El CISO frente al directorio: traducir el riesgo digital en decisiones de negocio



Por José Lagos, Docente UEjecutivos Facultad de Economía y Negocios Universidad de Chile.

Durante años, la ciberseguridad tuvo una ubicación relativamente cómoda dentro de las empresas: el área de tecnología. Los directorios, mientras tanto, recibían algún reporte periódico y aprobaban inversiones en nuevas herramientas de protección. Ese modelo está quedando obsoleto. Si bien hoy todos los procesos relevantes de una organización dependen de tecnología, datos, proveedores digitales y servicios en la nube, cuando alguno de ellos falla, el impacto deja rápidamente de ser tecnológico. Una interrupción puede detener operaciones, afectar ingresos, exponer información de clientes, generar incumplimientos regulatorios y deteriorar la reputación construida durante años.

El CISO White Paper 2026 refleja claramente esta transformación. El Chief Information Security Officer (CISO) ya no puede limitarse a administrar controles técnicos. Su desafío es gobernar el riesgo digital, conectarlo con los objetivos de la compañía y traducir amenazas técnicas en impactos que la alta dirección pueda comprender y decidir: continuidad, pérdidas económicas, regulación, reputación y confianza.

Pensemos en un ejemplo. Informar al directorio que existen 800 vulnerabilidades puede ser técnicamente correcto, pero aporta poco para tomar una decisión. Distinto es explicar que tres de ellas afectan un proceso crítico, que una podría interrumpir la operación por varios días y que corregirla exige postergar un proyecto o realizar una inversión adicional.

En ese momento, se deja de hablar de vulnerabilidades, para transitar a riesgo de negocio. El CISO administra y comunica el riesgo, pero no es quien determina cuánto riesgo está dispuesta a asumir la organización. Cuando una exposición relevante no puede eliminarse, alguien debe decidir si se mitiga, transfiere, evita o acepta. Esa decisión debe quedar en el nivel que tenga atribuciones y responsabilidad para tomarla.

Esta discusión adquiere particular relevancia en Chile con la implementación de la Ley 21.663, Marco de Ciberseguridad, y el despliegue institucional de la Agencia Nacional de Ciberseguridad (ANCI). Durante 2026, la ANCI completó su primer proceso de calificación de Operadores de Importancia Vital (OIV), incorporando organizaciones sujetas a obligaciones reforzadas de ciberseguridad.

Uno de los elementos más interesantes del nuevo modelo es precisamente el gobierno. Los OIV deben contar con un delegado de ciberseguridad que tenga un canal de reporte directo hacia la máxima autoridad de la institución y suficiente independencia para comunicar riesgos, incidentes y brechas de cumplimiento. La regulación establece, además, que no puede ser la misma persona responsable del área de TI, salvo determinadas condiciones organizacionales, que garanticen su independencia. El mensaje detrás de esta arquitectura es difícil de ignorar. La seguridad no puede quedar encerrada dentro del área que opera la tecnología que debe supervisar.

El sector financiero ya conoce esta lógica. La Comisión para el Mercado Financiero mantiene requerimientos específicos para la gestión de seguridad de la información y ciberseguridad, incorporando responsabilidades de gobierno, gestión de riesgos, continuidad y participación de los órganos superiores de las entidades.

Llevar la ciberseguridad al directorio tampoco significa convertir a sus integrantes en especialistas, ni llenar las reuniones de cifras provenientes del Centro de Operaciones de Seguridad (SOC). Para un director, cinco preguntas son más valiosas que cincuenta indicadores: ¿Cuáles son nuestros principales escenarios de riesgo cibernético?, ¿qué procesos podrían interrumpirse?, ¿qué proveedores podrían afectarnos significativamente?, ¿qué riesgos estamos aceptando y quién autorizó esa decisión?, ¿hemos probado realmente nuestra capacidad para responder y recuperarnos?

El CISO White Paper 2026 plantea justamente que el CISO debe transformarse en un interlocutor capaz de traducir complejidad tecnológica en información útil para las decisiones corporativas. La pregunta correcta para 2026 es ¿qué riesgo cibernético estamos aceptando, y estamos preparados para enfrentar las consecuencias si se materializa? El CISO ya llegó al directorio. Ahora falta que la conversación cambie.