KPMG

Ciberseguridad

Siete medidas básicas para proteger a su empresa

KPMG en México

¿Sabe cuánto dinero pierden las empresas en promedio por ataques cibernéticos?

¿Su empresa está invirtiendo lo suficiente en ciberseguridad actualmente?

Ciberseguridad

Medidas básicas para proteger a su empresa

El riesgo cibernético debe ser mitigado tomando acciones efectivas para evitar o minimizar los daños de un posible ataque. Una asesoría adecuada permite generar resultados confiables para la protección de datos.

57% fue el crecimiento de los costos para las empresas por fuga de datos en la última década.
Fuente: Ponemon Institute 2015 Cost of Data Breach Study: United States

Invertir con base en riesgos

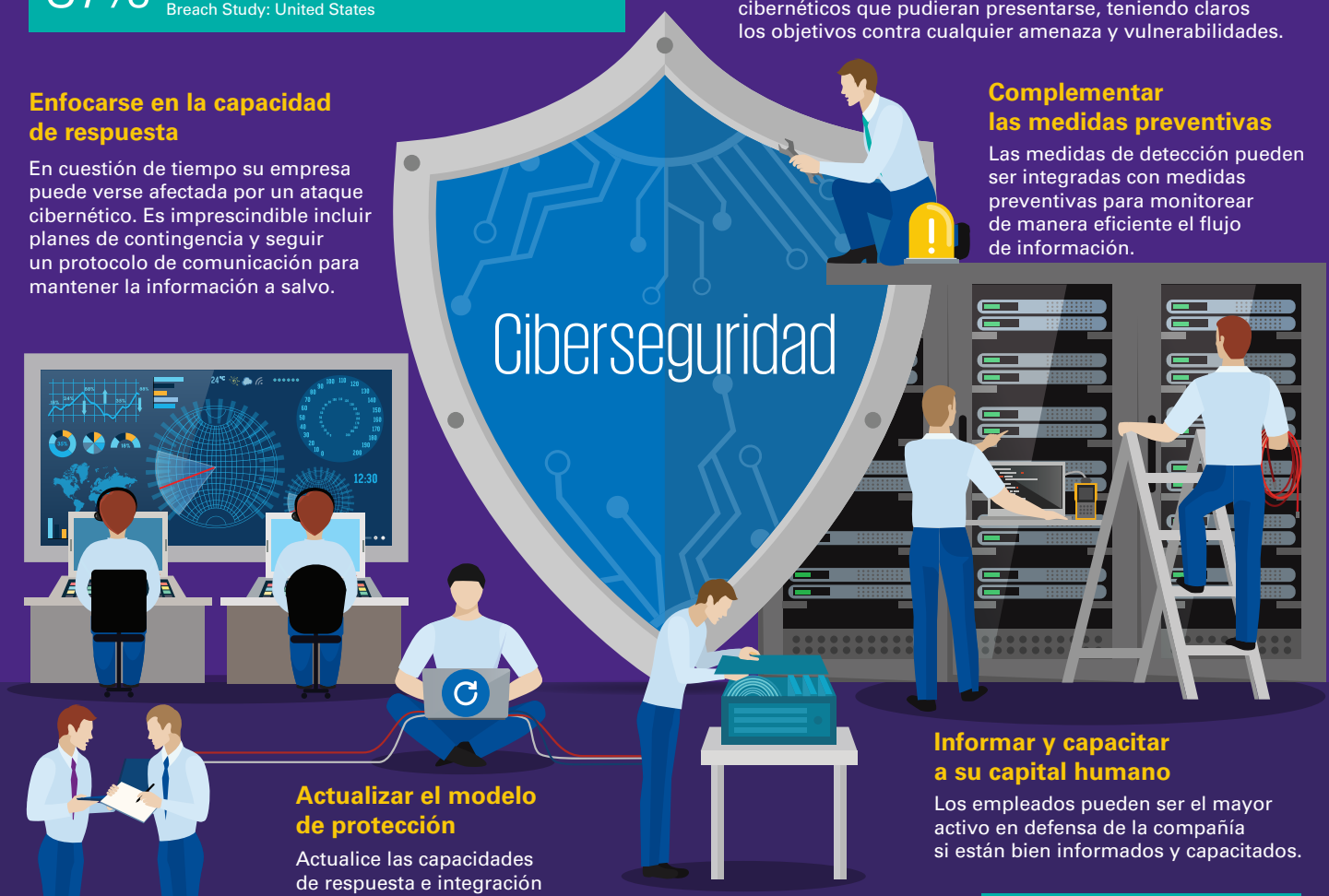
Es de vital importancia destinar los recursos necesarios para mantener la empresa protegida de ataques cibernéticos que pudieran presentarse, teniendo claros los objetivos contra cualquier amenaza y vulnerabilidades.

