Revista Política y Estrategia
Nº 143, (2024)

Editada por: **Academia Nacional de Estudios Políticos y Estratégicos (ANEPE) Chile**.

Lugar de edición: Santiago, Chile

Dirección web:
http://www.politicayestrategia.cl

ISSN versión digital: 0719-8027

ISSN versión impresa: 0716-7415

DOI: **https://doi.org/10.26797/rpye.vi143.1084**

Para citar este artículo / To cite this article: QUEIROLO Pellerano, Fulvio: "Descodificando la infraestructura crítica. Caso nacional".

Revista Política y Estrategia N° 143. 2024. pp. 139-154

DOI: **https://doi.org/10.26797/rpye.vi143.1084**

Si desea publicar en Política y Estrategia, puede consultar en este enlace las Normas para los autores:

To publish in the journal go to this link:

http://politicayestrategia.cl/index.php/rpye/about/submissions#authorGuidelines

DESCODIFICANDO LA INFRAESTRUCTURA CRÍTICA: CASO NACIONAL*∞

FULVIO QUEIROLO PELLERANO•

RESUMEN

Diversos incidentes, de carácter antrópico o natural, han afectado estructuras públicas y privadas, sean materiales o intangibles, provocando estragos en el buen desempeño funcional de servicios fundamentales que requiere un país, sociedad o colectivo. En este ámbito, numerosas administraciones estatales, organismos internacionales y organizaciones multilaterales han avanzado en identificar cuáles serían aquellos servicios y estructuras administrativas, cuya alteración o ruptura, podrían ver socavada su principal cometido. Dicho entorno se concibe como infraestructura crítica. Así las cosas, es posible observar que pese a todos los avances para otorgar una adecuada conceptualización, así como establecer niveles de responsabilidad en su protección, también es factible evidenciar que, para el caso nacional, la normativa no ha madurado adecuadamente. Por lo tanto, es esencial una definición rápida que contenga una descripción clara, así como una estrategia para proteger la infraestructura crítica nacional.

Palabras clave: *Infraestructura crítica; riesgo; amenaza; estrategia nacional.*

DECODING CRITICAL INFRASTRUCTURE: NATIONAL CASE

ABSTRACT

Various incidents, of an anthropogenic or natural nature, have affected public and private structures, whether material or intangible, wreaking havoc on the good functional performance of fundamental services required by a country, society or group. In this area, numerous state administrations, international and multilateral organizations have made progress in identifying those services and administrative structures whose alteration or rupture could see their main mission undermined.

---

* El escrito es resultado del trabajo de investigación elaborado durante la ejecución del programa de Seguridad Internacional, que desarrolla la Universidad Nacional de Educación a Distancia (UNED), conducente al grado académico de doctor.

• Magíster en Ciencia Política, Seguridad y Defensa (ANEPE). Doctorando en Seguridad Internacional (UNED, programa internacional, IUGGM, España). Investigador asociado Universidad UBO. Encargado de Estudios Estratégicos en Academia Nacional de Estudios Políticos y Estratégicos. Chile. fqueirolo@anepe.cl - fqueirolo3@alumno.uned.es ORCID: https://orcid.org/0000-0001-6837-0962

∞ Fecha de recepción: 030624 - Fecha de aceptación: 260624.

This environment is conceived as critical infrastructure. Thus, it is possible to observe that despite all the advances to provide an adequate conceptualization, as well as establish levels of responsibility in its protection, it is also possible to show that, in the national case, the regulations have not matured adequately. Therefore, a prompt definition containing a clear description as well as a strategy to protect national critical infrastructure is essential.

Key words: *Critical infrastructure; risk; threat; national strategy.*

DECODIFICANDO INFRAESTRUTURA CRÍTICA: CASO NACIONAL

RESUMO

Diversos incidentes, de natureza antropogénica ou natural, afectaram estruturas públicas e privadas, *sejam materiais ou imateriais, causando estragos no bom desempenho funcional de serviços fundamentais requeridos por um país, sociedade ou grupo. Nesta área, numerosas administrações estatais, organizações internacionais e organizações multilaterais têm feito progressos na identificação dos serviços e estruturas administrativas cuja alteração ou ruptura poderia ver prejudicada a sua missão principal. Este ambiente é concebido como infraestrutura crítica. Assim, é possível observar que apesar de todos os avanços para fornecer uma conceituação adequada, bem como estabelecer níveis de responsabilidade na sua proteção, também é possível mostrar que, no caso nacional, a regulamentação não amadureceu adequadamente. Portanto, é essencial uma definição* rápida que *contenha uma descrição clara, bem como uma estratégia para proteger as infra-estruturas críticas nacionais.*

Palavras-chave: *Infraestrutura crítica; risco; ameaça; estratégia nacional.*

Introducción

Evidencias sobre una creciente manifestación de elementos perturbadores, cuya consecuencia ha sido infringir daños en estructuras físicas e intangibles, principalmente sobre servicios públicos, proveedores privados, así como en organizaciones e instalaciones gubernamentales, exige una debida consideración. ¿Cuáles serían estos elementos perturbadores y qué estructuras se han visto comprometidas? ¿Quiénes debiesen asumir la responsabilidad de protegerlas? Son preguntas que requieren de una robusta respuesta por parte del Estado y previsión por parte de privados. En palabras simples, es necesario separar la nata de la leche para obtener un buen producto.

