Crónica Chillán

Fecha: 25/03/2026 Audiencia: 7.200 Sección: OPINION
Vpe: $148.470 Tirada: 2.800 Frecuencia: 0
Vpe pág: $664.000 Difusión: 2.800
Vpe portada: $664.000 Ocupación: 22,36%

Columna

Juan Luis Núñez Tissinetti,
Abogado especialista en telecomunicaciones, regulación y políticas públicas digitales.

Ciberseguridad y la infraestructura crítica

El país ha avanzado de manera significativa en la actualización de su marco normativo para enfrentar los riesgos asociados a un entorno digital cada vez más complejo. La reciente implementación de una legislación marco en materia de ciberseguridad, junto con la puesta en funcionamiento de la Agencia Nacional de Ciberseguridad, refleja un cambio de enfoque, que pasa de una lógica reactiva hacia un modelo institucional más preventivo y coordinado.

Uno de los aspectos más relevantes de este nuevo marco regulatorio es el reconocimiento explícito del rol que cumplen las redes de telecomunicaciones dentro de la infraestructura crítica del país. Estas redes no solo permiten la comunicación entre personas y empresas, sino que también soportan el funcionamiento de sistemas industriales, plataformas digitales, servicios financieros y múltiples procesos productivos que hoy operan de manera interconectada.

La actualización reciente de la normativa sobre infraestructura crítica incorpora precisamente esta dimensión. Entre otros elementos, establece obligaciones diferenciadas según el nivel de criticidad de las redes, introduciendo un esquema de tres categorías que busca priorizar las medidas de protección y resiliencia en función de la relevancia de cada componente del sistema. Este enfoque reconoce que no todas las infraestructuras enfrentan los mismos riesgos ni requieren las mismas exigencias regulatorias.

Al mismo tiempo, la evolución tecnológica ha ampliado de manera significativa la superficie de ataque. La convergencia entre redes tradicionales de telecomunicaciones, plataformas digitales y sistemas industriales conectados genera un ecosistema donde los incidentes cibernéticos pueden tener consecuencias que van mucho más allá del ámbito digital. Un ataque exitoso no solo podría comprometer información, sino también afectar la continuidad de servicios esenciales.

Por ello, el desafío regulatorio consiste en construir mecanismos de coordinación efectivos entre el sector público y los operadores privados. La protección de la infraestructura crítica no depende únicamente de normas o estándares técnicos, sino también de la capacidad de compartir información, gestionar incidentes y fortalecer la resiliencia de los sistemas frente a amenazas cada vez más sofisticadas.

De cara a los próximos meses, se espera además la dictación de una normativa específica de ciberseguridad para el sector de telecomunicaciones, destinada a profundizar las exigencias técnicas y operacionales para los operadores. Este nuevo marco regulatorio deberá equilibrar dos objetivos que no siempre son sencillos de compatibilizar, que implica fortalecer los estándares de seguridad y, al mismo tiempo, mantener condiciones que permitan seguir impulsando la inversión en infraestructura digital.

A ello se suma la situación internacional marcada por consideraciones geopolíticas en materia tecnológica. En distintos países, la discusión sobre la seguridad de las redes ha derivado también en debates sobre el origen de ciertas tecnologías y sobre la participación de determinados proveedores en infraestructuras estratégicas. No es descartable que este tipo de discusiones también influya en el diseño de futuras regulaciones.