Informe ISO/IEC 42001:2023
Sistema de Gestión de Inteligencia Artificial (SGIA)

Caso organizacional: Gestor de Proyectos

Autores:

Dylan Steve Rodríguez Castellanos, José Luis Martínez Acevedo, Juan Sebastián Pinzón Sánchez

Fecha:

05/11/2025

1. Introducción a ISO 42001

La norma **ISO/IEC 42001:2023** representa el primer estándar internacional diseñado específicamente para establecer un **Sistema de Gestión de Inteligencia Artificial (SGIA)**. Su objetivo principal es proporcionar a las organizaciones un marco de referencia que les permita **desarrollar, implementar y utilizar sistemas de inteligencia artificial de forma responsable, ética, segura y transparente**. Esta norma surge como respuesta a la creciente adopción de la inteligencia artificial (IA) en procesos empresariales, industriales y gubernamentales, donde el uso inadecuado o poco controlado de estas tecnologías puede generar impactos significativos en la seguridad, la privacidad y la confianza pública.

En un contexto global donde la IA impulsa la automatización, el análisis predictivo y la toma de decisiones basada en datos, la ISO/IEC 42001 busca asegurar que su aplicación se realice bajo **principios de gobernanza sólida, transparencia y control del riesgo**. Al igual que otras normas de la familia ISO, el estándar adopta la estructura de alto nivel (HLS, por sus siglas en inglés), lo que facilita su integración con otros sistemas de gestión, como la **ISO/IEC 27001 (Seguridad de la Información)**, la **ISO 9001 (Calidad)** o la **ISO/IEC 27701 (Privacidad de la Información)**. Esta compatibilidad promueve una administración coherente de la tecnología y la información dentro de las organizaciones modernas.

El enfoque central de la ISO/IEC 42001 radica en establecer políticas, responsabilidades, procedimientos y controles que garanticen el **uso confiable y ético de los sistemas de inteligencia artificial**. La norma enfatiza que el desarrollo y la operación de la IA deben ser **explicables, trazables y auditables**, reduciendo riesgos asociados con decisiones automatizadas y evitando la generación de sesgos o discriminaciones. Además, busca reforzar la rendición de cuentas, asignando roles claros en la gestión del ciclo de vida de la IA, desde su diseño y entrenamiento hasta su despliegue y mantenimiento.

Entre los beneficios que aporta la implementación de un SGIA conforme a la ISO/IEC 42001 se encuentran la **mejora en la calidad de los modelos de IA**, la **protección de los datos personales**, la **reducción de incidentes éticos o legales** y el **fortalecimiento de la reputación organizacional**. Asimismo, permite establecer un sistema de mejora continua que impulse la innovación responsable, garantizando que los modelos de inteligencia artificial evolucionen bajo controles y auditorías periódicas. De esta forma, la norma contribuye al equilibrio entre la eficiencia tecnológica y la responsabilidad social.

Otro aspecto relevante de la norma es su enfoque hacia la **confianza y la transparencia**. La ISO/IEC 42001 exige que las organizaciones documenten el comportamiento esperado de los sistemas de IA, incluyendo sus limitaciones y riesgos conocidos, para que los usuarios y las partes interesadas comprendan cómo se toman las decisiones automatizadas. Esta práctica fortalece la aceptación pública de la IA, al demostrar que su implementación está guiada por criterios verificables y auditables.

En conclusión, la ISO/IEC 42001:2023 no solo constituye un instrumento técnico, sino también un **marco ético y de gobernanza** que busca asegurar que el desarrollo de la inteligencia

artificial se realice de manera **responsable, justa y sostenible**. Para organizaciones que integran IA en sus procesos —como el proyecto *Gestor de Proyectos*— esta norma ofrece una base sólida para garantizar la seguridad, la transparencia y el cumplimiento normativo, promoviendo la confianza tanto de los usuarios internos como de los clientes externos.

