referencia, pero está ausente o débilmente desarrollado en el marco chileno.
- No abordado: el dominio o dimensión no es tratado explícita ni implícitamente en ninguno de los marcos comparados.

Esta escala no representa una métrica de cumplimiento ni de madurez, sino una herramienta analítica para evaluar coherencia técnica relativa.

Los marcos a comparar son: en el eje legal, la Directiva (UE) 2022/2555 (NIS2) y la Resolución Normativa ANEEL N.º 964 (Brasil); en el eje técnico, NERC-CIP — fuente directa del Estándar CEN— e IEC 62443; y como referencia conceptual, el NIST CSF 2.0, cuyas cinco funciones estructuran los dominios técnicos OT definidos en la sección 6.3. El detalle de cada marco se presenta en las secciones 6.2 y 6.3, donde se desarrolla su comparación. La Tabla 9 refleja visualmente el resumen de lo anterior.

Tabla 9. Enfoque metodológico del análisis comparativo OE3 (Fuente: Elaboración Propia)

Dimensión	Eje Legal	Eje técnico
Marcos comparados	Ley 21.663 / NIS2 / ANEEL RN 964	Estándar CEN / NERC-CIP / IEC 62443
Criterios de comparación	Naturaleza, alcance y sujetos obligados, gobernanza, proporcionalidad, gestión de riesgos, reporte de incidentes, infracciones/sanciones	Identificación, protección, detección, respuesta y recuperación
Referencias conceptuales	NIST CSF 2.0	NIST CSF 2.0
Escala de análisis	Convergencia / Parcial / Divergencia / No abordado	Convergencia / Parcial / Divergencia / No abordado
Exclusiones	Auditoría, certificación, evaluación de madurez	Auditoría, certificación, evaluación de madurez

6.2 Eje legal: Ley 21.663, NIS2 y ANEEL RN 964

El presente análisis examina la Ley Marco de Ciberseguridad (Ley N.º 21.663) en perspectiva con dos marcos jurídicos internacionales de naturaleza equivalente: la Directiva (UE) 2022/2555 (NIS2) y la Resolución Normativa ANEEL N.º 964 de Brasil. La comparación se estructura en torno a siete dimensiones jurídicas definidas

en la sección 6.1, sistematizadas en la Tabla 10.

6.2.1 Naturaleza del instrumento

Los tres marcos comparten su carácter jurídico obligatorio, aunque con naturalezas distintas: la Ley 21.663 es una ley marco multisectorial que delega su especificación técnica al Estándar CEN; NIS2 es una directiva multisectorial que requiere transposición nacional; la RN 964 es una resolución sectorial eléctrica de aplicación directa, diseñada específicamente para el sector, sin necesidad de mecanismos de designación intersectorial. **Correspondencia:** Convergencia parcial.

6.2.2 Mecanismos de gobernanza institucional

La Ley 21.663 centra su arquitectura en la ANCI, con roles complementarios del CSIRT de Gobierno y los CSIRT sectoriales, y define la gobernanza interna mediante el Delegado de Ciberseguridad. NIS2 descansa en una autoridad nacional competente por Estado miembro articulada con la red europea de coordinación. La RN 964 opera con ANEEL como regulador sectorial único. Los tres marcos convergen en exigir gobernanza interna con responsabilidad explícita y una autoridad externa de supervisión. **Correspondencia:** Convergencia con NIS2; Convergencia parcial con ANEEL.

6.2.3 Alcance y sujetos obligados

La Ley 21.663 designa sujetos obligados mediante calificación administrativa de la ANCI (DS 285) —ICI y, con obligaciones reforzadas, OIV—, lo que introduce mayor discrecionalidad que NIS2 (criterios objetivos de tamaño y sector, aplicación directa) y que la RN 964 (designación directa por tipo de agente regulado). Esta discrecionalidad constituye la divergencia más relevante del eje legal frente a ambos referentes. **Correspondencia:** Convergencia parcial con NIS2; Divergencia con ANEEL.

6.2.4 Principio de proporcionalidad

La Directiva NIS2 establece que los Estados miembros deben disponer que determinadas pequeñas empresas y microempresas que cumplan criterios específicos que pongan de manifiesto su papel clave para la sociedad, la economía o para determinados sectores o tipos de servicios, queden comprendidas en el ámbito de aplicación de la Directiva. La NIS2 diferencia explícitamente entre entidades esenciales e importantes, con regímenes de supervisión y sanciones distintos según la categoría.

La Ley 21.663 lo incorpora de forma explícita, diferenciando obligaciones entre ICI y OIV según naturaleza, tamaño y complejidad del operador, aunque su desarrollo reglamentario está pendiente. NIS2 diferencia formalmente entre entidades esenciales e importantes, con regímenes de supervisión distintos. La RN 964 aplica una proporcionalidad implícita, según relevancia y complejidad de la instalación, sin categorización formal. **Correspondencia:** Convergencia parcial con ambos.

6.2.5 Gestión de riesgos

La Ley 21.663 exige a los OIV un SGSI, planes de continuidad y auditorías periódicas, delegando el contenido mínimo al desarrollo reglamentario y al Estándar CEN. NIS2 es la más prescriptiva de los tres marcos, con contenido mínimo explícito en la propia Directiva (gestión de la cadena de suministro, seguridad en el desarrollo de sistemas, entre otros). La RN 964 exige política de seguridad, clasificación de información y planes de continuidad. Los tres convergen en un ciclo de gestión de riesgos basado en identificación de amenazas y mejora continua. **Correspondencia:** Convergencia parcial con ambos.

6.2.6 Reporte de incidentes

La Ley 21.663, mediante el DS 295, establece plazos diferenciados según la criticidad del evento. NIS2 es la más prescriptiva de los tres marcos, con un procedimiento escalonado explícito: alerta temprana en 24 horas, notificación ampliada en 72 horas e informe final en un mes. La RN 964 exige notificación al equipo de coordinación sectorial designado, sin plazos específicos. Los tres convergen en la obligación de reporte a una autoridad competente. **Correspondencia:** Convergencia parcial con ambos.

6.2.7 Régimen sancionatorio

La Ley 21.663 establece su propio régimen en el Título V —infracciones leves, graves y gravísimas, multas de hasta 40.000 UTM aplicadas por la ANCI. NIS2 cuantifica su régimen en el Art. 34, con multas de hasta 10 millones de euros o 2% de la facturación mundial anual para entidades esenciales. La RN 964 no contiene régimen sancionatorio propio: remite a las potestades generales de ANEEL bajo la Ley N.º 9.427/1996 —la divergencia más marcada de esta dimensión. **Correspondencia:** Convergencia con NIS2; Divergencia con ANEEL.

La Tabla 10 sintetiza el análisis comparativo desarrollado en los párrafos precedentes, sistematizando las siete dimensiones jurídicas evaluadas más el régimen sancionatorio para los tres marcos considerados. La tabla permite visualizar de forma estructurada los puntos de convergencia y divergencia entre la

Ley 21.663, la NIS2 y la RN 964 de ANEEL.

Tabla 10. Matriz de correspondencia legal: Ley 21.663, NIS2 y ANEEL RN N.º 964 (Fuente: Elaboración Propia)

Dimensión	Ley 21.663 (Chile)	NIS2 — UE	ANEEL RN N.º 964 (Brasil)	Conv. NIS2	Conv. ANEEL
Naturaleza del instrumento	Ley marco multisectorial obligatoria	Directiva multisectorial obligatoria	Resolución sectorial eléctrica obligatoria	Convergencia	Convergencia parcial
Gobernanza institucional	ANCI + CSIRT Gobierno/sectoriales + Delegado de Ciberseguridad	Autoridad nacional + CSIRT + red europea	ANEEL como regulador único	Convergencia	Convergencia parcial
Alcance y designación	Calificación administrativa ANCI (DS 285); ICI/OIV, obligaciones reforzadas solo a OIV. Mayor discrecionalidad	Criterios objetivos de tamaño/sector, aplicación directa; Esenciales/Importantes	Designación directa por tipo de agente regulado; sin categorización formal	Convergencia parcial	Divergencia
Proporcionalidad	Explícita en la ley; reglamento pendiente	Formal por categoría, operativa	Implícita, sin categorización formal	Convergencia parcial	Convergencia parcial
Gestión de riesgos	SGSI + continuidad + auditorías. Detalle delegado al reglamento y CEN	Más prescriptiva; contenido mínimo explícito	Política de seguridad + clasificación + continuidad	Convergencia parcial	Convergencia parcial
Reporte de incidentes	Plazos por DS 295 según criticidad	Más prescriptiva: 24h / 72h / 1 mes	Notificación sin plazos definidos	Convergencia parcial	Convergencia parcial
Régimen sancionatorio	Título V — leves/graves/gravísimas, hasta 40.000 UTM (ANCI)	Art. 34 — hasta 10M€ o 2% facturación	Sin régimen propio; remite a Ley N.º 9.427/1996	Convergencia	Divergencia

6.3 Eje técnico: Estándar CEN, NERC-CIP e IEC 62443

El análisis técnico se organiza en torno a los cinco dominios técnicos de ciberseguridad OT —identificación, protección, detección, respuesta y recuperación—, consistentes con las cinco funciones operativas originales del NIST Cybersecurity Framework [32] (ver Ilustración 5), comparando el Estándar CEN con NERC-CIP —su fuente normativa, adoptada directamente en sus trece controles

CIP— y con IEC 62443 —referente técnico OT de alcance multisectorial, que permite evaluar si ese enfoque sectorial cubre los dominios que un estándar industrial general considera esenciales.

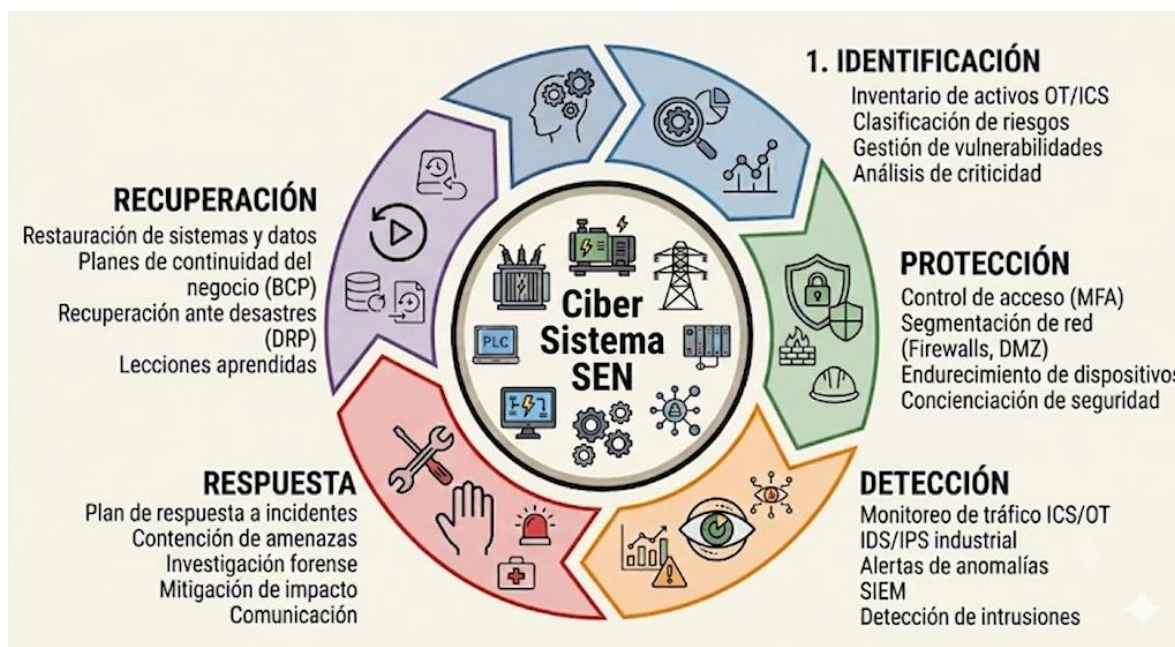


Ilustración 5. Dominios técnicos de ciberseguridad OT. (Fuente: Propia generada con IA)

6.3.1 Dominio 1: Identificación de activos críticos

Identificación de activos críticos (CIP-002). El Estándar CEN sigue fielmente a NERC-CIP: categoriza los Ciber Sistemas SEN por impacto (alto/medio/bajo) bajo un umbral objetivo de 15 minutos. IEC 62443 exige un inventario equivalente para definir zonas y conductos, pero sin prescribir criterios de impacto cuantitativos —define el qué, no el cómo. **Correspondencia:** Convergencia con NERC-CIP; Convergencia parcial con IEC 62443.

6.3.2 Dominio 2: Protección – segmentación, hardening y control de accesos

Protección — segmentación y control de accesos (CIP-005/CIP-007). El Estándar CEN define el Perímetro de Seguridad Electrónica y sus Puntos de Acceso, en línea directa con NERC-CIP. IEC 62443 logra un objetivo equivalente mediante zonas y conductos, pero gradúa la protección por Niveles de Seguridad (SL) —concepto que el Estándar CEN no incorpora, graduando en cambio por nivel de impacto del activo. **Correspondencia:** Convergencia con NERC-CIP; Convergencia parcial con IEC 62443.

6.3.3 Dominio 3: Detección y monitoreo

Detección y monitoreo (CIP-007). El Estándar CEN —adopción directa de NERC-CIP— orienta la detección a accesos no autorizados y eventos anómalos dentro del perímetro electrónico, sin extenderse al proceso físico. IEC 62443 amplía este alcance incorporando detección de anomalías en el proceso físico, relevante ante ataques que manipulan el proceso sin dejar huella detectable en red. **Correspondencia:** Convergencia con NERC-CIP; Convergencia parcial con IEC 62443.

6.3.4 Dominio 4: Respuesta a incidentes

Respuesta a incidentes (CIP-008). El Estándar CEN exige planes de respuesta con roles definidos y coordinación con el Coordinador del sistema. IEC 62443 distingue entre respuesta al incidente de seguridad y respuesta operacional (mantener el proceso) —ambos énfasis resultan complementarios en generación. **Correspondencia:** Convergencia con NERC-CIP y con IEC 62443, con diferencia de énfasis operacional/sistémico.

6.3.5 Dominio 5: Recuperación y continuidad operacional

Recuperación y continuidad operacional (CIP-009). El Estándar CEN centra la recuperación en los Ciber Sistemas SEN y sus respaldos de información. IEC 62443 extiende la recuperación al proceso industrial completo, incorporando validación de integridad de los activos físicos antes de reanudar operación. **Correspondencia:** Convergencia con NERC-CIP; Convergencia parcial con IEC 62443.

6.3.6 Síntesis del análisis técnico por dominios

El análisis desarrollado permite identificar tres conclusiones. **Primero**, la correspondencia entre el Estándar CEN y NERC-CIP es estructuralmente alta en todos los dominios —esperable dado que el primero es adaptación directa del segundo—, con diferencias solo de contexto (SEN chileno vs. BES norteamericano), no de contenido técnico. **Segundo**, la correspondencia con IEC 62443 es de convergencia parcial: ambos comparten objetivos equivalentes, pero IEC 62443 extiende sistemáticamente cada dominio hacia el proceso físico industrial, mientras el Estándar CEN mantiene el foco en los ciber sistemas. **Tercero**, el Estándar CEN no incorpora dos elementos que IEC 62443 sí considera estructurales: el modelo de Niveles de Seguridad (SL) y la extensión de detección y recuperación al proceso físico —diferencias que no constituyen brechas de protección, pero sí ámbitos de posible fortalecimiento ante arquitecturas OT heterogéneas. La Tabla 11 sistematiza el nivel de correspondencia por dominio. La Tabla 11 sistematiza el nivel de correspondencia por dominio.

Tabla 11. Matriz de correspondencia técnica: Estándar CEN, NERC-CIP e IEC62443 por Dominio OT (Fuente: Elaboración Propia)

Dominio técnico OT	Estándar CEN (Chile, oct. 2022)	NERC-CIP (fuente directa del CEN)	IEC 62443 (referente OT alternativo)	Convergencia CEN vs NERC-CIP	Convergencia CEN vs IEC 62443
Identificación de activos críticos	CIP-002: categoriza Ciber Sistemas SEN en tres niveles de impacto (alto, medio, bajo) según su capacidad de afectar la operación segura del SEN dentro de un umbral de 15 minutos. El nivel de impacto determina el conjunto de controles exigibles.	BES Cyber System categorization: misma clasificación por impacto sobre la confiabilidad del sistema eléctrico, con criterios objetivos y auditables. Fuente directa del CIP-002 del Estándar CEN — sin diferencias sustantivas.	Exige inventario detallado de activos del IACS y definición de zonas y conductos como paso previo a la protección. No prescribe criterios de impacto sectoriales específicos ni umbrales cuantitativos — la clasificación se adapta al contexto industrial.	Convergencia	Convergencia parcial
Protección — segmentación, hardening y control de accesos	CIP-005: define el Perímetro de Seguridad Electrónica (PSE) y los Puntos de Acceso Electrónico (PAE). CIP-007: regula puertos y servicios habilitados, gestión de parches, autenticación de usuarios y gestión de eventos de seguridad.	CIP-005 y CIP-007 de NERC-CIP son la fuente directa de los controles equivalentes del Estándar CEN. Mismos requisitos de PSE y PAE con igual nivel de prescripción — sin diferencias sustantivas de contenido.	Modelo de zonas y conductos con defensa en profundidad. Incorpora Nivel de Seguridad (SL) para graduar requisitos según el riesgo del sistema — metodología más granular que el PSE del CEN. No prescribe umbrales de acceso equivalentes al PAE.	Convergencia	Convergencia parcial
Detección y monitoreo	CIP-007 (gestión de eventos de seguridad): exige registro de logs, revisión periódica de eventos y umbrales para generación de alertas dentro del PSE. La detección se orienta a identificar accesos no autorizados y eventos anómalos en los ciber sistemas.	Mismos requisitos de CIP-007 que el Estándar CEN — adopción directa sin modificaciones sustantivas en este dominio. Ambos comparten el mismo enfoque y alcance: detección de eventos en el perímetro electrónico y ciber sistemas, sin extender el monitoreo al proceso físico.	Monitoreo continuo, correlación de eventos y análisis de comportamiento en redes industriales (IEC 62443-3-3). Incorpora detección de anomalías en el proceso físico — permite identificar ataques que manipulen el proceso sin generar eventos de red detectables. Alcance mayor que CEN y NERC-CIP.	Convergencia	Convergencia parcial
Respuesta a incidentes	CIP-008: planes de respuesta con roles y responsabilidades definidos, procedimientos de notificación al Coordinador, coordinación con el operador del SEN y pruebas periódicas de los planes.	CIP-008 de NERC-CIP es la fuente directa del control equivalente del CEN. Mismos requisitos con foco en preservar la confiabilidad del sistema eléctrico y coordinar con el operador — sin diferencias sustantivas.	Respuesta integrada en el ciclo de vida de seguridad del IACS. Distingue respuesta al incidente de seguridad (erradicar amenaza) y respuesta operacional (mantener proceso). Exige planes formales, roles definidos y pruebas periódicas equivalentes al CIP-008.	Convergencia	Convergencia
Recuperación y continuidad operacional	CIP-009: planes de recuperación para Ciber Sistemas SEN con condiciones de activación, roles, procedimientos de recuperación de respaldos y pruebas periódicas. El alcance se centra en los ciber sistemas.	CIP-009 de NERC-CIP es la fuente directa del control equivalente del CEN. Mismos requisitos centrados en los ciber sistemas — no incluye explícitamente validación de integridad de activos físicos antes de reanudar operación.	Recuperación integrada en el ciclo de vida de seguridad. Incluye validación de integridad de activos físicos controlados antes de reanudar operación. Exige planes formales y pruebas periódicas equivalentes al CIP-009.	Convergencia	Convergencia parcial

6.4 Análisis de Brechas (Gap Analysis)

La presente sección ejecuta el **Objetivo Específico 4 (OE4)** de la investigación, cuyo propósito es identificar y clasificar las brechas que limitan la efectividad práctica del marco regulatorio chileno en el sector de generación eléctrica. A diferencia del OE3 —que evaluó la coherencia normativa del marco frente a estándares internacionales— el OE4 pregunta por la viabilidad de implementación: dado que el marco es coherente en el papel, ¿qué obstáculos impiden que un operador lo cumpla efectivamente en su realidad tecnológica y operativa?

El diagnóstico opera en dos planos complementarios. El plano técnico, diferenciado por arquitectura de central (Grupos A, B y C), y uno normativo-institucional, transversal a todos los operadores, que identifica los vacíos del marco que ninguna inversión del operador puede resolver, y los solapamientos donde dos instrumentos exigen lo mismo duplicando el esfuerzo. Los estándares internacionales —NERC-CIP e IEC 62443— se invocan únicamente como referencia puntual para iluminar el origen de cada obstáculo o señalar cómo otros marcos lo han resuelto, no como objeto directo de comparación, función ya cumplida por el OE3.

6.4.1 Enfoque metodológico del Análisis de brechas de cumplimiento

El análisis comparativo del OE3 en las secciones 6.2 y 6.3 establecieron que el marco regulatorio chileno es, en lo sustantivo, coherente con los estándares internacionales de referencia. Sobre esa base, el OE4 no busca volver a comparar el marco chileno con NERC-CIP o IEC 62443, sino que busca identificar las brechas que afectan la efectividad práctica de la ley en el contexto operativo del sector de generación chileno.

Para ello, el diagnóstico se estructura en torno a los cinco dominios técnicos de ciberseguridad OT definidos en la sección 6.3— Identificación, Protección, Detección, Respuesta y Recuperación — y se diferencia por la tipología de central establecida en la sección 4.3: Grupo A (Solar/Eólica), Grupo B (Térmica/Hidráulica) y Grupo C (subestaciones/SMMC), reconociendo que la viabilidad de cumplimiento depende estructuralmente de la arquitectura de control de cada tipo de instalación.

Cada brecha identificada es evaluada conforme a tres criterios:

- **Impacto operativo:** consecuencia de la brecha sobre la continuidad operacional del activo de generación.
- **Criticidad de Implementación:** grado en que la brecha está condicionada por la arquitectura OT específica de cada grupo y la dificultad de resolverla.
- **Costo estimado de mitigación:** categorización del esfuerzo económico

requerido para cerrar la brecha, expresada como Alto / Medio / Bajo y vinculada con los drivers del modelo CAC.

Estos tres criterios se aplican de forma diferenciada según la naturaleza del hallazgo. Las brechas técnicas, al originarse en la arquitectura de control del operador, se evalúan en los tres criterios y se diferencian por grupo. Los vacíos normativos y los solapamientos, en cambio, son transversales: no dependen de la arquitectura de ninguna central en particular, por lo que el criterio de dependencia tecnológica no les resulta aplicable y se evalúan principalmente por su criticidad. La Matriz de brechas (6.5) sistematiza ambos tipos de hallazgo en una sola tabla, identificando en cada caso a quien afeta principalmente.

El resultado del análisis se expresa en cuatro categorías de hallazgo, cuya distinción metodológica es la siguiente (Tabla 12):

Tabla 12. Tabla metodológica de categorías de hallazgo del Gap Analysis OE4. (Fuente: Elaboración propia).

Categoría	Definición	Recomendación
Vacío normativo	El marco regulatorio no regula algo que debería. Lo genera el legislador o regulador.	Se cierra con nueva reglamentación o instrucción de la ANCI.
Brecha técnica	El operador no puede implementar lo exigido dado su contexto tecnológico.	Se cierra con inversión tecnológica o compensating controls.
Brecha institucional	El ecosistema no provee condiciones para el cumplimiento.	Se cierra con desarrollo de mercado, formación o guías técnicas.
Solapamiento	Dos instrumentos exigen lo mismo al mismo operador, duplicando esfuerzo.	Se resuelve con coordinación interinstitucional o reconocimiento mutuo.

6.5 Matriz de Brechas

El diagnóstico aplicado a los cinco dominios técnicos (6.3) y a la arquitectura institucional del marco (Cap. 5) ha permitido identificar 12 hallazgos, de estos y de acuerdo a la clasificación previa se han separado en 4 vacíos normativos, 3 brechas técnicas, 2 brechas institucionales y 3 solapamientos. La Tabla 13 los sistematiza, indicando además la vía de resolución y el actor responsable de cada uno.

