DA REDUÇÃO DE RISCOS À RECONFIGURAÇÃO DO PMO: GOVERNANÇA DA SHADOW AI EM AMBIENTES DE GESTÃO DE PROJETOS NA ERA COGNITIVA

FROM RISK REDUCTION TO PMO RECONFIGURATION: SHADOW AI GOVERNANCE IN PROJECT MANAGEMENT ENVIRONMENTS IN THE COGNITIVE ERA

EDSON MELO DE SOUZA
UNINOVE – UNIVERSIDADE NOVE DE JULHO

DANIELA CORREIA BATISTA
UNINOVE – UNIVERSIDADE NOVE DE JULHO

FÁBIO DE LIMA SILVA
UNINOVE – UNIVERSIDADE NOVE DE JULHO

JURANDIR OLIVEIRA RODRIGUES DOS SANTOS
UNINOVE – UNIVERSIDADE NOVE DE JULHO

Comunicação:
O XIV SINGEP foi realizado em conjunto com a 14th Conferência Internacional do CIK (CYRUS Institute of Knowledge) e com a SPARK (Society for Promoting Academic Research and Knowledge), em formato híbrido, com sede presencial na UNINOVE - Universidade Nove de Julho, no Brasil.

Agradecimento à orgão de fomento:
Fundo de Apoio à Pesquisa (FAP/Uninove – Universidade Nove de Julho)

DA REDUÇÃO DE RISCOS À RECONFIGURAÇÃO DO PMO: GOVERNANÇA DA SHADOW AI EM AMBIENTES DE GESTÃO DE PROJETOS NA ERA COGNITIVA

Objetivo do estudo
Propor um modelo conceitual de governança ativa da Shadow AI para o PMO, integrando controles práticos nas dimensões técnica, organizativa e educativa, alinhados à ISO/IEC 42001 e fundamentados em modelos comportamentais validados.

Relevância/originalidade
A Shadow AI introduz riscos qualitativamente distintos da Shadow IT convencional. O conceito de PMO Cognitivo, aqui proposto, representa contribuição original ao situar o escritório de projetos como estrutura de governança da inteligência operacional organizacional.

Metodologia/abordagem
Revisão integrativa da literatura (Torraco, 2005; Whittemore & Knafl, 2005), com buscas em Web of Science, Scopus e Google Scholar (2020–2026), combinando estudos empíricos, modelos teóricos e relatórios técnicos de referência sobre governança de IA em contextos organizacionais.

Principais resultados
O PMO Cognitivo requer quatro papéis especializados e controles estruturados em três dimensões. Políticas puramente proibitivas são ineficazes; a combinação de Dynamic Tracing, Fast-Track SLAs e Comunidades de Prática reduz a Shadow AI sem comprometer a agilidade das equipes.

Contribuições teóricas/metodológicas
Diferenciação conceitual entre Shadow IT e Shadow AI; integração da Teoria do Comportamento Planejado, Dissuasão Geral e Cognitive Offloading ao diagnóstico da evasão normativa; e arquitetura de governança desacoplada em BPM+, com nexo causal entre diagnóstico e prescrição.

Contribuições sociais/para a gestão
O enquadramento proposto endereça os ODS 8, 9, 10, 16 e 17 da Agenda 2030, posicionando a governança responsável de IA em projetos como vetor simultaneamente organizacional e normativo, com aplicabilidade direta a PMOs de diferentes portes e setores regulados.

Palavras-chave: Shadow AI, PMO Cognitivo, Governança Ativa de IA, Gestão de Projetos, Evasão Normativa

FROM RISK REDUCTION TO PMO RECONFIGURATION: SHADOW AI GOVERNANCE IN PROJECT MANAGEMENT ENVIRONMENTS IN THE COGNITIVE ERA

Study purpose
To propose a conceptual model of active Shadow AI governance for the PMO, integrating practical controls across technical, organizational, and educational dimensions, aligned with ISO/IEC 42001 and grounded in validated behavioral models.

Relevance / originality
Shadow AI introduces governance risks qualitatively distinct from conventional Shadow IT. The Cognitive PMO concept, originally proposed here, repositions the project management office as a governing structure for organizational operational intelligence.

Methodology / approach
Integrative literature review (Torraco, 2005; Whittemore & Knafl, 2005), drawing on Web of Science, Scopus, and Google Scholar (2020–2026), combining empirical studies, theoretical models, and technical reports on AI governance in organizational settings.

Main results
The Cognitive PMO requires four specialized roles and controls structured across three dimensions. Purely prohibitive policies are ineffective; combining Dynamic Tracing, Fast-Track SLAs, and Communities of Practice reduces Shadow AI adoption without compromising team agility.

Theoretical / methodological contributions
Behavior Theory, General Deterrence, and Cognitive Offloading into normative evasion diagnosis; and a decoupled governance architecture in BPM+, with causal nexus between diagnosis and prescription.

Social / management contributions
The proposed framework addresses SDGs 8, 9, 10, 16, and 17 of the 2030 Agenda, positioning responsible AI governance in project environments as both an organizational response and a normative contribution, with direct applicability across PMOs of varied sizes and regulated sectors.

Keywords: Shadow AI, Cognitive PMO, Active AI Governance, Project Management, Policy Bypass

DA REDUÇÃO DE RISCOS À RECONFIGURAÇÃO DO PMO: GOVERNANÇA DA *SHADOW AI* EM AMBIENTES DE GESTÃO DE PROJETOS NA ERA COGNITIVA

1 Introdução

A rápida incorporação da Inteligência Artificial Generativa (IAG) e de agentes autônomos ao ambiente corporativo ampliou o potencial de produtividade das organizações, mas também gerou um descompasso crescente entre as práticas das equipes de projeto e as políticas institucionais de governança organizacional (Waters-Lynch et al., 2025). Nesse contexto, surgiu o fenômeno denominado *Shadow AI* (*Artificial Intelligence*), caracterizado pelo uso de modelos de linguagem de larga escala (LLMs), assistentes de escrita e geradores de código sem homologação, autorização prévia ou auditoria pelas estruturas responsáveis pela governança da organização (Waters-Lynch et al., 2025; Silic et al., 2025).

