ANÁLISIS | ATHENALAB

El próximo terremoto podría ser digital.

La resiliencia de Chile frente a la fragilidad tecnológica

Alejandro Amigo
Investigador Senior AthenaLab

19 de Noviembre 2026



INTRODUCCIÓN

La digitalización de los servicios públicos y privados ha incrementado la eficiencia de las sociedades contemporáneas, pero también ha ampliado su exposición a riesgos antes considerados marginales. El 13 de noviembre pasado, la Administración Federal de Aviación de Estados Unidos (FAA) detuvo todos los despegues del país durante más de cuatro horas[1], mientras Microsoft enfrentaba una de las interrupciones globales más extensas de sus servicios[2]. Ninguna de estas fallas requirió la intervención de un atacante, lo que revela que la dependencia de sistemas digitales constituye por sí misma una fragilidad capaz de paralizar servicios críticos.

A esta fragilidad estructural se suma la amenaza creciente de ciberataques potenciados por inteligencia artificial, una tecnología que les permite a los actores estatales y no estatales explotar vulnerabilidades con mayor rapidez, escala y a menor costo. Frente a este escenario, la resiliencia digital de un país depende de la sociedad en su conjunto, y al Estado le corresponde coordinar la preparación y la respuesta de todos sus componentes. Desde luego, Chile no está ajeno a esta realidad y al menos tres escenarios plausibles permiten dimensionar su exposición.

El primero corresponde a la interrupción de un proveedor del que dependen simultáneamente todos los organismos públicos, como la Red de Conectividad Segura del Estado, o bien un servicio de nube o del que dependan diversas empresas privadas. El segundo es una falla de alcance nacional en el sistema eléctrico, similar al apagón de febrero de 2025[3], cuyos efectos se amplifiquen al desconectar centros de datos de los que dependen servicios públicos y privados. El tercero es un ciberataque ejecutado con herramientas de inteligencia artificial contra un operador de importancia vital, cuya detección y atribución pondría a prueba la institucionalidad creada por la Ley Marco de Ciberseguridad. Ninguno de estos escenarios requiere supuestos extraordinarios, y, en conjunto, revelan riesgos que superan la capacidad de cualquier institución para enfrentarlos por sí sola. Los casos recientes que se analizan a continuación, ocurridos en otros países y en Chile, muestran que los elementos que componen estos escenarios ya se han manifestado por separado.

2. CASOS RECIENTES

Los casos que se presentan a continuación se ordenan según el origen de la interrupción. El primer grupo reúne fallas técnicas ocurridas sin intervención de un atacante; el segundo corresponde a ataques contra sectores no críticos con impacto en la población, y el tercero examina cómo estas amenazas se expresan en Chile. Ciertamente, la inteligencia artificial atraviesa los tres ámbitos, porque tenderá a ampliar el número de dispositivos conectados, el alcance de las vulnerabilidades existentes y la velocidad con que pueden explotarse.

A. FALLAS TÉCNICAS NO ASOCIADAS A UN CIBERATAQUE

Una parte relevante de la fragilidad digital proviene de los propios sistemas, ya sea por la obsolescencia de sus equipos o la dependencia de proveedores externos cuya falla no puede compensarse. En el caso de la FAA de EE. UU., la detención nacional de despegues se produjo con cerca de 3.500 aeronaves en vuelo y provocó miles de cancelaciones en todo el territorio estadounidense. El secretario de Transporte atribuyó la falla a equipos antiguos que, al recibir un volumen excesivo de datos, entregaron información inconsistente a los sistemas de radar y comunicaciones[4]. En cuanto a la interrupción de Microsoft, esta se originó en una falla interna del proveedor y paralizó oficinas de gobierno y empresas en todo el mundo durante cerca de 24 horas[5]. Este episodio ilustra el primero de los escenarios planteados para Chile, porque demuestra cómo la caída de un solo proveedor tecnológico afecta simultáneamente a organismos públicos, empresas y ciudadanos. Ambos casos indican que la obsolescencia de los sistemas y la concentración en pocos proveedores son riesgos que exigen una atención comparable a la que se presta a la acción deliberada de un adversario en el ámbito del ciberespacio.

