REVISTA TÓPICOS
ISSN 2965-6672 | Qualis A2

O PAPEL DO CONSELHO DE ADMINISTRAÇÃO NA GESTÃO DE RISCOS EMERGENTES DE INTELIGÊNCIA ARTIFICIAL E A IMPLEMENTAÇÃO DA ISO/IEC 42001

THE ROLE OF THE BOARD OF DIRECTORS IN MANAGING EMERGING RISKS OF ARTIFICIAL INTELLIGENCE AND THE IMPLEMENTATION OF ISO/IEC 42001

Ciências Exatas e da Terra, Engenharias • 13/06/2026

REGISTRO DOI: 10.70773/revistatopicos/781229254

Vladimir Nunan Ribeiro Soares[1]

RESUMO

A rápida e disruptiva evolução da Inteligência Artificial (IA) tem transformado radicalmente o cenário corporativo global, introduzindo um espectro sem precedentes de oportunidades e desafios complexos que transcendem a esfera puramente tecnológica. Este artigo científico aprofunda a análise do papel crítico do conselho de administração na governança e gestão dos riscos emergentes e inerentes à IA, com um foco particular na implementação estratégica da norma internacional ISO/IEC 42001:2023. Realizamos uma análise integrativa de insights de lideranças da indústria e princípios de governança corporativa, confrontando-os e complementando-os com os requisitos e princípios fundamentais de um Sistema de Gestão de Inteligência Artificial (SGIA/AIMS). O estudo destaca a imperativa necessidade de uma abordagem proativa, estruturada, multidisciplinar e adaptativa para a governança da IA, enfatizando a importância da liderança executiva, da avaliação rigorosa e contínua de riscos, da ética intrínseca ao design, da transparência algorítmica e da melhoria contínua dos sistemas. Argumenta-se que a ISO 42001 oferece o framework operacional e auditável necessário para materializar a visão estratégica do conselho, permitindo que as organizações equilibrem a inovação acelerada com a responsabilidade social e fiduciária, mitiguem vieses algorítmicos, garantam a conformidade com um cenário regulatório global em constante mutação (como o EU AI Act) e construam uma base sólida e duradoura de confiança com todas as partes interessadas, desde acionistas a consumidores e reguladores.

Palavras-chave: Governança de Inteligência Artificial; ISO/IEC 42001; Conselho de Administração; Gestão de Riscos; Sistema de Gestão de Inteligência Artificial (SGIA); Governança Corporativa; Ética em Inteligência Artificial; Conformidade Regulatória.

ABSTRACT

The rapid and disruptive evolution of Artificial Intelligence (AI) has fundamentally transformed the global corporate landscape, introducing an unprecedented range of opportunities and complex challenges that extend far beyond the technological domain. This scientific article provides an in-depth analysis of the critical role of the board of directors in the governance and management of emerging AI-related risks, with a particular focus on the strategic implementation of the international standard ISO/IEC 42001:2023. An integrative analysis was conducted, combining insights from industry leaders and corporate governance principles with the requirements and foundational principles of an Artificial Intelligence Management System (AIMS). The study highlights the urgent need for a proactive, structured, multidisciplinary, and adaptive approach to AI governance, emphasizing the importance of executive leadership, continuous risk assessment, ethics by design, algorithmic transparency, and ongoing improvement. It argues that ISO 42001 provides the operational and auditable framework necessary to translate the board's strategic vision into practice, enabling organizations to balance accelerated innovation with social and fiduciary responsibility, mitigate algorithmic bias, ensure compliance with an evolving global regulatory environment (such as the EU AI Act), and build a strong and lasting foundation of trust among all stakeholders, including shareholders, customers, and regulators.

Keywords: Artificial Intelligence Governance; ISO/IEC 42001; Board of Directors; Risk Management; Artificial Intelligence Management System (AIMS); Corporate Governance; AI Ethics; Regulatory Compliance.

1. INTRODUÇÃO: A IA COMO IMPERATIVO ESTRATÉGICO E DE GOVERNANÇA

A Inteligência Artificial (IA) deixou de ser uma promessa futurista para se tornar uma realidade onipresente, redefinindo indústrias, otimizando processos e impulsionando a inovação em uma escala sem precedentes. No entanto, essa transformação acelerada não está isenta de complexidades e riscos significativos. Questões como viés algorítmico, privacidade de dados em larga escala, segurança cibernética sofisticada, responsabilidade jurídica, transparência de modelos "caixa-preta" e o impacto socioeconômico da automação exigem uma atenção rigorosa por parte das lideranças corporativas [1]. A proliferação de sistemas de IA, especialmente os modelos generativos e os agentes autônomos, introduz uma camada adicional de complexidade, onde as decisões podem ser tomadas com pouca ou nenhuma intervenção humana direta, levantando questões profundas sobre controle, previsibilidade e ética.

