KPMG

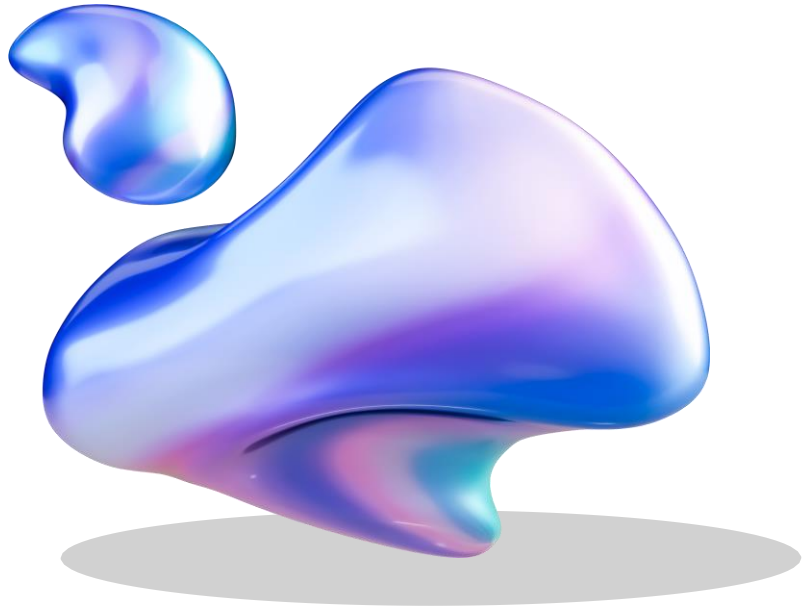
#CyberWatch:
Edición Abril 2023

KPMG en Chile

—

Abril 2023

Contenido



01
Chat GPT: Desafíos que presentan los avances en IA

Chat GPT: Desafíos que presentan los avances en IA

ChatGPT es una plataforma de chat gratuita basado en el modelo de lenguaje por IA GPT-3, desarrollado por la empresa OpenAI. Lanzada a finales del 2022, la plataforma en 2 meses ya cuenta con más de 100 millones de usuarios activos según el Union Bank of Switzerland (UBS). Las razones por las cuales esta plataforma de IA está teniendo un alto impacto, es que le puedes preguntar y solicitar gran variedad de contenido, con un alto nivel de redacción y eficiencia comparado con otros chatbots y asistentes virtuales actuales.

Esta herramienta permite realizar solicitudes para traducir textos, generar cuentos, artículos, poemas, entre otros. En este sentido, las organizaciones están buscando explotar el potencial que tiene esta IA para automatizar tareas, buscar información y optimizar procesos en sus contextos de negocio, sin dejar de lado la validación de la información entregada ya que a veces entrega información errónea.

Otro punto relevante del Chat GPT es la capacidad de generar scripts en distintos lenguajes de programación, por lo que el desarrollo de este tipo de herramientas también aumenta el riesgo en el contexto de la ciberseguridad. Si bien Chat GPT no es una herramienta preparada para generar ciberataques por si sola o brindar la información precisa para realizar uno, podría brindar metodologías a aquellas personas especializadas en materia de ciberseguridad.

Una encuesta realizada por KPMG en el 2022 evidencia que el 78% de los profesionales está de acuerdo que la IA y ML traerán nuevos desafíos en materia de ciberseguridad. En este sentido, un 51% de los expertos TI creen que habrá ciberataques potenciados por Chat GPT durante este año (Forbes, 2023).

¿Qué riesgos implica esta tecnología desde el punto de vista de potenciales hackers?