La aproximación más afín sobre esta discusión es la proporcionada por la Organización para la Cooperación y el Desarrollo (OCDE), al señalar:

"Los riesgos críticos pueden derivarse de fenómenos naturales, pandemias, accidentes industriales o tecnológicos graves y actos malintencionados que provoquen daños de importancia nacional. Sus consecuencias pueden provocar trastornos en sectores de la infraestructura vitales para las actividades económicas, degradar bienes ambientales clave, causar un efecto negativo en las finanzas públicas y erosionar la confianza pública en el gobierno. Ante un complejo escenario de cambios demográficos, adelantos tecnológicos, globalización y cambio climático, los riesgos críticos pueden desarrollarse con rapidez y por vías imprevistas, permitiendo que los impactos transfronterizos se dispersen en diferentes comunidades, sectores económicos y fronteras nacionales"[1].

El criterio, con visión económica, recomendado por la OCDE para definir una infraestructura crítica (IC) contempla "… *los sistemas, activos, instalaciones y redes que prestan servicios esenciales para el funcionamiento de la economía y para la seguridad, la protección y el bienestar de la población"*[2]. Si bien se orienta hacia el desarrollo y bienestar, no delimita si dichos servicios son solo provistas por el Estado y/o bien con participación de proveedores privados. Del mismo modo, deja abierta a la interpretación sobre la extensión de cuáles serían aquellos elementos perturbadores o amenazas que podrían afectar a la IC de servicios esenciales.

En el entorno descrito resulta fundamental contar con una eficaz y oportuna inteligencia que permita identificar cuáles serían aquellos riesgos y amenazas a la que se enfrenta un servicio, organización o instalación crítica. El diseño de estrategias nacionales, regionales y locales constituye el eslabón principal en la cadena de formación de una sociedad preparada y resiliente.

La condición actual de la normativa nacional presenta aspectos subjetivos y falta de especificidad en los niveles de gestión gubernamental. Así las cosas, se pone en riesgo la aplicabilidad de los criterios establecidos, un ambiente que, más temprano que tarde, se expone a juicios de interpretación y confusión de los actores del régimen establecido. Esta hipótesis se sustenta en lo indicado por el numeral 21 de la Ley Nº 21.542, que modificó la Carta Fundamental, al disponer que las fuerzas armadas asuman responsabilidades en la protección de la IC, prescribiendo:

> *"Disponer, mediante decreto supremo fundado, suscrito por los Ministros del Interior y Seguridad Pública y de Defensa Nacional, que las Fuerzas Armadas se hagan cargo de la protección de la infraestructura crítica del país cuando exista peligro grave o inminente a su respecto, determinando aquella que debe ser protegida"*[3].

En consideración a la relevancia de la temática el presente ensayo pretende llevar a cabo un juicio crítico sobre la capacidad de aplicación de la ordenanza nacional destinada al

---

1 OECD. "Recomendación del Consejo sobre la Gobernanza de Riesgos Críticos". 6 de mayo de 2014. En: https://www.oecd.org/gov/risk/Critical-Risks-Recommendation-Spanish.pdf

2 OCDE. "*Recomendación del Consejo sobre la gobernanza de infraestructuras*", OECD/LEGAL/0460, p. 6, 2020. En: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0460

3 BCN. Ley Nº 21.542. "Modifica *la carta fundamental con el objeto de permitir la protección de infraestructura crítica por parte de las fuerzas armadas, en caso de peligro grave o* inminente". 3 febrero, 2023. En: https://www.bcn.cl/leychile/navegar?idNorma=1188583

resguardo de la IC. Su objetivo se centrará en identificar factores que requieren ajustes y así alcanzar una efectiva sincronización de los agentes involucrados para la protección de la IC.

Para dilucidar la hipótesis planteada, se utilizará el método de cotejo de la normativa nacional comparándola con el régimen convenido a partir de lo establecido por la Unión Europea (UE), a través del Consejo Europeo y, posteriormente, sistematizado por la OCDE. La técnica escogida permitirá revelar aspectos sensibles que contribuirán a clarificar el planteamiento, así como aportar elementos para la discusión nacional.

La codificación de la infraestructura crítica (IC)

Literatura internacional respecto de la temática es nutrida, sin embargo, con el fin de acotar el examen propuesto, se seleccionarán tres perspectivas que permitan llevar a cabo una decodificación del concepto. La necesidad de decodificar surge de la perspectiva del estudio propuesta buscando descifrar conceptos. De esta manera, se analizará la ruta que han trazado organizaciones y entidades que presentan una evolución sostenida en el tratamiento de la IC., y a partir de dicha base sustentar el alcance de la conceptualización a nivel nacional.

- **Del proceso del Consejo Europeo y la Comisión**

- A partir de los atentados terroristas perpetrados en Madrid (11/03/2004) y Londres (7 y 21/07/2005), respectivamente, el Consejo Europeo mandató a la Comisión Europea para llevar a cabo un trabajo, cuyo resultado fue el diseño de una estrategia para la protección de la IC[4].

- El Consejo de Ministros, desde un principio, asumió que las IC podían ser dañadas por "*acciones terroristas deliberadas, catástrofes naturales, accidentes o actos de piratería informática, actividades delictivas o comportamientos malintencionados*".

