v7.n6.2026

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218

PROTOCOLO DE PADRONIZAÇÃO DA GOVERNANÇA DE INTELIGÊNCIA ARTIFICIAL COM BASE EM NORMAS E REGULAMENTAÇÕES INTERNACIONAIS: REVISÃO DE LITERATURA

STANDARDIZATION PROTOCOL FOR ARTIFICIAL INTELLIGENCE GOVERNANCE BASED ON INTERNATIONAL STANDARDS AND REGULATIONS: LITERATURE REVIEW

PROTOCOLO DE ESTANDARIZACIÓN PARA LA GOBERNANZA DE LA INTELIGENCIA ARTIFICIAL BASADO EN NORMAS Y REGULACIONES INTERNACIONALES: REVISIÓN DE LITERATURA

Umberto Alves Correia[1], Angelo Machado de Souza[2], Juliano Araújo Santana[3], Davis Souza Alves[4], Márcio Magera Conceição[5], Michel Souza Silva[6]

e768273

https://doi.org/10.47820/recima21.v7i6.8273

PUBLICADO: 06/2026

RESUMO

A rápida expansão dos sistemas de inteligência artificial (IA) ampliou os desafios de governança nas organizações, sobretudo quando princípios éticos, normas técnicas e obrigações regulatórias são tratados de maneira fragmentada. Este artigo propõe, com base em revisão de literatura e análise documental comparada, um protocolo de padronização para a governança de IA fundamentado em normas e regulamentações internacionais. A pesquisa, de natureza qualitativa, exploratória e descritiva, examinou um corpus de 27 referências, composto por estudos acadêmicos e por documentos normativos, regulatórios e institucionais publicados entre 2016 e 2026, incluindo ISO/IEC 42001, ISO/IEC 23894, ISO/IEC 42005, ISO/IEC 42006, NIST AI RMF, LGPD, GDPR, AI Act da União Europeia, recomendações da OECD e da UNESCO, além de documentos brasileiros vigentes ou em tramitação.

[1] Mestrando em Administração de Empresas pela Florida Christian University, na linha de pesquisa Negócios Globais. Pós-graduado em Administração de Empresas pela FAAP, extensão universitária em Gerenciamento de Empreendimentos pela FGV/SP e graduado em Processamento de Dados pela Universidade Presbiteriana Mackenzie.
[2] Mestrando em Administração pela Florida Christian University. Possui MBA em Gerenciamento de Projetos de TI, certificações internacionais como *Certified Information Security Officer* (CISO), ISO/IEC 27001 Lead Implementer e *Data Protection Officer* (DPO) – EXIN, além de graduação em Tecnologia de Redes de Computadores.
[3] Mestrando em Administração pela Florida Christian University. Pós-graduado em Gestão de Tecnologia da Informação e *Cloud Computing* pela Universidade Federal de São Carlos (UFSCar/2024) e graduado em Gestão de Tecnologia da Informação pela UNIP (2021). Possui certificações internacionais ITIL® 4 Foundation, CompTIA® Security+, EXIN® *Data Protection Officer* (DPO) e EXIN® ISO/IEC 27001 Professional (ISMP).
[4] Doutor em Administração de TI (Ph.D.) pela Florida Christian University; mestre em Administração com foco em TI Verde; possui extensão em Gestão de TI pela FGV/SP, pós-graduação em Gerenciamento de Projetos e graduação em Redes de Computadores e Internet. É professor de Segurança da Informação na Universidade Paulista (UNIP), na Universidade Municipal de São Caetano do Sul (USCS) e na Florida Christian University (FCU).
[5] Doutor em Economia pela PUC-Campinas; MBA em Marketing pela ESAMC, Sorocaba; mestre em Administração pela UNG-Guarulhos; mestre e doutor em Sociologia pela PUC-São Paulo; doutor em Administração pela Florida Christian University (FCU-USA); e pós-doutor pela Unicamp-Campinas, pela FCU-USA e pela Universidade de Coimbra (UC-Portugal).
[6] Tecnólogo em Marketing (UNIP) e pós-graduado em *Data Protection* Officer (LGPD/GDPR), com especialização em Social Media e atuação na gestão de redes sociais para profissionais de TI e instituições do terceiro setor. É Gerente de Marketing e Assessor do Comitê Diretivo da APDADOS, com atuação institucional em Brasília junto a órgãos federais entre 2021 e 2023.

Os resultados indicam convergência funcional em seis dimensões: governança institucional, classificação de risco, governança de dados e modelos, avaliação integrada de impacto, implantação com supervisão humana e monitoramento contínuo. O protocolo organiza essas dimensões em seis fases operacionais e em artefatos mínimos de conformidade, como inventário de sistemas, matriz de risco, documentação técnica, relatório integrado de impacto, plano de supervisão humana, registros de incidentes e relatório de auditoria. Conclui-se que a governança de IA depende da integração de controles, responsabilidades e evidências auditáveis ao longo de todo o ciclo de vida dos sistemas, com aplicabilidade tanto ao contexto brasileiro quanto a operações transnacionais.

_____

PALAVRAS-CHAVE: Governança de inteligência artificial. Protocolo de padronização. ISO/IEC 42001. NIST AI RMF. Regulamento Europeu de IA.

ABSTRACT

The rapid expansion of artificial intelligence (AI) systems has intensified organizational governance challenges, particularly when ethical principles, technical standards, and regulatory obligations are addressed in a fragmented manner. This article proposes, through a literature review and comparative documentary analysis, a standardization protocol for AI governance based on international standards and regulations. The qualitative, exploratory, and descriptive study examined a corpus of 27 references, including academic studies and normative, regulatory, and institutional documents published between 2016 and 2026, such as ISO/IEC 42001, ISO/IEC 23894, ISO/IEC 42005, ISO/IEC 42006, the NIST AI RMF, the Brazilian LGPD, the GDPR, the European Union AI Act, OECD and UNESCO recommendations, and Brazilian documents either in force or under legislative discussion. The findings reveal functional convergence across six dimensions: institutional governance, risk classification, data and model governance, integrated impact assessment, deployment with human oversight, and continuous monitoring. The protocol translates these dimensions into six operational phases and minimum compliance artifacts, including system inventories, risk matrices, technical documentation, integrated impact reports, human oversight plans, incident records, and audit reports. The article concludes that AI governance requires the integration of controls, responsibilities, and auditable evidence throughout the system lifecycle, with applicability to the Brazilian context and to transnational operations.

KEYWORDS: *Artificial Intelligence Governance. Standardization protocol. ISO/IEC 42001. NIST AI RMF. European AI Act.*

RESUMEN

La rápida expansión de los sistemas de inteligencia artificial (IA) ha intensificado los desafíos de gobernanza organizacional, especialmente cuando los principios éticos, las normas técnicas y las obligaciones regulatorias se abordan de manera fragmentada. Este artículo propone, mediante revisión de literatura y análisis documental comparado, un protocolo de estandarización para la gobernanza de la IA basado en normas y regulaciones internacionales. La investigación, de naturaleza cualitativa, exploratoria y descriptiva, examinó un corpus de 27 referencias, compuesto por estudios académicos y documentos normativos, regulatorios e institucionales publicados entre 2016 y 2026, incluidos ISO/IEC 42001, ISO/IEC 23894, ISO/IEC 42005, ISO/IEC 42006, NIST AI RMF, LGPD brasileña, GDPR, AI Act de la Unión Europea, recomendaciones de la OECD y de la UNESCO, y documentos brasileños vigentes o

en tramitación. Los resultados identifican convergencia funcional en seis dimensiones: gobernanza institucional, clasificación de riesgos, gobernanza de datos y modelos, evaluación integrada de impacto, implantación con supervisión humana y monitoreo continuo. El protocolo sintetiza esas dimensiones en seis fases operativas y en artefactos mínimos de conformidad. Se concluye que la gobernanza de la IA depende de la integración de controles, responsabilidades y evidencias auditables durante todo el ciclo de vida de los sistemas, con aplicabilidad al contexto brasileño y a operaciones transnacionales.

