DF
DIARIO FINANCIERO®
SANTIAGO DE CHILE /
MARTES 31 DE MARZO DE 2026
df.cl

EDICIÓN ESPECIAL

Déficit de expertos en ciberseguridad en Chile eleva la exposición en las organizaciones

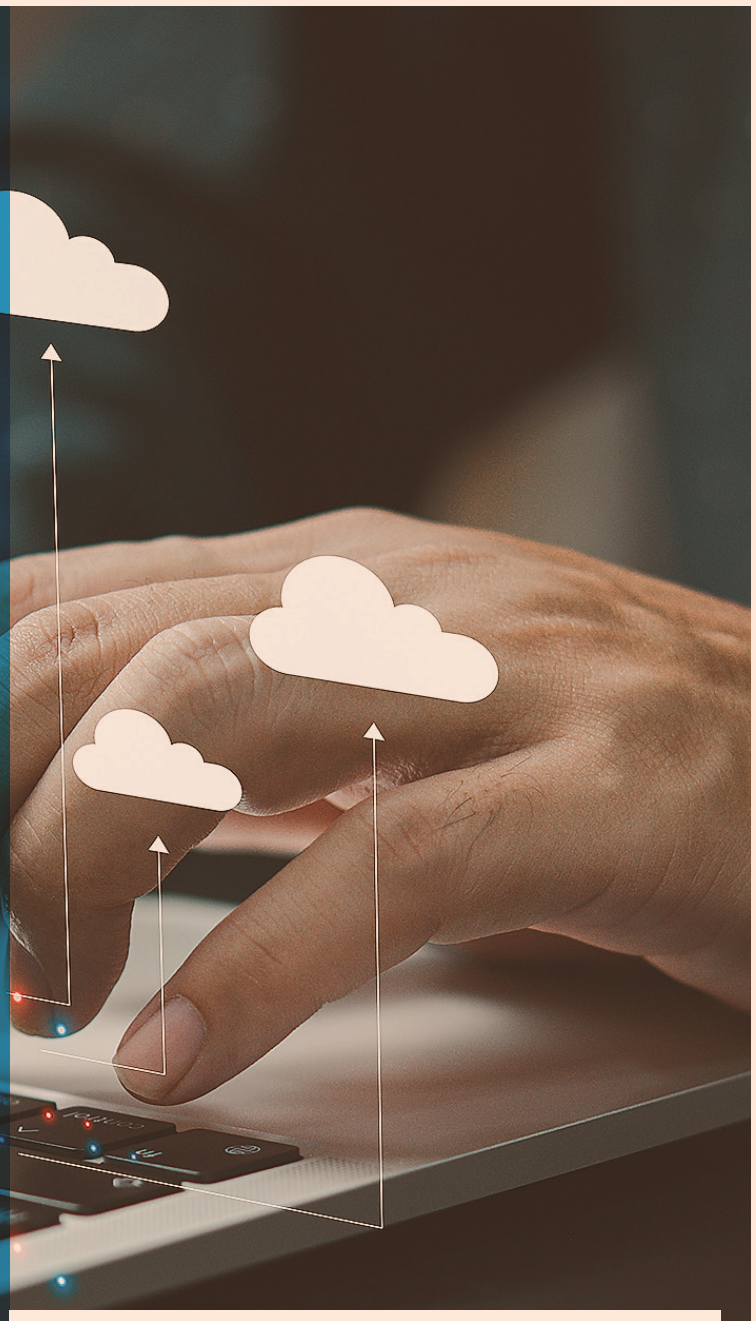
PÁG. 10

Qué tan preparadas están las pymes para operar bajo la nueva ley

PÁG.6

CIBERSEGURIDAD Y PROTECCIÓN DE DATOS PERSONALES

EL BACKUP COMO EJE DE LA CIBERSEGURIDAD MODERNA



Expertos advierten que, ante el aumento de incidentes y fallas operativas, contar con estrategias de respaldo robustas dejó de ser una práctica técnica para convertirse en un pilar clave de la continuidad del negocio.

POR ANAÍS PERSSON

Cada 31 de marzo se conmemora el Día Mundial del *Backup*, una fecha que busca generar conciencia sobre la importancia de respaldar la información digital. En un contexto donde las empresas se enfrentan a la amenaza de los ciberataques, esta estrategia es una respuesta óptima y siempre recomendada por expertos para apoyar la continuidad operacional de las organizaciones.

Según el último informe de Check Point Research, América Latina es hoy la región más golpeada por ciberataques, con un promedio de 3.123 ataques semanales por organización durante febrero de este año y un crecimiento interanual de 20%. En el caso de Chile, se registraron, en promedio, 1.780 ataques, lo que representa una disminución de 4% respecto al mismo período del año anterior.

Al evaluar el desempeño de Chile en este escenario, la directora subrogante de la Agencia Nacional de Ciberseguridad (ANCI), Michelle Bordachar, dice que el país ha dado importantes pasos, particularmente con la implementación de la Ley Marco de Ciberseguridad y la creación de la agencia. No obstante, menciona que, si bien hay sectores que han madurado significativamente, otros todavía no incorporan la seguridad digital "como parte esencial de su operación ni tienen planes claros para mantener sus servicios funcionando si algo falla".

"Contar con una estrategia de respaldo de datos ya no es opcional: es indispensable. Sin ella, cualquier incidente que comprometa la información puede resultar catastrófico. Y no se trata solo de ataques informáticos, los errores humanos, accidentes, incendios o inundaciones también pueden borrar datos críticos de un momento a otro", afirma.

El costo de no protegerse

"La pérdida de acceso a la información genera costos en múltiples dimensiones, desde la reputación de los clientes hasta ventas no concretadas o derechamente pérdidas por no poder realizar la transacción", señala el gerente de desarrollo de negocios de Nubatech, Luis González. A esto se suman posibles multas regulatorias y gastos asociados a brechas de seguridad.

