Matriz Lantyer de Avaliacao de IA Juridica

30 criterios em cinco blocos: finalidade, qualidade juridica, LGPD, seguranca, contrato, governanca e operacao.

Regra de uso

Qualquer criterio de risco alto nao respondido deve impedir uso sensivel ate que haja evidencia suficiente.

Bloco A: Finalidade, tarefa e dados nucleares

01 - Finalidade de uso

Pergunta: Para que exatamente a ferramenta será usada?

Por que importa: Finalidade define o risco e a governança necessária.

Risco se ignorado: Ferramenta adotada "para tudo" sem dimensionamento de risco por uso.

Evidencia exigida: Documento de casos de uso e limites declarados.

Responsavel: Jurídico / gestor da área | Nivel: Médio

02 - Tipo de tarefa jurídica

Pergunta: A tarefa envolve pesquisa, minuta, contrato, prova, atendimento, gestão ou decisão?

Por que importa: Cada tarefa exige nível diferente de validação.

Risco se ignorado: Validação fraca aplicada a tarefa crítica.

Evidencia exigida: Matriz de funcionalidades por tarefa.

Responsavel: Jurídico sênior | Nivel: Alto

03 - Tipo de dado inserido

Pergunta: Que dado será enviado à ferramenta?

Por que importa: O risco começa no input, não na resposta.

Risco se ignorado: Exposição consumada no primeiro prompt.

Evidencia exigida: Política de classificação de dados.

Responsavel: DPO / jurídico | Nivel: Alto

04 - Dados pessoais

Pergunta: Há informação sobre pessoa identificada ou identificável?

Por que importa: A LGPD pode se aplicar ao tratamento.

Risco se ignorado: Tratamento sem base legal, sem transparência e sem registro.

Evidencia exigida: Mapeamento de tratamento e base legal.

Responsavel: DPO | Nivel: Alto

05 - Dados sensíveis

Pergunta: Há saúde, biometria, origem racial, convicção, vida sexual, dado genético ou similar?

Por que importa: Dados sensíveis exigem cautela e hipóteses legais reforçadas.

Risco se ignorado: Dano grave a titulares e responsabilização agravada.

Evidencia exigida: RIPD quando pertinente, controles adicionais.

Responsavel: DPO / segurança | Nivel: Alto

06 - Sigilo profissional

Pergunta: O conteúdo envolve relação advogado-cliente?

Por que importa: Sigilo é estrutural à advocacia.

Risco se ignorado: Violação de dever estatutário e quebra de confiança do cliente.

Evidencia exigida: Cláusula de confidencialidade, não treinamento, segregação.

Responsavel: Sócio responsável / jurídico | Nivel: Alto

Bloco B: Confidencialidade estendida e cadeia de tratamento

07 - Segredo de justiça

Pergunta: O documento está sob restrição judicial?

Por que importa: Exige ambiente controlado e autorização específica.

Risco se ignorado: Infração processual e disciplinar por exposição de conteúdo restrito.

Evidencia exigida: Política de uso proibido/condicionado.

Responsavel: Jurídico sênior / compliance | Nivel: Alto

08 - Informação estratégica

Pergunta: Há tese, negociação, segredo empresarial ou risco reputacional?

Por que importa: Nem todo risco é dado pessoal; estratégia também vaza.

Risco se ignorado: Vazamento de tese, posição negocial ou segredo de negócio.

Evidencia exigida: Classificação de confidencialidade.

Responsavel: Jurídico / segurança | Nivel: Alto

09 - Retenção de dados

Pergunta: Por quanto tempo prompts, arquivos e outputs são armazenados?

Por que importa: Retenção amplia a janela de incidente e de reuso.

Risco se ignorado: Dado retido vira passivo permanente à espera de incidente.

Evidencia exigida: Política de retenção e deleção.

Responsavel: DPO / segurança | Nivel: Alto

10 - Uso para treinamento

Pergunta: O fornecedor usa dados do usuário para treinar, ajustar ou avaliar modelos?

Por que importa: Pode transformar dado do cliente em insumo do fornecedor.

Risco se ignorado: Informação confidencial incorporada a modelo de terceiro, sem retorno.

Evidencia exigida: Cláusula expressa de não treinamento ou opt-out.

Responsavel: DPO / jurídico contratual | Nivel: Alto

11 - Transferência internacional

Pergunta: Dados saem do Brasil? Para onde?

