

BOAS PRÁTICAS

GUIA PRÁTICO PARA O USO RESPONSÁVEL DA INTELIGÊNCIA ARTIFICIAL (IA) GENERATIVA NO DIA A DIA DO SERVIÇO PÚBLICO

Uso consciente para evitar riscos, com ética e segurança

PROTEÇÃO DE DADOS E INFORMAÇÕES



DADOS PESSOAIS E SENSÍVEIS

Evite inserir dados pessoais, sensíveis ou identificáveis. Utilize exemplos fictícios ou informações públicas e anonimizadas.



INFORMAÇÕES SIGILOSAS

Não utilize a IA para tratar informações estratégicas, sigilosas ou protegidas por lei. O uso inadequado pode comprometer a atuação institucional do órgão.

CUIDADOS COM O CONTEÚDO GERADO



REVISÃO HUMANA É INDISPENSÁVEL

A responsabilidade pelo conteúdo é do servidor. A IA não substitui análise técnica, jurídica ou administrativa.



TRANSPARÊNCIA

Sempre que possível, informe que o conteúdo foi produzido com apoio de IA, assegurando clareza sobre sua origem.



ALUCINAÇÕES E VIESES

A IA pode gerar informações incorretas ou reproduzir vieses. Avalie criticamente o conteúdo antes de utilizá-lo.



CONTEÚDO PARA PÚBLICO EXTERNO

Evite o uso direto de IA para comunicações oficiais ou conteúdos destinados ao público externo sem revisão e validação institucional.

OS "3 COMOS"



COMO DEVO FORMULAR MINHA SOLICITAÇÃO À IA?

Use comandos objetivos, sem incluir dados pessoais, sensíveis, sigilosos ou informações internas do órgão.



COMO DEVO USAR A RESPOSTA GERADA PELA IA?

Utilize a resposta apenas como apoio. Verifique informações, ajuste ao contexto institucional e não reproduza o conteúdo automaticamente.



COMO DEVO DECIDIR SE A IA É ADEQUADA PARA ESTA TAREFA?

Evite o uso de IA em decisões estratégicas e atos administrativos. Ela deve servir como apoio, não como substituta do julgamento humano.

TECNOLOGIA E SEGURANÇA



CÓDIGOS E LINKS

Nunca implemente códigos ou divulgue links gerados por IA sem revisão técnica especializada.



SOLUÇÕES INSTITUCIONAIS

Sempre que possível, utilize ferramentas de IA disponibilizadas ou homologadas pelo seu órgão.



REGISTROS E RASTREABILIDADE

Sempre que possível, mantenha registro do uso de IA (finalidade, versão e revisão), especialmente em atividades institucionais.



Quer usar a IA de modo responsável, maximizando benefícios e mitigando riscos? Confira a **Cartilha de IA Generativa** e outras iniciativas em **gov.br/amplia**

RISCOS

PRINCIPAIS RISCOS INSTITUCIONAIS, LEGAIS E SOCIAIS DO USO INADEQUADO DA INTELIGÊNCIA ARTIFICIAL (IA) GENERATIVA NO SERVIÇO PÚBLICO

Uso consciente para evitar riscos, com ética e segurança

ALUCINAÇÕES E DESINFORMAÇÃO



"CRIATIVIDADE SINTÉTICA"

Na ausência de dados confiáveis, a IA pode inventar informações, referências legais inexistentes ou interpretações incorretas.



OBSOLESCÊNCIA

O conhecimento da IA pode estar limitado à data do seu treinamento. Em alguns casos, pode ignorar fatos novos, legislações recentes ou mudanças de contexto que ocorreram após essa data.

IMPACTO: decisões baseadas em informações incorretas ou desatualizadas.

VAZAMENTO DE DADOS E ATAQUES



VAZAMENTO DE DADOS

Informações inseridas em prompts podem ser indevidamente memorizadas ou reproduzidas, gerando risco de vazamento.



USO MALICIOSO DA IA

Ferramentas de IA já são utilizadas para golpes digitais, como phishing (mensagens e páginas falsas), deepfakes (áudios ou vídeos manipulados) e outras formas de engenharia social cada vez mais sofisticadas.

IMPACTO: incidentes de segurança, danos à imagem institucional e ao cidadão.

IMPLICAÇÕES LEGAIS E RESPONSABILIDADE



RISCO JURÍDICO

Conteúdos gerados podem violar a Lei Geral de Proteção de Dados (LGPD), direitos autorais ou normas administrativas.



RESPONSABILIDADE INDELEGÁVEL

A ferramenta não responde por erros. A responsabilidade legal e administrativa permanece com o servidor e o órgão.

IMPACTO: passivo jurídico, responsabilização administrativa e questionamentos por órgãos de controle.

VIESSES E IMPACTOS SOCIAIS



REPRODUÇÃO DE DESIGUALDADES

A IA pode reforçar vieses históricos e discriminações presentes nos dados de treinamento.



FALSA NEUTRALIDADE

Respostas geradas por IA podem parecer neutras e objetivas, mas refletem dados e escolhas humanas. Confiar nelas sem questionamento pode levar a decisões inadequadas ou injustas.

IMPACTO: decisões injustas, exclusão de grupos e perda de legitimidade.

INTEGRIDADE E CONTEXTO



DADOS MANIPULADOS OU INADEQUADOS

O uso de dados falsos ou distorcidos pode comprometer os resultados da IA. É importante considerar a origem das informações para evitar decisões mal fundamentadas.



CONTEXTO BRASILEIRO

A IA pode não compreender a realidade local. Gírias, regionalismos e referências culturais do Brasil podem ser interpretados de forma incorreta.

IMPACTO: decisões desalinhadas com o contexto nacional e perda de qualidade nas políticas públicas.

FALTA DE TRANSPARÊNCIA E CONFIANÇA



OPACIDADE DOS SISTEMAS

Modelos não explicáveis dificultam auditoria, rastreabilidade e prestação de contas, dificultando a compreensão de como decisões e conteúdos foram produzidos.



CETICISMO DO CIDADÃO

O uso pouco transparente da IA pode gerar desconfiança e comprometer a legitimidade das decisões públicas.

IMPACTO: perda de confiança nas decisões públicas, entraves na transparência e aumento de fiscalizações.



Quer usar a IA de modo responsável, maximizando benefícios e mitigando riscos? Confira a **Cartilha de IA Generativa** e outras iniciativas em gov.br/amplia