Nesse contexto, o conselho de administração emerge como o guardião final da integridade e da estratégia organizacional. Tradicionalmente responsável pela supervisão estratégica e pela gestão de riscos fiduciários, o conselho agora enfrenta o imperativo de estender sua competência para a esfera da IA. A governança da IA não é meramente uma questão técnica delegável ao departamento de TI; é uma questão de sobrevivência estratégica que afeta diretamente a reputação da marca, a conformidade regulatória, o desempenho financeiro e a sustentabilidade a longo prazo da empresa [2]. A falha em abordar adequadamente os riscos da IA pode resultar em litígios caros, danos à reputação, perda de confiança do cliente e desvantagem competitiva.

A publicação da norma ISO/IEC 42001:2023, a primeira norma internacional certificável para Sistemas de Gestão de Inteligência Artificial (AIMS - Artificial Intelligence Management Systems), oferece um roteiro estruturado e globalmente reconhecido para que as organizações naveguem por esse território incerto. A norma fornece um framework abrangente que permite às empresas estabelecer, implementar, manter e melhorar continuamente seus processos de IA, garantindo que a tecnologia seja utilizada de forma ética, eficiente e responsável [3]. Sua adoção representa um compromisso formal com a gestão responsável da IA, um diferencial competitivo em um mercado cada vez mais consciente dos riscos e benefícios dessa tecnologia.

Este artigo tem como objetivo principal analisar a intersecção crítica entre as responsabilidades fiduciárias e estratégicas do conselho de administração na gestão de riscos de IA e a estrutura de governança operacional proposta pela ISO/IEC 42001. Através de uma análise detalhada de relatórios da indústria, literatura científica e requisitos normativos, buscamos demonstrar como a adoção e a certificação na ISO 42001 podem capacitar os conselhos a exercerem uma supervisão eficaz e proativa, transformando riscos potenciais em vantagens competitivas sustentáveis e duradouras. Além disso, exploraremos a sinergia da ISO 42001 com outros frameworks globais, como o EU AI Act e o NIST AI RMF, e discutiremos estudos de caso e desafios práticos de implementação.

2. FUNDAMENTAÇÃO TEÓRICA: GOVERNANÇA CORPORATIVA E A REVOLUÇÃO DA IA

2.1. A Evolução da Governança Corporativa na Era Digital

A governança corporativa refere-se ao sistema de regras, práticas e processos pelos quais uma empresa é dirigida e controlada. Ela envolve o equilíbrio dos interesses de muitas partes interessadas, como acionistas, gestão, clientes, fornecedores, financiadores, governo e comunidade. Com a ascensão da IA no "core business" das empresas, os modelos tradicionais de governança enfrentam uma pressão sem precedentes para se adaptarem à velocidade, à complexidade e à opacidade dos algoritmos [4]. A digitalização e, mais recentemente, a inteligência artificial, exigem que os conselhos expandam seu foco de riscos financeiros e operacionais tradicionais para incluir riscos tecnológicos, éticos e reputacionais de uma nova ordem.

Os conselhos de administração devem agora lidar com o que especialistas chamam de "riscos de segunda ordem" da IA – aqueles que surgem não do mau funcionamento técnico, mas das consequências sociais e éticas do funcionamento correto do sistema, como a exclusão inadvertida de grupos minoritários em processos de crédito ou recrutamento, ou a disseminação de desinformação por sistemas generativos. A complexidade e a natureza emergente desses riscos exigem uma reavaliação fundamental das estruturas de governança existentes [5].

2.2. O Novo Mandato do Conselho na Gestão de Riscos de IA: Insights Contemporâneos

Análises recentes de lideranças da indústria e especialistas em governança corporativa identificam uma mudança de paradigma inegável: a IA não é mais um "item de pauta" ocasional ou uma preocupação exclusiva do departamento de TI, mas um risco estratégico central que exige fluência técnica e vigilância constante

no mais alto nível da organização. Essas análises estabelecem quatro prioridades fundamentais e interconectadas para os conselhos de administração:

