Institucionalidad en ciberseguridad e infraestructura crítica a nivel internacional

Autor

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

Nº SUP: 135408

Resumen

La ciberseguridad puede ser concebida como “la práctica de proteger sistemas, redes y programas de ataques digitales, que buscan acceder, modificar o destruir información confidencial, extorsionar a las personas o interrumpir la continuidad de un servicio”.

A su vez, el Consejo Europeo ha conceptualizado la infraestructura crítica 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”.

En este contexto, países como Argentina, Corea del Sur, Estonia y Nueva Zelandia cuentan con una Estrategia Nacional de Ciberseguridad, dirigida a responder de forma eficiente ante las ciberamenazas, proteger la infraestructura crítica del país y estimular la cooperación internacional en el ciberespacio.

Por su parte, el Plan Nacional de Protección de Infraestructura Crítica Cibernética, define en Colombia un marco de roles, además de un conjunto de niveles de alertas, notificaciones y respuestas frente a eventos de ciberseguridad asociados a sectores críticos, en consonancia con los objetivos nacionales en materia de protección, tanto a corto, mediano como largo plazo.

En cuanto al paradigma español, existe 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.

Finalmente, en Reino Unido, el *National Cyber Security Centre* 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.

Introducción

El presente informe describe las características de algunos paradigmas internacionales en materia de institucionalidad asociada a ciberseguridad e infraestructura crítica.

El texto recoge información de los siguientes documentos: Jarufe, Juan Pablo. (2022, mayo). "Gobernanza en ciberseguridad: experiencia internacional". Disponible en: http://bcn.cl/3046o; Jarufe, Juan Pablo. (2020, diciembre). "Políticas de ciberseguridad en la experiencia internacional". Disponible en: http://bcn.cl/3046o; y Jarufe, Juan Pablo. (2020, octubre). "Protección de infraestructura crítica en la experiencia internacional". Disponible en: http://bcn.cl/3046i.

I. Ciberseguridad e infraestructura crítica

1. Conceptos generales

La ciberseguridad puede ser concebida como "la práctica de proteger sistemas, redes y programas de ataques digitales, que buscan acceder, modificar o destruir información confidencial, extorsionar a las personas o interrumpir la continuidad de un servicio" (CISCO, 2022).

Por su parte, en 2004 la Comisión Europea definió la infraestructura crítica como (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 (Consejo Europeo, 2008. En Horzella, B, 2019: 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".

A continuación se describen las principales características de los sistemas ciberespaciales de protección de infraestructura crítica, en un conjunto de países de diversas latitudes.

2. Institucionalidad en materia de ciberseguridad e infraestructura crítica

2.1. Argentina

En el caso argentino, la Dirección Nacional de Ciberseguridad es el organismo encargado de analizar los elementos propios de la ciberseguridad y el resguardo de las infraestructuras críticas de la información, así como de preocuparse de prevenir y generar respuestas frente a ciberincidentes que pudiesen afectar al sector público.

En este contexto, esta orgánica tiene entre sus competencias (Argentina.gob.ar, 2022):

- El desarrollo del Programa Nacional de Infraestructuras Críticas de la Información.

- El involucramiento en los procesos vinculados a los equipos de respuesta a emergencias informáticas a nivel nacional.

- La participación en iniciativas dirigidas a poner en marcha los objetivos establecidos en la Estrategia Nacional de Ciberseguridad, articulando proyectos con las diferentes áreas del Estado.

Precisamente esta última directriz multisectorial, publicada el 28 de mayo de 2019, busca entregar un marco para que los organismos públicos y privados puedan desarrollar acciones de prevención, detección, respuesta y recuperación ante las ciberamenazas.

Diseñada por el llamado Comité de Ciberseguridad, la Estrategia pretende instaurar una visión integradora en esta materia, sobre la base de la coordinación y colaboración entre la Administración Pública Nacional, las entidades de alcance provincial y municipal, los privados, las organizaciones no gubernamentales y la academia.

