



esta realidad quedó en evidencia. La mayoría de las organizaciones sigue enfocada en prevenir, pero no en resistir ni recuperarse con rapidez. Esa es la diferencia entre ciberseguridad y resiliencia. La continuidad operativa, la redundancia en procesos y talento humano capaz de responder con la urgencia que exige una crisis, son vitales en estos casos.

Centralizar funciones críticas en un solo organismo es una debilidad estructural. Urge descentralizar, invertir en especialistas y entender que la resiliencia digital no es un tecnicismo, sino un deber ético y social. De ella depende la continuidad de servicios esenciales y, en casos como el ISP, la salud de las personas.

PATRICIO CAMPOS
CEO DE RESILITY

Ciberataque al ISP

Señor Director:

El reciente ciberataque al Instituto de Salud Pública evidenció una vulnerabilidad crítica y que tiene relación con la resiliencia digital. La paralización de diagnósticos sensibles como VIH y hepatitis mostró que un incidente informático no es un problema técnico y una emergencia pública.

El Foro Económico Mundial advierte que casi la mitad de las instituciones gubernamentales carece de preparación ante un ataque masivo y, en Chile,