O ambiente de gestão de projetos apresenta características que favorecem a adoção informal de ferramentas com tais características. Lundin e Söderholm (1995) definem as organizações temporárias de projeto pela descontinuidade das equipes, pelo foco em tarefas com prazo definido e pela necessidade de integração acelerada de conhecimento entre participantes de diferentes origens disciplinares, condições que dificultam a internalização de políticas formais de governança tecnológica. A pressão estrutural por cumprimento de prazo, escopo e orçamento, empiricamente confirmada como o critério operacional dominante em ambientes de projeto (Serrador & Turner, 2015), reduz a tolerância dos colaboradores a processos formais de homologação percebidos como lentos. Estudos recentes indicam que gestores de projetos tendem a apresentar taxas elevadas de adoção de ferramentas de IA sem autorização formal, em razão da distância entre a capacidade analítica exigida e os recursos oficialmente disponíveis (Silic et al., 2025).

O fenômeno evolui em duas fases qualitativamente distintas. A primeira corresponde ao uso de chatbots conversacionais, marcado pela cópia manual de dados organizacionais para interfaces públicas acessadas por contas pessoais, com riscos delimitados pela ação direta do usuário. A segunda fase, caracterizada pelo emprego de agentes autônomos, introduz um cenário substancialmente mais dinâmico. Em configurações sem supervisão explícita, agentes dotados de credenciais de acesso a sistemas de arquivos, caixas de e-mail e interfaces de programação de aplicações (APIs) corporativas podem executar tarefas em segundo plano, ampliando a superfície de exposição de dados sensíveis e reduzindo a capacidade das equipes de segurança de identificar e auditar tais interações. Silic et al. (2025) caracterizam esse processo como uma falha de governança sociotécnica, na qual a natureza generativa, opaca e autônoma dos sistemas de inteligência artificial (IA) introduz riscos qualitativamente distintos dos já conhecidos na *Shadow IT* (*Information Technology*) tradicional.

O problema de pesquisa que orienta este trabalho fundamenta-se na seguinte questão: como estruturar um enquadramento de governança ativa no Escritório de Gestão de Projetos (*Project Management Office*, PMO) capaz de mitigar os riscos comportamentais, operacionais e regulatórios da *Shadow AI* sem comprometer a agilidade e a capacidade de inovação das equipes?

O objetivo é propor um modelo conceitual aplicado de governança para o PMO, integrando controles práticos derivados de modelos comportamentais validados e alinhados às diretrizes da ISO/IEC 42001. Trata-se de uma contribuição de natureza aplicada, sem pretensão de ineditismo teórico, voltada à utilidade prática para gestores de projetos e pesquisadores da área.

Este estudo oferece três contribuições principais. A primeira consiste na diferenciação conceitual entre *Shadow IT* e *Shadow AI* sob a perspectiva da governança em PMO, identificando as dimensões em que os riscos divergem qualitativamente. A segunda integra modelos comportamentais consolidados (Teoria do Comportamento Planejado, Teoria da

Dissuasão Geral e descarregamento cognitivo) à literatura emergente sobre governança de IA, estabelecendo nexo causal explícito entre diagnóstico comportamental e prescrição de controle. Por fim, a terceira propõe um enquadramento operacional de governança ativa composto por papéis organizacionais, arquitetura desacoplada baseada no padrão BPM+ (*Business Process Management Plus*) e controles estruturados nas dimensões técnica, organizativa e educativa.

A relevância do problema não se restringe ao contexto organizacional imediato. O fenômeno da *Shadow AI* e os mecanismos de governança propostos neste trabalho articulam-se diretamente com cinco Objetivos de Desenvolvimento Sustentável (ODS) da Agenda 2030 (Organização das Nações Unidas [ONU], 2015): o ODS 8, pela via do deslocamento não planejado de competências profissionais decorrente da automação cognitiva; o ODS 9, na medida em que a ausência de infraestrutura de governança compromete a sustentabilidade da inovação tecnológica nas organizações; o ODS 10, em razão da assimetria de acesso a ferramentas homologadas entre organizações de diferentes portes; o ODS 16, pelo vínculo direto entre governança de IA e construção de instituições transparentes, responsáveis e eficazes; e o ODS 17, considerando que a escalabilidade dos controles propostos depende de parcerias interorganizacionais entre PMOs, equipes de segurança da informação, reguladores e fornecedores. O alinhamento com esses objetivos não é periférico: a governança ativa da IA nos ambientes de projeto é, ao mesmo tempo, uma resposta organizacional e uma contribuição à agenda normativa global de desenvolvimento responsável. A correspondência entre cada ODS e os mecanismos específicos propostos no modelo é sistematizada na Tabela 5 (seção 4.3).

2. Referencial Teórico

O referencial teórico deste trabalho organiza-se em quatro eixos articulados. O primeiro delimita a *Shadow AI* como fenômeno qualitativamente distinto da tecnologia não homologada convencional, estabelecendo as bases conceituais para a análise de governança que se desenvolve nas seções seguintes. O segundo situa o PMO no contexto da transformação digital, identificando as funções institucionais que tornam esse ambiente particularmente suscetível à adoção informal de ferramentas de IA. O terceiro mobiliza três modelos comportamentais consolidados, cuja articulação fornece o diagnóstico causal necessário à prescrição de controles. O quarto apresenta os alicerces regulatórios e de modelagem de processos, o padrão BPM+ e a norma ISO/IEC 42001, que operacionalizam a arquitetura de governança ativa proposta.

A sequência é deliberada: sem a distinção estrutural entre *Shadow IT* e *Shadow AI* (2.1), o diagnóstico comportamental (2.3) perde especificidade; sem esse diagnóstico, os controles práticos propostos na seção 4 carecem de fundamentação teórica explícita.