Prioridade Estratégica	**Descrição Detalhada para o Conselho de Administração**
1. Fortalecer a Governança e a Responsabilidade (Accountability)	O conselho deve garantir que existam estruturas claras de governança para a IA, com responsabilidades bem definidas e rastreáveis em toda a organização, desde a concepção até a implantação e monitoramento. Isso inclui a criação de comitês de IA ou a expansão de mandatos de comitês existentes para incluir a supervisão de IA.
2. Equilibrar Inovação e Risco	É crucial que os conselhos compreendam os riscos associados à IA sem sufocar a inovação. Isso requer o estabelecimento de um "apetite de risco" claro e bem articulado para a IA, que permita a experimentação controlada e a avaliação contínua dos riscos e benefícios. A inovação não deve ser sacrificada, mas sim guiada por princípios de responsabilidade.
3. Construir Capacidade de Gestão de Risco em Tempo Real	A natureza dinâmica e em constante evolução da IA exige que as empresas desenvolvam a capacidade de identificar, avaliar e mitigar riscos em tempo real, em vez de depender de abordagens reativas ou auditorias anuais estáticas. Isso implica investir em ferramentas de monitoramento contínuo, telemetria de modelos e equipes especializadas em resposta a incidentes de IA.
4. Melhorar a Fluência em IA	Os membros do conselho precisam desenvolver um nível suficiente de compreensão sobre a IA – seus fundamentos, capacidades, limitações e implicações éticas – para fazer perguntas pertinentes, desafiar suposições da gestão e tomar decisões informadas. Isso pode envolver treinamento contínuo, a inclusão de especialistas em IA no conselho ou a contratação de consultores externos.

Um ponto central e inovador discutido por especialistas é a transição de uma mentalidade focada na proteção de dados (uma preocupação predominante na década passada com regulamentações como GDPR e LGPD) para a proteção do julgamento. À medida que sistemas de IA começam a tomar decisões autônomas ou a influenciar pesadamente o julgamento humano em áreas críticas como finanças, saúde ou justiça, o conselho deve garantir que esses sistemas operem com uma "bússola moral" alinhada aos valores da empresa e da sociedade. A ascensão da IA agentica, onde os sistemas podem planejar, agir e se adaptar autonomamente, intensifica a necessidade de supervisão humana e de mecanismos de controle robustos, pois a cadeia de causalidade e responsabilidade pode se tornar difusa [1].

3. ISO/IEC 42001:2023 – O FRAMEWORK DE OPERACIONALIZAÇÃO DA GOVERNANÇA DE IA

A ISO/IEC 42001:2023, intitulada "Tecnologia da Informação – Inteligência Artificial – Sistema de Gestão de Inteligência Artificial", é um marco significativo na padronização da governança de IA. Ela foi projetada para preencher a lacuna entre as intenções éticas de alto nível e a execução técnica diária, fornecendo requisitos e orientações para estabelecer, implementar, manter e melhorar continuamente um Sistema de Gestão de Inteligência Artificial (AIMS) [3]. A norma é aplicável a qualquer organização, independentemente do tipo, tamanho ou natureza, que desenvolva, forneça ou utilize sistemas de IA, oferecendo uma linguagem comum e um conjunto de práticas recomendadas para a gestão responsável da IA.

3.1. Estrutura e Princípios Fundamentais da ISO 42001

A ISO 42001 segue a estrutura de alto nível (Annex SL) comum a outras normas de sistemas de gestão, como ISO 27001 (Segurança da Informação), ISO 9001 (Gestão da Qualidade) e ISO 31000 (Gestão de Riscos). Essa harmonização facilita a integração da governança de IA com os sistemas de gestão existentes de uma organização, reduzindo a duplicação de esforços e promovendo uma abordagem holística [6]. As cláusulas principais da norma são:

- Cláusula 4: Contexto da Organização: Exige que a organização determine suas questões internas e externas relevantes para o AIMS, compreenda as necessidades e expectativas das partes interessadas e defina o escopo do sistema de gestão de IA [7]. Isso inclui a identificação de fatores tecnológicos (ex: IA generativa), éticos (ex: viés algorítmico), legais (ex: EU AI Act) e regulatórios que influenciam o uso da IA. Para o conselho, isso significa entender não apenas as ferramentas internas, mas como a IA de terceiros e as tendências globais afetam o modelo de negócio.

- Cláusula 5: Liderança: Esta é a cláusula mais crítica para o conselho, pois enfatiza o compromisso visível da alta direção com o AIMS. A liderança deve estabelecer a política de IA, atribuir responsabilidades e autoridades, e garantir que os recursos necessários estejam disponíveis. Isso alinha diretamente com a necessidade de o conselho de administração assumir a responsabilidade pela governança da IA, não apenas delegando, mas ativamente supervisionando e promovendo uma cultura de IA responsável [7].

- Cláusula 6: Planejamento: Foca na identificação e tratamento de riscos e oportunidades relacionados à IA. Diferente de riscos

tradicionais, o risco de IA é frequentemente probabilístico, multifacetado e mutável. A ISO 42001 exige uma metodologia de avaliação de risco que considere impactos éticos e sociais (ex: discriminação, manipulação), além de técnicos (ex: falhas de segurança, imprecisão). Este é um pilar central para a gestão proativa de riscos de IA, exigindo que o conselho compreenda e aprove o apetite de risco da organização [7].

- Cláusula 7: Suporte: Aborda os recursos necessários para o AIMS, incluindo competência, conscientização, comunicação e informação documentada. Garante que a organização tenha a capacidade, o conhecimento e as ferramentas para operar seu sistema de gestão de IA de forma eficaz. Isso inclui programas de treinamento para funcionários e membros do conselho, garantindo a "fluência em IA" em todos os níveis [7].

