Boletín N° 14.732-02

Proyecto de ley, iniciado en moción de los Honorables Senadores señor Pugh, señoras Aravena y Rincón y señores Araya y Elizalde, que instituye el mes de noviembre como el "Mes Nacional de la Infraestructura Crítica y su Resiliencia".

I.- Fundamentos del proyecto

La Política de Ciberdefensa del Estado de Chile, publicada en el Diario Oficial el 9 de marzo de 2018, define a las **Infraestructuras Críticas de la Información (ICI)** como 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. En efecto, estas infraestructuras se han puesto de relieve a partir del creciente uso de las tecnologías de la información, junto al vertiginoso desarrollo de la digitalización -fenómeno de alcance mundial-, y también frente al aumento de fenómenos meteorológicos extremos, lo que implica un desafío para la seguridad de los países, en orden a resguardar sus ICI para el mantenimiento de prestaciones sociales básicas o esenciales[1], ya sea de bienes o servicios, que se encuentran expuestas a vulneraciones que pueden producir graves afectaciones a la seguridad, la salud o la convivencia social de la población.

Nuestra Política Nacional de Ciberseguridad, de abril de 2017, considera dentro de sus objetivos de política para el año 2022, en su letra A., el contar con una infraestructura de la información robusta y resiliente, preparada para resistir y recuperarse de incidentes de ciberseguridad, bajo una óptica de gestión de riesgos, incorporando para ello la protección de dichas infraestructuras, la identificación y jerarquización de las mismas, la existencia de equipos de respuesta a incidentes de ciberseguridad (CSIRT Nacional)[2], la implementación de mecanismos estandarizados de reporte, gestión y recuperación de incidentes, como también la evaluación de sus riesgos y la gestión de acuerdo a estándares que contemplen la confidencialidad, integridad y disponibilidad de la ICI, junto con la prevención, manejo y recuperación de ciberataques y otros incidentes de seguridad informática, y planes de contingencia para asegurar la continuidad operativa de sus servicios.

Lo anterior requiere sin duda un impulso desde el propio Estado, que en nuestro caso ha elevado la importancia de esta materia a la categoría de defensa de la soberanía del país; así lo establece la referida Política de Ciberdefensa, declarando en su introducción que La Política de Ciberdefensa complementa a la de Ciberseguridad en aquellos aspectos relacionados directamente con la defensa de la soberanía del país a través de las redes digitales, con la protección de nuestra infraestructura crítica de información, y con la protección de los derechos humanos de todas las personas que habitan en nuestro territorio; y reafirma dicho concepto al referirse a la aplicación de las políticas de la Defensa Nacional al ciberespacio, señalando que El Estado de Chile protegerá su infraestructura crítica de la información, ejerciendo su soberanía sobre aquellas redes y recursos digitales. La Defensa Nacional se ocupará de identificar la ocurrencia de ataques, facilitar o permitir su correcta atribución a otros Estados o grupos no estatales, aplicar las contramedidas adecuadas, y dar cumplimiento a la obligación internacional

[1] Por ejemplo, servicios sanitarios, de telecomunicaciones, de energía, de salud, de defensa, financieros, administrativos, de transporte, de protección civil, entre otros.

[2] https://www.csirt.gob.cl/

de identificar y detener los ataques que otros países puedan realizar a través de su infraestructura de información.

De la misma forma en que la ciberseguridad requiere del fomento y desarrollo tanto de una cultura asociada a ella, como de una industria que sirva a sus objetivos estratégicos[3], la protección de la Infraestructura Crítica de la Información y su Resiliencia requieren de un constante ejercicio en torno a la educación, buenas prácticas, responsabilidad, prevención y generación de capacidades de respuesta ante situaciones adversas, que permitan, como se dijo, la continuidad de los servicios esenciales para el bienestar y la seguridad de la ciudadanía. Como prueba de ello, los países que han logrado estándares aceptables en el desarrollo de esta materia, consideran dentro de su Sistema Nacional de Ciberseguridad una institucionalidad adecuada a dichos fines, como es el caso del Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC) de España.

En la experiencia comparada, además, se han adoptado sucesivas y continuas medidas en orden a incorporar y mantener la protección de la infraestructura crítica como una prioridad estratégica. Por ejemplo, el pasado 29 de octubre de 2021, el Presidente de Estados Unidos, Joseph Biden, proclamó a noviembre como el Mes de la Seguridad de la Infraestructura Crítica y su Resiliencia en dicho país, haciendo un llamado a la ciudadanía para que reconozca la importancia de proteger la infraestructura de la nación y para destinar ese mes a observar las medidas apropiadas para mejorar la seguridad y resiliencia nacional[4]; mismo espíritu contenido en los principios que invoca la Agencia de Seguridad de Infraestructura y Ciberseguridad estadounidense (CISA), al señalar que Cada noviembre se celebra como el Mes de la Seguridad de la Infraestructura (…) es el esfuerzo anual de la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) para educar e involucrar a todos los niveles de gobierno, propietarios y operadores de infraestructura (…) sobre el papel vital que desempeña la infraestructura crítica en el bienestar de la nación y por qué es importante fortalecer su seguridad y resiliencia[5].

