KPMG

Cyber Maturity Assessment

Seis dimensiones clave para asegurar la información de una organización

KPMG en México

¿Sabe cuánto dinero se pierde a nivel mundial debido al crimen cibernético?

¿Sabe cuántos usuarios en México han sido víctimas de un ataque cibernético?

Cyber Maturity Assessment (CMA)

Seis dimensiones para asegurar su información

Ante un peligro inminente, una organización debe contar con la asesoría adecuada para alcanzar la madurez cibernética necesaria y así poder asegurar su información.

Liderazgo y Gobierno Corporativo

La Alta Dirección y los dueños de una organización deben administrar de manera efectiva los riesgos que presenta su negocio, con especial atención en la documentación de políticas y su entendimiento de ciberseguridad.

125,900 millones de dólares fue el costo total de los crímenes cibernéticos alrededor del mundo en el año 2016

Fuente: *Norton Cyber Security Insights Report 2016*

Manejo del riesgo de la información

Con el intercambio de información y buenas prácticas, una arquitectura digital sólida, y el establecimiento de políticas y procedimientos, se puede generar una estrategia integral de gestión de riesgo de la información.

Legal y cumplimiento

Toda organización que prepare una estrategia de ciberseguridad, debe contemplar el cumplimiento con las regulaciones y normas internacionales de certificación.

Continuidad y manejo de crisis

Se debe medir el nivel de preparación para un evento de seguridad y la capacidad de la organización para prevenir o minimizar el impacto a través de una gestión exitosa de la crisis por las partes interesadas.

Operaciones y tecnología

La seguridad del personal, la seguridad física, gestión de identidad y acceso, así como la identificación de amenazas y vulnerabilidades, son algunas de las medidas para abordar riesgos y minimizar el impacto de un ataque.

Factor Humano

Se deben medir las habilidades especializadas, cultura informática, entrenamiento, concientización y la administración del talento, para hacer de los colaboradores verdaderos activos para la protección de la información de una empresa.

22.4 millones de usuarios fueron víctimas de ataques cibernéticos en México en 2016

Fuente: *Norton Cyber Security Insights Report 2016*

Reflexión

Debido a que los ataques cibernéticos afectan a millones de organizaciones, es necesario contar con el nivel adecuado de madurez cibernética para así asegurar su información y minimizar el impacto de este tipo de amenazas.

Mientras las amenazas de criminales cibernéticos y 'hacktivistas' crecen en alcance y sofisticación, las organizaciones se vuelven cada vez más vulnerables como resultado de avances tecnológicos y manejo de datos a distancia.

Los costos financieros y la pérdida de reputación por no estar preparados ante un ataque cibernético son significativos. Se estima que el impacto global de crímenes cibernéticos es de cerca de 125,900 millones de dólares; esto representa un aumento de 10% en relación con cifras de 2014 de acuerdo con el *Norton Cyber Security Insights Report*. Las compañías absorben casi 80% de estos costos y la desconfianza de clientes y accionistas se ha convertido en una preocupación creciente. Además, en el caso de México, 22.4 millones de usuarios fueron afectados por este tipo de crímenes, tan solo en 2016.

Ante un peligro inminente, instancias gubernamentales, al igual que grandes corporativos demandan confianza en el manejo de la información antes de entablar una nueva relación de negocio. Debido a esta situación, las organizaciones deben identificar sus áreas de riesgo cibernético y establecer un plan de acción para hacer frente a estas amenazas.

El servicio de **Cyber Maturity Assessment (CMA)** de KPMG brinda una perspectiva integral de la capacidad de una empresa para manejar y proteger su información, así como su preparación ante un ataque cibernético. Este servicio hace un análisis de la gente, los procesos y la tecnología de una compañía para entender sus espacios de vulnerabilidad y encontrar áreas prioritarias de acción. Todo esto con el objetivo de transformar los riesgos de información en ventajas de negocio.

CMA combina estándares internacionales de seguridad de la información con nuestro enfoque global y mejores prácticas en manejo de riesgos, ciberseguridad, gobierno, procesos y gente. Para brindar una perspectiva profunda de la madurez cibernética de una organización y ayudar a las organizaciones a asegurar su información, CMA se enfoca en las siguientes seis dimensiones clave:

1 Liderazgo y Gobierno Corporativo

Uno de los ámbitos principales de una empresa para determinar su madurez cibernética, radica en la habilidad de la Alta Dirección, sus dueños y práctica de *due diligence* para administrar de manera efectiva los riesgos que presenta su negocio. Algunos de los asuntos sobre los que se debe prestar especial atención son la documentación de políticas, el marco de gobierno y el entendimiento de la compañía sobre la ciberseguridad.

2 Factor humano

Los colaboradores pueden convertirse en uno de los mayores activos de una empresa para proteger su información si cuentan con la capacitación y el entrenamiento adecuados. Se debe medir el nivel de cultura enfocada a la seguridad que impulse y refuerce sus habilidades. Esta medición cubre aspectos como habilidades especializadas, cultura informática, entrenamiento y concientización, además de la administración del talento.