- Con todo, el objetivo de la Comisión estuvo focalizado en brindar protección de sus activos de acciones de terrorismo. El resultado fue la elaboración un Libro Verde[5] cuyos lineamientos se orientaban sobre el resguardo de la infraestructura de la Comunidad Europea. En esta ruta se asumió de forma consensuada la siguiente definición de IC.:

> *"… aquellos recursos físicos, servicios e instalaciones, redes y activos de infraestructura de tecnología de la información que, si se interrumpieran o destruyeran, tendrían un impacto grave en la salud, la seguridad o el bienestar económico de los ciudadanos o el funcionamiento eficaz de los gobiernos"*[6].

4 COMISIÓN EUROPEA. "*Critical Infrastructure Protection in the fight against terrorism*". Brussels, 20.10.2004 COM (2004) 702 final, de 20 de octubre de 2004. En: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0702:FIN:EN:PDF

5 COMISIÓN DE LAS COMUNIDADES EUROPEAS. Libro Verde. "*Sobre un programa europeo para la protección de infraestructuras críticas".* Bruselas. 17.11.2005. Anexo 1, p. 22. En: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0576:FIN:ES:PDF

6 UE. Directiva 2008/114/CE del Consejo de la UE. "*Sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección"*. 8 diciembre 2008. En: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32008L0114

- Sin embargo, la discusión continuó avanzando conforme a nuevos entornos de riesgos y amenazas, que se ciernen sobre la Comunidad Europea, estableciendo e identificando una infraestructura crítica europea (ICE) para esta Comunidad como:

> *"… el elemento, sistema o parte de este situado en los Estados miembros que es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población y cuya perturbación o destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones"*[7].

- Tras la agresión rusa hacia Ucrania, así como la interrupción de servicios esenciales en áreas de Europa anexado a la crisis energética ocasionada por el corte de tuberías del gasoducto *Nord Stream,* reactivó el debate europeo para la actualización de una nueva agenda de seguridad. En esta oportunidad, el objetivo fue incorporar nuevos riesgos en ICE, articulando el advenimiento de amenazas híbridas. El parámetro de recomendaciones del Consejo se sitúa en:

> *"… la sociedad depende en gran medida de infraestructuras tanto físicas como digitales y la interrupción de los servicios esenciales, ya sea por ataques físicos convencionales o por ciberataques, o por una combinación de ambos, puede tener consecuencias graves para el bienestar de los ciudadanos, para nuestras economías y para la confianza en nuestros sistemas democráticos*[8].

- Como corolario del trabajo y actividades de la Comisión Europea se presentan recomendaciones a los países signatarios, con el fin de avanzar en la elaboración de estrategias nacionales para la protección de ICE. La prioridad converge en el reforzamiento y resiliencia de sectores y áreas vitales identificadas como:

> *"… energía, la infraestructura digital, el sector del transporte y el espacial, y cuando sea posible en aquellos sectores incluidos en el ámbito de aplicación de la nueva Directiva REC, a saber, la banca, las infraestructuras de los mercados financieros, la infraestructura digital, la salud, el agua potable, las aguas residuales, las administraciones públicas, el espacio y la producción, transformación y distribución de alimentos, teniendo en cuenta la posible naturaleza híbrida de las amenazas, incluidos los efectos en cascada y los efectos del cambio climático"*[9].

- El resultado de este proceso ha sido, entre otras, la elaboración de estrategias para la protección de IC nacionales. De esta manera, la mayoría de los países signatarios poseen instrumentos normativos que establecen roles, funciones, así como una estructura institucional para la protección de la IC a la luz de riesgos y amenazas.

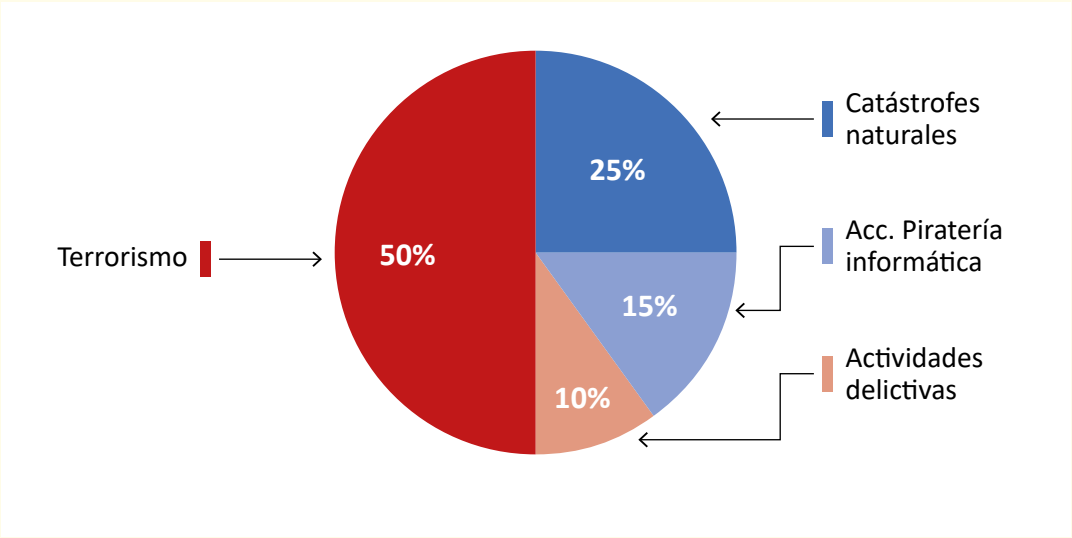
---

7 Ibid.

8 COMISIÓN EUROPEA. "*Sobre un enfoque coordinado de la Unión para reforzar la resiliencia de las infraestructuras críticas".* Estrasburgo, 18.10.2022. p. 1. En: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52022DC0551

9 Ibid. pp. 14–22.

Gráfico 1
Elementos perturbadores, riesgos y amenazas a la IC en porcentaje de preponderancia



Fuente: Elaboración propia en base a documentos base de la Comisión Europea (2008 y 2022).