2. Descripción del caso organizacional

El caso organizacional propuesto se centra en el desarrollo de una aplicación web denominada **"Gestor de Proyectos"**, concebida como una plataforma integral para la administración eficiente y segura de proyectos empresariales. Este sistema nace como respuesta a la creciente necesidad de las organizaciones modernas de **centralizar la información, coordinar tareas, supervisar equipos de trabajo y asegurar la integridad de los datos** mediante tecnologías digitales confiables. En un entorno donde la colaboración remota, la ciberseguridad y la automatización se han convertido en pilares estratégicos, este proyecto busca ofrecer una solución adaptable, escalable y alineada con estándares internacionales de gestión de la información y gobernanza tecnológica.

El **Gestor de Proyectos** fue ideado por un equipo conformado por **Dylan Steve Rodríguez Castellanos, José Luis Martínez Acevedo y Juan Sebastián Pinzón Sánchez**, quienes, desde una perspectiva académica y técnica, proponen una herramienta web construida con **Java (JSP y Servlets)**, utilizando **MySQL** como base de datos relacional y **Apache Tomcat** como servidor de aplicaciones. Su arquitectura modular permite dividir el sistema en componentes funcionales bien definidos, lo que facilita su mantenimiento, evolución y futura integración con tecnologías de inteligencia artificial. Los módulos principales previstos son: **Autenticación y Control de Acceso**, **Gestión de Usuarios** y **Gestión de Proyectos**, cada uno con funciones específicas que contribuyen a la seguridad, la eficiencia y la trazabilidad de la información.

El objetivo general del proyecto es **facilitar la gestión segura de proyectos mediante una plataforma que incorpore controles de seguridad y buenas prácticas alineadas con la norma ISO/IEC 27001**, garantizando así la protección de la información sensible y la continuidad de los procesos empresariales. En su diseño se contemplan mecanismos de autenticación de usuarios con diferentes roles, como administradores y empleados, lo que permite un control jerárquico de privilegios. De esta forma, se asegura que las operaciones críticas, como el registro o eliminación de usuarios y la modificación de datos, solo sean realizadas por personal autorizado.

Desde su concepción, el **Gestor de Proyectos** no solo busca cumplir con criterios de eficiencia técnica, sino también con principios de **gobernanza y ética digital**. Esto se refleja en la intención de integrar, en etapas posteriores, componentes basados en **inteligencia artificial (IA)** que optimicen la asignación de tareas, evalúen el rendimiento de los equipos y anticipen posibles retrasos en los proyectos. Dicha integración plantea un escenario idóneo para aplicar los

lineamientos de la **norma ISO/IEC 42001:2023**, garantizando que la incorporación de IA se realice de forma **responsable, transparente y controlada**.

En este contexto, la implementación de un **Sistema de Gestión de Inteligencia Artificial (SGIA)** dentro del Gestor de Proyectos busca fortalecer la estructura de control y supervisión sobre los modelos y algoritmos utilizados. Por ejemplo, un módulo de IA podría analizar métricas de productividad y ofrecer sugerencias automáticas de distribución de carga laboral, pero siempre dentro de un marco normativo que asegure la ausencia de sesgos, la protección de datos y la trazabilidad de las decisiones automatizadas. La aplicación de la ISO/IEC 42001 permitirá documentar cada fase del ciclo de vida de la IA —desde su diseño hasta su mantenimiento—, asegurando la calidad, seguridad y ética del sistema.

Además, este proyecto se concibe como una herramienta adaptable para distintos tipos de organizaciones, desde **pequeñas empresas en proceso de digitalización** hasta **entidades corporativas con estructuras complejas de gestión de proyectos**. Su flexibilidad tecnológica permite personalizar la plataforma según las políticas internas y los niveles de madurez digital de cada cliente. En un entorno empresarial cada vez más competitivo, disponer de un sistema de gestión basado en IA que cumpla con estándares internacionales representa una ventaja estratégica, ya que **refuerza la confianza de los clientes y facilita auditorías de cumplimiento** ante entes regulatorios o certificadores.

Otro aspecto relevante del caso organizacional es su **orientación hacia la ciberseguridad y la gestión de riesgos**. Alineado con la ISO/IEC 27001, el sistema implementa controles para evitar accesos no autorizados, pérdida de datos y vulnerabilidades en el tratamiento de información sensible. La futura adopción de la ISO/IEC 42001 complementará este enfoque, agregando una capa adicional de control sobre los modelos de IA y asegurando que su comportamiento sea verificable y explicable. De esta manera, el proyecto integra dos dimensiones complementarias: **la seguridad de la información y la gobernanza de la inteligencia artificial**.

