Centros de Protección de Infraestructura Crítica

Experiencia internacional

Autor

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

Nº SUP: 136196

Resumen

En España 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.

En el paradigma estadounidense, en tanto, los sectores más esenciales son cautelados por el *National Infrastructure Coordinating Center*, entidad que forma parte de la División de Seguridad e Infraestructura de la *Cybersecurity and Infrastructure Security Agency*, así como del Centro de Operaciones Nacionales del Departamento de Seguridad Interior, con un funcionamiento permanente, coordinando y compartiendo datos sobre la situación de la infraestructura crítica del gobierno federal.

Respecto al caso francés, el artículo 22 de la *Critical Infrastructures Information Protection Law*, de 2013, mandata a la Agencia Nacional de Ciberseguridad para incrementar los niveles de seguridad de los operadores de servicios críticos, establecer un nivel común mínimo de ciberseguridad para cada operador y exigir reportes de incidentes detectados en estos sistemas, modalidad aplicable a más de 200 operadores públicos y privados.

A su vez, el artículo 22 de la Ley 19.775, dispone entre las tareas subsidiarias de las Fuerzas Armadas uruguayas, la protección y salvaguarda, ya sea por sí mismas o en coordinación con otros organismos del Estado, de las infraestructuras críticas o vitales que establezca el Poder Ejecutivo.

Introducción

El presente informe da cuenta de las características de los Centros de Protección de Infraestructura Crítica en el plano internacional.

A petición del requirente, el documento considera los casos de España, Estados Unidos (EE.UU.), Francia y Uruguay.

La investigación incorpora datos de los informes BCN “Protección de infraestructura crítica en la experiencia internacional” (2020, octubre) e “Institucionalidad en ciberseguridad e infraestructura crítica a nivel internacional” (2022, julio), ambos del mismo autor del presente documento, así como del informe BCN “Protección de Infraestructura Crítica y Fuerzas Armadas. Conceptualización y experiencia comparada” (2019, diciembre), de autoría de la analista Bárbara Horzella.

I. Centros de Protección de Infraestructura Crítica

1. España

La creciente interdependencia de la sociedad española respecto al sistema de infraestructuras que le da soporte, trae aparejada una amenaza latente a la seguridad del país, con la opción cierta de que se produzcan fallos imprevistos e impactos de consideración sobre los servicios básicos y vitales para la población.

Para hacer frente a esta realidad, la normativa del país ibérico contempla la existencia de un Sistema Nacional de Gestión de Situaciones de Crisis (SNGSC), instancia que busca lidiar con los nuevos retos a la seguridad nacional, como el terrorismo, la proliferación de armas de destrucción masiva y el crimen organizado, entre otros.

A nivel más específico, existe 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.

En este contexto, el artículo 5 de la Ley 8, de 2011, por la que se establecen Medidas para la Protección de las Infraestructuras Críticas, conceptualiza al SPIC 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, que pueden corresponder a las siguientes categorías (Ley 8, 2011: 2-3):

- Servicio esencial, entendido como aquel indispensable para la preservación de las relaciones sociales básicas, la salud, la seguridad, el bienestar de las personas y la normal operación de las entidades públicas.
- Sector estratégico, que remite a cada área inserta en la actividad laboral, económica y productiva, que entrega un servicio vital, avala el ejercicio de la autoridad estatal o garantiza la seguridad del país.
- Subsector estratégico, concebido como cada uno de los espacios en que se dividen los diversos sectores estratégicos, de acuerdo a las propuestas de los ministerios involucrados y a partir de la orientación técnica que entregue el CNPIC.
- Infraestructuras estratégicas, referidas a las instalaciones, redes, sistemas, y equipos físicos y de tecnología de la información, que sustentan el funcionamiento de los servicios esenciales.
- Infraestructuras críticas, que son aquellas de carácter estratégico, cuyo funcionamiento es esencial, al no existir soluciones alternativas a su operación. En este caso, su perturbación o destrucción genera un severo impacto sobre los servicios vitales del país.
- Zona crítica, conceptualizada como un área geográfica continua, en la que se encuentran diversas infraestructuras críticas funcionando de manera interdependiente. La autoridad declara esta calidad, en aras de ayudar a la protección de los distintos operadores de infraestructuras críticas.