2.1 Diferenciação Estrutural: *Shadow IT* versus *Shadow AI*

A compreensão adequada do impacto da inteligência artificial (IA) não autorizada exige uma distinção precisa em relação à tecnologia não homologada convencional (*Shadow IT*). Segundo Silic et al. (2025), a *Shadow IT* envolve o uso de *hardware*, *software* ou serviços de nuvem comuns com comportamento determinístico e previsível, ao passo que a *Shadow AI* se baseia em modelos de aprendizado de máquina de caráter probabilístico e não determinístico, cujas saídas não são totalmente previsíveis nem auditáveis pelos mecanismos convencionais de controle de TI. Silic et al. situam a *Shadow AI* como extensão evolutiva do fenômeno da *Shadow IT* (Silic & Back, 2014), argumentando que os riscos qualitativamente distintos introduzidos pela IAG exigem enquadramentos de governança específicos, não contemplados nas abordagens desenvolvidas para a TI não homologada convencional.

Na *Shadow IT*, os dados inseridos permanecem sob a propriedade do usuário sem sofrer alteração estrutural. Na *Shadow AI*, os dados inseridos nos *prompts* são ativamente processados, e em plataformas públicas sem garantias contratuais de privacidade podem ser retidos e utilizados conforme os termos de serviço do provedor. Ademais, podem ser utilizados para o

treinamento de modelos de IA, disponibilizando os dados abertamente. Esse processo resulta na potencial externalização do conhecimento tácito corporativo para infraestruturas fora do controle da organização (Silic et al., 2025).

Um aspecto crítico desse fenômeno reside nos pontos cegos de governança criados por sistemas autônomos: ao operar em segundo plano e interagir com múltiplos recursos organizacionais simultaneamente, os agentes de IA não homologados produzem superfícies de exposição que os mecanismos tradicionais de auditoria de TI não foram projetados para mapear (Shunmugasundaram et al., 2026). Essa limitação estrutural tem implicações diretas para a governança corporativa: enquanto a *Shadow IT* comprometia dados estáticos em repositórios isolados, a *Shadow AI* opera sobre fluxos dinâmicos de conhecimento organizacional, podendo externalizar ativos intangíveis de alto valor estratégico, como modelos de precificação, metodologias proprietárias e dados de clientes, para infraestruturas fora do controle institucional. Em setores regulados, como o financeiro, o de saúde e o de infraestrutura crítica, essa exposição não se limita ao risco operacional: configura potencial violação de obrigações legais de proteção de dados, com consequências que incluem sanções regulatórias, perda de vantagem competitiva e erosão da confiança de stakeholders. A Tabela 1 sistematiza as principais dimensões dessa diferenciação.

Tabela 1 - Comparativo estrutural entre *Shadow IT* e *Shadow AI*

Dimensão	***Shadow IT***	***Shadow AI***
Comportamento	Determinístico e previsível	Probabilístico; sujeito a alucinações e viés de dados
Ciclo dos dados	Dados estáticos em repositório não autorizado	Dados consumidos nos prompts; possível retenção pelo provedor
Superfície de ataque	Identificável via inventário de rede	Expansiva; agentes criam conexões dinâmicas em segundo plano
Impacto no conhecimento	Silos de informação entre setores	Externalização do conhecimento tácito corporativo
Mecanismo de detecção	Tráfego básico e inventário de ativos	Monitoramento profundo de tráfego criptografado e permissões de API

Nota: Elaborada pelos autores com base em Silic et al. (2025) e Shunmugasundaram et al. (2026). ArmorCode (2026) contribui com caracterização operacional complementar.

2.2 O PMO na Era Digital: Funções, Pressões e Vulnerabilidades

O PMO consolidou-se como estrutura central para a padronização de processos, o alinhamento estratégico de portfólios e a disseminação de boas práticas em gerenciamento de projetos (Project Management Institute, 2021). A pesquisa de Hobbs e Aubry (2010), baseada em levantamento com mais de 500 PMOs em contexto internacional, identificou que as funções mais valorizadas pelas organizações consistem no monitoramento e controle do desempenho de projetos, na gestão de portfólios e na implementação de metodologias padronizadas.

É nesse conjunto de funções que a *Shadow AI* surge como problema específico de governança de projetos. A adoção informal de ferramentas de IA nos fluxos de trabalho das equipes compromete precisamente o núcleo das atividades de valor do PMO: elaboração de cronogramas, análise de riscos, estimativas de custo e geração de relatórios para *stakeholders* (Kopko, 2026). A reconfiguração do PMO como estrutura de governança ativa representa, contudo, uma evolução necessária de suas funções constitutivas diante das transformações do ambiente tecnológico (Kerzner, 2022).

Compreender por que as equipes de projeto recorrem a ferramentas não homologadas, mesmo quando cientes dos riscos, exige, portanto, ir além do diagnóstico institucional do PMO.

É nessa direção que os modelos comportamentais apresentados a seguir operam: não como quadros explicativos genéricos, mas como instrumentos de diagnóstico causal das condições que tornam a *Shadow AI* estruturalmente atraente em ambientes de alta pressão por resultados.

2.3 Modelos Comportamentais: Fundamentos para a Compreensão da Evasão Normativa

A fundamentação sobre o comportamento de descumprimento regulatório apoia-se em três arcabouços consolidados. A Teoria do Comportamento Planejado (Ajzen, 1991) permite compreender a intenção de uso informal como resultado da interação entre atitudes favoráveis à ferramenta, normas subjetivas do grupo de trabalho e percepção de controle comportamental. Quando o colaborador percebe que a via formal é lenta e burocrática, a intenção de recorrer a ferramentas não homologadas aumenta proporcionalmente.