3 Manejo del riesgo de la información

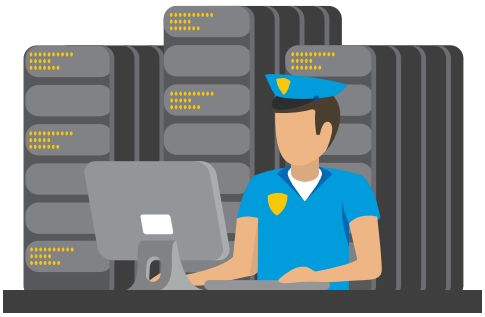
Un enfoque adecuado hacia los riesgos resulta determinante en el caso de un ataque cibernético en una empresa. Más allá de los esfuerzos de un departamento de TI, los tomadores de decisión deben buscar una gestión integral y eficaz del riesgo de la información en toda la organización, así como con sus socios y proveedores. Esto se logra a través del intercambio de información y buenas prácticas para proteger sus activos, una arquitectura digital sólida y el establecimiento de políticas y procedimientos de manejo de riesgo. Otra alternativa es contar con servicios de seguridad gestionados por un tercero.

4 Continuidad del negocio y manejo de crisis

Ante una posible intrusión o ataque cibernético es de vital importancia contar con un plan de comunicación y un protocolo de acción. CMA mide el nivel de preparación para un evento de seguridad y la capacidad de la organización para prevenir o minimizar el impacto a través de una gestión exitosa de la crisis por las partes interesadas. Toda empresa debe contar con un Plan de Continuidad del Negocio y realizar un Análisis de Impacto en los Negocios (BCP y BIA respectivamente, por sus siglas en inglés), así como un protocolo de recuperación de desastres y respuesta al incidente.

5 Operaciones y tecnología

El nivel operativo es donde se puede tener un mayor control sobre el nivel de medidas implementadas para abordar riesgos y así minimizar el impacto de un evento de seguridad. La medición incluye la seguridad del personal, seguridad física, gestión de identidad y acceso, al igual que la identificación de amenazas y vulnerabilidades. Obtenemos una perspectiva de la seguridad en la red de una organización, la administración de los servicios, sistemas para detección de intrusos y seguridad remota con dispositivos móviles y con acceso a red inalámbrica.



22.4 millones de usuarios fueron víctimas de ataques cibernéticos en México en 2016

Norton Cyber Security Insights Report 2016

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 Legal y cumplimiento

En toda estrategia de seguridad informática debe contemplarse el cumplimiento con las regulaciones y normas internacionales de certificación. Deben considerarse las Tres Líneas de Defensa, un modelo de trabajo que tiene como base métricas de cómo el Gobierno Corporativo de una organización lidia con los diferentes niveles de riesgo. Cumplimiento normativo y la transferencia de riesgos financieros son otros aspectos a considerar en esta dimensión.

125,900 millones de dólares fue el costo total de los crímenes cibernéticos alrededor del mundo en el año 2016

Norton Cyber Security Insights Report 2016

Para que una organización pueda mantener segura su información y minimice la pérdida de recursos, riesgos en su propia integridad, la de sus clientes o su reputación, debe tener un nivel de madurez cibernética adecuado. Una empresa debe contar con la asesoría especializada para manejar los riesgos de información y capacitar adecuadamente a su personal, para mantener la continuidad del negocio y responder de manera efectiva ante las amenazas que surjan.

CMA de KPMG incorpora nuestra visión de las mejores prácticas globales de los sectores público y privado e impulsa la transformación del negocio basada en el uso apropiado de los activos de información.

La evaluación de madurez es el inicio en el ciclo de mejora de seguridad de la información y permite que una organización entienda cuán maduro es su enfoque de la seguridad y cómo es capaz de resistir un ataque cibernético.

A través de una combinación de entrevistas, talleres, revisiones de procesos y políticas, y pruebas técnicas, CMA permite:

- Identificar brechas actuales en el cumplimiento y manejo de riesgos de los activos de información
- Evaluar la verdadera escala de vulnerabilidades cibernéticas
- Establecer áreas prioritarias para la remediación y un plan de acción integral

Asimismo, provee la flexibilidad para evaluar el nivel de madurez de una compañía. Identifica las mejores prácticas dentro de una empresa y brinda información comparativa con respecto a grupos similares y competidores.

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

Nuestros Servicios

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

- ***Strategy & Governance***
  - Estrategias de ciberseguridad
  - Resiliencia del negocio
  - Cumplimiento de marcos y análisis de brechas (ISO 27001, NITS, etc.)
  - Gobierno de información
  - Atestiguamiento en ciberseguridad

- ***Transformation***
  - *Identity & access management*
  - *Governance, Risk & Compliance* (GRC)

- ***Cyber Defense***
  - Hackeo ético y análisis de vulnerabilidades
  - Ciberinteligencia

- ***Cyber Response***

Contacte a nuestros especialistas para que establezcamos juntos una estrategia integral para asegurar la información de 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

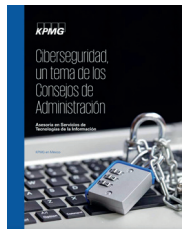
Rommel García
Socio de Asesoría en Tecnologías de la Información KPMG en México

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

Visite y consulte **Delineando Estrategias.com.mx** para más información sobre ciberseguridad:

Disrupt and grow. 2017 Global CEO Outlook

Ciberseguridad, un tema de los Consejos de Administración



SÚPER EMPRESAS EXPANSION 2017

ESR Empresa Socialmente Responsable 1% Inversión Social

THE GLOBAL COMPACT APOYAMOS EL PACTO MUNDIAL