

**UNIVERSIDADE DE SANTA CRUZ DO SUL
PROGRAMA DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO
MESTRADO PROFISSIONAL EM ADMINISTRAÇÃO**

Mariana Sandim Aguiar

**GOVERNANÇA E INTELIGÊNCIA ARTIFICIAL GENERATIVA:
DESAFIOS E RISCOS DA SHADOW AI NO AMBIENTE EMPRESARIAL**

Santa Cruz do Sul
2025

Mariana Sandim Aguiar

**GOVERNANÇA E INTELIGÊNCIA ARTIFICIAL GENERATIVA:
DESAFIOS E RISCOS DA SHADOW AI NO AMBIENTE EMPRESARIAL**

Dissertação apresentada ao Programa de Pós-Graduação em Administração – Mestrado da Universidade de Santa Cruz do Sul – UNISC, como requisito parcial para obtenção do título de Mestre em Administração.

Orientadores: Prof. Dr. Silvio Cesar Arend e Prof. Dr. Pietro Cunha Dolci

Santa Cruz do Sul

2025

Mariana Sandim Aguiar

**GOVERNANÇA E INTELIGÊNCIA ARTIFICIAL GENERATIVA:
DESAFIOS E RISCOS DA SHADOW AI NO AMBIENTE EMPRESARIAL**

Dissertação apresentada ao Programa de Pós-Graduação em Administração – Mestrado da Universidade de Santa Cruz do Sul – UNISC, Área de Concentração em Gestão de Negócios, Linha de Pesquisa em Gestão Estratégica de Operações e Relações Interorganizacionais, como requisito parcial para obtenção do título de Mestre em Administração.

Dr. Silvio Cezar Arend
Professor Orientador – UNISC

Dr. Pietro Cunha Dolci
Professor Coorientador - UNISC

Dr. Heron Sérgio Moreira Begnis
Professor Examinador – UNISC

Dr. Gabriel Silva Cogo
Professor Examinador - FGV

Santa Cruz do Sul

2025

CIP - Catalogação na Publicação

Sandim Aguiar, Mariana

Governança e Inteligência Artificial Generativa : Desafios e riscos da Shadow IA no ambiente empresarial / Mariana Sandim Aguiar. – 2025.

75f. ; 26 cm.

Dissertação (Mestrado em Administração) – Universidade de Santa Cruz do Sul, 2025.

Orientação: Prof. Dr. Silvio Cesar Arend.

Coorientação: Prof. Dr. Pietro Cunha Dolci.

1. Governança. 2. Inteligência Artificial Generativa. 3. Shadow IA. 4. Conformidade. I. Cezar Arend, Silvio. II. Cunha Dolci, Pietro. III. Título.

Dedico este trabalho a todos os professores.

Professores acadêmicos.

Professores da vida.

Professores da família e do trabalho.

Sem vocês, o aprendizado não teria direção, e a caminhada não teria sentido.

AGRADECIMENTOS

Este estudo tem o apoio exclusivo de dona Mara Núbia, minha mãe.
Obrigada pelo incentivo e por me lembrar que sou capaz.

RESUMO

A rápida evolução tecnológica tem ampliado o uso da Inteligência Artificial (IA) e, especialmente, da Inteligência Artificial Generativa (IA Gen) no ambiente corporativo, criando novas oportunidades, mas também desafios significativos de governança. Este estudo analisa como a governança corporativa pode mitigar os riscos decorrentes do uso indevido da Shadow IA e potencializar os benefícios da IA Gen nas organizações. A pesquisa, de natureza qualitativa e exploratória, baseou-se em entrevistas com gestores de três setores distintos — público, tecnológico e financeiro —, complementadas por revisão teórica sobre governança corporativa, IA e Shadow IT/AI. A análise evidenciou diferentes níveis de maturidade digital e de estruturação da governança, variando entre a ausência de políticas formais no setor público, a experimentação descentralizada no setor tecnológico e a postura cautelosa e regulatória no setor financeiro. Constatou-se que a governança exerce papel determinante na mitigação de riscos e na promoção de práticas éticas, transparentes e seguras. Como resultado, propõe-se o *Framework* de Governança para Inteligência Artificial (GIA), estruturado em cinco dimensões: princípios éticos, monitoramento e avaliação, engajamento de stakeholders, resolução de conflitos éticos e capacitação contínua. O modelo contribui para o uso responsável da IA Gen e para o fortalecimento das práticas de governança corporativa em um contexto de transformação digital acelerada.

Palavras-chave: Governança. Inteligência Artificial Generativa. Shadow IA. Conformidade.

ABSTRACT

The rapid technological evolution has expanded the use of Artificial Intelligence (AI), particularly Generative Artificial Intelligence (GenAI), in corporate environments, generating both opportunities and significant governance challenges. This study analyzes how corporate governance can mitigate the risks associated with the misuse of Shadow AI and enhance the benefits of GenAI within organizations. Using a qualitative and exploratory approach, the research was based on interviews with executives from three distinct sectors—public, technological, and financial—complemented by a theoretical review of corporate governance, AI, and Shadow IT/AI. The analysis revealed varying levels of digital maturity and governance structuring, ranging from the absence of formal policies in the public sector to decentralized experimentation in the technological sector and a cautious, compliance-oriented approach in the financial sector. The findings demonstrate that governance plays a decisive role in mitigating risks and promoting ethical, transparent, and secure practices. As a result, the Governance Framework for Artificial Intelligence (GIA) is proposed, structured around five dimensions: ethical principles, monitoring and evaluation, stakeholder engagement, ethical conflict resolution, and continuous training. The framework contributes to the responsible use of GenAI and strengthens corporate governance practices amid accelerated digital transformation.

Keywords: Governance. Generative Artificial Intelligence. Shadow AI. Compliance.

LISTA DE ILUSTRAÇÕES

Quadro 1 – Elementos e Barreiras <i>Shadow IT</i> e <i>Shadow AI</i>	20
Quadro 2 – Aspectos comparativos entre Governança Corporativa e Governança de IA	27
Quadro 3 – Elementos de Governança	33
Quadro 4 – Instrumento de Pesquisa (Entrevista)	35
Quadro 5 – Comparação entre os casos analisados nas dimensões de governança em IA	44
Figura 1 – Framework de Governança para Inteligência Artificial (GIA)	47

LISTA DE ABREVIATURAS

AI	<i>Artificial Intelligence</i> (Inteligência Artificial)
API	<i>Application Programming Interface</i> (Interface de Programação de Aplicações)
BYOAI	<i>Bring Your Own Artificial Intelligence</i> (Traga Sua Própria Inteligência Artificial)
CEO	<i>Chief Executive Officer</i> (Diretor Executivo)
COBIT	<i>Control Objectives for Information and Related Technologies</i> (Objetivos de Controle para Informação e Tecnologias Relacionadas)
GIA	Governança de Inteligência Artificial (<i>Framework</i> proposto para governança de IA Generativa)
GPT	<i>Generative Pre-trained Transformer</i> (Transformador Generativo Pré-Treinado)
IA	Inteligência Artificial
IA Gen	Inteligência Artificial Generativa
IBM	Institute for Business Value
ISO	International Organization for Standardization (Organização Internacional de Padronização)
IT	<i>Information Technology</i> (Tecnologia da Informação)
RAG	<i>Retrieval-Augmented Generation</i> (Geração Aumentada por Recuperação)
SaaS	<i>Software as a Service</i> (Software como Serviço)
TI	Tecnologia da Informação

SUMÁRIO

1	INTRODUÇÃO.....	01
1.1	Problema de Pesquisa.....	03
1.2	Objetivos.....	03
1.2.1	Objetivo Geral.....	03
1.2.2	Objetivos Específicos.....	03
1.3	Justificativa.....	04
2	REFERENCIAL TEÓRICO.....	07
2.1	Inteligência Artificial (IA).....	07
2.1.1	Inteligência Artificial Generativa (IA Gen).....	11
2.2	<i>Shadow IT e Shadow AI: Conceitos, Desafios e Implicações Organizacionais</i>	13
2.3	Bring-Your-Own-AI (BYOAI).....	20
2.4	Governança Corporativa e Governança de IA.....	22
2.4.1	Governança de TI (Tecnologia da Informação) como modelo de referência.....	28
2.4.2	Governança, Ética e a IA.....	30
3	METODOLOGIA.....	33
4	ANÁLISE DO USO DE IA GENERATIVA: PRÁTICAS, PERCEPÇÕES E DESAFIOS À LUZ DA GOVERNANÇA CORPORATIVA.....	38
5	PROPOSIÇÃO DE FRAMEWORK DE GOVERNANÇA PARA IA GENERATIVA (GIA).....	47
6	CONCLUSÃO.....	50
	REFERÊNCIAS.....	58

1 INTRODUÇÃO

As empresas enfrentam o risco constante de obsolescência, especialmente em mercados onde a inovação ocorre rapidamente e onde as expectativas dos consumidores evoluem com frequência. Um dos principais fatores que leva à obsolescência organizacional é o ciclo de vida curto dos produtos. Produtos bem-sucedidos podem perder relevância rapidamente diante do surgimento de alternativas superiores ou mais econômicas. Um exemplo emblemático pode ser observado no setor farmacêutico, em que tratamentos eficazes podem ser rapidamente superados por tecnologias mais avançadas ou pela entrada de novos competidores no mercado (WU; RANSBOTHAM, 2024). Essa dinâmica exige das empresas uma capacidade constante de adaptação e atualização de suas ofertas.

Outro aspecto que contribui para a obsolescência é a transformação no contexto de mercado e nas expectativas dos clientes. À medida que novas tecnologias, como veículos elétricos, ganham espaço, setores inteiros passam a demandar novos padrões de desempenho e qualidade. Nessa perspectiva, organizações que anteriormente satisfaziam bem determinados mercados podem ver suas soluções se tornarem insuficientes se não adaptarem seus produtos às novas exigências (WU; RANSBOTHAM, 2024). Soma-se a isso o aumento da complexidade e da variedade de possibilidades de inovação, o que demanda das organizações a exploração de um número crescente de materiais, tecnologias e modelos de desenvolvimento. A abordagem tradicional de tentativa e erro, além de morosa, torna-se custosa e menos competitiva nesse cenário.

Diante disso, a Inteligência Artificial (IA) e sua vertente generativa (IA Gen) emergem como ferramentas estratégicas para empresas que desejam inovar e manter-se competitivas. Segundo a *MIT Technology Review* (2024), em seu artigo “*Entre a inovação e a governança: desafios para a adoção da IA generativa*”, a adoção de IA Gen nas empresas desponta como uma tendência relevante, especialmente nos Estados Unidos, onde 83% das organizações planejam investir nessa tecnologia no biênio 2024–2025. Aplicada a processos de recombinação tecnológica, a IA permite a combinação de tecnologias existentes de maneiras inovadoras, viabilizando soluções e produtos mais alinhados às necessidades emergentes do mercado.

Essa capacidade é reforçada por estudos que apontam que a IA contribui significativamente para a redução do tempo e dos custos envolvidos no desenvolvimento de novas soluções, ao permitir testes rápidos e ajustes iterativos baseados em dados (WU; RANSBOTHAM, 2024). Outros autores, como Dwivedi *et al.* (2023), destacam que a aplicação da IA Gen tem acelerado ciclos de inovação e ampliado a personalização de processos em diversos setores. Além disso, ferramentas de IA são cada vez mais valorizadas por sua habilidade de sintetizar grandes volumes de dados e identificar padrões ocultos, orientando decisões estratégicas com maior precisão (TARIQ; POULIN; ABONAMAH, 2021). Em ambientes empresariais dinâmicos e sobrecarregados de informação, essa competência torna-se um diferencial competitivo. Nesse contexto, a adoção de soluções baseadas em IA e IA Gen está fortemente relacionada à busca por eficiência operacional e automação — pilares centrais da gestão moderna (BRYNJOLFSSON; McAFFEE, 2017; RANSBOTHAM *et al.*, 2021).

Adicionalmente, o alcance global da IA Gen e sua popularidade entre diferentes grupos demográficos destacam tanto seu potencial transformador quanto os desafios relacionados à sua adoção equitativa. Dados do Banco Mundial, apresentados por Qiang, Liu e Wang (2024), revelam que o ChatGPT, principal plataforma de IA Gen, ultrapassou a marca de 100 milhões de usuários ativos em apenas 64 dias após o lançamento da versão 3.5, alcançando 500 milhões de usuários mensais distribuídos por 209 países. Países de renda média como Índia e Brasil representam cerca de 50% do tráfego global da ferramenta, evidenciando sua penetração massiva em diferentes contextos.

Entretanto, a introdução da IA Gen no ambiente corporativo impõe uma série de riscos que não podem ser negligenciados. Esses riscos vão desde o uso inadequado — com impactos negativos sobre a governança corporativa, a ética e a conformidade regulatória — até vulnerabilidades ligadas à segurança cibernética e à proteção de dados (MACHADO *et al.*, 2022; NOZARI; SZMELTER-JAROSZ; GHAREMANI-NAHR, 2022). Nessa conjuntura, a governança corporativa assume papel central ao estabelecer diretrizes e mecanismos de controle que possibilitem a adoção segura e responsável dessas tecnologias, garantindo o alinhamento entre o uso da IA Gen, os objetivos estratégicos da organização e os princípios éticos (PREM, 2019; ZIANG; JIHAENG, 2021).

Neste estudo, a análise concentra-se na exploração da relação entre a governança corporativa e a adoção da Inteligência Artificial Generativa no ambiente empresarial. A pesquisa busca compreender de que forma a governança pode influenciar a implementação responsável da IA Gen, identificar os principais desafios enfrentados pelas empresas e avaliar os riscos associados ao uso não supervisionado dessas ferramentas.

Nesse cenário, torna-se essencial investigar não apenas as oportunidades oferecidas pela IA Gen, mas também as práticas de governança que podem atuar na mitigação de seus riscos. O objetivo é contribuir para que as empresas possam adotar essas tecnologias de forma ética, eficiente e segura, aproveitando suas potencialidades enquanto protegem os interesses dos stakeholders e a integridade organizacional.

1.1 Problema de Pesquisa

Como a governança corporativa pode mitigar riscos associados ao uso indevido da *Shadow AI* e potencializar os benefícios do uso da Inteligência Artificial Generativa (IA Gen) no ambiente empresarial?

1.2 Objetivos

1.2.1 Objetivo Geral

Analizar o papel da governança corporativa na mitigação dos riscos relacionados ao uso indevido da *Shadow AI* e na potencialização dos benefícios da Inteligência Artificial Generativa (IA Gen) em diferentes contextos organizacionais.

1.2.2 Objetivos Específicos

- a) Identificar, com base nas percepções dos entrevistados, os principais usos e riscos associados às ferramentas de Inteligência Artificial Generativa (IA Gen) nas organizações estudadas.

- b) Compreender as estruturas de governança existentes e avaliar em que medida elas funcionaram como mecanismos de mitigação dos potenciais riscos do mau uso da IA Gen.
- c) Propor um *framework* de governança corporativa para a gestão do uso de Inteligência Artificial Generativa nas empresas.

1.3 Justificativa

A adoção de ferramentas de Inteligência Artificial (IA) e Inteligência Artificial Generativa (IA Gen) está crescendo rapidamente nas empresas, oferecendo vantagens como aumento de eficiência, inovação e melhor tomada de decisão. De acordo com estudos recentes, a aplicação da IA Gen em ambientes corporativos têm mostrado potencial para transformar processos de negócios, desde a personalização de produtos até a automação do atendimento ao cliente (TARIQ; POULIN; ABONAMAH, 2021). Dwivedi *et al.* (2023) analisam essas transformações sob uma perspectiva multidisciplinar, destacando as oportunidades e riscos associados ao uso da IA generativa, especialmente no que diz respeito à confiança, ética e impactos nas práticas organizacionais. De forma complementar, Ransbotham *et al.* (2021) discutem como a IA vem redefinindo a inovação e a tomada de decisão empresarial, ao permitir maior integração entre análise de dados e estratégias corporativas. No entanto, o uso dessas tecnologias também traz riscos significativos, incluindo violações de privacidade, vieses nos algoritmos e uso indevido de dados (MACHADO *et al.*, 2023).

Apesar do crescente corpo de pesquisas sobre os benefícios da IA Gen, ainda existem lacunas substanciais em relação à governança dessas tecnologias. Estudos anteriores têm focado principalmente na implementação técnica e nos benefícios imediatos da IA, mas poucas investigações abordam de forma aprofundada os riscos e as melhores práticas para minimizá-los no contexto da governança corporativa (HOLANDA *et al.*, 2023). Além disso, há uma escassez de modelos estabelecidos que integrem a governança corporativa com a adoção de IA Gen, especialmente em relação à proteção contra vieses e à conformidade regulatória.

A governança corporativa em relação à Inteligência Artificial Generativa (IA Gen) enfrenta desafios substanciais, principalmente devido à ausência de modelos que integrem práticas éticas e gerenciem adequadamente os riscos associados. O

relatório do Institute for Business Value (IBM), “*The CEO Study 2024*”, identifica que, para muitos *Chief Executive Officers* (CEOs), a transparência e a governança são pilares essenciais para garantir a confiança e o uso responsável da IA Gen, especialmente no ambiente corporativo, onde essa tecnologia é empregada para ganho competitivo (IBM, 2024).

No Brasil, 82% dos líderes empresariais acreditam que a governança deve ser estabelecida desde o início do desenvolvimento da IA para evitar problemas éticos e regulatórios (IBM, 2024). A pressão para garantir conformidade aumenta ainda mais em contextos de *Bring-Your-Own-AI* (BYOAI), onde a introdução de ferramentas externas ao ambiente corporativo traz riscos adicionais, como a chamada *Shadow AI*, que pode comprometer a segurança e a integridade dos dados organizacionais (RUSSELL, 2023).

Para além das discussões éticas, a falta de diretrizes práticas na aplicação da governança de IA torna a tarefa das empresas ainda mais complexa. Kalkan (2024) aponta que, embora a disruptão tecnológica exija uma adaptação rápida e robusta, as empresas carecem de modelos de governança flexíveis que permitam essa adaptação de maneira segura. Segundo estudos como o de Pacheco *et al.* (2023), sem uma estrutura clara, as corporações ficam vulneráveis a usos indevidos e maliciosos da tecnologia. Nesse sentido, práticas de governança que envolvem a IA Gen precisam não só de uma estrutura inicial de implementação, mas de um acompanhamento contínuo para se adaptarem às rápidas inovações tecnológicas e aos novos riscos que surgem nesse cenário.