A Teoria da Dissuasão Geral (Straub, 1990), originalmente desenvolvida para o contexto de abuso computacional, é aqui adaptada pelos autores ao fenômeno da *Shadow AI*: o argumento central da teoria é que políticas puramente punitivas são eficazes apenas quando a percepção de detecção é alta. Em ambientes de *Shadow AI*, a invisibilidade do comportamento reduz essa percepção a ponto de anular o efeito dissuasório das sanções formais, tornando ineficaz qualquer estratégia de controle baseada exclusivamente em proibição. Essa transposição conceitual é interpretativa e não foi empiricamente validada no contexto específico de equipes de projeto.

Por fim, os estudos sobre Descarregamento Cognitivo (*Cognitive Offloading*) (Risko & Gilbert, 2016) documentam que a delegação sistemática de tarefas analíticas complexas a assistentes virtuais, sem verificação crítica dos resultados, reduz o esforço intelectual exigido no planejamento e na análise de projetos, comprometendo a aprendizagem ativa e a capacidade crítica das equipes sobre os entregáveis produzidos.

Esses três constructos articulam, de forma complementar, o diagnóstico comportamental que fundamenta os controles de mitigação propostos na seção 4.

2.4 Governança de Processos e Arquiteturas Desacopladas: BPM+ e ISO/IEC 42001

A operacionalização da governança ativa no PMO pressupõe dois alicerces complementares: um padrão de modelagem de processos suficientemente flexível para acomodar a variabilidade dos sistemas de IA e uma norma de gestão que forneça o arcabouço regulatório de referência. O padrão BPM+ integra três linguagens de modelagem complementares mantidas pelo Object Management Group (OMG): o BPMN (*Business Process Model and Notation*) para representar fluxos de trabalho estruturados e repetíveis (OMG, 2011); o DMN (*Decision Model and Notation*) para formalizar regras e critérios de decisão de forma auditável (OMG, 2021); e o CMMN (*Case Management Model and Notation*) para situações dinâmicas e não totalmente previsíveis, como a gestão adaptativa de incidentes de segurança de IA (OMG, 2014).

A prevalência do BPMN como linguagem de modelagem de processos dominante na prática organizacional é empiricamente documentada por Compagnucci et al. (2023), cuja análise de um repositório de mais de 54.500 modelos evidencia padrões de uso recorrentes, erros sintáticos em ferramentas de modelagem e violações de boas práticas, confirmando a maturidade e a disseminação da notação no ambiente corporativo. A integração das três notações permite isolar a lógica de negócios das dependências de implementações específicas, viabilizando arquiteturas desacopladas nas quais os modelos subjacentes podem ser substituídos ou atualizados sem impacto nas regras operacionais da organização. Esse princípio de desacoplamento é inerente à arquitetura do próprio padrão BPM+, conforme especificado pelo OMG nas normas que regulam o BPMN (OMG, 2011), o DMN (OMG, 2021) e o CMMN (OMG, 2014).

A norma ISO/IEC 42001 (International Organization for Standardization, 2023) responde ao segundo requisito ao estabelecer os requisitos para um sistema de gestão de IA em organizações. Sua estrutura define responsabilidades, controles de risco, critérios de avaliação de impacto e mecanismos de melhoria contínua aplicáveis ao ciclo de vida completo dos sistemas de IA. No contexto do PMO, a norma fornece o quadro regulatório que orienta tanto a homologação formal de ferramentas quanto a definição dos papéis especializados de governança discutidos na seção 4.2.

A combinação entre a flexibilidade arquitetural do BPM+ e o rigor normativo da ISO/IEC 42001 é adotada neste trabalho como base técnica e regulatória para o modelo de governança ativa proposto. Importa registrar que o BPM+ não opera apenas como mecanismo de modelagem de processos: ao manter desacoplados os controles, as regras decisórias e os mecanismos de auditoria em relação aos modelos específicos de IA, ele funciona como elemento habilitador da governança ativa, permitindo que o PMO adapte suas políticas sem depender de fornecedores particulares, aspecto desenvolvido operacionalmente na Seção 4.3.

3. Metodologia

Este artigo adota uma abordagem de revisão integrativa da literatura, de natureza qualitativa e descritiva, conforme os procedimentos propostos por Torraco (2005) e consolidados por Whittemore e Knafl (2005). A revisão integrativa distingue-se da revisão sistemática por permitir a combinação de fontes primárias de naturezas distintas (estudos empíricos, modelos teóricos e relatórios técnicos de referência), característica adequada a domínios emergentes como a governança de IA em ambientes organizacionais.

O corpus foi constituído a partir de buscas nas bases Web of Science, Scopus, Google Scholar, com os descritores "*Shadow AI*", "generative AI governance", "PMO artificial intelligence", "AI project management risk" e "*Policy Bypass* AI", combinados pelos operadores booleanos AND e OR. O recorte temporal abrangeu 2020-2026, com prioridade para produções de 2024-2026. Foram adotados como critérios de inclusão: (a) publicações em inglês ou português; (b) foco explícito em governança de IA, *Shadow AI* ou gestão de projetos mediada por tecnologia; e (c) disponibilidade do texto completo. Foram excluídos trabalhos restritos a aspectos técnicos de arquitetura de modelos sem implicações organizacionais. Os indicadores quantitativos de prevalência e custo da *Shadow AI*, apresentados na seção 4.1, derivam exclusivamente de relatórios setoriais utilizados como evidência contextual ilustrativa, não como fundamento teórico ou empírico do modelo proposto.

O procedimento analítico estruturou-se em quatro etapas: (1) mapeamento dos indicadores de prevalência e custos da *Shadow AI*; (2) análise comparativa dos modelos teóricos de aceitação tecnológica e comportamento organizacional; (3) sistematização das metodologias de governança existentes, incluindo a ISO/IEC 42001 e os princípios de modelagem BPM+; e (4) síntese integrativa e proposição do modelo conceitual de governança ativa. A natureza teórico-conceitual do estudo é reconhecida como limitação inerente à fase atual de desenvolvimento do campo, dada a escassez de estudos longitudinais sobre *Shadow AI* em ambientes de PMO.

