Facultades de las instituciones de ciberseguridad en la experiencia internacional

Jana Abujatum S.
jabujatum@bcn.cl

Juan Pablo Jarufe Bader
jjarufe@bcn.cl

SUP Nro. 139804

Introducción

A petición del requirente, el presente informe da cuenta de algunas de las tareas y facultades de las agencias de ciberseguridad en Alemania, Argentina, Bélgica, España, Italia, así como las directrices adoptadas por la Unión Europea (UE) en el ámbito de la ciberseguridad.

Alemania

La Oficina Federal para la Seguridad Digital (*Bundesamt für Sicherheit in der Informationstechnik* – BSI[1]), creada en 1990 y dependiente del Ministerio Federal del Interior, es la autoridad federal central para la ciberseguridad en Alemania. Esta entidad es responsable de la seguridad y la protección de la red de Alemania, a la vez que brazo ejecutor de la agenda gubernamental para la ciberseguridad.

El BSI diseña la seguridad de la información en la digitalización a través de la prevención, detección y respuesta para el Estado federal alemán. Además, es responsable de desarrollar e implementar estándares de seguridad criptográfica para la comunicación gubernamental, a la vez que de proteger las comunicaciones gubernamentales contra ataques cibernéticos. También proporciona asesoramiento criptográfico y capacitación a las agencias gubernamentales y a las organizaciones privadas que trabajan con el gobierno.

Anualmente, el BSI debe informar sobre su labor, tanto a la Comisión del Interior y Cohesión Territorial del *Bundestag*[2], como al Comisionado Federal para la Protección de Datos y Libertad de Información[3].

Las funciones y atribuciones del BSI están definidas por la Ley para la Oficina Federal de Seguridad de la Información (*BSI-Gesetz – BSIG, 2009*).

En esta línea, las funciones que le otorga la ley al BSI son, de acuerdo a lo dispuesto en el artículo 3°, defender al sistema de seguridad informático federal, desarrollar requisitos de seguridad tecnológicas, asesorar y apoyar a las agencias federales en temas de seguridad en tecnología de la información, así como también apoyar a:

- 13. a) la policía y las autoridades encargadas de hacer cumplir la ley en el desempeño de sus tareas legales,

---

[2] *Ausschuss für Inneres und Heimat*. Disponible en: https://www.bundestag.de/inneres

[3] *Bundesbeauftragten für den Datenschutz und die Informationsfreiheit.* https://www.bfdi.bund.de/DE/Home/home_node.html

> b) las autoridades de protección constitucional y el Servicio de Inteligencia Militar[4], en lo que respecta a la evaluación y valoración de la información que surja de la observación de esfuerzos terroristas o actividades de inteligencia dentro del alcance de las competencias estatutarias, bajo las leyes federales y estatales de protección constitucional o de acuerdo a la Ley del Servicio de Inteligencia Militar (*MAD-Gesetz, 1990*),
> c) del Servicio Federal de Inteligencia en el desempeño de sus funciones estatutarias.
> El apoyo solo podrá otorgarse en la medida en que sea necesario para prevenir o investigar actividades que vayan dirigidas contra la seguridad de las tecnologías de la información o que tengan lugar utilizando estos sistemas. Las solicitudes de apoyo deberán ser registradas por la Oficina Federal;

Por su parte, el artículo 3a dispone que la Agencia de Seguridad Digital podrá, en el caso que sea necesario, procesar datos personales, labor que debe estar enmarcada según lo dispuesto por el Reglamento (UE) 2016/679 del Parlamento Europeo.

A su vez, el artículo 4° señala que el BSI es, entre otras cosas, el órgano central para la cooperación entre las autoridades federales en materia de seguridad en tecnologías de la información; la recopilación y evaluación de todos los datos necesarios para evitar amenazas a la seguridad en las tecnologías de la información, en particular en lo que respecta a brechas de seguridad, *malware*, ataques a la seguridad en las tecnologías de la información que se hayan realizado o intentado, y los procedimientos observados. En tal contexto, los proveedores de energía y las empresas de telecomunicaciones tienen la obligación de informar a la BSI de todo ataque.

La Ley ha tenido y está en reformas para otorgar a la agencia mayores atribuciones. Es así como el año 2021 fueron ampliadas las facultades del BSI y se obliga a los operadores de infraestructuras críticas a cumplir con el Reglamento de Infraestructura Crítica (BSI-Kritisverordnung, 2016), para garantizar la ciberseguridad dentro de los sistemas de infraestructura crítica. Esta medida tiene como objetivo garantizar la prestación de servicios a la economía y la sociedad dentro de los sectores catalogados como críticos, a través de protocolos de ciberseguridad mejorados.

A partir de mayo de 2023, y según lo dispuesto por el artículo 8°, la ley obliga a los operadores de infraestructura crítica a integrar sistemas de detección de ataques en sus medidas de seguridad técnica y organizativa.

A partir de 2023 y 2024, el ámbito de aplicación del Reglamento de Infraestructura Crítica se ampliará. Esta ampliación será doble, debido a que más empresas entrarán en su ámbito de aplicación, según lo dispuesto por la normativa de la Unión Europea (NIS2, 2022).

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.

[4] *Militärisches Abschirmdienst-MAD*. https://www.bundeswehr.de/de/organisation/weitere-bmvg-dienststellen/mad-bundesamt-fuer-den-militaerischen-abschirmdienst

- 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.

Bélgica

El Centro para la Ciberseguridad (CCB) es 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.

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).

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.

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.

Italia

La *Agenzia per la Cybersicurezza Nazionale* (ACN) es una autoridad nacional de carácter autónomo, establecida en función del Decreto Ley 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.

Unión Europea

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.

Referencias

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

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

Bundesamt für Sicherheit in der Informationstechnik. Disponible en: https://www.bsi.bund.de/DE/Home/home_node.html.

BSI-Gesetz. (2009). Disponible en: https://www.gesetze-im-internet.de/bsig_2009/BSIG.pdf.

BSI-Kritisverordnung. (2016). Última modificación de 23 de febrero de 2023. Disponible en: https://www.gesetze-im-internet.de/bsi-kritisv/BJNR095800016.html.

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 .

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.
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 .

Militärischen Abschirmdienst Gesetz. (1990). Disponible en: https://www.gesetze-im-internet.de/madg/MADG.pdf.

NIS2. (2022). *Directive (EU) 2022/2555 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*. Disponible en: https://www.nis-2-directive.com/.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679.