En la misma línea, el gerente de Servicios SyA, Ricardo Riquelme, advierte que la incapacidad de recuperación de información tras un ataque o algún evento de otra naturaleza puede afectar la reputación del negocio. "Cuando una empresa demuestra incapacidad para recuperarse con rapidez, el mayor impacto es la pérdida de confianza de sus clientes, quienes en el corto o mediano plazo buscarán alternativas confiables", señala.

De acuerdo con datos de Kaspersky, el costo promedio de un incidente de fuga de datos alcanza los US$ 1,23 millones en grandes empresas y US$ 120 mil en pequeños negocios, lo que refuerza la necesidad de adoptar medidas proactivas de protección y recuperación de información. El director del equipo global de investigación y análisis de esa firma para América Latina, Fabio Assolini, señala que el *ransomware* seguirá siendo una de las principales amenazas. "Las copias de seguridad son una regla esencial que debe ser parte del protocolo de ciberseguridad de todas las organizaciones, sin importar su tamaño o sector", indica.

Recomendaciones

Según Assolini, existe "una brecha importante" entre la percepción y la realidad. Citando datos de Kaspersky, indica que el 72% de las empresas en Chile considera tener una estrategia proactiva de ciberseguridad, pero en la práctica existen carencias importantes: más de la mitad opera sin *firewall*, un 30% no utiliza inteligencia de amenazas y un 32% no cuenta con antivirus.

A esto se suman errores comunes en la implementación de estrategias de respaldo. Riquelme identifica cinco prácticas frecuentes: ver el *backup* solo como un componente tecnológico y no como algo estratégico, no contar con planes de recuperación probados, mantener las copias en la misma red productiva, no disponer de copias aisladas e inmutables y la falta de capacitación del personal.

Para fortalecer la resiliencia digital, desde la Agencia Nacional de Ciberseguridad recomiendan adoptar la regla 3-2-1-1-0, considerada el estándar de oro del respaldo: mantener tres copias de los datos, en dos medios distintos, con una copia fuera de las instalaciones, una offline y cero errores verificados.

Además, los expertos recomiendan contar con sistemas de monitoreo, encriptación de datos, infraestructura redundante y almacenamiento distribuido entre entornos locales y en la nube. También es clave realizar pruebas periódicas de recuperación, asegurar que los respaldos estén protegidos frente a ataques y, sobre todo, capacitar constantemente a los equipos.

HASTA US$ **1,23** MILLONES

PUEDE COSTAR UN INCIDENTE DE FUGA DE DATOS, SEGÚN CÁLCULOS DE KASPERSKY.

1.780

CIBERATAQUES SEMANALES POR ORGANIZACIÓN SE REGISTRARON DURANTE FEBRERO EN CHILE, SEGÚN CHECK POINT RESEARCH.

S&A CHILE | IBM Gold Partner

“La ciberseguridad deja de ser un discurso estratégico y pasa a ser una exigencia operativa inmediata”

Con la entrada en régimen de nuevas exigencias para los Operadores de Importancia Vital (OIV), la Ley 21.663 eleva el estándar: ya no basta con planes y declaraciones. La continuidad operacional y la resiliencia digital pasan a medirse por capacidades concretas —y demostrables— de contención, mitigación y respuesta.

El **26 de diciembre de 2025** entró en operación la **Instrucción General N°4** de la Agencia Nacional de Ciberseguridad (ANCI), que fija una línea base obligatoria para la gestión de incidentes en los OIV. En este contexto, conversamos con S&A Chile sobre cómo estas exigencias impactan a las organizaciones y qué estrategias recomiendan para abordarlas.

Ricardo Riquelme, Gerente de Servicios Profesionales y Consultoría; Patricia Muggioli, Gerente Comercial; Y Carlos Norambuena, Gerente General.

Exigencias que ya no admiten postergación

Ricardo Riquelme, Gerente de Servicios Profesionales y Consultoría de S&A Chile, advierte que “la normativa establece exigencias claras: implementación de sistemas de gestión de seguridad de la información, planes de continuidad operacional, capacidades de respuesta ante incidentes, notificación a afectados y programas de capacitación, entre otras. El incumplimiento expone a sanciones relevantes y, más crítico aún, a riesgos operacionales y reputacionales de alto impacto”.

De acuerdo con la información disponible, el diagnóstico es nítido: muchas organizaciones aún no dimensionan el desafío. Se observan empresas en etapas iniciales, sin un diagnóstico de brechas (GAP) que les permita priorizar inversiones, definir una hoja de ruta y avanzar con foco en los requerimientos más críticos. Ese desfase abre una brecha entre la exigencia regulatoria y la capacidad real de respuesta.

Una mirada desde la experiencia práctica (y desde el cumplimiento)

En esa línea, **Carlos Norambuena, Gerente General de S&A Chile**, plantea que la clave ya no es qué falta, sino si la organización puede operar bajo un incidente grave. Propone tres focos: gestión real de riesgos; continuidad probada, no declarada; y claridad absoluta sobre gobernanza y notificación a la ANCI. El objetivo no es solo cumplir, sino **construir una arquitectura de ciberseguridad resiliente.**

En S&A Chile, el abordaje se construye desde la experiencia operativa: como proveedor de servicios TI, datacenter y ciberseguridad, y también como organización incluida en el ecosistema regulado. Esa doble perspectiva permite traducir el alcance normativo en una propuesta concreta para el mercado.

Patricia Muggioli, Gerente Comercial de S&A Chile, sostiene que “las empresas declaradas en el listado publicado por la ANCI encontrarán en S&A Chile el socio tecnológico que necesitan: una compañía con más de 35 años en el mercado, con el Centro Tecnológico ‘Edward Seleme’, y con un equipo de especialistas que suma más de 300 certificaciones, capaces de apoyar en el diseño y ejecución de una estrategia realista para enfrentar los desafíos de la norma”.