Cumpre registrar que os relatórios setoriais de organizações como Optro (2026), IBM Security (2025) e Microsoft (2025) foram incorporados ao corpus de forma deliberada e delimitada: sua função restringe-se à composição dos indicadores de prevalência e custo de mercado apresentados na Tabela 2, não à fundamentação teórica ou metodológica do enquadramento proposto. Essa distinção é relevante porque tais fontes, embora amplamente referenciadas na literatura recente sobre *Shadow AI*, constituem literatura cinzenta produzida por organizações com interesse comercial na percepção de risco. Os constructos teóricos e as prescrições de controle do modelo derivam exclusivamente de literatura acadêmica revisada por pares, conforme indicado nas seções 2.3 e 2.4.

4. Análise dos Resultados e Discussões

A análise organiza-se em três movimentos complementares. O primeiro quantifica a magnitude do fenômeno da *Shadow AI* nas organizações, situando o problema em seu contexto empírico por meio de indicadores de prevalência e custo. O segundo propõe a reconfiguração estrutural do PMO, definindo os papéis especializados de governança necessários à mediação entre inovação e controle institucional. Por fim, o terceiro operacionaliza essa governança, apresentando controles práticos nas dimensões técnica, organizativa e educativa, cada um ancorado nos constructos comportamentais desenvolvidos na seção 2.3.

4.1 Dimensão do Problema: Indicadores Globais

Os dados recentes evidenciam que a adoção não homologada de IA deixou de ser comportamento marginal para se transformar na norma operacional da maioria dos profissionais do conhecimento. A Tabela 2 sintetiza os principais indicadores mapeados na revisão.

Tabela 2 - Indicadores globais de prevalência e custos da *Shadow AI*

Indicador	**Resultado apurado**	**Fonte**
Prevalência da *Shadow AI*	80% das organizações relatam uso de IA não autorizada	Optro (2026)
Visibilidade de TI	Apenas 25% das empresas têm visibilidade total do uso de IA	Optro (2026)
Adoção de ferramentas pessoais de IA	Maioria dos trabalhadores do conhecimento admite usar ferramentas de IA pessoais para cumprir metas diárias (dado aproximado; variação entre estudos)	Microsoft (2025)
Custo médio global de violação de dados	US$ 4,88 milhões em 2024, com incremento adicional em cenários envolvendo IAG não governada	IBM Security (2025)
Organizações sem visibilidade de IA em uso	Parcela expressiva das organizações não possui inventário formal das ferramentas de IA utilizadas pelos colaboradores	Optro (2026)

Nota: Elaborada pelos autores com base em fontes secundárias mapeadas (2025-2026).

Os indicadores revelam uma contradição estrutural: enquanto as organizações reconhecem a urgência da inovação guiada por IA, a ausência de ferramentas homologadas e acessíveis empurra os colaboradores para caminhos informais. Importa registrar que os dados da Tabela 2 provêm de relatórios setoriais com metodologias distintas e amostras não comparáveis diretamente; sua função aqui é ilustrativa da magnitude do fenômeno, não probatória de relações causais. O custo médio global de violação de dados apurado pela IBM Security (2025) em US$ 4,88 milhões sinaliza a exposição financeira estrutural associada a falhas de governança de IA, cujo impacto é agravado pela opacidade dos sistemas não homologados. A exposição regulatória é particularmente relevante em contextos sujeitos à Lei Geral de Proteção de Dados (LGPD) e ao Regulamento Geral de Proteção de Dados europeu (RGPD).

4.2 O PMO Cognitivo: Novos Papéis Estruturais de Governança

O avanço da IAG nas organizações coloca o PMO diante de uma inflexão institucional: permanecer como estrutura de controle burocrático de cronogramas e relatórios estáticos significa aceitar progressiva perda de relevância corporativa em um ambiente onde as decisões

de projeto são crescentemente mediadas por sistemas cognitivos autônomos. A resposta a esse desafio não é a simples adoção de ferramentas de IA, mas a reconfiguração do PMO como estrutura de governança ativa sobre essas ferramentas. O conceito de PMO Cognitivo, aqui proposto, designa essa transição: uma configuração organizacional na qual o escritório de projetos deixa de operar exclusivamente sobre processos e passa a operar também sobre os sistemas de conhecimento que alimentam esses processos, assumindo responsabilidade pela homologação, pelo monitoramento e pela auditoria contínua dos modelos de IA em uso nas equipes. Nessa configuração, a função central do PMO desloca-se do controle de conformidade procedimental para a governança da inteligência operacional da organização, posicionando-o como mediador institucional entre a demanda por inovação das equipes e os requisitos de conformidade regulatória e estratégica da organização.

A Tabela 3 apresenta essa estrutura de papéis, proposta pelos autores com base na articulação entre as funções constitutivas do PMO (Project Management Institute, 2021; Hobbs & Aubry, 2010) e as demandas específicas de governança de IA identificadas na revisão.

Tabela 3 - Matriz de novos papéis estruturais de governança no PMO Cognitivo

Papel no PMO Cognitivo	**Responsabilidades principais**	**Contribuição para a governança de IA**
Líder de Portfólio de Casos de IA	Monitorar alinhamento estratégico e conformidade de projetos de IA	Centralizar a homologação e manter catálogo de ferramentas oficiais
Orquestrador de Prontidão de Dados	Garantir consistência, integridade e privacidade das bases de dados	Estabelecer barreiras contra conexões via APIs externas não autorizadas
Gestor de Risco de Modelos	Traduzir requisitos legais e gerenciar validação contínua de modelos	Atuar junto ao Encarregado de Proteção de Dados (DPO, *Data Protection Officer*) para aprovações ágeis de novos casos de uso
Consultor de Mudança e Confiança	Avaliar adoção real pelos times e apoiar a transição cultural	Promover sessões de mentoria sobre uso ético e seguro de IA

Nota: Os papéis propostos constituem contribuição dos autores, fundamentada nas funções do PMO descritas por Hobbs e Aubry (2010) e PMI (2021), e inspirada em tendências de mercado discutidas em Batra (2026) e Kopko (2026). Fonte: Elaborada pelos autores.

