GUIA PRÁTICO

INTELIGÊNCIA ARTIFICIAL

Uso seguro e responsável no CBMPA



IA ajuda.
Quem responde é você.

01 · RESPONSABILIDADE

IA ajuda. Quem responde é você!

USO SEGURO E RESPONSÁVEL

Você assina. Você responde.



A IA já faz parte da rotina: ajuda a redigir, traduzir, resumir, programar e até executar tarefas. Mas ela erra, pode expor dados e também é usada por golpistas. Quem assina, envia ou executa o resultado responde por ele.

Antes de usar o resultado, confira

- **Tirei as informações sensíveis** do prompt?
- **Conferi a resposta** com fontes confiáveis?
- **Limitei o que os agentes de IA podem fazer?**

Entenda as limitações

- Não “sabe” a resposta certa: calcula a mais provável.
- Depende dos dados de treinamento: dados ruins geram respostas ruins.
- Tende a sempre responder, mesmo quando erra.

NO CBMPA

Ofício, parecer técnico ou relatório de ocorrência feito com apoio de IA continua sendo de autoria e responsabilidade de quem o assina.

02 · PRIVACIDADE

Ajuste as configurações de privacidade



USO SEGURO E RESPONSÁVEL

Configure antes de conversar.

Suas conversas com ferramentas de IA podem ser aproveitadas para melhorar o modelo. Se você não quer isso, é preciso conhecer e ajustar as opções de cada ferramenta.

- **Desative o uso das suas interações** para treinar o modelo.
- **Desligue o histórico de atividades**, principalmente se a ferramenta não oferecer a opção anterior.
- **Use chat temporário ou modo anônimo**, quando existir.
- Revise essas opções de tempos em tempos: as ferramentas mudam regras e menus com frequência.

NO CBMPA

Em tarefas de trabalho, use apenas ferramentas e contas autorizadas pela instituição. Ajustar a privacidade de uma conta pessoal não torna seguro enviar informação institucional.

03 · PROTEÇÃO DE DADOS

Não inclua dados sensíveis no prompt



USO SEGURO E RESPONSÁVEL

Se é sensível, não compartilhe.

O que você digita em um chatbot normalmente vai para a empresa que mantém a IA e pode ser usado para treinar o modelo, com o risco de reaparecer em respostas para outras pessoas.

- **Assuma que tudo o que vai para a IA é público.** Pergunte-se: “Eu colocaria isso em um cartaz na rua?”
- **Troque dados reais por termos genéricos**, como “nome”, “CPF”, “senha”, “órgão”, “endereço”.
- Se a tarefa exige o dado real, **não a faça em ferramenta externa**.

NO CBMPA · NÃO ENVIE À IA

Dados de vítimas e pacientes; endereços e coordenadas de ocorrências; dados pessoais de militares e servidores; senhas, chaves, tokens e arquivos .env; IPs, topologia e configurações de servidores; código-fonte; documentos com restrição de acesso.

04 · PROMPTS CONFIÁVEIS

Dê contexto e forneça fontes



USO SEGURO E RESPONSÁVEL

Contexto + fonte = mais controle.

Chatbots geram texto. Sem instruções claras, tendem a produzir respostas erradas ou sem fundamento (alucinações).

Elabore prompts com contexto

- Descreva a tarefa e o resultado esperado.
- Explique o cenário: situação, condições, quem vai ler (comando, público externo, crianças) e o tom (formal, simples).

Em temas específicos, indique a fonte

- Quanto mais técnico o assunto, maior o risco de invenção. Forneça um texto especializado e restrinja a resposta a ele:
- “Com base estritamente na fonte fornecida, responda...”
- “Cite a frase exata da fonte que sustenta cada afirmação.”

NO CBMPA

Para normas e portarias, anexe o texto oficial vigente e peça resposta apenas com base nele, desde que o documento possa ser enviado à ferramenta usada.

05 · CONFERÊNCIA

Faça a IA admitir que não sabe e revise tudo



USO SEGURO E RESPONSÁVEL

A resposta é um rascunho.

Em vez de dizer “não sei”, o chatbot costuma criar uma resposta plausível, que pode estar errada. Dê a instrução antes:

> **“Se faltar informação ou você não tiver certeza, diga que não sabe.”**

Trate a resposta como rascunho

- Usar a resposta sem checar pode levar a decisões erradas, perdas financeiras e riscos à saúde.
- Peça as fontes e confira se são reais e se tratam do assunto.
- Busque outras fontes para validar dados e fatos.
- Veja se está atualizado: prazos, valores e normas mudam.

NO CBMPA

Cite norma, artigo, número de portaria ou estatística só depois de conferir na fonte oficial. Referências inventadas por IA parecem verdadeiras.

06 · REVISÃO E AUTORIA

Limpe a resposta e evite o plágio



USO SEGURO E RESPONSÁVEL

Revise. Atribua. Proteja.

Revise o material gerado antes de compartilhar ou publicar. Uma conferência final protege dados, autoria e a credibilidade do trabalho.