Cuadro 1
Sectores estratégicos de Infraestructura Crítica

Sector		Servicios
I	Energía	- Producción, refinación, tratamiento y almacenamiento de petróleo y gas, incluyendo tuberías. - Generación eléctrica. - Transmisión de electricidad, gas y petróleo. - Distribución de electricidad, gas y petróleo.
II	Tecnologías, Comunicación e Información (TIC)	- Sistema de información y protección de redes. - Sistemas de automatización y control de instrumentación (SCADA, etc.) - Internet. - Provisión de telecomunicaciones fijas. - Provisión de telecomunicaciones móviles. - Radiocomunicación y navegación. - Comunicación por satélite - Radiodifusión
III	Agua	- Provisión de agua potable. - Control de la calidad del agua. - Destilado y control de cantidad de agua.

IV	Alimentación	- Suministro de alimentos y salvaguardia de la inocuidad y protección de los alimentos
V	Salud	- Atención médica y hospitalaria. - Medicamentos, sueros, vacunas y productos farmacéuticos. - Biolaboratorios y bioagentes.
VI	Financiero	- Servicios de pago/estructuras de pago (privadas). - Asignación financiera del gobierno.
VII	Orden y Seguridad Pública y Legal	- Mantener el orden público y legal, la seguridad y la protección. - Administración de justicia y detención.
VIII	Administración Civil	- Funciones gubernamentales. - Fuerzas Armadas. - Servicios de administración civil. - Servicios de emergencia. - Servicios postales y de mensajería.
IX	Transporte	- Transporte por carretera. - Transporte ferroviario. - Tráfico aéreo. - Transporte por vías navegables interiores. - Transporte marítimo y marítimo de corta distancia.
X	Industria química y nuclear.	- Producción y almacenamiento/procesamiento de productos químicos y sustancias nucleares. - Tuberías de mercancías peligrosas (sustancias químicas)
XI	Espacio e investigación	- Espacio. - Investigación.

Fuente: Libro Verde Comisión de las Comunidades Europeas, 2005. (Traducción propia)

- **Del proceso de decodificación nacional**

- Una de las aproximaciones más afines que, para este estudio resulta relevante, constituye el informe "Infraestructura Crítica para el Desarrollo" (ICD) 2016-2025, de la Cámara Chilena de la Construcción (CChC)[10]. Dicho documento, junto con actualizar la versión anterior, incorpora nuevos elementos de análisis como los cambios macroeconómicos globales y políticos locales, un entorno que ha modificado la agenda de desarrollo; por otra parte, examina las vulnerabilidades estructurales nacionales, esta vez, desde la perspectiva territorial. Finalmente, en su metodología aplica estándares más elevados que permiten vigencia de sus contenidos. En síntesis, se enfatiza

10 CChC. Cámara Chilena de la Construcción. Informe Infraestructura Crítica para el Desarrollo (ICD) 2016-2025. 6 de abril de 2016. p. 6. [Fecha de consulta: 15 de mayo de 2024] Disponible En: http://www.cchc.cl/uploads/archivos/archivos/Infraestructura-Critica-para-el-Desarrollo_2016-2025.pdf

una división de esferas, consideradas fundamentales, para el desarrollo nacional al establecer:

> *"…doce sectores clave para el progreso social y económico del país, agrupados en tres ejes estratégicos: infraestructura que nos sostiene o basal (agua, energía y telecomunicaciones), infraestructura que nos conecta o de apoyo logístico (vialidad interurbana, aeropuertos, puertos y ferrocarriles) e infraestructura que nos involucra o de uso social (vialidad urbana, espacios públicos, educación, hospitales y cárceles)"*[11].

- El mérito de la publicación se sustenta en alertar a diferentes autoridades y sectores productivos sobre la necesidad de diseñar estrategias para el desarrollo nacional. Los ejes se fundamentan en la necesidad de generar políticas para un progreso viable y eficiente, e impulsar un plan de inversiones que busque soluciones rentables y sostenibles en el tiempo respecto de las problemáticas actuales. Sin embargo, llama la atención la ausencia de la amenaza antrópica como componente de análisis. Una variable que irrumpe con mayor fuerza en diferentes escenarios, y que la OCDE ya lo incorporó.

- Sin embargo, la temática posee una extensa data de normas que han incorporado variables de afectación de IC, las que han sido abordadas acorde a contextos o bien experiencias nacionales. El relato se encuentra reflejado en el Mensaje n° 122-371 de S.E. el Presidente de la República al Senado, que propone a trámite una norma destinada a la protección de IC nacional, presentando los siguientes antecedentes[12]:

  - Decreto Ley N° 3.607 (1981), del Ministerio del Interior que establece nuevas normas sobre funcionamiento de vigilantes privados, haciendo mención a empresas estratégicas.