Esses papéis não substituem a estrutura existente do PMO, mas a complementam, respondendo à especificidade dos riscos introduzidos pela *Shadow AI*. O Líder de Portfólio de Casos de IA atua como ponto focal de homologação; o Orquestrador de Prontidão de Dados garante a integridade das bases que alimentam os modelos; o Gestor de Risco de Modelos viabiliza aprovações ágeis em conformidade com a ISO/IEC 42001; e o Consultor de Mudança e Confiança sustenta a transformação cultural necessária para que os controles sejam internalizados e não apenas tolerados.

4.3 Arquitetura de Governança Ativa: Controles Práticos e Fundamentos Comportamentais

A transição do diagnóstico para a prescrição exige que os controles de governança sejam ancorados nos mesmos constructos comportamentais que explicam a adesão informal. Nessa perspectiva, o enquadramento proposto organiza as táticas de mitigação em três dimensões complementares: técnica, organizativa e educativa.

Cada dimensão responde a um mecanismo distinto de produção da *Shadow AI*, conforme identificado nas seções 2.3 e 2.4, e nenhuma delas é suficiente isoladamente. A sustentabilidade da governança depende, adicionalmente, da adoção de arquiteturas desacopladas baseadas no padrão BPM+ (BPMN para fluxos de trabalho, DMN para modelagem de decisões e CMMN para casos dinâmicos), que permitem isolar a lógica de negócios e substituir modelos de IA sem reescrever as regras operacionais da organização.

A Tabela 4 sintetiza as táticas de controle prático recomendadas, explicitando, para cada uma, o fundamento teórico que a sustenta. Essa correspondência direta entre diagnóstico comportamental e prescrição de controle distingue o enquadramento proposto de recomendações genéricas de segurança da informação.

Tabela 4 - Táticas de controle prático e governança ativa da *Shadow AI* no PMO

Tipo de controle	**Prática recomendada**	**Objetivo de mitigação**	**Fundamento teórico**	**Métrica de monitoramento**
Técnico	*Dynamic Tracing*: visualização do fluxo de dados até APIs externas	Detectar agentes invisíveis e prevenir exfiltração em segundo plano	TCP: reduz percepção de controle informal	Nº de conexões externas não autorizadas interceptadas por período
Técnico	*Policy-as-Code*: firewalls de IA interceptando dados sensíveis na camada de rede	Bloquear envio involuntário de dados proprietários em tempo real	TDG: eleva percepção de detecção	Nº de *prompts* bloqueados e percentual de endpoints cobertos
Organizativo	Janela de anistia de 30 dias para revelação voluntária de ferramentas informais	Trazer o uso invisível à luz sem punição, mapeando demandas reais	TDG: reduz medo punitivo que induz ao silêncio	Nº de ferramentas declaradas e regularizadas no período
Organizativo	*Fast-Track SLAs*: aprovação ágil de ferramentas em até cinco dias úteis	Demonstrar que a via homologada é mais eficiente que o desvio informal	TCP: reduz barreiras à intenção de uso formal	Tempo médio de homologação (dias úteis) antes e após implantação
Educativo	Comunidades de Prática semanais com mentoria e demonstrações de uso seguro	Reconstituir o julgamento crítico corroído pelo *Offloading* cognitivo	*Cognitive Offloading* (Risko & Gilbert, 2016)	Nº de sessões realizadas e percentual de ferramentas em uso homologadas

Nota: TCP = Teoria do Comportamento Planejado (Ajzen, 1991); TDG = Teoria da Dissuasão Geral (Straub, 1990). Fonte: Elaborada pelos autores.

A coerência entre as três dimensões de controle (técnica, organizativa e educativa) é o que confere ao enquadramento sua característica sistêmica. Controles puramente técnicos falham porque não endereçam a motivação comportamental subjacente; controles puramente educativos falham porque dependem de adesão voluntária em contextos de alta pressão por resultados. A combinação das três dimensões, ancorada nos modelos comportamentais revisados, é o que permite reduzir a atratividade da via informal sem comprometer a agilidade das equipes.

O enquadramento de governança ativa proposto articula-se, de forma não trivial, com cinco Objetivos de Desenvolvimento Sustentável (ODS) da Agenda 2030 (Organização das Nações Unidas [ONU], 2015). A conexão não é retórica: cada ODS identificado corresponde a

uma dimensão de risco ou de potencial que o fenômeno da *Shadow AI* ativa de maneira direta nos ambientes de gestão de projetos. O ODS 8 (Trabalho Decente e Crescimento Econômico) é impactado pela automação cognitiva não governada, que pode deslocar competências profissionais sem planos estruturados de transição; os controles educativos propostos na Tabela 4, em especial as Comunidades de Prática, operam precisamente como mecanismos de requalificação contínua. O ODS 9 (Indústria, Inovação e Infraestrutura) sustenta a lógica central do PMO Cognitivo: a governança ativa não é obstáculo à inovação, mas condição para que ela seja escalável, auditável e institucionalmente sustentável. O ODS 10 (Redução das Desigualdades) emerge da assimetria de acesso a ferramentas homologadas entre organizações de diferentes portes, situação em que a *Shadow AI* frequentemente representa a única alternativa disponível para equipes com menor dotação tecnológica; o Fast-Track SLA proposto responde a essa pressão ao reduzir a barreira processual à homologação formal. O ODS 16 (Paz, Justiça e Instituições Eficazes) é o ODS estruturalmente mais próximo do objeto deste trabalho: a governança de IA não homologada é, em sua essência, uma questão de construção institucional, de *accountability* e de proteção de dados em contextos organizacionais sujeitos à LGPD e ao RGPD. Por fim, o ODS 17 (Parcerias e Meios de Implementação) remete à necessidade de colaboração interorganizacional para o desenvolvimento de frameworks de governança compartilhados, incluindo a parceria entre PMOs, equipes de segurança, reguladores e fornecedores de IA, condição sine qua non para que os controles propostos ultrapassem a escala organizacional. A Tabela 5 sistematiza essas correspondências, indicando, para cada ODS, o mecanismo de interface com o modelo proposto.