Si bien Chat GPT cuenta con una política de contenido que previene la entrega de información que puede ocasionar daño o efectos no éticos, este filtro puede ser evitado con métodos de insistencia, instrucciones precisas y/o acceso a través de la API. Algunas de las prácticas que Chat GPT podría facilitar, en su mayoría, a personas con intensiones maliciosas son:

1. Phishing: La capacidad de creación de texto de Chat GPT permitirá a los hackers utilizar textos sin problemas de redacción y ortografía, logrando evitar el principal filtro que se utiliza para detectar correos maliciosos.
2. Fake news: La capacidad de redacción del Chat GPT permitirá elaborar, rápidamente y sin esfuerzo, textos cuyo contenido puede ser falso, impulsando la presencia de fake news en internet.
3. Automatizar códigos maliciosos: Al hacer consultas continuas, se puede recibir un código único cada vez, haciendo posible crear un programa polimórfico que sea altamente evasivo y difícil de detectar.
4. Encontrar vulnerabilidades en los sistemas informáticos: Chat GPT está alimentado de una gran base de datos, por lo que también puede ser utilizado por los hackers para identificar los sistemas que han presentado vulnerabilidades.
5. Suplantación de identidad: Se le puede entregar una serie de textos redactados por una persona determinada al Chat GPT para luego solicitar que genere un texto determinado con ese estilo de redacción.
6. Optimizar códigos: Un hacker puede solicitar la detección de errores en un código y la optimización de ciertas partes de un programa.

¿Qué riesgos implica utilizar esta tecnología desde las organizaciones?

1. Ética: La IA de esta herramienta es poderosa, pero puede ser perjudicial para los individuos si la toma de decisiones automatizada es involuntariamente sesgada o discriminatoria.
2. Sesgo no intencional: Algunas respuestas de Chat GPT pueden mostrar sesgos. Algunos ejemplos en Twitter muestran que los usuarios han logrado evitar los filtros de Chat GPT y proporcionar respuestas que pueden ser parciales. Dado que Chat GPT ha sido entrenado con información disponible públicamente, es probable que algunas respuestas tengan un sesgo no intencional.
3. Información incorrecta: La información controvertida (fake news) a menudo tiene más probabilidades de volverse viral que la información regular. Como resultado, Chat GPT puede proporcionar resultados incorrectos si la base de conocimiento subyacente es defectuosa.
4. Errores lógicos: Chat GPT ha fallado en responder correctamente preguntas lógicas y acertijos simples. Por ejemplo, Chat GPT no puede deducir una respuesta a partir de: "Si mi hermana tenía la mitad de mi edad cuando yo tenía seis años, ¿cuántos años tendría ella cuando yo tenga 70?".
5. Información obsoleta: Chat GPT a veces proporcionará información incorrecta aunque nuevos hechos corrijan la información anterior. El modelo actual está entrenado utilizando información disponible hasta 2021. Aunque el modelo destaca este hecho, en algunos escenarios puede proporcionar información incorrecta.
6. Información confidencial: La información contenida en las solicitudes que se hagan al Chat GPT es recopilada y utilizada para mejorar el modelo de la herramienta.

¿Qué medidas de protección pueden tomar las empresas frente al Chat GPT?

A medida que las organizaciones exploran casos de uso para nuevas y potentes soluciones de inteligencia artificial como Chat GPT y otras, es fundamental que los equipos de ciberseguridad y riesgos establezcan límites para una implementación segura. A continuación, se presentan algunos pasos para ayudar a anticipar la implementación de este tipo de herramientas:

1. Establecer expectativas sobre cómo se deben utilizar Chat GPT y soluciones similares en un contexto empresarial. Desarrollar políticas de uso aceptable, definir una lista de todas las soluciones aprobadas, casos de uso y datos en los que el personal pueda confiar, y requerir que se establezcan controles para validar la precisión de las respuestas.
2. Establecer procesos internos para revisar las regulaciones sobre el uso de soluciones de automatización cognitiva, en particular la gestión de la propiedad intelectual, los datos personales y la inclusión y la diversidad cuando corresponda.
3. Educar a su personal sobre los beneficios y riesgos de usar estas soluciones de IA, incluidos casos de uso adecuados y la importancia de entrenar el modelo con conjuntos de datos confiables.
4. Implementar controles técnicos de ciberseguridad, prestando especial atención a la prueba de código para la resistencia operativa y la detección archivos maliciosos. Otros controles incluyen, pero no se limitan a:

- Autenticación multifactorial y el acceso solo a usuarios autorizados.
- Aplicación de soluciones de prevención de pérdida de datos (DLP).
- Procesos para garantizar que todo el texto producido por la herramienta sea revisado de forma estándar y no se pueda copiar directamente en entornos de producción.
- Configuración del filtrado web para proporcionar alertas cuando el personal accede a soluciones no aprobadas.

5. Evitar incluir información confidencial o datos personales al realizar solicitudes.

Privacidad en IA

Dado el creciente uso de herramientas como Chat GPT, es necesario tener una framework de gobernanza para las soluciones de IA que se utilizan y desarrollan dentro de la organización. En este sentido, KPMG define 4 principios fundamentales para una implementación exitosa de una herramienta IA:

- Integridad del algoritmo: tener confianza en el set de entrenamiento, procesos y métricas utilizadas para desarrollar y evaluar herramientas IA.
- Explicabilidad: conocer cómo y por qué genera un resultado determinado.
- Igualdad: utilizar set de datos relevantes y genera resultados transparentes libre de sesgos basados en características como raza, género o situación financiera.
- Resiliencia: resistir interferencia externa que genera insights incorrectos o malas decisiones.

Los beneficios de Chat GPT son claros y su introducción acelerará la adopción de la IA en los negocios y la sociedad. Pero para maximizar sus beneficios, acelerar el crecimiento de su empresa y mantener la confianza digital, es fundamental un uso responsable de Chat GPT y otros modelos de IA generativos.

Referencias

Does ChatGPT Pose A Cybersecurity Threat? I Asked The AI Bot Itself (forbes.com)

Chat GPT: ¿Un enemigo para la ciberseguridad? - Resguarda

Chatting Our Way Into Creating a Polymorphic Malware (cyberark.com)

Building trust in AI is a shared responsibility (kpmg.us)

privacy-principles-and-ai.pdf (kpmg.us)

02
Zero Trust

Zero Trust

Las organizaciones actuales han adoptado diversas modalidades, como Bring Your Own Device (BYOD) y entornos híbridos que permiten la conexión y trabajo remoto de colaboradores, clientes, proveedores y otros terceros. Estos cambios son necesarios, sin embargo, también generan una necesidad de adaptación en la estrategia de ciberseguridad. Debido a la ampliación de la superficie de ataque y la falta de un perímetro definido asociado a los puntos de acceso para usuarios y dispositivos, se requieren medidas de seguridad adicionales para garantizar la conectividad remota y la protección de los datos.

Natasha Passley, Socia de Ciberseguridad KPMG Australia, explica: “El enfoque de seguridad perimetral tradicional está obsoleto en nuestro mundo interconectado y digital. Los CISO tienen que proteger una superficie de ataque mucho más amplia en toda la infraestructura pública y privada y en un ecosistema de usuarios distribuidos. Como resultado, los CISO deben esforzarse por permitir que el negocio proporcione seguridad desde cualquier lugar, con cualquier dispositivo y de manera confiable.”

En este contexto, el 28% de los ejecutivos identifica la baja confiabilidad en los mecanismos de gobernanza como el principal factor que disminuye la confianza sobre el uso y gestión de los datos por parte de las organizaciones. Mientras que un 36% está preocupado en cómo están siendo protegidos sus datos.