Protección del dato: el punto crítico del cumplimiento

Para **Ricardo Riquelme**, la base está en implementar capacidades críticas de protección de datos, donde **IBM Guardium** cumple un rol central en el cumplimiento de la Ley 21.663: “esta plataforma permite establecer control efectivo sobre datos sensibles mediante monitoreo continuo, trazabilidad de accesos y actividades, y detección temprana de comportamientos anómalos”.

En un contexto donde la normativa exige visibilidad, control y capacidad de respuesta, **Guardium** habilita reducción del impacto con alertas en tiempo real y mecanismos de contención, además de generar evidencia robusta para auditorías y reportabilidad ante el regulador. Sobre esa base, la estrategia se complementa con capacidades de monitoreo y correlación de eventos a través de **IBM QRadar (SIEM)**, buscando una gestión integral de amenazas alineada a los requerimientos regulatorios y operacionales de las OIV.

Patricia Muggioli enfatiza que el instructivo recientemente vigente exige capacidades concretas y medibles: respuesta en tiempo crítico, control estricto de accesos y evidencia y coordinación.

Si su organización es OIV o se encuentra en proceso de evaluación, lo invitamos a contactar a S&A Chile para una asesoría especializada en cumplimiento y fortalecimiento de su estrategia de ciberseguridad.

El momento de actuar es ahora. Contar con un partner con experiencia comprobada permite acelerar el cumplimiento, optimizar inversiones y reducir riesgos de forma efectiva.

LA NUEVA ECONOMÍA DEL DATO: DE RECOLECTAR A GOBERNAR LA INFORMACIÓN

Ante las nuevas exigencias que introduce la Ley de Protección de Datos Personales, expertos evalúan las principales implicancias que tendrá para las organizaciones y cómo estas se preparan.

POR ANAÍS PERSSON

La nueva Ley de Protección de Datos Personales, que entrará en vigencia en diciembre, está impulsando un cambio estructural en la forma en que las empresas gestionan la información: los datos de las personas dejan de ser un activo libremente explotable para transformarse en un elemento regulado, con exigencias de gobernanza, trazabilidad y responsabilidad proactiva, que impactarán modelos de negocio, costos de cumplimiento y gestión de riesgos.

El presidente de la Asociación Gremial de Profesionales en Protección de Datos (AGPD) y socio de DataCompliance, Marcelo Drago, afirma que con la normativa "el dato personal pasa a ser un activo regulado". En ese escenario, agrega, el valor de la información ya no dependerá solo de su capacidad de segmentación o monetización, sino también de la legitimidad con que fue obtenida y tratada. "La nueva economía del dato no premia solo al que más datos tiene, sino al que mejor los gobierna", sostiene.

Bajo este nuevo estándar, la directora de Magliona Abogados, Bárbara Reyes, explica que las empresas van a tener que revisar y redefinir cómo capturan consentimiento, cómo informan al titular la finalidad del tratamiento, cómo comunican los plazos de conservación y cómo explicitan los derechos disponibles. "Esto obliga a rediseñar formularios, avisos y flujos de atención, porque lo que antes se hacía 'de otra manera', ahora exige verificar que se cumple con lo que exige la normativa", indica.

Según el director ejecutivo de Grupo Mitiga Latam, Víctor Cortés, este nuevo estándar también implica costos de cumplimiento, asociados a diagnósticos, rediseño de procesos, revisión de contratos e incorporación de herramientas tecnológicas. En ese sentido, Drago menciona que esta ley "no viene a frenar la innovación. Viene a ordenar el mercado y a elevar su estándar".

Cortés explica que los desafíos serán mayores para organizaciones que manejan grandes volúmenes de datos, datos sensibles o procesos altamente automatizados.

Sin embargo, las pymes también deberán adaptarse. Y, aunque las empresas ya empezaron a prepararse, el avance hasta ahora es disímil: las grandes empresas o las entidades altamente reguladas ya han avanzado en preparación e implementación, dice Cortés, mientras que otras organizaciones recién comenzaron su diagnóstico y el levantamiento de su estructura de cumplimiento.

