Chile en Riesgo Digital: Errores empresariales causan pérdidas millonarias

Ransomware, nuevas leyes y errores empresariales: cómo proteger a su organización en 2025

Alexis Campos Cut Security

CHILE, September 23, 2025 /EINPresswire.com/ -- Alexis Campos, especialista en ciberseguridad de Cut Security by Grupotech, advierte que, aunque el número de ataques disminuyó en 2023, estos son ahora más dirigidos y sofisticados. El ransomware es el principal riesgo, y un solo incidente puede causar pérdidas promedio de más de 300,000 dólares. Estos ataques afectan por igual a bancos, hospitales, tiendas retail y pymes.

En Chile, los ciberataques han dejado de ser una amenaza lejana para convertirse en un riesgo estratégico para las empresas. De acuerdo con reportes, el país enfrentó casi 29,000 ataques de ransomware en el último año, con pérdidas millonarias y una creciente presión por cumplir la Ley Marco de Ciberseguridad (21.663) y la Ley de Protección de Datos (21.719). Un sistema comprometido por un ataque de ransomware puede generar pérdidas promedio de más de 300,000 dólares. Estos ataques afectan por igual a bancos, hospitales, el sector retail y pymes.

> “Hoy los ataques son menos masivos, pero mucho más inteligentes”
>
> *Alexis Campos*

Alexis Campos, especialista de Cut Security by Grupotech, señala que, aunque el número de ataques disminuyó en 2023, estos son ahora mucho más dirigidos y sofisticados. Su experiencia como hacker ético le permite entender la mentalidad de los atacantes y anticipar sus movimientos.

¿Por qué las empresas chilenas siguen siendo vulnerables?
Según Campos, la principal causa de que las compañías sigan cayendo en las trampas del cibercrimen son errores comunes y prevenibles. Los fallos más frecuentes son:

1) No actualizar los sistemas ni aplicar parches de seguridad.
2) No usar autenticación multifactor (MFA) en accesos críticos.
3) Capacitar poco al personal, ya que el 80% de los ataques comienza con un error humano. Basta un solo clic en un correo de phishing para abrir las puertas a un ataque.
4) No tener planes de respuesta ante incidentes o ciberseguros. Más del 60% de las empresas en Chile no cuenta con un plan de respuesta a incidentes actualizado, lo que las deja a la deriva ante una crisis.

La inteligencia artificial y las nuevas leyes cambian el juego.

La Ley 21.663 de Ciberseguridad obliga a las empresas a implementar un Sistema de Gestión de Seguridad de la Información (SGSI), designar un delegado de ciberseguridad y reportar incidentes graves al CSIRT en un plazo máximo de tres horas. El incumplimiento puede acarrear multas de hasta 10,000 UTM. A esto se suma la Ley 21.719 de Protección de Datos, que entrará en plena vigencia en 2026 y impondrá sanciones millonarias por el mal uso de la información personal. En este contexto, la ciberseguridad y el cumplimiento normativo han dejado de ser opcionales, para convertirse en parte del ADN empresarial.

Además, la inteligencia artificial (IA) es una espada de doble filo. Si bien las empresas la usan para detectar ataques, los ciberdelincuentes la aprovechan para crear phishing hiperrealista y buscar vulnerabilidades. Hoy, cerca de la mitad de los ataques de ransomware en Chile usan IA para personalizar sus campañas.

Cinco medidas para proteger su empresa ahora.

Campos recomienda a los dueños y gerentes tomar estas acciones inmediatas para reducir riesgos:

1) Capacitar al personal con frecuencia.
2) Actualizar y aplicar parches a los sistemas de manera frecuente.
3) Implementar MFA en todos los accesos críticos.
4) Respaldar los datos fuera de línea de manera periódica.
5) Monitorear la red 24/7 con herramientas o a través de un SOC (Security Operations Center).

Según el experto, la inversión en ciberseguridad en Chile crecerá al menos un 20% anual. Sin embargo, la clave no es esperar a ser víctima, sino invertir en prevención hoy. Como concluye Campos, el desafío ya no es preguntarse si ocurrirá un ataque, sino cuándo.

La inversión en ciberseguridad crecerá al menos un 20% anual. Habrá más regulaciones, más colaboración entre sector público y privado, y más uso de IA en defensa. Pero lo esencial no cambiará: la diferencia estará entre quienes inviertan en prevención y quienes esperen a ser víctimas.

La ciberseguridad en Chile ya no es un tema técnico: es un asunto de continuidad operativa, reputación y cumplimiento legal. Como concluye Alexis Campos, el desafío no es preguntarse si ocurrirá un ataque, sino cuándo. Prepararse hoy, con expertos y una estrategia clara, puede marcar la diferencia entre sobrevivir a una crisis o quedar fuera del mercado.

Alexis Campos
Experto Ciberseguridad Cut Security
+56 9 9982 2311
contacto@cutsecurity.cl
Visit us on social media:
LinkedIn
Instagram
Other