En concreto, contiene una serie de principios rectores, entre los cuales se cuentan (Estrategia Nacional de Ciberseguridad de la República Argentina, 2019):

- El respeto por los derechos y libertades individuales de las personas en el ciberespacio.
- La construcción de capacidades mancomunadas de detección, prevención y respuesta ante incidentes cibernéticos, entre todos los actores involucrados.
- La integración internacional, habida cuenta del carácter transfronterizo de las ciberamenazas.
- La consolidación de una cultura de ciberseguridad y responsabilidad compartida, que involucre a las organizaciones públicas y privadas, el sector académico, la sociedad civil y la ciudadanía.

Los objetivos de esta directiva, en tanto, son (Estrategia Nacional de Ciberseguridad de la República Argentina, 2019):

- La capacitación y educación en el uso seguro del ciberespacio, meta que precisa de la formación de nuevos profesionales, técnicos e investigadores.
- El desarrollo de un marco normativo, que permita adecuar y generar textos legales, marcos regulatorios, estándares y protocolos que hagan frente a los retos ciberespaciales, en consonancia con las garantías fundamentales de las personas.
- El fortalecimiento de las capacidades de prevención, detección y respuesta en el ciberespacio.
- La protección y recuperación de los sistemas de información del sector público.
- El estímulo a una industria de la ciberseguridad, a través del impulso a las capacidades tecnológicas que permitan enfrentar las ciberamenazas, y por medio del despliegue de actividades de investigación, desarrollo e innovación en los ámbitos público y privado.
- La cooperación internacional, propiciando acuerdos regionales e internacionales, a la vez que proyectando al país en organismos globales alusivos a la ciberseguridad.
- La protección de las infraestructuras críticas nacionales de información, por medio de una estrategia de cooperación público-privada.

2.2. Colombia

En el ejemplo colombiano, en tanto, 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, en consonancia con cinco principios básicos en materia de protección y resiliencia a corto, mediano y largo plazo (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 del 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):

- 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 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).

Colombia también ha procurado proteger sus activos, mediante el reforzamiento de vínculos internacionales, como el que mantiene como Socio Global de la Organización del Tratado del Atlántico Norte (OTAN), que busca avanzar en el desarrollo de capacidades de ciberdefensa y en un marco jurídico que fortalezca esta línea de acción; la promoción de proyectos de investigación, formación de recurso humano de alto nivel técnico; la adopción de una doctrina conjunta que integre las capacidades en el ciberespacio, con las que se cuentan en

tierra, mar y aire; así como en programas de entrenamiento, en el marco de la cooperación con países aliados (Ministerio de Defensa Nacional de Colombia, 2022a).

Además, el pasado 8 de marzo, el gobierno de este país anunció la conformación de un modelo de gobernanza digital que, de acuerdo al Decreto 338, está dirigido a robustecer la coordinación entre los diversos actores presentes en este ámbito, que pasarían a articularse a partir de cinco niveles, como son los de la Coordinación Nacional de Seguridad Digital, el Comité Nacional de Seguridad Digital, los Grupos de Trabajo de Seguridad Digital, las Mesas de Trabajo Digitales y los Puestos de Mando Unificado de Seguridad Digital.

De igual modo, esta nueva matriz acota el alcance de los Equipos de Respuesta a Incidentes Cibernéticos, distinguiendo entre ("Eje 21", 2022):

- El Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT), que haría las veces de punto único de contacto y respuesta nacional ante incidentes de seguridad digital, asesorando y coordinando a las partes interesadas en la materia.

- El Equipo de Respuesta a Incidentes de Seguridad Cibernética (CSIRT Gobierno), constituido como un grupo de reacción ante eventos de seguridad digital en el aparato público, con capacidad para prevenir y gestionar incidentes.

2.3. 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.

De igual modo, en orden a responder a las ciberamenazas transnacionales, esta directriz aborda el diseño de un mecanismo cooperativo con aliados nacionales e internacionales, tales como Naciones Unidas (*National Cibersecurity Strategy*, s/i: 8-9), con la visión de configurar un ciberespacio libre y seguro, que aporte a la seguridad nacional, la prosperidad económica y la paz internacional.

