

¿Por qué la IA es un riesgo empresarial, y no solo una herramienta de productividad, para los directivos de la empresa?

Respuesta breve: Los equipos directivos suelen considerar la IA únicamente como un impulsor de la productividad, pero el uso no gestionado de la IA puede exponer secretos empresariales fundamentales —planes de producto, datos de ingresos y estrategia de ventas— directamente a partes externas. Se trata de un riesgo estratégico y financiero que debe estar sobre la mesa del CEO, el CFO, el COO y la dirección de ventas, y no solo del departamento de TI.

Un tipo de exposición diferente

Los incidentes tradicionales de ciberseguridad, como una filtración de datos que termina con registros de clientes en la dark web, siguen un patrón conocido: la dirección responde, los reguladores pueden intervenir, en ocasiones se pagan multas y la junta directiva recibe un informe. Las empresas ya han lidiado antes con este tipo de escenarios, y existen procesos para gestionarlos.

La IA introduce una nueva categoría de exposición, menos comprendida. Cuando los empleados utilizan herramientas de IA sin las salvaguardas adecuadas, es posible que estén introduciendo información empresarial confidencial —planes de producto futuros, previsiones de beneficios, canalizaciones de ventas— en sistemas que nunca fueron diseñados para contener esa información. A diferencia de un incidente de hackeo, esto no es necesariamente el resultado de un ataque. Puede ocurrir simplemente por el uso normal y bien intencionado de la IA por parte del personal.

El problema de las consultas internas

Un riesgo que suele pasarse por alto es lo que ocurre dentro de una empresa una vez que una herramienta de IA tiene un acceso amplio a documentos y datos internos. Si los controles de

acceso no se diseñan cuidadosamente, un empleado podría hacerle una simple pregunta a un asistente de IA y recibir una respuesta detallada que contenga planes confidenciales que nunca deberían circular libremente, ni siquiera internamente. Eso es un fallo de gobernanza, no un error técnico, y puede ser tan perjudicial como una filtración externa.

Por qué esto corresponde al nivel directivo

No invertir en un entorno de IA interno debidamente controlado no elimina esta categoría de riesgo; simplemente la desplaza fuera de la supervisión directa de la organización. Los líderes empresariales jamás considerarían publicar estados de pérdidas y ganancias o canalizaciones de ventas en un sitio web público. El uso no gestionado de la IA puede generar un resultado similar sin que nadie lo pretenda. Tratar esto como un riesgo empresarial central, y no como un asunto puramente técnico, es esencial para proteger las ventajas competitivas que la dirección se ha esforzado en construir.

<https://player.vimeo.com/video/1211538534?texttrack=es>

[Ver en Vimeo](#) · Subtítulos: English, Français, Español, العربية

Revision #2

Created 2026-07-24 02:12:52 UTC by Dennis Underwood

Updated 2026-08-06 18:34:34 UTC by Dennis Underwood