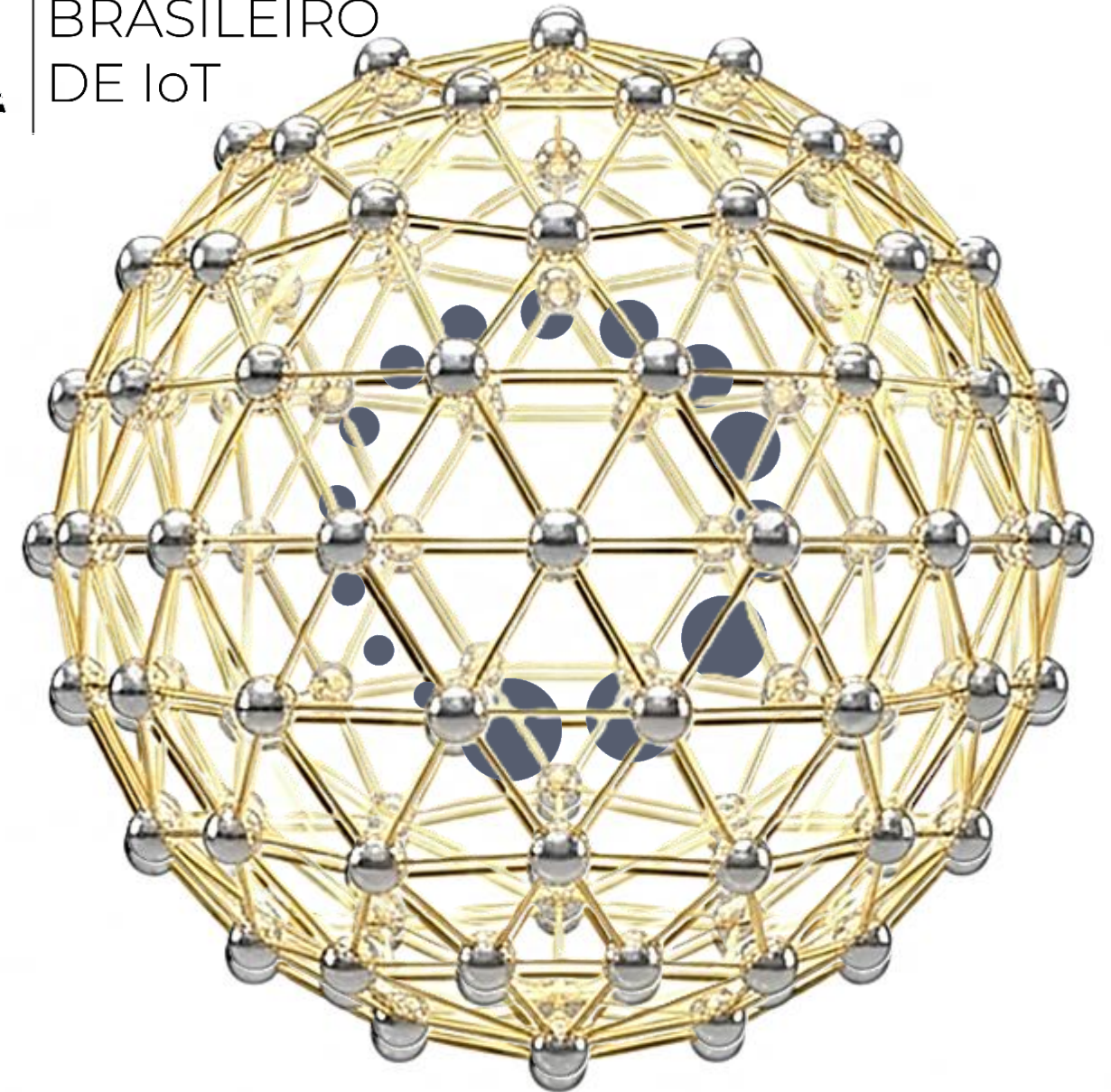


WORKSHOP

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



ESTÁGIO 2

PRIMEIRA PARTE

Metodologia BCP

Operação Profissional de IAG para IoT e AIoT



A metodologia BCP se fundamenta no contexto de “**Base Counter Prompt**” ou instrução primária de defesa, que é uma técnica na Engenharia de Prompts que age como um escudo contra técnicas de desvio de regras ou injeção de comandos maliciosos – a estrutura BCP apresentada também possui o mesmo objetivo básico.

**Vamos praticar
o uso de IAg
com Métodos
Seguros**

**BCP – Na Criação
Básica de Prompts.**

**Base Counter-Prompt
A defesa primária**

A Lógica BCP: Os 5 princípios

- A qualidade da resposta é literalmente proporcional à instrução original.
- A IAG não deduz intenções não expressas ou contextos ocultos.
- Um prompt vago gera uma resposta genérica; um prompt estruturado produz uma utilidade técnica real.



Fraco



Forte



Os Princípios BCP determinam que a inteligência gerada por um LLM não é um fator fixo, mas sim um reflexo direto da geometria matemática do prompt de entrada. Entradas amorfas e vagas dispersam a atenção da rede neural, gerando respostas turvas, genéricas e até enviesadas. Já entradas estruturadas e com alta densidade técnica funcionam como um vetor linear de proteção: canalizam o processamento do modelo diretamente para o alvo, extraindo o nível máximo de utilidade e precisão que a IA pode oferecer.

Princípio 1: Especificidade (Eliminar Ambiguidade)

A IAG processa exatamente o que recebe. Qualquer imprecisão na entrada se amplifica na saída.

<u>Fraco</u>	<u>Forte</u>
Quais são os riscos de segurança em IoT? (Nota: Gera apenas uma lista genérica de internet).	Liste os cinco principais vetores de ataque em redes de dispositivos IoT industriais que utilizam o protocolo MQTT 3.1.1 sem autenticação TLS, operando em ambiente de manufatura com acesso à internet. Classifique cada vetor por risco (alto, médio, baixo) segundo o framework ETSI EN 303 645.

