CIBERSEGURIDAD Y ANUARIO TI

EL ALTO PRECIO QUE PAGAN LAS EMPRESAS CUANDO SUFREN UN CIBERATAQUE

Aunque las cifras varían según el tipo de industria y su madurez digital, la paralización de operaciones, daños a la reputación y pérdida de datos estratégicos que deja un ciberataque pueden llegar a costarle varios millones de dólares a las grandes empresas locales.

POR ANDREA CAMPILLAY

Según el informe "Cost of a Data Breach 2025", de IBM, el costo promedio global de una filtración de datos asciende a US$ 4,4 millones, una cifra que ilustra la magnitud que puede alcanzar un ciberataque en un contexto de mayor digitalización con amenazas crecientes sobre las industrias críticas.

Cuando ocurre un incidente de ciberseguridad en empresas medianas o grandes en Latinoamérica, sin importar el tipo de ataque, el costo oscila "entre US$ 4 a US$ 5 millones" señala el director de Cyber de Deloitte, Felipe Catalán, sobre la base de estudios que ha realizado la firma. El ejecutivo puntualiza que esto puede variar por la regulación y la imposición de multas importantes en caso de filtración de información sensible, según el volumen de los datos que hayan sido afectados y cuánta dependencia digital haya en los procesos productivos. Resalta que en el caso de Chile, "la cifra puede ser mayor, dado el impacto de la entrada en vigencia de la Ley Marco de Ciberseguridad (...) y la nueva Ley de Protección de Datos Personales que incrementan las consecuencias económicas".

El impacto financiero que puede llegar a tener un ciberataque varía según el tipo de industria y su madurez digital, pero hay consecuencias que se repiten: "Los impactos observados incluyen paralización de operaciones, daños a la reputación, pérdida de datos estratégicos y costos operacionales derivados de la recuperación", asegura el managing director de Accenture Chile, Luis Eduardo Porta, quien explica que las diferencias se deben, principalmente, al nivel de madurez en ciberseguridad, el tipo de activos comprometidos y cuán crítico es el servicio entregado.

"Para empresas pequeñas o pymes, los costos directos e indirectos por un incidente pueden oscilar desde decenas de miles hasta unos cientos de miles de dólares", complementa el investigador de ciberseguridad de ESET Latinoamérica, Mario Micucci. Por industrias, detalla que en el costo monetario esperado por incidente, el sector financiero "suele pagar más que el promedio", con alrededor de US$ 6,08 millones como costo medio por brecha, según IBM. Asimismo, las pérdidas pueden llegar a ser mayores si hay fraude masivo, fuga de secretos comerciales o interrupción de servicios de pagos.

"Los impactos observados incluyen paralización de operaciones, daños a la reputación, pérdida de datos estratégicos y costos operacionales derivados de la recuperación", asegura el managing director de Accenture Chile, Luis Eduardo Porta.

En la industria minera, los costos causados por un ciberataque "combinan pérdida de producción (paradas de planta), remediación OT/IT y posibles multas y daños ambientales", dice Micucci. En el caso de los servicios básicos, señala que los costos económicos pueden ser muy altos por efecto cascada: la interrupción del servicio, sanciones regulatorias, costos de emergencia y reparación de tecnologías de operación e infraestructura. "A nivel regional hay estudios que muestran que ataques a infraestructuras críticas pueden generar impactos macro, como por ejemplo, un ciberincidente que afecte muchas entidades estatales puede equivaler a varios puntos del PIB en países pequeños", añade el investigador.

Sin embargo, el impacto en credibilidad suele ser "incluso más profundo que el financiero", plantea el líder de ciberseguridad & SI de Defontana, Israel Fuentes, ya que tras una filtración de datos, una parte relevante de los clientes deja de comprar o reduce su vínculo con la marca por pérdida de confianza. "Ese 'daño invisible' se refleja en menor crecimiento, más dificultad para cerrar nuevos negocios y, en algunos casos, afectación reputacional prolongada durante años", recalca Fuentes.

Medidas de mitigación

Frente a este panorama, "las organizaciones chilenas más maduras están trabajando en varios frentes simultáneos", comenta el CEO de Resility, Patricio Campos. Señala que hay un avance decidido hacia arquitecturas Zero Trust y "una disciplina más estricta en la gestión de parches y actualizaciones", cerrando las brechas que históricamente han sido la puerta de entrada de los atacantes.

Reducir el tiempo de detección y respuesta, incorporando centros de monitoreo y automatización con inteligencia artificial para "contener ataques en minutos y no en días", es otra de las medidas que Fuentes destaca junto al desarrollo de planes formales de respuesta a incidentes y continuidad operativa.

FORTINET

La ciberseguridad tiene que ser resiliente y responsable

La dependencia digital de las organizaciones cada vez más creciente, junto a los desafíos de la transformación digital y el advenimiento de la inteligencia artificial (IA) hacen más complejo el panorama.

En Chile, durante el primer semestre del año hubo 4.2 mil millones de intentos de ciberataques. Latinoamérica, en tanto, congregó el 25% del total de detecciones a nivel global. Y aunque hoy existe mayor concientización, lo cierto es que los riesgos crecen y se complejizan. “Las consecuencias financieras de un ataque son enormes. Solo en la Región llegaron al millón de dólares y mientras más avanza la digitalización, mayor es el riesgo”, indica Gonzalo García, vicepresidente de Ventas de Fortinet para América del Sur.

En efecto, la dependencia digital de las organizaciones cada vez más creciente, junto a los desafíos de la transformación digital y el advenimiento de la inteligencia artificial (IA) hacen más complejo el panorama de las amenazas.

Por una parte, los cibercriminales usan la IA para sofisticar aún más su ofensiva, generar correos de phishing, mapear superficies de ataque y automatizar campañas sumamente realistas de ingeniería social. “Hoy, incluso, pueden replicar la voz de una persona. Estamos expuestos a deepfakes en video y nos enfrentamos a adversarios cada vez más avanzados”, comenta el especialista.

En efecto, plantea Gonzalo García, ya estamos frente a una cadena de suministro del ciberataque, donde la dark web es su marketplace. “Allí transan desde kits de exploits hasta bases de datos para entrenar modelos de IA”, afirma.

No obstante, por otro lado, compañías como Fortinet también utilizan la IA para automatizar y apoyar la detección y respuesta temprana, así como detectar malware, resumir y priorizar alertas. “Nuestra misión es ayudar a las organizaciones no solo para que sean ciberseguras, sino también ciberresilientes y eso implica trabajar en la prevención, pero de manera consciente de que pueden tener un incidente, ante el cual tienen que reaccionar de forma certera y rápida para evitar mayores consecuencias”, explica García.