Além disso, a implementação de políticas de governança para IA Gen também exige um olhar atento à cultura organizacional e à aceitação pelos colaboradores, aspectos frequentemente mencionados como críticos para o sucesso da tecnologia. O relatório da IBM (2024), destaca que, para 74% dos CEOs, o engajamento e a aceitação cultural dos funcionários têm uma importância crucial na redução de riscos e no sucesso de longo prazo da IA Gen. Portanto, embora as capacidades técnicas sejam fundamentais, é a integração da governança com a cultura corporativa que realmente potencializa a tecnologia, criando um ambiente de inovação sustentável e minimizando possíveis resistências internas (IBM, 2024).

Portanto, esta pesquisa é relevante pois busca preencher essas lacunas, oferecendo uma análise de como a governança corporativa pode ser estruturada para minimizar as incertezas referentes ao uso de IA Gen. Ao estabelecer uma

estrutura de governança, a pesquisa não só contribui para a segurança e a ética na utilização dessas tecnologias, mas também promove uma abordagem que maximiza seus benefícios enquanto minimiza os riscos, proporcionando às empresas um equilíbrio necessário entre inovação e segurança.

2 REFERENCIAL TEÓRICO

Neste referencial teórico, são apresentados conceitos fundamentais que sustentam a base deste trabalho, abordando temas essenciais para a compreensão do estudo em questão. No cenário contemporâneo, a Inteligência Artificial (IA) emerge como um dos pilares da transformação digital, moldando o modo como as organizações operam e tomam decisões. Em particular, a vertente da Inteligência Artificial Generativa (IA Gen) tem ganhado destaque por sua capacidade de criar conteúdos inovadores e automatizar processos que anteriormente dependiam de intervenção humana. Este capítulo aborda a evolução e os impactos da IA e da IA Gen no contexto empresarial, explorando suas aplicações, vantagens e os desafios éticos e de governança que surgem com sua adoção.

A análise começa com uma visão abrangente dos conceitos fundamentais de IA, destacando o papel da IA Gen e suas implicações para a eficiência e a inovação nos negócios. Em seguida, abordamos o fenômeno do *Shadow IT* e sua extensão para o *Shadow AI*, explorando como o uso não autorizado dessas tecnologias pode afetar a segurança e a conformidade organizacional. A discussão também inclui a tendência do *Bring-Your-Own-AI* (BYOAI), uma prática que traz tanto oportunidades de inovação quanto riscos significativos para as empresas.

Por fim, destaca-se a importância da governança corporativa e suas adaptações necessárias para gerenciar o uso de IA de maneira ética e responsável. O capítulo analisa práticas de governança de IA e Tecnologia da Informação (TI), incluindo estruturas e diretrizes que buscam mitigar riscos, promover a transparência e assegurar que as tecnologias sejam alinhadas aos objetivos estratégicos das organizações.

2.1 Inteligência Artificial (IA)

A Inteligência Artificial (IA) é um campo vasto que envolve o desenvolvimento de máquinas capazes de realizar tarefas que exigem inteligência humana, como percepção, aprendizado e tomada de decisão. Esse conceito foi inicialmente abordado por pesquisadores como Stuart Russell e Peter Norvig, que definem a IA como “o estudo de agentes que recebem percepções do ambiente e realizam ações” (RUSSELL; NORVIG, 2010, p. 8). A IA moderna engloba diversas áreas, incluindo

aprendizado de máquina, redes neurais, processamento de linguagem natural, entre outras, sendo aplicada em diferentes campos, como a robótica, a automação de processos e a análise de dados.

Historicamente, a IA passou por várias fases de desenvolvimento. Conforme exposto por Barbosa e Bezerra (2020), a IA foi amplamente explorada desde meados do século XX, especialmente a partir da criação de sistemas especializados, como o Deep Blue, que derrotou o campeão mundial de xadrez Garry Kasparov, em 1997, e esse marco ilustra o avanço das máquinas em simular capacidades cognitivas humanas.

Antes disso, formalmente estabelecida em 1956, na Conferência de Dartmouth, onde o termo “inteligência artificial” foi utilizado pela primeira vez. Com os avanços na ciência computacional durante a Segunda Guerra Mundial, como os modelos matemáticos de Warren McCulloch e Walter Pitts, contribuíram para o surgimento da IA ao criar sistemas que imitavam processos cognitivos humanos (BARBOSA; BEZERRA, 2020). Na década de 1950, Frank Rosenblatt desenvolveu o Perceptron, uma rede neural que classificava informações, representando um avanço crucial no campo do aprendizado de máquinas.

Outro marco importante foi o desenvolvimento do chatbot Eliza na década de 1960, que permitiu simular interações humanas com base em palavras-chave. E, desde então, a evolução da IA tornou-se cada vez mais rápida, impulsionada pelo desenvolvimento de novos algoritmos e pela disponibilidade de grandes quantidades de dados para treinamento de sistemas (BARBOSA; BEZERRA, 2020).

Por outro lado, a introdução da IA em diversos setores traz consigo desafios significativos. Segundo um estudo de Machado *et al.* (2023), os principais desafios para a implementação da IA em processos organizacionais incluem a escassez de especialistas na área, a dificuldade de integração tecnológica e a necessidade de adaptação das leis e regulamentos (MACHADO *et al.*, 2023). Esses desafios estão associados à rápida expansão da IA e à incapacidade de muitos setores em acompanhar sua evolução. Além disso, o aumento da automação suscita questões éticas, especialmente no que se refere à substituição de trabalhadores por sistemas de IA e à privacidade dos dados processados por essas máquinas (BARBOSA; BEZERRA, 2020).

Outro fator crucial no avanço da IA é a colaboração entre seres humanos e máquinas. Tariq, Poulin e Abonamah (2021) apontam que a aliança entre IA e

trabalhadores humanos pode ser um diferencial para alcançar a excelência operacional em empresas. A IA, ao automatizar tarefas rotineiras, libera os funcionários para se concentrarem em atividades mais estratégicas e criativas, promovendo maior inovação e produtividade (TARIQ; POULIN; ABONAMAH, 2021). Essa ideia é reforçada no relatório da Microsoft (2023), que destaca como a IA pode ajudar a reduzir o “débito digital” — termo usado para descrever o excesso de informações e dados que sobrecarregam os trabalhadores —, permitindo maior foco em atividades inovadoras (MICROSOFT, 2023).

Entretanto, o uso da IA em áreas críticas, como a jurídica, ainda levanta preocupações quanto à confiabilidade dos sistemas. Magesh *et al.* (2024) alertam que, apesar de avanços como a Geração Aumentada por Recuperação (RAG), muitos sistemas de pesquisa legal assistida por IA ainda apresentam “alucinações” — ou seja, a geração de informações incorretas ou inventadas (MAGESH *et al.*, 2024). Esse problema demonstra que, embora a IA tenha potencial para melhorar a eficiência em muitos setores, sua implementação precisa ser supervisionada por especialistas, especialmente em áreas sensíveis, como o direito e a medicina.

Portanto, ao se considerar o impacto da IA em diversas áreas do conhecimento e da sociedade, percebe-se que, embora os benefícios sejam consideráveis, é necessário abordar os desafios de maneira cuidadosa. A IA tem o potencial de transformar o trabalho humano, aumentar a produtividade e impulsionar a inovação, desde que seus riscos sejam adequadamente gerenciados. Para isso, é imprescindível que os responsáveis pela implementação desses sistemas adotem práticas éticas, promovam a educação contínua em IA e garantam que as regulações acompanhem o ritmo das inovações tecnológicas (MACHADO *et al.*, 2023; TARIQ; POULIN; ABONAMAH, 2021).

E quando o tema é inovação e o uso de IA, pode-se considerar uma ferramenta poderosa que está remodelando a maneira como as sociedades e organizações operam conforme observam Wu e Ransbotham (2024). O futuro da IA depende tanto de avanços tecnológicos quanto de uma gestão responsável de suas aplicações, com foco em abrandar os desafios e maximizar os benefícios que ela pode trazer para a sociedade. Sua evolução deve ser guiada não apenas pela eficiência técnica, mas também pela reflexão ética e pelo compromisso com a melhoria das condições de trabalho humano.

A implementação da IA em processos de inovação apresenta desafios e, embora essa tecnologia seja eficaz em promover recombinações e melhorias incrementais, mostra-se limitada em inovações radicais, que frequentemente dependem de auxílio humano e de processos movidos pela criatividade. Segundo Wu e Ransbotham (2024), a IA é essencialmente uma ferramenta analítica e, portanto, pode não capturar nuances e intuições necessárias para romper totalmente com padrões estabelecidos. Além disso, o uso da IA para inovar requer uma infraestrutura adequada, tanto em termos de dados quanto de talentos.

Na mesma linha, os autores ressaltam que as empresas precisam investir em profissionais qualificados capazes de interpretar as sugestões fornecidas pelos algoritmos e aplicá-las no desenvolvimento de novos produtos. Esse investimento, contudo, pode representar um desafio financeiro e cultural, especialmente para organizações menos familiarizadas com o uso de tecnologias avançadas. Em complemento, Wu e Ransbotham (2024) argumentam que, apesar dessas dificuldades, a IA oferece um caminho promissor para que as empresas superem o risco de declínio, auxiliando na exploração rápida e eficiente de novas combinações tecnológicas e no aprimoramento de processos.

Em paralelo a IA, o uso da Inteligência Artificial Generativa tem crescido de forma exponencial, marcando 2023 como um ano decisivo para essa tecnologia. De acordo com pesquisa realizada pela consultoria McKinsey & Company (2023), um terço das empresas entrevistadas já utiliza regularmente a IA generativa em pelo menos uma função empresarial, e cerca de 40% planejam aumentar o investimento nessas ferramentas. É importante destacar, contudo, que o estudo reflete uma amostra composta majoritariamente por empresas de grande porte e alta maturidade digital, o que limita a generalização dos resultados. Em contrapartida, estudos acadêmicos têm corroborado a tendência de adoção crescente da IA em contextos empresariais diversos, indicando seu papel estratégico na transformação organizacional (BRYNJOLFSSON; McAfee, 2017; RANSBOTHAM *et al.*, 2021; DWIVEDI *et al.*, 2023).

Com destaque para áreas como marketing, desenvolvimento de produtos e operações de serviços, as organizações estão explorando as capacidades transformadoras da IA para otimizar processos e inovar em suas ofertas. Esse crescimento acelerado é também impulsionado pelo uso pessoal, com executivos do C-suite adotando o uso dessas ferramentas no dia a dia, o que reflete a

popularização e o reconhecimento da tecnologia como estratégica para o ambiente corporativo.

2.1.1 Inteligência Artificial Generativa (IA Gen)

A Inteligência Artificial Generativa (IA Gen) é uma vertente da Inteligência Artificial (IA) focada na criação de novos conteúdos a partir de padrões previamente aprendidos por sistemas de aprendizado profundo. De acordo com Trocin *et al.* (2021), a IA Gen difere da IA tradicional por ser capaz de gerar novas informações em vez de apenas processar e analisar dados. Exemplos práticos incluem a criação de imagens, textos, músicas e até mesmo soluções inovadoras em design de produtos ou otimização de processos. O uso de redes neurais profundas permite que esses sistemas identifiquem padrões complexos em grandes volumes de dados e, a partir disso, geram novas saídas criativas e funcionais (TROCIN *et al.*, 2021).

Com esse cenário a IA Gen ganhou ainda mais força e o que permitiu um salto qualitativo no processamento de grandes volumes de dados e na capacidade de “aprender” com esses dados de maneira autônoma. Isso possibilitou a criação de novos conteúdos, algo que até então era uma característica exclusiva do ser humano (TROCIN *et al.*, 2021). Essas ferramentas têm sido utilizadas em diversas indústrias para automatizar processos criativos, personalizar experiências do cliente, e inovar na criação de novos produtos e serviços.

A expansão recente da IA Gen intensificou sua incorporação em rotinas organizacionais de modo descentralizado e, por vezes, fora de processos formais de governança. Isso se deve, em grande medida, à acessibilidade das ferramentas generativas via interfaces web e serviços em nuvem, que reduz barreiras de adoção e permite que indivíduos e equipes utilizem soluções de IA sem mediação do departamento de TI. Nesse contexto, observa-se o crescimento do fenômeno denominado **Shadow AI**, definido como o “*uso de ferramentas, modelos ou sistemas de IA por funcionários de uma organização sem endosso explícito, supervisão ou gestão por parte dos departamentos de TI e cibersegurança*” (PUTHAL *et al.*, 2025, p. 1). Assim, a capacidade da IA Gen de gerar conteúdo e automatizar tarefas cognitivas, somada à facilidade de acesso, favorece usos que extrapolam canais formais, exigindo atenção às implicações organizacionais e aos riscos de segurança e conformidade.

Segundo Mandapuram, Gutlapalli e Bodepudi (2018), a IA Gen permite não apenas a criação de conteúdos inéditos, mas também facilita processos como simulações de materiais em várias escalas, reduzindo custos de desenvolvimento. Essa tecnologia tem um impacto considerável em setores criativos, como design de moda e interiores, onde ela pode gerar designs únicos e adaptados. O desenvolvimento da IA Gen foi impulsionado pelo avanço de modelos de aprendizado profundo (DL), que permitem a modelagem de representações complexas de dados e a geração de novos conteúdos similares aos dados reais (BANH; STROBEL, 2023).

Modelos como redes adversariais generativas (GANs) utilizam duas redes neurais em competição, onde um gerador cria amostras de dados e um discriminador as avalia, promovendo a geração de conteúdos cada vez mais realistas (GUTLAPALLI, 2017). Outros exemplos de modelos de IA Gen incluem os autoencoders variacionais (VAEs), que são eficazes em reproduzir dados complexos em espaços latentes, e os transformadores, como o GPT (*Generative Pre-trained Transformer*), que se destacam na produção de texto humano (GOODFELLOW; BENGIO; COURVILLE, 2016; MANDAPURAM; GUTLAPALLI; BODEPUDI, 2018).

A evolução histórica da IA Gen pode ser rastreada até os avanços iniciais em redes neurais e aprendizado profundo. Nos anos 2010, a introdução das GANs por Ian Goodfellow e sua equipe foi um marco significativo que revolucionou a geração de imagens e vídeos (GOODFELLOW; BENGIO; COURVILLE, 2016). A partir dessa descoberta, surgiram modelos mais sofisticados, como os modelos de difusão, que permitem a criação de imagens de alta qualidade a partir de ruído, e os transformadores, que se tornaram a base para os modelos de linguagem modernos, como o GPT-3 e GPT-4 da empresa OpenAI.

Os exemplos práticos de IA Gen são vastos e incluem a criação de assistentes virtuais que interagem de forma natural com os usuários, a produção de obras de arte digitais inovadoras e a composição de músicas originais. Modelos como o DALL-E e o Midjourney tornaram possível a criação de imagens realistas a partir de descrições textuais, impactando áreas como marketing e design (THODUPUNORI; GUTLAPALLI, 2018). No campo da medicina, a IA Gen tem sido usada para simular estruturas moleculares e auxiliar na descoberta de novos medicamentos, reduzindo significativamente o tempo e os custos de pesquisa (ALI; MURAD; SHAH, 2023).

A IA Gen também apresenta desafios éticos e técnicos, como a necessidade de lidar com a qualidade dos dados e evitar vieses que possam estar presentes nos conjuntos de treinamento. Esses rumos podem impactar negativamente os resultados, levando a resultados potencialmente discriminatórios (STANTON; CLUNE, 2016). Além disso, a proteção de dados e a privacidade são preocupações crescentes, pois a coleta massiva de dados para treinamento pode ameaçar a segurança das informações pessoais (GUTLAPALLI, 2017).

2.2 *Shadow IT* e *Shadow AI*: Conceitos, Desafios e Implicações Organizacionais

O conceito de *Shadow IT* refere-se ao uso de sistemas de tecnologia da informação por funcionários dentro de uma organização sem o conhecimento, controle ou aprovação formal do departamento de TI. Essas tecnologias são frequentemente adotadas como resposta às percepções de inadequação dos sistemas oficiais disponibilizados pela empresa, permitindo que os usuários encontrem alternativas para melhorar sua eficiência e produtividade. Embora esse fenômeno tenha potencial para inovar e otimizar processos, ele também traz desafios significativos no que diz respeito à segurança da informação, conformidade com normas internas e governança de TI (HAAG; ECKHARDT, 2014; GYÖRY *et al.*, 2012; SILIC; BACK, 2014).

A literatura sobre *Shadow IT* explora amplamente o uso de tecnologias não sancionadas em ambientes de trabalho, destacando as razões que levam os funcionários a recorrerem a essas soluções. Conforme Haag e Eckhardt (2014), o fenômeno de *Shadow IT* ocorre como uma reação a restrições percebidas nos sistemas oficiais. Essas restrições incluem falta de flexibilidade, complexidade de uso ou simplesmente a inadequação das ferramentas disponíveis para atender às demandas específicas do trabalho. Como resultado, funcionários recorrem a tecnologias alternativas, como serviços em nuvem ou aplicativos de comunicação, sem a devida aprovação ou controle do departamento de TI.

Segundo Mallmann, Maçada e Oliveira (2018), o uso de *Shadow IT* é especialmente prevalente em contextos em que a colaboração e a troca de conhecimento são essenciais. Os autores identificam o uso de sistemas como WhatsApp, Google Drive e Skype como exemplos de tecnologias não autorizadas

que facilitam a comunicação e o compartilhamento de informações em tempo real entre colegas de trabalho, clientes e parceiros externos. O uso dessas ferramentas ocorre principalmente porque as soluções corporativas oficiais são vistas como ineficientes para promover uma colaboração rápida e eficaz.

Além disso, a flexibilidade das soluções alternativas permite que os usuários adaptem essas tecnologias às suas necessidades individuais ou de equipe. Conforme M. Silic, D. Silic e Oblakovic (2016), essa autonomia na adoção de soluções de *Shadow IT* muitas vezes resulta em inovações não previstas pelos gestores de TI. Esses autores apontam que, embora a *Shadow IT* traga preocupações em relação à segurança, ela também pode ser uma fonte significativa de inovação, à medida que permite aos usuários desenvolverem novos processos e soluções para problemas que os sistemas tradicionais não conseguem resolver adequadamente.

O conceito de *Shadow AI* surge como uma extensão natural do fenômeno de *Shadow IT*, com foco na adoção de tecnologias de IA sem o consentimento ou supervisão formal do departamento de TI. Embora *Shadow AI* possa ser compreendida como um desdobramento do fenômeno de *Shadow IT*, sua especificidade está relacionada ao tipo de processamento realizado por sistemas de inteligência artificial e ao potencial de impacto sobre dados, rotinas e decisões organizacionais. Puthal et al. (2025) caracterizam *Shadow AI* como o uso de ferramentas, modelos ou sistemas de IA por colaboradores sem autorização formal e sem supervisão das áreas responsáveis por tecnologia da informação e cibersegurança. Segundo os autores, esse uso pode ocorrer mesmo quando os funcionários buscam atender demandas legítimas de produtividade, automação e eficiência, porém fora dos mecanismos institucionais de controle e governança (PUTHAL et al., 2025). Nesse sentido, *Shadow AI* não deve ser interpretada apenas como um desvio individual, mas como um fenômeno organizacional que pode gerar ganhos operacionais no curto prazo, ao mesmo tempo em que amplia riscos relacionados à segurança, conformidade e responsabilização sobre o uso e o tratamento de dados.

