

12 perguntas antes de dar acesso à IA.

O que ela pode consultar? Que ações pode executar? Quem intervém quando algo falha? Leve estas perguntas para a conversa com sua equipe e seus fornecedores.

Escolha uma tarefa da empresa. Os exemplos foram preparados para discussão, não representam testes executados. Cada controle precisa ser definido e verificado na aplicação.

01-04 **Defina o uso.**

Tarefa, dados e ações.

05-08 **Confira os limites.**

Acessos, revisão e testes.

09-12 **Prepare a operação.**

Registros, falhas e responsáveis.

Qual trabalho entra no escopo?

Comece pela tarefa e pelo que a IA precisa para cumpri-la.

01 Qual tarefa a IA faz - e quem decide depois?

Na prática

A IA reúne os itens de um pedido. A equipe comercial ainda precisa conferir preço, quantidade e prazo antes de confirmar a proposta.

O que pedir

Uma descrição da entrada, da saída, dos usos proibidos e do responsável pela próxima decisão. No teste, confira se a sugestão continua pendente até a revisão. Descrever a regra não comprova que o sistema a aplica.

02 Quais dados entram? Quais ficam de fora?

Na prática

Conferir itens e quantidades não exige enviar dados bancários ou observações pessoais do cadastro.

O que pedir

A finalidade de cada campo, inclusive nos anexos. Com dados preparados para o teste, confira o que chega à ferramenta e aparece na resposta. Mascaram nomes não garante anonimato; avalie dados reais antes de usá-los.

Qual trabalho entra no escopo?

Comece pela tarefa e pelo que a IA precisa para cumpri-la.

03 Qual fonte vale para esta tarefa?

Na prática

A pasta contém duas tabelas comerciais. A IA encontra ambas, mas só uma vale para o pedido recebido.

O que pedir

Origem, versão, responsável e uso permitido de cada fonte. Teste a troca de um documento e confira a referência usada na resposta. Se fontes autorizadas divergem, defina quem resolve o conflito. Citar uma fonte não garante acerto.

04 Consultar também permite alterar ou enviar?

Na prática

Consultar estoque, reservar mercadoria e enviar uma proposta são ações diferentes, com consequências diferentes.

O que pedir

A lista de operações e registros permitidos. Teste uma alteração fora do escopo e confira o bloqueio no sistema executor. Uma instrução escrita para a IA agir com cuidado não impõe, sozinha, uma restrição técnica.

O limite resiste a uma exceção?

Peça evidências também para situações em que a IA deve parar ou encaminhar.

05 Em nome de quem a IA acessa os sistemas?

Na prática

Dois atendentes cuidam de carteiras diferentes. Uma consulta não deve revelar pedidos da outra carteira.

O que pedir

Uma matriz de identidades, funções, dados e ações. Teste acessos entre carteiras, a retirada de uma permissão e o conteúdo das respostas geradas. A IA dizer "não tenho acesso" não comprova que a consulta foi bloqueada.

06 E se um anexo tentar mudar a tarefa?

Na prática

O pedido traz um anexo com uma ordem para enviar a lista de clientes a outro endereço. Isso não faz parte da conferência solicitada.

O que pedir

Um teste controlado de instrução indevida em documento, página ou resposta de ferramenta. Confira o bloqueio da ação e o encaminhamento para investigação. Filtros não são infalíveis; permissões e limites de ação continuam necessários.

O limite resiste a uma exceção?

Peça evidências também para situações em que a IA deve parar ou encaminhar.

07 O que a pessoa aprova antes da ação?

Na prática

A equipe revisa uma proposta. Se o destinatário ou o conteúdo mudar depois, aquela aprovação já não cobre o envio.

O que pedir

Uma prévia com conteúdo, destino e efeitos da ação, além do registro da aprovação específica. Teste se uma mudança exige nova revisão. A pessoa precisa de informação, tempo e autoridade para decidir; um botão de confirmação não basta.

08 Quais erros impedem avançar?

Na prática

Um anexo ilegível, um item sem código ou uma fonte contraditória podem exigir complemento, não uma resposta inventada.

O que pedir

Casos comuns e exceções, com resultado esperado antes do teste e resultado observado por versão. Separe erros graves da média. Uma amostra pequena não cobre tudo; mudanças em fontes, modelos ou ferramentas exigem reavaliar os testes pertinentes.

Quem age quando algo sai do previsto?

Combine como investigar, interromper, corrigir e encerrar o uso.

09 O que fica registrado - e quem pode ver?

Na prática

Uma consulta foi negada. A equipe precisa entender o motivo sem copiar o documento inteiro para o registro.

O que pedir

Uma amostra protegida com horário, identidade, ação, resultado e motivo. Confira acesso, retenção e tratamento de campos sensíveis. Registros também precisam de proteção; guardar senhas, credenciais ou dados desnecessários amplia a exposição.

10 Quando a tentativa precisa parar?

Na prática

O estoque está indisponível. Repetir a consulta sem limite aumenta o consumo e deixa pedidos esperando.

O que pedir

Limites de tempo, tentativas e consumo por tarefa, com procedimento alternativo. Teste a interrupção e a comunicação do estado. Antes de repetir uma ação que altera dados, confira o resultado anterior para evitar duplicação. Os limites dependem do processo.

Quem age quando algo sai do previsto?

Combine como investigar, interromper, corrigir e encerrar o uso.

11 Como interromper e corrigir o que já aconteceu?

Na prática

Um endereço de entrega foi alterado incorretamente. Parar novas ações não corrige o pedido que já seguiu para transporte.

O que pedir

Um procedimento ensaiado com responsável, interrupção, conferência dos efeitos e critérios de retomada. Verifique os sistemas envolvidos. Nem toda ação pode ser desfeita; uma mensagem já lida, por exemplo, pode exigir correção e comunicação.

12 Quem responde pelo uso - e pelo encerramento?

Na prática

O piloto termina. Acessos, documentos, registros e cópias podem continuar em sistemas da empresa e de fornecedores.

O que pedir

Responsáveis por revisão e incidentes, prazos de retenção justificados e plano de saída. Inclua revogação de acessos, cópias e evidências do encerramento. Prazos e deveres dependem do contexto e da avaliação técnica e jurídica pertinente.

Da pergunta à decisão

Uma resposta precisa de algo que a sustente.

Para cada pergunta, registre a decisão, a evidência disponível, o responsável e a pendência. Se faltar uma verificação, combine como fazê-la antes de ampliar o uso.

Decisão

O que fica permitido?

Evidência

O que foi conferido?

Responsável

Quem decide e acompanha?

Pendência

O que falta verificar?

Converse com a Gaulett

gaulett.com/contato/

[Prepare seu projeto](#)

[Conheça a validação](#)

Referências para aprofundar

As perguntas aplicam estas referências à rotina de uma empresa. Não representam testes das instituições citadas.

NIST · AI RMF 1.0

<https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf>

NIST · Generative AI Profile

<https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf>

OWASP · AI Agent Security

https://cheatsheetseries.owasp.org/cheatsheets/AI_Agent_Security_Cheat_Sheet.html

OWASP · Prompt Injection

<https://genai.owasp.org/llmrisk/llm01-prompt-injection/>

OWASP · Logging

https://cheatsheetseries.owasp.org/cheatsheets/Logging_Cheat_Sheet.html