Política Nacional de Ciberseguridad: 2017-2022

Autor

Verónica Barrios Achavar
Email: vbarrios@bcn.cl
Tel.: (56) 32 226 3179
(56 2) 22701884

Nº SUP: 116794

Resumen

La revolución que ha vivido el denominado ciberespacio no sólo ha traído consigo avances a la humanidad, sino también esta causando un aumento en crímenes tecnológicos, con *hackers* cada vez más sofisticados a la hora de generar estafas, espionaje entre naciones e infectar equipos, entre otros. A ello se suma el peligro al que está expuesta la infraestructura crítica de un Estado, el cual puede verse seriamente colapsado por un ataque cibernético.

Por ello, es que la Ciberseguridad ha dejado de ser un tema circunscrito al ámbito técnico, pasando a ser parte de la Política Pública, situación a lo que no es ajeno nuestro país, que en el año 2017 dio a conocer la primera Política Nacional de Ciberseguridad, la que deberá negociar cursos de acción en el legislativo y lograr consolidar una educación y cultura ciber, aún desconocida especialmente en el ámbito público nacional.

En forma previa y de acuerdo a lo expuesto en la Agenda Digital y con el fin de formular una estrategia en materia de seguridad cibernética, en abril de 2015, y mediante el Decreto Supremo N° 533, se creó el Comité Interministerial sobre Ciberseguridad (CICS).

La Política Nacional de Ciberseguridad se articula en dos ejes centrales, el primero de ellos establece una agenda con disposiciones específicas para ser implementadas entre los años 2017-2018, y objetivos a largo plazo orientados al año 2022, siendo su principal objetivo el lograr para Chile un ciberespacio libre, abierto, seguro y resiliente.

Introducción

Debido a la creciente dependencia del ciberespacio, la seguridad de su infraestructura, y las interacciones humanas que allí tienen lugar lo han transformado en una de las preocupaciones contemporáneas, y la gestión de dichos riesgos una prioridad a nivel global.

Infraestructuras críticas como los servicios básicos, transportes, sector financiero y la administración del Estado son susceptibles de ser atacadas en el ciberespacio, pudiendo amenazar la estabilidad, seguridad y soberanía de los países de múltiples formas.

En el ámbito de la Defensa, hoy se considera al ciberespacio como un ambiente en el que se desenvuelven conflictos de diversa naturaleza, nacionales e internacionales. Esto se traduce en la definición del ciberespacio como una dimensión diferente al espacio terrestre, aéreo y marítimo, que requiere contar con políticas, planificaciones y capacidades que permitan ejercer los roles propios de la Defensa Nacional en este ámbito.

I. Antecedentes previos a la Política de Ciberseguridad

El año 2014, la Orden Ministerial N°1 dispuso la actualización de los planes y políticas de la defensa nacional, con miras a su inclusión en el Libro de la Defensa 2017. En la misma línea, la Orden Ministerial N°2, de 2015, instruyó el diseño de una política de Ciberdefensa, que debía ser elaborada en paralelo al mencionado Libro Blanco.

Posteriormente, mediante la Orden Ministerial Nº3, se ordenó al Estado Mayor Conjunto la elaboración de la planificación secundaria en materia de Ciberseguridad. Esta programación contempla las necesidades del EMCO en materia de infraestructura, personal, capacitación y equipamiento.

De esta forma el desafío del Ciberespacio fue abordado a nivel nacional, a través del establecimiento del Comité Interministerial sobre Ciberseguridad, órgano asesor de la Presidencia de la República, que junto con proponer una Política Nacional de Ciberseguridad, debe asesorar en la coordinación de acciones, planes y programas en materia de Ciberseguridad, conforme el Decreto Supremo Nº533, de 27 de abril de 2015, que lo creó. El Ministerio de Defensa integra el Comité Interministerial, representados por el Sr. Subsecretario de Defensa, quien está a cargo de la Secretaría Ejecutiva del Comité.

Por las características propias del Ciberespacio, sus políticas deben ser objeto de evaluación y actualización constante, a fin de garantizar un ciberespacio libre, abierto, seguro y resiliente.

II. Política Nacional de Ciberseguridad

En abril de 2017 el gobierno de la ex presidenta Bachelet dio a conocer la *Política Nacional de Ciberseguridad 2017-2022*, (en adelante, PNCS), constituyéndose en el primer instrumento de política pública del Estado de Chile tendiente a desarrollar una estrategia nacional en esta materia, con el propósito de contar con un ciberespacio libre, abierto, seguro y resiliente.

La PNCS se articula en dos secciones centrales, la primera de ella establece una agenda con disposiciones específicas para ser implementadas entre los años 2017-2018, y objetivos a largo plazo orientados al año 2022.

a. Objetivos de la Política de Ciberseguridad para 2022

En este eje articulador, se establecen los lineamientos generales que la Política Nacional de Ciberseguridad pretende alcanzar al año 2022, así como también los subobjetivos necesarios para poder concretarlos.

