LITORALPRESS

Fecha: 08-01-2026
Medio: Diario Financiero
Supl. : Diario Financiero
Tipo: Opinión - Cartas
Título: **Cartas: Ciberresiliencia en salud**

Pág. : 12
Cm2: 71,2
VPE: $ 631.212

Tiraje: 16.150
Lectoría: 48.450
Favorabilidad: No Definida

Ciberresiliencia en salud

Señor Director:

El incidente en Clínica Dávila se suma al del ISP ocurrido este año, demostrando que este sector es un blanco constante de ataques para materializar un riesgo sistémico. La Ley Marco 21.663 busca fortalecer las capacidades y obligar a los prestadores de salud y su cadena de abastecimiento a mejorar su postura de riesgo.

Estas OIV -operador de importancia vital- deben ver la ciberseguridad como un activo que opera en tiempo real, transversal a la organización, y no como un checklist de preguntas de cumplimiento. En vez de de un gasto opcional, deben abordarla como una inversión y un pilar de la resiliencia operativa para la continuidad del servicio.

La filtración de datos sensibles es un vector de extorsión, donde la pérdida de la privacidad de los pacientes tiene consecuencias mucho más costosas que cualquier multa.

La ciberresiliencia exige una gobernanza que trascienda el cumplimiento reactivo y proteja efectivamente la privacidad, bajo la Ley Protección de Datos Personales. Además, la Ley 21.595 responsabiliza la ausencia de un modelo de prevención de delitos robusto que integre controles, ya que no es solo una negligencia técnica, sino un riesgo penal para la alta dirección. La ciberseguridad no se adquiere comprando un software o una auditoría, se construye con una cultura de gestión de riesgos desde el directorio hacia la organización.

RICARDO SEGUEL
PROFESOR FACULTAD DE INGENIERÍA Y CIENCIAS UAI, DIRECTOR DE DTC CYBER