Modelos de ciberseguridad en la experiencia internacional

Autor

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

Nº SUP: 139264

Resumen

Los desafíos y amenazas de naturaleza ciberespacial han obligado a que los países adopten normativas, políticas y programas orientados a proteger los activos más sensibles del Estado.

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

En cuanto al paradigma español, el Instituto Nacional de Ciberseguridad es la entidad subordinada al Ministerio de Economía y Empresa, que tiene a su cargo el desarrollo de la ciberseguridad, tanto en lo que respecta a la situación de la sociedad civil, la academia y las compañías privadas, como a la realidad de los sectores estratégicos del país.

A su vez, en Italia, la *Agenzia per la Cybersicurezza Nazionale* es la autoridad nacional de carácter autónomo, que busca proteger el ciberespacio, previniendo y mitigando incidentes, al tiempo de propender a la restauración de los sistemas atacados, mediante alianzas internacionales con agencias de terceros estados, la puesta en marcha de iniciativas público-privadas y el desarrollo de cursos de capacitación para formar una fuerza especializada en ciberseguridad.

Finalmente, el 16 de enero de 2023 entró en vigor la Directiva NIS2 de la Unión Europea, cuyo artículo 1 fija un conjunto de obligaciones para los países del bloque, en cuanto a adoptar estrategias de ciberseguridad y designar autoridades especializadas, para hacer frente a distintas crisis en este ámbito; emitir reportes de ciberseguridad; compartir información; y hacer cumplir las obligaciones asumidas como partes integrantes de la alianza europea.

Introducción

A petición del requirente, el presente informe da cuenta de algunas políticas implementadas en materia de ciberseguridad en la experiencia internacional.

El trabajo recoge la evidencia disponible en paradigmas como los de Argentina, Bélgica, Corea del Sur, España, Italia, Nueva Zelandia y Uruguay, así como las últimas directrices adoptadas por la Unión Europea (UE) sobre este ámbito en particular.

El texto recoge información de los informes BCN "Ciberseguridad e infraestructura crítica: los casos de Bélgica, Estonia, Italia y la UE" (Junio, 2023); "Institucionalidad en ciberseguridad e infraestructura crítica a nivel internacional" (Julio, 2022); "Gobernanza en ciberseguridad: experiencia internacional" (Mayo, 2022); y "Políticas de ciberseguridad en la experiencia internacional" (Diciembre, 2020), todos del mismo autor del presente documento.

I. Ciberseguridad

1. Concepto general

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, 2023).

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 claves".

Cuatro años más tarde, el Consejo Europeo, a partir de su Directiva Nro. 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 una serie de países a nivel internacional.

2. Modelos internacionales

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, 2023):

- 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 integrada 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. Bélgica

En el paradigma belga, en tanto, existe desde el 20 de mayo de 2021 una Estrategia de Ciberseguridad Nacional, aprobada por el Consejo de Seguridad Nacional, que constituye el marco para la aproximación de este país en este ámbito.

Esta directriz es implementada por el Centro para la Ciberseguridad (CCB), autoridad nacional que supervisa, coordina y monitorea su aplicación.

Se trata de una entidad establecida a partir del Real Decreto del 10 de octubre de 2014, que opera bajo la autoridad del Primer Ministro, con las misiones de (*Centre for Cybersecurity Belgium*, 2023a):

- Monitorear, coordinar y supervisar la implementación de esta política sectorial.
- Gestionar los diversos proyectos sobre ciberseguridad, utilizando un enfoque integrado y centralizado.
- Lanzar proyectos que robustezcan la ciberseguridad de sectores vitales para el país, tales como energía, transportes, telecomunicaciones, finanzas, servicios sanitarios y salud.
- Asegurar la coordinación entre los departamentos gubernamentales, el sector privado y actores científicos relevantes.
- Formular propuestas adaptables al marco regulatorio vigente.
- Asegurar un buen manejo de crisis, en caso de ciberincidentes, en consonancia con la labor del Centro de Coordinación y Crisis del gobierno.
- Preparar, divulgar y fiscalizar la implementación de estándares y lineamientos de seguridad para los diversos sistemas de información del gobierno y las instituciones públicas del país.
- Coordinar la participación de Bruselas en foros de ciberseguridad internacionales.
- Coordinar la evaluación de seguridad, así como la certificación de sistemas de comunicación e información.