PALABRAS CLAVE: *Gobernanza de Inteligencia Artificial. Protocolo de estandarización. ISO/IEC 42001. NIST AI RMF. Reglamento Europeo de IA.*

1. INTRODUÇÃO

A difusão acelerada de sistemas de inteligência artificial (IA) em processos decisórios, cadeias produtivas, serviços públicos e plataformas digitais deslocou o debate sobre inovação algorítmica de uma agenda predominantemente técnica para uma agenda centrada em governança, *accountability*, segurança e conformidade. Embora sistemas de IA possam ampliar produtividade, automação e capacidade analítica, sua implementação sem controles institucionais adequados também pode produzir opacidade decisória, discriminações, riscos à privacidade, fragilidades de segurança e impactos coletivos de difícil rastreabilidade (FLORIDI *et al.*, 2018; JOBIN; IENCA; VAYENA, 2019; TABASSI, 2023).

Nos últimos anos, esse movimento foi acompanhado pela proliferação de princípios éticos, normas técnicas, *frameworks* voluntários e regulações vinculantes. Princípios intergovernamentais, como a *Recommendation of the Council on Artificial Intelligence* da OECD e a *Recommendation on the Ethics of Artificial Intelligence* da UNESCO, consolidaram valores associados à confiança, à centralidade humana, à inclusão e ao respeito aos direitos fundamentais (OECD, 2019; UNESCO, 2021). Em paralelo, normas e estruturas técnicas, como ISO/IEC 22989, ISO/IEC 38507, ISO/IEC 23894, ISO/IEC 42001, ISO/IEC 5338, ISO/IEC 42005, ISO/IEC 42006 e NIST AI RMF 1.0, buscaram converter governança, risco, ciclo de vida, avaliação de impacto, auditoria e melhoria contínua em requisitos ou orientações mais operacionais (ISO/IEC, 2022a; 2022b; 2023a; 2023b; 2023c; 2025a; 2025b; TABASSI, 2023).

No plano regulatório europeu, o Regulamento (UE) 2024/1689, conhecido como AI Act, entrou em vigor em 1º de agosto de 2024. Sua aplicação ocorre de maneira escalonada: as proibições e as obrigações de alfabetização em IA passaram a aplicar-se em 2 de fevereiro de 2025; as regras de governança e as obrigações relativas a modelos de propósito geral passaram a aplicar-se em 2 de agosto de 2025; a aplicação geral de várias disposições está prevista para 2 de agosto de 2026; e determinadas obrigações específicas seguem prazos

próprios até etapas posteriores. O GDPR permanece como referência central para a proteção de dados pessoais e para a lógica de *accountability* procedimental, especialmente por meio de documentação, avaliações de impacto e demonstração de conformidade (UNIÃO EUROPEIA, 2016; 2024; COMISSÃO EUROPEIA, 2026).

No contexto brasileiro, a governança de IA ainda se organiza por camadas. A Lei Geral de Proteção de Dados Pessoais (LGPD) constitui o principal marco vinculante aplicável a sistemas de IA que tratam dados pessoais; a Estratégia Brasileira de Inteligência Artificial (EBIA) oferece diretrizes de política pública; e, na data de atualização documental deste artigo, o Projeto de Lei nº 2.338/2023 tramitava na Câmara dos Deputados, após remessa do Senado Federal em 17 de março de 2025 (BRASIL, 2018; 2021; 2025). A interpretação de que esses elementos apontam para a consolidação progressiva de um marco brasileiro de governança de IA é analítica, e não afirmação de fato legislativo consumado.

A lacuna enfrentada neste artigo decorre da fragmentação entre princípios, normas, modelos de gestão e obrigações jurídicas. A literatura demonstra que a adesão meramente declaratória a princípios éticos não é suficiente para assegurar governança efetiva, pois as organizações precisam de papéis, rotinas, registros, métricas, trilhas de auditoria, mecanismos de remediação e processos de revisão capazes de converter compromissos normativos em evidências verificáveis (MITTELSTADT, 2019; MÖKANDER *et al.*, 2021; MÖKANDER *et al.*, 2022). Diante disso, formula-se a seguinte pergunta-problema: como estruturar um protocolo padronizado de governança de inteligência artificial que seja interoperável entre normas técnicas e marcos regulatórios, preserve direitos fundamentais e produza evidências auditáveis ao longo do ciclo de vida do sistema?

O objetivo geral consiste em propor um protocolo de padronização para a governança de IA baseado em normas e regulamentações nacionais e internacionais. De modo específico, busca-se mapear convergências entre instrumentos normativos relevantes; diferenciar suas naturezas jurídicas e técnicas; comparar contribuições para gestão, risco, impacto e auditoria; sintetizar artefatos mínimos de conformidade; e discutir a aplicabilidade do protocolo ao contexto brasileiro e a organizações com atuação transnacional. O percurso metodológico adota revisão bibliográfica não exaustiva e análise documental comparada de um corpus de 27 referências, delimitado entre 2016 e maio de 2026.

2. REVISÃO DA LITERATURA

2.1. Governança de IA e a transição do discurso ético para modelos operacionais

A literatura inicial sobre governança de IA procurou responder à expansão de sistemas algorítmicos por meio da formulação de princípios de alto nível, como transparência, justiça, responsabilidade, não maleficência e respeito à autonomia. Floridi *et al.* (2018) sistematizaram oportunidades, riscos, princípios e recomendações para uma boa sociedade de IA, ao passo que Jobin, Ienca e Vayena (2019) evidenciaram uma convergência global aparente em torno de princípios recorrentes. Essa convergência, entretanto, não eliminou divergências sobre o significado operacional de cada princípio, nem superou a distância entre compromissos declaratórios e práticas efetivas de desenvolvimento, implantação e supervisão.

Mittelstadt (2019) examinou criticamente essa distância ao argumentar que princípios isolados não garantem mudança organizacional, uma vez que o ecossistema de IA ainda carece de deveres profissionais claros, mecanismos robustos de responsabilização e instrumentos maduros de tradução normativa para a prática. Nessa perspectiva, governança de IA não se confunde com ética declaratória: ela exige estruturas organizacionais, procedimentos documentados, instâncias decisórias e mecanismos de revisão capazes de tornar valores verificáveis em contextos concretos de uso.

Mökander *et al.* (2021) definem auditoria baseada em ética como um processo estruturado de avaliação de comportamentos presentes ou passados à luz de princípios ou normas relevantes. Em estudo subsequente, Mökander *et al.* (2022) demonstram que a implementação da governança corporativa de IA depende de harmonização de escopo, alinhamento entre áreas, definição de responsabilidades e integração com estruturas preexistentes de compliance e gestão de risco. Falco *et al.* (2021) complementam esse debate ao enfatizar que auditorias independentes podem atuar como vetor pragmático de segurança e confiança pública quando articulam avaliação prospectiva de risco, trilhas operacionais de auditoria e aderência a requisitos jurisdicionais.