  - Ley N° 18.168 (1982), General de Telecomunicaciones, en el Cap. VII "De las Infraestructuras Críticas de Telecomunicaciones".

  - Ley N° 20.478 (2011), sobre recuperación y continuidad en condiciones críticas y de emergencia del sistema público de telecomunicaciones.

  - Decreto 60 (2012), del Ministerio de Transportes y Telecomunicaciones, el que establece un reglamento para la interoperación y difusión de la mensajería de alerta, declaración y resguardo de la infraestructura crítica de telecomunicaciones e información.

- Por otra parte, el 2018 se publica la Política de Ciberdefensa (PCD)[13]. Dicho instrumento normativo busca establecer la debida protección a la IC de la información,

11 Ibid.

12 MENSAJE Nº 122-371 "*Proyecto de ley, iniciado en Mensaje de S.E. el Presidente de la República para la protección de la infraestructura crítica del país*". 01 agosto, 2023. En: https://www.doe.cl/alerta/04082023/20230804034

13 LEY Nº 42.003. Política de Ciberdefensa. Ministerio de Defensa Nacional. 9 de marzo de 2018. [en línea] [Fecha de consulta: 15 de mayo de 2024] Disponible En: http://www.diariooficial.interior.gob.cl/publicaciones/2018/03/09/42003/01/1363153.pdf

en este caso, desde la lógica de la Defensa Nacional. Dimensión que requería estar sintonizada con el articulado promulgado para el ámbito de la Ciberseguridad. Este último cuerpo legal describe:

> *"Dentro de las infraestructuras de la información, existe un conjunto especialmente relevante para la marcha del país, las denominadas infraestructuras críticas de la información (ICI), que comprende las instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya afectación, degradación, denegación, interrupción o destrucción pueden tener una repercusión importante en la seguridad, la salud, el bienestar de los ciudadanos y el efectivo funcionamiento del Estado y del sector privado"*[14].

- La administración gubernamental, a través de los documentos señalados, procura establecer una separación inequívoca respecto de la IC de la información, sin embargo no concluye sobre el alcance y efectos que se ciernen sobre la IC en particular, al establecer:

> *"En el caso chileno, mientras se adopta una política específica para infraestructuras críticas, la infraestructura de la información de los siguientes sectores será considerada como crítica: energía, telecomunicaciones, agua, salud, servicios financieros, seguridad pública, transporte, administración pública, protección civil y defensa, entre otras".*
>
> *"Por otra parte, deberá evaluarse la pertinencia de crear un Computer Security Incident Response Team, (CSIRT), de infraestructuras críticas"* [15].

- La preocupación gubernamental por establecer lineamientos sobre IC con el fin de sincronizar en toda su extensión, a través de diferentes normativas legales, también ha contribuido en retardar su aplicabilidad por parte de los actores involucrados, sean públicos o privados. A mayor abundamiento, mediante la promulgación de la nueva Política Nacional de Ciber Seguridad (PNCS) el país recoge el principio señalado por el Art. 51 de la Carta de Naciones Unidas, otorgando un nivel superlativo al dominio del internet. El problema se sitúa en el grado de responsabilidad que le compete a quien provee el servicio, cuando éstos son privados, al señalar:

> *"… Este principio pone la infraestructura de comunicaciones de Internet al mismo nivel que la infraestructura considerada estratégica y vital para el país, como la red de transporte y la red de centros de salud, entre otros"*[16].

- En línea con lo ya prescrito, la Política de Defensa Nacional 2020 (PDN) enfatiza sobre las amenazas a las que se enfrenta el país, y en lo pertinente a la IC establece:

---

14 PNCS. Política Nacional de Ciber Seguridad, 2017-2022. p. 16. https://biblioteca.digital.gob.cl/server/api/core/bitstreams/b5b26f36-2c47-441b-8848-00d767ec9b5c/content

15 Ibid. p. 17.

16 PNCS. Política Nacional de Ciber Seguridad, 2023–2028. p. 7. https://www.diariooficial.interior.gob.cl/publicaciones/2023/12/04/43717/01/2415658.pdf

> *"En el caso de Chile, cobra relevancia para la seguridad nacional la protección de las infraestructuras críticas de información asociadas a servicios esenciales para el país, cuya paralización o uso con fines maliciosos puede afectar gravemente a nuestra población. Una agresión de este nivel puede ser calificada como un acto hostil que podría configurar el derecho a legítima defensa"*[17].

- Finalmente, frente a una serie de eventos perturbadores para la seguridad interna, cuya expresión más álgida se constató durante el último lustro, la autoridad política resuelve autorizar el empleo de las Fuerzas Armadas para permitir la protección de la IC, en caso de peligro grave o inminente, prescribiendo:

> *"La infraestructura crítica comprende el conjunto de instalaciones, sistemas físicos o servicios esenciales y de utilidad pública, así como aquellos cuya afectación cause un grave daño a la salud o al abastecimiento de la población, a la actividad económica esencial, al medioambiente o a la seguridad del país"* [18].

