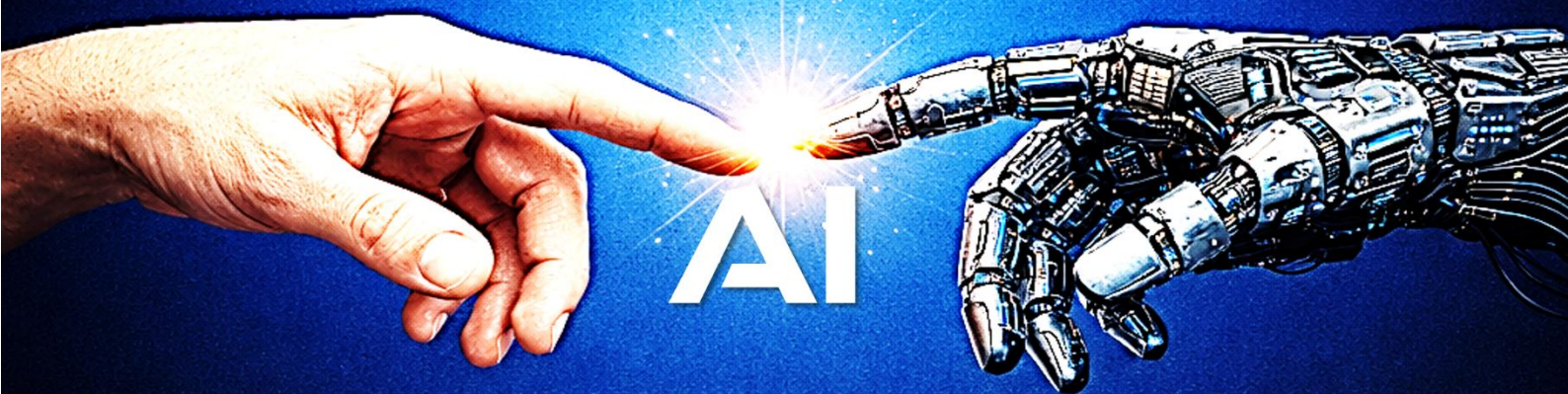


FÓRUM
BRASILEIRO
DE IoT



WORKSHOP

Inteligência Artificial
Generativa com Métodos:
Técnicas que Multiplicam
Resultados.

WORKSHOP 03/03



EDITORA



JOÃO ROBERTO PERES

APOSTILA

Inteligência Artificial Generativa: Uso Prático, Seguro e Estratégico - Do zero ao uso profissional — com foco em IoT e AIoT.

Edição: Junho de 2026 **Carga workshop horária:** 3 horas-aula | 3 seções de 60 minutos *Material produzido com curadoria humana e apoio colaborativo de ferramentas de IAG. Direitos reservados Prof. João R. Peres. Sem revisão ortográfica e técnica profunda.*

Workshop: “Inteligência Artificial Generativa com Métodos: Técnicas que Multiplicam Resultados.”

APRESENTAÇÃO

Esta apostila acompanha um workshop intensivo de aperfeiçoamento prático no uso de Inteligências Artificiais Generativas (IAG — sistemas capazes de criar conteúdo original a partir de instruções em linguagem natural).

O conteúdo foi estruturado para atender simultaneamente dois perfis: o profissional que está iniciando seu contato com essas ferramentas e busca uma base sólida e aplicável, e o especialista em tecnologias conectadas — especialmente IoT (Internet das Coisas) e AIoT (Inteligência Artificial das Coisas) — que precisa integrar IAG ao seu ecossistema técnico com precisão, segurança e discernimento.

A proposta é direta: pouca teoria, muita prática, fundamentação real e verificável. Cada conceito apresentado tem base comprovável. Cada ferramenta indicada foi avaliada quanto ao seu status atual. Cada exemplo foi desenhado para refletir situações reais de uso profissional.

Compreender e usar IAG com método não é acompanhar uma tendência. É assumir protagonismo sobre uma tecnologia que já está redefinindo como profissionais criam, analisam, decidem e comunicam — e que, no contexto de IoT e AIoT, representa uma camada adicional de inteligência sobre bilhões de dispositivos conectados.

Plataforma on-line de apoio: <https://abrir.link/cgNxM>

[Padrão de operação BIGMASTER](#)

Sumário da apostila

APRESENTAÇÃO	2
PARTE 5 — FRAMEWORK ILR E METODOLOGIA MDM-AI	4
5.1 Framework ILR — IAG, Learn, Refine	4
SPIN — para diagnóstico e análise de problemas	4
STAR — para execução de tarefas bem definidas	5
REFINE — o ciclo de melhoria contínua	8
5.2 Metodologia MDM-AI — Método Delphi Multiagente com IA	14
5.3 Integração ILR + MDM-AI: o fluxo completo	15
PARTE 6 — LABORATÓRIO DE VALIDAÇÃO	16
PARTE 7 — PROMPTOTECA PESSOAL	17
Estrutura recomendada para cada entrada	17
Categorias sugeridas para organização	17
Hábito de manutenção	18
PARTE 8 — AGENTE DE IA E IA AGÊNTICA	19
8.1 O que é IA agêntica	19
8.2 Agente de IA x IA agêntica	19
8.3 O padrão técnico por trás da autonomia: MCP e A2A	19
8.4 Uma forma de situar o conceito: a evolução da automação	20
8.5 Como o sistema funciona: o ciclo operacional	20
8.6 Arquiteturas de agentes	20
8.7 Exemplo aplicado — uso geral	21
8.8 Exemplo aplicado — IoT/AIoT	21
8.9 Riscos: da governança genérica ao risco de atuação física	21
8.10 Como usar de forma eficaz	22
Conclusão	22

PARTE 5 — FRAMEWORK ILR E METODOLOGIA MDM-AI

5.1 Framework ILR — IAG, Learn, Refine

O ILR organiza a interação com a IAG em três componentes sequenciais que se complementam: SPIN para diagnóstico de problemas, STAR para execução de tarefas definidas e REFINE para aperfeiçoamento iterativo do resultado. A lógica central é que uma boa resposta raramente emerge do primeiro prompt — ela é construída em camadas progressivas de precisão.

