Neural Nets

GUIA GRATUITO · EDIÇÃO 1

PARA SÓCIOS E GESTORES DE PEQUENAS E MÉDIAS EMPRESAS

IA no dia a dia da empresa: o que decidir antes de usar

Um guia para você entender, com calma, onde a IA ajuda, onde ela expõe os dados dos seus clientes e como escolher sem depender da promessa de nenhum fornecedor.

Lucas Cléopas

Engenheiro de IA sênior, mestre em Ciência da Computação pela Unicamp e sócio da NeuralNets

Uma conversa antes do guia

IA para ~~automatizar tudo~~ o que vale a pena na sua empresa.

Quase todo mundo me pergunta qual é a melhor IA. Ou qual é a mais barata. Antes de responder, eu devolvo outra pergunta: o seu problema precisa de IA?

Pesquiso inteligência artificial desde 2018 e coloco IA em produção desde 2021. Nesse tempo, vi muita empresa escolher a ferramenta antes de entender o problema. Ninguém escolhe o melhor martelo antes de saber se existe um prego. Às vezes o problema é de dados, e uma análise simples resolve. Outras vezes a IA é mesmo o caminho, e aí vale fazer direito.

Escrevi este guia para sócios e gestores de pequenas e médias empresas que querem entender o assunto com calma, sem jargão e sem susto. Vou te mostrar onde a IA costuma ajudar, onde ela atrapalha, quais riscos são reais, com números e fontes que você pode conferir, e um modelo de política de uso para adaptar ainda nesta semana.

O passo a passo de ferramentas ficou de fora de propósito. Ferramenta de IA muda de um mês para o outro, e a escolha certa depende dos sistemas da sua empresa e de quem vai revisar o que a IA produz. Esse trabalho eu faço junto com cada empresa, no Diagnóstico Estratégico de IA.

São cinco partes curtas, cada uma com uma pergunta para você levar à conversa com seus sócios. Leia no seu ritmo, que eu vou junto.

Um abraço,
Lucas Cléopas

PARTE 1 · ONDE VOCÊ ESTÁ

A IA já entrou na sua empresa

57% dos funcionários ouvidos dizem esconder o uso de IA no trabalho e apresentar como próprio o que a IA produziu.

O número vem de uma pesquisa da Universidade de Melbourne com a KPMG, publicada em maio de 2025, que ouviu mais de 48 mil pessoas em 47 países, o Brasil entre eles. Quase metade (48%) admitiu já ter colocado informações da empresa em ferramentas públicas de IA, e 66% disseram usar o que a IA entrega sem conferir se está correto.

Na prática, isso tem uma cara conhecida. A pessoa do financeiro descobre que um assistente gratuito monta o resumo do mês em minutos. Alguém do comercial cola a lista de clientes para “organizar os contatos”. O atendimento usa IA para responder reclamações mais rápido. Ninguém faz isso por mal: as pessoas usam porque funciona e porque o trabalho não espera.

Só que, a partir desse momento, dados dos seus clientes passaram por uma conta pessoal, sob termos de uso de consumidor. E o histórico vai embora com o funcionário no dia em que ele sair.

Como a mesma pesquisa mostra, boa parte usa sem conferir o resultado. Proibir quase nunca resolve: quem sentiu o ganho de tempo continua usando, só que escondido. O caminho mais tranquilo é oferecer uma ferramenta aprovada, combinar regras claras e trazer para a luz o que já acontece.

Fonte: Gillespie, N. et al., Trust, attitudes and use of artificial intelligence: a global study 2025, Universidade de Melbourne e KPMG, maio de 2025.

Antes das regras, uma pergunta mais básica →

Sua empresa precisa de IA agora?

Vou ser sincero com você: nem toda empresa precisa de IA neste trimestre. E descobrir isso cedo economiza dinheiro e dor de cabeça.

Comece pelo problema. A ferramenta vem depois. Os sinais abaixo vêm do que eu vejo em projetos de IA, em empresas de tamanhos bem diferentes. Nenhum deles decide a questão sozinho, mas o conjunto costuma apontar o caminho.

Sinais de que sim

- A equipe repete as mesmas tarefas toda semana: responder clientes, conferir planilhas, montar relatórios.
- Pessoas da equipe já usam IA por conta própria, e o ganho de tempo é visível.
- Os clientes fazem as mesmas perguntas todos os dias.
- Informação importante fica espalhada em documentos que ninguém acha.

