

Uso Seguro de Ferramentas de Inteligência Artificial no Ambiente Corporativo: Guia de Boas Práticas para Funcionários de Pequenas Empresas Brasileiras

Tales U. W. F. Rosário¹, Davi C. Oliveira¹, Luan C. Muhlbeier², Gustavo M. Lima²,

Tais R. Vicensi², Gustavo Lunkes², Julio C. E. Lauermann³, Marcos A. Guido⁴

¹Curso de Análise e Desenvolvimento de Sistemas — Faculdade Donaduzzi

²Curso de Engenharia de Software — Faculdade Donaduzzi

³Curso de Inteligência Artificial — Faculdade Donaduzzi

⁴Faculdade Donaduzzi — Toledo, PR

{talesuriel, davchagasz, luancarlosmuhlbeier, rossetto.tais05, gustavolunkes1, juliolauermann16}@gmail.com, {gustavomarqueslima}@outlook.com
marcos.guido@bpkedu.com.br

Abstract. The popularization of generative Artificial Intelligence tools in the corporate environment has brought productivity gains, but has also introduced risks related to employee behavior. According to a survey by Ipsos and Google (2024), 54% of Brazilians already adopt generative AI, above the global average of 48%, while most small businesses do not have formal governance policies. This scenario favors Shadow AI, the unauthorized use of AI tools outside of organizational control, which can expose sensitive data and constitute an infraction of the General Data Protection Law (LGPD). Based on ISO/IEC 42001:2023, IEEE 7002-2022, and the LGPD, this work proposes a guide to best practices for the safe use of AI aimed at employees of small businesses.

Resumo. A popularização das ferramentas de Inteligência Artificial generativa no ambiente corporativo trouxe ganhos de produtividade, mas também introduziu riscos ligados ao comportamento dos colaboradores. Segundo levantamento do Ipsos e Google (2024), 54% dos brasileiros já adotam IA generativa, acima da média global de 48%, enquanto a maioria das pequenas empresas não possui políticas formais de governança. Esse cenário favorece o Shadow AI, uso não autorizado de ferramentas de IA fora do controle organizacional, que pode expor dados sensíveis e configurar infração à Lei Geral de Proteção de Dados (LGPD). Fundamentado na ISO/IEC 42001:2023, no IEEE 7002-2022 e na LGPD, este trabalho propõe um guia de boas práticas para o uso seguro de IA voltado a colaboradores de pequenas empresas.

1. Introdução

O Brasil está entre os países com maior adoção de IA generativa: 54% dos brasileiros já utilizaram essas ferramentas em 2024, acima da média global de 48% [Ipsos e Google 2024]. No ambiente corporativo, essa adoção ocorre de forma acelerada e sem políticas internas, levando colaboradores a utilizarem ferramentas pessoais para fins profissionais, ampliando significativamente os riscos de segurança da informação.

Consequências concretas já foram observadas. A OpenAI tornou públicos diálogos privados do ChatGPT em resultados de busca, expondo informações internas de empresas sem o conhecimento dos usuários [Fast Company Brasil 2024]. Esse episódio ilustra o fenômeno Shadow AI, uso de ferramentas de IA fora do controle organizacional, amplamente

documentado na literatura recente [Silic et al. 2025]. Juridicamente, tais práticas podem infringir a LGPD (Lei nº 13.709/2018) [Brasil 2018]. Pequenas empresas enfrentam esse desafio sem equipes especializadas em segurança da informação [CERT.br 2024] e sem políticas formais sobre IA, lacuna ainda pouco explorada na literatura nacional, inclusive quanto às implicações da LGPD para sistemas de IA generativa [Revista do TCU 2024].

Diante desse cenário, o objetivo deste trabalho é desenvolver um guia de boas práticas para o uso seguro de IA, voltado a colaboradores de pequenas empresas brasileiras. O guia aborda riscos de exposição de dados sensíveis em plataformas abertas de IA, o fenômeno do Shadow AI e o papel ativo dos funcionários na construção de uma cultura organizacional orientada à segurança da informação.

2. Referencial Teórico

2.1 Governança de IA: ISO/IEC 42001:2023, Proteção de Dados: IEEE 7002-2022 e LGPD

A ISO/IEC 42001:2023, primeiro padrão internacional para sistemas de gestão de IA, estabelece que o uso seguro da IA depende não apenas de controles técnicos, mas de uma cultura organizacional com políticas claras e treinamento periódico dos colaboradores [ISO/IEC 42001 2023; Administrative Sciences 2024]. O padrão IEEE 7002-2022 complementa essa visão ao definir processos para integrar a proteção de privacidade ao ciclo de vida de sistemas que tratam dados [IEEE 2022].

