Incorporando la ciberseguridad en la organización

Ampliando el concepto de seguridad

La ciberseguridad no puede considerarse separada de los procesos centrales del negocio.

Las organizaciones necesitan asegurar sus procesos clave de negocio como ser marketing, gestión de clientes, procesos de facturación, adquisición, etc., junto con los procesos de gestión de acceso lógico, gestión de riesgos, cambios, incidentes, gestión de programas y otros, tomando en cuenta la ciberseguridad.

Estos procesos deben funcionar juntos para proteger adecuadamente a la organización.

> **La ciberseguridad no es solamente un tema del personal de TI, es un vehículo para generar confianza en las relaciones comerciales.**

KPMG
Circunvalación Dr. Enrique Tarigo
(ex Plaza de Cagancha) 1335
Piso 7, CP: 11.100
Montevideo, Uruguay
Teléfono: (598) 2902 4546
Fax: (598) 2902 1337
e-mail: kpmg@kpmg.com.uy

Contactos:
Cr. Rodrigo Ribeiro
rribeiro@kpmg.com

Ing. Pablo Romero
pabloromero@kpmg.com

Lic. Marcelo Cagnani
marcelocagnani@kpmg.com

Lic. Ana Lucero
alucero@kpmg.com

kpmg.com.uy

Actuamente, las organizaciones son conscientes de que necesitan mecanismos técnicos para protegerse de las amenazas cibernéticas. Como resultado, la mayoría han realizado grandes inversiones en tecnologías de ciberseguridad. Sin embargo, esto a menudo no tiene en cuenta dos factores:

¿Cuáles son los activos y sistemas de información de mayor valor para la organización?

¿Los procesos y niveles de conocimiento del personal se encuentran en un nivel de madurez acorde con la inversión en tecnología?

Los esfuerzos de ciberseguridad deben centrarse en las amenazas a los activos de información de la organización y a los activos físicos conectados a la red.

Las preguntas que las organizaciones deben ser capaces de responder incluyen:

¿Cuáles son los activos de información y recursos físicos conectados a la red?

¿Cuán valiosos son estos activos para la organización? ¿Cuán valiosos son para un perpetrador externo?

¿Dónde se encuentran los activos de información y cómo se accede a ellos?

¿Quién está utilizando la información y activos físicos?

¿Cómo se mantienen seguros estos activos desde una perspectiva tecnológica, de procesos y de personas?

Responder a estas preguntas no necesariamente conducirá a definir controles técnicos adicionales.

Debe ser prioritario proteger los activos de información que realmente importan. Esto requiere mecanismos de protección específicos, tanto desde una perspectiva tecnológica como desde una perspectiva de concientización y procesos.

Mientras que ciertas industrias como por ejemplo la financiera, están en niveles más altos de madurez de ciberseguridad, la mayoría de las organizaciones tienen algún camino por recorrer.

Solamente a través de la identificación y comprensión de sus activos críticos, el conocimiento de las amenazas y el análisis de riesgo correspondiente, es que se puede determinar el nivel de madurez de ciberseguridad. Una vez que esta línea base se encuentra establecida, es posible desarrollar un enfoque holístico para mejorar la madurez general de la ciberseguridad en relación con las personas, los procesos y la tecnología. Esto, a su vez, proporciona a la organización una sólida base de ciberseguridad para permitir que el negocio crezca, se transforme y se expanda.