Sinais de que ainda não

- Os processos ainda não estão escritos nem padronizados.
- O volume é pequeno e o ganho não paga o esforço de implantar.
- Ninguém tem tempo para revisar o que a IA produz.
- O problema é de dados ou de sistema, e uma análise simples resolveria.

Se a maior parte caiu na segunda coluna, tudo bem. A decisão mais inteligente agora pode ser organizar os processos ou olhar os dados com calma. IA aplicada a um processo bagunçado produz bagunça mais rápido, e com cara de trabalho bem feito.

Se caiu na primeira, a próxima pergunta é por onde começar. O conselho que eu mais repito: escolha uma tarefa, meça, acerte, e só depois vá para a próxima.

PARA LEVAR À CONVERSA COM SEUS SÓCIOS

Quem aqui já usa IA no trabalho, em qual conta? E quais três tarefas mais consomem horas da equipe toda semana?

PARTE 2 · COMO A MUDANÇA ACONTECE

Quando a IA certa nem era a mais famosa

Caso real de um projeto que conduzi, contado sem nomes.

Uma empresa precisava extrair informações de milhares de notas fiscais: números, datas, valores e fornecedores. A primeira ideia de quase todo mundo seria mandar cada nota para um modelo de linguagem, desses que conversam, e pedir os campos de volta.

Fazendo as contas, a ideia não parava em pé. Com milhares de documentos, o custo por nota ia pesar no orçamento todo mês. E cada nota levaria dados confidenciais da empresa e dos fornecedores para fora do ambiente que ela controlava.

A solução que levamos para produção foi mais simples: um serviço de OCR do Azure, que lê o texto das imagens e já atendia às regras de conformidade da empresa. A IA generativa entrou num papel menor e muito útil, ajudando a escrever as regras que encontram cada campo dentro do texto lido.

Ponto	Primeira ideia	Solução em produção
Ferramenta	Modelo de linguagem para cada nota	OCR já aprovado, com regras escritas com ajuda da IA
Custo	Cresce a cada documento	Menor
Dados	Saem para um serviço externo	Ficam no ambiente aprovado
Velocidade	Depende de cada chamada	Mais rápida em produção

Conto essa história porque ela resume o que eu defendo. A pergunta certa é qual é o problema. Só depois vem qual ferramenta resolve, e às vezes a melhor resposta é a menos famosa.

Agora, o que a IA faz bem e o que deve ficar com a sua equipe →

O que a IA faz bem, e o que fica com a sua equipe

Modelos de linguagem são muito bons com texto e padrão: escrevem, resumem, reorganizam e comparam. Tropeçam na exatidão de números, prazos e regras. E erram com a mesma segurança com que acertam, sem avisar.

Onde costuma ajudar

- Rascunhos de resposta a perguntas frequentes de clientes, a partir de respostas aprovadas.
- Resumos de reuniões, relatórios e documentos longos.
- Conferência de planilhas, apontando o que não bate.
- E-mails, propostas e comunicados escritos com mais rapidez.

O que fica com a equipe

- Mensagem a cliente enviada sem ninguém ler. A IA não tem todo o contexto, e o que falta vira problema lá na frente.
- Decisões com impacto financeiro, jurídico ou sobre pessoas.
- Números finais sem conferência.

A IA ajuda muito a rascunhar, mas o que vai para o cliente precisa passar pelos olhos de alguém. Atendimento automático só faz sentido quando quatro coisas aparecem juntas: o contexto vem da própria conversa, a solução foi testada, um erro custa pouco e a pessoa sabe que está falando com uma IA. Quando o cliente é antigo e a relação importa, alguém da equipe revisa antes de enviar.

Falo isso por experiência. Na NeuralNets, a gente opera agentes de IA que atendem clientes de clínicas, e cada uma dessas condições foi aprendida no dia a dia.

PARA LEVAR À CONVERSA COM SEUS SÓCIOS

Quais mensagens saem hoje da empresa para clientes, e quem lê cada uma antes de enviar?

PARTE 3 · OS RISCOS QUE QUASE NINGUÉM CONTA

O que os ataques com IA já custam

Quando falo de segurança, muita gente pensa que é assunto de empresa grande. Os números de 2026 mostram que o problema já é comum.

