De la innovación al control

ISO 42001 como sistema de gobernanza de la IA

Mateos Consultores

MATEOS CONSULTORES / ARTÍCULO / Luis D. Mateos

PLANTEAMIENTO

La inteligencia artificial dejó de ser una promesa de laboratorio para convertirse en un componente operativo cotidiano. Hoy se incorpora en motores de recomendación, modelos de scoring crediticio, asistentes conversacionales, sistemas de visión para control de calidad y herramientas de productividad que la organización adquiere casi sin advertirlo, embebidas dentro de un software de uso común. Esta adopción acelerada ha seguido un patrón conocido: primero se experimenta, luego se despliega y solo al final —cuando algo falla— alguien pregunta quién es el responsable.

El concepto de gobernanza de la inteligencia artificial se deriva del mismo principio que sustenta el gobierno corporativo y el gobierno de tecnología: la serie de mecanismos empleados para controlar y dirigir una capacidad de la organización de modo que sus resultados sean consistentes con su estrategia, sus obligaciones legales y sus valores. Así como toda empresa tiene gobierno corporativo aunque no siempre formalice sus reglas, prácticamente toda organización que utiliza IA ya la está gobernando —bien o mal, de forma explícita o por omisión.

La norma ISO/IEC 42001:2023 responde precisamente a este vacío. Es el primer estándar internacional certificable que define los requisitos para establecer, implementar, mantener y mejorar de manera continua un Sistema de Gestión de Inteligencia Artificial (SGIA). Su propósito no es frenar la innovación, sino dotarla de una estructura de control que permita escalar el uso de la IA sin que la organización pierda visibilidad sobre los riesgos que asume. En otras palabras, ISO 42001 traduce un fenómeno tecnológico difuso en un sistema de gestión auditable, con responsabilidades claras, evidencia documental y ciclos de mejora.

PROBLEMÁTICA

La ausencia de un gobierno formal de la IA produce una sintomatología reconocible, en buena medida análoga a la que padecen las organizaciones cuyo gasto tecnológico nunca fue cuestionado. En la práctica de consultoría observamos, de forma recurrente, las siguientes manifestaciones:

- **Adopción descentralizada y sin inventario.** Distintas áreas contratan o activan funcionalidades de IA por su cuenta. Nadie posee una lista consolidada de qué modelos están en uso, con qué datos se alimentan ni qué decisiones automatizan. La organización no puede gobernar lo que no sabe que tiene.
- **Riesgos sin propietario.** Un modelo puede introducir sesgos, vulnerar la privacidad de datos personales o producir resultados erróneos con consecuencias materiales. Cuando ocurre, la pregunta sobre quién responde encuentra a un comité disperso entre el área técnica, jurídico, cumplimiento y la unidad de negocio, sin que ninguno tenga el mandato claro.
- **Opacidad de las decisiones automatizadas.** Sistemas que recomiendan, aprueban o rechazan sin que exista trazabilidad sobre la lógica empleada ni mecanismos de revisión humana. Esto compromete tanto la rendición de cuentas como la capacidad de defenderse ante un cuestionamiento regulatorio o un cliente afectado.
- **Exposición regulatoria creciente.** Marcos como el Reglamento de IA de la Unión Europea introducen obligaciones escalonadas según el nivel de riesgo del sistema, con sanciones relevantes. Para una empresa mexicana que exporta servicios, opera con socios internacionales o procesa datos de ciudadanos extranjeros, la falta de un sistema de gestión demostrable se convierte en una barrera comercial y en un pasivo latente.

- **Pérdida de confianza.** Clientes, socios e inversionistas exigen cada vez más evidencia de que la IA se utiliza de forma responsable. Sin un marco verificable, las afirmaciones de "IA ética" quedan como declaraciones de buena voluntad, no como compromisos auditables.

El denominador común de estos síntomas es el mismo que hemos descrito para otras disciplinas de gestión: la IA se percibe como un asunto puramente técnico —prerrogativa del área de sistemas o de un proveedor— en lugar de una capacidad organizacional que cruza estrategia, riesgo, cumplimiento y operación. Mientras esa percepción persista, las decisiones sobre IA seguirán siendo unilaterales, mal fundamentadas y difíciles de defender.

SOLUCIÓN PROPUESTA

Proponemos abordar la gobernanza de la IA no como un proyecto tecnológico aislado, sino como la implementación de un sistema de gestión bajo ISO/IEC 42001, integrado al gobierno de tecnología existente. La norma comparte la estructura de alto nivel (Anexo SL) de ISO 9001, ISO 27001 e ISO 27701, lo que permite a una organización ya certificada aprovechar su sistema vigente —política, gestión de riesgos, auditoría interna, revisión por la dirección— en lugar de construir uno paralelo. Esta integración es, en la práctica, el principal acelerador de la implementación.

El sistema se articula alrededor de cuatro componentes que, en conjunto, convierten la intención de "usar la IA de forma responsable" en un mecanismo de control verificable:

Componentes del Sistema de Gestión de IA

LIDERAZGO Y POLÍTICA DE IA	EVALUACIÓN DE RIESGOS E IMPACTO
CONTROLES OPERATIVOS Y CICLO DE VIDA	MEDICIÓN, AUDITORÍA Y MEJORA

FIG. 1 — COMPONENTES DEL SISTEMA DE GESTIÓN DE INTELIGENCIA ARTIFICIAL (ISO/IEC 42001).

