

## Norma ISO/IEC 42001:2023 Sistema de Gestión de la Inteligencia Artificial

**Rosa Mayelin Guerra Bretaña**

mayelin@biomat.uh.cu

Centro de Biomateriales de la Universidad de La Habana

### EDITORIAL

La inteligencia artificial (IA) se integra cada vez más en las operaciones, los productos y servicios y, por ese motivo, crece el interés de las organizaciones por aprovecharla como fuente de ventajas competitivas, generando desafíos sociales, éticos y legales. Como toda tecnología emergente la adopción de la IA implica riesgos.

Para contribuir a que las organizaciones gestionen los riesgos y las oportunidades asociados a los sistemas de IA, como resultado del trabajo conjunto de la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC), en diciembre de 2023 fue publicada la norma internacional ISO/IEC 42001 de sistemas de gestión específica para la IA. Esta norma proporciona un marco organizativo para desarrollar y gestionar sistemas de IA de manera responsable y eficaz, al abordar de forma holística los aspectos técnicos, éticos y organizativos propios de la IA, alineados con los valores corporativos, estratégicos y regulatorios.

Los principios rectores para el desarrollo de la ISO/IEC 42001 fueron:

1. Transparencia, no se aceptan decisiones sesgadas, discriminatorias o que impliquen segregaciones sociales, impactos ambientales negativos o afectaciones sociales.
2. Responsabilidad como elemento esencial para generar confianza digital.
3. Equidad, al promover la toma de decisiones justas, que no afecten en modo alguno a grupos específicos o a personas debido a sus posiciones políticas, credos religiosos, preferencias sexuales, etc.
4. Comunicación, con vista a elevar la capacidad para explicar a las personas el funcionamiento y las expectativas reales sobre IA.
5. Seguridad de la información y privacidad de datos, que tiene implicaciones regulatorias, y también reputacionales.
6. Confiabilidad en el uso de la IA es el propósito fundamental que se tuvo en cuenta al elaborar la norma y definir sus consideraciones éticas.

En el complejo marco de leyes y regulaciones de la IA para las organizaciones que operan en entornos internacionales, el cumplimiento normativo representa un desafío, pero también una oportunidad de liderazgo, y una base sólida para el desarrollo de una IA confiable, transparente y ética.

La norma ISO/IEC 42001 especifica los requisitos para establecer, implementar, mantener y mejorar de forma continua un sistema de gestión de inteligencia artificial (SGIA) en las organizaciones. Este sistema abarca el uso, el desarrollo y la supervisión de la IA, así como la provisión de los productos y servicios que la integran.

Se considera especialmente beneficiosa, para:

- Empresas tecnológicas que desarrollan productos de IA.
- Organizaciones que utilizan IA en procesos de negocio críticos, como instituciones financieras o proveedores de servicios sanitarios.
- Sector público o agencias gubernamentales donde se exigen altos niveles de responsabilidad, ética y cumplimiento normativo.
- Industrias con una alta regulación que deben alinearse con las normas en torno a la IA. Entre ellas se incluyen las industrias farmacéutica y biotecnológica, energética y de servicios públicos, aeronáutica y automotriz.
- Instituciones académicas y de investigación.

La IA se aplica cada vez más en todos los sectores que utilizan tecnologías de la información y se prevé que sea uno de los principales motores económicos. Como consecuencia de esta tendencia, ciertas aplicaciones pueden generar desafíos sociales en los próximos años.

La IA plantea elementos específicos a considerar, como:

- El uso de la IA para la toma de decisiones automática, a veces de forma poco transparente e inexplicable, puede requerir una gestión específica que va más allá de la gestión de los sistemas clásicos de tecnología de la información.
- El uso del análisis de datos, la comprensión y el aprendizaje automático (AA), en lugar de la lógica humana para diseñar sistemas, aumenta las oportunidades de aplicación de los sistemas de IA y cambia la forma en que estos se desarrollan e implementan.
- Los sistemas de IA que realizan aprendizaje continuo cambian su comportamiento durante su uso. Requieren una consideración especial para garantizar su uso responsable.