Como fazer a retrospectiva de um projeto?

(Nota: Gera apenas uma lista genérica de passos teóricos encontrados em manuais da internet).



Atue como um Agile Coach sênior. Escreva o roteiro para uma reunião de Retrospectiva de Sprint de 1 hora para um time de engenharia de software focado em DevOps. O time não atingiu a meta da Sprint devido a gargalos no pipeline de CI/CD e falta de documentação das APIs. Inclua dinâmicas de quebra-gelo, divisão de tempo por etapa, técnica de causa-raiz (5 Porquês) e um formato de tabela para registrar os planos de ação com responsáveis e prazos.



Princípio 2: Contextualização (Quem Escreve e Quem Lê)

O Emissor

Sou engenheiro de sistemas embarcados responsável por uma linha de produção farmacêutica com 280 sensores IoT de temperatura e umidade.

O Objetivo

Explicar por que a ausência de autenticação nos dispositivos representa risco de conformidade com a RDC 658/2022 da ANVISA, mantendo um tom técnico, porém acessível.

O Receptor

Relatório técnico interno para a diretoria, que não possui formação em TI.

Exemplo de prompt:

Markdown

[FATO] A migração para a nuvem atrasou 2 semanas porque a equipe precisou refazer o treinamento de segurança de dados.

[EMISSOR] Sou o Diretor de Tecnologia.

[OBJETIVO] Explicar o atraso sem parecer defensivo, focando no ganho de conformidade.

[RECEPTOR] e-mail para a Diretora de RH, indicando que em breve teremos um novo cronograma.

Modelos de IA não conhecem o seu cenário de negócios. Contextualizar é calibrar a perspectiva: define o papel de quem comanda (Emissor), o perfil de quem consome (Receptor) e a meta real da entrega (Objetivo) para alinhar o tom e o nível técnico da resposta."



Princípio 3: Persona (Atuação como Especialista)

Assumir um papel força a IAG a abandonar o ponto médio e adotar o rigor e as referências de um especialista.



Exemplos de Ativação:

Arquiteto IoT:

Atue como arquiteto de soluções IoT. Avalie os desafios de interoperabilidade entre dispositivos em uma rede de iluminação pública inteligente, contrastando os padrões Matter 1.3 e Zigbee 3.0.

Especialista AloT:

Atue como especialista em AloT em manutenção preditiva. Explique para para engenheiros mecânicos como um modelo de Machine Learning (Edge ML) em um microcontrolador pode detectar anomalias em rolamentos.

A Persona atua como um filtro probabilístico na rede neural da IA. Ao delimitar o papel do profissional, o modelo restringe seu vocabulário ativo aos jargões daquela profissão, eleva o rigor metodológico e adota o padrão estrutural de relatórios técnicos do setor, eliminando respostas comerciais, vagas ou superficiais.

Princípio 4: Delimitadores Estruturais

Marcadores textuais (tags) isolam as instruções do conteúdo, eliminando falhas por confusão de contexto.



Arquitetura de Tags:

[CONTEXTO]: A situação primária, o ambiente restrito ou os dados técnicos que servem de base.

[TAREFA]: O comando executável; a instrução exata do processamento exigido sobre os dados.

[FORMATO]: A restrição de saída; a estrutura estrutural, extensão e nível de detalhamento do resultado final.

Modelos de IA processam textos de forma linear e contínua, o que pode gerar 'vazamento de dados' onde o modelo confunde o texto que deve ser analisado com as ordens que deve executar. O uso de delimitadores estruturais, como colchetes [TAG] ou tags XML <tag> — funciona como uma barreira arquitetônica. Eles blindam o prompt contra ataques de injeção e separam nitidamente os metadados de controle dos dados brutos, otimizando a atenção da rede neural e garantindo previsibilidade total na saída do formato.

Princípio 5: Divisão de Tarefas (Fragmentação)

Prompts longos com múltiplas exigências degradam o raciocínio matemático do modelo. A regra de ouro é: fragmente arquiteturas complexas em ciclos. A saída (output) de um sub-prompt deve ser a entrada (input) do próximo.



A capacidade de processamento cognitivo de um LLM degrada exponencialmente quando ele é exposto a prompts extensos que exigem múltiplos passos de raciocínio lógico ou cálculos matemáticos simultâneos.