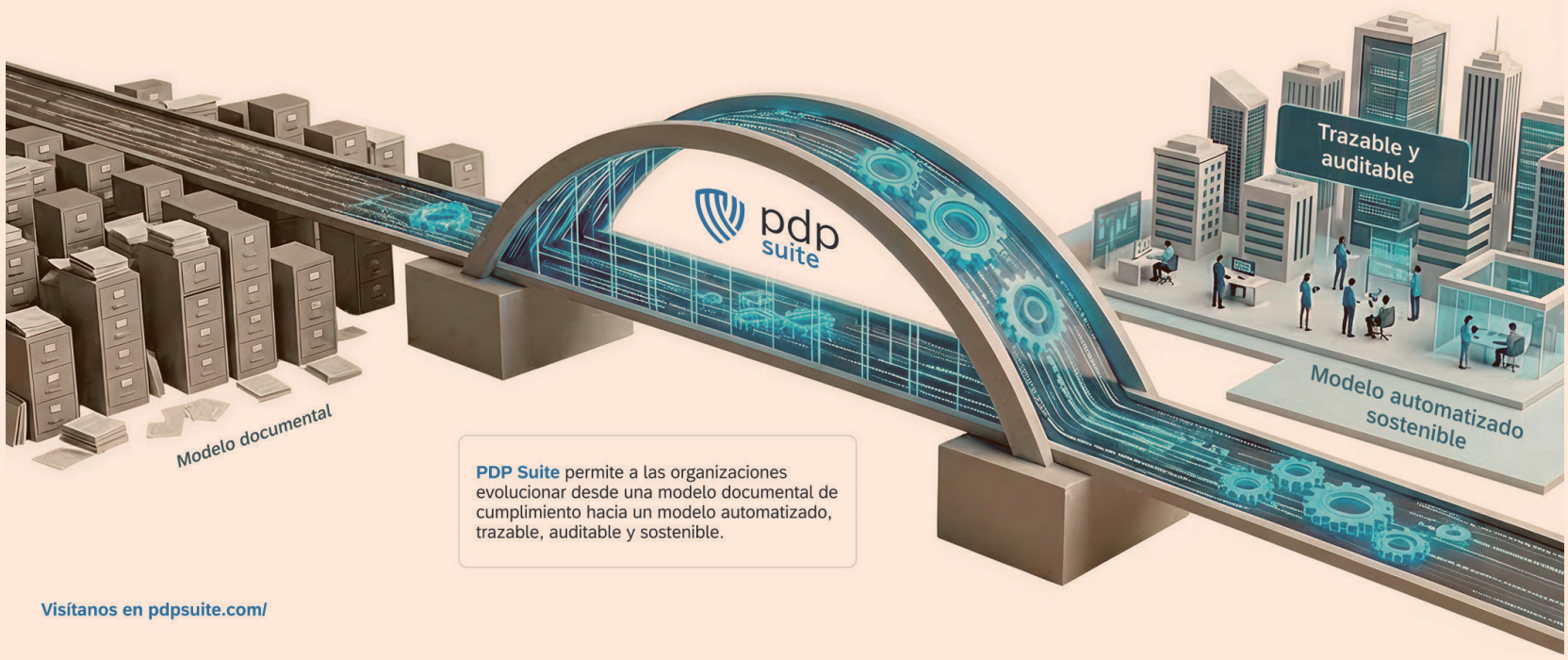
"El tercer grupo todavía no inicia este trabajo, y siento que es la inmensa mayoría, lo que en sí mismo ya representa un riesgo de alto impacto", concluye el ejecutivo.

PDP Suite: la innovadora solución chilena que integra el cumplimiento de la Ley 21.719 en solo una plataforma

PDP Suite permite a las organizaciones implementar y gestionar un modelo integral de cumplimiento en protección de datos personales, automatizando procesos críticos, reduciendo riesgos regulatorios y facilitando la toma de decisiones estratégicas.

PDP Suite es tu plataforma SAAS para la gestión de privacidad y cumplimiento

Su propósito es apoyar a las organizaciones en la implementación de un modelo integral de gobierno de datos personales, alineado con la Ley 21.719, GDPR y otros marcos regulatorios aplicables.



Visítanos en pdpsuite.com/

Frente a la entrada en vigor de la nueva Ley N° 21.719 que modifica la Ley N°19.628 sobre protección de datos personales, que incorpora multas que pueden llegar hasta las 20.000 UTM, las organizaciones enfrentan un desafío estructural: pasar desde un cumplimiento documental a un modelo operativo, continuo y auditable.

En este contexto surge PDP Suite, una solución tecnológica desarrollada por un equipo de profesionales liderados por el ingeniero Raúl Tapia y el abogado Juan Avendaño (DPO Certificado – Vicepresidente de la AGPD - Chair para Chile de la Asociación Latinoamericana de Privacidad), que integra en solo una plataforma todos los elementos necesarios para implementar y gestionar un modelo de cumplimiento en protección de datos personales.

Una solución integral para un nuevo estándar regulatorio

PDP Suite responde directamente a las exigencias de la nueva normativa, permitiendo a las empresas implementar un modelo de prevención de infracciones automatizado en protección de datos, gestionar de forma centralizada el ciclo completo del tratamiento de datos personales, automatizar obligaciones legales tales como responder a las solicitudes de los derechos ARSO-BP y asegurar la trazabilidad, evidencia y accountability.

La plataforma incorpora funcionalidades clave como, un gestor de consentimiento y cookies con trazabilidad completa, portal público para el canal de denuncia y ejercicio de derechos, automatización de flujos de atención de derechos, módulo de gestión de terceros, gestor de plazos de conservación de datos y documentos, matriz de cumplimiento y gestión de riesgos, gestor de evidencia, brechas de seguridad y respaldo documental, gestor de capacitaciones, módulo de alertas y Dashboards ejecutivos para DPO y alta dirección.

“En términos generales, PDP Suite permite implementar y operar un modelo de cumplimiento alineado con las nuevas obligaciones legales, pasando desde una lógica reactiva a una gestión preventiva y continua”, señala Juan Avendaño.

Uno de los principales diferenciales de PDP Suite es su capacidad de integrar procesos legales con sistemas tecnológicos de la organización.

En palabras de sus creadores, el objetivo es claro:

“Transformar el cumplimiento en protección de datos en un proceso gestionable, medible y alineado con la estrategia del negocio”.

Los socios de PDP Suite, Juan Avendaño y Raúl Tapia.

“El sistema no solo gestiona el consentimiento, sino que permite operar los derechos de los titulares, asegurando el cumplimiento de plazos, trazabilidad y control”, explica Raúl Tapia.

Integración tecnológica y enfoque SaaS

PDP Suite opera bajo un modelo Software as a Service (SaaS), lo que permite una implementación ágil y escalable.

Destaca por su capacidad de integración con cualquier solución o sistema que opere bajo estándares abiertos y además conecta de manera nativa con los entornos SAP, incluyendo soluciones como SAP ERP, SAP Success Factor, SAP S/4HANA , SAP Business One y otros sistemas empresariales.

Cumplimiento end-to-end con soporte legal y técnico

Más allá de la tecnología, PDP Suite ofrece un modelo de acompañamiento que incluye, un diagnóstico inicial, levantamiento de actividades de tratamiento, RAT, elaboración de políticas y documentación, identificación de riesgos, definición de controles, evaluaciones y capacitación organizacional.

