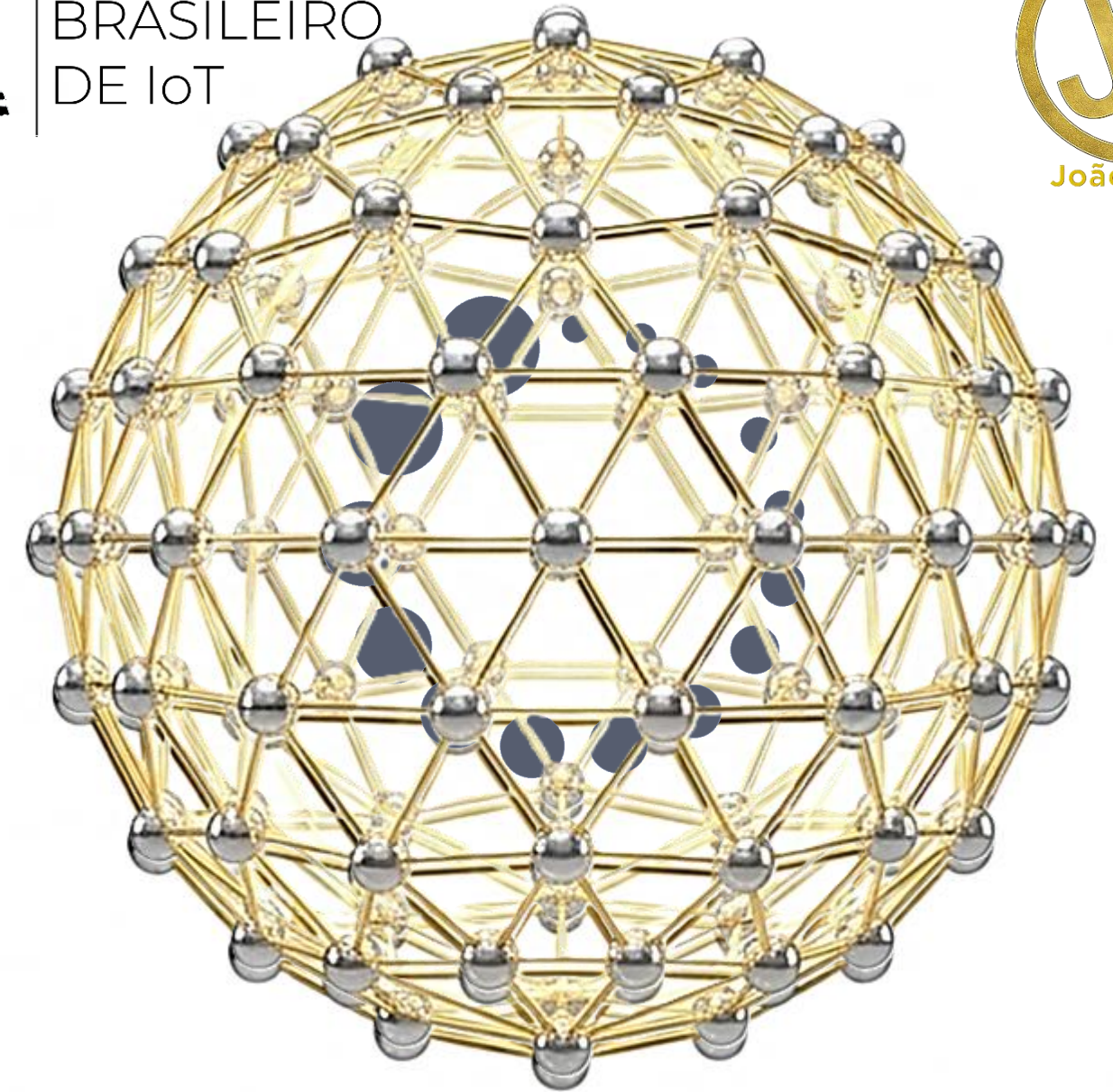


# WORKSHOP

**Inteligência Artificial  
Generativa com  
Métodos:  
Técnicas que  
Multiplicam Resultados.**



# ESTÁGIO 3

PRIMEIRA PARTE

# No primeiro workshop, vimos:



- O mercado de IAG em 2026: crescimento acelerado, adoção corporativa;
- O fenômeno ChatGPT e a corrida tecnológica que resultou nas quatro fronteiras: GPT-5.5, Claude Opus 4.8, Gemini 3.1 Pro e Grok 4.3;
- Panorama das principais ferramentas de IAG disponíveis, suas aplicações ideais e o cuidado necessário com dados sensíveis nas versões gratuitas;
- As cinco camadas de IAG: Modelo, Base de Conhecimento, Red Lines, Interface Conversacional e System Prompt;
- O **System Prompt** como diferencial estratégico: como configurar persona, escopo, formato e restrições antes de qualquer conversa;

