Infraestructura crítica en la experiencia internacional

Autor

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

Nº SUP: 141234

Resumen

De acuerdo al artículo 2 de la Directiva (UE) 2557 del Parlamento Europeo, de 14 de diciembre de 2022, se entiende por infraestructura crítica a todo elemento, instalación, equipo, red o sistema, o parte de ellos, que sea necesario para la prestación de un servicio esencial, vale decir, aquel considerado crucial para el mantenimiento de las funciones sociales vitales, las actividades económicas, la salud pública, la seguridad o el medio ambiente.

A su vez, el artículo 1 de este texto obliga a los Estados miembros a identificar las entidades críticas y respaldarlas, fijando deberes para que robustezcan su resiliencia y capacidad para cumplir con la prestación de servicios que la ley les encomienda.

En el ejemplo colombiano, el Plan Nacional de Protección de Infraestructura Critica Cibernética define un marco de gobierno, roles y responsabilidades, además de un conjunto de niveles de alertas, actuaciones, notificaciones y respuestas frente a eventos de ciberseguridad asociados a sectores críticos.

Corea del Sur, en tanto, cuenta con la *Act on the Protection of Information and Communications Infrastructure*, cuyo fin es operar de forma estable la infraestructura de información crítica y comunicaciones, formulando e implementando medidas alusivas a la protección de dichas instalaciones, de modo que puedan hacer frente a cualquier intrusión por medios electrónicos.

A su vez, España posee un Sistema de Protección de Infraestructuras Críticas, que se articula en torno a la conformación del Centro Nacional para la Protección de las Infraestructuras Críticas, orgánica en la cual coexisten y trabajan mancomunadamente actores públicos y privados, cuya labor se concentra, a su vez, en la asesoría al Secretario de Estado de Seguridad, así como en la coordinación entre las reparticiones públicas y los gestores de infraestructuras esenciales para el funcionamiento del país.

Estonia, por su parte, ha desarrollado la noción de *Critical Information Infrastructure Protection*, principio que busca mantener un funcionamiento libre de problemas a los sistemas esenciales de información y comunicación; mientras respecto a Singapur, el artículo 10 de la *Cybersecurity Act*, de 2018, establece que 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.

Introducción

El presente informe busca definir el concepto de infraestructura crítica y sus mecanismos de resguardo, a la luz de la experiencia internacional.

El documento recoge la evidencia presente en la Unión Europea, así como en la legislación interna de países como Colombia, Corea del Sur, España, Estonia, Nueva Zelandia, Reino Unido y Singapur.

El texto incorpora datos de los informes BCN "Exigencias a directores de empresas de infraestructura crítica a nivel internacional", "Ciberseguridad e infraestructura crítica: los casos de Bélgica, Estonia, Italia y la UE" y "Centros de Protección de Infraestructura Crítica. Experiencia internacional", elaborados por el mismo autor del presente documento.

I. Aproximación general

De acuerdo al artículo 2 de la Directiva (UE) 2557 del Parlamento Europeo, de 14 de diciembre de 2022, se entiende por infraestructura crítica a todo elemento, instalación, equipo, red o sistema, o parte de ellos, que sea necesario para la prestación de un servicio esencial, vale decir, aquel considerado crucial para el mantenimiento de las funciones sociales vitales, las actividades económicas, la salud pública, la seguridad o el medio ambiente.

A su vez, el artículo 1 de este texto obliga a los Estados miembros a identificar las entidades críticas y respaldarlas, fijando deberes para que robustezcan su resiliencia y capacidad para cumplir con la prestación de servicios que la ley les encomienda.

Enseguida, el artículo 4 de la norma establece el 17 de enero de 2026 como plazo para que los Estados miembros implementen una estrategia actualizable al menos cada cuatro años, que permita incrementar la resiliencia de sus organismos críticos. Esta directriz tiene que contener (Directiva (UE) 2557 del Parlamento Europeo y del Consejo, 2022):

"(…) objetivos estratégicos y medidas de actuación, basándose en estrategias nacionales y sectoriales, planes o documentos similares existentes en la materia, teniendo en cuenta las dependencias e interdependencias transfronterizas e intersectoriales; así como un marco de gobernanza para alcanzar los objetivos estratégicos y las prioridades, incluida una descripción de las funciones y responsabilidades de las diferentes autoridades y entidades críticas".

En este contexto, el artículo siguiente dispone que el análisis de riesgo de cada país considere las amenazas naturales y antrópicas, así como los peligros intersectoriales o transfronterizos, los accidentes, las emergencias de salud pública y las amenazas híbridas, incluyendo el terrorismo.

