

7

GUIA DE BOAS PRÁTICAS

Ferramentas Externas de Inteligência Artificial Generativa



Programa de
Transformação
Digital (PTD)

TJDFT

EXPEDIENTE

CONTEÚDO

Secretaria de Tecnologia da Informação — SETI

COORDENAÇÃO EDITORIAL

Comitê de Gestão de Tecnologia da Informação —
CGETI

Comitê Gestor de Segurança da Informação e
Proteção de Dados Pessoais — CGSI

REVISÃO

Núcleo de Revisão e Técnica Normativa — NURTE

PROJETO GRÁFICO E DIAGRAMAÇÃO

Assessoria de Comunicação Social — ACS

7

GUIA DE BOAS PRÁTICAS

Ferramentas Externas de Inteligência Artificial Generativa

1ª Edição

Brasília, 27 de maio de 2024.

TJDFT

COMPOSIÇÃO ADMINISTRATIVA

PRESIDÊNCIA

Waldir Leôncio Júnior / Desembargador Presidente

Eduardo Henrique Rosas / Juiz Auxiliar

Francisco Antonio Alves de Oliveira / Juiz Auxiliar

Adriana Prazeres Salgueiro Reis Vidal / Chefe de Gabinete

Jussara Resende Nogueira / Chefe de Gabinete dos Juízes Auxiliares

Celso de Oliveira e Sousa Neto / Secretário-Geral

PRIMEIRA VICE-PRESIDÊNCIA

Roberval Casemiro Belinati / Desembargador Primeiro Vice-Presidente

Luis Martius Holanda Bezerra Junior / Juiz Auxiliar

Andrea Leonardo Coimbra / Chefe de Gabinete

SEGUNDA VICE-PRESIDÊNCIA

Angelo Passareli / Desembargador Segundo Vice-Presidente

Marília Garcia Guedes / Juíza Auxiliar

Julião Ambrosio de Aquino / Chefe de Gabinete

CORREGEDORIA

Mário-Zam Belmiro Rosa / Desembargador Corregedor

Caio Brucoli Sembongi / Juiz Auxiliar

João Marcos Guimarães Silva / Juiz Auxiliar

Monize da Silva Freitas Marques / Juíza Auxiliar

Lara Maria Costa Rodrigues de Souza / Chefe de Gabinete

Érika Maroja de Medeiros / Secretária-Geral da Corregedoria

TRIBUNAL PLENO

Des. Getúlio de Moraes Oliveira

Des. Cruz Macedo

Des. Waldir Leôncio Júnior

Des. J. J. Costa Carvalho

Des. Jair Soares

Desa. Vera Andrighi

Des. Mário-Zam Belmiro

Des. Angelo Passareli

Des. Roberval Casemiro Belinati

Des. Silvanio Barbosa dos Santos

Des. Sérgio Rocha

Des. Arnaldo Camanho de Assis

Des. Fernando Habibe

Des. João Egmont

Des. Teófilo Caetano

Desa. Nilsoni de Freitas Custódio

Des. Jesuino Rissato

Desa. Simone Lucindo

Des. Alfeu Machado

Desa. Leila Arlanch

Desa. Fátima Rafael

Desa. Maria de Lourdes Abreu

Des. Josaphá Francisco dos Santos

Des. James Eduardo Oliveira

Des. Sandoval Gomes de Oliveira

Des. Esdras Neves Almeida

Desa. Gislene Pinheiro de Oliveira

Desa. Ana Cantarino

Des. Diaulas Costa Ribeiro

Des. Rômulo de Araújo Mendes

Des. Roberto Freitas Filho

Des. Robson Teixeira de Freitas

Desa. Maria Ivatônia Barbosa dos Santos

Des. Hector Valverde Santanna

Desa. Diva Lucy de Faria Pereira

Des. Luís Gustavo Barbosa

