

2026 y la protección de datos: cuando la teoría deja de ser suficiente

Si miramos el calendario, el 1 de diciembre de 2026 podría parecer una fecha lejana, pero en tiempos de transformación digital y adecuación normativa, diez meses es apenas un suspiro. Ese día marca el inicio de la plena vigencia y fiscalización de la nueva Ley de Protección de Datos Personales N° 21.719, un hito que cambiará la forma en la que las organizaciones gestionan su activo más crítico, la información de las personas.

Durante el último año, hemos visto a muchas empresas en etapa de diagnóstico, analizando brechas y revisando cláusulas. Sin embargo, es momento de pasar de las evaluaciones preliminares a la acción concreta. Con la reciente publicación de la Ley N° 21.806 en el Diario Oficial, se confirma que la instalación del Consejo de la Agencia se adelan-

tará para junio de este año. Este hecho nos entrega una certeza fundamental, el regulador estará constituido y operativo meses antes de que se active el régimen sancionatorio. Más que una señal de alerta, debemos leer esto como una ventaja estratégica que nos permite ajustar nuestros procesos con una institucionalidad ya definida, facilitando una transición ordenada hacia el cumplimiento en diciembre.

El error más común que observamos es tratar esta ley como un checklist puramente legal. Si bien los contratos y el consentimiento son la base, el desafío está en el terreno tecnológico y operativo. Un contrato perfecto no evitará una sanción si la organización no tiene la capacidad técnica para encontrar, borrar o portar los datos de un cliente cuando este lo solicite.

Aquí es donde la tecnología se convierte en el gran habilitador del cumplimiento. Para lograrlo, las organizaciones deben resolver tres desafíos prácticos:

Primero, la visibilidad. No se puede proteger lo que no se ve. Implementar herramientas automatizadas de data discovery es el punto de partida. Segundo, la orquestación de la respuesta. Una cosa es saber dónde está el dato y otra es tener la capacidad técnica de intervenirlo. El desafío radica en ejecutar acciones como la supresión o el bloqueo en sistemas interconectados que no fueron diseñados para olvidar. Y, en tercer lugar, la gobernanza efectiva. No basta con designar a un Delegado de Protección de Datos (DPO).

Carolina Eyquem, Responsable de Soluciones de Estrategia y Riesgo en SONDA.