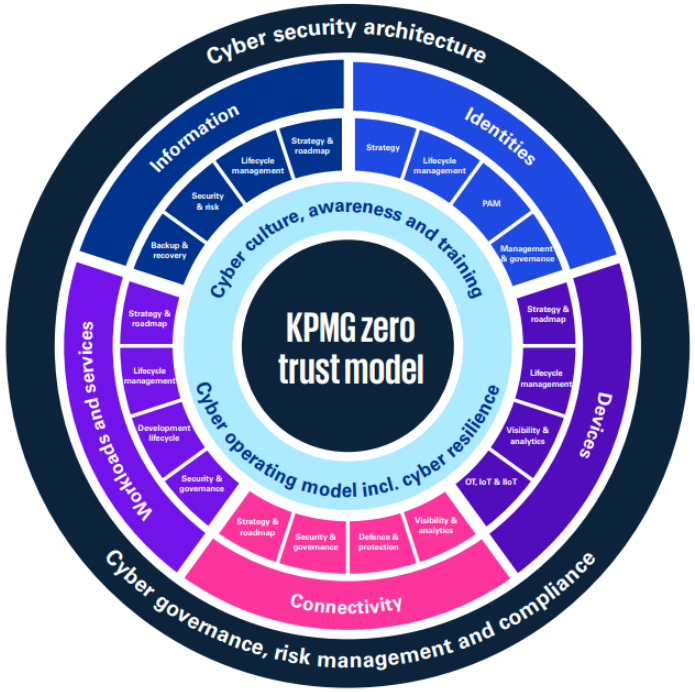
Zero Trust (Confianza Cero) es un enfoque para diseñar e implementar medidas de seguridad. Su definición se basa en creer que todo lo que se encuentra detrás del firewall corporativo no es seguro, el modelo de Zero Trust presupone que hay brechas y, por consiguiente, comprueba todas las solicitudes como si provinieran de una red no controlada. Independientemente del lugar en el que se origine la solicitud o del recurso al que acceda, el modelo de Zero Trust enseña a no confiar nunca y a realizar siempre todas las comprobaciones pertinentes.

3 Principios fundamentales

1. Verificación explicita: Realizar las operaciones de autorización y autenticación en función de todos los puntos de datos disponibles.
2. Acceso con privilegios mínimos: Limitar el acceso de los usuarios con los modelos Just-In-Time y Just-Enough-Access (JIT/JEA), directivas que se adaptan al nivel de riesgo y protección de datos
3. Asumir nada, supuesto de que hay brechas: Minimizar la superficie de ataques y movimientos laterales. Comprobar el cifrado de un extremo a otro y usar análisis para obtener visibilidad, impulsar la detección de amenazas y mejorar las defensas.

Metodología KPMG

KPMG ha desarrollado distintos modelos, basado en los resultados del análisis de brechas y las mejores prácticas modernas para complementar las estrategias de ciberseguridad de las distintas organizaciones, Zero Trust no es un enfoque único para implementar un marco de ciberseguridad, ni tampoco una tecnología única. Es por esto que a la hora de escoger la más adecuada, es importante establecer los lineamientos generales de la entidad e identificar los puntos a mejorar, las metas y objetivos, además de sus proyecciones a futuro, así se podrá tener una idea general hasta que nivel pueden acogerse a este modelo o incorporarlo como una medida adicional de prevención ante amenazas.



¿Qué beneficio entrega a nuestros clientes?

1. Escalabilidad rápida y agilidad: El uso de una arquitectura, principios y guías de Zero Trust permite adoptar de manera segura servicios en la nube para uso empresarial e innovación.
2. Intercambio de información sin interrupciones: El marco y los principios de Zero Trust permiten intercambiar información de manera segura con terceros, así como también obtener servicios tercerizados de manera segura.
3. Mentalidad ciberseguridad: Incorporar una mentalidad de Zero Trust promueve una mentalidad de seguridad común, responsabilidad y responsabilidad compartida para mantener la seguridad y reducir los incidentes centrados en el usuario.
4. Adopción segura de tecnología digital: El uso de un marco de Zero Trust permite reducir la complejidad del control, mejorar la efectividad y reducir el costo de los controles asociados con la transformación digital.
5. Cadena de suministro segura: La obtención de servicios compatibles con los principios de Zero Trust proporciona una postura de seguridad general mejor al reducir su exposición a riesgos y vulnerabilidades de terceros.
6. Reducción de sobrecarga operativa: El uso de tecnologías habilitadas para Zero Trust ayuda a reducir la carga en las operaciones de seguridad al proporcionar una mejor visión de los incidentes y la capacidad de respuesta automatizada.

