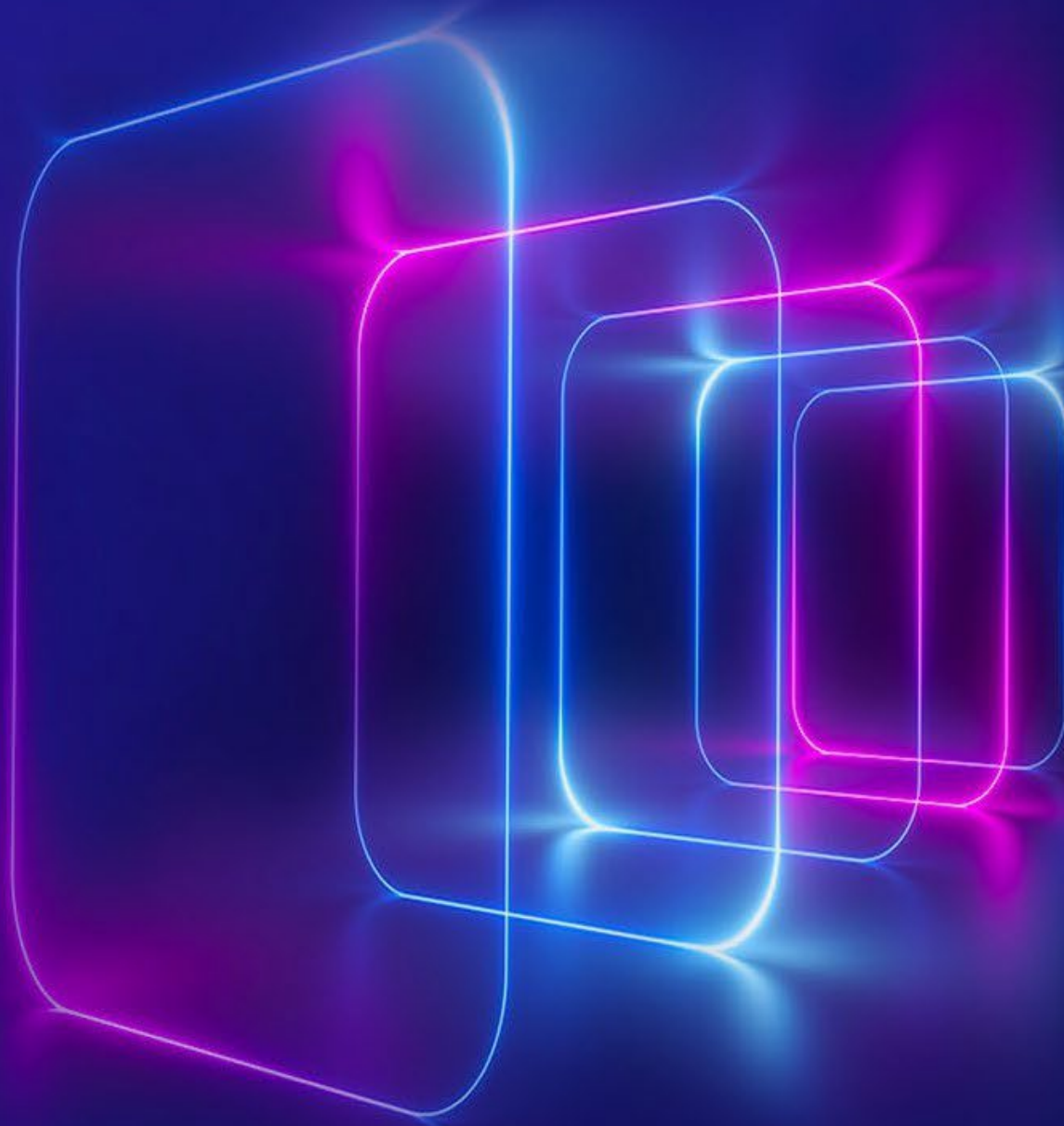
KPMG

KPMG Cyber trust insights 2022

8 Puntos para generar confianza



Abril 2023
KPMG México

Vocero

Rommel García

Socio de Asesoría en Ciberseguridad de KPMG en México

Retos actuales

- Nuestro futuro depende de los datos y la infraestructura digital
- Las tecnologías innovadoras dan forma a ese futuro
- La lista de industrias que consideramos sistémicamente importantes también está cambiando
- A medida que aumenta el grado de interconexión y dependencia, también lo hace el interés de aquellos que buscan atacar y explotar esas infraestructuras