Gonzalo García, vicepresidente de Ventas de Fortinet para América del Sur.

Negocio non stop

El complejo escenario del mercado actual conlleva un nuevo desafío: dar seguridad a los datos en movimiento, lo cuales se potencian de manera creciente con la adopción de la IA, al ser la mayor consumidora de datos. Así, los datos están en diversos dispositivos de todo tipo, en los usuarios, en data center, en la nube y en las aplicaciones.

“Una organización puede tener distintas tecnologías de distintos proveedores, por lo que se hace más complejo operar y mantener. En Fortinet entendemos que el negocio es non stop y acompañamos a cada organización en todo el ciclo de vida de la ciberseguridad”, asegura Gonzalo García.

“Nuestra misión es ayudar a las organizaciones no solo para que sean ciberseguras, sino también ciberresilientes”, Gonzalo García, vicepresidente de Ventas de Fortinet para América del Sur.

Para ello, Fortinet dispone de la mejor tecnología, un gran canal de partners y más de 1.200 colaboradores en Latinoamérica, enfocados en cubrir los requerimientos de sus clientes de punta a punta.

Adicionalmente, la compañía ha levantado Fortinet Security Academy para la formación de especialistas en convenio con entidades educativas, así como la capacitación de sus socios de negocios. Y también dispone de programas especializados para fomentar la concientización, ya que la ciberseguridad no se detiene.

“Compañías y personas son cada vez más dependientes de la tecnología y deben usarla con confianza, pero también con conciencia. Sin duda, viene una nueva era con la IA, así como la revolución que produjo internet en un principio. No hay que temerle, pero sí hay que ser consciente y responsable”, sostiene el vicepresidente.

Lo que viene

Según datos de IDC, el mercado de la ciberseguridad crecerá entre un 10 y 15% en Latinoamérica, donde Fortinet está muy bien posicionado: 7 de cada 10 dispositivos desplegados le pertenecen.

Y es que no solo ha invertido en su desarrollo y expertise, también lo ha hecho en puntos de presencia para dar seguridad como servicio, teniendo equipos in situ para acompañar a sus clientes y tener mejores tiempos de respuestas.

El equipo de ingenieros de Chile propuso la idea de crear un Centro de Experiencia en la oficina local, siendo pioneros, y se ha replicado en otros países como Argentina, Brasil, Colombia y Perú, mejorando así la experiencia de sus clientes para ver por sí mismos cómo se resuelven sus problemáticas de ciberseguridad. “Ahora nuestra proyección es seguir creciendo a doble dígito”, concluye Gonzalo García.

CIBERSEGURIDAD Y ANUARIO TI

LA NUEVA ECONOMÍA DEL CIBERCRIMEN Y EL AVANCE DE LAS MAFIAS DIGITALES

La profesionalización del delito digital ha multiplicado la velocidad y el alcance de los ataques. Expertos advierten que Chile enfrenta un crecimiento explosivo de intentos de intrusión y que empresas y reguladores deben escalar su respuesta al mismo ritmo.

POR VALENTINA CÉSPEDES

La nueva economía del delito digital dejó atrás al hacker aislado para dar paso a mafias cibernéticas que operan con lógica empresarial. Con cadenas de suministro, herramientas basadas en inteligencia artificial (IA) y modelos criminales escalables, los ataques son hoy más rápidos y rentables. Esta profesionalización ha convertido al cibercrimen en una amenaza transversal para empresas, instituciones y ciudadanos.

Según el Reporte de Ciberseguridad 2025 de Entel Digital, 2024 estuvo marcado por un aumento sostenido en ataques, con el *ransomware* como principal amenaza en América Latina y el Caribe. Este tipo de ataque que cifra sistemas y exige un rescate, tuvo especial impacto en Chile, que se ubicó como el cuarto país más afectado, con el 7% de los incidentes, reflejando el interés de los ciberactores por economías emergentes.

El subgerente de soluciones y servicios de ciberseguridad de Entel Digital, Luis Elola, sostiene que el cibercrimen se ha consolidado en "organizaciones altamente estructuradas y profesionalizadas, con financiamiento estable y capacidades tecnológicas avanzadas, incluida la adopción de IA". Este modelo, explica, convierte el delito digital "en una economía global con enorme impacto", capaz de interrumpir operaciones críticas, secuestrar información y operar con la eficiencia de una empresa. "La mayor sofisticación de estos grupos incrementa la velocidad, precisión y alcance de los ataques, elevando significativamente el riesgo para gobiernos, empresas y ciudadanos", detalla.

Expansión del ransomware

El gerente de ingeniería de Fortinet Chile, Juan Pablo Arias, señala que en América Latina "el *ransomware* y el fraude digital están creciendo en frecuencia y severidad", esto basándose en datos de FortiGuard Labs, que entre 2023 y 2024 registró un incremento de 6 mil a 26 mil millones de intentos en ciberataques en Chile, lo que refleja la escala y velocidad del fenómeno.

Así lo profundiza el director de ingeniería en ciberseguridad de la U. Andrés Bello, Edgardo Fuentes, explicando que estos sistemas "no solo democratizan el acceso al delito al permitir que grupos con poca experiencia alquilen herramientas y servicios de ataque, sino que además instauran un verdadero ecosistema de proveedores y clientes en la economía criminal". Añade que este esquema "actúa como una empresa", entregando paquetes personalizables, mientras los afiliados ejecutan ataques y comparten ganancias.

El cibercrimen se ha consolidado en "organizaciones altamente estructuradas y profesionalizadas, con financiamiento estable y capacidades tecnológicas", dice Luis Elola, de Entel Digital.

Asimismo, Fuentes relata que la IA y la automatización permiten "ataques más selectivos, rápidos y rentables", consolidando una economía criminal paralela en la *dark web* donde se venden kits de *malware*, credenciales robadas y servicios de lavado de criptomonedas.

Arias proyecta que, de acuerdo con predicciones de FortiGuard Labs para 2026, el cibercrimen está entrando a una "era industrial", impulsada por automatización e IA. A su vez, advierte que ya no solo se está atacando a grandes corporaciones y están apuntando "a proveedores de servicios, software de terceros y sistemas de nube, sabiendo que, al comprometer un eslabón, pueden escalar hacia múltiples víctimas".

Según analiza Fuentes, este aumento de fraudes cibernéticos "debilitan la credibilidad ciudadana en el comercio electrónico, la banca digital y la administración pública", generando un impacto social que trasciende lo tecnológico.