Finalmente, el **Gestor de Proyectos** no solo constituye un ejercicio académico, sino una propuesta aplicable en entornos empresariales reales, donde la combinación de automatización, seguridad y responsabilidad digital es fundamental. El sistema busca consolidarse como una plataforma que apoye la **toma de decisiones informadas, la transparencia operativa y la mejora continua**, cumpliendo con las mejores prácticas establecidas por la norma ISO/IEC 42001:2023. A través de esta implementación, se pretende demostrar que el uso ético y regulado de la IA puede convertirse en un motor de innovación y eficiencia, siempre que esté respaldado por un marco normativo sólido y una cultura organizacional comprometida con la confianza tecnológica.

3. Propuesta del Sistema de Gestión de Inteligencia Artificial (SGIA)

La implementación de un **Sistema de Gestión de Inteligencia Artificial (SGIA)** en el proyecto *Gestor de Proyectos* busca garantizar que el uso de tecnologías de inteligencia artificial dentro de la plataforma se realice bajo **criterios de responsabilidad, transparencia, seguridad y ética**. Esta propuesta pretende integrar el SGIA dentro de la estructura de gestión ya existente en el sistema, el cual actualmente se rige por principios de la **norma ISO/IEC 27001**, ampliando su alcance hacia la gobernanza de la inteligencia artificial conforme a los lineamientos de la **ISO/IEC 42001:2023**. De esta manera, el proyecto evolucionará desde un sistema de gestión de información segura hacia un sistema integral que controle tanto la seguridad de los datos como el comportamiento y los riesgos derivados del uso de IA.

El **objetivo general del SGIA** es establecer un marco normativo y operativo que permita **diseñar, desarrollar, implementar y mantener los modelos de inteligencia artificial del Gestor de Proyectos de manera controlada y auditable**. Este sistema debe asegurar que las decisiones automatizadas sean justificables, explicables y consistentes con los principios éticos y legales aplicables. Asimismo, debe fomentar la mejora continua del desempeño de los algoritmos mediante la evaluación constante de métricas de precisión, sesgo, trazabilidad y satisfacción del usuario.

3.1 Política de gestión de inteligencia artificial

La política del SGIA establece los principios rectores que guiarán todas las actividades relacionadas con el desarrollo y uso de la inteligencia artificial dentro del proyecto. Dicha política se sustenta en los siguientes compromisos fundamentales:

- **Responsabilidad y ética:**
  Toda implementación de IA deberá respetar los derechos humanos, la equidad y la no discriminación, evitando sesgos que puedan afectar negativamente a los usuarios o grupos específicos.

- **Transparencia y trazabilidad:**
  Los procesos de entrenamiento, validación y uso de modelos deberán ser documentados exhaustivamente para garantizar la trazabilidad y la posibilidad de auditorías.

- **Seguridad y privacidad:**
  Se aplicarán controles de seguridad que garanticen la confidencialidad, integridad y disponibilidad de los datos utilizados por los sistemas de IA, en cumplimiento con la ISO/IEC 27001 y la legislación vigente.

- **Fiabilidad y explicabilidad:**
  Los modelos de IA deberán ser comprensibles para los usuarios y administradores, asegurando que sus resultados puedan interpretarse de manera clara y verificable.

- **Mejora continua:**
  Se establecerán mecanismos de revisión periódica para optimizar los modelos y procesos de IA, garantizando su alineación constante con los objetivos organizacionales y las exigencias normativas.

Esta política será comunicada a todos los miembros del equipo de desarrollo y revisada al menos una vez al año o cuando se produzcan cambios relevantes en la tecnología o en el entorno normativo.

3.2 Roles y responsabilidades

El éxito del SGIA depende de una clara definición de roles y responsabilidades. Dentro del proyecto *Gestor de Proyectos*, se propone la siguiente estructura organizativa:

- **Director del Proyecto:**
  Garantiza que la implementación del SGIA esté alineada con la estrategia general de la organización y con los principios establecidos en la política de IA. Supervisa la asignación de recursos y la toma de decisiones estratégicas.

