

“La ciberseguridad deja de ser un discurso estratégico y pasa a ser una exigencia operativa inmediata”

Con la entrada en régimen de nuevas exigencias para los Operadores de Importancia Vital (OIV), la Ley 21.663 eleva el estándar: ya no basta con planes y declaraciones. La continuidad operacional y la resiliencia digital pasan a medirse por capacidades concretas —y demostrables— de contención, mitigación y respuesta.

El 26 de diciembre de 2025 entró en operación la Instrucción General N°4 de la Agencia Nacional de Ciberseguridad (ANCI), que fija una línea base obligatoria para la gestión de incidentes en los OIV. En este contexto, conversamos con S&A Chile sobre cómo estas exigencias impactan a las organizaciones y qué estrategias recomiendan para abordarlas.

Exigencias que ya no admiten postergación

Ricardo Riquelme, Gerente de Servicios Profesionales y Consultoría de S&A Chile, advierte que “la normativa establece exigencias claras: implementación de sistemas de gestión de seguridad de la información, planes de continuidad operacional, capacidades de respuesta ante incidentes, notificación a afectados y programas de capacitación, entre otras. El incumplimiento expone a sanciones relevantes y, más crítico aún, a riesgos operacionales y reputacionales de alto impacto”.

De acuerdo con la información disponible, el diagnóstico es nítido: muchas organizaciones aún no dimensionan el desafío. Se observan empresas en etapas iniciales, sin un diagnóstico de brechas (GAP) que les permita priorizar inversiones, definir una hoja de ruta y avanzar con foco en los requerimientos más críticos. Ese desfase abre una brecha entre la exigencia regulatoria y la capacidad real de respuesta.

Una mirada desde la experiencia práctica (y desde el cumplimiento)

En esa línea, Carlos Norambuena, Gerente General de S&A Chile, plantea que la clave ya no es qué falta, sino si la organización puede operar bajo un incidente grave. Propone tres focos: gestión real de riesgos; continuidad probada, no declarada; y claridad absoluta sobre gobernanza y notificación a la ANCI. El objetivo no es solo cumplir, sino **construir una arquitectura de ciberseguridad resiliente**.

En S&A Chile, el abordaje se construye desde la experiencia operativa: como proveedor de servicios TI, datacenter y ciberseguridad, y también como organización incluida en el ecosistema regulado. Esa doble perspectiva permite traducir el alcance normativo en una propuesta concreta para el mercado.

Patricia Muggioli, Gerente Comercial de S&A Chile, sostiene que “las empresas declaradas en el listado publicado por la ANCI encontrarán en S&A Chile el socio tecnológico que necesitan: una compañía con más de 35 años en el mercado, con el Centro Tecnológico ‘Edward Seleme’, y con un equipo de especialistas que suma más de 300 certificaciones, capaces de apoyar en el diseño y ejecución de una estrategia realista para enfrentar los desafíos de la norma”.

El momento de actuar es ahora. Contar con un partner con experiencia comprobada permite acelerar el cumplimiento, optimizar inversiones y reducir riesgos de forma efectiva.



Ricardo Riquelme, Gerente de Servicios Profesionales y Consultoría; Patricia Muggioli, Gerente Comercial; Y Carlos Norambuena, Gerente General.

Protección del dato: el punto crítico del cumplimiento

Para Ricardo Riquelme, la base está en implementar capacidades críticas de protección de datos, donde IBM Guardium cumple un rol central en el cumplimiento de la Ley 21.663: “esta plataforma permite establecer control efectivo sobre datos sensibles mediante monitoreo continuo, trazabilidad de accesos y actividades, y detección temprana de comportamientos anómalos”.

En un contexto donde la normativa exige visibilidad, control y capacidad de respuesta, Guardium habilita reducción del impacto con alertas en tiempo real y mecanismos de contención, además de generar evidencia robusta para auditorías y reportabilidad ante el regulador. Sobre esa base, la estrategia se complementa con capacidades de monitoreo y correlación de eventos a través de IBM QRadar (SIEM), buscando una gestión integral de amenazas alineada a los requerimientos regulatorios y operacionales de las OIV.

Patricia Muggioli enfatiza que el instructivo recientemente vigente exige capacidades concretas y medibles: respuesta en tiempo crítico, control estricto de accesos y evidencia y coordinación.

Si su organización es OIV o se encuentra en proceso de evaluación, lo invitamos a contactar a S&A Chile para una asesoría especializada en cumplimiento y fortalecimiento de su estrategia de ciberseguridad.

