

Tecnología

Ciberseguridad: estrategias para proteger la infraestructura crítica de Chile

Chile ha enfrentado un aumento significativo en los ciberataques durante 2024, registrando un promedio de 1.636 ciberataques por empresa cada semana en el segundo trimestre. Además, en lo que va de 2025, el 60% de las empresas ha experimentado filtraciones, pérdidas y daños de datos debido a brechas de seguridad.

En un mundo cada vez más digitalizado y conectado, la ciberseguridad se ha convertido en una de las principales prioridades para gobiernos y empresas de todo el mundo. Chile, reconocido como un líder regional en términos de legislación en ciberseguridad, ha demostrado un compromiso firme con la protección de su infraestructura crítica. La Ley de Ciberseguridad, vigente desde abril de 2024, ha sido un reconocido ejemplo para otros países de Latinoamérica, ayudando a fortalecer las defensas nacionales contra las crecientes amenazas del cibercrimen.

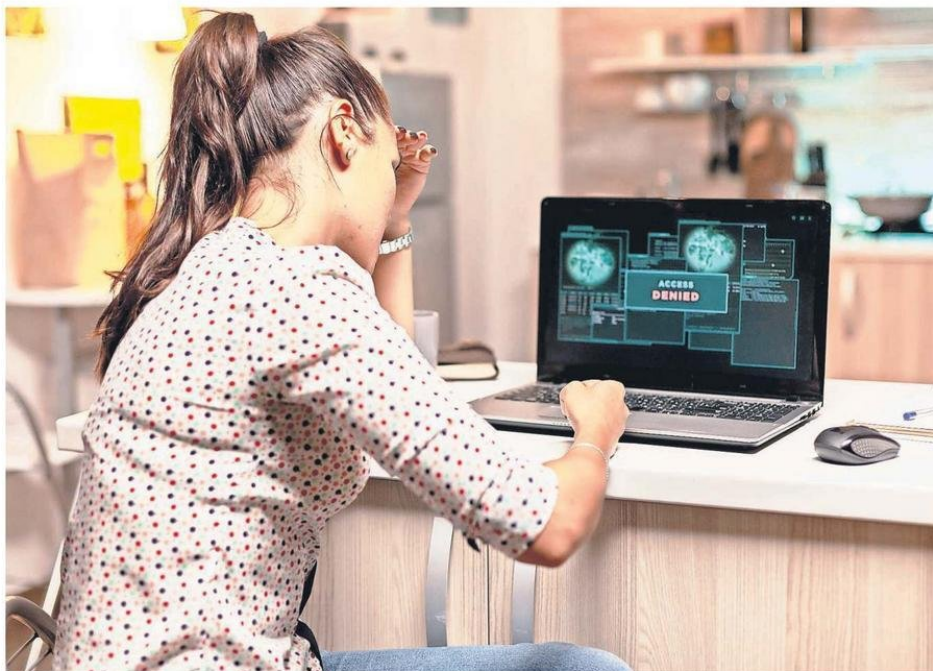
Según datos de Check Point Research, Chile experimentó un preocupante aumento en los ciberataques en 2024, con un promedio de 1.636 ciberataques por empresa cada semana durante el segundo trimestre, lo que representa un incremento del 30% en comparación con el mismo período del año anterior. Esta tendencia se ha mantenido en 2025, cuando un estudio de Kaspersky reveló que el 60% de las empresas chilenas han sufrido filtraciones de datos debido a brechas de seguridad.

En este contexto, expertos en ciberseguridad coinciden en la importancia de adoptar herramientas adecuadas para mitigar los riesgos cibernéticos. Cristina

Fritz, cofundadora de Digital Exp, una empresa especializada en tecnología empresarial y ciberseguridad, afirma: "Para protegerse contra las sofisticadas tácticas del cibercrimen, las organizaciones deben centrarse en habilitar herramientas impulsadas por Inteligencia Artificial en tiempo real. Esto permitirá detectar actividades sospechosas y mitigar ataques de manera rápida y eficiente".

Fritz subraya que el uso de tecnologías innovadoras, como el machine learning y la Inteligencia Artificial, puede mejorar significativamente la capacidad de identificar amenazas antes de que se materialicen. "Los errores humanos siguen siendo la principal causa de vulneraciones. Por eso, la conciencia sobre seguridad es fundamental", agrega la experta. Además, resalta la importancia de mantener los sistemas actualizados y de contar con aliados estratégicos en ciberseguridad para proteger la información de manera eficaz.

Ante estos desafíos, las organizaciones chilenas, tanto públicas como privadas, deben reforzar su preparación. Fritz recomienda medidas clave como el monitoreo continuo, la implementación de alertas tempranas y la creación de un eco-



sistema tecnológico simplificado y robusto, lo que no solo ayudará a prevenir ataques, si-

no que también optimizará el rendimiento de las tecnologías implementadas en el futuro.

La Ley de Ciberseguridad, vigente desde abril de 2024, ha sido un reconocido ejemplo para otros países de Latinoamérica, ayudando a fortalecer las defensas nacionales contra las crecientes amenazas del cibercrimen. La normativa transformaron a Chile en un líder en este tema.

Por supuesto acompañado de un proceso de concientización continuo, capacitar no es suficiente. Normalmente no percibimos la dimensión de los daños potenciales hasta que estamos expuestos a un ataque.

La ciberseguridad en el sector público es particularmente crucial, dada la creciente digitalización de servicios públicos, legales y sociales. Según Fritz, la capacidad de respuesta ante un ciberataque puede reducir en un 20% los costos tecnológicos asociados con la gestión de estos incidentes. "Contar con un sistema de respaldo ro-

busto y eficiente es esencial para garantizar la continuidad de los servicios públicos tras un ataque, asegurando que las operaciones no se vean interrumpidas", concluye.

Con el aumento de los ciberataques en todo el mundo, se hace indispensable que Chile refuerce aún más sus estrategias de ciberseguridad, asegurando la protección de su infraestructura crítica, datos sensibles y, en última instancia, la confianza de sus ciudadanos.

La verdad es que hoy, y cada vez más, el mayor valor de las organizaciones, son sus datos.