Des. Alvaro Ciarlini

Des. Fábio Eduardo Marques

Des. Leonardo Bessa

Des. Arquibaldo Carneiro

Des. Carlos Pires Soares Neto

Des. José Firmo Reis Soub

Des. Renato Rodovalho Scussel

Desa. Carmen Nícea Nogueira Bittencourt

Desa. Lucimeire Maria da Silva

Des. Robson Barbosa de Azevedo

Desa. Sandra Reves Vasques Tonussi

Des. Maurício Silva Miranda

GUIA DE BOAS PRÁTICAS

Ferramentas Externas de Inteligência Artificial Generativa

CONTEÚDO

VISÃO GERAL	4	CONFIABILIDADE DAS INFORMAÇÕES	7
OBJETIVO	4	<i>VERIFICAÇÃO INDEPENDENTE</i>	8
ABRANGÊNCIA	4	<i>CONTEXTO JURÍDICO</i>	8
GLOSSÁRIO	5	<i>RISCOS DE VIÉS</i>	8
BOAS PRÁTICAS	6	<i>RISCOS DE VIOLAÇÃO DE PROPRIEDADE INTELECTUAL</i>	8
PRIVACIDADE DE DADOS	6	SEGURANÇA DE ACESSO	8
<i>NÃO DIVULGUE INFORMAÇÕES RESTRITAS</i>	6	<i>SENHAS FORTES</i>	8
<i>DADOS PESSOAIS SENSÍVEIS</i>	6	<i>AUTENTICAÇÃO DE MÚLTIPLOS FATORES (MFA)</i>	9
<i>UTILIZE REDAÇÕES GENÉRICAS</i>	7	RESPONSABILIDADES DOS USUÁRIOS	10
<i>ANONIMIZAÇÃO DE DADOS</i>	7		
<i>LIMPEZA DE DADOS</i>	7		
<i>RESPEITO À LEGISLAÇÃO DE PROTEÇÃO DE DADOS</i>	7		

VISÃO GERAL

OBJETIVO

O objetivo deste guia é orientar e auxiliar magistrados, servidores, prestadores de serviço e estagiários quanto ao uso responsável, seguro e consciente de ferramentas externas de inteligência artificial generativa, tais como ChatGPT e similares. Tem como foco a padronização, a segurança e a proteção de dados no ambiente do TJDFT.

As orientações divulgadas aqui baseiam-se nas melhores práticas de mercado, nas normas e nas políticas de segurança e proteção de dados implantadas no âmbito do TJDFT.

ABRANGÊNCIA

O presente guia visa nortear o uso de ferramentas externas de inteligência artificial generativa no ambiente do TJDFT decorre da necessidade de:

- ✓ atender ao disposto na Resolução 370 do Conselho Nacional de Justiça — CNJ, de 28 de janeiro de 2021, que institui a Estratégia

Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário — ENTIC-JUD para o período de 2021 a 2026, na qual consta a determinação para que sejam constituídas e mantidas estruturas organizacionais adequadas e compatíveis com a relevância e demanda de TIC, considerando no mínimo, entre outros, o macroprocesso de segurança da informação;

- ✓ atender o que preconiza a Resolução 21 de 8 de novembro de 2016, que dispõe, no âmbito do TJDFT, sobre o Sistema de Gestão de Segurança da Informação — SGSI e a Política Corporativa de Segurança da Informação — PCSI;
- ✓ atender aos dispositivos da Lei 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), que dispõe sobre o tratamento de dados pessoais;
- ✓ mitigar o risco de exposição de dados sensíveis custodiados pelo TJDFT.

