Modelo de gobernanza para la protección de infraestructura crítica en el país

Autor

Juan Pablo Jarufe Bader
Email: jjarufe@bcn.cl
Tel.: (56) 32 226 3173
(56) 22 270 1850

Nº SUP: 141125

Resumen

El tránsito hacia una arquitectura de resguardo a la infraestructura crítica en Chile debiese considerar algunos elementos ya presentes en otras latitudes, entre los cuales es posible mencionar:

- Un tratamiento sectorial, como el recogido por el artículo 7 de la *Loi relative à la Sécurité et la Protection des Infrastructures Critiques*, de 2011, conforme al cual cada autoridad pública en Bélgica debe emitir un listado de infraestructuras críticas potencialmente susceptibles de ser atacadas, acompañado de un plan de seguridad preventivo, una proyección de escenarios y un análisis de vulnerabilidades, tendientes a neutralizar los riesgos de interrupción del servicio o de destrucción de instalaciones sensibles para el Estado.

- Un esquema con una asignación clara de roles y responsabilidades, junto a un sistema de alertas, notificaciones y respuestas ante eventos críticos, con horizontes de corto, mediano y largo plazo, así como instancias de cooperación internacional, tal cual lo ha desarrollado Colombia, a partir de su Plan Nacional de Protección de Infraestructura Critica Cibernética.

- La alianza público-privada, como elemento clave para configurar un modelo sistémico e integrado de resguardo a la infraestructura crítica nacional, que está recogido en el artículo 5 de la Ley Nro. 8, de 2011, que consagra en España la existencia de un Sistema de Protección de Infraestructuras Críticas, articulado en torno a un Centro Nacional para la Protección de las Infraestructuras Críticas, en el cual coexisten y trabajan mancomunadamente actores de ambas esferas.

- El reforzamiento del trabajo interagencial, tal cual aparece reforzado en el caso de EE.UU., donde los sectores de infraestructura crítica son cautelados por el llamado *National Infrastructure Coordinating Center*.

- La concientización de los ciudadanos en cuanto al uso correcto del ciberespacio, un aspecto que aparece desarrollado con nitidez en Nueva Zelandia, donde la Estrategia de Ciberseguridad está acompañada de un programa de trabajo con un reporte anual ministerial, que busca combatir proactivamente el cibercrimen, consolidar una cultura de la ciberseguridad, y estimular el desarrollo de una comunidad académica e investigativa vinculada con la industria.

Introducción

El presente informe esboza algunas de las características esenciales que podría asumir un modelo de gobernanza en materia de protección de infraestructura crítica en Chile, a la luz de la evidencia internacional de países que ya han regulado en profundidad esta materia.

I. Hacia un modelo nacional de gobernanza en infraestructura crítica

Hacia 2004, la Comisión Europea definió a la infraestructura crítica como (Comisión Europea, 2004. En Horzella, B., 2024: 2):

"(…) aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información, cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos, o en el eficaz funcionamiento de los gobiernos de los estados miembros. Las infraestructuras críticas se extienden a través de muchos sectores de la economía, incluyendo la banca y finanzas, el transporte y la distribución, la energía, los servicios públicos, la salud, el suministro de alimentos, y las comunicaciones, así como los servicios gubernamentales claves".

Cuatro años más tarde, el Consejo Europeo, a partir de su Directiva 114, de 2008, la conceptualizó como (Consejo Europeo, 2008. En Horzella, B, 2024: 2):

"(…) 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, cuya perturbación o destrucción afectaría gravemente a un estado miembro, al no poder mantener esas funciones".

En cuanto al esquema que podría adoptar un modelo de gobernanza en este ámbito en el país, bien valdría traer a la luz algunos de los elementos ya presentes en otras latitudes.

Es así como una fórmula en este sentido debería tener en consideración un tratamiento sectorial, como el recogido por el artículo 7 de la *Loi relative à la Sécurité et la Protection des Infrastructures Critiques*, de 2011, conforme al cual cada autoridad pública en Bélgica debe emitir un listado de infraestructuras críticas potencialmente susceptibles de ser atacadas, acompañado de un plan de seguridad preventivo, una proyección de escenarios y un análisis de vulnerabilidades, tendientes a neutralizar los riesgos de interrupción del servicio o de destrucción de instalaciones sensibles para el Estado (*Loi relative à la Sécurité et la Protection des Infrastructures Critiques*, 2011).

En la misma línea, una arquitectura que robustezca la protección de la infraestructura crítica nacional tendría que tener en cuenta una asignación clara de roles y responsabilidades, junto a un sistema de alertas, notificaciones y respuestas ante eventos críticos, con horizontes de corto, mediano y largo plazo, tal cual lo ha desarrollado Colombia, a partir de su Plan Nacional de Protección de Infraestructura Critica Cibernética (Plan Nacional de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia, 2017: 8).

En esta directriz, el objetivo principal es identificar a los responsables y definir un esquema de coordinación, en el ánimo de activar y articular las capacidades estratégicas y operativas de las instituciones del Estado, apuntando a optimizar la prevención, alistamiento y respuesta ante el riesgo, robusteciendo la resiliencia y aportando al fortalecimiento del desarrollo económico, la seguridad y la defensa nacional del país en el plano ciberespacial.