- **Ingeniero de Inteligencia Artificial:**
  Responsable del diseño, entrenamiento, validación y mantenimiento de los modelos de IA. Debe asegurar que los algoritmos cumplan con los requisitos de rendimiento, ética y transparencia.

- **Responsable de Cumplimiento Normativo:**
  Supervisa la correcta aplicación de la ISO/IEC 42001 y otras normativas aplicables. También gestiona auditorías internas y reportes de conformidad.

- **Administrador de Seguridad:**
  Encargado de controlar los accesos, garantizar la protección de datos y verificar que los entornos de desarrollo cumplan con las políticas de seguridad establecidas.

- **Usuarios Finales:**
  Interactúan con los módulos del sistema e informan sobre comportamientos anómalos o resultados inesperados generados por la IA, sirviendo como fuente de retroalimentación para el proceso de mejora continua.

3.3 Identificación, evaluación y mitigación de riesgos

El SGIA integrará un proceso sistemático para la **identificación, evaluación y mitigación de riesgos** asociados al uso de IA. Este proceso se desarrollará en cuatro etapas:

- **Identificación:**
  Se registrarán todos los posibles riesgos relacionados con el ciclo de vida de la IA, incluyendo sesgos en los datos de entrenamiento, errores de predicción, uso no autorizado de la información, pérdida de explicabilidad y fallos de seguridad.

- **Evaluación:**
  Cada riesgo será analizado según su probabilidad e impacto, clasificándose en niveles (alto, medio o bajo). Se priorizarán aquellos que puedan comprometer la privacidad, la equidad o la reputación del sistema.

- **Mitigación:**
  Se aplicarán controles preventivos y correctivos, tales como validación cruzada de datos, revisión manual de decisiones automatizadas y aplicación de métricas de equidad.

- **Monitoreo:**
  Los riesgos residuales serán observados mediante indicadores continuos que permitan detectar desviaciones y tomar acciones correctivas en tiempo real.

Este proceso se documentará y actualizará periódicamente, formando parte del sistema general de mejora continua del SGIA.

3.4 Mecanismos de ética, transparencia y cumplimiento

El cumplimiento ético y legal es un pilar fundamental de esta propuesta. Para garantizar la **ética y transparencia**, el SGIA incluirá los siguientes mecanismos:

- **Documentación completa del ciclo de vida de los modelos:**
  Desde el diseño hasta la puesta en producción, cada versión de modelo contará con registros detallados sobre sus fuentes de datos, métodos de entrenamiento y resultados de validación.
- **Auditorías internas de IA:**
  Se realizarán auditorías regulares para verificar la conformidad con los principios éticos, técnicos y legales establecidos.
- **Panel de explicabilidad:**
  Se desarrollará un módulo que permita a los administradores visualizar las decisiones o predicciones generadas por la IA y comprender los factores que influyeron en ellas.
- **Gestión de consentimiento y privacidad:**
  Los datos utilizados para entrenar modelos de IA serán anonimizados y tratados bajo políticas de privacidad compatibles con la normativa ISO/IEC 27701.
- **Comité de Ética y Gobernanza de IA:**
  Grupo de revisión interdisciplinario encargado de evaluar los posibles impactos sociales y técnicos de los nuevos desarrollos en IA antes de su implementación.

3.5 Integración con otros sistemas de gestión

Finalmente, el SGIA del *Gestor de Proyectos* se diseñará de manera que pueda integrarse armónicamente con otros sistemas de gestión existentes, especialmente el **Sistema de Gestión de Seguridad de la Información (SGSI)** basado en la ISO/IEC 27001. Esta integración permitirá compartir políticas, indicadores y auditorías conjuntas, reduciendo redundancias y fortaleciendo el control integral sobre la información y la tecnología. La combinación de ambos sistemas creará un entorno de desarrollo seguro, donde la inteligencia artificial opere dentro de un marco de confianza, trazabilidad y cumplimiento normativo.