Enfocarse en la capacidad de respuesta

En cuestión de tiempo su empresa puede verse afectada por un ataque cibernético. Es imprescindible incluir planes de contingencia y seguir un protocolo de comunicación para mantener la información a salvo.

Complementar las medidas preventivas

Las medidas de detección pueden ser integradas con medidas preventivas para monitorear de manera eficiente el flujo de información.



Informar y capacitar a su capital humano

Los empleados pueden ser el mayor activo en defensa de la compañía si están bien informados y capacitados.

Actualizar el modelo de protección

Actualice las capacidades de respuesta e integración con otras áreas para disminuir los riesgos cibernéticos a los que se expone la empresa.

Proteger sus activos más importantes

Proteja las "joyas de la corona" de su empresa con un sistema integral y atención especializada.

Fomentar la cooperación entre organizaciones

Es importante promover la participación entre empresas para mantenerse actualizadas e informadas sobre amenazas emergentes y que obtengan un aprendizaje recíproco.

6.5 millones de USD

costo promedio por pérdidas debido a ataques cibernéticos.

Reflexión

Debido a que los ataques cibernéticos afectan a millones de empresas, es necesario contar con servicios especializados para abordar temas en materia de gestión de vulnerabilidades, monitoreo continuo, ciberinteligencia, respuesta a incidentes y administración de seguridad.

Un ataque informático es considerado como el mayor riesgo que enfrenta una empresa en la actualidad.

Durante la Tercera Revolución Industrial, el principal reto de las empresas fue establecer de forma efectiva la seguridad en internet. En la Cuarta Revolución Industrial, este sigue siendo un elemento crucial para las organizaciones. La ciberseguridad consiste en el esfuerzo para prevenir daños por alteración, interrupción o mal uso de las Tecnologías de la Información (TI); si ocurre un daño, se contempla su reparación.

Los daños podrían incluir el deterioro de la disponibilidad de las TI, restricción sobre estas, o violación de la confidencialidad y/o la integridad de la información almacenada en los entornos de TI.

Por ello, es de vital importancia que las empresas cuenten con una estrategia integral de ciberseguridad y sepan cuáles son las medidas más adecuadas para proteger su información y recursos.

El riesgo cibernético puede y debe ser mitigado aplicando las medidas necesarias y actuando efectivamente. Una asesoría especializada le ayudará a identificar las áreas de oportunidad, generando resultados confiables para la empresa. A continuación, se plantean siete medidas básicas que toda compañía debe tomar en cuenta para salvaguardar su información:

1 Proteger sus activos más importantes

En vista de la dificultad que implica proteger toda una organización, la ciberseguridad requiere una atención especial para salvaguardar la información más valiosa de la empresa; identificar las "joyas de la corona" que necesitan ser resguardadas.

2 Informar y capacitar a su capital humano

Contar con tecnologías para llevar a cabo la protección, identificar a los intrusos y responder a un ataque resulta indispensable para las organizaciones, sin embargo, el ser humano suele ser el eslabón más débil. Al mismo tiempo, los colaboradores pueden ser el mayor activo en defensa de la compañía si están debidamente informados y capacitados.

La Alta Dirección de una empresa debe abordar la ciberseguridad de manera estructural, destinando los recursos necesarios para mantenerla segura.

3 Complementar las medidas preventivas con las de detección

Enfocarse en el monitoreo técnico para analizar y detectar el flujo de información, así como implementar medidas preventivas para evitar incidentes de ciberseguridad, es de vital importancia para las entidades.

4 Enfocarse en la capacidad de respuesta de la empresa

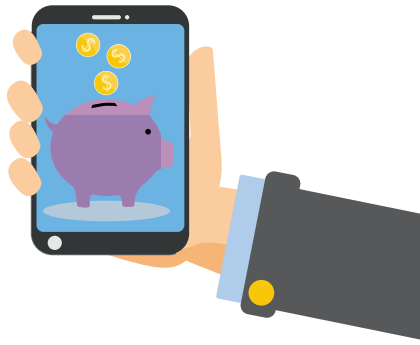
Es cuestión de tiempo que una empresa se convierta en víctima de un incidente cibernético. Incluir planes de contingencia contra estos ataques y un protocolo para las comunicaciones durante un suceso de este tipo, debe ser una prioridad para la compañía.

5 Fomentar la cooperación entre organizaciones

Es crucial que las compañías se mantengan actualizadas e informadas sobre las amenazas emergentes y aprendan de otras organizaciones las mejores tácticas para reaccionar ante los incidentes. Para facilitar esto, existen organismos cuyo objetivo es ayudar a otras en ese ámbito. También es importante promover la participación activa de la empresa en este tipo de redes; un incidente en otra entidad es, de igual forma, una amenaza potencial para la propia organización.

En KPMG tenemos la experiencia para fortalecer su estructura de seguridad. **Trabajamos con usted** hombro con hombro, aportando un enfoque global y pasión **para brindarle** las **herramientas necesarias en materia de ciberseguridad**.

