CIENCIA CONTABLE: VISIÓN Y PERSPECTIVA

Libro homenaje por los 75 años de la Facultad de Ciencias Contables de la PUCP

Capítulo 34

Óscar Alfredo Díaz Becerra
José Carlos Dextre Flores
Editores

BIBLIOTECA NACIONAL DEL PERÚ
Centro Bibliográfico Nacional

657
C4

Ciencia contable: visión y perspectiva / Óscar Alfredo Díaz Becerra, José Carlos Dextre Flores, editores.-- 1a ed.-- Lima: Pontificia Universidad Católica del Perú, Fondo Editorial, 2017 (Lima: Tarea Asociación Gráfica Educativa).
405 p.: il., diagrs.; 24 cm.

«Libro homenaje por los 85 años de la Facultad de Ciencias Contables de la PUCP».
Incluye bibliografías.

D.L. 2017-15495
ISBN 978-612-317-308-1

1. Contabilidad - Ensayos, conferencias, etc. 2. Contabilidad - Normas 3. Contadores - Ética profesional 4. Auditoría - Normas 5. Finanzas públicas - Contabilidad 6. Contabilidad tributaria I. Díaz Becerra, Óscar Alfredo, 1962-, editor II. Dextre Flores, José Carlos, 1944-, editor III. Pontificia Universidad Católica del Perú

BNP: 2017-2877

Ciencia contable: visión y perspectiva
Libro homenaje por los 85 años de la Facultad de Ciencias Contables de la PUCP
Óscar Alfredo Díaz Becerra y José Carlos Dextre Flores, editores

Av. Universitaria 1801, Lima 32, Perú
feditor@pucp.edu.pe
www.fondoeditorial.pucp.edu.pe

Diseño, diagramación, corrección de estilo
y cuidado de la edición: Fondo Editorial PUCP

Primera edición: noviembre de 2017
Tiraje: 500 ejemplares

Hecho el Depósito Legal en la Biblioteca Nacional del Perú Nº 2017-15495
ISBN: 978-612-317-308-1
Registro del Proyecto Editorial: 31501361701192

Impreso en Tarea Asociación Gráfica Educativa
Pasaje María Auxiliadora 156, Lima 5, Perú

Cybersecurity: generando confianza en un mundo digital

Elder Cama Aréstegui

En un mundo cada vez más interconectado a través del ciberespacio, proteger los activos de información digitales de una organización se convierte en una preocupación empresarial clave. La seguridad cibernética ya no es considerada como un tema solo de los especialistas informáticos, sino que está siendo reconocida como un desafío empresarial fundamental para la mayoría de las organizaciones.

Dada la gran atención mediática que algunos recientes ataques cibernéticos han recibido, nadie puede decir que no conoce o no está al tanto de estos peligros; por lo tanto, hay pocas excusas para las organizaciones que aún no han establecido esquemas de seguridad cibernética básicos en sus sistemas de información y procesos.

Palabras clave: ciberseguridad, defensa activa, información.

En un mundo cada vez más interconectado a través del ciberespacio, proteger los activos de información digitales de una organización se convierte en una preocupación empresarial clave. La seguridad cibernética ya no es considerada como un tema solo de los especialistas informáticos, sino que está siendo reconocida como un desafío empresarial fundamental para la mayoría de las organizaciones.

Hemos sido testigos a través de la prensa especializada de cómo, en los últimos años, un gran número de empresas a nivel global han sido víctimas de ataques cibernéticos. A pesar de esto, la realidad es que no son muchas las empresas que valoran lo que hoy denominamos *cybersecurity* o ciberseguridad. Asimismo, a medida que las diversas amenazas siguen evolucionando rápidamente, tanto en sofisticación como en escala, la necesidad de proteger la propiedad intelectual, las operaciones, la marca y los intereses de las organizaciones, y, adicionalmente, la información de clientes, es cada vez más importante. Los avances en la industria de seguridad no se han ajustado

al ritmo del conjunto diverso de amenazas que enfrentamos hoy en día; por lo tanto, las organizaciones se encuentran en una posición en la que los productos vigentes y los servicios tradicionales de seguridad no son suficientes para enfrentar estos nuevos escenarios de riesgo.

Ciertamente, existe una real necesidad de contar con estrategias más audaces e innovadoras en la seguridad cibernética. Si hoy en día prepararse para los ataques conocidos de seguridad tecnológica es bastante difícil para muchas organizaciones, ¿cómo pueden las organizaciones controlar y enfrentar de manera adecuada los riesgos de seguridad que aún no conocen?

Las principales organizaciones del mundo, líderes en diversas industrias, están haciendo esfuerzos para no solo mejorar su estado actual, sino que están buscando incrementar sus esfuerzos para implementar medidas más audaces a fin de combatir las amenazas cibernéticas y ajustarse al ritmo de los atacantes cibernéticos o incluso llegar a tomarles la delantera. En lugar de esperar a que las amenazas se presenten, estas organizaciones están aprovechando el tiempo en analizar la información disponible sobre amenazas cibernéticas para priorizar acciones que permitan lograr una mayor visibilidad y, de esta manera, lograr una «defensa activa» (concepto que desarrollaremos más adelante) a través de la supervisión personalizada, el análisis, la búsqueda y la rápida detección de escenarios de riesgo en sus sistemas de mayor importancia.