1 em 4

vazamentos maliciosos analisados teve IA nas mãos do atacante, 56% a mais que no ano anterior

US$ 6 mi

foi o custo médio desses vazamentos, cerca de US$ 1 milhão acima da média geral

20%+

das organizações relataram vazamentos que atingiram modelos ou aplicações de IA

Os dados são do relatório Cost of a Data Breach 2026, da IBM com o Ponemon Institute, publicado em julho de 2026, a partir de vazamentos sofridos por 602 organizações entre março de 2025 e fevereiro de 2026. Os ataques com IA foram, na maior parte, falsificação de identidade com deepfake e programas maliciosos feitos com IA. Quando o alvo eram sistemas de IA, as falhas mais comuns estavam ao redor deles: integrações e plug-ins comprometidos (27%) e configurações erradas na nuvem (27%), problemas básicos que custam pouco para corrigir.

Toda empresa guarda dados de terceiros: cadastro de clientes, CPF, contratos, histórico de compras, dados de funcionários. Se esses dados vazam, quem responde ao cliente e perante a Lei Geral de Proteção de Dados é a empresa. E uma empresa pequena tem bem menos estrutura que uma grande para atravessar um incidente desses.

Na prática, pense no e-mail com o boleto “atualizado” de um fornecedor, ou no áudio com a voz de um sócio pedindo um Pix urgente. A IA deixou esses golpes mais baratos e mais convincentes.

Fonte: IBM, comunicado do Cost of a Data Breach Report 2026, 29/07/2026. Valores globais.

Um risco que cresce rápido, porque nasce de uma boa intenção →

O sistema que alguém fez num fim de semana

Você quer um painel para acompanhar os pedidos dos clientes. Alguém da equipe, ou um parente que entende de computador, descreve a ideia numa ferramenta que cria aplicativos com IA. Em poucas horas está pronto e publicado na internet, para todo mundo acessar de casa. Parece ótimo.

A tela abre, o login aparece e os dados carregam, mas nada disso garante que um estranho não consiga ler a mesma tabela sem senha.

45%

dos testes da Veracode com código gerado por IA trouxeram falhas de segurança conhecidas

170+

projetos de uma plataforma popular de criar apps com IA ficaram com o banco de dados aberto, sem login

O primeiro número vem de um estudo de julho de 2025 com mais de 100 modelos de IA e 80 tarefas de programação: a IA entregava código que funcionava, mas em 45% dos testes ele trazia uma falha de segurança conhecida. O segundo é um caso real de 2025, registrado como falha crítica (CVE-2025-48757): faltava uma regra no banco de dados, e qualquer pessoa conseguia ler e alterar as tabelas dos sites gerados em mais de 170 projetos.

Segundo a Veracode, a IA também facilita para atacantes, até os pouco experientes, encontrar e explorar essas falhas. Criar ferramentas internas com IA pode valer a pena; o cuidado é revisar a segurança antes de pôr na internet qualquer uma com dados de clientes.

PARA LEVAR À CONVERSA COM SEUS SÓCIOS

Existe hoje algum sistema, planilha online ou formulário da empresa que ninguém sabe exatamente quem consegue acessar?

Fontes: Veracode, comunicado do 2025 GenAI Code Security Report, 30/07/2025; NVD, CVE-2025-48757, maio de 2025; Superblocks, análise do caso, setembro de 2025.

PARTE 4 · REGRAS QUE PROTEGEM

Conta pessoal ou conta corporativa

Essa diferença parece burocracia até o dia em que alguém sai da empresa levando o histórico de conversas com dados de clientes. A tabela resume o que muda.

Ponto	Conta pessoal	Conta corporativa
Quem controla o acesso	A própria pessoa	A empresa
Uso dos dados para treinar modelos	Depende do plano e da configuração de cada pessoa	OpenAI e Google declaram não usar por padrão
Quando alguém sai	O histórico vai junto	A empresa remove o acesso
Contrato	Termos de consumidor	Termos empresariais

Sobre o treinamento de modelos, fui conferir nas páginas oficiais. A OpenAI informa que, por padrão, não usa os dados dos planos ChatGPT Business e Enterprise para treinar ou melhorar seus modelos. O Google afirma que o Gemini nos aplicativos do Workspace usa o seu conteúdo para responder, mas não para treinar modelos de IA. Nas contas pessoais, isso depende do plano e da configuração escolhida por cada pessoa.