- Dado el amplio espectro establecido se colige que mientras no se adopte una política nacional que instaure el marco de acción y regulatorio para la protección de la IC, se mantendrá el dilema respecto de quién hace qué. Además, se constata una preeminencia de misiones, roles y cometidos de las FF. AA. en ámbitos que le son ajenos a su función principal. En este estado de las cosas resulta imprescindible identificar las estructuras vitales que requieren y deben ser protegidas, para luego avanzar en el diseño de una gobernanza del sistema.

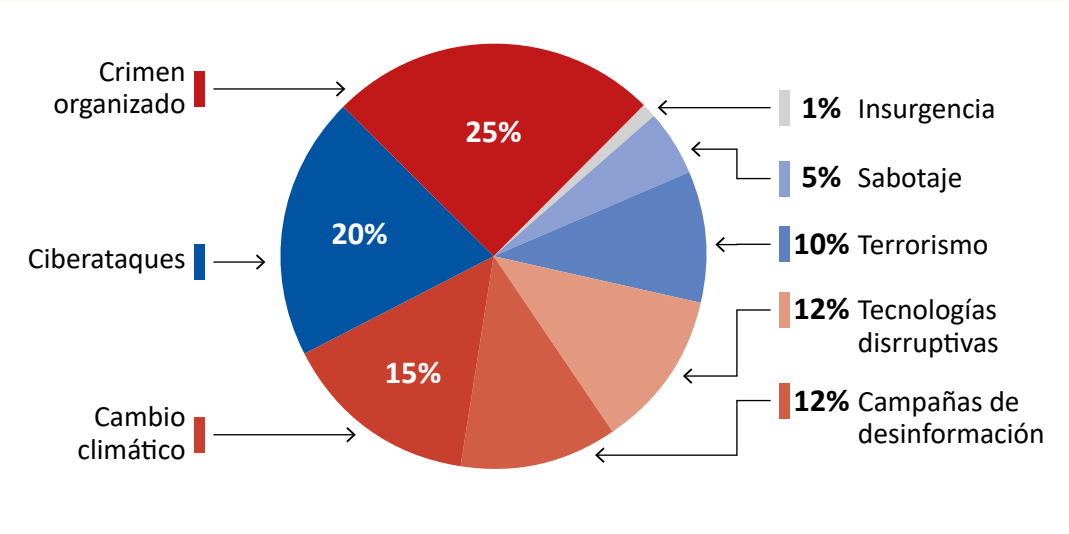
- Como resultado del proceso nacional, entre otras, ha sido la elaboración de documentos normativos cuyo objetivo ha sido abordar la temática de la IC de forma parcial o compartimentada. Pese a la transversalidad que ofrece el concepto no se identifica una estructura de gestión para la protección de sectores vitales y áreas sensibles, menos aún una estrategia que guie fórmulas y métodos para la protección de la IC a la luz de incidentes que se han manifestado con devastadoras consecuencias.

- En gráfico 2 y cuadro 2, respectivamente, se aprecia la magnitud de las amenazas, en términos de mayor incidencia perturbadora, que han afectado las estructuras nacionales y, del mismo modo, densidad normativa en que se ha abordado la codificación y sistematización de IC.

17 PDN. 2020. pp. 43–49. En: https://www.defensa.cl/wp-content/uploads/2023/06/POLÍTICA-DE-DEFENSA-NACIONAL-DE-CHILE-2020.pdf

18 BCN. Ley Nº 21.542. Loc. Cit.

Gráfico 2
Elementos perturbadores y amenazas a la IC de Chile en porcentaje de priorización



Fuente: Elaboración propia basado en Política de Defensa Nacional de Chile (2020) e incidencias de afectación.

Cuadro 2
Sectores de estratégicos de Infraestructura Crítica

Sector		Servicios
I	Energía, gas, agua	- Generación. - Transmisión. - Transporte. - Producción. - Almacenamiento. - Distribución.
II	Conexión vial, aérea, terrestre, portuaria o ferroviaria	- Conjunto de instalaciones. - Sistemas físicos. - Servicios esenciales
III	Servicios de utilidad pública (Asistencia sanitaria)	- Atención médica y hospitalaria. - Servicios esenciales.

Fuente: Elaboración propia basado en Ley Nº 21.542 de 3 de febrero, 2023.

- **Cotejando *IC nacionales a partir de lo establecido por la OCDE*[19]**

Como se ha señalado, para la OCDE el concepto "crítico" se refiere a instalaciones que, si se inutilizaran o destruyeran, provocaría daños catastróficos y de gran alcance afectando el desarrollo y bienestar. Por lo amplio del espectro conceptual, varios países concurrentes han establecido un catálogo de infraestructuras a las que el Estado debe proteger.