Las metas trazadas por este documento apuntan a fortalecer la seguridad y resiliencia de la infraestructura crítica del país, de forma de garantizar su operación continua, pese a la existencia de ciberamenazas; responder a los ciberataques de forma oportuna; y construir un ecosistema ciberespacial libre y autónomo, con industrias y recursos humanos competitivos. Todo lo anterior, a partir de un enfoque balanceado entre la ciberseguridad, el derecho a la privacidad de las personas, la transparencia y el imperio de la ley.

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 (*National Cibersecurity Strategy*, s/i: 13-24).

Para darle operatividad a la Estrategia, el gobierno surcoreano estableció un Plan Nacional Básico de Ciberseguridad y un Plan Nacional de Implementación de Ciberseguridad, en el que cada ministerio y agencia estatal asume tareas en materia de respeto a la normativa vigente, así como en cuanto al funcionamiento de las instituciones y políticas afines a la materia.

La Oficina Nacional de Seguridad, en tanto, es la encargada de monitorear la implementación de la Estrategia, mientras otros entes insertos en el modelo, son (*National Cibersecurity Strategy*, s/i: 26) (*Korea Internet & Security Agency*, 2022):

- El *Security Verification Scheme National Intelligence Service System*, que verifica la seguridad de los sistemas de información utilizados en organismos públicos, a objeto de incrementar el nivel de seguridad de la red nacional de comunicaciones e información, al tiempo de responder a las ciberamenazas.

- El *National Cyber Security Center National Intelligence Service*, que supervigila la Política Nacional de Ciberseguridad, previniendo cibercrisis y detectando ataques de este tipo.

- El Cibercomando del Ministerio de Defensa Nacional, establecido para responder a los ciberataques.

- La *Cyber Bureau National Police Agency*, que incluye una División de Investigación de Ciberseguridad y Cibercrimen.

- La *Korea Internet & Security Agency*, que busca expandir la ciberseguridad en cada sector de la sociedad, ayudando a construir una infraestructura y servicios innovadores basados en nuevas tecnologías.

- El *Korea National Computer Emergency Response Team* (KN-CERT) y el *National Cyber Security Center*, cuyas misiones se orientan a monitorear permanentemente y detectar de forma temprana eventuales ciberataques al sector privado; cooperar con otras entidades locales y foráneas; y garantizar una rápida respuesta frente a incidentes informáticos, de forma de minimizar daños a los sistemas del país.

Asimismo, Corea del Sur cuenta con un entramado legal que contribuye al funcionamiento del sistema de ciberseguridad. Este cuerpo normativo está conformado por (*Cybersecurity Policy*, 2020):

- La *Act on Promotion of Information and Communications Network Utilization and Information Protection*, dirigida a facilitar el uso de información y redes de comunicación, proteger los datos personales y los servicios de comunicación, desarrollando un ambiente en el que las personas puedan emplear la información en un ambiente más seguro.

- La *Personal Information Protection Act*, que cautela la privacidad de las personas ante cualquier abuso de la información.

- La *Electronic Government Act No.* 6439, de 2001, que busca facilitar los proyectos de gobierno electrónico, mejorar la productividad, transparencia y democracia de las agencias oficiales, lo mismo que mejorar la calidad de vida de los ciudadanos del país.

- 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.

2.4. España

La estructura de la ciberseguridad en el marco del Sistema de Seguridad Nacional español, está constituida por los siguientes componentes (Estrategia Nacional de Ciberseguridad de España, 2019: 61-64):

- El Consejo de Seguridad Nacional: es el órgano al que corresponde asistir al Presidente del Gobierno en la dirección de la Política de Seguridad Nacional. Actúa, a través del Departamento de Seguridad Nacional, como punto de contacto único para ejercer una función de enlace y garantizar la cooperación transfronteriza con otros países de la Unión Europea.

- El Comité de Situación: tiene carácter único para el conjunto del Sistema de Seguridad Nacional y actúa, apoyado por el Departamento de Seguridad Nacional, de acuerdo con las directrices político-estratégicas dictadas por el Consejo de Seguridad Nacional, en materia de gestión de crisis.