Bélgica cuenta igualmente con un Plan Nacional de Ciberemergencia, aprobado en 2017, con la participación del CCB y del Centro Nacional de Crisis, cuyo objetivo primordial es responder a las crisis del ciberespacio y los incidentes que requieran una coordinación a nivel nacional (*Centre for Cybersecurity Belgium*, 2023a).

A su vez, existe un Departamento de Inteligencia e Investigación de Ciberamenazas, que revisa cualquier incidente, recolectando, analizando y distribuyendo información sobre vulnerabilidades y ataques a los sistemas críticos de la información y comunicación del país.

También es responsable de emitir un Sistema de Alerta Temprana, que incluye el intercambio de información entre el Equipo de Respuesta ante Incidentes de Seguridad Informática belga (CSIRT) y el de otros estados (*Centre for Cybersecurity Belgium*, 2023b).

A nivel normativo, en tanto, el Código Penal sanciona una serie de conductas ilegales en el ciberespacio, como en el caso del sabotaje informático, concebido en el artículo 550 *ter* como la comisión de cualquier acto sin autorización, que modifique o elimine un sistema de información por medios tecnológicos o no tecnológicos, y castigado con penas de entre seis meses y hasta tres años de prisión, o multa de entre 208 y 200.000 Euros. Si la información resulta dañada, la sanción se eleva hasta cinco años de reclusión y multa de 600 mil Euros.

Asimismo, el *phishing* es castigado por el artículo 504 *quater* con entre seis meses de cárcel y multa de hasta 800 mil Euros (*Code Penal*, 2021).

Por otra parte, conforme al artículo 7 de la *Loi relative à la Sécurité et la Protection des Infrastructures Critiques*, de 2011, cada autoridad sectorial debe emitir un listado de infraestructuras críticas potencialmente susceptibles de ser atacadas, acompañado de un plan de seguridad preventivo, una proyección de escenarios y un análisis de vulnerabilidades, tendientes a neutralizar los riesgos de interrupción del servicio o de destrucción de instalaciones sensibles para el Estado (*Loi relative à la sécurité et la protection des infrastructures critiques*, 2011).

La legislación belga sobre ciberseguridad se vio reforzada además con la aprobación, el 3 de mayo de 2019, de la *Belgian Network and Information Systems Law*, dirigida a mejorar los estándares de seguridad de sectores críticos para el Estado, como economía, seguridad pública, energía, transporte, salud, servicios sanitarios e infraestructura digital (KPMG, 2023).

Finalmente, el 15 de febrero de 2023 entró en vigor en este país una nueva normativa, que legalizó, incluso en ausencia de consentimiento, el llamado "*hacking* ético", concebido como el intento por vulnerar la seguridad de un mecanismo informático, a fin de hallar posibles debilidades a corregir, de manera preventiva a cualquier intrusión de parte de ciberdelincuentes (*Ku Leuven*, 2023).

2.3. Corea del Sur

En el modelo surcoreano, a su vez, 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*, 2023):

- 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*, 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.

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, actuando 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 UE.

- El Comité de Situación: tiene carácter único para el conjunto del Sistema de Seguridad Nacional y funciona 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 compuesta 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 Nro. 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 Nro. 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, 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 Permanente de Ciberseguridad, 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 Nro. 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 Nro. 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 de España, 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, 2023a).

El INCIBE-CERT tiene atribuciones para (INCIBE-CERT, 2023b):

- 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 Organisation* (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, 2023):

- 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. Italia

La *Agenzia per la Cybersicurezza Nazionale* (ACN) es una autoridad nacional de carácter autónomo, establecida en función del Decreto Ley Nro. 82, del 14 de junio de 2021, que busca proteger el ciberespacio italiano, previniendo y mitigando incidentes, al tiempo de propender a la restauración de los sistemas atacados, mediante (ACN, 2023):

- La implementación de la Estrategia Nacional de Ciberseguridad.
- La promoción de un marco regulatorio coherente, con inspecciones periódicas y un régimen de sanciones.
- La consolidación de alianzas internacionales con agencias de terceros estados.
- La coordinación entre actores públicos y la puesta en marcha de iniciativas público-privadas, para fortalecer la autonomía digital del país.
- El desarrollo de cursos de capacitación para formar una fuerza especializada en ciberseguridad, junto a la promoción de campañas que hagan consciente entre la población una cultura de la ciberseguridad.

