Seguridad en tecnología de la información

Escrito por Luis Alberto Cá... el 15 Mayo 2018

Hace un año, en artículos publicados el 9 y el 16 de mayo del 2017, hablamos sobre el gobierno de la tecnología de la información; asimismo, el 24 de marzo del 2015, abordamos el proceso de seleccionar sistemas. **Hoy quiero hablar sobre la seguridad informática.**

Actualmente, todas las organizaciones dependen de la tecnología de información para llevar a cabo muchas de sus tareas, desde la planeación de las actividades, pasando por el registro de todas las transacciones hasta la emisión de los reportes conteniendo los resultados obtenidos por cada proceso.

Además, ahora los sistemas de información pueden controlar desde los equipos industriales más sofisticados hasta la simple operación de un elevador.

La ciberseguridad es el área que se encarga de la protección de todos los aspectos que componen un sistema de información, desde los equipos de computación, almacenamiento y comunicaciones, los programas que ayudan a que funcionen, hasta los datos que procesan y almacenan. **La seguridad de la información es un componente de la ciberseguridad.**

Cualquier empresario o administrador de empresa debe estar preocupado por mantener la información de su empresa en resguardo y a salvo de robos o mal uso de ella; además de que no pueda ser alterada o destruida. También debe estar preocupado en proteger la infraestructura física y los sistemas operacionales que ayudan a que la organización pueda llevar a cabo su misión.

Los riesgos para la organización son múltiples, como perder datos de clientes que pongan a la empresa de estar en incumplimiento de la **Ley de Protección de Datos Personales y Acceso a la Información**, o la imposibilidad de continuar las operaciones por un ataque pernicioso a sus sistemas.

La seguridad de los sistemas de información empieza desde el gobierno de la entidad, es decir, que quienes toman las decisiones estratégicas de la empresa deben comprometerse con una filosofía de seguridad y todas las políticas y procedimientos que de ella surjan.

El gobierno de la entidad deberá asesorarse para emitir tales políticas y procedimientos enfocados a la protección de todos los sistemas de tecnología de la entidad.

Para lograr una protección de todos los sistemas, es necesario conocer los riesgos que deben ser cubiertos, como son: daños causados por los usuarios o personal técnico; intrusión de programas maliciosos; errores de programación; accesos no autorizados; fallos eléctricos, electrónicos o lógicos en los sistemas; y siniestros y catástrofes naturales.

Asimismo, deben asegurarse medidas de protección como son:

1. Controles para la selección de los sistemas a ser utilizados, para que tengan las características operacionales y de seguridad necesarias.
2. Gestión de desarrollo y cambios de sistemas, así como ambientes de prueba separados de áreas en funcionamiento.
3. Acceso físico a las áreas de servidores y medios de almacenamiento y lógico a los sistemas, cuidando una adecuada división de funciones y evitando la incompatibilidad de actividades.
4. Programas antivirus y antimalware
5. Firewall de protección a todos los accesos lógicos externos.
6. Implementación de redes virtuales o VPN para asegurar que la información interna fluya libre

de contaminación o accesos o salidas de información externas.
7. Gestión de entradas y salidas de información, para verificar que la de entrada sea real y completa y que la de salida cumpla con las expectativas.
8. Verificar que los procesos contengan todas las variables necesarias para el adecuado proceso de datos.

En otros artículos ampliaremos estos temas.