- Con lo anterior, llega un impulso global hacia una mayor regulación de la ciberseguridad
- La ciberseguridad debe ser parte de todas las líneas de negocio, funciones, productos y servicios
- Las organizaciones tienen que empezar a pensar en la ciberseguridad como el hilo dorado que recorre toda su organización

Ocho consideraciones clave de ciberseguridad

01 Digital trust:
Una responsabilidad compartida

02 La seguridad no intrusiva impulsa comportamientos seguros

03 Un futuro sin perímetro y centrado en los datos

04 Nuevas asociaciones, nuevos modelos

05 Confianza en la automatización

06 Asegurar un mundo inteligente

07 Contrarrestar adversarios ágiles

08 Ser resiliente cuándo y dónde sea importante

1. Digital trust: Una responsabilidad compartida

Más de 1/3 de las organizaciones reconoce que a mayor confianza se obtienen mejores resultados en rentabilidad.

65% reporta que los requisitos de seguridad de la información están moldeados por las necesidades de cumplimiento en lugar de las ambiciones estratégicas a largo plazo.

65% de los ejecutivos continúan viendo la seguridad de la información como una actividad de reducción de riesgos en lugar de un facilitador de negocios.

49% creen que el Consejo Directivo ve la seguridad como un costo necesario en lugar de una forma de obtener una ventaja competitiva.

2. La seguridad no intrusiva impulsa comportamientos seguros

Confianza en el CISO

Las organizaciones muestran altos niveles de confianza y una fuerte creencia en la capacidad del CISO para cumplir con tareas cruciales.

79% de las organizaciones confían en que los CISO pueden mapear con precisión dónde se encuentran los datos críticos en toda la empresa

3/4 confían en que los CISO puedan identificar cuáles son sus joyas de datos de la corona

78% confían en que los CISO saben qué parte de sus datos confidenciales están con terceros y que son debidamente protegidos

Aspectos relevantes

- La experiencia del cliente también se aplica a la seguridad
- La tecnología por sí sola no puede resolver el problema.
- Es importante crear una sólida cultura de seguridad en toda la organización

3. Un futuro sin perímetro y centrado en los datos

Confianza cero (Zero Trust) para empresas sin perímetro

Los enfoques de confianza cero pueden ayudar a reducir el radio de afectación en caso de interrupción o violación y limitar el impacto para que el incidente pueda gestionarse y contenerse mejor.

La seguridad de los datos es una cuestión clave para las partes interesadas

En un entorno sin perímetro, las preocupaciones sobre cómo se protegen, utilizan y comparten los datos son los principales factores que socavan la confianza de las partes interesadas en la capacidad de una organización para utilizar y gestionar sus datos.

28% de los directivos considera que "la falta de confianza en los mecanismos de gobernanza existentes" es uno de los principales factores que socavan la confianza de las partes interesadas en el uso y la gestión de sus datos

32% señala "la falta de claridad sobre por qué se necesitan datos para un servicio concreto y las ventajas de compartir o facilitar datos"

36% le preocupa la protección de sus datos

35% se preocupan por cómo se utilizan o comparten sus datos

4. Nuevas asociaciones, nuevos modelos

Comunidades de confianza

Se espera que las asociaciones externas también sean vitales para el éxito en ecosistemas hiperconectados, pero las barreras prácticas se interponen en el camino de la colaboración.