Ahora bien, ante la ocurrencia de un incidente contra un activo esencial, el artículo 15 determina que las entidades críticas del Estado presenten, en un plazo no superior a un día, una notificación inicial, que luego dé paso a un reporte detallado, que permita dimensionar la magnitud de la perturbación, conforme a estándares como el porcentaje de usuarios afectados, el tiempo de interrupción del servicio y el territorio afectado.

Finalmente, el artículo 19 contempla la existencia de un Grupo de Resiliencia de las Entidades Críticas, integrado por representantes de los Estados miembros y de la Comisión Europea, con la función de apoyar a este último organismo, facilitando la colaboración y el intercambio de datos a nivel interestatal (Directiva (UE) 2557 del Parlamento Europeo y del Consejo, 2022).

II. Experiencia internacional

1. Colombia

En el ejemplo colombiano, el Plan Nacional de Protección de Infraestructura Critica Cibernética define un marco de gobierno, roles y responsabilidades, además de un conjunto de niveles de alertas, actuaciones, notificaciones y respuestas frente a eventos de ciberseguridad asociados a sectores críticos (Plan Nacional de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia, 2017: 8).

Esta directriz tiene por norte identificar a los responsables y la definición de un esquema de coordinación que permita activar y articular las capacidades estratégicas y operativas de las instituciones del Estado encargadas de preservar la seguridad y defensa de las Infraestructuras Críticas Cibernéticas Nacionales, así como de los operadores o propietarios de estas últimas.

El objetivo general de este plan es incrementar el grado de protección de las infraestructuras criticas cibernéticas, mediante la coordinación y articulación de las entidades responsables, a objeto de aminorar el peligro y las vulnerabilidades, junto con 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, se cuentan (Plan Nacional de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia, 2017: 9-10):

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

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 otra parte, 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 evaluaciones 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 (Decreto 338, 2022: 13-14).

2. Corea del Sur

En el caso surcoreano, el Estado ha establecido un impulso a las capacidades de ciberdefensa, construyendo una Estrategia Nacional de Ciberseguridad, capaz de articular un sistema de detección y respuesta en tiempo real ante los ciberataques, a la vez que separando las redes de gobierno del *Internet* abierto al público.

Las tareas estratégicas incluidas en el texto se dirigen a incrementar la seguridad de la infraestructura crítica nacional; aumentar la capacidad de respuesta ante ciberataques; establecer una gobernanza basada en la cooperación nacional e internacional; e impulsar una cultura de la ciberseguridad.

A nivel específico, las labores contenidas en esta directriz apuntan a (*National Cibersecurity Strategy*, s/i: 13-24):

- Mejorar el ecosistema de ciberseguridad para la infraestructura crítica del país.
- Apoyar a las instituciones que operan estos sistemas críticos, de manera de conformar departamentos con presupuesto suficiente para dedicarse a materias de ciberseguridad.
- Definir lineamientos para estas entidades en el ámbito de la seguridad, sobre todo en la etapa inicial de establecer infraestructura crítica y crear parámetros de inspección.
- Impulsar un ambiente que permita a los operadores privados sumarse voluntariamente a los requerimientos y condiciones de seguridad necesarios para salvaguardar los intereses vitales del Estado.
- Diseñar estándares de evaluación para las vulnerabilidades de seguridad de cada sector específico, implementando medidas para asegurar la continuidad de los servicios, ante el evento de un incidente.
- Desarrollar infraestructuras de ciberseguridad de última generación.
- Elaborar planes técnicos e institucionales para responder ante amenazas de seguridad emergentes.
- Desarrollar productos tecnológicos con un diseño y servicio seguros para las personas.
- Establecer mecanismos de autenticación de alta seguridad, para permitir a las personas utilizar de forma segura los servicios *online*, en un ambiente hiperconectado.

Asimismo, Corea del Sur cuenta con la *Act on the Protection of Information and Communications Infrastructure*, cuyo fin es operar de forma estable la infraestructura de información crítica y comunicaciones, formulando e implementando medidas alusivas a la protección de dichas instalaciones, de modo que puedan hacer frente a cualquier intrusión por medios electrónicos.

3. España

De acuerdo al artículo 2 de la Ley 8, de 2011, se entiende en España por servicio esencial a todo aquel indispensable para la preservación “de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas” (Ley 8, 2011).

Por su parte, las infraestructuras críticas son definidas 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” (Ley 8, 2011).

