Gestión de riesgos de IA en empresas latinoamericanas:

Enfoque en la ciberseguridad y la transferencia de seguros

Mayo 2024

Introducción

La inteligencia artificial (IA) se destaca como una fuerza transformadora que impulsa la eficiencia operativa, la innovación y la ventaja competitiva en diversas industrias. Las empresas latinoamericanas están aprovechando cada vez más el poder de la IA para mantenerse a la vanguardia. Sin embargo, con gran potencial vienen riesgos inherentes, especialmente en el ámbito de la ciberseguridad. A medida que las empresas de la región integran la IA en sus operaciones, enfrentan desafíos únicos debido a las prácticas de ciberseguridad en constante evolución y a menudo controles tecnológicos insuficientes.

Este artículo, **generado utilizando IA,** tiene como objetivo arrojar luz sobre los riesgos asociados con la adopción de la IA en América Latina y ofrecer estrategias para mitigar estos riesgos. También subraya la importancia del seguro cibernético como un componente vital de un enfoque integral de gestión de riesgos. Curiosamente, aunque este artículo es un producto de la IA, también sirve como un recordatorio significativo de las limitaciones y riesgos de confiar únicamente en contenido impulsado por IA sin supervisión humana.

Gestionando los riesgos de la IA en las empresas latinoamericanas: Enfoque en la ciberseguridad y la transferencia de seguros

Las empresas latinoamericanas están adoptando cada vez más tecnologías de inteligencia artificial (IA) para mejorar sus operaciones, aumentar la eficiencia y obtener una ventaja competitiva. Sin embargo, con esta adopción vienen riesgos inherentes, especialmente en el ámbito de la ciberseguridad. Muchas empresas en la región aún están en proceso de evolucionar sus prácticas de ciberseguridad y pueden carecer de controles tecnológicos robustos. Este artículo explora los riesgos asociados con el uso de la IA en las empresas latinoamericanas, destaca estrategias para mitigar estos riesgos y enfatiza la importancia de buscar la transferencia de seguros como parte de un enfoque integral de gestión de riesgos.

Los riesgos de la IA en las empresas de la región

- **Vulnerabilidades de ciberseguridad**
  A medida que las compañías de América Latina integran la IA en sus sistemas y procesos, se vuelven más susceptibles a las amenazas cibernéticas, como las filtraciones de datos, los ataqueslos ataques de ransomware y la manipulación maliciosa de la IA. La infraestructura de ciberseguridad débil y los recursos limitados para el personal de ciberseguridad exacerban estas vulnerabilidades.

- **Inquietudes sobre la privacidad de los datos**
  Los sistemas de IA a menudo dependen de grandes cantidades de datos para operar de manera efectiva. Sin embargo, el manejo o almacenamiento inadecuados de estos datos pueden dar lugar a violaciones de la privacidad e incumplimiento normativo, especialmente con la introducción de leyes de protección de datos como el Reglamento General de Protección de Datos (General Data Protection Regulation, GDPR), y la LGPD (Lei Geral de Proteção de Dados) en Brasil.
- **Interrupciones operativas**
  Los sistemas de IA, si no se prueban e integran correctamente, pueden provocar interrupciones operativas y tiempo de inactividad. Para las empresas de América Latina, donde la infraestructura tecnológica puede ser menos sólida en comparación con las regiones desarrolladas, estas interrupciones pueden tener implicaciones financieras significativas.

Mitigación de riesgos de IA

- **Medidas de ciberseguridad sólidas**
  Las empresas latinoamericanas deben priorizar la inversión en infraestructura de ciberseguridad, incluidos firewalls, cifrado, sistemas de detección de intrusiones y programas de capacitación para empleados. Las auditorías regulares de seguridad y las evaluaciones de vulnerabilidad son esenciales para identificar y abordar las debilidades.
- **Prácticas éticas de IA**
  Las organizaciones deben implementar pautas y protocolos para garantizar el desarrollo ético y la implementación de sistemas de IA. Esto incluye establecer equipos diversos e inclusivos para diseñar y probar algoritmos, así como un monitoreo continuo para detectar y abordar sesgos.

Planificación de la continuidad del negocio

Las compañías en América Latina deben desarrollar planes sólidos de continuidad del negocio y recuperación ante desastres para minimizar el impacto de las interrupciones operativas relacionadas con la IA. Esto incluye copias de seguridad regulares de datos críticos, redundancia en sistemas y procesos, y protocolos claros para responder a incidentes cibernéticos.