Como plantea la ISO/IEC 42001, el SGIA debe integrarse con los procesos y la estructura de gestión existente en la organización, por ejemplo, en:

- la determinación de la política, los objetivos de la organización y las relaciones con las partes interesadas;
- la gestión de riesgos y oportunidades;
- la gestión de la fiabilidad de los sistemas de IA, como la seguridad, la protección, la equidad, la transparencia, la calidad de los datos y la calidad de los sistemas de IA a lo largo de su ciclo de vida;
- la gestión de proveedores, socios y terceros que proporcionan o desarrollan sistemas de IA para la organización.

Las organizaciones que implementan la norma ISO/IEC 42001 pueden obtener los beneficios siguientes:

- Demostrar prácticas éticas en las iniciativas de IA que realizan, así como, el cumplimiento de las regulaciones y las expectativas de las partes interesadas.
- Garantizar la transparencia en la toma de decisiones sobre IA.
- Generar confianza con clientes, socios y organismos reguladores a través de la integración sostenible de la IA.

Como otras normas de sistemas de gestión de la ISO, la norma ISO/IEC 42001 sigue la estructura armonizada de 10 capítulos, que incluyen:

1. Alcance: define su propósito, público objetivo y aplicabilidad.
2. Referencias normativas: incluye la norma ISO/IEC 22989:2022, que proporciona conceptos y terminología de IA.
3. Términos y definiciones: proporciona los términos y definiciones esenciales para interpretar los requisitos de la norma.
4. Contexto de la organización: requiere que las organizaciones analicen los aspectos internos y externos que pueden influir en sus objetivos, incluidos los roles relacionados con los sistemas de IA y diversos elementos contextuales que afectan las operaciones.
5. Liderazgo: requiere que la alta dirección demuestre compromiso, integre los requisitos de la IA y fomente una cultura de uso responsable de la IA.
6. Planificación: requiere que las organizaciones planifiquen acciones para abordar los riesgos y las oportunidades, establezcan objetivos de IA y la forma de alcanzarlos y planifiquen los cambios.
7. Soporte: requiere que las organizaciones garanticen los recursos, la competencia, la conciencia, la comunicación efectiva y la información documentada necesaria para la implementación, mantenimiento y mejora del SGIA.
8. Operación: proporciona requisitos con respecto a los procesos de planificación, implementación y control operativos para cumplir con el SGIA, abordar los riesgos y oportunidades identificados, realizar evaluaciones de impacto del sistema de IA y gestionar los cambios de manera efectiva.
9. Evaluación del desempeño: requiere que las organizaciones realicen el seguimiento y medición, analicen y evalúen el desempeño y la eficacia de los procesos. Además, requiere la realización de auditorías internas y revisiones por la dirección para garantizar la idoneidad, adecuación y eficacia continua de los SGIA.
10. Mejora: se refiere a la mejora continua, abordando las no conformidades mediante acciones correctivas, evaluando la eficacia y manteniendo la información documentada para la rendición de cuentas y el seguimiento de los esfuerzos de mejora.

Anexo A: Establece un conjunto de controles diseñados específicamente para abordar los riesgos relacionados con la IA, como la mitigación de sesgos, la transparencia, la rendición de cuentas y la gobernanza de datos.

Anexo B: ofrece orientaciones para el diseño, implementación y uso de los controles mencionados en el Anexo A.

Anexo C (Informativo): no aplica para todas las organizaciones, solo para las que hagan de la gestión de riesgos de IA un objetivo estratégico.

Anexo D (Informativo): habla de la aplicabilidad del sistema en todo tipo de organizaciones que desarrollen, comercialicen, utilicen, proporcionen o incorporen en sus productos Sistemas de Inteligencia Artificial.

Un SGIA, según ISO/IEC 42001:

- Apoya la toma de decisiones, basada en información precisa y oportuna.
- Brinda ventaja competitiva para las organizaciones, al ser más ágiles, innovadoras y responder prontamente a los cambios del contexto.
- Garantiza el cumplimiento de las normas jurídicas, éticas y regulatorias en el desarrollo y utilización de la IA.
- Contribuye a definir roles y responsabilidades en el uso de la IA.
- Contribuye a asignar mejor los recursos, al identificar áreas de mejora y áreas donde los recursos se están subutilizando.
- Ayuda a las organizaciones a identificar y mitigar riesgos mediante el análisis de patrones y tendencias en los datos, ayudando a anticipar y abordar problemas potenciales de manera proactiva.
- Permite la automatización de tareas repetitivas, analiza grandes cantidades de datos y proporciona información que puede conducir a procesos más eficientes.
- Proporciona directrices para implementar controles aplicables para respaldar los procesos relacionados con la IA.
- Propone la integración transversal de la gestión de riesgos de la IA con los objetivos empresariales.