Tabla 13. Matriz de brechas del Gap Analysis OE4 (Fuente: Elaboración propia)

Tipo	Brecha	Impacto operativo	Criticidad de implementación	Costo estimado de mitigación	Afecta a	Cómo se cierra	Responsable
Vacío normativo	Reglamento Art. 28° no publicado: sin él, no existe criterio oficial para certificar cumplimiento ante la autoridad	Bajo	Alta	Bajo	Transversal	Publicar el reglamento de auditoría y certificación	ANCI
Vacío normativo	Ausencia de excepción técnica (TFE): el Estándar CEN no define qué hacer cuando un control no es técnicamente factible	Medio	Alta	Bajo	Transversal (Grupo B)	Incorporar compensating controls en el Estándar CEN	CEN
Vacío normativo	Criterios sectoriales de calificación OIV: el DS 285 define el procedimiento general, pero no si la calificación aplica a nivel de empresa, instalación o activo	Bajo	Media-Alta	Bajo	Transversal	Precisar el nivel de calificación (empresa/instalación/activo)	ANCI
Vacío normativo	NT CNE no publicada: su contenido, plazos y relación con el Estándar CEN son aún desconocidos	Bajo	Media	Bajo	Transversal	Publicar la norma y articularla con el Estándar CEN	CNE
Brecha técnica	Ausencia de Niveles de Seguridad (SL): el Estándar CEN gradúa solo por nivel de impacto del activo, sin el modelo de graduación de riesgo por zona que exige IEC 62443	Medio	Media	Medio	Transversal	Incorporar un modelo de graduación de requisitos por nivel de riesgo	CEN
Brecha técnica	Detección no extendida al proceso físico: el CEN limita la detección al perímetro cibernético, sin cubrir anomalías en el proceso físico como exige IEC 62443	Alto	Alta	Alto	Transversal (mayor en Grupo B y C)	Incorporar monitoreo de comportamiento del proceso físico	CEN
Brecha técnica	Recuperación sin validación de integridad física: el CEN no exige verificar la integridad de los activos físicos antes de reanudar operación tras un incidente, a diferencia de IEC 62443	Alto	Alta	Medio	Transversal (mayor en Grupo C)	Incorporar requisito de validación post-incidente	CEN
Brecha institucional	Déficit de capital humano híbrido: escasean en Chile los perfiles con formación conjunta en ingeniería eléctrica y ciberseguridad industrial	Medio	Alta	Medio	Transversal (Grupo B)	Formación especializada y desarrollo del mercado laboral	Academia / Estado
Brecha institucional	Ausencia de guías técnicas sectoriales: no existen guías de implementación del Estándar CEN adaptadas al contexto chileno	Medio	Media	Bajo	Transversal	Publicar guías de implementación por tipología	CEN
Solapamiento	Reporte de incidentes dual: un mismo incidente OT activa obligaciones de reporte simultáneas ante la ANCI y el Coordinador, sin coordinación formal entre ambos	Medio	Media	Bajo	Transversal	Protocolo de coordinación interinstitucional	ANCI + CEN
Solapamiento	SGSI dual: la Ley 21.663 y la NT CNE proyectada exigirían, sin reconocimiento mutuo, demostrar el mismo SGSI ante dos autoridades	Bajo	Media	Bajo	Transversal	Mecanismo de reconocimiento mutuo	ANCI + CNE
Solapamiento	Delegado de Ciberseguridad vs. responsable CEN: no está aclarado si ambos roles pueden recaer en la misma persona	Bajo	Baja	Bajo	Transversal	Aclarar la compatibilidad de ambos roles	ANCI + CEN

6.6 Síntesis del Capítulo

Este capítulo desarrolló los Objetivos Específicos 3 y 4: la comparación del marco chileno con estándares internacionales (6.2 - 6.3) y el diagnóstico de brechas que condicionan su implementación efectiva (6.4 - 6.5).

El eje legal (Tabla 10) muestra que la Ley 21.663 presenta coherencia conceptual con NIS2 y la RN 964, particularmente en gestión de riesgos, gobernanza y reporte de incidentes; su principal divergencia es el mecanismo de designación de entidades obligadas, basado en calificación administrativa antes que en criterios objetivos de aplicación directa. El eje técnico (Tabla 11) muestra que el Estándar CEN es estructuralmente convergente con NERC-CIP —su fuente directa— y parcialmente convergente con IEC 62443, del cual no incorpora el modelo de Niveles de Seguridad ni la extensión de la detección y recuperación al proceso físico.

Un hallazgo central de este capítulo es que la coherencia normativa no equivale a facilidad de implementación: el diagnóstico del OE4 (6.5) identificó 12 hallazgos — 4 vacíos normativos, 3 brechas técnicas propias del Estándar CEN, 2 brechas institucionales y 3 solapamientos regulatorios— que condicionan la implementación efectiva de un marco que, en su diseño, es conceptualmente sólido.

Las principales convergencias identificadas son la gestión de riesgos como eje central de los tres marcos legales, la importancia compartida de la detección temprana y el reporte de incidentes, y el tratamiento de la ciberseguridad como problema de gobernanza —con roles y responsabilidades definidos— y no solo tecnológico. Las principales divergencias —el mecanismo de designación administrativa en el eje legal, y el alcance acotado de la detección y recuperación en el eje técnico— no constituyen inconsistencias normativas, sino diferencias de diseño que, junto con los hallazgos del Gap Analysis, constituyen el insumo directo para la estimación del costo de cumplimiento.

En conclusión, el marco chileno —Ley 21.663 y Estándar CEN— es conceptualmente coherente con sus referentes internacionales, pero enfrenta brechas concretas de implementación identificadas en el Gap Analysis: 4 vacíos que corresponde cerrar a la autoridad regulatoria, 3 brechas técnicas del propio Estándar CEN, 2 brechas institucionales del ecosistema, y 3 solapamientos que requieren coordinación interinstitucional. Estos resultados —normativos, técnicos y de implementación— constituyen la base sobre la cual se desarrolla la estimación del Costo Anualizado de Cumplimiento en el Capítulo 7, que costea las obligaciones concretas de la Ley 21.663 y el Estándar CEN, no las brechas frente a estándares internacionales identificadas en este capítulo.

7. MODELO DE ESTIMACIÓN DE COSTO ANUALIZADO DE CUMPLIMIENTO (OE5)

A partir del análisis normativo y técnico desarrollado en las secciones anteriores, se constata que la aplicación de la Ley N.º 21.663 introduce una carga económica permanente asociada al cumplimiento de obligaciones de ciberseguridad en el sector de generación eléctrica. Dichas obligaciones no se traducen únicamente en inversiones puntuales, sino que requieren capacidades operativas sostenidas en el tiempo, involucrando tanto componentes de inversión (CAPEX) como gastos operativos recurrentes (OPEX). En este contexto, resulta necesario contar con una metodología que permita analizar de manera estructurada y comparable el impacto económico del cumplimiento regulatorio.

El presente capítulo desarrolla el modelo de estimación del Costo Anualizado de Cumplimiento (CAC), concebido como una herramienta metodológica orientada a traducir las exigencias de la normativa de ciberseguridad en una métrica económica anualizada. El modelo no pretende determinar costos contables exactos ni establecer precios normativos, sino proporcionar un marco analítico que permita evaluar el esfuerzo económico inducido por la regulación, integrando inversiones y gastos operativos bajo un horizonte temporal común y coherente con la gestión de activos del sector eléctrico.

El capítulo se organiza en catorce secciones. Las primeras ocho (7.1 a 7.8) construyen el modelo: su fundamento, la arquitectura por Grupos A, B y C, los diecisiete drivers de costo, sus fuentes de calibración, su formulación matemática y su implementación computacional. Las seis restantes (7.9 a 7.14) presentan y analizan los resultados para las tipologías de generación evaluadas —estructura CAPEX/OPEX, proporcionalidad regulatoria, sensibilidad y dispersión de mercado—, y cierran con una síntesis que da cumplimiento al Objetivo Específico 5.

7.1 Fundamento y Justificación del modelo

En las secciones precedentes de este informe se ha analizado el marco normativo de ciberseguridad aplicable al sector eléctrico chileno, así como la coherencia técnica entre la Ley N.º 21.663, su normativa complementaria y los estándares sectoriales utilizados como referencia en infraestructuras críticas. Dicho análisis permitió identificar un conjunto de obligaciones técnicas, organizacionales y operativas exigibles a los operadores de instalaciones eléctricas, particularmente a aquellos clasificados como Operadores de Importancia Vital (OIV). Estas obligaciones emanan de la Ley N.º 21.663 y el Estándar de Ciberseguridad del CEN, habilitado por el Art. 26º de la misma ley, ya caracterizados en el Capítulo 5.

Estos marcos regulatorios y técnicos, al igual que sus referentes internacionales

comparados en el Capítulo 6 (NERC-CIP, NIS2, ANEEL RN 964/2021, IEC 62443 y NIST CSF) cumplen un objeto distinto al de este estudio: establecen qué debe cumplirse en materia de gestión de riesgos, gobernanza y prescripción técnica, y su función regulatoria se agota en ese proposito. Ninguno de estos instrumentos tiene por objeto cuantificar el esfuerzo económico que su cumplimiento impone a los operadores, ni existe evidencia de que exista una metodología de este tipo en la literatura regulatoria disponible. Esto no constituye una omisión de dichos marcos, sino que refleja que la estimación del costo de cumplimiento es una pregunta distinta —de economía aplicada— a la que los instrumentos normativos y técnicos están diseñados para responder.

Precisamente en esa distinción radica la pertinencia académica del modelo desarrollado en este capítulo: no se trata de suplir una carencia de la regulación, sino de construir la herramienta metodológica —hoy inexistente en la literatura revisada— que permite traducir obligaciones ya definidas por esos marcos en una métrica económica comparable.

Este vacío de conocimiento es relevante porque la ciberseguridad se ha transformado en un componente estructural de la gestión de activos eléctricos, con efectos directos sobre el CAPEX y el OPEX de los operadores, sin que exista una métrica que permita analizar ese impacto de forma sistemática y comparable.

Sobre esta base se justifica la introducción del **Costo Anualizado de Cumplimiento (CAC)** como instrumento metodológico central de este estudio. El CAC busca formalizar, desde una perspectiva de economía aplicada, el esfuerzo económico que implica cumplir y mantener las obligaciones de ciberseguridad impuestas por la Ley N.º 21.663, sus decretos reglamentarios y el Estándar de Ciberseguridad del CEN, permitiendo expresar dicho esfuerzo en términos anuales y normalizados. De este modo, el modelo propuesto contribuye a cerrar la brecha identificada entre exigencias regulatorias y análisis económico, habilitando una evaluación más transparente de la proporcionalidad y consistencia del marco normativo en el sector de generación eléctrica.

El desarrollo del modelo CAC se guía por tres principios que estructuran la metodología presentada en las subsecciones siguientes: (i) **proporcionalidad**, reconociendo que el impacto económico del cumplimiento depende de la complejidad y criticidad de los activos involucrados; (ii) **consistencia regulatoria**, al articular el análisis de costos con los marcos de gestión de activos y supervisión ya existentes en el sector eléctrico; y (iii) **replicabilidad**, de modo que la metodología pueda ser aplicada a distintos tipos de instalaciones sin depender de estudios de caso particulares. Estos principios permiten posicionar el CAC como una herramienta analítica complementaria al marco normativo, orientada al análisis económico y no a la fiscalización o determinación de sanciones.

A partir del fundamento, el Costo Anualizado de Cumplimiento (CAC) se define como una estimación anual agregada del esfuerzo económico requerido para implementar y mantener el cumplimiento regulatorio en materia de ciberseguridad, considerando tanto inversiones de capital como gastos operativos recurrentes inducidos por la normativa.

Desde una perspectiva conceptual, el CAC no representa un costo contable exacto ni una cifra referencial de mercado, sino una métrica analítica de carácter anualizado, orientada a capturar la carga económica estructural asociada al cumplimiento normativo. Su propósito es permitir la entre distintos tipos de instalaciones eléctricas, evitando la fragmentación del esfuerzo en proyectos aislados o en partidas presupuestarias no integradas. En este sentido, el CAC se concibe como una herramienta de apoyo al análisis regulatorio y a la gestión de activos, más que como un instrumento de evaluación financiera empresarial.

El CAC integra dos componentes conceptuales principales. El primero es un componente de inversión (CAPEX), correspondiente a aquellos elementos de carácter estructural necesarios para cumplir con las exigencias regulatorias — infraestructura de protección perimetral, plataformas de gestión OT, sistemas de gestión de seguridad— los cuales no se registran como gasto en un único año sino que se distribuyen a lo largo de su vida útil mediante un proceso de anualización financiera. El mecanismo utilizado para esta anualización es el **Factor de Recuperación de Capital (FRC)**, que convierte una inversión inicial en su equivalente anual uniforme incorporando el costo de oportunidad del capital a través de la tasa de descuento (WACC). Este mecanismo se desarrolla matemáticamente en la sección 7.6, donde se presentan su fórmula explícita, los valores calculados para cada categoría de activo cibernético y su comparación con la depreciación lineal simple. El segundo componente es el **OPEX**, asociado a los recursos, servicios y actividades requeridas para sostener el cumplimiento en el tiempo — monitoreo continuo, auditorías, capacitación, parcheo—, cuya periodicidad anual los hace directamente incorporables al modelo sin necesidad de anualización. La combinación de ambos componentes, bajo un horizonte temporal homogéneo, permite representar de manera fiel el esfuerzo económico total inducido por la normativa, superando aproximaciones parciales centradas exclusivamente en inversiones iniciales o en gastos operativos.

Resulta igualmente relevante precisar el alcance conceptual del CAC y, en particular, aquello que queda explícitamente fuera de su definición. El CAC no incluye los costos asociados a incidentes de ciberseguridad, tales como interrupciones del servicio, multas, sanciones administrativas o pérdidas económicas derivadas de eventos adversos. Estos elementos corresponden al ámbito del riesgo residual y del costo del no cumplimiento, fuera del alcance de este modelo. El CAC, por tanto, se limita al costo del cumplimiento normativo, no al costo de sus eventuales incumplimientos.

Asimismo, el CAC no pretende establecer valores normativos, precios de referencia ni comparaciones directas entre proveedores o soluciones tecnológicas. Su formulación se apoya en rangos, índices y coeficientes relativos, con el objetivo de preservar la generalidad, replicabilidad y transparencia del modelo, evitando dependencias de información sensible o de decisiones comerciales específicas.

7.2 Enfoque metodológico general

El enfoque metodológico adoptado para la estimación del Costo Anualizado de Cumplimiento (CAC) se enmarca en la lógica de la economía de la regulación, orientada a analizar los costos que la normativa impone a los agentes regulados como consecuencia del cumplimiento de obligaciones legales y técnicas. En particular, el modelo adopta la taxonomía de costos regulatorios de la OCDE [33], que distingue entre costos sustantivos de cumplimiento —la implementación y operación efectiva de capacidades exigidas por la norma— y cargas administrativas —las obligaciones de información, reporte y documentación ante la autoridad. Esta distinción se aplica en concreto a cada uno de los diecisiete drivers de costo del modelo en la sección 7.4.

En este contexto, la ciberseguridad se aborda no como una externalidad ni como un riesgo abstracto, sino como un requerimiento regulatorio que induce decisiones económicas concretas, tanto en inversión como en operación, y que debe ser evaluado en términos de su impacto estructural sobre los activos regulados.

Desde esta perspectiva, el modelo CAC se concibe como un **modelo paramétrico**, cuyo objetivo es capturar el orden de magnitud y la estructura del esfuerzo económico asociado al cumplimiento, más que estimar costos contables exactos a nivel de empresa o proyecto específico. Este enfoque resulta adecuado en un entorno donde existe heterogeneidad tecnológica y diversidad de arquitecturas de control, sin que ello implique una carencia atribuible al marco regulatorio. En lugar de apoyarse en precios únicos o valores determinísticos, el modelo integra rangos, escenarios y coeficientes de normalización, permitiendo representar la incertidumbre inherente a los costos de ciberseguridad sin perder coherencia analítica.

Metodológicamente, la estimación del CAC se estructura en tres etapas conceptuales. En primer lugar, se identifican las obligaciones regulatorias de ciberseguridad aplicables al sector de generación eléctrica, a partir del marco normativo vigente. En segundo lugar, dichas obligaciones se traducen en drivers de costo, entendidos como categorías de inversión y gasto necesarias para implementar y mantener el cumplimiento. Finalmente, los costos asociados a estos drivers se integran bajo un horizonte anual común, permitiendo combinar componentes de inversión (CAPEX) y operación (OPEX) en una única métrica anualizada.

Un elemento central del enfoque metodológico es la normalización del impacto económico, que permite comparar el esfuerzo de cumplimiento entre distintos tipos de centrales. Dado que las instalaciones de generación presentan diferencias relevantes en su complejidad técnica y arquitectura de control, el modelo no recurre al conteo de equipos individuales, sino a la desagregación funcional de subsistemas ciberfísicos relevantes. Esta normalización facilita el análisis comparativo sin introducir un nivel de detalle técnico que desplace el foco principal del estudio, que es la evaluación económica del impacto regulatorio.

La Ilustración 6 sintetiza este enfoque, mostrando el flujo desde las obligaciones regulatorias hasta la obtención del CAC como métrica económica anualizada.

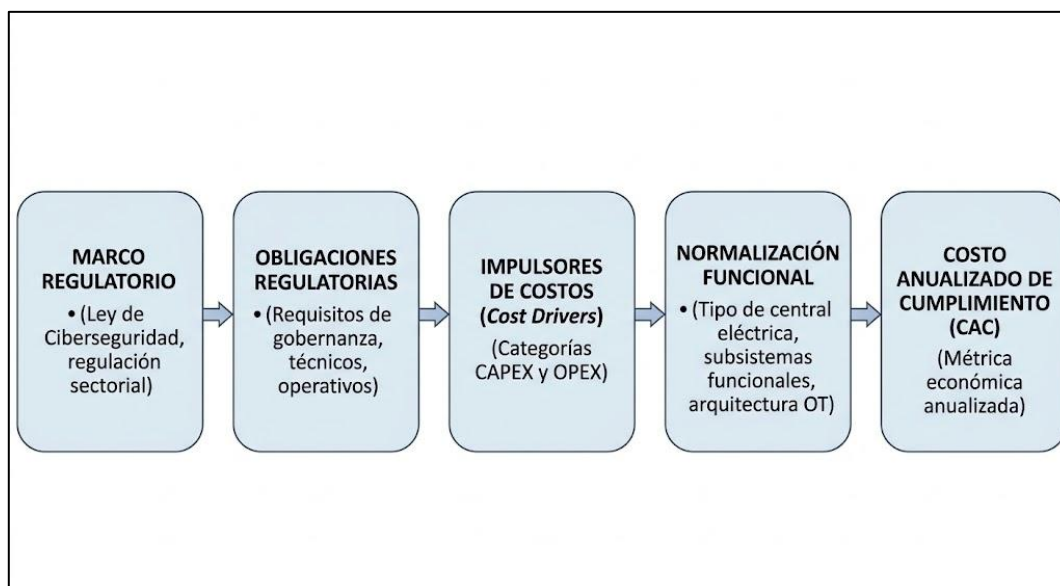


Ilustración 6. Enfoque metodológico general adoptado para la estimación del CAC. (Fuente: Propia generada con IA)

7.2.1 Alcance y supuestos operativos del modelo

El modelo de estimación del Costo Anualizado de Cumplimiento (CAC) se desarrolla con el propósito de analizar el impacto económico del cumplimiento de la normativa de ciberseguridad en el sector de generación eléctrica, desde una perspectiva regulatoria y sectorial. En consecuencia, su alcance se circunscribe a las obligaciones derivadas de la Ley N.º 21.663 con sus decretos reglamentarios y el Estándar de Ciberseguridad del CEN, en tanto estas afectan a las instalaciones de generación a través de requerimientos técnicos, organizacionales y operativos que inducen costos identificables y recurrentes en el tiempo.

El modelo se aplica a centrales de generación eléctrica consideradas como unidades representativas, definidas a partir de tipologías tecnológicas y arquitectónicas, y no a instalaciones individuales específicas. Esta aproximación permite abstraerse de configuraciones particulares o decisiones de diseño propias

de cada proyecto, privilegiando una visión comparativa y replicable del impacto económico del cumplimiento. Asimismo, el análisis se concentra en los costos directamente asociados a la implementación y mantenimiento de capacidades de ciberseguridad, excluyendo aquellos efectos económicos que responden a la materialización de incidentes, sanciones o fallas operativas, los cuales se consideran fuera del alcance del CAC y se abordan desde una lógica distinta.

Desde el punto de vista operativo, el modelo asume tres supuestos estructurales. **Primero**, el cumplimiento en materia de ciberseguridad constituye una condición permanente de operación y no una fase transitoria, por lo que los costos se estructuran en CAPEX y OPEX integrados bajo un horizonte anual común. **Segundo**, las diferencias entre tipologías de central se capturan mediante la desagregación funcional de sus sistemas de control OT, sin recurrir al conteo detallado de equipos individuales. **Tercero**, los costos de ciberseguridad presentan un grado inherente de incertidumbre derivado de la heterogeneidad del mercado, por lo que la estimación se apoya en rangos y escenarios que permiten analizar órdenes de magnitud y tendencias.

Las implicancias de estos supuestos y las limitaciones derivadas de ello se abordan de manera explícita en la sección 7.8.

7.3 Arquitectura del modelo: Grupo A/B/C y unidad de análisis

El modelo CAC adopta la clasificación en Grupos A, B y C desarrollada en la sección 4.3 de este informe, donde se caracterizaron las arquitecturas dominantes de control OT de cada tipología de central generadora, sus perfiles diferenciados de riesgo cibernético y las implicancias de esas diferencias sobre las estrategias de protección exigibles. Se remite a esa sección para el detalle técnico de cada grupo.

En el contexto del modelo CAC, la relevancia de esa clasificación es económica y no técnica: los Grupos A, B y C presentan estructuras de costo de cumplimiento estructuralmente distintas que el modelo debe capturar de forma diferenciada. Esas diferencias se expresan en tres dimensiones concretas: la intensidad del CAPEX requerido, la estructura del OPEX recurrente, y la complejidad de la auditoría de certificación. La Ilustración 7 sintetiza las implicancias económicas de la clasificación.

Esta tipología (Ilustración 7) no pretende ser un inventario exhaustivo de equipos ni una clasificación operativa de las instalaciones del parque generador chileno. Su propósito es diferenciar el perfil de costo de cumplimiento entre tecnologías. Las obligaciones regulatorias son esencialmente las mismas para todas las tecnologías. La diferencia no está en la norma sino en la arquitectura de control que cada tipología exige proteger, y es esa diferencia arquitectónica la que el modelo CAC captura mediante la clasificación A, B y C.

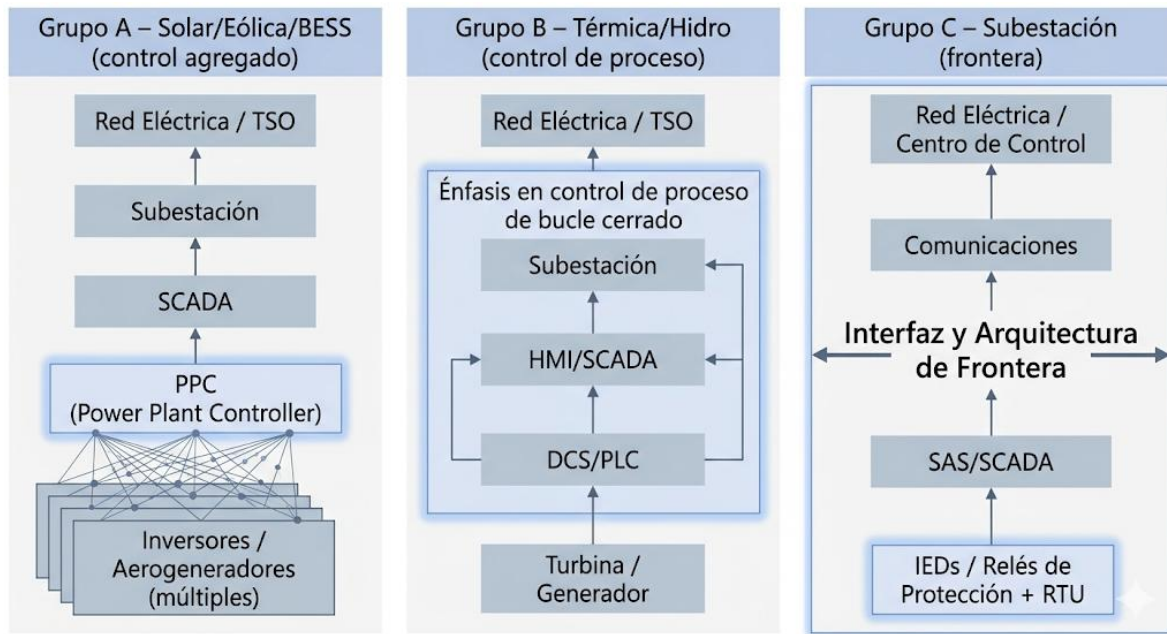


Ilustración 7. Tipología basada en arquitectura OT/ICS para normalización del CAC. (Fuente: Propia generada con IA)

7.3.1 Definición de la unidad de análisis y normalización del modelo

Con el fin de permitir un análisis económico comparable del impacto del cumplimiento regulatorio en ciberseguridad, el modelo CAC adopta una unidad de análisis estandarizada, definida como una *central de generación representativa*. Esta decisión metodológica responde a la necesidad de abstraerse de configuraciones específicas, tamaños particulares o decisiones de diseño propias de cada proyecto, privilegiando una aproximación normalizada que permita evaluar el efecto estructural de la normativa sobre distintas tipologías de instalaciones.

La unidad de análisis se define a partir de centrales tipo, clasificadas según la tipología A, B y C, y caracterizadas por su arquitectura dominante de control OT/ICS. Esta aproximación es consistente con la literatura de seguridad industrial: NIST SP 800-82 establece que los sistemas ICS deben analizarse por su configuración y rol funcional —no por número de equipos individuales—, y la serie IEC 62443 refuerza la segmentación en unidades lógicas y funcionales como base para la gestión de la seguridad.

Desde el punto de vista de la normalización económica, el modelo no busca comparar instalaciones por cantidad de equipos o por potencia instalada de manera aislada, sino por el **esfuerzo relativo de cumplimiento** que impone la normativa en función de la complejidad funcional del sistema OT. Para ello, el CAC se expresa, además del valor absoluto anual, en dos indicadores normalizados que conectan el análisis económico con los marcos de gestión de activos ya existentes en el sector, tal como se representa en la Ilustración 8.

El primero es el CAC por MW instalado, que expresa el costo de cumplimiento en relación con la potencia de la central y permite comparar el esfuerzo entre instalaciones de distinto tamaño:

Ecuación 1

$$CAC/MW \text{ (USD/MW} \cdot \text{año)} = CAC_{total} / Potencia_{MW}$$

El segundo, desarrollado con mayor detalle en la sección 7.6, son los indicadores ΔXX del RPTD N.º 17 de la SEC, que expresan el CAPEX anualizado y el OPEX de cumplimiento como variación porcentual sobre el Valor de Inversión de la central, conectando el análisis del CAC con los indicadores regulatorios que el sector eléctrico ya reporta a la SEC:

Ecuación 2

$$\Delta XX - CAPV (\%) = CAPEX_{ciber_anualizado} / V.I._{planta} \times 100$$

Ecuación 3

$$\Delta XX - OPEV (\%) = OPEX_{ciber_anual} / V.I._{planta} \times 100$$

Estos indicadores permiten capturar diferencias estructurales relevantes entre tecnologías, expresando el esfuerzo de cumplimiento en métricas comparables y coherentes con los instrumentos de supervisión ya existentes en el sector eléctrico chileno. Su implementación computacional se desarrolla en la sección 7.6, y sus resultados completos por tecnología se presentan en la sección 7.11.

