Gobierno de la IA facilitado por la tecnología

Un enfoque práctico para la gobernanza, el riesgo y los controles

Cuando se trata de aplicaciones de inteligencia artificial (IA), en particular del uso de inteligencia artificial generativa (IAGen), la seguridad y el cumplimiento normativo se están convirtiendo en una prioridad absoluta. Actualmente, a medida que aumenta la demanda regulatoria sobre la función de gobierno, riesgo y cumplimiento (GRC), los directores de tecnología (CTO, por sus siglas en inglés), información (CIO, por sus siglas en inglés) y seguridad de la información (CISO, por sus siglas en inglés) se enfrentan a un mayor escrutinio. Esto representa un cambio significativo en la forma en que se gobierna la tecnología de IA, propiciando un futuro en el que esta se implemente y utilice de manera responsable, ética y eficiente.

Una nueva dimensión de riesgos, creada en parte por las alucinaciones[1] de la IAGen, las inyecciones rápidas, los conjuntos de datos sesgados y otras amenazas emergentes y en evolución, produce una carga mayor para los responsables de gestionar y mitigar el riesgo en toda la empresa. El equilibrio entre la adopción de la innovación habilitada por esta herramienta tecnológica y los riesgos que introduce se convertirá rápidamente en una alta prioridad para los programas de riesgo empresarial.

¿Cómo pueden las organizaciones adoptar e innovar con IA de forma segura y eficiente mientras se adhieren a los complejos y cambiantes requisitos normativos y las preocupaciones de seguridad?



Una estrategia global de IA se vuelve fundamental, la cual debe regir la forma en que se utilizan las aplicaciones para producir resultados seguros y fiables, así como los datos que se introducen y generan a partir de grandes modelos de lenguaje (LLM, por sus siglas en inglés). Además, el cumplimiento de los requisitos reglamentarios puede fomentar un espíritu de confianza entre las partes interesadas, mientras que la ausencia de confianza puede conducir a una cultura de escepticismo y evitación de riesgos. Así, la creación de un modelo de gobernanza adecuado establece las barreras necesarias para que el talento, los clientes y los inversionistas se sientan más seguros.

Un enfoque centrado en las personas para la gobernanza de la IA

La IA es una herramienta para los humanos. Por ello, las compañías deben tener en cuenta tanto los componentes tecnológicos como la contribución humana al momento de crear su modelo de gobernanza. No basta con que la IA sea segura; su tecnología y usuarios deben estar sujetos a controles que permitan que todas las partes interesadas que puedan verse afectadas por su uso confíen en ella.

KPMG Trusted AI es un enfoque centrado en las personas para gobernar la IA, el cual se basa en prácticas éticas que inspiran un compromiso con la confianza, ayudan a garantizar que las prácticas de datos mantengan los más altos estándares éticos y refuerzan la necesidad de cumplir con la privacidad, las regulaciones de protección de datos y los requisitos de confidencialidad.

[1] *Fenómeno en el que un modelo de IA percibe patrones inexistentes o imperceptibles para los seres humanos, creando resultados sin sentido o inexactos.*

© 2024 KPMG Cárdenas Dosal, S.C., sociedad civil mexicana y firma miembro de la organización mundial de KPMG de firmas miembros independientes afiliadas a KPMG International Limited, una compañía privada inglesa limitada por garantía. Todos los derechos reservados. Prohibida la reproducción parcial o total sin la autorización expresa y por escrito de KPMG.

Nuestro enfoque Trusted AI se basa en diez acciones éticas a lo largo del ciclo de vida de la herramienta:

Equidad
Diseñar soluciones de IA que trabajen activamente para reducir o eliminar los sesgos contra individuos, comunidades y grupos.

Fiabilidad
Ayudar a garantizar que las soluciones de IA funcionen de forma coherente con su propósito, alcance y nivel de precisión deseado.

Transparencia
Hacer que la información pertinente sea accesible para todas las partes interesadas, facilitando una comprensión profunda de las funciones y el rendimiento de las soluciones.

Seguridad
Implementar prácticas sólidas y resilientes apara proteger las soluciones de IA contra malos actores, información errónea o eventos adversos.

Explicabilidad
Dar respuestas al "cómo" y "por qué" de las conclusiones extraídas de las soluciones.

Protección
Crear soluciones de IA que prevengan daños a personas, empresas y propiedades.

Responsabilidad
Incorporar la supervisión y responsabilidad humanas en todo el ciclo de vida de la IA, a fin de gestionar el riesgo y garantizar el cumplimiento de las leyes y normativas aplicables.

Privacidad
Diseñar soluciones de IA que permitan cumplir con las leyes y regulaciones de privacidad y protección de datos.

Integridad de los datos
Asegurarse de que los datos utilizados se alinean con las leyes aplicables y verificaciones periódicas de exactitud, integridad, idoneidad y calidad.

Sostenibilidad
Diseñar soluciones de IA de manera eficiente desde el punto de vista energético para reducir las emisiones de carbono y promover un medioambiente limpio.