Regulación y desafíos

La CEO de Idónea y socia de la Alianza Chilena de Ciberseguridad, Catherine Muñoz, destaca que la Ley Marco de Ciberseguridad (que creó la ANCI y el CSIRT Nacional) alinea a Chile con el modelo europeo de la Directiva NIS2, que obliga a sus 27 países a tener autoridades y equipos de respuesta. Sin embargo, advierte que el plazo que exige Chile para notificar al CSIRT Nacional es de tres horas, lo que representa, dice, estándares muy altos y, en caso de que una organización no tenga listos los procedimientos, "automáticamente incumple la ley", pues es "materialmente imposible" cumplir con ese plazo. También subraya que las multas del Operador de Importancia Vital (OIV) por incumplimiento son serias y comparables a las europeas, y apuntan directamente a la alta dirección, obligando a los directorios a asumir un rol activo.

En este sentido, Arias afirma que "las empresas que no inviertan en cultura, formación y preparación quedarán estructuralmente expuestas". Por ello plantea ejercicios de crisis, simulaciones y planes de continuidad, además de "integrar inteligencia de amenazas, gestión de exposición y automatización en una arquitectura coherente". Y advierte que, ante atacantes que ya explotan IA, las organizaciones deberán elevar sus estándares de protección de datos y trazabilidad, en línea con la nueva Ley de Protección de Datos Personales y la Ley Marco de Ciberseguridad.

PUBLIRREPORTAJE

Para NIVEL4 el gran desafío de la industria es que la ciberseguridad va más allá de lo técnico

El mercado actual exige integrar estrategia, cumplimiento y cultura organizacional. “En NIVEL4 asumimos ese reto impulsando un modelo de cumplimiento normativo integral, que une marcos globales con leyes locales”, afirma Christian Navarro, Líder Comercial.

NIVEL4 es una consultora integral con 10 años de trayectoria y presencia en Chile, Perú y Colombia. Acompaña a organizaciones de toda la región y de diferentes sectores a gestionar la ciberseguridad como una práctica continua, midiendo riesgos, cerrando brechas y conectando estrategia, tecnología y cumplimiento. Opera en un ecosistema de partners legales y técnicos de primer nivel, transformamos la seguridad en una ventaja competitiva sostenible.

En la amplia oferta de servicios que ofrece, actualmente destaca su Programa Integral de Cumplimiento y alineación con frameworks, el cual opera en los planos jurídico y técnico a la vez. “El diagnóstico y el roadmap se entregan en el lenguaje que cada equipo necesita para cerrar brechas. Mapeamos y cruzamos controles para ganar eficiencia: una misma acción cubre exigencias de Ley de Protección de Datos, Ley Marco de Ciberseguridad, CMF y superintendencias, entre otras. Todo se ancla en NIST CSF, CIS o ISO/IEC 27001, fortaleciendo en el tiempo la postura de ciberseguridad, la gobernanza y el cumplimiento”, explica Diego Philippi, Gerente de Negocios.

De acuerdo al Gerente, la ciberseguridad es la gestión de riesgos que muchas veces no se visualiza en términos de riesgos muy reales, con impactos operacionales, financieros y reputacionales. “Podemos tener el mejor portón, pero si el guardia no sabe a quién deja pasar, es irrelevante. La mayoría de los ataques entra por las personas y debemos hacernos cargo de esa realidad; por eso la respuesta no es un checklist por cumplir, sino una actividad tan relevante como las finanzas, que exige la misma disciplina y continuidad”, plantea Diego Philippi.

Bajo la óptica de NIVEL4, las leyes ponen el piso y los marcos normativos, la estructura. “Nosotros debemos instalar las puertas y aprender a quién abrirles. Cuando institucionalizamos la concientización continua, medimos vulnerabilidades y tiempos de respuesta, y reforzamos las capacidades instaladas, el riesgo baja, el cumplimiento se acelera y la reputación se protege”, señala el Gerente de Negocios.

Christian Navarro, Líder Comercial.

Diego Philippi, Gerente de Negocios.

Así, para NIVEL4 el gran desafío de la industria es que la ciberseguridad va más allá de lo técnico. “Hoy se exige integrar estrategia, cumplimiento y cultura organizacional. En NIVEL4 asumimos ese reto impulsando un modelo de cumplimiento normativo integral, que une marcos globales con leyes locales. Nuestra proyección es consolidar en Latinoamérica una oferta que combine lo legal y lo técnico, y participar activamente en la definición de las reglas del juego, que guiarán la ciberresiliencia del futuro”, concluye Christian Navarro, Líder Comercial.

CIBERSEGURIDAD Y ANUARIO TI

LAS RAZONES QUE HACEN DE LAS PYMES UN BLANCO ATRACTIVO PARA LOS ATAQUES

La rápida digitalización dejó a muchas pymes expuestas: brechas básicas, baja capacitación y controles débiles las mantienen entre los blancos favoritos del cibercrimen.

POR ANAÍS PERSSON

En Chile, las pequeñas y medianas empresas se han convertido en uno de los focos más activos del cibercrimen. Solo en 2023, Kaspersky bloqueó 7,6 millones de intentos de ataque y 8,8 millones de acciones de *phishing* dirigidas a este segmento. La digitalización acelerada —pagos, facturación y servicios en la nube— no ha ido acompañada del mismo nivel de preparación. "Muchas carecen de políticas robustas, presentan errores humanos frecuentes y administran inadecuadamente permisos sensibles", afirma el director del equipo global de investigación y análisis de Kaspersky para América Latina, Fabio Assolini.

A nivel regional, el panorama se repite. Según la firma, el *phishing* afectó al 43% de las pymes de América Latina el último año; el *malware*, al 37%; el compromiso del correo electrónico, al 28%; y el *ransomware*, al 20%. En un 83% de los incidentes, los atacantes intentaron acceder a las redes internas, y en un 60% lograron ejecutar código malicioso. Para Assolini, la rentabilidad del *phishing* explica parte del fenómeno: "Un simple clic puede comprometer toda la red corporativa. En Chile vimos un aumento del 125% en mensajes falsos y 22 millones de bloqueos, equivalentes a 42 intentos por minuto". El bajo nivel de capacitación y la presión por operar rápido siguen abriendo puertas que los atacantes conocen bien.

"En Chile vimos un aumento del 125% en mensajes falsos y bloqueos equivalentes a 42 intentos por minuto", dice el director del equipo global de investigación y análisis de Kaspersky para América Latina, Fabio Assolini.

Brechas persistentes

En Chile, la baja madurez digital y la sobredependencia de sistemas críticos se repite en empresas de todos los tamaños, pero en las pymes las brechas suelen estar menos formalizadas. Para los atacantes, estas organizaciones concentran "datos de alto valor, como información financiera o credenciales, con un esfuerzo mucho menor para obtenerlos", señala el gerente de ingeniería de Fortinet Chile, Juan Pablo Arias.