La Tabla 14 sintetiza la unidad de análisis adaptada para cada tipología, detallando la arquitectura OT dominante, la lógica de normalización económica y su justificación metodológica.

Tabla 14. Unidad de análisis y criterios de normalización del modelo CAC (Fuente: Elaboración Propia)

Tipología	Tipo de instalación representativa	Arquitectura OT dominante	Lógica de normalización económica	Justificación metodológica	Referencias conceptuales
Grupo A	Solar FV / Eólica	Electrónica de potencia distribuida con control agregado (PPC + SCADA de planta)	Dominios funcionales de control agregado, no conteo de inversores/aerogeneradores individuales	El costo depende de la capacidad de control y comunicaciones concentrada en el PPC, no del número de equipos	NIST SP 800-82 (ICS Security); IEC 62443 (IACS)

Grupo B	Térmicas / Hidroeléctricas	Control de proceso en lazo cerrado (DCS / PLC jerárquico + SCADA)	Ciber-Sistemas SEN altamente acoplados al proceso, con baja tolerancia a fallas	Mayor acoplamiento ciberfísico concentra el esfuerzo de cumplimiento en plataformas OT críticas (DCS/PLC)	NIST 800-82 (SCADA vs DCS); IEC 62443 (seguridad de sistemas de control industrial).
Grupo C	Subestaciones e interconexión	Automatización de subestaciones (SAS, IEDs, RTU, protecciones y comunicaciones)	Rol funcional como frontera crítica entre central y SEN, independiente de la potencia generada	Aunque no generan energía, concentran funciones esenciales de protección y coordinación	IEC 62443 (zonas & conduits); NIST 800-82; literatura de automatización de subestaciones.

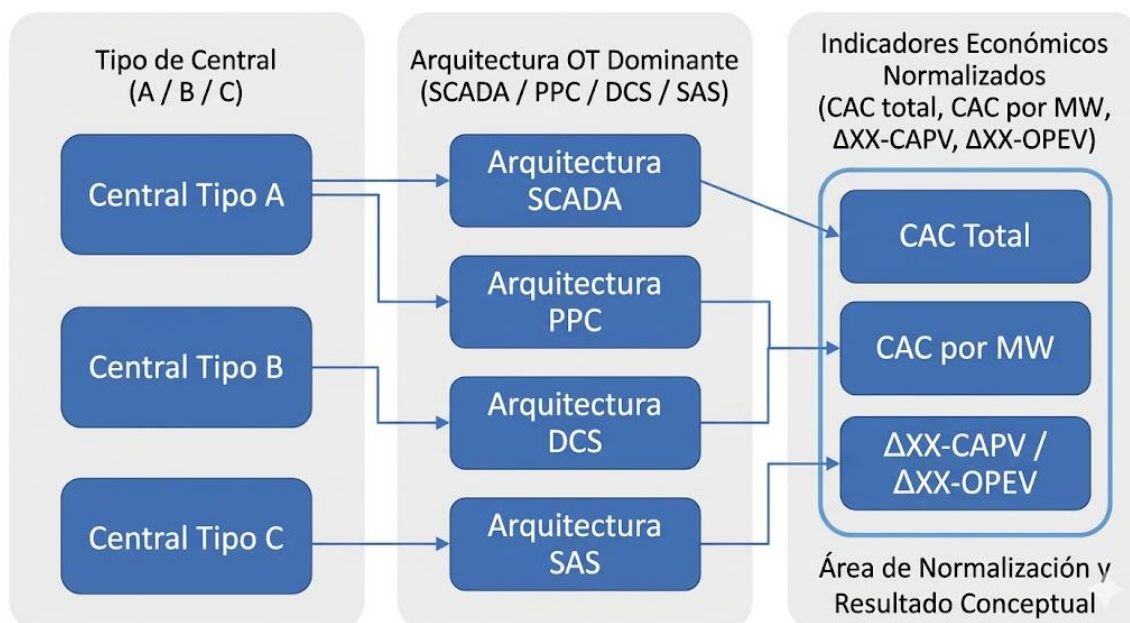


Ilustración 8. Modelo de Costo de Cumplimiento de Ciberseguridad (CAC) para Generación de Energía. (Fuente: Propia generada con IA)

7.3.2 Determinación del número de Ciber-Sistemas SEN por tecnología

El Estándar CEN define formalmente el Ciber Sistema SEN como "uno o más Ciber Activos SEN agrupados lógicamente por una Entidad Responsable", donde un Ciber Activo SEN es aquel que, de fallar dentro de un intervalo de 15 minutos, podría

impactar adversamente la operación segura y confiable del SEN. Bajo esta definición, el número de Ciber-Sistemas SEN de una instalación no corresponde a un conteo de equipos individuales, sino al número de plataformas de control lógicamente independientes que gobiernan sus distintos subprocesos físicos.

La Tabla 15. Determinación del número de Ciber-Sistemas SEN por tecnología (Fuente: Elaboración Propia, en base a la definición del Estándar CEN) opera esta definición para cada tecnología evaluada, identificando las plataformas de control que constituyen un Ciber-Sistema SEN diferenciado en cada caso.

Tabla 15. Determinación del número de Ciber-Sistemas SEN por tecnología (Fuente: Elaboración Propia, en base a la definición del Estándar CEN)

Tecnología	N° CS-SEN	Ciber-Sistemas SEN identificados	Base de la clasificación
Solar FV	2	CS1: PPC (Power Plant Controller) + inversores; CS2: SCADA de planta	Arquitectura centralizada homogénea — un único controlador agregado coordina todo el activo distribuido
Eólica	3	CS1: PPC + controladores de aerogenerador; CS2: SCADA de parque; CS3: Sistema meteorológico/hidrológico de predicción	Misma lógica que Solar FV, más un sistema adicional por la mayor dispersión geográfica del parque
Térmica Gas (CC)	5	CS1: DCS de turbina; CS2: DCS de BOP (Balance of Plant); CS3: PLC de quemadores; CS4: PLC de planta de agua/tratamiento; CS5: SCADA integrador de planta	Múltiples DCS/PLC propietarios interdependientes, cada uno gobernando un subproceso físico distinto
Hidro (pasada)	4	CS1: DCS de turbina/gobernador; CS2: SCADA hidrológico; CS3: Sistema de excitación; CS4: PLC de auxiliares	DCS propietario del proceso principal, más sistemas de control hidrológico específicos
Subestación (ref.)	3	CS1: RTU principal; CS2: Sistema de relés de protección; CS3: SCADA de subestación	Arquitectura basada en IEC 61850, con función de protección física separada del control

Esta tabla opera como una traducción cuantitativa de un concepto que el Estándar CEN define en términos cualitativos —agrupación lógica de activos por proceso—, en un parámetro contable utilizable por el modelo. Esta operacionalización constituye, en sí misma, un supuesto metodológico de este estudio: el criterio de conteo (una plataforma de control por subproceso físico diferenciado) es razonado y trazable a la definición del Estándar, pero no es la única forma posible de

operacionalizar el concepto. El N° de CS-SEN así determinado es el parámetro que activa el escalamiento de los drivers de costo descrito en la sección 7.4 (Tabla 17).

7.4 Drivers de costo: Identificación y correspondencia normativa

La traducción de las obligaciones regulatorias en drivers de costo, requiere precisar primero sobre qué fuentes normativas y técnicas se construye el modelo. El modelo de Costo Anualizado de Cumplimiento cuantifica el esfuerzo económico asociado a un conjunto de obligaciones trazables a fuentes regulatorias verificables, analizadas en los objetivos específicos previos. Su construcción se apoya en cuatro pilares, de los cuales dos estructuran directamente la matriz de convergencia que da origen a los drivers, y dos cumplen un rol complementario de anticipación y validación.

El primer pilar es la Ley N.º 21.663 con sus decretos reglamentarios, que establece el marco de gobernanza y los deberes generales de ciberseguridad exigibles a los Operadores de Importancia Vital —fuente jurídica primaria consolidada en la Tabla 4 de la sección 5.3.

El segundo pilar es el Estándar de Ciberseguridad CEN, habilitado por el Art. 26°, que opera como "última milla técnica", y traduce obligaciones jurídicas abstractas en medidas técnicas específicas —perímetros de seguridad electrónica, gestión de parches, monitoreo de eventos—, Este segundo pilar se consolida en la Tabla 5 de la sección 5.4.5.

Estos dos primeros pilares son los que estructuran directamente la matriz de convergencia normativa que da origen a los drivers de costo. La Tabla 6, sintetiza la integración de ambos instrumentos, cruzando los deberes legales con los controles técnicos del Estándar CEN para identificar, en cada caso, el control integrado que satisface simultáneamente ambas obligaciones. Esta tabla de convergencia se construyó exclusivamente sobre la base de la Ley y el Estándar CEN, por constituir el marco vigente y exigible al cierre de este estudio; se extiende con una columna adicional que asocia a cada control su driver de costo en el modelo CAC.

El tercer pilar es el proyecto de Norma Técnica de Ciberseguridad y Seguridad de la Información de la Comisión Nacional de Energía (NT CNE). Esta norma no se incorporó a la matriz de convergencia por no encontrarse publicada ni sometida a consulta pública al momento de su elaboración, no obstante, su anticipada incorporación de un Sistema de Gestión de Seguridad de la Información basado en ISO 27001 si fue reconocida como driver de costos del modelo, dotándolo de capacidad prospectiva frente a la evolución del marco regulatorio.

El cuarto pilar son las mejores prácticas internacionales analizadas en el Capítulo 6. El contraste sistemático del marco chileno con NERC-CIP, IEC 62443, la Directiva NIS2 y la Resolución ANEEL N.º 964 no generó drivers de costo adicionales, pero

aportó el marco de referencia que permite situar los controles derivados del marco chileno dentro de las prácticas técnicas de la industria.

En síntesis, la matriz de convergencia que estructura los drivers del modelo se funda en los dos primeros pilares —la Ley 21.663 y el Estándar CEN—, mientras que el proyecto de NT CNE y las mejores prácticas internacionales del cumplen, respectivamente, un rol de anticipación regulatoria y de validación técnica.

7.4.1 Identificación de obligaciones regulatorias y drivers de costo

Una vez definida la unidad de análisis y la lógica de normalización del modelo CAC, el siguiente paso metodológico consiste en identificar las obligaciones regulatorias de ciberseguridad aplicables al sector de generación eléctrica y establecer su correspondencia con los drivers de costo considerados en la estimación CAC. Dichas obligaciones no se interpretan de manera literal o artículo por artículo, sino como requerimientos funcionales que imponen al operador la necesidad de contar con ciertas capacidades organizacionales, técnicas y operativas, permitiendo concentrarse en los efectos económicos inducidos por la regulación.

Para efectos del modelo CAC, se define como *driver de costo* toda categoría de inversión o gasto que resulta necesaria para implementar, mantener o demostrar el cumplimiento de una o más obligaciones regulatorias en materia de ciberseguridad. No existe una correspondencia unívoca entre obligación y driver: una misma obligación puede generar múltiples drivers de costo, y un mismo driver puede contribuir simultáneamente al cumplimiento de distintas obligaciones, reflejando el carácter transversal de la ciberseguridad en sistemas industriales.

La Tabla 16, retoma la estructura de convergencia normativa desarrollada en la Tabla 6 de la sección 5.5 e incorpora una columna adicional que identifica el driver de costo del modelo CAC que corresponde a cada control técnico. De este modo, la tabla que en la sección 5.5 cumplía un propósito normativo —identificar qué debe cumplirse y bajo qué instrumento regulatorio— adquiere aquí su dimensión económica: qué cuesta cumplirlo y a través de qué categoría de gasto o inversión.

Los controles se organizan en tres bloques: primero los que generan un driver de costo modelable en el CAC, numerados correlativamente del 1 al 16; luego los controles cuyo costo queda absorbido dentro de otro driver ya contabilizado, marcados con "—" para indicar que no generan un costo adicional independiente; y finalmente los excluidos del modelo genérico por variabilidad indeterminada o por aplicación caso a caso, marcados con X o Δ según corresponda, con la justificación metodológica respectiva.

Tabla 16. Convergencia Normativa – Ley N° 21.663 y Estándar CEN + Drivers de Costos (Fuente: Elaboración Propia)

N°	Control técnico OT	Descripción del control integrado	Satisface Ley 21.663 (Artículo)	Satisface Estándar CEN (Bloque CIP)	Nivel de impacto CEN aplicable	Perfil Económico	Justificación Económica	Control / Driver de Costo
1	Inventario y clasificación de Ciber Sistemas SEN	Un único inventario de activos OT satisface la obligación de SGSI de la ley y la clasificación de impacto de CIP-002. El mismo registro sirve como base del SGSI mandatado por la ley y como lista de Ciber Sistemas SEN exigida por el estándar.	Art. 8°(a) – SGSI + inventario de activos ICI	CIP-002 – Categorización de Ciber Sistemas SEN	Todos los niveles	CAPEX + OPEX	Plataforma de gestión certificable; base del SGSI mandatado. Licencia inicial (CAPEX) y renovación anual (OPEX).	→ Driver 1: Asset Inventory OT
2	Software SGSI — plataforma de gestión ISO 27001	El software de gestión del SGSI exigido por Art. 8°(a) materializa la política de ciberseguridad OT requerida por CIP-003. Un mismo sistema documenta, gestiona y certifica el SGSI para ambas obligaciones.	Art. 8°(a) – SGSI política de seguridad	CIP-003 – Controles de Gestión de la Seguridad	Todos los niveles	CAPEX	Plataforma certificable ISO 27001 (CAPEX implementación). Costo independiente del rol del Delegado.	→ Driver 2: Software SGSI
3	Designación del Encargado CIP / Delegado de Ciberseguridad	El Delegado exigido por Art. 8°(i) cumple el rol de Encargado CIP requerido por CIP-003. La política de ciberseguridad OT exigida por CIP-003 forma parte del SGSI del Art. 8°(a). Un mismo rol y un mismo documento cubren ambas obligaciones.	Art. 8°(i) – Delegado con acceso a alta dirección Art. 8°(a) – SGSI política de seguridad	CIP-003 – Controles de Gestión de la Seguridad	Todos los niveles	OPEX	Responsabilidad jerárquica mandatada por ley. Sueldo del Delegado / Encargado CIP es OPEX puro. Mayor especialización en centrales con DCS propietario.	→ Driver 3: delegado de Ciberseguridad
4	Programa de capacitación y verificación de antecedentes	El programa de capacitación OT para Art. 8°(h) satisface los requisitos de formación y registro de CIP-004. Los mismos módulos y registros de completación cubren ambas obligaciones. En Chile, CIP-004 admite Declaración Jurada para verificación de antecedentes.	Art. 8°(h) – capacitación y ciberhigiene	CIP-004 – Personal y Capacitación	Impacto Alto y Medio	OPEX	Reducción del riesgo humano. Costo recurrente por persona con acceso a Ciber Sistemas SEN.	→ Driver 4: Capacitación OT básica → Driver 5: Capacitación OT avanzada (dos drivers diferenciados en Tabla 6 extendida)
5	Firewall OT ruggedizado — Perímetro de Seguridad Electrónica (PSE)	El firewall industrial implementado para CIP-005 satisface simultáneamente el deber de defensa en profundidad del Art. 8°(e). Control técnico único, doble cumplimiento normativo.	Art. 8°(e) – defensa en profundidad + restricción de acceso	CIP-005 – Perímetro de Seguridad Electrónica (PSE)	Impacto Alto y Medio	CAPEX	Segmentación red OT/IT. Inversión en activo fijo de infraestructura industrial.	→ Driver 6: Firewall OT ruggedizado
6	Diodo de datos — aislamiento unidireccional zona crítica	Para zonas con Ciber Sistemas SEN de mayor criticidad, el diodo de datos proporciona aislamiento unidireccional que elimina la posibilidad de acceso bidireccional. Complementa el firewall donde se requiere aislamiento total.	Art. 8°(e) – defensa en profundidad zona crítica	CIP-005 – PSE zona crítica (complemento al firewall)	Impacto Alto y Medio (según evaluación de riesgo)	CAPEX	Aislamiento unidireccional red crítica. Costo complementario al firewall OT.	→ Driver 7: Diodo de datos
7	Control de acceso remoto seguro — PAM / MFA / Sistema Intermedio	La solución PAM/MFA implementada para el ARI de CIP-005 R2 satisface el control de accesos del Art. 8°(a) y la gestión de cuentas de CIP-007. El Sistema Intermedio es el mecanismo específico exigido por el Estándar CEN para ARI.	Art. 8°(e) – reducción de impacto Art. 8°(a) – SGSI gestión de accesos	CIP-005 R2 – Acceso Remoto Interactivo (ARI)	Impacto Alto y Medio	OPEX	Acceso remoto seguro para proveedores y mantenimiento. Licencias anuales PAM/MFA.	→ Driver 8: Control acceso remoto PAM/MFA

8	Control de acceso físico a sala de control y cuarto de servidores OT (PSF)	CIP-006 exige controlar físicamente el acceso al recinto donde se alojan los Ciber Sistemas SEN: sala de control, cuarto de servidores OT, celdas de protección. Incluye lectoras de tarjeta/badge, cerradura electrónica, CCTV interior y bitácora de accesos. Distinto de CIP-014: aplica al recinto interior OT, no a la instalación completa.	Art. 8°(e) – defensa en profundidad (dimensión física sala OT)	CIP-006 – Seguridad Física de Ciber Sistemas SEN (PSF)	Impacto Alto y Medio	CAPEX	Costo acotado y predecible (CAPEX). Aplica principalmente a Grupo B y C; con menor intensidad en Grupo A por menor complejidad del recinto de control. Componentes: lectoras de tarjeta/badge, cerradura electrónica, CCTV interior sala OT, bitácora digital de accesos.	→ Driver 9: Control acceso físico sala OT (CIP-006)
9	Hardening OT — configuración segura de sistemas	El hardening de sistemas OT (deshabilitar puertos innecesarios, configuración segura) satisface simultáneamente el deber de reducción de impacto del Art. 8°(e) y el requisito de gestión de puertos y servicios de CIP-007 R1.	Art. 8°(e) – reducción de superficie de ataque	CIP-007 R1 – Gestión de puertos y servicios	Impacto Alto y Medio	CAPEX	Reducción de superficie de ataque mediante configuración segura inicial. Inversión de implementación única con revisiones periódicas.	→ Driver 10: Hardening OT
10	Gestión de parches OT — ciclo de evaluación y aplicación	Los ciclos de evaluación y aplicación de parches OT satisfacen el SGSI continuo del Art. 8°(a) y el requisito de gestión de parches de CIP-007 R2. Las mismas horas-técnico cubren ambas obligaciones normativas.	Art. 8°(e) – reducción de riesgos continua Art. 8°(a) – SGSI gestión de riesgos	CIP-007 R2 – Gestión de parches (evaluación cada 35 días)	Impacto Alto y Medio	OPEX	Horas-técnico recurrentes para ciclos de evaluación y aplicación de parches OT. Ciclo trimestral efectivo.	→ Driver 11: Gestión de parches OT
11	SIEM industrial + monitoreo de eventos de seguridad OT	El SIEM industrial cubre: trazabilidad legal del Art. 8°(b), capacidad de detección para plazos DS 295, monitoreo de eventos de CIP-007 R4/R5 y base para evaluación de vulnerabilidades de CIP-010 R3. Un sistema, cuatro obligaciones simultáneas.	Art. 8°(b) – registro auditable SGSI Art. 9°/DS 295 – trazabilidad para reportes	CIP-007 R4/R5 – Monitoreo de eventos de seguridad CIP-010 R3 – Evaluación de vulnerabilidades	Impacto Alto y Medio	CAPEX + OPEX	Trazabilidad legal obligatoria; retención de logs mínimo 90 días (DS 295 Art. 9°). Plataforma requiere licencia inicial (CAPEX) y gestión continua (OPEX).	→ Driver 12: SIEM industrial
12	SOC MDR-OT 24/7 — monitoreo continuo externalizado	El SOC MDR-OT cubre: detección en menos de 3h para DS 295, monitoreo de eventos CIP-007 R4, evaluación pasiva de vulnerabilidades CIP-010 R3, coordinación de respuesta CIP-008 R2, y comunicación al CSIRT del Art. 8°(d). Un servicio, cinco obligaciones normativas simultáneas.	Art. 9°/DS 295 – notificación 3h/24h/7d/15d Art. 8°(d) – detección y comunicación al CSIRT	CIP-007 R4 – Monitoreo de eventos CIP-008 R2 – Coordinación de respuesta CIP-010 R3 – Evaluación pasiva vulnerabilidades	Impacto Alto y Medio	OPEX	Monitoreo continuo 24/7 con especialización OT. Mayor driver de costo por cobertura multifuncional.	→ Driver 13: SOC MDR-OT 24/7
13	Plan de Continuidad + Infraestructura DRP + Plan IR	Plan de Continuidad (ley), Plan IR (CIP-008) y Plan de Recuperación (CIP-009) se fusionan en un instrumento único. La infraestructura DRP incluye: servidor de respaldo DCS, NAS externo para configuraciones, software de backup OT y medios fuera de línea.	Art. 8°(c) – planes de continuidad bienales Art. 8°(d) – simulacros periódicos	CIP-008 R1-R3 – Plan IR CIP-009 R1-R3 – Plan de recuperación OT	Impacto Alto y Medio	CAPEX + OPEX	Resiliencia operacional; certificación bianual Art. 28°. Infraestructura DRP es CAPEX. Ejercicios de recuperación son OPEX anual.	→ Driver 14: Plan Continuidad + DRP + Plan IR
14	Pentesting OT y simulacros de respuesta a incidentes	El pentesting OT y los ejercicios tabletop son el mecanismo técnico con que se ejecuta el Art. 8°(d) sobre sistemas OT. CIP-008 R1-R3 exige ejercicios periódicos del Plan IR. Los resultados se reportan al CSIRT Nacional conforme al Art. 8°(d).	Art. 8°(d) – revisiones, simulacros y comunicación al CSIRT	CIP-008 R1-R3 – Ejercicios del Plan IR	Impacto Alto y Medio	OPEX	Costo anual por ejercicio de pentesting OT. Separado del DRP porque tiene diferente frecuencia y proveedor.	→ Driver 15: Pentesting OT y simulacros

15	Análisis de Impacto de Negocio (BIA) — matriz de criticidad de incidentes	El BIA produce la matriz de criticidad de incidentes exigida por el DS 295 Art. 3° para determinar qué eventos califican como de impacto significativo. Es un entregable independiente del SGSI general: requiere una consultoría o análisis específico para sistemas OT.	DS 295 Art. 3° — criterios de impacto significativo Art. 8°(a) — SGSI gestión de riesgos	CIP-008 — soporte metodológico Plan IR	Impacto Alto y Medio	OPEX	Consultoría o análisis específico recurrente (revisión anual recomendada). Costo predecible e independiente de otros controles.	→ Driver 16: Análisis BIA
16	Auditorías externas integradas — Art. 28° y Estándar CEN	La auditoría externa exigida por Art. 28° puede cubrir simultáneamente: verificación de controles del SGSI, verificación de vulnerabilidades OT (CIP-010 R3), revisión de gestión de proveedores (CIP-013) y verificación de evaluación de riesgo físico (CIP-014 R2). Una auditoría integrada reemplaza evaluaciones independientes.	Art. 28° — certificaciones y auditorías periódicas Art. 8°(a) — SGSI y gestión de riesgos	CIP-010 R3 — Verificación vulnerabilidades CIP-013 — Verificación supply chain CIP-014 R2 — Verificación evaluación riesgo físico	Impacto Alto y Medio (Art. 28° aplica a todos los OIV)	OPEX	Validación independiente del SGSI; costo recurrente bianual (Art. 28°). Integración reduce costo vs auditorías separadas por instrumento normativo.	→ Driver 17: Auditorías externas integradas
—	Baseline de configuración + plataforma monitoreo OT pasivo	El baseline de configuración de CIP-010 R1 y el change management de R2 satisfacen la gestión de riesgos continua del Art. 8°(a). La evaluación de vulnerabilidades de CIP-010 R3 se ejecuta mediante la plataforma de monitoreo OT pasivo, que integra también la función de Asset Inventory (CIP-002). Nota: Claroty/Nozomi/Dragos integran Asset Inventory (CIP-002) + monitoreo pasivo (CIP-010) en una sola plataforma.	Art. 8°(a) — SGSI gestión de riesgos continua Art. 8°(e) — reducción de impacto	CIP-010 R1 — Baseline de configuración CIP-010 R2 — Gestión de cambios CIP-010 R3 — Evaluación de vulnerabilidades (cada 15 meses)	Impacto Alto y Medio	CAPEX + OPEX	Plataforma de monitoreo OT pasivo (Claroty / Nozomi / Dragos). Licencia inicial (CAPEX) y suscripción anual (OPEX). La misma plataforma cubre CIP-002 (control 1) y CIP-010 (este control). * Nota2 *	Absorbido en Driver 1: Asset Inventory OT (plataforma integra CIP-002 + CIP-010)
—	Protección de información OT — responsabilidad del Delegado	CIP-011 exige proteger la información de los Ciber Sistemas SEN (configuraciones, planos, credenciales). Esta responsabilidad recae sobre el Delegado / Encargado CIP — el mismo rol del control 3. No genera un control técnico adicional: es una política administrada por el mismo rol.	Art. 8°(a) — SGSI protección de datos Art. 8°(b) — registro íntegro y auditable	CIP-011 R1-R2 — Protección de información de Ciber Sistemas SEN	Todos los niveles	OPEX (marginal)	Costo marginal absorbido en el rol del Delegado / Encargado CIP. Sin tecnología adicional. * Nota2 *	Absorbido en Driver 3: Delegado de Ciberseguridad (política CIP-011 gestionada por el mismo rol)
—	Integración normativa Ley 21.663 ↔ Estándar CEN ↔ NTSyCS	El Art. 26° de la Ley 21.663 establece que prevalece la normativa sectorial del CEN cuando su efecto es equivalente o superior. El operador debe mantener una matriz de integración normativa que asegure coherencia entre los tres instrumentos y se actualice ante cada modificación regulatoria.	Art. 7° y Art. 26° — integración sectorial y prevalencia normativa CEN	Estándar CEN general — coherencia normativa entre instrumentos	Todos los niveles	OPEX (marginal)	Labor de cumplimiento administrativo (horas-hombre). Costo marginal absorbido en el rol del Delegado. * Nota2 *	Absorbido en Driver 3: Delegado de Ciberseguridad
—	Monitoreo y adaptación a instrucciones técnicas ANCI	El Art. 11°(b) obliga a los OIV a cumplir las instrucciones técnicas que dicte la ANCI en ejercicio de su potestad normativa, en la medida en que sean aplicables al sector eléctrico y no contradigan normativa sectorial equivalente (Art. 26°). Requiere seguimiento permanente de la normativa ANCI.	Art. 11°(b) — instrucciones técnicas ANCI	Sin CIP equivalente directo — obligación legal transversal	Todos los niveles	OPEX (marginal)	Gestión operativa continua (horas-hombre de compliance). Costo marginal absorbido en el rol del Delegado. Puede implicar CAPEX puntual si la instrucción exige nuevo hardware. * Nota2 *	Absorbido en Driver 3: Delegado de Ciberseguridad