- El Consejo Nacional de Ciberseguridad: da apoyo al Consejo de Seguridad Nacional para el cumplimiento de sus funciones y, en particular, en la asistencia al Presidente del Gobierno en la dirección y coordinación de la Política de Seguridad Nacional en el ámbito de la ciberseguridad. Entre sus funciones, se encuentra el reforzamiento de las relaciones de coordinación, colaboración y cooperación entre las distintas administraciones públicas con competencias en materia de ciberseguridad, así como entre los sectores público y privado, en pos de facilitar la toma de decisiones del propio Consejo, mediante el análisis, estudio y propuesta de iniciativas, tanto en el ámbito nacional como internacional. De igual modo, puede valorar los riesgos y amenazas, analizar los posibles escenarios de crisis, estudiar su posible evolución, elaborar y mantener actualizados los planes de respuesta, y formular directrices para la realización de ejercicios de gestión de crisis en el ámbito de la ciberseguridad, evaluando los resultados de su ejecución, todo ello en coordinación con los órganos y autoridades directamente competentes.

- La Comisión Permanente de Ciberseguridad: se establece con objeto de facilitar la coordinación interministerial a nivel operacional, en el ámbito de la ciberseguridad. Presidida por el Departamento de Seguridad Nacional, está compuesto por aquellos organismos representados en el Consejo Nacional de Ciberseguridad, con responsabilidades operativas. Es el órgano al que corresponde asistir al Consejo Nacional de Ciberseguridad, sobre aspectos relativos a la valoración técnica y operativa de los riesgos y amenazas a la ciberseguridad. El funcionamiento de la Comisión se enmarca en el procedimiento de gestión de crisis de ciberseguridad, que busca detectar y valorar los riesgos y amenazas, facilitar el proceso de toma de decisiones, y asegurar una respuesta óptima y coordinada de los recursos del Estado. Además, incluye los diferentes niveles de activación del Sistema de Seguridad Nacional, junto a instrucciones para la gestión de la comunicación pública.

- El Foro Nacional de Ciberseguridad: actúa en la potenciación y creación de sinergias público-privadas, particularmente en la generación de conocimiento sobre las oportunidades, desafíos y amenazas a la seguridad en el ciberespacio. La puesta en marcha de esta instancia y la armonización de su funcionamiento con los órganos existentes, se realiza mediante la aprobación de las disposiciones normativas necesarias, con el objetivo de alcanzar el funcionamiento coordinado y eficiente de estos componentes en el Sistema de Seguridad Nacional.

Para hacer frente a los peligros cibernéticos, en tanto, España cuenta con un Sistema Nacional de Gestión de Situaciones de Crisis (SNGSC), instancia que busca lidiar con los nuevos retos a la seguridad nacional.

A nivel más específico, existe en este país 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: 2-3).

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 críticos 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: 2-3).

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: 2-3).

Por último, 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.

El marco estratégico e institucional de la ciberseguridad se complementa con las autoridades públicas competentes en materia de seguridad de las redes y sistemas de información, así como con los Equipos de Respuesta ante Incidentes de Seguridad Informática (CSIRT), que aparecen recogidos en el marco jurídico del país.

Asimismo, los CSIRT de las comunidades autónomas, de las ciudades autónomas, de las entidades locales y sus organismos vinculados o dependientes, los de los organismos privados, la red de CSIRT.es y otros servicios de ciberseguridad relevantes, deben estar coordinados con los anteriores, en función de las competencias de cada cual (Estrategia Nacional de Ciberseguridad, 2019: 61-64).

Por otra parte, la gobernanza en ciberseguridad de este país contempla la existencia del Instituto Nacional de Ciberseguridad de España (INCIBE), conocido hasta 2014 como Instituto Nacional de Tecnologías de la

Comunicación. Esta unidad cuenta con un centro de respuesta a incidentes de seguridad (INCIBE-CERT), subordinado a la Secretaría de Estado de Digitalización e Inteligencia Artificial, que actúa en coordinación con el resto de los equipos nacionales e internacionales, en pos de mejorar los resultados en el combate a los delitos que involucran redes de información (INCIBE-CERT, 2022a).

El INCIBE-CERT tiene atribuciones para (INCIBE-CERT, 2022b):

- Entregar soporte técnico para resolver incidentes de ciberseguridad.
- Utilizar técnicas de detección temprana de incidentes, notificando a los afectados.
- Mantener el contacto con los proveedores de *Internet* y otros CERT nacionales e internacionales.