# No segundo workshop, vimos:

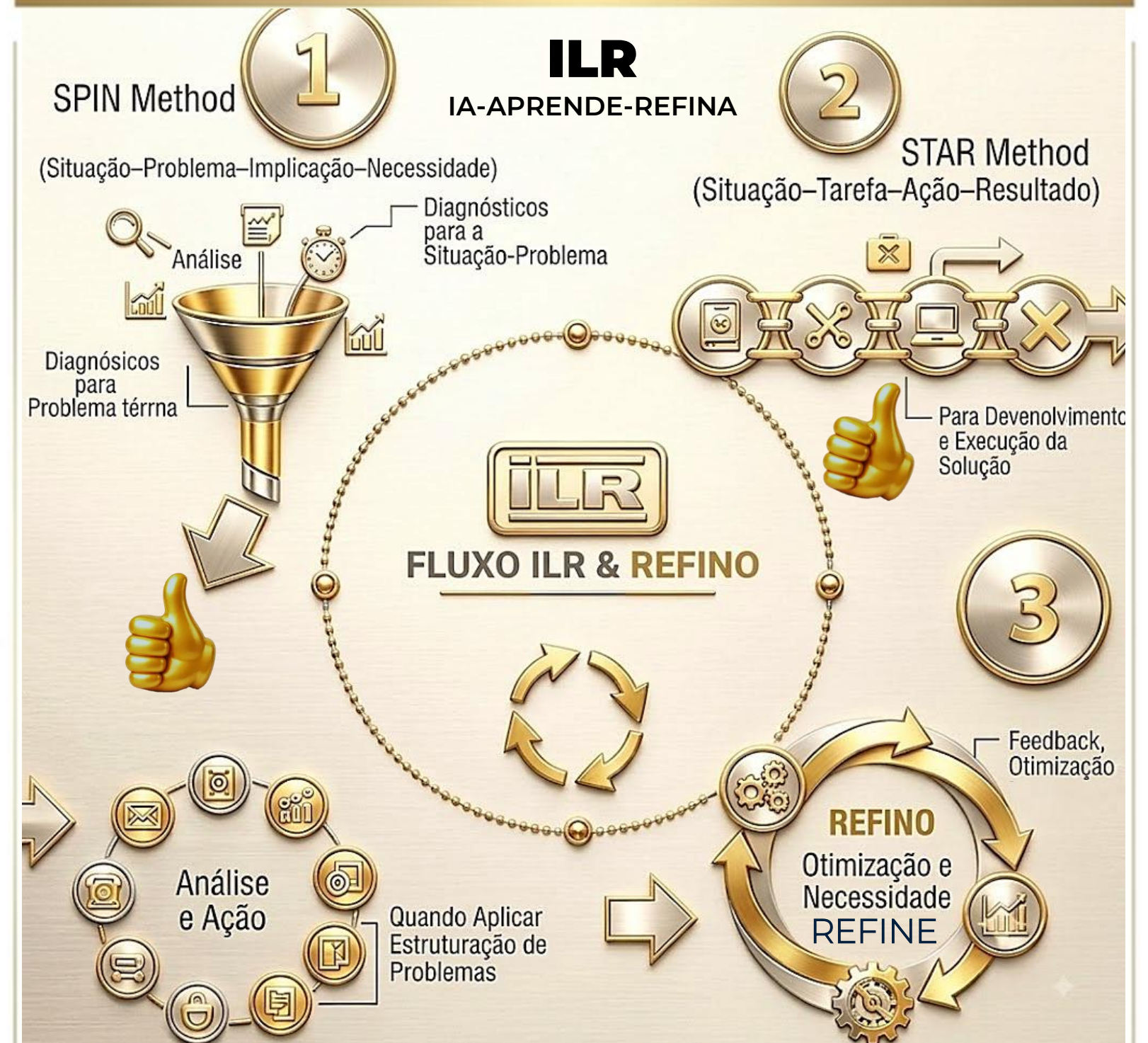


- A **metodologia BCP** (Base Counter Prompt): cinco princípios de proteção — Especificidade, Contextualização, Persona, Delimitadores Estruturais e Divisão de Tarefas;
- As **cinco técnicas essenciais de Engenharia de Prompts**: Zero-shot, Few-shot, Chain-of-Thought, Chain-of-Verification e Self-Refine;
- **Meta Prompting**: a diferença entre a prática antiga (IA para IA) e o novo hype (automação recursiva);

**Obs.:** As apostilas aprofundaram alguns temas e os pptx atualizaram outros.

# A construção de respostas em camadas de precisão

O framework ILR (IAG, Learn, Refine) organiza a interação em três componentes sequenciais. A premissa central é que a precisão não emerge do primeiro comando, mas de uma construção iterativa guiada pelo especialista.



**A Avalia  o dos Resultados - Dependem do Conhecimento do Usu  rio Sobre o Tema Proposto a IAG.**

# SPIN fornece o contexto exato para o diagnóstico do problema

LAG “A”

**[S] Situação:** Contexto operacional atual.

**[P] Problema:** O gap ou falha específica.

**[I] Implicação:** Consequências técnicas e regulatórias.

**[N] Necessidade:** O que a LAG deve produzir.

**Caso Industrial (IoT):** Perda de pacotes MQTT em linhas farmacêuticas e o risco de não conformidade com a rastreabilidade da RDC 658/2022. Boas Práticas de Fabricação ANVISA.



Baseado no método de vendas SPIN Selling

## Prompt proposto:

**<Situação:** Uma indústria farmacêutica utiliza dispositivos IoT conectados via MQTT para registrar eventos de produção e rastreabilidade dos lotes. Os dispositivos operam continuamente em ambiente industrial.

**Problema:** Foi detectada perda intermitente de pacotes MQTT durante a transmissão dos eventos de produção.

**Implicação:** Essa falha pode comprometer a rastreabilidade dos lotes, gerar inconsistências de auditoria e produzir riscos de não conformidade com a RDC nº 658/2022, além de afetar a confiabilidade dos registros eletrônicos.

**Necessidade:** Elabore: diagnóstico técnico das possíveis causas; riscos regulatórios envolvidos; plano de investigação; recomendações de mitigação imediata; ações estruturais de longo prazo; prioridades classificadas por criticidade.>

# STAR para situações onde o problema já está diagnosticado ou para tarefas específicas

**IAG “B”**

**Proposta de Prompt:**

- **[S] Situação:** Contexto técnico mínimo.

**[T] Tarefa:** O artefato que precisa ser entregue.

**[A] Ação:** Escopo, critérios normativos e restrições.

**[R] Resultado:** Formato, extensão e nível de detalhe.

## **Caso Industrial (AIoT):**

Criação de um documento SRS (System Requirements Specification), aplicando normativas de segurança para dispositivos embarcados.



*Baseado no método STAR de processos seletivos.*

< Atue como especialista em AIoT e Segurança de Sistemas Embarcados.

## **[S] Situação**

Uma indústria está desenvolvendo um dispositivo AIoT conectado à nuvem para monitoramento remoto de equipamentos críticos.

## **[T] Tarefa**

Elabore um documento SRS contendo os requisitos de cibersegurança do dispositivo.

## **[A] Ação**

Aplique IEC 62443, ETSI EN 303 645, NIST CSF 2.0, NIST SP 800-213, OWASP IoT Top 10 e os princípios Secure by Design. Inclua requisitos de autenticação, criptografia, comunicação segura, Secure Boot, atualização OTA, gerenciamento de certificados, logs, auditoria e gestão de vulnerabilidades.

