PODER JUDICIÁRIO
SUPERIOR TRIBUNAL MILITAR
PRSTM/SECSTM/DITIN/COGET/SECIA

GUIA

GUIA DE DIRETRIZES E BOAS PRÁTICAS NO USO DE SOLUÇÕES DE INTELIGÊNCIA ARTIFICIAL GENERATIVA NA JUSTIÇA MILITAR DA UNIÃO

1. INTRODUÇÃO

1.1. Bem-vindo ao **Guia de Diretrizes e Boas Práticas no Uso de Soluções de Inteligência Artificial Generativa na Justiça Militar da União**. Este documento tem como objetivo orientar magistrados, servidores, estagiários e prestadores de serviço sobre o uso responsável, seguro, ético e consciente de ferramentas de inteligência artificial (IA) generativa, tais como ChatGPT, Gemini e Copilot, destacando a importância da governança e supervisão adequadas na adoção dessas tecnologias.

1.2. A utilização de ferramentas de IA generativa no contexto laboral da Justiça Militar da União (JMU) pode trazer inúmeros benefícios e oportunidades, como a automação de tarefas repetitivas, pesquisa de jurisprudência e legislação, além de auxiliar na elaboração de documentos. No entanto, é necessário que todos utilizem essas ferramentas com responsabilidade e ética, avaliando as limitações, os potenciais riscos à Segurança da Informação, bem como a privacidade e transparência, além de possíveis vieses nos sistemas de IA. Assim, é fundamental a orientação e a adoção de diretrizes e boas práticas que assegurem a privacidade dos dados, a confiabilidade das informações, a segurança de acesso, a ética e a transparência no uso dessas ferramentas, além de promover a capacitação e a conscientização de todos os envolvidos, bem como a governança e o controle no uso de IA generativa.

1.3. Este guia foi elaborado com base nas melhores práticas de mercado e em conformidade com a Resolução nº 351, de 16 de abril de 2024, que institui a Política de Segurança da Informação da JMU, além de outros normativos relevantes, como a Lei Geral de Proteção de Dados Pessoais (LGPD), as normas da ABNT NBR ISO/IEC e as resoluções do Conselho Nacional de Justiça (CNJ), como a Resolução CNJ nº 332, de 21 de agosto de 2020.

2. ABRANGÊNCIA

2.1. Este guia se aplica a todos os usuários de ferramentas de IA generativa na JMU, incluindo:

- Magistrados;
- Servidores;
- Estagiários;
- Prestadores de serviço;
- Terceirizados.

2.2. As diretrizes e boas práticas apresentadas neste documento são aplicáveis tanto a dispositivos institucionais quanto pessoais, sempre que utilizados para fins profissionais ou no manuseio de dados da JMU.

3. DEFINIÇÕES

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 estar incorporada a outros aplicativos.

Modelo de linguagem de grande escala (LLM): ou grandes modelos de linguagem, é uma grande rede neural artificial, treinada em extensos conjuntos de dados textuais, com o objetivo de entender e gerar texto de maneira natural.

Ferramentas externas de IA generativa: soluções de IA generativa, fornecidas por terceiros, gratuitas ou pagas, que não foram aprovadas oficialmente pela Diretoria de Tecnologia da Informação e Transformação Digital (DITIN). Exemplos incluem o ChatGPT e o Gemini, dentre diversas outras disponíveis no mercado.

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

Prompt: comando de texto fornecido 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: tendências presentes nos conjuntos de dados usados para treinar ferramentas de IA generativa, que podem influenciar os resultados gerados, introduzindo preconceitos ou distorções.

4. DIRETRIZES E BOAS PRÁTICAS

4.1. PRIVACIDADE DE DADOS

É importante que o usuário esteja ciente de que as ferramentas externas de IA Generativa registram e armazenam todas as suas conversas, incluindo informações pessoais ou sensíveis fornecidas. Essas informações podem ser utilizadas para o aprendizado contínuo da IA, tornando-se, assim, públicas e acessíveis a terceiros. Em resumo, os dados coletados podem servir como insumo para aprimorar a ferramenta, com o risco de que dados internos ou sensíveis sejam disponibilizados em interações com outros usuários que não possuem qualquer vínculo com a JMU.

4.1.1. Não divulgue informações restritas

É proibido inserir qualquer informação não pública produzida ou custodiada pela JMU em ferramentas extermas de IA 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.

4.1.2. Tenha atenção com dados pessoais e dados sensíveis

Esteja ciente de que dados pessoais e dados sensíveis devem ser tratados com extrema cautela. Em nenhuma hipótese insira esses 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 Lei Geral de Proteção de Dados Pessoais - LGPD (Lei nº 13.709, de 14 de agosto de 2018) e a Política de Governança Arquivística, da Informação, dos Dados e do Conhecimento, no âmbito da JMU (Resolução nº 340, de 27 de novembro de 2023).