E tem a lei. A LGPD exige que quem trata dados pessoais adote medidas de segurança para protegê-los de acesso indevido (art. 46). Dados de saúde de funcionários, como atestados, são dados sensíveis (art. 5º, II). Colar isso numa conta pessoal de IA tira da empresa o controle sobre onde esses dados ficam e quem os acessa.

Fontes: OpenAI, Business data privacy; Google, privacidade do Gemini no Workspace; ambos consultados em 25/11/2026. Lei 13.709/2018. Este guia não é orientação jurídica.

Ferramenta escolhida, falta combinar o jogo com a equipe →

Um modelo de política de uso

Uma política de uso de IA cabe numa página e responde a quatro perguntas: o que pode, o que não pode, o que nunca entra e quem responde. Deixo aqui um modelo para você usar como ponto de partida e ajustar com seus sócios.

Pode

- Rascunhar e-mails, propostas e comunicados, sempre com revisão.
- Resumir documentos e relatórios sem dados pessoais.
- Organizar textos e planilhas sem dados que identifiquem pessoas.

Não pode

- Usar conta pessoal para trabalho da empresa.
- Enviar ao cliente texto gerado por IA sem revisão.
- Decidir algo financeiro, jurídico ou sobre pessoas só com base na IA.

Nunca entra em ferramenta não aprovada

- CPF, contratos e dados de clientes.
- Dados de funcionários e de saúde.
- Senhas, chaves de acesso e dados bancários, em nenhuma ferramenta.

Quem responde

- Só ferramentas aprovadas pelos sócios.
- Quem usa revisa e responde pelo resultado.
- Dúvidas e incidentes vão para [nome do responsável].

Dois cuidados fazem a política sair do papel. Apresente numa conversa com a equipe, com exemplos da própria empresa, em vez de mandar o arquivo por e-mail. E marque na agenda uma revisão a cada seis meses, porque as ferramentas mudam rápido.

PARA LEVAR À CONVERSA COM SEUS SÓCIOS

Quem, na empresa, vai aprovar as ferramentas e responder às dúvidas sobre IA?

Modelo simplificado, para adaptar e revisar com os sócios. Quando envolver a LGPD, vale a revisão de um advogado.

PARTE 5 · SEU PRÓXIMO PASSO

Desconfie de quem só vende ferramenta

Eu prefiro ensinar a pescar.

Ferramenta de IA muda de um mês para o outro. Quem aprendeu só a usar uma fica sem saída quando ela muda de preço, troca de recurso ou sai do ar. Quando o gestor entende como a IA funciona e onde ela falha, muita decisão passa a ser dele, sem depender de fornecedor.

Também não existe receita única. Uma empresa de 8 pessoas tem gargalos diferentes de uma de 40. Uma usa Google Workspace, a outra Microsoft 365. Uma tem a equipe animada para testar, a outra acabou de perder duas pessoas-chave. Tudo isso muda as respostas que importam: qual tarefa atacar primeiro, se vale assinar alguma coisa ou se o que vocês já pagam resolve, e o que deve continuar exatamente como está.

Tudo o que eu sei dá para explicar, e por isso entrego o raciocínio por escrito, para você aplicar sem depender de mim nem de um produto. Sento com você, entendo como a sua empresa funciona e mostro o caminho que faz sentido. Se a resposta honesta for “ainda não”, eu te digo isso com todas as letras.

PARA LEVAR À CONVERSA COM SEUS SÓCIOS

Se a empresa pudesse resolver um único problema com IA nos próximos 90 dias, qual seria?

Como eu faço isso junto com você →

Diagnóstico Estratégico de IA

É assim que eu te ajudo a dar o primeiro passo com segurança. O diagnóstico é realizado pela NeuralNets e conduzido por mim, do começo ao fim.

01

Questionário de diagnóstico

Cerca de 15 minutos, preenchido antes da sessão.

02

Sessão de diagnóstico

90 minutos, online, com roteiro fixo.

03

Relatório de diagnóstico

Assinado e entregue em até 48 horas úteis.

04

Acompanhamento de 30 dias

Para ver o que foi aplicado e ajustar.

No relatório, você recebe as oportunidades priorizadas, com estimativa de ganho e de custo; as ferramentas indicadas e o motivo de cada escolha; os riscos com dados que existem hoje na empresa; o que não automatizar; e um plano para 30, 60 e 90 dias. Quando houver algo a implementar, comparo pelo menos duas opções pelos mesmos critérios, e a decisão fica com você.