Magunduni e Chigona (2018) observam que a *Shadow AI* está relacionada à crescente disponibilidade de ferramentas de IA acessíveis, como algoritmos de aprendizado de máquina e assistentes virtuais, que podem ser usados por funcionários sem a necessidade de aprovação dos gestores de TI. Esses sistemas,

muitas vezes, são implantados para resolver problemas operacionais específicos ou para aumentar a produtividade. No entanto, assim como ocorre com a Shadow IT, o uso não supervisionado de IA levanta questões importantes sobre segurança e privacidade, especialmente no que diz respeito ao tratamento de dados sensíveis.

Do ponto de vista da cibersegurança, Shadow AI pode ampliar significativamente os riscos organizacionais, pois envolve o uso de ferramentas não monitoradas para processar informações potencialmente sensíveis e operar fora de padrões de controle e auditoria. Puthal et al. (2025) destacam que esse tipo de uso pode aumentar a exposição a incidentes como vazamento de dados, falhas de segurança e descumprimento de requisitos de conformidade, ampliando o cenário de ameaças enfrentado pelas organizações. Além disso, os autores ressaltam que a ausência de supervisão facilita vulnerabilidades técnicas relevantes, como o risco de envenenamento de modelos (*model poisoning*), quando modelos podem ser corrompidos por dados manipulados, comprometendo a integridade de suas saídas e decisões (PUTHAL et al., 2025). Dessa forma, a Shadow AI deve ser compreendida como um fenômeno que não se restringe à adoção informal de tecnologia, mas que pode afetar diretamente a proteção de dados, a confiabilidade de processos e a responsabilidade institucional sobre decisões apoiadas por IA.

O conceito de 'inovações sombrias' (*shadow innovations*) de M. Silic, D. Silic e Oblakovic (2016) é particularmente relevante para entender o fenômeno da Shadow AI. Os autores definem o conceito a partir do uso de soluções de Shadow IT por funcionários para criar processos ou produtos, gerando benefícios significativos para a organização. Essa mesma dinâmica pode ser observada com o uso de ferramentas de IA Generativa, onde os colaboradores, sem o conhecimento ou aprovação dos departamentos de TI, aplicam essas soluções para otimizar fluxos de trabalho ou desenvolver novas ideias. Esse é o cerne do que pode ser chamado de Shadow AI. No entanto, assim como no contexto original do Shadow IT, a ausência de supervisão formal representa uma ameaça para a segurança e a integridade dos dados organizacionais.

Além da interpretação de Shadow AI como continuidade de Shadow IT, estudos recentes aprofundam o fenômeno ao enquadrá-lo como uma forma de inovação conduzida por usuários de maneira não institucionalizada e, em certos casos, deliberadamente oculta. Waters-Lynch et al. (2025) propõem o conceito de *Shadow User Innovation (SUI)* para descrever inovações iniciadas por colaboradores

que ocorrem sem transparência formal para a organização, favorecidas pela facilidade de acesso e pela baixa rastreabilidade de ferramentas digitais, como as soluções de IA generativa. Nesse sentido, o uso de IA Gen pode permanecer invisível à gestão, o que dificulta a captura de aprendizado organizacional e a disseminação de melhorias que poderiam ser escaladas de forma segura. Assim, Shadow AI passa a representar não apenas um risco de conformidade e segurança, mas também um desafio para transformar ganhos individuais e locais em capacidade organizacional estruturada (WATERS-LYNCH et al., 2025).

Embora a *Shadow IT* e a *Shadow AI* sejam frequentemente associadas a riscos relacionados à segurança da informação e conformidade com normas internas, elas também podem trazer benefícios consideráveis para as organizações. Conforme M. Silic, D. Silic e Oblakovic (2016), os usuários dessas tecnologias muitas vezes encontram soluções que atendem melhor às suas necessidades específicas de trabalho, resultando em maior produtividade e eficiência. Além disso, o uso de *Shadow IT* pode permitir que os funcionários inovem de maneira mais rápida e flexível, uma vez que não estão sujeitos às limitações impostas pelos sistemas oficiais.

No entanto, os riscos associados à *Shadow IT* e à *Shadow AI* não podem ser ignorados. Györy et al. (2012) destacam que o uso de sistemas não sancionados pode comprometer a segurança dos dados organizacionais, uma vez que esses sistemas muitas vezes não seguem os protocolos de segurança estabelecidos. Além disso, o uso não autorizado de tecnologias pode levar à duplicação de dados e à criação de silos de informações, dificultando a gestão eficiente e a tomada de decisões estratégicas.

Outro desafio destacado por Haag e Eckhardt (2014) é a violação das normas injuntivas de TI, que são regras formais estabelecidas pelas organizações para garantir a conformidade e a segurança no uso das tecnologias da informação. O uso de *Shadow IT* e *Shadow AI* representa uma transgressão dessas normas, o que pode resultar em consequências graves para as empresas, incluindo sanções legais e danos à reputação. Os exemplos de *Shadow IT* mais comumente observados incluem o uso de soluções em nuvem, como Google Docs e Dropbox, para armazenar e compartilhar dados empresariais fora do controle do departamento de TI. Além disso, os funcionários frequentemente recorrem a ferramentas de comunicação, como WhatsApp e Slack, para colaborar com colegas de trabalho de

forma mais rápida e eficiente, sem utilizar os sistemas oficiais da empresa (MALLMANN; MAÇADA; OLIVEIRA, 2018).

Uma contribuição teórica relevante para compreender por que determinadas práticas associadas à Shadow AI permanecem ocultas nas organizações é o mecanismo de “limiar de revelação” proposto por Waters-Lynch et al. (2025). De acordo com os autores, a decisão de revelar ou manter uma inovação em caráter não declarado depende da relação entre (i) benefícios percebidos de produtividade, (ii) nível de confiança no ambiente organizacional e (iii) expectativa de sanções formais ou informais. Os autores sintetizam essa relação pela expressão $\Delta P \times T > S$, na qual ΔP representa o ganho percebido, T corresponde ao nível de confiança e S refere-se à sanção esperada (WATERS-LYNCH et al., 2025). Essa formulação contribui para interpretar Shadow AI como um fenômeno influenciado não apenas por lacunas técnicas de governança, mas também por fatores organizacionais e culturais que podem desestimular a transparência e incentivar o uso de ferramentas fora dos canais institucionais.

Em relação à *Shadow AI*, um exemplo típico é o uso de algoritmos de aprendizado de máquina para analisar grandes volumes de dados sem a supervisão do departamento de TI. Essas práticas podem ser benéficas em termos de automação de processos e melhoria da eficiência, mas também trazem desafios significativos, especialmente no que diz respeito à conformidade com as leis de proteção de dados, como o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia.

Para os gestores de TI, o desafio está em equilibrar os benefícios potenciais da *Shadow IT* e *Shadow AI* com os riscos associados a essas práticas. Conforme Silic e Back (2014), é necessário desenvolver políticas de governança de TI que permitam aos funcionários explorar inovações tecnológicas de forma segura, ao mesmo tempo em que garantem que as normas de segurança e conformidade sejam respeitadas. Uma abordagem contemporânea para equilibrar inovação e governança no uso de IA, especialmente em aplicações de IA generativa, consiste em estruturar processos de validação controlada em ambiente real de trabalho antes da adoção plena. Sidorkin (2025) argumenta que benchmarks tradicionais de IA, embora úteis para comparações gerais entre modelos, oferecem pouca orientação para gestores que precisam avaliar o desempenho em tarefas específicas, com regras e particularidades organizacionais. Como alternativa, o autor propõe o

Shadow Testing Protocol (STP), um protocolo baseado na execução paralela entre humanos e sistemas de IA, com registro sistemático das divergências e análise de desempenho com base em evidências auditáveis (SIDORKIN, 2025). Essa lógica permite testar a tecnologia sem interromper rotinas críticas, estabelecer parâmetros comparativos com o desempenho humano e construir trilhas de validação e monitoramento, reduzindo riscos associados à adoção precipitada e favorecendo a institucionalização segura do uso de IA nas organizações.

O fenômeno da *Shadow AI* representa um desafio crescente para as organizações, à medida que tecnologias de inteligência artificial se tornam acessíveis e populares entre os funcionários. Assim como na *Shadow IT*, o uso de IA não supervisionado por áreas de TI ocorre frequentemente devido à percepção de que as ferramentas oficiais são insuficientes para resolver as necessidades diárias de trabalho. Esse uso de IA sem controle apresenta riscos significativos, que vão desde a segurança da informação até questões éticas e de conformidade. Tais riscos requerem que os gestores encontrem um equilíbrio entre incentivar a inovação liderada pelos usuários e assegurar que as normas e políticas da organização sejam rigorosamente seguidas.

Os riscos de segurança e de ética envolvidos na *Shadow AI* são profundos e complexos, como ilustrado pelo conceito da “Síndrome de Frankenstein”. Inspirado na obra de Mary Shelley, esse conceito destaca o temor de que criações tecnológicas possam escapar ao controle de seus criadores e trazer consequências imprevistas. Argumenta Hernán Poblete Miranda (2024) que a IA permite desde a criação de *deep fakes* até a vigilância em massa, gerando uma nova dimensão de manipulação da informação e controle que vai além das preocupações tradicionais de segurança digital. Assim, a *Shadow AI* amplia as ameaças ao possibilitar o uso indevido de dados e à criação de conteúdos enganosos, intensificando a perda de controle sobre decisões e operações que antes eram exclusivas dos gestores (MIRANDA, 2024).

Essas práticas descontroladas da IA são motivadas, em grande parte, pela facilidade com que os funcionários podem acessar ferramentas de inteligência artificial. Segundo Chuvakin e Kaganovich (2024), as tecnologias de IA gerativa – como modelos de linguagem e assistentes virtuais – têm potencial para aumentar a produtividade e eficiência, mas, ao serem adotadas sem a supervisão apropriada, tornam-se um risco iminente para a segurança da informação corporativa e para o

compliance. Eles destacam que as empresas precisam desenvolver abordagens eficazes de governança para evitar o vazamento de dados sensíveis e garantir que as tecnologias utilizadas estejam em conformidade com as normas de segurança e privacidade estabelecidas.

Para reduzir os possíveis impactos da inteligência artificial, especialistas destacam a importância de estratégias robustas que envolvam políticas de governança bem definidas e treinamento contínuo. Joaquim Campos (2024) reforça a necessidade de diretrizes claras para o uso responsável de IA, sugerindo a criação de uma plataforma centralizada para a governança de dados e modelos. Esse controle unificado garante que as práticas de IA estejam alinhadas aos objetivos corporativos e que o uso de dados cumpra os padrões éticos e regulatórios. Além disso, Campos recomenda que treinamentos recorrentes capacitem os colaboradores a operar essas ferramentas de forma ética e segura, promovendo uma compreensão clara dos limites e potenciais da tecnologia de IA (CAMPOS, 2024).

Outra recomendação fundamental é a adoção de soluções corporativas específicas para IA, projetadas para operar em um ambiente seguro. Segundo o artigo da Forbes sobre o assunto, escrito por Sharon Maher (2024), declara que a utilização de IA corporativa, desenvolvida com robustez e controles de segurança, é crucial para proteger dados organizacionais e para garantir o uso ético das ferramentas de IA. Ela ressalta que plataformas como a Duet AI, que oferece criptografia e controle rigoroso de dados, são alternativas mais seguras em comparação com ferramentas de IA voltadas ao consumidor, minimizando os riscos de vazamento de informações e fortalecendo o compliance da organização.

Em suma, o uso não supervisionado de IA nas organizações – ou *Shadow AI* – exige uma abordagem criteriosa e equilibrada. Embora a inovação tecnológica impulsionada pelos usuários possa trazer benefícios consideráveis, como aumento da produtividade e flexibilidade nos processos, ela também implica desafios que podem comprometer a segurança e a integridade dos dados organizacionais. O estabelecimento de políticas robustas de governança, o investimento em capacitação e treinamento contínuo e a adoção de soluções de IA específicas para o ambiente corporativo são passos essenciais para assegurar que os benefícios da IA sejam aproveitados de maneira ética e segura, protegendo a integridade e a reputação das organizações frente aos riscos inerentes a essa tecnologia.

Todos esses elementos, aspectos e barreiras discutidos pelos autores estão sintetizados no Quadro 1 abaixo:

Quadro 1 – Elementos e Barreiras *Shadow IT* e *Shadow AI*

Aspecto	<i>Shadow IT</i>	<i>Shadow AI</i>
Conceito	Uso de tecnologias de TI sem aprovação formal da organização.	Uso de ferramentas de IA sem aprovação ou supervisão formal da organização.
Motivação para Uso	Responder a necessidades não atendidas pelos sistemas oficiais, aumento de flexibilidade e eficiência.	Automação de processos, personalização de serviços, aumento de produtividade.
Principais Ferramentas Utilizadas	Google Drive, WhatsApp, Dropbox, Slack.	Algoritmos de <i>Machine Learning</i> , assistentes virtuais, ferramentas de IA Gerativa.
Benefícios Potenciais	Inovação, colaboração eficiente, aumento de produtividade.	Automação, análise de dados avançada, inovação em processos
Desafios e Riscos	Riscos de segurança, conformidade e governança, duplicação de dados e silos informacionais.	Segurança de dados, questões éticas e de compliance, manipulação de dados.
Exemplos de Riscos	Violação de normas de TI, vazamento de dados.	<i>Deep fakes</i> , vigilância em massa, manipulação de informação.
Soluções Recomendadas	Políticas de Governança, capacitação e treinamento contínuo, ferramentas corporativas seguras.	Governança de IA, diretrizes claras para uso ético, IA corporativa com controle de segurança.
Diferenças Claras	Relaciona-se ao uso de tecnologias não sancionadas para comunicação, colaboração e armazenamento de dados fora dos canais oficiais da organização.	Focado em ferramentas de Inteligência Artificial não sancionadas que automatizam tarefas, processam dados avançados ou personalizam serviços sem supervisão de TI.

Fonte: Elaborado pela autora.

2.3 Bring-Your-Own-AI (BYOAI)

Para a autora Emilie Blin (2024) que aborda o conceito emergente de *Bring-Your-Own-AI* (BYOAI), que, à semelhança do *Bring-Your-Own-Device* (BYOD),

permite que os colaboradores utilizem suas próprias ferramentas de Inteligência Artificial (IA) no ambiente de trabalho. Segundo a autora, essa tendência está prevista para ganhar relevância em 2024, com uma estimativa de que 60% dos trabalhadores em grandes empresas utilizem suas soluções de IA personalizadas. O BYOAI pode incluir desde robôs-táxis até drones para entrega de produtos, e promete aumentar a produtividade e personalização nas operações diárias.

Contudo, Blin (2024) destaca que essa prática também levanta preocupações, principalmente em relação à segurança de dados, conformidade com políticas corporativas, e o controle sobre o uso indevido ou não regulamentado dessas tecnologias no ambiente empresarial. Assim, ela sugere que as empresas precisam adotar uma governança sólida para garantir que as ferramentas de IA sejam usadas de maneira ética e responsável, minimizando os riscos associados (BLIN, 2024). Ou seja, embora o BYOAI possa oferecer vantagens em termos de inovação e eficiência, ele também apresenta desafios significativos para a governança e a segurança das empresas.

Segundo Russell (2023), o BYOAI representa uma nova era em que os funcionários utilizam suas próprias ferramentas de Inteligência Artificial para aumentar a produtividade e personalizar processos no trabalho. A facilidade de acesso a IA de ponta, como o ChatGPT e o GitHub Copilot, permite aos funcionários inovarem de forma descentralizada. No entanto, a implementação descontrolada dessa prática pode gerar riscos significativos, como falhas de segurança, perda de propriedade intelectual e questões éticas, principalmente em modelos de IA que não passam por uma supervisão adequada.

Para Hewitt (2023), o uso de ferramentas de IA sem o conhecimento da empresa pode ser descrito como *Shadow AI*, uma forma de BYOAI que ocorre de maneira informal, fora das políticas corporativas. Esse fenômeno acentua problemas relacionados à conformidade e governança. As empresas que adotam o BYOAI sem estabelecer políticas claras podem enfrentar desde vazamento de dados sensíveis até falhas na conformidade regulatória, além do risco de modelos de IA perpetuar vieses discriminatórios.

Tanto Russel (2023) e Hewitt (2023) sugerem que, para conter esses riscos, as organizações devem implementar um Centro de Excelência em IA (CoE). O CoE seria responsável por estabelecer diretrizes de governança, melhores práticas e oferecer suporte à experimentação controlada de IA pelos colaboradores. Hewitt

(2023) também destaca que a criação de uma política de BYOAI mais flexível e empática pode ajudar a fomentar um ambiente de inovação segura, permitindo que as empresas aproveitem as vantagens competitivas do uso de IA de forma alinhada às metas corporativas.

Além disso, Russell (2023) afirma que a adoção do BYOAI prenuncia um momento de virada semelhante ao da introdução do BYOD (*Bring-Your-Own-Device*), com a IA se tornando parte essencial tanto da vida pessoal quanto profissional dos colaboradores. Ele alerta que, assim como o BYOD, o BYOAI traz complexidade para a governança corporativa, exigindo maior vigilância quanto à integração de dispositivos com IA nas operações empresariais.

2.4 Governança Corporativa e Governança de IA

O conceito de governança é amplamente discutido em diversos campos do conhecimento, principalmente a partir dos anos 1990. De acordo com Gonçalves (2021), o termo “*governance*” foi introduzido em reflexões conduzidas pelo Banco Mundial, com o objetivo de compreender as condições que garantem a eficiência de um Estado. O conceito é definido como o “*exercício da autoridade, controle, administração, poder de governo*” (BANCO MUNDIAL, 1992 *apud* GONÇALVES, 2021, p. 400), sendo uma maneira pela qual o poder é exercido na administração dos recursos sociais e econômicos com foco no desenvolvimento sustentável e na equidade social.

