ANÁLISIS | De la normativa a la estrategia: Por qué Chile necesita una conducción estratégica de la ciberseguridad

ALEJANDRO AMIGO
Investigador senior AthenaLab
18 de marzo 2026

Chile está en proceso de consolidación de su institucionalidad de ciberseguridad, pero el escenario global exige más que el cumplimiento normativo. Ante la "militarización" del ciberespacio y el preposicionamiento de potencias en redes críticas, el país debe transitar desde la gestión de incidentes hacia una conducción estratégica de su seguridad digital.

Durante la última década, Chile ha avanzado de manera significativa en la construcción de un marco institucional y normativo para enfrentar los riesgos asociados al ciberespacio. Este proceso refleja un cambio de paradigma en la comprensión del problema, ya que la ciberseguridad no se concibe únicamente como una cuestión técnica vinculada a la protección de redes informáticas, sino también como un ámbito directamente relacionado con la seguridad nacional, la resiliencia del Estado y la protección de infraestructuras críticas.

Dentro de los avances más relevantes se encuentran la Ley Marco de Ciberseguridad e Infraestructura Crítica de la Información de 20241, la creación del Sistema Nacional de Ciberseguridad y de la Agencia Nacional de Ciberseguridad (ANCI), como órgano rector encargado de coordinar la prevención, gestión y respuesta frente a incidentes que afecten a servicios esenciales y operadores críticos. Este marco legal se articula con la segunda versión de la Política Nacional de Ciberseguridad (2023–2028)2, que busca contar con una infraestructura resiliente, proteger los derechos de las personas en internet y fomentar una

[1] https://www.bcn.cl/leychile/navegar?idNorma=1202434
[2] https://anci.gob.cl/documents/4430/Pol%C3%ADtica_Nacional_de_Ciberseguridad_2023-2028.pdf

cultura de ciberseguridad. En paralelo, el ámbito de la defensa se encuentra consolidando su propia arquitectura estratégica, destacando que la Política Nacional de Ciberdefensa reconoce el ciberespacio como un dominio operativo relevante para la seguridad nacional.

La implementación de esta institucionalidad ha comenzado a evidenciar resultados concretos. A nivel internacional, Chile ha mejorado de manera significativa su posicionamiento en distintos indicadores de ciberseguridad. En el Índice Nacional de Ciberseguridad, desarrollado por el E-Governance Academy Foundation de Estonia3, el país avanzó desde el lugar 53 en 2023 al 25 en 2026, alcanzando el primer lugar en América Latina. De manera similar, en el Índice Global de Ciberseguridad de la ITU4, Chile se ubica actualmente entre los países que están en una etapa de "consolidación", posicionándose entre los primeros de la región latinoamericana. A nivel regional, el reporte de ciberseguridad 2025 del BID y la OEA5 sitúa a Chile en el primer lugar entre 30 países de América Latina y el Caribe, obteniendo el puntaje más alto del estudio y logrando resultados sobresalientes en más de la mitad de los indicadores evaluados. En el plano interno, la Agencia Nacional de Ciberseguridad, en su balance de gestión del año pasado6, reportó sobre el fortalecimiento de la gestión de incidentes, el aumento de operadores críticos bajo supervisión y la consolidación de los estándares de protección en las redes del Estado.

Sin embargo, estos progresos ocurren en un contexto internacional donde el ciberespacio se ha convertido en un ámbito central de competencia estratégica entre Estados, desafiando las nociones tradicionales de soberanía y seguridad. Ejemplo de lo anterior es la operación Gridtide, analizada por Google y Mandiant7, que identificó una campaña de espionaje cibernético dirigida contra entidades gubernamentales y sectores vitales de las economías en múltiples regiones. Este tipo de operaciones, caracterizadas por su persistencia y su capacidad de mantener accesos prolongados a sistemas sensibles, evidencia cómo actores estatales buscan posicionarse dentro de redes críticas, lo que refuerza la necesidad de que países como Chile fortalezcan sus capacidades de detección temprana y protección de infraestructuras esenciales.

