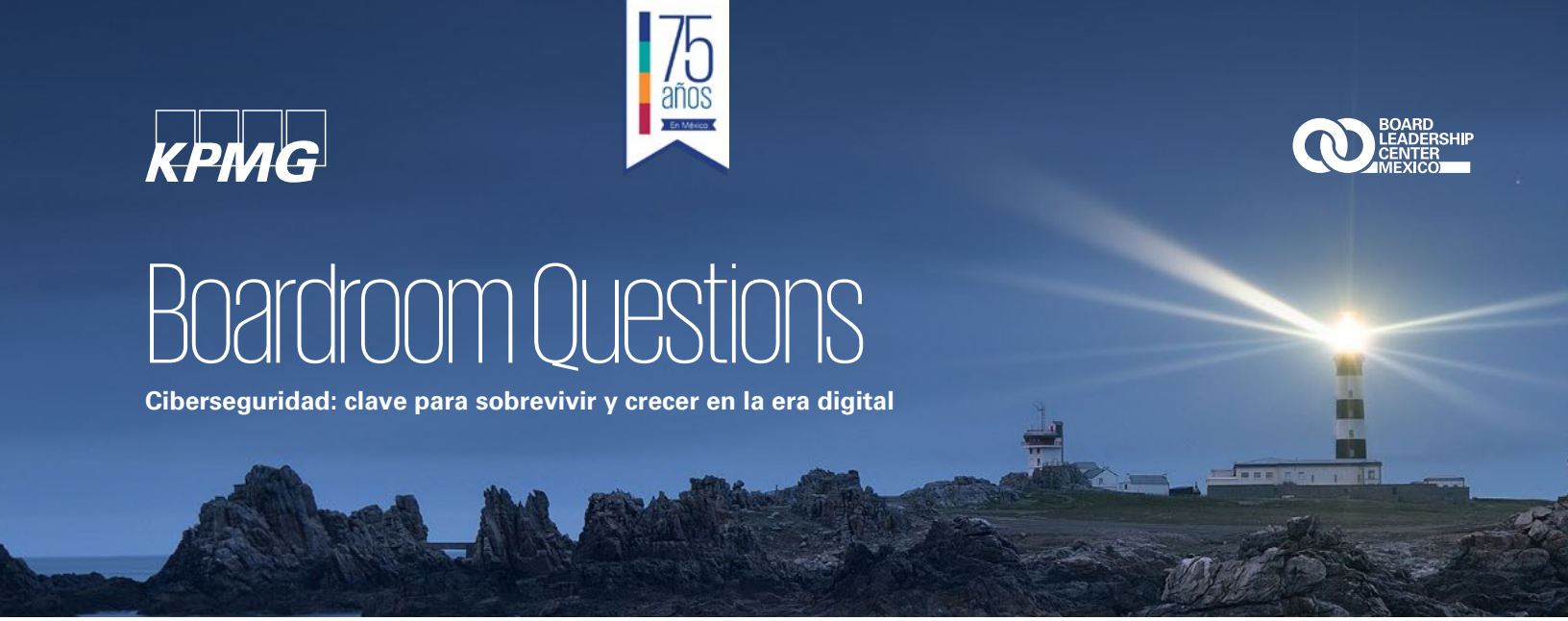

Boardroom Questions

Ciberseguridad: clave para sobrevivir y crecer en la era digital

Combatir amenazas a la seguridad de la información es ahora más importante que nunca

Como es bien sabido, la pandemia aceleró la **automatización** y **digitalización de los procesos de las empresas.** Se presentaron **rápidas expansiones** de los canales de comercio digital y los comportamientos de los consumidores cambiaron drásticamente.

Lo anterior ha provocado una mayor dependencia hacia la tecnología de la información y, por lo tanto, las consecuencias de una falla en esta serán mucho mayores que en el pasado. El sondeo *Combatir el cibercrimen en la nueva realidad*, realizado por KPMG en México, muestra que las amenazas a la disrupción de los activos tecnológicos de las empresas han aumentado; tras la pandemia, **79%** de las entidades enfrenta **un mayor número de ciberataques.** Asimismo, **97%** de las corporaciones mencionan incrementos de entre **6%** y más de **15%** de amenazas a partir de la coyuntura actual.

Cuestiones clave: entornos digitales seguros

Habilitador del negocio

Los especialistas siempre nos han dicho que **proteger la información**, práctica ahora denominada ciberseguridad, debe ser considerada como un **habilitador del negocio**. Este pensamiento es hoy una realidad; sin la protección adecuada de los activos, será imposible para las empresas realizar transacciones.