Tabela 5 - Alinhamento do modelo de governança ativa com os ODS da Agenda 2030

ODS	**Denominação**	**Interface com a *Shadow AI* e o PMO**	**Mecanismo de resposta no modelo proposto**
ODS 8	Trabalho Decente e Crescimento Econômico	A automação cognitiva não governada desloca competências profissionais sem transição planejada, comprometendo a qualidade do trabalho e a aprendizagem organizacional	Comunidades de Prática (controle educativo) como mecanismo de requalificação contínua e reconstituição do julgamento crítico
ODS 9	Indústria, Inovação e Infraestrutura	A *Shadow AI* evidencia que a inovação tecnológica avança mais rapidamente do que a infraestrutura de governança organizacional, gerando lacunas de controle em ambientes de projeto	PMO Cognitivo como infraestrutura de governança que viabiliza inovação responsável e escalável via arquitetura desacoplada BPM+ e ISO/IEC 42001
ODS 10	Redução das Desigualdades	A assimetria de acesso a ferramentas homologadas entre organizações de diferentes portes empurra equipes com menor dotação tecnológica para o uso informal, aprofundando a desigualdade de capacidade analítica	*Fast-Track* SLA (aprovação ágil em até cinco dias úteis) como redutor da barreira processual ao acesso formal a ferramentas de IA
ODS 16	Paz, Justiça e Instituições Eficazes	A *Shadow AI* constitui, em essência, uma falha de accountability institucional; a exposição de dados sensíveis em plataformas não contratadas configura potencial violação de	*Policy-as-Code e Dynamic Tracing* (controles técnicos) como mecanismos de auditabilidade e conformidade institucional; Gestor de Risco

		obrigações regulatórias (LGPD, RGPD), comprometendo a integridade das instituições	de Modelos como papel de *accountability* formal
ODS 17	Parcerias e Meios de Implementação	A eficácia dos controles propostos depende de colaboração interorganizacional entre PMOs, equipes de segurança, reguladores e fornecedores de IA; sem parceria, os frameworks permanecem restritos à escala organizacional individual	Arquitetura desacoplada BPM+ como habilitador de interoperabilidade entre organizações; Consultor de Mudança e Confiança como agente de integração cultural entre parceiros

Nota: ODS = Objetivos de Desenvolvimento Sustentável (ONU, 2015). Apenas os ODS com interface direta e verificável com o fenômeno da *Shadow AI* e o modelo de governança proposto foram incluídos. Fonte: Elaborada pelos autores.

5. Conclusões

O fenômeno da *Shadow AI* na gestão de projetos representa a manifestação de um descompasso estrutural profundo: o desejo das equipes de aumentar sua eficiência operacional contrasta com a incapacidade dos processos formais de TI de responder na velocidade exigida pelo mercado. A literatura analisada sugere que políticas puramente proibitivas tendem a falhar na contenção da adoção informal, resultando no afastamento das práticas operacionais da visibilidade corporativa e no consequente aumento das vulnerabilidades de segurança e conformidade.

A transição do PMO para um papel de governança ativa fundamenta-se na reconfiguração de seus papéis constitutivos e na adoção de controles práticos derivados de modelos comportamentais validados. Ao incorporar papéis especializados, adotar arquiteturas desacopladas baseadas no padrão BPM+ e implementar controles nas dimensões técnica, organizativa e educativa, o PMO amplia sua capacidade de equilibrar a demanda por inovação com os requisitos de conformidade institucional, superando o modelo exclusivamente reativo de controle de cronogramas e relatórios. Nessa perspectiva, o enquadramento proposto transcende o escopo organizacional estrito: ao endereçar simultaneamente a qualidade do trabalho cognitivo (ODS 8), a sustentabilidade da infraestrutura de inovação (ODS 9), a equidade de acesso a ferramentas homologadas (ODS 10), a integridade institucional frente às obrigações regulatórias (ODS 16) e a necessidade de parcerias interorganizacionais para a escalabilidade dos controles (ODS 17), o PMO Cognitivo posiciona-se como vetor de contribuição à Agenda 2030 (ONU, 2015) no plano da governança responsável de sistemas inteligentes.

As três contribuições anunciadas na introdução foram cumpridas de forma articulada. A primeira, a diferenciação conceitual entre *Shadow IT* e *Shadow AI* sob a perspectiva da governança em PMO, foi desenvolvida na seção 2.1 e sistematizada na Tabela 1, evidenciando que os riscos introduzidos pela IAG são qualitativamente distintos dos já conhecidos na TI não homologada convencional. A segunda, a integração de modelos comportamentais consolidados ao diagnóstico da evasão normativa, foi operacionalizada na seção 2.3, estabelecendo nexo causal explícito entre a Teoria do Comportamento Planejado, a Teoria da Dissuasão Geral e o descarregamento cognitivo, de um lado, e as prescrições de controle da Tabela 4, de outro. A terceira, o enquadramento operacional de governança ativa, foi detalhada nas seções 4.2 e 4.3, com a proposição de papéis estruturais para o PMO Cognitivo e controles práticos nas dimensões técnica, organizativa e educativa. Como limitação central, aponta-se a natureza estritamente conceitual do trabalho, que não permite inferências causais sobre a eficácia dos controles propostos.

A agenda de pesquisa futura mais promissora envolve estudos empíricos com estrutura de equações estruturais (*Structural Equation Modeling*, SEM) ou experimentos quase-naturais em contextos de PMO, nos quais os controles de governança ativa operem como variáveis independentes, por exemplo *Fast-Track SLAs* (mensurado pelo tempo médio de homologação), *Policy-as-Code* (cobertura percentual de *endpoints*) e frequência das Comunidades de Prática. As variáveis dependentes prioritárias são a taxa de conformidade normativa das equipes e o desempenho de portfólio (índice de prazo e custo agregado). Estudos longitudinais em PMOs de diferentes portes e setores permitiriam calibrar quais dimensões de controle (técnica, organizativa ou educativa) produzem maior impacto sobre a conformidade.