En cuanto a institucionalidad, el país ibérico posee un Sistema de Protección de Infraestructuras Críticas (SPIC), que se articula en torno a la conformación del Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC), orgánica en la cual coexisten y trabajan mancomunadamente actores públicos y privados, cuya labor se concentra, a su vez, en la asesoría al Secretario de Estado de Seguridad, así como en la coordinación entre las reparticiones públicas y los gestores de infraestructuras esenciales para el funcionamiento del país.

Respecto al SPIC, el artículo 5 de la Ley 8, de 2011, por la que se establecen Medidas para la Protección de las Infraestructuras Críticas, lo conceptualiza como el sistema conformado por "una serie de instituciones, órganos y empresas, procedentes tanto del sector público como privado, con responsabilidades en el correcto andamiaje de los servicios esenciales o en la seguridad de los ciudadanos" (Ley 8, 2011).

Entre estos actores, cabe mencionar como primer responsable a la Secretaría de Estado de Seguridad, del Ministerio del Interior, para luego continuar con el CNPIC, los ministerios integrados en el sistema, las comunidades autónomas, las ciudades con estatuto de autonomía, las corporaciones locales, la Comisión Nacional para la Protección de las Infraestructuras Críticas (en adelante, la Comisión), el Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas, y los propios operadores del sector público y privado.

Ahora bien, en cuanto al CNPIC, el artículo 7 de la citada norma lo define como un órgano ministerial abocado a estimular, coordinar y supervisar las acciones dispuestas por la Secretaría de Estado de Seguridad, en lo atingente al resguardo de las infraestructuras críticas en el territorio nacional.

La propia Secretaría de Estado de Seguridad debe asumir la responsabilidad de mantener actualizado el Catálogo de Infraestructuras Críticas, velando porque este listado contenga todos los datos y el análisis en torno a las infraestructuras estratégicas del país, tal cual lo dispone el artículo 4 de la norma.

Otra institucionalidad propia de este sistema es la antes mencionada Comisión, que en virtud del artículo 11 del texto legal, es considerada un órgano colegiado bajo subordinación de la Secretaría de Estado de Seguridad, con facultades para visar los distintos planes estratégicos sectoriales, a la vez que para nombrar a los operadores críticos del sistema, previa propuesta del Grupo de Trabajo Interdepartamental para la Protección de Infraestructuras Críticas, al que a su vez le compete el diseño de los diferentes planes estratégicos sectoriales (Ley 8, 2011).

Ahora bien, la operatoria del sistema aparece desglosada en el artículo 14, que hace referencia a una serie de planes de actuación, entre los que se encuentran el Plan Nacional de Protección de las Infraestructuras Críticas (PNPIC), los planes estratégicos sectoriales, los planes de seguridad del operador, los planes de protección específicos y los planes de apoyo operativo.

El primero de esos ejes de acción es elaborado por la Secretaría de Estado de Seguridad, constituyendo el documento estructural para la conducción y coordinación de las diferentes funciones que a cada actor le competen en el sistema en su conjunto, frente a situaciones de amenaza a la infraestructura crítica nacional.

Por su parte, los planes estratégicos sectoriales son aprobados por la Comisión, considerando un conjunto de criterios, que definen las medidas a desplegar ante un evento riesgoso; mientras los planes de apoyo operativo son elaborados por la policía estatal, debiendo incluir "las medidas de vigilancia, prevención, protección o reacción a prestar, de forma complementaria a aquellas previstas por los operadores críticos" (Ley 8, 2011).

Además, es dable relevar que el artículo 3 de la norma excluye de su ámbito de aplicación a los reductos bajo dependencia del Ministerio de Defensa, y de las Fuerzas y Cuerpos de Seguridad, los cuales funcionan a partir de sus propios reglamentos (Estrategia Nacional de Ciberseguridad, 2019: 61-64).

Por último, 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 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.

4. Estonia

En Estonia, la infraestructura crítica es concebida como los sistemas de información y comunicaciones, cuyo mantenimiento, confiabilidad y seguridad son esenciales para el apropiado funcionamiento del país (*Republic of Estonia*, 2018).

La Política de Ciberseguridad de este país báltico busca asegurar la provisión ininterrumpida de servicios y su resiliencia, para lo cual busca resguardar (*Republic of Estonia*, 2018):

- La disponibilidad y funcionamiento seguro de los servicios esenciales.
- La continuidad digital de los procesos gubernamentales.
- La gestión de la interdependencia entre servicios vitales y críticos.
- El aseguramiento de la capacidad para gestionar ciberataques que amenacen al Estado y las empresas privadas.
- La administración de servicios ofrecidos por países extranjeros, en el caso de servicios críticos.
- La implementación de un sistema de monitoreo, análisis y reporte.
- La gestión de riesgos de seguridad de nuevas soluciones y tecnologías emergentes.