A governança corporativa, como abordada por Pacheco *et al.* (2023) no livro “*Ética, Governança e Inteligência Artificial*”, é apresentada como um conjunto essencial de práticas e processos que asseguram o equilíbrio entre os interesses dos stakeholders e a transparéncia nas decisões empresariais. Os autores Pacheco *et al.* (2023) destacam que, no contexto atual, onde as inovações tecnológicas, como a Inteligência Artificial (IA), desempenham um papel cada vez mais central, a governança precisa ir além das práticas tradicionais. A governança corporativa, alinhada com essas novas realidades tecnológicas, exige uma abordagem multifacetada que garanta a adoção de decisões éticas, transparentes e sustentáveis no uso da IA.

Nesse contexto, as contribuições de Kalkan (2024) e Hilb (2020) complementam essa visão ao explorarem como a IA está moldando o futuro da

governança corporativa. Eles destacam que a IA, ao fornecer capacidades analíticas avançadas e previsões preditivas, oferece uma oportunidade significativa para melhorar a eficiência dos processos decisórios e otimizar a operação empresarial. No entanto, esses benefícios não estão isentos de desafios. Conforme enfatizado por Kalkan (2024), a governança corporativa precisa ser redefinida para acomodar a natureza disruptiva da IA, integrando considerações éticas e promovendo a transparência em suas aplicações. Assim, o uso da IA exige a adoção de diretrizes éticas específicas, práticas transparentes e monitoramento contínuo, de modo que suas decisões estejam alinhadas aos objetivos de governança corporativa e aos valores da sociedade.

Hilb (2020) avança com uma análise mais profunda dos níveis de automação que a IA pode alcançar na governança corporativa, propondo cinco cenários de “inteligência sinérgica”, que variam desde a inteligência assistida, na qual a IA apenas apoia os humanos, até a inteligência autopoética, onde a IA poderia evoluir de forma autônoma, tomando decisões e expandindo seu escopo sem a necessidade de intervenção humana. Essa visão amplia o debate proposto por Pacheco *et al.* (2023) sobre a importância de uma governança que regule e supervisione o uso da IA.

Além disso, Hilb (2020) destaca os desafios éticos e legais que surgem com o uso da IA em decisões empresariais de alto nível, particularmente no que diz respeito à responsabilidade corporativa e à proteção de dados. Para ele, a responsabilidade pela utilização de algoritmos e o viés algorítmico devem ser cuidadosamente geridos, tal como discutido por Pacheco *et al.* (2023), que sublinham a importância de mitigar riscos relacionados a tendências nos algoritmos e impactos sobre a privacidade. As implicações éticas da IA, como o controle do viés nos algoritmos e a distribuição justa dos benefícios gerados pela tecnologia, são centrais nas discussões sobre como a IA deve ser implementada nas organizações.

Kalkan (2024) reforça essa necessidade de regulação, enfatizando que a governança corporativa deve evoluir para garantir que os avanços tecnológicos sejam utilizados de forma responsável, evitando riscos e maximizando os benefícios para todas as partes envolvidas. Em uma linha semelhante, Pacheco *et al.* (2023) apontam que as práticas de governança precisam se adaptar às crescentes exigências de responsabilidade social corporativa, especialmente no que diz respeito às implicações éticas da IA no ambiente empresarial. Ambos os autores defendem

que a governança eficaz deve se alinhar a princípios éticos, com foco na transparência, integridade e na criação de valor de longo prazo, não apenas para os acionistas, mas para toda a sociedade.

Portanto, a integração das análises de Kalkan (2024) e Hilb (2020) com as observações de Pacheco *et al.* (2023) ressalta a importância de uma governança corporativa adaptativa, capaz de lidar com os desafios éticos, tecnológicos e legais apresentados pela IA. A governança do futuro precisará equilibrar a inovação com a responsabilidade, garantindo que a IA seja uma ferramenta para a criação de valor sustentável, ética e transparente.

Sendo assim a governança da Inteligência Artificial (IA) um tema emergente e fundamental no contexto do avanço tecnológico global, especialmente devido ao impacto crescente da IA em diversos setores da sociedade. Diversos autores abordam a necessidade de estruturar e regular essa tecnologia de maneira que ela beneficie a sociedade, minimizando os riscos associados. Almeida (2022) destaca que, embora a IA traga benefícios significativos, como maior eficiência e soluções inovadoras para problemas complexos, também apresenta riscos consideráveis, como discriminação, perda de privacidade e desemprego. A autora afirma que a regulação da IA é necessária para mitigar esses riscos, balanceando inovação e segurança. Para isso, ela sugere uma combinação de *hard law* e *soft law*: onde legislações obrigatórias se combinam com diretrizes flexíveis para assegurar que o desenvolvimento da IA seja ético e confiável (ALMEIDA, 2022).

Nesse cenário, Schneider *et al.* (2022) reforçam a importância de uma estrutura robusta de governança de IA dentro das empresas, propondo um arcabouço conceitual que abrange a governança de dados, modelos de aprendizado de máquina e sistemas de IA como um todo. A preocupação central é garantir que esses elementos sejam geridos de forma transparente e responsável, evitando a perpetuação de vieses nos dados e assegurando a conformidade com regulamentações de privacidade e segurança. A governança de IA, segundo os autores, é essencial para lidar com os desafios éticos e operacionais da tecnologia, especialmente no que se refere ao controle dos resultados produzidos por sistemas autônomos, os quais muitas vezes são difíceis de prever ou entender. Essa estrutura visa proporcionar clareza no processo decisório da IA, reduzindo o risco de discriminação ou uso inadequado dos dados e assegurando a integridade dos sistemas que operam em um contexto empresarial.

Schneider *et al.* (2022), alinhando-se com os conceitos de governança apresentados por Abraham, Schneider e vom Brocke (2019), propõem seis componentes essenciais para a governança eficaz da IA. O primeiro componente é a promoção da colaboração entre diferentes funções da organização, garantindo que o uso da IA seja integrado a diversas áreas e não isolado em um único setor. Em seguida, os autores destacam a importância de estruturar e formalizar a gestão da IA por meio de um *framework* robusto, que define padrões claros para sua aplicação.

O terceiro ponto é focar na IA como um ativo estratégico, o que envolve tratá-la como uma ferramenta fundamental para o sucesso organizacional, indo além de seu valor meramente tecnológico. Além disso, é fundamental definir claramente como e quem tomará as decisões relacionadas à IA, para que as responsabilidades estejam distribuídas de maneira adequada dentro da empresa.

Outro aspecto crucial é o desenvolvimento de artefatos de apoio, como políticas, padrões e procedimentos, que assegurem a conformidade e a uniformidade na aplicação da IA. Finalmente, o monitoramento da conformidade é essencial para garantir que todas as operações envolvendo IA sigam as regulamentações e normas estabelecidas, proporcionando um ambiente controlado e seguro.

Complementando essas ideias, Braga *et al.* (2024) sugerem uma abordagem multisectorial para a governança de IA, inspirada no modelo de governança da internet. Eles argumentam que a colaboração entre governos, empresas, academia e sociedade civil é crucial para o desenvolvimento de uma IA responsável. A proposta se baseia na criação de um comitê multidisciplinar que atue em conjunto para estabelecer padrões e diretrizes que considerem aspectos éticos, sociais e técnicos. Essa abordagem adaptativa, que evolui com o progresso da tecnologia, é vista como fundamental para garantir que a governança de IA acompanhe as rápidas mudanças tecnológicas e normativas que a IA impõe.

Nesse sentido, Taeihagh (2021) aborda a governança da IA em um contexto mais amplo, examinando os desafios globais associados ao uso da IA em áreas críticas como saúde, transporte e segurança. Ele argumenta que as estruturas de governança atuais são insuficientes para lidar com os riscos da IA, propondo um modelo híbrido de governança que envolva tanto atores públicos quanto privados. Para ele, a inclusão do público no processo de tomada de decisão é vital para garantir que as tecnologias de IA sejam desenvolvidas e implementadas em

conformidade com os valores éticos e as expectativas da sociedade, o que reforça a necessidade de participação ativa da sociedade na formulação das políticas de IA.

No ambiente organizacional, Mäntymäki *et al.* (2022) destacam que a governança de IA compreende um conjunto de regras, práticas, processos e ferramentas tecnológicas que visam garantir que o uso da IA esteja alinhado com as estratégias organizacionais, os requisitos legais e os princípios éticos seguidos pela instituição. Esses autores sugerem que a implementação da governança de IA requer uma abordagem que integre diferentes áreas de governança já estabelecidas, como a governança de tecnologia da informação (TI) e a governança de dados. A interação dessas áreas é essencial para formar um sistema de governança coeso, assegurando que tanto a infraestrutura tecnológica quanto os dados utilizados estejam sob controle, de modo a garantir um uso responsável e transparente da IA.

Para comodir os riscos ligados à IA, os autores propõem a adoção de soluções tecnológicas como algoritmos explicáveis (XAI) e ferramentas de detecção de tendências, que permitem maior clareza e justiça no processo de tomada de decisão dos sistemas de IA. Além disso, sugerem a criação de conselhos de revisão ética, responsáveis por avaliar o impacto das decisões automatizadas e assegurar que estejam em conformidade com os valores organizacionais e normas éticas. A realização de auditorias contínuas também é considerada uma prática essencial para assegurar que os sistemas de IA operem dentro dos limites estabelecidos pela governança organizacional.

Assim, a governança da IA deve ser multidimensional, integrando aspectos legais, éticos e técnicos. A participação de múltiplos atores, a adaptação contínua das regulamentações e o equilíbrio entre inovação e responsabilidade são essenciais para garantir que a IA seja usada de maneira benéfica e segura para a sociedade. O desenvolvimento de frameworks de governança de IA, como sugere Mäntymäki *et al.* (2022), facilita a aplicação prática dos princípios éticos e regulatórios, permitindo que as organizações ajustem suas operações de IA de acordo com diretrizes claramente estabelecidas. Desse modo, a governança de IA emerge como um campo essencial para promover a utilização segura e eficiente da IA, ao mesmo tempo em que se busca minimizar os riscos inerentes ao seu uso em larga escala.

Quadro 2 – Aspectos comparativos entre Governança Corporativa e Governança de IA

Aspectos	Governança Corporativa	Governança de IA
Origem / Contexto	Consolida-se nos anos 1990, ligada a boas práticas de administração e transparéncia nas empresas.	Surge no século XXI, com a expansão da IA e a necessidade de regular seu impacto ético, social e tecnológico.
Definição	Conjunto de práticas, processos e estruturas para equilibrar interesses dos stakeholders e garantir transparéncia e sustentabilidade (PACHECO <i>et al.</i> , 2023).	Estrutura de regras, processos e ferramentas que asseguram uso responsável, transparente e alinhado a princípios éticos e regulatórios (SCHNEIDER <i>et al.</i> , 2022).
Objetivos centrais	Transparéncia nas decisões empresariais; equilíbrio entre stakeholders; criação de valor de longo prazo.	Mitigar riscos (viés, privacidade, discriminação); assegurar conformidade legal; promover uso ético e seguro da IA.
Desafios	Conflito de interesses; pressões de mercado; manutenção da confiança social.	Opacidade dos algoritmos; responsabilidade por decisões autônomas; impactos sociais (desemprego, discriminação).
Ferramentas / Mecanismos	Conselhos de administração; auditorias financeiras e de compliance; políticas de integridade e ESG.	<i>Frameworks</i> de governança de IA; algoritmos explicáveis (XAI); conselhos de revisão ética; auditorias contínuas de sistemas.
Abordagem ética	Ênfase em responsabilidade social corporativa e sustentabilidade empresarial.	Ênfase em transparéncia algorítmica, aplicabilidade e justiça no uso da IA.
Participação social	Foco em acionistas, investidores e stakeholders internos.	Envolve múltiplos atores: governos, empresas, academia e sociedade civil (BRAGA <i>et al.</i> , 2024; TAEIHAGH, 2021).

Fonte: Elaborado pela autora.

O quadro comparativo evidencia que, embora a governança corporativa e a governança de IA compartilhem princípios comuns — como transparéncia,

responsabilidade e criação de valor sustentável —, diferem substancialmente quanto à natureza dos desafios que enfrentam. Enquanto a governança corporativa surgiu em resposta às necessidades de controle e equilíbrio entre stakeholders no ambiente empresarial tradicional, a governança de IA emerge como resposta aos riscos éticos, sociais e tecnológicos decorrentes da autonomia dos sistemas inteligentes. Assim, a governança de IA amplia o escopo da governança corporativa ao incorporar novas dimensões, como aplicabilidade algorítmica, proteção de dados e mitigação de vieses. Essa evolução demonstra que a governança organizacional contemporânea precisa se adaptar às transformações digitais, consolidando práticas que unam eficiência tecnológica, ética e responsabilidade social.

2.4.1 Governança de TI (Tecnologia da Informação) como modelo de referência

Para compreender as práticas de governança de IA e os desafios da *Shadow AI*, é fundamental examinar a governança de TI (Tecnologia da Informação). Este campo, estabelecido há mais tempo, fornece um modelo de referência crucial para a gestão de riscos e a otimização de recursos tecnológicos, servindo como um precedente para a forma como a IA deve ser gerenciada nas organizações.

Como preditora, pode-se considerar a governança de TI um conjunto de processos, práticas e estruturas que visam alinhar a Tecnologia da Informação (TI) com os objetivos estratégicos da organização, garantindo o uso eficiente dos recursos tecnológicos para gerar valor para o negócio, gerenciar riscos e promover a automação dos processos corporativos (BARBOSA *et al.*, 2011). Este conceito é amplamente discutido no âmbito empresarial, especialmente em um contexto em que a informação e a tecnologia são vistas como os recursos mais valiosos das organizações. Pois fornecem suporte à tomada de decisão em ambientes de negócios cada vez mais dinâmicos e competitivos.

A governança de TI é, portanto, responsabilidade da alta direção e dos executivos da organização, que devem assegurar que as operações de TI sejam eficazes e alinhadas com os objetivos empresariais (BARBOSA *et al.*, 2011). Para isso, *frameworks* como COBIT (*Control Objectives for Information and Related Technology*) e ITIL (*Information Technology Infrastructure Library*) são amplamente utilizados. O COBIT, por exemplo, fornece um modelo de controle para gerenciar riscos, aumentar a segurança da informação e melhorar o desempenho, enquanto o

ITIL se concentra na entrega de serviços de TI de alta qualidade e na melhoria contínua (BARBOSA *et al.*, 2011).

No artigo “*Análise dos Mecanismos de Governança de TI mais difundidos entre as empresas brasileiras*”, Lunardi *et al.* (2014) discutem a importância e a implementação da governança de Tecnologia da Informação (TI) nas organizações brasileiras. A governança de TI é considerada uma forma de garantir que os investimentos em TI agreguem valor aos negócios e otimizem recursos. E nele os autores Lunardi *et al.* (2014) apresentam benefícios da adoção desses mecanismos que foram agrupados em sete categorias principais: processos de TI, área de TI, segurança da TI, projetos de TI, serviços de TI, infraestrutura de TI e integração da área de TI com outras áreas. Esses mecanismos favorecem desde a melhoria na qualidade dos processos e segurança da informação até a centralização de procedimentos e melhor gestão da infraestrutura. A adoção de comitês de TI e o envolvimento da área de TI na formulação de estratégias corporativas contribuem para um alinhamento estratégico e a criação de valor.

Em contraponto, os desafios da governança de TI moderna estão relacionados à proliferação da *Shadow IT* (SIT), ou TI “nas sombras”, que se refere ao uso de soluções tecnológicas não aprovadas ou desconhecidas pelo departamento de TI da organização. Esse fenômeno, que cresce à medida que os funcionários buscam por soluções mais ágeis e adaptadas às suas necessidades, apresenta tanto riscos quanto oportunidades para as empresas (MACHADO, 2023). Segundo Machado (2023), a *Shadow IT* pode contribuir para a inovação e satisfação dos usuários, mas também cria riscos significativos de segurança, compliance e eficiência operacional.

O ciclo de vida da *Shadow IT* dentro das organizações segue uma trajetória que inclui fases de adoção, uso e descontinuidade. A adoção geralmente é impulsionada por fatores como a experiência do usuário e a utilidade percebida, enquanto a descontinuidade está relacionada a riscos percebidos e à intervenção da governança de TI (MACHADO, 2023). Além disso, as organizações podem escolher entre integrar essas soluções à sua infraestrutura oficial de TI ou descontinuá-las por completo, dependendo do impacto na segurança e na performance geral (MACHADO, 2023).

De acordo com Luciano, Costa Netto e Wiedenhöft (2015), a governança de TI também abrange o gerenciamento de artefatos de TI, que inclui tanto os sistemas físicos, como hardware e software, quanto os dados gerados por esses sistemas. A

adoção de *frameworks* de governança como COBIT ajuda a garantir que esses artefatos estejam devidamente alinhados aos objetivos do negócio, além de maximizar o valor que a TI pode gerar para a organização (LUCIANO; COSTA NETTO; WIEDENHÖFT, 2015).

Portanto, a governança de TI é fundamental para garantir que as soluções tecnológicas sejam utilizadas de maneira eficaz, gerando valor para o negócio e minimizando as consequências. Compreender como e quais são os principais conceitos da governança de TI faz com que se amplie a temática relacionada à governança de IA e o contextos da *Shadow IT* e *AI*. Contextos dos quais apresentam novos desafios para a governança, exigindo uma abordagem flexível que permita às organizações aproveitar os benefícios da inovação sem comprometer a segurança ou a conformidade.

2.4.2 Governança, Ética e a IA

A governança e a ética no contexto da Inteligência Artificial (IA) tem se tornado um tema central, dado o aumento do uso de sistemas automatizados em diversas áreas da sociedade conforme apresentado anteriormente. Os termos “governança” e “ética” referem-se ao conjunto de normas, princípios e regulamentações que visam garantir que o desenvolvimento e a aplicação da IA sejam realizados de forma responsável, transparente e benéfica, sem comprometer os direitos fundamentais ou a segurança das pessoas, conforme destacado por Carini e Morais (2020). Eles enfatizam também, que a confiança pública na IA depende diretamente da existência de regulação eficiente, que deve acompanhar o ritmo acelerado de inovações no campo tecnológico.

A IA, conforme definida por Hildebrandt (2008), é uma tecnologia capaz de identificar padrões e fazer previsões a partir de dados. Essa capacidade permite que a IA tome decisões que antes eram exclusivamente humanas. No entanto, a governança e a ética, como explica o World Bank (1992), é essencial para que esse poder seja exercido de forma justa e segura. A governança com o contexto da ética é fundamental para garantir que os sistemas de IA sejam desenvolvidos e utilizados com base em princípios que assegurem a transparência, a imparcialidade e o controle de riscos.

O rápido avanço da IA tem trazido inúmeros benefícios para a sociedade, mas também levanta preocupações quanto ao seu uso indiscriminado e sem supervisão adequada. Como exemplificado por Bonnefon, Rahwan e Shariff (2016), a tomada de decisões por carros autônomos pode gerar dilemas morais, como priorizar a segurança do passageiro ou de terceiros em situações de risco. Esse tipo de questão destaca a necessidade de uma governança com ética mais robusta e que estabeleça diretrizes claras para a programação de algoritmos, evitando o uso irresponsável da tecnologia.