La ausencia de controles básicos sigue siendo frecuente: contraseñas débiles, falta de autenticación multifactor, inventarios incompletos y respaldos deficientes. "Un atacante que entra por un equipo remoto puede moverse con relativa facilidad", añade Arias.

Desde Nivel4 Cybersecurity matizan el panorama. Su CEO, Fernando Lagos Berardi, afirma que, si bien las pymes están menos estructuradas, eso no las convierte necesariamente en objetivos más fáciles. "El atacante manda el anzuelo y caiga quien caiga. Los *hackeos* grandes siguen siendo para empresas grandes", dice. Aun así, reconoce fallas comunes: "Cuando se va un trabajador, no le bajan la cuenta; no tienen protocolos para registrar accesos ni definir qué sistemas son críticos".

Qué deben mejorar

Para Assolini, el primer paso es identificar vulnerabilidades críticas, capacitar de forma continua y mantener sistemas actualizados. "Hoy existen plataformas accesibles con simulaciones de *phishing* que permiten reforzar la defensa sin grandes inversiones", afirma.

Arias propone un "kit mínimo" que considere gobernanza básica, autenticación multifactor, higiene digital, segmentación de redes y respaldos resilientes, además de revisar políticas a la luz de la Ley de Protección de Datos Personales y la Ley Marco de Ciberseguridad. Lagos sugiere adoptar marcos internacionales que permitan ordenar procesos y auditar avances: "La estrategia debe alinearse con las normativas vigentes y con lo que los clientes exigen".

CIBERSEGURIDAD Y ANUARIO TI

"HOY TENEMOS INFORMACIÓN SISTEMATIZADA Y COMPARABLE, ALGO QUE CHILE NO TENÍA"

El director de la Agencia Nacional de Ciberseguridad, Daniel Álvarez, analiza los avances del trabajo realizado en el primer año del organismo y los desafíos que vienen.

POR ANAÍS PERSSON

A un casi año de su puesta en marcha, la Agencia Nacional de Ciberseguridad (ANCI) cierra un primer ciclo marcado por instalación institucional y despliegue regulatorio. Su director, Daniel Álvarez, define este período como "un año intenso, pero exitoso", en el que la entidad debió levantarse "desde cero" mientras asumía un rol central en el sistema nacional de ciberseguridad.

El primer hito fue la instalación administrativa y técnica. "Construir las capacidades internas era nuestra primera prioridad", afirma. Luego vino la plataforma de reporte de incidentes, mediante la cual los servicios esenciales deben informar eventos significativos. "Logramos habilitar un sistema robusto, con altos estándares de confidencialidad e integridad", destaca.

El tercer eje fue la calificación de Operadores de Importancia Vital (OIV), que "debiera ocurrir a mediados de diciembre". A esto se suman los reglamentos de la Ley Marco, la creación de una taxonomía propia de incidentes y las primeras estadísticas oficiales del país. "Hoy tenemos información sistematizada y comparable, algo que Chile no tenía", señala.

La coordinación con operadores de infraestructura crítica también evolucionó, aunque también evidenció brechas. "Hay instituciones que aún no cuentan con una cultura interna de ciberseguridad lo suficientemente desarrollada", advierte. También han identificado "capacidades técnicas limitadas y estructuras internas poco preparadas para las nuevas exigencias".

Sobre la madurez del país, Álvarez afirma que, a pesar de los avances, todavía se encuentra en construcción: "Tenemos una buena base institucional, pero necesitamos consolidar capacidades operativas y humanas". Entre los aspectos a reforzar menciona equipos profesionales, sistemas de detección y respuesta, y cultura de ciberseguridad transversal.

Para 2026, los desafíos serán decisivos. "Debemos finalizar la lista definitiva de OIV y supervisar su cumplimiento", afirma. También se desplegará el plan anual de fiscalización, con mecanismos de supervisión y posibilidad de aplicar sanciones.

El talento será otro eje crítico. "Chile necesita más profesionales capaces de gestionar riesgos tecnológicos y asegurar continuidad operativa", sostiene. Por ello, la ANCI impulsará capacitación, certificación de habilidades y "planes de educación temprana en ciberseguridad".

PUBLIRREPORTAJE

ECIJA OTERO: Experiencia europea en protección de datos, aplicada al contexto local

ECIJA OTERO

"Las obligaciones que establece la nueva regulación sobre protección de los datos personales en Chile no se aborda con un 'parche' de último minuto, sino como una estrategia de cumplimiento integral que vincule la protección de datos personales con el gobierno corporativo, la ciberseguridad, y, en definitiva con todas las aristas del negocio", afirma Constanza Pasarin, Manager de Protección de Datos de la firma.

Constanza Pasarin, manager de Protección de Datos de la firma.

Gerardo Otero, socio.

Como firma legal chilena especializada en tecnología, protección de datos y ciberseguridad, ECIJA OTERO es el puente entre la experiencia europea, especialmente la española, y las necesidades concretas del mercado local.

En efecto, desde su práctica en España, donde ECIJA ha sido reconocida por más de dos décadas como referente en el diseño e implementación de modelos de cumplimiento en privacidad, ciberseguridad y tecnologías emergentes, pone ese know how jurídico y técnico al servicio de las organizaciones chilenas que hoy se están preparando para enfrentar el nuevo escenario regulatorio.

"Nuestra propuesta de valor combina tres elementos claves: un entendimiento jurídico profundo del modelo del Reglamento General de Protección de Datos (RGPD) y del funcionamiento de la autoridad de control española; un equipo local que conoce la realidad regulatoria y de negocio en Chile; y una aproximación práctica que busca aterrizar la normativa en documentos, procesos y decisiones corporativas concretas", indica Gerardo Otero, socio.

Como firma legal, ECIJA OTERO no se limita a elaborar políticas, sino que también, diseña modelos de gobernanza en protección de datos, construye matrices de riesgo y registros de actividades de tratamiento, realiza evaluaciones de impacto y apoya la definición de medidas de seguridad y concientización de una nueva cultura respecto a los datos personales en las organizaciones, siempre con foco en soluciones implementables y sostenibles en el tiempo.

"La experiencia española muestra que el éxito de una ley de protección de datos no depende solo del texto normativo, sino de cómo las organizaciones incorporan tres claves: un enfoque basado en riesgos y responsabilidad proactiva (accountability), gobernanza clara y el uso sistemático de herramientas como el Registro de Actividades del Tratamiento (RAT), Evaluaciones de Interés Legítimo (LIAs, por sus siglas en inglés) y Evaluación de Impacto en Protección de Datos (PIAs, por sus siglas en inglés)", explica Constanza Pasarin.