La gestión de riesgos de la IA con la norma ISO/IEC 42001 se realiza a través de las etapas siguientes:

- Identificación proactiva de los riesgos, anticipando potenciales fallos o sesgos antes de que afecten a las operaciones.
- Evaluación de riesgos, con metodologías cualitativas y cuantitativas para valorar cada riesgo en función de su gravedad, probabilidad de ocurrencia y detectabilidad.
- Mitigación y tratamiento mediante estrategias proporcionales al nivel de exposición.
- Monitorización continua de los riesgos identificados y los nuevos.

Para implementar la ISO/IEC 42001, las organizaciones deben:

- Diagnosticar qué tan alineada está la organización con los requisitos de la norma.
- Establecer políticas internas y lineamientos para el desarrollo y uso de IA.
- Capacitar al personal en los conceptos y requisitos de la norma.
- Implementar los requisitos del sistema de gestión.
- Realizar el seguimiento y medición de los procesos, la auditoría interna y la revisión por la dirección.

Para evaluar la eficacia del SGIA se establecen indicadores de desempeño, como:

- Porcentaje de riesgos identificados frente a los mitigados: mide la capacidad de respuesta del sistema ante amenazas conocidas.
- Tasa de incidentes o fallos no detectados en el análisis de riesgos inicial.
- Tiempo medio de respuesta ante desviaciones detectadas.
- Nivel de cumplimiento normativo.

Además de la ISO/IEC 42001, otras normas ayudan a mitigar los riesgos y maximizar los beneficios de la IA, entre ellas:

- ISO/IEC 22989:2022, Information technology — Artificial intelligence — Artificial intelligence concepts and terminology
- ISO/IEC 23053:2022 Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML).
- ISO/IEC 23894:2023 Information technology — Artificial intelligence — Guidance on risk management.

## REFERENCIAS BIBLIOGRÁFICAS

- Almanza, R. (2024). *Guía Completa para entender el rol de ISO/IEC 42001*. <https://tecnasau.tecnasa.com/guia-completa-para-entender-el-rol-de-iso-iec-42001/>
- CYNTHUS. (2025). *Inteligencia artificial y ética: Todo lo que debes saber sobre la norma ISO 42001*. <https://www.cynthus.com.mx/inteligencia-artificial-etica-norma-iso-42001/>
- International Organization for Standardization (2023). *ISO/IEC 42001:2023 Information technology — Artificial intelligence — Management system*. <https://committee.iso.org/es/norma/42001>
- ISOTools. (2024). *Principios y estructura de ISO 42001: la norma para sistemas de gestión de IA*. <https://www.isotools.us/2024/11/19/principios-y-estructura-de-iso-42001-la-norma-para-sistemas-de-gestion-de-ia/>
- ISOTools. (2025). *Gestión de riesgos de IA con ISO 42001: fundamentos y buenas prácticas*. <https://www.isotools.us/2025/07/22/gestion-de-riesgos-de-ia-con-iso-42001-fundamentos-y-buenas-practicas/>
- ISOTools. (2025). *Panorama global de las leyes de IA y cómo cumplir con la norma ISO 42001 puede ayudar*. <https://www.isotools.us/2025/06/26/panorama-global-de-las-leyes-de-ia-y-como-cumplir-con-la-norma-iso-42001-puede-ayudar/>
- Partes Interesadas. (2025). *Cómo implementar un sistema de gestión de IA con ISO 42001*. <https://partesinteresadas.com/como-implementar-un-sg-con-iso-42001/>
- Roberts, S. (2025). *Gestionar los riesgos de la IA y aprovechar las nuevas oportunidades con la norma ISO 42001*. <https://www.nqa.com/es-es/resources/blog/july-2025/iso-42001-ai>