- Cláusula 8: Operação: Detalha os controles operacionais para o ciclo de vida da IA, desde o projeto e desenvolvimento até a implantação e manutenção. Inclui a necessidade de Avaliações de Impacto de IA (AIA) para sistemas de alto risco, gestão de mudanças, e processos para garantir a qualidade dos dados e modelos. Para o conselho, o destaque aqui é a garantia de que as AIAs sejam realizadas de forma independente e que suas recomendações sejam implementadas [7].

- Cláusula 9: Avaliação de Desempenho: Requer o monitoramento, medição, análise e avaliação do desempenho do AIMS. Auditorias internas e análises críticas pela direção são essenciais para garantir a eficácia contínua do sistema. Esta cláusula fornece ao conselho os mecanismos para verificar a conformidade e a eficácia das políticas de IA [7].

- Cláusula 10: Melhoria: Foca na melhoria contínua do AIMS por meio da identificação de não conformidades, ações corretivas e otimização geral do sistema. A natureza dinâmica da IA exige que o AIMS seja um sistema vivo, adaptando-se a novas tecnologias, riscos e regulamentações [7].

3.2. Detalhamento dos Controles do Anexo a: Um Guia Prático para a Governança

O Anexo A da ISO 42001 é particularmente valioso, pois fornece uma lista de controles específicos que são essenciais para mitigar os riscos identificados por especialistas em governança de IA e para operacionalizar as cláusulas da norma. Estes controles não são meramente técnicos, mas representam salvaguardas de governança que garantem a transparência, a responsabilidade e a confiabilidade do sistema de IA [3]. Abaixo, organizamos esses controles em categorias estratégicas, destacando sua relevância para a supervisão do conselho:

Categoria de Controle	Objetivo de Governança para o Conselho	Exemplos de Implementação e Supervisão
A.5 Políticas Relacionadas à IA	Assegurar que a organização possua diretrizes claras e aprovadas para o uso responsável da IA.	O conselho deve revisar e aprovar a Política de IA da organização, garantindo que ela reflita os valores éticos e os requisitos regulatórios. Deve questionar sobre a comunicação e treinamento dessas políticas.
A.6 Recursos para IA	Garantir que a organização aloque recursos adequados (humanos, financeiros,	O conselho deve aprovar orçamentos para investimentos em infraestrutura de IA segura,

	tecnológicos) para o desenvolvimento, implantação e gestão responsável da IA.	contratação de talentos especializados em ética e segurança de IA, e programas de capacitação interna.
A.7 Análise de Impacto da IA (AIA)	Assegurar que os impactos potenciais (éticos, sociais, legais, de segurança) dos sistemas de IA sejam sistematicamente avaliados antes da implantação e durante seu ciclo de vida.	O conselho deve exigir relatórios periódicos das AIAs para sistemas de alto risco, questionando as metodologias utilizadas, os resultados e as ações mitigadoras propostas. Deve garantir a independência da equipe que realiza a AIA.
A.8 Ciclo de Vida do Sistema de IA	Garantir que a governança da IA seja integrada em todas as fases do ciclo de vida do sistema, desde a concepção até a desativação.	O conselho deve supervisionar a implementação de "portões de decisão" (gatekeeping) em cada fase do desenvolvimento da IA, exigindo aprovações formais e documentação de conformidade antes de avançar.
A.9 Dados para IA	Assegurar a qualidade, integridade, privacidade e segurança dos dados utilizados para treinar e operar sistemas de IA, mitigando vieses e garantindo a conformidade.	O conselho deve questionar sobre as práticas de curadoria de dados, técnicas de anonimização, auditorias de viés em conjuntos de dados e a conformidade com regulamentações de privacidade (LGPD, GDPR).
A.10 Transparência e Explicabilidade	Promover a compreensão sobre como os sistemas de IA funcionam e tomam decisões, especialmente em contextos críticos.	O conselho deve exigir que a gestão demonstre a explicabilidade dos modelos de IA, especialmente aqueles que afetam decisões sobre indivíduos, e que mecanismos de comunicação clara sejam estabelecidos para as partes interessadas.

A.11 Supervisão Humana	Garantir que haja um nível apropriado de supervisão humana sobre os sistemas de IA, especialmente os autônomos, para prevenir resultados indesejados e garantir a responsabilidade.	O conselho deve entender a arquitetura de "Human-in-the-loop" (HITL), "Human-on-the-loop" (HOTL) ou "Human-in-command" (HIC) para sistemas críticos, e garantir que os operadores humanos estejam devidamente treinados e capacitados para intervir.
A.12 Responsabilidade e Remediação	Estabelecer processos claros para atribuir responsabilidade por resultados de IA e para remediar danos ou não conformidades.	O conselho deve garantir que existam planos de resposta a incidentes de IA, mecanismos de reclamação para partes afetadas e processos de investigação para falhas éticas ou de segurança relacionadas à IA.