SPIN — para diagnóstico e análise de problemas

SPIN é um acrônimo para Situação, Problema, Implicação e Necessidade. Cada elemento responde a uma pergunta específica que, juntos, fornecem à IAG o contexto completo necessário para produzir uma análise realmente útil.

- **Situação:** qual é o contexto técnico, organizacional ou operacional atual?
- **Problema:** qual é o gap, a falha ou o desafio específico dentro desse contexto?
- **Implicação:** quais são as consequências — técnicas, regulatórias, financeiras, operacionais — se o problema não for resolvido?
- **Necessidade:** o que exatamente a IAG deve produzir para endereçar esse problema?

Exemplo SPIN — uso geral (gestão de documentos):

- **Situação:** "Nossa empresa de 80 funcionários ainda gerencia contratos em pastas físicas e planilhas Excel sem controle de versão."
- **Problema:** "Perdemos dois clientes nos últimos seis meses por atrasos em renovações contratuais que não foram detectadas a tempo."
- **Implicação:** "Além da perda de receita direta, o risco jurídico de contratos vencidos sem renovação formal nos expõe a disputas sobre vigência de obrigações."
- **Necessidade:** "Elabore um mapeamento dos critérios que devo avaliar ao escolher um sistema de gestão de contratos, incluindo funcionalidades mínimas, perguntas para fazer a fornecedores e critérios de descarte."

Prompt SPIN completo gerado: "Nossa empresa de 80 funcionários ainda gerencia contratos em pastas físicas e planilhas Excel sem controle de versão. Perdemos dois clientes nos últimos seis meses por atrasos em renovações contratuais que não foram detectadas a tempo. Além da perda de receita, contratos vencidos sem renovação formal nos expõem a disputas jurídicas sobre vigência de obrigações. Elabore um mapeamento dos critérios que devo avaliar ao escolher um sistema de gestão de contratos, incluindo funcionalidades mínimas, perguntas para fazer a fornecedores e critérios de descarte imediato."

Exemplo SPIN — uso IoT industrial:

- **Situação:** "Opero uma rede de 340 sensores de temperatura em linha de produção farmacêutica, comunicando via MQTT sobre Wi-Fi industrial com broker centralizado."

- Problema: "Estou observando perda de pacotes acima de 15% em horários de pico, comprometendo a rastreabilidade exigida pela RDC 658/2022 da ANVISA."
- Implicação: "Falhas de rastreabilidade podem invalidar lotes inteiros de produção e gerar não conformidades em auditorias regulatórias, com impacto direto sobre certificações vigentes."
- Necessidade: "Elabore um plano de diagnóstico em cinco etapas, indicando ferramentas de análise de tráfego adequadas para ambiente industrial e parâmetros de QoS (*Quality of Service* — qualidade de serviço) MQTT recomendados para alta confiabilidade em ambientes com interferência de RF."

STAR — para execução de tarefas bem definidas

STAR é adequado quando o problema já está diagnosticado e o que se precisa é de um produto específico: um relatório, uma especificação, um plano, uma análise. Os elementos são Situação, Tarefa, Ação e Resultado.

- **Situação:** contexto mínimo necessário
- **Tarefa:** o que precisa ser entregue
- **Ação:** como deve ser feito — escopo, critérios, restrições, fontes a considerar
- **Resultado:** formato, extensão e nível de detalhe da saída

Exemplo STAR — uso geral (treinamento corporativo):

- Situação: "Sou responsável por RH em uma empresa de logística com 200 funcionários, dos quais 60% operam em campo sem acesso regular a computador."
- Tarefa: "Preciso criar um plano de capacitação em uso básico de IAG para esse público."
- Ação: "O plano deve considerar formato de aprendizado mobile-first, sessões de no máximo 30 minutos, linguagem acessível sem jargão técnico e exemplos práticos do cotidiano de entregadores e motoristas."
- Resultado: "Estrutura do plano em formato de tabela, com módulos, objetivos de aprendizado, duração estimada e formato de entrega recomendado para cada módulo."

Exemplo STAR — uso AIoT (manutenção preditiva):

- Situação: "Estou especificando uma solução AIoT para manutenção preditiva em compressores de ar industrial em uma planta petroquímica."
- Tarefa: "Criar um documento de requisitos de sistema simplificado — SRS (*System Requirements Specification*) — para essa solução."
- Ação: "Incluir requisitos funcionais de coleta de dados de vibração, temperatura e pressão; inferência local no edge para detecção de anomalias; protocolo de comunicação com a nuvem; e requisitos de segurança mínimos segundo IEC 62443-4-2 para dispositivos embarcados. Excluir requisitos de interface de usuário nesta versão."
- Resultado: "Documento estruturado em tópicos com linguagem técnica, máximo de duas páginas, formato adequado para aprovação por comitê de engenharia."

Na apresentação em PPT apresentamos o método STAR para o caso Industrial (AIoT) correspondente a: Criação de um documento SRS(System Requirements Specification) aplicando normativas de Segurança para dispositivos embarcados.

O Prompt proposto poderá ter dois níveis, um mais simples do PPTx e um mais sofisticado – aqui apresentamos o mais sofisticado, que obviamente trará melhores resultados:

Prompt proposto:

< Atue como Engenheiro de Sistemas Embarcados, especialista em AIoT, IoT Industrial e normas internacionais de cibersegurança para dispositivos conectados. Utilize o método STAR para executar a solicitação.