B. ATAQUES CONTRA SECTORES NO CRÍTICOS CON IMPACTO EN LA POBLACIÓN

Cuando a esa fragilidad se suma la intención hostil de un atacante, los efectos alcanzan directamente la vida cotidiana de la población. El 2 de noviembre pasado, un ciberataque contra los sistemas de refrigeración de supermercados afectó tiendas en varios países europeos. Los atacantes modificaron de forma remota la temperatura de refrigeradores y congeladores que llegaron hasta 50 °C y obligaron a desechar grandes cantidades de alimentos[6]. El episodio siguió a un ataque similar ocurrido en octubre, en Francia, que afectó a cientos de supermercados a través de controladores fabricados por la empresa danesa Danfoss[7]. Parte de la prensa ha vinculado estos ataques con grupos hacktivistas prorrusos, aunque su autoría aún no ha sido confirmada oficialmente[8]. Estos casos muestran que un equipo comercial corriente conectado a internet para facilitar su gestión remota, puede convertirse en una vía para afectar la cadena de abastecimiento de alimentos. Ello plantea la pregunta de si los operadores de sistemas equivalentes en Chile están sujetos a exigencias de seguridad comparables a las que la Ley Marco de Ciberseguridad impone a los operadores de importancia vital.

C. LA EXPRESIÓN DE ESTAS AMENAZAS EN CHILE

Los incidentes registrados recientemente en el país muestran que estas tendencias globales ya tienen una expresión nacional. Desde que la Ley Marco de Ciberseguridad hizo obligatorio el reporte de incidentes en marzo de 2025, la Agencia Nacional de Ciberseguridad (ANCI) recibió 213 incidentes significativos hasta diciembre de ese año[9]. Entre enero y el 15 de octubre de 2026, un periodo de duración similar, la cifra llegó a 566, lo que representa un alza de 166%; aunque parte de ese aumento podría explicarse por la consolidación de la obligación de reportar. Durante el primer semestre de 2026, la Administración del Estado concentró la mayor cantidad de reportes, seguida por los servicios digitales y los proveedores de tecnología gestionados por terceros, mientras que la exfiltración o exposición de datos fue el impacto más frecuente[10].

Dos casos recientes ilustran el alcance que pueden tener estos incidentes sobre servicios esenciales e infraestructura crítica. En septiembre de 2026, el Hospital Clínico de la Universidad de Chile presentó una querella tras la filtración de datos personales y resultados de exámenes de sus pacientes, obtenidos mediante un acceso no autorizado a su plataforma de imagenología[11]. Por otra parte, desde el 27 de agosto de 2026, el parque solar Huatacondo y su sistema de baterías se mantienen fuera de servicio por una desconexión atribuida a un ciberataque, cuyo alcance aún no ha sido esclarecido[12]. Este último caso resulta especialmente relevante, porque vincula directamente la ciberseguridad con la estabilidad del sistema eléctrico, ámbito del segundo escenario planteado al inicio.

Ninguno de los incidentes descritos ha sido atribuido al uso de inteligencia artificial. Sin embargo, esta tecnología ha comenzado a reducir el costo y a aumentar la velocidad con que los adversarios descubren y explotan vulnerabilidades como las expuestas en estos casos. Según el CrowdStrike 2026 Global Threat Report, la actividad de adversarios habilitados por inteligencia artificial aumentó un 89% interanual[13], una tendencia que probablemente se reflejará también en Chile.

En conjunto, estos casos muestran que la fragilidad digital ya alcanza diversos ámbitos de los que depende directamente la vida cotidiana de la población y que la inteligencia artificial tiende a agravarla. Frente a esta realidad, la pregunta relevante para Chile es cómo prepararse para enfrentar sus consecuencias antes de que ocurran.

3. ¿QUÉ NECESITAMOS HACER?