4. Plan de Implementación del SGIA

La implementación del **Sistema de Gestión de Inteligencia Artificial (SGIA)** en el proyecto *Gestor de Proyectos* se concibe como un proceso estructurado, gradual y participativo, que garantice el cumplimiento de los requisitos establecidos por la norma **ISO/IEC 42001:2023**. Este plan tiene como propósito definir las **fases, actividades, recursos y herramientas necesarias** para poner en marcha el sistema, así como los **indicadores de desempeño y mecanismos de evaluación** que permitirán verificar su eficacia.

El enfoque adoptado se basa en el **ciclo de mejora continua (Planificar–Hacer–Verificar–Actuar, PHVA)**, ampliamente utilizado en las normas ISO. A través de este modelo, se busca que la organización adopte una cultura de aprendizaje constante, en la que las decisiones sobre la inteligencia artificial se fundamenten en evidencia técnica y se ajusten progresivamente según los resultados obtenidos.

4.1 Fases del plan de implementación

Fase 1: Diagnóstico inicial:

Durante esta etapa se realizará un análisis exhaustivo del estado actual del proyecto *Gestor de Proyectos* frente a los requisitos de la norma ISO/IEC 42001. Se identificará el grado de madurez tecnológica, la existencia de políticas o procedimientos relacionados con IA y las brechas normativas existentes.
Las principales actividades de esta fase son:

- Levantamiento de información documental sobre los procesos actuales del sistema.
- Entrevistas con los responsables técnicos y de seguridad.
- Identificación de riesgos y oportunidades del uso de IA.
- Elaboración de un informe de brechas frente a los requisitos del SGIA.
  El producto final de esta fase será un **plan de acción preliminar** que establezca prioridades y metas para las siguientes etapas.

Fase 2: Diseño del SGIA

En esta fase se desarrollará la estructura formal del sistema, incluyendo la definición de políticas, roles, responsabilidades, procesos y controles asociados a la gestión de IA.
Entre las actividades clave se encuentran:

- Redacción y aprobación de la política de IA.
- Diseño de procedimientos para el desarrollo, validación y mantenimiento de modelos de IA.
- Definición de un mapa de procesos y su interrelación con los sistemas existentes (como el SGSI).
- Diseño de indicadores de desempeño y mecanismos de auditoría interna.
  Al culminar esta fase, el proyecto contará con un **marco documental consolidado** que servirá de guía para la implementación operativa del sistema.

Fase 3: Implementación operativa

Esta etapa corresponde a la puesta en marcha de los procedimientos definidos. Se establecerán entornos de prueba controlados para validar los modelos de IA y verificar que cumplan con los criterios de seguridad, ética y rendimiento.
Las actividades principales son:

- Entrenamiento de los modelos de IA con conjuntos de datos validados.
- Aplicación de controles de acceso y auditoría.
- Ejecución de pruebas piloto en entornos seguros.
- Capacitación del personal involucrado en el uso y mantenimiento del SGIA.

El resultado esperado es que los procesos de IA queden operativos bajo un **entorno controlado y conforme a los lineamientos normativos**.

Fase 4: Monitoreo y evaluación

Una vez implementado el sistema, se establecerá un mecanismo de supervisión continua para verificar su desempeño.

Las actividades incluyen:

- Seguimiento de indicadores de precisión, confiabilidad y cumplimiento ético.
- Revisión de logs de auditoría y trazabilidad de decisiones automatizadas.
- Elaboración de reportes periódicos de desempeño del SGIA.
- Aplicación de auditorías internas semestrales.

Esta fase permitirá identificar desviaciones o no conformidades y aplicar medidas correctivas de forma oportuna.

Fase 5: Mejora continua

Basada en los resultados de la fase anterior, se actualizarán políticas, procedimientos y modelos de IA para mantener la conformidad con la norma y responder a los cambios tecnológicos o regulatorios.

Las actividades clave son:

- Análisis de resultados de auditorías y retroalimentación de usuarios.
- Revisión y actualización de la política de IA.
- Incorporación de nuevas técnicas o herramientas de inteligencia artificial.
- Reentrenamiento de modelos con datos actualizados.

El propósito de esta fase es consolidar una cultura de mejora continua que mantenga la efectividad del SGIA a largo plazo.