2.2. Normas técnicas, *frameworks* voluntários e sistemas de gestão

A revisão exige distinguir a natureza dos instrumentos mobilizados. Norma técnica é documento elaborado por organismo de normalização, orientado à padronização de conceitos, processos, requisitos ou boas práticas; em regra, sua adoção é voluntária, salvo quando incorporada por contrato, regulação ou política pública. *Framework* voluntário é uma estrutura aberta de orientação, geralmente modular e adaptável, que auxilia organizações na implementação de controles sem constituir, por si só, obrigação jurídica. Regulação vinculante,

por sua vez, estabelece deveres juridicamente exigíveis e sanções. Recomendações intergovernamentais expressam compromissos políticos e padrões de legitimidade internacional, enquanto estratégias públicas orientam prioridades de Estado e políticas de fomento.

As normas ISO/IEC oferecem um eixo relevante de amadurecimento técnico. A ISO/IEC 22989 estabelece terminologia e conceitos fundamentais, reduzindo ambiguidades semânticas. A ISO/IEC 38507 volta-se às implicações do uso da IA para a governança de tecnologia da informação, conectando o tema à alta administração e ao órgão dirigente. A ISO/IEC 42001 especifica requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de IA, aproximando a governança de IA de lógicas já conhecidas em qualidade, segurança da informação e *compliance* (ISO/IEC, 2022a; 2022b; 2023b).

Essa cadeia normativa é complementada pela ISO/IEC 23894, dedicada à gestão de riscos em IA; pela ISO/IEC 5338, relativa aos processos de ciclo de vida de sistemas de IA; pela ISO/IEC 42005, voltada à avaliação de impactos de sistemas de IA sobre indivíduos, grupos e sociedade; e pela ISO/IEC 42006, relativa aos requisitos para organismos que auditam e certificam sistemas de gestão de IA (ISO/IEC, 2023a; 2023c; 2025a; 2025b). Como várias normas ISO/IEC possuem acesso comercial, a análise deste artigo limita-se aos escopos oficiais, metadados bibliográficos e descrições públicas verificáveis, evitando inferências sobre cláusulas não disponíveis publicamente.

No âmbito estadunidense, o NIST AI RMF 1.0 traduz a governança de IA em uma arquitetura operacional aberta, voluntária e setorialmente agnóstica. O modelo organiza a gestão de risco nas funções Govern, Map, Measure e Manage, enfatizando que a governança deve atravessar todo o ciclo de vida do sistema, com papéis definidos, cultura organizacional, documentação, mensuração, participação de partes interessadas e revisão contínua (TABASSI, 2023).

2.3. Regulação baseada em risco, direitos fundamentais e *accountability*

A terceira camada da revisão reúne instrumentos regulatórios e quase regulatórios que deslocam a governança de IA para o campo dos direitos fundamentais e da responsabilidade jurídica. O GDPR consolidou deveres de transparência, *accountability* e avaliação de impacto no tratamento de dados pessoais. Kaminski e Malgieri (2021) demonstram que, no contexto algorítmico, a *Data Protection Impact Assessment* atua como elo entre direitos individuais e

governança sistêmica, ao conectar documentação interna, mitigação de riscos e explicações passíveis de comunicação a titulares, reguladores e demais partes interessadas.

O AI Act da União Europeia aprofunda essa lógica ao adotar abordagem baseada em risco, proibir determinadas práticas, estabelecer requisitos para sistemas de alto risco e impor obrigações de transparência, governança, monitoramento e conformidade. Para sistemas de alto risco, o regulamento enfatiza gestão de risco contínua e iterativa, documentação técnica, governança de dados, registro de eventos, supervisão humana, precisão, robustez e cibersegurança. Além disso, introduz avaliação de impacto sobre direitos fundamentais para determinados casos de uso, reforçando a passagem do discurso ético para um modelo verificável (UNIÃO EUROPEIA, 2024).

A Convenção-Quadro do Conselho da Europa sobre Inteligência Artificial, Direitos Humanos, Democracia e Estado de Direito amplia a abordagem ao se apresentar como tratado internacional voltado à consistência entre as atividades do ciclo de vida da IA e os direitos humanos, a democracia e o Estado de Direito (CONSELHO DA EUROPA, 2024). Em paralelo, a UNESCO estabelece um padrão ético global assentado em dignidade, direitos, inclusão, diversidade e sustentabilidade; a OECD combina princípios de *stewardship* responsável com orientação de *due diligence* para que empresas incorporem a IA responsável a políticas, sistemas de gestão, identificação e mitigação de impactos, monitoramento, comunicação e remediação (UNESCO, 2021; OECD, 2019; OECD, 2026).

No Brasil, a governança de IA permanece juridicamente distribuída. A LGPD impõe base normativa sempre que sistemas de IA tratam dados pessoais, sobretudo em relação a finalidade, base legal, segurança, transparência e responsabilização. A EBIA orienta a ação estatal por eixos de governança, inovação, capacitação e uso ético. O PL nº 2.338/2023, ainda em tramitação na Câmara dos Deputados na data de atualização documental, procura estabelecer normas gerais de governança responsável da IA, reunindo princípios, deveres, mecanismos de transparência e categorias de risco (BRASIL, 2018; 2021; 2025).

2.4. Lacuna de interoperabilidade

A revisão evidencia uma lacuna de interoperabilidade. Princípios internacionais indicam valores; normas técnicas estruturam processos; *frameworks* voluntários auxiliam a implementação; regulações vinculantes definem obrigações e sanções; tratados e estratégias nacionais orientam políticas e direitos. Esses instrumentos, entretanto, raramente chegam às organizações como uma arquitetura integrada de decisão, documentação e evidência.

Na prática, essa fragmentação pode gerar relatórios éticos sem documentação técnica suficiente, avaliações de impacto desconectadas da gestão corporativa de riscos, controles de

privacidade sem rastreabilidade do modelo ou políticas internas sem trilhas de auditoria. A contribuição deste artigo consiste em tratar esses instrumentos como camadas complementares de um protocolo padronizado, capaz de organizar a governança de IA de forma funcional, auditável e adaptável a diferentes setores e jurisdições.

3. METODOLOGIA

Este estudo caracteriza-se como pesquisa qualitativa, exploratória e descritiva, desenvolvida por meio de revisão bibliográfica não exaustiva e análise documental comparada. A unidade de análise é a função de governança desempenhada por cada instrumento no ciclo de vida de sistemas de IA, e não a reprodução textual de cláusulas específicas. O desenho metodológico foi orientado por uma pergunta aplicada: identificar, nos documentos efetivamente mobilizados, quais requisitos, orientações ou categorias convergem para uma arquitetura mínima de governança de IA capaz de produzir evidências auditáveis.

O recorte temporal foi delimitado entre 2016 e maio de 2026. O marco inicial corresponde ao Regulamento (UE) 2016/679, que inaugura no corpus a lógica procedimental de *accountability* em proteção de dados, enquanto o marco final corresponde às verificações documentais realizadas durante a revisão do manuscrito. O corpus final reuniu 27 referências efetivamente utilizadas no texto: 9 trabalhos acadêmicos revisados por pares e 18 documentos normativos, regulatórios ou institucionais. O número de fontes decorre do critério de pertinência e de efetivo uso argumentativo: foram mantidas apenas as referências que contribuíam para pelo menos uma categoria do protocolo ou para sua fundamentação crítica.

