ChatTCU

GUIA DE USO DE INTELIGÊNCIA ARTIFICIAL GENERATIVA NO TRIBUNAL DE CONTAS DA UNIÃO **(TCU)**

INTRODUÇÃO

Bem-vindo ao guia prático, uma bússola para a **exploração ética e responsável da inteligência artificial (IA) generativa no Tribunal de Contas da União (TCU)**. Em um mundo onde a tecnologia avança a passos largos, nosso objetivo é sermos pioneiros na adoção de IA, garantindo ao mesmo tempo a segurança, a privacidade e a confiabilidade dos dados. Este guia é o seu mapa para maximizar os benefícios da IA, como a produtividade e a inovação, sem perder de vista a qualidade técnica e a integridade dos nossos valores.

Quem deve ler este guia?

Se você é **servidor, estagiário ou terceirizado** no TCU, este guia é para você. Abrange o uso de aplicativos de IA generativa, tanto internos quanto externos, e é relevante para o desenvolvimento de novas soluções que integram essas tecnologias. As orientações aqui presentes são aplicáveis tanto em dispositivos institucionais quanto pessoais, sempre que utilizados para fins profissionais ou ao manusear dados do TCU.

DEFINIÇÕES BÁSICAS

Inteligência artificial generativa (IA generativa): tecnologia que gera conteúdo, seja texto, áudio, imagens ou vídeo, a partir de comandos ou perguntas realizadas pelo usuário. Pode ser a funcionalidade principal de um aplicativo ou ser incorporada a outros aplicativos.

***Large Language Model* (LLM):** ou grandes modelos de linguagem, é uma grande rede neural artificial, treinada em enormes conjuntos de dados textuais, com o objetivo de entender e gerar texto de maneira natural.

Alucinação: termo usado na IA generativa para descrever respostas fictícias, confiantes e convincentes, que podem ser erroneamente aceitas devido a algum viés, podendo escapar a uma revisão superficial por quem não conhece profundamente do assunto.

ChatTCU e CopilotTCU: soluções aprovadas de IA generativa, desenvolvidas internamente, que mantêm a confidencialidade das informações sigilosas da instituição e cumprem outros requisitos definidos por este guia e demais normativos.

Microsoft Copilot (Windows, 365 e Bing): soluções aprovadas de IA generativa, contratadas de terceiros, que mantêm a confidencialidade das informações sigilosas da instituição e cumprem outros requisitos definidos por este guia e demais normativos.

Plataformas externas de IA generativa: soluções de IA generativa, fornecidas por terceiros, não aprovadas oficialmente. São exemplos desse tipo de solução o ChatGPT e o Gemini, dentre diversos outros disponíveis no mercado.

Prompt: comando de texto dado a um modelo de linguagem de IA para gerar uma resposta ou realizar uma tarefa específica. A qualidade e precisão da resposta podem variar significativamente de acordo com a formulação do prompt.

Viés do modelo: tendências dos conjuntos de dados usados para treinar as ferramentas de IA generativa, que podem influenciar os resultados gerados.

Viés de automação: tendência de aceitar cegamente as sugestões de sistemas automatizados de tomada de decisão, muitas vezes ignorando seu próprio bom senso.

Unidade executiva de TI: unidade da estrutura organizacional do Tribunal com a finalidade de provimento, gerenciamento, operação e sustentação de infraestrutura, soluções e serviços digitais e de tecnologia da informação. Atualmente, esta unidade no TCU é a Secretaria de Tecnologia da Informação e Evolução Digital (Setid).

DIRETRIZES

- Recomenda-se que todo uso de IA generativa durante a realização de trabalhos para o TCU seja sujeito à revisão pela instituição e seja avaliado em função dos princípios deste Guia, dos riscos relacionados e da evolução das boas práticas no uso de IA generativa.