Esto permite a las organizaciones implementar un modelo de cumplimiento completo, desde el diagnóstico hasta la operación continua.

La plataforma incorpora dashboards que permiten monitorear en tiempo real el estado del cumplimiento, facilitando el trabajo del DPO o encargado de cumplimiento, disponibilizando reportes para la mejora continua a nivel ejecutivo.

Una respuesta concreta al nuevo escenario regulatorio

La Ley 21.719 no solo aumenta las obligaciones, sino también las sanciones y el nivel de exigencia en materia de gobernanza de datos.

En este escenario, PDP Suite se posiciona como una solución estratégica para organizaciones que buscan eliminar el modelo documental, reducir exposición a sanciones, profesionalizar su gestión de datos y escalar su modelo de prevención.

QUÉ TAN PREPARADAS ESTÁN LAS PYMES PARA OPERAR BAJO LA NUEVA LEY

Aunque su experiencia en este tema aún es baja, expertos creen que la normativa permitirá a pequeñas y medianas empresas profesionalizar la gestión de datos y fortalecer su competitividad.

POR VALENTINA CÉSPEDES

Falta de visibilidad sobre los datos, debilidad en sus procesos de resguardo y escasa cultura organizacional en este tema son parte del escenario actual de las pymes, a solo meses de la entrada en vigencia de la nueva Ley de Protección de Datos en diciembre próximo.

El lead product owner de soluciones digitales de Entel, Álvaro Fernández, advierte un punto de partida crítico: "Muchas organizaciones no saben con precisión qué datos tienen, quién los gestiona ni dónde están". A su juicio, esto contrasta con una normativa que exige control en un entorno digitalizado, lo que implica un cambio profundo en tecnología, procesos y cultura organizacional. Por ello, cree que el principal desafío es la concientización, ya que muchos tomadores de decisiones no dimensionan el impacto de la ley, especialmente en pymes donde "no hay roles, procedimientos ni sistemas adecuados para gestionar datos personales".

Coincide el líder de la plataforma legal de la Alianza Chilena de Ciberseguridad (ACC), Claudio Magliona, quien destaca que para dar solución a esa falta de concientización, la Agencia de Protección de Datos Personales -organismo que se encargará de fiscalizar y sancionar- comenzará a operar seis meses antes de la vigencia de la ley, por lo que es clave que esta inicie campañas de educación. "Es tanta la relevancia de las pymes para esta ley, que durante el primer año de vigencia, la Agencia podrá decidir no aplicar multas a las pymes, sino que limitarse a amonestaciones", advierte Magliona.

"Muchas organizaciones no saben con precisión qué datos tienen, quién los gestiona ni dónde están", advierte Álvaro Fernández, de Entel.

Barreras que persisten

"El error más común, muchas veces inocente, está en el uso de bases de datos sin poder acreditar consentimiento", indica la socia de Alessandri Abogados, Carla Illanes, quien también señala prácticas como la ausencia de políticas de privacidad claras, debilidades en seguridad y falta de canales para ejercer derechos. En la práctica, explica, muchas pymes recolectan datos sin protocolos formales, algo que puede derivar en incumplimientos y que trae riesgos significativos. "Para una pyme, una sola multa puede ser existencial", afirma, considerando sanciones que pueden alcanzar las 5 mil UTM y un impacto reputacional prolongado, pues las infracciones quedarán publicadas por cinco años.

Para el director del equipo global de investigación y análisis de Kaspersky para América Latina, Fabio Assolini, esta vulnerabilidad responde a múltiples factores: falta de personal especializado, crecimiento digital más rápido que la inversión en seguridad y debilidades en la protección de datos en la nube.

En materia de recursos, el gerente de operaciones ITQ Chile, Luis Abarca, indica que los costos de asesoría, adecuación contractual y controles tecnológicos pueden impactar en el presupuesto de una pyme y plantea que la adaptación requiere un enfoque integral. "No se trata solo de cumplir la ley, sino de ordenar el activo más crítico del negocio: la información".

Para enfrentar estas barreras, Magliona señala que "las asociaciones gremiales deben ser motor de capacitación de pymes disponiendo modelos de prevención de infracción de datos personales y políticas de privacidad modelos para ser implementadas. Por su parte, la Agencia de Datos Personales también debe redactar y proponer estas guías de educación".

A su vez, el profesional destaca el rol de las herramientas tecnológicas accesibles para automatizar procesos de cumplimiento, gestión de riesgos y protección de la informacion, lo que reduciría la necesidad de contar con grandes equipos especializados.

EL CAMBIO ORGANIZACIONAL QUE TRAE LA NUEVA LEY DE PROTECCIÓN DE DATOS

La normativa obliga a las empresas a justificar, gestionar y resguardar cada dato con trazabilidad y evidencia, impulsando un cambio estructural que integra la protección de datos en la gobernanza, los procesos y la toma de decisiones del negocio.

POR VALENTINA CÉSPEDES

Ante la entrada en vigencia de la Ley de Protección de Datos, en diciembre próximo, las organizaciones enfrentan un desafío más allá de lo técnico: dejar atrás la lógica de acumular datos y gestionarlos con propósito y responsabilidad, lo que trae consigo un cambio en su cultura organizacional.

"El cambio más relevante es que introduce responsabilidad efectiva. No basta con declarar cumplimiento, hay que demostrarlo con procesos, controles y evidencia. Eso empuja a que los datos dejen de ser un subproducto operativo y pasen a ser un activo que requiere gestión, criterio y supervisión permanente", advierte el CEO de Asimov Consultores y presidente de Chiletec, Felipe Mancini.

