Checklist Lantyer para Fornecedores de IA Juridica

Perguntas praticas antes de usar, contratar ou recomendar ferramentas juridicas de inteligencia artificial.

Perguntas para fornecedores

Dados e privacidade

- Quais dados são coletados quando o usuário utiliza a ferramenta?
- Prompts, arquivos enviados, metadados e outputs são armazenados?
- Por quanto tempo cada categoria de dado é retida?
- Há opção de zero data retention? Em quais planos?
- A negativa de retenção está prevista contratualmente?
- O cliente pode solicitar deleção completa?
- O cliente pode exportar dados, prompts, logs e documentos?
- Há DPA compatível com a LGPD?
- O fornecedor atua como operador, controlador ou controlador conjunto em cada fluxo?
- Há tratamento de dados sensíveis? Sob quais salvaguardas?

Treinamento do modelo

- Prompts, arquivos ou outputs são usados para treinamento, fine-tuning, avaliação humana, melhoria de produto ou monitoramento automatizado?
- A resposta está prevista contratualmente?
- Há opt-out real de treinamento?
- O opt-out vale para modelos próprios e de terceiros?
- Dados do cliente podem ser usados para avaliação humana por funcionários ou contratados?
- Como o fornecedor separa dados de clientes diferentes?

Suboperadores e transferência internacional

- Quais suboperadores participam do serviço?
- Em quais países os dados são armazenados ou processados?
- O cliente é notificado antes da troca de suboperador?
- Há cláusulas ou salvaguardas para transferência internacional?
- O fornecedor informa localização de backup e logs?

Segurança da informação

- Há criptografia em trânsito e em repouso?
- Há SSO, MFA e controle de acesso por perfil?
- Há logs exportáveis?
- Há relatório SOC 2, ISO 27001 ou evidência equivalente?
- A ferramenta foi testada contra prompt injection?
- Como lida com sensitive information disclosure?
- Há controle para evitar insecure output handling?
- Há limitação de permissões para agentes ou integrações?
- Há plano documentado de resposta a incidentes?

Arquitetura, RAG e base jurídica

- A ferramenta usa RAG, fine-tuning, base própria, base licenciada ou web aberta?
- Quais bases jurídicas são consultadas?
- A base cobre Direito brasileiro?

- A ferramenta diferencia lei vigente, revogada, projeto, decisão, súmula e opinião?
- Com que frequência a base é atualizada?
- A resposta apresenta fontes verificáveis?
- A ferramenta mostra o trecho usado como base?
- Como o sistema escolhe e ranqueia documentos recuperados?
- A ferramenta indica quando a base é insuficiente?
- Há testes independentes ou relatórios de avaliação?

Contrato, SLA e responsabilidade

- Qual é o SLA de disponibilidade?
- Há suporte técnico em português?
- Há obrigação de notificar incidente em prazo definido?
- O contrato limita responsabilidade? Em quanto?
- Há indenização por vazamento ou falha grave?
- Há direito de auditoria?
- Há obrigação de comunicar mudança de modelo?
- Há obrigação de comunicar mudança de suboperadores?
- Há plano de saída e portabilidade?
- O contrato permite uso com dados sensíveis, segredo profissional ou setor público?

Sinais vermelhos

- "Não podemos responder por segurança por questão de segredo comercial."
- "A política de treinamento está só nos termos gerais."
- "Não há lista de suboperadores."
- "Não há logs exportáveis."
- "Não garantimos atualização da base."
- "A ferramenta sempre responde; não trabalha com recusa."
- "O contrato não prevê notificação de incidente."
- "A demo cita fontes, mas o contrato não promete base jurídica atualizada."

Checklists por perfil

Advogado autônomo

- O conteúdo tem dado de cliente?
- Tem dado sensível?
- Tem estratégia processual?
- Tem documento confidencial?
- A ferramenta é aberta ou contratada com garantias?
- O fornecedor usa meus prompts para treinamento?
- Há retenção dos dados?
- A resposta tem fonte verificável?
- Eu conferi lei, jurisprudência e números?
- Eu conseguiria explicar ao cliente como usei a ferramenta?
- Eu assinaria esse resultado como meu?

Regra pratica: se você não sabe o que acontece com o dado, não coloque dado de cliente.

Escritório de advocacia

- Faça inventário das ferramentas já usadas.
- Crie política interna simples e aplicável.