Junto a lo anterior, el texto legal validó un primer Plan Nacional de Protección de las Infraestructuras Críticas (PNPIC), directiva sancionada el 7 de mayo de 2007, lo mismo que un primer Catálogo Nacional de Infraestructuras Estratégicas y un Acuerdo sobre Protección de Infraestructuras Críticas.

La propia Secretaría de Estado de Seguridad debe asumir la responsabilidad de mantener actualizado el Catálogo, 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.

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 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 definidores de 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: 23).

Respecto al rol de estos últimos, les asiste el deber de nombrar a un Responsable de Seguridad y Enlace, así como a los delegados de seguridad en las infraestructuras críticas identificadas, garantizando su presencia física en la infraestructura afectada en un tiempo prudencial, cuando fuere necesario.

Por su parte, en el ámbito de la ciberseguridad, el CERT de Seguridad e Industria es el encargado de resolver los incidentes cibernéticos que puedan lesionar la prestación de servicios esenciales, entregando un respaldo directo al CNPIC, a partir de la entrega de “servicios de prevención, detección, alerta temprana y respuesta a incidentes, en apoyo a los departamentos encargados de esta labor en el seno de cada organización (Resolución de la Secretaría de Estado de Seguridad, por la que se aprueban los nuevos contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos, 2015: 6).

2. EE.UU.

En EE.UU., en tanto, la infraestructura crítica describe a los activos y sistemas físicos de vital importancia para el país, en tanto su destrucción o inhabilitación tendría un impacto debilitador sobre la economía, la salud pública o la seguridad de la Nación (*Homeland Security*, 2020).

Al respecto, el país norteamericano ha detectado una serie de áreas críticas, cuales son las del sector químico, las instalaciones comerciales, las comunicaciones, el rubro manufacturero, las represas, la base industrial de la defensa, los servicios de emergencia, la energía, la alimentación y agricultura, las oficinas de gobierno, el sector salud, los reactores nucleares, los materiales de desecho, el sistema de transporte y los sistemas de agua (*Cybersecurity & Infrastructure Security Agency*, 2020a).

Estos sectores son cautelados por el llamado *National Infrastructure Coordinating Center* (NICC), entidad que forma parte de la División de Seguridad e Infraestructura de la *Cybersecurity and Infrastructure Security Agency* (CISA), así como del Centro de Operaciones Nacionales del Departamento de Seguridad Interior, con un funcionamiento permanente, coordinando y compartiendo datos sobre la situación de la infraestructura crítica del gobierno federal.

En caso de algún incidente contra estos reductos, el NICC se encarga de aglutinar los esfuerzos de colaboración entre el Departamento de Seguridad Interior y los operadores del rubro afectado (*Cybersecurity & Infrastructure Security Agency*, 2020b).

Respecto al ámbito legal, el 16 de noviembre de 2018, el entonces Presidente estadounidense, Donald Trump, firmó la *Cybersecurity and Infrastructure Security Agency Act*, que establece mecanismos de cooperación público-privados, entregando asistencia técnica y emitiendo análisis a actores federales, así como a propietarios y operadores de infraestructura.

De acuerdo a la sección 2202 de la norma, el Director de la *Cybersecurity and Infrastructure Security Agency* tiene entre sus responsabilidades (*Cybersecurity and Infrastructure Agency Act*, 2018):

- Liderar los programas de seguridad en materia de infraestructura crítica, considerando actividades de respuesta frente a incidentes asociados a activos de interés nacional.
- Articular estrategias de cooperación con agencias federales, no federales e internacionales.
- Coordinar un esfuerzo nacional para enfrentar las amenazas a la infraestructura crítica.
- Entregar análisis, experiencia y asistencia técnica a los operadores de infraestructura crítica, de manera mancomunada con otras agencias sectoriales de alcance federal.
- Desarrollar, coordinar e implementar planes estratégicos comprehensivos para las actividades de la Agencia.

