



Marzo 2026

Área: Auditoría

Inteligencia Artificial (IA) y Control Interno (CI): Riesgos, gobierno y supervisión bajo el marco COSO

Resumen: El uso de **Inteligencia Artificial en las empresas** introduce nuevos riesgos operativos y de control. El marco **COSO** permite fortalecer la supervisión y el control interno sobre estas tecnologías. Este boletín analiza los principales riesgos y consideraciones para su implementación.

Escrito por:

José Luis Zamora Morales - Socio

jlzamora@bhrmx.com

55 5447 7400

dn@bhrmx.com

www.bhrmx.com

La inteligencia artificial suele incorporarse dentro de una **cadena de procesamiento de datos** que incluye distintas etapas, cada una con riesgos y controles específicos.

Captura e ingestión de datos

La **primera etapa** consiste en capturar información desde sistemas estructurados o fuentes no estructuradas. En esta fase pueden surgir riesgos como:

- Extracción incorrecta de datos.
- Pérdida de trazabilidad de la información.
- Inclusión de datos sensibles o confidenciales.

Si la información capturada es incorrecta o incompleta, los errores pueden propagarse en todo el **ciclo analítico posterior**.



Transformación e integración de datos

Una vez capturados, los datos suelen **depurarse, normalizarse o combinarse** con otras fuentes. Los principales riesgos incluyen:

- Errores de mapeo entre sistemas.
- Pérdida de información durante la integración.
- Sesgos introducidos por reglas de transformación.

Estas situaciones pueden generar **distorsiones** en reportes financieros, análisis operativos o modelos predictivos.

Automatización de transacciones y conciliaciones

La **inteligencia artificial** puede **automatizar** procesos contables o financieros de gran volumen, como conciliaciones o registros contables.

Entre los riesgos más relevantes se encuentran:

- Clasificación incorrecta de transacciones.
- Automatización excesiva sin supervisión humana.
- Conflictos de segregación de funciones en configuraciones de sistemas.

Cuando estos errores ocurren, pueden **escalar rápidamente** y **afectar cierres contables** o la información presentada en los estados financieros y sus notas.



Procesos y flujos de trabajo

Los sistemas de inteligencia artificial pueden coordinar procesos empresariales complejos y tomar decisiones sobre la asignación de tareas o la priorización de actividades.

Sin controles adecuados pueden surgir:

- Violaciones de segregación de funciones.
- Decisiones automatizadas sin transparencia.
- Cambios de configuración no autorizados.

Generación de análisis, pronósticos e *insights*

Los modelos de **inteligencia artificial** también pueden **generar proyecciones financieras**, análisis estratégicos o recomendaciones operativas.

En este contexto destacan riesgos como:

- Generación de información incorrecta o no verificable
- Uso de fuentes desactualizadas
- Dependencia excesiva de resultados generados por la IA.

Monitoreo automatizado de riesgos y anomalías

La **inteligencia artificial** también puede utilizarse para **detectar fraude, anomalías o incumplimientos regulatorios** mediante el análisis continuo de grandes volúmenes de datos.

Entre los riesgos asociados se encuentran:

- Tasas elevadas de falsos positivos o falsos negativos.
- Configuraciones incorrectas de alertas.
- Uso indebido de información sensible.

Recuperación de conocimiento y generación de resúmenes

Los **sistemas de IA** pueden **analizar** grandes volúmenes de información y generar resúmenes o reportes ejecutivos.

Los principales riesgos incluyen:

- Omisión de información relevante.
- Generación de conclusiones incorrectas.
- Difusión de información no verificada.

Impacto para la entidad

La adopción de **inteligencia artificial** puede representar una **ventaja competitiva significativa**, pero también implica **responsabilidades** para la alta dirección.

Entre los principales impactos destacan:

Riesgo de decisiones estratégicas basadas en información incorrecta

Modelos **incorrectamente** diseñados o datos incompletos pueden generar proyecciones financieras equivocadas.

Riesgos de fraude o errores contables automatizados

La **automatización** de **procesos financieros** puede amplificar el impacto de configuraciones incorrectas.

Exposición reputacional y regulatoria

El uso de **inteligencia artificial sin controles adecuados** puede derivar en incumplimientos regulatorios o en vulneraciones a la protección de datos e información.

Costos de remediación tecnológica

Cuando los sistemas de IA se implementan sin **una arquitectura de control** adecuada, las organizaciones enfrentan altos costos para rediseñar procesos o corregir errores.



Implicaciones fiscales y de cumplimiento

Aunque la inteligencia artificial es una herramienta tecnológica, su uso dentro de procesos empresariales tiene **implicaciones regulatorias relevantes**, particularmente en materia de cumplimiento y gobierno corporativo.

Entre los principales aspectos a considerar se encuentran:

- **Trazabilidad de decisiones automatizadas.**
- **Control sobre el uso de datos sensibles o personales**, conforme a la normativa de protección de datos.
- **Documentación de modelos y algoritmos utilizados en procesos críticos.**
- **Supervisión humana sobre decisiones relevantes generadas por IA.**

Para evitar algún **impacto negativo**, las organizaciones deberán demostrar que los sistemas de inteligencia artificial:

- Operan conforme a controles documentados.
- Generan resultados verificables.
- Cuentan con mecanismos de monitoreo continuo.



Puntos críticos para Alta Dirección

Desde la perspectiva de gobierno corporativo, la implementación de **inteligencia artificial** debe ser **supervisada por la alta dirección** y los comités de sistemas, auditoría interna mediante una agenda clara de control.

Entre los puntos críticos destacan:

- **Gobierno de datos**

Definir responsables de la calidad, integridad y seguridad de la información utilizada por sistemas de IA.

- **Transparencia de modelos**

Asegurar que los modelos utilizados en decisiones críticas puedan ser explicados y auditados.

- **Segregación de funciones**

Evitar que la misma área configure, opere y supervise sistemas automatizados.

- **Monitoreo continuo**

Establecer indicadores de desempeño y control sobre los sistemas de inteligencia artificial.

- **Gestión de riesgos tecnológicos**

Integrar los riesgos asociados a IA dentro del mapa de riesgos corporativos.



Conclusión

La inteligencia artificial está redefiniendo la forma en que las organizaciones analizan información, automatizan procesos y toman decisiones estratégicas. Sin embargo, su adopción exige **una evolución paralela en los sistemas de control interno y gobierno corporativo**.

Las empresas que implementen estas tecnologías bajo marcos de control sólidos —como COSO— estarán en mejor posición para aprovechar sus beneficios sin comprometer la confiabilidad de su información financiera, el cumplimiento regulatorio o la integridad de sus operaciones.

En **BHR México** apoyamos a las organizaciones en la **evaluación de riesgos tecnológicos, fortalecimiento del control interno y auditoría de procesos automatizados**, incluyendo aquellos impulsados por inteligencia artificial.

Si su organización está incorporando soluciones de IA en procesos financieros, operativos o de cumplimiento, es fundamental evaluar **su impacto en el sistema de control interno y en los mecanismos de supervisión corporativa**.