



TELECOMUNICACIONES

ENCI 2025: 48% DE LAS GERENCIAS DEL PAÍS PARTICIPAN DE LA DEFINICIÓN DE LAS ESTRATEGIAS DE CIBERSEGURIDAD



En un mundo interconectado, contar con un área de ciberseguridad definida y usuarios capacitados en este ámbito, se ha vuelto cada vez más importante para las organizaciones chilenas. Así lo constatan los resultados preliminares del Estudio Nacional de Ciberseguridad (ENCI) 2025, desarrollado por el Centro de Estudios de Tecnologías de la Información de la Pontificia Universidad Católica de Chile (CETIUC), que revela que, de las 50 organizaciones que participaron en esta edición, en un 48% de los casos la gerencia general participa de la definición de la estrategia de ciberseguridad.

“Eso es muy importante porque quiere decir que el tema de la ciberseguridad, y principalmente la definición de una estrategia

Tener una estrategia que cumpla con los requisitos del negocio es cada vez más relevante para las organizaciones chilenas, según los primeros resultados del Estudio Nacional de Ciberseguridad 2025, elaborado por CETIUC.

POR ANDREA CAMPILAY

que cumpla con los requisitos del negocio, está siendo cada vez más importante”, afirma el director de estudios y tecnología en CETIUC, Matías Fuentes.

Una de las nuevas dimensiones de esta versión del estudio es el impacto que han tenido los ciberataques en

las organizaciones, donde un 72% señaló que el principal impacto ha sido la interrupción de operaciones, y en segundo lugar la pérdida de confianza en la tecnología.

En 2024, los resultados revelaron que un 61% de las organizaciones contaba con un área de ciberseguri-

dad con responsabilidad definida y recursos propios. Este indicador muestra una leve mejora en esta edición, llegando a un 62,3%, señala Fuentes, y añade que hasta el año pasado, el presupuesto era uno de los principales desafíos para una adecuada gestión de la ciberseguridad, un reto que se mantiene, ya que “en Chile, del total del presupuesto de TI, un 8% va a ciberseguridad”, según el estudio 2024, cifra que a nivel global está entre un 12% y 15%, lo que muestra una brecha relevante a nivel presupuestario.

Otro tema que preocupa es la falta de habilidades técnicas de las áreas de ciberseguridad, el segundo desafío más importante de estos departamentos para el 38% de las organizaciones. “Esto está cambiando con la participación de las gerencias generales en la definición de las estrategias para cerrar estas brechas”, dice Fuentes, y añade que también “hay un brecha importante en la educación y cultura de los usuarios de TI”, dimensión que un 76% de los encuestados señaló como un punto a mejorar.

Los resultados finales de esta medición serán liberados a fin de año, adelanta Fuentes.