No caso “*State v. Loomis*”, mencionado por Israni (2017), o uso de um sistema de IA para auxiliar na sentença de um réu gerou debates sobre a transparência e a responsabilidade das decisões automatizadas, já que o algoritmo utilizado não era conhecido pelos próprios juízes que aplicavam a decisão. Esse exemplo revela os riscos de se utilizar IA sem regulamentação apropriada, o que reforça a necessidade de diretrizes que promovam a confiança e a justiça na aplicação dessas tecnologias.

Iniciativas regulatórias já estão surgindo para enfrentar esses desafios. Um exemplo é a ISO (International Organization for Standardization) 13482, que estabelece requisitos de segurança para robôs de cuidados pessoais, além da Lei de Responsabilidade Algorítmica de Nova York, que busca garantir a transparência em decisões automatizadas utilizadas por agências governamentais (THE NEW YORK CITY COUNCIL, 2018). Essas iniciativas demonstram que a governança deve integrar tanto padrões técnicos quanto princípios éticos que garantam o uso responsável da tecnologia. A relação entre governança, ética e IA é central para garantir que os avanços tecnológicos respeitem valores sociais e direitos fundamentais. Ou seja, a construção de uma governança em IA mais robusta, baseada em princípios como transparência, segurança e responsabilidade, se tornam cruciais para assegurar que a IA continue beneficiando a sociedade sem comprometer valores éticos e legais.

Portanto, a construção de uma governança de IA robusta e eficaz emerge como um imperativo, exigindo uma abordagem multidimensional que vai além das diretrizes tradicionais. Um *framework* para a gestão da IA Generativa nas empresas deve ser fundamentado em quatro pilares interconectados: conformidade, ética, transparência e segurança da informação. A conformidade garante que o uso da tecnologia esteja alinhado com as regulamentações vigentes e evite riscos legais, enquanto a ética assegura que os sistemas de IA sejam desenvolvidos e aplicados

de forma justa, mitigando vieses e respeitando valores sociais. A transparéncia é crucial para construir a confiança pública, tornando as decisões dos algoritmos comprehensíveis e responsáveis, como evidenciado no caso *State v. Loomis*. Por fim, a segurança da informação estabelece as defesas necessárias contra os riscos inerentes à *Shadow AI*, protegendo a integridade dos dados e dos sistemas. A interligação desses pilares não apenas minimiza os riscos, mas também capacita as organizações a utilizar a IA como uma ferramenta estratégica e sustentável, promovendo o benefício para a sociedade sem comprometer os valores fundamentais.

3 METODOLOGIA

Esta pesquisa adota uma abordagem qualitativa de caráter exploratório, fundamentada no framework de Creswell (2013), que orienta a investigação para a compreensão dos significados que indivíduos ou grupos atribuem a um problema social ou humano. A escolha metodológica justifica-se pela necessidade de capturar as complexidades e nuances contextuais da governança de IA e do fenômeno da Shadow AI, priorizando a perspectiva dos participantes em seu ambiente natural. Para a coleta de dados, optou-se pela estratégia de entrevistas estruturadas, aplicadas a uma amostragem intencional que abrange três segmentos distintos com vivência prática em ferramentas de IA Generativa.

Essa diversidade na seleção dos participantes visa assegurar a credibilidade e a fidedignidade dos achados, permitindo que o pesquisador realize uma interpretação holística a partir de múltiplos pontos de vista, conforme preconizado para a precisão da pesquisa qualitativa de acordo com Creswell (2013). O processo de análise segue uma lógica indutiva, partindo dos dados particulares das entrevistas para a construção de temas e interpretações amplas sobre a relação entre governança corporativa e o uso de tecnologias emergentes como a IA generativa.

Inicialmente, realizou-se o levantamento dos elementos de governança corporativa na literatura de Pacheco et al. (2023) e Kalkan (2024). A partir dessa base teórica, foram estabelecidas as categorias *a priori* que nortearam a investigação: práticas de conformidade, ética, transparência e segurança da informação (conforme detalhado no Quadro 3).

Quadro 3 – Elementos de Governança

Tema	Dimensões
Conformidade	Políticas de uso, regulação, auditoria de TI.
Ética	Princípios éticos, vieses algorítmicos, transparência.
Transparência	Divulgação de práticas, <i>accountability</i> , relatórios de desempenho.
Segurança da Informação	Proteção de dados, prevenção de <i>Shadow AI</i> , resposta a incidentes.

Fonte: Elaborado pela autora.

Na segunda fase, com as categorias definidas, procedeu-se à construção do roteiro de entrevista estruturada. As perguntas foram formuladas com o objetivo de operacionalizar cada categoria, garantindo que o diálogo com os participantes cobrisse todos os pilares de governança selecionados. Os dados foram coletados por meio de entrevistas direcionadas a lideranças organizacionais de nível estratégico, incluindo cargos de CEO, Diretor e Coordenador. A seleção das organizações teve como objetivo contemplar diferentes setores — instituição financeira, empresa de base tecnológica e instituição pública — de modo a ampliar a diversidade da análise e permitir a comparação entre realidades distintas.

A instituição financeira participante é uma cooperativa de crédito com cerca de 4.300 colaboradores distribuídos em todo o Brasil e 30 anos de atuação no mercado, tendo como representante entrevistado o Diretor de Operações. A empresa de base tecnológica, por sua vez, é uma organização de pequeno porte, composta por aproximadamente 22 colaboradores, que atua no modelo SaaS (*Software as a Service*) há 12 anos, e teve como respondente o CEO da companhia. Já a instituição pública pertence ao setor de administração e gestão, com uma média total de 4.000 servidores, e teve como participante o Coordenador de Tecnologia da Informação da Prefeitura de Santa Cruz do Sul, que também exerce o cargo de programador no Departamento de TI.

Quanto ao formato de aplicação, a entrevista com o representante da instituição pública foi realizada presencialmente, com duração aproximada de 45 minutos, enquanto nas outras duas organizações (técnologica e financeira) a coleta ocorreu por meio de formulário estruturado, elaborado a partir do mesmo roteiro de perguntas. Para assegurar equivalência metodológica, após o preenchimento dos formulários foi feita uma conversa complementar com os respondentes, garantindo que a profundidade das respostas fosse compatível à de uma entrevista presencial.

Em todos os casos, assegurou-se o anonimato dos participantes e a confidencialidade das informações prestadas. O roteiro das entrevistas foi estruturado a partir do Quadro 4, estruturado a partir de cinco seções principais (Uso e Percepção da IA Gen; Riscos Associados e *Shadow AI*; Práticas de Governança; Desafios e Oportunidades; Sugestões e Diretrizes Finais). Ao todo, o instrumento contemplou 21 perguntas, elaboradas a partir do referencial teórico e alinhadas aos objetivos da pesquisa.

Quadro 4 – Instrumento de Pesquisa (Entrevista)

Seção	Perguntas
Introdução	Contexto: "Investiga-se como a governança corporativa pode mitigar os riscos associados ao uso de IA Gen no ambiente empresarial. Sua participação nos ajudará a compreender melhor as práticas e desafios enfrentados na sua organização."
Seção 1: Uso e Percepção de IA Gen	<p>1. Sua empresa já utiliza ferramentas de Inteligência Artificial Generativa? Se sim, quais são as principais aplicações? Para que utiliza?</p> <p>2. Qual é o nível de familiaridade dos gestores com as tecnologias de IA Gen? E dos colaboradores?</p> <p>3. Quais são os principais benefícios percebidos/previstos com o uso de IA Gen em sua empresa?</p> <p>4. Quem decide na sua empresa quais ferramentas de IA Gen utilizar ou implementar?</p> <p>5. Quais resultados espera alcançar com o uso de ferramentas de IA Gen?</p>
Seção 2: Riscos Associados e Shadow AI	<p>6. Quais desafios sua empresa espera encontrar na utilização de IA Gen? (como privacidade, viés algorítmico ou segurança de dados)</p> <p>7. Existem iniciativas para treinamento da equipe para o melhor uso de ferramentas de IA Generativa em sua empresa? Já houve casos de uso de IA Gen não supervisionado em sua organização? Se sim, como isso foi identificado e gerido?</p> <p>8. Quais fatores levam os colaboradores a adotarem soluções de IA Gen sem a aprovação do departamento de TI?</p> <p>9. Quando identificado o uso indevido, o que é feito?</p>
Seção 3: Práticas de Governança e Mitigação de Riscos	<p>10. Existe atualmente na sua empresa práticas implementadas para regular o uso de IA Gen?</p> <p>11. De que maneira a empresa promove a transparência no uso de IA Gen? E a ética?</p> <p>12. Quais medidas de segurança são adotadas para evitar o uso não autorizado de IA? E as conformidades?</p>

Seção 4: Desafios e Oportunidades	13. Quais são os principais desafios enfrentados ou que sua empresa pretende encontrar na integração de ferramentas de IA Gen? 14. Como sua empresa equilibra a inovação com a necessidade de manter práticas éticas e conformes às regulamentações? 15. Quais estratégias você acredita que seriam eficazes para melhorar a governança da IA Gen no ambiente corporativo?
Seção 5: Sugestões e Diretrizes Finais	16. Com base em sua experiência, que diretrizes ou práticas adicionais você recomendaria para gerenciar de forma eficaz o uso de IA Gen? 17. Como você vê a evolução do uso de ferramentas de IA Gen no futuro?
Demográficos	18. Quantos funcionários tem sua empresa? E/ou quantas pessoas seu setor contempla? 19. Qual o segmento da sua empresa? 20. Qual seu cargo? 21. A empresa atua no mercado a quantos anos?
Observações Finais	Tempo Estimado: Informa-se o tempo médio de duração da entrevista (30-45 minutos). Confidencialidade: As respostas são tratadas de forma confidencial e anônima.

Fonte: Elaborado pela autora.

Por fim, a terceira fase consistiu no processamento e análise das respostas, estruturada em um modelo de análise transversal. Após a transcrição e organização dos relatos, os dados foram submetidos a um confronto direto, no qual cada categoria (conformidade, ética, transparência e segurança) foi analisada de forma comparativa entre todos os participantes. Esse procedimento permitiu identificar convergências, onde as percepções sobre a governança de IA Gen eram unâimes, e divergências, que revelaram como diferentes setores ou perfis profissionais enfrentam desafios distintos. A partir desse cruzamento de dados, foi possível não apenas validar as categorias teóricas iniciais, mas também interpretar as nuances práticas da Shadow AI e as particularidades da maturidade digital de cada organização, conforme consolidado na discussão dos resultados.

Em suma, a trajetória metodológica partiu da sistematização teórica para a investigação empírica, utilizando as categorias de governança como eixo integrador. A aplicação das entrevistas estruturadas, seguida pela análise transversal dos relatos, permitiu identificar convergências e divergências significativas entre as percepções dos participantes. Esse processo de convergência entre a literatura de base, o roteiro de coleta e a análise comparativa das respostas garantiu o rigor necessário para compreender não apenas a aplicação formal das práticas de governança, mas também os fenômenos emergentes e os desafios práticos da IA Gen nas organizações. Com a estrutura metodológica consolidada, o tópico seguinte apresenta a análise detalhada dos resultados obtidos.

4 ANÁLISE DO USO DE IA GENERATIVA: PRÁTICAS, PERCEPÇÕES E DESAFIOS À LUZ DA GOVERNANÇA CORPORATIVA

A Inteligência Artificial Generativa (IA Gen) consolidou-se como um dos marcos mais significativos das transformações digitais recentes, prometendo ganhos em produtividade, inovação e eficiência. No entanto, sua adoção não ocorre de maneira homogênea, variando de acordo com o contexto institucional, regulatório e cultural. A literatura ressalta que tais diferenças impactam diretamente não apenas o modo de uso, mas também as estruturas de governança e de mitigação de riscos (HILB, 2020; MAHER, 2024; CAMPOS, 2024). Este estudo analisa entrevistas realizadas com três instituições: uma do setor público (Público), uma empresa de base tecnológica (Tecno) e uma cooperativa financeira (Finanças). Para preservar a confidencialidade dos participantes e das organizações, adotou-se a codificação mencionada, e os entrevistados são identificados apenas por seus cargos.

No caso da PÚBLICO, o entrevistado ocupava o cargo de Coordenador de Tecnologia da Informação, em um órgão da administração pública municipal. Embora demonstrasse conhecimento sólido sobre o potencial das ferramentas de IA Generativa, sua percepção foi marcada pelas limitações institucionais de aplicabilidade, especialmente relacionadas a restrições orçamentárias, regulatórias e burocráticas típicas da esfera pública, como destacou o Coordenador de TI: “*O uso é muito limitado, porque a gente tem uma série de entraves burocráticos, falta orçamento, e não tem uma política definida para isso*”. Conforme destaca Taeihagh (2021), as estruturas de governança atuais são, muitas vezes, insuficientes para lidar com os riscos da IA em setores públicos, exigindo modelos híbridos que integrem múltiplos atores e sejam sensíveis às restrições institucionais. Importante destacar que a restrição identificada não estava associada ao desconhecimento técnico do entrevistado, mas sim à baixa capacidade de implementação prática por parte da instituição.

Na Tecno, o estudo foi respondido pelo CEO da empresa, líder de uma empresa jovem, mas em crescimento acelerado, com atuação há mais de dez anos no mercado de SaaS. O entrevistado demonstrou elevado nível de familiaridade com a IA Generativa, articulando tanto seus usos internos para otimização de processos e inovação em produtos quanto às preocupações estratégicas relacionadas à governança, transparência e mitigação de riscos como a *Shadow AI*. Essa atuação

remete à perspectiva de governança experimental discutida por Hilb (2020), em que a liderança atua como agente-chave na mediação entre inovação e controle. Além disso, M. Silic, D. Silic e Oblakovic (2016) já alertavam que soluções adotadas sem formalização criam um ambiente propício à *Shadow AI*, mesmo quando bem-intencionadas. Sua posição como dirigente máximo da organização possibilitou trazer uma visão ampla, que conciliava tanto a dimensão operacional quanto a estratégica do uso da tecnologia.

Por fim, na Finanças, o entrevistado foi o Diretor de Operações, pertencente a uma cooperativa consolidada, com mais de vinte anos de presença no mercado financeiro regional. O respondente revelou conhecimento aprofundado sobre a tecnologia e suas aplicações, reconhecendo o potencial da IA Generativa em atividades administrativas e analíticas, mas destacando sobretudo a necessidade de enquadramento em rígidos mecanismos de compliance e conformidade, que caracterizam o setor financeiro. A experiência relatada evidenciou cautela na adoção, priorizando a segurança da informação e a minimização de riscos éticos e regulatórios. Schneider *et al.* (2022) destacam que estruturas robustas de governança exigem integração entre governança de dados, modelos e sistemas, sendo a conformidade regulatória um dos pilares centrais para ambientes financeiros.

Em conjunto, os três entrevistados demonstraram compreender com clareza o funcionamento, os potenciais e os riscos associados à IA Generativa, ainda que sob perspectivas distintas, moldadas por seus respectivos contextos institucionais. Enquanto na Público a principal barreira encontrada foi institucional, na Tecno prevaleceu uma visão de exploração estratégica e, na Finanças, um posicionamento prudente, marcado pela exigência regulatória. Essa diversidade de percepções fornece a base para uma análise comparativa robusta, permitindo identificar pontos de convergência e divergência nas práticas de governança aplicadas à IA Generativa.

Como resumiu o coordenador da Público: “*Não tem regra nenhuma, cada um usa o que acha melhor*”, revelando um cenário marcado por ausência de diretrizes formais e uso descentralizado. No contexto do setor público, a fala do entrevistado (“*Não tem regra nenhuma, cada um usa o que acha melhor*”) evidencia um ambiente em que o uso de IA generativa ocorre de forma difusa e pouco observável para a gestão, o que dificulta tanto a mitigação de riscos quanto a captura institucional de

benefícios. Um caminho relevante para lidar com essa tensão, sem depender de uma adoção imediata e formal de ferramentas, é a estruturação de rotinas de validação em modo paralelo, com registros sistemáticos, antes da institucionalização definitiva. Sidorkin (2025) propõe um protocolo de teste em “modo sombra” voltado a organizações públicas, no qual humanos e sistemas de IA operam simultaneamente, permitindo comparar resultados com base em evidências, registrar divergências e consolidar aprendizado organizacional. A adoção de um procedimento dessa natureza pode ser especialmente útil em ambientes com restrições orçamentárias e burocráticas, pois permite experimentar e avaliar a tecnologia com menor risco operacional e maior controle, contribuindo para reduzir o uso informal e aumentar a capacidade de governança (SIDORKIN, 2025).

Em contraste, o CEO da Tecno afirmou: “*Liberdade é o que impulsiona nosso crescimento*”, indicando uma cultura organizacional orientada à experimentação, com autonomia para os colaboradores testarem soluções baseadas em IA. Já na Finanças, o Diretor de Operações reforçou uma visão mais cautelosa e regulada ao declarar: “*Sem diretriz clara, IA pode ser um risco maior do que uma solução*”. Essas falas evidenciam como cada organização lida com a governança da IA Generativa conforme seu contexto: descontrole no setor público, agilidade com risco no setor tecnológico e rigor regulatório no setor financeiro.

As entrevistas evidenciam estágios distintos de adoção. No caso de Público, observa-se um uso pulverizado e informal de ferramentas abertas como ChatGPT, sem respaldo da área de TI, sem diretrizes e sem treinamentos, o que caracteriza um cenário típico de *Shadow AI* e um estágio embrionário de maturidade digital. Como mencionado pelo próprio servidor em entrevista: “*Sabe que os funcionários usam, ele mesmo usa o Chat GPT por exemplo para auxiliar nas atividades e tarefas*”. E, ainda, segundo ele: “*É tudo meio escondido, porque a gente não tem nenhuma diretriz. Cada servidor vai usando por conta própria*”. A afirmação de que o uso é “meio escondido” indica que o fenômeno observado não se restringe à ausência de política, mas envolve também um componente comportamental: a tendência de manter práticas de uso de IA generativa fora da visibilidade institucional, mesmo quando elas produzem ganhos individuais de produtividade. Waters-Lynch et al. (2025) analisam esse padrão como uma forma de inovação iniciada por usuários em caráter não declarado, favorecida pela facilidade de acesso e pelo baixo custo de adoção de ferramentas de IA generativa, o que reduz barreiras

técnicas e amplia a autonomia do colaborador. Nesse enquadramento, a invisibilidade do uso não é apenas um “efeito colateral” da falta de diretrizes, mas um obstáculo para o aprendizado organizacional, pois impede que melhorias sejam avaliadas, validadas e escaladas de modo seguro (WATERS-LYNCH et al., 2025).

