LITORALPRESS

Fecha: 29-01-2026
Medio: Revista Gerencia
Supl. : Revista Gerencia
Tipo: Noticia general
Título: Operadores vitales: cuando la ciberseguridad deja de ser opcional

Pág. : 16
Cm2: 584,7
VPE: $ 824.451

Tiraje: Sin Datos
Lectoría: Sin Datos
Favorabilidad: No Definida

ESPECIAL Operadores de Importancia Vital (OIV)

Operadores vitales: cuando la ciberseguridad deja de ser opcional

La publicación de la nómina de Operadores de Importancia Vital redefine el alcance de la ciberseguridad en Chile, trasladándola desde el ámbito técnico hacia la estrategia, la gobernanza y la responsabilidad de directorios y autoridades, en un escenario donde la continuidad digital ya es un asunto de interés público.

Por **José Lagos**, Docente UEjecutivos, Facultad de Economía y Negocios de la Universidad de Chile.

La publicación de la nómina oficial de Operadores de Importancia Vital (OIV) marca un punto de no retorno en la forma en que Chile entiende la ciberseguridad. Por primera vez, el Estado no solo declara que ciertos servicios son críticos para la vida económica y social del país, sino que identifica con nombre y apellido a más de 900 instituciones (públicas y privadas), cuya continuidad operativa ya no es solo un asunto interno, sino un interés nacional.

La medida, emanada de la Agencia Nacional de Ciberseguridad y publicada en el Diario Oficial de la República de Chile, se enmarca en la implementación de la Ley N°21.663. Más allá del tecnicismo jurídico, el mensaje es claro: en un país hiperconectado, la ciberseguridad ya no es un "tema TI", sino un componente esencial de la seguridad nacional.

La nómina incluye empresas eléctricas, operadores de telecomunicaciones, bancos, prestadores de salud, servicios digitales, organismos del Estado y empresas públicas. No es casualidad. Son precisamente estos sectores los que, al fallar, generan efectos en cascada: apagones, interrupción de pagos, colapso de servicios de emergencia o pérdida de datos sensibles de millones de personas.

"Obligaciones concretas"

Uno de los cambios más relevantes que introduce la ley es el fin de la autorregulación complaciente. Ser OIV implica obligaciones concretas: gestión de riesgos, notificación de incidentes, planes de continuidad operacional y estándares mínimos de seguridad.

Ya no basta con "hacer lo posible"; ahora se exige demostrarlo. Lo anterior no es reducir el debate a firewalls, Centro de Operaciones de Seguridad (SOCs) o protocolos, ya que el verdadero desafío que plantea la nómina de operadores vitales es cultural. Obliga a directorios, gerencias generales y autoridades públicas a incorporar la ciberseguridad en la toma de decisiones estratégicas, al mismo nivel que el riesgo financiero o legal.

Para muchas organizaciones, esto implicará inversiones relevantes, escasez de talento especializado y procesos de cambio interno que no siempre serán cómodos. Pero también abre una oportunidad: profesionalizar la gestión del riesgo digital y elevar estándares que, hasta ahora, eran desiguales y opacos.

Lo que viene

La implementación de la ley será la verdadera prueba. La Agencia Nacional de Ciberseguridad (ANCI) deberá demostrar capacidad técnica, criterio regulatorio y proporcionalidad en la fiscalización.

El sector privado, por su parte, tendrá que abandonar la lógica reactiva y asumir que la ciberseguridad es parte del contrato social moderno. En esa línea, la ciberseguridad como la privacidad de datos, son la licencia para operar en una economía digital modera.

No se trata de criminalizar a las empresas ni de burocratizar la innovación, sino de reconocer que ciertos servicios son tan esenciales que su interrupción no puede depender de decisiones aisladas o de presupuestos postergables.

La publicación de la nómina de operadores vitales no es el final del camino, sino el comienzo. Vendrán ajustes, revisiones y probablemente controversias. Pero el principio ya está instalado: en Chile, la continuidad digital de los servicios esenciales es un asunto de interés público.

La pregunta ya no es si esta regulación era necesaria, sino si estaremos a la altura de implementarla con seriedad, colaboración y visión de largo plazo. Porque en un país cada vez más digital, proteger lo vital es, simplemente, protegernos a todos.