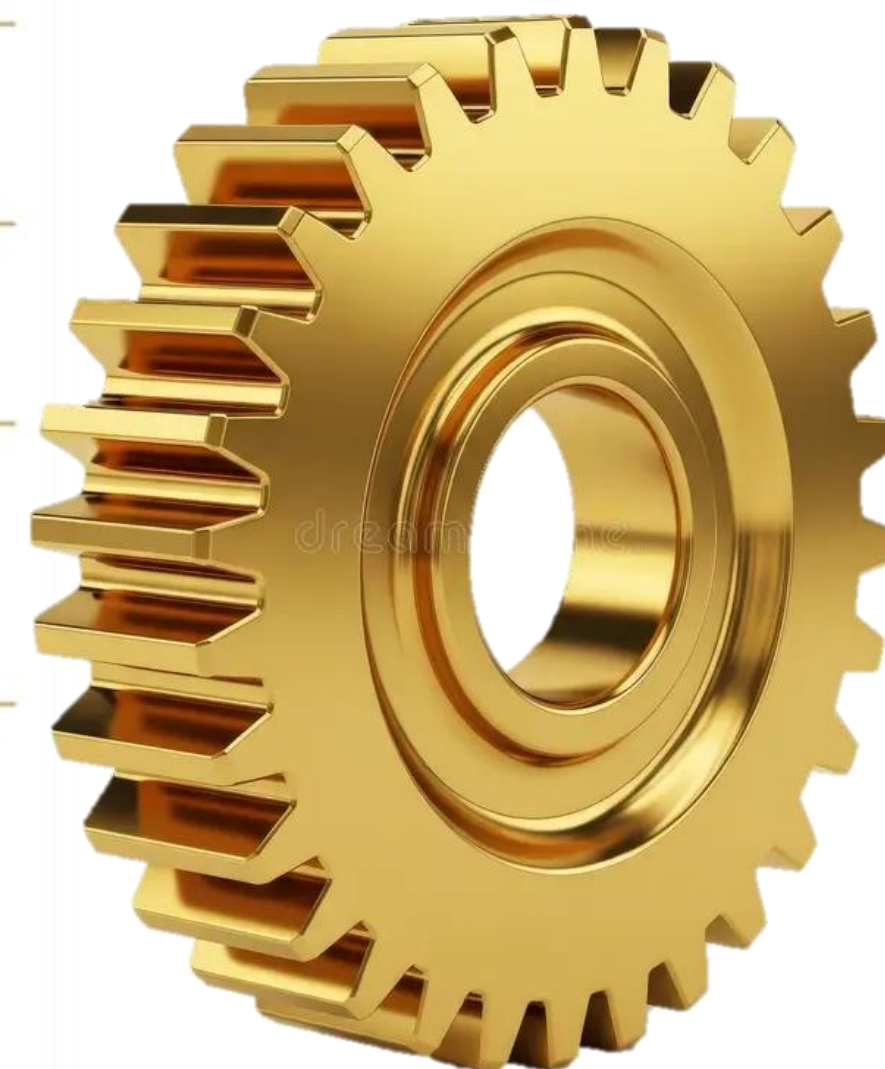
O Princípio da Fragmentação para a proteção, estabelece que arquiteturas complexas devem ser quebradas em ciclos de sub-tarefas lineares.

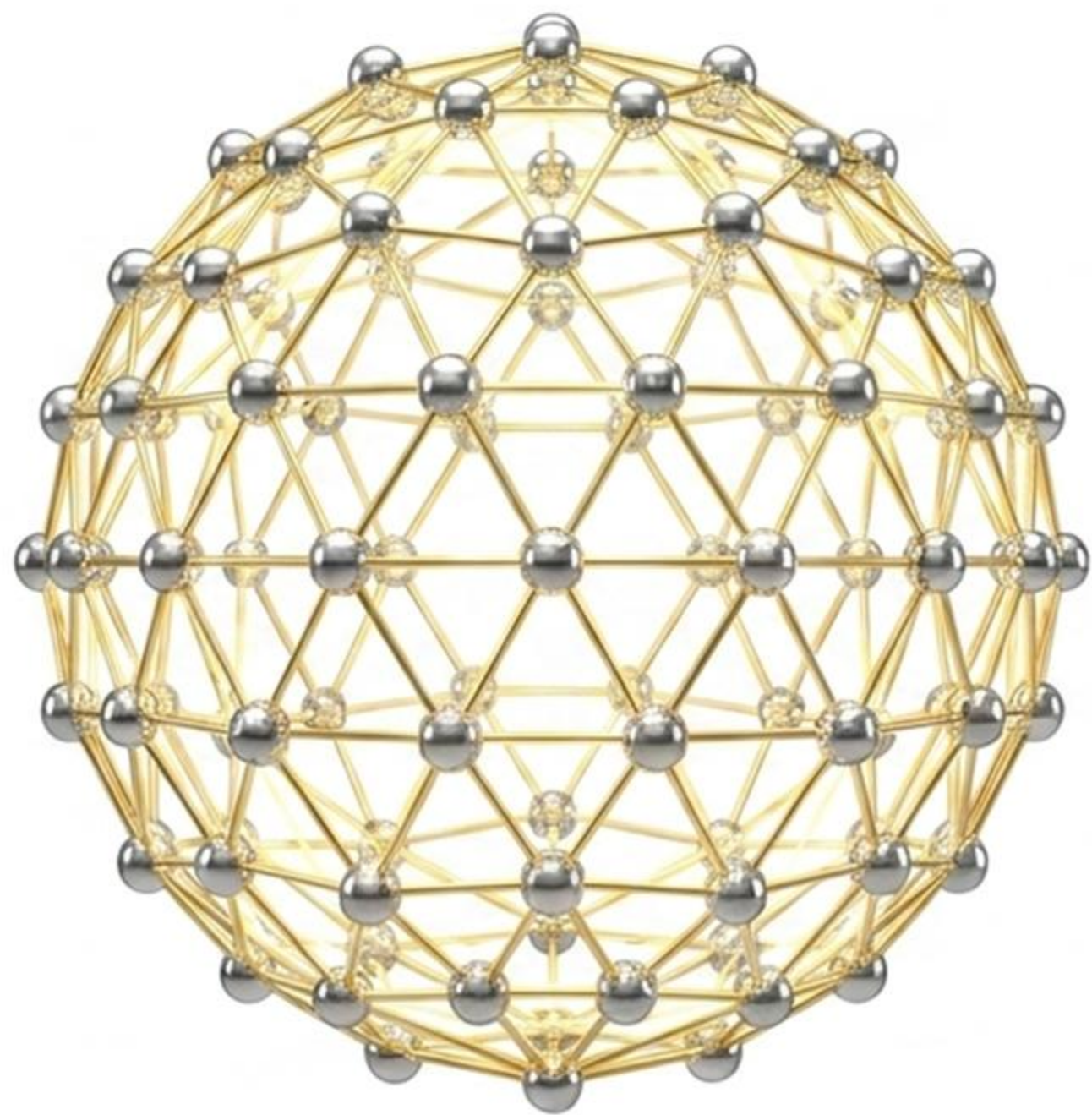
Ao transformar a saída (output) de um bloco de instrução no dado de entrada (input) do bloco seguinte, blindamos o modelo contra sobrecarga de atenção, reduzindo drasticamente as taxas de alucinação e garantindo rigor técnico em cada etapa do processo.