- Separe usos verdes, amarelos, vermelhos e roxo/preto.
- Proíba dados de cliente em ferramenta aberta.
- Defina protocolo de conferência de fontes.
- Estabeleça quem revisa documentos finais.
- Treine sócios, associados, estagiários e administrativo.
- Inclua regras para timesheet, honorários e transparência.
- Exija DPA, não treinamento, retenção limitada e logs de fornecedores.
- Crie canal para dúvidas e incidentes.

Regra pratica: política que só proíbe cria Shadow AI; política que orienta traz o uso para a governança.

Departamento jurídico

- Envolva jurídico, DPO, segurança, compras, TI e área usuária.
- Avalie dados empresariais estratégicos, não só dados pessoais.
- Verifique suboperadores e transferência internacional.
- Exija plano de incidente e notificação.
- Avalie integração com sistemas internos.
- Teste com casos anonimizados.
- Exija portabilidade e plano de saída.
- Inclua cláusulas sobre treinamento, retenção e confidencialidade.
- Meça produtividade líquida após revisão.
- Documente a decisão de aprovação ou rejeição.

Regra pratica: se a ferramenta entra no fluxo corporativo, ela entra no mapa de risco corporativo.

Procuradorias e setor público

- Distinguir apoio administrativo, apoio redacional, análise jurídica e decisão.
- Verificar base normativa e política institucional.
- Classificar dados de cidadãos, servidores e processos.
- Evitar ferramenta aberta com dados reais.
- Exigir logs, transparência e prestação de contas.
- Garantir revisão humana efetiva.
- Avaliar impacto em direitos fundamentais.
- Considerar controles internos e auditoria.
- Cuidar de procurement público e motivação administrativa.
- Não automatizar decisão sem governança específica.

Regra pratica: no setor público, a régua é mais alta porque o risco não é apenas privado; é institucional e democrático.

Professores e pesquisadores

- Explique que IA não substitui fonte primária.
- Proíba bibliografia inventada.
- Exija declaração de uso quando a instituição assim determinar.
- Diferencie apoio de escrita, apoio de pesquisa e autoria.
- Ensine verificação de fontes.
- Não aceite citação que o aluno não leu.
- Teste ferramentas em temas de Direito brasileiro.
- Oriente sobre dados pessoais em pesquisa.
- Use IA como objeto de crítica, não como oráculo.

- Preserve integridade acadêmica.

Regra pratica: IA pode ajudar a pensar, mas não deve terceirizar autoria, leitura ou responsabilidade intelectual.

Semaforo rapido

Verde: uso geralmente permitido

Exemplos: brainstorming genérico, organização de ideias, revisão linguística de texto sem dados reais, explicação conceitual, roteiro de aula, estrutura inicial de artigo, checklist abstrato.

Condicoes: sem dado de cliente, sem informação confidencial, sem citação jurídica usada sem conferência.

Amarelo: uso condicionado

Exemplos: resumo de documento anonimizado, estrutura de parecer, comparação de argumentos, minuta inicial de contrato simples, apoio em pesquisa preliminar, preparação de reunião.

Condicoes: anonimização adequada, revisão humana, conferência de fontes, ferramenta autorizada quando houver documento real.

Vermelho: uso proibido em ferramenta aberta ou sem contrato adequado

Exemplos: dados de cliente identificável, dados sensíveis, segredo de justiça, estratégia processual, documentos trabalhistas sensíveis, prova, relatório final para cliente, peça processual com jurisprudência, análise de chance de êxito.

Condicoes: ferramenta institucional autorizada, contrato robusto, política interna, revisão humana substantiva, logs e validação de fontes.

Roxo/preto: uso proibido salvo autorização formal e ambiente controlado

Exemplos: bases de clientes, documentos sob segredo de justiça, grandes volumes de dados pessoais, dados de crianças e adolescentes, dados de saúde, material probatório, automação decisória, integração com sistemas internos sensíveis.

Condicoes: autorização formal, ambiente controlado, DPA, análise de risco, segurança, logs, plano de incidente e revisão qualificada.

Validacao minima de fontes

1. Verifique se a fonte existe.
2. Leia o trecho relevante na fonte primária ou base confiável.
3. Confira se a fonte está vigente ou atualizada.
4. Confira se a jurisdição é adequada.
5. Verifique se há entendimento contrário relevante.
6. Analise se o precedente é aplicável ao caso concreto.
7. Registre a conferência quando o risco for alto.
8. Remova qualquer citação não verificada.