GUIA DE BOAS PRÁTICAS

Ferramentas Externas de Inteligência Artificial Generativa

CONTEÚDO

VISÃO GERAL	4	CONFIABILIDADE DAS INFORMAÇÕES	7
OBJETIVO	4	VERIFICAÇÃO INDEPENDENTE	8
ABRANGÊNCIA	4	CONTEXTO JURÍDICO	8
GLOSSÁRIO	5	RISCOS DE VIÉS	8
BOAS PRÁTICAS	6	RISCOS DE VIOLAÇÃO DE PROPRIEDADE INTELECTUAL	8
PRIVACIDADE DE DADOS	6	SEGURANÇA DE ACESSO	8
NÃO DIVULGUE INFORMAÇÕES RESTRITAS	6	SENHAS FORTES	8
DADOS PESSOAIS SENSÍVEIS	6	AUTENTICAÇÃO DE MÚLTIPLOS FATORES (MFA)	9
UTILIZE REDAÇÕES GENÉRICAS	7	RESPONSABILIDADES DOS USUÁRIOS	10
ANONIMIZAÇÃO DE DADOS	7		
LIMPEZA DE DADOS	7		
RESPEITO À LEGISLAÇÃO DE PROTEÇÃO DE DADOS	7		

GLOSSÁRIO

AUTENTICAÇÃO MULTIFATOR (MFA): emprego de dois ou mais fatores para atestar a identidade de um usuário para permissão de acesso a um sistema.

CHATGPT: sigla para *Generative Pre-Trained Transformer* é um modelo de linguagem desenvolvido pela OpenAI, baseado em aprendizagem profunda (*deep learning*), que é um campo da Inteligência artificial.

CONFIABILIDADE DAS INFORMAÇÕES: grau de fidelidade de um dado em relação a realidade.

DADO PESSOAL SENSÍVEL: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

DADOS PÚBLICOS: são dados que não estão sujeitos a limitações válidas de privacidade, segurança ou controle de acesso, reguladas por estatutos.

DADOS RESTRITOS: aqueles submetidos à restrição de acesso público, nos termos da lei.

FERRAMENTA DE INTELIGÊNCIA ARTIFICIAL GENERATIVA: *software* que utiliza algoritmos de inteligência

artificial para criar conteúdo como texto, imagem, ou música, com base em dados de entrada.

LGPD: Lei 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais.

PPD: Política de Privacidade dos Dados das Pessoas Físicas do TJDF (Resolução 9 de 2/9/2020)

PRIVACIDADE DE DADOS: garantia de que os dados estão sendo usados apenas por pessoas autorizadas e para a finalidade pretendida.

SENHA FORTE: conjunto de caracteres de alta complexidade, formado pela combinação de letras maiúsculas, letras minúsculas, números e caracteres especiais (!@#%&*).

USUÁRIOS: pessoas que utilizam os recursos de tecnologia da informação e comunicação do TJDF.

VIÉS: ocorre quando um modelo de IA produz resultados tendenciosos que não correspondem a uma visão equitativa e justa do mundo.

GUIA DE BOAS PRÁTICAS

Ferramentas Externas de Inteligência Artificial Generativa

CONTEÚDO

VISÃO GERAL	4	CONFIABILIDADE DAS INFORMAÇÕES	7
OBJETIVO	4	<i>VERIFICAÇÃO INDEPENDENTE</i>	8
ABRANGÊNCIA	4	<i>CONTEXTO JURÍDICO</i>	8
GLOSSÁRIO	5	<i>RISCOS DE VIÉS</i>	8
BOAS PRÁTICAS	6	<i>RISCOS DE VIOLAÇÃO DE PROPRIEDADE INTELECTUAL</i>	8
PRIVACIDADE DE DADOS	6	SEGURANÇA DE ACESSO	8
<i>NÃO DIVULGUE INFORMAÇÕES RESTRITAS</i>	6	<i>SENHAS FORTES</i>	8
<i>DADOS PESSOAIS SENSÍVEIS</i>	6	<i>AUTENTICAÇÃO DE MÚLTIPLOS FATORES (MFA)</i>	9
<i>UTILIZE REDAÇÕES GENÉRICAS</i>	7	RESPONSABILIDADES DOS USUÁRIOS	10
<i>ANONIMIZAÇÃO DE DADOS</i>	7		
<i>LIMPEZA DE DADOS</i>	7		
<i>RESPEITO À LEGISLAÇÃO DE PROTEÇÃO DE DADOS</i>	7		

BOAS PRÁTICAS

O emprego de ferramentas externas de inteligência artificial generativa no contexto laboral dos colaboradores do TJDFT pode trazer inúmeros benefícios, como a automação de tarefas, pesquisa de jurisprudência e auxílio na redação de documentos. No entanto, é necessário que os colaboradores utilizem a tecnologia com cautela bem como avaliem as limitações e potenciais riscos envolvidos. Assim, faz-se fundamental a adoção de boas práticas para garantir a segurança, a privacidade dos dados e a confiabilidade das informações.

