Nota Técnica TJSC nº 01/2026

Cuidado com o Prompt Injection no uso da Inteligência Artificial

Instruções escondidas em documentos podem tentar enganar a IA.
Saiba reconhecer, prevenir e agir — a decisão é sempre humana.

1 O QUE É?

Prompt injection é um truque: alguém esconde comandos disfarçados dentro de peças, anexos, e-mails ou documentos para enganar a ferramenta de IA — fazendo-a omitir argumentos, distorcer resumos, simular conclusões ou sugerir decisões fora da finalidade real.

COMO O GOLPE SE ESCONDE

Texto invisível
fonte branca, transparente ou minúscula

Caracteres ocultos
largura zero e símbolos invisíveis

Metadados e comentários
em PDF, DOCX e RTF

Legendas de imagens
e textos fora da área visível

OCR induzido a erro
ordenação proposital de palavras

Comandos codificados
Base64, hexadecimal e similares

INSERIR COMANDOS OCULTOS TEM CONSEQUÊNCIAS

Litigância de má-fé
Alterar a verdade dos fatos ou usar o processo para fim ilegal.

art. 80 e 81 do CPC

Ato atentatório à justiça
Criar embaraços e não expor os fatos conforme a verdade.

art. 77, §2º, do CPC

Fraude processual
Inovar artificiosamente documento para induzir o juiz a erro.

art. 347 do Código Penal

4 VOCÊ ESTÁ PROTEGIDO EM 3 CAMADAS

CAMADA 1
Microsoft 365 Copilot
Filtros automáticos, isolamento dos dados no ambiente do TJSC e proteções que não podem ser desligadas.

CAMADA 2
Medidas da DTI
Tenant em configuração restritiva e testes de resistência a cada nova ferramenta de IA liberada.

CAMADA 3
Conferência humana
Indispensável e indelegável: magistrados e servidores validam todo resultado. A decisão é sempre humana.

5 O QUE FAZER JÁ

- **Prefira o Microsoft 365 Copilot** ambiente institucional seguro; não use soluções externas.
- **Leia o resultado inteiro** e compare sempre com o documento original.
- **Encontrou algo suspeito?** sinalize a ocorrência e registre nos autos.
- **Use os prompts de salvaguarda** do Anexo I ao analisar documentos de terceiros.
- **A IA é apoio** a decisão final é sempre do magistrado ou servidor.
- **Na dúvida, informe a lacuna** nunca deixe a IA preencher com suposições.

Nenhuma proteção técnica substitui a conferência humana.
A última linha de defesa é você.

Base normativa: Res. CNJ nº 615/2025 · Res. GP nº 56/2025 · Res. GP nº 27/2026.
Conheça os manuais e guias de uso de IA na Nuvem do PJSC.

CGIA — Comitê de Governança de IA
Tribunal de Justiça de Santa Catarina
Florianópolis, 2 de junho de 2026