Proyecto de ley para la protección de la infraestructura crítica

Indicación sustitutiva

Senadores Pedro Araya, Francisco Huenchumilla y Gastón Saavedra

Boletín N.º

16.143-02

6 de octubre de 2026

Senado de la República de Chile

Ejes temáticos

01 Contexto y antecedentes de la reforma constitucional

02 Tendencias de la legislación comparada

03 Qué debemos regular

04 Enfoque estratégico de la indicación

05 Sectores estratégicos

06 Instrumentos de planificación y gestión

07 Diseño institucional

08 Obligaciones para los operadores

09 Sanciones para los operadores

10 Concepto de empleo de las Fuerzas Armadas

11 Comparativo con las indicaciones del Ejecutivo

12 Conclusiones: principales ejes de la propuesta

13 Síntesis político-legislativa

Contexto y antecedentes de la reforma constitucional

a El proyecto de ley de **infraestructura crítica** (IC) deriva de la reforma constitucional aprobada por la Ley N.º 21.542, de 2023.

b La discusión se dio en un escenario de alta demanda social por aumentar la intervención de las FF.AA. en labores de seguridad y orden público, y de resguardo de las fronteras.

c La reforma habilitó al Presidente de la República para requerir a las FF.AA. hacerse cargo de la **protección de la IC cuando exista peligro grave o inminente** a su respecto.

d Estableció que se considera IC aquellas instalaciones —físicas o virtuales— que presten **servicios esenciales o de utilidad pública**.

e Encomendó a la ley **establecer los criterios para identificar a los operadores de la IC y determinar sus obligaciones**.

f Reguló, de manera general, el ejercicio del mando de las FF.AA. cuando se disponga su empleo para proteger la IC, el procedimiento, su extensión y el control político del Congreso Nacional.

g Extendió esta misma facultad al Presidente para emplear las FF.AA. en el **resguardo de las fronteras**.

Tendencias de la legislación comparada (UE y EE.UU.)

01 **Del activo al servicio esencial.** El esfuerzo ya no se agota en proteger instalaciones: apunta a asegurar la continuidad de las funciones y servicios indispensables para la sociedad.

02 **Enfoque de "todos los riesgos".** Los sistemas más desarrollados no se limitan al terrorismo, el sabotaje u otras amenazas deliberadas; incorporan catástrofes naturales, pandemias, ciberataques, amenazas híbridas y cambio climático.

03 **Regulación basada en riesgos.** Las medidas no son uniformes: el Estado y los operadores evalúan periódicamente amenazas, vulnerabilidades e impactos, y adoptan medidas adecuadas y proporcionales al riesgo.

04 **De la seguridad a la resiliencia.** La protección física sigue siendo relevante, pero se integra en un concepto más amplio: capacidad de prevenir, proteger, responder, resistir, mitigar, adaptarse y recuperarse frente a incidentes.

05 **Corresponsabilidad público-privada.** El Estado define la estrategia, identifica entidades críticas, supervisa y apoya; los operadores públicos o privados gestionan sus riesgos, adoptan medidas de resiliencia y reportan incidentes.

Qué debemos regular

1 Primero

Establecer los criterios y estándares para **determinar qué se considera infraestructura crítica**, conforme al numeral 21 del artículo 32 de la Constitución Política de la República (servicios esenciales y de utilidad pública).

2 Segundo

Crear los instrumentos y mecanismos institucionales de planificación, coordinación y gestión para la **protección y resiliencia** de la infraestructura crítica.

3 Tercero

Establecer las **obligaciones de los operadores públicos y privados** de la infraestructura catalogada como crítica.

4 Cuarto

Determinar el rol de las FF.AA. cuando **excepcionalmente** son requeridas para la protección de la IC, conforme al numeral 21 del artículo 32 de la Constitución Política de la República.

Enfoque estratégico de la indicación

Diseño institucional y de gobernanza **liviano**, inspirado en los principios de **resiliencia**, **evaluación de riesgos** y un **modelo de control de gestión** a cargo de organismos civiles y sectoriales, y no centrado en la inteligencia civil. Ante un incidente, se prioriza la mantención o recuperación —en el menor tiempo posible— del servicio esencial o de utilidad pública afectado.