4.1.3. Use redações genéricas

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

4.1.4. Anonimize os dados pessoais e dados sensíveis

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

4.2. CONFIABILIDADE DAS INFORMAÇÕES

As ferramentas de IA generativa podem produzir respostas que aparentam ser precisas e confiáveis, mas que nem sempre refletem a realidade. Devido à natureza probabilística desses modelos, existe o risco de "alucinações", nas quais a IA gera informações incorretas ou fictícias que podem parecer como verdadeiras para não especialistas no assunto.

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, precisas, livres de vieses e que não haja violação de propriedade intelectual ou direitos autorais de terceiros.

4.2.1. Revise as informações geradas

Confirme sempre as informações geradas pela IA consultando fontes oficiais ou especialistas na área. Você é o responsável por qualquer documento que tenha produzido, com ou sem o 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.

4.2.2. Cuidado com alucinações

Esteja consciente de que os algoritmos de IA generativa podem conter viéses em seu treinamento, o que pode afetar a objetividade e precisão de suas respostas. Analise criticamente as informações fornecidas, especialmente quando se tratar de questões delicadas ou controversas, para assegurar que o conteúdo produzido seja justo, imparcial, ético e livre de preconceitos.

4.2.3. Evite riscos de violação de propriedade intelectual

Considerando que a base de dados usada para treinamento das ferramentas de IA generativa 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 ou direitos autorais de terceiros.

4.2.4. Evite automatizações sem revisão humana

Deve ser evitada a adoção de decisões automatizadas criadas pela IA generativa sem revisão humana. Além disso, recomenda-se evitar o uso de IA generativa para tomada de decisões estratégicas ou fornecimento de informações diretamente ao público externo sem que se passe por processo de revisão humana.

4.2.5. Não implemente código sem revisão especializada

Não implemente e nem utilize código de programação gerado por IA generativa nos sistemas da JMU, sem a revisão por especialista de TI.

4.3. SEGURANÇA DE ACESSO

Garantir a segurança no acesso às ferramentas externas de IA generativa é fundamental para proteger os sistemas da JMU contra ameaças cibernéticas. O uso inadequado ou descuidado pode expor dados e comprometer a integridade das informações institucionais.

4.3.1. Use senhas fortes

Proteja o acesso às ferramentas externas de IA generativa com senhas fortes e altere-as regularmente ou sempre que houver indícios de comprometimento. Nunca compartilhe suas senhas com terceiros, nem as reutilize em outros serviços. Em nenhuma hipótese utilize a mesma senha dos sistemas internos da JMU.

4.3.2. Habilite a autenticação de múltiplos fatores

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

4.3.3. Não utilize credenciais institucionais

Evite o uso de credenciais institucionais, como endereços de e-mail ou números de telefone da JMU, como login para ferramentas externas de IA generativa. Isso evita a criação de vínculo entre o uso pessoal dessas plataformas e a relação de trabalho na instituição. Recomenda-se o uso de contas pessoais ao criar contas em plataformas externas de IA generativa.

4.4. ÉTICA E TRANSPARÊNCIA

É fundamental que o uso de ferramentas de IA generativa seja pautado pela ética e transparência. Espera-se ainda que o uso da IA generativa esteja alinhado com o Código de Ética e a Política de Prevenção e Enfrentamento do Assédio Moral, do Assédio Sexual e da Discriminação para a JMU.

4.4.1. Atenda aos princípios éticos da instituição

Certifique-se de que o uso de IA generativa esteja alinhado com o Código de Ética da JMU.

4.4.2. Seja transparente no uso de IA generativa

Seja transparente em relação ao uso de IA generativa nas atividades profissionais, informando quando decisões ou conteúdos foram auxiliados por essas ferramentas.

4.4.3. Evite danos à reputação da JMU

Para proteger servidores, cidadãos e a instituição de danos à reputação, bem como prevenir a ocorrência de possíveis vieses, recomenda-se utilizar a IA generativa em conformidade com a Política de Prevenção e Enfrentamento do Assédio Moral, do Assédio Sexual e da Discriminação para a JMU (Resolução n° 333, de 22 de agosto de 2023). Conteúdo criado pela IA generativa que seja inapropriado, discriminatório, incorreto devido a alucinações ou vieses, ou que possa ser prejudicial aos servidores ou cidadãos, não deve ser utilizado para fins de trabalho.

4.5. GOVERNANÇA E CONTROLE NO USO DE IA GENERATIVA

A governança e o controle no uso de IA generativa são essenciais para garantir que essas ferramentas sejam utilizadas de forma alinhada aos objetivos e valores da JMU, além de permitir o monitoramento e a mitigação de riscos associados.

4.5.1. Reporte o uso corporativo de IA generativa

O uso corporativo e contínuo de funcionalidades providas por ferramentas externas de IA generativa deve ser reportado à DITIN. Isso permite manter um registro centralizado do uso de soluções de IA externas, conforme previsto na Política de Gestão de Ativos de Tecnologia da Informação e Comunicação da JMU (PGATIC/JMU), regulamentada pelo Ato Normativo nº 743, de 26 de abril de 2024. A medida visa ajudar a organização a proteger os ativos de TIC, identificando riscos e vulnerabilidades e implementando mecanismos de segurança para assegurar sua integridade.