4.2 Recursos y competencias necesarias

La implementación exitosa del SGIA requerirá tanto **recursos humanos especializados** como **infraestructura tecnológica adecuada**.
En cuanto a recursos humanos, se contará con un **equipo multidisciplinario** conformado por ingenieros de software, especialistas en seguridad informática, analistas de datos, expertos en ética de IA y personal administrativo. Este equipo será responsable de diseñar, ejecutar y auditar los procesos del SGIA, asegurando el cumplimiento de las políticas definidas.

En el ámbito tecnológico, se necesitarán servidores dedicados para el entrenamiento y despliegue de modelos, bases de datos seguras para el almacenamiento de registros, herramientas de control de versiones (como Git), plataformas de auditoría y sistemas de monitoreo de desempeño. También se recomienda el uso de frameworks especializados como TensorFlow, Scikit-learn o PyTorch, que facilitan la trazabilidad y documentación de los modelos.

La capacitación continua del personal es un factor clave. Por ello, se implementarán **programas de formación y concienciación** sobre los principios éticos, legales y técnicos de la IA. Esto garantizará que todos los involucrados comprendan la importancia del SGIA y participen activamente en su correcta ejecución.

4.3 Indicadores de desempeño y evaluación

Para evaluar la eficacia del SGIA, se definirán **indicadores clave de desempeño (KPI)** que reflejen el cumplimiento de los objetivos estratégicos y operativos. Algunos de los más relevantes son:

- **Cumplimiento normativo:** porcentaje de requisitos de la ISO/IEC 42001 implementados y verificados.
- **Precisión de los modelos:** nivel de exactitud de los algoritmos en las tareas asignadas.
- **Tasa de incidentes éticos o de seguridad:** cantidad de desviaciones detectadas por periodo.
- **Nivel de satisfacción del usuario:** percepción de los usuarios sobre la transparencia y confiabilidad del sistema.
- **Tiempo promedio de respuesta ante no conformidades:** eficiencia en la gestión de acciones correctivas.

Estos indicadores se recopilarán periódicamente y se analizarán en reuniones de revisión de la dirección, donde se tomarán decisiones orientadas a la mejora continua del sistema.

4.4 Cronograma tentativo

El plan de implementación se desarrollará en un periodo aproximado de **12 meses**, distribuido de la siguiente manera:

- Meses 1–2: Diagnóstico inicial y análisis de brechas.
- Meses 3–4: Diseño del SGIA y elaboración documental.
- Meses 5–7: Implementación operativa y pruebas piloto.
- Meses 8–10: Monitoreo y evaluación de desempeño.
- Meses 11–12: Auditoría interna y mejora continua.

Este cronograma podrá ajustarse según la disponibilidad de recursos, el nivel de complejidad técnica y la madurez digital del sistema.

5. Conclusiones y recomendaciones

La aplicación de la norma **ISO/IEC 42001:2023** en el proyecto *Gestor de Proyectos* permite fortalecer la **gobernanza y el control ético** del uso de la inteligencia artificial dentro de la plataforma. Su implementación promueve la transparencia, la seguridad y la responsabilidad en los procesos automatizados, garantizando que los modelos de IA sean confiables y estén alineados con los valores organizacionales.

El **Sistema de Gestión de Inteligencia Artificial (SGIA)** planteado contribuye a establecer políticas claras, roles definidos y mecanismos de evaluación continua, lo que asegura la trazabilidad y el cumplimiento normativo. Además, su integración con el sistema de gestión de seguridad de la información basado en la **ISO/IEC 27001** fortalece la protección de datos y mejora la confianza de los usuarios.

En conclusión, la adopción del SGIA representa un paso estratégico hacia una gestión tecnológica más segura, ética y sostenible. Al implementar la ISO/IEC 42001, el *Gestor de Proyectos* se posiciona como una iniciativa responsable, innovadora y orientada a la mejora continua.

Recomendaciones

- Mantener actualizada la documentación del SGIA y sus políticas de IA.
- Capacitar periódicamente al personal en ética, seguridad y gestión de riesgos de IA.
- Realizar auditorías internas semestrales para evaluar el cumplimiento de la norma.
- Promover la participación de los usuarios en la retroalimentación y mejora del sistema.
- Considerar, a mediano plazo, la certificación formal en **ISO/IEC 42001**.