Os critérios de inclusão foram: i) pertinência direta à governança de IA; ii) contribuição operacional, normativa ou analítica para pelo menos uma das seis categorias adotadas; iii) disponibilidade de fonte oficial, texto integral aberto, escopo público ou metadado bibliográfico verificável; e iv) efetiva utilização no argumento do artigo. Foram excluídos: i) materiais jornalísticos, opinativos ou promocionais; ii) textos sem relação direta com governança, risco, impacto, auditoria ou accountability em IA; iii) documentos redundantes que apenas reiterassem conteúdo já coberto por fonte primária; e iv) normas cujo conteúdo não estivesse publicamente acessível nem pudesse ser descrito com segurança a partir de escopos oficiais.

O corpus bibliográfico incluiu estudos sobre ética da IA, auditoria, *accountability* algorítmica, avaliação de impacto e governança corporativa. O corpus documental compreendeu: Recommendation of the Council on Artificial Intelligence; OECD *Due Diligence* Guidance for Responsible AI; Recommendation on the Ethics of Artificial Intelligence; ISO/IEC 22989, 38507, 23894, 42001, 42005, 42006 e 5338; NIST AI RMF 1.0; Regulamento (UE)

2016/679; Regulamento (UE) 2024/1689; Convenção-Quadro do Conselho da Europa; Lei nº 13.709/2018; Portaria MCTI nº 4.617/2021; e Projeto de Lei nº 2.338/2023.

A matriz comparativa foi construída em duas etapas. Inicialmente, adotaram-se categorias a priori, extraídas das funções recorrentes de governança, risco, impacto e auditoria identificadas no NIST AI RMF, na ISO/IEC 42001, na ISO/IEC 23894 e no AI Act. Em seguida, essas categorias foram refinadas durante a leitura do corpus, até se estabilizarem em seis dimensões: governança institucional; classificação de risco; governança de dados e modelos; avaliação integrada de impacto; implantação, transparência e supervisão humana; e monitoramento, auditoria e melhoria contínua.

O procedimento analítico ocorreu em cinco passos: listagem e classificação das fontes; leitura crítica das fontes abertas e, no caso das normas ISO/IEC, dos escopos e metadados públicos; extração da função de governança de cada documento; comparação das convergências funcionais entre instrumentos de natureza distinta; e síntese dessas convergências em um protocolo de seis fases, com artefatos documentais e evidências mínimas de conformidade. A replicação do estudo exige reconstituir o mesmo corpus, aplicar a matriz categorial e verificar se a síntese protocolar permanece justificável a partir das mesmas fontes.

4. RESULTADOS E DISCUSSÃO: O QUE O PROTOCOLO RESOLVE E O QUE PERMANECE EM ABERTO

4.1. Convergência normativa sem arquitetura operacional única

A comparação entre os instrumentos examinados indica que o problema central da governança de IA não reside na ausência de princípios, normas ou deveres regulatórios, mas na tradução fragmentada desses referenciais em rotinas organizacionais. O corpus reúne bases de ética, gestão, risco, direitos fundamentais, conformidade e auditoria; contudo, esses referenciais não se apresentam, de forma integrada, como uma arquitetura única de decisão, evidência e melhoria contínua.

A convergência torna-se visível quando se observa a função desempenhada por cada instrumento. A OECD e a UNESCO oferecem valores de legitimidade internacional e centralidade humana. A ISO/IEC 38507 aproxima a IA da governança organizacional e da alta administração. A ISO/IEC 42001 estrutura o sistema de gestão. A ISO/IEC 23894 orienta a identificação e o tratamento de riscos. A ISO/IEC 5338 conecta governança ao ciclo de vida do sistema. A ISO/IEC 42005 fortalece a avaliação de impactos. A ISO/IEC 42006 projeta requisitos para auditoria e certificação. O NIST AI RMF oferece uma arquitetura operacional

voluntária. GDPR, LGPD e AI Act estabelecem obrigações de proteção de dados, risco, transparência, documentação e supervisão humana. A Tabela 1 sintetiza essa convergência funcional.

Tabela 1. Síntese comparativa dos principais instrumentos para governança de IA

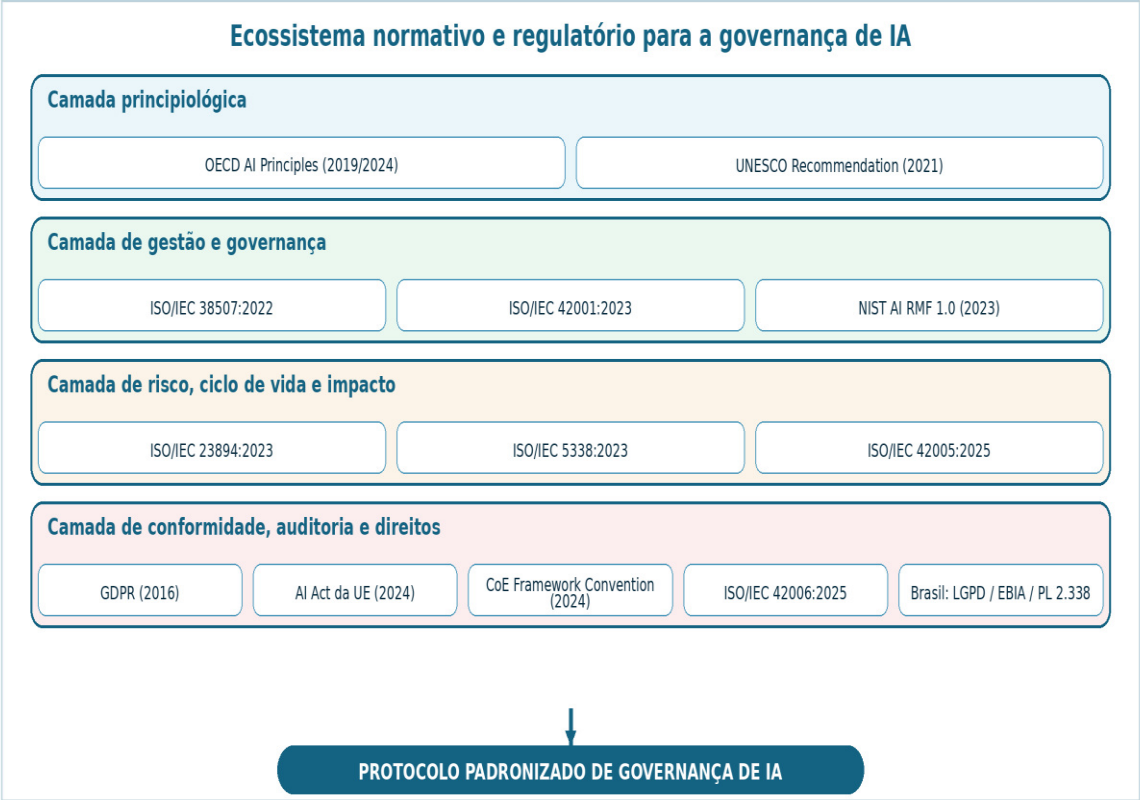
Instrumento	**Natureza**	**Ênfase**	**Contribuição ao protocolo**
OECD AI Principles	Princípios intergovernamentais	*Stewardship* responsável, direitos e confiança	Define valores, recomendações e base de interoperabilidade internacional
UNESCO Recommendation	Padrão ético global	Dignidade, inclusão, diversidade e impactos socioambientais	Amplia a legitimidade pública e a perspectiva de impacto social
ISO/IEC 38507	Norma técnica de governança organizacional	Papel da alta direção e governança de TI com IA	Liga IA à governança corporativa e à prestação de contas
ISO/IEC 42001	Norma técnica de sistema de gestão	Políticas, objetivos, controles e melhoria contínua	Estrutura institucionalmente o sistema de gestão de IA
ISO/IEC 23894	Norma técnica de gestão de risco	Identificação, avaliação, tratamento e revisão de riscos	Orienta matriz de risco e recalibração contínua
ISO/IEC 5338	Norma técnica de ciclo de vida	Processos de desenvolvimento, aquisição e operação	Conecta governança às etapas do sistema de IA