PRIVACIDADE DE DADOS

É importante que o usuário tenha ciência de que as ferramentas de IA Generativa registram e armazenam todas as suas conversas, incluindo qualquer informação sensível que seja fornecida. Acrescenta-se a isso o fato de que essas informações são utilizadas para aprendizado da própria IA, o que promove o compartilhamento com terceiros. Em síntese, os dados coletados podem servir de

entrada/treinamento para aperfeiçoar a ferramenta como um todo, com o risco de que dados internos/sensíveis sejam disponibilizados em interações com outros usuários que não têm qualquer vínculo com o TJDFT.

Não divulgue informações restritas

É vedada a entrada de qualquer informação não pública produzida ou custodiada pelo TJDFT em ferramentas externas de inteligência artificial generativa. Isso inclui *e-mails*, minutas, relatórios, dados processuais, dados pessoais, sobretudo dados corporativos. Lembre-se de que a plataforma pode armazenar as conversas e compartilhar os dados coletados, portanto, mantenha as informações confidenciais em ambientes seguros e restritos.

Dados Pessoais Sensíveis

Esteja ciente de que dados classificados por este Tribunal como sensíveis devem ser tratados com extrema cautela. Em nenhuma hipótese insira esses

GUIA DE BOAS PRÁTICAS

Ferramentas Externas de Inteligência Artificial Generativa

CONTEÚDO

VISÃO GERAL	4	CONFIABILIDADE DAS INFORMAÇÕES	7
OBJETIVO	4	<i>VERIFICAÇÃO INDEPENDENTE</i>	8
ABRANGÊNCIA	4	<i>CONTEXTO JURÍDICO</i>	8
GLOSSÁRIO	5	<i>RISCOS DE VIÉS</i>	8
BOAS PRÁTICAS	6	<i>RISCOS DE VIOLAÇÃO DE PROPRIEDADE INTELECTUAL</i>	8
PRIVACIDADE DE DADOS	6	SEGURANÇA DE ACESSO	8
<i>NÃO DIVULGUE INFORMAÇÕES RESTRITAS</i>	6	<i>SENHAS FORTES</i>	8
<i>DADOS PESSOAIS SENSÍVEIS</i>	6	<i>AUTENTICAÇÃO DE MÚLTIPLOS FATORES (MFA)</i>	9
<i>UTILIZE REDAÇÕES GENÉRICAS</i>	7	RESPONSABILIDADES DOS USUÁRIOS	10
<i>ANONIMIZAÇÃO DE DADOS</i>	7		
<i>LIMPEZA DE DADOS</i>	7		
<i>RESPEITO À LEGISLAÇÃO DE PROTEÇÃO DE DADOS</i>	7		

dados em ferramentas externas. Lembre-se que todo usuário tem o dever de garantir o sigilo dessas informações, bem como o tratamento adequado de acordo com a legislação vigente.

Utilize Redações Genéricas

Ao fazer perguntas ou redigir textos, evite fornecer detalhes específicos que possam identificar indivíduos ou processos. Empregue termos genéricos para proteger a privacidade dos envolvidos.

Anonimização de Dados

Se necessário, anonimize os dados antes de inseri-los nas plataformas, substituindo nomes, números de identificação ou quaisquer outros detalhes identificáveis por informações fictícias.

Limpeza de Dados

Certifique-se de apagar todas as conversas após o uso para reduzir o risco de exposição de dados restritos.

