



ESPECIAL Operadores de Importancia Vital (OIV)

Un verdadero reto humano

¿Cómo avanza la implementación de la Ley de Protección de Datos Personales en Chile?

La entrada en vigencia de la Ley de Protección de Datos Personales no solo eleva los estándares regulatorios, sino que expone un desafío profundo para las organizaciones: alinear tecnología, procesos y personas en un entorno de creciente fiscalización. Más allá del cumplimiento normativo, el verdadero reto está en construir una cultura de seguridad y responsabilidad digital que sostenga la confianza y la continuidad de los servicios.



El país sigue allanando el camino de su larga y angosta carretera digital con la implementación de la red 5G, la expansión de la fibra óptica a lo largo del territorio, la conexión a cables submarinos de última generación, el despliegue de tecnología satelital y un creciente parque de centros de datos de alta capacidad. De esta manera, sigue sentando las bases de su ecosistema tecnológico robusto para una economía digital en auge y una sociedad más conectada. Sin embargo, este progreso tecnológico va de la mano de importantes desafíos: la Ley Marco de Ciberseguridad y la

pronta entrada en vigencia de la Ley de Protección de Datos Personales. En este contexto, el país se encuentra en un proceso de ordenamiento interno a nivel organizacional, ya que ambas legislaciones obligan a las empresas y entidades públicas a adaptar sus procesos, infraestructuras y cultura para cumplir con los nuevos estándares. “Para hacernos una idea de la ‘presión’ que viven las compañías, hace un tiempo la Agencia Nacional de Ciberseguridad (ANCI) publicó la lista preliminar de Operadores de Importancia Vital (OIV), lo que implica que, por la “críticidad de los servicios” que

proveen y su relevancia en la seguridad digital, deben adoptar medidas extras de protección digital, políticas preventivas y planes de continuidad”, explica Rafael Onetto, Director Comercial en Coasin Logicalis.

Esto quiere decir que ante cualquier interrupción o vulneración, podría tener un impacto significativo en la seguridad digital y el funcionamiento del país. Por esta razón, se les exige la implementación de medidas de protección adicionales, el establecimiento de políticas preventivas robustas y la elaboración de planes de continuidad operacional detallados.

“Desde la encriptación de datos sensibles hasta la realización de auditorías de seguridad periódicas y la capacitación constante de su personal en materia de ciberseguridad, el objetivo es mitigar al máximo los riesgos cibernéticos, filtraciones de datos o cualquier incidente que pudiera comprometer la integridad y disponibilidad de sus servicios”, precisa Onetto.

La puesta en marcha de estas medidas busca garantizar la protección de los datos, la confianza de los usuarios y salvaguardar la reputación de las empresas en un entorno digital complejo y amenazante. Para muchas compañías esto representa un reto humano y organizacional, que implica una reestructuración de procesos internos y una inversión significativa en tecnología y personal especializado.

ESPECIAL Operadores de Importancia Vital (OIV)



El rol del outsourcing

Onetto explica que, como integradores de tecnología, también están involucrados y son responsables de la admi-



nistración de entornos digitales para numerosas organizaciones en diversos sectores. “Las leyes actuales fiscalizan a todo el ecosistema involucrado, por lo que si uno de nuestros clientes experimenta una violación de datos o un incumplimiento, tenemos un rol clave”. La criticidad de esto se hace evidente en infraestructuras críticas para sectores como la salud, la banca o la energía. Una brecha de seguridad que cause una fuga masiva de fichas clínicas, la divulgación de datos financieros o una paralización del sistema eléctrico podría tener consecuencias devastadoras para la provisión de servicios básicos. En este escenario, la inversión en programas de capacitación se vuelve un pilar fundamental. “Hoy no se puede dejar esto al azar. Es inaceptable esperar que ocurra una vulneración para impulsar

cambios. Tomando como referencia la Ley Karin en Chile, la gestión de las personas ha tomado una relevancia crítica en las empresas, llevándolas a un cambio profundo y proactivo, allanando el camino para construir equipos más empoderados, eficientes y estratégicos, que utilizan la tecnología no solo como una herramienta, sino como un aliado fundamental en la consecución de sus objetivos”, añade Onetto.

Con esto, el país tiene ante sí una oportunidad sin precedentes para catalizar el uso de las nuevas tecnologías para su crecimiento y desarrollo. “Pese a los avances significativos en adopción e inversión, es crucial que los colaboradores internalicen de raíz el uso ético y responsable de estas herramientas. No basta con tener la tecnología; es fundamental saber cómo usarla de manera que beneficie a la sociedad y garantice la seguridad de la información”, sentencia Onetto. 