[S] **Situação:** Uma empresa do setor industrial está desenvolvendo um dispositivo embarcado inteligente (AIoT) para monitoramento remoto de equipamentos críticos. O produto será conectado à Internet, realizará processamento local de dados e comunicação contínua com uma plataforma em nuvem. O equipamento deverá atender requisitos elevados de disponibilidade, integridade, confidencialidade e atualização segura de firmware durante todo o seu ciclo de vida.

[T] **Tarefa:** Elabore um documento SRS (System Requirements Specification) contendo os requisitos de segurança cibernética do dispositivo embarcado, considerando requisitos funcionais e não funcionais de segurança.

[A] **Ação:** Desenvolva a especificação aplicando boas práticas e requisitos das principais normas e frameworks aplicáveis, incluindo, sempre que pertinente:

- IEC 62443 (Industrial Automation and Control Systems Security);
- ETSI EN 303 645 (Cyber Security for Consumer IoT);
- NIST Cybersecurity Framework (CSF 2.0);
- NIST SP 800-213; • OWASP IoT Top 10;
- Princípios Secure by Design e Secure by Default. O documento deverá contemplar, entre outros:
 - autenticação e autorização;
 - gerenciamento de identidades;
 - controle de acesso;
 - armazenamento seguro de credenciais;
 - proteção criptográfica dos dados;
 - comunicação segura (TLS, MQTT seguro etc.);
 - secure boot;
 - cadeia de confiança;
 - assinatura digital de firmware;
 - atualização OTA segura;
 - gerenciamento de certificados;
 - proteção contra adulteração física;

- registro de eventos (logs);
- auditoria;
- monitoramento;
- gestão de vulnerabilidades;
- requisitos de disponibilidade;
- recuperação após falhas;
- requisitos de privacidade quando aplicáveis. Sempre que um requisito possuir referência normativa conhecida, indique a norma correspondente.

[R] **Resultado:** Produza um documento SRS profissional contendo:

1. Objetivo
2. Escopo
3. Arquitetura resumida do sistema
4. Premissas
5. Requisitos Funcionais de Segurança
6. Requisitos Não Funcionais de Segurança
7. Requisitos de Comunicação Segura
8. Requisitos de Gerenciamento de Firmware
9. Requisitos de Criptografia
10. Requisitos de Monitoramento e Auditoria
11. Requisitos de Manutenção e Atualizações
12. Matriz de rastreabilidade entre requisitos e normas aplicáveis
13. Recomendações finais de engenharia: Utilize linguagem técnica compatível com documentação de engenharia de sistemas, numeração formal de requisitos (REQ-001, REQ-002...), tabelas quando apropriado e nível de detalhamento suficiente para servir como base para desenvolvimento, testes e validação do dispositivo. > **Fim do prompt**

O REFINE transforma uma primeira resposta funcional em um produto final preciso. A lógica é: gera → avalia criticamente → instrui com especificidade → repete até convergir.

O ponto mais importante do REFINE é a **instrução de refinamento**: ela deve ser específica, não genérica. "Melhore o texto" não é uma instrução de refinamento — é uma instrução vaga que produz uma versão levemente diferente da anterior. Uma instrução de refinamento eficaz aponta exatamente o que mudar e por quê.

Comandos de refinamento eficazes — uso geral:

- "Substitua os três primeiros parágrafos por uma única frase de abertura impactante."
- "Remova todas as afirmações que não poderiam ser defendidas com dados públicos verificáveis."
- "Reescreva em primeira pessoa do plural, tom colaborativo, sem usar a palavra 'solução'."
- "Adicione um parágrafo final com a pergunta que o leitor deve se fazer após ler este texto."

Comandos de refinamento eficazes — uso IoT/AIoT:

- "Adicione para cada requisito listado o critério de verificação mensurável que confirmaria seu cumprimento."
- "Inclua uma coluna na tabela indicando qual provisão da ETSI EN 303 645 cada requisito de segurança endereça."
- "Reescreva a seção de riscos diferenciando riscos de implantação (projeto) de riscos de operação (pós-implantação)."
- "Adicione estimativa de impacto em termos de disponibilidade do sistema para cada risco identificado."

Exemplo completo de ciclo REFINE — uso IoT:

Prompt inicial (STAR): "Crie uma lista de verificação de segurança para o onboarding de um novo dispositivo IoT em rede corporativa."

Resposta inicial: lista genérica de dez itens sem critérios de verificação, sem referências normativas, sem distinção por tipo de dispositivo.

Refinamento 1: "Adicione, para cada item da lista, a referência normativa aplicável (ETSI EN 303 645, NIST SP 800-213 ou IEC 62443) e um critério de verificação binário — como o responsável pela aprovação confirmaria que o item foi cumprido?"

Refinamento 2: "Reorganize a lista em três fases: pré-implantação (avaliação do dispositivo antes da compra), implantação (configuração inicial) e pós-implantação (monitoramento contínuo). Remova itens redundantes."

Refinamento 3: "Adicione uma coluna de responsável sugerido para cada item: Segurança da Informação, TI Infraestrutura, Engenharia de Campo ou Fornecedor."

Resultado final: uma lista de verificação estruturada em três fases, com referências normativas, critérios de aprovação binários e responsáveis definidos — pronta para uso real em processo de onboarding.

PROCESSO DETALHADO DO CONJUNTO SPIN + STAR+ REFINE (Usando a mesma ferramenta de IAG)

O refinamento (**REFINE**) é o principal elemento do framework sendo complementar ao SPIN ou STAR, como uma **fase iterativa de otimização da resposta**. Na prática, SPIN e STAR produzem um primeiro artefato de alta qualidade; o REFINE conduz esse artefato até um nível profissional por meio de ciclos sucessivos de revisão.