No Brasil, a LGPD (Lei nº 13.709/2018) exige base legal, finalidade definida e medidas de segurança para qualquer tratamento de dados pessoais, incluindo o envio de informações a plataformas externas de IA. Seu art. 20 prevê o direito à explicação de decisões automatizadas, mas a literatura especializada aponta limitações neste dispositivo por restringir o direito apenas a decisões inteiramente automatizadas, deixando de fora processos híbridos [RBDCivil 2020]. Essa fragilidade é evidenciada empiricamente: a Autoridade Nacional de Proteção de Dados (ANPD) identificou que 67% dos casos envolvendo sistemas automatizados investigados entre 2021 e 2024 não apresentaram explicações algorítmicas satisfatórias [Revista do TCU 2024].

2.2 Shadow AI e o Comportamento dos Colaboradores

O fenômeno Shadow AI é caracterizado pelo uso não autorizado de ferramentas de IA por colaboradores fora do controle e aprovação da organização. Estudo recente conduzido com 140 profissionais e 10 executivos evidencia que, embora a IA seja amplamente vista como ferramenta de produtividade, os frameworks de governança frequentemente ficam para trás das práticas dos colaboradores, gerando o que os autores denominam zona de deriva de governança, na qual políticas formais existem mas carecem de aplicação real [Silic et al. 2025]. Conforme reportado pela Fast Company Brasil (2024), 31% dos usuários admitem já ter utilizado informações sensíveis em ferramentas de IA generativa e 14% confessam ter compartilhado segredos comerciais da empresa, majoritariamente por meio de contas pessoais completamente fora do alcance dos controles corporativos. Esse problema é agravado pelo fato de que plataformas abertas de IA podem armazenar os dados inseridos para treinar seus modelos, tornando a recuperação ou exclusão dessas informações praticamente impossível após o envio [Wachter et al. 2017], enquanto a ausência de políticas formais na maioria das pequenas empresas brasileiras transfere ao comportamento individual de cada funcionário uma responsabilidade que, em organizações maiores, é gerenciada por equipes especializadas [TI Inside 2025].

2.3 O Papel do Funcionário na Governança de IA

A Autoridade Nacional de Proteção de Dados (ANPD) publicou, em novembro de 2024, o Radar Tecnológico: Inteligência Artificial Generativa [ANPD 2024], que destaca riscos como coleta de dados sem consentimento claro, geração de conteúdo sintético com dados pessoais inadvertidos e dificuldades em eliminar informações após o refinamento dos modelos [ANPD 2024], reforçando que a responsabilidade pela proteção de dados se distribui por todos os colaboradores que interagem com sistemas de IA. A conscientização dos usuários é o mecanismo de prevenção mais eficaz disponível [CERT.br 2024], posição corroborada pela literatura internacional, que aponta o erro humano como responsável por 74% de todas as violações de dados [IJSRA 2024]. A literatura sobre governança organizacional reforça que, na ausência de frameworks éticos estruturados, como ocorre na maioria das pequenas empresas brasileiras, o funcionário consciente dos riscos do Shadow AI passa a atuar como camada primária de proteção [Administrative Sciences 2024].

A partir desse referencial, a metodologia a seguir organiza os achados em categorias de boas práticas.

3. Metodologia

Este trabalho adota a pesquisa bibliográfica como metodologia, de caráter qualitativo e exploratório. Foram priorizadas fontes oficiais, normas ISO/IEC 42001:2023 e IEEE 7002-2022, Lei nº 13.709/2018 (LGPD), publicações da ANPD e do CERT.br, e publicações brasileiras e internacionais especializadas no período de 2020 a 2025.

A partir da análise temática dessas fontes, foram identificados os principais riscos associados ao uso corporativo desgovernado de ferramentas de IA na realidade brasileira, agrupados em três categorias recorrentes: (a) exposição de dados sensíveis; (b) Shadow AI; (c) lacunas de governança em pequenas empresas. Sobre essa base, foram selecionadas e organizadas as práticas mais relevantes e aplicáveis ao cotidiano de funcionários de pequenas empresas sem formação técnica em segurança da informação, resultando no guia apresentado na seção 4.

4. Resultados: Guia de Boas Práticas

O guia está organizado em quatro categorias, cobrindo os riscos identificados no referencial teórico e orientando o funcionário quanto a comportamentos seguros no uso cotidiano de ferramentas de IA.

4.1 Compreendendo o Risco: O Que Acontece com os Dados Inseridos na IA

Antes de utilizar qualquer ferramenta de IA no ambiente corporativo, o colaborador deve compreender que plataformas abertas podem armazenar os dados inseridos para treinar seus modelos e que, uma vez enviados, esses dados não podem ser recuperados ou excluídos com garantia [Wachter et al. 2017]. Usar uma ferramenta de IA pessoal para processar informações da empresa equivale a enviá-las a um terceiro sem contrato de confidencialidade [Fast Company Brasil 2024], configurando potencial infração à LGPD [Brasil 2018; Revista do TCU 2024; RBDCivil 2020].

