DIARIO FINANCIERO®

Fecha: 31/03/2026 Audiencia: 48.450 Sección: CONTRAPORTADA
Vpe: $5.198.359 Tirada: 16.150 Frecuencia: 0
Vpe pág: $7.443.240 Difusión: 16.150
Vpe portada: $7.443.240 Ocupación: 69,84%

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.