—	Reporte de incidentes DS 295 — protocolo cuatro hitos	El DS 295 exige notificar incidentes significativos en cuatro hitos: alerta inicial (3h), reporte detallado OIV (24h), plan de acción (7 días) y informe final (15 días). El costo del reporte en sí es marginal: es una tarea ejecutada por el Delegado y el SOC que ya están modelados como controles independientes.	Art. 9° / DS 295 Arts. 2–12 – protocolo de reportabilidad	CIP-008 – Notificación de Incidente de Ciberseguridad Reportable (ICR)	Todos los OIV	OPEX (marginal — absorbido en SOC y Delegado)	Costo marginal absorbido en los roles del Delegado de Ciberseguridad y el SOC MDR-OT ya modelados. No genera un costo adicional independiente. * Nota2 *	<i>Absorbido en Driver 13: SOC MDR-OT + Driver 3: Delegado de Ciberseguridad</i>
—	Gestión de riesgos en la cadena de suministro OT	CIP-013 exige un plan de gestión de riesgos de supply chain para software y hardware OT, con cláusulas de ciberseguridad en contratos con proveedores y registro de software/firmware autorizado por fabricante.	Art. 8°(a) – SGSI y gestión de riesgos Art. 8°(e) – integridad de componentes OT	CIP-013 – Gestión de Riesgos en la Cadena de Suministros	Impacto Alto y Medio	OPEX	Esfuerzo administrativo: revisión de contratos y evaluación de proveedores OT. Sin CAPEX significativo. * Nota2 *	<i>Absorbido en arquitectura core (Driver 8 PAM/MFA + Driver 3 Delegado + Driver 17 Auditorías)</i>
X	Seguridad de comunicaciones entre Centros de Control	CIP-012 exige proteger la confidencialidad e integridad de datos de evaluación en tiempo real entre Centros de Control. Aplica al Coordinador y a Empresas Coordinadas que operen un Centro de Control propio (SCADA ≥2 instalaciones). No aplica a generadoras sin CC propio: costo variable según arquitectura.	Art. 8°(a) – SGSI integridad de datos Art. 8°(e) – protección de comunicaciones críticas	CIP-012 – Comunicaciones entre Centros de Control	Entidades con Centro de Control propio (SCADA ≥2 instalaciones)	CAPEX + OPEX	Encriptación de enlaces inter-CC (CAPEX). Mantenimiento plan de protección (OPEX). Costo variable según arquitectura de comunicaciones. No aplica a generadoras sin CC propio. * Nota3 *	<i>X Excluido del modelo CAC genérico (aplica caso a caso — ver Tabla 6 extendida)</i>
⚠	Evaluación de riesgo físico de instalación crítica — por tercero	CIP-014 exige una evaluación de riesgo físico de la instalación completa frente a amenazas deliberadas, realizada por tercero acordado con el CEN. Solo el costo de la evaluación es predecible y modelable. Las medidas resultantes (CCTV perimetral, cercado, iluminación, sensores perimetrales) presentan variabilidad indeterminada y no se modelan en un CAC genérico por razones metodológicas explícitas.	Art. 8°(e) – defensa en profundidad (amenazas físicas deliberadas a la instalación completa)	CIP-014 – Seguridad Física de instalaciones críticas del SEN	Instalaciones identificadas por el CEN como críticas para estabilidad del SEN	OPEX (evaluación) + CAPEX variable (medidas no modelables)	Solo la evaluación de riesgo físico por tercero acordado con el CEN es un costo predecible y modelable como driver del CAC. Las medidas resultantes de la evaluación (CCTV perimetral, cercado, iluminación, sensores de intrusión, refuerzo de perímetro) no se modelan en el CAC genérico: su variabilidad por instalación es prácticamente inmodelable y modelar un costo genérico introduciría una imprecisión mayor que declarar la limitación explícitamente. * Nota4 *	<i>⚠ Parcialmente excluido Solo evaluación de riesgo físico por tercero es modelable (ver Tabla 6 extendida)</i>

Nota2: Varios controles técnicos se solapan entre ellos, lo que se reflejará en el Modelo CAC y en la Capítulo 7

Nota3: La protección de comunicaciones en tránsito (CIP-012) varía críticamente según la arquitectura y propiedad de los enlaces de cada operador, haciéndola no modelable como un driver genérico sectorial. No obstante, desde el punto de vista del CAC, sus componentes técnicos de mitigación ya se encuentran absorbidos en los drivers core de infraestructura perimétrica: (1) Firewalls OT y Diodos de datos, los cuales ya proveen el aislamiento perimétrico, segmentación y tunelización segura (VPN) requerida para los canales de comunicación hacia el Coordinador (CDC) u otros centros de control, evitando la doble contabilidad de activos de red.

Nota4: Solo la evaluación de riesgo físico por tercero acordado con el CEN es un costo predecible y modelable (OPEX consultoría). Las medidas resultantes se EXCLUYEN del modelo CAC genérico por tres razones: (1) dependen completamente de los hallazgos específicos de cada instalación; (2) la variabilidad entre instalaciones es prácticamente inmodelable; (3) incluir un costo genérico introduciría una imprecisión mayor que declarar la limitación. La evaluación sí debe tener su propio driver de costo en el modelo CAC.

La Tabla 16 desarrolla exclusivamente los controles del primer bloque, es decir, aquellos que generan un driver de costo independiente en el modelo CAC. La separación de la capacitación en dos drivers independientes —básica (IEC 62443) y avanzada (GICSP/ISA IC34)— responde a que tienen estructuras de costo distintas: diferente nivel de certificación, diferente número de personas por grupo y diferente costo unitario entre Grupo A y Grupo B, lo que hace metodológicamente incorrecto tratarlos como un único componente.

Para la clasificación de los drivers, la Tabla 17 adopta la taxonomía de la OCDE [33], descrita en la sección 7.2, que distingue entre costos sustantivos de cumplimiento, y cargas administrativas. De los diecisiete drivers identificados, dieciséis corresponden a costos sustantivos y solo las auditorías externas del Art. 28° tienen naturaleza predominantemente administrativa.

Tabla 17. Drivers de Costos del Modelo CAC – Clasificación y correspondencia normativa (Fuente: Elaboración Propia)

N°	Control / Driver de Costo	Descripción del control integrado	Tipo OCDE	Naturaleza	Satisface Ley 21.663	Satisface Estándar CEN	Nivel impacto CEN	Perfil Económico	Justificación Económica
1	Asset Inventory OT	Un único inventario de activos OT satisface la obligación de SGSI de la ley (CIP-002) y a la vez permite establecer el baseline de configuración y la evaluación de vulnerabilidades (CIP-010), ya que las plataformas líderes del mercado (Claroty, Nozomi, Dragos) integran ambas funciones en un solo producto. Este control absorbe el CIP-010 R1-R3 sin costo adicional independiente.	Sustantivo	Tecnológica	Art. 8°(a) — SGSI + inventario activos ICI	CIP-002 — Categorización Ciber Sistemas SEN CIP-010 R1/R2/R3 — Baseline + gestión cambios + evaluación vulnerabilidades	Todos los niveles	CAPEX + OPEX	Plataforma de gestión e inventario OT con capacidad de monitoreo pasivo. Inversión inicial de implementación (CAPEX) y licencia/suscripción anual (OPEX). Driver diferenciado por Grupo A y Grupo B por diferencia de complejidad de integración.
2	Software SGSI — plataforma gestión ISO 27001	La plataforma de gestión del SGSI documenta, gestiona y certifica el sistema de seguridad exigido por la ley y materializa la política de ciberseguridad OT requerida por CIP-003. Genera un costo de implementación inicial independiente del rol del Delegado.	Sustantivo	Tecnológica	Art. 8°(a) — SGSI política de seguridad	CIP-003 — Controles de Gestión de la Seguridad	Todos los niveles	CAPEX	Costo de implementación y configuración inicial (CAPEX). Plataforma certificable ISO 27001 con funcionalidad de gestión documental y seguimiento de controles. Costo diferenciado de la herramienta Asset Inventory.
3	Delegado de Ciberseguridad / Encargado CIP	El Delegado exigido por Art. 8°(i) cumple el rol de Encargado CIP requerido por CIP-003. Un mismo rol y un mismo cargo cubren ambas obligaciones. Adicionalmente, este rol absorbe sin costo adicional: la gestión de la política de información OT (CIP-011), la integración normativa Ley↔CEN↔NTSyCS (Art. 26°) y el monitoreo de instrucciones ANCI (Art. 11°b).	Administrativo	Humana	Art. 8°(i) — Delegado con acceso alta dirección Art. 8°(a) — SGSI política de seguridad Art. 26° — integración normativa Art. 11°(b) — instrucciones ANCI	CIP-003 — Controles de Gestión CIP-011 — Protección información OT	Todos los niveles	OPEX	Sueldo anual del Delegado/Encargado CIP (OPEX puro). Denominado en CLP y convertido a USD mediante tipo de cambio parametrizable. Mayor especialización requerida en centrales con DCS propietario.
4	Capacitación OT básica — IEC 62443 (IC32/IC33)	Programa de capacitación en ciberseguridad OT de nivel básico-intermedio para todo el personal con acceso a Ciber Sistemas SEN. Certificaciones ISA IC32 (Fundamentals) o IC33 (Risk & Security). Satisface Art. 8°(h) y el programa de formación de CIP-004.	Administrativo	Humana	Art. 8°(h) — capacitación y ciberhigiene	CIP-004 — Personal y Capacitación	Impacto Alto y Medio	OPEX	Costo por persona capacitada al año (OPEX recurrente). Aplica a todo el personal con acceso a sistemas OT. Número de personas diferenciado por tipo de central.
5	Capacitación OT avanzada — GICSP / ISA IC34	Programa de capacitación avanzada en ciberseguridad OT para personal técnico especializado. GICSP (Global Industrial Cyber Security Professional) para Grupo B. ISA IC34 (nivel intermedio) para Grupo A. Menor número de personas que la capacitación básica.	Administrativo	Humana	Art. 8°(h) — capacitación continua personal OT	CIP-004 — Personal y Capacitación (nivel avanzado)	Impacto Alto y Medio	OPEX	Costo por persona certificada (mayor que capacitación básica). Grupo B requiere GICSP completo; Grupo A nivel ISA IC34. Menor número de personas que el .
6	Firewall OT ruggedizado — PSE	Firewall industrial que implementa el Perímetro de Seguridad Electrónica (PSE) de CIP-005. Satisface simultáneamente el deber de defensa en profundidad del Art. 8°(e). Control técnico único con doble cumplimiento normativo.	Sustantivo	Tecnológica	Art. 8°(e) — defensa en profundidad + restricción de acceso	CIP-005 — Perímetro de Seguridad Electrónica (PSE)	Impacto Alto y Medio	CAPEX	Activo fijo de infraestructura industrial (CAPEX). Precio por nodo diferenciado: Grupo A usa equipos entry-level (FortiGate Rugged); Grupo B requiere NGFW enterprise de mayor capacidad.
7	Diodo de datos — aislamiento unidireccional	Complementa el firewall en zonas con Ciber Sistemas SEN de mayor criticidad. Proporciona aislamiento físicamente unidireccional, eliminando la posibilidad de acceso bidireccional. Requerido donde CIP-005 exige aislamiento total más allá del firewall.	Sustantivo	Tecnológica	Art. 8°(e) — defensa en profundidad zona crítica	CIP-005 — PSE zona crítica (complemento al firewall)	Impacto Alto y Medio (según evaluación de riesgo)	CAPEX	Activo fijo complementario al firewall (CAPEX). Precio diferenciado: Grupo A usa modelos entry-level; Grupo B requiere modelos premium para DCS propietario.
8	Control acceso remoto — PAM / MFA / Sistema Intermedio	Solución de gestión de accesos privilegiados (PAM) con autenticación multifactor (MFA) para los Accesos Remotos Interactivos (ARI) exigidos por CIP-005 R2. El Sistema Intermedio es el mecanismo específico del Estándar CEN para ARI.	Sustantivo	Tecnológica	Art. 8°(e) — reducción de impacto Art. 8°(a) — SGSI gestión de accesos	CIP-005 R2 — Acceso Remoto Interactivo (ARI)	Impacto Alto y Medio	OPEX	Licencias anuales de plataforma PAM/MFA (OPEX). Aplica a todos los grupos donde existe acceso remoto a sistemas OT.

9	Control acceso físico sala OT — PSF (CIP-006)	Sistema de control de acceso físico al recinto interior donde están los Ciber Sistemas SEN: sala de control, cuarto de servidores OT, celdas de protección. Incluye lectoras de tarjeta/badge, CCTV interior y bitácora digital de accesos. Distinto de CIP-014: aplica al recinto interior OT, no a la instalación completa.	Sustantivo	Tecnológica	Art. 8°(e) — defensa en profundidad (dimensión física sala OT)	CIP-006 — Seguridad Física Ciber Sistemas SEN (PSF)	Impacto Alto y Medio	CAPEX	Costo acotado y predecible (CAPEX). Aplica principalmente a Grupo B y C; menor intensidad en Grupo A. Componentes: lectoras de tarjeta + controlador de acceso, CCTV interior, bitácora digital.
10	Hardening OT — configuración segura de sistemas	Configuración segura de sistemas OT: deshabilitación de puertos innecesarios, eliminación de servicios no requeridos y aplicación de configuración segura inicial. Satisface CIP-007 R1 y el deber de reducción de superficie de ataque del Art. 8°(e).	Sustantivo	Técnica	Art. 8°(e) — reducción superficie de ataque	CIP-007 R1 — Gestión de puertos y servicios	Impacto Alto y Medio	CAPEX	Inversión de implementación única con revisiones periódicas menores (CAPEX dominante). Costo por activo OT configurado.
11	Gestión de parches OT — ciclo CIP-007 R2	Ciclos periódicos de evaluación y aplicación de parches de seguridad en sistemas OT. CIP-007 R2 exige evaluación cada 35 días. El ciclo efectivo del modelo es trimestral (4 ciclos/año) por restricciones operacionales del sector eléctrico. Costo calculado como: N° Ciber-Sistema × horas-hombre × ciclos/año × costo HH técnico OT.	Sustantivo	Técnica	Art. 8°(e) — reducción de riesgos continua Art. 8°(a) — SGSI gestión de riesgos	CIP-007 R2 — Gestión de parches (evaluación cada 35 días)	Impacto Alto y Medio	OPEX	Horas-técnico OT recurrentes (OPEX). Costo proporcional al número de Ciber-Sistemas SEN de la central. Driver calculado internamente: N°Ciber-Sistema × 8 HH/activo × 4 ciclos/año × USD/HH.
12	SIEM industrial + monitoreo eventos seguridad OT	El SIEM industrial cubre cuatro obligaciones simultáneas: (1) trazabilidad legal del SGSI (Art. 8°b), (2) capacidad de detección para cumplir plazos DS 295, (3) monitoreo de eventos CIP-007 R4/R5, (4) soporte para evaluación de vulnerabilidades CIP-010 R3. Retención mínima de logs: 90 días (DS 295 Art. 9°).	Sustantivo	Tecnológica	Art. 8°(b) — registro auditable SGSI Art. 9°/DS 295 — trazabilidad para reportes	CIP-007 R4/R5 — Monitoreo eventos de seguridad CIP-010 R3 — Evaluación de vulnerabilidades	Impacto Alto y Medio	CAPEX + OPEX	Plataforma con componente de implementación inicial (CAPEX) y gestión/licencia continua (OPEX). Retención mínima 90 días es requisito legal verificable.
13	SOC MDR-OT 24/7 — monitoreo continuo externalizado	El servicio SOC MDR-OT externalizado es el mayor driver de costo del modelo. Cubre cinco obligaciones simultáneas: (1) detección en < 3h para alerta temprana DS 295, (2) monitoreo de eventos CIP-007 R4, (3) evaluación pasiva de vulnerabilidades CIP-010 R3, (4) coordinación de respuesta CIP-008 R2, (5) comunicación al CSIRT Nacional Art. 8°(d). Adicionalmente, absorbe el costo del Reporte DS 295 (protocolo 4 hitos) como tarea del SOC.	Sustantivo	Tecn. + Humana	Art. 9°/DS 295 — notificación 3h/24h/7d/15d Art. 8°(d) — detección y comunicación CSIRT	CIP-007 R4 — Monitoreo eventos CIP-008 R2 — Coordinación respuesta CIP-010 R3 — Evaluación pasiva	Impacto Alto y Medio	OPEX	Mayor driver de costo del modelo (OPEX puro). Precio diferenciado por Grupo A y B: entornos con DCS propietario requieren integraciones más complejas con fabricantes OEM.
14	Plan Continuidad + Infraestructura DRP + Plan IR	Plan de Continuidad (ley), Plan de Respuesta a Incidentes (CIP-008) y Plan de Recuperación (CIP-009) se fusionan en un instrumento único. La infraestructura DRP incluye: servidor de respaldo DCS, NAS externo para configuraciones OT, software de backup y medios fuera de línea. Certificación bianual exigida por Art. 28°.	Sustantivo	Tecnológica	Art. 8°(c) — planes de continuidad bienales Art. 8°(d) — simulacros periódicos	CIP-008 R1-R3 — Plan IR CIP-009 R1-R3 — Plan de recuperación OT	Impacto Alto y Medio	CAPEX + OPEX	Infraestructura DRP (servidor backup, NAS, software) es CAPEX. Ejercicios de recuperación y actualización del plan son OPEX anual. Mayor impacto en Grupo B por complejidad del DCS.
15	Pentesting OT y simulacros de respuesta	Ejercicios de pentesting OT y simulacros tabletop que ejecutan el deber de detección del Art. 8°(d) sobre sistemas OT. Los resultados se reportan al CSIRT Nacional. CIP-008 R1-R3 exige ejercicios periódicos del Plan IR. Control separado del DRP por tener diferente frecuencia y proveedor.	Sustantivo	Técnica	Art. 8°(d) — revisiones, simulacros y comunicación al CSIRT	CIP-008 R1-R3 — Ejercicios del Plan IR	Impacto Alto y Medio	OPEX	Costo por ejercicio anual de pentesting OT (OPEX). Precio diferenciado por Grupo A y B por complejidad del entorno OT.
16	Análisis BIA — matriz de criticidad de incidentes	El Análisis de Impacto de Negocio (BIA) produce la matriz de criticidad de incidentes exigida por el DS 295 Art. 3° para determinar qué eventos califican como de impacto significativo. Es un entregable independiente del SGSI general: requiere consultoría o análisis específico para sistemas OT. No está absorbido por ningún otro control.	Administrativo	Administrativa	DS 295 Art. 3° — criterios de impacto significativo Art. 8°(a) — SGSI gestión de riesgos	CIP-008 — soporte metodológico Plan IR	Impacto Alto y Medio	OPEX	Consultoría o análisis específico recurrente (OPEX). Revisión anual recomendada. Costo predecible e independiente de otros controles.
17	Auditorías externas	La auditoría externa bianual exigida por Art. 28° cubre simultáneamente: verificación del SGSI, CIP-010 R3	Administrativo	Administrativa	Art. 28° — certificaciones y auditorías periódicas	CIP-010 R3 — Verificación vulnerabilidades	Impacto Alto y Medio (Art.	OPEX	Costo recurrente bianual (OPEX). Precio diferenciado por Grupo A y B por alcance de la auditoría. La

	integradas — Art. 28° y Estándar CEN	(vulnerabilidades), CIP-013 (supply chain) y CIP-014 R2 (evaluación riesgo físico). Una auditoría integrada reemplaza evaluaciones independientes por instrumento normativo.			Art. 8°(a) — SGSI y gestión de riesgos	CIP-013 — Verificación supply chain CIP-014 R2 — Verificación evaluación riesgo físico	28° aplica a todos OIV)		integración en una sola auditoría reduce el costo total respecto a auditorías separadas.
⚠	Evaluación de riesgo físico instalación — CIP-014	CIP-014 exige una evaluación de riesgo físico de la instalación completa frente a amenazas deliberadas, realizada por tercero acordado con el CEN. Solo la evaluación es un costo predecible. Las medidas resultantes (CCTV perimetral, cercado, iluminación, sensores perimetrales) presentan variabilidad indeterminada y no se modelan en el CAC genérico.	Sustantivo	Técnica / Administrativa	Art. 8°(e) — defensa en profundidad (física instalación completa)	CIP-014 — Seguridad Física instalaciones críticas SEN	Instalaciones identificadas por CEN	OPEX (evaluación sola)	⚠ PARCIALMENTE EXCLUIDO: ** Nota 5 **
✗	Seguridad comunicaciones entre Centros de Control — CIP-012	CIP-012 exige proteger la confidencialidad e integridad de datos en tiempo real entre Centros de Control. Solo aplica a operadores con Centro de Control propio (SCADA ≥2 instalaciones). No aplica a generadoras sin CC propio.	Sustantivo	Tecnológica	Art. 8°(a) — SGSI integridad datos Art. 8°(e) — protección comunicaciones críticas	CIP-012 — Comunicaciones entre Centros de Control	Entidades con CC propio (SCADA ≥2 instalaciones)	CAPEX + OPEX	EXCLUIDO POR VARIABILIDAD E INTEGRADO EN ARQUITECTURA CORE ** Nota 6 **
⚠	Gestión de riesgos en cadena de suministro OT — CIP-013	CIP-013 exige plan de gestión de riesgos de supply chain para software y hardware OT, con cláusulas de ciberseguridad en contratos con proveedores y registro de firmware autorizado.	Administrativo	Administrativa	Art. 8°(a) — SGSI y gestión de riesgos Art. 8°(e) — integridad componentes OT	CIP-013 — Gestión Riesgos Cadena de Suministros	Impacto Alto y Medio	OPEX	ABSORBIDO EN CAPEX/OPEX EXISTENTE ** Nota 7 **

Nota5: Solo la evaluación de riesgo físico por tercero acordado con el CEN es un costo predecible y modelable (OPEX consultoría). Las medidas resultantes se EXCLUYEN del modelo CAC genérico por tres razones: (1) dependen completamente de los hallazgos específicos de cada instalación; (2) la variabilidad entre instalaciones es prácticamente inmodelable; (3) incluir un costo genérico introduciría una imprecisión mayor que declarar la limitación. La evaluación sí debe tener su propio driver de costo en el modelo CAC.

Nota6: La protección de comunicaciones en tránsito (CIP-012) varía críticamente según la arquitectura y propiedad de los enlaces de cada operador, haciéndola no modelable como un driver genérico sectorial. No obstante, desde el punto de vista del CAC, sus componentes técnicos de mitigación ya se encuentran absorbidos en los drivers core de infraestructura perimétrica: (1) Firewalls OT y Diodos de datos, los cuales ya proveen el aislamiento perimétrico, segmentación y tunelización segura (VPN) requerida para los canales de comunicación hacia el Coordinador (CDC) u otros centros de control, evitando la doble contabilidad de activos de red.

Nota7: El cumplimiento práctico de la cadena de suministro (CIP-013) no requiere un presupuesto aislado, sino que se mitiga a través de tres drivers core del modelo: (1) Control de Acceso Remoto (PAM) para la gestión y trazabilidad técnica de las conexiones de terceros; (2) Horas-hombre del Delegado de Ciberseguridad para la evaluación de riesgos contractuales de proveedores; y (3) Auditorías Externas (Art. 28°) para la verificación bianual del cumplimiento de los fabricantes. Se integra en estos ítems para reflejar la realidad operativa y evitar la doble contabilidad en el CAC.

La Tabla 17 presenta diecisiete drivers porque desagrega la capacitación en dos componentes independientes respecto de los dieciséis controles de la Tabla 16. El modelo diferencia el esfuerzo de cumplimiento entre tipologías mediante dos mecanismos verificables, ambos trazables en el modelo computacional:

Escalamiento por número de Ciber-Sistemas SEN (CS-SEN). Un subconjunto de drivers tiene su cantidad —no su costo unitario— determinada por el número de CS-SEN de la instalación, cuyo valor por tecnología se justifica en la sección 7.3.2 (Tabla 15), y se parametriza en la hoja 02_PARAMETROS de acuerdo a lógica de escalamiento presentada en la Tabla 18.

