DIARIO FINANCIERO®

Fecha: 24/10/2025 Audiencia: 48.450 Sección: CIENCIA Y TECNOLOGIA
Vpe: $5.473.014 Tirada: 16.150 Frecuencia: 0
Vpe pág: $7.443.240 Difusión: 16.150
Vpe portada: $7.443.240 Ocupación: 73,53%

Estudio de la FEN de la Universidad de Chile advierte brechas en gobernanza y estrategias de protección de datos en empresas del país

POR MARCO ZECCHETTO

A casi un año de la entrada en vigencia de la Ley de Protección de Datos Personales -diciembre de 2026- la Facultad de Economía y Negocios (FEN) de la Universidad de Chile, realizó, entre junio y julio de este año, la primera Encuesta de Seguridad y Protección de Datos en Chile, con el fin de medir el nivel de madurez y gobernanza de datos personales en las organizaciones del país.

El reporte se basó en encuestas aplicadas a ejecutivos vinculados a la seguridad, cumplimiento y auditoría de la protección de datos de 986 empresas que operan en Chile y de entidades públicas y reveló que menos de un tercio (29,11%) tiene una estrategia clara de protección de datos personales y un 39,96% de las organizaciones no sabe si está preparada para enfrentar los cambios normativos.

El estudio, que fue elaborado por el profesor Gustavo Zurita del Departamento de Control de Gestión y Sistemas de Información y el docente de UEjecutivos de la FEN, José Lagos, también concluyó que el 44,52% de estas entidades presenta un nivel de madurez intermedio en gestión de datos personales, es decir, cumplen con regulaciones mínimas, pero sin una estrategia avanzada y solo el 24,54% se ubica en un nivel avanzado, e integra la privacidad en la estrategia de negocio.

Lagos señaló que aunque hay avances incipientes en la incorporación de roles -como el director o gestor de datos- y estructuras para gestionar los datos, todavía predomina un enfoque reactivo en las empresas, y que "muchas están esperando qué hacer, sin una estrategia clara desde el punto de vista del cumplimiento".

A poco más de un año de la entrada en vigor de la normativa, el análisis detectó brechas para cumplir con la futura ley, bajo involucramiento de los directorios y falta de capacitación de los colaboradores.

Un dato clave, explicó Lagos, es que el 33,77% tiene "grandes brechas" para cumplir con las exigencias normativas. Entre los factores que han incidido en las brechas, está la carga de *compliance* (cumplimiento normativo) que tienen las empresas -como el Modelo de Prevención de Delitos, la Ley Marco de Ciberseguridad y la implementación de la Ley de Protección de Datos- apalancado por la falta de cultura organizacional, de talento, habilidades, conocimiento y "competencias adecuadas" ante la protección de datos.

"Esto finalmente se traduce en que no hay claridad de cómo avanzar hacia ese tipo de empresas que gestionan los datos de forma íntegra. Los colaboradores deben tener ese cambio de mente, entender que el tratamiento de los datos personales a partir de diciembre de 2026 cambiará, y que un error no intencional podría llevar a su organización a tener una infracción gravísima por parte de la futura Agencia de Protección de Datos Personales", comentó.

Gestión de los datos y capacitación

El estudio también evidenció que un 41,08% de las empresas gestiona los derechos de los titulares -como acceso, rectificación, eliminación o portabilidad- mediante procesos "manuales y lentos", como formularios, mientras que solo un 29,51% realiza estas gestiones de forma automatizada.

En tanto, el 54,36% declaró que no realiza evaluaciones de impacto en la privacidad y el 29,01% solo las ejecuta "cuando lo exige la normativa".

"Las empresas recién se están dando cuenta de que es necesario automatizar una serie de cosas que en etapas iniciales no habían visualizado, y la mayoría están atrasadas en el análisis de impacto de privacidad. Pero cuando las organizaciones usan, por ejemplo, inteligencia artificial o *machine learning*, esos algoritmos están tomando decisiones, por lo que hay que hacer esas evaluaciones de impacto", dijo Lagos.

Otra de las brechas que destaca el estudio es la formación continua, ya que el 43,61% de las organizaciones no realiza capacitaciones regulares en privacidad y protección de datos a sus colaboradores, y el 36,11% no mide la efectividad de estas.

Para el investigador, la falta de conocimiento de protección de datos podría tener un impacto en la ciberseguridad de las organizaciones, ya que el 90% de estos incidentes son provocados por errores humanos, de los cuales, "el 82% tiene compromiso de datos personales", como *ransomware* (secuestro de datos) o *phishing* (suplantación de identidad).

Desafíos y rol de directorios

Si bien queda poco más de un año para la entrada en vigencia de la ley, Lagos advirtió que hay una serie de desafíos que las organizaciones deben sortear antes.

Entre los desafíos, destacó la adopción de estrategias avanzadas y modelos de gobernanza de datos, implementar programas de "cultura de datos" y establecer mecanismos para la trazabilidad y el traspaso transfronterizo de datos.

En este punto, advirtió que existe una "deuda importante" en los directorios, tanto en el nivel de conocimiento en protección de datos como en el involucramiento en la supervisión y estrategia en la materia, lo que atribuyó a la velocidad de cómo la tecnología impulsa las regulaciones.

"Se necesita un recambio, desde el punto de vista de la habilidad y de los conocimientos que todas las personas deben tener, pues esto afecta a toda la compañía", dijo.

Otro aspecto clave para Lagos es fortalecer la relación con proveedores y terceros que manejen datos personales, de manera de protegerlos en toda la cadena.

Lagos también señaló que las organizaciones deben incorporar herramientas de inteligencia artificial generativa y el diseño de agentes autónomos que permitan automatizar la prevención de infracciones.