Referencias

https://learn.microsoft.com/es-es/security/zero-trust/zero-trust-overview

https://deliverybackbone.kpmg.com/collaboration/display/MTLDir/Cybersecurity+considerations+2023+%7C+The+golden+thread

03
Los nuevos desafíos de la ciberseguridad Industrial

Los nuevos desafíos de la ciberseguridad Industrial

Nos dirigimos hacia una nueva realidad para la seguridad cibernética en la industria. Los eventos de este año han interrumpido los mercados y las cadenas de suministro, han forzado un cambio importante en los modelos operativos y han exacerbado las tensiones políticas. En medio de esto, nos enfrentamos a un futuro de amenazas de seguridad cibernética implacables y cada vez más sofisticadas que exigen que las empresas eleven el nivel de sus medidas de seguridad de sistemas de control mientras lidian con las crecientes presiones de costos. Pero como revelan los resultados de nuestra nueva encuesta, tal vez de manera alarmante, demasiadas empresas siguen estando peligrosamente expuestas a ataques cibernéticos costosos y potencialmente debilitantes.

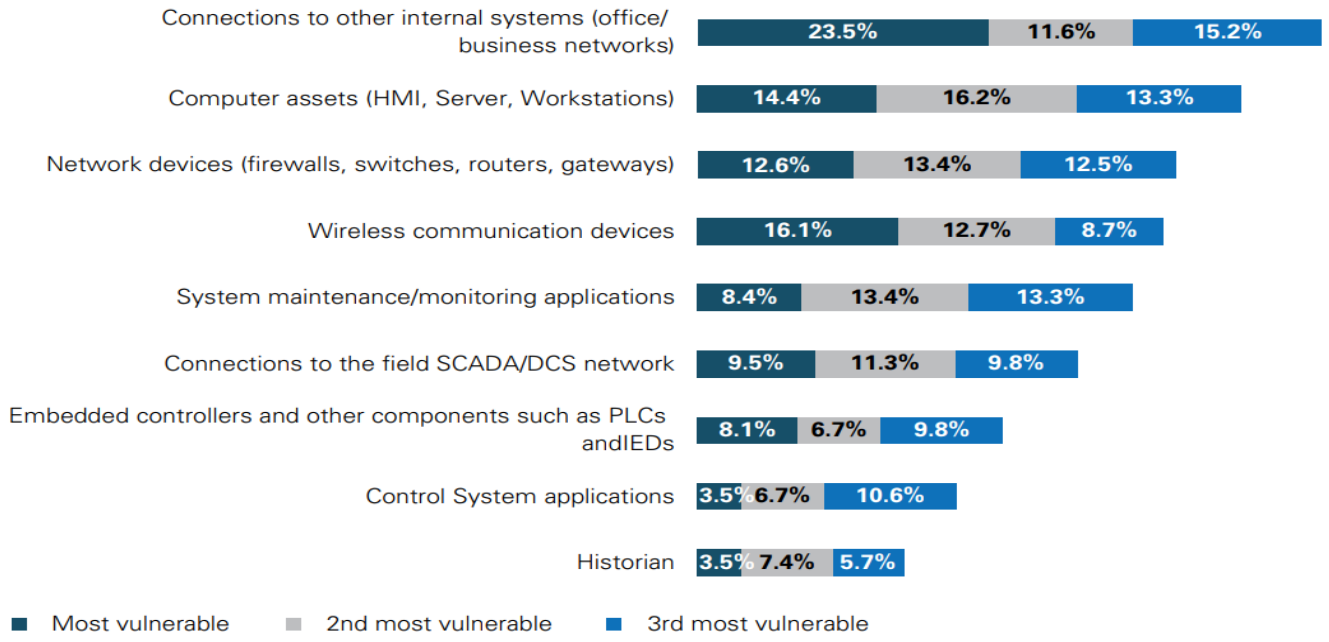
Producido en colaboración con The Control System Cyber Security Association International (CS)2AI, el Informe de la Encuesta de Seguridad Cibernética de Sistemas de Control (CS)2AI-KPMG ofrece una mirada en profundidad al estado de las prácticas de seguridad de los sistemas de control, amenazas y riesgos en el entorno actual de seguridad cibernética cambiante e interminablemente desafiante. Nuestro análisis se basa en los aportes de una muestra representativa de los más de 16,000 miembros de la Asociación Internacional de Seguridad Cibernética del Sistema de Control, profesionales en la primera línea de la seguridad cibernética para todo tipo de sistemas de control.