Por último, cabe mencionar los principales lineamientos del Plan Estratégico 2023-2025 de la CISA, cuyo foco es (CIS, 2022):

- Liderar el esfuerzo nacional por asegurar la defensa y resiliencia del ciberespacio,contra actores que busquen lesionar la infraestructura crítica del país, tanto a nivel gubernamental como privado.

- Fortalecer los activos críticos, de manera de adaptarlos a las cambiantes condiciones del entorno y prepararlos para una rápida recuperación ante ataques hostiles.

- Propiciar el trabajo colaborativo con las agencias oficiales, la industria, el sector académico y los socios internacionales del país.

3. Francia

El 7 de julio de 2009 fue creada en Francia la Agencia Nacional de Ciberseguridad (ANSSI), cuyas funciones fueron precisadas cuatro años más tarde, mediante la *Critical Infrastructures Information Protection Law* (CIIP), de 19 de diciembre de 2013.

Esta norma estipula que el Primer Ministro del país debe fijar políticas y coordinar la acción oficial en el campo de la ciberseguridad y la ciberdefensa, para lo cual se vale, precisamente, de la ANSSI, que queda subordinada al Secretario General para la Defensa y la Seguridad Nacional.

En concreto, las misiones de la ANSSI están detalladas en el artículo 22 de este texto legal, apuntando a incrementar los niveles de seguridad de los operadores de servicios críticos, establecer un nivel común mínimo de ciberseguridad para cada operador y exigir reportes de incidentes detectados en estos sistemas (*The National Cybersecurity Agency of France*, 2020).

Esta ley es aplicable a más de 200 operadores públicos y privados, de doce sectores identificados como críticos, los cuales deben notificar directamente a la ANSSI acerca de cualquier incidente que afecte a sus sistemas críticos de información, cautelando la confidencialidad de cada operador, al tiempo que la ANSSI debe implementar planes de gestión de crisis para el buen funcionamiento del sector (*The French CIIP Framework*, 2020).

De igual modo, el 16 de octubre de 2015 fue anunciada la Estrategia Nacional Digital, cuyo fin es apoyar la transición digital de la sociedad francesa, como resultado de un conjunto de esfuerzos coordinados entre diversos departamentos gubernamentales.

Esta evolución favorece la innovación y el crecimiento, abordando diversas problemáticas en el ámbito de la ciberseguridad e identificando cinco prioridades estratégicas, entre las que se incluyen los intereses fundamentales de la defensa y seguridad del país, como las infraestructuras críticas y de sistemas, vinculadas a operadores esenciales para la economía y sociedad del país (*Cibersecurity in France*, 2020).

Precisamente, las actividades críticas en Francia son aquellas que contribuyen a la producción y distribución de bienes y servicios esenciales para el Estado, en cuanto al ejercicio de su autoridad, la función económica, la defensa continua y la seguridad nacional (*The Critical Infrastructure Protection in France*, 2017: 1).

Al respecto, existen cuatro áreas de responsabilidad, que aglutinan a doce sectores de importancia crítica para el país, a saber (*Strategic Review of Cyber Defence*, 2018):

- Necesidades humanas básicas: alimentación, gestión del agua y salud.
- Soberanía: actividades civiles, actividades legales y actividades militares.
- Economía: energía, finanzas y transporte.
- Tecnología: comunicación, tecnologías, e industria espacial e investigación.

La responsabilidad del Estado ante la ciberseguridad comprende una serie de objetivos estratégicos, entre los que se cuenta el fortalecimiento de la protección de la infraestructura crítica, a partir de la protección de los operadores de vital importancia.

Esta labor se hace incrementando los requerimientos de regulación de seguridad exigibles a los operadores en el ámbito de las comunicaciones electrónicas y en la provisión de servicios eléctricos (*Strategic Review of Cyber Defence*, 2018).

Sobre este punto en particular, el Primer Ministro del país delega en la Secretaría General para la Defensa y la Seguridad Nacional, la responsabilidad de coordinar y organizar el sistema, determinando el ámbito de la política

de protección de infraestructura crítica contra actos maliciosos y riesgos tecnológicos, aprobando la Directiva de Seguridad Nacional y fijando las reglas que deben seguir los operadores.