Por último, destaca la manager de ECIJA OTERO, aunque Chile avanza por una senda fuertemente inspirada en el RGPD, lo que permite no partir de cero, persisten cuatro grandes desafíos: mapear correctamente el flujo de datos, articular una gobernanza interna sólida, gestionar adecuadamente a terceros y sus contratos, y fortalecer una cultura de protección transversal. "Anticiparse no solo reduce la exposición sancionatoria, sino que también se convierte en una ventaja competitiva ante a clientes, trabajadores y proveedores", concluyen Gerardo y Constanza.

CIBERSEGURIDAD Y ANUARIO TI

LOS RIESGOS DE CIBERSEGURIDAD PARA EL SISTEMA ELÉCTRICO

La incorporación de tecnologías de información, de operación y de control remoto ha aumentado la vulnerabilidad del sistema eléctrico, convirtiéndolo en un blanco apetecido para los ciberatacantes. Por eso, la industria ya avanza en mayores resguardos. POR FRANCISCA ORELLANA

Pese a los beneficios y la mayor eficiencia que ofrece, el avance de la digitalización del sistema eléctrico aumenta los riesgos de ataques cibernéticos a esta infraestructura crítica, los que pueden generar apagones masivos, pérdidas económicas, información y vulnerabilidad.

"La digitalización trajo eficiencia, pero también multiplicó el riesgo. Hoy el sistema eléctrico no solo enfrenta fallas físicas, sino ataques que pueden comprometer subestaciones, centros de control y el despacho energético, pues existe una interconexión de los sistemas", destaca Constanza Pasarin, manager de Ecija. Con la convergencia de las tecnologías de información, las

Un ataque cibernético involucra pérdida de visibilidad y control: "Si los operadores no pueden ver qué está pasando en la red ni enviar comandos correctivos, estaríamos volando a ciegas", dice Leonardo Causa, de la U. del Desarrollo.

tecnologías operativas y la operación remota, "el riesgo es mayor y tiene impacto directo en la continuidad del servicio", agrega.

Para el académico de la Facultad de Ingeniería de la Universidad Adolfo Ibáñez y director de DTC Cyber, Ricardo Seguel, el sistema eléctrico chileno ha experimentado un cambio significativo en los últimos diez años, avanzando a un estado de riesgo alto, donde los incidentes más preocupantes están relacionados con el *malware* destructivo (*wipers*) y *ransomware* para extorsión, "utilizados para generar una indisponibilidad prolongada de los sistemas de control".

También buscan tomar el control de sistemas de generación y distribución para desestabilizar el flujo eléctrico o destruir equipos con, por ejemplo, la sobrecarga de transformadores. "Y están las brechas de seguridad provocadas por los *insiders* (trabajadores internos o externos de una empresa) por falta de controles que mantengan la higiene de ciberseguridad que no se refuerzan por omisión, error o intención. Estas brechas representan más del 70% de los incidentes ocurridos en una empresa", advierte Seguel.

Según datos de CS4CA, los daños económicos de los ciberataques pueden exceder el 1% del PIB de algunos países, pero si se golpea la infraestructura crítica pueden llegar hasta el 6%. De los ataques producidos, un 58% ha afectado la infraestructura TI y un 77% ha involucrado la pérdida de datos.

No son cifras exageradas, dice Leonardo Causa, director de ingeniería civil en informática e innovación tecnológica de la U. del Desarrollo: "Para dimensionarlo, en Chile eso equivale a cerca de US$ 18 mil millones". Un ataque cibernético involucra pérdida de visibilidad y control: "Si los operadores no pueden ver qué está pasando en la red ni enviar comandos correctivos, estaríamos volando a ciegas. La recuperación de un *blackout* nacional podría tomar varios días, con costos económicos incalculables para industrias como la minería, que representa el 10% de nuestro PIB".

No obstante, el país está avanzando en resguardo: "Chile ha hecho esfuerzos importantes. Contamos con normativa específica desde 2016 con la Ley 20.936 que establece estándares de ciberseguridad para el sector eléctrico y el Coordinador Eléctrico Nacional ha implementado protocolos de seguridad. Sin embargo, el riesgo crece más rápido que nuestra capacidad de respuesta", destaca Causa.

Coincide Pasarin, al reconocer el avance de la Ley Marco de Ciberseguridad, pero considera también que hoy no es suficiente tener controles técnicos: "El sector debe demostrar gobernanza, contratos seguros con proveedores, trazabilidad de decisiones y resiliencia operacional, la seguridad eléctrica ya es un asunto de riesgo-país y de cumplimiento legal".

Desafíos

Para los analistas, el país debe avanzar en el resguardo cibernético tanto en el ámbito público como privado. "El gran desafío es pasar del enfoque técnico a uno legal y sistémico de cumplimiento: ciberseguridad *by design* en la operación y, especialmente, en la cadena de suministro digital", dice Pasarin, y ejemplifica con los contratos con proveedores, que "deben establecer obligaciones concretas y exigibles, incluyendo mínimos de resiliencia operacional, segmentación segura de entornos, gestión de cambios con trazabilidad y controles auditables, entre otros".

Causa agrega que hoy muchas empresas eléctricas mantienen sus redes operacionales conectadas directamente con sus redes corporativas: "Es como si la puerta de tu casa diera directamente a una calle muy transitada. Se necesita una separación clara entre ambas redes, con zonas intermedias que filtren el tráfico y controles de acceso estrictos que impidan que una intrusión llegue hasta los sistemas que operan la red eléctrica". También se necesita un plan de modernización gradual de equipos que ya tienen más de 20 años de antigüedad: "Reemplazarlos es costoso, pero mantenerlos sin protección adecuada es un riesgo existencial", indica.

Seguel advierte que existe un déficit de capital humano capacitado en ciberseguridad e infraestructura crítica que dominen no solo los temas técnicos de la operación industrial, sino también los marcos de ciberseguridad que apuntan a ese fin, por lo que hay que formarlo para tener los especialistas necesarios para abordar la nueva etapa del sistema eléctrico.

CIBERSEGURIDAD Y ANUARIO TI

"NUESTRO PAÍS VIVE UNA PELIGROSA ASIMETRÍA ENTRE DIGITALIZACIÓN Y PROTECCIÓN"

Desde la Alianza Chilena de Ciberseguridad, Hugo Galilea plantea que las empresas locales deben avanzar hacia gobiernos corporativos alineados con los desafíos de la ciberseguridad.

La ciberseguridad se ha transformado en un eje crítico para la gestión que desarrollan todas las organizaciones. En ese contexto, y a pesar del significativo desarrollo que registra Chile en este ámbito, todavía resta camino por avanzar, con el propósito de consolidar una visión que se vincule con el negocio y neutralizar amenazas emergentes.