Tabla 18. Tipos de escala por CS-SEN en el modelo CAC (Origen: hoja 05_DRIVERS del modelo Excel) (Fuente: Elaboración Propia)

Tipo de escala	Regla de cálculo	Drivers afectados
Compartido	Cantidad fija = 1, independiente del N° de CS-SEN	Asset Inventory, Software SGSI, Delegado de Ciberseguridad, PAM/MFA, Control de acceso físico sala OT, Hardening OT, SIEM, SOC, Pentesting, Análisis BIA, Auditorías externas (11 de 17 drivers)
Ciclos	El costo se repite un número de veces al año en función del N° de CS-SEN. Gestión de parches (OPEX): $CS-SEN \times 8 \text{ HH/ciclo} \times 4 \text{ ciclos/año}$. Plan DRP: $CS-SEN \times 1 \text{ plan/backup}$ (CAPEX) y $CS-SEN \times 1 \text{ ejercicio/año}$ (OPEX)	Gestión de parches CIP-007, Plan DRP + Plan IR
Escalón-CS	La cantidad crece de forma no lineal según el N° de CS-SEN, con distinta fórmula por driver: Capacitación básica: $CS-SEN \times 8 \text{ personas/año}$. Capacitación avanzada: $MAX(1, CS-SEN - 1)$ especialistas. Firewall OT: $MAX(1, ROUND((CS-SEN-1)/2, 0))$. Diodo de datos: $MAX(1, CS-SEN - 1)$	Capacitación básica, Capacitación avanzada, Firewall OT, Diodo de datos

Esta clasificación evidencia que la mayoría de los drivers (11 de 17) tiene un costo de gobernanza fijo por instalación, no proporcional a su complejidad OT, mientras que solo los drivers técnicos directamente ligados a la arquitectura de control —capacitación, perímetro electrónico, parcheo, recuperación— escalan con el número de Ciber-Sistemas SEN.

Aplicabilidad y costo unitario diferenciado por grupo. Independiente del escalamiento por cantidad, la hoja 05_DRIVERS define qué drivers aplican a cada grupo y a qué costo unitario, reconociendo que un mismo control puede tener costo

distinto según la complejidad del entorno OT —por ejemplo, el Grupo A usa firewall pero no diodo de datos, y un firewall entry-level para el Grupo A cuesta distinto que un NGFW enterprise para el Grupo B.

Los drivers de naturaleza administrativa o de gobernanza —software SGSI, Delegado de Ciberseguridad, SOC MDR-OT, BIA, auditorías del Art. 28°— no escalan con CS-SEN ni varían sistemáticamente por grupo; se comportan como un costo de gobernanza por instalación, no por nodo. Los factores de escalamiento por grupo (F_GrA/B/C) son supuestos metodológicos propios del modelo, fijados con criterio técnico a partir de la caracterización de la sección 4.3, y no derivan de un estándar o benchmark externo verificable —su declaración explícita como supuestos es parte de la transparencia metodológica del modelo.

Si bien las obligaciones regulatorias son esencialmente comunes para el sector, el impacto económico de los drivers asociados no se manifiesta de manera homogénea en todas las instalaciones. Tal como se desarrolló en las secciones precedentes, las tipologías A, B y C presentan diferencias relevantes en su arquitectura de control y en la criticidad funcional de sus subsistemas OT. En consecuencia, el modelo considera que un mismo driver puede tener distinta expresión económica según la tipología de central, manteniendo una estructura común de obligaciones y drivers, pero permitiendo capturar diferencias estructurales en el esfuerzo de cumplimiento.

Finalmente, la identificación de obligaciones y drivers se realiza con un **criterio funcional y económico**, orientado a representar el esfuerzo mínimo necesario para cumplir con la normativa, más que a enumerar la totalidad de medidas posibles. Esta decisión metodológica es coherente con el objetivo del estudio, que busca estimar el impacto económico de la regulación a nivel comparativo y sectorial. La cuantificación de los drivers identificados y la definición de rangos de costos asociados se desarrollan en la siguiente subsección, sobre la base de la estructura establecida en la Tabla 16 y Tabla 17.

7.5 Fuentes de Costos y Calibración (Min/Med/Max)

La presente subsección fundamenta económicamente los diecisiete drivers de costo identificados en la Tabla 17, explicitando las fuentes de información utilizadas y los criterios de calibración aplicados para traducir cada driver en un rango de costo incorporable al modelo Excel. Esta sección no introduce obligaciones nuevas ni modifica la estructura de drivers definida en la sección anterior — su propósito exclusivo es explicar de dónde provienen los valores que alimentan las hojas 09_CAPEX y 10_OPEX del modelo computacional.

7.5.1 Enfoque metodológico de obtención y calibración de costos

La estimación de costos de ciberseguridad OT presenta una característica estructural que condiciona la metodología de esta sección: los principales proveedores de servicios y plataformas del segmento — servicios de monitoreo continuo MDR-OT, plataformas de inventario de activos industriales y servicios de auditoría IEC 62443 — no publican listas de precios de catálogo, dado que toda cotización se ajusta al tamaño de la instalación, al número de activos y al alcance del servicio requerido.

Ante esta realidad de mercado, la metodología de calibración del modelo adopta un enfoque en dos niveles. El primer nivel consiste en la investigación sistemática de fuentes públicas de referencia: benchmarking de mercado publicado por organizaciones sectoriales, informes de analistas especializados en ciberseguridad industrial, catálogos de fabricantes cuando están disponibles, y encuestas de mercado laboral para los drivers de recursos humanos. Este nivel establece los rangos Mínimo, Base y Máximo de cada driver. El segundo nivel consiste en la calibración con referencias del mercado chileno y latinoamericano, que permite ajustar los rangos obtenidos en el primer nivel a la realidad de precios local, evitando extrapolaciones directas desde mercados norteamericanos o europeos que no son representativos del costo efectivo en Chile.

Esta aproximación de dos niveles es metodológicamente consistente con el enfoque de estimación de costos regulatorios de la OCDE [33], que reconoce el uso de benchmarking sectorial y datos de mercado como fuentes válidas para la estimación de costos de cumplimiento cuando los precios de catálogo no están disponibles.

7.5.2 Drivers con fuentes de costo verificables públicamente

Como excepción a la dinámica general del mercado OT, dos categorías de drivers disponen de fuentes de costo con información pública verificable directamente:

Los programas de **capacitación y certificación** (drivers 4 y 5 de la Tabla 17) tienen aranceles publicados en los sitios web oficiales de los organismos certificadores. El programa ISA IC32, el examen GICSP del GIAC y los programas ISA IC34 publican sus tarifas vigentes, constituyendo los únicos drivers del modelo con precio directamente verificable.

El **Delegado de Ciberseguridad** (driver 3 de la Tabla 17) tiene su costo salarial respaldado por encuestas del mercado laboral chileno con metodología publicada. Las encuestas anuales de IT Hunters, TrendTIC y PROSFY Chile proveen rangos salariales para perfiles de Ingeniería OT con especialización en ciberseguridad, expresados en pesos chilenos. El modelo convierte estos valores a dólares mediante el tipo de cambio parametrizable en la hoja 02_PARAMETROS, de modo

que cualquier variación del tipo de cambio se propaga automáticamente al cálculo.

7.5.3 Criterios metodológicos transversales de selección de fuentes

De manera transversal a los diecisiete drivers, la selección de fuentes se rige por tres criterios explícitos:

El primero es la **trazabilidad normativa**: cada driver de costo está vinculado a una obligación identificable en la Tabla 21 y a un artículo específico de la Ley N.º 21.663 o del Estándar CEN, asegurando que ningún componente de costo carezca de ancla regulatoria.

El segundo es la **triangulación de fuentes**: cada driver se calibra con un mínimo de tres fuentes independientes, lo que permite establecer un rango verificable y justificar el valor del escenario base ante la dispersión natural de precios del mercado OT.

El tercero es la **aplicabilidad sectorial**: las fuentes de costos salariales priorizan encuestas del mercado laboral chileno, y para tecnología OT se utilizan referencias de distribuidores con presencia verificable en América Latina, descartando extrapolaciones directas desde benchmarks de mercados que no reflejan el nivel de precios local.

La calibración se estructura en tres escenarios — Mínimo, Base y Máximo — que reflejan la dispersión natural de precios del mercado. El escenario Base corresponde al valor medio de las fuentes consultadas, el Mínimo al cuartil inferior y el Máximo al cuartil superior o precio de soluciones premium. Esta estructura alimenta el análisis de dispersión de la sección 7.13 y la sensibilidad de la sección 7.12.

La Tabla 19 presenta la trazabilidad completa entre los diecisiete drivers, su estado de calibración y las fuentes de referencia utilizadas.

Tabla 19. Trazabilidad de Drivers, Estado de Calibración y fuentes de referencia (Fuente: Elaboración Propia)

N°	Driver de Costo	Tipo	Unidad	Fuente 1	Fuente 2	Fuente 3	Escenario Base
1	Asset Inventory OT (Implementación + Licencia)	CAPEX + OPEX	USD/año	Claroty CTD bundle mediano (CDW)	Dragos / Nozomi (Reddit benchmark)	Cotización referencial	USD 34.856
2	Software SGSI ISO 27001	CAPEX	USD (impl.)	Cybersafety — ISO 27001 empresa mediana	Orbit — ISO 27001 Certification Cost	ISM Directory — ISO 27001 Cost	USD 72.500
3	Delegado de Ciberseguridad <i>■ Convertido a USD: CLP 40.600.000 ÷ TC 940</i>	OPEX	CLP/año → USD	TrendTIC / IT Hunters — sueldos TI Chile 2024	TrendTIC — mercado ciberseg. Chile 2025	ITWorkers — Sueldo CISO Chile 2025	USD 43.191 (TC 940)
4	Capacitación OT básica (IEC 62443 IC32) <i>■ Cantidad: CS-SEN × 8 personas/año (escala con complejidad)</i>	OPEX	USD/persona/año	ISA Spain — curso IC32 IEC 62443	KnowBe4 — Security Awareness Training	TELEDUC — Ciberseguridad tácticas OT	USD 765
5	Capacitación OT avanzada (GICSP / ISA IC34) <i>■ Cantidad: MAX(1, CS-SEN – 1) especialistas</i>	OPEX	USD/persona/año	ISA Spain — curso IC34 IEC 62443	FEN UChile — Diploma en Ciberseguridad	SANS Institute — ICS Security (4 cursos)	USD 3.162
6	Firewall OT ruggedizado <i>■ Cantidad: MAX(1, ROUND((CS-SEN–1)/2,0)) - Grupos A y C</i>	CAPEX	USD/nodo	TuConsultorTI Chile — FortiGate Rugged 70F	CDW — FortiGate Rugged 70F + soporte	IndustrialNetworking — Hirschmann EAGLE40	USD 4.902
7	Diodo de datos OT <i>■ Cantidad: MAX(1, CS-SEN – 1) - Grupos B y C</i>	CAPEX	USD/unidad	Näringsliv — cuánto cuesta un data diode	Advenica — pricing FAQ data diodes	OPSWAT — guía data diodes OT	USD 20.050
8	Control acceso remoto PAM / MFA	OPEX	USD/año	ITPrices — Fortinet FortiPAM Solution	CDW — Claroty SRA licencia anual	Cotización referencial	USD 18.992
9	Control acceso físico sala OT (PSF) <i>■ Aplica principalmente Grupos B y C</i>	CAPEX	USD	ControlDeAccesos.eu — sistema básico acceso	Safe and Sound Security	LatestCost — Commercial Security System	USD 13.667
10	Hardening OT (implementación)	CAPEX	USD	DeciferU — cybersecurity freelancers rates	Scale Up Ally — IT Consulting Rates 2026	Clutch — Cybersecurity Pricing Guide 2026	USD 27.333
11	Gestión parches CIP-007 (horas técnico OT) <i>■ F11-A (Gr.A): USD 336/HH base. F11-BC (Gr.B/C): USD 264/HH base. Escala: CS-SEN × 8 HH/ciclo</i>	OPEX	USD/hora técnico	Cotización referencial Gr.A	Cotización referencial Gr.B/C	Cotización referencial	USD 336

12	SIEM industrial (Implementación + Licencia) <i>■ CAPEX impl: USD 326.667 base. OPEX lic.: USD 79.633/año base</i>	CAPEX + OPEX	USD impl. / USD lic./año	Uptrace — Splunk Implementation & Pricing	A-Listware — SIEM Implementation Cost	SIEMCostCalculator / Blumira — SIEM TCO	USD 326.667
13	SOC MDR-OT 24/7 externalizado <i>■ Mayor driver de OPEX. Precio diferenciado Gr.A vs Gr.B por complejidad DCS</i>	OPEX	USD/año	UnderDefense — calculadora costos SOC	BorneoCR — SOC as a Service 24/7 LATAM	Cotización referencial	USD 66.000
14	Plan DRP + Plan IR (Infraestructura + Ejercicios) <i>■ CAPEX infra: USD 28.833 base. OPEX ejercicios: USD 21.832/año base. Escala: CS-SEN × 1 plan/ejercicio</i>	CAPEX + OPEX	USD	DELL EMC — Storage / ServerBasket — NAS 100TB	ZManda — DR Cost Comparison	Acronis Lic. + Veeam Software	USD 28.833
15	Pentesting OT y simulacros	OPEX	USD/ejercicio/año	Blaze — Penetration Testing Cost & Pricing	DeepStrike — Penetration Testing Pricing 2026	Security Wall — Penetration Test Cost	USD 38.000
16	Análisis BIA (consultoría impacto negocio) <i>■ Revisión anual recomendada. Costo predecible e independiente</i>	OPEX	USD	PricingLink — Business Continuity Plan Pricing	Core MBA — Consulting Rates Benchmark	Fractional CFO — Consulting Fees Guide	USD 57.333
17	Auditorías externas integradas Art. 28° <i>■ Bianual (Art. 28°). Cubre CIP-010 R3, CIP-013, CIP-014 R2 en una sola auditoría</i>	OPEX	USD/evento	Astra Security — IT Security Audit Cost 2026	IBSSCORP — Cybersecurity Audit Cost 2026	PentestingTeam — Auditoría ciberseguridad	USD 26.083

- Notas metodológicas:**
- Escenario Base = media de las tres fuentes consultadas por driver. Rango completo (Mín–Máx) disponible en hoja 06_FUENTES_COSTOS del modelo v33.
 - F04 y F05 (capacitaciones): la unidad es USD/persona/año; la cantidad escala con CS-SEN según lógica ESCALÓN-CS definida en hoja 05_DRIVERS.
 - F03 (Delegado): valor expresado en CLP/año; convertido a USD mediante tipo de cambio parametrizable (TC) en celda 02_PARAMETROS/C11.
 - F11 (parches): valor unitario por hora técnico OT. El OPEX total se calcula como: N° CS-SEN × 8 HH/ciclo × 4 ciclos/año × USD/HH.
 - F06, F07, F14 (FW/diodo/DRP): cantidades no fijas; escalan con N° Ciber-Sistemas SEN (CS-SEN) según reglas definidas en hoja 07b del modelo.
 - Estado de calibración: todos los drivers cuentan con ≥3 fuentes verificadas. Fuentes con cotización directa: F01C, F01O, F08, F11-A, F11-BC.
 - Fuente: elaboración propia a partir de la hoja 06_FUENTES_COSTOS del modelo Modelo_CAC_Ley21663_Final_v33.xlsx.

7.6 Formulación matemática del modelo CAC

La sección 7.5 fundamentó económicamente los diecisiete drivers de la Tabla 17 y sus fuentes de calibración. La presente sección completa el ciclo metodológico del OE5 mediante dos contribuciones: (i) la formulación matemática explícita del CAC; y (ii) la descripción del mecanismo de anualización de inversiones a través del Factor de Recuperación de Capital (FRC). La arquitectura computacional del modelo se desarrolla en la sección 7.7 y los resultados aplicados a las cinco tipologías se presentan en la secciones 7.9 y 7.11.

7.6.1 Estructura matemática del modelo

El Costo Anualizado de Cumplimiento se define formalmente como la suma de dos componentes que operan bajo una lógica temporal común: el CAPEX inducido por la normativa, expresado en términos anuales equivalentes, y el OPEX recurrente, que por su naturaleza ya tiene periodicidad anual:

Ecuación 4

$$CAC = CAPEX_{ciber_anualizado} + OPEX_{ciber_anual}$$

El componente CAPEX_ciber_anualizado representa la anualización de las inversiones en infraestructura de ciberseguridad OT requeridas por la normativa. El componente OPEX_ciber_anual agrupa los gastos operativos recurrentes necesarios para sostener el cumplimiento en el tiempo. Ambos se expresan en dólares estadounidenses por año (USD/año) y se obtienen a partir de los drivers identificados en la Tabla 17 de la sección 7.4.1.

El CAPEX_ciber_anualizado se calcula como la sumatoria sobre todos los drivers de inversión i aplicables a la tipología de central analizada:

Ecuación 5

$$CAPEX_{ciber_anualizado} = \sum_i [Qty(i) \times Costo_unitario(i) \times FRC(r, n_i)]$$

donde Qty(i) es la cantidad de unidades del driver i , Costo_unitario(i) es el valor unitario obtenido de la hoja 06_FUENTES_COSTOS, y FRC(r, n_i) es el Factor de Recuperación de Capital para la tasa de descuento r y la vida útil específica del activo n_i . El OPEX_ciber_anual se obtiene directamente como:

Ecuación 6

$$OPEX_{ciber_anual} = \sum_j OPEX(j)$$

donde j recorre todos los drivers de gasto recurrente aplicables. A diferencia del CAPEX, los drivers OPEX no requieren anualización porque ya tienen horizonte temporal de un año.

Las Ecuaciones 5, 6 y 7 pueden expresarse de forma compacta en una única formulación integrada que explicita el FRC directamente en la sumatoria del CAPEX, dejando claro que el CAC es un indicador estático anualizado (USD/año) y no un flujo de caja plurianual:

Ecuación 7 - Expresión general integrada

$$CAC = \sum_{j=1}^M \left(CAPEX_j * \frac{i * (1 + i)^{n_j}}{(1 + i)^{n_j} - 1} \right) + \sum_{k=1}^V OPEX_k$$

Donde j es el índice de cada uno de los M drivers de inversión de capital, k es el índice de cada uno de los V drivers de gasto operativo recurrente, i es el WACC (8%) y n_j es la vida útil específica del driver j .

7.6.2 El Factor de Recuperación de Capital (FRC)

El elemento matemático central del modelo CAC —y el que lo distingue de una simple suma de costos— es el **Factor de Recuperación de Capital (FRC)**. Su propósito es convertir una inversión de capital realizada en un período determinado en su equivalente anual uniforme, incorporando el costo de oportunidad del capital a través de la tasa de descuento. La expresión es:

Ecuación 8

$$FRC(r, n) = \frac{r \cdot (1 + r)^n}{(1 + r)^n - 1}$$

donde r es el WACC del sector (parámetro P01 en la hoja 02_PARAMETROS, fijado en 8% nominal en USD, como valor base a partir de resoluciones tarifarias de la CNE) y n es la vida útil del activo cibernético en años. El CAPEX anualizado de un driver individual resulta entonces:

Ecuación 9

$$CAPEX_{anu}(i) = CAPEX_{total}(i) \times FRC(r, n_i)$$

La razón por la que el modelo utiliza el FRC en lugar de la depreciación lineal simple radica en que esta última ignora el costo de oportunidad del capital inmovilizado. Si un operador invierte USD 28.000 en ocho firewalls OT industriales hoy, ese capital tiene un costo alternativo: de no haberse invertido, podría estar generando un retorno del 8% anual en otra aplicación del sector. El FRC incorpora este costo de oportunidad. La diferencia concreta para el caso de los firewalls OT ($n = 5$ años, $r =$

8%) es:

Depreciación lineal: USD 28.000 / 5 = USD 5.600 / año

FRC(8%, 5 años): $0,08 \times (1,08)^5 / [(1,08)^5 - 1] = 0,2505$

CAPEX anualizado (FRC): USD 28.000 $\times$ 0,2505 = USD 7.013 / año

Diferencia (costo de oportunidad del capital): USD 1.413 / año

La formulación adoptada en este modelo corresponde al **Capital Recovery Factor (CRF)** utilizado por el NREL en su Annual Technology Baseline 2024, definido como $CRF = WACC \times (1+WACC)^n / [(1+WACC)^n - 1]$, el cual constituye el núcleo del Fixed Charge Rate (FCR) empleado por dicha fuente para anualizar costos de capital en tecnologías de generación eléctrica [34].

El modelo aplica tres valores de FRC diferenciados según la naturaleza del activo, dado que la vida útil es el parámetro que mayor variación produce en el factor de anualización. La Tabla 20 siguiente sistematiza estos valores:

Tabla 20. Valores del FRC por categoría de activo cibernético (WACC = 8%) (Fuente: Elaboración Propia – Proviene Excel)

Tipo de activo cibernético	Vida útil (n)	FRC (r=8%)	Activos incluidos
Hardware OT	5 años	0,2505	Firewalls industriales, diodos de datos, switches OT
Software / licencias	3 años	0,3880	Plataformas asset inventory, SIEM OT, software SGSI
Infraestructura OT	7 años	0,1921	Redundancia DCS, servidores historian, cableado estructurado

Obsérvese que el FRC es inversamente proporcional a la vida útil: un software que debe reemplazarse cada 3 años genera una carga anual equivalente (FRC = 0,388) significativamente mayor que una infraestructura con vida útil de 7 años (FRC = 0,192), aun si ambos tienen el mismo costo inicial. Esta diferencia tiene consecuencias directas sobre la composición del CAPEX anualizado entre tecnologías.

7.6.3 Indicadores regulatorios como output del modelo

El CAC no se presenta únicamente como valor absoluto en USD/año, sino que sus componentes se expresan como variaciones porcentuales sobre los indicadores del RPTD N.º 17, conectando el análisis económico con el lenguaje de gestión de activos de la SEC:

Ecuación 10

$$\Delta XX - CAPV (\%) = CAPEX_ciber_anualizado / V.I._planta \times 100$$

Ecuación 11

$$\Delta XX - OPEV (\%) = OPEX_ciber_anual / V.I._planta \times 100$$

donde V.I._planta es el Valor de Inversión de la central tipo de 100 MW, obtenido de la hoja 06_FUENTES_COSTOS para cada tecnología. Adicionalmente, el modelo calcula un tercer indicador integrador que sintetiza el esfuerzo total de cumplimiento como fracción del valor del activo:

Ecuación 12

$$\Delta CAC / V.I. (\%) = CAC_total / V.I._planta \times 100$$

Este denominador común es lo que permite comparar el esfuerzo de cumplimiento entre tecnologías de generación con escalas de inversión muy distintas. Un mismo CAC absoluto puede representar un impacto proporcional muy distinto según el Valor de Inversión de cada tecnología. Esta propiedad del indicador es la base del análisis de proporcionalidad desarrollado en la sección 7.11, donde se presetan los resultados completos para las cinco tipologías evaluadas. Cabe precisar que el $\Delta CAC/V.I.$ mide el esfuerzo de cumplimiento como proporción del capital invertido en la construcción de la central —es decir, la intensidad del costo de cumplimiento respecto del tamaño económico de la inversión inicial de cada tipología—, coherente con la lógica de los indicadores ΔXX del RPTD N.º 17 que el sector ya reporta a la SEC (Ecuación 10 y Ecuación 11).

7.7 Arquitectura computacional del modelo Excel

La operacionalización de la metodología descrita se materializa en el modelo computacional **Modelo_CAC_Ley21663_EstandarCEN_Final.xlsx**, desarrollado en Microsoft Excel con arquitectura modular de 13 hojas interconectadas. El modelo fue concebido como herramienta de análisis académico y no como software de gestión empresarial; su propósito es permitir la verificación, replicación y análisis de sensibilidad de los resultados del CAC de manera transparente y trazable.

La arquitectura sigue un flujo lógico de tres capas. La primera capa, de referencia normativa, contiene las hojas de contexto y documentación. La segunda capa, de parámetros de entrada, contiene las hojas que alimentan todos los cálculos —siendo la hoja 02_PARAMETROS el nodo raíz desde el cual cualquier cambio se propaga automáticamente a todo el modelo. La tercera capa, de cálculo y

resultados, contiene las hojas de cómputo y visualización. La Tabla siguiente detalla el rol de cada hoja en el flujo:

Tabla 21. Arquitectura del modelo computacional Modelo Excel CAC (13 hojas) (Fuente: Modelo Excel - Elaboración Propia)

Hoja	Tipo	Contenido y rol en el modelo
00_PORTADA	Navegación	Índice de hojas y contexto de la tesis. Punto de entrada al modelo.
01_GUIA_USO	Documentación	Flujo entre hojas, convención de colores, fórmulas clave explicadas en lenguaje simple.
02_PARAMETROS	Entrada ★	Parámetros editables por el usuario: WACC (8%), vidas útiles diferenciadas, TC CLP/USD (940), potencia (100 MW), N° Ciber-Sistemas SEN. Nodo raíz: cualquier cambio aquí se propaga automáticamente a todo el modelo.
03_TIPOS_PLANTA	Referencia	Caracterización técnica OT de los Grupos A, B y C (protocolo, N° Ciber-Sistemas SEN, complejidad de parcheo, riesgo cinético).
04_OBLIGACIONES	Referencia	Matriz de obligaciones de la Ley 21.663 y el Estándar CEN con sus drivers de costo, tipo OCDE y aplicabilidad por grupo.
05_DRIVERS	Referencia	Factores de escala en función de los CS-SEN que calculan mediante polinomio el costo base según arquitectura OT.
06_FUENTES_COSTOS	Entrada	Base de datos de costos: ≥3 fuentes verificadas por driver con URL activa, rangos Mín/Med/Máx. Fuente primaria del modelo. Sin valores hardcodeados.
07_CAPEX	Cálculo	CAPEX anualizado: $CAPEX_{total} \times FRC(r, n)$ para cada driver y tecnología. Escenarios Mín/Med/Máx. Fila 15 = totales por tecnología.
08_OPEX	Cálculo	OPEX anual por driver y tecnología. Escenarios Mín/Med/Máx. Salarios CLP convertidos a USD con TC de hoja 02. Fila 20 = totales.
09_SIMULADOR	Resultado	CAC Total = $CAPEX_{anu} + OPEX$. Tabla de rangos Mín/Med/Máx. $\Delta XX-CAPV$, $\Delta XX-OPEV$ y $\Delta CAC/V.I.$ por tecnología.
10_RESULTADOS	Resultado	Dashboard comparativo con presentación recomendada 'USD X – USD Y (base: USD Z)' para defensa ante comité.