Además de implementar medidas preventivas, las empresas deben considerar transferir su riesgo a pólizas de seguro cibernético que puedan proporcionar protección financiera contra pérdidas que surjan de filtraciones de datos, extorsión cibernética y otros incidentes cibernéticos; el seguro puede mejorar su estrategia de gestión de riesgos y mitigar las consecuencias financieras potencialmente devastadoras de los incidentes cibernéticos. En América Latina, el mercado de seguros cibernéticos evoluciona constantemente para adaptarse a nuevas tecnologías y riesgos emergentes, como la inteligencia artificial (IA). Si bien la cobertura específica para los riesgos relacionados con la IA puede variar según las aseguradoras y los términos de la póliza, algunas compañías de seguros cibernéticos están comenzando a analizar el riesgo y allí habrá una evolución en los seguros antes de lo que pensamos.

A medida que las compañías latinoamericanas continúan adoptando tecnologías de IA, es imperativo que aborden los riesgos asociados, particularmente en el ámbito de la ciberseguridad. Al implementar medidas sólidas de ciberseguridad, cumplir con las prácticas éticas de IA, garantizar el cumplimiento de las regulaciones de protección de datos y desarrollar planes integrales de continuidad del negocio, las empresas pueden mitigar los riesgos que plantea la adopción de IA.

Nota del autor

El artículo aclara que la adopción de tecnologías de IA por parte de las empresas latinoamericanas trae consigo importantes riesgos de ciberseguridad y describe estrategias para mitigar estos riesgos mediante medidas de ciberseguridad robustas, prácticas de IA éticas y una planificación integral de la continuidad del negocio. También destaca la importancia de buscar la transferencia de seguros a través de pólizas de seguro cibernético para protegerse contra posibles pérdidas financieras derivadas de incidentes cibernéticos.

Sin embargo, la naturaleza generada por IA de este artículo también nos enseña sobre los riesgos de depender únicamente de la IA. La crítica de este artículo revela que, si bien la IA puede transmitir mensajes clave y proporcionar valiosos conocimientos, puede carecer de la narrativa atractiva y la relevancia práctica que la supervisión humana puede ofrecer.

La ausencia de ejemplos de la vida real, narrativas convincentes y elementos interactivos en el contenido generado por IA lo hace mucho menos impactante que una conversación con su corredor de seguros.

Puntos clave:

01
Estrategias mejoradas de gestión de riesgos cibernéticos: Desarrollar estrategias integrales para combatir las amenazas cibernéticas y prevenir la pérdida de datos mediante la implementación de medidas robustas de ciberseguridad.

02
Aumentar la participación de la junta y del CEO: Fomentar la participación activa de los ejecutivos de alto nivel en la supervisión de los riesgos cibernéticos para garantizar la alineación con los objetivos de cumplimiento más amplios.

03
Inversiones estratégicas en ciberseguridad: Asignar suficientes recursos y presupuesto para mejorar las medidas de ciberseguridad y gestionar eficazmente los riesgos crecientes asociados con los ataques cibernéticos.

04
Cobertura ampliada y perspectivas globales: Considerar las dinámicas geográficas y buscar perspectivas de diversas regiones para obtener una comprensión más completa de los factores de riesgo cibernético y adaptar las estrategias de gestión de riesgos en consecuencia.

05
Mejorar las estrategias de respuesta a incidentes: Fortalecer los planes de respuesta a incidentes para aumentar la confianza en el manejo eficiente y efectivo de los incidentes cibernéticos.

06
Mejorar la conciencia y la comunicación: Educar a los empleados y a las partes interesadas sobre los detalles de la cobertura de seguros cibernéticos, con especial énfasis en el seguro de directores y administradores (D&O), para cerrar las brechas de conocimiento y mejorar la preparación general para la gestión de riesgos.

07
Aumentar la participación de la junta y del CEO: Fomentar la participación activa de los ejecutivos de alto nivel en la supervisión de los riesgos cibernéticos para garantizar la alineación con los objetivos de cumplimiento más amplios.

Al implementar estas recomendaciones, las empresas pueden mitigar proactivamente los riesgos cibernéticos, mejorar sus prácticas de gestión de riesgos cibernéticos y fortalecer su resiliencia general ante las amenazas cibernéticas persistentes y los riesgos emergentes.

Sin embargo, es crucial reconocer que la IA, aunque es una herramienta poderosa, requiere supervisión humana para asegurar que el contenido sea atractivo, relevante e impactante.

¿Cómo podemos ayudarte?

Dentro de nuestro equipo de FINEX de WTW, contamos con expertos en el tema, que te pueden apoyar.

Contactos:

Rodrigo Flores
Regional Cyber Manager LatAm
M: + (52) 55 4383 8517
rodrigo.flores@wtwco.com