Un enfoque estratégico para gestionar los riesgos de la IA

Mes de Concienciación sobre la Ciberseguridad 2025

Un enfoque estratégico para gestionar los riesgos de la IA

Adam Ihlenfeldt
BDO Belgium

Supported by:
Sacha Blasiak-Priestley
Director, Cloud Security
BDO Canada

La inteligencia artificial (IA) está transformando los negocios a un ritmo sin precedentes. La IA generativa, en particular, ha avanzado mucho más rápido de lo que habían previsto los expertos, comprimiendo décadas de progreso anticipado en solo unos pocos años.

Para 2028, el 62% de los líderes empresariales espera que la IA esté integrada en todas las áreas de sus organizaciones[1]. Pero, aunque el 45% considera que la IA es una oportunidad importante, el 56% está preocupado por los riesgos de ciberseguridad y privacidad que conlleva esta rápida adopción.

> Nos encontramos en un momento crucial en el que la IA ya no es algo teórico. Está al alcance de todos. Esa accesibilidad está impulsando la innovación, pero también está creando puntos ciegos".
>
> Kirstie Tiernan, Líder de IA, BDO USA

[1] BDO Techtonic States

Comprensión de los riesgos y retos de la IA

La IA generativa amplifica muchos de los riesgos de ciberseguridad a los que se han enfrentado las organizaciones durante años, como la ingeniería social, la fuga de datos y las deficiencias en la gobernanza. Casi la mitad de los líderes encuestados afirman que las preocupaciones sobre la seguridad de los datos están frenando nuevas inversiones en IA[1]. Los riesgos son tangibles. Por ejemplo, el escándalo de los subsidios para el cuidado infantil en Países Bajos, impulsado por un algoritmo de aprendizaje automático primitivo, provocó que miles de familias inocentes fueran erróneamente señaladas como fraudulentas. Las consecuencias incluyeron dificultades económicas, indignación pública e incluso la pérdida de vidas humanas. Este caso pone de relieve los riesgos reputacionales, legales y éticos que pueden surgir cuando los sistemas de IA carecen de una supervisión adecuada.

Entre los retos más amplios se incluyen la ampliación de las superficies de ataque, las preocupaciones éticas, como los sesgos y la automatización excesiva, y la gobernanza insuficiente. A medida que las tecnologías de IA evolucionan, a menudo superando a la regulación, la legislación como la Ley de IA de la UE cobra cada vez más importancia.

> “Si bien los riesgos relacionados con los datos, la privacidad y el sesgo de los modelos son reales, también debemos tener en cuenta el impacto más amplio en la dinámica de la fuerza laboral, la adopción y la posible dependencia excesiva de la IA. Una planificación cuidadosa que integre la tecnología con el capital humano y la gestión del cambio puede acelerar significativamente el retorno de la inversión en IA”.
>
> Rocco Galletto, Líder Nacional y Global de Ciberseguridad, BDO Canadá

[1] BDO Techtonic States

Creación de una estrategia cohesionada de gobernanza de la IA

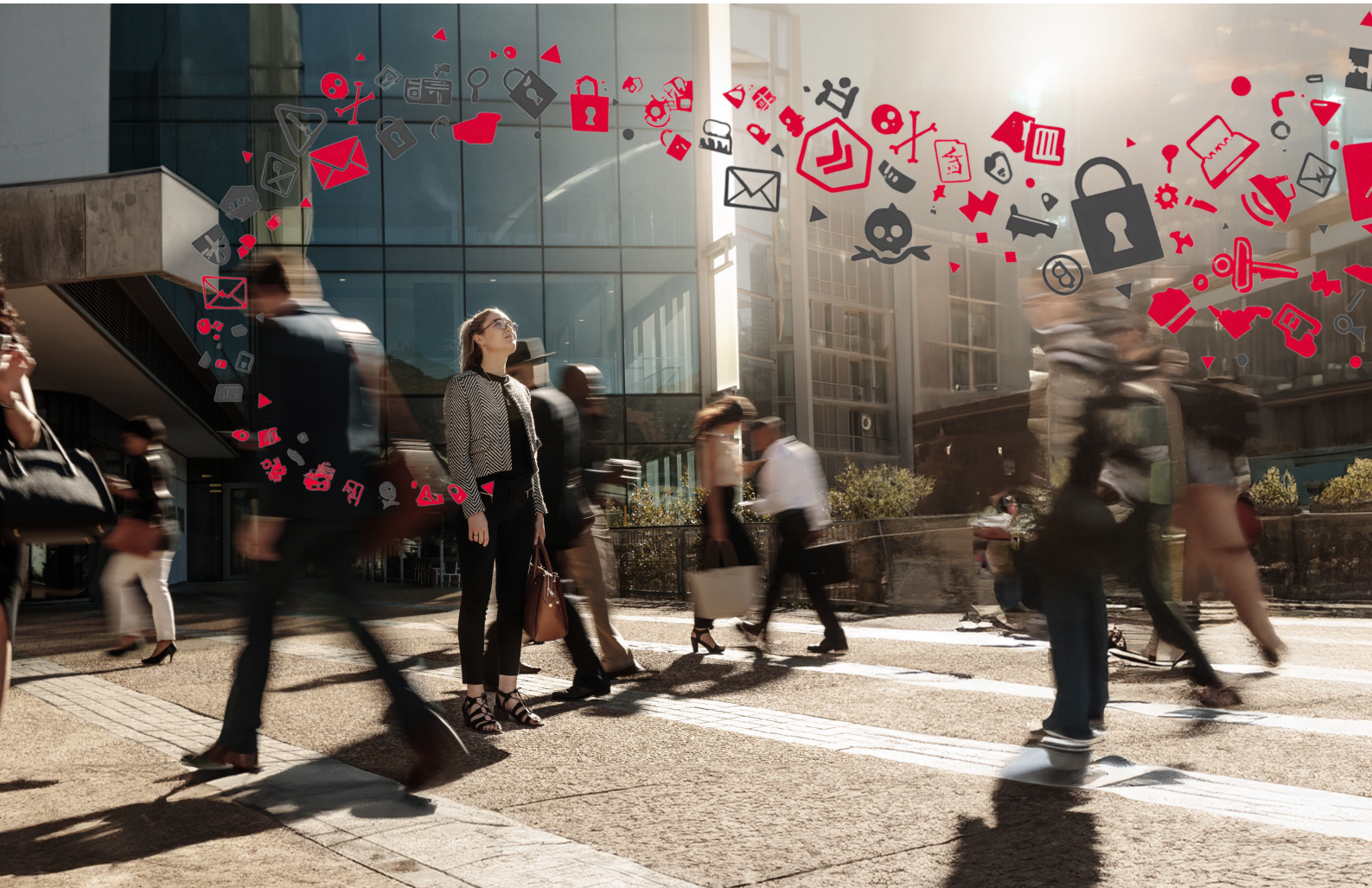
Para mantenerse al día con los cambios tecnológicos y la evolución de la legislación, las organizaciones deben crear comités de gobernanza de la IA con representación interfuncional.