Los hallazgos clave del informe revelan que las empresas están luchando para resolver las vulnerabilidades de seguridad cibernética en los sistemas de control (CS) y los entornos de tecnología operativa (OT). Los hallazgos notables incluyen:

- Menos del 25% de las empresas han incorporado una defensa activa de sus sistemas de control y activos.
- El 58% de los encuestados identificó la insuficiente experiencia en seguridad de CS como un obstáculo, seguido de personal insuficiente (48%), los requisitos de tiempo de actividad operativa (44%), la falta de recursos financieros (37%) y el apoyo de liderazgo inadecuado (35%).
- El 47% de los programas de seguridad de CS maduros utilizan servicios de seguridad de CS gestionados frente al 6% de los programas menos maduros.
- El 53% de los programas de seguridad de CS maduros realizan evaluaciones de seguridad de extremo a extremo con más frecuencia que los programas menos maduros (36%).

Riesgos en los componentes de sistema de control.

Cualquiera sea el progreso que se haya hecho en la obtención de sistemas en el último año, nuestros encuestados continúan teniendo en cuenta conexiones a otros sistemas internos (redes de oficina/negocio) y activos informáticos (HMI, servidor, estaciones de trabajo) como los componentes de sistema de control más susceptible de compromiso. Los dispositivos de comunicaciones inalámbricas recibieron casi un 50% más de atención que hace un año, sugiriendo una mayor conciencia de la proliferación de dispositivos inalámbricos inseguros o débiles sobre ese período.



Las primeras 72 horas son críticas

KPMG ha sido testigo que una falta de planificación sólida y capacidades a la hora de hacer copias de seguridad, sumado al costoso impacto durante el tiempo de recuperación, hace urgente la necesidad de una pronta recuperación. Sin embargo, demasiadas organizaciones asumen erróneamente que la recuperación se dará durante las primeras semanas, y la realidad es que esto puede tardar hasta varios meses. Esto porque a la hora de identificar, y a la hora de responder al incidente, la respuesta tiende a ser lenta.

Cuando se produce un ataque, las 72 horas iniciales son críticas, pero nunca fáciles para los dirigentes, presas del pánico, que se ven envueltos en un escenario catastrófico que exige negociar con un grupo de delincuentes, mientras se intenta tomar las mejores decisiones para evitar mayores daños.

La necesidad de programas de recuperación en industrias OT se ha hecho indispensable. Estos programas deben incluir el entorno completo en términos de procesos y activos críticos, capacidades de soporte y copia de seguridad, y los pasos necesarios para restablecer rápidamente las operaciones. Los roles y responsabilidades deben estar claramente definidas. Este programa de recuperación también debe contener un plan de comunicación con todas las partes interesadas.

