LA TERCERA
Fecha: 25/05/2025 Audiencia: 271.020 Sección: ACTUALIDAD
Vpe: $3.973.178 Tirada: 76.017 Frecuencia: OTRAS
Vpe pág: $9.829.612 Difusión: 76.017
Vpe portada: $9.829.612 Ocupación: 40,42%

[INFORMACIÓN BIOMÉTRICA]

Desafíos y avances en la protección de datos personales

Con el avance de la biometría como herramienta de control de acceso, es crucial conocer cómo se administra esta información.

Por: Rodrigo M. Ancamil

La implementación de datos biométricos ha optimizado el control de accesos, siendo una opción personalizada y eficiente. Sin embargo, la administración de estos datos es sumamente sensible, los datos biométricos, como huellas dactilares, rasgos faciales, iris e incluso patrones de movimiento. son únicos e irrepetibles.

Por lo mismo, su valor y sensibilidad requieren altos estándares de seguridad. "Estos pueden ser, por ejemplo, la huella digital, el rostro, los movimientos corporales o el iris. El uso de la biometría como medio de autenticación en el mundo digital ha sido vital, porque nos entrega un alto grado de seguridad para verificar y reconocer a las personas", explica Cristián Ojeda, gerente general de Nubatech.

A su vez, Tomás Valdés, consultor en Ciberseguridad de Entelgy Chile, detalla que estos datos no se almacenan en formatos simples. "En particular estos datos, de carácter sensible y personal, no se almacenan en texto/imágenes plano, sino que a través de representaciones parciales de estos datos, es decir, podemos encontrar estos datos almacenados en manera encriptada o en algoritmos para evitar su reconstrucción directa".

Pese a los mecanismos técnicos, el riesgo de filtraciones existe. De ahí la importancia de un enfoque global en ciberseguridad. "La estrategia integral debe considerar la protección en las capas del acceso físico, perímetro, red interna, endpoints, aplicaciones, código, datos y personas", destaca el consultor en Ciberseguridad de Entelgy Chile.

Pero, ¿qué ocurre cuando un usuario deja de utilizar un servicio? Antes de la Ley de Protección de Datos Personales, no había respuestas claras. Eso cambiará a partir del 1 de diciembre de 2026. "La nueva ley establece los derechos ARCOP: Acceso, Rectificación, Cancelación, Oposición y Portabilidad. Por ejemplo, la cancelación obliga a las empresas a eliminar los datos cuando la finalidad ha terminado o el consentimiento es revocado", afirma el gerente general de Nubatech.

Valdés coincide en que este nuevo marco legal marcará un antes y un después: "Empodera a los propietarios de los datos para tener acceso, derecho a rectificación, cancelación y oposición a los datos, fortaleciendo la privacidad digital de los usuarios".

En tiempos donde los rostros abren puertas y las huellas desbloquean cuentas, la protección de los datos biométricos ya no es una opción, sino una responsabilidad urgente y compartida.