3.3. Sinergia Entre o Papel do Conselho e a ISO 42001

A ISO 42001 oferece o "como" para as diretrizes estratégicas e as prioridades estabelecidas para o conselho de administração. Enquanto o conselho define a visão, o apetite de risco e os princípios éticos para a IA, a norma fornece o framework operacional para traduzir essa visão em práticas concretas, mensuráveis e auditáveis. Por exemplo:

- A exigência da Cláusula 5 (Liderança) da ISO 42001 de que a alta direção estabeleça uma política de IA e atribua responsabilidades complementa diretamente a prioridade do conselho de fortalecer a governança e a responsabilidade [1, 7].

- A Cláusula 6 (Planejamento), com seu foco na avaliação de riscos e oportunidades de IA, fornece a metodologia para o

conselho equilibrar inovação e risco e construir capacidade de gestão de risco em tempo real [1, 7].

- Os requisitos de competência e conscientização na Cláusula 7 (Suporte) apoiam a necessidade do conselho de melhorar a fluência em IA em toda a organização, garantindo que os membros do conselho e a equipe executiva possuam o conhecimento necessário para supervisionar a IA de forma eficaz [1, 7].

A implementação da ISO 42001 não apenas ajuda as organizações a gerenciar riscos de forma sistemática, mas também demonstra um compromisso mensurável com o desenvolvimento e uso responsável da IA, o que é cada vez mais valorizado por reguladores, investidores e partes interessadas [8]. A certificação na norma pode servir como um selo de confiança, diferenciando a organização no mercado e atraindo talentos e parceiros que valorizam a responsabilidade na IA.

4. ANÁLISE CRÍTICA: A IA AGENTICA, AUTONOMIA E O DESAFIO DA SUPERVISÃO

Um dos pontos mais inovadores e, ao mesmo tempo, mais preocupantes discutidos por especialistas em governança de IA é a ascensão da IA Agentica. Diferente da IA tradicional, que responde a comandos específicos e opera dentro de parâmetros estritamente definidos, a IA agentica tem a capacidade de planejar ações, interagir com outros sistemas, aprender com o ambiente e tomar decisões intermediárias para atingir um objetivo final, muitas vezes sem intervenção humana direta. Exemplos incluem agentes autônomos de negociação financeira, sistemas de otimização de cadeia de suprimentos e assistentes virtuais avançados.

4.1. Riscos de Autonomia e a Necessidade de "Human-in-command"

A crescente autonomia da IA cria um desafio fundamental de responsabilidade e controle. Se um agente de IA toma uma decisão que resulta em perda financeira significativa, dano reputacional ou até mesmo consequências sociais adversas, quem é o responsável final? A ISO 42001 aborda essa questão crucial através da exigência de supervisão humana apropriada, que pode ser implementada em diferentes níveis:

- Human-in-the-loop (HITL): O humano está ativamente envolvido em cada decisão ou etapa do processo da IA, revisando e aprovando as ações do sistema. Embora ofereça alto controle, pode ser ineficiente para sistemas de alta velocidade.

- Human-on-the-loop (HOTL): O humano monitora o sistema de IA e intervém apenas quando necessário, geralmente em caso de desvio ou anomalia. Exige sistemas de alerta robustos e capacidade de intervenção rápida.

- Human-in-command (HIC): O humano define os objetivos e os limites operacionais do sistema de IA, mas o sistema tem ampla autonomia para operar dentro desses limites. O humano mantém a capacidade de desligar ou reconfigurar o sistema. Este é o modelo mais relevante para IA agentica avançada, onde a intervenção contínua é impraticável, mas a responsabilidade final permanece humana [11].

O conselho deve questionar a gerência sobre os "guardrails" (proteções) e os mecanismos de "kill switch" (botão de desligar)

colocados nesses agentes autônomos. A implementação da ISO 42001 fornece o mecanismo para documentar, testar e auditar esses controles, garantindo que a autonomia da IA nunca ultrapasse a autoridade delegada pela governança humana e que a responsabilidade final seja sempre atribuível.

Um risco emergente associado à IA agentica é o "Agentic Drift", onde agentes de IA, ao interagir e aprender, podem desenvolver comportamentos ou estratégias imprevistas que se desviam dos objetivos originais ou dos limites éticos estabelecidos. Isso exige monitoramento contínuo e a capacidade de reavaliar e recalibrar os sistemas de IA de forma iterativa.