4.2 Dados que Não Devem ser Inseridos em Ferramentas de IA Abertas

Não devem ser inseridos em plataformas abertas de IA: dados pessoais de clientes, fornecedores ou colaboradores (nomes, CPFs, e-mails, dados bancários); informações financeiras da empresa (resultados, contratos, orçamentos, margens); código-fonte,

documentação técnica ou propriedade intelectual interna; credenciais de acesso, senhas ou tokens de sistemas corporativos.

4.3 Como Usar Ferramentas de IA de Forma Segura e Comportamentos Cotidianos

A literatura aponta que programas de treinamento em segurança são mais eficazes quando adaptados ao perfil dos colaboradores e atualizados continuamente [IJSRA 2024]. Com base nesse princípio, devem ser adotadas as seguintes práticas: utilizar apenas ferramentas aprovadas pela empresa e consultar o setor de TI na ausência de política definida; substituir previamente nomes reais, valores e identificadores por dados fictícios ao usar IA para redigir textos, podendo ferramentas como o Microsoft Presidio automatizar esse processo [Microsoft 2023]; preferir plataformas corporativas com contrato de privacidade que garantam que os dados não serão usados para treinamento de modelos; avaliar, antes de qualquer tarefa, se ela envolve dados sensíveis; relatar ao setor de TI qualquer suspeita de vazamento; e manter-se atualizado sobre as políticas de privacidade das ferramentas utilizadas, pois elas mudam com frequência [ANPD 2024].

4.4 Construindo uma Cultura Organizacional de Segurança

O padrão IEEE 7002-2022 orienta que a privacidade deve ser considerada em todas as etapas do uso de sistemas que processam informações [IEEE 2022]. A adoção responsável de IA exige comunicação transparente e envolvimento de todos os níveis da organização na definição de políticas de uso [Administrative Sciences 2024]. A Samsung proibiu o uso do ChatGPT em 2023 após vazamento de código-fonte por funcionários [Bloomberg Línea Brasil 2023], ilustrando que, sem políticas claras, o funcionário torna-se o elo mais vulnerável. Cada colaborador consciente dos riscos do Shadow AI atua como camada de proteção organizacional [Silic et al. 2025], tornando a conscientização individual a medida de governança mais acessível às pequenas empresas brasileiras.

5. Conclusão

O Brasil apresenta alta adoção de IA, ausência de políticas de governança em pequenas empresas e responsabilização organizacional pela LGPD, fatores que tornam o colaborador desinformado o elo mais vulnerável da segurança corporativa. A literatura científica recente confirma que o erro humano é a principal causa de incidentes de segurança da informação [IJSRA 2024], e que a deriva de governança, situação em que políticas existem formalmente mas não se traduzem em comportamentos reais, é o principal mecanismo pelo qual o Shadow AI se propaga nas organizações [Silic et al. 2025].

O guia proposto oferece orientações práticas focadas no principal risco desse contexto: o uso desgovernado de IA por funcionários, capaz de expor dados sensíveis e gerar infrações legais à LGPD, legislação cujos desafios de aplicação ao contexto da IA generativa ainda carecem de regulamentação complementar no Brasil [Revista do TCU 2024; RBDCivil 2020]. Conclui-se que o funcionário consciente dos riscos do Shadow AI pode atuar como uma barreira de proteção eficaz e de baixo custo de implementação.

Como trabalho futuro, sugere-se a aplicação prática do guia em empresas reais, com acompanhamento estruturado para avaliação de impacto na cultura organizacional de segurança.

Nota: Este trabalho foi elaborado com auxílio de ferramenta de IA generativa para revisão textual e organização das ideias, sendo o conteúdo científico, as fontes e as análises de inteira responsabilidade dos autores.

Referências

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Radar Tecnológico: Inteligência Artificial Generativa**. Brasília: ANPD, nov. 2024. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/radar_tecnologico_ia_generativa_anpd.pdf. Acesso em: mar. 2026.

BLOOMBERG LÍNEA BRASIL. Samsung proíbe funcionários de usar o ChatGPT após vazamento de código-fonte. **Bloomberg Línea Brasil**, 2 maio 2023. Disponível em: <https://www.bloomberglinea.com.br/2023/05/02/samsung-proibe-funcionarios-de-usar-o-chat-gpt-apos-vazamento-de-codigo-fonte/>. Acesso em: abr. 2026.