Cadena de mitigación

01

Operador

Prevención, mitigación y recuperación del servicio como primera respuesta.

›

02

Reguladores civiles y sectoriales

Control de gestión y cumplimiento de los planes de resiliencia.

›

03

Fuerzas Armadas

Instrumento que se activa después de la cadena de mitigación, ante peligro grave o inminente.

Sectores estratégicos con rango legal

11

sectores fijados en la ley

Disminuye la volatilidad en la determinación, reduce el espacio para la discrecionalidad política y minimiza el riesgo de judicialización.

Se sigue el modelo de la UE y EE.UU.

01 Agua

02 Aguas residuales

03 Energía

04 Transporte público y de carga

05 Banca y servicios financieros

06 Sanidad

07 Producción, transformación y distribución de productos alimentarios

08 Telecomunicaciones

09 Infraestructura digital

10 Espacio

11 Administración pública

Instrumentos de planificación y gestión

01

Catálogo nacional de infraestructura crítica y sus operadores

02

Matriz de evaluación de riesgos

03

Plan operativo de protección de riesgos y resiliencia del operador de infraestructura crítica

04

Modelo de control y cumplimiento

Cómo se construyen

Mediante una evaluación integral de los riesgos, de manera descentralizada e interinstitucional, incorporando a gobiernos regionales y municipios, y considerando riesgos antrópicos y naturales.

Diseño institucional

Coordinación interinstitucional

Es una coordinación civil e interagencial.

Control y cumplimiento con enfoque transversal

1. Se crea un **Modelo de Control y Cumplimiento** en el que participan SENAPRED, CONAF, la Comisión para el Mercado Financiero (CMF) y las agencias de Ciberseguridad e Inteligencia.

2. Sus metas: asegurar la coordinación regulatoria entre estas agencias, bajar los costos de transacción para las empresas operadoras y fomentar el cumplimiento efectivo de los planes de prevención y resiliencia.

3. Este modelo normativo centralizado será aprobado mediante resolución exenta del Ministerio del Interior.

Rol del Ministerio del Interior

1. Actuará como **ente articulador del sistema**, asegurando que los operadores públicos y privados tengan las herramientas necesarias para mitigar riesgos.

2. Elabora el catálogo, asesorado por los reguladores sectoriales técnicos.

3. La ANI es un **colaborador metodológico**, no el órgano ejecutor.

Modelos de prevención

1. Los operadores de IC pueden adoptar programas de cumplimiento o modelos específicos de prevención de riesgos y resiliencia.

2. La certificación, los lineamientos técnicos, la fiscalización y la puesta en marcha de estos modelos serán regulados por el **Ministerio del Interior**.

Diseño institucional: facultades del Ministerio del Interior

01

Actuación sectorial

El Ministerio del Interior **actuará directamente o a través de los organismos reguladores sectoriales** de cada servicio esencial o de utilidad pública (por ejemplo: la SEC en energía, la SISS en aguas, la Subtel en telecomunicaciones).

02

Supervisión

Podrán **realizar inspecciones y auditorías, supervisar el cumplimiento y exigir información** sobre las medidas adoptadas.

03

Instrucciones obligatorias

Ante un peligro grave o inminente para la continuidad de un servicio, las autoridades podrán **emitir instrucciones directas y obligatorias**, proporcionales al impacto del riesgo y a la capacidad económica de la empresa.

Obligaciones para los operadores

Obligación general y permanente del operador de IC

Mantener sus planes de prevención de riesgos y resiliencia activos y actualizados, ejecutando todas las medidas necesarias para asegurar su efectividad.

01

Enlace
Designar una persona de contacto con el Ministerio del Interior y con el regulador de su sector.

02

Actualización
Enviar la actualización de su plan de prevención en forma anual o semestral, según el nivel de riesgo determinado por su regulador.

03

Aviso en 24 horas
Ante cualquier evento que afecte gravemente el servicio, avisar mediante un mecanismo rápido, en un plazo máximo de 24 horas desde que se detectó el incidente.

04

Reporte posterior
Superado el incidente y aplicado el plan de resiliencia, entregar un reporte con las medidas de mitigación aplicadas, las correcciones realizadas y las lecciones aprendidas.