Remova informações sensíveis do resultado

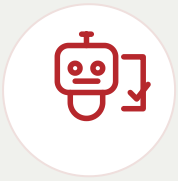
- Imagens, códigos e documentos gerados podem carregar trechos do prompt, metadados ou comentários que não deveriam sair.
- Examine além do conteúdo principal: metadados e comentários de código.
- Retire prompt original, senhas e outros dados sensíveis antes de divulgar.

Evite o plágio

- Modelos são treinados com enormes volumes de texto, inclusive obras protegidas, e podem reproduzir trechos sem citar a fonte.
- Revise e reescreva o texto da IA com suas palavras.
- Cite fonte e autoria ao usar trabalho alheio.
- Se usou IA, informe onde e para qual finalidade.

07 · AUTOMAÇÃO COM CONTROLE

Agentes de IA: limite acesso e decisões



USO SEGURO E RESPONSÁVEL

Menos acesso. Mais supervisão.

Agentes agem em seu nome: leem arquivos, navegam, enviam mensagens. Podem ser manipulados por instruções escondidas em sites, arquivos ou mensagens (prompt injection) ou entender mal um pedido, como apagar todos os e-mails ao ouvir “limpe minha caixa”.

- **Autorize só o necessário:** se só precisa ler, não permita escrever.
- **Defina uma pasta de trabalho** sem informação sensível.
- Não entregue senhas e dados bancários: digite você mesmo.

Exija sua aprovação antes de

- pagamentos e transações; uso de informações sensíveis;
- envio de mensagens ou publicações em seu nome;
- ações irreversíveis, como excluir dados.

NO CBMPA

Nunca conecte agentes a servidores de produção, bancos de dados, e-mail institucional ou repositórios sem autorização e acompanhamento da área responsável.

08 · REGRAS INSTITUCIONAIS

Respeite as regras do CBMPA para uso de IA



USO SEGURO E RESPONSÁVEL

No trabalho, use o canal autorizado.

Pedir para a IA processar conteúdo interno, como código-fonte, atas, relatórios ou dados de cidadãos, pode vazar informação confidencial.

Antes de usar IA no trabalho, informe-se sobre

- quais ferramentas podem ou não ser usadas;
- quais usos são permitidos e quais são proibidos;
- como tratar informações sensíveis e sigilosas.
- **Não use contas pessoais** de ferramentas de IA em tarefas do trabalho.
- Na dúvida sobre uma ferramenta ou um uso, consulte sua chefia imediata antes de usar.

09 · PREVENÇÃO A GOLPES

Desconfie de imagens, áudios, vídeos e comprovantes



USO SEGURO E RESPONSÁVEL

Confirme por outro canal.

Golpistas usam IA para criar deepfakes (rosto e voz de pessoas conhecidas) e imagens falsas, como comprovantes de transferência, para pedir dinheiro, cobrar indevidamente ou espalhar desinformação.

Antes de acreditar, pergunte-se

- Essa pessoa realmente diria isso?
- Envolve dinheiro, vantagem ou dados pessoais?
- Há urgência, ameaça ou apelo emocional?
- Na dúvida, considere falso e confirme por outro canal.

Em pagamentos e compras

- Use a plataforma oficial e confira valor e recebedor.
- Ao receber comprovante, confira o crédito na conta.

NO CBMPA

Pedidos urgentes de dinheiro, acesso ou dados em nome de chefia ou comando, por áudio, vídeo ou mensagem, devem ser confirmados por um segundo canal conhecido.

10 · SAÚDE E BEM-ESTAR

Não troque o profissional de saúde por IA

USO SEGURO E RESPONSÁVEL

IA não substitui cuidado profissional.

Chatbots de uso geral não têm treino específico, usam informações nem sempre confiáveis e não conhecem o seu contexto. Podem dar respostas erradas ou prejudiciais, gerar pânico ou falsa tranquilidade, e não atuam em emergências.

- **Não se autodiagnostique nem se automedique com IA.** Se não se sente bem, procure atendimento profissional.
- **Não faça da IA um terapeuta:** ela não tem emoção, não "entende" você e tende a concordar, o que pode reforçar ideias negativas.
- Conversas com IA não têm sigilo profissional.

NO CBMPA

Em atendimento a ocorrências, siga os protocolos oficiais e a orientação de profissionais habilitados. IA não define conduta clínica nem substitui a regulação.

11 · GUIA DE BOLSO

Resumo: 8 hábitos de uso seguro



USO SEGURO E RESPONSÁVEL

Use IA com responsabilidade.

Antes de usar inteligência artificial, passe por esta lista rápida:

- **1.** Nada sensível no prompt.
- **2.** Só ferramentas e contas autorizadas.
- **3.** Privacidade ajustada: sem treino, sem histórico.
- **4.** Contexto e fonte em todo pedido importante.
- **5.** Resposta é rascunho: confira antes de usar.
- **6.** Agente com pouco acesso e aprovação humana.
- **7.** Desconfie de áudio, vídeo e comprovante.
- **8.** Saúde e ocorrências: protocolos e profissionais, não IA.

LEMBRE-SE

Na dúvida, pare e confirme.