Asimismo, el ejecutivo identifica que esto instala una nueva forma de operar que va más allá de las sanciones y la fiscalización de la futura Agencia de Protección de Datos Personales. "El impacto real es otro: obliga a profesionalizar la gestión de datos dentro de las organizaciones e integrarla en la toma de decisiones del negocio", plantea.

Desde el directorio de la Asociación Gremial de Profesionales en Protección de Datos Personales coinciden con ese análisis y añaden que "ya no se trata solo de recolectar datos y usarlos, sino de preguntarse para qué se usan, bajo qué base de licitud, con qué resguardos y con qué impacto para las personas", por lo que, afirman, la protección de datos pasa a formar parte de la gobernanza.

El desafío es, además, tecnológico. El especialista en ciberseguridad de ITQ Chile, Edgar Echeverría, advierte que "el control manual ya es imposible". Añade que este nuevo escenario exige automatizar las operaciones de seguridad mediante plataformas capaces de centralizar y correlacionar eventos en tiempo real. "La capacidad clave es la orquestación: detectar y contener incidentes reduciendo al mínimo la reacción humana", explica.

Este tránsito implica rediseñar procesos completos: desde la recolección hasta el almacenamiento y uso de los datos, incorporando criterios de necesidad, proporcionalidad, seguridad y respuesta a derechos de los titulares, analiza el gerente de asesoría legal y tributaria de PwC Chile, Jonathan Israel.

En esa línea, advierte que la figura del Data Privacy Officer se "vuelve clave como articulador de la gobernanza, pero no actúa solo", ya que la responsabilidad también cae en áreas legales, tecnológicas, negocios y de compliance, lo que requiere mayor articulación. En paralelo, afirma Israel, las organizaciones deben desarrollar capacidades internas y una cultura orientada al uso responsable de los datos.

CÓMO IMPACTA LA LEY A LOS SECTORES QUE TIENEN A LOS DATOS AL CENTRO

Cumplir con ley sin perder la viabilidad del negocio es el reto para las empresas que hacen uso intensivo de información personal. Consentimiento explícito de los dueños de los datos es solo uno de los conceptos que entran en juego en diciembre.

POR FRANCISCA ORELLANA

La nueva Ley de Protección de Datos Personales transformará por completo la forma en que algunos sectores económicos utilizan la información personal como centro de su negocio, lo que implica una transformación relevante en su estrategia para seguir siendo competitivas.

La norma entrega un nuevo marco y estándar para la privacidad y seguridad de los datos personales y su implementación plantea desafíos legales, tecnológicos y operativos para cumplir con ella sin perder la viabilidad del negocio.

El director de KPMG Law de KPMG Chile, Edmundo Varas, explica que actualmente los datos personales son utilizados en diversos ámbitos, como procesos laborales, desarrollo educacional, analítica urbana, gestión de políticas públicas, prevención de fraudes, análisis de proveedores y otros, tanto en el sector público como privado.

"Hay sectores como banca, seguros, servicios financieros, telecomunicaciones, salud, retail y economía digital que se verán fuertemente afectados, ya que realizan tratamiento de datos a gran escala, manejan datos sensibles y utilizan mecanismos de decisiones automatizadas o perfilamiento", dice Varas, mientras advierte que existe una infinidad de sectores que aún no han evaluado adecuadamente cómo la ley los podría impactar.

Ricardo Seguel, docente de la Facultad de Ingeniería de la U. Adolfo Ibáñez y senior advisor en Technology Unit, menciona que la nueva ley impacta en los derechos ARCO —las facultades de acceso, rectificación, cancelación/supresión y oposición, que permiten a las personas controlar sus datos personales— y "empodera las personas a demandar a las instituciones públicas o privadas de forma transversal por el uso no autorizado de su información en campañas de publicidad o en cómo están custodiando su información privada".

En ese marco, ahora, las empresas deberán contar con el consentimiento "explícito de cómo y qué datos utilizar o compartir para actividades de publicidad, mejoras de procesos internos e incluso en entrenamiento de modelos de IA y GenAI", agrega.

El director de la Asociación Gremial de Profesionales en Protección de Datos Personales, Diego Morandé, indica que las empresas deberán implementar, por ejemplo, registros de actividades de tratamiento (RAT) y, en muchos casos, realizar estudios de impacto en protección de datos, especialmente cuando tratan información sensible, hacen perfilamiento o usan tecnologías de alto riesgo. "Esto implica rediseñar procesos, contratos, sistemas y modelos de negocio que históricamente se construyeron sin estándares formales de rendición de cuentas en protección de datos y privacidad", precisa.

Para lograrlo, añade Seguel, las organizaciones "deberán implementar varios pasos administrativos de forma automática para poder responder en tiempo y forma a las personas y a la Agencia de Protección de Datos".

SOLO **36%** DE LAS INSTITUCIONES FINANCIERAS TENÍA IDENTIFICADOS Y CLASIFICADOS LOS DATOS PERSONALES SENSIBLES, SEGÚN UN ESTUDIO DE EY A FEBRERO PASADO.

Más derechos

Las empresas están poco a poco ajustando sus procesos a la nueva normativa y buscando tener el consentimiento explícito de las personas para poder utilizar su información.

En la industria financiera, por ejemplo, un estudio de EY indica que, a febrero de este año, solo un 36% de las instituciones ya tenía identificados y clasificados los datos personales sensibles, mientras que el 50% se encontraba en desarrollo y solo el 29% de los encuestados había implementado la obtención del consentimiento explícito del titular antes de tratar sus datos personales.

Morandé agrega que, con la ley, las estrategias de marketing, fidelización y analítica de clientes deberán ajustarse a nuevas bases de licitud y a principios como minimización y responsabilidad proactiva, lo que cambia la forma de capturar y explotar datos. "Las empresas que no inviertan en capacidades internas enfrentarán mayores riesgos sancionatorios, mayores costos de corrección y una clara desventaja competitiva frente a quienes integren la protección de datos como un activo estratégico. El desafío más importante se encuentra en la concientización y evangelización de estos temas", dice.