SPIN → STAR → REFINE → VALIDAÇÃO

- **SPIN** identifica e contextualiza corretamente o problema.
- **STAR** transforma o diagnóstico em uma execução estruturada.
- **REFINE** melhora continuamente a saída produzida.
- **VALIDAÇÃO** verifica aderência técnica, normativa e qualidade final.

Processo REFINE

Passo 1 — Avaliação da primeira versão

Primeiro, peça para a IA avaliar criticamente a própria resposta.

Prompt:

< Analise criticamente a resposta produzida.

Identifique:

- pontos fortes;
- informações superficiais;
- omissões;
- inconsistências;
- ambiguidades;
- redundâncias;
- riscos técnicos;
- oportunidades de melhoria.

Não reescreva ainda.

Apresente apenas o diagnóstico. >

Passo 2 — Identificação das lacunas

Agora transforme o diagnóstico em ações.

Prompt

< Com base nas lacunas identificadas, liste todas as melhorias necessárias.

Classifique-as em:

- Essenciais
- Recomendáveis
- Opcionais

Explique o motivo de cada melhoria. >

Passo 3 — Refinamento

Somente agora a IA reescreve.

Prompt

< Reescreva completamente o documento incorporando todas as melhorias essenciais e recomendáveis.

Preserve todas as informações corretas.

Melhore:

- clareza;
- precisão técnica;
- organização;
- profundidade;
- consistência;
- linguagem profissional.

Não reduza conteúdo. >

Passo 4 — Enriquecimento

Agora agregue valor.

Prompt

< Enriqueça o documento adicionando, quando pertinente:

- exemplos;
- tabelas;
- checklists;
- diagramas textuais;
- fluxos;
- boas práticas;
- riscos;
- métricas;

- indicadores;
- referências normativas.

Não remova conteúdo existente. >

Passo 5 — Revisão técnica

Aqui a IA assume outro papel.

Prompt

< Agora atue como um revisor técnico sênior.

Revise todo o documento procurando:

- erros conceituais;
- erros técnicos;
- conflitos internos;
- afirmações sem fundamento;
- requisitos ausentes;
- inconsistências normativas.

Explique cada problema encontrado. >

Passo 6 — Revisão editorial

Depois da técnica, vem a forma.

Prompt

< Revise apenas a qualidade editorial.

Melhore:

- objetividade;
- fluidez;
- organização;
- padronização;
- títulos;
- subtítulos;
- listas;
- tabelas.

Não altere o conteúdo técnico.>

Passo 7 — Autoavaliação

Peça uma nota.

Prompt

< Avalie o documento utilizando notas de 0 a 10 para:

- precisão técnica
- completude
- organização
- clareza
- aderência ao objetivo
- qualidade profissional

Justifique cada nota.

Caso alguma nota seja inferior a 9, proponha melhorias. >

Passo 8 — Refinamento final

Somente após todas as revisões.

Prompt

< Produza a versão final incorporando todas as melhorias identificadas.

Esta versão deve representar a melhor qualidade possível, mantendo precisão técnica, linguagem profissional, consistência e completude.

Evite redundâncias.

Preserve toda a rastreabilidade das informações. >

Fluxo recomendado para Engenharia de Prompts

1. SPIN



Entender corretamente o problema

2. STAR



Executar a tarefa

3. REFINE 1



Diagnóstico da qualidade

4. REFINE 2



Correção das lacunas

5. REFINE 3



Enriquecimento do conteúdo

6. REFINE 4



Revisão técnica

7. REFINE 5



Revisão editorial

8. REFINE 6



Autoavaliação

9. REFINE FINAL



Documento definitivo

Regra prática

Uma forma simples e didática de explicar a sequência é:

- **SPIN** → "Entenda exatamente o problema."
- **STAR** → "Execute corretamente a tarefa para atender ao problema."
- **REFINE** → "Não aceite a primeira resposta; transforme-a em uma entrega de nível profissional."

Essa abordagem reflete uma prática consolidada no uso produtivo de LLMs: em vez de buscar um "prompt perfeito" que gere a resposta ideal em uma única interação, utiliza-se um processo iterativo de revisão, crítica e aprimoramento, semelhante ao ciclo de revisão adotado em engenharia, desenvolvimento de software e produção de documentos técnicos. Isso tende a produzir resultados mais consistentes e de maior qualidade.

5.2 Metodologia MDM-AI — Método Delphi Multiagente com IA

O Método Delphi é uma técnica consagrada de construção de consenso entre especialistas: cada especialista contribui com sua perspectiva, as contribuições são confrontadas, e o processo iterativo converge para uma resposta mais robusta do que qualquer especialista isolado produziria. A metodologia MDM-AI adapta essa lógica para o ambiente de múltiplas IAGs, tratando cada ferramenta como um especialista virtual com perfil diferente.

O fluxo envolve quatro papéis funcionais, que podem ser executados com IAGs distintas ou, em versão simplificada, com a mesma IAG recebendo instruções de papel diferentes em sequência:

- **IAG A — Agente Pesquisador:** levanta dados, contexto técnico, estado da arte, referências iniciais.
- **IAG B — Agente Desafiador:** recebe a saída de A, identifica lacunas, questiona premissas, propõe ângulos alternativos.
- **IAG C — Agente Árbitro:** recebe A e B, avalia qual análise é mais consistente, extrai os pontos mais sólidos de cada uma e identifica onde há divergência real.
- **IAG D — Agente de Síntese:** recebe o consolidado de C e produz o documento final coeso, estruturado e no formato de entrega desejado.