El Ministerio del Interior, a su vez, supervigila la organización territorial del sistema, apoyando la acción a nivel zonal y departamental.

Cada cartera sectorial, en tanto, debe diseñar los requerimientos de su área, en función de la Directiva de Seguridad Nacional, definiendo desafíos, vulnerabilidades y amenazas.

Por su parte, la Prefectura de Defensa y Zona de Seguridad se encarga de organizar, respaldar a las prefecturas territoriales y enlazar la información entre los niveles central y local, al tiempo de inspeccionar la infraestructura crítica dentro de su área de jurisdicción.

En tanto, las prefecturas departamentales aprueban el plan de protección específico para cada operador, definiendo las medidas de vigilancia e intervención a adoptar ante algún ataque o amenaza contra los sectores más sensibles.

Los operadores críticos, finalmente, tienen que asumir varios tipos de responsabilidad, como el nombramiento de oficiales de enlace de seguridad; el diseño de planes de seguridad operacional y de programas específicos de protección para cada sector sensible identificado; y la adecuación de sus medidas con el llamado "Plan VIGIPIRATE". Todo lo anterior, en consonancia con los estándares del Programa Europeo para la Protección de Infraestructura Crítica (*The Critical Infrastructure Protection in France*, 2017: 2-4).

A su vez, uno de los objetivos planteados por la Estrategia de Ciberseguridad, es velar por los intereses fundamentales, la defensa y seguridad de los sistemas de información e infraestructura crítica del Estado, para lo cual se creó el llamado *Expert Panel for Digital Trust*, que opera bajo la égida de la Secretaría de Estado para la Tecnología Digital y de la Autoridad Nacional para la Seguridad de los Sistemas de Información.

Finalmente, Francia ha continuado aportando a la consolidación de un ambiente colaborativo frente a las crisis cibernéticas de nivel europeo, respaldando el trabajo de la *European Union Agency for Network and Information Security* (ENISA); del *Computer Emergency Response Team*, de la Unión Europea; y de la *Computer Incidence Response Capability*, de la Organización del Tratado del Atlántico Norte (OTAN) (*French National Digital Security Strategy*, 2015: 14-17).

4. Uruguay

El modelo de protección de infraestructuras críticas uruguayo, surge desde una concepción del resguardo de los recursos estratégicos como función de la Defensa Nacional.

Según se consagra en el artículo 1 de la Ley 18.650, Ley Marco de Defensa Nacional:

(…) "la Defensa Nacional comprende el conjunto de actividades civiles y militares dirigidas a preservar la soberanía y la independencia de nuestro país, a conservar la integridad del territorio y de sus recursos estratégicos, así como la paz de la República, en el marco de la Constitución y las leyes, contribuyendo a generar las condiciones para el bienestar social, presente y futuro de la población" (Ley 18.650, 2010).

El artículo 18 de la misma norma, así como el artículo 20 de la Ley 19.775, establecen las misiones de las ramas castrenses, entre las cuales mencionan la salvaguarda de los recursos estratégicos del país, según la definición realizada por el Poder Ejecutivo (Ley 18.650, 2010) (Ley 19.775, 2019).

De esta forma, la protección y el fortalecimiento de las infraestructuras vitales y estratégicas para el país, de las cuales dependan la provisión de los servicios y recursos esenciales, como la energía, el agua, el transporte y las comunicaciones, están consagrados entre los lineamientos estratégicos de la Política de Defensa Nacional.

En esta línea, la Política Militar (2016) establece dentro de los objetivos de la Defensa Militar, el empleo de medios militares para proteger la bioseguridad, los recursos naturales estratégicos renovables, no renovables y las infraestructuras críticas, a fin de asegurar las condiciones de seguridad necesarias para el desarrollo económico y social del país, contemplando la seguridad jurídica de los actores económicos.

A su vez, el artículo 22 de la Ley 19.775 dispone entre las tareas subsidiarias de las Fuerzas Armadas, la protección y salvaguarda, ya sea por sí mismas o en coordinación con otros organismos del Estado, de las infraestructuras críticas o vitales que establezca el Poder Ejecutivo.