4.5.2. Colabore com a DITIN na avaliação de riscos

A DITIN pode avaliar e mitigar os riscos associados ao uso de IA, como a dependência excessiva de fornecedores externos ou a introdução de vulnerabilidades nos sistemas. Forneça as informações necessárias para essa avaliação e siga as orientações recebidas.

4.6. CAPACITAÇÃO E CONSCIENTIZAÇÃO

A educação contínua é vital para acompanhar a evolução das tecnologias de IA e compreender seus impactos no ambiente de trabalho. A capacitação permite que os usuários utilizem as ferramentas de forma eficaz e segura, enquanto a conscientização promove uma cultura de responsabilidade e ética no uso da IA.

4.6.1. Esteja atento aos normativos

Mantenha-se informado sobre mudanças nas políticas, normas e regulamentações relacionadas à IA, tanto internas quanto externas à JMU.

4.6.2. Participe de programas de capacitação Engaje-se regularmente em programas de treinamento e workshops oferecidos pela JMU sobre o uso seguro e ético da IA.
4.6.3. Compartilhe boas práticas Colabore com colegas para disseminar conhecimentos e experiências positivas no uso de IA, promovendo um ambiente de aprendizagem colaborativa.

5. RESPONSABILIDADES DOS USUÁRIOS

5.1. As disposições da Política de Segurança da Informação da Justiça Militar da União (Resolução nº 351, de 16 de abril de 2024) também se aplicam no uso de IA generativa.

5.2. Os usuários que não observarem o disposto neste guia poderão estar sujeitos a medidas disciplinares por descumprimento de normativos da instituição.

5.3. Violações por parte de terceiros contratados podem ser consideradas quebra de contrato. As empresas terceirizadas precisam acatar os dispositivos deste guia para IA generativa, para poderem receber informações sigilosas.

5.4. É vedado o desenvolvimento de aplicativos baseados em IA generativa voltado para o público externo que não sejam produzidos ou validados pela DITIN.

5.5. O STM 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.

5.6. Casos de não conformidade com este guia deverão ser reportados para a ouvidoria da JMU ou diretamente à DITIN.

5.7. Os casos não previstos neste guia, relacionados ao uso de IA, serão resolvidos pela área competente da DITIN.

6. REFERÊNCIAS

BRASIL. Conselho Nacional de Justiça. **Resolução CNJ nº 332, de 21 de agosto de 2020**. Dispõe sobre a implementação de inteligência artificial no âmbito do Poder Judiciário. Brasília: Diário da Justiça Eletrônico, 2020.

BRASIL. Superior Tribunal Militar. **Ato Normativo nº 743, de 26 de abril de 2024**. Institui a Política de Gestão de Ativos de Tecnologia da Informação e Comunicação da Justiça Militar da União (PGATIC/JMU). Boletim da Justiça Militar, Poder Judiciário, Brasília, DF, n. 17, p. 1158, 3 maio 2024.

BRASIL. Superior Tribunal Militar (STM). **Resolução n° 333, de 22 de agosto de 2023**. Estabelece a Política de Prevenção e Enfrentamento do Assédio Moral, do Assédio Sexual e da Discriminação para a Justiça Militar da União e institui a Comissão de Prevenção e Enfrentamento do Assédio Moral, do Assédio Sexual e da Discriminação da Justiça Militar da União (COMPREV). Boletim da Justiça Militar, Poder Judiciário, Brasília, DF, n. 34, pág. 2226, 1 set. 2023.

BRASIL. Superior Tribunal Militar (STM). **Resolução n° 340, de 27 de novembro de 2023**. Institui a Política de Governança Arquivística, da Informação, dos Dados e do Conhecimento, no âmbito da Justiça Militar da União. Boletim da Justiça Militar, Poder Judiciário, Brasília, DF, n. 47, pág. 3140, 1º dez. 2023.

BRASIL. Superior Tribunal Militar. **Resolução nº 351, de 16 de abril de 2024**. Institui a Política de Segurança da Informação da Justiça Militar da União. Boletim da Justiça Militar, Poder Judiciário, Brasília, DF, n. 16, p. 104, 26 abril 2024.

BRASIL. Superior Tribunal Militar. **Código de ética dos servidores da Justiça Militar da União**. 2. ed. Brasília: Superior Tribunal Militar, 2015. 27 p. (Série Legislação; 4). Publicação organizada pela Diretoria de Documentação e Gestão do Conhecimento.

BRASIL. Tribunal de Contas da União. **Guia de uso de inteligência artificial generativa no Tribunal de Contas da União (TCU)**. Brasília: TCU, 2024. Disponível em: https://portal.tcu.gov.br/guia-de-uso-de-inteligencia-artificial-generativa-no-tribunal-de-contas-da-uniao-tcu.htm. Acesso em: 12 nov. 2024.

BRASIL. Tribunal de Justiça do Distrito Federal e dos Territórios. **Guia de boas práticas: ferramentas externas de inteligência artificial generativa**. Brasília: TJDFT, 2024. Disponível em: https://www.tjdft.jus.br/institucional/imprensa/noticias/imagens-e-arquivos-2024/07_guia-boas-praticas.pdf. Acesso em: 12 nov. 2024.