En este contexto, estas dinámicas se traducen en desafíos concretos para países como Chile. Un primer desafío surge de la creciente utilización de ciberoperaciones como parte

[3] https://ncsi.ega.ee/ncsi-index/?order=rank
[4] https://www.itu.int/epublications/publication/global-cybersecurity-index-2024
[5] https://publications.iadb.org/en/2025-cybersecurity-report-vulnerability-and-maturity-challenges-bridging-gaps-latin-america-and
[6] http://www.dipres.cl/597/articles-406737_doc_pdf.pdf
[7] https://cloud.google.com/blog/topics/threat-intelligence/disrupting-gridtide-global-espionage-campaign

de los medios empleados en conflictos actuales. Los ataques atribuidos a grandes potencias contra sistemas digitales críticos ilustran cómo el dominio cibernético se integra cada vez más en la planificación de operaciones militares y de inteligencia. Desde luego, esto tiene implicancias directas para Estados como Chile. Aunque el país no participe en estas disputas, la interdependencia digital global aumenta la exposición a daños colaterales. Un caso ejemplificador fue el ataque NotPetya de 2017 —inicialmente dirigido contra Ucrania y posteriormente atribuido a actores vinculados al Estado ruso—, el cual terminó afectando a empresas e infraestructuras en múltiples países y demostró que crisis digitales originadas en conflictos lejanos pueden impactar economías altamente interconectadas, lo que refuerza la necesidad de que el país incremente su preparación frente a disrupciones sistémicas.

La persistencia de agentes de actores estatales dentro de redes extranjeras mediante el "preposicionamiento" estratégico representa un segundo desafío. Las operaciones de espionaje y presencia latente se han convertido en prácticas habituales de la competencia entre potencias. Un caso paradigmático es la operación "Volt Typhoon", detectada en 2024, donde agentes de un actor estatal lograron infiltrarse de manera silenciosa en redes de energía, agua y transporte de EE. UU. A diferencia de los ciberataques tradicionales, estas acciones no buscan el robo inmediato de datos, sino mantener un acceso que permita sabotear servicios esenciales en caso de un conflicto futuro.

Un tercer desafío emerge de la creciente dimensión geopolítica de la infraestructura digital. El debate reciente en Chile sobre proyectos de conectividad submarina con participación de empresas extranjeras ha puesto de relieve cómo estos canales de comunicación pueden transformarse en puntos de presión geopolítica. Según la ITU, los cables submarinos de telecomunicaciones transportan más del 99% del tráfico internacional de datos8, lo que los convierte en activos críticos. Por esta razón, diversas potencias han comenzado a considerar estas infraestructuras desde la perspectiva de la seguridad nacional, evaluando no solo su viabilidad económica, sino también sus implicancias estratégicas y la integridad de la cadena de suministro tecnológica.

Frente a estos desafíos, Chile debiera avanzar hacia una visión integral que articule la seguridad pública, la defensa nacional y las políticas en el ámbito tecnológico. Esto podría materializarse mediante la institucionalización de ejercicios nacionales de cibercrisis que

[8] https://www.itu.int/digital-resilience/submarine-cables/

integren a diversos actores9, ampliando iniciativas ya desarrolladas en el país y proyectándolas hacia un sistema permanente de preparación para la protección de infraestructuras críticas; la creación de mecanismos de evaluación desde la perspectiva de la seguridad nacional para proveedores tecnológicos en sectores sensibles; el desarrollo de capacidades de inteligencia para monitorear amenazas que combinan dimensiones digitales y económicas; y una mayor y más ágil coordinación e intercambio de información estratégica en el nivel ministerial que permitan anticipar riesgos en un entorno internacional cada vez más competitivo.

Estas propuestas apuntan, en última instancia, a un desafío mayor: el Estado de Chile debiera avanzar desde una política de ciberseguridad hacia una estrategia nacional de ciberseguridad propiamente tal. Mientras una política establece principios generales, una estrategia define prioridades frente a amenazas concretas, fija objetivos operativos y orienta el uso de las capacidades del Estado. Esta estrategia debiera insertarse en el marco más amplio de la seguridad nacional, articulándose con la arquitectura institucional encargada de la seguridad, para asegurar coherencia en la toma de decisiones, asignación de recursos y conducción frente a amenazas que trascienden el ámbito estrictamente tecnológico. En particular, debiera concentrarse en tres objetivos centrales: proteger la infraestructura crítica digital del país; fortalecer la resiliencia de la economía frente a disrupciones tecnológicas, y desarrollar capacidades para prevenir, disuadir por negación y responder a operaciones hostiles en el ciberespacio.

En un escenario internacional donde el dominio digital se ha convertido en un espacio de competencia geopolítica entre Estados, avanzar hacia una conducción estratégica de la ciberseguridad es una condición necesaria para alcanzar los fines de la seguridad nacional.

ALEJANDRO AMIGO
Investigador senior AthenaLab
18 de marzo 2026

[9] Entre otros, a ministerios, Fuerzas Armadas, Fuerzas de Orden y Seguridad, ANCI, los operadores de importancia vital designados por la ANCI, e Instituciones académicas y de investigación relacionadas con el ámbito de la ciberseguridad.