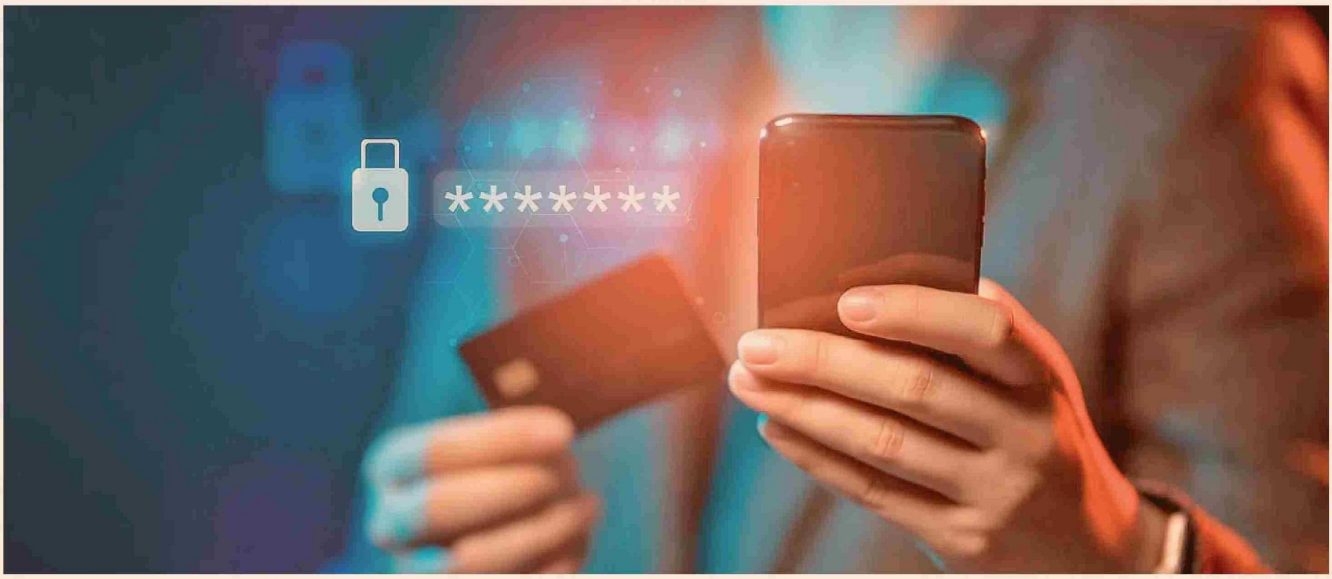
LITORALPRESS

Fecha: 27-06-2025
Medio: Diario Financiero
Supl. : Diario Financiero
Tipo: Noticia general
Título: **Seguridad y Gobernanza en IA: el desafío para las empresas**

Pág. : 21
Cm2: 615,3

Tiraje: 16.150
Lectoría: 48.450
Favorabilidad: No Definida

tigabytes



# Seguridad y Gobernanza en IA: el desafío para las empresas

La rápida adopción de la inteligencia artificial está transformando la forma en que las empresas operan, toman decisiones e interactúan con sus clientes. Sin embargo, junto con sus beneficios, la IA presenta desafíos críticos de seguridad y gobernanza que deben abordarse para garantizar un uso responsable y eficiente de la tecnología.

Sin un marco sólido de gobernanza, las empresas se exponen a riesgos como **sesgos algorítmicos, filtración de datos y ciberataques**, lo que no solo socava la confianza de los clientes y el cumplimiento de normativas cada vez más estrictas, sino que puede derivar en **sanciones millonarias y una grave afectación a la reputación y el valor de marca.**

Si la IA ya forma parte de tu negocio o está en tus planes, este artículo te mostrará cómo estructurar una estrategia sólida de seguridad y gobernanza en IA para mitigar riesgos y garantizar una innovación segura.

**Principales desafíos de seguridad y gobernanza en IA**

La inteligencia artificial tiene el potencial de impulsar la innovación y aumentar la productividad, pero su uso inadecuado puede generar serios problemas para las empresas. Algunos de los desafíos más críticos incluyen:

- **Sesgo algorítmico.** Los modelos de IA pueden reforzar prejuicios presentes en los datos con los que fueron entrenados, lo que puede llevar a decisiones injustas o discriminatorias. Esto es particularmente preocupante en sectores como finanzas, recursos humanos y salud.
- **Falta de transparencia.** Muchos sistemas de IA funcionan como una "caja negra", dificultando la auditoría y explicación de las decisiones tomadas por los algoritmos.
- **Ciberseguridad.** Los modelos de IA pueden ser objetivo de ataques adversariales, en los que actores malintencionados manipulan datos de entrada para influir en los resultados.
- **Regulación y cumplimiento.** Normativas como GDPR y LGPD exige que las empresas implementen IA de manera ética y transparente, asegurando la privacidad y protección de datos.