GARANTIA

Se o relatório não trouxer pelo menos duas oportunidades concretas com estimativa de ganho, eu devolvo o valor.

R$ 990 de lançamento, pagamento único, nas 20 primeiras vagas. Depois, R$ 1.200. A NeuralNets realiza o diagnóstico e emite a nota fiscal.

Antes de decidir, vamos conversar.

Uma conversa curta e gratuita pelo WhatsApp, para entender o que faz sentido no seu caso.

WhatsApp (98) 98491-9854 · lucascleopas.com.br

Prazer, eu sou o Lucas



Sou engenheiro de IA sênior. Pesquiso inteligência artificial desde 2018 e coloco IA em produção desde 2021. Hoje atuo em consultoria, atendendo clientes corporativos, e sou sócio da NeuralNets, a empresa que realiza os diagnósticos.

Agentes de IA em sistemas corporativos

Sinch, centro de excelência em IA

Segurança de modelos de IA na pesquisa

Na consultoria, liderei de ponta a ponta a arquitetura de um sistema com vários agentes de IA para um cliente industrial, do escopo e do roteiro técnico até o alinhamento com as áreas de negócio. O sistema consulta bancos de dados e documentos da empresa e responde com base nessas fontes.

Antes disso, passei mais de três anos no centro de excelência em IA da Sinch, empresa global de comunicação em nuvem. Lá comparei modelos de linguagem para reconhecer intenção, analisar sentimento e transcrever voz, ajudando a escolher a tecnologia certa para cada restrição de custo e qualidade. Também entreguei projetos de classificação de conteúdo, geração de textos e assistentes para desenvolvedores.

Na NeuralNets, a gente opera agentes de IA que atendem os clientes de clínicas. É desse dia a dia que vem boa parte do que eu sei sobre os riscos de colocar uma IA para conversar com o cliente de alguém.

Sou bacharel em Engenharia da Computação pela UFMA e mestre em Ciência da Computação pela Unicamp, com pesquisa sobre a segurança de modelos de aprendizado de máquina contra ataques de envenenamento de dados. Levo essa bagagem para cada empresa que analiso: saber o que a IA faz de verdade, onde ela falha e como escolher sem depender da promessa de um fornecedor. Se fizer sentido para você, vai ser um prazer caminhar junto.

Me acompanhe: Instagram @lucascleopas.ia · YouTube @lucascleopas · lucascleopas.com.br

Referências

1. Gillespie, N.; Lockey, S. et al. Trust, attitudes and use of artificial intelligence: a global study 2025. Universidade de Melbourne e KPMG, maio de 2025. kpmg.com
2. KPMG e Universidade de Melbourne. Comunicado do estudo global sobre confiança e uso de IA. 09/05/2025. kpmg.com
3. IBM. “IBM Study: One in Four Malicious Breaches are AI-Enabled, Costing Companies $6 Million on Average” (Cost of a Data Breach Report 2026, com o Ponemon Institute). 29/07/2026. newsroom.ibm.com
4. Veracode. “AI-Generated Code Poses Major Security Risks in Nearly Half of All Development Tasks” (2025 GenAI Code Security Report). 30/07/2025. veracode.com
5. National Vulnerability Database. CVE-2025-48757. Maio de 2025. nvd.nist.gov
6. Superblocks. “Lovable Vulnerability Explained: How 170+ Apps Were Exposed”. Setembro de 2025. superblocks.com/blog
7. OpenAI. “Business data privacy, security, and compliance”. openai.com/business-data. Consultado em 25/11/2026.
8. Google. “Learn how Gemini in Gmail, Calendar, Chat, Docs, Drive, Sheets, Slides, Meet & Vids protects your data”. support.google.com, artigo 14615114. Consultado em 25/11/2026.
9. Brasil. Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais, arts. 5º e 46. planalto.gov.br

As políticas dos fornecedores de IA mudam com frequência. Confira a versão vigente antes de contratar qualquer ferramenta.

O caso da parte 2 é real e foi contado sem nomes. Este guia não é orientação jurídica.

Diagnóstico realizado por Neuralnets Consultoria em TI LTDA, CNPJ 69.031.567/0001-21.

Antes de decidir, vamos conversar.

Conversa curta e gratuita pelo WhatsApp (98) 98491-9854 · lucascleopas.com.br

NeuralNets