Ciberseguridad: La evolucion necesaria de los profesionales de control preventivo

Viernes, 14 de Julio de 2017 - Id nota:635913

Medio : Gerencia
Sección : Ciberseguridad
Valor publicitario estimado : $0.-
Página : 34-35
Tamaño : 36 x 25

Ver en formato web

Ciberseguridad: La evolución necesaria de los profesionales de control corporativo

El escenario de la seguridad ha cambiado, sin lugar a dudas. Las compañías deben lograr identificar y cuantificar las distintas amenazas que rodean a los negocios, especialmente aquellas que provienen de la "ciber realidad". En este sentido, formar profesionales con una mirada global será fundamental.

Por Miguel Ángel Díaz, Director Centro de Auditoría, Riesgo y Cumplimiento, UCh. madiaz@fen.uchile.cl

La protección de los activos de las empresas ha evolucionado de forma dramática en los últimos 15 años. Hemos pasado de un escenario en que estas consideraban que la infraestructura e inventarios eran lo más importante, a un período en el que el conocimiento y la información se han transformado en aspectos tan valiosos, que de no ser protegidos de manera adecuada, una compañía puede quedar fuera de toda posibilidad de competir.

Esta evolución, como es tradicional, ha sido más rápida que la adaptación de las medidas de seguridad que se implementan en las empresas. No es poco frecuente encontrar situaciones donde las organizaciones cambian sus procesos o mejoran tecnologías, realizando grandes esfuerzos por lograr la efectividad de los proyectos e invirtiendo grandes recursos para alcanzar sus objetivos propuestos. Sin embargo, en muchas ocasiones, el esfuerzo y recursos empleados para asegurar que los riesgos se mantengan bajo los niveles tolerables no es suficiente.

Un cambio de enfoque

Si a lo mencionado se agrega el contexto global cambiante, en el que diariamente se presentan nuevas amenazas que pueden afectar la viabilidad de los negocios, la integridad de los activos e incluso la seguridad de las personas, da como resultado que las organizaciones se ven enfrentadas a un escenario en el que es muy complejo gestionar las compañías por los medios que tradicionalmente eran considerados adecuados para implementar soluciones. Por lo tanto, es necesario cambiar el enfoque de quienes están llamados a asegurar los objetivos del negocio, la sustentabilidad en el largo plazo de este y la salvaguarda de sus activos.

El foco debe evolucionar para que las compañías logren identificar y cuantificar las distintas amenazas que rodean a nuestros negocios, especialmente aquellas que provienen de la "ciber realidad", ya que es allí donde existen potenciales amenazas sin que las podamos ver de forma sencilla.

Considerar estos aspectos es fundamental para aquellos profesionales que desempeñan labores en el ámbito de las tecnologías, así como para los distintos profesionales encargados de entregar seguridad y confianza a los stakeholders de las empresas.

A ellos se suma el rol clave que juegan en este aspecto las áreas de auditoría -interna y externa-, y contraloría dentro de las compañías. Estas unidades, sin duda, deben comenzar a visualizar las "ciberamenazas", considerando en sus enfoques metodológicos las medidas de ciberseguridad necesarias para el cumplimiento del negocio y la sustentabilidad de largo plazo de la empresa.

Por lo tanto, las prácticas utilizadas por las entidades de control de las compañías, deben considerar en sus procesos, técnicas de alta tecnología, para asegurar la cobertura de riesgos. Entre ellas, podemos encontrar el uso de técnicas de monitoreo continuo, la permanente actualización de conocimientos y, especialmente, trabajar de manera colaborativa entre profesionales de distintas empresas e industrias. Todo esto debe complementarse con el uso de herramientas tecnológicas disponibles en la actualidad. Un ejemplo de ello es el análisis predictivo de riesgos. En este, se analiza en línea el comportamiento de las personas (Big Data), considerando la experiencia de miles de casos en los que se pudo determinar que un patrón de conducta llevaba con una muy alta probabilidad a una irregularidad o error significativo.

En muchas ocasiones, el esfuerzo y recursos empleados para asegurar que los riesgos se mantengan bajo los niveles tolerables no es suficiente.

Una mirada global

En conclusión, los cambios que estamos viviendo no solo constituyen un problema, sino que un desafío más que interesante, que nos obliga a evolucionar y analizar cómo realizamos las cosas actualmente y cómo lo haremos en el futuro. Por ello, debemos presionar a las entidades educacionales a formar profesionales con una mirada global, basada en principios fundamentales y no en técnicas específicas, que de seguro quedarán obsoletas en el corto plazo. Actualmente, los profesionales vinculados al área de la ciberseguridad deben desarrollar nuevas habilidades y, al mismo tiempo, enfrentar materializaciones de riesgos diariamente, estudiar nuevas amenazas y lograr incorporar nuevas tecnologías para proteger a las organizaciones. Su desafío es enorme. G

Sobre el autor

Miguel Ángel Díaz es miembro del Departamento de Control de Gestión y Sistemas de Información, de la Facultad de Economía y Negocios de la Universidad de Chile.