A

mayor uso de los computadores, mayor exposición a los denominados ataques cibernéticos. A partir del [Audit Executive Center's website](https://aec.theiia.org/Pages/default.aspx), el IIA publicó el artículo [CAE Action Steps in Response to Recent Cyberattacks](https://na.theiia.org/news/Pages/CAE-Action-Steps-in-Response-to-Recent-Cyberattacks.aspx), escrito por Jim Pelletier and Doug Anderson.

Debido a la realidad de nuestras empresas, tenemos que hacer constantes esfuerzos para adaptar las reflexiones que se hacen desde otras percepciones, a nuestras organizaciones. Pocas empresas tienen auditores internos en Colombia. Sin embargo, todas deberían tener control interno. La gran paradoja es que, sin tener control interno, varias tienen revisor fiscal.

Según el artículo, ante los repetidos ataques, se deberían tener en cuenta estas afirmaciones: (1) Cyberthreats are constantly changing and never-ending, (2) The primary focus of cyber risk must be its business impact, (3) Risk assessment is hard, especially with the type of risks in which cyber falls, (4) Cyber risks involve more than protecting the "crown jewels.", (5) Cyber risk is not an "IT thing.", (6) Never forget the "human element.".

La gran mayoría de nuestros usuarios de equipos electrónicos, no entienden cómo funcionan, no comprenden cómo se ataca el funcionamiento de los equipos, de los programas o se afectan datos. Es precisamente esta ignorancia de la que se sirven muchos atacantes para penetrar sistemas, vulnerables por simples mensajes de datos que son abiertos desprevenidamente, descargando instrucciones destructivas que rápidamente usan las redes internas para dispersarse por las organizaciones.

La pobreza de muchos los hace especialmente afectos a la información y los programas gratuitos. Hay cosas muy serias y bien intencionadas, pero también las hay que son verdaderos *caballos de Troya*. Muchos confían su seguridad a herramientas de contención gratuitas. Aquí la regla se confirma: los hay buenos y los hay débiles. Solo los que tienen detrás batallones de ingenieros estudiando y elaborando herramientas de inmediata difusión, pueden brindar niveles perceptibles de seguridad.

Los contadores públicos, en sus diversas prácticas (véase Áreas de trabajo del Experto Contable Acreditado, Amat Salas, Oriol, Revista Contable, Nº 47, Sección Auditoría, Septiembre 2016, Editorial Wolters Kluwer España), trabajan con información, la cual está crecientemente conservada en medios electrónicos. No hay otro camino que fortalecer sus competencias en estas cuestiones, pues si la información no es consultable, o no es confiable, de poco servirán sus demás competencias.

Es muy preocupante que frecuentemente se tengan noticias de bandas dedicadas a alterar datos para que ciertas personas obtengan determinados beneficios a los que no tienen derecho. Estos ataques vienen de adentro, aprovechando el conocimiento de las empresas. Los departamentos de contabilidad requieren especiales controles.

*Hernando Bermúdez Gómez*