De esta manera, del análisis a los documentos publicados por la organización, se pueden identificar aquellas áreas estratégicas en que diferentes niveles de autoridades poseen atributos y responsabilidades para su resguardo. En palabras simples, se ha diseñado un sistema de protección de IC, estratificando áreas sensibles y sectores estratégicos para gestionar la respectiva protección. El cuadro 3 permite cotejar el listado de sectores críticos:

Cuadro 3
Cotejo de sectores esenciales e IC

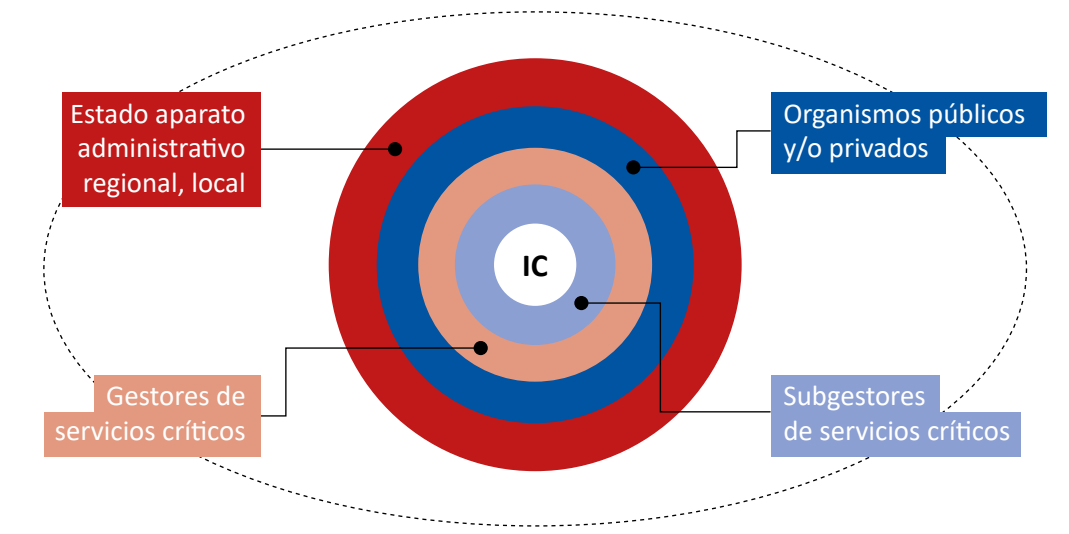
Comunidad Europea (Recomendaciones Comisión)	**OCDE Normas de IC**	**Chile (Políticas que refieren a IC)**
Energía	Energía	Energía (Electricidad, gas) **Ley nº** 21.542
Tecnologías, Comunicación e Información (TIC)	Comunicaciones, radio, televisión, correos	Tecnologías, Comunicación e Información (TIC) **Ley n° 18.168 – nº 20.478** (**PNCS**)
Agua	Agua y tratamiento	Agua **Ley nº** 21.542
Alimentación	Agricultura y alimentación	NO
Salud	Salud	Salud **Ley nº** 21.542
Financiero	Banca y finanzas	**Circular Bancos nº 2261** **CMF Resolución n°**3255
Orden y Seguridad Pública y Legal	Defensa	Ciberdefensa (**PCD**)
Administración Civil	NO	NO

19 OCDE. "*Protection of "critical infrastructure" and the role of investment policies relating to national security*". 2008. En: https://www.oecd.org/investment/investment-policy/40700392.pdf

Transporte	Transporte	Transporte (vial, aéreo, terrestre, portuario, ferroviario) **Ley nº** 21.542 **Decreto nº** 60
Industria química y nuclear	Industria química y petrolera	NO
Espacio e investigación	Transversales	NO

Fuente: Elaboración propia. Resumen conclusivo.

Imagen 1
Sistematización de gestores de protección de IC.



Fuente: Elaboración propia.

Conclusiones

Las diferentes aproximaciones conceptuales, normativas y metodológicas, que se han analizado apuntan a establecer que las IC se vinculan con instalaciones y sistemas que proveen servicios esenciales para un Estado. En dicha condición, su destrucción, alteración o mal funcionamiento provocarían afectaciones de amplio espectro. Este socavamiento se produce tanto en espacios individuales, organizacionales y estructurales, generando una brecha de vulnerabilidad a la seguridad nacional.

Considerando el espectro señalado, las IC establecidas por países signatarios de la OCDE y Comunidad Europea se identifican y agrupan de acuerdo al grado de sensibilidad, así como en sectores estratégicos. Dichos sectores constituyen parte medular de un mapa de riesgos y amenazas establecidas por el Estado. Por consiguiente, se precisa de una adecuada y actualizada inteligencia para la oportuna toma de decisiones de nivel central.

Para una adecuada gestión de la estratificación sectorial de la IC, y su consecuente delegación de responsabilidades, la experiencia acumulada por países de la Comunidad Europea, así como integrantes de la OCDE, se constata una preeminencia de un diseño de gestión centralizado en su control (Estado) y descentralizado para la ejecución (actores del sistema).

En el caso nacional, si bien se ha avanzado en normativas de protección de la IC y discusión de temáticas afines, se confirma que los instrumentos no logran generar una sincronización de la gestión de protección de IC. Esta condición se origina, principalmente, por la amplitud y ambigüedad de criterios que intentan abordar desde diferentes ordenanzas su conceptualización; por otra parte, a la falta de un catastro sectorial de estructuras sensibles y, finalmente, a la inexistencia de una fórmula que permita el control y coordinación de los actores del sistema. En otras palabras, la ausencia de un plan maestro y estrategias para la protección de la IC Nacional.