1. Liderazgo y política de IA.

Todo arranca con un compromiso de la alta dirección que defina el propósito del uso de la IA en la organización, sus límites éticos y los objetivos que persigue. Esta política no es un documento decorativo: establece el alcance del sistema, designa roles —incluida la figura de un responsable del SGIA con autoridad real— y fija los principios que guiarán cada decisión. Aquí se materializa el tránsito del título de este artículo: del impulso por innovar hacia un control deliberado.

2. Evaluación de riesgos e impacto.

ISO 42001 introduce un elemento distintivo frente a otras normas: además de la evaluación de riesgos para la organización, exige una evaluación del impacto de los sistemas de IA sobre individuos y la sociedad. Se valoran sesgos potenciales, efectos sobre la privacidad, transparencia, seguridad y consecuencias del uso indebido. Cada sistema se clasifica según su nivel de riesgo, lo que permite concentrar el esfuerzo de control donde realmente importa, en lugar de aplicar el mismo rigor a un asistente de redacción que a un modelo que decide sobre el otorgamiento de un crédito.

3. Controles operativos a lo largo del ciclo de vida.

El Anexo A de la norma ofrece un catálogo de controles que cubren la totalidad del ciclo de vida de la IA: gobierno de los datos de entrenamiento, documentación del diseño, validación y pruebas antes del despliegue, supervisión humana de las decisiones críticas, monitoreo del desempeño en producción y gestión de proveedores externos de IA. Estos controles son el equivalente operativo del Anexo A de ISO 27001 y constituyen la columna vertebral de la implementación. La trazabilidad —saber qué datos, qué versión del modelo y qué validación respaldan cada decisión— deja de ser una aspiración para convertirse en un requisito documentado.

4. Medición, auditoría y mejora continua.

Finalmente, el sistema se sostiene mediante indicadores de desempeño, auditorías internas periódicas y la revisión por la dirección. Aquí aplica el principio que sostenemos en toda implementación: lo que no se mide no se gobierna. La medición permite demostrar que los controles funcionan, detectar desviaciones —como la degradación de un modelo con el tiempo— y alimentar el ciclo de mejora continua que caracteriza a todo sistema de gestión maduro.

Para ordenar la implementación, en nuestra práctica articulamos estos cuatro componentes con la metodología **MAPA®** (Medición, Análisis, Planeación y Adecuación), que aporta una secuencia probada para llevar a la organización desde un diagnóstico de su madurez actual en el uso de la IA hasta un sistema certificable. La ruta típica comprende:

1. **Medición.** Levantamiento del inventario de sistemas de IA en uso y diagnóstico de la brecha respecto a los requisitos de la norma.
2. **Análisis.** Evaluación de riesgos e impacto por sistema y priorización de los controles según su criticidad.
3. **Planeación.** Diseño de la política, los roles, los procedimientos y el plan de tratamiento de riesgos, integrados al sistema de gestión existente.
4. **Adecuación.** Implementación de los controles, capacitación, auditoría interna y acompañamiento hasta la certificación.

CONCLUSIÓN

El hilo conductor de este planteamiento es que la gobernanza de la inteligencia artificial no consiste en elegir entre innovar y controlar, sino en hacer ambas cosas de forma deliberada. Una organización que adopta IA sin gobierno no innova más rápido; simplemente acumula riesgos que tarde o temprano se materializan en pérdidas económicas, sanciones regulatorias o erosión de la confianza de sus clientes. ISO/IEC 42001 ofrece el marco para que la innovación ocurra sobre cimientos sólidos.

Implementar un Sistema de Gestión de IA produce beneficios inmediatos —visibilidad sobre los sistemas en uso, asignación clara de responsabilidades y una base de evidencia para responder a clientes y reguladores— y beneficios estructurales de mediano plazo, al integrar la IA en la cultura de gestión por procesos de la organización. Para empresas que ya operan bajo ISO 9001, ISO 27001 u otras normas, el esfuerzo incremental es considerablemente menor, pues la mayor parte de la maquinaria de gestión ya está en marcha.

En sentido estricto, una gobernanza madura de la IA descansa sobre cinco aspectos generales que conviene tener presentes en cualquier escenario de adopción:

1. Alineación estratégica y ética del uso de la IA.
2. Asignación clara de responsabilidades y rendición de cuentas.
3. Gestión de riesgos y del impacto sobre las personas.
4. Transparencia y trazabilidad de las decisiones automatizadas.
5. Medición del desempeño y mejora continua.

La pregunta que las organizaciones deben hacerse ya no es si van a utilizar inteligencia artificial, sino si están dispuestas a gobernarla con la misma disciplina con que gobiernan su calidad, su seguridad de la información o sus finanzas. ISO 42001 ofrece el camino para transitar, con orden y evidencia, de la innovación al control.

Referencias

ISO/IEC 42001:2023, Information technology — Artificial intelligence — Management system. International Organization for Standardization.

Reglamento (UE) 2024/1689 sobre Inteligencia Artificial. Parlamento Europeo y Consejo de la Unión Europea.