- Espera-se que o uso de IA generativa esteja alinhado com o código de conduta institucional e as políticas de não discriminação do TCU, garantindo que o conteúdo criado seja apropriado e não discriminatório.

- Observa-se que se mantêm aplicáveis ao uso de IA generativa no TCU todos os respectivos normativos que regem suas diversas atividades. Portanto, permanece a plenitude da responsabilidade do autor sobre qualquer documento que tenha produzido, com ou sem uso de IA generativa. Eventuais falhas introduzidas por uso inadequado de IA generativa não afastam a responsabilidade do autor de revisar a produção da IA e assumir a autoria plena e exclusiva do resultado.

- Sugere-se evitar o uso de endereços de e-mail, credenciais e números de telefone do Tribunal para criar conta nas plataformas externas de IA generativa, a fim de que não haja vínculo entre o uso pessoal dessas plataformas e a relação de trabalho na instituição.

- Aconselha-se que apenas dados públicos da instituição sejam enviados às plataformas externas de IA generativa. Eventuais protótipos para avaliação de funcionalidades ainda não disponíveis em ferramentas do Tribunal requerem aprovação da gerência e uso de dados sintéticos ou anonimizados.

- Orienta-se que o uso corporativo e continuado de funcionalidades providas por IA generativa externa seja reportado à unidade executiva de TI, que deverá manter registro para facilitar a governabilidade do uso de IA generativa no TCU.

- Indica-se que a implementação de soluções de IA generativa siga processo de concordância prévia pela Secretaria-Geral correspondente e pela unidade executiva de TI, e seja aprovada em definitivo pela Comissão Gestora de Tecnologia da Informação (CGTI) do TCU.

- Para manter a segurança dos dados e sistemas do Tribunal, sugere-se que sejam avaliados com cautela os riscos de acessar e utilizar plataformas externas de IA generativa ao realizar as atividades institucionais.

- Para manter a confidencialidade das informações sensíveis da instituição, incluindo, dentre outras, informações protegidas por lei, informações pessoais de servidores e cidadãos e material protegido por propriedade intelectual, recomenda-se aos servidores e prestadores de serviços que só insiram informações confidenciais em soluções aprovadas de IA generativa.

- Para proteger servidores e cidadãos e para proteger a instituição de danos à reputação, assim como prevenir quanto à incorrência de viés de modelo e de automação, recomenda-se usar a IA generativa em harmonia com o código de conduta institucional e as políticas de não discriminação do TCU. O conteúdo criado pela IA generativa que seja inapropriado, discriminatório, incorreto devido ao fenômeno da alucinação ou de viés, ou ainda prejudicial aos servidores ou cidadãos, não deve ser usado para fins de trabalho.

- Deve ser evitada a adoção de decisões automatizadas criadas pela IA generativa sem revisão humana.

- Na produção de conteúdo voltado para o público externo, recomenda-se não usar aplicativos de IA generativa que não sejam desenvolvidos pela unidade executiva de TI do Tribunal.

- Sugere-se evitar o uso de IA Generativa para tomada de decisões estratégicas ou fornecimento de informações diretamente para o público externo sem que se passe por processo de revisão humana.

BOAS PRÁTICAS

Para evitar possíveis vazamentos de dados ou incidentes de segurança:

- Não use credenciais da instituição, endereços de e-mail ou números de telefone como login para aplicativos de IA generativa disponíveis publicamente.
- Não implemente nem use código de programação gerado por IA generativa nos sistemas da instituição, sem revisão por especialista de TI.

Para manter a confidencialidade das informações sigilosas da instituição:

- Não insira informações internas da instituição em aplicativos de IA generativa que não seja uma solução aprovada.
- Não insira informações pessoais de servidores, cidadãos ou outros terceiros em nenhum aplicativo de IA generativa que não seja uma solução aprovada.

