LITORALPRESS

Fecha: 30-05-2025
Medio: El Mercurio
Supl. : El Mercurio - Chile Tecnológico
Tipo: Noticia general
Título: **Un avance para la privacidad de los usuarios**

Pág. : 18
Cm2: 156,6

Tiraje: 126.654
Lectoría: 320.543
Favorabilidad: No Definida

NUEVA LEY DE PROTECCIÓN DE DATOS PERSONALES:

Un avance para la privacidad de los usuarios

La legislación recién promulgada obliga a las empresas a implementar una serie de cambios para adoptar prácticas más transparentes.

FELIPE LAGOS R.

Un profundo cambio. Así es como describe la industria tecnológica los pasos que debe seguir para implementar lo que establece la nueva Ley 21.719, de Protección de Datos Personales, específicamente en la forma en que recopilan, procesan y protegen la información de sus usuarios.

La ley, que entra en vigor en diciembre de 2026, pone a la par a Chile con la Unión Europea en derechos digitales, ya que impone prácticas más estrictas y transparentes basadas en el Reglamento General de Protección de Datos de la UE (GDPR, por sus siglas en inglés). Por lo mismo, y aunque el plazo parece largo, impone grandes desafíos para las empresas.

Entre las acciones más urgentes están actualizar políticas de privacidad, revisar contratos con proveedores que procesen datos, nombrar un delegado de protección de datos, mantener un registro de actividades de tratamiento y evaluar los riesgos asociados a cada tipo de dato.

"Los mecanismos de recopilación ahora deben ser transparentes y granulares, informando al usuario de forma clara y concisa sobre la identidad del responsable, la finalidad específica, los tipos de datos a recopilar, los destinatarios, sus derechos y el período de conservación", explica Carolina Eyquem, experta en Soluciones de Ciberseguridad en SONDA. "Además, se debe ofrecer una posibilidad de revocación del consentimiento simple y sin costo", agrega.

La ejecutiva también explicó que la compañía está fortaleciendo sus controles de gestión e implementando ajustes técnicos y organizativos que se ajusten a las nuevas exigencias.

"Esto incluye la anonimización y cifrado de datos para proteger la información en tránsito y en reposo, así como sistemas de gestión de identidades y accesos que aseguran que solo personal autorizado acceda a los datos. A nivel organizativo, se mantienen registros de actividades de tratamiento y se asignan roles clave como el delegado de protección de datos, brindando capacitación continua y aplicando un modelo de prevención de infracciones", dice Eyquem.

EL ROL DEL DELEGADO

Fundamental en todo este andamiaje es el delegado de protección de datos, cuyo rol es ser un asesor interno y supervisor del cumplimiento de la nueva normativa. "(Es) el punto de contacto para los titulares de datos y el interlocutor principal con la futura Agencia de Protección de Datos Personales. Sus funciones también incluyen fomentar una cultura de protección de datos, participar en la gestión de incidentes, mantener registros de actividades de tratamiento y gestionar los riesgos asociados al tratamiento de datos personales", concluye la experta.