En otro ámbito, Uruguay también cuenta con la denominada Agencia para el Desarrollo del Gobierno de Gestión Electrónica, y la Sociedad de la Información y del Conocimiento (AGESIC), que conforme al artículo 1 del Decreto 451, de 2009, actúa a través del Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTuy), en el resguardo de los sistemas informáticos que soportan activos de información críticos del Estado, así como los sistemas circundantes a estos.

Más específicamente, el artículo 4 del texto legal le delega las funciones de (Decreto 451, 2009):

- Responder ante incidentes de seguridad informática que afecten a organismos estatales.
- Emprender labores de coordinación con los encargados de la seguridad de la información de los entes oficiales, a fin de prevenir, detectar, manejar y recopilar información sobre incidentes de seguridad informática.
- Articular planes de recuperación frente a desastres, realizando análisis forenses de los incidentes de seguridad informática.
- Mantener actualizado un registro de datos sobre incidentes de seguridad informática en agencias del Estado.

Por último, cabe mencionar el “Plan de Gobierno Digital 2025”, que entre sus líneas de acción contempla un fortalecimiento del ecosistema nacional de ciberseguridad, mejorando la prevención y ampliando las capacidades de respuesta público-privada ante ciberincidentes de naturaleza nacional o transfronteriza (Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento, 2022).

Referencias

Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento. (2022, noviembre 5). Disponible en: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/institucional/plan-estrategico/plan-gobierno-digital-2025.

CIS. (2022, noviembre 5). *Strategic Plan*. Disponible en: https://www.cisa.gov/strategy.

Cybersecurity & Infrastructure Security Agency. (2020, marzo 24). *Critical Infrastructure Sectors*. Disponible en: https://www.cisa.gov/critical-infrastructure-sectors.

Cybersecurity & Infrastructure Security Agency. (2020, octubre 9). *National Infrastructure Coordinating Center*. Disponible en: https://www.cisa.gov/national-infrastructure-coordinating-center.

Cibersecurity in France. (2020, octubre 9). Disponible en: https://www.ssi.gouv.fr/en/cybersecurity-in-france/.

Homeland Security. (2020, julio 14). *Critical Infrastructure Security*. Disponible en: https://www.cisa.gov/infrastructure-security.

Strategic Review of Cyber Defence. (2018, febrero). Disponible en: http://www.sgdsn.gouv.fr/uploads/2018/03/revue-cyber-resume-in-english.pdf.

The Critical Infrastructure Protection in France. (2017, enero). Disponible en: http://www.sgdsn.gouv.fr/uploads/2017/03/plaquette-saiv-anglais.pdf.

The French CIIP Framework (ANSSI). (2020, octubre 9). Disponible en: https://www.ssi.gouv.fr/en/cybersecurity-in-france/ciip-in-france/.

The National Cybersecurity Agency of France. (2020, octubre 9). Disponible en: https://www.ssi.gouv.fr/en/cybersecurity-in-france/the-national-cybersecurity-agency-of-france/.

Textos normativos

Cybersecurity and Infrastructure Agency Act. (2018, noviembre 16). Disponible en: https://www.congress.gov/bill/115th-congress/house-bill/3359/text?overview=closed.

Decreto 451, Centro Nacional de Respuesta a Incidentes de Seguridad Informática. Funcionamiento y organización. (2009, octubre 8). Disponible en: https://www.impo.com.uy/bases/decretos/451-2009.

Ley 8, por la que se establecen Medidas para la Protección de las Infraestructuras Críticas. (2011, abril 28). Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2011-7630.

Ley 18.650, Ley Marco de Defensa Nacional. (2010, marzo 8). Disponible en: https://legislativo.parlamento.gub.uy/temporales/leytemp7206449.htm.

Ley 19.775, Modificación de la Ley Orgánica de las Fuerzas Armadas. (2019, agosto 5). Disponible en: https://www.impo.com.uy/bases/leyes/19775-2019.

Resolución de la Secretaría de Estado de Seguridad, por la que se aprueban los nuevos contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos. (2015, septiembre 8). Disponible en: file:///C:/Users/jjarufe/Downloads/BOE-400_Ambitos_de_la_Seguridad_Nacional_Proteccion_de_Infraestructuras_Criticas.pdf.