A continuación, se describen estos pilares y sus respectivos cursos de acción:

1. **El país contará con una infraestructura de la información robusta y resiliente, preparada para resistir y recuperarse de incidentes de Ciberseguridad, bajo una óptica de gestión de riesgos.**

Este primer pilar busca llegar a contar con una infraestructura de la información robusta y resiliente[1], preparada para resistir y recuperarse de incidentes de Ciberseguridad, bajo una óptica de gestión de riesgos.

Para el logro de lo planteado se hace necesario cumplir con:

- estipular medidas técnicas tendientes a prevenir, gestionar y superar los riesgos cuando estos se verifican a fin de proteger la infraestructura de la información;
- identificar y jerarquizar las infraestructuras críticas de la información;
- contar con equipos de respuesta a incidentes de Ciberseguridad;
- implementar mecanismos estandarizados de reporte, gestión y recuperación de incidentes;
- fijar estándares diferenciados en materia de Ciberseguridad.

2. **El Estado velará por los derechos de las personas en el Ciberespacio**

Este objetivo se centra en proteger los derechos de los ciudadanos en el ciberespacio, responsabilidad que recae en el Estado. Para su cumplimiento será necesario:

- la prevención de ilícitos y generación de confianza en el ciberespacio;
- el establecimiento de prioridades en la implementación de medidas sancionatorias;
- la existencia de prevención multisectorial;
- el respeto y la promoción de derechos fundamentales.

3. **Chile desarrollará una cultura de la Ciberseguridad en torno a la educación, buenas prácticas y responsabilidad en el manejo de tecnologías digitales.**

La necesidad de educar a los ciudadanos en una cultura ciber lleva al desarrollo de este tercer pilar estratégico:

[1] La Resiliencia en el ámbito de la Tecnología de la Información (TI) se entiende como la capacidad de la infraestructura, ya sea de servidores, comunicaciones o de seguridad, de proveer y mantener una continuidad operacional, a pesar de las fallas, tales como: problemas por sobrecarga, fallas en el datacenter , ancho de banda saturada, tráfico malicioso en la organización, amenazas avanzadas al descubierto, filtración de información confidencial y de ataques de secuestro digital de información (ransomware), etc.. Esta capacidad adquiere especial importancia en la Administración Pública y los Sistemas de Información y Telecomunicaciones.

- Una cultura de la Ciberseguridad;
- Sensibilización e información a la comunidad;
- Formación para la Ciberseguridad.

4. El país establecerá relaciones de cooperación en Ciberseguridad con otros actores y participará activamente en foros y discusiones internacionales.

El ciberespacio constituye un ámbito mundial por lo que se hace necesario desplegar estrategias globales para su pleno y positivo desarrollo. La cooperación internacional resulta imprescindible para enfrentar el desafío de esta Revolución Científica y Tecnológica.

Para ello la PNCS propone las siguientes acciones:

- Principios de política exterior chilena;
- Cooperación y asistencia;
- Reforzar la participación en instancias multilaterales y en instancias de múltiples partes interesadas (multistakeholder);
- Fomentar normas internacionales que promuevan la confianza y seguridad en el ciberespacio.

5. El país promoverá el desarrollo de una industria de la Ciberseguridad, que sirva a sus objetivos estratégicos.

El avance en el desarrollo de los países hoy esta íntimamente ligado a la creación y manejo de nuevas tecnologías. Este objetivo buscar impulsar el estudio y comprensión del ciberespacio para colocar al país en la vanguardia del conocimiento.

- Importancia de la innovación y desarrollo en materia de Ciberseguridad;
- Ciberseguridad como medio para contribuir al desarrollo digital de Chile;
- Desarrollo de la industria de Ciberseguridad en Chile;
- Contribuir a la generación de oferta por parte de la industria local;
- Generación de demanda de parte del sector público basado en los intereses estratégicos del Estado.

III. Política de Ciberseguridad del actual Gobierno del Presidente Sebastián Piñera

Las opiniones sobre la Política Nacional de Ciberseguridad y la situación actual de nuestro país ante el Ciberespacio son tomadas de las principales conclusiones del seminario *'Hacia una política pública para el ciberespacio',* organizado por la Comisión de Defensa Nacional del Senado, el Centro de Extensión de dicha corporación y la Biblioteca del Congreso Nacional, en mayo del presente año.

En representación del Ministerio del Interior y Seguridad Pública, Carlos Landeros, Director del programa *'Red de Conectividad del Estado'*, relevó los principales alcances de la 'Estrategia Gubernamental sobre Ciberseguridad 2018-2022' (en adelante, la Estrategia).

Según el personero, se trata de una directriz con visión de Estado, que marca una continuidad respecto a los planes del gobierno anterior, si bien desde este año con el foco puesto en la implementación de gran parte de los objetivos planteados en la Estrategia Nacional de Ciberseguridad.

Landeros explicó que el Ejecutivo decidió separar las competencias propias de la Ciberdefensa, dejándolas en manos de la cartera del ramo; Ciberseguridad, que pasan a ser asumidas por el Ministerio del Interior; y Ciberinteligencia, definidas desde la óptica de la ANI, si bien todas ellas coordinadas a través del Comité Interministerial de Ciberseguridad.

