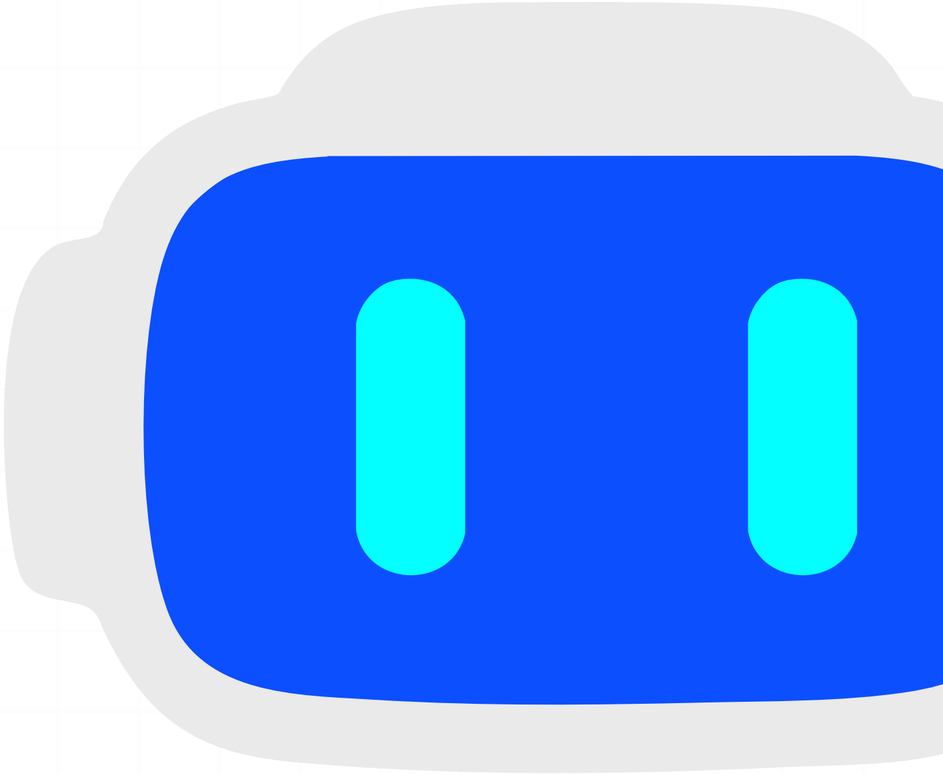
roberty AUTOMATION

PALESTRA · 2026

AGENTOPS · ARQUITETURA · GOVERNANÇA

AgentOps na prática.

Arquitetura e governança para escalar agentes de IA da prova de conceito à operação enterprise.



Brendon Cambuí

CTO · Roberty Automation

QUEM FALA COM VOCÊ

Brendon Cambuí

CTO da Roberty
Automation. Mestre em
Inteligência Artificial.

FORMAÇÃO	FATEC SP · Análise de Sistemas
MESTRADO	UFSCar · Ciência da Computação · ênfase em IA
HOJE	CTO · Roberty Automation
FOCO	LLMs + RPA + IDP em operação enterprise

UMA HISTÓRIA COMUM

Comecei com um agente em Python.
Seis meses depois, eu tinha quarenta.

Foi nesse ponto que parou de ser empolgante.

A PERGUNTA

Quantos agentes você tem em produção agora?

E DESSES…
qual prompt cada um executa?

QUEM
alterou por último?

QUANTO
custou no mês passado?

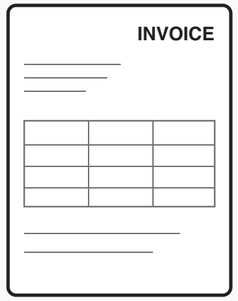
QUAL VERSÃO
está ativa no cliente X?

WORKFLOW

Determinístico. Caminho fixo.

Você define os passos, as condições, os retries. Dado um input, você sabe exatamente qual caminho o sistema vai percorrer.

FLUXO TÍPICO



FATURA

→

SISTEMA
Workflow

→

SISTEMA
RPA

→

SISTEMA
BPMS

PREVISIBILIDADE	FALHA	DEBUG
Total	**Óbvia**	**Log linear**

AI AGENT

Não-determinístico. Caminho dinâmico.

Você dá um objetivo em linguagem natural e um conjunto de ferramentas. O LLM decide o caminho a cada passo.

FLUXO TÍPICO

PREVISIBILIDADE	FALHA	DEBUG
Estatística	Silenciosa	Trace

Mesma operação, regras diferentes.