La necesidad de actuar se vuelve más urgente si se consideran los avances de la necesaria modernización del Estado chileno. La Ley 21180 de Transformación Digital[14] ha impulsado la evolución hacia procedimientos administrativos electrónicos, lo que extiende la superficie de vulnerabilidades y reduce los canales analógicos que hoy funcionan como respaldo.

A ello se agrega una interdependencia público-privada creciente, en la cual la falla de un proveedor privado puede interrumpir de manera inmediata la prestación de servicios públicos. Para enfrentar este desafío, se proponen tres fases sucesivas que permiten visualizar los riesgos, anticipar escenarios y prevenir y monitorear posibles eventos.

A. VISUALIZAR RIESGOS

La primera fase consiste en concebir qué puede fallar, mediante un mapa nacional de riesgos que identifique las interdependencias entre servicios críticos y sus posibles efectos en cascada. La resolución de la Agencia Nacional de Ciberseguridad (ANCI) que calificó a los operadores de importancia vital (OIV) ya evalúa los estamentos que sustentan el funcionamiento digital del ámbito público y privado[15], información que se debiera integrar y conectar en una visión de conjunto. La medición de riesgos también debiera incorporar el impacto social, es decir, cuántas personas resultarían afectadas por una falla y durante cuánto tiempo. En esta fase, el aporte de la sociedad en su conjunto resulta indispensable, porque los OIV disponen de datos sobre sus propias dependencias que el Estado no alcanza a ver. La academia, por su parte, puede construir y difundir metodologías independientes de evaluación de riesgos, mientras que organismos públicos y empresas privadas pueden identificar vulnerabilidades en sus respectivos territorios.

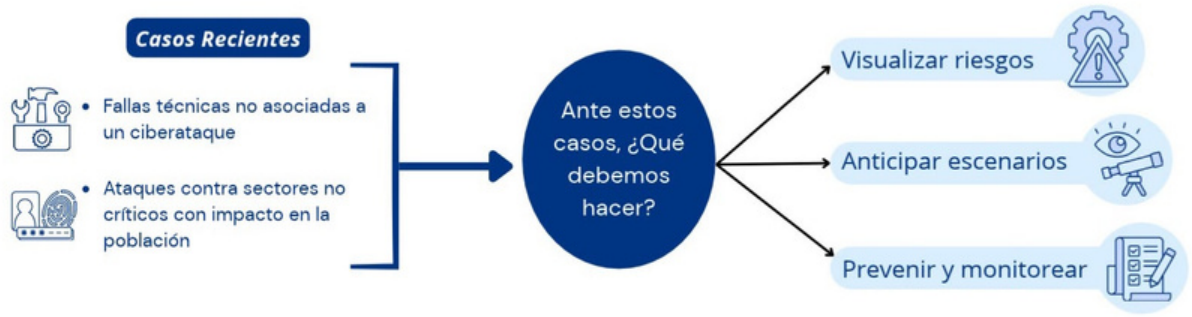
B. ANTICIPAR ESCENARIOS

Una vez identificados los riesgos, la segunda fase consiste en proyectar su evolución mediante escenarios que simulen cómo se desarrollaría una crisis concreta. Este ejercicio permite probar decisiones antes de que la crisis ocurra y revelan efectos de segundo orden que un mapa estático no logra mostrar. Asimismo, crea un lenguaje común entre actores que habitualmente no trabajan juntos y permiten decidir inversiones en prevención sobre la base de evidencia. La construcción de un escenario comienza al combinar un riesgo identificado en el mapa, como la caída de un proveedor de nube, con una amenaza plausible, como un ciberataque a un operador de servicios básicos.

