LA TERCERA

Fecha: 24/05/2026 Audiencia: 271.020 Sección: PORTADA
Vpe: $7.702.459 Tirada: 76.017 Frecuencia: OTRAS
Vpe pág: $9.829.612 Difusión: 76.017
Vpe portada: $9.829.612 Ocupación: 78,36%

[ESTABLECER NUEVOS ESTÁNDARES]

Transformación digital y datos personales: cómo innovar sin comprometer la seguridad

En medio del avance de la IA, la biometría y el uso masivo de datos, empresas y expertos enfrentan el desafío de fortalecer la privacidad, la transparencia y la seguridad de la información personal.

El primero de agosto marca la eliminación oficial de la tarjeta de coordenadas, mecanismo que por años fue clave para las transacciones bancarias de los chilenos. ¿La razón? la evolución de la digitalización y el uso de nuevos mecanismos más seguros, como las claves dinámicas y la biometría.

Pero al igual que la seguridad, la delincuencia también evoluciona, lo que marca nuevos desafíos para proteger un activo tan o más importante como el dinero: los datos personales. Nuestra vida diaria cada vez depende más de plataformas digitales, información como nombres, ubicación, hábitos de consumo quedan registradas y pueden ser claves para que delincuentes puedan realizar fraudes.

En este escenario, el resguardo de los datos personales se vuelve cada vez más relevante para el país, especialmente en un contexto donde la economía digital depende del procesamiento masivo de información sensible, desde datos biométricos hasta geolocalización en tiempo real. La próxima entrada en vigencia de la Ley 21.719 y la creación de la Agencia de Protección de Datos Personales apuntan precisamente a fortalecer la transparencia, la seguridad y la confianza en el uso de estos datos.

Para Miguel Villar, Chief Technology Officer de Redvoiss "la conectividad digital es el principal factor habilitador para la transmisión de datos. Hoy en día contamos cada vez más con aplicaciones basadas en IA, las cuales necesitan grandes volúmenes de información para su entrenamiento. En este contexto, los datos pasan a ser parte de una infraestructura crítica para la economía digital".

Uno de los principales focos de la nueva normativa es el tratamiento de datos sensibles, como la información biométrica, incluyendo reconocimiento facial y huellas digitales, además de antecedentes relacionados con la salud y otros datos personales de alta sensibilidad.

Villar comenta que en un ambiente donde industrias como la banca, salud, telecomunicaciones, o retail están incorporando biometría con el fin de personalizar servicios y la autenticación de sus usuarios, la mejora en los estándares para el uso de este tipo de datos y su resguardo es vital.

Otro aspecto que toma relevancia es el uso y tratamiento de datos de geolocalización, considerados información sensible por la normativa debido al creciente uso de aplicaciones móviles, plataformas de transporte y servicios digitales que operan en función de la ubicación de los usuarios, muchas veces en tiempo real.

CONTRASEÑAS SEGURAS

La seguridad de las contraseñas se ha convertido en un tema prioritario ante el aumento de las filtraciones de datos. De acuerdo con el último informe de Check Point External Risk Management (ERM), este tipo de incidentes creció un 160% durante 2025. En América Latina, Brasil, Argentina y Chile figuran entre los países más afectados por credenciales comprometidas, reflejando la necesidad de reforzar las prácticas de ciberseguridad tanto a nivel empresarial como personal.

Frente a este escenario, Jorge Pavez, de Redvoiss, enfatiza la importancia de proteger las contraseñas, ya que resguardan información sensible como datos bancarios, correos electrónicos, fotografías y otros antecedentes personales. Para fortalecer la seguridad digital, el ejecutivo entrega las siguientes recomendaciones:

· Crear contraseñas largas, idealmente de entre 8 y 10 caracteres o más.
· Utilizar combinaciones de letras mayúsculas, minúsculas, números y caracteres especiales.
· Evitar datos personales evidentes, como fechas de cumpleaños o nombres de mascotas.
· Mantener claves distintas para cada cuenta y actualizarlas periódicamente.
· Activar la autenticación en dos pasos mediante correo electrónico, SMS u otros métodos.
· Utilizar administradores de contraseñas reconocidos y confiables.
· Activar herramientas biométricas, como huella digital o reconocimiento facial, cuando estén disponibles.