La fórmula establecida por la autoridad, conforme a la Ley Nº 21.542 y lo propuesto en el Mensaje Nº 122-371, deposita en las FF. AA. e instituciones de seguridad y policiales una prerrogativa superlativa para la protección de la IC. Dicho entorno se mantendrá hasta que no se diseñe una gobernanza que sincronice a los diferentes actores y servicios del sistema, sean públicos o privados. Así las cosas, las instituciones de la defensa y de seguridad podrían destinarse al resguardo de supermercados, farmacias, bancos o estaciones de combustible, antenas de radiocomunicación, entre otras instalaciones de carácter privado que se identifican como de alta sensibilidad o estratégicas.

La sensibilidad descrita requiere de normas explícitas, no solo para asegurar el actuar y empleo de la fuerza de instituciones encargadas del orden público o de defensa nacional, sino que demanda el desarrollo de capacidades de organismos civiles y del propio aparato público, tal como lo prescribe la CChC en su segundo informe.

La comunidad académica, en su rol de gestión del conocimiento y vinculación social, puede y debe contribuir significativamente en propuestas de políticas que faciliten una eficaz decodificación de la IC que impulse a superar las vulnerabilidades y brechas de las normativas evidenciadas. La base científica de estudios, promovida por investigadores especializados, constituyen un estadio de reconocida fuente de retroalimentación. Un entorno que, por ahora, se observa alejado de la discusión.

REFERENCIAS BIBLIOGRÁFICAS

BCN. "Circular Bancos *2261. Recopilación actualizada de normas"*. Capítulos 1-13 y 20-10 Gestión de la seguridad de la información y ciberseguridad. [en línea] [Fecha de consulta: 26 de mayo de 2024] En: https://www.bcn.cl/leychile/navegar?i=1150515&f=2020-07-06

BCN. Ley Nº 21.542. "*Modifica la carta fundamental con el objeto de permitir la protección de infraestructura crítica por parte de las fuerzas armadas, en caso de peligro grave o* inminente". Febrero, 2023. [en línea] [Fecha de consulta: 11 de mayo de 2024] En: https://www.bcn.cl/leychile/navegar?idNorma=1188583

CChC. Cámara Chilena de la Construcción. "*Informe Infraestructura Crítica para el Desarrollo"* (ICD) 2016-2025. 6 de abril de 2016. Pág. 6. [Fecha de consulta: 15 de mayo de 2024] Disponible En: http://www.cchc.cl/uploads/archivos/archivos/Infraestructura-Critica-para-el-Desarrollo_2016-2025.pdf

CMF. Capítulo 20-10 "*Gestión de seguridad de la información y ciberseguridad*". 2020. En: https://www.cmfchile.cl/portal/principal/613/articles-29310_doc_pdf.pdf

COMISIÓN DE LAS COMUNIDADES EUROPEAS. Libro Verde. "*Sobre un programa europeo para la protección de infraestructuras críticas".* Bruselas. 17.11.2005. Anexo 1, p. 22. [en línea] [Fecha de consulta: 20 de mayo de 2024] En: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0576:FIN:ES:PDF

COMISIÓN EUROPEA. "S*obre un enfoque coordinado de la Unión para reforzar la resiliencia de las infraestructuras críticas".* Estrasburgo, 18.10.2022. p. 1. [en línea] [Fecha de consulta: 20 de mayo de 2024] En: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52022DC0551

COMISIÓN EUROPEA. "*Critical Infrastructure Protection in the fight against terrorism*". Brussels, 20.10.2004 COM (2004) 702 final, de 20 de octubre de 2004. En: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0702:FIN:EN:PDF

MENSAJE Nº 122-371. "*Proyecto de ley, iniciado en Mensaje de S.E. el Presidente de la República para la protección de la infraestructura crítica del país*". 01 agosto, 2023. En: https://www.doe.cl/alerta/04082023/20230804034

MINDEF. PDN. 2020. pp. 43–49. [en línea] [Fecha de consulta: 17 de mayo de 2024] En: https://www.defensa.cl/wp-content/uploads/2023/06/POLÍTICA-DE-DEFENSA-NACIONAL-DE-CHILE-2020.pdf

MINDEF. Ley Nº 42.003. Política de Ciberdefensa. 9 de marzo de 2018. [en línea] [Fecha de consulta: 15 de mayo de 2024] Disponible En: http://www.diariooficial.interior.gob.cl/publicaciones/2018/03/09/42003/01/1363153.pdf

OCDE. "*Recomendación del Consejo sobre la gobernanza de infraestructuras*", OECD/LEGAL/0460, p. 6, 2020. En: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0460

OECD. "*Recomendación del Consejo sobre la Gobernanza de Riesgos Críticos*". 6 de mayo de 2014. En: https://www.oecd.org/gov/risk/Critical-Risks-Recommendation-Spanish.pdf

PNCS. Política Nacional de Ciber Seguridad, 2017 - 2022. p. 16. [en línea] [Fecha de consulta: 15 de mayo de 2024] En: https://biblioteca.digital.gob.cl/server/api/core/bitstreams/b5b26f36-2c47-441b-8848-00d767ec9b5c/content

PNCS. Política Nacional de Ciber Seguridad, 2023–2028. p. 7. [en línea] [Fecha de consulta: 15 de mayo de 2024] En: https://www.diariooficial.interior.gob.cl/publicaciones/2023/12/04/43717/01/2415658.pdf

UE. Directiva 2008/114/CE del Consejo de la UE. "*Sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección"*. 8 diciembre 2008. [en línea] [Fecha de consulta: 20 de mayo de 2024] En: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32008L0114