

PROTECCIÓN DE DATOS PERSONALES E INTELIGENCIA ARTIFICIAL

Por **Arnoldo Araya**

CEO Isecurity y director Eliac



Chile ha logrado avances significativos en ciberseguridad, como lo refleja el Índice Nacional de Seguridad Cibernética (NCSI) de Estonia, que ubica al país en el puesto 25 a nivel mundial y segundo en América Latina. Con un 100% de cumplimiento en “Estrategia de Ciberseguridad”, demuestra capacidad para diseñar políticas digitales robustas. Pero en “Ciberseguridad Preventiva”, Chile alcanza solo un 50% de cumplimiento, lo que evidencia una debilidad en la protección de datos personales.

La pronta aprobación de la Ley sobre Protección de Datos Personales es un paso crucial, porque establece la titularidad de los datos y exige que las empresas ajusten sus procesos en el tratamiento de la información.

Pero es necesario ir más allá y enfrentar los desafíos que plantea la inteligencia artificial (IA) en esta materia.

Los datos personales incluyen información como nombres, direcciones, números de teléfono, identificadores únicos y datos biométricos. En manos equivocadas, pueden ser utilizados para fraudes, como la apertura de cuentas bancarias falsas o la creación de perfiles falsos en redes sociales. Además, es cada vez más común la suplantación de identidad mediante técnicas donde se generan videos o audios falsos que imitan a la perfección la voz y el rostro de una persona.

Estas herramientas, potenciadas por el uso de IA, también pueden influir en procesos electorales o desinformar masivamente. Según el “Informe de Amenazas Cibernéticas 2024” de Sophos, el 64% de las organizaciones en América Latina reportaron un aumento de los ataques cibernéticos en 2023. Amenazas como correos electrónicos falsos creados mediante IA tienen hasta un 50% más de éxito que los métodos tradicionales.

En este contexto, es vital seguir el ejemplo de la UE con su Reglamento General de Protección de Datos (GDPR), que establece un marco robusto para evitar la vulneración de información. Chile debe adoptar un enfoque igual de riguroso, integrando medidas preventivas avanzadas.

Nuestro país tiene la oportunidad de ser un líder en ciberseguridad en la región. Para ello, la palabra clave es adaptabilidad, porque la protección de datos en la era de la IA es un imperativo estratégico para el país.