Além disso, esse tipo de uso é característico do fenômeno conhecido como *Bring-Your-Own-AI* (BYOAI), discutido por Blin (2024), no qual colaboradores recorrem a ferramentas pessoais de IA no trabalho, sem supervisão formal, ampliando os riscos à segurança e à governança corporativa. E corrobora diretamente com o conceito de *Shadow AI* (SILIC, M.; SILIC, D.; OBLANKOVIC, 2016), e os benefícios são percebidos como potenciais e individuais (agilidade e produtividade), enquanto os riscos de vazamento de dados e de falhas de segurança se tornam críticos.

Os riscos mencionados nas entrevistas são coerentes com a literatura recente que trata *Shadow AI* como fonte de vulnerabilidades ampliadas em organizações. Puthal et al. (2025) destacam que o uso de sistemas de IA sem supervisão formal pode elevar o risco de incidentes relacionados à segurança e à conformidade, especialmente quando envolve processamento de dados sensíveis, integrações com serviços externos e ausência de mecanismos de auditoria. Os autores também apontam que a falta de monitoramento facilita vulnerabilidades mais complexas, como a corrupção de modelos por insumos manipulados, comprometendo a confiabilidade das saídas e, consequentemente, a qualidade das decisões apoiadas por IA (PUTHAL et al., 2025). Assim, em contextos como o caso Público — no qual a prática é informal e dispersa — e o caso Tecno — onde a experimentação é intensa e a governança tende a ser reativa — a ausência de critérios mínimos de classificação de dados, registro de uso e controle de ferramentas aumenta a exposição organizacional de forma estrutural (PUTHAL et al., 2025).

Em Tecno, o uso é disseminado e estratégico: ferramentas como ChatGPT, Claude e *Application Programming Interfaces* (APIs) da OpenAI são incorporadas a fluxos internos, com alta familiaridade da liderança e familiaridade intermediária entre colaboradores. Os ganhos relatados são concretos (“economia de tempo”, “aumento de produtividade”, “redução de erros”), e a liderança exerce papel central na experimentação, em linha com a noção de governança experimental (HILB, 2020). A empresa se apoia na confiança e no “*bom senso*” dos colaboradores. O CEO relatou: “A gente não tem uma governança forte, logo, o time tem bastante

liberdade de testar” e “*a gente prefere errar testando rápido do que ficar travado esperando um processo que nunca vem. Mas isso tem custo*”. Tal postura alinha-se à noção de “inovações sombrias” descritas por M. Silic, D. Silic e Oblakovic (2016), em que a ausência de governança formal permite avanços rápidos, porém à custa de maior exposição a riscos operacionais e éticos. Ainda assim, os riscos tendem a ser tratados de forma reativa, como o caso de um vazamento de dados que levou a empresa a parar de usar a ferramenta Deepseek por exemplo.

Em Finanças, a adoção é moderada e cautelosa, direcionada a memorandos e relatórios, com supervisão por uma área central de IA. A familiaridade é média entre gestores e baixa/média entre colaboradores; a segurança da informação e o compliance regulatório conduzem a postura institucional. O Diretor de Operações confirmou a postura proativa da instituição “*existe um normativo e um guia de uso de IA no ambiente corporativo*” e afirmou também “*se a IA não seguir os protocolos de compliance, a gente nem considera. Aqui é segurança primeiro*”. Os benefícios são reconhecidos, ainda que restritos pelo estágio inicial de adoção, e a abordagem de treinamento e conscientização reforça a importância de capacitação, como defendido por Schneider *et al.* (2022).

No que se refere à governança, a comparação mostra um gradiente nítido. Em Público, inexistem políticas ou diretrizes formais; em Tecno, a governança ocorre de modo experimental e centralizado na liderança, com supervisão mínima; em Finanças, há aderência a práticas de compliance e condução por áreas técnicas, com processos de regulamentação em fase inicial. Em todos os casos, há lacuna de capacitação formal e contínua, como afirmam Mäntymäki *et al.* (2022), a formação contínua é parte essencial de uma governança eficaz em IA, pois garante o alinhamento entre os princípios éticos, as regulamentações vigentes e a prática cotidiana dos colaboradores.

Essa carência foi confirmada pelos próprios entrevistados: o representante da Público afirmou: “*Nunca tivemos treinamento específico para isso: quem sabe usar, aprendeu por conta própria*”, enquanto o CEO da Tecno pontuou: “*A gente orienta o básico, mas não tem uma trilha de capacitação estruturada*”. Já na Finanças, o Diretor de Operações relatou: “*Estamos começando um plano de capacitação, mas ainda é muito no início*”. A ausência de capacitação formal limita, portanto, a padronização técnica e o alinhamento ético, ao mesmo tempo em que a dependência de ferramentas abertas — sem a adoção de soluções corporativas

seguras — amplia vulnerabilidades e dificulta a conformidade. Como resumiu o Diretor da Finanças: “*A gente ainda depende de ferramentas abertas, mas isso é algo que nos preocupa. Já estamos olhando pra soluções mais seguras e controladas*”.

À luz do segundo objetivo deste trabalho — analisar o papel da governança corporativa na mitigação dos riscos do uso indevido de *Shadow AI* — a eficácia das medidas relatadas pelos participantes foi avaliada a partir de quatro dimensões centrais: conformidade, ética, transparência e segurança da informação. Em Público, a ausência de políticas de uso, regulação e auditoria de TI, somada à inexistência de princípios éticos formalizados, de mecanismos de transparência e de controles de segurança (classificação de dados, prevenção de *Shadow AI* e resposta a incidentes), reduz a eficácia mitigadora praticamente a zero; a governança, inexistente, não oferece barreiras à materialização de riscos. Em Tecno, há diretrizes informais lideradas pela alta gestão e uma cultura pró-inovação que, embora favoreça ganhos de eficiência, opera com salvaguardas limitadas: não há política corporativa específica para IA, a transparência restringe-se ao nível interno e a segurança é predominantemente reativa.

Como resultado, a mitigação se mostra parcial: a liderança impõe freios pontuais e a baixa burocracia acelera correções, mas permanecem riscos residuais de vazamento de dados e de uso indevido. Em Finanças, o conjunto de práticas de compliance, a supervisão técnica e as práticas de proteção de dados elevam a capacidade preventiva: controles de acesso, segregação de ambientes e restrições de uso reduzem a superfície de ataque. Contudo, a ausência de política específica para IA Generativa, a dependência de ferramentas abertas e a carência de treinamentos estruturados mantêm riscos estruturais. Comparativamente, a eficácia mitigadora é mínima em Público, moderada em Tecno e relativamente mais robusta em Finança. Essa variação se alinha aos estágios de maturidade organizacional descritos por Machado *et al.* (2023), em que instituições mais regulamentadas tendem a desenvolver controles preventivos mais sólidos, ainda que nem sempre suficientes frente aos riscos da IA generativa.

A síntese comparativa dessas dimensões encontra-se no Quadro 5, que organiza o que cada organização possui e o que não possui em termos de conformidade, ética, transparência e segurança da informação. A leitura do quadro

evidencia lacunas comuns e distanciamentos estruturais que se refletem diretamente na probabilidade de ocorrência e no impacto dos riscos associados à *Shadow AI*.

A variação observada entre os três casos pode ser interpretada também como expressão de diferentes formas de governança frente ao uso de IA generativa pelos usuários. Waters-Lynch et al. (2025) discutem que organizações podem reagir ao uso não institucionalizado de IA de maneiras distintas: desde abordagens mais restritivas, voltadas a contenção por sanções e controle, até abordagens integrativas, que buscam internalizar o uso por meio de diretrizes, ambientes controlados e incentivos à transparência. À luz dessa discussão, o caso Público se aproxima de uma situação de baixa capacidade de governança (ausência de política e baixa visibilidade do uso), o caso Tecno reflete um modelo fortemente orientado à experimentação com controles predominantemente reativos, e o caso Finanças tende a operar com maior ênfase em conformidade e supervisão, ainda que com lacunas na formalização específica para IA generativa. Esse enquadramento ajuda a evidenciar que o desafio central não é apenas “permitir ou proibir” o uso, mas criar mecanismos institucionais que reduzam o uso oculto e convertam iniciativas dispersas em aprendizagem organizacional com segurança (WATERS-LYNCH et al., 2025).

Quadro 5 – Comparação entre os casos analisados nas dimensões de governança em IA

Dimensão	Público	Tecno	Finanças
Conformidade	Não possui políticas de uso; inexistem regulação interna ou auditoria de TI; ausência de controles formais.	Diretrizes informais e liderança ativa; sem política corporativa específica; auditoria incipiente.	Aderência parcial a compliance setorial; auditorias e controles existem, política específica para IA Gen em fase inicial.
Ética	Sem princípios éticos formalizados para IA; inexistência de abordagem para vieses e aplicabilidade.	Considerações éticas pragmáticas e não sistematizadas; pouca atenção a vieses algorítmicos.	Ética vinculada ao compliance; reconhecimento de riscos, mas sem framework próprio de IA

			para vieses e transparência.
Transparência	Não divulga práticas; ausência de <i>accountability</i> e de relatórios sobre uso de IA.	Transparência restrita ao âmbito interno; inexistência de relatórios formais de desempenho.	Relatórios de conformidade financeira; ainda não divulga métricas específicas de IA ou <i>accountability</i> dedicada.
Segurança da Informação	Sem controles para prevenção de <i>Shadow AI</i> ; inexistência de classificação de dados e de resposta a incidentes.	Controles reativos; mitigação pontual.	Segurança priorizada; controles de acesso e proteção de dados presentes; fazem prevenção em 'Talks' na empresa sobre o assunto.

Fonte: Elaborado pela autora.

O Quadro 5 reforça a existência de fragilidades comuns: a ausência de políticas específicas para IA Generativa, a carência de programas formais de capacitação e a dependência de ferramentas abertas. Ao mesmo tempo, os distanciamentos entre os casos revelam modelos de governança com graus distintos de eficácia na mitigação de riscos. Em Público, a inexistência de conformidade, ética institucionalizada, transparência e controles de segurança amplia a probabilidade de incidentes e a severidade de seus impactos, o que se confirma na fala do coordenador de TI: “*Não tem nenhuma diretriz. Cada setor vai usando como quer, se usar*”. Em Tecno, a governança experimental e centrada na liderança impulsiona resultados e permite respostas rápidas, mas a mitigação permanece parcial sem políticas, auditorias e métricas de desempenho. Como pontuou o CEO da empresa: “*Governança não pode virar um muro. Mas também não pode ser só um enfeite*”, revelando uma consciência da necessidade de equilíbrio entre liberdade e controle. Já em Finanças, o arcabouço regulatório e a priorização da segurança reduzem a exposição, ainda que a plena efetividade exija avanços. O Diretor de Operações destacou: “*O segredo está no equilíbrio: controle sem engessar*”. Assim, embora as

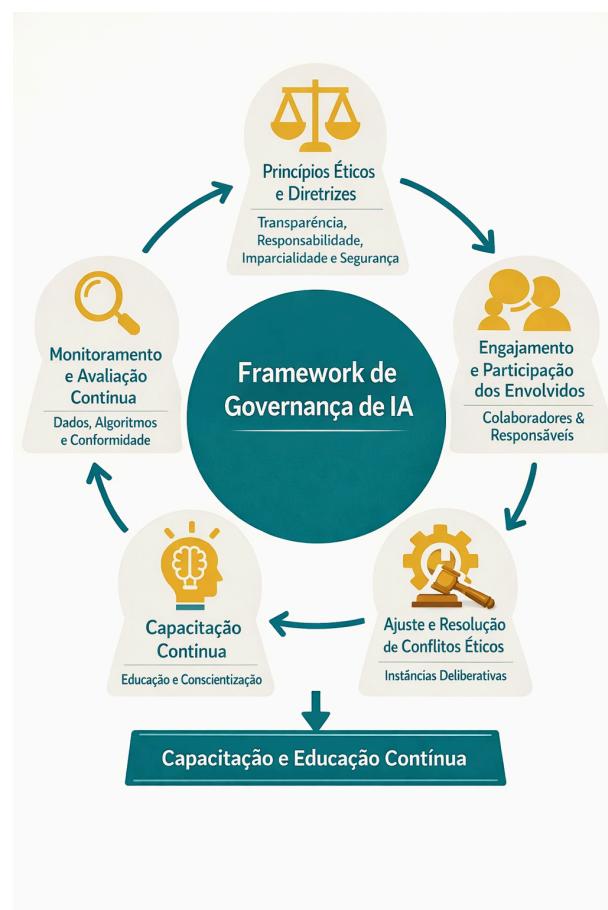
três instituições apresentem níveis distintos de maturidade, todas compartilham desafios críticos na estruturação de uma governança de IA mais robusta e proativa, conforme recomenda a literatura (CHUVAKIN; KAGANOVICH, 2024; CAMPOS, 2024; MAHER, 2024).

Dessa forma, conclui-se que a governança corporativa exerce papel decisivo na mitigação dos riscos de *Shadow AI*: quanto mais formal, preventiva e transparente a governança, menor a superfície de ataque e maior a capacidade de resposta, sem inviabilizar a captura de valor pela inovação. Vale a ressalva de que as empresas mencionadas não são do mesmo setor e nenhuma delas se opõe ao uso dessa tecnologia, entretanto ainda não estão seguras de um processo que poderá dar mais definição ao uso interno e aos impactos que a tecnologia pode gerar. E essa conclusão é corroborada por Pacheco *et al.* (2023), que defendem que a governança eficaz de IA deve combinar conformidade legal, transparência algorítmica, princípios éticos e segurança da informação como pilares interdependentes.

5 PROPOSIÇÃO DE FRAMEWORK DE GOVERNANÇA PARA IA GENERATIVA (GIA)

A partir da análise crítica do uso da IA Generativa em três contextos organizacionais distintos e das diretrizes teóricas identificadas ao longo deste estudo, constrói-se nesta seção, uma proposta de *framework* que busca sistematizar os fundamentos para uma governança e operacionalmente eficaz da Inteligência Artificial Generativa no ambiente corporativo. O *Framework* de Governança para Inteligência Artificial (GIA) é apresentado como um modelo estruturado em cinco dimensões integradas, alinhando os três pilares discutidos anteriormente – políticas claras, capacitação contínua e soluções seguras – com mecanismos de responsabilização, transparência e participação ativa dos envolvidos (colaboradores ou responsáveis).

Figura 1 – Framework de Governança para Inteligência Artificial (GIA)



Fonte: Elaborada pela autora a partir da literatura e da pesquisa de campo.

A primeira dimensão do *framework* estabelece os Princípios Éticos e Diretrizes como base para qualquer implementação tecnológica. Trata-se da formalização de valores como transparência, responsabilidade, imparcialidade e segurança de dados. Em consonância com o que foi identificado nos dados empíricos, organizações que não estabelecem previamente esses parâmetros acabam permitindo o uso informal da IA, o que compromete tanto a eficácia quanto a integridade do processo decisório. Portanto, a definição e publicização desses princípios funcionam como marcos normativos mínimos a serem seguidos, promovendo alinhamento institucional e conformidade regulatória desde o início do ciclo de adoção (HILB, 2020; MAHER, 2024; CAMPOS, 2024). A segunda etapa concentra-se nos Mecanismos de Monitoramento e Avaliação, essenciais para garantir a operacionalização contínua dos princípios éticos declarados. Aqui, recomenda-se a criação de sistemas automatizados e periódicos de auditoria de modelos e dados, permitindo a identificação e correção de desvios, bem como a publicação de relatórios de conformidade. Esta dimensão dialoga diretamente com os achados da pesquisa de campo, em especial no que se refere ao risco de *Shadow AI* identificado na administração pública, onde a ausência de monitoramento favorece práticas informais e potencialmente lesivas (SILIC, M.; SILIC, D.; OBLANKOVIC, 2016).

Em seguida, o *framework* propõe o fortalecimento do Engajamento e Participação dos Envolvidos (colaboradores ou responsáveis), contemplando a criação de espaços formais para a escuta ativa de usuários, desenvolvedores, gestores e representantes da sociedade civil. Essa abordagem amplia a legitimidade das decisões automatizadas e contribui para o aprimoramento constante dos sistemas de IA com base em feedbacks reais. A inclusão dessa dimensão reflete a compreensão de que a governança tecnológica não pode ser verticalizada ou restrita a especialistas, devendo envolver todos os agentes impactados pelas decisões algorítmicas (WORLD BANK, 1992).

A quarta dimensão trata do Ajuste e Resolução de Conflitos Éticos, reconhecendo que, mesmo com diretrizes e monitoramento, dilemas morais e riscos emergentes podem surgir. Assim, a proposta contempla a constituição de comitês de ética em IA, independentes e multidisciplinares, com competência para intervir em situações críticas, além da definição de protocolos que permitam pausas ou ajustes na operação dos sistemas sempre que necessário. Essa camada de resolução

autônoma reforça a flexibilidade adaptativa do *framework* frente a mudanças regulatórias, sociais ou tecnológicas (CHUVAKIN; KAGANOVICH, 2024; CAMPOS, 2024).

Por fim, o pilar de sustentação do modelo está na Capacitação e Educação Contínua, tanto para os responsáveis técnicos quanto para usuários e lideranças organizacionais. Conforme evidenciado nas entrevistas e sustentado pela literatura, a ausência de formação sobre os limites e responsabilidades do uso de IA é uma das principais brechas para a proliferação da *Shadow AI*. Assim, o incentivo a uma cultura organizacional orientada por princípios éticos e fundamentada no conhecimento sobre a tecnologia torna-se indispensável para consolidar um ambiente seguro e inovador (MAH, 2021; SCHNEIDER *et al.*, 2022).

A implementação do *Framework GIA* se dá por meio de um ciclo contínuo de planejamento, execução, monitoramento e revisão. Esse ciclo deve ser respaldado por métricas de avaliação que incluem indicadores de transparência, frequência de revisões técnicas e grau de satisfação dos stakeholders. Ao operar com base em valores e práticas multidimensionais, o *framework* se configura como uma proposta viável para organizações que buscam aliar inovação tecnológica à responsabilidade institucional.

6 CONCLUSÃO

A crescente inserção da Inteligência Artificial Generativa (IA Gen) nos ambientes corporativos têm reconfigurado não apenas os fluxos de trabalho, mas também os fundamentos da governança organizacional. Este estudo buscou compreender, por meio de uma abordagem qualitativa e exploratória, como estruturas de governança corporativa podem ser mobilizadas para mitigar os riscos associados à *Shadow AI* (uso das IA Gen não autorizadas) e, ao mesmo tempo, potencializar os benefícios da adoção da IA Gen no contexto empresarial.