Aspectos clave

- Saber qué retener
- Encontrar la combinación adecuada de habilidades

79% dice que la colaboración constructiva con proveedores y clientes es vital, sin embargo; solo **42%** dice hacerlo

60% admite que las cadenas de suministro son los principales fuentes de vulnerabilidades

78% de los ejecutivos confían en que el CISO puede proteger sus datos en toda la cadena de suministro

5. Confianza en la automatización

Existen crecientes preocupaciones sociales y empresariales sobre las implicaciones éticas, de seguridad y privacidad de la adopción de soluciones de inteligencia artificial (IA) y *machine learning (*ML) para el análisis de *big data*.

Aspectos clave

- Construyendo modelos de IA confiables
- IA y privacidad de los datos

78%

está de acuerdo en que la IA y el ML traen desafíos únicos de ciberseguridad.

3 de 4 dice que la IA y el ML plantean cuestiones éticas fundamentales.

76% de los ejecutivos están de acuerdo en que la adopción de IA / ML requiere salvaguardas sobre cómo se entrenan y monitorean los sistemas de IA / ML.

6. Un mundo inteligente y seguro

5G

Ofrece velocidad, hiperconectividad y latencia reducida

Procesamiento cuántico

Reduce significativamente el tiempo de procesamiento y cálculo

Arquitecturas de confianza

Ayuda a garantizar que los datos y las identidades sean seguros y fiables de un dispositivo conectado a otro

Software 2.0

Código rápido escrito con IA que puede reducir la complejidad al tiempo que aumenta la velocidad de desarrollo de meses a semanas

IA Aplicada

La aplicación de la inteligencia artificial es fundamental como soporte de desarrollo de productos inteligentes.

La creciente experiencia con los retos de la ciberseguridad también está dando a los CEOs una idea más clara de lo preparados -o poco preparados- que pueden estar.

24% de los CEO reconocen que no están suficientemente preparados para un ciberataque, frente al 13% en 2021.

56% afirman estar preparados.

3/4 afirman que su organización dispone de un plan para hacer frente a los ataques de *ransomware*.

3 de 4 CEOs afirman que proteger a sus socios es tan importante como reforzar las ciberdefensas de su organización.

7. Contrarrestar a adversarios ágiles

Los equipos de ciberseguridad están luchando para mantenerse al día

Los equipos de ciberseguridad están bajo presión para mantenerse al día con las amenazas en evolución y la escasez de talento, con frecuencia deshabilitando los esfuerzos de seguridad.

Más de la mitad

de las organizaciones admiten que están atrasadas con su posición sobre ciberseguridad.

Más del 50%

tienen mucha o extrema confianza en la lucha contra diversas amenazas cibernéticas, incluidos los grupos del crimen organizado, personas con información privilegiada y cadenas de suministro comprometidas.

59%

están de acuerdo en que los atacantes están explotando vulnerabilidades en las adquisiciones y la cadena de suministro, pero no saben si sus defensas son lo suficientemente fuertes como para evitar que sean vulnerados.

#1

El desafío interno para lograr los objetivos de ciberseguridad es la falta de habilidades clave (40%).

8. Ser resiliente - cuándo y dónde es importante

Perspectivas regulatorias

Los legisladores y reguladores están prestando mayor atención, aumentando las demandas de transparencia y supervisión. Muchas organizaciones están preocupadas por navegar por un panorama regulatorio global cada vez más complejo.

- Se requiere coordinación proactiva dentro y fuera de la batalla
- Recuperándose a su negocio mínimo viable
- El papel de la regulación en la resiliencia

36%

se preocupa por su capacidad para cumplir con la regulación de ciberseguridad existente o nueva cuando las actividades se subcontratan a proveedores de servicios digitales.

31%

se preocupa por las crecientes demandas en torno a la infraestructura critica, que es objeto de una creciente regulación en el Reino Unido, la UE y los Estados Unidos.

93%

muestra preocupación por la regulación existente o nueva relacionada con la resiliencia de los sistemas clave.