El consejero de la Alianza Chilena de Ciberseguridad, Hugo Galilea, puntualiza que "nuestro país vive una peligrosa asimetría entre digitalización y protección", que describe como una fachada digital del primer mundo con cimientos en desarrollo. "Tras evaluar a cientos de empresas, el diagnóstico es bastante claro: existe una ilusión de cumplimiento. Muchas organizaciones creen que por tener herramientas están seguras. Sin embargo, al auditar bajo la norma ISO 27001 o el marco NIST CSF 2.0 queda en evidencia que la tecnología está presente, pero el gobierno corporativo, ausente", plantea.

En esa línea, precisa que la industria financiera y los sectores regulados, como energía y telecomunicaciones, han alcanzado una madurez muy robusta, mientras que rubros como el retail, la industria productiva y los servicios B2B de gran tamaño operan con una deuda técnica y de procesos alarmante. "La ciberseguridad sigue secuestrada en el área de TI. Nuestro país está digitalizado, sí, pero la resiliencia operativa no ha crecido a la misma velocidad que la transformación digital", subraya.

A su juicio, el hito indiscutible de este año lo constituye el avance de la Ley Marco de Ciberseguridad, además de la adopción del NIST CSF 2.0, que representa un progreso metodológico clave, ya que incorpora explícitamente la función de "gobernanza", lo que obliga a las empresas a vincular la ciberseguridad con la estrategia de negocio.

Mirando hacia 2026, Galilea sostiene que no le preocupa tanto el malware tradicional, sino los deepfakes corporativos, donde, a través de ingeniería social hiperrealista dirigida a CEO y CFO, utilizando voz y videos generados por inteligencia artificial, se buscará autorizar transferencias o revelar credenciales.

"Un segundo vector serán los ataques a las cadenas de suministro. Las grandes empresas se están blindando, por lo tanto, la ofensiva irá por el lado de los proveedores más pequeños con el fin de usarlos como verdaderos 'caballos de Troya' y, de esa manera, entrar a la gran corporación. Si un eslabón crítico cae, la firma mandante se detiene. Esa interdependencia constituirá el gran riesgo sistémico para 2026", advierte.

PUBLIRREPORTAJE

Notaría Leiva
SEGUNDA NOTARÍA DE SANTIAGO

CisoServiceChile

Con CisoServiceChile, Notaría Leiva se convierte en la primera notaría de Chile en implementar ISO 27001

Junto a la consultora, proyecta certificación para enero de 2026.

La Notaría Leiva y CisoServiceChile anunciaron que prontamente finalizarán del proceso de implementación del Sistema de Gestión de Seguridad de la Información (SGSI) bajo la norma internacional ISO/IEC 27001:2022, posicionándose oficialmente como la primera notaría del país en adoptar este estándar de seguridad reconocido mundialmente. La certificación formal se proyecta para enero, marcando un antes y un después en la modernización del ecosistema notarial chileno.

"Para nosotros, ser la primera notaría de Chile en implementar ISO 27001 tiene un profundo valor institucional", señaló **Francisco Leiva, notario y titular de la Notaría Leiva**. "Entendemos que la ciudadanía exige servicios modernos, seguros y confiables. Esperamos recibir la certificación en enero como reflejo de un compromiso real con la protección de la información y con una fe pública acorde a los desafíos actuales".

Por su parte, **Jairo Ibáñez, Gerente General de CisoServiceChile** menciona: "Este proyecto demuestra que una notaría puede innovar y liderar cambios estructurales en seguridad de la información".

Este hito no solo responde a necesidades operativas, sino a un compromiso profundo con la fe pública y la protección de los datos sensibles que diariamente se resguardan en una notaría. La implementación de ISO 27001 aporta beneficios concretos como:

- Proteger los activos y garantizar la continuidad del negocio
- Proteger los procesos críticos y gestionar el riesgo
- Asegurar una gobernanza sólida de la información, habilitando controles, procesos trazables y una operación más ágil y confiable.

VALOR INMEDIATO

Para la alta dirección, el valor es inmediato: reducción efectiva de riesgos reputacionales y financieros, mayor continuidad operativa y una capacidad reforzada para responder a incidentes con precisión y anticipación. Esto se traduce en una organización que opera con menos incertidumbre y más control, alineada con exigencias regulatorias y expectativas globales. Y, quizás lo más relevante, la certificación ISO 27001 se convierte en un diferenciador competitivo que inspira confianza en clientes, socios estratégicos y organismos públicos. En un entorno donde la seguridad y la transparencia son determinantes, este estándar posiciona a la empresa como un actor moderno, responsable y preparado para liderar en mercados cada vez más exigentes. El proyecto ha sido acompañado por un robusto programa de capacitaciones continuas que ha permitido que todo el personal avance hacia una cultura más madura de seguridad de la información. Esta formación será sostenida durante 2026, consolidando la operación segura de todos los procesos críticos de la notaría.

Desde CisoServiceChile, **Jairo Ibáñez** menciona que esta implementación apunta a un avance que puede transformar la industria. "Notaría Leiva abrió un camino que el resto del país podrá seguir. Integrar ISO 27001 no solo moderniza procesos: establece un estándar que eleva la confianza ciudadana y fortalece la fe pública. Creemos que esto marcará un precedente para todas las notarías del país".

Con la implementación, Notaría Leiva se sitúa como un referente nacional en seguridad de la información, aplicada a servicios públicos y privados, demostrando que la transición desde un modelo analógico hacia uno más seguro, digital y trazable es posible, alcanzable y urgente para el sector.

CIBERSEGURIDAD Y ANUARIO TI

LOS RETOS DEL DÉFICIT DE ESPECIALISTAS EN SEGURIDAD INFORMÁTICA

Se estima que en el país faltan 28 mil expertos en ciberseguridad, lo que podría afectar las estrategias que las organizaciones impulsen para prevenir y defenderse de posibles ataques. ¿Cómo enfrentar la brechas?

Una serie de estudios elaborados a nivel tanto internacional como también en nuestro país advierten una situación preocupante: una brecha global de profesionales especialistas en seguridad informática. En Chile, el Equipo Nacional de Respuesta a Incidentes de Seguridad Informática de Chile (CSIRT) ha estimado que este déficit llegaría a 28 mil expertos y que recién podría solucionarse en 2033, lo que impone grandes desafíos para el presente y el futuro.

La directora de la carrera de ingeniería en computación e informática de la Universidad Andrés Bello, Jenny Pantoja, explica que la falta de capital humano en este ámbito no solo constituye un desafío técnico, sino que también estratégico y social, ya que compromete la confianza digital, la competitividad y la protección de datos en un entorno global cada vez más interconectado.

