LITORALPRESS

Fecha: 26-08-2025
Medio: Diario Financiero
Supl. : Diario Financiero
Tipo: Noticia general
Título: DÉFICIT DE TALENTO Y ALZA DE ATAQUES TENSIONAN LA CIBERSEGUYRIDAD LOCAL

Pág. : 28
Cm2: 325,0
VPE: $ 2.879.511

Tiraje: 16.150
Lectoría: 48.450
Favorabilidad: No Definida

DÉFICIT DE TALENTO Y ALZA DE ATAQUES TENSIONAN LA CIBERSEGURIDAD LOCAL

Ante el sostenido aumento de ataques informáticos y en medio de una fuerte escasez de especialistas, los proveedores refuerzan sus servicios y ajustan estrategias de defensa. Aquí, actores de la industria lo analizan. POR MACARENA PACULL M.

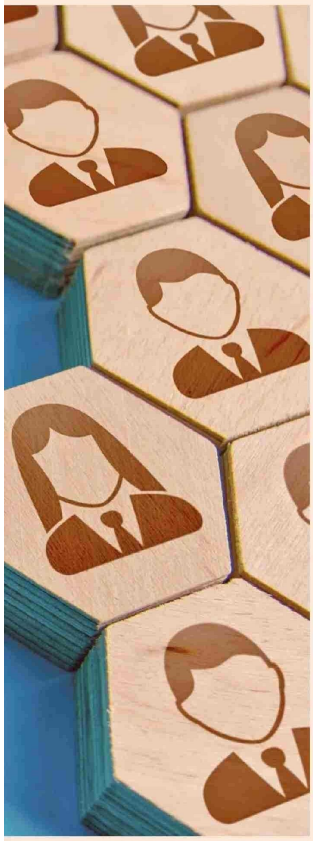
Los crecientes incidentes informáticos en Chile han posicionado a la ciberseguridad como una prioridad estratégica para organizaciones públicas y privadas. De acuerdo con el informe Kaspersky IT Security Economics, publicado a principios de agosto, en los últimos meses las grandes empresas chilenas experimentaron la mayor tasa de incidentes de seguridad de red, a pesar de contar con las medidas de protección más completas. El *ransomware* es la principal amenaza mundial y regional, según el Reporte Ciberseguridad 2025 de Entel Digital, y tiene a Chile como uno de sus blan-

LITORALPRESS

Fecha: 26-08-2025
Medio: Diario Financiero
Supl. : Diario Financiero
Tipo: Noticia general
Título: DÉFICIT DE TALENTO Y ALZA DE ATAQUES TENSIONAN LA CIBERSEGUYRIDAD LOCAL

Pág. : 29
Cm2: 340,7
VPE: $ 3.019.038

Tiraje: 16.150
Lectoría: 48.450
Favorabilidad: No Definida



cos preferidos: es el cuarto país más afectado con esta modalidad de ataque.

En este escenario, los proveedores locales han encontrado una oportunidad y han ganado terreno para desarrollar y ofrecer soluciones que van desde centros de operaciones de seguridad (SOC) y arquitecturas *zero trust*, hasta plataformas de detección de *phishing* y servicios avanzados de protección de datos.

A juicio del jefe CSIRT en ITQ Latam, Sebastián Ávila, la industria local de ciberseguridad está en auge, pero tiene desafíos, especialmente de capital humano. El experto explica que la digitalización y el avance de los ataques cibernéticos revelaron un problema no menor: falta talento para enfrentar esta situación. Apunta que, para este año, se estima una falta de más de 7 mil profesionales del rubro en Chile, lo que se refleja en salarios más exigentes y afecta a las pymes de manera directa.

Un hito positivo que resalta Ávila es la entrada en vigencia, a principios de año, de la Ley Marco de Ciberseguridad. "Establece una institucionalidad y reglas claras, impulsando a las empresas a dedicarse, a invertir y profesionalizarse en esta materia, más aún en la actualidad, ya que las organizaciones se enfrentan a desafíos importantes como la brecha y fuga de talento; la creciente sofisticación de los ataques, impulsados por tecnologías como la inteligencia artificial", sostiene.

El *ransomware* es la principal amenaza mundial y regional, según el Reporte Ciberseguridad 2025 de Entel Digital, y tiene a Chile como uno de sus blancos preferidos: es el cuarto país más afectado con esta modalidad de ataque.

La gerenta general para la Región Sur de América Latina de Kaspersky, Andrea Fernández, dice que el país es el más avanzado en ciberseguridad en Latinoamérica por su madurez, adopción de leyes y la creación de entidades para hacerse cargo del tema a nivel nacional. "Muchos países en la región no tienen ni uno, ni otro. En el caso de los ataques y vulnerabilidades, podemos decir que Chile no se destaca por la creación de ciberataques, sino que es blanco de amenazas extranjeras, principalmente troyanos desarrollados en Brasil, ataques de ransomware internacionales e *infostealers*", acota.

Soluciones

Los expertos coinciden en que no hay una estrategia estandarizada para que las empresas estén más protegidas. Las firmas que proveen estos servicios así lo han entendido, y por eso la oferta es variada. En este escenario, la adopción del enfoque *zero trust* toma fuerza. Desde Mainsoft explican que en los últimos cuatro años, muchas empresas empezaron a planificar cómo implementarlo. Una tendencia que se debe, sobre todo, al auge de tecnologías *cloud* y a las nuevas modalidades de trabajo remoto, dicen desde la firma.

Ávila destaca los sistemas de detección y respuesta ante incidentes, y explica que los EDR/XDR permiten automatización defensiva frente amenazas en tiempo real. Resalta el uso de plataformas de Gestión de Identidad y Acceso (IAM), con soluciones como la implementación de dos o más tipos de verificación de identidad, o la administración de accesos y permisos de los colaboradores de forma centralizada. Dice que otra solución clave está en los Centros de Operaciones de Seguridad (SOC), una unidad centralizada y externa responsable de supervisar y administrar la seguridad de una organización.

A juicio del gerente general de Widefense, Kenneth Daniels, los SOC locales tienen una ventaja que los internacionales no tienen: el idioma, la cercanía, el conocimiento del entorno normativo y del mercado, lo que les da una capacidad de respuesta más ágil y personalizada. Acota que los internacionales, en cambio, "atienden a miles de empresas y principalmente a grandes corporaciones".

"Los SOC locales somos más personalizados en la atención y nos enfocamos en mantener un acompañamiento cercano y permanente", plantea.