La estructura de la ACN contempla un Equipo de Respuesta ante Incidentes de Ciberseguridad ("CSIRT Italia"), un Centro Nacional de Coordinación, y un Centro de Certificación y Evaluación Nacional, para el escrutinio tecnológico de los activos digitales estratégicos del país.

Asimismo, en el plano normativo, el artículo 4 del *Decreto-Legge 14, per disposizioni urgenti in materia di Cybersicurezza, Definizione dell'Architettura Nazionale di Cybersicurezza e Istituzione dell'Agenzia per la Cybersicurezza Nazionale*, establece la existencia del *Comitato Interministeriale per la Cybersicurezza*, encargado de asesorar a la Presidencia del Consejo de Ministros en materias de ciberseguridad, proponiendo al titular de este órgano indicaciones generales para proceder en este ámbito (*Decreto-legge 14*, 2021).

En cuanto a la Estrategia Nacional de Ciberseguridad, esta directiva prescribe tres grandes ámbitos de desarrollo en el ciberespacio, como son (*Strategia Nazionale di Cybersicurezza*, 2022-2026):

- La protección de los activos esenciales del Estado, con el objetivo de minimizar riesgos y facilitar la transición digital.
- La respuesta ante vulnerabilidades digitales, apoyando la aplicación de configuraciones de ciberseguridad y favoreciendo el desarrollo criptográfico en el ámbito financiero, en el afán de contribuir a la consolidación de un ecosistema nacional en materia de ciberseguridad. Esta función va en línea con el desarrollo de un sistema de gestión de crisis cibernéticas de alcance nacional y transnacional, denominado *Nucleo per la Cybersicurezza* (NCS), que busca asegurar el despliegue de un mecanismo sinérgico, de coordinación continua entre todos los departamentos del Estado, con una actualización permanente de los procedimientos previstos ante ciberincidentes.
- El desarrollo de las tecnologías digitales y de la competitividad de la industria afín, con el objetivo de estar en sintonía con las necesidades del país en materia de ciberseguridad.

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 y apoyar a las organizaciones de infraestructura crítica nacional, estimulándolas a ser responsables de sus propios sistemas, usando ciber-herramientas 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 principios estratégicos del país (*Department of the Prime Minister and Cabinet*, 2023).

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 (NCSC, 2023):

- 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 (NCSC, 2023):

- 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*.

2.7. UE

El 27 de diciembre de 2022 fue publicada y el 16 de enero del presente año entró en vigor la Directiva NIS2 de la UE (*European Parliament*, 2023: 12), cuyo artículo 1 fija un conjunto de obligaciones para los estados miembros del bloque, en cuanto a adoptar estrategias de ciberseguridad y designar autoridades especializadas en la materia, para hacer frente a distintas crisis en este ámbito; emitir reportes de ciberseguridad; compartir información; y supervisar y hacer cumplir las obligaciones asumidas como partes integrantes de la alianza europea.

El siguiente artículo, en tanto, dispone la aplicación de esta Directiva para organismos públicos y privados, sin consideración del tamaño de cada entidad.

Bajo esta lógica, el artículo 7 del texto legal precisa que las antes mencionadas estrategias de ciberseguridad diseñadas por cada país, tienen que incluir (*Directive (EU) 2.555*, 2022):

- Objetivos y prioridades en la cobertura de sectores vitales.
- Un marco de gobernanza para alcanzar las metas trazadas en el punto anterior.
- El establecimiento de roles y responsabilidades claros para el caso de los agentes relevantes del sistema a nivel nacional.
- La coordinación y cooperación entre autoridades gubernamentales y equipos de respuesta ante crisis.
- Los mecanismos que permitan identificar los activos críticos, junto a una evaluación de riesgos.
- La disposición de medidas para responder ante ciberincidentes, así como para recuperar las capacidades afectadas, con un foco en la colaboración público-privada.
- El diseño de un plan para incrementar la conciencia ciudadana en torno a materias de ciberseguridad.
- La puesta en marcha de directrices que promuevan el desarrollo e integración de tecnologías avanzadas para la implementación de medidas de gestión de riesgos en el ciberespacio.

Junto a lo anterior, la norma dispone que la Agencia para la Ciberseguridad de la UE (ENISA) debe asesorar a los decisores de gobierno en la revisión, al menos quinquenal, de las estrategias de seguridad de cada país.