"Los cargos más críticos que se requieren son jefes de seguridad, analistas de seguridad, ingenieros tanto de seguridad como también de redes seguras y especialistas en respuesta a incidentes. Ello obedece a que las amenazas evolucionan muy rápido y la formación en estas áreas no ha crecido al mismo ritmo", detalla, y puntualiza que la dificultad radica en la alta especificidad exigida, la escasez de preparación avanzada y la creciente demanda impulsada por regulaciones y amenazas cada vez más sofisticadas.

¿Qué impacto tiene este déficit en las organizaciones? Según el director del magíster en ciberseguridad e investigador de la Facultad de Ingeniería de la U. San Sebastián, Thierry De Saint Pierre, existen cuatro dimensiones críticas: gestión reactiva en vez de preventiva; mayor exposición a sufrir incidentes graves; dificultades para cumplir la Ley Marco de Ciberseguridad; y la sobrecarga del capital humano que se desempeña en esta área.

"La solución para enfrentar esta brecha debe ser multinivel e integrar Estado, empresas y personas", dice, y detalla que desde el nivel central se requiere, entre otras cosas, implementar plenamente la Política Nacional de Ciberseguridad 2023-2028. "De igual manera es fundamental incentivar programas de becas y de reconversión laboral, además de alfabetizar en ciberseguridad a las personas a lo largo de toda la vida", subraya.

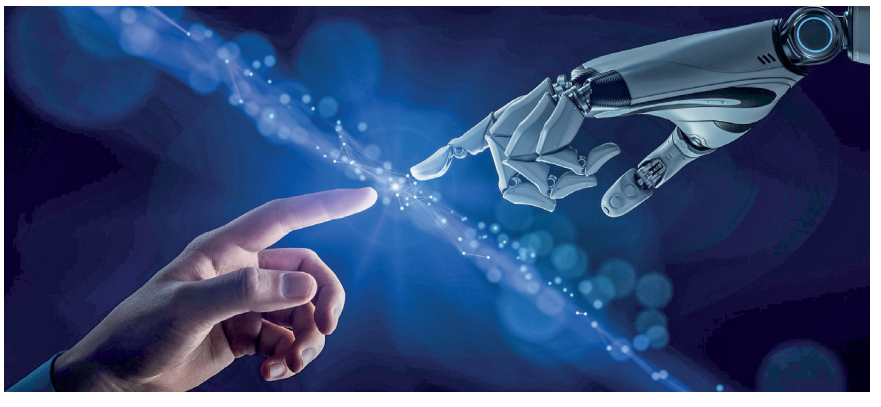
Ante este desafiante escenario ambos expertos plantean que consolidar estrategias claves, mejorar tanto las condiciones laborales como retener el talento, impulsar certificaciones internacionales y promover alianzas público-privadas son acciones decisivas para el futuro.

PUBLIRREPORTAJE

INDUSTRIA 5.0

La ventaja competitiva es cultural: 3IT y la IA al servicio de las personas y del negocio

AutonomIA es un modelo que integra autonomía operativa, IA aplicada y aprendizaje activo para lograr velocidad con control, lo cual se refleja en sus líneas de negocio de outsourcing TI y desarrollo de software.



La **Industria 5.0** pone el foco en las personas y promueve la **colaboración humano-máquina** para lograr productividad sostenible, aprendizaje continuo y decisiones mejor informadas. En ese marco, **3IT sostiene que el verdadero diferencial no está en la herramienta, sino en la capacidad de los equipos para operarla de forma consistente**.

"La tecnología impulsa, pero el sentido lo ponen las personas", señala Mario Salces, gerente general de 3IT.

Por eso desarrolló **AutonomIA**, un modelo que integra **autonomía operativa**, **IA aplicada** y **aprendizaje activo** para lograr **velocidad con control**, lo cual se refleja en sus líneas de negocio de outsourcing TI y desarrollo de software. La premisa es clara: primero el criterio y la colaboración; luego la tecnología como acelerador que no reemplaza, **potencia**.

"La tecnología impulsa, pero el sentido lo ponen las personas", señala **Mario Salces, gerente general de 3IT**. ***"Nuestra cultura promueve equipos que confían, conversan con datos y aprenden rápido. La IA libera tiempo para lo importante: escuchar al cliente y decidir mejor".***

En la práctica, AutonomIA se traduce en células orientadas a objetivos, documentación viva y transferencia de conocimiento que evita dependencias. La IA se usa donde aporta: generar estimaciones de esfuerzo sobre una base de conocimiento, automatización de procesos, Quality Assurance e insumos de documentación, mientras el juicio experto de las personas guía las decisiones críticas. En cuentas donde opera el modelo, 3IT ha observado **–30% en tiempos de entrega** y **–40% en horas de supervisión**, junto con reuniones más efectivas gracias a contexto compartido y **trazabilidad end-to-end**.

La proyección de la empresa sigue esa misma lógica de negocio. ***"Nos guía un propósito: crecer de manera sostenible y diferenciada"***, añade Salces. "De cara al 2026-2029, ampliaremos nuestra presencia en Chile y el exterior para consolidarnos como socio tecnológico estratégico y confiable a nivel internacional, con calidad e innovación como pilares. **Porque en 3IT los equipos piensan, la IA acelera y el valor permanece donde importa: en las personas y en el negocio".**

Contáctanos

CIBERSEGURIDAD Y ANUARIO TI

INTELIGENCIA ARTIFICIAL: ¿AMIGA O ENEMIGA?

En un escenario donde los ciberatacantes utilizan técnicas cada vez más sofisticadas, la inteligencia artificial es una pieza esencial para lograr mayor resiliencia en las organizaciones. La clave, según los expertos, es lograr que las empresas logren "gobernarla".

La relación entre el desarrollo de tecnologías y la ciberseguridad siempre ha sido muy estrecha: a medida que se desarrollan innovaciones, los ataques se vuelven más sofisticados, pero la defensa ante estos también tiene nuevas herramientas. Y esto se ha visto aún más profundizado con el desarrollo de la inteligencia artificial. De hecho, el Global Cybersecurity Outlook 2025, elabora-

do por el World Economic Forum, revela un aumento de *deepfakes*, estafas más creíbles y sofisticación en la ingeniería social basada en IA.

El presidente de la mesa de ciberseguridad de ACTI, Diego Macor, advierte que al menos el 18% de los ataques de *ransomware* en 2025 se disparan a través de campañas de *phishing* cada vez más automatizadas y personalizadas, a lo que se suma un 300% de aumento del tráfico de *bots* basados en IA en el último año -según datos de Akamai-, que está afectando operaciones online al imitar comportamiento humano, extraer datos y ejecutar fraudes a escala.