En términos específicos, la labor gubernamental estará orientada por la búsqueda de respuestas a objetivos como el mejoramiento de la infraestructura ciberespacial; la mayor difusión de contenidos de Ciberseguridad; y la colaboración internacional con terceros países y con la misma industria tecnológica.

Finalmente, el especialista enunció algunas de las prioridades insertas en la Estrategia, a saber:

- La renovación de los equipos de respuesta ante emergencias informáticas a nivel nacional;
- La optimización de los sistemas de autocontrol;
- La suscripción de acuerdos en materia de infraestructura crítica con otros estados, la academia y entes privados; y
- El envío a tramitación legislativa de proyectos de ley alusivos al tratamiento de datos personales, la tipificación de nuevos delitos informáticos, infraestructura crítica y la conceptualización misma de la Ciberseguridad.

Por su parte, Héctor Gómez, Asesor en Ciberdefensa y Ciberseguridad de la Subsecretaría de Defensa Nacional, a la vez que Secretario Ejecutivo del Comité Interministerial de Ciberseguridad, efectuó diversas aproximaciones al concepto mismo de ciberespacio. En primer término mencionó como desafíos la atribución de responsabilidades en el ciberespacio y una vinculación más estrecha con el sistema de inteligencia nacional.

El Ciberespacio lo concibió como un dominio artificial, en el que se representan nuestras actividades físicas, con impacto directo en la vida de las personas. A su juicio, esta dimensión estaría menos regulada que el espacio físico, razón por la cual se prestaría para la comisión de numerosas actividades maliciosas. También aludió a este concepto como el conjunto de medidas que permiten asegurar el funcionamiento y resiliencia de las estructuras de la información.

En sentido más amplio, añadió que el ciberespacio compromete todos aquellos esfuerzos para asegurar un acceso igualitario a la red, así como interacciones confiables de las personas en este ámbito.

Posteriormente, el especialista puntualizó los contrastes entre la Ciberdefensa (con minúscula) y la Ciberdefensa (con mayúscula). Mientras la primera se vincula con la protección de la infraestructura crítica del sector; la segunda remite a la extensión de las actividades de la defensa hacia el ciberespacio.

En otro plano, Gómez aseguró que si el conflicto tradicional, en palabras de Clausewitz, se caracterizaba por el intento de un país por imponer su voluntad sobre otro, con el empleo de la

violencia de por medio; hoy interviene un sinnúmero de actores y no siempre se verifica el uso de medios coercitivos.

El experto mencionó algunos de los desafíos a abordar en esta materia, entre los que citó:

- La atribución de responsabilidades en el ciberespacio;
- Una vinculación más estrecha con el sistema de inteligencia nacional, orientada al análisis de riesgos y amenazas; y
- La capacitación de civiles en materia de Ciberseguridad.

Desde el punto de vista policial, el Comisario Danic Maldonado, Jefe de Análisis Forense Informático, de la Brigada Investigadora del Cibercrimen de la PDI en la Región Metropolitana, hizo un llamado a actualizar la normativa vigente en materia de delitos informáticos, incorporando nuevas tendencias, tales como el *phishing*, la denegación de acceso y el robo informático.

Asimismo, subrayó la importancia de superar la opacidad informativa en materia de Cibercriminalidad, para lo cual se hizo eco de lo planteado por la abogada Silva, en cuanto a la relevancia de obligar por ley a las empresas a que den cuenta del momento en que sufren ataques informáticos.

Bajo la misma lógica, se mostró proclive a reforzar la coordinación internacional con organismos policiales como INTERPOL y el *Federal Bureau of Investigation* (FBI), así como con compañías multinacionales, entre las que nombró a *Microsoft*, *Google*, *Facebook* e *Instagram*.

Respecto a los desafíos institucionales, consideró importante:

- Contar con profesionales entrenados para levantar un laboratorio de análisis de códigos maliciosos;
- Hacer análisis de inteligencia sobre la *deep web*, que suele utilizarse como un espacio para perpetrar acciones criminales; y
- Certificar profesionales, para que puedan constituirse en voces válidas durante juicios orales.

Referencias

Ciberseguridad. Interior. ñBases para una Política Nacional de Ciberseguridadò Ministerio del Interior y Seguridad Pública-Ministerio de Defensa Nacional. Marzo 2015. Recuperado en julio de 2018 desde: http://bcn.cl/248az

Ley Chile. Decreto N°533 ñCrea Comité Interministerial sobre Ciberseguridadò Abril 2017. Recuperado en julio de 2018 desde: http://bcn.cl/245mg

Política Nacional de Ciberseguridad. Disponible en: www.ssdefensa.cl (Julio, 2018)

Disclaimer

Asesoría Técnica Parlamentaria, está enfocada en apoyar preferentemente el trabajo de las Comisiones Legislativas de ambas Cámaras, con especial atención al seguimiento de los proyectos de ley. Con lo cual se pretende contribuir a la certeza legislativa y a disminuir la brecha de disponibilidad de información y análisis entre Legislativo y Ejecutivo.