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

CERT.BR. **Fascículo Proteção de Dados**. Cartilha de Segurança para Internet. São Paulo: NIC.br, jan. 2024. Disponível em: <https://cartilha.cert.br/fasciculos/protecao-de-dados/fasciculo-protecao-de-dados.pdf>. Acesso em: mar. 2026.

COMITÊ GESTOR DA INTERNET NO BRASIL. **Guia de Boas Práticas em Inteligência Artificial**. São Paulo: CGI.br, 2021.

FAST COMPANY BRASIL. Conversas privadas no ChatGPT estão aparecendo no Google (e ninguém avisou). **Fast Company Brasil**, set. 2025. Disponível em: <https://fastcompanybrasil.com/tech/conversas-privadas-no-chatgpt-estao-aparecendo-no-goog-e-e-ninguem-avisou/>. Acesso em: mar. 2026.

FAST COMPANY BRASIL. Seus funcionários podem estar vazando segredos corporativos para o ChatGPT. **Fast Company Brasil**, 4 fev. 2026. Disponível em: <https://fastcompanybrasil.com/worklife/seus-funcionarios-podem-estar-vazando-segredos-corporativos-para-o-chatgpt/>. Acesso em: mar. 2026.

IEEE. **IEEE 7002-2022: Standard for Data Privacy Process**. New York: Institute of Electrical and Electronics Engineers, 2022.

OLATUNJI, Ayobami P.; AJIBOLA, Oluwafemi S.; AGUNBIADE, Nafisat O. Leveraging AI-driven training programs for enhanced organizational security awareness. **International Journal of Science and Research Archive**, v. 13, n. 1, p. 301–311, 2024. Disponível em: <https://ijsra.net/sites/default/files/IJSRA-2024-1649.pdf>. Acesso em: abr. 2026. DOI: 10.30574/ijsra.2024.13.1.1649.

ISO/IEC. **ISO/IEC 42001: Information technology — Artificial intelligence — Management system**. Genebra: International Organization for Standardization, 2023.

MICROSOFT. **Presidio: Data Protection and De-identification SDK**. [S. l.]: Microsoft, 2023. Disponível em: <https://microsoft.github.io/presidio/>. Acesso em: abr. 2026.

MURIRE, O. T. et al. Artificial Intelligence and Its Role in Shaping Organizational Work Practices and Culture. **Administrative Sciences**, Basel, v. 14, n. 12, p. 316, 2024. Disponível em: <https://www.mdpi.com/2076-3387/14/12/316>. Acesso em: abr. 2026.

LIMA, Taisa Maria Macena de; SÁ, Maria de Fátima Freire de. Inteligência artificial e Lei Geral de Proteção de Dados Pessoais: o direito à explicação nas decisões automatizadas. **Revista Brasileira de Direito Civil**, Belo Horizonte, v. 26, p. 227-246, out./dez. 2020. Disponível em: <https://rbdcivil.ibdcivil.org.br/rbdc/article/download/584/425>. Acesso em: abr. 2026.

SAMPAIO, Daniel de Oliveira; VITA, Jonathan Barros. Regulação de dados pessoais no Brasil, ChatGPT e inteligência artificial: desafios e propostas. **Revista do TCU**, Brasília, v. 155, n. 1, p. 185–206, 2025. DOI: 10.69518/rtcu.155.185-206. Disponível em: <https://revista.tcu.gov.br/ojs/index.php/RTCU/article/view/2073>. Acesso em: abr. 2026.

SERASA EXPERIAN. **Brasil tem recorde nas tentativas de fraude registradas em janeiro**. São Paulo: Serasa Experian, jan. 2025. Disponível em: <https://www.serasaexperian.com.br/sala-de-imprensa/indicadores/brasil-tem-recorde-nas-tentativas-de-fraude-registradas-em-janeiro-aponta-serasa-experian/>. Acesso em: mar. 2026.

SILIC, Mario; SILIC, Dario; KIND-TRÜLLER, Kathrin. From Shadow IT to Shadow AI: threats, risks and opportunities for organizations. **Strategic Change**, Hoboken, p. 1–16, jun. 2025. DOI: 10.1002/jsc.2682. Disponível em: <https://onlinelibrary.wiley.com/doi/abs/10.1002/jsc.2682>. Acesso em: abr. 2026.

TI INSIDE. Brasil está entre os países que mais usam IA generativa, segundo estudo Google e Ipsos. **TI Inside Online**, 14 jan. 2025. Disponível em: <https://tiinside.com.br/14/01/2025/brasil-esta-entre-os-paises-que-mais-usam-ia-generativa-segundo-estudo-google-e-ipsos/>. Acesso em: mar. 2026.

WACHTER, S.; MITTELSTADT, B.; FLORIDI, L. Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. **International Data Privacy Law**, Oxford, v. 7, n. 2, p. 76–99, 2017.