Este organismo, conforme al artículo 18 del texto, también debe remitir al Parlamento Europeo un reporte bienal sobre el estado de la ciberseguridad en el bloque, incluyendo aspectos como el nivel de riesgo en el ciberespacio y un análisis del desarrollo de cibercapacidades, tanto a nivel público como privado.

De igual modo, el artículo 9 puntualiza que los estados miembros deben adoptar un plan nacional a gran escala para hacer frente a crisis e incidentes en el ciberespacio, considerando tareas, procedimientos de gestión, ejercicios de entrenamiento y alianzas público-privadas.

Respecto a los equipos de respuesta ante incidentes, el artículo 11 les encomienda las misiones de (*Directive (EU) 2.555*, 2022):

- Monitorear y analizar en tiempo real las redes y sistemas de información.
- Entregar alertas tempranas y divulgar información que sea relevante para las autoridades, en materia de ciberamenazas, vulnerabilidades e incidentes.
- Responder ante eventos críticos, con asistencia a las entidades afectadas.
- Recoger y analizar información sensible, realizando análisis de riegos situacionales.

Finalmente, el artículo 23 de la norma obliga a las entidades especializadas de cada estado parte a notificar a la brevedad cualquier ciberincidente en sus servicios esenciales, teniendo presente que un ciberataque será considerado significativo cuando sea capaz de causar una severa disrupción operacional en los servicios; una pérdida financiera estimable; o un perjuicio material o inmaterial sobre personas naturales o jurídicas.

2.8. Uruguay

En el paradigma uruguayo, el Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTuy) fue creado en 2008, a partir de la publicación de la Ley Nro. 18.362, con el objetivo de proteger los activos de información críticos del Estado y promover el conocimiento en seguridad de la información, de manera de prevenir y responder a los incidentes de seguridad.

El CERTuy está conformado por un grupo de expertos responsables del desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información.

Sus principales objetivos son (Agencia de Gobierno Electrónico, y Sociedad de la Información y del Conocimiento, 2023a):

- Centralizar, coordinar y optimizar los procesos de respuesta a incidentes en seguridad de la información.
- Realizar tareas preventivas.
- Difundir mejores prácticas en seguridad de la información.

El primer objetivo es abordado por el *Computer Emergency Response Team / Coordination Center*, un equipo de respuesta y un centro de coordinación de emergencias informáticas que actúa cuando ocurre un incidente informático, como el acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; el impedimento en la operación normal de las redes, sistemas o recursos informáticos; o la violación a la Política de Seguridad de la Información del organismo.

Por su parte, el Centro de Operaciones de Ciberseguridad tiene la función de detectar en tiempo real eventos e incidentes de ciberseguridad en los Activos de Información Críticos del Estado, así como colectar y analizar información de ciberseguridad, para prevenir y detectar incidentes de ciberseguridad.

En Uruguay, la política digital nace a partir de la “Agenda Uruguay Digital”, hoja de ruta que fija, prioriza, articula y transmite los programas de desarrollo de la sociedad de la información y el conocimiento en el sector público, mediante una visión de alcance nacional, fórmulas de seguimiento y sustentabilidad.

Esta directriz se hace operativa mediante dos grandes planes de acción, como son (Agencia de Gobierno Electrónico, y Sociedad de la Información y del Conocimiento, 2023a):

- Plan de Gobierno Digital, que puntualiza el destino de los proyectos prioritarios de transformación digital del gobierno, por medio de las oportunidades que entrega el empleo de las tecnologías, en un enfoque integrado entre el Estado, la ciudadanía, la industria y la academia.

- Plan de Acción de Gobierno Abierto, que tiene como fin robustecer la democracia y el Estado de Derecho, a partir de la inclusión de un saber colectivo, sustentado en principios como la transparencia, la participación ciudadana y el *accountability*.

Este esquema adquiere entidad gracias a la labor de la Agencia de Gobierno Electrónico, y Sociedad de la Información y del Conocimiento (AGESIC), entidad con autonomía técnica, creada en virtud de la Ley Nro. 17.930, de diciembre de 2005, que se encuentra subordinada a la Presidencia del país.

