SEÑAL DF
DIARIO FINANCIERO

Fecha: 16/05/2026 Audiencia: 14.344 Sección: REPORTAJE
Vpe: $5.890.942 Tirada: 4.781 Frecuencia: 0
Vpe pág: $8.127.680 Difusión: 4.781
Vpe portada: $21.104.600 Ocupación: 72,48%

eKNOW

Todas las empresas pueden alcanzar un 100% de cumplimiento legal y normativo en la ley de Protección de datos Personales.

En simple, para efectos prácticos, el objetivo de la Ley 21.719 se explica en base a 4 criterios esenciales: La Licitud en el uso de los datos personales, aplicada a los procesos del negocio mediante un uso legal y válido, con una finalidad explicable y en coherencia con la actividad desarrollada; La Transparencia, respetando el derecho de los titulares de los datos; La Confidencialidad, con que se debe manejar la información I de datos personales durante todo el ciclo de vida, dentro de la compañía; y La Seguridad, que debe garantizar la protección de los datos personales frente a accesos no autorizados o robo de información. Alcanzar el 100% de cumplimiento legal es un deber de todas las empresas y hoy se logra, apalancado en la tecnología DLP, que es el eje central de la seguridad de los datos personales y una herramienta fundamental en el diagnóstico.

La solución tecnológica definitiva a la ecuación en Protección de Datos Personales

La tecnología DLP (Data Loss Prevention) es la mejor herramienta en ciberseguridad, para lograr garantizar la protección de datos, al disminuir de forma sustancial, el riesgo inherente al que están sometidos los datos personales.

Safetica DLP se posiciona como la mejor solución tecnológica para apoyar el cumplimiento de la Ley 21.719 y tal como indica esta ley en materia de medidas de seguridad, reporte de vulneraciones, resguardo de la cesión de datos y prevención de infracciones, las empresas con Safetica, logran asegurar licitud, transparencia, confidencialidad y seguridad en el tratamiento de los datos personales, implementando medidas de prevención, control y gestión de incidentes. En este contexto, Safetica DLP permite dar respuesta directa a estas exigencias mediante clasificación inteligente de datos, fortaleciendo la trazabilidad, el control de acceso y el bloqueo para evitar exfiltraciones no autorizadas, con alertas frente a incidentes que refuerzan la evidencia para un cumplimiento legal efectivo.

La clave del Diagnóstico.

El diagnóstico en protección de datos no se limita a levantar información y su desarrollo constituye una exigencia legal para todas las empresas del país, cuyo plazo final es el 1° de diciembre de 2026. La clave es comprender cómo circulan los datos dentro de la empresa, por qué existen, quién decide sobre ellos y bajo qué fundamento legal se sostiene cada operación. Este proceso permite detectar brechas, ordenar responsabilidades, establecer controles y asegurar que los derechos de los titulares puedan ejercerse de forma efectiva. A ello se suma la necesidad de regular a proveedores o encargados del tratamiento de datos personales y controlar riesgos, como las transferencias internacionales, manteniendo evidencia suficiente para demostrar cumplimiento, trazabilidad y capacidad de mejora continua.

El RAT y DPIA como eje central.

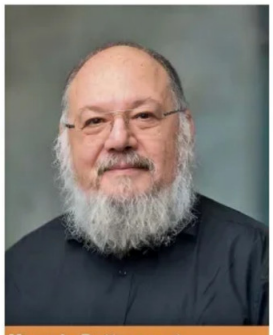
El eje central del diagnóstico es levantar el Registro de Actividades de Tratamiento (RAT) para identificar finalidades, bases legales, flujos, responsables, conservación y transferencias, y aplicar la Evaluación de Impacto en la Protección de Datos (DPIA) cuando exista alto riesgo, definiendo medidas de control y mitigación. Esta documentación es clave para la construcción del PIMS (Privacy Information Management System) y para enfrentar fiscalizaciones.

La trazabilidad del dato personal.

Safetica DLP materializa el cumplimiento legal de trazabilidad del dato personal mediante etiquetado, clasificación de información sensible, control de acceso por rol, monitoreo de canales de salida y registro forense. Su capacidad técnica asegura la trazabilidad mediante evidencia verificable.

Hector Lazo
Experto en Ciberseguridad (FEN)
CEO EKNOW

"A mi juicio, las empresas deben entender que el diagnóstico en protección de datos personales debe tener una proporcionalidad respecto de las exigencias de la ley y de su adecuada implementación; es decir, no hay que sobredimensionar el esfuerzo ni caer en una retórica jurídica exacerbada. Su implementación presenta desafíos, pero al contar con las herramientas adecuadas, esto se vuelve un ejercicio eficaz, y el resultado busca tres objetivos: gestionar adecuadamente el gobierno de los datos personales, cumplir frente a la fiscalización y mitigar el riesgo tecnológico."



Marcelo Bettancourt
Experto TI (USACH)
Director de Tecnologia EKNOW

"Opino que la mejor característica de Safetica DLP es el uso de Inteligencia Artificial, la cual entiende el contexto del riesgo antes de que la fuga de datos ocurra. No se limita a detectar archivos sensibles, sino que aprende patrones de trabajo e identifica conductas anómalas. Esto convierte a la IA en una capa de protección operativa."