Síntese: A Matriz BCP

Mecanismos de proteção ampla

Princípio	O que fazer
1. Especificidade	Elimine ambiguidade; ordene exatamente os parâmetros técnicos e protocolos.
2. Contextualização	Defina o emissor, o receptor e o cenário regulatório aplicável.
3. Persona	Instrua o modelo a adotar rigorosamente a especialidade requerida (Ex: Arquiteto IoT).
4. Delimitadores	Separe parâmetros operacionais de dados textuais usando tags como [CONTEXTO] e [TAREFA].
5. Divisão de Tarefas	Fragmente problemas técnicos sistêmicos em prompts sequenciais em cadeia.





Técnicas de Engenharia de Prompts

Estratégias de Alta
Performance

ESTÁGIO 2

SEGUNDA PARTE

Engenharia de Prompt: A Interface do Pensamento Humano com a IA

O que são?

As Técnicas de Engenharia Imediata de Prompt (TEIP) não compreendem apenas a escrita de perguntas; é a disciplina técnica que projeta, estrutura e otimiza entradas de texto para direcionar o comportamento de Modelos de Linguagem (LLMs/SLMs).

É a ponte que traduz a intenção humana na linguagem probabilística da inteligência artificial. Efetivamente EP é o estudo evolutivo da CHC (Comunicação Humano-Computador) para transformar a linguagem natural humana em interface técnica de comunicação com computadores.

Aplicação Técnica

No ambiente corporativo e de desenvolvimento, ela é a chave para:

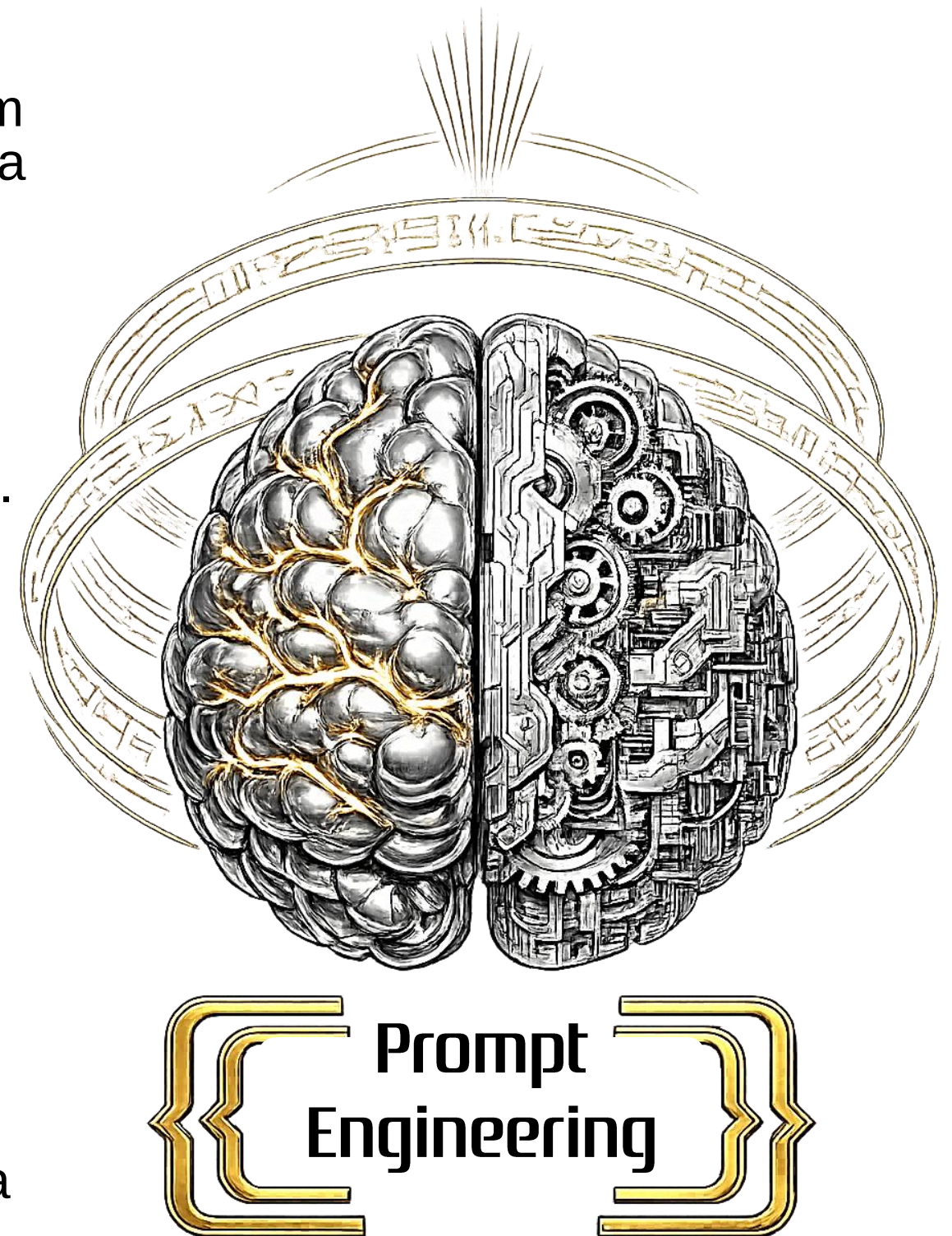
Mitigar Alucinações: Blindar sistemas contra respostas inventadas ou imprecisas.

Garantir Previsibilidade: Forçar a IA a entregar dados estritamente estruturados (como tabelas, JSON ou relatórios técnicos padronizados).

Automação e Integração: Permitir que modelos de IA conversem com APIs, ferramentas externas e bancos de dados de forma confiável.

Nosso Foco no Workshop: Embora o ecossistema de Engenharia de Prompt conte com **dezenas de abordagens acadêmicas** e avançadas, a verdadeira maestria técnica começa pela base estrutural.

Neste workshop, vamos dominar de forma prática os 5 Princípios Fundamentais da Entrega de Alta Performance.