Declaração de uso de inteligência artificial

Este trabalho recorreu a ferramentas de Inteligência Artificial Generativa (IAG), especificamente Claude Sonnet 4.6 (Anthropic) e Gemini Flash 3.6 (Google), em caráter estritamente instrumental, nas seguintes funções: revisão ortográfica, gramatical e linguística; aprimoramento da clareza e da estrutura textual; síntese exploratória de informações durante o levantamento bibliográfico; formatação e adequação editorial às normas da revista; e apoio na estruturação textual do manuscrito. Em nenhuma etapa as ferramentas de IAG foram empregadas para geração autônoma de argumentos, interpretações teóricas ou conclusões. Todo o conteúdo produzido foi submetido a revisão crítica pelos autores, que assumem integral e exclusiva responsabilidade pela originalidade, integridade e precisão do manuscrito submetido.

Referências

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

ArmorCode. (2026). *What is Shadow AI? The complete guide for enterprise security*. ArmorCode Learning Center. https://www.armorcode.com/learning-center/what-is-shadow-ai-the-complete-guide-for-enterprise-security

Batra, A. (2026). *Redesigning the PMO for an AI-first world: From control tower to cognitive operating system*. Medium Insights. https://thought-walks.medium.com/redesigning-the-pmo-for-an-ai-first-world-from-control-tower-to-cognitive-operating-system-54c6d27934ee

Compagnucci, I., Corradini, F., Fornari, F., & Re, B. (2023). A study on the usage of the BPMN notation for designing process collaboration, choreography, and conversation models. *Business & Information Systems Engineering*, 66, 1–24. https://doi.org/10.1007/s12599-023-00818-7

Hobbs, B., & Aubry, M. (2010). *The project management office: A quest for understanding*. Project Management Institute.

IBM Security. (2025). *Cost of a data breach report 2025*. IBM Corporation. https://www.ibm.com/reports/data-breach

International Organization for Standardization. (2023). *ISO/IEC 42001: Information technology - Artificial intelligence - Management system*. ISO. https://www.iso.org/standard/81230.html

Kerzner, H. (2022). *Project management: A systems approach to planning, scheduling, and controlling* (13th ed.). John Wiley & Sons.

Kopko, M. (2026). *5 steps to integrate AI into project, program and portfolio management*. International Institute for Learning. https://blog.iil.com/5-steps-to-integrate-ai-into-project-program-and-portfolio-management-webcast-preview/

Lundin, R. A., & Söderholm, A. (1995). A theory of the temporary organization. *Scandinavian Journal of Management*, 11(4), 437–455. https://doi.org/10.1016/0956-5221(95)00036-U

Microsoft. (2025). *Work trend index annual report 2025: AI at work, the push for progress*. Microsoft Corporation. https://www.microsoft.com/en-us/worklab/work-trend-index/ai-at-work

Object Management Group. (2011). Business Process Model and Notation (BPMN), Version 2.0. OMG. https://www.omg.org/spec/BPMN/2.0/PDF

Object Management Group. (2014). Case Management Model and Notation (CMMN), Version 1.0. OMG. https://www.omg.org/spec/CMMN/1.0/PDF

Object Management Group. (2021). Decision Model and Notation (DMN), Version 1.3. OMG. https://www.omg.org/spec/DMN/1.3/PDF

Organização das Nações Unidas [ONU]. (2015). *Transformando nosso mundo: A Agenda 2030 para o Desenvolvimento Sustentável*. https://brasil.un.org/sites/default/files/2020-09/agenda2030-pt-br.pdf

Optro. (2026). *Shadow AI stats for 2026: The hidden adoption gap defining enterprise risk*. Optro AI Oversight Report. https://optro.ai/blog/shadow-ai-stats

Project Management Institute. (2021). *A guide to the project management body of knowledge (PMBOK Guide)* (7th ed.). Project Management Institute.

Risko, E. F., & Gilbert, S. J. (2016). *Cognitive Offloading*. *Trends in Cognitive Sciences*, 20(9), 676–688. https://doi.org/10.1016/j.tics.2016.07.002

Serrador, P., & Turner, R. (2015). The relationship between project success and project efficiency. *Project Management Journal*, 46(1), 30–39. https://doi.org/10.1002/pmj.21468

Shunmugasundaram, M., Gangadharan, S., Dave, R., Kala, S., & Michael, O. P. (2026). *Shadow AI* as the new *Shadow IT*: Governance blind spots in autonomous enterprise systems. *EDPACS*, ahead of print. https://doi.org/10.1080/07366981.2026.2679653

Silic, M., Silic, D., & Kind-Trüller, K. (2025). From *Shadow IT* to *Shadow AI*: Threats, risks and opportunities for organizations. *Strategic Change*, 1–16. https://doi.org/10.1002/jsc.2682

Silic, M., & Back, A. (2014). *Shadow IT*: A view from behind the curtain. *Computers & Security*, 45, 274–283. https://doi.org/10.1016/j.cose.2014.06.037

Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research*, 1(3), 255–276. https://doi.org/10.1287/isre.1.3.255

Torraco, R. J. (2005). Writing integrative literature reviews: Guidelines and examples. *Human Resource Development Review*, 4(3), 356–367. https://doi.org/10.1177/1534484305278283

Waters-Lynch, J., Allen, D. W. E., Potts, J., & Berg, C. (2025). Shadow user innovation: governing covert generative-AI use for dynamic-capability renewal. *Innovation: Organization & Management* (Taylor & Francis). https://doi.org/10.1080/14479338.2025.2519546

Whittemore, R., & Knafl, K. (2005). The integrative review: Updated methodology. *Journal of Advanced Nursing*, 52(5), 546–553. https://doi.org/10.1111/j.1365-2648.2005.03621.x