Cumplimiento regulatorio

Existe una fuerte **tendencia regulatoria**, nacional e internacional, hacia la protección de datos y la privacidad, elementos que exigen un cambio en el **tratamiento de la información** y **gestión de datos personales**. La combinación de impactos operativos y reputacionales trae consigo la necesidad de **fortalecer la ciberseguridad** y salvaguardar los **activos que las organizaciones emplean**.

La realidad presente

El **teletrabajo** y la utilización de **herramientas colaborativas** ampliaron las **fronteras digitales** de los negocios; el concepto de una red interna de computadoras se empieza a ver cada vez más difuso y términos como "agile", "DevOps", "migración a la nube" y "transformación digital" son empleados con mayor frecuencia.

Efectos y repercusiones de una estrategia de ciberseguridad débil

El estudio mencionado también muestra cuáles son los principales riesgos que las organizaciones enfrentan:

1) Para 74% de las entidades encuestadas tener una **fuga, filtración o robo de información confidencial** representa el principal riesgo a evitar
2) La **interrupción de las operaciones** de la empresa es el segundo peligro más importante con un **57%**
3) El que la **infraestructura pueda sufrir daños** por un ciberataque o evento natural es el tercer riesgo más importante, al ser señalado por **27%** de los encuestados
4) La **extorsión por parte del cibercrimen** es el cuarto, siendo destacado por **22%**
5) Con **17%**, un posible **impacto en la calidad de los productos o servicios** derivado de un ciberataque es el quinto obstáculo que debe atenderse

Preguntas para el Consejo de Administración

El **Consejo** reconoce que el principal desafío que encaran las organizaciones por ciberataques es el económico, aunque se perciben otros, como los daños reputacionales, de imagen, legales, pérdida de clientes, entre otros. Teniendo todos como consecuencia final una pérdida monetaria.

Para evitarlo, es importante que el Consejo de Administración considere lo siguiente:

1) ¿Existe un **apoyo adecuado** a la ciberseguridad en la empresa?
2) ¿Se ha abordado el **tema en el Consejo**?
3) ¿El Consejo de Administración sabe cuáles son los **principales riesgos** que enfrenta la entidad?
4) ¿Qué tan **madura es la organización** en términos de seguridad informática?
5) ¿El Consejo conoce el monto de la **inversión** destinada a la **protección de la información y datos personales?**
6) ¿Se cuenta con **asesoría independiente** en ciberseguridad que ayude a determinar las **mejoras** que sean necesarias para la **protección de la compañía**?
7) ¿Es necesario considerar a la ciberseguridad dentro de las **iniciativas estratégicas** a futuro?

Preguntas para la Alta Dirección

1) ¿Se cuenta con una **estrategia de ciberseguridad**? ¿Se ha realizado un **análisis de riesgos** en la materia?
2) ¿Qué **ataques** se han tenido en el último año? ¿Cuáles han sido los **impactos** que estos han tenido en la organización?
3) ¿Cuáles son las **principales iniciativas** en materia de seguridad de la información que se están ejecutando dentro de la compañía?
4) ¿Se **capacita a los usuarios**? ¿Cómo se mide la efectividad de dicha capacitación?
5) ¿Cómo se **gestionan las vulnerabilidades**?
6) ¿Se ha evaluado la ciberseguridad en los **proveedores y terceros** que manejan información de la empresa?

¿Qué acciones debe considerar el Consejo?

Con la **evolución de la tecnología** y la creciente relevancia que tiene para las empresas, es necesario que el **Consejo de Administración** esté consciente de que la ciberseguridad es preponderante y que, para **lograr su efectividad**, es necesaria una **comunicación eficaz**, así como difundir **políticas y procedimientos, capacitar a los colaboradores** e, incluso, asumir las **consecuencias del incumplimiento** de las medidas implementadas.

KPMG

BOARD LEADERSHIP CENTER MEXICO

Acerca de KPMG Board Leadership Center en México

Es un programa global con presencia local exclusivo para miembros del Consejo de Administración en México, que tiene como objetivo promover un gobierno corporativo efectivo para impulsar el valor de la empresa a corto, mediano y largo plazo, generando confianza en los *stakeholders* de las organizaciones.

kpmg.com.mx
800 292 KPMG (5764)
blc@kpmg.com.mx

KPMG MÉXICO @KPMGMEXICO KPMGMX KPMG MÉXICO