26%

aseguran estar preocupados por los requisitos de notificación de incidentes más estrictos

Conclusiones

1. Personas

- Priorizar una cultura de ciberseguridad sólida que sea interesante, atractiva y, cuando corresponda, divertida para inspirar a los empleados a hacer lo correcto y funcionar como cortafuegos humanos
- Crear un equipo de seguridad con la combinación de habilidades necesarias para administrar una organización sin perímetro, incluidas las dependencias de la nube y de terceros
- Comunicarse de manera amplia y clara. Pregunte a los líderes de otras funciones organizacionales sobre sus puntos débiles y cómo podrían ayudar los procesos automatizados
- Adoptar un enfoque multidisciplinario e intercultural. Establecer un ecosistema de seguridad compuesto por especialistas internos de la línea de negocios, profesionales de la seguridad, científicos de datos, abogados orientados a la privacidad y profesionales externos de la industria y las políticas
- Insertar en la organización y actuar como un compañero, una caja de resonancia y un asesor

Conclusiones

2. Proceso

- Desarrollar enfoques consistentes para la gestión de riesgos cibernéticos con una comprensión de los escenarios de amenazas y las rutas de ataque
- Informar la reducción de la superficie de ataque y priorizar las mejoras de control.
- Concentrarse en procesos de seguridad adecuados para su propósito que presenten experiencias de usuario consistentes.
- Establecer controles de identidad estrictos y trabaje para lograr un estado maduro de servicios y gobernanza de identidad.
- Segmentar los entornos heredados para limitar la superficie de ataque y ayudar a contener cualquier infracción.
- Tener un plan de recuperación proactivo que se centre en los flujos de trabajo más críticos de la organización con una estructura de comunicación

Conclusiones

3. Datos y tecnología

- Adoptar la inevitable automatización
- Confiar en las herramientas más recientes, como procesos robóticos, orquestación de seguridad, automatización y respuesta (SOAR) y sistemas de detección y respuesta extendida (XDR).
- Trabajar con proveedores de la nube para ayudar a garantizar una amplia visibilidad de cómo se configuran los productos y servicios para evitar vulnerabilidades involuntarias.
- Considerar los problemas de seguridad cibernética y privacidad desde el principio cuando explore tecnologías emergentes, incluidos los riesgos en evolución asociados con la adopción de sistemas de IA.
- Asignar responsabilidades y establezca responsabilidades sobre cómo se procesan y administran los datos críticos y cómo respaldan los procesos comerciales críticos.
- En aras de la velocidad, la escalabilidad y la confianza, la transición a la identidad como servicio en la nube debe ocurrir lo antes posible.