A combinação recomendada para uso profissional técnico, considerando o ecossistema atual:

- IAG A: Perplexity (busca com citação de fontes) ou NotebookLM (se houver documentação própria)
- IAG B: Claude Opus / Sonnet ou Qwen3/Kimi K2 ou 3 (raciocínio crítico, janela de contexto longa)
- IAG C: ChatGPT GPT-5.5 ou Gemini 3.1 Pro (agente árbitro)
- IAG D: Claude ou ChatGPT, conforme o formato de entrega (síntese do relatório)

Exemplo completo MDM-AI — uso geral (política de uso de IAG em empresa):

Prompt-Mestre (*Seed Prompt*): "Elabore uma política corporativa de uso responsável de ferramentas de IAG para uma empresa de serviços financeiros com 500 funcionários, considerando os riscos de privacidade de dados, propriedade intelectual e conformidade regulatória."

IAG A (Perplexity — Agente Pesquisador): levanta regulações aplicáveis ao setor financeiro, exemplos de políticas publicadas por empresas e referências de frameworks como NIST AI RMF e ISO/IEC 42001.

IAG B (Claude — Agente Desafiador): recebe a saída de A e aponta lacunas — por exemplo, ausência de distinção entre uso em tarefas operacionais e uso em tarefas estratégicas com dados de clientes; falta de critérios para avaliação de novas ferramentas que surgirem após a publicação da política; ausência de protocolo de resposta a incidentes envolvendo IAG.

IAG C (Gemini — Agente Árbitro): avalia A e B, identifica quais elementos de A são mais sólidos regulatoriamente, quais adições de B são críticas versus desejáveis, e propõe uma estrutura consolidada de seções para a política.

IAG D (Claude — Agente de Síntese): recebe a estrutura de C e produz o documento final da política, com linguagem formal, seções organizadas, critérios operacionalizáveis e tom adequado para aprovação pelo conselho jurídico.

Exemplo completo MDM-AI — uso IoT/AIoT (governança de dados de dispositivos AIoT):

Prompt-Mestre: "Analise os desafios de governança de dados gerados por dispositivos AIoT em ambiente industrial brasileiro, considerando a LGPD (Lei Geral de Proteção de Dados — Lei 13.709/2018), a Política Nacional de IoT (Decreto 9.854/2019) e os requisitos de segurança da IEC 62443."

IAG A (Perplexity — Pesquisador): levanta o estado atual da regulação, artigos aplicáveis da LGPD para dados de dispositivos industriais, o Decreto 9.854/2019 e sua estrutura de governança, e as camadas da IEC 62443 relevantes para dispositivos embarcados.

IAG B (Claude — Desafiador): recebe A e aponta questões não abordadas — por exemplo: dados de inferência gerados no edge por um modelo AIoT se enquadram como "dados pessoais" nos termos da LGPD quando o dispositivo monitora comportamento de operadores humanos? Quem é o controlador de dados: o fabricante do dispositivo, o integrador de sistemas ou o operador da planta? Como a IEC 62443 endereça dispositivos com capacidade de aprendizado adaptativo pós-implantação?

IAG C (Gemini — Árbitro): avalia A e B, identifica onde há consenso regulatório claro e onde há genuína lacuna normativa que exige posicionamento do jurídico, e propõe estrutura do documento final com seções que distinguem obrigações legais claras de recomendações de boas práticas.

IAG D (Claude — Síntese): produz análise consolidada, estruturada com: resumo executivo, mapa de obrigações legais verificáveis, mapa de lacunas normativas com recomendações de posicionamento, e lista de controles operacionais sugeridos para implantação imediata.

5.3 Integração ILR + MDM-AI: o fluxo completo

Os dois métodos são complementares e se potencializam quando combinados:

1. **SPIN** (ILR) para diagnosticar com precisão o problema técnico ou organizacional
2. **Prompt-Mestre** construído com base no diagnóstico SPIN, incorporando os princípios BCP
3. **MDM-AI** para explorar o tema em múltiplas perspectivas com IAGs distintas nos papéis A, B, C e D
4. **REFINE** (ILR) para ajustar o documento consolidado ao formato, tom e profundidade da entrega final

Este fluxo transforma a IAG de gerador de respostas genéricas em parceiro técnico estruturado — capaz de acompanhar o nível de especialização que contextos técnicos complexos exigem.

PARTE 6 — LABORATÓRIO DE VALIDAÇÃO

Receber uma resposta da IAG não é o fim do processo: é o começo da validação. Esta é a etapa onde a inteligência humana atua como curadora da inteligência artificial — garantindo que o que será usado, publicado ou encaminhado seja preciso, ético e verificável.

A tabela abaixo organiza os tipos mais comuns de problemas em respostas de IAG e como tratá-los:

Tipo de problema	O que observar	Como verificar
Alucinação de referência normativa	IAG cita norma, versão ou artigo que não existe	Checar diretamente no site do organismo emissor (ABNT, ETSI, IEEE, IEC, ANATEL)
Dado estatístico sem fonte	IAG afirma percentual ou valor de mercado sem citar origem	Buscar o dado no Perplexity ou Google Scholar com o valor exato; se não encontrar, descartar
Citação acadêmica inventada	IAG atribui afirmação a autor ou artigo que não existe	Verificar em Google Scholar, Scopus ou base da instituição antes de usar
Protocolo ou versão incorreta	IAG confunde versões de especificações técnicas (ex.: MQTT 3.1 vs 5.0; Matter 1.2 vs 1.3)	Verificar na documentação oficial do consórcio ou grupo de trabalho responsável
Viés ideológico ou cultural	IAG generaliza com base em padrões de mercado que não se aplicam ao contexto brasileiro	Identificar afirmações sobre "mercado", "regulação" ou "prática comum" e checar sua validade no contexto nacional
Tradução técnica distorcida	IAG traduz termo técnico com significado diferente do original	Verificar em dicionários técnicos especializados ou documentação oficial bilíngue
Sugestão técnica questionável	IAG recomenda abordagem que não é aceita pelo setor	Confirmar em fóruns técnicos especializados (Stack Overflow, GitHub Discussions, grupos IEEE) ou com especialista do domínio

Regra prática para uso profissional: qualquer afirmação de uma IAG que será usada em documento formal, apresentação para tomada de decisão ou comunicado com implicação regulatória deve passar por ao menos uma verificação em fonte primária antes de ser incorporada. Isso não é desconfiança excessiva — é o mínimo de diligência que qualquer profissional técnico aplicaria a qualquer outra fonte de informação.