A Mudança de Paradigma

A Engenharia de Prompts não é uma habilidade reservada a programadores. É a disciplina de estruturar instruções para maximizar a qualidade, relevância e confiabilidade das respostas.

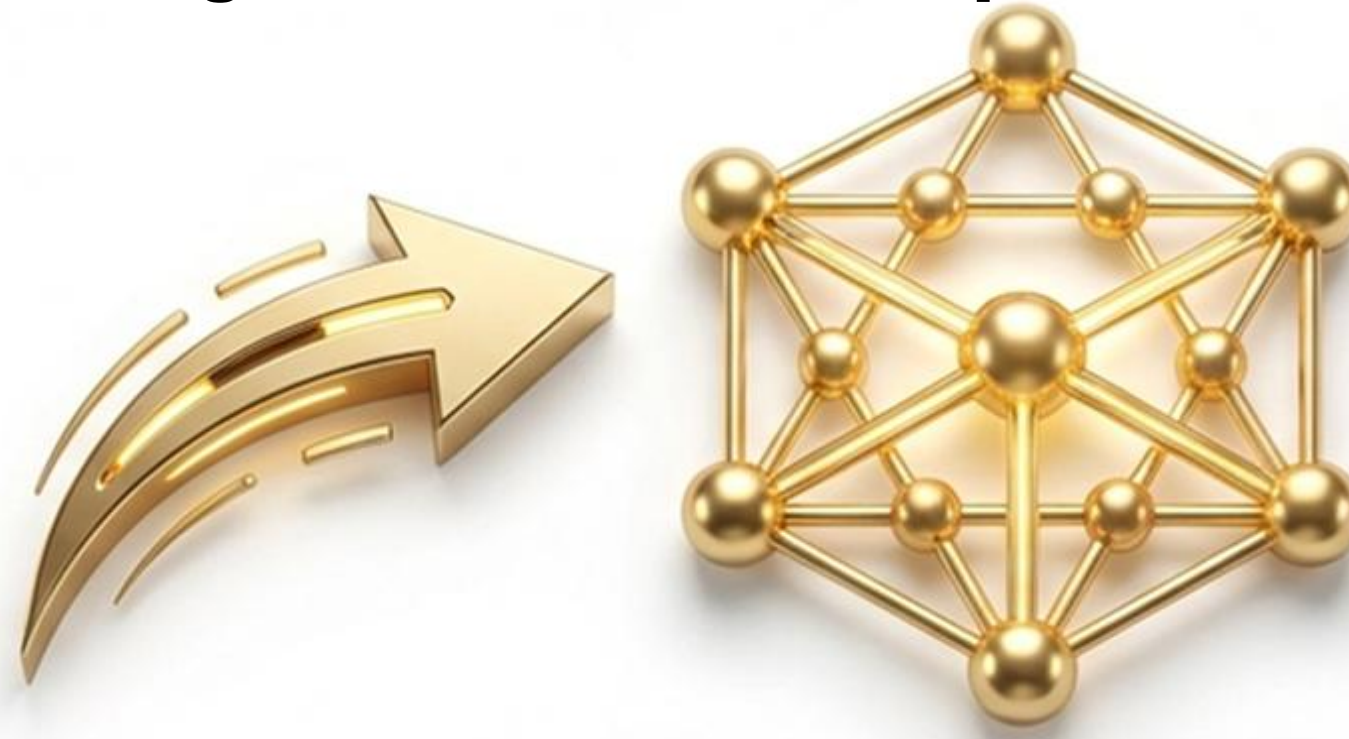
**Engenharia de Prompts, também
nominada recentemente de
Engenharia de Contexto para IA.**

De: Comando Técnico



De: Comando Técnico

Sintaxe rígida, execução linear.



Para: Comunicação Estratégica

Contexto claro, clareza de
objetivo, vocabulário preciso.

A evolução da Inteligência Artificial Generativa exige uma mudança profunda na forma como interagimos com os sistemas computacionais. Deixamos para trás o modelo clássico do 'Comando Técnico' — baseado em sintaxe rígida, lógica estritamente linear e execução de scripts fechados — para adotar a era da 'Comunicação Estratégica'. A Engenharia de Prompt estabelece que o sucesso da entrega não depende de saber programar em linguagens tradicionais, mas sim da habilidade humana de desenhar arquiteturas de instruções focadas em **contexto** claro, clareza de objetivos e precisão de vocabulário, transformando a linguagem natural das IAGs na ferramenta de maior relevância e confiabilidade técnica do mercado.

Objetivo: transformar App de IAG em assistentes privados de trabalho humano.

Técnica 1: Zero-shot Prompting (Fraco)

Mecânica Oculta: Execução direta baseada puramente em instruções claras e vocabulário técnico preciso do qual o modelo já possui amplo treinamento.

OBS.: O Zero-Shot serve como a linha de base (baseline) para avaliar a inteligência bruta de uma IA. Os cientistas de dados usam essa técnica para testar o quanto o modelo realmente aprendeu durante seu treinamento geral, sem precisar de "ajuda" ou pistas contextuais no momento do uso.



Uso Geral

Ação: Classificar contratos por nível de risco jurídico.

: Prestação de serviços, franquia, SaaS, joint venture.

Aplicação IoT

Ação: Classificar protocolos de comunicação por consumo energético.

Alvos: BLE 5.3, Zigbee 3.0, Wi-Fi 6, LoRaWAN, NB-IoT, Z-Wave.

Zero-Shot= Prompt fraco sem exemplo algum – serve para mostrar o nível de compreensão de cada IA – use em 03 IAs diferentes.

Exemplo de prompt Zero-Shot

“Markdown

[TAREFA] Pesquise na internet e apresente um resumo factual sobre as últimas atualizações regulatórias envolvendo o uso de Inteligência Artificial no Brasil publicadas nos últimos 3 meses.

[DIRETRIZES]* Baseie-se apenas em fontes oficiais ou portais de notícias confiáveis.* Inclua as datas das publicações e os órgãos responsáveis pelas medidas.* Não adivinhe ou extrapole informações se não encontrar dados recentes.”

