Ciberseguridad, ¿es una urgencia en las empresas?

El panorama de las amenazas cibernéticas está en constante evolución. Según E&Y, el 86% de los ataques tiene una motivación económica, y 92% de estos se transmite por e-mail. Lo alarmante es que puede demorar hasta 6 meses ser detectada una intrusión de seguridad. Estas cifras nos llevan a la pregunta: **¿el Directorio está priorizando en su agenda la revisión del plan de ciberseguridad de su empresa?**

Mirtha Zamudio Rodriguez
Agosto de 2024

La ciberseguridad siempre ha sido un tema de atención en el directorio, pero hoy es un tema critico por la complejidad y frecuencia de los ataques cibernéticos.

La seguridad informática se centraba en proteger las redes y los sistemas contra virus informáticos, y evitar la fuga de información por accesos mal controlados o por la posibilidad de un hackeo. El mundo cambió y en esta era digital, junto con el mayor acceso al internet, el trabajo remoto y la diversidad de dispositivos conectados, han surgido nuevas amenazas.

Los ciberdelicuentes se vuelven más hábiles y organizados, sus ataques también se vuelven más sofisticados y complejos. La modalidad más utilizada es el phishing por correo electrónico; pero la amenaza más compleja y peligrosa es el ransomware, a través de la cual los ciberdelincuentes aprovechan vulnerabilidades en sistemas y redes para secuestrar información, cifrar datos y exigir rescates.

Por la mayor frecuencia de estos ataques, que ocasionan no solo grandes pérdidas económicas sino dañan de forma importante la reputación de la organización, el Foro Económico Mundial ha publicado en su Informe sobre Riesgos Globales 2024, que entre los principales 5 riesgos se encuentran la ciberdelincuencia, pues están adoptando nuevas tecnologías, como las herramientas de IA generativa, para aumentar el número de mercados en los que pueden operar

Varias entidades avanzan en el desarrollo de reportes que muestren la mayor frecuencia de estos ataques. Uno de los más recientes es el Informe Ransomware 2024, presentado por la multinacional de ciberinteligencia y ciberseguridad S2 Grupo. En este reporte indican que, a nivel de Latinoamérica, los 4 países más atacados son Brasil, México, Argentina y Colombia. Perú no se libra de estos ataques cibernéticos, hace poco se publicó el caso en Ingemmet – Instituto Geológico, Minero y Metalúrgico – ocurrido 14 de julio en Lima, que fue víctima de este ataque de ransomware, obligando a suspender sus servicios.

Si bien los directores no debemos ser expertos en el tema, si debemos mantenernos informados pues somos responsables de la supervisión de la seguridad en la empresa, según el Resolución SBS 504-2021. Por lo tanto, debemos solicitar a la dirección ejecutiva que cuenten con una estrategia de seguridad de corto, mediano y largo plazo para tener la garantía de que los riesgos materiales se están gestionando de forma adecuada.

El plan de ciberseguridad, de acuerdo a mi experiencia debe trabajar 3 puntos claves: **Concientización** en toda la organización, sobre las mejores prácticas de ciberseguridad; tener un **marco de gobierno** que permita hacer un seguimiento y una medición de las acciones a través de KPIs; y lo fundamental **contar con profesionales especialistas** en ciberseguridad capaces de operar con las herramientas de seguridad y adaptarlas al contexto de la organización.

Economista de la Pontificia Universidad Católica del Perú, MBA en Adolfo Ibáñez y Certificada en el Programa de Directores de Empresas (PDE) por la Universidad del Pacífico, Georgetown y EY ¡ Amplia trayectoria de más de 30 años en el sector financiero, ex Gerente General Adjunto del BBVA ¡Directora Independiente de COFIDE, ex asesora del Comité de Innovación en Mall Aventura del Grupo Ripley.
Asesora de Alta Dirección en temas de Transformación Cultural Digital con foco en transformación de procesos, desarrollos analíticos con riguroso gobierno del dato

Ddd