Sanciones para el operador privado

Hasta 50%

Aumento de las multas sectoriales

Término

de la concesión

Revocación

de patentes

Resolución

de contratos

Régimen sancionatorio

Las infracciones serán tramitadas y sancionadas por la autoridad regulatoria de cada sector (por ejemplo, energía o telecomunicaciones), según lo definido en las leyes sectoriales.

Frente a incumplimientos graves y reiterados la autoridad puede adoptar sanciones como el término de la concesión, revocación de patente o resolución de contrato sin derecho a indemnización.

Sanciones para el operador público

Responsabilidad personal

Las responsabilidades recaen personalmente en el jefe superior del servicio.

Se aplica el régimen de sanciones del Título VI de la Ley N.º 20.285, sobre acceso a la información pública.

20% – 50%

Multa sobre la remuneración del jefe superior del servicio.

Duplo + 5 días

Si persiste la conducta, la multa se duplica y conlleva suspensión del cargo por cinco días.

Concepto de empleo de las Fuerzas Armadas

Misión

Proteger la IC considerada en el Catálogo Nacional, dentro de las áreas y condiciones establecidas por el decreto supremo suscrito por Interior, Defensa y Seguridad.

Mando y conducción

Un oficial general nombrado por el Presidente ejerce el mando sobre la fuerza, con apoyo del Estado Mayor Conjunto, que además entrega los instrumentos de planificación y gestión pertinentes.

Apreciación integrada del ambiente operacional

Asesoría al mando para identificar amenazas, riesgos, vulnerabilidades e impactos, integrando inteligencia civil (ANI), policial, estratégica (DID) y de contrainteligencia militar, más información de SENAPRED.

Habilitación y límites

Actuación conforme a la Constitución, las reglas del uso de la fuerza (RUF) y la legislación vigente, con deber de respeto a los DD.HH. y reserva de la información militar.

Facultades de naturaleza policial

Control de identidad, examen de vestimentas, detención en flagrancia y funciones preventivas y de tránsito, ejercidas conforme a las RUF.

Comparativo con las indicaciones del Ejecutivo I

ENFOQUE, SECTORES E INSTRUMENTOS

Materia	Ejecutivo	Indicación senadores	Diferencia central
Objeto	Identificar la IC y regular obligaciones vinculadas a su protección ante peligro grave o inminente.	Regula criterios, sectores, instrumentos, operadores, resiliencia, control y coordinación.	Protección específica → **sistema permanente de gestión**
Sectores	Se determinan por reglamento del Ministerio del Interior.	Se fijan en la ley: agua, energía, transporte, banca, salud, alimentos, telecomunicaciones, digital, espacio y administración pública.	Flexibilidad reglamentaria → **certeza legal**
Riesgos	Criterios de criticidad e impacto.	Evaluación multirriesgo: amenazas naturales, humanas, ciber, cambio climático, crimen organizado, sabotaje y pandemias.	Seguridad física → **enfoque de todos los riesgos**
Instrumentos	Plan Nacional y Catálogo Nacional.	Catálogo, matriz de riesgos, planes operativos de resiliencia y modelo de control y cumplimiento.	Planificación estratégica → **gestión operacional y resiliencia**

Comparativo con las indicaciones del Ejecutivo II

GOBERNANZA, OPERADORES Y SANCIONES

Materia	Ejecutivo	Indicación senadores	Diferencia central
Gobernanza	Consejo Interministerial: Interior, Defensa y Seguridad Pública, con rol relevante de la ANI.	Modelo civil e interagencial: Interior, reguladores sectoriales, SENAPRED, CONAF, CMF, Ciberseguridad e Inteligencia.	Centralización → **coordinación sectorial**
Catálogo	Registro secreto elaborado desde un catastro de la ANI y aprobado por decreto secreto.	Registro reservado elaborado por Interior con asesoría de reguladores y organismos técnicos.	Inteligencia como eje → **regulación técnica y sectorial**
Operadores	Información, reportes, encargado de enlace y exigencias vinculadas a seguridad privada.	Planes de resiliencia, reportes periódicos, aviso en 24 horas, mitigación, correcciones y lecciones aprendidas.	Deberes reactivos → **deber permanente de prevención y recuperación**
Fiscalización y sanciones	Subsecretaría de Prevención del Delito y régimen de la Ley de Seguridad Privada; delito por información falsa u omisión relevante.	Reguladores sectoriales; aumento de multas; término de concesión, revocación o resolución de contratos ante casos gravísimos.	Régimen transversal → **régimen sectorial reforzado**