11_SENSIBILIDAD	Análisis	3 variables × 5 niveles: WACC, Tipo de Cambio CLP/USD, N° Nodos CS-SEN. Fórmulas 100% dinámicas.
12_GLOSARIO	Documentación	30 términos clave con definición técnica y relevancia específica para el CAC.

Fuente: elaboración propia. ★ = nodo raíz: los cambios en 02_PARAMETROS se propagan automáticamente a todo el modelo.

El modelo entrega resultados en tres formatos complementarios: (i) **valores absolutos** (CAC en USD/año); (ii) **rangos Mín/Máx** que reflejan la dispersión de precios de mercado documentada en las fuentes —metodológicamente más honestos que un valor puntual único dado que los proveedores de servicios de ciberseguridad OT no publican listas de precios uniformes—; y (iii) **indicadores regulatorios normalizados** ($\Delta XX\text{-CAPV}$, $\Delta XX\text{-OPEV}$, $\Delta CAC/V.I.$) que conectan el análisis económico con el lenguaje del RPTD N.º 17 ya analizado en la sección 7.6. Finalmente, la hoja 11_SENSIBILIDAD permite explorar el impacto de tres variables clave —WACC, tipo de cambio CLP/USD y número de nodos CS-SEN— sobre el CAC total, con cinco niveles de variación por variable, dotando al modelo de capacidad analítica para evaluar la robustez de los resultados bajo distintos escenarios.

7.8 Alcances y limitaciones del modelo

El modelo de Costo Anualizado de Cumplimiento (CAC) desarrollado en la presente investigación tiene por objetivo estimar, de forma estructurada y comparable, el esfuerzo económico anual que representa el cumplimiento de las obligaciones de ciberseguridad establecidas por la Ley N.º 21.663 con sus decretos reglamentarios y el Estándar de Ciberseguridad del CEN para operadores del sector de generación eléctrica. En este contexto, resulta necesario precisar de manera explícita los alcances, supuestos y limitaciones del modelo, con el fin de asegurar una interpretación adecuada de los resultados que se presentarán en las secciones 7.9 a 7.13.

En cuanto a su alcance, el modelo CAC se concibe como una herramienta de análisis económico de carácter comparativo y agregado, orientada a capturar el orden de magnitud de los costos asociados al cumplimiento normativo. El CAC integra tanto costos de inversión (CAPEX) como costos operativos (OPEX), anualizados bajo supuestos explícitos, permitiendo comparar el impacto relativo del cumplimiento entre distintas tecnologías de generación, tipologías de activos y escenarios regulatorios. El modelo no persigue la elaboración de presupuestos detallados ni la simulación financiera de proyectos específicos, sino la construcción de un marco económico consistente que permita evaluar proporcionalidades, impactos relativos y tendencias generales.

El modelo se apoya en un conjunto de supuestos estructurales necesarios para su operacionalización. Entre ellos se encuentran la definición de vidas útiles económicas para los componentes de inversión, la utilización de tasas de descuento representativas del sector energético y la estandarización de ciertas unidades de análisis con fines comparativos. Asimismo, el uso de rangos de costo y escenarios (bajo, medio y alto) constituye un supuesto metodológico central, diseñado para capturar la heterogeneidad existente en la implementación real de medidas de ciberseguridad sin perder coherencia analítica.

Una característica estructural del mercado de ciberseguridad OT es que los principales servicios y soluciones no disponen de precios públicos de catálogo, dado que las cotizaciones se realizan de forma directa y se ajustan al tamaño y criticidad de cada instalación.

El modelo aborda esta característica mediante el enfoque de dos niveles descrito en la sección 7.5, investigación sistemática de fuentes públicas de referencia para establecer rangos de orden de magnitud, complementada con calibración mediante referencias del mercado chileno y latinoamericano para ajuste fino. Esta aproximación es consistente con las prácticas de análisis económico regulatorio reconocidas por la OCDE [33] y se refleja en el uso de escenarios Mínimo, Base y Máximo a lo largo del modelo.

Asimismo, el CAC no incorpora de manera explícita ciertos **costos** indirectos o de segundo orden, tales como pérdidas por indisponibilidad, impactos reputacionales, sanciones potenciales por incumplimiento o efectos dinámicos asociados a incidentes de ciberseguridad de alta severidad. Estos elementos, aunque relevantes desde una perspectiva de riesgo, presentan una elevada variabilidad y dependencia de contextos específicos, por lo que su inclusión excede el alcance metodológico definido para el modelo.

Desde el punto de vista de su aplicabilidad, los resultados del CAC deben interpretarse como estimaciones representativas para operadores del sector de generación eléctrica bajo supuestos de cumplimiento razonable y sostenido de la normativa. El modelo no pretende capturar particularidades extremas de instalaciones individuales ni sustituir evaluaciones técnicas o económicas detalladas a nivel de proyecto o empresa. En este sentido, el CAC debe entenderse como una herramienta de análisis económico regulatorio y no como un instrumento de planificación financiera operativa.

Finalmente, las limitaciones y supuestos aquí expuestos no invalidan la utilidad del modelo, sino que delimitan de manera clara su campo de aplicación. Al explicitar estos elementos, el modelo CAC refuerza su rigurosidad metodológica y establece un marco transparente para la interpretación de los resultados que se presentarán a posterior en las secciones 7.9 a 7.13, los cuales deben leerse a la luz de los

alcances definidos en esta sección.

7.9 Resultados del modelo: Comparación entre tipologías

Aplicando la metodología descrita en las secciones 7.4 a 7.6 —identificación de drivers por grupo tecnológico, cálculo del CAPEX anualizado mediante el Factor de Recuperación de Capital y del OPEX anual, y agregación en el Costo Anualizado de Cumplimiento— se obtienen los resultados para las tipologías de generación caracterizadas en la sección 7.3. El detalle completo de cálculo por driver —CAPEX y OPEX individual de cada uno de los diecisiete drivers, según la fórmula presentada en las Ecuaciones 4 a 9— es reproducible y auditable directamente en el modelo Excel que acompaña este informe; la Tabla 22 presenta los resultados agregados por tecnología.

Tabla 22. Costo Anualizado de Cumplimiento (CAC) por tipología de central — Escenario base (Med), 100 MW (Fuente: Elaboración Propia)

Tecnología	Grupo	CS-SEN	CAPEX anu. (USD/año)	OPEX anual (USD/año)	CAC Total (USD/año)	CAC/MW (USD/MW·año)	CAC/CS-SEN (USD)
Solar FV	A	2	190.988	424.492	615.480	6.155	307.740
Eólica	A	3	196.526	451.305	647.831	6.478	215.944
Térmica Gas	B	5	219.615	505.201	724.816	7.248	144.963
Hidro	B	4	209.056	478.966	688.022	6.880	172.005
Subestación (ref.)	C	3	72.966	449.569	522.535	5.225	174.178

El rango entre tecnologías de generación va de USD 615.480/año (Solar FV) a USD 724.816/año (Térmica Gas), con una dispersión relativa del **17,8%** entre el valor mínimo y máximo dentro del segmento de generación. Esta diferencia responde principalmente a la mayor cantidad de Ciber-Sistemas SEN en tecnologías de proceso continuo del Grupo B (4-5 CS-SEN) frente al Grupo A (2-3 CS-SEN), que amplifica los drivers cuya cantidad escala con el número de CS-SEN, identificados en la Tabla 18 (sección 7.4). La Subestación se incluye como referencia adicional de infraestructura de interconexión, fuera del alcance de generación que constituye el objeto de este estudio.

7.9.1 La normalización por CS-SEN invierte el ordenamiento entre tecnologías

La comparación en valores absolutos posiciona a Térmica Gas con el CAC más alto (USD 724.816) y a Solar FV con el más bajo (USD 615.480) dentro del segmento de generación. Sin embargo, al normalizar por Ciber-Sistema SEN —columna

CAC/CS-SEN de la Tabla 22— la relación se invierte: Solar FV presenta el CAC/CS-SEN más elevado (USD 307.740), mientras que Térmica Gas presenta el más bajo (USD 144.963).

Esta inversión ocurre porque una parte significativa de los drivers del modelo —los de naturaleza administrativa y de gobernanza clasificados como "Compartido" en la Tabla 18 (Asset Inventory, Software SGSI, Delegado de Ciberseguridad, PAM/MFA, Control de acceso físico, Hardening OT, SIEM, SOC, Pentesting, Análisis BIA y Auditorías externas)— tienen cantidad fija, independiente del número de CS-SEN de la instalación. Solar FV distribuye ese costo fijo entre solo 2 Ciber-Sistemas SEN, mientras que Térmica Gas lo distribuye entre 5. Por unidad de sistema de control a proteger, las centrales del Grupo A soportan así un mayor costo de cumplimiento relativo, aun cuando su CAC absoluto sea menor que el de Térmica Gas.

Este hallazgo anticipa un patrón que se desarrolla con mayor profundidad en la sección 7.11: la concentración de costos fijos de gobernanza en un número reducido de Ciber-Sistemas SEN penaliza proporcionalmente más a las tecnologías con arquitecturas de control más simples, con independencia de su costo absoluto de cumplimiento.

7.10 Estructura CAPEX/OPEX y dominancia operativa

La Tabla 22 mostró el CAC total por tecnología, pero no su composición interna. La Tabla 23 desagrega ese total en sus dos componentes —CAPEX anualizado y OPEX anual— y calcula la participación porcentual de cada uno, revelando un patrón estructural común a todas las tipologías evaluadas.

Tabla 23. Composición CAPEX/OPEX del CAC por tipología — Escenario base (Med) (Fuente: Elaboración Propia)

Tecnología	CAPEX anualizado (USD/año)	% CAPEX	OPEX anual (USD/año)	% OPEX
Solar FV	190.988	31,0%	424.492	69,0%
Eólica	196.526	30,3%	451.305	69,7%
Térmica Gas	219.615	30,3%	505.201	69,7%
Hidro	209.056	30,4%	478.966	69,6%
Subestación (ref.)	72.966	14,0%	449.569	86,0%

El resultado central es que el OPEX domina el CAC en las cinco tipologías, con una participación que se mantiene notablemente estable entre el 69,0% y el 69,7% en las cuatro tecnologías de generación —Solar FV, Eólica, Térmica Gas e Hidro—, con independencia de su arquitectura de control OT o de su grupo tecnológico. Esta

uniformidad no es casual: refleja que la estructura del cumplimiento normativo está dominada por servicios recurrentes —monitoreo continuo, licenciamiento de software, capital humano especializado— antes que por infraestructura física de protección.

Este hallazgo tiene una implicancia directa sobre la naturaleza económica del cumplimiento: la ciberseguridad OT no es una inversión puntual que se deprecia y desaparece del balance del operador, sino una carga operativa permanente que debe presupuestarse año a año, de forma análoga a otros costos de operación y mantenimiento del activo eléctrico, y no como un proyecto de capital que se ejecuta una vez.

7.10.1 Drivers OPEX de mayor peso individual

Para Solar FV, los tres drivers OPEX de mayor peso individual son la licencia SIEM OT (USD 79.633/año, 12,9% del CAC total), el SOC MDR-OT 24/7 (USD 66.000/año, 10,7% del CAC total) y el Análisis BIA (USD 57.333/año, 9,3% del CAC total). Este patrón —dominado por servicios de monitoreo continuo y consultoría especializada, más que por licencias de software puntuales— es consistente en las demás tecnologías de generación, con variaciones menores en el peso relativo de cada driver según el grupo tecnológico y el número de Ciber-Sistemas SEN a proteger.

El hallazgo central es que el SIEM industrial —su implementación (CAPEX) y su licencia anual (OPEX), combinadas— concentra por sí solo entre el 28% y el 33% del CAC total en las cuatro tecnologías, siendo el componente individual más costoso del modelo en todos los casos, muy por encima del segundo driver en importancia.

El segundo patrón relevante es que el Plan DRP + Plan IR (ejercicios de recuperación) es el único driver del grupo de mayor costo que se desplaza significativamente en el ranking entre tipologías, escalando su participación con el número de Ciber-Sistemas SEN de cada tecnología: de un peso menor en Solar FV (2 CS-SEN) a la segunda posición en Térmica Gas (5 CS-SEN). El resto de los drivers principales —SOC MDR-OT 24/7, Asset Inventory OT y Análisis BIA— mantiene una magnitud prácticamente idéntica entre tecnologías, reflejando su naturaleza de costo fijo de gobernanza.

En el extremo opuesto, los drivers de menor costo —Firewall OT ruggedizado, Control de acceso físico y Capacitación OT avanzada— representan en conjunto menos del 3% del CAC total, y algunos de ellos —Firewall y Hardening OT— no aplican a los Grupos B (Térmica, Hidro), que utilizan en su lugar el Diodo de datos como mecanismo de aislamiento perimetral, consistente con la aplicabilidad diferenciada por grupo establecida en la sección 7.4.

La Ilustración 9 desagrega el CAC en sus diecisiete drivers de costo para las cuatro tecnologías de generación evaluadas. Las barras representan el escenario base (Med); las líneas horizontales indican el rango de dispersión de mercado entre los escenarios Mínimo y Máximo (sección 7.13) para cada driver y tecnología.

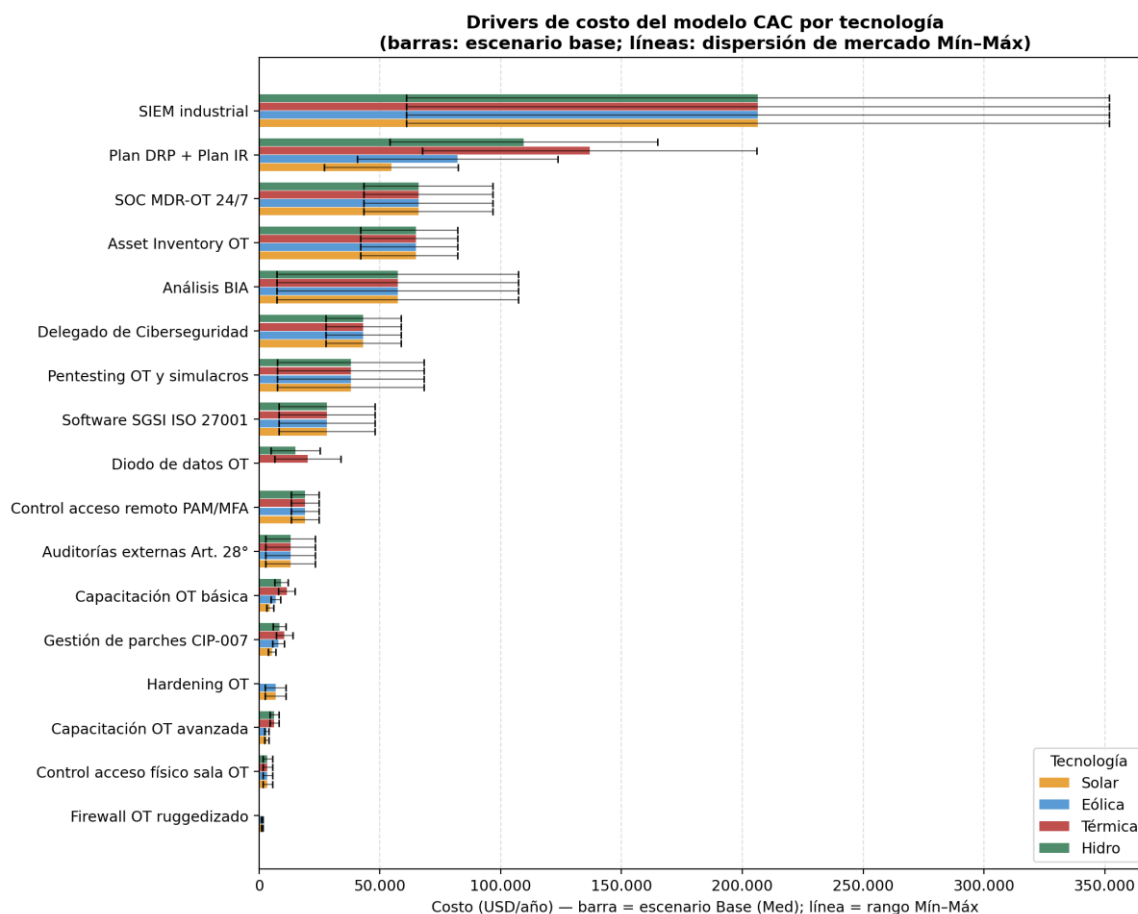


Ilustración 9. Drivers de costo del modelo CAC por tecnología, escenario base con rango de dispersión Mín-Máx (Fuente: Elaboración Propia)

7.11 La paradoja de la proporcionalidad

La sección 7.6 introdujo el indicador $\Delta\text{CAC}/\text{V.I.}$ como medida del esfuerzo de cumplimiento relativo al capital invertido en cada tecnología. La Tabla 24 aplica ese indicador a las cuatro tecnologías de generación evaluadas, incorporando el Valor de Inversión (V.I.) de cada una desde la fuente CNE ICTGA2025.

Tabla 24. Indicadores de proporcionalidad regulatoria ΔXX por tipología de generación, sobre el Valor de Inversión
(Fuente: Elaboración Propia, V.I. desde CNE ICTGA2025)

Tecnología	Grupo	V.I. Base (USD)	ΔXX -CAPV	ΔXX -OPEV	$\Delta CAC/V.I.$	Clasificación
Solar FV	A	80.900.000	0,236%	0,525%	0,761%	Moderado
Eólica	A	148.300.000	0,133%	0,304%	0,437%	Bajo
Térmica Gas	B	111.700.000	0,197%	0,452%	0,649%	Moderado
Hidro	B	488.000.000	0,043%	0,098%	0,141%	Bajo

El indicador $\Delta CAC/V.I.$ varía entre el 0,141% de Hidro y el 0,761% de Solar FV —una diferencia de 5,4 veces—, revelando lo que este estudio denomina la paradoja de proporcionalidad: pese a que el CAC absoluto de Hidro (USD 688.022/año) es superior al de Solar FV (USD 615.480/año) en términos de dólares por año, su esfuerzo relativo al capital invertido es sustancialmente menor. Esta asimetría se explica enteramente por el denominador: el V.I. de Hidro (USD 488.000.000) es aproximadamente 6 veces mayor que el de Solar FV (USD 80.900.000), de modo que un CAC absoluto similar se diluye de forma muy distinta según la escala de capital de cada tecnología.

7.11.1 La paradoja no refleja una diferencia en las obligaciones exigidas

Es necesario precisar el alcance de este hallazgo: la variación del $\Delta CAC/V.I.$ entre tecnologías es de carácter puramente proporcional y no implica que el marco regulatorio —la Ley 21.663 y el Estándar CEN— imponga obligaciones distintas según la tecnología. Las obligaciones son, en lo sustantivo, las mismas para todas las tipologías de generación (sección 7.4); lo que varía es la capacidad de absorción económica de cada una, determinada por la relación entre un costo de cumplimiento de magnitud similar y un capital invertido de magnitud muy distinta.

Esta distinción es relevante para la interpretación de la paradoja: no se trata de que el marco regulatorio discrimine contra las tecnologías de menor intensidad de capital, sino de que un régimen de obligaciones uniforme —diseñado sin diferenciar formalmente por tamaño de inversión— produce, como consecuencia aritmética, una carga relativa desigual entre tecnologías con estructuras de capital estructuralmente distintas. Esta observación conecta directamente con el principio de proporcionalidad analizado en el eje legal del Cap. 6 (sección 6.2), donde se constató que la Ley 21.663 incorpora el principio de proporcionalidad de forma explícita, pero su desarrollo reglamentario específico —que podría traducir este principio en exigencias diferenciadas por escala— se encuentra pendiente al cierre de este estudio.

7.11.2 Segunda paradoja: la normalización por CS-SEN

Como se adelantó en la sección 7.9, existe una segunda dimensión de la paradoja de proporcionalidad, esta vez normalizada por Ciber-Sistema SEN en lugar de por V.I.: Solar FV presenta el mayor costo de cumplimiento por CS-SEN (USD 307.740) de las cuatro tecnologías, mientras que Térmica Gas presenta el menor (USD 144.963) —un ordenamiento inverso al que resulta de comparar el CAC absoluto. Ambas paradojas —por V.I. y por CS-SEN— apuntan en la misma dirección: las tecnologías con arquitecturas de control más simples y menor escala de capital (Grupo A) soportan, bajo el marco regulatorio vigente, un esfuerzo de cumplimiento proporcionalmente mayor que las tecnologías de mayor escala y complejidad de control (Grupo B).

7.12 Análisis de Sensibilidad

La hoja 11_SENSIBILIDAD del modelo Excel evalúa el impacto de tres variables — WACC, tipo de cambio CLP/USD y número de Ciber-Sistemas SEN— sobre el CAC total, con cinco niveles de variación por variable y fórmulas dinámicas que recalculan el resultado completo ante cualquier cambio de parámetro. Este análisis permite evaluar la robustez de los resultados presentados en las secciones 7.9 a 7.11 frente a distintos escenarios de mercado y regulatorios.

7.12.1 Sensibilidad al WACC

La Tabla 25 evalúa el CAC de las cuatro tecnologías de generación ante variaciones del WACC entre 5% y 12%, en torno al valor base de 8%.

Tabla 25. Sensibilidad del CAC al WACC, por tecnología (Fuente: Elaboración Propia)

WACC	FRC (HW, n=5)	CAC Solar FV	CAC Eólica	CAC Térmica Gas	CAC Hidro	Δ% Solar vs. base
5%	0,2310	604.437	636.233	711.173	675.325	-1,79%
7%	0,2439	611.772	643.936	720.230	683.755	-0,60%
8% (base)	0,2505	615.480	647.831	724.816	688.022	0,00%
10%	0,2638	622.973	655.709	734.102	696.656	+1,22%
12%	0,2774	630.566	663.698	743.535	705.420	+2,45%

Duplicando el WACC de 5% a 12%, el CAC de Solar FV varía en un rango total de apenas **4,24 puntos porcentuales** (de -1,79% a +2,45%). Esta baja elasticidad se explica directamente por la estructura CAPEX/OPEX establecida en la sección 7.10:

el WACC afecta únicamente al FRC, y por tanto solo a la fracción CAPEX del CAC (31% del total en Solar FV); el 69% restante, correspondiente al OPEX, es insensible a este parámetro.

7.12.2 Sensibilidad al tipo de cambio (CLP/USD)

La Tabla 26 evalúa el CAC ante variaciones del tipo de cambio entre CLP 800 y CLP 1.100 por dólar, en torno al valor base de CLP 940. El tipo de cambio afecta exclusivamente al salario del Delegado de Ciberseguridad (driver F03), único driver del modelo cotizado originalmente en pesos chilenos; el resto de los drivers, cotizados en dólares, no varía ante este parámetro.

Tabla 26. Sensibilidad del CAC al tipo de cambio CLP/USD, por tecnología (Fuente: Elaboración Propia)

TC (CLP/USD)	Salario Delegado (USD/año)	CAC Solar FV	CAC Eólica	CAC Térmica Gas	CAC Hidro	Δ% Solar vs. base
800 (CLP débil)	50.750	623.038	655.390	732.375	695.580	+1,23%
870	46.667	618.955	651.306	728.291	691.497	+0,56%
940 (base)	43.191	615.480	647.831	724.816	688.022	0,00%
1.000	40.600	612.888	645.240	722.225	685.430	-0,42%
1.100 (CLP fuerte)	36.909	609.198	641.549	718.534	681.739	-1,02%

El rango de variación es aún menor que el del WACC: **2,25 puntos porcentuales** entre los extremos (CLP 800 a CLP 1.100). Un tipo de cambio más depreciado (CLP débil frente al dólar) encarece el salario del Delegado en términos de dólares, incrementando levemente el CAC; un tipo de cambio apreciado lo reduce. El impacto acotado confirma que el modelo, al cotizar la mayoría de sus drivers directamente en USD, es en gran medida inmune a la volatilidad cambiaria local.

7.12.3 Sensibilidad al número de Ciber-Sistema SEN

La Tabla 27 evalúa el CAC de cada tecnología ante variaciones de ± 2 y ± 4 CS-SEN respecto de su valor base, afectando únicamente a los drivers que escalan con este parámetro (firewall/diodo, horas de parcheo, Plan DRP), según lo establecido en la Tabla 18 (sección 7.4).

Tabla 27. Sensibilidad del CAC al N° de Ciber-Sistemas SEN, por tecnología (Fuente: Elaboración Propia)

Tecnología	CS-SEN mín.	CAC (mín.)	CS-SEN base	CAC (base)	CS-SEN máx.	CAC (máx.)	Rango Δ% total
Solar FV	1	585.422	2	615.480	6	738.166	-4,9% a +19,9%
Eólica	1	587.716	3	647.831	7	770.517	-9,3% a +18,9%
Térmica Gas	3	655.815	5	724.816	9	862.818	-9,5% a +19,0%
Hidro	2	619.021	4	688.022	8	826.024	-10,0% a +20,1%

El rango de variación del CS-SEN es sustancialmente mayor que el de WACC o tipo de cambio: entre 19 y 20 puntos porcentuales en el extremo superior para las cuatro tecnologías, con un patrón consistente —duplicar aproximadamente el N° de CS-SEN respecto del valor base incrementa el CAC en torno al 19-20%, mientras que reducirlo a la mitad lo disminuye entre 5% y 10%, según la tecnología.

7.12.4 Síntesis: Jerarquía de sensibilidad del modelo

Comparando el rango total de variación de las tres variables sobre el CAC, el orden de impacto es consistente en las cuatro tecnologías evaluadas: N° de CS-SEN (rango total entre 19 y 24,8 puntos porcentuales, según tecnología) > WACC (≈4,2 puntos porcentuales) > tipo de cambio CLP/USD (≈2,3 puntos porcentuales). Esta jerarquía es consistente con la estructura del modelo establecida en las secciones 7.4 y 7.10: el CS-SEN es la única variable que altera la cantidad de drivers técnicos aplicados —una parte estructural del CAC—, mientras que el WACC y el tipo de cambio solo modifican el valor unitario de fracciones acotadas del CAPEX y el OPEX respectivamente, sin alterar el conjunto de obligaciones a cumplir, con igual efecto proporcional en todas las tecnologías.