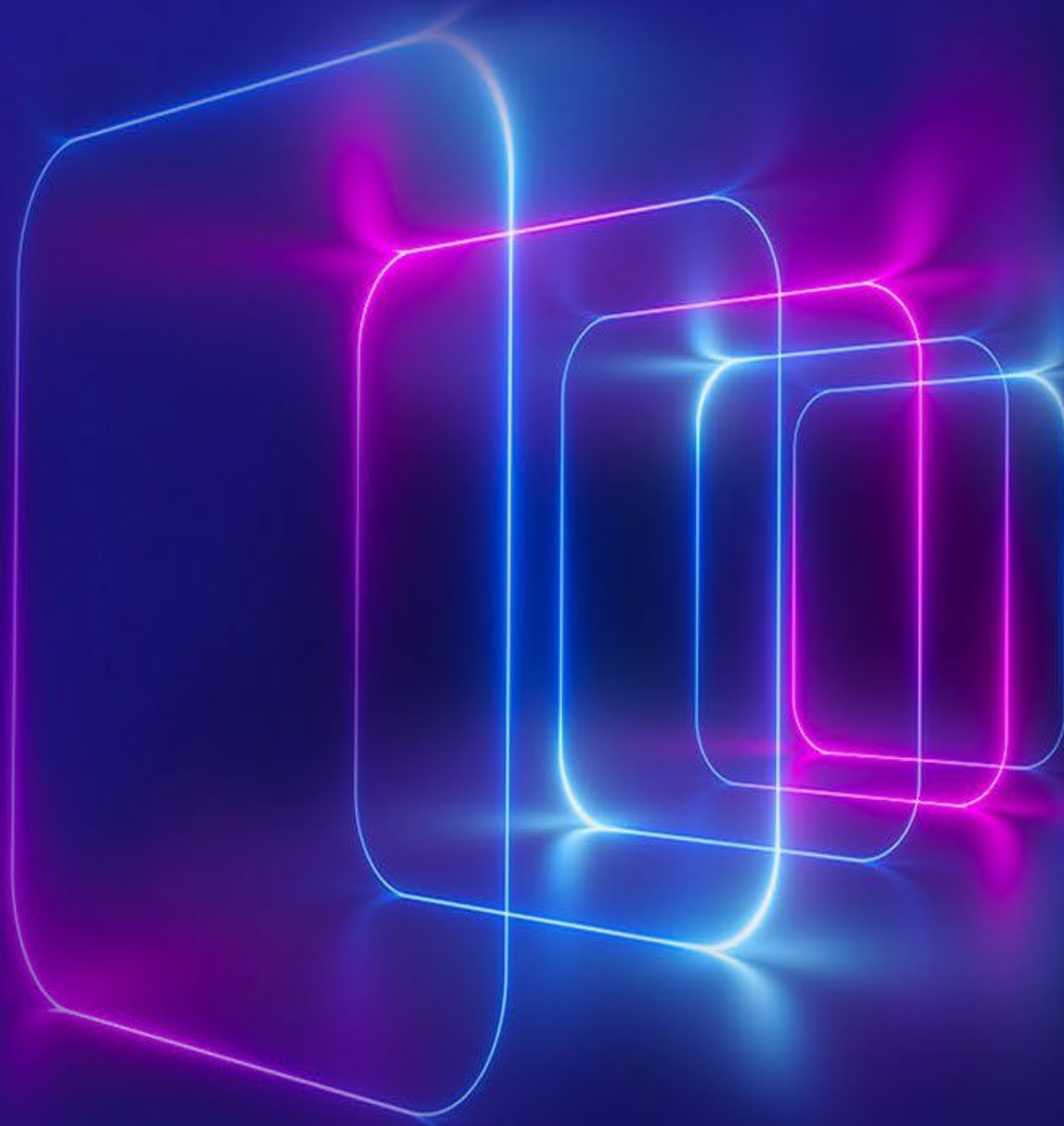
Conclusiones

4. Regulaciones

- Monitorear las tendencias e impulsores normativos y lo que podrían significar para la futura estrategia tecnológica, el desarrollo de productos y las operaciones de la empresa.
- Considerar los impactos regulatorios en relación con la IA y la automatización: establecer un concepto claro de lo que la empresa puede y no puede hacer en estos ámbitos y esté atento a las preocupaciones del público y las expectativas cambiantes.
- Explorar la automatización del monitoreo y los informes de cumplimiento y monitorear para mantenerse al tanto de las tendencias regulatorias de privacidad y seguridad.
- Alinear la estrategia de cumplimiento de la seguridad y la privacidad con la estrategia comercial amplia de la empresa para ayudar a garantizar que las partes interesadas de toda la organización estén en sintonía.
- Mirar más allá de la letra de la regulación y prepararse para hacerse preguntas más fundamentales sobre la confianza digital y cómo hacer que sea central para su pensamiento estratégico.

Gracias

Abril 2023
KPMG México



Metodología

Encuesta realizada entre mayo y junio de 2022 por KPMG International

Fueron entrevistados 1,881 ejecutivos y a 5 líderes de corporativos, alrededor del mundo

1,881 participantes

42% Nivel C o superior

5 líderes de corporativos

Preguntas y respuestas

Rommel García

Socio de Asesoría en Ciberseguridad de KPMG en México

KPMG

KPMG MÉXICO KPMG MÉXICO @KPMGMEXICO KPMGMX