Por que importa: Pode exigir salvaguardas e análise sob a LGPD.

Risco se ignorado: Tratamento fora do país sem salvaguardas exigíveis.

Evidencia exigida: Mapa de dados e cláusulas de transferência.

Responsavel: DPO / jurídico | Nivel: Alto

12 - Suboperadores

Pergunta: Quais terceiros tratam dados no serviço?

Por que importa: O risco pode estar na cadeia do fornecedor.

Risco se ignorado: Elo invisível da cadeia concentra o risco que ninguém mapeou.

Evidencia exigida: Lista de suboperadores e direito de notificação.

Responsavel: DPO / procurement | Nivel: Alto

Bloco C: Segurança, acesso e auditoria

13 - Controle de acesso

Pergunta: Quem pode acessar a ferramenta e os dados?

Por que importa: Limita exposição interna e externa.

Risco se ignorado: Acesso amplo indevido a documentos e histórico de prompts.

Evidencia exigida: RBAC, MFA, SSO, perfis e permissões.

Responsavel: Segurança / TI | Nivel: Médio/Alto

14 - Logs e auditoria

Pergunta: Há registro de uso, prompts, arquivos e respostas?

Por que importa: Sem logs, não há investigação adequada.

Risco se ignorado: Incidente sem reconstrução possível: erro vira mistério.

Evidencia exigida: Exportação de logs e trilha de auditoria.

Responsavel: Segurança / compliance | Nivel: Alto

15 - Segurança da informação

Pergunta: Como a ferramenta previne vazamento, manipulação e acesso indevido?

Por que importa: LLMs trazem riscos próprios, como prompt injection e divulgação sensível.

Risco se ignorado: Ataques específicos de LLM sem mitigação documentada.

Evidencia exigida: Relatórios de segurança, pentest, controles OWASP.

Responsavel: Segurança / TI | Nivel: Alto

16 - Certificações e evidências

Pergunta: O fornecedor tem certificações ou auditorias relevantes?

Por que importa: Ajuda a separar promessa de evidência.

Risco se ignorado: Decisão de contratação baseada em marketing, não em prova.

Evidencia exigida: ISO 27001, SOC 2, ISO/IEC 42001, quando aplicáveis.

Responsavel: Segurança / procurement | Nivel: Médio

Bloco D: Qualidade jurídica, fontes e supervisão

17 - Validação de fontes

Pergunta: A resposta mostra fontes verificáveis e contextualizadas?

Por que importa: Direito depende de autoridade e fonte.

Risco se ignorado: Citação sem lastro migra para documento final.

Evidencia exigida: Demonstração com fontes, links, trechos e datas.

Responsavel: Jurídico sênior | Nivel: Alto

18 - Atualização da base jurídica

Pergunta: A base está atualizada? Com qual frequência?

Por que importa: Lei e jurisprudência mudam.

Risco se ignorado: Uso de norma revogada ou entendimento superado.

Evidencia exigida: Log de atualização e escopo de cobertura.

Responsavel: Jurídico / fornecedor | Nivel: Alto

19 - Risco de alucinação

Pergunta: Que tipos de erro a ferramenta comete?

Por que importa: Erro jurídico pode gerar dano profissional.

Risco se ignorado: Erro com aparência de precisão passa pela revisão apressada.

Evidencia exigida: Benchmark independente, testes locais, relatório de falhas.

Responsavel: Jurídico / inovação | Nivel: Alto

20 - Capacidade de recusa

Pergunta: A ferramenta sabe dizer que não sabe?

Por que importa: Resposta forçada é perigosa.

Risco se ignorado: Lacuna de base preenchida com invenção plausível.

Evidencia exigida: Testes com perguntas sem base ou com lacunas.

Responsavel: Jurídico / IA | Nivel: Médio/Alto

21 - Explicabilidade mínima

Pergunta: A ferramenta explica o caminho da resposta?

Por que importa: Ajuda na revisão e na responsabilização.

Risco se ignorado: Revisão às cegas, sem saber de onde a resposta veio.

Evidencia exigida: Documentação de método e justificativa.

Responsavel: Jurídico / TI | Nivel: Médio

22 - Supervisão humana

Pergunta: Quem revisa, quando e como?

Por que importa: Revisão decorativa não reduz risco.

Risco se ignorado: Erro aprovado com carimbo humano e responsabilidade integral.

Evidencia exigida: Protocolo de revisão por nível de risco.