Para evitar riscos de violação de propriedade intelectual ou de transparência no uso de IA generativa:

- Não use em nenhum material institucional resultados que contenham material que se suspeite que possam estar sob proteção de direitos autorais.
- Nos casos em que se mostrar necessário, sem prejuízo da responsabilização do autor, identifique como tal o conteúdo gerado usando IA generativa.

Para proteger servidores e cidadãos e para proteger a instituição de danos à reputação, e prevenir quanto a incorrência de viés de modelo e de automação:

- Analise os resultados dos aplicativos de IA generativa para garantir que eles atendam aos padrões da Instituição quanto aos princípios de legalidade, equidade, ética e adequação.
- Avalie o conteúdo gerado por IA generativa para garantir que não discrimine indivíduos com base em raça, cor, religião, sexo, nacionalidade, idade, deficiência, estado civil, afiliação política ou orientação sexual.
- Sempre avalie e revise criteriosamente o conteúdo gerado por IA generativa, ainda que o sistema pareça confiável, de modo a garantir o uso de respostas precisas e apropriadas para o fim a que se destina sem a ocorrência do fenômeno da alucinação.
- Considere criteriosamente sua capacidade de identificar eventuais imprecisões de conteúdos gerados antes de usar a IA Generativa. Evite o seu uso se considerar que não conseguirá validar o conteúdo gerado.

Para não incorrer em violação de direitos de propriedade ou autoral:

- Não adote ou reformule a resposta gerada caso haja suspeita de violação de direitos de terceiros.

DIRETRIZES

- As disposições da Política Corporativa de Segurança da Informação (PCSI/TCU, Resolução-TCU nº 342, de 28 de setembro de 2022) também se aplicam no uso de IA generativa.
- Os usuários que não observarem o disposto neste Guia poderão estar sujeitos a medidas disciplinares por descumprimento de normativos da instituição.
- Violações por parte de terceiros contratados podem ser consideradas quebra de contrato. As empresas terceirizadas precisam acatar os dispositivos desse guia para IA generativa, para poderem receber informações sigilosas.
- Incidente de violação das orientações deste Guia será tratado nos termos dos processos apropriados de resposta a incidentes de segurança (Política Corporativa de Segurança da Informação – PCSI/TCU).
- É vedado o desenvolvimento de aplicativos baseados em IA generativa voltado para o público externo que não sejam produzidos pela unidade executiva de TI.
- O TCU se reserva o direito de acessar e monitorar o uso dos aplicativos de IA generativa em qualquer dispositivo da instituição ou que apareça nas redes gerenciadas pela instituição para garantir o uso compatível desses sistemas.
- Casos de não conformidade com este guia deverão ser reportados para a ouvidoria do TCU ou diretamente à Secretaria de Tecnologia da Informação e Inovação Digital (Setid).

DIRETRIZES

Comitê Gestor de Tecnologia da Informação (CGTI), Portaria-TCU nº 386, de 19/02/2019.

Estrutura e Competências da Setid, Portaria Setid nº 2, de 17 de abril de 2023.

Política Corporativa de Segurança da Informação (PCSI/TCU), Resolução-TCU nº 342, de 28 de setembro de 2022.

Política de Governança e Gestão Digital e de Tecnologia da Informação, Resolução-TCU nº 303, de 28 de novembro de 2018.

Cartilha de Governança de Dados do Poder Executivo Federal: https://www.gov.br/governodigital/pt-br/governanca-de-dados/governanca-de-dados.

Levantamento de Inteligência Artificial na Administração Pública: TC 006.662/2021-8.

ISO/IEC 38507:2022 Information technology — Governance of IT — Governance implications of the use of artificial intelligence by organizations - https://www.iso.org/standard/56641.html.

ISO/IEC 23894:2023 Information technology — Artificial intelligence — Guidance on risk management - https://www.iso.org/standard/77304.html

Singapore - Model AI Governance Framework - https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/SGModelAIGovFramework2.pdf

TRIBUNAL DE CONTAS DA UNIÃO