Entre los objetivos específicos, en tanto, aparecen (Plan Nacional de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia, 2017: 9-10):

- El establecimiento de una estructura intersectorial para conducir o coordinar actuaciones necesarias para proteger las infraestructuras críticas cibernéticas, a objeto de movilizar y articular las capacidades logísticas, operativas y técnicas para la toma de decisiones y respuestas frente a incidentes cibernéticos.

- La identificación y análisis de amenazas, vulnerabilidades, impactos e incidencia de ataques cibernéticos sobre la infraestructura crítica nacional, para determinar los niveles de seguridad y los criterios de activación de acciones de respuesta.

- La fijación de fórmulas para prevenir y reportar incidentes, gestionar crisis, respuestas y recuperación para la protección de la infraestructura crítica ciberespacial.

- El estímulo a la generación de conocimiento, sustentado en la colaboración intersectorial.

- El mejoramiento de la capacidad de resiliencia cibernética, por medio de la planificación anticipada y el uso de mecanismos de protección, para una pronta recuperación de los servicios esenciales.

Este plan es elaborado, gestionado y salvaguardado por el Ministerio de Defensa, mediante el Grupo de Respuesta a Emergencias Cibernéticas, el Comando Conjunto Cibernético y el Centro Cibernético Policial, siendo objeto de revisión cada cuatro años (Plan Nacional de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia, 2017: 17).

Por último, un elemento adicional que ha aportado valor a esta cadena es la cooperación internacional con actores como la Organización del Tratado del Atlántico Norte (OTAN), así como la búsqueda de nuevos desarrollos en materia de investigación, recursos humanos, adiestramiento con otras fuerzas nacionales y doctrina conjunta.

La alianza público-privada es otro elemento clave para configurar un modelo consistente, sistémico e integrado de resguardo a la infraestructura crítica nacional, como bien lo recoge el paradigma español. Al respecto, el artículo 5 de la Ley Nro. 8, de 2011, consagra en este país europeo la existencia de un Sistema de Protección de Infraestructuras Críticas, articulado en torno a un Centro Nacional para la Protección de las Infraestructuras Críticas, en el cual coexisten y trabajan mancomunadamente actores de ambas esferas, cuya labor se concentra, a su vez, en la asesoría al Secretario de Estado de Seguridad, adscrito al Ministerio del Interior, así como en la coordinación entre las reparticiones públicas y los gestores de infraestructuras esenciales para el funcionamiento del país (Ley Nro. 8, 2011: 2-3).

El reforzamiento del trabajo interagencial es otro factor a considerar, tal cual aparece reforzado en el caso de Estados Unidos (EE.UU.), donde los sectores de infraestructura crítica son cautelados por el llamado *National Infrastructure Coordinating Center* (NICC), entidad que forma parte de la División de Seguridad e Infraestructura de la *Cybersecurity and Infrastructure Security Agency* (CISA), así como del Centro de Operaciones Nacionales, del Departamento de Seguridad Interior, con un funcionamiento permanente y coordinado, que permite compartir la información situacional sobre la infraestructura crítica del gobierno federal.

En caso de algún incidente contra estos reductos, el NICC se encarga de aglutinar los esfuerzos de colaboración entre el Departamento de Seguridad Interior y los operadores del rubro afectado *(Cybersecurity & Infrastructure Security Agency*, 2024).

Por último, otro elemento a tener en cuenta es el de la formación y concientización de los ciudadanos, en cuanto al correcto uso del ciberespacio, un aspecto que aparece desarrollado con nitidez en Nueva Zelandia, donde la Estrategia de Ciberseguridad está acompañada de un programa de trabajo con un reporte anual ministerial, que busca combatir proactivamente el cibercrimen; consolidar una cultura de la ciberseguridad, con énfasis en grupos más vulnerables, como los menores de edad y los adultos mayores; a la vez que estimular el desarrollo de una comunidad académica e investigativa vinculada con la industria (*New Zealand's Cyber Security Strategy*, 2019: 11-15).

Referencias

Comisión Europea. (2004). Protección de Infraestructura Crítica y Fuerzas Armadas. Conceptualización y experiencia comparada. En Horzella, Bárbara. [2024, marzo 26]. BCN. Disponible en: http://bcn.cl/2lf8z.

Consejo Europeo. (2008). Protección de Infraestructura Crítica y Fuerzas Armadas. Conceptualización y experiencia comparada. En Horzella, Bárbara. [2024, marzo 26]. BCN. Disponible en: http://bcn.cl/2lf8z.

Cybersecurity & Infrastructure Security Agency. (2024, marzo 26). *National Infrastructure Coordinating Center*. Disponible en: https://www.cisa.gov/national-infrastructure-coordinating-center.

Ley Nro. 8, por la que se establecen Medidas para la Protección de las Infraestructuras Críticas. (2011, abril 28). Disponible en: http://bcn.cl/33h65.

Loi relative à la Sécurité et la Protection des Infrastructures Critiques. (2011, julio 1). Disponible en: https://centredecrise.be/sites/default/files/documents/files/2021-03/PDFsam_15_2.pdf.

New Zealand's Cyber Security Strategy. (2019). Disponible en: http://bcn.cl/2lkwg.

Plan Nacional de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia. (2017). Disponible en: http://bcn.cl/33h6c.