De igual forma, Estonia ha desarrollado la noción de *Critical Information Infrastructure Protection* (CIIP), principio que busca mantener un funcionamiento libre de problemas de los sistemas esenciales de información y comunicación.

En este contexto, los propósitos de la CIIP apuntan a recolectar y administrar datos, compilar informes sectoriales sobre riesgos asociados, intercambiar información sobre proveedores de servicios, desarrollar medidas de seguridad, entregar análisis de riesgos a los proveedores de servicios y elevar los niveles de conciencia en torno a la ciberseguridad entre la población.

Bajo esta lógica, la *Information System Authority* es la entidad que organiza los niveles nacionales de protección para las redes y sistemas informáticos de los sectores público y privado que resulten esenciales para el funcionamiento del Estado (*Republic of Estonia*, 2018).

En el ámbito normativo, la sección 7 de la *Cybersecurity Act* dispone que los proveedores de servicios críticos deben aplicar de forma permanente una serie de medidas de seguridad física y de información tecnológica, para prevenir y resolver incidentes cibernéticos, a la vez que para mitigar el impacto en la continuidad de servicios.

En tal sentido, el proveedor de servicios tiene que preparar un sistema de análisis de riesgos, que contemple un listado de amenazas a la seguridad de los activos críticos, determinando la severidad de las consecuencias de ciberincidentes asociados, y monitoreando los sistemas para detectar acciones que comprometan la seguridad y los sistemas de información (*Cybersecurity Act*, 2018).

Frente a cualquier ataque ciberespacial, la Sección 8 de la norma establece que los proveedores de servicios deben notificar a la *Estonian Information System Authority*, en un plazo no mayor a 24 horas, mediante un reporte que considere las posibles causas del incidente, el tiempo de resolución del problema y las medidas aplicadas frente al evento.

En cuanto a la prevención de ciberataques a la infraestructura crítica, la Sección 12 del texto legal dispone que este último organismo envíe alertas a la población, permitiéndole adoptar medidas para evitar o reducir el impacto de un ciberincidente.

De igual forma, la Sección 16 de la ley dispone que la autoridad puede restringir el uso de o el acceso a un sistema, en caso de que el ciberincidente comprometa o dañe la seguridad de otro sistema; o cuando el administrador del mencionado servicio sea incapaz de contrarrestar la amenaza o de eliminar la perturbación originada a partir del incidente (*Cybersecurity Act*, 2018).

5. Nueva Zelandia

La Estrategia de Ciberseguridad neozelandesa, de 2019, define la infraestructura crítica como aquellos activos y servicios digitales y físicos, cuya disrupción impactaría severamente en la seguridad nacional, la seguridad pública, los derechos fundamentales y el bienestar de los habitantes del país (*New Zealand's Cyber Security Strategy*, 2019: 16).

En tal sentido, el documento estratégico considera a los atentados contra la infraestructura crítica como una de las principales ciberamenazas contra el país, a la par con flagelos como el espionaje estatal, el ciberterrorismo y el robo de propiedad intelectual, por lo que establece la necesidad de proteger la seguridad nacional, a través de un enfoque adaptable, resiliente y preparado para lidiar con la incertidumbre.

La Estrategia es acompañada por un programa de trabajo, que contempla un reporte anual ministerial y esboza un rango de acciones dirigidas a avanzar en cinco áreas prioritarias durante el período 2019-2023, a saber (*New Zealand's Cyber Security Strategy*, 2019: 11-15):

- El resguardo a los intereses nacionales en el plano internacional, para lo cual establece actuaciones bilaterales, regionales y globales, para construir confianza en el ciberespacio.
- La consagración de un país resiliente y con capacidad para responder de manera expedita frente a las ciberamenazas, protegiendo las infraestructuras de la información, así como apoyando a la comunidad de negocios, las organizaciones no gubernamentales y comunitarias.
- El combate proactivo al cibercrimen, previniendo, investigando, disuadiendo y respondiendo al uso delictual y terrorista de la red. En este ánimo, el país continuará implementando el Plan Nacional 2015 de Dirección frente al Cibercrimen, que incluye el acceso al Convenio de Budapest.

En términos específicos, este enfoque se concentra en cautelar la infraestructura de información más sensible, apoyar a las organizaciones de infraestructura crítica nacional y estimularlas a ser responsables de sus propios sistemas, usando ciberherramientas y alianzas para proyectar a futuro los intereses nacionales (*New Zealand's Cyber Security Strategy*, 2019: 14).