Un enfoque tecnológico para la gobernanza de la IA

El marco de KPMG Trusted AI puede combinarse con las capacidades nativas de la plataforma ServiceNow para respaldar la gestión de GRC de las aplicaciones de IA. KPMG incorpora las diez acciones del enfoque de Trusted AI en objetivos detallados de riesgo y control en la *suite* de gestión integrada de riesgos (IRM, por sus siglas en inglés) de ServiceNow para ayudar a las organizaciones a adoptar la IA de forma segura y ética. Este enfoque ayuda a los clientes a centrarse en la creación de una sólida biblioteca de controles con actualizaciones periódicas e indicadores automatizados a medida que las soluciones de gestión de IA evolucionan y difieren entre las empresas.

El uso de ServiceNow para habilitar el marco de referencia de KPMG Trusted AI crea un espacio de trabajo interactivo e integrado para gestionar los componentes de gestión de riesgos de IA, las clases de inventario de activos y de la base de datos de la gestión de configuración (CMDB, por sus siglas en inglés), los perfiles de casos de uso de IA y otras capacidades básicas de la plataforma.

La asignación de todos los requisitos de gobernanza, en conjunto con las soluciones de ServiceNow, permite a los clientes gestionar sistemáticamente su inventario de modelos de IA y su gobernanza, así como el seguimiento de riesgos, la automatización del flujo de trabajo, la auditabilidad, la transparencia y la trazabilidad.

© 2024 KPMG Cárdenas Dosal, S.C., sociedad civil mexicana y firma miembro de la organización mundial de KPMG de firmas miembros independientes afiliadas a KPMG International Limited, una compañía privada inglesa limitada por garantía. Todos los derechos reservados. Prohibida la reproducción parcial o total sin la autorización expresa y por escrito de KPMG.

Gobernanza y controles regulatorios

Activos

Integraciones

Plataforma principal de ServiceNow

1

CMDB y gestión de activos

Se encarga de la gestión del inventario de modelos, el proceso de certificación y la gestión de roles de gobernanza, así como de las aplicaciones a las que sirven, sus respectivos ciclos de vida y costos operativos.

2

IRM/GRC *Suite*

Gestiona el seguimiento de riesgos y problemas, además de la automatización del flujo de trabajo.

3

Motor de aplicaciones

Impulsa un espacio de trabajo centralizado que concentra informes, flujos, diseños de procesos, nuevas clases de elementos de configuración (CI, por sus siglas en inglés) y activos, así como métricas y otras funciones adaptadas a la empresa.



Al combinar un marco digitalizado de Trusted AI con las funciones de ServiceNow, los clientes pueden simplificar, optimizar y automatizar varios aspectos de su gobernanza de IA, permitiendo una toma de decisiones más ágil y la atención de los requisitos internos de cumplimiento. Con medidas eficaces de gestión de riesgos, los CTO, CIO, CISO y líderes de riesgos (CRO, por sus siglas en inglés) pueden demostrar que la IA se está aplicando de forma responsable y ética, lo que ayuda a ganarse la confianza de reguladores, inversionistas, colaboradores, terceros y clientes.

Contactos

Abraham Espinosa
Socio de Asesoría en Gobierno Corporativo, Riesgo y Cumplimiento
KPMG México

Elias Rivera
Director de Asesoría en Gobierno Corporativo, Riesgo y Cumplimiento
KPMG México

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

KPMG MÉXICO · @KPMGMEXICO · KPMG MÉXICO · KPMGMX

Para mayor información, visite:

Alianzas - KPMG y ServiceNow - KPMG México.

Todos los servicios profesionales son proporcionados por las firmas miembro de KPMG registradas y autorizadas por KPMG International.

A lo largo de este documento, "nosotros", "KPMG", "nos", "nuestro" y "nuestra" se refieren a la organización global o a una o más de las firmas miembro de KPMG International Limited ("KPMG International"), cada una de las cuales es una entidad legal separada.

Es posible que algunos o todos los servicios descritos en este documento no estén permitidos para los clientes de auditoría de KPMG y sus afiliados o entidades relacionadas.

La información aquí contenida es de naturaleza general y no tiene el propósito de abordar las circunstancias de ningún individuo o entidad en particular. Aunque procuramos proveer información correcta y oportuna, no puede haber garantía de que dicha información sea correcta en la fecha en que se reciba o que continuará siendo correcta en el futuro. Nadie debe tomar medidas con base en dicha información sin la debida asesoría profesional después de un estudio detallado de la situación en particular.

© 2024 KPMG Cárdenas Dosal, S.C., sociedad civil mexicana y firma miembro de la organización mundial de KPMG de firmas miembros independientes afiliadas a KPMG International Limited, una compañía privada inglesa limitada por garantía. Todos los derechos reservados. Prohibida la reproducción parcial o total sin la autorización expresa y por escrito de KPMG.