El funcionamiento de este organismo aparece regulado en el artículo 2 del Decreto Nro. 205, de junio de 2006, que fija entre sus objetivos generales (Agencia de Gobierno Electrónico, y Sociedad de la Información y del Conocimiento, 2023b):

"(…) la mejora de los servicios al ciudadano, utilizando las posibilidades que brindan las tecnologías de la información y las comunicaciones, así como el impulso al desarrollo de la sociedad de la información en el país, con énfasis en la inclusión de la práctica digital de sus habitantes y el fortalecimiento de las habilidades de la sociedad en la utilización de las tecnologías".

Asimismo, el artículo 55 de la Ley Nro. 18.046, de Rendición de Cuentas, de octubre de 2006, añade como nuevas metas la planificación y coordinación de iniciativas vinculadas con el gobierno electrónico, como sustento para una mayor transparencia de los procesos estatales, y para una mejor prevención y respuesta ante incidentes que pudiesen lesionar los activos más sensibles del país.

A nivel específico, en tanto, el Decreto Nro. 184, de 14 de julio de 2015, faculta a la AGESIC para (Agencia de Gobierno Electrónico, y Sociedad de la Información y del Conocimiento, 2023b):

- Esbozar los programas y la Estrategia Nacional de Desarrollo de Gobierno Electrónico y Gobierno Abierto.
- Sugerir medidas a los órganos estatales y no estatales, al momento de diseñar planes de gobierno electrónico.
- Normar la implementación de acciones relacionadas con la puesta en marcha de proyectos particulares de gobierno electrónico, por medio de la articulación de fórmulas tales como fondos concursables y planes directores de gobierno electrónico.
- Elaborar las directrices y la estrategia nacional de gobernanza, integración, interoperabilidad, capital humano y compras relativas a las tecnologías de la información en organismos públicos.
- Formular reglas técnicas para servicios atingentes a las tecnologías de la información en entes públicos, al tiempo de efectuar auditorías, seguimientos y análisis.
- Desarrollar planes específicos para la realización de trámites y servicios en línea, en aras de avanzar hacia una gestión pública moderna, eficaz y eficiente.
- Estimular la vinculación entre la ciudadanía y el Estado, mediante un mejor acceso a la tecnología y una política de inclusión digital.
- Fijar metodologías y consagrar buenas prácticas en la seguridad de la información.
- Entablar relaciones con sus pares de otros estados, así como con organismos nacionales e internacionales, tanto públicos como privados.

En la misma línea, el artículo 149 de la Ley Nro. 18.719, de 5 de enero de 2011, encomienda a la AGESIC la dirección de las políticas, metodologías y mejores prácticas en materia de ciberseguridad a nivel nacional, así como la fiscalización de las medidas de implementación de estas directrices en las entidades públicas y privadas que se vinculan con los sectores críticos del país, que se efectúan a través de la Dirección de Seguridad de la Información, que alberga al Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTuy).

A su vez, el artículo 119 de esta norma crea el Consejo Asesor Honorario de Seguridad de la Información, conformado por el Director de Seguridad de la Información de la AGESIC, un miembro académico y un representante de la Presidencia de la República, el Ministerio de Defensa Nacional, el Ministerio del Interior, el

Ministerio de Industria, Energía y Minería, el Banco Central del Uruguay, y la Unidad Reguladora de Servicios de Comunicaciones (Presupuesto Nacional 2020-2024, s/i: 35-36).

En tanto, el D-CSIRT es un Equipo de Respuesta a Incidentes de Seguridad Informática de Defensa, creado por el Decreto Nro. 36, de 27 de enero de 2015, cuya tarea es "participar de forma eficaz y eficiente en la respuesta a incidentes cibernéticos sobre infraestructuras críticas y servicios esenciales de la comunidad objetivo, así como desarrollar capacidades de prevención y detección temprana de incidentes de seguridad informática" (Centro Nacional de Respuesta a Incidentes de Seguridad Informática, 2023).

Los objetivos generales de esta instancia son hacer las veces de punto de contacto para su comunidad ante la ocurrencia de incidentes cibernéticos; ser enlace del Ministerio de Defensa, en la respuesta a incidentes informáticos internos y externos; concientizar y capacitar a la comunidad nacional en materia de ciberseguridad; impulsar investigaciones en el ámbito de la seguridad informática; y colaborar activamente con el CERTuy.