4.2. Métricas de Sucesso e o Papel do Auditor Interno de IA

Estudos sobre governança de IA destacam que muitas empresas ainda usam "métricas suaves" (soft metrics) para medir o sucesso da IA, como economia de tempo de desenvolvedores ou aumento da velocidade de processamento, que nem sempre se traduzem em lucro direto ou em benefícios sociais tangíveis. A ISO 42001, na sua Cláusula 9 (Avaliação de Desempenho), incentiva a criação de KPIs (Key Performance Indicators) que vão além do financeiro e técnico, incluindo:

- KPIs Técnicos: Acurácia do modelo, precisão, recall, F1-score, latência, consumo de recursos.

- KPIs de Ética e Responsabilidade: Níveis de viés detectados e mitigados, explicabilidade das decisões do modelo, conformidade com políticas éticas internas, número de reclamações relacionadas à IA.

- KPIs de Negócio: Retorno sobre o Investimento (ROI) real (considerando custos de governança e infraestrutura), satisfação do cliente, retenção de talentos, reputação da marca.

- KPIs de Governança: Frequência de AIAs realizadas, número de não conformidades identificadas e resolvidas, taxa de participação em treinamentos de IA para o conselho e executivos.

Para garantir a integridade e a objetividade dessas métricas, o papel do Auditor Interno de IA torna-se crucial. Este profissional, ou equipe, deve ser independente das equipes de desenvolvimento e operação de IA, reportando-se diretamente ao conselho ou a um comitê de auditoria. Sua função é verificar a conformidade com a ISO 42001, a eficácia dos controles e a precisão dos relatórios de desempenho, fornecendo ao conselho uma visão imparcial sobre a postura de risco da IA da organização.

5. IMPLEMENTAÇÃO PRÁTICA E INTEGRAÇÃO REGULATÓRIA: UM GUIA PARA CONSELHOS

A implementação da ISO 42001 não ocorre no vácuo. Ela deve ser integrada a outras regulamentações e frameworks globais para garantir uma cobertura total e uma abordagem de governança de IA verdadeiramente robusta. Para os conselhos, entender essa paisagem interconectada é fundamental.

5.1. Análise Comparativa de Frameworks Globais: ISO 42001, EU AI Act e NIST AI RMF

É fundamental que os conselhos compreendam como a ISO 42001 se posiciona em relação a outros frameworks globais de governança

de IA. Embora todos busquem promover a IA responsável, eles têm focos e mecanismos distintos:

Característica	ISO/IEC 42001:2023	EU AI Act	NIST AI Risk Management Framework (AI RMF)
Natureza	Norma de Sistema de Gestão (certificável)	Regulamentação legal (obrigatória)	Framework voluntário de gestão de riscos
Foco Principal	Como gerenciar a IA de forma responsável (processos, controles)	O que é permitido/proibido e requisitos para sistemas de alto risco	Como identificar, avaliar e mitigar riscos de IA
Mecanismo	Estabelece um AIMS auditável e certificável	Define obrigações legais e penalidades para não conformidade	Fornece um guia de melhores práticas e funções de risco (Govern, Map, Measure, Manage)
Abordagem	Orientada a processos e melhoria contínua	Baseada em risco (classificação de sistemas)	Baseada em funções e atividades de gestão de risco
Sinergia	Fornece o sistema de gestão para cumprir os requisitos do EU AI Act e operacionalizar o NIST AI RMF.	Define os requisitos legais que a ISO 42001 pode ajudar a cumprir.	Oferece uma metodologia de risco que pode ser integrada ao AIMS da ISO 42001.

A ISO 42001 é, portanto, o "elo de ligação" que fornece o sistema de gestão auditável para cumprir os requisitos do EU AI Act e operacionalizar as funções de risco do NIST AI RMF [9]. Para um

conselho, a certificação ISO 42001 demonstra um compromisso proativo e verificável com a conformidade regulatória e a gestão de riscos, independentemente da jurisdição.

5.2. Estudos de Caso e Desafios de Implementação

Embora a ISO 42001 seja relativamente nova, já existem exemplos e discussões sobre sua implementação:

- Microsoft: A Microsoft tem sido uma das primeiras grandes corporações a alinhar seus princípios de IA responsável com a ISO 42001, utilizando a norma para validar seu "Responsible AI Standard" interno. Isso demonstra como a ISO 42001 pode ser usada para formalizar e auditar práticas de IA já existentes em grandes empresas [12].

- PMEs vs. Grandes Corporações: Os desafios de implementação variam significativamente. Pequenas e Médias Empresas (PMEs) podem enfrentar custos iniciais mais altos e falta de recursos especializados, enquanto grandes corporações lidam com a complexidade de integrar a ISO 42001 em sistemas legados e em uma vasta gama de aplicações de IA [10]. Para PMEs, a modularidade da ISO 42001 permite uma implementação faseada, focando nos sistemas de IA de maior risco primeiro.

Os desafios comuns na implementação incluem:

- Lacuna de Conhecimento: A necessidade de capacitar equipes e conselhos sobre os princípios da IA e da norma.