Ancoragem de Segurança: A diretriz para não adivinhar serve para mitigar o risco do modelo misturar notícias reais com especulações antigas do banco de dados dele no treinamento.

Técnica 2: Few-shot Prompting

Mecânica Oculta: Fornecer de 2 a 5 exemplos práticos para ensinar implicitamente o tom, a profundidade e o formato exigidos.

Uso Geral

A técnica consiste em embutir um repositório mínimo de referências no prompt para calibrar o modelo. Em vez de gastar linhas explicando regras gramaticais ou estilos de escrita, você entrega a estrutura pronta. A IA mapeia a sintaxe dos exemplos e passa a replicar o padrão estético.

Aplicação

Utilizada para treinar a IA em tomadas de decisão complexas e triagens analíticas que possuem critérios subjetivos. Ao expor cenários reais emparelhados com as suas respectivas soluções ideais, você ensina o modelo a ponderar variáveis de negócio. Isso elimina a necessidade de criar fluxogramas rígidos de programação, garantindo previsibilidade total nas respostas.



Markdown

[CONTEXTO]

Atue como um Diretor de RH sênior. Vou te passar frases extraídas da nossa pesquisa de clima organizacional e quero que você gere o diagnóstico e o plano de ação.

[EXEMPLOS DE REFERÊNCIA]

Exemplo 1: "Equipe sobrecarregada, mas entrega tudo"

-> Plano: "Risco de Burnout alto. Ação: Revisar capacidade da sprint e travar novas demandas."

Exemplo 2: "Líder centraliza decisões e time se omite"

-> Plano: "Gargalo de liderança. Ação: Workshop de delegação e segurança psicológica."

[TAREFA]

Siga estritamente o tom e o formato dos exemplos acima para analisar a nova frase:

Nova frase: "Colaboradores reclamam de falta de feedback e direcionamento da gestão."

-> Plano:

O que acontece na mente da IA (A Mágica do Few-Shot):

Quando você deixa o prompt parado na última linha (-> **Plano:**), a IA lê os dois exemplos anteriores e compreende o padrão implicitamente. Ela preenche o espaço em branco gerando uma resposta imediatamente no mesmo formato:

Resposta gerada pela IA: "Falha de comunicação interna e liderança. Ação: Implementar rituais de 1-on-1 semanais e matriz de metas clara."

Prompt com poucos exemplos

Técnica 3: Chain-of-Thought (CoT)

Mecânica Oculta: Indução de raciocínio lógico passo a passo antes da conclusão. Cria transparência técnica e reduz erros analíticos em modelos de fronteira.

Quando Aplicar: Análises de risco, diagnósticos técnicos, avaliações regulatórias e problemas com múltiplas variáveis interdependentes.

Uso Geral (ROI de IAG)

Cenário: Empresa com 30 funcionários, custo de plataforma a R\$ 8.000/mês.

Calcular horas gastas

Estimar redução

Converter em custo de mão de obra

Comparar investimento

Concluir

Markdown

[CENÁRIO] Empresa com 30 funcionários avalia ferramenta de IAG que custa R\$ 8.000/mês. O custo médio da hora de trabalho é de R\$ 50.

[TAREFA] Calcule o ROI do investimento utilizando a técnica cadeia de pensamento CoT. Você deve, obrigatoriamente, exibir a memória de cálculo de cada etapa abaixo ANTES de apresentar o veredito final:

1. ****Horas Gastas:**** Total de horas e custo da folha mensal do time.
2. ****Redução:**** Horas economizadas assumindo 15% de ganho de eficiência.
3. ****Conversão:**** Valor monetário do tempo economizado.
4. ****Comparação:**** Ganho financeiro líquido (Valor Economizado - R\$ 8.000).
5. ****Conclusão:**** Veredito de viabilidade e porcentagem final do ROI.

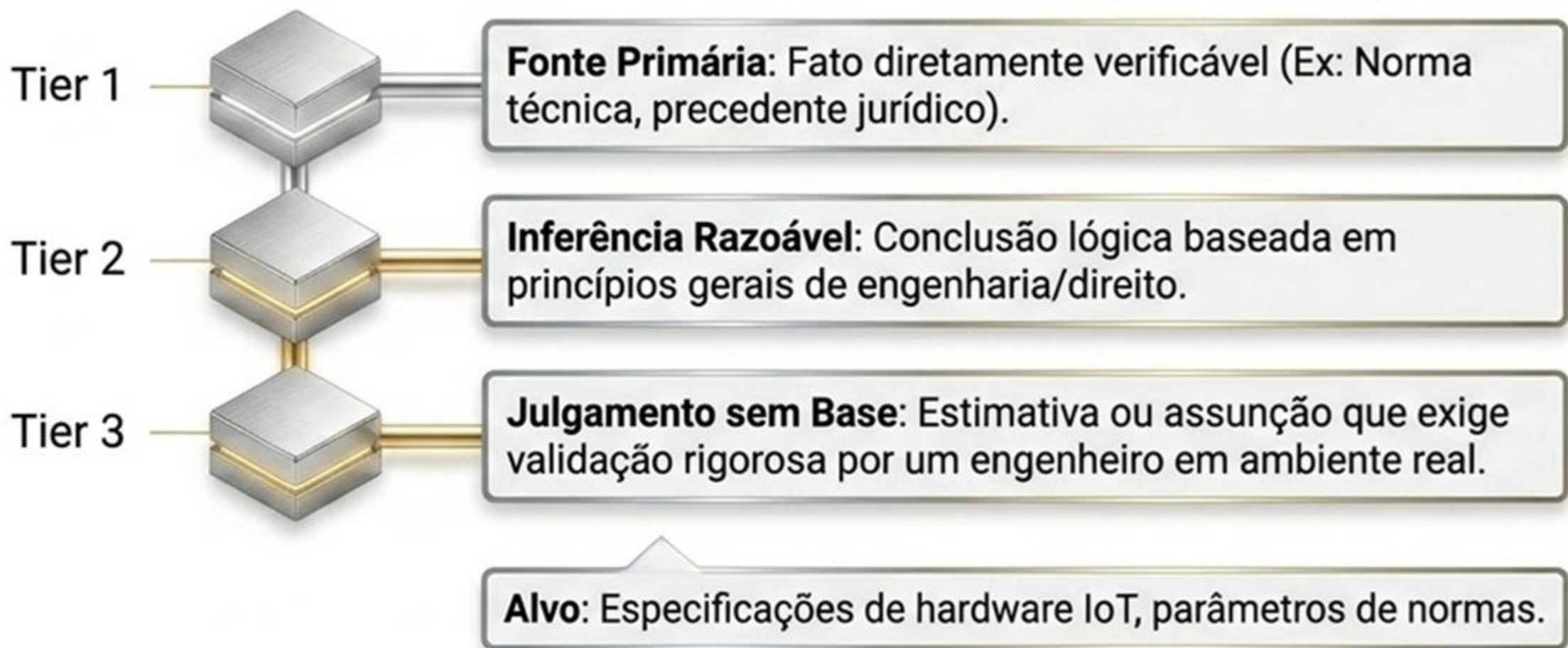
Prompt com Cadeia de Pensamento.