Luego, se ajustan variables críticas que modifican la gravedad de la crisis, como que ocurra de noche, en pleno invierno o durante un terremoto. A partir de esa configuración, es posible modelar efectos en cascada y probarlos en simulaciones con participación de los distintos actores involucrados. La inteligencia artificial puede contribuir en esta etapa, porque permite generar un mayor número de escenarios y someterlos a condiciones extremas que difícilmente se considerarían de otro modo. Para esto, un ecosistema de innovación compuesto por la academia, la industria y los organismos públicos podría desarrollar simuladores y herramientas de detección basadas en inteligencia artificial. Estas capacidades reducirían, además, la dependencia de soluciones tecnológicas extranjeras en un ámbito sensible para la seguridad nacional.

C. PREVENIR Y MONITOREAR

Los escenarios orientan la tercera fase, que consiste en prevenir sus efectos y monitorear de forma permanente el estado de la resiliencia digital a nivel nacional. Una primera iniciativa sería crear un observatorio de resiliencia con indicadores como el tiempo de recuperación de los servicios y los niveles de redundancia. Una segunda medida consiste en promover centros sectoriales de intercambio y análisis de información en sectores como el comercio, la energía y la salud. Estos centros, liderados por las propias empresas y vinculados al CSIRT Nacional, permitirían alertar a los demás actores de un sector antes de que una falla se masifique o un ataque se propague. En tercer lugar, se pueden programar ejercicios nacionales periódicos con participación de privados, municipios y ciudadanos que preparen a la sociedad para reaccionar ante fallas en servicios digitales críticos. Este entrenamiento permitiría ensayar cómo comunicarse, acceder a atención de salud o recibir información oficial cuando los sistemas de las instituciones dejen de funcionar. Finalmente, los planes de continuidad operacional que la Ley 21663 exige a los OIV debieran extenderse a fallas tecnológicas de gran escala que no se originan en ciberataques[16]. De este modo, episodios como los antes relatados dejarían de ser imprevistos y pasarían a formar parte de la planificación nacional.



4. CONCLUSIONES

La resiliencia de una sociedad digitalizada se mide por su capacidad de seguir funcionando cuando los sistemas informáticos de los que depende dejan de operar. Los casos analizados demuestran que esas interrupciones pueden originarse en equipos obsoletos, en proveedores externos o en atacantes que explotan la conectividad de sistemas comerciales e industriales. La inteligencia artificial acelera esta tendencia, porque les permite a los adversarios explotar dichas vulnerabilidades con mayor rapidez y escala y a un menor costo. Frente a este panorama, el Estado chileno ha dado pasos relevantes con la Ley Marco de Ciberseguridad y la creación de la ANCI; aunque su alcance se concentra en la ciberseguridad sin considerar otras fallas tecnológicas de gran escala.

Para que las fases propuestas de visualizar, anticipar, prevenir y monitorear sean efectivas, se requieren al menos dos condiciones habilitantes de carácter institucional. La primera es una arquitectura de seguridad nacional que integre la resiliencia digital como un componente de la seguridad del país y articule los aportes del Estado y de la sociedad civil. La segunda es una instancia al más alto nivel que identifique los riesgos transversales a la sociedad, anticipe escenarios y coordine la fase de prevención entre los distintos sectores.

La resiliencia digital de Chile dependerá de la capacidad del Estado para coordinar a una sociedad que ya dispone de conocimientos, datos y recursos para enfrentar estas amenazas. Cuanto antes se asuma que la próxima crisis podría comenzar con la caída de un servidor, tal como hoy se asume con un terremoto, mejor preparado estará nuestro país para sostener su funcionamiento cotidiano.

NOTAS

[1] “FAA Lifts Ground Stop as U.S. Airports Grapple with Thousands of Canceled Flights”, NBC News, 13 de noviembre de 2026, https://www.nbcnews.com/news/us-news/live-blog/live-updates-flights-grounded-faa-communications-outage-rcna609268

[2] "Microsoft Services Hit by Major Outage across the World," NBC News, 12 de noviembre de 2026, actualizado el 13 de noviembre de 2026, https://www.nbcnews.com/tech/tech-news/outlook-widespread-outage-hits-microsoft-apps-rcna609047