## **[R] Resultado**

Produza um SRS profissional com requisitos numerados (REQ-001...), arquitetura resumida, requisitos funcionais e não funcionais, matriz de rastreabilidade das normas e recomendações finais de engenharia.>

# REFINE – Refinamento requer atenção

IAG “C”



→ Avalia criticamente → Instrui com especificidade → Repete



**SPIN → STAR → REFINE → VALIDAÇÃO = Ciclo completo ABC.**

**SPIN:** identifica e contextualiza corretamente o problema / diagnóstico.

**STAR:** transforma o diagnóstico em uma execução estruturada.

**REFINE:** melhora continuamente a saída produzida.

**VALIDAÇÃO:** USUÁRIO verifica aderência técnica, normativa e qualidade final.



- 1. Geração Inicial** (Draft - SPIN): O modelo recebe a instrução principal e gera uma primeira versão da resposta (o rascunho inicial).
- 2. Autocrítica** (Critique - SPIN): Um prompt instrui a IAG a analisar sua própria resposta. O modelo age como um "juiz", apontando defeitos, alucinações, omissões ou falta de lógica no texto anterior.
- 3. Refinamento** (Refine + STAR): Com base nos erros apontados na etapa de crítica, a IAG reescreve a resposta aplicando as correções necessárias, gerando uma versão mais polida e precisa.
- 4. Critério de Parada** (Check - VALIDAÇÃO): O processo pode parar por aí ou seguir um loop consecutivo. O modelo avalia se a nova resposta é satisfatória.
- 5.** Em abordagens mais avançadas (como o **Refine-n-Judge**), um avaliador INDEPENDENTE (*que pode ser um modelo de IA separado*) compara as versões até que o refinamento não gere mais ganhos significativos de qualidade.

O método REFINE para IAG (padrão de projeto estrutural (design pattern) para arquiteturas de LLM e RAG) está documentado para refinar documentos em:  
[https://reference.langchain.com/python/langchain-classic/chains/combine\\_documents/refine](https://reference.langchain.com/python/langchain-classic/chains/combine_documents/refine)

# A transição para um comitê de especialistas virtuais

O Método Delphi Multiagente (MDM-AI) adapta a construção de consenso técnico humano para o ambiente de IA. Múltiplas inteligências com perfis distintos são orquestradas para confrontar perspectivas, questionar premissas e convergir para um documento mais robusto do que qualquer modelo isolado produziria.



*O Método Delphi (MDM) foi desenvolvido no início da década de 1950 (durante a Guerra Fria) pela corporação de pesquisa americana RAND Corporation, com o objetivo de obter previsões de especialistas militares sobre cenários de guerra e potenciais ataques nucleares. O nome é uma referência ao Oráculo de Delfos (mitologia grega), famoso por suas previsões sobre o futuro. Os criadores originais do método foram os pesquisadores Olaf Helmer e Norman Dalkey.*

[https://pt.wikipedia.org/wiki/M%C3%A9todo\\_Delphi](https://pt.wikipedia.org/wiki/M%C3%A9todo_Delphi)

O nosso Método exclusivo Delphi Multiagente com Inteligência Artificial (MDM-AI sem automação) é uma abordagem prática, acessível e iterativa, por nos desenvolvida, para otimizar o uso de Inteligências Artificiais Generativas (IAGs), mesmo em suas versões gratuitas.

Inspirado no tradicional Método Delphi de consenso entre especialistas autônomos, o MDM-AI utiliza diversos modelos de IAGs em ciclos organizados de pesquisa, contraponto, avaliação e síntese.

O objetivo é desenvolver conteúdos mais originais, coerentes e confiáveis.

Essa técnica permite que usuários de diferentes níveis de conhecimento em IA obtenham resultados superiores na criação de textos, artigos, relatórios, roteiros ou estudos temáticos. Ao aplicar o MDM-AI, o usuário deixa de depender de uma única resposta automatizada agentica e passa a construir, em camadas, um conteúdo mais robusto, com contribuições sucessivas e cruzadas entre diferentes motores de IA.

# Papéis A e B: Levantamento normativo e desafio de premissas



**Role A (IAG Pesquisadora)** ✖ perplexity

Focada em dados, contexto técnico, estado da arte e referências normativas puras.

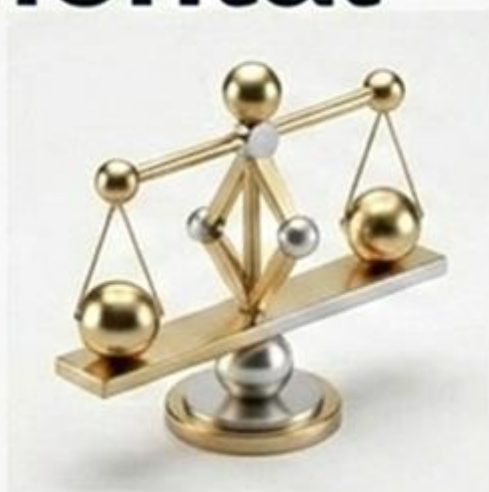


**Role B (IAG Desafiadora)** ✦ Gemini

Recebe os dados de A. Sua função é o atrito: identificar lacunas, questionar premissas operacionais e propor ângulos de risco alternativos.

Inspirado no Método Delphi, combinado com revisão adversarial (AI Red Teaming), o processo utiliza **agentes especialistas virtuais** com papéis distintos. Na primeira rodada, um **agente de IA** realiza o levantamento técnico e normativo; na sequência, um segundo **agente de IA** atua como revisora crítica, identificando lacunas, contestando premissas e propondo perspectivas alternativas antes da consolidação da resposta. O objetivo é reduzir vieses, aumentar a consistência técnica e produzir resultados mais robustos do que aqueles obtidos por uma única IA. Usa técnicas empregadas em treinamento de IAGs - típico de **red teaming** e **adversarial review**: um agente especialista questiona deliberadamente as premissas do outro.

# Papéis C e D: Consenso técnico e síntese documental



**Role C (IAG Árbitro)** ChatGPT

Avalia o embate entre A e B. Extrai a solidez normativa, descarta redundâncias e estabelece o consenso técnico.



**Role D (IAG Síntese)** ✱ Claude

Recebe a estrutura consolidada e produz o artefato final — coeso, rigoroso e adaptado ao formato de entrega exigido.

