

DIRECTORES Y CIBERSEGURIDAD: UNA RELACIÓN AMBIVALENTE

Análisis

FADUA GAJARDO
Directora ejecutiva del Instituto de Directores de Chile



Se acerca el mes de la ciberseguridad, pero hay una paradoja en este tema que me llama la atención: en múltiples estudios —como el de “Tendencias en Directorios 2024” realizado por el Instituto de Directores— la ciberseguridad aparece como una de las principales preocupaciones de las empresas; no obstante, cuando consultamos si los directorios en los que participan cuentan con integrantes calificados en esta materia, el 76% dice que no.

Y es que la posibilidad de pensar que alguien, provisto de códigos y conocimientos que el común de los mortales no manejamos, entre a tus documentos más importantes, los modifique o los robe, es simplemente aterradora. Pero da

la impresión de que, por el mismo carácter cinematográfico que tiene, no lo tomamos tan en serio como deberíamos. Lo “ciber” sigue siendo algo bastante ajeno, e incluso aparece como uno de esos temas que mejor dejar a las generaciones más jóvenes, que por su propia configuración entenderán mejor. De hecho, en nuestro estudio “Radiografía de la Ciberseguridad en Directorios en Chile”, realizado en noviembre pasado, vemos que la mayoría de las empresas no presentan informes de ciberseguridad al directorio o lo hacen cuando están frente a un caso crítico, o que los directores no suelen incluir este factor cuando están frente a decisiones comerciales relevantes tales como

fusiones o adquisiciones. ¿Saben cuán frecuentes son los intentos de ciberataque? El boletín semanal de la Comisión Nacional de Seguridad reportó más de 200 alertas de vulnerabilidades en la última semana. Como vemos, no es asunto ni de las películas ni de otra generación. Es nuestro deber como directores anticiparnos a los riesgos que pueden amenazar la continuidad y la reputación de nuestras organizaciones.

El directorio debe asegurarse de que la organización cuente con políticas robustas de ciberseguridad, que existan controles internos adecuados, y que se lleven a cabo evaluaciones periódicas de vulnerabilidades. Ade-

más, deben recibir informes regulares sobre el estado de la ciberseguridad y los incidentes que puedan surgir, incluso si no son críticos. La falta de conocimiento técnico no exime a los directores de su responsabilidad; por el contrario, deben buscar capacitación y asesoramiento especializado para poder tomar decisiones informadas.

En este mes de la ciberseguridad, hacemos un llamado a los directores a priorizar e integrar la ciberseguridad en la estrategia de sus empresas. Para así poder ser resilientes, a tener la capacidad de anticiparse, prepararse, responder y adaptarse a un entorno cambiante en lugar de intentar “volver a la normalidad”.