PARTE 7 — PROMPTOTECA PESSOAL

A Promptoteca Pessoal é o ativo prático mais duradouro que este curso proporciona. É uma biblioteca estruturada de prompts testados, organizados por contexto de uso, que cresce a cada interação bem-sucedida com uma IAG.

Para profissionais de IoT e AIoT, esse ativo tem valor operacional imediato: evita retrabalho em consultas recorrentes, garante consistência de qualidade entre diferentes usuários da equipe e acumula aprendizado organizacional ao longo do tempo.

Estrutura recomendada para cada entrada

TÍTULO: [nome funcional do prompt — o que ele faz]

CONTEXTO DE USO: [quando e para que situações usar este prompt]

SISTEMA (System Prompt, se aplicável): [bloco de configuração]

TÉCNICA APLICADA: [BCP / Zero-shot / Few-shot / CoT /

Chain-of-Verification / Self-Refine /

SPIN / STAR / MDM-AI]

PROMPT: [texto completo, pronto para copiar e ajustar]

RESULTADO OBSERVADO: [o que funcionou bem, limitações
identificadas, ajustes feitos]

IAG TESTADA: [qual ferramenta foi usada]

VERSÃO: [data da última revisão]

Categorias sugeridas para organização

Para uso geral:

- Análise e síntese de documentos
- Redação profissional (relatórios, comunicados, propostas)
- Pesquisa e verificação de informações
- Brainstorming e geração de ideias
- Tradução e adaptação de linguagem por público

Para uso em IoT e AIoT:

- Análise de protocolos e arquiteturas de rede
- Revisão de requisitos e especificações técnicas (SRS, RFP, RFI)

- Análise de conformidade regulatória (LGPD, ANATEL, ABNT, ETSI, IEC)
- Avaliação de segurança de dispositivos e redes
- Documentação técnica (pareceres, relatórios, manuais simplificados)
- Preparação de apresentações para comitês técnicos e executivos

Hábito de manutenção

Uma Promptoteca que não é atualizada envelhece rapidamente — especialmente porque as próprias IAGs evoluem e prompts que funcionavam com um modelo podem ter comportamento diferente com versões mais recentes. Reserve quinze minutos por semana para revisar, atualizar e adicionar entradas. Com o tempo, esse arquivo se torna um diferencial real de produtividade — e um patrimônio intelectual transferível para a equipe.

Obs.: Os temas **Agentes de IA e IA Agêntica** não estavam previstos na programação original deste workshop, por se tratar de tópicos mais avançados, normalmente reservados a uma etapa posterior de aprofundamento. Optamos, no entanto, por incluir os fundamentos essenciais nesta apostila em razão da ampla divulgação do assunto pelas mídias especializadas e generalistas nos últimos meses, o que tem gerado curiosidade legítima e, por vezes, expectativas desalinhadas com a realidade técnica. O aprofundamento prático segue reservado aos três workshops específicos já anunciados na Parte 8 a seguir.

PARTE 8 – AGENTE DE IA E IA AGÊNTICA

8.1 O que é IA agêntica

IA agêntica (agentic AI, ou inteligência artificial com capacidade de agência) designa sistemas capazes de perseguir um objetivo com supervisão humana limitada. Diferente da IA conversacional tradicional, que responde a uma pergunta e encerra o ciclo ali, esse tipo de sistema decompõe um objetivo em etapas, aciona ferramentas externas, executa ações e ajusta o percurso conforme os resultados aparecem. A raiz do termo é agência, a capacidade de agir com intenção e produzir efeitos concretos no mundo, não apenas gerar texto sobre ele.

8.2 Agente de IA x IA agêntica

Os dois termos são próximos, mas descrevem camadas diferentes. Um agente de IA é a unidade executora, recebe uma tarefa específica e decide o próximo passo para cumpri-la. IA agêntica é o padrão de sistema mais amplo, que coordena uma ou várias dessas unidades, com planejamento e revisão, para transformar uma intenção em um resultado completo. Na prática cotidiana, os dois termos costumam ser usados de forma intercambiável, e esta apostila segue essa convenção, exceto quando a distinção for relevante para o ponto em discussão.

Vale um esclarecimento importante: uma ferramenta agente especializada em uma única função, como classificar e-mails ou resumir documentos, não equivale sozinha a um sistema de IA agêntica completo. Ela funciona como um agente especialista de nicho, competente naquela tarefa isolada, mas sem iniciativa própria para acionar outros sistemas ou decidir os próximos passos de um processo maior.

8.3 O padrão técnico por trás da autonomia: MCP e A2A

A afirmação de que um agente "aciona ferramentas externas" deixa de ser uma promessa genérica quando se conhece o padrão técnico que sustenta essa integração hoje. Dois protocolos abertos consolidaram esse terreno em pouco mais de um ano, e ambos são relevantes para quem avalia soluções de IAG aplicadas a IoT e AIoT.

