

EL CAMBIO ORGANIZACIONAL QUE TRAE LA NUEVA LEY DE PROTECCIÓN DE DATOS

Ante la entrada en vigencia de la Ley de Protección de Datos, en diciembre próximo, las organizaciones enfrentan un desafío más allá de lo técnico: dejar atrás la lógica de acumular datos y gestionarlos con propósito y responsabilidad, lo que trae consigo un cambio en su cultura organizacional.

“El cambio más relevante es que introduce responsabilidad efectiva. No basta con declarar cumplimiento, hay que demostrarlo con procesos, controles y evidencia. Eso empuja a que los datos dejen de ser un subproducto operativo y pasen a ser un activo que requiere gestión, criterio y supervisión permanente”, advierte el CEO de Asimov Consultores y presidente de Chiletec, Felipe Mancini.

Asimismo, el ejecutivo identifica que esto instala una nueva forma de operar que va más allá de las sanciones y la fiscalización de la futura

La normativa obliga a las empresas a justificar, gestionar y resguardar cada dato con trazabilidad y evidencia, impulsando un cambio estructural que integra la protección de datos en la gobernanza, los procesos y la toma de decisiones del negocio.

POR VALENTINA CÉSPEDES

Agencia de Protección de Datos Personales. “El impacto real es otro: obliga a profesionalizar la gestión de datos dentro de las organizaciones e integrarla en la toma de decisiones del negocio”, plantea.

Desde el directorio de la Asociación Gremial de Profesionales en Protección de Datos Personales coinciden con ese análisis y

añaden que “ya no se trata solo de recolectar datos y usarlos, sino de preguntarse para qué se usan, bajo qué base de licitud, con qué resguardos y con qué impacto para las personas”, por lo que, afirman, la protección de datos pasa a formar parte de la gobernanza.

El desafío es, además, tecnológico. El especialista en ciberseguridad

de ITQ Chile, Edgar Echeverría, advierte que “el control manual ya es imposible”. Añade que este nuevo escenario exige automatizar las operaciones de seguridad mediante plataformas capaces de centralizar y correlacionar eventos en tiempo real. “La capacidad clave es la orquestación: detectar y contener incidentes reduciendo al mínimo la reacción humana”, explica.

Este tránsito implica rediseñar procesos completos: desde la recolección hasta el almacenamiento y uso de los datos, incorporando criterios de necesidad, proporcionalidad,

seguridad y respuesta a derechos de los titulares, analiza el gerente de asesoría legal y tributaria de PwC Chile, Jonathan Israel.

En esa línea, advierte que la figura del Data Privacy Officer se “vuelve clave como articulador de la gobernanza, pero no actúa solo”, ya que la responsabilidad también cae en áreas legales, tecnológicas, negocios y de compliance, lo que requiere mayor articulación. En paralelo, afirma Israel, las organizaciones deben desarrollar capacidades internas y una cultura orientada al uso responsable de los datos.