Cabe agregar que el INCIBE también ha impulsado la cooperación público-privada en materia de ciberseguridad, en el marco del Plan de Confianza en el Ámbito Digital, a partir de iniciativas como el proceso de conformación de la Red de Excelencia Nacional de Investigación en Ciberseguridad (RENIC), que quedó constituida el 1 de julio de 2016, para seis días más tarde adscribirse como miembro pleno de la *European Cyber Security Organistion* (ECSO).

Se trata de un conglomerado que considera centros de investigación, universidades y otros actores del ecosistema de ciberseguridad, cuyos objetivos buscan alinearse con una estrategia de alcance europeo, además de configurarse en función de las necesidades de la industria y los usuarios finales.

La Red pretende conseguir (INCIBE, 2022):

- La colaboración de los agentes expertos en ciberseguridad.
- La reunión y centralización de una masa crítica de recursos investigadores.
- La difusión de las conclusiones de trabajos investigativos, que posibiliten la transferencia de conocimiento.
- La promoción de una capacitación y desarrollo de talentos, a partir de una política de incentivos.

En cuanto a planes específicos, este organismo ha propuesto la definición de un mapa de conocimiento de investigación y desarrollo en ciberseguridad, la organización de las Jornadas Nacionales de Investigación en Ciberseguridad y el estímulo a un plan director, que busque sentar las bases de una Estrategia de Ciberseguridad.

2.5. Estonia

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

En cuanto a la institucionalidad, el *Cyber Security Council*, creado en 2009 y presidido por el Secretario General del Ministerio de Asuntos Económicos y Comunicaciones, es el encargado de aportar a una cooperación más fluida entre diversos organismos púbicos de Estonia, al tiempo de velar por el cumplimiento de las metas de la Estrategia de Ciberseguridad, documento horizontal, que considera acuerdos y coordinación en este campo,

incorporando a diversos actores, tales como las instituciones de gobierno, la academia, los centros de pensamiento y el sector privado.

Esta directriz se enfoca en cuatro objetivos principales, como son (*Cybersecurity Strategy*, 2019-2022: 14-15):

- La construcción de una sociedad digital sostenible, que descanse sobre una resiliencia y preparación frente a las emergencias, en el afán de construir una gobernanza y el desarrollo de una comunidad de ciberseguridad.

- El diseño de una industria de ciberseguridad, investigación y desarrollo, competitiva a nivel global, innovadora y confiable.

- La búsqueda de liderazgo en materia de cooperación internacional en el ámbito de la ciberseguridad, mediante la promoción de un espacio sostenible alrededor del mundo.

- El desarrollo de una sociedad ciberalfabetizada, con participación del Estado, los privados y los propios ciudadanos.

Para lo anterior, la Estrategia considera una aproximación basada en riesgos y en el monitoreo permanente de cualquier intrusión en las redes, mediante un manejo interdependiente de activos digitales, considerando aquellos de carácter transfronterizo.

Asimismo, esta hoja de ruta considera la inclusión de la defensa nacional, integrando la ciberseguridad en aquellos documentos de planificación de la seguridad del país; conduciendo ejercicios conjuntos regulares con los proveedores de servicios vitales, autoridades políticas y organizaciones militares; y desarrollando la capacidad del Comando de Ciberfuerzas de la Defensa, con aptitudes para ciberatacar y promover un modelo de ciberconscripción, con la innovación tecnológica como factor clave (*Cybersecurity Strategy*, 2019-2022: 16-18).

Por otra parte, 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) (*Ministry of Economic Affairs and Communications*, 2020):

- 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.

Además, conforme a la Sección 11 de la ley, la notificación de un ciberincidente debe sustentarse en los criterios provistos por el artículo 16 de la Directiva 1148, de 2016, del Parlamento Europeo, de manera que ante un problema que llegue a tener un impacto significativo sobre la continuidad de un servicio digital en un tercer estado, la *Estonian Information System Authority* dé inmediato aviso al país que ha sido víctima del ataque.

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.

La Sección siguiente, en tanto, considera la existencia de un registro de incidentes ciberespaciales, entendido como una base de datos mantenida por la propia *Estonian Information System Authority*, con el fin de grabar y analizar los ciberincidentes, para luego resolverlos.