- Gestão de Dados: Garantir a qualidade, a privacidade e a segurança dos dados em todo o ciclo de vida da IA.

- Cultura Organizacional: Promover uma cultura de responsabilidade e ética em IA em todos os níveis.

- Integração: Alinhar a ISO 42001 com outros sistemas de gestão e regulamentações existentes.

5.3. Guia Prático de Implementação para Conselhos de Administração

Para conselhos que buscam liderar a implementação da ISO 42001 e a governança de IA, os seguintes passos práticos são recomendados:

1. realizar um Inventário Abrangente de Sistemas de IA: Mapear todos os sistemas de IA em uso, incluindo "Shadow AI" (sistemas não oficialmente aprovados ou monitorados). Entender onde a IA está sendo usada, por quem e com que propósito é o primeiro passo para a governança. Isso inclui sistemas desenvolvidos internamente e soluções de terceiros.

2. definir o Apetite de Risco Ético e Estratégico: Em colaboração com a gestão, o conselho deve articular claramente o nível de risco que a organização está disposta a aceitar em relação à IA, considerando não apenas riscos financeiros, mas também éticos, sociais e reputacionais. Isso informará as decisões sobre quais sistemas de IA desenvolver e como gerenciá-los.

3. estabelecer um Comitê de Ética em IA ou Expandir Mandatos: Criar um comitê dedicado à ética em IA ou expandir o mandato de um comitê existente (ex: risco, auditoria) para

incluir a supervisão da IA. Este comitê deve ter membros com diversas formações, incluindo especialistas em tecnologia, ética, direito e negócios.

4. investir em Capacitação e Fluência em IA: Implementar programas de treinamento contínuo para membros do conselho e executivos sobre os fundamentos da IA, seus riscos, oportunidades e as exigências da ISO 42001. A fluência em IA é essencial para uma supervisão eficaz.

5. exigir Monitoramento Contínuo e Relatórios Transparentes: O conselho deve exigir da gestão relatórios regulares sobre o desempenho dos sistemas de IA, incluindo métricas de viés, explicabilidade, segurança e conformidade. Isso deve incluir o monitoramento de "Model Drift" (degradação do desempenho do modelo ao longo do tempo) e a eficácia das ações mitigadoras.

6. promover uma Cultura de IA Responsável: A governança de IA não é apenas sobre processos, mas sobre pessoas. O conselho deve promover ativamente uma cultura organizacional que valorize a ética, a transparência e a responsabilidade no desenvolvimento e uso da IA, incentivando a denúncia de preocupações e a aprendizagem contínua.

6. CONCLUSÃO: LIDERANDO NA ERA DA IA RESPONSÁVEL

A gestão de riscos de Inteligência Artificial é, fundamentalmente, uma questão de governança corporativa moderna e um imperativo estratégico para a sobrevivência e prosperidade das organizações. Como destacado por análises recentes da indústria, o conselho de administração não pode mais se dar ao luxo de tratar a IA como uma

"caixa-preta" tecnológica ou uma responsabilidade delegada sem supervisão. A responsabilidade pela integridade, ética e eficácia dos sistemas de IA reside no topo da organização, exigindo uma abordagem proativa e informada.

A norma ISO/IEC 42001:2023 surge como a solução ideal e o framework mais abrangente para esse desafio. Ela fornece a estrutura necessária para que as empresas saiam do discurso ético abstrato e entrem na prática de gestão rigorosa e auditável. Ao implementar a ISO 42001, o conselho garante que a organização tenha os controles necessários para mitigar riscos de viés, segurança, privacidade e autonomia, enquanto maximiza as oportunidades de inovação e crescimento sustentável. A norma atua como uma ponte entre a estratégia de alto nível e a execução operacional, garantindo que os princípios de IA responsável sejam incorporados em cada etapa do ciclo de vida do sistema.

Em última análise, a adoção da ISO 42001 não é apenas uma escolha de conformidade regulatória, mas uma decisão estratégica que fortalece a resiliência organizacional, protege o valor da marca, atrai e retém talentos, e assegura que a empresa lidere de forma ética, segura e sustentável na era da Inteligência Artificial. Os conselhos que abraçam ativamente essa responsabilidade não apenas protegem suas organizações, mas também contribuem para o desenvolvimento de uma IA que serve ao bem maior da sociedade.

REFERÊNCIAS BIBLIOGRÁFICAS

1. Batool, A. (2025). AI governance: a systematic literature review. AI and Ethics, 366.

https://link.springer.com/article/10.1007/s43681-024-00653-w. Acessado em 05 de Junho de 2026.

2. Diligent.AI governance: A guide to responsible AI for boards. https://www.diligent.com/resources/blog/ai-governance. Acessado em 05 de Junho de 2026.