Respeito à Legislação de Proteção de Dados

Atente-se às normas de proteção de dados, em especial, à Política de Privacidade dos Dados das Pessoas Físicas — PPD do TJDFT (Resolução 9 de 2/9/2020) e à LGPD (Lei 13.709, de 14 de agosto de 2018) para garantir que o tratamento de dados seja realizado de modo legal e ético.

CONFIABILIDADE DAS INFORMAÇÕES

Insta salientar que embora as ferramentas de inteligência artificial generativa sejam treinadas com uma vasta variedade de conteúdo, incluindo legislações, doutrinas e jurisprudências, não há garantia de que elas forneçam sempre informações consistentes. Inclusive, não são raros os casos em que essas ferramentas citam jurisprudências falsas que nunca sequer existiram.

Portanto, é fundamental que todo conteúdo produzido por IA Generativa passe por análise minuciosa por parte do usuário a fim de se garantir que as informações apresentadas sejam verídicas,

GUIA DE BOAS PRÁTICAS

Ferramentas Externas de Inteligência Artificial Generativa

CONTEÚDO

VISÃO GERAL	4	CONFIABILIDADE DAS INFORMAÇÕES	7
OBJETIVO	4	<i>VERIFICAÇÃO INDEPENDENTE</i>	8
ABRANGÊNCIA	4	<i>CONTEXTO JURÍDICO</i>	8
GLOSSÁRIO	5	<i>RISCOS DE VIÉS</i>	8
BOAS PRÁTICAS	6	<i>RISCOS DE VIOLAÇÃO DE PROPRIEDADE INTELECTUAL</i>	8
PRIVACIDADE DE DADOS	6	SEGURANÇA DE ACESSO	8
<i>NÃO DIVULGUE INFORMAÇÕES RESTRITAS</i>	6	<i>SENHAS FORTES</i>	8
<i>DADOS PESSOAIS SENSÍVEIS</i>	6	<i>AUTENTICAÇÃO DE MÚLTIPLOS FATORES (MFA)</i>	9
<i>UTILIZE REDAÇÕES GENÉRICAS</i>	7	RESPONSABILIDADES DOS USUÁRIOS	10
<i>ANONIMIZAÇÃO DE DADOS</i>	7		
<i>LIMPEZA DE DADOS</i>	7		
<i>RESPEITO À LEGISLAÇÃO DE PROTEÇÃO DE DADOS</i>	7		

precisas, livres de vieses e que não haja violação de propriedade de intelectual.

Verificação Independente

Não confie apenas nas informações fornecidas por ferramentas de inteligência artificial generativas. Sempre faça verificações independentes de jurisprudência, leis e regulamentos relevantes.

Contexto Jurídico

Convém ressaltar que as ferramentas de inteligência artificial generativas não podem substituir a experiência e o julgamento humano, ou seja, não podem desempenhar as funções que competem ao profissional de direito. Lembre-se de que tais ferramentas não possuem conhecimento atualizado, além de que a interpretação jurídica pode variar. Dessa forma, utilize-a apenas como uma ferramenta de apoio, nunca como fonte única e irrefutável.

Riscos de Viés

Esteja consciente de que os algoritmos de inteligência artificial generativa podem conter vieses em seu treinamento, o que pode afetar a

objetividade e precisão de suas respostas. Assim, analise criticamente as informações fornecidas, especialmente quando se tratar de questões delicadas ou controversas, de modo a assegurar que o conteúdo produzido seja justo, imparcial, ético e livre de preconceitos.

Riscos de Violação de Propriedade Intelectual

Considerando que a base de dados usada para treinamento da ferramenta pode conter elementos que não são de domínio público, esteja atento antes de reproduzir o conteúdo gerado por IA (textos, imagens etc), verifique sempre se há indícios de plágio ou violação de propriedade intelectual/direitos autorais de terceiros.

SEGURANÇA DE ACESSO

Senhas Fortes

Proteja o acesso às plataformas com senhas fortes e altere-as regularmente, ou sempre que houver indícios de comprometimento. Nunca compartilhe suas senhas com terceiros, nem as reutilize.