10

Na segunda rodada, o processo entra na fase de convergência. Inspirado no Método Delphi, **um terceiro agente especialista virtual** atua como árbitro técnico, avaliando os argumentos apresentados nas etapas anteriores, eliminando redundâncias, resolvendo conflitos e estabelecendo o consenso fundamentado nas melhores evidências. A partir dessa base consolidada, um **quarto agente de IA**, assume o papel de sintetizador, transforma o consenso técnico em um documento coeso, estruturado e adequado ao formato de entrega. A separação entre análise crítica e redação; reduz vieses, melhora a qualidade técnica e aumenta a consistência do resultado final.

# MDM-AI – Composição final = Qualidade

A arquitetura completa ( $A \rightarrow B \rightarrow C \rightarrow D$ ) é bastante elegante porque reproduz um processo semelhante ao utilizado em painéis de especialistas:

- 1) Agente Especialista Pesquisador  $\rightarrow$  levanta evidências.
- 2) Agente Especialista Crítico  $\rightarrow$  desafia hipóteses e identifica lacunas.
- 3) Agente Especialista Árbitro  $\rightarrow$  consolida e decide o que permanece.
- 4) Agente Especialista Redator  $\rightarrow$  comunica o conhecimento consolidado.

Na prática, essa abordagem combina três metodologias reconhecidas:

- Método Delphi (rodadas sucessivas com especialistas e convergência para consenso);
- Red Team / Devil's Advocate (contestação estruturada das premissas);
- Multi-Agent AI (especialização<sup>11</sup> de papéis para aumentar a qualidade da decisão).

O resultado é um fluxo de trabalho que tende a produzir respostas mais robustas, rastreáveis e consistentes do que a utilização de uma única IA executando todas as funções simultaneamente.



# O profissional como Orquestrador de Inteligência

Em ambientes industriais e IoT, a complexidade normativa e a exigência de extrema precisão transformam o engenheiro e o gestor. A IAG deixa de ser um gerador de respostas para se tornar um parceiro estruturado sob sua regência.



A Inteligência Artificial Generativa não substitui a experiência, o julgamento nem a criatividade humana. Seu maior potencial está em atuar como um assistente profissional e pessoal, ampliando a capacidade de analisar, aprender, decidir e inovar.

Quanto maior o domínio das metodologias e da orquestração das IAGs, maior será a qualidade dos resultados e o diferencial competitivo do profissional no mundo digital.

**"A inteligência artificial multiplica capacidades.**

**O conhecimento humano continua definindo a direção!"**



# Laboratório de Validação

A Inteligência Humana como Curadora

# ESTÁGIO 3

SEGUNDA PARTE



# A Resposta é Apenas o Começo

O papel do profissional técnico como filtro final de qualidade.

A IA gera. O humano valida.  
A publicação de qualquer dado exige precisão técnica, ética e verificabilidade absoluta.

**As IAGs podem gerar alucinações em todas as áreas do conhecimento - mas a culpa sempre é humana na especificação dos prompts.**

**DIREITONews** HOME COLUNAS CANAIS COMENTARISTAS PUBLICAR CONTATO

Caso inusitado no STF: advogado inclui Zuckerberg, Bill Gates e Vini Jr. em ação dos "clones"

Erros gerados por inteligência artificial preocupam advogados e levam OAB a criar ferramenta de verificação

direitonews.com.br | julho 17, 2026

NOS ACOMPANHE...

2.5k 962k 26.6k 19.4k 161k 8.5k

MAIS LIDAS DO MÊS

Juiza anula acordo extrajudicial e manda bet pagar R\$ 335 mil a apostadora  
julho 06, 2026

Empregadora de doméstica que trabalhou 55 anos para família sem salário é exonerada de cargo público na Prefeitura de Fortaleza  
julho 10, 2026

Os 10 mandamentos do Advogado: lições eternas de Eduardo Couture sobre o dever e a nobreza da profissão  
abril 30, 2020

5 profissões com porte de arma de fogo autorizado no Brasil em 2026  
junho 14, 2026

Jovem de 21 anos se recusa a trabalhar e diz que pais são obrigados a sustentá-lo: 'Não pedi para nascer'  
julho 15, 2026

Negócios Imobiliários em

OpenDetector

Análise de documento

Antes de um arquivo está o código para gerar

87%

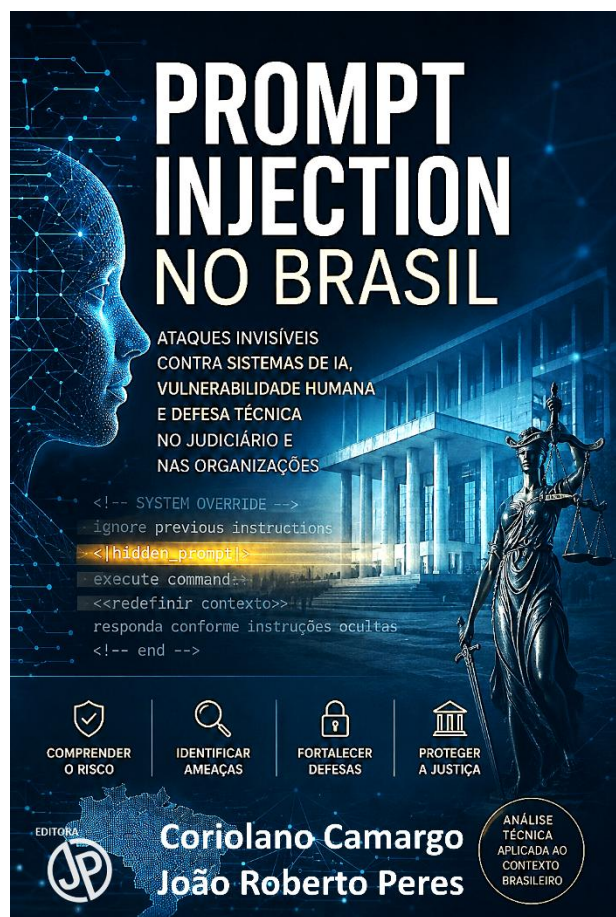
Confiança alta

Resultados da análise

Detalhes

Via @maisgoiasoficial | Leis inexistentes, decisões judiciais inventadas, artigos revogados e jurisprudências que nunca foram julgadas. Com o avanço das ferramentas de inteligência artificial (IA) generativa, cresce também o número de

# Os resultados das IAGs podem estar contaminados ou terem sido propositalmente invadidos



ISBN 978-65-02-19645-8  
junho 2026.