Comparativo con las indicaciones del Ejecutivo III

FUERZAS ARMADAS, INTELIGENCIA Y MATERIAS SECTORIALES

Materia	Ejecutivo	Indicación senadores	Diferencia central
Activación de FF.AA.	Decreto supremo fundado ante peligro grave o inminente; determina área y oficial general.	Mantiene el mismo supuesto constitucional y exige que la IC esté incorporada en el Catálogo.	Misma habilitación → **requisito adicional: IC catalogada**
Mando y atribuciones	El oficial general coordina y requiere colaboración sin alterar competencias legales.	El oficial general puede dictar órdenes dentro del área y requerir colaboración fuera de ella.	Coordinación y colaboración → **mando circunscrito al área del decreto**
Facultades policiales	Control de identidad y registro de vestimentas, equipaje o vehículos.	Control de identidad, examen de vestimentas, detención en flagrancia, funciones preventivas y tránsito.	Control y registro → **facultades operativas sujetas a las RUF**
Inteligencia y sectores	ANI entrega información pertinente al mando; confidencialidad amplia.	Integra inteligencia policial, defensa, ciberseguridad, SENAPRED y agrega reglas de telecomunicaciones, energía y agravantes penales.	Inteligencia como eje → **inteligencia como asesoría al mando**
Límites y controles	**Aporte de la indicación: solo sobre IC incorporada al Catálogo.** Además: área fijada en el decreto · Constitución, RUF y legislación vigente · respeto a los DD.HH. · control político del Congreso (art. 32 N.º 21 CPR).		

Para concluir

Principales ejes estratégicos de la propuesta de los senadores

DEFINIR	lo que se busca proteger: el objetivo último debiera ser asegurar la continuidad de los servicios esenciales y de utilidad pública, y no exclusivamente la integridad física de determinadas instalaciones.
ADOPTAR	una concepción amplia del riesgo (natural, tecnológico, cibernético y humano), sea accidental o deliberado.
INCORPORAR	una lógica preventiva: anticipar amenazas y vulnerabilidades, evaluar periódicamente los riesgos y adoptar medidas antes de que ocurra el incidente.
INCORPORAR	la resiliencia, abarcando todo el ciclo del riesgo: prevención, protección, respuesta, continuidad, recuperación y adaptación.
ESTABLECER	obligaciones diferenciadas y proporcionales al riesgo, la criticidad y el impacto de la interrupción del servicio, según las distintas realidades.
CONSTRUIR	un sistema de gestión y no solo un catálogo de IC: la identificación se complementa con evaluación de riesgos, planes de resiliencia, reporte de incidentes, supervisión y actualización periódica.
ARTICULAR	Estado y operadores: la resiliencia exige coordinación más que una relación exclusivamente fiscalizadora.

Síntesis político-legislativa

El texto del Ejecutivo y la indicación de los senadores responden a **énfasis normativos distintos**. El primero ordena un mecanismo de identificación y protección de la infraestructura crítica frente a un peligro grave o inminente; la segunda desarrolla un **sistema permanente** de gestión de riesgos, resiliencia, control sectorial y continuidad operacional.

La discusión legislativa debiera precisar **qué elementos de ambos modelos se integran**: planificación nacional, criterios legales, coordinación regulatoria, obligaciones de los operadores, límites del despliegue militar, régimen sancionatorio y resguardos de proporcionalidad.

Objetivo común

Asegurar la continuidad de los servicios esenciales y de utilidad pública, evitando duplicidad de competencias, costos regulatorios innecesarios y afectaciones desproporcionadas a garantías constitucionales.

Proyecto de ley para la protección de la infraestructura crítica

Indicación sustitutiva

Senadores Pedro Araya, Francisco Huenchumilla y Gastón Saavedra

Boletín N.º

16.143-02

6 de octubre de 2026

Senado de la República de Chile