Instrumento	Natureza	Ênfase	Contribuição ao protocolo
ISO/IEC 42005	Norma técnica de avaliação de impacto	Impactos sobre indivíduos, grupos e sociedade	Sustenta o relatório integrado de impacto
NIST AI RMF 1.0	*Framework* voluntário	Govern, Map, Measure e Manage	Traduz governança em funções operacionais e iterativas
GDPR	Regulação vinculante	Proteção de dados, *accountability* e DPIA	Base jurídica para documentação, transparência e impacto em dados pessoais
AI Act da UE	Regulação vinculante	Risco, alto risco, FRIA, supervisão e fiscalização	Consolida deveres de conformidade e controle regulatório
Brasil: LGPD, EBIA e PL 2.338/2023	Base nacional em formação	Proteção de dados, estratégia pública e governança responsável	Adapta o protocolo ao contexto jurídico e institucional brasileiro.

Fonte: elaboração própria, com base em OECD (2019; 2026), UNESCO (2021), ISO/IEC (2022a; 2022b; 2023a; 2023b; 2023c; 2025a; 2025b), Tabassi (2023), União Europeia (2016; 2024), Conselho da Europa (2024) e Brasil (2018; 2021; 2025).

A Tabela 1 evidencia que os instrumentos analisados não competem necessariamente entre si; ao contrário, cumprem funções complementares. O problema surge quando a organização adota uma camada sem conectá-la às demais, como ocorre quando há política ética sem matriz de risco, documentação técnica sem avaliação de impacto ou avaliação de impacto sem plano de monitoramento. O protocolo proposto atua como ponte operacional entre essas camadas, conforme representado na Figura 1.

Figura 1. Arquitetura normativa integrada para governança de IA



Fonte: elaboração própria, com base em OECD (2019), UNESCO (2021), ISO/IEC (2022a; 2022b; 2023a; 2023b; 2023c; 2025a; 2025b), Tabassi (2023), União Europeia (2016; 2024), Conselho da Europa (2024) e Brasil (2018; 2021).

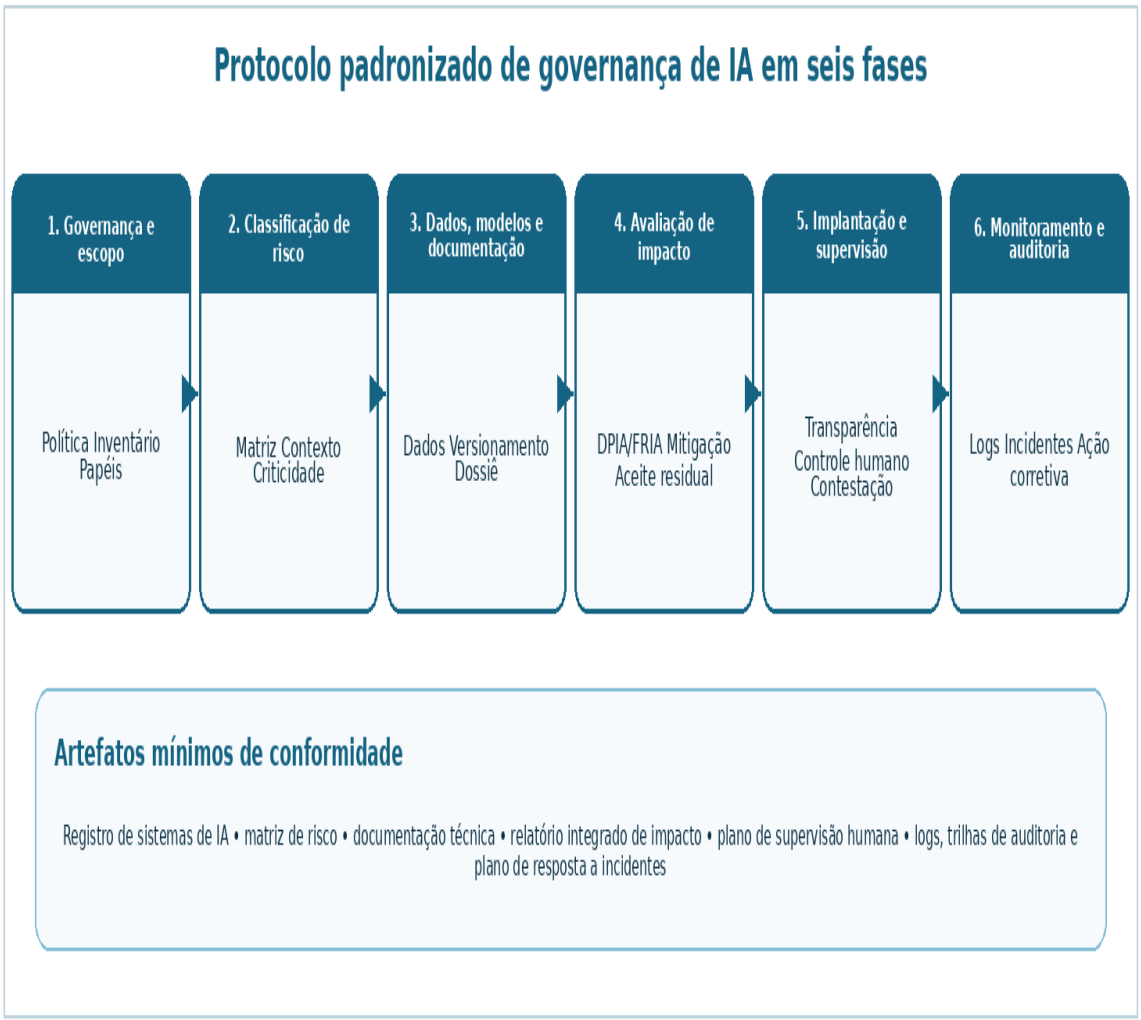
Desse modo, a contribuição do protocolo não é criar novo princípio, nova taxonomia universal ou equivalência automática entre regimes jurídicos distintos. Sua função é organizar convergências verificáveis em uma sequência de governança capaz de apoiar decisão, registro, supervisão, auditoria e melhoria contínua. Essa delimitação é relevante para evitar duas distorções: a normatividade excessivamente abstrata, que não produz evidências, e a conformidade meramente documental, que não reduz risco real.

4.2. Protocolo padronizado de governança de IA em seis fases

Com base nas convergências mapeadas, propõe-se um protocolo estruturado em seis fases. Cada fase possui finalidade própria, função dentro da arquitetura de governança, aplicação prática e relação com normas técnicas, regulação, auditoria e gestão de riscos. A

sequência é lógica e iterativa: sistemas podem retornar a fases anteriores quando houver mudança de finalidade, dados, modelo, contexto de uso, base legal, requisito regulatório ou nível de risco. As seis fases se estabilizaram porque correspondem às funções recorrentes identificadas no corpus e porque cobrem, sem sobreposição excessiva, o percurso mínimo entre escopo, risco, documentação, impacto, implantação e monitoramento.