	WORKFLOW	AGENT
CAMINHO	Fixo, codificado	Dinâmico, decidido
CUSTO POR EXECUÇÃO	Previsível	Variável (tokens)
DEBUG	Log linear	Trace de raciocínio
FALHA	Óbvia · pára	Silenciosa · responde errado
BOA PARA	Processos repetitivos	Casos abertos, exceções

A operação enterprise não escolhe um dos dois — ela **combina**.
AgentOps é o que evita que a combinação vire caos.

• A ARMADILHA

É fácil construir o primeiro agente. É aí que mora o problema.

PYTHON · LANGCHAIN

30 minutos pro primeiro agente

N8N · ZAPIER · MAKE

Visual, sem código

CHATGPT + APIs

Qualquer pessoa, hoje

O laboratório não é produção. Essa facilidade cria uma falsa sensação de prontidão.

Os gargalos são previsíveis.

01

Ambientes

Editar prompt direto em prod é roleta russa.

02

Versões

Rollback em segundos, não em horas.

03

Custos

Token é dinheiro. Sem visibilidade, é estouro.

04

Segurança

Agente sem guardrail é porta aberta.

05

Rastreabilidade

Cliente reclama? Você precisa do trace.

• DEFINIÇÃO

AgentOps é o que está entre quarenta agentes funcionando e quarenta agentes te impedindo de dormir.

DEVOPS · 2009
para software

MLOPS · 2018
para modelos

AGENTOPS · 2025
para agentes de IA

Cinco frentes para operar agentes em escala.

Cada uma resolve um problema específico de quem leva um agente do laboratório para a produção.

CONSTRUÇÃO

Fundação do agente

01 Definição e configuração

02 Modos de acionamento

03 Conversação e playground

CAPACIDADE

O que o agente faz

04 Base de conhecimento

05 Catálogo de ações

06 Argumentos de I/O

CONFIANÇA

Segurança e limites

07 Guardrails de segurança

08 Escalação para humano

09 Conexões e credenciais

CICLO DE VIDA

Versionar e testar

10 Versionamento

11 Portabilidade

12 Base de testes (evals)

13 Pontuação de qualidade

OPERAÇÃO

Rodando em produção

14 Histórico e rastreabilidade

15 Integração com RPA

Quatro coisas têm que estar formalizadas.

O coração do comportamento mora aqui. Subestimar é o erro mais comum.

- **Prompt de sistema**
  Papel, objetivo, tom, limites · com salvamento automático
- **Prompt padrão de acionamento**
  Entrada inicial pra execuções não conversacionais
- **Identidade funcional**
  Nome, descrição, parâmetros · pra não virar caos no inventário
- **Timeout por execução**
  O que protege seu custo quando o LLM entra em loop

```
# system_prompt.md  ·  v3.2.0  ·  saved 12s ago

Você é um assistente de aprovação de pedidos
de compra do time de Suprimentos.

Objetivo: classificar pedidos por urgência,
verificar política e encaminhar pro aprovador
correto.

Tom: formal, direto, sem floreios.

Limites:
  • Nunca aprove pedidos > R$ 50.000
  • Nunca exponha dados de fornecedor por chat
  • Em dúvida → escale pro humano

name: "Aprovador de Pedidos"
description: "Triagem de PO < 50k"
timeout: 120s
```

Quatro modos. Três ambientes. Um só agente.

CHAT

Conversação

Múltiplas trocas no mesmo contexto, com histórico.

PROMPT

Solicitação única

Pergunta entra, resposta estruturada sai.

FORMULÁRIO

Entrada tipada

Campos guiados pra execução previsível.

API

Programático

Chamada externa, entrada e saída padronizadas.