6. Reino Unido

En cuanto a la infraestructura crítica del Reino Unido, el gobierno la define, en el documento "*Public Summary of Sector Security and Resilience Plans*", de 2018, como (*UK Cabinet Office*, 2018):

"(...) aquellos elementos tales como instalaciones, sistemas, lugares, propiedades, informaciones, personas, redes y procesos, cuya pérdida o compromiso redundaría en un impacto negativo sobre la disponibilidad, entrega e integridad de los servicios esenciales del país, conduciendo a severas consecuencias económicas o sociales, así como a la pérdida de vidas humanas. Entre estos activos también cabe incluir algunas funciones específicas, sitios y organizaciones no considerados críticos para el mantenimiento de servicios esenciales, los cuales de todos modos requieren una protección especial, dados los potenciales peligros a los que podrían exponer a la comunidad, en caso de una emergencia de tipo nuclear o química, entre otras".

En concreto, la infraestructura crítica del país se vincula con sectores como la industria química, energía nuclear, comunicaciones, defensa, servicios de emergencia, energía, finanzas, alimentación, gobierno, salud, espacio, transporte y agua, muchos de los cuales son de propiedad privada. Varios de estos sectores contemplan, a su vez, subdepartamentos como los de policía, salud y bomberos, en el caso de los servicios de emergencia.

Respecto a la política referida a la infraestructura más sensible del país, la Oficina del Gabinete Presidencial lidera los departamentos gubernamentales responsables de los trece sectores calificados como críticos, en aras de generar los denominados Planes de Resiliencia y Seguridad Sectorial, que describen (*UK Cabinet Office*, 2018):

- Las aproximaciones de cada departamento al manejo de seguridad de infraestructura crítica.
- El análisis de riesgos significativos para cada sector.
- Las actividades implementadas para mitigar riesgos.

El análisis gubernamental de amenazas y riesgos se basa en un ciclo continuo de lecciones aprendidas, en base a eventos reales, construyéndose en función de la evidencia y la mejora de las fórmulas para calcular los potenciales impactos o consecuencias de las amenazas.

Los posibles riesgos definidos en el informe oficial incluyen el ataque de terceros estados hostiles; los ciberataques; los actos de terrorismo o crimen organizado; y el espionaje político, militar o comercial.

A su vez, existen varios riesgos naturales, como las inundaciones, el cambio climático y las tormentas, que pueden lesionar el funcionamiento diario de la infraestructura del país. Adicionalmente, el reporte menciona el desorden público y la presión social, así como la ausencia del aparato estatal y las pandemias, como factores que pueden llevar a la clausura temporal o a la reducción de servicios (*UK Cabinet Office*, 2018).

Por lo mismo, el objetivo central del gobierno apunta a reducir la vulnerabilidad, construyendo una capacidad de infraestructura resistente, que pueda recuperarse rápidamente tras posibles ataques.

Respecto a las autoridades locales y los servicios de emergencia, la *Civil Contingencies Act*, de 2004, les delega la función de identificar y analizar la probabilidad de impacto de potenciales emergencias que podrían afectar a la sociedad en sus áreas de jurisdicción, así como el deber de desarrollar planes de respuesta ante emergencias.

Finalmente, el *National Cyber Security Centre* (NCSC) respalda a las organizaciones críticas del Estado, activando protocolos de respuesta inmediata ante ciberincidentes que pudiesen amenazar la continuidad de los activos vitales del país, como las redes del aparato público y de la industria (NCSC, 2022).

7. 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 gubernamental 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

Directiva (UE) 2557 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a la resiliencia de las entidades críticas y por la que se deroga la Directiva 2008/114/CE del Consejo. (2022). Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81965.

Estrategia Nacional de Ciberseguridad. (2019). Disponible en: http://bcn.cl/30d3o.

National Cybersecurity Strategy. (s/i). Disponible en: http://bcn.cl/2m658.

NCSC. (2022, abril 28*). What we do*. Disponible en: http://bcn.cl/30ghn.

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.

Republic of Estonia. (2018, septiembre 9). *Critical Information Infrastructure Protection (CIIP)*. Disponible en: http://bcn.cl/2lkso.

UK Cabinet Office. (2018). *Public Summary of Sector Security and Resilience Plans*. Disponible en: http://bcn.cl/2c9ye.

Textos normativos

Cybersecurity Act. (2018, mayo 9). Disponible en: http://bcn.cl/33h69.

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

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