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).

Asimismo, el CERT-EE es una organización establecida en 2006, que gestiona los incidentes de ciberseguridad que afectan a las redes del país, o que son notificados por ciudadanos e instituciones locales o extranjeras.

Entre sus competencias, esta unidad se encarga de (*Information System Authority*, 2021):

- Compartir información y entregar notificaciones acerca de riesgos y brechas de seguridad, o de eventos que puedan alterar la confidencialidad, integridad y procesabilidad de los sistemas de información.

- Ayudar a las instituciones públicas y privadas a responder ante ciberincidentes, otorgándoles también apoyo legal, en caso de ser necesaria una investigación.

- Impulsar campañas periódicas en los medios de comunicación, respecto a la importancia de tomar conciencia acerca de la seguridad informática.

Esta organización prioriza los ciberincidentes, según su potencial severidad y ámbito, teniendo en cuenta factores como el número de usuarios afectados, el tipo de incidente, el blanco de un ataque, el origen del mismo y los recursos requeridos para manejar el problema. Así, por ejemplo, los ciberataques graves son aquellos que amenazan la vida de las personas o dañan la infraestructura crítica del país.

Finalmente, otro actor relevante es el Cibercomando, órgano asesor del Ministerio de Defensa, que se encarga de conducir las operaciones ciberespaciales. Sus principales misiones específicas son (*Defence Forces*, 2022):

- Proveer información e infraestructura tecnológica en materia de comunicaciones y servicios.

- Planificar y ejecutar operaciones de ciberdefensa.

- Obtener, mantener y compartir análisis situacionales sobre el ciberespacio.

- Planificar y ejecutar misiones de información y comunicación estratégica.

- Entrenar, preparar y movilizar a las unidades para tiempos de guerra y reserva.

2.6. 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):

- Ciudadanos conscientes en materia de ciberseguridad: busca consolidar una cultura de ciberseguridad entre las personas, para que puedan efectuar operaciones *online* de manera segura, con énfasis en la capacitación de grupos vulnerables, como los menores de edad y los adultos mayores.

- Una fuerza de trabajo, junto con un ecosistema de ciberseguridad fuerte y sostenible, con el foco puesto en incrementar las habilidades de la fuerza de trabajo; apoyar la expansión de roles y oportunidades para cibertrabajadores; y animar el desarrollo de una comunidad académica e investigativa, que se vincule con la industria.

- 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).

Por otra parte, la Oficina de Política Nacional de Ciberseguridad fue instaurada en 2012, con el propósito de liderar el desarrollo de una directriz de ciberseguridad, para dotar al gobierno con una orientación permanente en cuanto a las actividades y medidas a implementar.

Este plan depende directamente del Ministro de Radiodifusión, Comunicaciones y Medios Digitales, que actúa en consulta con el Primer Ministro, el Ministro de Seguridad Nacional e Inteligencia, y otras autoridades pertinentes.

Asimismo, existe la figura del Cibercoordinador, que funge como representante especial del Primer Ministro en materias ciberdigitales, siendo responsable de entregar consejo, desarrollar y coordinar la entrega de un programa de trabajo; y de asegurar que la labor gubernamental sobre riesgos digitales, sea consistente y esté alineada con los lineamientos estratégicos del país (*Department of the Prime Minister and Cabinet*, 2020).

También opera el *National Cyber Security Centre* (NCSC), que ayuda a las agencias de gobierno a proteger sus sistemas de información frente a las ciberamenazas, a partir de acciones tales como (*National Cyber Security Centre* (NCSC, 2020):

- La provisión de capacidades de protección y detección de ciberamenazas avanzadas.
- La respuesta a ciberincidentes de alto impacto a nivel nacional.
- La gestión de los estándares de seguridad informática del país.
- La generación de reportes de ciberamenazas.

Las potenciales ciberamenazas incluyen (*National Cyber Security Centre* (NCSC), 2020):

- El ciberespionaje y el robo de propiedad intelectual para propósitos políticos o comerciales.

- El ciberterrorismo o la disrupción de servicios que buscan dañar los sistemas de infraestructura crítica del país.