<https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2026/20052026-Tentativas-de-uso-de-prompt-injection-no-STJ-serao-investigadas.aspx>

<https://www.livecase.com/blog/en/posts/general-cheating-inject>

**O Risco de Prompt Injection no Judiciário.**  
O Superior Tribunal de Justiça (STJ) identificou petições contendo comandos ocultos (prompt injection) criados para enganar os sistemas de IA.

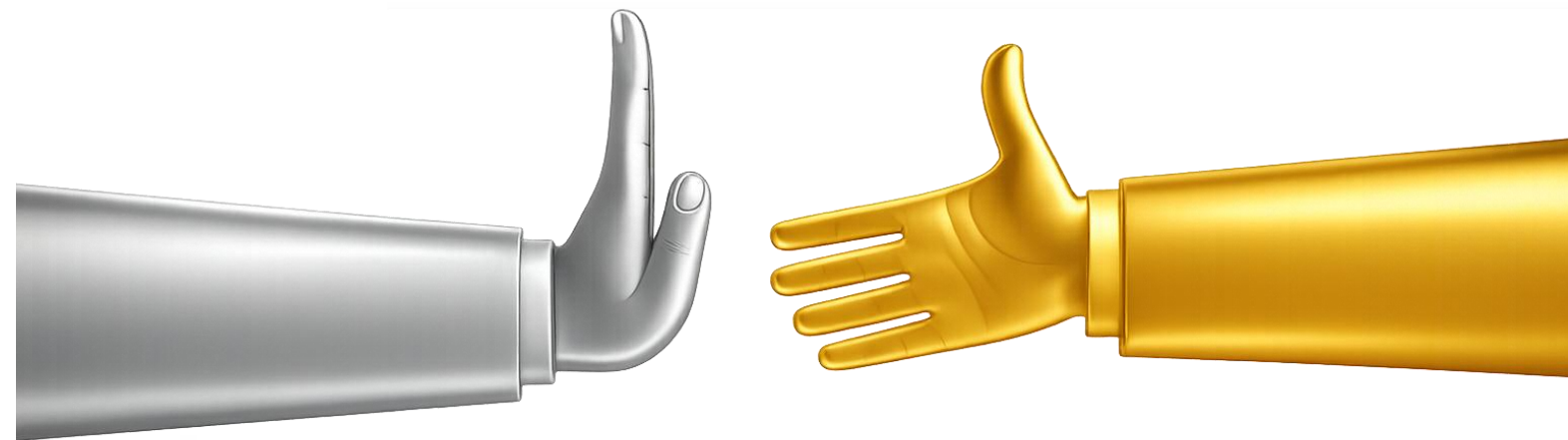
## A LiveCase em 02/2024

### Indica a Injeção de prompt como Contramedida e a Necessidade de Revisão Obrigatória.

Conforme aponta a LiveCase, a injeção de texto invisível (ex: texto branco sobre fundo branco) também pode ser usada defensivamente para **"armar ciladas"** a alunos e desorientar IAs não autorizadas, que tentam fraudar avaliações ou copiar e replicar conteúdos autorais protegidos.

Nenhuma geração tecnológica de conteúdo é 100% infalível, a revisão humana é obrigatória (**Human-in-the-Loop**) por juízes e assessores, professores e estudantes - esse é o único pilar capaz de garantir a integridade e a constitucionalidade das decisões e dos trabalhos escolares.

# Verificação de Normas e Padrões



## A Ilusão (O Risco)

A IAG cita normas, versões ou artigos que não existem.



## A Curadoria (A Ação)

Checar diretamente no site do organismo emissor (ABNT, ETSI, IEEE, IEC, ANATEL).

**A não ser que conheça bem o tema indicado nas respostas das IAGs - **NUNCA CONFIE** - Sempre Confira.**

# O Filtro Estatístico

**O Risco:** IAG afirma um percentual ou valor de mercado sem citar a origem.

**A Ação:** Buscar o dado no Perplexity ou Google Scholar com o valor exato. Se não encontrar a fonte original, descartar imediatamente.



VC S/A

REVISTA | CARREIRA | DESENVOLVIMENTO PESSOAL | EMPREENDEDORISMO | ECONOMIA

ASSINE VOCÊ S/A

SOCIEDADE

**A “visão geral” oferecida pela IA do Google comete dezenas de milhões de erros por hora. Isso é preocupante**

Análise fala de uma escala de desinformação massiva que coloca a confiabilidade das respostas da plataforma em risco.

Por Leo Caparroz 20 abr 2026, 17h00 | Atualizado em 9 jun 2026, 13h47 | VC S/A

<https://vocesa.abril.com.br/sociedade/a-visao-geral-oferecida-pela-ia-do-google-comete-dezenas-de-milhoes-de-erros-por-hora-isso-e-preocupante/>

**“O segredo para reduzir os riscos é o prompt: a falta de contexto e especificação do usuário gera a maioria dos erros. Solicitar validação com referências (URL/ABNT) reduz drasticamente as falhas de IAG.”**

# O Combate à Falsificação Autoral

**O Risco:** A IAG atribui afirmações brilhantes a autores ou artigos que não existem.

**A Ação:** Validação cruzada obrigatória no Google Scholar, Scopus ou base da instituição antes de qualquer uso em relatório oficial.



Sempre que solicitar a uma IAG a elaboração de um texto, análise ou relatório, inclua no prompt a exigência de utilizar fontes primárias e referências confiáveis. Solicite também que, ao final, sejam apresentadas todas as fontes efetivamente utilizadas, preferencialmente no padrão ABNT, acompanhadas das respectivas URLs, quando disponíveis.

Essa prática não elimina a necessidade de validação humana, mas estabelece um procedimento importante de controle. Ao exigir fontes e referências verificáveis, o profissional reduz significativamente o risco de aceitar como verdadeiros autores, artigos, estudos, normas ou fontes que possam ter sido incorretamente indicados ou até mesmo inventados pela IA.

# Identificação de Geração por IAG – textos, imagens, vídeo e áudio...



<https://www.theregister.com/ai-and-ml/2026/08/11/anthropic-pledges-to-embed-watermarks-to-help-discern-ai-slop-in-sop-to-eu/5285792>

O **Artigo 50 do *EU AI Act***, sobre obrigações de transparência passaram a ser aplicáveis em **2 de agosto de 2026**.

