

Nuevas estrategias para enfrentar los principales riesgos empresariales modernos

Autor: UNEGOCIOS FEN - UChile , Expertos advierten que la forma de reaccionar ante las amenazas cambió, y que adaptarse a esta realidad es clave para la continuidad de un negocio. La gestión de la seguridad ya no puede concentrarse únicamente en cómo responder frente a una emergencia. El foco comienza a desplazarse hacia la preparación previa: qué vulnerabilidades ha identificado la organización, qué recursos ha destinado y qué tan preparada está para mantener sus operaciones frente a una interrupción. Para Cristián Clavería, director académico del Diplomado en Seguridad, Resiliencia y Continuidad del Negocio de Unegocios FEN de la Universidad de Chile, el escenario actual exige abandonar la idea de que la seguridad constituye un ámbito aislado del resto de la gestión empresarial. “El futuro llegó y no trae instrucciones”, plantea el especialista. Una frase con la que busca graficar un entorno en que las organizaciones enfrentan amenazas cada vez más diversas, interconectadas y difíciles de anticipar. Conflictos geopolíticos, ciberdelincuencia, crimen organizado, eventos climáticos extremos, exposición de datos y nuevas amenazas tecnológicas forman parte de un escenario en que incluso acontecimientos ocurridos a miles de kilómetros pueden terminar repercutiendo en las operaciones de una empresa en Chile. “Debemos administrar localmente la seguridad con una mirada global”, sostiene Clavería. El desafío, explica, está en reconocer qué amenazas podrían impactar a la organización, identificar sus vulnerabilidades y utilizar fuentes de información confiables que permitan tomar decisiones antes de que un riesgo se transforme en una crisis. De reaccionar a anticiparse. Durante años, gran parte de la gestión de seguridad estuvo concentrada en cómo responder frente a una emergencia. Hoy el foco comienza a desplazarse hacia una pregunta anterior: ¿qué hizo la organización para prepararse antes de que ocurriera? Presupuesto, protocolos, identificación de vulnerabilidades, protección de las operaciones críticas y capacidad de respuesta son algunas de las variables que permiten dimensionar qué tan preparada está una empresa. La experiencia del terremoto y tsunami de 2010, por ejemplo, dejó en evidencia tanto la importancia de contar con protocolos como las consecuencias que pueden producir las fallas de comunicación durante una emergencia. Pero los riesgos actuales van mucho más allá de las catástrofes naturales. El crimen organizado, los ataques informáticos, la violencia, los delitos que afectan a las cadenas logísticas o las amenazas sobre ejecutivos son fenómenos que pueden repercutir directamente en las organizaciones y que obligan a revisar continuamente los sistemas de prevención y respuesta. En este contexto, Clavería advierte también sobre un riesgo menos evidente: asumir que tercerizar una operación significa también transferir sus riesgos. El especialista cuestiona que algunas organizaciones descansen excesivamente en proveedores externos o en la existencia de seguros, sin considerar que una vulnerabilidad en la cadena puede terminar afectando su propia continuidad operacional y cumplimiento. Compartir información también es seguridad. Existe otra debilidad que, a juicio del especialista, sigue presente en muchas organizaciones: trabajar de manera aislada. “Existen muchas organizaciones que se aíslan, que se encapsulan, que no comparten datos y eso tiene un efecto que es la pérdida de oportunidades”, afirma Clavería. El problema adquiere especial relevancia frente a delitos que atraviesan distintas industrias. Un mismo grupo puede afectar, por ejemplo, a empresas eléctricas, autopistas, operadores logísticos u otras compañías, por lo que compartir información puede contribuir a identificar patrones y fortalecer las acciones preventivas y judiciales. Esto también ha impulsado una relación cada vez más estrecha entre el sector privado y organismos públicos vinculados a la seguridad y la persecución del delito. La lógica es sencilla: frente a riesgos que funcionan como redes, las organizaciones difícilmente pueden responder de manera completamente aislada. La seguridad entra a la estrategia del negocio. Esta transformación también está cambiando el perfil de quienes lideran las áreas de seguridad. Ya no basta con conocer procedimientos operativos o reaccionar adecuadamente ante una emergencia. Las organizaciones requieren profesionales capaces de comprender el negocio, identificar riesgos interdependientes y conectar sus decisiones con la continuidad operacional y los objetivos estratégicos de la compañía. Humberto Santibáñez, especialista en seguridad estratégica corporativa y gestión de riesgos, Certified Protection Professional (CPP) y docente del Diplomado en Seguridad, Resiliencia y Continuidad del Negocio, sostiene que ese cambio ya puede observarse en las empresas. “Hoy día los negocios sí están mirando a la seguridad, sí le están dando la importancia que merece para poder mantener la continuidad operacional y garantizar la obtención de sus objetivos estratégicos”, señala. A ello se suma que las amenazas actuales se desarrollan simultáneamente en entornos físicos y digitales. Para Santibáñez, esto obliga a quienes ocupan posiciones de liderazgo a desarrollar una mirada integral que conecte seguridad, tecnología, personas, operaciones y estrategia. El objetivo ya no consiste únicamente en proteger instalaciones o responder frente a incidentes, sino en comprender de qué manera un riesgo puede afectar el funcionamiento completo de una organización. Profesionalizar la gestión del

riesgoEste nuevo escenario también está aumentando la importancia de contar con estándares comunes y profesionales especializados. ASIS International, organización global que reúne a profesionales de la seguridad, cuenta con distintas certificaciones orientadas a áreas como investigaciones, seguridad física y gestión integral de la seguridad. Entre ellas se encuentra la CPP (Certified Protection Professional), enfocada en profesionales con experiencia en posiciones de gestión y liderazgo. Según Santibáñez, este tipo de estándares permite que especialistas de diferentes países e industrias compartan metodologías y un lenguaje común para abordar los riesgos. Esto adquiere particular relevancia en compañías multinacionales, donde las decisiones locales deben integrarse a estrategias globales y donde los responsables de seguridad necesitan comprender no solo las amenazas, sino también el negocio que buscan proteger. La profesionalización, en ese sentido, responde a una transformación más profunda: la seguridad comienza a dejar de ser vista exclusivamente como un costo o una función de soporte para convertirse en una capacidad estratégica de la organización. Una compañía preparada no es necesariamente aquella capaz de anticipar cuál será su próxima crisis. En un escenario marcado por la incertidumbre, el desafío está en construir organizaciones capaces de identificar señales, reducir vulnerabilidades, responder oportunamente y mantener sus operaciones incluso frente a aquello que no habían previsto. Porque, finalmente, la pregunta relevante ya no es solo si una empresa enfrentará alguna vez una situación crítica, sino qué tan preparada estará para continuar operando cuando esa situación ocurra. Estas perspectivas fueron abordadas durante la masterclass “¿Está tu organización preparada para la próxima crisis? Cómo una Certificación de ASIS International te ayuda a fortalecer la Seguridad, la Resiliencia y la Continuidad del Negocio”, organizada en el marco del Diplomado en Seguridad, Resiliencia y Continuidad del Negocio de Unegocios FEN de la Universidad de Chile. La conversación completa está disponible en el canal de YouTube de Unegocios FEN: https://www.youtube.com/watch?v=mtnTwqC_5p4