Exigencias a directores de empresas de infraestructura crítica a nivel internacional

Autor

Juan Pablo Jarufe Bader
Email: jjarufe@bcn.cl
Tel.: (56) 32 226 3173
(56)222701850

Nº SUP: 137403

Resumen

De acuerdo al Consejo Europeo, la infraestructura crítica puede ser concebida 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, cuya perturbación o destrucción afectaría gravemente a un estado miembro, al no poder mantener esas funciones”.

Respecto al nivel de preparación de los directores de empresas esenciales australianas, el artículo 30AC de la *Security of Critical Infrastructure Act*, de 2018, les entrega la misión de implementar un programa de gestión de riesgos de infraestructura crítica.

En Colombia, en tanto, el artículo 2.2.21.1.4.2 del Decreto 338, de 2022, dispone que las autoridades titulares de infraestructura crítica, presenten un plan de seguridad digital, protección de redes, infraestructuras críticas cibernéticas y de sistemas de información ciberespacial, para lo cual deben actualizar periódicamente sus evaluaciones de riesgo digital.

Por su parte, la regulación española incluye en el artículo 13 de la Ley 8, de 2011, por la que se establecen Medidas para la Protección de las Infraestructuras Críticas, a los operadores críticos dentro del Sistema de Protección de Infraestructuras Críticas del país, para que coadyuven con las autoridades gubernamentales en la optimización de los mecanismos que permitan cautelar estos activos. Para esto, se les exige asesorar al Ministerio del Interior, mediante el Centro Nacional de Protección de Infraestructuras Críticas, en el análisis de los activos esenciales, renovando cada año la información disponible; contribuir al diseño de planes estratégicos sectoriales y a la elaboración de análisis de riesgos; y nombrar a un Responsable de Seguridad y Enlace, así como a un Delegado de Seguridad para cada una de las empresas de infraestructura.

Finalmente, en Singapur, el artículo 15 de la *Cybersecurity Act*, de 2018, obliga al director de un activo esencial a ordenar, al menos cada dos años, una auditoría que dé cuenta del nivel de cumplimiento de las prácticas y estándares de rendimiento asociados a infraestructura crítica.

Introducción

El presente informe da cuenta de los requisitos exigidos legalmente a directores de compañías de infraestructura crítica en la experiencia internacional.

El documento comienza por definir el concepto mismo de infraestructura crítica, para luego concentrarse en los paradigmas de Australia, Colombia, España y Singapur, que registran alguna clase de evidencia sobre esta materia.

I. Aproximación al concepto de infraestructura crítica

A nivel internacional, la infraestructura crítica ha sido conceptualizada desde diversas ópticas.

Al respecto, en 2004 la Comisión Europea la vinculó con (Comisión Europea, 2004. En Horzella, B., 2019: 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 clave.

Cuatro años más tarde, el Consejo Europeo, a partir de su Directiva 114, de 2008, la conceptualizó como (Ibíd., 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.

II. Requisitos para directores de infraestructura crítica. Experiencia internacional

Según Jorge Atton, ex Delegado Presidencial de Ciberseguridad, los directores de las firmas de infraestructura crítica tienen que promover la formación de una cultura empresarial de ciberseguridad, atendiendo a elementos como la certificación de niveles de ciberseguridad de los sistemas digitales, y la supervigilancia activa de las modificaciones normativas y las prácticas internacionales (Inteligencia Digital, 2020).

Por su parte, el *EY Center for Board Matters* ha establecido que los directorios necesitan enfocarse en objetivos como la comprensión de las ciberamenazas que enfrenta su organización y la seguridad de la información que reciben (Lehuedé, H., 2020: 35).

Estas aproximaciones denotan una preocupación por el rol de los directores de firmas ligadas a infraestructura crítica, en cuanto a la preparación y los conocimientos que deben asumir frente a las ciberamenazas. Un interés que se ha plasmado en algunos ordenamientos legales, como los de los países que se repasan a continuación.

1. Australia

En la experiencia australiana, el artículo 8D de la *Security of Critical Infrastructure Act*, de 2018, considera como partes del entramado de infraestructura crítica, a los sectores de comunicaciones, procesamiento de datos, servicios financieros, servicios sanitarios, energía, salud, educación superior, investigación, alimentación, transporte, tecnología espacial e industria de la defensa.

En este contexto, el artículo 30AC de la norma, les entrega a los responsables de cada empresa ligada a estos rubros, la misión de implementar un programa de gestión de riesgos de infraestructura crítica.

En la misma línea, el artículo 30AF llama a estos ejecutivos a mantener actualizado este plan; mientras el artículo 30AG obliga a estos personeros a emitir un reporte anual dentro de un plazo de noventa días desde el fin del año financiero, incorporando información asociada a los riegos que tuvieron un impacto significatuivo sobre uno o más activos durante el período en cuestión, así como una evaluación de la efectividad de las medidas adoptadas (*Security of Critical Infrastructure Act*, 2018).