O problema de pesquisa que orientou este estudo — “Como a governança corporativa pode mitigar riscos associados ao uso indevido da *Shadow AI* e potencializar os benefícios do uso da Inteligência Artificial Generativa (IA Gen) no ambiente empresarial?” — foi integralmente respondido. Os resultados confirmam que a governança, quando estruturada em políticas claras, mecanismos de monitoramento, engajamento dos envolvidos no processo e práticas de capacitação, atua de maneira decisiva tanto na mitigação dos riscos quanto na transformação da tecnologia em um ativo estratégico para as organizações.

Além de controles formais e mecanismos técnicos, os achados sugerem que a governança de IA generativa depende também de condições organizacionais que incentivem a transparência do uso pelos colaboradores. Waters-Lynch et al. (2025) indicam que a decisão de revelar ou ocultar práticas de uso de IA pode estar associada à percepção de benefícios, ao nível de confiança institucional e ao receio de sanções, o que implica que abordagens exclusivamente punitivas tendem a deslocar o uso para a invisibilidade. Assim, políticas de governança eficazes devem combinar diretrizes e controles com estratégias de estímulo ao reporte, orientação e validação segura das práticas, transformando usos individuais e informais em aprendizagem organizacional e mitigando o risco de *Shadow AI* por meio de institucionalização progressiva (WATERS-LYNCH et al., 2025).

Os objetivos que nortearam a pesquisa foram atingidos de forma consistente, permitindo uma compreensão abrangente do fenômeno em análise. O primeiro objetivo, que buscou identificar os principais usos e riscos associados ao uso de ferramentas de IA Gen, foi contemplado na seção inicial das entrevistas, que explorou aplicações práticas e percepções de riscos como segurança de dados, viés nos algoritmos e impactos éticos. O segundo objetivo, que analisou o papel da

governança corporativa na mitigação dos riscos do uso indevido da *Shadow AI* dentro do contexto da IA generativa, foi alcançado pela investigação das políticas e práticas relatadas pelos entrevistados, permitindo avaliar sua eficácia na redução desses riscos. Por fim, o terceiro objetivo, de sistematizar diretrizes de governança corporativa, foi atendido pela síntese dos achados comparativos entre os três contextos organizacionais, que possibilitou a elaboração de recomendações alinhadas às dimensões de conformidade, ética, transparência e segurança da informação.

A partir do levantamento teórico e da análise empírica conduzida com três organizações de naturezas distintas — setor público, empresa de base tecnológica e cooperativa financeira —, evidenciou-se que a adoção da IA Gen ocorre de forma heterogênea e condicionada por fatores institucionais, regulatórios e culturais. Constatou-se que, em diferentes graus, a ausência de diretrizes claras, a insuficiência de programas de formação e o uso de soluções de consumo individual ampliam os riscos de segurança, privacidade e conformidade, além de dificultarem a exploração do potencial estratégico da tecnologia. Ao mesmo tempo, verificou-se que todos os entrevistados, independentemente do setor, possuíam compreensão sólida sobre os usos e riscos da IA Gen, revelando tanto consciência crítica quanto disposição para avançar na criação de práticas de governança mais robustas.

A análise comparativa mostrou que, no Público, as limitações para adoção não decorrem do desconhecimento técnico do entrevistado, mas de barreiras institucionais ligadas a orçamento, burocracia e ausência de políticas específicas, mencionou-se que ao chegar a demanda geralmente eles (o setor de TI) fazem o estudo para a viabilidade, pois precisam ser compradas e/ou adquiridas por licitações e dificilmente vêm de iniciativa própria essa demanda de novas ferramentas. As ferramentas precisam ser compradas formalmente. Cada setor e área é um sistema único no Público, até para documentação interna de cada setor: “*situação bem complexa*” comentou o entrevistado do Público.

Já a empresa de base tecnológica apresenta maior abertura para a experimentação e para o uso estratégico da inteligência artificial generativa, ainda que com lacunas de formalização em termos de governança. No entanto, ao ser questionado sobre como a organização promove a transparência e a ética no uso dessa tecnologia, o entrevistado afirmou não reconhecer tais aspectos como relevantes ou merecedores de atenção no contexto atual. Em suas palavras, “não é

um tema que eu me preocupe ou ache que mereça minha energia", acrescentando que sequer identifica com clareza o que poderia ser compreendido como transparência ou como práticas antiéticas nesse campo. O entrevistado chegou a ironizar o tema, exemplificando que um possível uso antiético seria "*alguém ficar em home office e deixar a IA trabalhando no seu lugar*". Essa perspectiva evidencia a ausência de reflexão crítica e de diretrizes institucionais sobre ética e transparência, reforçando a lacuna de governança identificada na empresa.

Adicionalmente, quando indagado sobre as medidas de segurança e conformidade voltadas a evitar o uso não autorizado de ferramentas de inteligência artificial generativa, o entrevistado reconheceu a inexistência de práticas sistematizadas. Segundo ele, eventuais restrições são tratadas de forma pontual e informal, como ocorreu no caso do "Deepseek", em que foi solicitado apenas ao time de desenvolvimento que não utilizasse a ferramenta, sem que houvesse um comunicado institucional abrangente. O entrevistado reconhece que a ausência de comunicação mais ampla é uma falha, ainda que justificada pela percepção de que os demais colaboradores provavelmente não fariam uso da tecnologia. Tal postura evidencia não apenas a falta de processos estruturados de segurança e conformidade, mas também a predominância de ações reativas e casuais frente aos riscos relacionados à adoção da IA generativa.

Por fim, ao ser questionado sobre estratégias que poderiam contribuir para o aprimoramento da governança de IA generativa no ambiente corporativo, o entrevistado apontou a necessidade de estabelecer processos formais de aprovação das ferramentas a serem utilizadas, bem como a implementação de treinamentos direcionados às equipes. Esses treinamentos, segundo ele, deveriam contemplar orientações sobre boas práticas de uso, incluindo aspectos relacionados ao que enviar ou não às ferramentas, cuidados de segurança e diretrizes claras de conduta. Essa reflexão, ainda que incipiente, indica um reconhecimento da importância de mecanismos preventivos e educativos como caminhos possíveis para estruturar uma governança mais consistente.

No caso de Finanças, por sua vez, predomina uma postura de cautela, pautada pelo compliance e pela necessidade de alinhamento regulatório, o que resulta em maior controle, mas também em um ritmo mais lento de adoção. Esse comportamento encontra respaldo na própria estrutura organizacional, uma vez que a decisão sobre quais ferramentas de inteligência artificial generativa podem ser

utilizadas ou implementadas é centralizada em uma área específica de IA na *Central Nacional*, como eles denominam.

Entre os principais resultados esperados com a adoção da tecnologia, destacam-se a busca por maior eficiência, assertividade e a obtenção de insights estratégicos que contribuam para o negócio. Contudo, os desafios também são reconhecidos, sendo a segurança apontada como a principal preocupação, dado que a instituição lida diretamente com dados sensíveis e protegidos por legislações de confidencialidade, o que impõe limitações e demanda maior rigor no uso.

Nesse contexto, observa-se um movimento estruturado de preparação interna. A organização iniciou suas práticas com um processo de sensibilização e mapeamento conjunto de oportunidades de uso da IA generativa, conduzido pela própria equipe especializada em IA da empresa. Além disso, há incentivos para que os colaboradores participem de cursos e capacitações voltados ao tema, demonstrando uma preocupação em garantir que a adoção da tecnologia ocorra de maneira supervisionada, ética e tecnicamente embasada.

Em síntese para essa conclusão, no caso da empresa de base tecnológica, observa-se uma abertura significativa para o uso e a exploração das ferramentas de inteligência artificial generativa, principalmente com o objetivo de ampliar a agilidade e melhorar a execução das tarefas e entregas organizacionais. Contudo, não há, até o momento, uma preocupação efetiva em relação à segurança de dados e informações, tampouco um processo definido e claro para orientar o uso da tecnologia no ambiente corporativo. Tal cenário expõe a organização a riscos mais eminentes de vazamento de dados, que podem ser de extrema relevância estratégica.

No PÚBLICO, por sua vez, identifica-se um contexto marcado pela burocratização, característica inerente às estruturas administrativas desse ambiente. Entretanto, ainda não existem processos específicos ou mesmo discussões consistentes sobre o uso adequado da inteligência artificial generativa. Nesse caso, a aplicação da tecnologia depende do cumprimento de protocolos internos, o que pode dificultar sua adoção de maneira ágil e efetiva.

Dentre os três casos analisados, o setor financeiro se destaca por apresentar maior maturidade no tema. Há processos e reflexões mais estruturados acerca da utilização da inteligência artificial generativa, que já foram incorporados a práticas internas de troca de ideias entre colaboradores. O entrevistado de Finanças

destacou, ainda, iniciativas em formato de *talks* de boas práticas, guias e cartilhas de uso, além da elaboração de normativos acessíveis a todos os colaboradores. Embora tais iniciativas ainda estejam em estágio inicial e passíveis de aprimoramento, elas indicam um esforço mais consistente em direção à institucionalização da governança da IA no contexto organizacional.

Nesse sentido, pode-se concluir que, embora cada setor apresente especificidades em sua relação com a inteligência artificial generativa, existe um consenso quanto à inevitabilidade da construção de políticas e processos formais que assegurem a transparência, a segurança e a ética no uso da tecnologia. A diversidade de abordagens reforça a necessidade de que a governança da IA seja pensada de forma contextualizada, respeitando as particularidades de cada ambiente organizacional, mas sem negligenciar a urgência de estabelecer mecanismos regulatórios que mitiguem riscos e potencializem os benefícios da inovação.

Ao aprofundar a análise sobre os desafios da integração da IA generativa, percebe-se que cada setor manifesta preocupações distintas. No Público, a principal barreira identificada refere-se à resistência interna a mudanças, traduzida pela expressão recorrente “*pra que mudar, sempre foi assim*”. Esse fator, aliado ao predomínio de processos manuais, pode retardar a adoção da tecnologia em larga escala. Já no Tecno, os desafios concentram-se em aspectos técnicos, sobretudo no controle da “alucinação” dos modelos, no refinamento de *prompts* e na garantia de que os sistemas executem de fato o que se espera deles. Nesse caso, o entrevistado destacou o risco ampliado no uso via API, uma vez que erros podem não ser identificados pelos clientes finais, o que representaria um problema grave. No setor financeiro, por sua vez, as limitações de segurança, a necessidade de homologação de fornecedores e parceiros e os entraves regulatórios foram apontados como obstáculos que podem gerar atrasos ou até inviabilizar projetos.

Em relação às perspectivas futuras, os entrevistados convergem em considerar que a inteligência artificial generativa será uma tecnologia inevitável. No setor público, o entrevistado reconhece que “*não vai ter volta*”, apontando a necessidade de validação do uso e a possibilidade de ganhos significativos diante de processos internos manuais, mas alerta que “*vai substituir quem não sabe usar*”. No setor de base tecnológica, a visão é marcada pelo entusiasmo e pela ênfase na urgência da adoção: “*Só vai! Só melhora! Vai dominar, quem não usar tá ferrado! Mas tem que*

saber fazer as perguntas certas!”. Já no setor financeiro, o entrevistado destacou sua posição de entusiasta do tema, avaliando que há “um grande potencial a ser explorado” e ressaltando que as ferramentas “se aprimoram diariamente”.

Dessa forma, a análise evidencia que, embora os setores estejam em estágios distintos de maturidade, existe um consenso quanto ao caráter irreversível da integração da IA generativa. E mesmo que persistem desafios de ordem técnica, cultural, regulatória e de segurança, cuja superação será determinante para que a adoção da tecnologia ocorra de forma responsável, estratégica e sustentável.

Com base nessas evidências, foram identificados três pilares fundamentais para orientar a construção de diretrizes voltadas ao uso responsável da IA Gen: (i) definição de políticas de governança e regulação claras; (ii) implementação de programas contínuos de treinamento e comunicação interna; e (iii) adoção de plataformas corporativas seguras, capazes de reduzir riscos de *Shadow AI* e fortalecer a proteção da informação. Tais pilares, já apontados pela literatura (CAMPOS, 2024; MAHER, 2024; CHUVAKIN; KAGANOVICH, 2024), funcionam como alicerces para o desenvolvimento de estruturas institucionais que integrem inovação tecnológica, responsabilidade ética e conformidade regulatória.

Como resultado prático, esta pesquisa propõe o *Framework* de Governança para Inteligência Artificial (GIA), um modelo adaptável, multidimensional e baseado em valores, destinado à gestão responsável da IA Gen em ambientes corporativos. O *framework* organiza-se em cinco dimensões centrais: (i) princípios éticos e diretrizes formais (transparência, responsabilidade, imparcialidade e segurança); (ii) mecanismos de monitoramento e avaliação contínua de dados, algoritmos e conformidade regulatória; (iii) engajamento dos envolvidos para ampliar a legitimidade e a transparência das práticas; (iv) procedimentos de resolução de conflitos éticos, com instâncias deliberativas capazes de intervir em casos críticos; e (v) capacitação contínua de colaboradores, tanto em aspectos técnicos quanto em sensibilização ética.

A operacionalização do GIA deve ocorrer por meio de um ciclo iterativo de planejamento, execução, monitoramento e melhoria contínua, apoiado em métricas de avaliação que considerem indicadores de conformidade, satisfação dos envolvidos e correção de desvios (MÄNTYMÄKI *et al.*, 2022). Dessa forma, contribui-se para a consolidação de uma abordagem de governança que, ao mesmo tempo, responde aos dilemas contemporâneos da IA e potencializa suas

capacidades inovadoras em alinhamento com os objetivos estratégicos das organizações.

No plano operacional, uma implicação prática dos resultados é a necessidade de mecanismos de validação que reduzam riscos sem bloquear experimentação, especialmente em tarefas administrativas e rotinas intensivas em informação. Nesse sentido, a lógica de testes em “modo paralelo”, discutida por Sidorkin (2025), é compatível com a proposta do Framework GIA ao sugerir que a organização registre divergências, estabeleça baseline humano e avalie evidências antes de expandir o uso de IA generativa. Integrar esse tipo de procedimento ao ciclo de planejamento, execução e revisão do GIA pode fortalecer a dimensão de monitoramento, ampliar a transparência e reduzir o uso informal ao oferecer caminhos institucionais seguros para experimentar e aprender com a tecnologia (SIDORKIN, 2025).

Os resultados deste estudo contribuem para o campo da Governança de IA de forma teórica e prática. A pesquisa enriquece a literatura ao investigar a *Shadow AI* no viés do uso não autorizado de ferramentas de IA Gen a partir de uma perspectiva de governança, analisando-a em três setores distintos. A análise comparativa mostra que a percepção e a resposta aos riscos da IA Gen variam de acordo com as especificidades culturais, institucionais e regulatórias de cada organização. Além disso, a proposta do *Framework GIA* consolida os pilares de governança identificados na literatura e nos dados empíricos em um modelo coeso e aplicável.

O *Framework GIA* se configura como um guia prático para gestores e líderes que buscam implementar o uso ético e responsável da IA Gen. O modelo propõe um ciclo de melhoria contínua que permite às organizações não apenas reagirem aos desafios, mas também se adaptarem prontamente às inovações. Essa abordagem oferece uma rota propositiva para que organizações públicas e privadas possam enfrentar, de forma estruturada, os desafios e oportunidades de uma tecnologia que já redefine os contornos do ambiente corporativo contemporâneo.

Apesar das importantes contribuições, esta pesquisa apresenta algumas limitações que podem ser abordadas em trabalhos futuros. A principal limitação reside no número reduzido de casos de estudo (três organizações), o que restringe a generalização dos resultados. Futuros estudos poderiam expandir a amostra para incluir mais empresas de diferentes setores e portes, a fim de validar as evidências aqui encontradas em um escopo mais amplo, incluir um estudo de maturidade das

organizações para compreender o nível de aplicação de governança e em relação ao uso de IA Gen.

Ademais, sugere-se a aplicação prática do *Framework GIA* em uma organização para avaliar sua eficácia na implementação e verificar a adequação de suas dimensões ao longo do tempo. Pesquisas quantitativas também poderiam ser realizadas para mensurar o impacto financeiro da *Shadow AI*, complementando a abordagem qualitativa deste estudo. Por fim, estas temáticas abordadas no estudo como IA Gen, *Shadow AI* e governança são atuais e relevantes para serem cada vez mais aprofundados e pautados no ambiente corporativo e fora dele.

REFERÊNCIAS

- ABRAHAM, R.; SCHNEIDER, J.; VOM BROCKE, J. Data Governance: A Conceptual Framework, Structured Review, and Research Agenda. *Int. J. Inf. Manag.*, Oxford, v. 49, p. 424-438, 2019. Disponível em: <https://ideas.repec.org/a/eee/ininma/v49y2019icp424-438.html>. Acesso em: 8 nov. 2025.
- ALI, H.; MURAD, S.; SHAH, Z. Spot the fake lungs: Generating synthetic medical images using neural diffusion models. In: IRISH CONFERENCE ON ARTIFICIAL INTELLIGENCE AND COGNITIVE SCIENCE, 30., 2023, Munster. **Anais** [...]. Munster: AICS, 2023, p. 32-39. Disponível em: <https://arxiv.org/abs/2211.00902>. Acesso em: 8 nov. 2025.
- ALMEIDA, P. G. R. de. Regulação da Inteligência Artificial: Ação Coletiva que Requer Governança. **Computação Brasil**, Porto Alegre, n. 47, p. 23-26, 2022. Disponível em: <https://journals-sol.sbc.org.br/index.php/comp-br/article/view/4403/2614>. Acesso em: 8 nov. 2025.
- BANH, L.; STROBEL, G. Fundamentals of generative artificial intelligence. **Electron. Markets**, v. 33, n. 63, p. 1-27, 2023. Disponível em: <https://link.springer.com/article/10.1007/s12525-023-00680-1>. Acesso em: 7 nov. 2024.
- BARBOSA, A. M. et al. Governança em TI: COBIT e ITIL. **Rev. Cienc. Electron. Adm.**, Garça, v. 11, n. 19, jan. 2011. Disponível em: http://faef.revista.inf.br/imagens_arquivos/arquivos_destaque/b4K1BphABn6CaKb_2013-5-3-11-17-0.pdf. Acesso em: 8 nov. 2025.
- BARBOSA, X. de C.; BEZERRA, R. F. Breve introdução à história da inteligência artificial. **Jamaxi**, [s.l.], v. 4, n. 2, p. 90-97, 2020. Disponível em: <https://periodicos.ufac.br/index.php/jamaxi/article/view/4730/2695>. Acesso em: 8 nov. 2025.
- BARDIN, L. **Análise de conteúdo**. Lisboa: Edições 70, 2011.
- BLIN, E. **IA/I(ADE) ROBOT ? L'essor de l'intelligence artificielle dans l'exercice professionnel des infirmiers anesthésistes**: un maintien de leur identité professionnelle et une modification de leur processus de raisonnement clinique. 2024. Mémoire de fin d'études (Diplôme d'État d'infirmier anesthésiste) – École IADE, Pôle de Formation des Professionnels de Santé, Centre Hospitalier Universitaire de Rennes, Rennes, França, 2024. Disponível em: https://sofia.medicalistes.fr/spip/IMG/pdf/ia-ia_de_robot__memoire_emilie_blin_juin_2024_chu_rennes_version_finalisee_.pdf. Acesso em: 8 nov. 2025.
- BONNEFON, J.-F.; RAHWAN, I.; SHARIFF, A. The social dilemma of autonomous vehicles. **Science**, [s.l.], v. 352, n., 6293, p. 1573-1576, 2016. Disponível em: <https://www.science.org/doi/10.1126/science.aaf2654>. Acesso em: 8 nov. 2025.