Sin embargo, esto no necesariamente ocurre en el resto de organizaciones. Esta situación es sumamente preocupante, puesto que hace a las empresas vulnerables en uno de sus activos más importantes: la información. Según nuestra encuesta global de seguridad de la información, denominada «Generando confianza en un mundo digital», sorprende que se haya visto disminuido, o se mantenga igual, el presupuesto asignado a la ciberseguridad con respecto a años anteriores[1]. Si bien en el Perú no ha ocurrido —o no ha sido de público conocimiento— un ataque cibernético de gran magnitud, el 100% de los encuestados considera que su actual esquema de seguridad de información no cubre plenamente las necesidades de su organización: a nivel global, un 88% tiene esta percepción.

Es esencial para cada tipo de negocio, independientemente de su envergadura, contar con un responsable de ciberseguridad no solo por el riesgo de sufrir robos de información, sino por las pérdidas de dinero, reputación o crisis que podrían enfrentar al ser atacados. Sin embargo, estas inversiones se ven aplazadas en muchas

[1] EY's Global Information Security Survey. http://www.ey.com/gl/en/services/advisory/ey-global-information-security-survey-2015-1

ocasiones, puesto que se priorizan otros factores, sin entender el enorme riesgo al que se expone una empresa frente a las posibilidades de ser *hackeadas*.

Nuestra encuesta también indica que la fuente más probable de un ataque a nivel global son los cárteles criminales, lo cual deja en segundo lugar a los propios empleados de la empresa, que solían ser los primeros en esta lista. Sobre este punto, por ejemplo, a través de la prensa nos enteramos de que, en México, se han registrado casos de secuestro de hackers por parte de cárteles criminales, debido a que han visto que pueden aprovechar sus habilidades informáticas para contar con una nueva fuente de ingresos delictivos. Algunos expertos señalan que no sería nada extraño que esta modalidad llegue a nuestra región antes de lo esperado.

Cuando un hacker logra penetrar en los sistemas informáticos de la organización, pueden pasar semanas, meses o hasta años sin ser detectado. Una manera a partir de la cual una empresa puede darse cuenta de si está debidamente protegida consiste en analizar los diversos detalles de comportamiento de sus sistemas de información, los cuales podrían volverse anómalos —PC lentas, tráfico de red extraño o programación extraña en los sistemas—. Asimismo, son muchos los casos en los cuales se confunde un ataque cibernético con una falla operativa del sistema, porque no se cuenta con gente debidamente capacitada, con la experiencia y las habilidades técnicas necesarias para poder identificar a tiempo un ataque. De nuestra encuesta, a nivel global, el 36% de las empresas considera tener poca probabilidad de detectar un ataque sofisticado, mientas que en el Perú un 41% las empresas se considera en este escenario.

También es preocupante que sean pocas las empresas en el Perú que cuenten con un rol o función dentro del área de seguridad de información dedicado específicamente al análisis o evaluación de tecnologías emergentes.

La seguridad cibernética tiene un alcance que contempla temas más allá de la tecnología, por lo cual no puede mantenerse solamente en el dominio de las áreas de Tecnología y Sistemas de Información. Tampoco puede ser responsabilidad de un miembro del directorio, ya que afecta a los diferentes niveles de la compañía con diferentes niveles de complejidad. Si estas afirmaciones son bien entendidas por las organizaciones, entonces, ¿cuáles son los principales motivos que dificultan la efectividad de la seguridad de la información? A escala global, un 62% establece que son las restricciones presupuestarias y un 57% la falta de recursos especializados, mientras en el Perú los encuestados indican que las cifras son de 100% y 89% respectivamente.

En este contexto, las organizaciones deben trabajar de manera coordinada a fin de consolidar los recursos necesarios para un mejor análisis de riesgos. Debemos mantenernos en un estado constante de «defensa activa». Para entender cómo la «defensa activa» puede ayudar a mejorar la eficacia de un programa de seguridad, necesitamos una analogía. Muchas organizaciones piensan que la red ideal de una empresa

es como un castillo o una fortaleza: este modelo mental incluye muros gruesos de piedra, torres de guardia y, quizás, también un foso. Los castillos podrán mantener lejos a los invasores del mundo real, pero hemos aprendido una y otra vez que los atacantes casi siempre tienen éxito en penetrar incluso las redes más seguras a través de ataques dirigidos. Los profesionales de seguridad no pueden confiar solo en la integridad del perímetro de la red, por lo que deben operar bajo el supuesto de que tarde o temprano enfrentarán escenarios de ciberataques.

Debido a lo comentado anteriormente, es muy importante que entendamos que al hablar de ciberseguridad en nuestras empresas no debemos involucrar solamente a nuestro responsable de TI, sino que es indispensable lograr la participación comprometida de nuestras áreas de negocio. De lo contrario, solo tendremos la tarea a medio hacer. Así, también, debemos tener en cuenta que las compañías interactúan con terceros —proveedores, clientes, etcétera— vinculados a la operativa del negocio. Ellos también deben contar con el mismo criterio de seguridad cibernética, para de esta forma evitar situaciones que afecten a toda la cadena de negocio. El mensaje que no debemos olvidar es que es nuestra responsabilidad promover un entorno operativo confiable para evitar un posible impacto negativo que nos afecte tanto local como internacionalmente.

Dada la gran atención mediática que algunos recientes ataques cibernéticos han recibido, nadie puede decir que no conoce o no está al tanto de estos peligros; por lo tanto, hay pocas excusas para las organizaciones que aún no han establecido esquemas de seguridad cibernética básicos en sus sistemas de información y procesos. Una vez que los fundamentos hayan sido establecidos y controlados, la siguiente etapa será contribuir a que la seguridad cibernética sea más dinámica, y esté más alineada e integrada a los procesos clave del negocio. Solo así tendremos una real oportunidad de estar adelante del crimen cibernético.