Las organizaciones deben entender que la recuperación en OT presenta retos únicos que deben ser abordados y de acuerdo al contexto estos varían según la industria.

Detener los sistemas o desconectar elementos de la red no siempre es factible en OT, dado que este puede controlar sistemas críticos y/o procesos físicos sensibles.

Un enfoque demasiado simplista de recurrir a la operación manual durante una crisis puede resultar imposible por muchas razones. Un ejemplo de esto son las bodegas automatizadas, las cuales no cuentan con el personal para la entrega manual. En este sentido, un distribuidor eléctrico puede no tener personal cualificado en operaciones manuales al momento de la falla.

Recomendaciones de KPMG

Hay algunos conceptos clave que sugieren nuestro alcance a asegurar su entorno CS. En primer lugar, la seguridad es una búsqueda continua. El estado ideal de estar completamente seguro es sólo hipotético y probablemente no alcanzable en el mundo de hoy. Derivado de eso, damos por sentado que la misión principal de la seguridad es gestionar el riesgo, es decir, reducirlo a niveles aceptables. Los parámetros de esta misión son establecidos por los líderes de la organización, que definen la tolerancia al riesgo y deben proporcionar los recursos necesarios para alinear los riesgos con ese apetito.

La ausencia de una solución de "talla única" limita la especificidad de las recomendaciones para guiar a esos líderes, pero podemos sugerir y sugerimos que cada organización persiga algunos objetivos básicos en la medida de lo posible:

Desarrolle su fuerza laboral, a través de capacitación, educación y creación / mejora de una cultura de seguridad dentro de su organización. Esto reducirá el riesgo de ocurrencia de incidentes, impactos y tiempo de recuperación.

Aumente su visibilidad de los entornos de su sistema de control mejorando el inventario de activos y la supervisión de la actividad del tráfico de red. Esto reducirá la probabilidad y duración de las interrupciones.

Segmente sus sistemas de control, tanto de redes no operativas como, cuando sea posible, entre sí. Esto reducirá el alcance de los incidentes al limitar su capacidad de propagación.

Proporcione la seguridad de su cadena de suministro e implemente controles alrededor de los puntos de entrada de sus entornos. Esto podría reducir el potencial de ataques en sus proveedores que puedan impactarlo.

Referencias

(CS)2AI - KPMG Control System Cyber Security Annual Report 2022

Reports | Find all CS2AI Report Publications Here

Contactos KPMG en Chile

Erick Palencia
Managing Director
erickpalencia@kpmg.com
KPMG en Chile

Felipe Palma
Gerente Senior
felipepalma@kpmg.com
KPMG en Chile

María Lobos
Gerente ITA MC
mlobos@kpmg.com
KPMG en Chile

Yoislender Martinez
Gerente ITA MC
yoislendermartinez@kpmg.com
KPMG en Chile

Este material ha sido preparado por KPMG únicamente para proporcionar educación profesional continua. Este material no debe ser utilizado para referencia de uso.

- La información contenida en esta presentación y sus anexos son de naturaleza general y no está dirigido a ninguna circunstancia en particular de cualquier individuo o empresa. Aunque hacemos el mejor esfuerzo para proveer información oportuna y exacta, no puede haber garantía que tal información es exacta a la fecha o que continuará siendo exacta en el futuro.
- Continuos cambios en la literatura técnica causarán reiterados cambios en los requerimientos de información financiera. Este documento está preparado en base de las normas NIC/NIIF vigentes al 29 de marzo de 2023. En consecuencia, será responsabilidad del Cliente revisar y actualizar periódicamente el contenido de las materias tratadas en esta actividad de capacitación.
- Nadie debe actuar sobre esta información sin la debida asesoría profesional luego de un examen exhaustivo de la situación en particular.
- KPMG y el logotipo de KPMG son marcas registradas usadas bajo licencia por las firmas miembro independientes de la organización global de KPMG.

Clasificación de Documento: Público