En conjunto, el modelo resulta robusto ante variaciones razonables de WACC y tipo de cambio —parámetros macroeconómicos fuera del control del operador—, y más sensible al parámetro que sí depende de decisiones de diseño del operador: la arquitectura de control de la instalación, medida a través del número de Ciber-Sistemas SEN. Esto refuerza la validez de la clasificación por Grupos A, B y C (sección 7.3) como el criterio de diferenciación más relevante del modelo, por sobre la incertidumbre de mercado capturada en la sección 7.13.

7.13 Dispersión de mercado (rangos Min-Max)

Como se estableció en la sección 7.5, el mercado de ciberseguridad OT no dispone de precios de catálogo públicos: cada driver se calibró con un mínimo de tres fuentes, y el modelo reporta tres escenarios —Mínimo, Base (Med) y Máximo— en lugar de un valor puntual único. La Tabla 28 presenta esos tres escenarios de CAC total para las cuatro tecnologías de generación.

Tabla 28. Rangos de CAC por escenario de mercado, por tecnología (Fuente: Elaboración Propia)

Tecnología	CAC Mínimo (USD/año)	CAC Base/Med (USD/año)	CAC Máximo (USD/año)	Factor de dispersión (Máx/Mín)
Solar FV	254.539	615.480	978.853	3,85×
Eólica	271.564	647.831	1.026.530	3,78×
Térmica Gas	308.581	724.816	1.143.482	3,71×
Hidro	290.393	688.022	1.088.081	3,75×

El factor de dispersión entre el escenario Mínimo y el Máximo es notablemente consistente entre tecnologías, oscilando entre **3,71×** y **3,85×**, con un promedio cercano a 3,8×. Esta uniformidad indica que la dispersión de precios de mercado es una característica estructural del sector de ciberseguridad OT en su conjunto, y no un artefacto de la calibración de una tecnología en particular: **el CAC máximo puede llegar a ser prácticamente cuatro veces el CAC mínimo**, para cualquiera de las cuatro tipologías evaluadas.

7.13.1 Este rango no constituye un margen de error metodológico

Es necesario precisar el significado de esta dispersión: no representa incertidumbre o imprecisión del modelo, sino que **refleja fielmente la realidad del mercado** de ciberseguridad OT, donde los proveedores cotizan individualmente y no existen listas de precios públicas uniformes (sección 7.5). Dos operadores con instalaciones técnicamente equivalentes pueden enfrentar un CAC muy distinto según sus decisiones de aprovisionamiento —por ejemplo, contratar un SOC MDR-OT de nivel básico frente a uno con cobertura ampliada, o adquirir una plataforma SIEM de gama media frente a una de gama premium— sin que ello implique una diferencia en el nivel de cumplimiento normativo alcanzado.

7.13.2 Comparación con la dispersión de las demás variables de sensibilidad

El factor de dispersión de mercado (≈3,8×, equivalente a un rango de

aproximadamente 280 puntos porcentuales entre extremos) es sustancialmente mayor que el rango de variación de cualquiera de las tres variables analizadas en la sección 7.12 —N° de CS-SEN (≈ 20 -25 puntos porcentuales), WACC ($\approx 4,2$ puntos porcentuales) y tipo de cambio ($\approx 2,3$ puntos porcentuales). Esto permite establecer una conclusión metodológica relevante: la principal fuente de incertidumbre en la estimación del CAC no proviene de los parámetros macroeconómicos ni de la arquitectura de control de la instalación, sino de la heterogeneidad de precios del mercado de proveedores de ciberseguridad OT, un factor exógeno tanto al operador como al diseño del marco regulatorio.

7.13.3 Implicancia para la interpretación de los resultados del capítulo

Esta dispersión respalda la decisión metodológica, adoptada desde la sección 7.2, de presentar los resultados del modelo como rangos y no como cifras puntuales. El valor Base (Med) utilizado en las secciones 7.9 a 7.11 debe interpretarse como una estimación central razonable, no como una cifra exacta o determinística: el costo real de cumplimiento que enfrentará un operador específico dependerá de sus decisiones de contratación dentro del rango de mercado documentado en la Tabla 19 (sección 7.5).

7.14 Síntesis del modelo y cierre del Objetivo Específico 5

El desarrollo de este capítulo permitió construir, calibrar y aplicar el modelo de Costo Anualizado de Cumplimiento (CAC) como respuesta a la pregunta central de esta investigación: cuánto cuesta cumplir las obligaciones de ciberseguridad que la Ley N.º 21.663 y el Estándar CEN imponen al sector de generación eléctrica. El modelo traduce diecisiete drivers de costo en una métrica anualizada que integra la inversión de capital anualizada, y el gasto operativo recurrente.

El capítulo deja seis hallazgos consolidados, desarrollados con los resultados aplicados a las cuatro tecnologías de generación evaluadas —Solar FV, Eólica, Térmica Gas e Hidro— y a la Subestación como referencia informativa adicional:

Primero, el costo de cumplimiento es una carga económica estructural y permanente, no una inversión puntual: el componente operativo (OPEX) domina sobre el CAPEX en las cuatro tecnologías de generación, con una participación notablemente estable entre 69,0% y 69,7% del CAC total (sección 7.10).

Segundo, la clasificación por arquitectura de control OT —Grupos A, B y C— captura que un mismo conjunto de obligaciones regulatorias genera estructuras de costo materialmente distintas según la tipología de central, mediante dos mecanismos verificables: el escalamiento por número de Ciber-Sistemas SEN y la aplicabilidad diferenciada de cada driver por grupo (sección 7.4).

Tercero, la normalización del costo sobre el Valor de Inversión revela la paradoja de proporcionalidad: el esfuerzo relativo de cumplimiento ($\Delta\text{CAC}/\text{V.I.}$) varía 5,4 veces entre Hidro (0,141%) y Solar FV (0,761%), sin que ello refleje una diferencia en las obligaciones exigidas, sino en la capacidad de absorción económica de cada tecnología según su escala de capital. Una segunda normalización, por Ciber-Sistema SEN, revela un patrón equivalente en sentido inverso (sección 7.11).

Cuarto, el análisis de sensibilidad establece que el modelo es robusto ante variaciones de parámetros macroeconómicos —WACC y tipo de cambio CLP/USD, con rangos de variación de apenas 2 a 4 puntos porcentuales— y más sensible a decisiones de arquitectura del operador, capturadas en el número de Ciber-Sistemas SEN (sección 7.12).

Quinto, la dispersión de precios del mercado de ciberseguridad OT —con un factor de variación de hasta 3,85× entre los escenarios Mínimo y Máximo— constituye la principal fuente de incertidumbre en la estimación del CAC, superando ampliamente el rango de las variables de sensibilidad evaluadas (sección 7.13).

Sexto, la desagregación del CAC por driver individual (sección 7.10.1) muestra que el costo de cumplimiento no se distribuye de forma pareja entre los diecisiete drivers del modelo: el SIEM industrial —su implementación y su licencia anual combinadas— concentra por sí solo entre el 28% y el 33% del CAC total en las cuatro tecnologías, muy por encima de cualquier otro driver individual. Esta concentración tiene una implicancia directa para la discusión de política regulatoria del Capítulo 8: cualquier medida —normativa, de mercado o tecnológica— que logre reducir el costo de este driver específico tendría un impacto proporcionalmente mayor sobre el costo total de cumplimiento que medidas dirigidas a drivers de menor peso individual.

Con ello, el Objetivo Específico 5 queda cumplido: se dispone de una herramienta metodológica replicable, trazable a fuentes regulatorias verificables y transparente en sus supuestos y limitaciones, que cuantifica el esfuerzo económico de cumplimiento de forma comparable entre tipologías de central.

Los resultados desarrollados en este capítulo —normativos (Cap. 5-6), técnicos (Cap. 4) y económicos (Cap. 7)— constituyen la base sobre la cual se desarrolla la discusión integrada del Capítulo 8 y las conclusiones y recomendaciones del Capítulo 9.

8. DISCUSIÓN DE LOS RESULTADOS FINALES

Los capítulos precedentes desarrollaron, de forma independiente, la comparación del marco chileno con estándares internacionales y el diagnóstico de brechas (Capítulo 6), y la estimación del costo de cumplimiento mediante el modelo CAC (Capítulo 7). El presente capítulo no repite esos resultados, sino que los cruza, organizándolos en tres dimensiones de evaluación —técnica, regulatoria y económica— con el propósito de identificar patrones que solo emergen al leer ambos capítulos en conjunto.

Antes de desarrollar esta discusión, es necesario precisar su alcance metodológico. Este estudio se aproxima a la evaluación del marco regulatorio mediante dos ejercicios: uno de comparación documental —benchmarking normativo y técnico frente a estándares internacionales, desarrollado en el Capítulo 6— y otro de cuantificación económica del esfuerzo de cumplimiento, desarrollado en el Capítulo 7. Esta aproximación no constituye una demostración de que los controles exigidos por la Ley N° 21.663 y el Estándar CEN reduzcan efectivamente el riesgo cibernético del sector, ni de que cubran la totalidad de las amenazas relevantes para la infraestructura de generación, ni permite establecer una relación empírica verificada entre las exigencias normativas y sus objetivos regulatorios declarados. Establecer esas relaciones requeriría datos de siniestralidad, series históricas de incidentes o evaluaciones de efectividad de controles que no están disponibles públicamente en Chile a la fecha de este estudio. En consecuencia, la discusión que sigue evalúa coherencia conceptual y consistencia económica del marco regulatorio, no su efectividad ni su suficiencia en sentido estricto.

8.1 Dimensión técnica

El eje técnico del Capítulo 6 estableció que el Estándar CEN es estructuralmente convergente con NERC-CIP —su fuente directa— y parcialmente convergente con IEC 62443, del cual no incorpora el modelo de Niveles de Seguridad ni la extensión de la detección y la recuperación al proceso físico. El Gap Analysis del mismo capítulo tradujo esas divergencias en tres brechas técnicas atribuibles al diseño del propio Estándar CEN, no a la capacidad de implementación del operador: la ausencia de graduación de requisitos por nivel de riesgo, la limitación de la detección al perímetro cibernético, y la ausencia de validación de integridad física antes de reanudar la operación tras un incidente.

El Capítulo 7 permite leer estas brechas desde su expresión económica. El SIEM industrial —la plataforma que en el modelo CAC concentra entre el 28% y el 33% del costo total en las cuatro tecnologías de generación evaluadas— es precisamente la función que el Gap Analysis identificó con mayor divergencia

respecto de IEC 62443: la capacidad de detección. El driver de mayor peso económico del modelo coincide con el dominio técnico donde el Estándar CEN muestra menor convergencia con el referente internacional más exigente en la materia. Esta coincidencia no permite afirmar que el costo esté correctamente calibrado al riesgo —esa relación no fue evaluada empíricamente en este estudio—, pero sí sugiere que el esfuerzo económico del sector se concentra, de facto, en la función de ciberseguridad OT que el marco técnico chileno cubre de forma más parcial.

La diferenciación de costos por Grupo A, B y C (Cap. 4, Cap. 7) es igualmente consistente con la caracterización técnica de cada arquitectura de control: los drivers que escalan con el número de Ciber-Sistemas SEN —parcheo, perímetro electrónico, recuperación— son más numerosos en el Grupo B (proceso continuo, DCS propietario), reflejando económicamente la mayor complejidad de control ya documentada en la caracterización técnica del parque generador.

8.2 Dimensión regulatoria

El eje legal del Capítulo 6 mostró que la Ley N.º 21.663 es conceptualmente convergente con NIS2 y la RN 964 en gestión de riesgos, gobernanza y reporte de incidentes, con una divergencia relevante en el mecanismo de designación de entidades obligadas: mientras NIS2 y la RN 964 aplican criterios objetivos de designación directa, la Ley 21.663 opera mediante calificación administrativa de la ANCI, sin criterios sectoriales de escala publicados a la fecha de este estudio. El Gap Analysis del mismo capítulo identificó cuatro vacíos normativos —el reglamento del Art. 28º no publicado, la ausencia de un mecanismo de excepción técnica, los criterios sectoriales de calificación OIV no definidos, y la Norma Técnica de la CNE no publicada—, los cuatro de responsabilidad exclusiva de la autoridad regulatoria, no del operador.

El modelo CAC permite dimensionar el efecto económico de uno de estos vacíos: el driver de auditorías externas del Art. 28º —de naturaleza administrativa según la taxonomía OCDE aplicada en el Cap. 7— representa un componente comparativamente menor del CAC total (en torno al 2%), lo que indica que el vacío normativo de mayor criticidad identificado en el Gap Analysis no es, en sí mismo, económicamente significativo en magnitud absoluta. Su relevancia no es de costo, sino de certeza: mientras el reglamento no se publique, ningún operador puede planificar con precisión el criterio bajo el cual será auditado, una incertidumbre que el modelo económico —construido sobre supuestos explícitos y verificables— no puede capturar por definición, y que constituye en sí misma una limitación de lo que un modelo de costos puede representar, no del marco regulatorio.

Los solapamientos regulatorios identificados en el Cap. 6 —el reporte dual de incidentes ante la ANCI y el Coordinador Eléctrico Nacional, y la eventual coexistencia de dos SGSI ante la Ley y la NT CNE proyectada— no generan drivers de costo adicionales en el modelo, dado que sus componentes técnicos ya están absorbidos en drivers existentes (SOC, Delegado de Ciberseguridad). Esto sugiere que la ineficiencia de estos solapamientos es, ante todo, administrativa y de coordinación institucional, y no una carga económica directa medible en el CAC.

8.3 Dimensión económica

Los seis hallazgos del modelo CAC (Cap. 7.14) —dominancia del OPEX, diferenciación por grupo tecnológico, la paradoja de proporcionalidad, la baja sensibilidad a variables macroeconómicas, la alta dispersión de mercado, y la concentración del costo en el SIEM industrial— constituyen, en conjunto, la evidencia cuantitativa central de este estudio. De ellos, la paradoja de proporcionalidad —el hecho de que Solar FV soporte un esfuerzo relativo ($\Delta\text{CAC}/\text{V.I.} = 0,761\%$) 5,4 veces mayor que Hidro (0,141%), pese a tener un CAC absoluto menor— es el hallazgo con mayor conexión directa a la dimensión regulatoria: la Ley 21.663 no distingue formalmente el nivel de exigencia según la escala de capital del operador, a diferencia de NIS2, que sí diferencia obligaciones entre entidades esenciales e importantes según criterios de tamaño (Cap. 6.2).

La paradoja de proporcionalidad económica documentada en el Cap. 7 es, en este sentido, la contraparte cuantitativa de la divergencia regulatoria identificada en el eje legal del Cap. 6: un régimen de designación sin diferenciación explícita por escala produce, como consecuencia aritmética y no como diseño deliberado, una carga relativa desigual entre tecnologías.

8.4 Síntesis de la discusión

La Tabla 29 sintetiza los tres cruces desarrollados en esta discusión, conectando el hallazgo cualitativo de origen (Cap. 6) con su expresión cuantitativa (Cap. 7).

Tabla 29. Síntesis de la discusión por dimensión de evaluación (Fuente: Elaboración Propia)

Dimensión	Hallazgo cualitativo (Cap. 6)	Hallazgo cuantitativo (Cap. 7)	Cruce / implicancia
Técnica	Estándar CEN parcialmente convergente con IEC 62443; brecha mayor en detección (sin extensión al proceso físico)	El SIEM industrial concentra 28%-33% del CAC, el driver individual más costoso en las cuatro tecnologías	El mayor gasto del modelo se concentra en la función técnica con mayor brecha respecto al referente internacional

Dimensión	Hallazgo cualitativo (Cap. 6)	Hallazgo cuantitativo (Cap. 7)	Cruce / implicancia
Regulatoria	Cuatro vacíos normativos identificados, todos de responsabilidad de la autoridad (Reglamento Art. 28°, TFE, criterios OIV, NT CNE)	Las auditorías del Art. 28° representan solo ≈2% del CAC total	El vacío normativo de mayor criticidad no es económicamente grande; su costo es de incertidumbre de planificación, no de magnitud
Económica	Divergencia en el mecanismo de designación: sin diferenciación formal por escala de capital (a diferencia de NIS2)	Paradoja de proporcionalidad: el Δ CAC/V.I. de Solar FV es 5,4 veces el de Hidro	La ausencia de diferenciación regulatoria por escala se expresa económicamente como carga desigual entre tecnologías

En conjunto, esta discusión no permite concluir que el marco regulatorio chileno sea suficiente o insuficiente en un sentido normativo estricto, pregunta que excede el alcance metodológico de este estudio. Permite, en cambio, establecer que el marco es conceptualmente coherente con sus referentes internacionales (Cap. 6) y que ese diseño se traduce en un esfuerzo económico cuantificable, estructural y desigualmente distribuido entre tecnologías (Cap. 7), con brechas técnicas y vacíos normativos que —aunque no invalidan el diseño regulatorio— condicionan su implementación efectiva y su certeza de planificación para los operadores. Estas conclusiones se desarrollan de forma sistemática en el Capítulo 9.

9. CONCLUSIONES Y RECOMENDACIONES

Este capítulo cierra la investigación en tres partes: las conclusiones específicas alcanzadas para cada uno de los cinco objetivos del estudio (9.1), una conclusión general que integra el conjunto (9.2), y las recomendaciones dirigidas a los actores relevantes del ecosistema regulatorio del sector eléctrico chileno (9.3).

9.1 Conclusiones por objetivo específico

9.1.1 Marco normativo y de gobernanza (OE1)

La Ley N.° 21.663 y el Estándar CEN configuran una arquitectura regulatoria complementaria, no redundante: la ley establece la gobernanza nacional y los deberes generales de ciberseguridad; el Estándar CEN, habilitado por su Art. 26°, los traduce en controles técnicos específicos para el entorno OT del sector eléctrico. El cumplimiento efectivo requiere satisfacer ambos instrumentos de forma simultánea, resuelto en este estudio en diecisiete drivers de costo trazables (Cap. 7), no en una suma aditiva de obligaciones independientes. El marco conserva, no obstante, una naturaleza parcialmente incompleta: instrumentos técnicos complementarios —el reglamento de auditoría del Art. 28° y la Norma Técnica de la CNE— permanecían sin publicar al cierre de este estudio, lo que introduce incertidumbre en la planificación del cumplimiento (Cap. 5, Cap. 6).

9.1.2 Integración de la ciberseguridad en la gestión de activos (OE2)

La aplicación conjunta de la Ley y el Estándar CEN se integra operativamente en los planes de mantenimiento y en los indicadores de gestión de activos ya utilizados por el sector (RPTD N.° 17), sin requerir sistemas paralelos de gestión. Los controles técnicos del Estándar CEN —gestión de parches, hardening, monitoreo, planes de respuesta y recuperación— se incorporan a los procesos regulares de operación, mientras que la Ley aporta el marco de gobernanza y trazabilidad. Este resultado es consistente con la convergencia normativa documentada en el Cap. 5.

9.1.3 Comparación con estándares internacionales (OE3)

El marco chileno —Ley 21.663 y Estándar CEN— es conceptualmente coherente con sus referentes internacionales: convergente con NIS2 y la RN 964 en el eje legal, y estructuralmente convergente con NERC-CIP —su fuente técnica directa— en el eje técnico, con convergencia parcial respecto de IEC 62443. Las divergencias identificadas no se concentran en los principios ni en los dominios cubiertos, sino en el mecanismo de designación de entidades obligadas (eje legal) y en el alcance de la detección y la recuperación (eje técnico). Esta coherencia es de naturaleza

conceptual y documental —establecida mediante comparación normativa (Cap. 6)—, no una validación empírica de que el marco chileno logre los mismos resultados de protección que sus referentes internacionales.

9.1.4 Diagnóstico de brechas (OE4)

El Gap Analysis identificó doce hallazgos: cuatro vacíos normativos, tres brechas técnicas propias del Estándar CEN, dos brechas institucionales y tres solapamientos regulatorios (Cap. 6.5). Los vacíos y solapamientos son responsabilidad de la autoridad regulatoria y no imponen, en su mayoría, un costo directo cuantificable al operador; las brechas técnicas e institucionales sí tienen expresión económica directa en el modelo CAC. Estas brechas no invalidan la coherencia normativa establecida en el OE3, pero condicionan la velocidad, la certeza y el costo de la implementación efectiva del marco en el parque generador chileno.

9.1.5 Modelo CAC (OE5)

El modelo CAC cuantifica, para las tipologías evaluadas, un costo de cumplimiento cuyo escenario base va de USD 615.480/año (Solar FV) a USD 724.816/año (Térmica Gas) para una central de 100 MW —no un valor puntual, sino una estimación central dentro de un rango que, por la dispersión de precios del mercado de ciberseguridad OT, puede llegar a representar hasta 3,85 veces entre los escenarios Mínimo y Máximo (Cap. 7.13)—, dominado en un 69%-70% por el componente operativo (OPEX) y concentrado en un 28%-33% en un único driver: el SIEM industrial. El esfuerzo relativo al Valor de Inversión ($\Delta\text{CAC}/\text{V.I.}$) varía 5,4 veces entre Hidro (0,141%) y Solar FV (0,761%) —la paradoja de proporcionalidad—, hallazgo que no refleja diferencias en las obligaciones exigidas sino en la capacidad de absorción económica de cada tecnología. El modelo es robusto ante variaciones de WACC y tipo de cambio, y más sensible a la arquitectura de control del operador (N.º de Ciber-Sistemas SEN) y, sobre todo, a la dispersión de precios del mercado de ciberseguridad OT, que puede representar hasta 3,85 veces entre el escenario mínimo y el máximo. El modelo constituye una herramienta metodológica replicable y trazable a fuentes regulatorias verificables.

9.2 Conclusión General

La Ley N.º 21.663 y el Estándar de Ciberseguridad del CEN representan un hito regulatorio en el sector eléctrico chileno: la protección de los sistemas de control industrial deja de ser una práctica voluntaria para convertirse en un régimen de obligaciones legales y técnicas articuladas, con consecuencias económicas verificables sobre los operadores de generación. Esta investigación aporta dos

resultados centrales y complementarios. El primero es de naturaleza cualitativa: el marco regulatorio chileno es conceptualmente coherente con los estándares internacionales de referencia, tanto en su diseño legal como en su instrumento técnico sectorial, aunque con brechas y vacíos identificables que condicionan su implementación (Cap. 6). El segundo es de naturaleza cuantitativa: el cumplimiento simultáneo de ambos instrumentos impone un costo anualizado significativo y estructuralmente permanente, cuya magnitud y distribución relativa varían de forma sistemática entre tecnologías de generación (Cap. 7).

Es necesario precisar, como se hizo en el Capítulo 8, el alcance de estas conclusiones. **Este estudio no evalúa —ni pretende evaluar— la suficiencia regulatoria del marco chileno en un sentido estricto: hacerlo exigiría demostrar que los controles exigidos reducen efectivamente el riesgo cibernético del sector, que cubren las amenazas relevantes para la infraestructura de generación, y que existe una relación verificada entre las exigencias normativas y sus objetivos declarados —evidencia que requeriría datos de siniestralidad e indicadores de efectividad de controles no disponibles públicamente en Chile.** Lo que este estudio aporta es una aproximación a esa pregunta mediante dos vías indirectas y complementarias: la comparación documental con marcos internacionales y la cuantificación económica del esfuerzo de cumplimiento.

El modelo CAC desarrollado en esta investigación proporciona, en ese sentido, una herramienta metodológica replicable para traducir obligaciones normativas en costos económicos comparables, en el lenguaje de gestión de activos que el sector eléctrico chileno ya utiliza. Su principal aporte es hacer visible —de forma trazable, verificable y diferenciada por tecnología— cuánto cuesta cumplir el marco normativo de ciberseguridad.

9.3 Recomendaciones

Los hallazgos del presente estudio permiten formular nueve recomendaciones concretas, sistematizadas en la Tabla 30, dirigidas a las autoridades regulatorias con competencia sobre el marco normativo —ANCI, CEN y CNE—, a los operadores de generación eléctrica como sujetos obligados directos, y a la comunidad académica como continuadora del desarrollo metodológico iniciado en este trabajo. Cada recomendación se deriva directamente de los hallazgos de los capítulos precedentes, indicados en la columna de origen.

Tabla 30. Recomendaciones del estudio, por destinatario (Fuente: Elaboración Propia)

Destinatario	N°	Recomendación	Justificación	Origen
ANCI	R1	Establecer mecanismos formales de coordinación con el CEN para unificar el reporte de incidentes.	El reporte dual ante el CSIRT Nacional (DS 295) y el Coordinador (CIP-008) duplica la carga administrativa. Se recomienda un protocolo único de notificación y criterios de reconocimiento mutuo.	Cap. 6.5
	R2	Publicar el Reglamento de Auditoría y Certificación del Art. 28°.	Vacío normativo de mayor criticidad del Gap Analysis: sin él, ningún operador puede certificar formalmente su cumplimiento. Su costo directo es acotado en el CAC, pero su publicación es condición para la certeza de planificación.	Cap. 6.5 / 8.2
CEN	R3	Desarrollar un mecanismo de Excepción de Factibilidad Técnica (TFE), equivalente al de NERC-CIP.	Su ausencia expone a los operadores del Grupo B (DCS propietario) a incumplimiento formal cuando restricciones operacionales impiden cumplir los plazos prescriptivos del Estándar CEN.	Cap. 6.3
CNE	R4	Publicar la Norma Técnica de Ciberseguridad, consolidando el tercer nivel del marco.	Mientras este tercer nivel normativo no se publique, el marco permanece estructuralmente incompleto. Su coherencia con la Ley y el Estándar CEN debe asegurarse vía el mecanismo de prevalencia del Art. 26°.	Cap. 5.6
Operadores	R5	Planificar el cumplimiento como costo operacional permanente, no como inversión puntual.	El OPEX representa 69%-70% del CAC en todas las tipologías. El enfoque de gestión debe ser el de un gasto recurrente presupuestado anualmente, no un proyecto con fecha de término.	Cap. 7.10
	R6	Gestionar activamente la incertidumbre regulatoria sin paralizar la implementación.	La falta del reglamento del Art. 28° no suspende las obligaciones vigentes. Se recomienda implementar controles exigibles desde ya y documentar su trazabilidad normativa progresivamente.	Cap. 6.5
	R7	Aprovechar la convergencia del Art. 26° para evitar sistemas de gestión duplicados.	Un mismo control técnico puede satisfacer simultáneamente la Ley y el Estándar CEN.	Cap. 5
Investigación futura	R8	Extender el modelo CAC al segmento de transmisión.	El estudio acotó su alcance a generación por razones metodológicas. La transmisión concentra activos críticos de alto impacto sistémico y es la extensión natural más relevante del modelo.	Cap. 7
	R9	Incorporar el costo esperado de incidentes para avanzar hacia una evaluación de suficiencia regulatoria.	Este estudio no evalúa si el marco es suficiente frente al riesgo, por falta de datos de siniestralidad públicos en Chile. Estimar el costo esperado de incidentes permitiría, a futuro, comparar costo de cumplir vs. costo evitado.	Cap. 8 / 9.2

10. ANEXOS

10.1 ANEXO A: Metodología

La presente investigación se desarrollará bajo un **enfoque aplicado**, de carácter cualitativo–analítico, orientado al análisis regulatorio, técnico y económico del impacto de la Ley Marco de Ciberseguridad (Ley 21.663) en el sector de generación eléctrica chileno.