2. Colombia

Respecto al modelo colombiano, el artículo 2.2.21.1.4.2 del Decreto 338, de 2022, dispone que las autoridades titulares de infraestructura crítica, o que desarrollen servicios calificados como esenciales para el Estado, deben relacionarse con el Ministerio de Tecnologías de la Información y las Comunicaciones, así como con el Grupo de Respuesta a Emergencias Cibernéticas.

En esta línea, el artículo siguiente les mandata a presentar un plan de seguridad digital, protección de redes, infraestructuras críticas cibernéticas y de sistemas de información ciberespacial, para lo cual deben actualizar periódicamente sus evaluciones de riesgo digital.

Además, se les exige certificar regulaciones, directrices, elementos técnicos, administrativos y humanos, para gestionar de manera eficiente los peligros, a la vez que conformar equipos de respuesta ante incidentes sectoriales de seguridad cibernética (artículo 2.2.21.1.5.4) (Decreto 338, 2022: 13-14).

3. España

En cuanto a España, el artículo 2 de la Ley 8, de 2011, por la que se establecen Medidas para la Protección de las Infraestructuras Críticas (norma actualizada el 29 de julio de 2022), define a estas últimas como aquellas “cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales del país” (Ley 8, 2011).

Por su parte, el artículo 13 de la norma incluye a los operadores críticos dentro del Sistema de Protección de Infraestructuras Críticas del país, para que coadyuven con las autoridades gubernamentales en la optimización de los mecanismos que permitan cautelar estos activos. Para esto, se les exige (Ley 8, 2011):

- Asistir a nivel técnico al Ministerio del Interior, mediante el Centro Nacional de Protección de Infraestructuras Críticas (CNPIC), en el análisis de los activos esenciales, renovando cada año la información disponible, a solicitud de la mencionada cartera.
- Contribuir al diseño de planes estratégicos sectoriales y a la elaboración de análisis de riesgos referidos a las diferentes áreas estratégicas.
- Preparar el Plan de Seguridad del Operador, en consonancia con los dictámenes reglamentarios de la autoridad, previa certificación.
- Elaborar un plan de protección específico por cada infraestructura crítica.
- Nombrar a un Responsable de Seguridad y Enlace, así como a un Delegado de Seguridad para cada una de las empresas de infraestructura.

- Colaborar con las fiscalizaciones oficiales, que busquen acreditar el cumplimiento de la ley y de las medidas de seguridad.
- Conformar un área de seguridad del operador.

Las obligaciones y responsabilidades del representante de cada empresa, están determinadas por la actuación del CNPIC, que hace las veces de intermediario ante el Ministerio del Interior.

Por último, el artículo 18 le entrega al operador crítico la responsabilidad de avalar la seguridad de la información clasificada, que se vincule con los propios activos esenciales.

4. Singapur

En el caso de Singapur, los servicios esenciales están vinculados al sector energético, las comunicaciones, los servicios sanitarios, la salud, el sector financiero, la defensa civil, las prestaciones de seguridad, los servicios de inmigración y la aeronavegación.

De acuerdo al artículo 10 de la *Cybersecurity Act*, de 2018, las autoridades oficiales del país pueden solicitar al operador de una infraestructura crítica, información sobre el diseño, configuración y seguridad de los activos esenciales bajo su dirección, así como respecto a los cambios que puedan afectar la ciberseguridad de la infraestructura crítica de la información.

El artículo 15, en tanto, obliga al director de un activo esencial a ordenar, al menos cada dos años, una auditoría que dé cuenta del nivel de cumplimiento de las prácticas y estándares de rendimiento asociados a infraestructura crítica.

Asimismo, el artículo siguiente dispone que la autoridad gubernamenal puede conducir ejercicios de ciberseguridad para probar el estado de preparación de los directores de las diferentes infraestructuras críticas, en respuesta ante ciberincidentes.

Finalmente, el artículo 22 de la norma establece la posibilidad de que el gobierno designe a un experto técnico en ciberseguridad, por un período específico, para apoyar la respuesta ante incidentes (*Cybersecurity Act*, 2018).

Referencias

Comisión Europea. (2004). En Horzella, Bárbara. [2019, diciembre]. Protección de Infraestructura Crítica y Fuerzas Armadas. Conceptualización y experiencia comparada. BCN. Disponible en: http://bcn.cl/2lf8z.

Inteligencia Digital. (2020, septiembre 26). Los desafíos de ciberseguridad para los directorios de empresas. Disponible en: http://bcn.cl/3c03w.

Lehuedé, Héctor. (2020). *Cybersecurity and the role of the Board of Directors in Latin America and the Caribbean*. ECLAC. Disponible en: http://bcn.cl/3c03t.

Textos normativos

Cybersecurity Act. (2018, marzo 12). Disponible en: http://bcn.cl/3c02f.

Decreto 338. (2022, marzo 8). Disponible en: http://bcn.cl/3c046.

Ley 8, por la que se establecen Medidas para la Protección de las Infraestructuras Críticas. (2011, abril 28). Disponible en: http://bcn.cl/3c1ht.

Security of Critical Infrastructure Act. (2018). Disponible en: http://bcn.cl/3c1hg.