Figura 2. Protocolo padronizado de governança de IA em seis fases



Fonte: elaboração própria, com base em ISO/IEC (2023a; 2023b; 2023c; 2025a), Tabassi (2023), União Europeia (2016; 2024), OECD (2026) e Janssen, Lee e Singh (2022).

Tabela 2. Fases, evidências documentais e bases normativas predominantes do protocolo proposto

Fase	Evidências documentais	Bases predominantes	Resultado esperado
1. Governança e escopo	Política de IA; inventário de sistemas; papéis e responsabilidades; critérios de apetite a risco.	OECD; UNESCO; ISO/IEC 38507; ISO/IEC 42001; NIST Govern.	Mandato institucional e responsabilidade definida.
2. Classificação de risco	Matriz de criticidade; classificação do caso de uso; justificativa de contexto.	ISO/IEC 23894; NIST Map/Measure; AI Act.	Priorização proporcional de controles.
3. Dados, modelos e documentação	Registro de dados; versionamento; ficha técnica; documentação técnica.	ISO/IEC 42001; ISO/IEC 5338; AI Act.	Rastreabilidade e explicabilidade mínima.
4. Avaliação integrada de impacto	DPIA/FRIA/relatório integrado de impacto; medidas mitigatórias; aceite residual.	GDPR; AI Act; ISO/IEC 42005; Janssen, Lee e Singh.	Identificação e mitigação de riscos a direitos e sociedade.
5. Implantação e supervisão humana	Plano de supervisão humana; aviso de transparência; canal de contestação.	AI Act; NIST Manage; OECD; UNESCO.	Uso monitorado e reversibilidade decisória.
6. Monitoramento, auditoria e melhoria	Logs; registro de incidentes; plano de ação corretiva; relatório de auditoria.	ISO/IEC 42001; ISO/IEC 42006; AI Act; Mökander et al.; Falco et al.	Assurance, correção e melhoria contínua.

Fonte: elaboração própria, com base em OECD (2019; 2026), ISO/IEC (2022b; 2023a; 2023b; 2023c; 2025a; 2025b), Tabassi (2023), União Europeia (2016; 2024) e Conselho da Europa (2024).

A Figura 2 resume o fluxo lógico do protocolo. A Tabela 2, mantida como imagem para preservar a formatação visual solicitada pelos pareceres, explicita as evidências documentais, as bases predominantes e os resultados esperados de cada fase. A descrição textual a seguir torna o protocolo autônomo em relação às figuras e tabelas, permitindo compreender sua aplicação mesmo quando os elementos visuais forem consultados apenas como síntese.

A Fase 1 - governança institucional e delimitação de escopo tem como finalidade estabelecer o mandato organizacional da governança de IA. A organização deve manter inventário de sistemas, política interna de IA, papéis e responsabilidades, critérios de apetite a risco e registro de finalidade. Na prática, essa fase define quem decide, quem aprova, quem monitora e quem responde por cada sistema. Sua função é conectar a governança de IA à alta administração, aos controles internos e ao sistema de gestão, em diálogo com OECD, UNESCO, ISO/IEC 38507, ISO/IEC 42001 e NIST Govern (OECD, 2019; UNESCO, 2021; ISO/IEC, 2022b; 2023b; TABASSI, 2023).

A Fase 2 - classificação de risco e criticidade do caso de uso tem como finalidade calibrar controles de forma proporcional. Devem ser avaliados o contexto de aplicação, os grupos afetados, o uso de dados pessoais ou sensíveis, a autonomia operacional, a possibilidade de erro material, a reversibilidade da decisão, a escala de impacto e a sensibilidade setorial. Na prática, essa fase evita a aplicação de controles homogêneos a sistemas heterogêneos e define quando o sistema exige salvaguardas reforçadas, avaliação de impacto, supervisão humana ou revisão jurídica específica. Sua função é aproximar a lógica do AI Act da gestão contínua de riscos indicada pela ISO/IEC 23894 e pelo NIST AI RMF (ISO/IEC, 2023a; TABASSI, 2023; UNIÃO EUROPEIA, 2024).

A Fase 3 - governança de dados, modelos e documentação técnica tem como finalidade assegurar rastreabilidade. A organização deve registrar fontes de dados, critérios de qualidade, retenção, versionamento, limitações conhecidas, métricas de desempenho, validações e justificativas de design. Na prática, essa documentação permite reconstruir decisões de desenvolvimento, implantação e alteração. Sua função é sustentar explicabilidade mínima, auditoria e prestação de contas, articulando ISO/IEC 42001, ISO/IEC 5338 e AI Act (ISO/IEC, 2023b; 2023c; UNIÃO EUROPEIA, 2024).

A Fase 4 - avaliação integrada de impacto tem como finalidade reunir riscos relativos a dados pessoais, direitos fundamentais, grupos afetados, sociedade e organização em um artefato único. Em vez de relatórios isolados, o protocolo propõe articular DPIA, FRIA e avaliação social em relatório integrado de impacto, com finalidade, proporcionalidade, riscos, mitigação, responsáveis e aceite residual. Na prática, reduz duplicidades e permite uma visão transversal. Sua função é conectar GDPR, LGPD, AI Act, literatura sobre avaliação de direitos fundamentais e ISO/IEC 42005 (UNIÃO EUROPEIA, 2016; KAMINSKI; MALGIERI, 2021; JANSSEN; LEE; SINGH, 2022; ISO/IEC, 2025a).

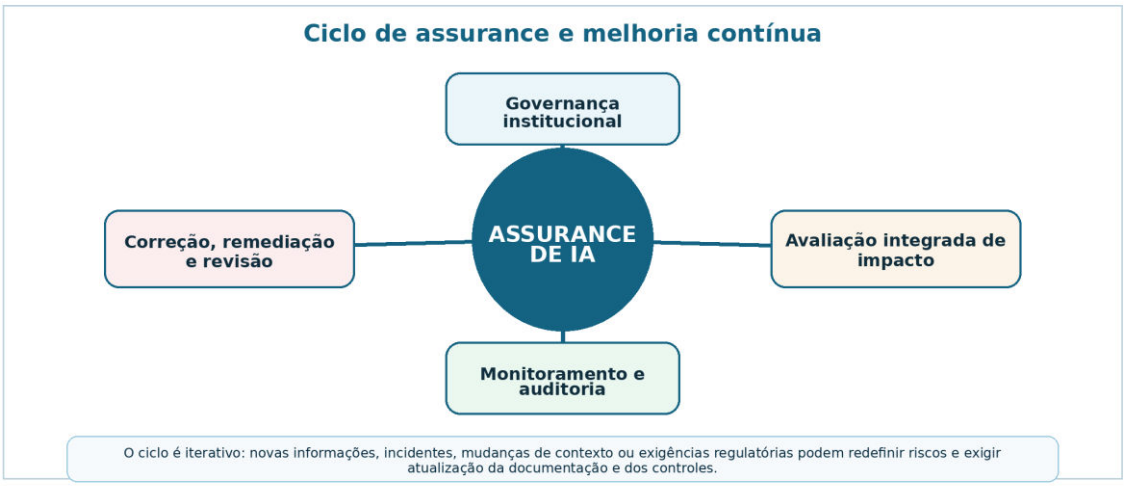
A Fase 5 - implantação controlada, transparência e supervisão humana tem como finalidade condicionar a entrada em operação à existência de controles compatíveis com o

risco. Devem existir plano de supervisão humana, avisos de transparência, canais de contestação, critérios de reversibilidade, rotinas de revisão e gatilhos para suspensão ou descontinuidade. Na prática, a supervisão humana deixa de ser uma declaração genérica e passa a funcionar como processo de controle. Sua função é materializar direitos, reduzir assimetrias informacionais e permitir intervenção efetiva (MÖKANDER; AXENTE, 2023; UNIÃO EUROPEIA, 2024).