En el caso en comento, contar con un mes que concentra los esfuerzos en orden a concientizar en esta materia, es una instancia que otorga la oportunidad de dar a conocer los recursos y las medidas clave que pueden adoptar las organizaciones y la ciudadanía, además de las iniciativas que influyen en el futuro de la seguridad y la resiliencia de las infraestructuras críticas, incluyendo la nueva legislación, la política y la doctrina. Los beneficios de dicho ejercicio alcanzan ámbitos tan importantes y sensibles como (i) el compartir información sobre las mejores prácticas, realizar evaluaciones para identificar las vulnerabilidades, crear asociaciones en la comunidad de infraestructuras críticas, ofrecer formación y proporcionar herramientas a las partes interesadas en las infraestructuras críticas, (ii) contribuir a la seguridad de la democracia mediante la creación de una mayor resiliencia en el proceso electoral, (iii) reconocer la experiencia y las capacidades únicas de los sectores gubernamental, privado y sin fines de lucro e integrarlos en el esfuerzo nacional para aumentar la resiliencia de las infraestructuras críticas del país, entre otros.

En Chile se ha abierto y destinado un espacio para la promoción y realización de ejercicios nacionales en materia de ciberseguridad, mediante la dictación de la Ley N° 21.113, que declaró el mes de octubre de cada año como el "Mes Nacional de la

[3] Objetivos C y E de la Política Nacional de Ciberseguridad.
[4] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/10/29/a-proclamation-on-critical-infrastructure-security-and-resilience-month-2021/
[5] https://www.cisa.gov/infrastructure-security-month

Ciberseguridad", y que se publicó precisamente el 1 de octubre del año 2018, completando a la fecha cuatro versiones en que se ha puesto de relieve la importancia en la concientización de dicha materia y su desarrollo en el país. La protección y resguardo de la Infraestructura Crítica es también objeto de algunos proyectos de ley que actualmente se encuentran en tramitación en el Congreso Nacional[6], que, si bien se refieren a casos específicos o coyunturales para su procedencia, dan cuenta de la preocupación que ya existe sobre la materia. En la misma línea, cabe destacar la dictación de la Ley N° 20.478, en diciembre de 2010, sobre recuperación y continuidad en condiciones críticas y de emergencia del sistema público de telecomunicaciones, que incorporó a la Ley N° 18.168, General de Telecomunicaciones, un Título VIII, “De las Infraestructuras Críticas de Telecomunicaciones”.

Si bien dichos hitos constituyen avances, nuestro país requiere ser un actor y no un mero espectador en esta materia; para ello, debe generar las condiciones y las instancias necesarias para fomentar y ampliar el ámbito de interés hacia una cultura de protección de las ICI que permita lograr estándares adecuados de desarrollo, seguridad y resiliencia de las mismas. Las infraestructuras críticas de la información proporcionan servicios esenciales que la ciudadanía utiliza a diario, y en la actualidad se constituyen como uno de los pilares de la seguridad institucional y social de los países.

II.- Objetivo y contenido del proyecto de ley

El presente proyecto de ley tiene por objetivo instituir al mes de noviembre de cada año, como el “Mes Nacional de Ia Infraestructura Crítica y su Resiliencia”, proveyendo así de un periodo de tiempo adecuado, durante dicho mes, para poder efectuar actividades de concientización, compartir información, realizar ejercicios nacionales, participar en asociaciones y fomentar la cooperación, difundir conocimiento, generar el encuentro de los diferentes actores nacionales, tanto públicos como privados, involucrados en el desarrollo de esta materia, y mantener la periodicidad para enfrentar de forma coordinada y actualizada las múltiples amenazas que afectan a la Infraestructura Crítica, que requieren de a lo menos una instancia anual para comprobar las capacidades y los avances logrados en el país.
Por todo lo anterior, venimos en presentar a este Honorable Senado, el siguiente

PROYECTO DE LEY

Artículo único. – Institúyese el mes de noviembre de cada año, como el “Mes Nacional de la Infraestructura Crítica y su Resiliencia”, con el fin de promover el desarrollo de las capacidades nacionales para fortalecer la seguridad y resiliencia de las infraestructuras críticas.

[6] Boletines 13.086-07, 13.087-07, 13.088-02 y 13.085-07.