BRAGA, J. et al. Como a Governança de Múltiplas Partes Interessadas Pode Moldar a IA Responsável. **Ethikai**, [s.l.], n. 10, p. 224, 2024. Disponível em: https://osf.io/preprints/osf/kdw52_v1. Acesso em: 8 nov. 2025.

CAMPOS, J. F. P. de. Como proteger sua empresa da *Shadow AI*. **IBM Comunica**, [s.l.], 28 fev. 2024. Disponível em: <https://brasil.newsroom.ibm.com/2024-02-28-Como-proteger-sua-empresa-da-Shadow-AI>. Acesso em: 6 nov. 2024.

BRYNJOLFSSON, E.; McAFFEE, A. **Machine, platform, crowd: harnessing our digital future**. New York: W.W. Norton & Company, 2017.

CARINI, L.; MORAIS, F. S. de. Governança ética para construção de confiança em sistemas de inteligência artificial. **Prim@ Facie**, João Pessoa, v. 19, n. 40, p. 1-26, 2020. Disponível em: <https://periodicos.ufpb.br/index.php/primafacie/article/view/48406/29765>. Acesso em: 8 nov. 2025.

CHUVAKIN, A.; KAGANOVICH, M. Spotlighting *Shadow AI*: How to Protect Against Risky AI Practices. **Google Cloud Blog**, [s.l.], 2024. Disponível em: <https://cloud.google.com/transform/spotlighting-shadow-ai-how-to-protect-against-risky-ai-practices>. Acesso em: 6 nov. 2024.

CRESWELL, J. W. **Research design**: Qualitative, quantitative, and mixed methods approaches. 4. ed. Thousand Oaks, CA: Sage, 2013.

DENZIN, N. K.; LINCOLN, Y. S. **The Sage Handbook of Qualitative Research**. 3. ed. Thousand Oaks, CA: Sage, 2005.

DWIVEDI, Y. K. et al. So what if ChatGPT wrote it? Multidisciplinary perspectives on opportunities, challenges and implications of generative artificial intelligence for research, practice and policy. **Int. J. Inf. Manag.**, [s.l.], v. 71, 2023. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0268401223000233?via%3Dihub>. Acesso em: 8 nov. 2025.

GONÇALVES, A. O conceito de governança. In: GONÇALVES, A. **Governança e relações internacionais**. São Paulo: X, 2021. p. 400-416.

GUTLAPALLI, S. S. The role of deep learning in the fourth industrial revolution: a digital transformation approach. **Asian Account. Audit. Adv.**, [s.l.], v. 8, n. 1, p. 52-56, 2017. Disponível em: <https://4ajournal.com/article/view/77>. Acesso em: 7 nov. 2024.

GOODFELLOW, I.; BENGIO, Y.; COURVILLE, A. **Deep learning**. Cambridge: MIT Press, 2016.

GYÖRY, A. et al. Exploring the Shadows: IT Governance Approaches to Deal with *Shadow IT*. In: EUROPEAN CONFERENCE ON INFORMATION SYSTEMS, 20., 2012, Barcelona. **Anais** [...]. Barcelona: ECIS, 2012. Disponível em: <https://aisel.aisnet.org/ecis2012/222/>. Acesso em: 8 nov. 2025.

HAAG, S.; ECKHARDT, A. Normalizing the Shadows: The Role of Symbolic Models for Individuals' *Shadow IT* Usage. In: INTERNATIONAL CONFERENCE ON INFORMATION SYSTEMS, 35., 2014, Auckland. **Anais** [...]. Auckland: ICIS, 2014. Disponível em:
<https://aisel.aisnet.org/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1421&context=icis2014>. Acesso em: 8 nov. 2025.

HEWITT, Andrew. Are You Ready for BYOAI?. **Forrester**, Cambridge, 2023. Disponível em: <https://www.forrester.com/what-it-means/ep340-bring-your-own-ai>. Acesso em: 29 set. 2024.

HILB, M. Toward artificial governance? The role of artificial intelligence in shaping the future of corporate governance. **J. Manag. Gov.**, [s./], v. 24, p. 851-870, 2020. Disponível em: <https://link.springer.com/article/10.1007/s10997-020-09519-9>. Acesso em: 8 nov. 2025.

HILDEBRANDT, M. Defining profiling: A new type of knowledge?. In: HILDEBRANDT, M.; GUTWIRTH, S. (ed.). **Profiling the European Citizen**. Dordrecht: Springer, 2008. p. 17-45.

INSTITUTE FOR BUSINESS VALUE – IBM. The CEO Study 2024: 6 hard truths CEOs must face. **IBM Institute for Business Value**, Armonk, 16 maio 2024. Disponível em:
<https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/2024-ceo>. Acesso em: 14 nov. 2024.

ISRANI, E. Algorithmic due process: mistaken accountability and attribution in State v. Loomis. **J. Law Technol.**, Cambridge, 31 ago. 2017. Disponível em:
<https://jolt.law.harvard.edu/digest/algorithmic-due-process-mistaken-accountability-and-attribution-in-state-v-loomis-1>. Acesso em: 29 set. 2024.

KALKAN, G. The Impact of Artificial Intelligence on Corporate Governance. **J. Corp. Finance Res.**, [s./], v. 18, n. 2, p. 17-25, 2024. Disponível em:
https://journals.rcsi.science/2073-0438/article/view/302653/278054/en_US. Acesso em: 8 nov. 2025.

LUCIANO, E. M.; COSTA NETTO, Y. W. E.; WIEDENHÖFT, G. C. Artefatos de TI e suas inter-relações: uma contribuição para a teorização da governança de TI. In: SEMINÁRIOS EM ADMINISTRAÇÃO DA UNIVERSIDADE DE SÃO PAULO, 18., 2015, São Paulo. **Anais** [...]. São Paulo, 2015. Disponível em:
https://www.researchgate.net/publication/283645505_Artefatos_de_TI_e_Suas_Interrelacoes_Uma_Contribuicao_Para_A_Teorizacao_da_Governanca_de_TI_IT_Artifacts_and_their_Interrelationships_a_Contribution_to_the_IT_Governance_theorization. Acesso em: 8 nov. 2025.

LUNARDI, G. L. et al. Análise dos mecanismos de governança de TI mais difundidos entre as empresas brasileiras. **Alcance**, Porto Alegre, v. 21, n. 1, p. 46-76, 2014. Disponível em: <https://lume.ufrgs.br/handle/10183/105135>. Acesso em: 8 nov. 2025.

MACHADO, H. G. **O ciclo de vida do uso da Shadow IT no contexto da governança de TI.** 2023. Dissertação (Mestrado em Administração) – Universidade Federal do Rio Grande do Sul, Porto Alegre, 2023.

MACHADO, J. dos S. et al. A inovação tecnológica e os desafios representados pela Inteligência Artificial. **Thema**, Pelotas, v. 22, n. 1, p. 151-168, 2023. Disponível em: <https://periodicos.ifsul.edu.br/index.php/thema/article/view/2991/2230>. Acesso em: 8 nov. 2025.

MACHADO, J. dos S. et al. As principais ameaças digitais e suas formas de mitigação no contexto da segurança da propriedade intelectual. **Conjecturas**, [s.l.], v. 22, n. 8, p. 147-162, 2022. Disponível em: <https://pdfs.semanticscholar.org/2485/88032ed59eca158f0530d8e71c0365454442.pdf>. Acesso em: 8 nov. 2025.

MAGESH, V. et al. Hallucination-Free? Assessing the Reliability of Leading AI Legal Research Tools. **J. Empir. Leg. Stud.**, [s.l.], p. 1-27, 2024. Disponível em: https://dho.stanford.edu/wp-content/uploads/Legal_RAG_Hallucinations.pdf. Acesso em: 8 nov. 2025.

MAGUNDUNI, J.; CHIGONA, W. Revisiting *Shadow IT* research: What we already know, what we still need to know, and how do we get there?. In: CONFERENCE ON INFORMATION COMMUNICATIONS TECHNOLOGY AND SOCIETY, 2018, Durban. **Anais** [...]. Durban: ICTAS, 2018. Disponível em: https://www.researchgate.net/publication/325495495_Revisiting_shadow_IT_research_What_we_already_know_what_we_still_need_to_know_and_how_do_we_get_the_re. Acesso em: 8 nov. 2025.

MAHER, S. What Is *Shadow AI* And What Can IT Do About It?. **Forbes**, [s.l.], 31 out. 2023. Disponível em: <https://www.forbes.com/sites/delltechnologies/2023/10/31/what-is-shadow-ai-and-what-can-it-do-about-it/>. Acesso em: 6 nov. 2024.

MALLMANN, G. L.; MAÇADA, A. C.; OLIVEIRA, M. The influence of *Shadow IT* usage on knowledge sharing: An exploratory study with IT users. **Bus. Inf. Rev.**, [s.l.], v. 35, n. 1, p. 17-28, 2018. Disponível em: <https://2024.sci-hub.cat/6735/b1e5c0e0e634d3393e290a69e74e9db6/10.1177@0266382118760143.pdf>. Acesso em: 8 nov. 2025.

MANDAPURAM, M.; GUTLAPALLI, S. S.; BODEPUDI, A. Investigating the prospects of generative artificial intelligence. **Asian J. Humanit. Art Lit.**, [s.l.], v. 5, n. 2, p. 167-174, 2018. Disponível em: https://www.researchgate.net/publication/370789251_Investigating_the_Prospects_of_Generative_Artificial_Intelligence. Acesso em: 8 nov. 2025.

MÄNTYMÄKI, M. et al. Defining organizational AI governance. **AI and Ethics**, [s.l.], v. 2, n. 3, p. 603-609, 2022. Disponível em: <https://link.springer.com/article/10.1007/s43681-022-00143-x>. Acesso em: 8 nov. 2025.

McKINSEY & COMPANY. The state of AI in 2023: Generative AI's breakout year.

McKinsey & Company, [s.l.], 1 ago. 2023. Disponível em:

<https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-in-2023-generative-ais-breakout-year>. Acesso em: 2 nov. 2025.

NOZARI, H.; SZMELTER-JAROSZ, A.; GHAHREMANI-NAHR, J. Analysis of the challenges of Artificial Intelligence of Things (AloT) for the Smart Supply Chain (Case Study: FMCG Industries). **Sensors**, [s.l.], v. 22, n. 8, p. 2931, 2022. Disponível em: <https://www.mdpi.com/1424-8220/22/8/2931>. Acesso em: 8 nov. 2025.

MICROSOFT. Work Trend Index: Annual Report – Will AI Fix Work?. **Microsoft**, Redmond, 9 maio 2023. Disponível em:

<https://www.microsoft.com/en-us/worklab/work-trend-index/will-ai-fix-work>. Acesso em: 14 nov. 2024.

MIRANDA, H. P. Frankenstein e as Sombras da IA. **Outras Palavras**, São Paulo, 5 nov. 2024. Disponível em:

<https://outraspalavras.net/tecnologiaemdisputa/frankenstein-e-as-sombras-da-ia/>. Acesso em: 6 nov. 2024.

MIT TECHNOLOGY REVIEW. Entre a inovação e a governança: desafios para a adoção da IA generativa. **MIT Technology Review**, Rio de Janeiro, 25 abr. 2024. Disponível em:

<https://mittechreview.com.br/entre-a-inovacao-e-a-governanca-desafios-para-a-adocao-da-ia-generativa/>. Acesso em: 14 nov. 2024.

PACHECO, A. et al. **Ética, Governança e Inteligência Artificial**. São Paulo: XYZ, 2023.

PUTHAL, Deepak; MISHRA, Amit Kumar; MOHANTY, Saraju P.; LONGO, Antonella; YEUN, Chan Yeob. **Shadow AI: Cyber Security Implications, Opportunities and Challenges in the Unseen Frontier**. *SN Computer Science*, [S. l.], v. 6, art. 405, 2025. DOI: 10.1007/s42979-025-03962-x. Disponível em: <https://link.springer.com/article/10.1007/s42979-025-03962-x>. Acesso em: 23 jan. 2026.

PREM, E. Artificial intelligence for innovation in Austria. **Technol. Innov. Manag. Rev.**, [s.l.], v. 9, n. 12, 2019. Disponível em: <https://timreview.ca/article/1287>. Acesso em: 8 nov. 2025.

QIANG, C. Z.; LIU, Y.; WANG, H. **Who on Earth Is Using Generative AI?**. Washington, DC: World Bank Group, 2024.

RANSBOTHAM, S. et al. The state of AI in 2021: the business of artificial intelligence. **MIT Sloan Management Review**, Cambridge, 2021. Disponível em: <https://sloanreview.mit.edu/big-ideas/artificial-intelligence-business-strategy/>. Acesso em: 29 set. 2024.

RUSSELL, C. Bring Your Own AI — (BYOAI). Harnessing the Employee-Driven AI Revolution. **Medium**, [s.l.], 10 nov. 2023. Disponível em:

<https://chuckrussell.medium.com/bring-your-own-ai-byoai-ab096e04dbd9>. Acesso em: 29 set. 2024.

RUSSELL, S.; NORVIG, P. **Artificial Intelligence**: A Modern Approach. 3. ed. Upper Saddle River: Pearson Education, 2010.

SCHNEIDER, J. et al. Artificial intelligence governance for businesses. **Inf. Syst. Manag.**, [s.l.], v. 40, n. 3, p. 229-249, 2022. Disponível em: <https://www.tandfonline.com/doi/full/10.1080/10580530.2022.2085825>. Acesso em: 8 nov. 2025.

SIDORKIN, Alexander M. **Shadow Testing Protocol: Accelerating AI Adoption Through Evidence Sharing in Government**. 2025. 14 p. Disponível em: <https://ssrn.com/abstract=5264238>. Acesso em: 23 jan. 2026. DOI: 10.2139/ssrn.5264238.

SILIC, M.; BACK, A. *Shadow IT*: A view from behind the curtain. **Comput. Secur.**, [s.l.], v. 45, p. 274-283, 2014. Disponível em: <https://www.sciencedirect.com/science/article/abs/pii/S016740481400100X>. Acesso em: 9 nov. 2025.

SILIC, M.; SILIC, D.; OBLANKOVIC, G. Influence of *Shadow IT* on Innovation in Organizations. **Complex Syst. Inform. Model. Q.**, Riga, n. 8, p. 68-80, 2016. Disponível em: <https://csimq-journals.rtu.lv/csimq/article/view/csimq.2016-8.06/47>. Acesso em: 9 nov. 2025.

STANTON, C.; CLUNE, J. Curiosity search: producing generalists by encouraging individuals to continually explore and acquire skills throughout their lifetime. **PLoS One**, [s.l.], v. 11, n. 9, 2016. Disponível em: <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0162235>. Acesso em: 7 nov. 2024.

TAEIHAGH, A. Governance of Artificial Intelligence. **Policy Soc.**, [s.l.], v. 40, n. 2, p. 137-157, jun. 2021. Disponível em: <https://academic.oup.com/policyandsociety/article/40/2/137/6509315>. Acesso em: 8 nov. 2025.

TARIQ, M. U.; POULIN, M.; ABONAMAH, A. A. Achieving operational excellence through artificial intelligence: driving forces and barriers. **Front. Psychol.**, [s.l.], v. 12, 2021. Disponível em: <https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2021.686624/full>. Acesso em: 8 nov. 2025.

THODUPUNORI, S. R.; GUTLAPALLI, S. S. Overview of LeOra Software: a statistical tool for decision makers. **Technol. Manag. Rev.**, [s.l.], v. 3, p. 7-11, 2018. Disponível em: <https://upright.pub/index.php/tmr/article/view/123>. Acesso em: 8 nov. 2025.

THE NEW YORK CITY COUNCIL. Introduction of Law Number 2018/048. **The New York City Council**, New York, 2018. Disponível em:

<https://legistar.council.nyc.gov/legislationDetail.aspx?ID=3137815&GUID=437A6A6D-62E1-47E2-9C42-461253F9C6D0>. Acesso em: 29 set. 2024.

TROCIN, C. *et al.* How Artificial Intelligence affords digital innovation: a cross-case analysis of Scandinavian companies. **Technol. Forecast. Soc. Change**, New York, v. 173, p. 121081, 2021. Disponível em:
<https://www.sciencedirect.com/science/article/pii/S0040162521005138>. Acesso em: 8 nov. 2025.

WATERS-LYNCH, Julian; ALLEN, Darcy W. E.; POTTS, Jason; BERG, Chris. **Shadow user innovation: governing covert generative-AI use for dynamic-capability renewal**. *Innovation: Management, Policy and Practice*, [S. I.], p. 1–17, 20 jun. 2025. DOI: 10.1080/14479338.2025.2519546. Disponível em:
<https://www.tandfonline.com/doi/full/10.1080/14479338.2025.2519546>. Acesso em: 23 jan. 2026.

WORLD BANK. **Governance and development**. Washington, DC: The World Bank, 1992.

WU, L.; RANSBOTHAM, S. Can AI Help Your Company Innovate? It Depends. **Harvard Business Review**, [s./.], 25 jul. 2024. Disponível em:
<https://hbr.org/2024/07/can-ai-help-your-company-innovate-it-depends>. Acesso em: 12 nov. 2024.

YIN, R. K. **Case Study Research: Design and Methods**. 5. ed. Thousand Oaks, CA: Sage, 2015.

ZIANG, Z.; JIHAENG, L. Research on development and challenges of Chinese medical artificial intelligence. In: INTERNATIONAL CONFERENCE ON PUBLIC MANAGEMENT AND INTELLIGENT SOCIETY, 2021, Shanghai. **Anais** [...]. Shanghai: PMIS, 2021. p. 371-375.