GUIA DE BOAS PRÁTICAS

Ferramentas Externas de Inteligência Artificial Generativa

CONTEÚDO

VISÃO GERAL	4	CONFIABILIDADE DAS INFORMAÇÕES	7
OBJETIVO	4	<i>VERIFICAÇÃO INDEPENDENTE</i>	8
ABRANGÊNCIA	4	<i>CONTEXTO JURÍDICO</i>	8
GLOSSÁRIO	5	<i>RISCOS DE VIÉS</i>	8
BOAS PRÁTICAS	6	<i>RISCOS DE VIOLAÇÃO DE PROPRIEDADE INTELECTUAL</i>	8
PRIVACIDADE DE DADOS	6	SEGURANÇA DE ACESSO	8
<i>NÃO DIVULGUE INFORMAÇÕES RESTRITAS</i>	6	<i>SENHAS FORTES</i>	8
<i>DADOS PESSOAIS SENSÍVEIS</i>	6	<i>AUTENTICAÇÃO DE MÚLTIPLOS FATORES (MFA)</i>	9
<i>UTILIZE REDAÇÕES GENÉRICAS</i>	7	RESPONSABILIDADES DOS USUÁRIOS	10
<i>ANONIMIZAÇÃO DE DADOS</i>	7		
<i>LIMPEZA DE DADOS</i>	7		
<i>RESPEITO À LEGISLAÇÃO DE PROTEÇÃO DE DADOS</i>	7		

Autenticação de Múltiplos Fatores (MFA)

Sempre que disponível, habilite a autenticação de múltiplos fatores para adicionar uma camada extra de segurança ao acesso.

GUIA DE BOAS PRÁTICAS

Ferramentas Externas de Inteligência Artificial Generativa

CONTEÚDO

VISÃO GERAL	4	CONFIABILIDADE DAS INFORMAÇÕES	7
OBJETIVO	4	<i>VERIFICAÇÃO INDEPENDENTE</i>	8
ABRANGÊNCIA	4	<i>CONTEXTO JURÍDICO</i>	8
GLOSSÁRIO	5	<i>RISCOS DE VIÉS</i>	8
BOAS PRÁTICAS	6	<i>RISCOS DE VIOLAÇÃO DE PROPRIEDADE INTELECTUAL</i>	8
PRIVACIDADE DE DADOS	6	SEGURANÇA DE ACESSO	8
<i>NÃO DIVULGUE INFORMAÇÕES RESTRITAS</i>	6	<i>SENHAS FORTES</i>	8
<i>DADOS PESSOAIS SENSÍVEIS</i>	6	<i>AUTENTICAÇÃO DE MÚLTIPLOS FATORES (MFA)</i>	9
<i>UTILIZE REDAÇÕES GENÉRICAS</i>	7	RESPONSABILIDADES DOS USUÁRIOS	10
<i>ANONIMIZAÇÃO DE DADOS</i>	7		
<i>LIMPEZA DE DADOS</i>	7		
<i>RESPEITO À LEGISLAÇÃO DE PROTEÇÃO DE DADOS</i>	7		

RESPONSABILIDADES DOS USUÁRIOS

Em que pese todas as recomendações expostas no presente Guia de Boas Práticas: Ferramentas Externas de Inteligência Artificial Generativa, a responsabilidade pela preservação da segurança da informação e dos recursos é de toda a organização e demanda a colaboração de ponta a ponta, do desenvolvedor ao usuário.

Cabe aos usuários:

- ✓ entender, respeitar e fazer cumprir a política de segurança e normas aplicáveis;
- ✓ utilizar as informações apenas para seus propósitos finalísticos;
- ✓ informar imediatamente pelo canal de comunicação da SETI qualquer incidente ou violação de segurança.
- ✓ seguir as recomendações expostas, ficando cientes que caso venham a causar algum dano à instituição ou à terceiros, podem ser responsabilizados civil e penalmente.

SETI
Secretaria de Tecnologia
da Informação

TRIBUNAL DE JUSTIÇA
DO DISTRITO FEDERAL
E DOS TERRITÓRIOS

TJDFT