LITORALPRESS

Fecha: 30-05-2025
Medio: El Mercurio
Supl. : El Mercurio - Chile Tecnológico
Tipo: Noticia general
Título: **Monitoreo, detección y respuesta, claves de la ciberdefensa**

Pág. : 24
Cm2: 253,3

Tiraje: 126.654
Lectoría: 320.543
Favorabilidad: No Definida

CHILE ES UNO DE LOS PAÍSES MÁS ATACADOS DE LATINOAMÉRICA:

Monitoreo, detección y respuesta, claves de la ciberdefensa

El avance criminal y las nuevas leyes instan al sector público y privado a establecer soluciones tecnológicas avanzadas ante peligros cada vez más sofisticados.

FRANCIA ROMERO

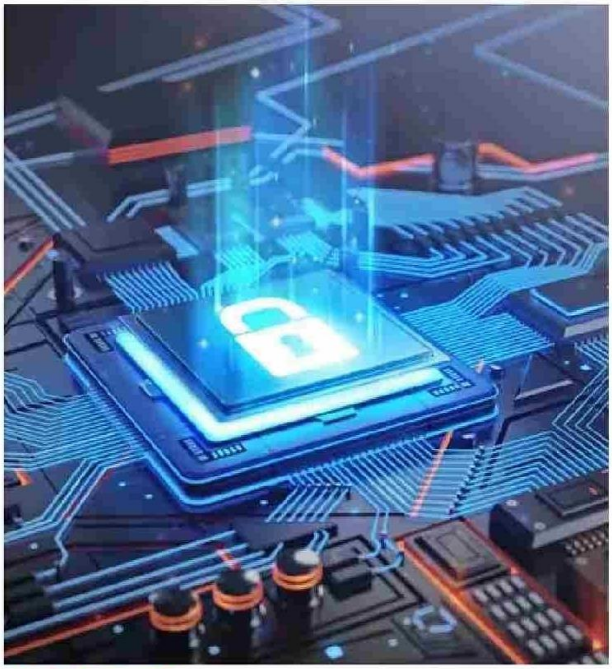
Durante 2024, Chile registró más de 27.600 millones de intentos de ciberataques, según el informe Global Threat Landscape, de FortiGuard Labs. Esto representó un crecimiento sostenido frente a años anteriores, consolidando al país como uno de los más atacados de la región. Solo en *malware*, se detectaron 8,3 millones de incidentes, con un promedio de 22.000 diarios.

En este contexto, la reciente entrada en vigor de la Ley Marco de Ciberseguridad impone nuevas exigencias, y obliga a instituciones públicas y privadas consideradas infraestructuras críticas a implementar medidas preventivas, reportar incidentes y garantizar una protección efectiva de sus sistemas. A ello se suma la Ley de Protección de Datos Personales, que regirá a partir del 1 de diciembre de 2026. Se trata de una legislación inédita en Latinoamérica, con multas que podrían llegar a 20.000 UTM.

El cumplimiento de ambas leyes exige un enfoque preventivo y sostenido, especialmente en un entorno donde las ciberamenazas se diversifican y sofistican, por lo que su entrada en vigor ha generado "un cambio importante en la percepción de las empresas sobre la ciberseguridad", afirma Alexander Espinoza, subgerente general de AdvanSolution.

El ejecutivo añade que "organizaciones de todos los tamaños deben comprender que la ciberseguridad no es un gasto, sino una inversión crítica para la continuidad operativa".

En respuesta a este escenario, han ido ganando terreno soluciones de monitoreo, detección y respuesta ante ciberincidentes. Una de ellas es Barracuda XDR (*Extended Detection and Response*), que realiza un monitoreo continuo a través de un SOC 24/7, así como detección proactiva y respuesta automatizada ante amenazas en distintos vectores: correo electrónico, *endpoints*, servidores, redes y aplicaciones en la nube. En paralelo, herramientas como SentinelOne entregan una plataforma de protección autónoma para *endpoints*, que incluye inteligencia artificial y capacidades de remediación automatizada.



LA CIBERSEGURIDAD no es un gasto, sino una inversión crítica para la continuidad operativa.

Alexander Espinoza comenta que han visto "un interés creciente desde sectores como educación, salud, *retail*, financiero y servicios públicos. Muchos se enfrentan a desafíos de infraestructura heredada o equipos de tecnologías de la información (TI) limitados, por lo que buscan soluciones que sean potentes, automatizadas y fáciles de operar".

Finalmente, afirma que uno de los principales problemas que observan es la escasez de profesionales especializados y la dificultad de mantener una operación continua de monitoreo y respuesta. "Otro factor crítico es la complejidad en la integración de distintas herramientas, especialmente cuando se trabaja con ambientes híbridos o soluciones fragmentadas", puntualiza.