O **Model Context Protocol** (MCP, ou protocolo de contexto de modelo) foi criado pela Anthropic em novembro de 2024 como um padrão aberto para conectar modelos de linguagem a ferramentas externas, bancos de dados e sistemas corporativos, funcionando como uma interface universal entre o modelo e o mundo operacional ao seu redor. Em dezembro de 2025, a Anthropic doou o protocolo à **Agentic AI Foundation**, uma entidade de governança neutra sob a **Linux Foundation**, com OpenAI, Google, Microsoft, AWS, Block e Bloomberg entre os membros fundadores. Até março de 2026, os kits de desenvolvimento em Python e TypeScript do MCP somavam aproximadamente 97 milhões de downloads mensais, um indicador de que deixou de ser uma iniciativa de um único fornecedor e passou a ser infraestrutura de mercado.

O **Agent2Agent** (A2A, ou agente para agente) resolve um problema distinto, a comunicação entre agentes de fornecedores e organizações diferentes. Criado pelo Google e anunciado em abril de 2025, foi doado à Linux Foundation em junho do mesmo ano, contando hoje com mais de 150 organizações apoiadoras, incluindo Microsoft, AWS, Salesforce, SAP e ServiceNow. A distinção prática entre os dois protocolos é direta: o MCP conecta um agente às suas ferramentas e fontes de dados, o A2A conecta um agente a outro agente, possivelmente de uma empresa parceira ou fornecedora, para delegação e coordenação de tarefas entre sistemas independentes.

Para o profissional de IoT e AIoT, essa distinção tem consequência operacional imediata: um agente que consulta o histórico de telemetria de uma planta industrial provavelmente o faz via MCP; um agente que precisa negociar um chamado de manutenção com o sistema de um fornecedor de equipamentos provavelmente o faz via A2A.

8.4 Uma forma de situar o conceito: a evolução da automação

Para quem já acompanhou etapas anteriores da automação corporativa, vale uma comparação direta. O arquivo de lote (batch) automatiza comandos fixos, uma sequência rígida que trava diante de qualquer imprevisto. O RPA (automação robótica de processos) avançou ao automatizar a interação humana com a tela, cliques, digitação, abertura de janelas, mas manteve a mesma rigidez de fundo, quebrando quando o layout do sistema muda. A **IA agêntica** rompe esse padrão porque não repete uma sequência fixa, ela persegue um objetivo e decide, em tempo real, qual caminho seguir.

Uma imagem que ajuda a fixar essa diferença é a do trânsito. Um trem segue trilhos fixos e para diante de qualquer obstáculo na linha. Um carro com condução autônoma recebe apenas o destino final, escolhe a rota, contorna imprevistos e recalcula o caminho quando necessário, sempre dentro de limites definidos, como velocidade, sinalização e faixas permitidas. A IA agêntica bem configurada opera como esse segundo caso, autonomia real de decisão, dentro de limites que a organização estabeleceu previamente.

8.5 Como o sistema funciona: o ciclo operacional

Sistemas agênticos operam em ciclo dentro de um fluxo determinado, não em uma única resposta: compreensão do objetivo (o que se espera alcançar, em qual formato, sob quais restrições), planejamento (divisão em etapas menores), execução (realização das etapas dentro dos limites de permissão), revisão (confronto do resultado com o objetivo original) e ajuste (correção do plano ou pedido de esclarecimento humano, quando necessário).

8.6 Arquiteturas de agentes

Arquitetura	Quando usar	Exemplo	Supervisão recomendada
Agente único	Tarefa focada, escopo bem definido	Triagem automática de chamados de suporte	Revisão por amostragem
Multiagente	Trabalho dividido entre especialistas coordenados	Pesquisa, desafio e síntese (ver MDM-AI, Parte 5.2)	Revisão do resultado consolidado
Domínio específico	Escopo restrito e previsível	Análise de conformidade de um único protocolo IoT	Revisão por amostragem
Propósito geral	Gama ampla de tarefas	Assistente corporativo multifuncional	Revisão constante
Segundo plano	Continuidade de trabalho sem presença do usuário	Monitoramento contínuo de indicadores de rede	Aprovação humana obrigatória antes de qualquer ação

8.7 Exemplo aplicado — uso geral

Situação: uma equipe de atendimento ao cliente recebe centenas de solicitações por e-mail diariamente, hoje triadas manualmente.

Configuração do agente: objetivo de classificar cada e-mail por urgência e departamento responsável, ferramenta de acesso limitada à leitura da caixa de entrada e escrita apenas em um sistema de tickets, sem permissão de resposta automática ao cliente. O agente sinaliza os casos ambíguos para revisão humana em vez de decidir sozinho.

8.8 Exemplo aplicado — IoT/AIoT

Situação: uma rede de sensores AIoT monitora vibração e temperatura de compressores industriais, com potencial de identificar falhas antes que ocorram.

Configuração do agente: objetivo de analisar continuamente os dados de telemetria e abrir um chamado de manutenção preditiva quando os indicadores ultrapassarem o limiar definido, com acesso de leitura ao sistema de telemetria via MCP e permissão de escrita apenas no sistema de chamados. Qualquer ação sobre o equipamento físico, como parada programada ou ajuste remoto de parâmetros, exige aprovação humana explícita antes da execução.

Prompt de configuração proposto:

< Atue como especialista em automação industrial e AIoT, responsável por configurar um agente de monitoramento preditivo.

Objetivo do agente: analisar dados de vibração e temperatura recebidos de sensores instalados em compressores industriais e identificar padrões que indiquem risco de falha.

Ferramentas permitidas: leitura do sistema de telemetria; escrita exclusiva no sistema de abertura de chamados de manutenção.

Ferramentas proibidas: qualquer ação de escrita ou comando sobre o equipamento físico, incluindo parada, reinício ou ajuste de parâmetros operacionais.