Si tu empresa no está preparada para enfrentar estos desafíos, puede estar expuesta a riesgos financieros, legales y reputacionales.

**Cómo implementar una estrategia sólida de seguridad y gobernanza en IA**

Para garantizar que tu IA sea segura y confiable es fundamental adoptar prácticas sólidas de gobernanza y ciberseguridad. A continuación, se presentan algunas estrategias esenciales:

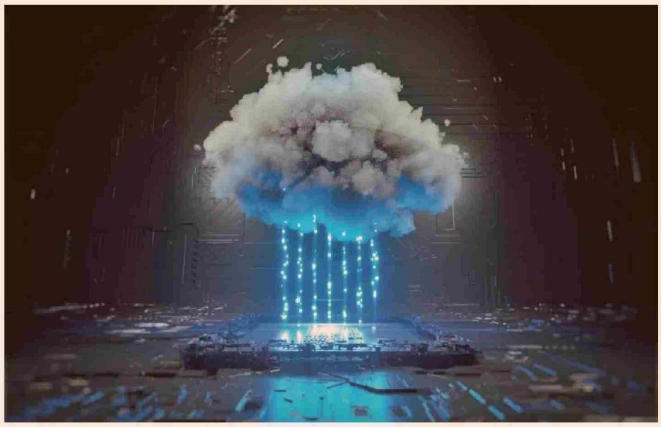
- **Establecer transparencia y explicabilidad**

Para que la IA sea confiable, es fundamental que los procesos de toma de decisiones sean comprensibles y auditables. Esto permitirá que reguladores, usuarios y empresas confíen en la tecnología y mitiguen riesgos legales.

Una solución eficaz es aplicar técnicas como XAI (Explainable AI), que facilitan la interpretación de los modelos de IA y revelan qué factores influyen en sus decisiones.

- **Monitoreo continuo y auditoría de modelos**

Los modelos de IA no son estáticos y pueden desviarse de su propósito inicial con el tiempo. Las empresas deben monitorear constantemente su desempeño para evitar errores o sesgos involuntarios.



Algunas buenas prácticas incluyen:

- Realizar pruebas periódicas para detectar sesgos y garantizar la precisión de los modelos.
- Monitorear el desempeño de la IA en tiempo real para evitar decisiones desactualizadas o incorrectas.
- Incluir intervención humana en decisiones críticas para reducir el riesgo de fallas automatizadas.
- Ciberseguridad para modelos de IA
- Proteger los modelos de IA contra ciberataques y manipulación de datos es fundamental para la seguridad empresarial.

**Cumplimiento normativo y ética en IA**

El cumplimiento normativo y la ética son cada vez más relevantes en el desarrollo de IA. Para evitar sanciones y problemas legales, las empresas deben:

- Adoptar marcos de IA responsable, asegurando que los modelos operen sin sesgos indebidos.
- Garantizar la protección de datos, minimizando riesgos de filtración y acceso no autorizado.
- Cumplir con regulaciones como GDPR y LGPD, asegurando transparencia en el uso de la IA.

**IA segura y confiable: cómo Tigabytes puede ayudar**

La seguridad y gobernanza en IA no son solo cuestiones técnicas, sino factores estratégicos esenciales para proteger a tu empresa y a tus clientes. Sin una estrategia sólida, tu organización puede enfrentar graves riesgos financieros, reputacionales y legales.

En Tigabytes, ayudamos a las empresas a implementar la IA de manera segura, transparente y conforme a las regulaciones vigentes.

**¿Cómo proteger tu empresa?**

La IA ya está moldeando el futuro de los negocios, pero sin un marco adecuado de seguridad y gobernanza, las empresas enfrentan riesgos significativos.

Implementar buenas prácticas de ciberseguridad, cumplimiento normativo y monitoreo continuo es esencial para garantizar una IA ética, responsable y alineada con los objetivos estratégicos de la empresa.

Si tu empresa busca un socio especializado en gobernanza y seguridad de IA, Tigabytes tiene la experiencia y la tecnología necesarias para transformar tu IA en una ventaja competitiva confiable y segura.

Contáctanos y descubre cómo podemos ayudarte a implementar IA con seguridad y gobernanza.