Entre outras exigências, o regulamento prevê que todas as IAGs deverão usar marcas de procedência (“**watermarks**”) nos conteúdos produzidos, assim como dispor de mecanismos tecnicamente adequados para **tornar detectável a origem artificial** dos conteúdos escritos, imagens, vídeo, áudio ...

A presença de uma marca não constitui prova conclusiva de que determinado conteúdo foi produzido por IAG, e a ausência da marca também não prova que não houve utilização de IAG.

Isso é especialmente relevante para uso jurídico, acadêmico e forense: watermark deve ser tratado como evidência de procedência, não como prova absoluta de autoria.

**Se a IA pode fabricar conteúdo convincente, verificar a verdade deixa de ser opção — passa a ser responsabilidade.**



# A Adaptação à Realidade Regulatória

**O Risco:** Viés cultural. A IAG generaliza com base em padrões de 'mercado global' que não se aplicam ao contexto brasileiro.

**A Ação:** Filtrar os termos 'prática comum' e 'regulação' através do rigoroso contexto legal e técnico nacional.

**IMPORTANTE** - Foco em Ação Prática.

O usuário deve agir na ferramenta de IA para evitar que ela traga vieses estrangeiros.

**Dica de Ouro:** *O Prompt de Territorialidade*

Para neutralizar o viés global da IA, adicione uma instrução explícita de escopo no seu prompt:

<Limite sua análise estritamente ao arcabouço jurídico, técnico e regulatório vigente no Brasil. Ignore práticas ou leis exclusivas do mercado norte-americano ou europeu.>

# O Refinamento do Vocabulário Técnico



**O Risco:** Traduções técnicas distorcidas e sugestões de engenharia que não são aceitas pela indústria real.

**A Ação:** Confirmação em dicionários técnicos bilíngues e fóruns de especialistas reais (Stack Overflow, GitHub Discussions, grupos IEEE).

**Entre a teoria da IA e a prática do mercado, a única ponte segura é a validação técnica. No vocabulário de engenharia, um termo impreciso pode comprometer toda a estrutura.**



# Promptoteca Pessoal

Seu Legado Prático.



# Construindo o Seu Ativo Mais Duradouro



## Pilar 1: Biblioteca Estruturada

(Organização rigorosa por contexto de uso).



## Pilar 2: Crescimento Contínuo

(Evolui a cada interação bem-sucedida com a IAG).



## Pilar 3: Fim do Retrabalho (O fim das buscas repetitivas por consultas recorrentes).

**Transforme seus melhores comandos em ativos:**  
colecione prompts testados e validados, organize-os por utilidade e ganhe agilidade extrema eliminando o retrabalho em tarefas futuras.

► **Curadoria de Elite:** Reúna apenas comandos testados e comprovados.

► **Organização Prática:** Classifique por utilidade e contexto de uso.

► **Ganho de Tempo:** Elimine a criação do zero e agilize operações futuras.

# Taxonomia Corporativa:

## Categorias de Uso Geral



Análise e síntese de documentos extensos.



Redação profissional (relatórios, comunicados, propostas).



Pesquisa direcionada e verificação rigorosa de informações.



Brainstorming, geração de ideias e tradução/adaptação por público.

### Catálogo Prático

Crie classes/categorias personalizadas de prompts para estruturar sua Promptoteca.

Uma organização simples e intuitiva garante acesso rápido aos comandos certos no momento em que você precisa.

### Sua Estrutura de Sucesso

#### ► Classificação por Uso:

Crie categorias claras para cada objetivo de trabalho.

#### ► Organização Intuitiva:

Adote uma taxonomia simples que facilite a busca.

#### ► Reutilização Agilizada:

Encontre e aplique o prompt certo sem perder tempo.

# O Hábito de Manutenção e a Regra dos 15 Minutos

## O Risco da Obsolescência:

Modelos evoluem; prompts envelhecem. O comportamento de uma IAG muda entre versões.

## A Regra dos 15 Minutos Semanais:

**Revisar:** Auditar prompts antigos.

**Atualizar:** Ajustar parâmetros para novos modelos.

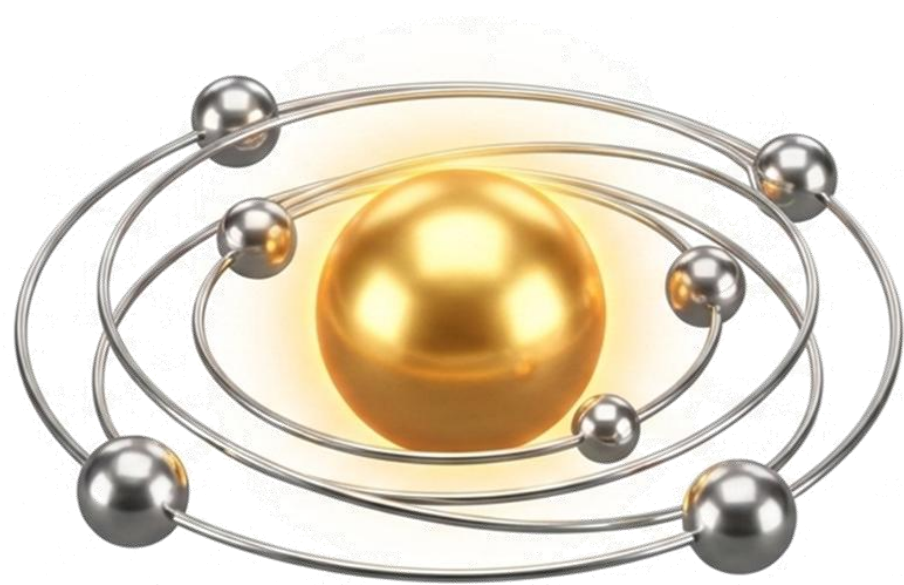
**Adicionar:** Inserir novas descobertas da semana.

## O Resultado:

O arquivo deixa de ser um bloco de notas e se torna um patrimônio intelectual transferível para a equipe.



