



Riesgo sistémico en ciberseguridad: el talón de Aquiles de la resiliencia nacional

José Lagos
Docente UEjecutivos
Facultad de Economía y Negocios
Universidad de Chile

La reciente publicación por parte de la Agencia Nacional de Ciberseguridad (ANCI) de la nómina preliminar de Operadores de Importancia Vital (OIV) marca un hito en la implementación de la Ley de Ciberseguridad. Por primera vez, se establece un universo formal de entidades públicas y privadas cuya operación es considerada esencial para el funcionamiento del país.

Este acto normativo, más allá de su formalidad administrativa, revela una verdad crítica: la existencia de un riesgo sistémico latente en la arquitectura digital y de infraestructura de Chile.

El concepto de riesgo sistémico en ciberseguridad se refiere a la posibilidad de que una disrupción en una entidad o sector genere un efecto dominó, comprometiendo la continuidad operativa de otros servicios esenciales. Este afecta al conjunto del ecosistema, tal como se ha visto en incidentes internacionales como el ataque a Colonial Pipeline en Estados Unidos o la cadena de infección provocada por NotPetya, que comprometió empresas, infraestructuras públicas y redes logísticas a nivel global.

La nómina publicada por la ANCI expone con claridad el nivel de interdependencia entre sectores. El listado incluye instituciones de gobierno, empresas del Estado, operadores de energía eléctrica, compañías de telecomunicaciones y proveedores de servicios digitales gestionados por terceros. Muchas dependen de las mismas plataformas tecnológicas, redes físicas y servicios de infraestructura. Una vulnerabilidad en un nodo aparentemente periférico podría escalar rápidamente y afectar a múltiples actores.

El caso de los servicios de salud es ilustrativo. Muchos hospitales públicos dependen de servicios externos para su operación digital, incluyendo conectividad, alma-

cenamiento de datos clínicos e incluso plataformas de atención en línea. Estos servicios, a su vez, dependen de operadores de telecomunicaciones y de proveedores de nube y centros de datos privados. Si uno de ellos sufriera un ataque de ransomware o una interrupción masiva, el impacto podría afectar transversalmente a una institución, región o incluso al país.

Esta concentración operacional representa un punto único de falla que, de ser explotado, podría comprometer la seguridad y estabilidad de varias instituciones de manera simultánea.

Por ello, el análisis del riesgo sistémico en ciberseguridad no puede limitarse a diagnósticos sectoriales ni a marcos de cumplimiento mínimos. Requiere una mirada estructural del ecosistema digital del país. Es imprescindible que los órganos del Estado, junto con el sector privado, desarrollen mapas de interdependencias, refuercen las capacidades de monitoreo y respuesta, y eleven los estándares exigidos a sus proveedores. La resiliencia de la infraestructura crítica nacional no depende de las capacidades de defensa perimetral de cada organización, sino de la fortaleza colectiva del entramado digital que sostiene los servicios fundamentales.

La consulta pública de la ANCI sobre esta nómina preliminar representa una oportunidad para que las entidades evaluadas documenten su criticidad, y el país inicie una conversación sobre cómo fortalecer su soberanía digital frente a amenazas que no reconocen fronteras ni jerarquías institucionales.

Es momento de pasar de una lógica de cumplimiento a una de resiliencia, donde el riesgo sistémico se entienda como una amenaza potencial y un desafío estratégico de Estado.