A Fase 6 - monitoramento, auditoria e melhoria contínua tem como finalidade assegurar que a governança permaneça ativa após a implantação. A organização deve monitorar desempenho, *drift*, erro, viés, reclamações, incidentes, mudanças de contexto e requisitos regulatórios, mantendo logs, trilhas de auditoria, plano de ação corretiva e relatórios periódicos. Na prática, essa fase permite recalibrar risco, atualizar documentação e acionar medidas de remediação. Sua função é conectar ISO/IEC 42001, ISO/IEC 42006, literatura de auditoria e requisitos de monitoramento do AI Act (ISO/IEC, 2023b; 2025b; MÖKANDER *et al.*, 2021; FALCO *et al.*, 2021; UNIÃO EUROPEIA, 2024).

Registro de sistemas de IA, matriz de risco, ficha técnica, relatório integrado de impacto, plano de supervisão humana, registros de incidentes e relatório de auditoria compõem a memória institucional do sistema. Em conjunto, esses artefatos sustentam *accountability*, rastreabilidade e capacidade de auditoria, sem pressupor que a adoção de um único instrumento seja suficiente para atender a todos os regimes normativos aplicáveis.

Figura 3. Ciclo de assurance e melhoria contínua da governança de IA



Fonte: elaboração própria, com base em ISO/IEC (2023b; 2025b), Tabassi (2023), Mökander *et al.* (2021) e Falco *et al.* (2021).

4.3. Aplicabilidade no contexto brasileiro e em operações transnacionais

A aplicabilidade do protocolo ao Brasil é relevante porque o país convive com obrigação jurídica forte em proteção de dados, orientação estratégica de política pública e transição legislativa para um marco específico de IA. A LGPD continua sendo base vinculante para sistemas que tratam dados pessoais; a EBIA permanece como orientação estratégica; e o PL nº 2.338/2023, na data de atualização documental, seguia em análise na Câmara dos Deputados (BRASIL, 2018; 2021; 2025). Nesse cenário, um protocolo interoperável oferece utilidade mesmo antes da estabilização do marco setorial, pois antecipa rotinas organizacionais que tendem a permanecer relevantes sob diferentes arranjos normativos.

Do ponto de vista jurídico-prudencial, a principal vantagem do protocolo é não depender da promulgação de uma única lei para produzir valor organizacional. Se a operação envolve dados pessoais, a camada de impacto e documentação dialoga com a LGPD; se a organização busca maturidade de gestão, o protocolo se conecta à racionalidade sistêmica da ISO/IEC 42001; se a operação alcança o mercado europeu, classificação de risco, documentação técnica, supervisão humana e monitoramento pós-implantação aproximam a organização de requisitos do AI Act. Trata-se de uma estrutura de preparação normativa e documental, não de equivalência automática entre regimes distintos.

Em aplicações brasileiras, essa lógica pode ser ilustrada por cenários hipotéticos, sem pretensão de representar dados empíricos. Em uma instituição financeira que utiliza IA para triagem de crédito ou prevenção a fraudes, o protocolo exigiria inventário, base legal para dados pessoais, matriz de risco, documentação do modelo, análise de impacto, supervisão humana proporcional e monitoramento de vieses e incidentes. Em uma organização de saúde que utiliza IA para apoio à triagem clínica, a classificação de risco e a avaliação integrada de impacto precisariam considerar sensibilidade dos dados, consequências do erro, possibilidade de contestação e responsabilidade profissional. Em processos de recursos humanos, como triagem de currículos, a etapa de supervisão humana e contestação seria central para reduzir discriminação e opacidade.

As operações transnacionais acrescentam complexidade. Organizações que desenvolvem, compram ou integram sistemas de IA em cadeias de fornecedores podem enfrentar sobreposição regulatória entre LGPD, GDPR, AI Act, contratos, normas setoriais e exigências de auditoria independente. O protocolo contribui ao criar uma linguagem comum entre áreas jurídicas, técnicas, de segurança da informação, privacidade, negócios, compras e auditoria. Ainda assim, o custo de conformidade pode ser assimétrico: grandes organizações tendem a possuir recursos para documentação, testes, *red teaming* e auditorias; pequenas e

médias empresas podem demandar modelos proporcionais, ferramentas compartilhadas e orientação setorial.

A interoperabilidade, portanto, não elimina tensões. Ela reduz duplicidades, explicita responsabilidades e facilita evidências, mas não resolve automaticamente conflitos entre jurisdições, lacunas de supervisão, incertezas sobre modelos fundacionais, dependência de fornecedores ou atualização contínua de modelos de propósito geral. Por isso, o protocolo deve ser aplicado como arquitetura adaptativa de governança, e não como checklist estático.

4.4. Limitações do estudo

Este estudo possui limitações. A primeira é metodológica: por se tratar de revisão bibliográfica e análise documental comparada, a proposta protocolar ainda não foi validada empiricamente em organizações específicas ou setores regulados, como saúde, finanças, transporte, educação, trabalho ou administração pública. A segunda decorre do acesso comercial a parte das normas ISO/IEC, o que impôs uso restrito a escopos, resumos oficiais e metadados publicamente verificáveis. A terceira refere-se ao dinamismo regulatório, especialmente em matéria europeia e brasileira, exigindo atualização periódica do protocolo. A quarta decorre da ausência de mensuração prática de custos, maturidade organizacional, capacidade de auditoria e efetividade dos artefatos sugeridos em ambientes reais de implantação.

Essas limitações não invalidam a utilidade da proposta, mas restringem sua generalização. O protocolo deve ser entendido como síntese operacional do corpus analisado e como ponto de partida para validações empíricas, não como certificação de conformidade, parecer jurídico ou substituto de auditorias independentes. Em contextos de alto risco, sua aplicação deve ser complementada por análise jurídica, técnica, setorial e de segurança da informação. A validação prática futura deverá verificar aderência setorial, esforço de implementação, qualidade das evidências produzidas, capacidade de integração com controles existentes e efeitos sobre redução de risco.

5. CONSIDERAÇÕES FINAIS

O artigo respondeu à pergunta de pesquisa ao demonstrar que o corpus examinado oferece base normativa e institucional para estruturar um protocolo padronizado de governança de IA, desde que seus instrumentos sejam lidos de forma interoperável. O objetivo geral foi atendido por meio da proposição de um protocolo de seis fases, acompanhado de artefatos

mínimos de conformidade capazes de sustentar controles internos, prestação de contas, auditoria e diálogo regulatório.

A contribuição do estudo deve ser compreendida com prudência. O protocolo não cria novo regime jurídico, não substitui avaliação setorial e não garante conformidade automática. Sua originalidade consiste em organizar, de modo operacional, convergências entre princípios, normas técnicas, *frameworks* voluntários e regulações vinculantes, permitindo que organizações transformem compromissos normativos em registros, responsabilidades, decisões e evidências auditáveis ao longo do ciclo de vida dos sistemas de IA.