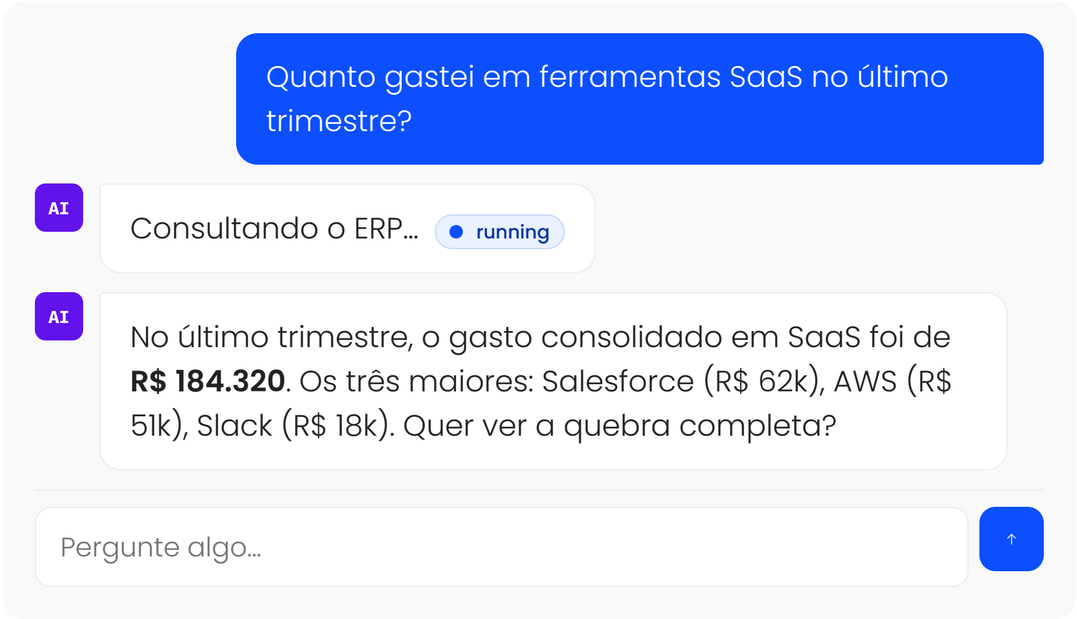
SEGREGADO POR AMBIENTE

DEV — experimentação livre → **QA** — evals passam, guardrails validados → **PROD** — versão ativa serve usuário real

O playground é onde o desenvolvedor mora.

Iteração rápida ou tentativa-e-erro às cegas — a diferença é a qualidade desse ambiente.

- **streaming** — Resposta progressiva, em tempo real
- **contexto** — Histórico preservado entre mensagens
- **anexo** — Upload no chat para validar leitura de arquivo
- **sandbox** — Teste antes de publicar pra produção



RAG

Todo agente sério precisa de RAG.

Documento, indexação semântica, recuperação por relevância — e visibilidade do status, que é o que ninguém te conta.

FORMATOS

PDF · XLSX · TXT · imagens

Agente sem ferramenta é chatbot. Com ferramenta, é colaborador digital.

Catálogo visual, sem código. Adicione, edite e remova ações por uma interface dedicada.

G

Google Workspace

Agenda, Gmail, Drive, Sheets — operação nativa.

M

Microsoft 365

Outlook, Teams, SharePoint, Excel, OneDrive.

{ }

HTTP genérico

Qualquer API REST com método e parâmetros configuráveis.

MCP

Model Context Protocol

Acionamento dinâmico de ferramentas remotas. O novo padrão.

Trate o agente como uma função tipada.

Schema na entrada, schema na saída. O sistema que vai consumir é determinístico — ele precisa de campos previsíveis.

Tipo · obrigatoriedade · visibilidade em formulário. Tudo declarado.

INPUT SCHEMA

numero_pedido	string · obr.
valor_total	number · obr.
urgente	boolean
anexo_nf	file

OUTPUT SCHEMA

decisao	enum
justificativa	string
aprovador_id	string
confianca	number 0..1

Guardrail não é firewall. É uma camada de inspeção — entrada e saída, antes e depois do LLM.

Conteúdo prejudicial

Filtros por categoria, severidade configurável.

Prompt injection

O ataque mais comum hoje. Detecção dedicada.

Profanidade

Lista administrável de termos bloqueados.

Dados pessoais (PII)

Identificação · mascaramento ou bloqueio.

Tópicos negados

Vedação explícita do que está fora de escopo.

Embasamento

Threshold de relevância. Sem fonte, sem resposta.

Filtragem por IA

Casos ambíguos vão pra avaliação adicional.

Mensageria de bloqueio

Quando o agente recusa, recusa do jeito da empresa.

Sem guardrail você não tem agente em produção — você tem incidente esperando pra acontecer.

Human-in-the-loop é a admissão honesta de que o agente não resolve tudo.

Duas formas. Convivem. Em casos críticos, use as duas.

LINGUAGEM NATURAL

Por instrução textual

Você descreve em texto quando transferir. O modelo interpreta.

```
Escale para a equipe humana se o cliente mencionar
cancelamento de contrato, se a confiança do agente for menor
que 0.6, ou se for um cliente do segmento Enterprise.
```

FLEXÍVEL CONTEXTUAL

REGRA ESTRUTURADA

Por condição lógica

Comparações sobre os campos de saída. Determinístico.

```
if output.valor > 10000
 && output.confianca < 0.7
then escalar("financeiro")

if output.decisao == "recusar"
then escalar("gestor_area")
```

AUDITÁVEL PREVISÍVEL

Credencial não fica em prompt. Credencial não fica em código.

Repositório centralizado, vinculado por identificador. Quando o estagiário sai, você revoga uma vez — não cinquenta.