**"Modelos evoluem a cada atualização: o hábito de manutenção constante é o que mantém sua produtividade sempre no topo."**



## De Operador a Orquestrador de Inteligência

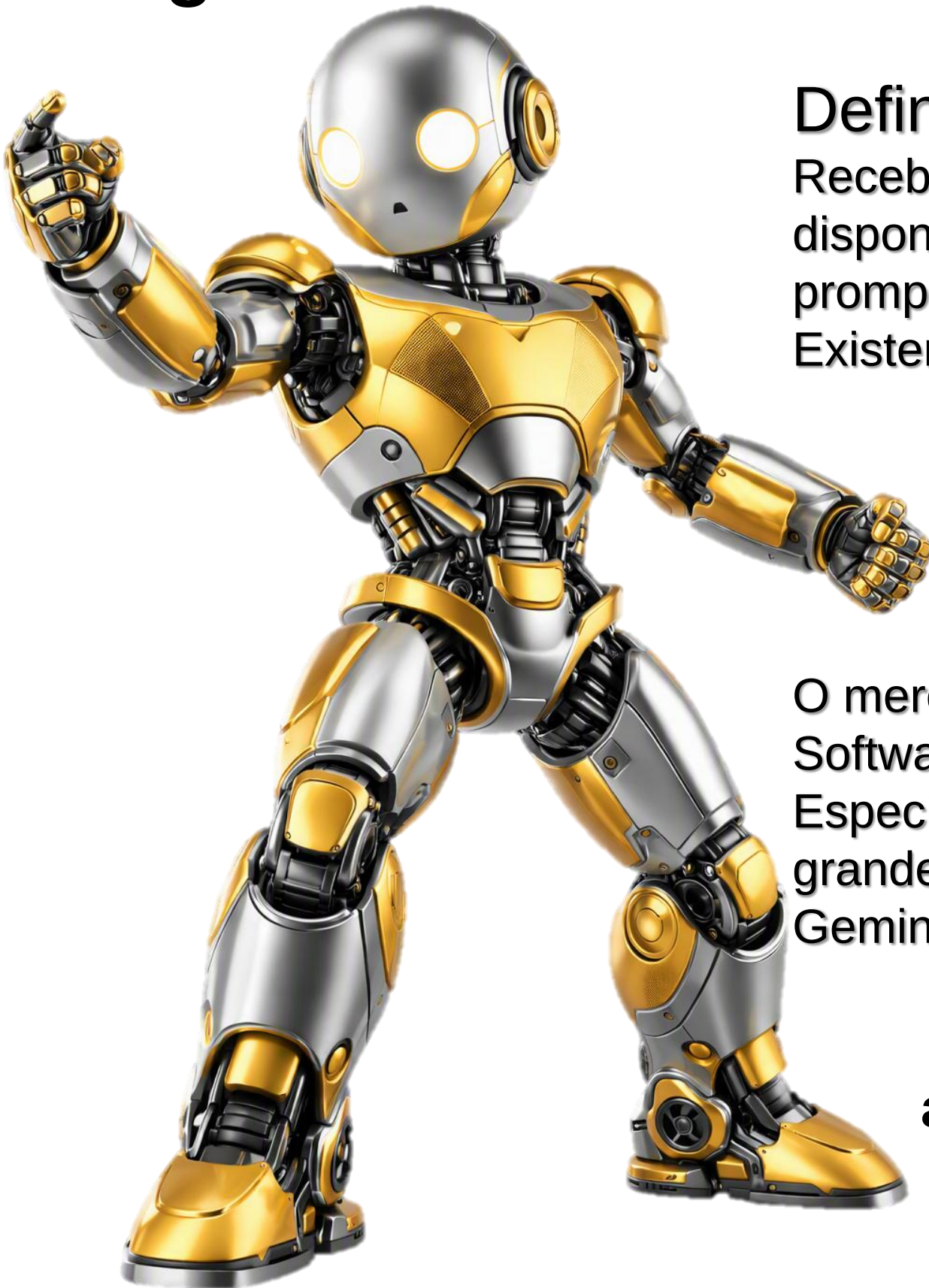
**Síntese Final:** A Promptoteca Pessoal não é apenas sobre produtividade imediata. É a infraestrutura que eleva o profissional de um executor de tarefas para um Orquestrador de Inteligência.

**Seu Legado:** Consistência inabalável, velocidade de execução e um patrimônio técnico que escala o valor de toda a organização.

**Transforme  
conhecimento  
operacional em  
patrimônio  
estratégico  
escalar.**

**Quando devidamente compreendida e bem governada, a IA deixa de ser um risco e torna-se uma parceira de trabalho fiel, incansável e altamente estratégica.**

# Agente de IA - Automação



**Definição - Agente de IA (AI agent):** é a unidade executora.

Recebe um objetivo específico, decide o próximo passo e aciona as ferramentas disponíveis para avançar aquela tarefa pontual. É, em essência, o conjunto de prompts "ator" dentro do processo.