- El cibercrimen, que involucra las inversiones falsas o la sustracción de datos financieros personales.

- El cibervandalismo a sitios *web*, cuyos servicios son intervenidos con propósitos políticos.

Nueva Zelandia igualmente ha intentado abordar la problemática de la ciberseguridad, a partir de un enfoque colaborativo con terceros países y organismos internacionales, participando en discusiones patrocinadas por

Naciones Unidas, foros regionales e instancias multilaterales, como el *Internet Governance Forum* (*New Zealand Foreign Affairs & Trade*, 2020).

2.7. 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.

En cuanto a la institucionalidad vigente, 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.

Nacido en 2016, este organismo se nutre de la experiencia de entidades como la *National Technical Authority for Information Assurance* (CESG), el *Centre for Cyber Assessment*, el CERT-UK y el *Centre for Protection of National Infrastructure*.

En esta línea, el NCSC ofrece un solo punto de contacto para organizaciones de gran tamaño, agencias de gobierno, terceros estados y público en general (NCSC, 2022).

Junto a esta orgánica, entra en acción el *Cybersecurity Incident Response Team*, que se ocupa de minimizar el impacto de los ciberataques, a partir de un rápido despliegue de expertos en ciberseguridad; investigar la respuesta a ciberincidentes, dirigir investigaciones forenses, implementar medidas para incrementar los niveles de ciberseguridad del sector afectado y emitir un informe final sobre el ciberincidente, con hallazgos y recomendaciones; y elaborar un Análisis de Preparación ante Incidentes (Gov.uk, 2022).

Referencias

Argentina.gob.ar. (2022, julio 9). Objetivos de la Dirección Nacional de Ciberseguridad. Disponible en: http://bcn.cl/33km3.

CISCO. (2022, julio 8). ¿Qué es la ciberseguridad? Disponible en: http://bcn.cl/33jwp.

Cybersecurity Strategy. (2019-2022). Disponible en: http://bcn.cl/2an8g.

Defence Forces. (2022, abril 26). *Cyber Command*. Disponible en: http://bcn.cl/30d1z.

Department of the Prime Minister and Cabinet. (2020, septiembre 16). *National Cyber Policy Office*. Disponible en: http://bcn.cl/2mw3h.

“Eje 21”. (2022, abril 28). Gobierno Nacional crea Modelo de Gobernanza, para liderar coordinación entre actores del entorno digital. “*Eje 21*”. Disponible en: http://bcn.cl/30ghg.

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

Estrategia Nacional de Ciberseguridad de la República Argentina. (2019, mayo 28). Disponible en: http://bcn.cl/33h8h.

European Commission. (2022, julio 6). *Critical infrastructure*. Disponible en: http://bcn.cl/33hdy.

Gov.uk. (2022, abril 26). *Cyber Security Incident Response Team (CSIRT) Service*. Disponible en: http://bcn.cl/30d2l.

Homeland Security. (2020, julio 14). *Cybersecurity and Critical Infrastructure*. Disponible en: http://bcn.cl/33h50.

INCIBE. (2022, abril 28). Red de Excelencia Nacional de Investigación en Ciberseguridad. Disponible en: http://bcn.cl/30gg5.

INCIBE-CERT. (2022, abril 26). Qué es INCIBE-CERT. Disponible en: http://bcn.cl/30czu.

INCIBE-CERT. (2022, abril 26). Respuesta a incidentes. Disponible en: http://bcn.cl/30d01.

Information System Authority. (2021, julio 26). CERT-EE. Disponible en: http://bcn.cl/30d1e.

Korea Internet & Security Agency. (2022, julio 9). *About KISA*. Disponible en: http://bcn.cl/33kms.

Ministry of Economic Affairs and Communications. (2020, abril 15). *Cyber security*. Disponible en: http://bcn.cl/2lkt6.

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.

New Zealand Foreign Affairs & Trade. (2020, septiembre 22). *Cybersecurity*. Disponible en: http://bcn.cl/2mw3q.

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.

Cybersecurity and Infrastructure Agency Act. (2018, noviembre 16). Disponible en: http://bcn.cl/33h55.

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