Para o contexto brasileiro, a proposta oferece uma base de maturidade institucional mesmo em ambiente de transição legislativa. Para operações transnacionais, auxilia a coordenação entre requisitos de proteção de dados, gestão corporativa de riscos, auditoria independente, supervisão humana, documentação técnica e monitoramento pós-implantação. Seus limites de generalização, contudo, exigem cautela, especialmente em setores críticos, em modelos de propósito geral e em cadeias de fornecedores complexas.

Como agenda futura, recomenda-se validar empiricamente o protocolo por meio de estudos de caso setoriais em saúde, finanças, educação, trabalho, administração pública e serviços digitais; testar sua aplicação a modelos fundacionais e modelos de propósito geral; examinar práticas de *red teaming*, *accountability* em cadeias de fornecedores e proteção de dados *by design*; avaliar sua integração com segurança da informação, *RegTech*, *XAI* e gestão de maturidade organizacional em governança de IA; e comparar sua aderência a auditorias independentes e programas reais de conformidade.

REFERÊNCIAS

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. *Acesso em: 29 mar. 2026.*

BRASIL. Ministério da Ciência, Tecnologia e Inovação. Portaria MCTI nº 4.617, de 6 de abril de 2021. Institui a Estratégia Brasileira de Inteligência Artificial. Brasília, DF: MCTI, 2021. Disponível em: https://antigo.mctic.gov.br/mctic/opencms/legislacao/portarias/Portaria_MCTI_n_4617_de_06042021.html. *Acesso em: 3 abr. 2026.*

BRASIL. Câmara dos Deputados. Projeto de Lei nº 2.338, de 2023. Dispõe sobre o desenvolvimento, o fomento e o uso ético e responsável da inteligência artificial com base na

centralidade da pessoa humana. Brasília, DF: Câmara dos Deputados, 2025. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2487262. *Acesso em: 4 abr. 2026.*

COMISSÃO EUROPEIA. AI Act. Brussels: European Commission, 2026. Disponível em: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai. *Acesso em: 5 abr. 2026.*

CONSELHO DA EUROPA. Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law. Strasbourg: Council of Europe, 2024. Disponível em: https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence. *Acesso em: 11 abr. 2026.*

FALCO, Gregory et al. Governing AI safety through independent audits. Nature Machine Intelligence, v. 3, p. 566-571, 2021. DOI: https://doi.org/10.1038/s42256-021-00370-7.

FLORIDI, Luciano et al. AI4People - An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations. Minds and Machines, v. 28, p. 689-707, 2018. DOI: https://doi.org/10.1007/s11023-018-9482-5.

ISO/IEC. ISO/IEC 22989:2022. Information technology - Artificial intelligence - Artificial intelligence concepts and terminology. Geneva: ISO/IEC, 2022a. Disponível em: https://www.iso.org/standard/74296.html. *Acesso em: 12 abr. 2026.*

ISO/IEC. ISO/IEC 38507:2022. Information technology - Governance of IT - Governance implications of the use of artificial intelligence by organizations. Geneva: ISO/IEC, 2022b. Disponível em: https://www.iso.org/standard/56641.html. *Acesso em: 18 abr. 2026.*

ISO/IEC. ISO/IEC 23894:2023. Information technology - Artificial intelligence - Guidance on risk management. Geneva: ISO/IEC, 2023a. Disponível em: https://www.iso.org/standard/77304.html. *Acesso em: 19 abr. 2026.*

ISO/IEC. ISO/IEC 42001:2023. Information technology - Artificial intelligence - Management system. Geneva: ISO/IEC, 2023b. Disponível em: https://www.iso.org/standard/42001.html. *Acesso em: 21 abr. 2026.*

ISO/IEC. ISO/IEC 42005:2025. Information technology - Artificial intelligence (AI) - AI system impact assessment. Geneva: ISO/IEC, 2025a. Disponível em: https://www.iso.org/standard/42005.html. *Acesso em: 25 abr. 2026.*

ISO/IEC. ISO/IEC 42006:2025. Information technology - Artificial intelligence - Requirements for bodies providing audit and certification of artificial intelligence management systems. Geneva: ISO/IEC, 2025b. Disponível em: https://www.iso.org/standard/42006.html. *Acesso em: 26 abr. 2026.*

ISO/IEC. ISO/IEC 5338:2023. Information technology - Artificial intelligence - AI system life cycle processes. Geneva: ISO/IEC, 2023c. Disponível em: https://www.iso.org/standard/81118.html. *Acesso em: 1 maio 2026.*

JANSSEN, Heleen; LEE, Michelle Seng Ah; SINGH, Jatinder. Practical fundamental rights impact assessments. International Journal of Law and Information Technology, v. 30, n. 2, p. 200-232, 2022. DOI: https://doi.org/10.1093/ijlit/eaac018.

JOBIN, Anna; IENCA, Marcello; VAYENA, Effy. The global landscape of AI ethics guidelines. Nature Machine Intelligence, v. 1, p. 389-399, 2019. DOI: https://doi.org/10.1038/s42256-019-0088-2.

KAMINSKI, Margot E.; MALGIERI, Gianclaudio. Algorithmic impact assessments under the GDPR: producing multi-layered explanations. International Data Privacy Law, v. 11, n. 2, p. 125-144, 2021. DOI: https://doi.org/10.1093/idpl/ipaa020.

MITTELSTADT, Brent. Principles alone cannot guarantee ethical AI. Nature Machine Intelligence, v. 1, p. 501-507, 2019. DOI: https://doi.org/10.1038/s42256-019-0114-4.

MÖKANDER, Jakob; AXENTE, Maria. Ethics-based auditing of automated decision-making systems: intervention points and policy implications. AI & Society, v. 38, p. 153-171, 2023. DOI: https://doi.org/10.1007/s00146-021-01286-x.

MÖKANDER, Jakob; MORLEY, Jessica; TADDEO, Mariarosaria; FLORIDI, Luciano. Ethics-Based Auditing of Automated Decision-Making Systems: Nature, Scope, and Limitations. Science and Engineering Ethics, v. 27, art. 44, 2021. DOI: https://doi.org/10.1007/s11948-021-00319-4.

MÖKANDER, Jakob; SHETH, Margi; GERSBRO-SUNDLER, Maria; BLOMGREN, Pontus; FLORIDI, Luciano. Challenges and best practices in corporate AI governance: Lessons from the biopharmaceutical industry. Frontiers in Computer Science, v. 4, art. 1068361, 2022. DOI: https://doi.org/10.3389/fcomp.2022.1068361.

OECD. Recommendation of the Council on Artificial Intelligence. Paris: OECD, 2019. OECD/LEGAL/0449. Disponível em: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449. *Acesso em: 2 maio 2026.*

OECD. OECD Due Diligence Guidance for Responsible AI. Paris: OECD Publishing, 2026. DOI: https://doi.org/10.1787/41671712-en. Disponível em: https://www.oecd.org/en/publications/oecd-due-diligence-guidance-for-responsible-ai_41671712-en.html. *Acesso em: 3 maio 2026.*

TABASSI, Elham. Artificial Intelligence Risk Management Framework (AI RMF 1.0). Gaithersburg, MD: National Institute of Standards and Technology, 2023. NIST AI 100-1. DOI: https://doi.org/10.6028/NIST.AI.100-1.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia, Bruxelas, 2016. Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=pt. *Acesso em: 10 maio 2026.*

UNIÃO EUROPEIA. Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento da Inteligência Artificial). Jornal Oficial da União Europeia, Bruxelas, 2024. Disponível em: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng. *Acesso em: 16 maio 2026.*