



Gestión de riesgos de IA en empresas latinoamericanas:

Enfoque en la ciberseguridad y la
transferencia de seguros

Mayo 2024

Introducción

Las compañías latinoamericanas están adoptando cada vez más tecnologías de Inteligencia Artificial (IA) para mejorar sus operaciones, mejorar la eficiencia y obtener una ventaja competitiva. Sin embargo, con esta adopción vienen riesgos inherentes, particularmente en el ámbito de la ciberseguridad. Muchas empresas de la región aún están en proceso de desarrollar sus prácticas de ciberseguridad y pueden carecer de controles tecnológicos sólidos. Este artículo explora los riesgos asociados con el uso de la IA en organizaciones de Latinoamérica, destacando las estrategias para mitigar estos riesgos y enfatizando 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 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.

Conclusión

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.

Además, buscar la transferencia de seguro, a través de pólizas de seguro cibernético, puede proporcionar una capa adicional de protección contra posibles pérdidas financieras. Al adoptar un enfoque proactivo para gestionar los riesgos de la IA, las organizaciones de América Latina pueden aprovechar los beneficios de la IA, mientras protegen sus operaciones y su reputación.

¿Cómo podemos ayudarte?

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

Contactos:

Ana Milena Barreto

Head of Finex Retail Centro América

M: + (57) 300 689 6250

ana.barreto@wtwco.com

Rodrigo Flores

Regional Cyber Manager LatAm

M: + (52) 55 4383 8517

rodrigo.flores@wtwco.com

Acerca de WTW

En WTW (NASDAQ: WTW), proporcionamos soluciones analíticas basadas en datos en las áreas de personas, riesgo y capital. Potenciando la visión global y la experiencia local de nuestros profesionales presentes en más de 140 países y mercados, te ayudamos a perfilar tu estrategia, a mejorar tu resiliencia organizacional, a motivar a tu personal y maximizar tu rendimiento — y aportamos la perspectiva que te impulsa.

Aviso Legal (Disclaimer)

WTW ofrece intermediación de seguros, y servicios de consultoría a través de entidades legales debidamente registradas ante los reguladores de cada país donde WTW opera. Para más detalles sobre las licencias y regulaciones de las entidades legales de WTW que operan en su país por favor referirse al sitio web de WTW: <https://www.wtwco.com/en-GB/Notices/global-regulatory-disclosures>. Es un requisito normativo para nosotros considerar nuestros requerimientos de licencias locales antes de establecer cualquier acuerdo comercial, y/o contractual con nuestros clientes. Las informaciones compartidas en esta publicación son consideradas precisas en la fecha de su comunicación, indicada en este documento. Estas informaciones pueden haber sido cambiadas o reemplazadas posteriormente y no se deben clasificar como precisas o adecuadas después de esta fecha. La presente publicación ofrece un resumen general sobre el tema al que se refiere. No aborda necesariamente todos sus aspectos ni todos los productos disponibles en el mercado. No es la intención que se la utilice (ni debe utilizarse) en reemplazo de asesoramiento específico referido a situaciones individuales. WTW no ofrece (y no debe suponerse que la presente constituye) asesoramiento en materia contable, jurídica, regulatoria o tributaria. Si tiene previsto adoptar medidas o tomar decisiones sobre la base de los contenidos de esta publicación, le recomendamos consultar primero a un profesional apropiado para recibir asesoramiento específico en la materia. Es probable que parte de la información contenida en la presente se haya obtenido de fuentes externas que consideramos confiables, no obstante, lo cual no garantizamos ni asumimos responsabilidad por la exactitud de dicha información. Las opiniones expresadas no necesariamente reflejan las de WTW.