6 Invertir con base en los riesgos de la empresa



Con el fin de determinar el perfil de riesgo de una empresa, debemos utilizar un modelo que cubra cinco diferentes aspectos. En el **ambiente de negocio**, hay que identificar cuáles son los mercados en los que se encuentra activa la entidad y cómo se desempeña en los mismos. Tenemos que estar conscientes de las **amenazas** y **vulnerabilidades** que podrían explotar los cibercriminales y anticipar a qué grupo de delincuentes cibernéticos le resulta atractiva la compañía y con qué recursos podría desplegar el ataque. Asimismo, teniendo claros qué **objetivos** podrían estar sujetos a ataques en la organización y qué **requisitos legales** debemos cumplir en materia de ciberseguridad, se pueden destinar los recursos pertinentes para mantener protegida a la empresa.

7 Actualizar el modelo de protección para anticipar amenazas emergentes

Las estrategias de ciberseguridad de una compañía tienen que actualizarse constantemente para hacerle frente a nuevas amenazas que surjan. Estas nuevas estrategias deben cubrir las capacidades de respuesta y la integración con otras áreas, tomar como base la inteligencia de amenazas y los activos más importantes para el atacante. Una búsqueda continua de vulnerabilidades en los sistemas, aunado a la integración con áreas legales, manejo de crisis y continuidad, permitirán mantener un modelo de protección actualizado, disminuyendo los riesgos cibernéticos a los que está expuesta una empresa.

6.5 millones de USD fue el costo promedio por pérdidas para las empresas por ataques cibernéticos en 2016.

Experian.com - 2016 Data Breach Industry Forecast

En la Cuarta Revolución Industrial donde nos encontramos actualmente, una organización sin una estrategia integral de ciberseguridad está expuesta tanto a la pérdida de recursos como a riesgos a su propia integridad, la de sus clientes y su reputación. Una empresa que busque mantener su información vital segura debe dejar atrás los enfoques tradicionalistas que ponen en peligro sus activos.

Una corporación debe contar con la asesoría especializada en ciberseguridad para seguir las mejores prácticas y así salvaguardar su información más importante, además de capacitar adecuadamente al personal para proteger mejor los activos de la compañía. Asimismo, los ayuda a implementar servicios de detección, a mejorar la capacidad de reacción de la empresa ante una eventualidad y promover la participación activa e informada de los empleados en todos los niveles.

Mantenerse actualizado en cuanto a las posibles amenazas y la manera de contrarrestarlas es de suma importancia para una compañía. Al conocer el perfil de los atacantes e identificar los probables objetivos dentro de la entidad, es posible hacer una inversión efectiva, en las áreas donde mayores riesgos se presentan.

Los especialistas en materia de ciberseguridad de KPMG en México trabajarán con usted hombro con hombro, brindando enfoques innovadores para mantener la estrategia informática de su organización y entregar resultados confiables.

Nuestra oferta KPMG

La Asesoría de KPMG en materia de ciberseguridad abarca las áreas de gestión de vulnerabilidades, ciberinteligencia, monitoreo continuo, respuesta a incidentes y administración de seguridad con una amplia variedad de servicios a su disposición, incluyendo los siguientes:

- ***Strategy & Governance***
  - Estrategias de ciberseguridad
  - *Cyber maturity assessment*
  - Resiliencia del negocio
  - Cumplimiento de marcos y análisis de brechas (ISO 27001, NITS, etc.)
  - Atestiguamientos en ciberseguridad
- ***Transformation***
  - *Identity & access management*
  - *Governance, Risk & Compliance (GRC)*
- ***Cyber Defense***
  - Hackeo ético y análisis de vulnerabilidades
  - Ciber-Inteligencia
- ***Cyber Response***

Contacte a nuestros especialistas para que establezcamos juntos una estrategia integral de ciberseguridad para su organización.

KPMG

kpmg.com.mx
01 800 292 KPMG (5764)
asesoria@kpmg.com.mx

KPMG MÉXICO
@KPMGMEXICO
KPMG MÉXICO
KPMGMX

Contacto

Rolando Garay
Socio Líder de Servicios de Tecnología y Transformación KPMG en México

Eduardo Cocina
Socio de Asesoría en Tecnologías de la Información KPMG en México

Rommel García
Socio de Asesoría en Tecnologías de la Información KPMG en México

Christian Andreani
Socio de Asesoría en Tecnologías de la Información KPMG en México

Regístrese en **Delineando Estrategias.com.mx** y consulte más información sobre ciberseguridad:

Disrupt and grow. 2017 Global CEO Outlook

SÚPER EMPRESAS EXPANSIÓN 2017

ESR Empresa Socialmente Responsable 1% Inversión Social

THE GLOBAL COMPACT APOYAMOS EL PACTO MUNDIAL