3. ISO.ISO/IEC 42001:2023 - AI management systems. https://www.iso.org/standard/42001. Acessado em 05 de Junho de 2026.

4. Ludwig, L. (2025). The Role of AI in Risk Management: Benefits, Challenges, and.... https://digitalcommons.bryant.edu/cgi/viewcontent.cgi?article=1011&context=honors_cis. Acessado em 05 de Junho de 2026.

5. Schellman. Responsible AI Governance and ISO 42001 Explained. https://www.schellman.com/blog/iso-certifications/iso-42001-and-responsible-ai-governance. Acessado em 05 de Junho de 2026.

6. Hicomply. The Core Requirements of ISO 42001 Clauses 4–10. https://www.hicomply.com/hub/the-core-requirements-of-iso-42001-clauses-4-10. Acessado em 05 de Junho de 2026.

7. Hyperproof. ISO 42001: Paving the Way Forward for AI Governance. https://hyperproof.io/iso-42001-paving-the-way-forward-for-ai-governance/. Acessado em 05 de Junho de 2026.

8. Optro.ai. How to integrate NIST AI RMF and ISO 42001. https://optro.ai/blog/nist-ai-rmf-and-iso-42001. Acessado em 05 de Junho de 2026.

9. Cornerstone OnDemand.ISO/IEC 42001 explained: Why Responsible AI and.... https://www.cornerstoneondemand.com/resources/article/iso-iec-42001-explained/. Acessado em 05 de Junho de 2026.

10. Vanta. AI roles in ISO 42001 certification explained. https://www.vanta.com/collection/iso-42001/roles-in-iso-42001. Acessado em 05 de Junho de 2026.

11. Microsoft. ISO/IEC 42001:2023 Artificial intelligence management system. https://learn.microsoft.com/en-us/compliance/regulatory/offering-iso-42001. Acessado em 05 de Junho de 2026.

12. Trail ML. ISO 42001 Certification: Case Study. https://www.trail-ml.com/blog/iso-42001-certification-case-study-unique. Acessado em 05 de Junho de 2026.

13. EC-Council. EU AI Act vs NIST AI RMF vs ISO/IEC 42001. https://www.eccouncil.org/cybersecurity-exchange/responsible-ai-governance/eu-ai-act-nistai-rmf-and-iso-iec-42001-a-plain-english-comparison/. Acessado em 05 de Junho de 2026.

14. GSDCouncil. Designing an AI Governance Operating Model Aligned to ISO 42001. https://www.gsdcouncil.org/blogs/designing-an-ai-

governance-operating-model-aligned-to-iso-42001. Acessado em 05 de Junho de 2026.

---

[1] É doutorando (PhD Student) em Inteligência Artificial na Lund University, onde desenvolve pesquisa sobre taxonomias de estados não ordinários de consciência utilizando Inteligência Artificial, Processamento de Linguagem Natural, aprendizado de máquina e Grandes Modelos de Linguagem (LLMs). Seu trabalho integra um projeto internacional voltado ao desenvolvimento e à validação empírica de uma taxonomia de estados de consciência a partir da análise de relatos em primeira pessoa de experiências conscientes. Atua também como Pesquisador Sênior em Inteligência Artificial Educacional no Cambridge Innovation Center (CIC), em Cambridge, Massachusetts, EUA. Sua atuação está voltada ao desenvolvimento de soluções inovadoras que integram ciência da aprendizagem, inteligência artificial avançada e ambientes digitais de ensino. Conduz pesquisas aplicadas envolvendo modelos de linguagem, agentes inteligentes e sistemas adaptativos de aprendizagem, com foco em personalização da experiência educacional, engajamento, avaliação de competências e desenvolvimento humano apoiado por IA. No CIC, contribui para o avanço de metodologias que combinam inteligência artificial e práticas pedagógicas baseadas em evidências, buscando transformar a forma como indivíduos e organizações aprendem, ensinam e se desenvolvem em escala. Mestre em Inovação e Empreendedorismo, atua como consultor, palestrante e professor nas áreas de Educação Corporativa, Desenvolvimento Humano, Liderança, Cultura Organizacional e Inteligência Artificial aplicada à aprendizagem. Possui mais de duas décadas de experiência no desenvolvimento de pessoas e organizações, tendo participado da concepção, implementação e

gestão de programas de educação corporativa, universidades corporativas e iniciativas de transformação organizacional em empresas de diversos segmentos. É fundador da Eduvem, referência nacional em Aprendizagem Corporativa e Educação Digital. Seus interesses de pesquisa e atuação concentram-se na interseção entre inteligência artificial, aprendizagem, consciência, desenvolvimento humano, inovação organizacional e transformação digital da educação. Lattes: http://lattes.cnpq.br/5147229153266247. ORCID: https://orcid.org/0009-0006-1192-2782. E-mail: acesse o artigo original para visualizar o e-mail