En ese objetivo, detalla Seguel, la brecha digital en las instituciones públicas y en las pymes es la mayor tarea pendiente en Chile.

Varas agrega que el ordenar las bases de datos, establecer medidas tecnológicas para captar, utilizar y proteger los mismos, así como diseñar reglas que permitan aprovechar de manera segura el dato con respecto a los grupos de interés con que se relaciona la empresa, no debe considerarse un costo, sino una inversión. "Preparará a la empresa para acceder, analizar y emplear datos de manera segura y eficiente para respaldar decisiones estratégicas y optimizar los resultados del negocio", concluye el ejecutivo.

¿Prevención o infracción? Un tema transversal en la agenda de este año

El llamado es que, desde el directorio hasta los responsables operativos que administran datos personales, en organizaciones grandes, medianas y pequeñas, incorporen a su agenda conceptos como MPI, DPO, RAT, EIPD y ARSOPB para prevenir el mal uso de los datos personales; de lo contrario, quedan expuestos a sanciones, daño reputacional e infracciones.

¿Qué se deben preguntar hoy el Directorio y los Altos Ejecutivos?

Víctor Cortés, Director Ejecutivo de Grupo Mitiga LATAM y fundador de soluciones de software de riesgo corporativo, propone comenzar con cinco preguntas muy concretas.

- ¿Tenemos un Modelo de Prevención de Infracciones (MPI), con responsable definido, recursos, facultades y controles verificables?
- ¿Existe un Registro de Actividades de Tratamiento (RAT) alineado con la ley, la regulación aplicable y estándares internacionales?
- ¿Aplicamos Evaluaciones de Impacto en Protección de Datos (EIPD) para identificar riesgos y controles mitigantes?
- ¿Podemos atender en plazo los derechos de Acceso, Rectificación, Supresión, Oposición, Portabilidad y/o Bloqueo (ARSOPB), con trazabilidad y evidencia?
- ¿Contamos con evidencia auditable de la debida diligencia desplegada antes, durante y después de un incidente?

A su juicio, estas son preguntas mínimas para cualquier organización, pública o privada, grande, mediana o pequeña, que quiera iniciar este desafío sobre una base concreta y alineada con la nueva normativa.

“Es imposible que la prevención mitigue el 100% de los incidentes, pero sí es muy probable que, un incidente genere infracciones con altos costos adicionales”.

¿Cuál es el costo de que te infraccionen?

No es sólo la multa, también hay exposición reputacional, pérdida de confianza y tensión con clientes, colaboradores, reguladores y directorio. Además, muchas empresas aún dudan en reportar incidentes por temor a ser tratadas como victimarias, incluso cuando han sido víctimas.

Un sistema maduro debiera distinguir entre negligencia y diligencia, y valorar la corrección oportuna y la transparencia responsable.

Con todo, plantea una mirada optimista: si una entidad se prepara a tiempo y de forma genuina, reconoce el derecho que tienen las personas sobre sus datos y cuenta con un modelo robusto, evidencia y reporte oportuno, un incidente no debería traducirse en un daño reputacional irreparable. Un MPI certificado por la Agencia no vuelve inmune a una organización, pero sí puede transformarse en una señal concreta de diligencia, control y capacidad real de respuesta.

La pregunta correcta no es solo qué ocurrió, sino cuánta diligencia se puede demostrar antes, durante y después de un incidente.

¿En qué estado de cumplimiento se encuentran las empresas?

A su juicio, hoy existen tres grandes grupos. El primero reúne a organizaciones que se anticiparon y ya avanzan en preparación e implementación. Allí ubica a la ACHS, cliente de Grupo Mitiga, que está próxima a salir en vivo con MitigaData tras un trabajo exigente y muy coordinado.

El segundo grupo está formado por entidades que recién comenzaron su diagnóstico o el levantamiento de su MPI y sus sistemas de soporte. En general, ambos grupos se concentran en las grandes empresas del país.

El tercer grupo, en cambio, sigue sin iniciar este desafío. Para él, esto es un riesgo en sí mismo, especialmente en empresas medianas y pequeñas que prestan servicios a grandes corporaciones, porque la ley alcanza a toda persona jurídica, independiente de su tamaño o sector.

Director Ejecutivo de Grupo Mitiga LATAM, empresa dueña de las herramientas tecnológicas MitigaData, Ética en Línea, Reporte Integral y B-GRC.

¿Cuáles son tus principales aprendizajes prácticos a la fecha?

El primero es simple: los dos años de implementación pasan rápido. Un MPI serio debe incorporar, al menos, RAT, EIPD, atención de derechos ARSOPB, evidencia auditable y trazabilidad inalterable. Si una organización aún no reconoce estos conceptos, la cuenta regresiva ya comenzó.

También advierte que la ley exigirá un rol responsable al interior de las organizaciones para coordinar con la nueva Agencia y orquestar tareas operativas: identificar procesos y bases de tratamiento, definir RAT, activar EIPD cuando corresponda, revisar contratos con colaboradores, proveedores y clientes, y ordenar consentimientos y respaldos junto al área legal.

Destaca, además, que hoy existe tecnología capaz de apoyar gran parte de este trabajo. Estas soluciones ayudan a sistematizar, dar seguimiento y hacer más eficiente un proceso que, de otro modo, suele depender de planillas, correos y esfuerzos dispersos.

¿Qué experiencia real puedes destacar y comentar?

