REVIEW OF GLOBAL MANAGEMENT
FACULTAD DE NEGOCIOS UPC

CIBERSEGURIDAD: CÓMO ADOPTAR MEDIDAS PARA PROTEGER SUS ACTIVOS DE INFORMACIÓN

Jimmy A. Armas
ORCID: 0000-0002-1176-8969
Profesor de Business Intelligence and Predictability
Dirección de Computación e Informática
Facultad de Ingeniería, UPC
Lima – Perú
jimmy.armas@upc.pe

Recibido: 16 de noviembre de 2018
Aprobado: 23 de noviembre de 2018
Cómo citar este artículo:
Armas, J. (2018). Ciberseguridad: cómo adoptar medidas para proteger sus activos de información. *Review of Global Management, 4*(2), 20–21.

En las últimas décadas, la tecnología ha facilitado el desarrollo de nuevos modelos de negocio y formas de brindar soluciones utilizando la información, convirtiéndose así en un activo importante de las empresas. En esta nueva realidad, las empresas deben adoptar medidas para proteger sus activos y así evitar que terceros puedan cometer delitos y fraudes financieros, con lo que se generaría un nuevo entorno de amenazas creciente, con efectos devastadores en la continuidad operativa de los negocios.

Según la Information Systems Audit and Control Association (ISACA), "la ciberseguridad es la protección de activos de información a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados". La ciberseguridad implica que las empresas tengan una actitud preventiva y proactiva para evitar graves consecuencias. Por ello, se recomienda mejorar la seguridad dentro de la organización de acuerdo con los siguientes pasos, que puedan reducir significativamente las posibilidades de que la empresa sea víctima de un delito cibernético: 1) realizar copias de seguridad periódica de los datos importantes, considerando herramientas de almacenamiento *cloud*; 2) proteger la organización de *software* malicioso, instalando antivirus y adoptando técnicas de protección; y 3) elaborar directrices deseguridad que puedan ser aplicadas por los empleados, ya que en muchos casos

los incidentes no son provocados por ciberataques, sino que son los propios empleados quienes, bien por falta de conocimiento, bien por poco cuidado, ponen en peligro a la empresa.

Con la implementación de las nuevas tendencias y el impacto de la digitalización, la ciberseguridad cada día cobra más peso estratégico en las organizaciones. Esto obliga a replantear y proteger los procesos tecnológicos de las empresas, ya que con la Internet están expuestas a numerosas amenazas cibernéticas.
¿Cuáles son las amenazas que ponen en riesgo a las empresas?

He aquí cuatro de ellas:

• *Hackers*: "Ciberdelincuentes" que adoptan rápidamente nuevas estrategias para atacar a las empresas. Tratan de buscar cierta información de los usuarios a través de dispositivos móviles.
• *Malware:* Programas maliciosos que se instalan en las bases de datos de las empresas y pueden hacer colapsar el funcionamiento de las computadoras o dispositivos móviles, utilizándolos para monitorear y controlar la actividad privada en la Internet.
• Errores de programación: una mala programación puede poner en peligro los sistemas operativos y las aplicaciones de la empresa, logrando el desequilibrio de algunos datos o acciones en la Internet.
• Fallos electrónicos, siniestros o catástrofes que, por razones externas, perjudican la información de los usuarios.

Es un error pensar que los ataques informáticos únicamente van dirigidos contra grandes compañías u órganos gubernamentales. Cualquier individuo y empresa puede ser el objetivo de los ciberdelincuentes.

Es importante que las empresas presten atención a los diferentes tipos de ataques cibernéticos. No sólo están en juego sus datos, sino que ser víctima de estos ataques también puede generar una mala reputación, hasta multas, demandas o una desvalorización de la compañía como resultado de la pérdida de confianza de la sociedad por los productos o servicios ofrecidos al cliente.