Por otra parte, hay una rápida incorporación de agentes de IA en ciberseguridad, capaces de asumir tareas operativas como el *triage* de incidentes, el análisis de *phishing* y la auditoría de eventos y gestión de alertas. "Estos sistemas ya avanzan hacia modelos más autónomos (llamados 'agentics'), donde múltiples agentes colaboran y aprenden en conjunto. El gran problema es que esta misma capacidad está siendo utilizada por los atacantes, quienes emplean agentes para automatizar campañas, generar o modificar código, y ajustar y perfeccionar sus ataques de manera continua", explica Macor.

Para el ejecutivo, la respuesta a estos riesgos no es frenar la IA, sino gobernarla. En esto coincide la vicepresidenta de la Alianza Chilena de Ciberseguridad, Pía Salas, quien asegura que, frente a un mayor uso de los ciberdelincuentes de IA generativa para crear *malware* polimórfico y campañas de *phishing* hiperpersonalizadas, la IA se presenta como la única forma de escalar nuestra defensa contra la alta automatización del atacante.

"La gran oportunidad se centra en dos frentes clave, que son vitales para cualquier ejecutivo. Primero, la seguridad predictiva: algoritmos de *machine learning* nos permiten pasar de ser reactivos a proactivos, identificando patrones anómalos y comportamientos sospechosos antes de que se materialicen en ataques", explica.

Lo segundo es la eficiencia operacional, agrega Salas: "La IA resuelve la fatiga de alertas del analista; al procesar masivamente datos de la red, *endpoints* y la nube, correlaciona eventos y reduce el ruido, esto se traduce en una optimización brutal del SOC (centro de operaciones de seguridad, por su sigla en inglés), permitiendo que los analistas se enfoquen solo en las amenazas de alto impacto y acelerando la contención de incidentes de días a segundos". Esto, dice, es crucial para el presupuesto.

"Estos sistemas ya avanzan hacia modelos más autónomos, donde múltiples agentes colaboran y aprenden en conjunto. El gran problema es que esta misma capacidad está siendo utilizada por los atacantes," dice el presidente de la mesa de ciberseguridad de ACTI, Diego Macor.

Frentes de acción

Luis Ignacio Jaque, jefe nacional de especialidad de la Escuela de Ingeniería, Energía y Tecnología de AIEP, detalla que las organizaciones están trabajando en tres frentes para robustecer su seguridad ante la mayor sofisticación de los ataques: en tecnología -con la implementación e integración de soluciones basadas en IA-, en gobernanza -con la creación de políticas de uso seguro de IA y la alineación con normas y marcos regulatorios- y en capital humano. "La IA no es aliada ni enemiga por naturaleza. Es un multiplicador. Su impacto depende del conocimiento, ética y responsabilidad con que sea implementada", puntualiza Jaque.

Para el managing director de Accenture Chile, Luis Eduardo Porta, las organizaciones en el país están acelerando la implementación de modelos de gestión de riesgo cibernético con marcos internacionales como FAIR, NIST CSF, ISO 27001 y CIS18, que permiten integrar la ciberseguridad al control financiero y operativo del negocio; y, a la vez, adoptan modelos predictivos basados en IA para pasar de un enfoque reactivo a uno adaptativo, siguiendo estándares de madurez observados en mercados desarrollados.

En este escenario, el déficit de más de 15 mil profesionales especializados para 2025 y la capacitación de colaboradores como primera línea de defensa se ha vuelto prioritaria, dice Porta. "Esto se complementa con mayor involucramiento directivo, y cada vez más directorios incorporan gobernanza digital y priorizan la ciberresiliencia como eje estratégico", concluye.

GRUPO DF
DF DFLIVE DFMAS DFSUD SEÑAL DF CAPITAL ED BIO BIO

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.

PUBLIRREPORTAJE

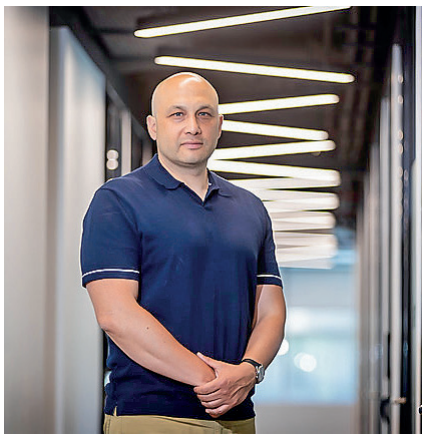
Kvalue: Rentabilizar la inversión tecnológica comienza por gobernar el ciclo de vida del dato

Un dato mal gobernado genera costos ocultos, riesgos operativos y barreras para adoptar IA, algo que hoy no se pueden permitir ni grandes compañías ni medianas en expansión.

Juan Pablo Lopez Legent, Gerente de Arquitectura; Nelson Henríquez Milesi, Gerente Comercial; y Ariel Linetzky Fuentes, Gerente de Arquitectura.

En un escenario donde la Inteligencia Artificial acelera la competencia empresarial y la transformación digital dejó de ser una iniciativa aislada para convertirse en un requisito estructural, las organizaciones enfrentan un desafío transversal: **cómo asegurar que cada peso invertido en tecnología —especialmente en datos y en plataformas SAP— se traduzca en valor real para el negocio**.

En este contexto, Kvalue se posiciona como un actor clave en el mercado chileno, con un mensaje que resuena con la urgencia que viven hoy las compañías: **sin datos gobernados, armonizados y automatizados, la IA no es posible. Y sin un ciclo de vida del dato correctamente diseñado, la inversión tecnológica no se rentabiliza.**



Nelson Henríquez Milesi, Gerente Comercial.

"Cuando una organización quiere avanzar hacia **advanced analytics** o IA, lo primero que se debe evaluar no es la herramienta, sino el **estado de sus datos y su nivel de madurez**. Solo con un diagnóstico completo es posible determinar qué parte de la inversión ya realizada puede ser rentabilizada, dónde están los brechas, y qué arquitectura permitirá sostener el crecimiento futuro", explica **Nelson Henríquez, gerente de Kvalue**.

Según el ejecutivo, este enfoque es especialmente relevante en un mercado que enfrenta desafíos regulatorios, presión por eficiencia, ciberseguridad y auditorías más exigentes.

Un dato mal gobernado genera costos ocultos, riesgos operativos y barreras para adoptar IA, algo que hoy no se pueden permitir ni grandes compañías ni medianas en expansión.

Kvalue aborda este problema desde una perspectiva integral del **ciclo de vida del dato**, entendiendo que la información nace en las unidades de negocio, se transforma en los procesos operativos y finalmente debe ser explotada por las áreas financieras, de administración y dirección.

https://kvaluetecnologia.com/