Técnica 4: Chain-of-Verification (CoVe)

Mecânica Oculta: Auditoria reversa. O modelo lista suas próprias afirmações factuais, avalia a confiança e sinaliza onde o humano deve validar.



Taxonomia de Verificação Exigida no Prompt



Prompt com Cadeia de Verificação.

Markdown

[CONTEÚDO] "A migração do ERP local para a nuvem reduzirá os custos de infraestrutura em 40% no primeiro ano, garantirá conformidade total com as normas de auditoria e eliminará completamente as janelas de manutenção aos finais de semana."

[TAREFA] Audite as afirmações acima usando Cadeia de Verificação (CoVe). Classifique cada alegação de acordo com a taxonomia exigida:

****Tier 1 (Fonte Primária):**** O que é fato diretamente verificável em contratos ou SLAs **ANEXOS**?

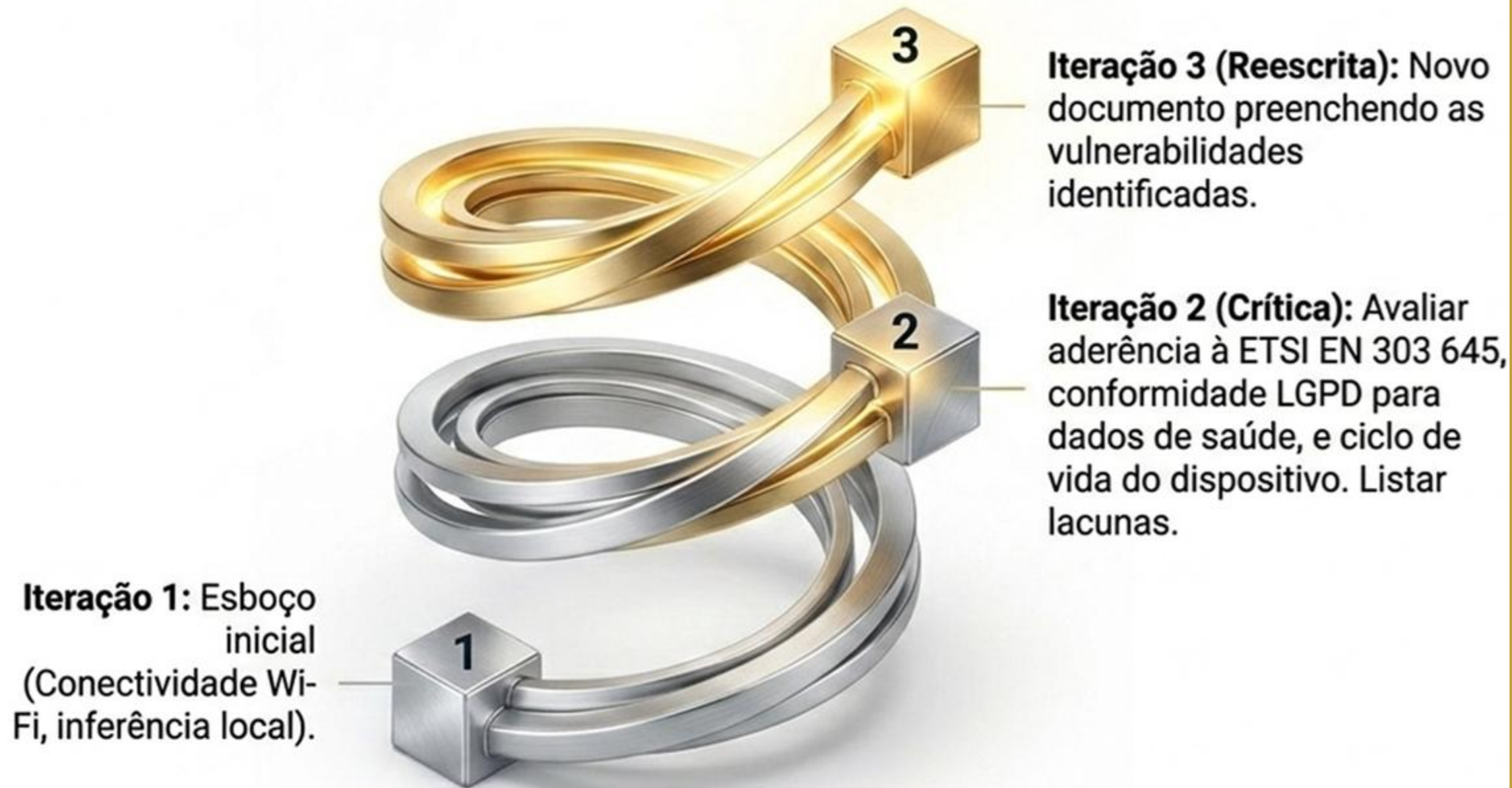
****Tier 2 (Inferência Razoável):**** O que é uma conclusão lógica aceitável pelo mercado?