10.1.1 Enfoque metodológico general

La investigación adopta como **marco integrador el enfoque de Gestión de Activos Físicos**, el cual permite vincular los requerimientos de ciberseguridad con la **disponibilidad, confiabilidad y resiliencia de la infraestructura crítica física**, en particular de los Ciber-Sistemas SEN (o Infraestructura Crítica de la Información – ICI) del sector de generación eléctrica. En este contexto, la Gestión de Activos — en línea con los principios de la norma ISO 55001— se utiliza como **marco conceptual de referencia**, y no como un estándar objeto de evaluación.

Desde el punto de vista técnico-sectorial, el análisis se estructura en torno al **Estándar de Ciberseguridad para el Sector Eléctrico del Coordinador Eléctrico Nacional**, el cual adopta como base el estándar internacional **NERC-CIP**. En consecuencia, NERC-CIP se utiliza como **referente técnico principal** para el análisis sectorial, mientras que otros marcos (NIST CSF, IEC 62443) se emplean únicamente como **apoyo conceptual**, sin constituir ejes centrales del estudio.

10.1.2 Estructura general del estudio

El estudio se estructura en una serie de **etapas metodológicas claramente definidas**, cada una de las cuales aborda un aspecto específico del problema de investigación. Estas etapas se articulan de manera secuencial y permiten construir progresivamente los resultados del estudio, desde el análisis normativo y técnico-conceptual, hasta la evaluación económica y la formulación de conclusiones y recomendaciones.

Para efectos de su desarrollo y presentación, la metodología se organiza en **cinco etapas de desarrollo**, los cuales integran de manera acumulativa los resultados parciales en el informe final de tesis.

10.1.3 Etapas de desarrollo y entregables

Etapas I – Febrero-Marzo: Ajustes del Estado del Arte

Contenido Abordado:

En esta etapa se realizará la revisión bibliográfica y el ajuste exhaustivo del Estado del Arte, contextualizando la evolución de la ciberseguridad en Chile y los enfoques internacionales.

Entregable:

- Informe parcial 1 y presentación.

Contribución al trabajo final:

Esta etapa define el sustento teórico del estudio, establecerá los límites del análisis y proporcionará el marco conceptual inicial.

Etapla II – Marzo-Abril: Marco Normativo y Gestión de Activos**Contenido Abordado:**

En esta etapa se abordará el marco normativo vigente de la Ley Marco de Ciberseguridad (Ley 21.663) y sus reglamentos asociados (DS 285 y DS 295), junto con un análisis documental orientado a comprender la infraestructura crítica física asociada a la generación eléctrica en Chile.

Se integrará explícitamente un enfoque de gestión de activos, considerando la caracterización de dichos activos en función de su criticidad, función operativa y dependencia tecnológica como base para interpretar los requerimientos regulatorios de ciberseguridad.

Objetivo:

Caracterizar el marco normativo y los Ciber Sistemas del sector de generación eléctrica, estableciendo la base técnica y conceptual necesaria para el análisis posterior de la coherencia técnica y económica del cumplimiento de la Ley 21.663.

En esta etapa se pretende avanzar principalmente en el cumplimiento de los Objetivos Específicos OE1 y OE2.

Fuentes de información:

- Ley Marco de Ciberseguridad (Ley No 21.663)
- Decreto Supremo N.º 285 y Decreto Supremo N.º 295.

- Documentos oficiales de la Agencia Nacional de Ciberseguridad y de la Biblioteca del Congreso Nacional.
- Documentación técnica pública del Coordinador Eléctrico Nacional (normativa técnica, bases operativas)
- Bibliografía académica especializada en sistemas OT y SCADA en energía.
- Principios y literatura de referencia en gestión de activos físicos (ISO 55001 como marco conceptual, no como estándar a evaluar).

Tipo de Estudio:

Análisis documental y normativo de carácter cualitativo, complementado con una caracterización técnico-conceptual basada en principios de gestión de activos.

Entregable:

- **Informe parcial 2 y presentación.**
- Secciones consolidadas del informe final: introducción, pregunta de investigación, objetivos, marco normativo, marco técnico-conceptual y definición de Ciber Sistema SEN según el Estándar del CEN.

Contribución al trabajo final:

Esta etapa define el **alcance efectivo del estudio**, establece los límites normativos y técnicos del análisis y proporciona el marco conceptual sobre el cual se construyen las etapas posteriores.

Etapas III – Abril-Mayo: Coherencia técnica de la Ley y Modelo CAC preliminar

Contenido abordado

En esta etapa se evaluará la **coherencia técnica** entre los requerimientos relevantes de la Ley 21.663 y el estándar **NERC-CIP**, considerado como el **estándar sectorial de referencia principal** para la protección de infraestructuras eléctricas.

El análisis se realizará desde una perspectiva legal y técnica, evaluando cómo los controles y principios de equivalente contribuyen a proteger la disponibilidad, integridad y continuidad operacional de dichos activos. Los estándares NERC-CIP, NIST CSF, IEC 62443 e ISO/IEC 27019 se utilizarán para ser comparados con el marco normativo chileno.

Objetivo de la etapa

Evaluar la coherencia técnica del marco regulatorio chileno en relación con el estándar NERC-CIP, considerando su contribución a la protección de los Ciber Sistemas SEN del sistema de generación.

En esta etapa se pretende avanzar principalmente en el cumplimiento del Objetivo Específico OE3. También se pretende avanzar en el modelo CAC.

Fuentes de información

- Estándares NERC-CIP.
- Documentación técnica sectorial de NERC y del U.S. Department of Energy.
- NIST Cybersecurity Framework e IEC 62443 como referencias conceptuales complementarias.

Tipo de estudio

Análisis técnico-regulatorio comparativo de carácter cualitativo, focalizado en coherencia técnica y protección de activos críticos.

- **Entregable**
- **Informe parcial 3 y presentación.**
- Capítulo del informe final: análisis de coherencia técnica entre la Ley 21.663 y el estándar NERC-CIP.

Contribución al trabajo final

Esta etapa justifica técnicamente la relevancia del cumplimiento regulatorio y establece el vínculo entre ciberseguridad y resiliencia de activos, preparando el terreno para el análisis económico.

Etapas IV – Mayo-Junio: Gap Análisis y Desarrollo de la metodología económica de cumplimiento

Contenido abordado

En esta etapa se realizará el Gap Análisis derivado de los hallazgos detectados en el avance anterior y resumiéndolos en el OE4, además se completará el diseño de la **metodología de estimación del Costo Anualizado de Cumplimiento (CAC)**

asociado al cumplimiento de los requerimientos de ciberseguridad establecidos por la Ley 21.663.

Objetivo de la etapa

Diseñar una metodología económica aplicada que permita estimar el costo del cumplimiento regulatorio en ciberseguridad desde la perspectiva de la protección y gestión de activos.

En esta etapa se pretende avanzar principalmente en el cumplimiento del Objetivo Específico OE4 y completar el cumplimiento del OE5.

Fuentes de información

- Literatura de economía de la regulación y análisis costo-cumplimiento.
- Estudios de organismos internacionales (IEA, ENISA, DOE).
- Literatura técnica sobre costos de ciberseguridad OT y resiliencia operacional.

Tipo de estudio

Diseño metodológico económico aplicado, con enfoque en eficiencia regulatoria y gestión de activos.

Entregable

- **Informe parcial 4 y presentación.**
- Sección casi definitiva del informe final: metodología económica de cumplimiento y discusión preliminar de impacto económico.

Contribución al trabajo final

Esta etapa constituye el **aporte central del estudio al Magíster en Economía Energética**, traduciendo el marco regulatorio-técnico en implicancias económicas concretas.

Etapas V – Junio-Julio: Ajustes, calibraciones y generación de Paper

Contenido abordado

En la etapa final se evaluará la **aplicabilidad de la metodología propuesta**

mediante análisis de escenarios y una validación acotada. A partir de ello, se desarrollarán las conclusiones y recomendaciones finales del estudio, manteniendo el alcance original y evitando evaluaciones empíricas no previstas.

Objetivo de la etapa

Verificar la coherencia interna y aplicabilidad práctica de la metodología propuesta, y consolidar las conclusiones del estudio desde una perspectiva económica y de gestión de activos.

En esta etapa se pretende avanzar principalmente en el cumplimiento del Objetivo Específico OE5.

Fuentes de información

- Retroalimentación experta limitada (especialistas en regulación, ciberseguridad OT y gestión de activos).
- Síntesis de resultados obtenidos en las etapas anteriores.

Tipo de estudio

Síntesis analítica con validación cualitativa no empírica.

Entregable

- **Informe final de tesis, paper de tesina y presentación final.**

Contribución al trabajo final

Esta etapa cierra el ciclo metodológico, asegurando la coherencia del estudio y reforzando su utilidad como herramienta de análisis económico-regulatorio para la gestión de activos en el sector de generación.

10.2 ANEXO B: Carta Gantt

La Carta Gantt presentada (Tabla 31) ha sido diseñada para reflejar el desarrollo metodológico de la tesina, considerando el período acotado de trabajo y los hitos formales de entrega definidos por el programa. La planificación se estructura en unidades semanales, representadas mediante bloques de trabajo por mes, lo que permite visualizar la secuencia y superposición de actividades propias del estudio

Tabla 31. Carta Gantt (Fuente: Elaboración Propia)

Fase / Actividad Principal	Descripción resumida de la tarea	Marzo				Abril				Mayo					Junio				Julio				Resultado esperado
		S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S5	S1	S2	S3	S4	S1	S2	S3	S4	
Informe Parcial 1	Entrega diseño metodológico, objetivos, alcance, Estado del Arte y Gantt		▲																				Informe Parcial 1 entregado (12-03-2026)
Fase I – Marco Conceptual Técnico y Operacional																							
I.1 Revisión Ley 21.663 y DS 285/295	Análisis normativo y fichas regulatorias			■	■																		Fichas normativas consolidadas
I.2 Identificación de infraestructura crítica y Ciber Sistemas	Clasificación de activos por función y criticidad				■	■	■																Taxonomía de los Ciber Sistemas
I.3 Gestión de activos y dependencias OT	Dependencias OT y marco técnico-conceptual					■																	Marco conceptual Ciber Sistemas-OT
Informe Parcial 2	Redacción y entrega resultados Etapa I						▲																Informe Parcial 2 (09-04-2026)
Etapa II - Coherencia Técnica y Preparación del Análisis Económico																							
II.1 Revisión NERC-CIP	Identificación de controles sectoriales relevantes							■	■														Síntesis técnica NERC-CIP
II.2 Coherencia Ley 21.663 – NERC-CIP	Análisis técnico enfocado Ciber Sistemas							■	■														Matriz de coherencia técnica
II.3 Identificación preliminar de componentes de costo	Relación controles técnicos ↔ impactos económicos							■	■														Listado preliminar de drivers de costo
Informe Parcial 3	Redacción y entrega Etapa II										▲												Informe Parcial 3 (07-05-2026)
Etapa III - Metodología Económica de Cumplimiento (CAC)																							
III.1 Definición conceptual del CAC	Enfoque económico y gestión de activos											■	■										Marco Conceptual CAC
III.2 Estructuración CAPEX / OPEX	Identificación de costos por activo y ciclo de vida												■	■									Estructura económica del CAC
III.3 Supuestos y criterios de proporcionalidad	Alcances, límites y replicabilidad														■								Supuestos económicos definidos
Informe Parcial 4	Redacción y entrega Etapa III														▲								Informe Parcial 4 (04-06-2026)
Etapa IV - Aplicabilidad, Cierre y Defensa																							
IV.1 Aplicabilidad y escenarios	Análisis conceptual de uso del CAC															■							Escenarios evaluados
IV.2 Validación acotada	Revisión coherencia técnica-económica															■	■						Ajustes iniciales
IV.3 Redacción final y paper	Conclusiones, recomendaciones y paper																■	■					Informe final
Informe Parcial 5 + Paper	Entrega final de tesina																		▲				Informe + Paper (02-07-2026)
Ajustes Finales	Ajustes Finales																		■	■			Ajustes finales
Defensa de Tesina	Examen de grado																					◆	Defensa (31-07 a 02-08)

11. REFERENCIAS

- [1] Z. Peterson, «Cyberattacks on Power Systems: Lessons from Ukraine and Beyond», IEEE Security & Privacy, vol. 21, no. 3,» 2023.
- [2] US Department Of Energy, «Colonial Pipeline Cyber Incident,» 7 May 2021. [En línea]. Available: <https://www.energy.gov/ceser/colonial-pipeline-cyber-incident>.
- [3] Fortinet, «2025 Global Trend Landscape Report,» 2026. [En línea]. Available: <https://www.fortinet.com/resources/reports/threat-landscape-report>.
- [4] CheckPoint, «Latin America 2025 Mid-Year Cyber Snapshot Reveals 39% Surge in Attacks as AI Threats Escalate Regional Risk,» 10 Jul 2025. [En línea]. Available: <https://blog.checkpoint.com/research/latin-america-2025-mid-year-cyber-snapshot-reveals-39-surge-in-attacks-as-ai-threats-escalate-regional-risk/>.
- [5] CEN, «Estándar de Ciberseguridad para el Sector Eléctrico,» 2022. [En línea]. Available: <https://www.coordinador.cl/wp-content/uploads/2024/08/Estandar-Ciberseguridad-SEN-October-2022.pdf>.
- [6] BCN Chile, «Ley No 21.663: Ley Marco de Ciberseguridad,» 2025.
- [7] ENISA, «NIS Investments 2024,» [En línea]. Available: https://www.enisa.europa.eu/sites/default/files/2024-11/CSPA%20-%20NIS%20Investments%20-%202024_0.pdf.
- [8] BCN, «Crea Comité Interministerial sobre Ciberseguridad,» 17 Jul 2015. [En línea]. Available: <https://www.bcn.cl/leychile/navegar?idNorma=1079608>.
- [9] BCN, «Ley 21113, Declara Octubre mes nacional de la ciberseguridad,» Oct 2018. [En línea]. Available: <https://www.bcn.cl/leychile/navegar?i=1123489>.
- [10] CNE, «Estado de Procedimientos Normativos del Plan Normativo Anual,» [En línea]. Available: <https://www.cne.cl/wp-content/uploads/2026/03/Estado-normas-tecnicas-2026.03.06.pdf>.
- [11] CEN, «Sistema Eléctrico Nacional,» 2025. [En línea]. Available:

<https://www.coordinador.cl/sistema-electrico/>.

- [12] Electrominería, «Sistema eléctrico parte 2025 con más de 1.000 generadoras en operación y más de 1.000 empresas coordinadas,» 2025. [En línea]. Available: <https://electromineria.cl/sistema-electrico-parte-2025-con-mas-de-1-000-generadoras-en-operacion-y-mas-de-1-000-empresas-coordinadas/>.
- [13] CEN, «CEN - Reporte Cuenta Pública,» 2025. [En línea]. Available: <https://www.coordinador.cl/wp-content/uploads/2025/06/20250602-UCRI-Reporte-Cuenta-Publica-2024.pdf>.
- [14] C. -. Infotécnica, «InfoTecnica (Subestaciones),» 2026. [En línea]. Available: <https://infotecnica.coordinador.cl/instalaciones/subestaciones>.
- [15] CEN, «Coordinador publica Propuesta de Expansión del Sistema de Transmisión 2025 con inversiones por US\$ 708 millones,» 2025. [En línea]. Available: <https://www.coordinador.cl/novedades/coordinador-publica-propuesta-de-expansion-del-sistema-de-transmision-2025-con-inversiones-por-us-708-millones/>.
- [16] E. E. A.G., «Memoria Anual 2024,» 2025. [En línea]. Available: <https://www.electricas.cl/wp-content/uploads/2025/06/Memoria-EEAG-2024.pdf>.
- [17] IBM, «What is Critical Infrastructure,» [En línea]. Available: <https://www.ibm.com/think/topics/critical-infrastructure>.
- [18] America's Cyber Defense Agency, «Critical Infrastructure Systems,» [En línea]. Available: <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/resilience-services/infrastructure-dependency-primer/learn/critical-infrastructure-systems>.
- [19] ANCI, «Resolución 87 EXENTA - APRUEBA NÓMINA DE OPERADORES DE IMPORTANCIA VITAL CORRESPONDIENTE AL PRIMER PROCESO DE CALIFICACIÓN,» 2025. [En línea]. Available: <https://www.bcn.cl/leychile/navegar?idNorma=1219600>.
- [20] CEN, «Coordinador Eléctrico Nacional entrega a la SEC informe sobre el apagón del 25 de febrero,» Marzo 2025. [En línea]. Available: <https://www.coordinador.cl/novedades/coordinador-electrico-nacional->

entrega-a-la-sec-informe-sobre-el-apagon-del-25-de-febrero/.

- [21] A. C. D. Agency, «CISA collaborates with the OT community to address immediate operational cyber events and long-term risk affecting ICS.,» [En línea]. Available: <https://www.cisa.gov/topics/industrial-control-systems>.
- [22] E-ISAC, «Analysis of the Cyber Attack on the Ukrainian Power Grid,» Marzo 2016. [En línea]. Available: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC_SANS_Ukraine_DUC_5.pdf.
- [23] WeLiveSecurity, «Industroyer: Biggest threat to industrial control systems since Stuxnet,» Jun 2017. [En línea]. Available: <https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/>.
- [24] CiperChile, «Hackeo masivo al Estado Mayor Conjunto expuso miles de documentos de áreas sensibles de la defensa,» Sep 2022. [En línea]. Available: <https://www.ciperchile.cl/2022/09/22/hackeo-masivo-al-estado-mayor-conjunto-expuso-miles-de-documentos-de-areas-sensibles-de-la-defensa/>.
- [25] N. 4. Cyber, «CSIRT Nacional alerta sobre incidente de efecto significativo en entidad estratégica e identifica a ransomware Qilin como autor,» Ene 2026. [En línea]. Available: <https://blog.nivel4.com/anci/csirt-nacional-alerta-sobre-incidente-de-efecto-significativo-en-entidad-estrategica-e-identifica-a-ransomware-qilin-como-autor>.
- [26] CNE, «NTSyCS (Norma Técnica de Seguridad y Calidad de Servicio),» 2025. [En línea]. Available: <https://www.cne.cl/wp-content/uploads/2025/01/NTSyCS-Ene-2025.pdf>.
- [27] C. (. I. s. Ciberseguridad), «Política Nacional de Ciberseguridad,» 2017. [En línea]. Available: https://anci.gob.cl/documents/1/Pol%C3%ADtica_Nacional_de_Ciberseguridad.pdf.
- [28] CEN, «Coordinador presentó Estándar Ciberseguridad para SEN,» 2020. [En línea]. Available: <https://www.coordinador.cl/novedades/coordinador-presento-estandar-de-ciberseguridad-para-el-sector-electrico-de-chile/>.

- [29] Electrominería, «Ciberseguridad del sector eléctrico: CNE prepara consulta pública para Norma Técnica en esta materia,» Oct 2024. [En línea]. Available: <https://electromineria.cl/ciberseguridad-del-sector-electrico-cne-prepara-consulta-publica-para-norma-tecnica-en-esta-materia/>.
- [30] I. Ciberseguridad, «Chile presenta Norma de Seguridad de la Información y Ciberseguridad para el Sector Eléctrico,» Oct 2023. [En línea]. Available: <https://www.linkedin.com/pulse/chile-presenta-norma-de-seguridad-la-informaci%C3%B3n-j5wkf>.
- [31] SEC, «Pliego Tecnico Normativo RPTD N° 17,» [En línea]. Available: <https://rimaconsultores.cl/assets/files/Pliego-T%C3%A9cnico-RPDT-N%C2%B0-17.pdf>.
- [32] NIST, «Guide to Operational Technology (OT) Security,» Sep 2023. [En línea]. Available: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf>.
- [33] OECD, «OECD Regulatory Compliance Cost Assessment Guidance,» 2014. [En línea]. Available: https://www.oecd.org/content/dam/oecd/en/publications/reports/2014/04/oecd-regulatory-compliance-cost-assessment-guidance_g1g400de/9789264209657-en.pdf.
- [34] N. L. O. T. Rockies, «Annual Technology Baseline,» 2024. [En línea]. Available: https://atb.nrel.gov/electricity/2024/equations_&_variables.
- [35] Diario Financiero, «Noticias de Ciberseguridad,» [En línea]. Available: https://www.df.cl/noticias/site/tag/port/all/tagport_1520_1.html.
- [36] generadoras.cl, «Boletín Generadoras de Chile (Febrero 2026),» Febrero 2026. [En línea]. Available: https://generadoras.cl/wp-content/uploads/2026/04/BoletinGeneradorasdeChile_26040.pdf.
- [37] Energyloop, «Imagen de Funcionamiento de Un Aerogenerador,» [En línea]. Available: <https://energyloop.es/como-funciona-un-aerogenerador/>.
- [38] U. P. d. Madrid, «Imagen Esquema Fotovoltaico,» [En línea]. Available: <https://blogs.upm.es/faraday/2022/05/11/integracion-masiva-de-la-solar-fotovoltaica-si-pero-con-inercia-por-favor/>.

- [39] T. E. Mexico, «Imagen Esquema Simplificado Térmico,» [En línea]. Available: <https://transicionenergetica.ineel.mx/Revista.mvc/CD1n4v1>.
- [40] Akamai, «Imagen - Vectores de Ataque,» [En línea]. Available: <https://www.akamai.com/es/glossary/what-is-attack-vector>.
- [41] SEC, «Anexo Técnico del Pliego Normativo RPTD N° 17,» Feb 2023. [En línea]. Available: <https://www.sec.cl/sitio-web/wp-content/uploads/2023/03/Anexo-Tecnico-RPTD-17-Indicadores-final-V-23-02-2023-1.pdf>.
- [42] NIS2, «Directiva (UE) 2022/2555 - Ciberseguridad en UE,» [En línea]. Available: <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32022L2555>.
- [43] NIST, «Framework for Improving Critical Infrastructure Cybersecurity,» [En línea]. Available: <https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf>.
- [44] G. Engineering, «Imagen - SCADA & PPC Systems,» [En línea]. Available: <https://www.glopowereng.com/scadappc/>.
- [45] DECOWELL, «Imagen - DCS,» [En línea]. Available: <https://decowellauto.com/es/que-es-un-sistema-de-control-distribuido-dcs/>.
- [46] SciELO, «Imagen - Redundancia IEC-61850 para subestaciones,» [En línea]. Available: https://www.scielo.cl/scielo.php?pid=S0718-07642019000100075&script=sci_arttext.
- [47] Wired, «Cómo 30 líneas de código hicieron explotar un generador de 27 toneladas,» 23 Oct 2020. [En línea]. Available: <https://www.wired.com/story/how-30-lines-of-code-blew-up-27-ton-generator/>.
- [48] B. News, «El virus que tomó control de mil máquinas y les ordenó autodestruirse,» 11 Oct 2015. [En línea]. Available: https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet.
- [49] Incibe-cert, «Industroyer2, El amperio contraataca,» 09 Feb 2023. [En línea]. Available: <https://www.incibe.es/incibe-cert/blog/industroyer2-el-amperio->

contraataca.

- [50] ENISA, «ENISA Threat Landscape 2024,» Sep 2024. [En línea]. Available: https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf.
- [51] N. S. Archive, «Dragos, CRASHOVERRIDE: Analyzing the Threat to Electric Grid Operations, June 2017. Not classified.,» Jun 2017. [En línea]. Available: <https://nsarchive.gwu.edu/document/15319-dragos-crashoverride-analyzing-threat>.
- [52] Emol, «Hackers norcoreanos de élite fueron vinculados a robo del Banco de Chile,» Oct 2018. [En línea]. Available: <https://www.emol.com/noticias/Economia/2018/10/04/922763/Hackers-norcoreanos-de-elite-fueron-vinculados-a-mega-atracos-contr-Banco-de-Chile.html>.
- [53] Meganoticias, «Intentan hackear Redbanc simulando una entrevista de trabajo por Skype,» Ene 2019. [En línea]. Available: <https://www.meganoticias.cl/nacional/247406-intento-hackeo-redbanc-corea-del-norte-sistema-bancario-chile-skype.html>.
- [54] CISA, «PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure,» Feb 2024. [En línea]. Available: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a>.
- [55] ANCI, «La ANCI publica nuevas instrucciones que aclaran elementos de la Ley Marco de Ciberseguridad,» Dic 2025. [En línea]. Available: <https://anci.gob.cl/noticias/anci-instrucciones-2025/>.
- [56] C. Camargo, L. Durán y N. Rosas, «Plataforma hardware/softwareabierta para aplicaciones en procesos de automatización Industrial,» 2013. [En línea]. Available: <https://revistas.usb.edu.co/index.php/Ingenium/article/view/1335/1126>.