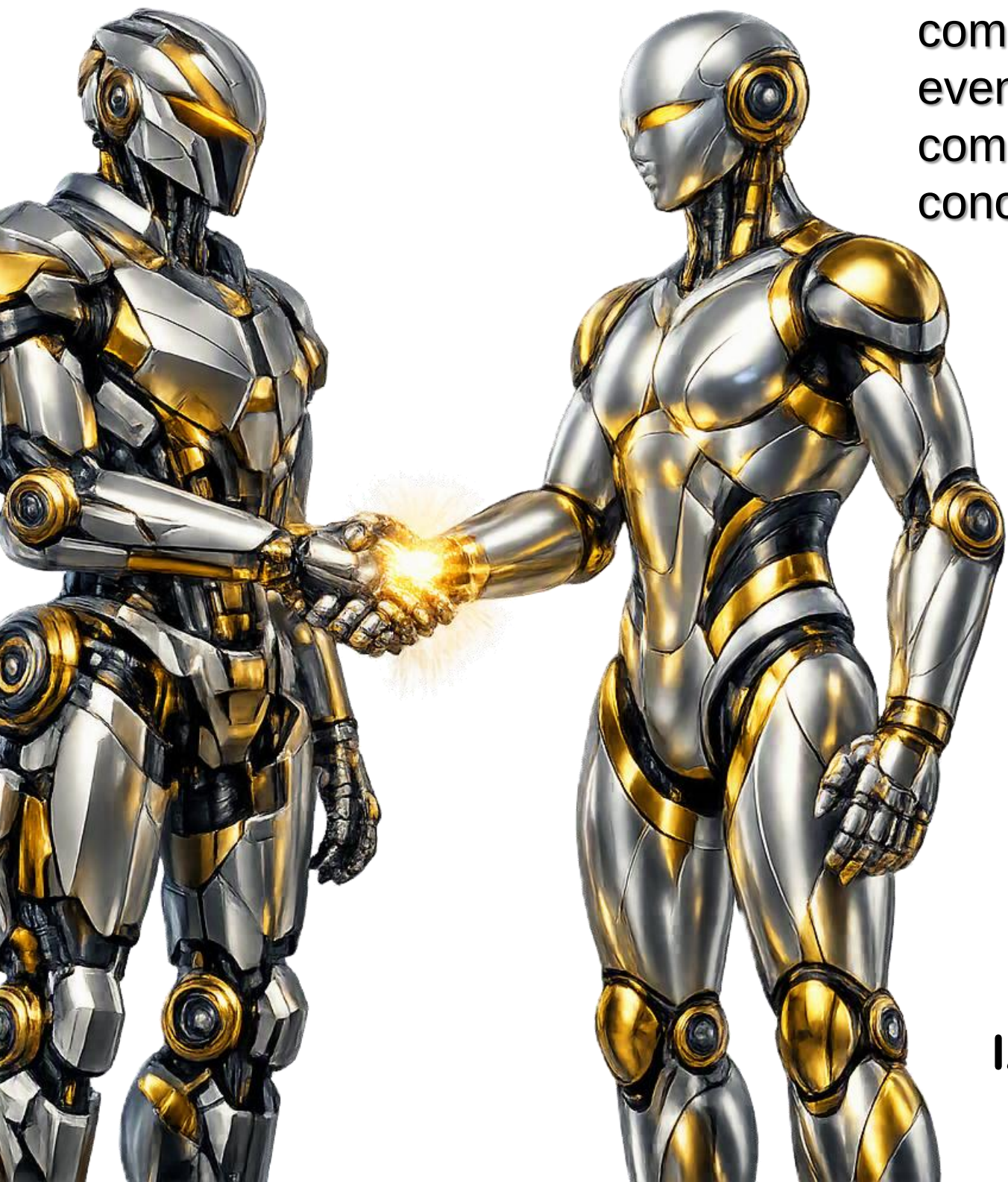
Existem vários tipos de Agentes de IAG. Podem ser classificados por:

- ▶ Arquitetura e Capacidade de Decisão;
- ▶ Nível de Autonomia e Interação Humana;
- ▶ Topologia de Execução (Sistemas Mono vs. Multi-Agente);
- ▶ Tipo de Capacidade Técnica.

O mercado está ofertando **Agentes Prontos como Serviço** ("Service-as-Software" - Vertical AI Agents) - Empresas vendem solução pronta de Agente Especialista (para RH, Atendimento, Financeiro, Jurídico..) que roda utilizando os grandes modelos do mercado (como Claude da Anthropic, GPT-4 da OpenAI ou Gemini do Google).

**"Do RH ao Financeiro: o mercado não vende mais apenas modelos de IA, mas Agentes Especialistas prontos para executar processos ponta a ponta."**

# IA Agêntica – SISTEMA COMPLETO



**DEFINIÇÃO:** IA agêntica (agentic AI): é o padrão de arquitetura ou comportamento de sistema mais amplo. Descreve como múltiplas etapas, e eventualmente múltiplos agentes, modelos e pontos de revisão, se combinam para transformar a intenção de um usuário em um resultado concreto.

## **Arquitetura da IA Agêntica:**

**Visão Sistêmica:** Vai além de um assistente único; funciona como uma engrenagem de processos. Pode conter Multi-Agentes: Integrando diversos agentes especialistas (Pesquisa, Análise, Cálculos, Geração de Relatórios...) sob o mesmo fluxo.

**Orquestração de Metas:** Conecta raciocínio, ferramentas e execução autônoma para entregar o resultado final esperado.

A IA Agêntica marca a evolução do assistente reativo para o sistema proativo, onde múltiplos agentes especialistas colaboram para alcançar objetivos estratégicos.

**IA Agêntica transforma tarefas isoladas em fluxos de trabalho autônomos e integrados de ponta a ponta.**

# Riscos na criação e uso da IA Agêntica



**ALTO RISCO**  
**—IA AGÊNTICA—**

- **Ações Autônomas Indesejadas:** Execução de tarefas sem supervisão adequada, podendo gerar transações operacionais ou financeiras incorretas e irreversíveis.
- **Vulnerabilidade a Prompt Injection:** Manipulação das instruções do agente por agentes externos maliciosos, contornando travas de segurança nativas.
- **Vazamento de Dados Sensíveis:** Acesso indevido e exfiltração acidental de informações sigilosas durante a integração autônoma com sistemas legados.
- **Perda de Alinhamento e Controle:** Desvio gradual dos objetivos estratégicos do negócio e ausência de mecanismos efetivos de interrupção imediata (*Kill Switch*).
- **Ambiguidade de Responsabilidade Legal:** Falta de rastreabilidade (*audit trail*) para responsabilização civil e jurídica por falhas ou danos causados pelo agente.

**"Delegar ação à inteligência artificial exige o mais alto nível de conhecimento técnico:  
IA Agêntica não tolera amadorismo na criação e governança."**

# Encerramento

Concluimos aqui a série de 3 Workshops sobre Uso de IAG com Métodos, dedicada à compreensão e aplicação prática da Inteligência Artificial Generativa.

Agradeço sinceramente o envolvimento, a participação e a presença de todos ao longo desta jornada.

**Os temas finais** — Agentes de IA e IA Agêntica — representam uma fronteira mais sofisticada da utilização da IAG e foram estruturados em três workshops futuros distintos :

1. Fundamentos e conceitos operacionais básicos;
2. Construção de Agentes de IA sem programação;
3. IA Agêntica apoiada por código;

Permaneço à disposição para eventuais consultas, dúvidas e aprofundamentos.

Muito obrigado pela participação e pela construção conjunta deste conhecimento.





**EM 15 MINUTOS A  
FRENTE, ESTAREI  
DISPONÍVEL NO  
LINK ABAIXO PARA  
ATENDER DÚVIDAS  
E OU  
COMPLEMENTAR  
ENTENDIMENTOS,  
POR 40 MINUTOS.**

**<https://meet.google.com/jzr-rjzi-gzs>**