A su vez, entre sus objetivos específicos, se encuentran (Ministerio de Defensa Nacional de Uruguay, 2023):

- La coordinación de respuestas ante ciberincidentes, con la emisión de alertas y avisos.
- La implementación de una Política de Gestión de Riesgos de Activos de Información, así como de una metodología para detectar amenazas, en coordinación con las directrices establecidas por el CERTuy.
- La identificación, planificación y coordinación de actividades de protección de activos críticos.

Referencias

ACN. (2023). *About Us*. Disponible en: https://www.acn.gov.it/en/agenzia/chi-siamo.

Agencia de Gobierno Electrónico, y Sociedad de la Información y del Conocimiento. (2023, agosto 22). Cometidos. Disponible en: http://bcn.cl/2l030.

Agencia de Gobierno Electrónico, y Sociedad de la Información y del Conocimiento. (2023, agosto 22). CERTuy. Disponible en: http://bcn.cl/30e48.

Argentina.gob.ar. (2023, agosto 21). Objetivos de la Dirección Nacional de Ciberseguridad. Disponible en: http://bcn.cl/33km3.

Centre for Cybersecurity Belgium. (2023). *Organisation*. Disponible en: https://ccb.belgium.be/en/organisation.

Centre for Cybersecurity Belgium. (2023). *Vital sectors*. Disponible en: https://ccb.belgium.be/en/vital-sectors.

Centro Nacional de Respuesta a Incidentes de Seguridad Informática. (2023, agosto 22). Cometidos. Disponible en: http://bcn.cl/30d2g.

CISCO. (2023, agosto 21). ¿Qué es la ciberseguridad? Disponible en: http://bcn.cl/33jwp.

Code Penal. (2021, febrero 24). Disponible en: https://legislationline.org/sites/default/files/documents/6e/BELG_CC_fr.pdf.

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

Consejo Europeo. (2008). En Horzella, Bárbara. [2019, diciembre]. Protección de Infraestructura Crítica y Fuerzas Armadas. Conceptualización y experiencia comparada. BCN. Disponible en: http://bcn.cl/2lf8z.

Decreto-legge 14, Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale. (2021, junio 15). Disponible en: https://www.gazzettaufficiale.it/eli/id/2021/06/14/21G00098/SG.

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

Directive (EU) 2022/2.555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No. 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). (2022, diciembre 27). Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555.

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 Parliament. (2023). *The NIS2 Directive. A high common level of cybersecurity in the EU*. Disponible en: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf.

INCIBE. (2023, agosto 21). Red de Excelencia Nacional de Investigación en Ciberseguridad. Disponible en: https://www.incibe.es/incibe/informacion-corporativa/con-quien-trabajamos/red-excelencia-idi.

INCIBE-CERT. (2023, agosto 21). Qué es INCIBE-CERT. Disponible en: http://bcn.cl/30czu.

INCIBE-CERT. (2023, agosto 21). Respuesta a incidentes. Disponible en: http://bcn.cl/30d01.

Korea Internet & Security Agency. (2023, agosto 22). *About KISA*. Disponible en: http://bcn.cl/33kms.

KPMG. (2023). *NIS - Belgium's first complete cyber security...* Disponible en: https://kpmg.com/be/en/home/insights/2020/04/ta-nis-belgium-first-complete-cyber-security-legislation.html.

Ku Leuven. (2023, mayo 3). *Belgium legalises ethical hacking: a threat or an opportunity for cybersecurity?* Disponible en: https://www.law.kuleuven.be/citip/blog/belgium-legalises-ethical-hacking-a-threat-or-an-opportunity-for-cybersecurity/.

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

Loi relative à la sécurité et la protection des infrastructures critiques. (2011, julio 1). Disponible en: https://centredecrise.be/sites/default/files/documents/files/2021-03/PDFsam_15_2.pdf.

Ministerio de Defensa Nacional de Uruguay. (2023, agosto 22). Equipo de Respuesta a Incidentes de Seguridad Informática de Defensa (D-CSIRT). Disponible en: http://bcn.cl/30d2j.

NCSC. (2023, agosto 22). *What we do*. Disponible en: http://bcn.cl/30ghn.

New Zealand's Cyber Security Strategy. (2019). Disponible en: http://bcn.cl/2lkwg.

Presupuesto Nacional 2020-2024. (s/i). Disponible en: http://bcn.cl/304re.

Strategia Nazionale di Cybersicurezza. (2022-2026). Disponible en: https://www.acn.gov.it/ACN_Strategia.pdf.