Como experiencia concreta, menciona el trabajo con ACHS en el levantamiento y sistematización del modelo y sus elementos. Señala que ha sido un desafío exigente y, al mismo tiempo, muy valioso, donde incluso han aprovechado herramientas de inteligencia artificial para acelerar tareas de levantamiento, ordenamiento y análisis, siempre con supervisión humana.

DÉFICIT DE EXPERTOS EN CIBERSEGURIDAD EN CHILE ELEVA LA EXPOSICIÓN EN LAS ORGANIZACIONES

Ante una demanda estimada que supera los 60 mil profesionales para este año, expertos advierten una gran brecha en los perfiles especializados. Esto impacta la gestión de riesgos, encarece costos y obliga a externalizar capacidades clave.

POR ANDREA CAMPILLAY

El déficit de talento en ciberseguridad en el país ya no se explica solo por la falta de profesionales, sino por la escasez de especialistas con una experiencia práctica real. Con una demanda estimada de 63.500 profesionales para este año —según el Equipo Nacional de Respuesta a Incidentes de Seguridad Informática de Chile (CSIRT)—, la brecha está tensionando la seguridad y el cumplimiento en las organizaciones.

Pero el problema no es solo cuántos profesionales hay disponibles, sino "qué tan preparados están para enfrentar desafíos específicos", plantea el líder de la plataforma de educación y talento de la Alianza Chilena de Ciberseguridad, Alejandro Hevia. En la práctica, detalla, las organizaciones "no están buscando perfiles generalistas", sino expertos con conocimientos concretos y experiencia aplicada en ámbitos como respuestas a incidentes, *hacking* ético, análisis de amenazas, seguridad en la nube o gestión de riesgos. En ese sentido, dice Hevia, "el déficit es principalmente cualitativo", pues no basta con aumentar el número de profesionales, sino que es clave desarrollar talento con habilidades alineadas a las necesidades del mercado.

Actualmente, los perfiles más demandados en Chile "coinciden, en gran medida, con los más escasos", afirma la gerente de operaciones de HunTI Consultores, Bertha Venegas. Entre ellos destacan los CISO o directores de seguridad de la información. "Este es un perfil particularmente difícil de encontrar, ya que requiere no solo conocimientos técnicos avanzados, sino también comprensión del negocio y del marco regulatorio", dice Venegas. También se requieren analistas de operaciones de seguridad, especialistas en pruebas de penetración o los llamados hackers éticos. "Si bien hay interés en esta área, son pocos los profesionales con trayectoria comprobable", apunta la ejecutiva.

Impacto

La escasez de talento "está provocando que las empresas destinen personal general de TI a labores de ciberseguridad, lo que constituye un riesgo crítico", asegura el CEO de Lockbits, André Goujon. Aunque hoy existen herramientas que ayudan a la detección, "la capacidad de interpretar alertas, priorizar riesgos y responder a tiempo sigue dependiendo de personas con experiencia", aclara Goujon. Esto impacta directamente la capacidad de las organizaciones para prevenir, detectar y responder a incidentes, pues dificulta la correcta implementación, operación y actualización de controles clave.

Ante la creciente presión por cumplir con el marco regulatorio, "muchas empresas logran avanzar en definiciones y marcos formales, pero enfrentan dificultades para llevarlos a una operación efectiva", sostiene el gerente de negocios y ciberseguridad de Entelgy Chile, Pablo Álvarez, lo que incrementa el nivel de exposición. Además, señala que la brecha está "forzando un cambio estructural en la forma de invertir en ciberseguridad", con organizaciones transitando desde un modelo centrado en capacidades internas hacia uno enfocado en la eficiencia operativa y el acceso a talento externo especializado.

"Cuando faltan expertos, no solo se debilita la seguridad tecnológica, sino también la capacidad efectiva de cumplir con los estándares que exige el nuevo marco regulatorio", asegura el directorio de la Asociación Gremial de Profesionales en Protección de Datos Personales. Mientras, en el mercado laboral, como consecuencia "se observa una extensión en tiempo muy significativa en los procesos de selección, que hoy pueden extenderse entre tres y seis meses, e incluso quedar abiertos sin lograr cubrir las vacantes", complementa Venegas.

Cerrar la brecha

Para los expertos, las empresas, el sistema educativo y el Estado están reaccionando. "Por ejemplo, han aumentado la inversión en capacitación interna, certificaciones y atracción de talento", dice Hevia. Aunque señala que muchas veces compiten por un grupo reducido de especialistas, lo que eleva costos y dificulta cubrir todas las necesidades.

"Las universidades y centros de formación han ampliado significativamente la oferta de carreras, diplomados y *bootcamps* en ciberseguridad", expresa Venegas. A su juicio, si bien este avance es positivo y necesario, aún no logra cubrir la demanda real del mercado. En cuanto al Estado, destaca los avances en materia de regulación, institucionalidad y posicionamiento de la ciberseguridad como un tema prioritario a nivel país. No obstante, aclara que el impacto de estas medidas es progresivo y se verá reflejado en el largo plazo.

"No basta con aumentar el número de profesionales, sino que es clave desarrollar talento con habilidades específicas y alineadas a las necesidades reales del mercado", asegura el líder de la plataforma de educación y talento de la Alianza Chilena de Ciberseguridad, Alejandro Hevia.

GRUPO DF
DF DFLIVE DFMAS DFSUDI SEÑAL DF CAPITAL BD BD

Director: José Tomás Santa María / **Subdirectora:** Paula Vargas / **Gerente Comercial:** José Ignacio De la Cuadra / **Editora:** Claudia Marín / **Director Creativo y Arte:** Rodrigo Aguayo
Coordinadora: Marcia Aguilar / **Dirección** Edificio Fundadores, Badajoz 45, piso 10, Las Condes, Fono: 2 23391000 / e-mail: buzondf@df.cl / **Impreso por** Gráfica Andes Limitada, que sólo actúa como impresor.