Responsavel: Gestor jurídico | Nivel: Alto

Bloco E: Contrato, governança e implementação

23 - Responsabilidade por erro

Pergunta: Quem responde por falha, vazamento ou indisponibilidade?

Por que importa: Marketing não aloca responsabilidade; contrato aloca.

Risco se ignorado: Dano concretizado sem alocação contratual clara.

Evidencia exigida: Termos, SLA, indenização, limitação de responsabilidade.

Responsavel: Jurídico contratual | Nivel: Alto

24 - Integração com fluxo de trabalho

Pergunta: A IA acessa e-mail, drive, GED, CRM ou processo?

Por que importa: Integração aumenta poder e risco.

Risco se ignorado: Superfície de ataque ampliada sem escopos de permissão.

Evidencia exigida: Mapa de integrações e escopos de permissão.

Responsavel: TI / segurança | Nivel: Alto

25 - Vendor lock-in

Pergunta: É possível exportar dados e migrar?

Por que importa: Dependência pode prender a instituição.

Risco se ignorado: Migração cara, lenta ou impossível quando for necessária.

Evidencia exigida: Plano de saída e formato de exportação.

Responsavel: Procurement / TI | Nivel: Médio

26 - Custo total

Pergunta: Qual é o custo real além da licença?

Por que importa: Inclui treinamento, revisão, suporte, integração e auditoria.

Risco se ignorado: Produtividade aparente com custo real oculto.

Evidencia exigida: TCO, proposta detalhada e custos variáveis.

Responsavel: Financeiro / gestor | Nivel: Médio

27 - Ordenamento brasileiro

Pergunta: A ferramenta foi testada no Direito brasileiro?

Por que importa: Jurisdição importa.

Risco se ignorado: Categoria estrangeira importada como se fosse local.

Evidencia exigida: Testes com legislação e jurisprudência brasileiras.

Responsavel: Jurídico sênior | Nivel: Alto

28 - Testes locais

Pergunta: A instituição testou com casos próprios anonimizados?

Por que importa: Demo comercial não prova adequação.

Risco se ignorado: Contratação decidida com base em teatro controlado.

Evidencia exigida: Relatório de piloto, critérios e pontuação.

Responsavel: Inovação / jurídico | Nivel: Alto

29 - Política interna

Pergunta: O uso está coberto por política clara?

Por que importa: Sem política, há improviso e Shadow AI.

Risco se ignorado: Uso clandestino, critérios divergentes e risco invisível.

Evidencia exigida: Política de uso, semáforo e treinamento.

Responsavel: Compliance / DPO | Nivel: Alto

30 - Plano de incidente

Pergunta: O que acontece se houver vazamento, erro ou citação falsa?

Por que importa: Incidente sem plano vira crise.

Risco se ignorado: Crise administrada no improviso, sem papéis definidos.

Evidencia exigida: Playbook de incidente e responsáveis.

Responsavel: Segurança / jurídico / comunicação | Nivel: Alto

Pontuacao local

Correção jurídica

0: Erra conceitos centrais

3: Acerta parte, mas exige forte revisão

5: Resposta juridicamente sólida com revisão normal

Fontes

0: Não apresenta ou inventa

3: Apresenta fontes incompletas

5: Fontes verificáveis, relevantes e atuais

Atualização

0: Usa norma/entendimento desatualizado

3: Atualização incerta

5: Indica data e fonte atualizada

Adequação ao Brasil

0: Importa conceitos estrangeiros

3: Acerta temas gerais

5: Opera bem com Direito brasileiro

Recusa

0: Responde qualquer coisa

3: Recusa raramente

5: Sabe indicar insuficiência de base

Confidencialidade

0: Termos frágeis

3: Garantias parciais

5: Contrato robusto e não treinamento

Segurança

0: Sem evidência

3: Evidência limitada

5: Controles documentados e auditáveis

Logs

0: Não há

3: Logs parciais

5: Logs exportáveis e úteis

Produtividade líquida

0: Piora o fluxo

3: Economiza pouco

5: Economiza tempo após revisão

Integração

0: Risco alto sem controle

3: Integração parcial

5: Integração com escopos e permissões claros

- média abaixo de 3: rejeitar ou limitar a uso experimental;

- média entre 3 e 4: piloto controlado;

- média acima de 4: considerar contratação, se riscos jurídicos e contratuais forem aceitáveis;

- qualquer nota 0 em confidencialidade, segurança ou treinamento com dados deve bloquear uso sensível.