****Tier 3 (Julgamento sem Base):**** Qual estimativa ou assunção exige validação e cálculo rigoroso?

[ALVO] Valide especificamente os parâmetros de custos e as métricas de disponibilidade declaradas.

Técnica 5: Self-Refine Prompting

Mecânica Oculta: Ciclo iterativo autônomo. O modelo gera, critica o próprio resultado com base em critérios estritos, e reescreve a saída.



Prompt com Auto-refinamento Iterativo.

Markdown

[TAREFA] Crie um plano de implantação de rede corporativa executando um ciclo autônomo de Self-Refine em 3 iterações obrigatórias:

****Iteração 1 (Esboço):**** Gere a primeira versão focando em Conectividade Wi-Fi e processamento local.

****Iteração 2 (Crítica):**** Analise seu próprio esboço anterior. Avalie detalhadamente a aderência à norma ETSI EN 303 645, conformidade LGPD para dados sensíveis e o ciclo de vida dos dispositivos. Liste abertamente todas as lacunas encontradas.

****Iteração 3 (Reescrita):**** Reescreva o documento final, corrigindo e preenchendo as vulnerabilidades que você identificou na autocrítica.

[SAÍDA] Exiba o resultado de cada iteração para demonstrar a evolução do texto.

Matriz de Especialidades: O Framework de Seleção

Técnica	Nome em Português	Melhor Caso de Uso
Zero-shot	Prompt sem exemplos	Tarefas diretas com vocabulário técnico bem definido.
Few-shot	Prompt com exemplos	Quando o padrão ou tom de saída é difícil de descrever em palavras.
Chain-of-Thought	Cadeia de Pensamento	Análises complexas com múltiplas variáveis e diagnósticos técnicos.
Chain-of-Verification	Cadeia de Verificação	Toda resposta que será usada em decisão técnica, contratual ou regulatória.
Self-Refine	Auto-refinamento iterativo	Documentos formais que precisam equilibrar precisão profunda e clareza simultâneas.



Meta Prompting: A IA Engenheira de Si Mesma

Conceito: Do grego meta ('além' ou 'sobre'). Consiste em usar o próprio modelo para pensar e estruturar o prompt antes de executá-lo.

A Mecânica: Modelos de linguagem são hipersensíveis ao contexto. O Meta Prompting não cria capacidades novas na IA; ele elimina a ambiguidade entre o que o humano quer e o que o modelo interpreta.



Meta Prompting é usar a própria IA para planejar, estruturar e aperfeiçoar os comandos que ela mesma vai executar. É como a imagem dos espelhos em uma reflexão interna, onde você pede para a inteligência artificial traduzir a sua intenção no formato ideal que ela mesma melhor compreende, eliminando ambiguidades e improvisos.

A Regra: Quanto melhor o contexto delineado, menor a necessidade de a IA 'improvisar'.

O Gatilho da Alta Fidelidade

“Antes de responder, reescreva este prompt para que seja mais preciso e eficaz. Depois, responda usando essa versão melhorada.”

O Impacto: Uma solicitação genérica é automaticamente transformada em um roteiro estruturado com contexto, consequências e resumos-chave. O limite agora é apenas a sua capacidade de delegar.



O poder da IA não está apenas em responder, mas na capacidade de arquitetar as próprias perguntas.”

Atenção!!!



A versão corrigida e expandida

Para contextos profissionais, vale uma formulação mais completa e muito Importante:

"Antes de responder, analise este prompt e reescreva-o para que seja mais preciso e eficaz.

Na reescrita: mantenha o contexto e as intenções originais; indique o que foi alterado e por quê; aponte eventuais ambiguidades que identificou; apresente a versão reescrita para minha avaliação antes de qualquer execução.

Após minha confirmação explícita, use a versão aprovada para produzir a resposta."

Essa versão faz três coisas que a versão popular não faz:

- ▶ Preserva as intenções originais como critério explícito para ajustes.
- ▶ Exige transparência sobre as mudanças realizadas.
- ▶ Torna a confirmação humana uma etapa obrigatória, não uma opção.

A Evolução Profissional



A maestria da Engenharia de Prompts é o alicerce que transforma a IA de um gerador de rascunhos em um parceiro estratégico de alta fidelidade.

Contudo, as fronteiras de aprendizado continuam se expandindo. Nova técnicas avançadas aqui não exercitadas como ReAct (Raciocínio e Ação Combinados), Tree-of-Thoughts (Árvores de Pensamento para Exploração de Hipóteses), e até **Meta-Prompting**, abrem um novo ecossistema de automação corporativa.

Dominar essa arquitetura de comunicação não é apenas otimizar tarefas; é liderar a governança, a inovação e o futuro da eficiência operacional em qualquer especialidade.

“Do rascunho à estratégia: o verdadeiro valor da IA está na sofisticação do seu comando.”



Encerramento do Bloco 2: Método BCP e Engenharia de Prompts



Concluimos o domínio das bases operacionais com a Metodologia BCP e as estratégias avançadas de Engenharia de Prompts, como a Cadeia de Pensamento e o Meta Prompting.

No entanto, este é apenas o alicerce da nossa jornada; a evolução do workshop nos levará agora à orquestração de fluxos complexos:

- **Nas próximas etapas, exploraremos o Framework ILR e a Metodologia MDM-AI para gerenciar múltiplos agentes de IA, aplicaremos o rigor técnico no Laboratório de Validação e consolidaremos todo esse aprendizado na sua Promptoteca Pessoal.**
- **Prepare-se para transitar de um usuário avançado para um verdadeiro orquestrador de inteligência técnica.**

Obrigado!



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

<https://meet.google.com/wqa-rgfc-dsg>