[3] Coordinador Eléctrico Nacional, Estudio de Análisis de Falla EAF 089/2025. Apagón total del 25 de febrero de 2025 (Santiago: Coordinador Eléctrico Nacional, 2025), https://www.ciperchile.cl/wp-content/uploads/EAF-089-2025.pdf

[4] “Nationwide Ground Stop Lifted after More than 4 Hours as Trump Administration Blames Old, Overloaded Tech”, ABC News, 13 de noviembre de 2026, https://abcnews.com/US/nationwide-ground-stop-ordered-airports-faa/story?id=138121848

[5] “Microsoft Says Services Fully Restored after Outage Roiled World”, Bloomberg, 13 de noviembre de 2026, https://www.bloomberg.com/news/articles/2026-11-13/microsoft-says-making-progress-fixing-one-of-its-longest-outages

[6] Reuters. “Temperature Soars in Swedish Grocery Store Freezers, One Store Blames Hackers”, 2 de noviembre de 2026, https://www.reuters.com/business/retail-consumer/temperature-soars-swedish-grocery-store-freezers-one-store-blames-hackers-2026-11-02/

[7] Agence France-Presse. “Des supermarchés français touchés par une cyberattaque inédite de leurs installations frigorifiques”, 12 de octubre de 2026, actualizado el 13 de octubre de 2026, reproducido en Le Petit Journal, https://lepetitjournal.com/expat-mag/societe/des-supermarches-francais-touches-par-une-cyberattaque-inedite-de-leurs-installations-frigorifiques

[8] “European Supermarket Fridge Cyberattack: 7 Countries, 50 °C”, Tech Insider, noviembre de 2026, https://tech-insider.org/european-supermarket-fridge-cyberattack-7-countries-50c-2026/

[9] Yerko Roa Núñez. “Servicios esenciales bajo ciberataque: 'incidentes significativos' crecieron 166% este 2026”, BioBioChile, 7 de noviembre de 2026, https://www.biobiochile.cl/especial/bbcl-investiga/noticias/de-pasillo/2026/11/07/ciberataques-a-servicios-esenciales-organismos-han-reportado-566-incidentes-significativos-en-2026.shtml

[10] Agencia Nacional de Ciberseguridad (ANCI). Panorama de las amenazas en Chile. Primer semestre 2026 (Santiago: ANCI, 2026), https://anci.gob.cl/documents/5140/Panorama_Actual_de_Amenazas_2026_Octubre.pdf

[11] Natalia Cancino y Daniela Lobos J. “Hospital Clínico de la U. de Chile se querella tras sufrir ciberataque y filtración de información médica confidencial”, T13, 30 de septiembre de 2026, https://www.t13.cl/noticia/nacional/hospital-clinico-chile-querella-tras-ciberataque-filtracion-informacion-confidencial-30-9-2026

[12] Cristian Recabarren Ortiz. “Una planta solar lleva meses desconectada tras un ciberataque y ahora el Congreso exige explicaciones”, Redimin, 16 de noviembre de 2026, https://www.redimin.cl/una-planta-solar-lleva-meses-desconectada-tras-un-ciberataque-y-ahora-el-congreso-exige-explicaciones

[13] CrowdStrike. 2026 Global Threat Report (Austin: CrowdStrike, 2026), https://www.crowdstrike.com/global-threat-report.html

[14] Biblioteca del Congreso Nacional de Chile. “Ley 21180. Transformación Digital del Estado”, https://www.bcn.cl/leychile/navegar?idNorma=1138479

[15] Agencia Nacional de Ciberseguridad, Resolución Exenta N.° 87, “Aprueba nómina de operadores de importancia vital correspondiente al primer proceso de calificación”, Diario Oficial de la República de Chile, N.° 44.326-B, 17 de diciembre de 2025, CVE 2743431, https://www.diariooficial.interior.gob.cl

[16] Biblioteca del Congreso Nacional de Chile. “Ley 21663. Ley Marco de Ciberseguridad”, https://www.bcn.cl/leychile/navegar?idNorma=1202434