Regra de escalonamento: quando os indicadores ultrapassarem o limiar de risco definido, o agente deve abrir um chamado de manutenção preditiva classificado por nível de urgência, e não executar nenhuma ação corretiva diretamente.

Regra de aprovação humana: qualquer recomendação de parada ou intervenção física deve ser apresentada como sugestão a um responsável técnico humano, nunca executada de forma autônoma.

Produza a especificação de configuração deste agente em formato estruturado, pronta para implementação. Entregue também texto com os passos explicados da especificação do plano do agente para aprovação. >

8.9 Riscos: da governança genérica ao risco de atuação física

O principal benefício da IA agêntica é a continuidade, o contexto passa de uma etapa para a próxima, reduzindo transferência manual entre ferramentas. As limitações mais comuns incluem escolha de plano inadequado, interpretação equivocada do objetivo e afirmações sem lastro (alucinação).

Para o público de IoT e AIoT, existe uma categoria de risco que merece destaque próprio, distinta dos riscos de um agente que apenas manipula texto ou documentos: o risco de atuação sobre um ativo físico. Um

agente que erra ao redigir um relatório produz um documento incorreto, revisável antes de qualquer consequência. Um agente com permissão de atuação que erra ao decidir sobre um equipamento conectado pode gerar uma consequência física irreversível antes que qualquer humano perceba o erro.

O **OWASP Top 10 for Agentic Applications 2026**, publicado pelo OWASP Gen AI Security Project em dezembro de 2025, formaliza essa preocupação em categorias específicas, entre elas o sequestro de objetivo (Agent Goal Hijack), o uso indevido de ferramentas (Tool Misuse) e o abuso de identidade e privilégio (Identity and Privilege Abuse), esta última descrita como evolução do risco de excesso de agência (Excessive Agency) já mapeado no OWASP Top 10 for LLM Applications. O princípio central recomendado pelo documento é o da menor agência (least agency): um agente deve operar apenas com as permissões estritamente necessárias para a tarefa declarada, de modo que, mesmo comprometido, não seja capaz de causar dano além do escopo previsto. Esse princípio é a mesma lógica de menor privilégio já apresentada no adendo sobre BCP desta apostila, aplicada agora à camada de execução do agente, e não apenas à camada de instrução do prompt.

Para uso corporativo em ambientes conectados, três cuidados se destacam: privacidade e confidencialidade dos dados processados, verificação humana obrigatória antes de qualquer ação sobre equipamento físico, e governança de permissões proporcional ao grau de autonomia concedido ao sistema.

8.10 Como usar de forma eficaz

Defina o resultado final esperado e o destinatário. Forneça contexto confiável, arquivos, exemplos, restrições. Estabeleça limites desde o início, o que o sistema pode fazer, o que deve evitar e quando deve pedir aprovação. Para tarefas longas ou sensíveis, peça um plano antes da execução, e use pontos de verificação intermediários. O princípio central: a IA agêntica não substitui o julgamento humano, ela absorve o trabalho repetitivo de múltiplas etapas, enquanto humanos definem objetivos e aprovam os resultados que realmente importam.

Conclusão

A IA agêntica representa uma mudança de eixo, da geração de respostas isoladas para a condução de trabalho orientado a objetivos, hoje sustentada por padrões técnicos abertos e vendor-neutral como o MCP e o A2A, e acompanhada por frameworks de segurança dedicados como o OWASP Top 10 for Agentic Applications. Seu valor é maior quando a tarefa tem propósito claro, contexto suficiente, permissões bem delimitadas e um resultado passível de revisão humana, especialmente quando essa revisão precede qualquer ação sobre um ativo físico.

Os temas Agentes de IA e IA Agêntica poderão ser aprofundados em três novos workshops distintos:

1. Conceitos e Estruturas: fundamentos teóricos, arquiteturas e distinções conceituais.
2. Agentes de IA sem Programação: construção e uso prático de agentes por meio de ferramentas de baixo código ou sem código.
3. IA Agêntica Apoiada por Código: implementação técnica de fluxos agênticos com uso de programação e integração de ferramentas.

A compreensão desses fundamentos prepara o terreno para o próximo passo natural do percurso, que é a configuração prática de agentes de nicho nos workshops especializados anunciados acima.

Referências

ANTHROPIC. Introducing the Model Context Protocol. Disponível em:

<https://www.anthropic.com/news/model-context-protocol>.

LINUX FOUNDATION. Linux Foundation Launches the Agent2Agent Protocol Project to Enable Secure, Intelligent Communication Between AI Agents. Denver, 23 jun. 2025. Disponível em:

<https://www.linuxfoundation.org/press/linux-foundation-launches-the-agent2agent-protocol-project-to-enable-secure-intelligent-communication-between-ai-agents>.

GOOGLE DEVELOPERS BLOG. Announcing the Agent2Agent Protocol (A2A). 9 abr. 2025. Disponível em:

<https://developers.googleblog.com/en/a2a-a-new-era-of-agent-interoperability/>.

OWASP GEN AI SECURITY PROJECT. OWASP Top 10 for Agentic Applications 2026. Disponível em:

<https://genai.owasp.org/resource/owasp-top-10-for-agentic-applications-for-2026/>.

OWASP FOUNDATION. OWASP Top 10 for Large Language Model Applications, LLM06: Excessive Agency.

Disponível em: <https://owasp.org/www-project-top-10-for-large-language-model-applications/>.

Material produzido com curadoria humana e apoio colaborativo de ferramentas de IAG. Todos os dados de mercado foram verificados em fontes primárias identificadas. Versão: julho de 2026. Sem revisão ortográfica formal — versão de trabalho para ajustes editoriais do autor.