Una estrategia de gobernanza cohesionada incluye:

- Mapeo de las normativas y estándares globales para mantener el cumplimiento en todas las jurisdicciones (como la Ley de IA de la UE, NIST AI 100-2 e ISO/IEC 42005:2025).
- Alineación de las iniciativas de IA con las prioridades de la organización, como la experiencia del cliente, la eficiencia operativa y la innovación.
- Comprensión de las oportunidades de alineación estratégica en toda la empresa. Las organizaciones que incorporan la IA en sus estrategias empresariales suelen obtener un mejor retorno de la inversión.

La IA debe integrarse en los marcos existentes de riesgo, cumplimiento y gobernanza, con salvaguardias aplicadas a lo largo de todo su ciclo de vida.

> Recomendamos contar con una estrategia de IA, una persona responsable de la IA y un comité de gobernanza de la IA formado por múltiples partes interesadas. Esto garantiza que no se produzca un único punto de fallo".
>
> Jason Gottschalk, Socio de Ciberseguridad, BDO Reino Unido



Prácticas medidas que se pueden adoptar hoy

El riesgo suele derivarse de la falta de comprensión. Al fomentar una cultura de concienciación, las organizaciones pueden convertir los riesgos desconocidos en retos gestionables.

Casi la mitad de las organizaciones ya imparten formación a sus empleados sobre el uso seguro y ético de la IA, y el 46% está implementando herramientas de seguridad específicas para la IA[2].

Para hacer frente a los riesgos actuales, las organizaciones deben:

- Sensibilizar y desarrollar las habilidades de los empleados para un uso seguro y ético de la IA.
- Invertir en herramientas avanzadas para detectar y mitigar las amenazas relacionadas con la IA, como la fuga de datos y el acceso no autorizado.
- Limitar la exposición a información confidencial mediante controles y políticas de acceso más estrictos.
- Realizar evaluaciones del impacto de la IA para identificar y abordar los riesgos potenciales.

Se espera que la IA tenga el mayor impacto en la ciberseguridad (55%), la supervisión del cumplimiento normativo (52%) y la gestión de la cadena de suministro (50%)[3].

Es el momento de actuar.

[2] IDC BDO Security Survey
[3] Global Landscape 2025

Preparar la adopción de IA para el futuro

Las organizaciones que adoptan una mentalidad de "fracasar rápido, aprender más rápido", están mejor posicionadas para una integración exitosa de la IA. La adopción de la IA no se trata solo de innovación, sino de desarrollar resiliencia y agilidad en un entorno empresarial dinámico.

A medida que la tecnología evoluciona, es esencial establecer objetivos claros, supervisar continuamente el rendimiento de la IA, actualizar los indicadores de riesgo clave y promover los cambios normativos. Este enfoque permite a las organizaciones crear una gobernanza resiliente que evoluciona con la IA, en lugar de resistirse al cambio y arriesgarse a quedar expuestas a amenazas emergentes.

DESCARGUE EL INFORME

INSCRÍBASE EN NUESTRO PRÓXIMO WEBINAR

EXPLORE LA HERRAMIENTA CYBER RISK ANALYZER

Referencias

[1] BDO Techtonic States
[2] IDC BDO Security Survey
[3] Global Landscape 2025