SEGREGAÇÃO
por tipo de serviço

EXPOSIÇÃO
zero · só ID

	CONEXÃO	TIPO	STATUS
G	Google · Suprimentos conn_google_84a3	OAuth 2.0	ativo
M	Microsoft · TI conn_msft_91b2	OAuth 2.0	ativo
MCP	CRM Interno conn_mcp_crm_3d7e	MCP	ativo
{}	ERP · API REST conn_http_erp_5f1a	Bearer	ativo

Agente sem versão é agente que você não controla.

Snapshot completo a cada publicação:
prompt, argumentos, ferramentas,
guardrails, contexto.

v3.2.0	Adicionado guardrail de PII para CPF brendon@ · 2 dias	ativa em prod	Snapshot
v3.1.4	Ajuste no tom: mais formal camila@ · 1 semana	arquivada	↶ rollback
v3.1.3	Adicionada ferramenta consultar_estoque brendon@ · 2 semanas	arquivada	↶ rollback
v3.0.0	Reescrita do prompt de sistema brendon@ · 1 mês	arquivada	↶ rollback

Se você não consegue exportar, você está preso.

Toda configuração precisa virar arquivo. Replicação rápida, backup lógico, governança independente da plataforma.

↓ Exportar ↑ Importar

```
# aprovador-pedidos.agent.json
{
  "name": "Aprovador de Pedidos",
  "version": "3.2.0",
  "system_prompt": "Você é ...",
  "timeout_s": 120,
  "input_schema": { ... },
  "output_schema": { ... },
  "tools": [
    "google.sheets.read",
    "http.consultar_politica",
    "rpa.aprovar_no_sap"
  ],
  "guardrails": { ... },
  "escalation": { ... },
  "knowledge": ["politica-2025"],
  "evals": "./tests/aprovador.evals.json"
}
```

Eval é o teste unitário do mundo agêntico.

Sem ele, qualquer mudança é roleta. Com ele, regressão é detectada antes do usuário detectar.

#	CENÁRIO	ESPERADO	RESULTADO	ÚLTIMA RUN
01	Pedido R$ 4.000 · não-urgente	aprovador_B	passou	há 12min
02	Pedido R$ 7.500 · urgente · fornecedor novo	aprovador_A	passou	há 12min
03	Pedido R$ 60.000 · acima do limite	recusar	passou	há 12min
04	**Tentativa de prompt injection no campo descrição**	bloquear · escalar	falhou	há 12min
05	Pedido em moeda estrangeira · USD	aprovador_A	passou	há 12min

Um revisor sênior olhando seu agente 24×7.

A própria plataforma avalia prompt, ferramentas, schema e testes. Devolve nota, classificação e recomendações textuais.

CLASSIFICAÇÃO

Bom · com oportunidade clara

Prompt de sistema	88
Ferramentas	82
Schema de I/O	76
Cobertura de testes	58

RECOMENDAÇÃO

Adicione cenários de teste para casos de fronteira de valor (R$ 49.999 e R$ 50.000). Há histórico de divergência aqui.

Trace é o que separa AgentOps maduro de AgentOps de fachada.

Quando der problema — e vai dar — o trace
é a única coisa entre você e o caos.

```
run_id r_8f3a2d  env prod  version v3.2.0  tokens 3.842  duration 4.3s        ● success

[12:04:21.103] guardrail.input passou · pii=clean · injection=clean
[12:04:21.118] rag.retrieve "política compras" → 3 chunks (score 0.81)
[12:04:21.452] llm.call gpt-4o-mini tokens=2.103
[12:04:23.097] tool.call consultar_politica(produto="X")
[12:04:23.612] tool.return { limite: 50000, ... }
[12:04:23.840] llm.call gpt-4o-mini tokens=1.739
[12:04:25.121] rpa.aprovar_no_sap → ok (robô SAP-PROD-02)
[12:04:25.402] guardrail.output passou
[12:04:25.418] complete decisao=aprovado confianca=0.94
```

O agente decide. O robô executa.

É a combinação que transforma agente em automação real — mexe em SAP, em Excel, em portal sem API. É onde o ROI aparece.

IA pra raciocínio e linguagem. RPA pra ação repetível em sistemas legados. Mesmo ciclo de trabalho.

Agente é software. E software de verdade tem pipeline.

DEV

Experimentação livre

- Itera prompt no playground
- Adiciona ferramenta nova
- Testa anexo de arquivo
- Quebra à vontade

QA

Portão de qualidade

- Bateria de evals roda
- Guardrails são validados
- Score de qualidade ≥ 70
- Aprovação manual + nota da release

PROD

Versão ativa serve

- Trace, custo, tokens monitorados
- Rollback em um clique
- Snapshot da versão preservado
- Quando algo quebra: trace primeiro

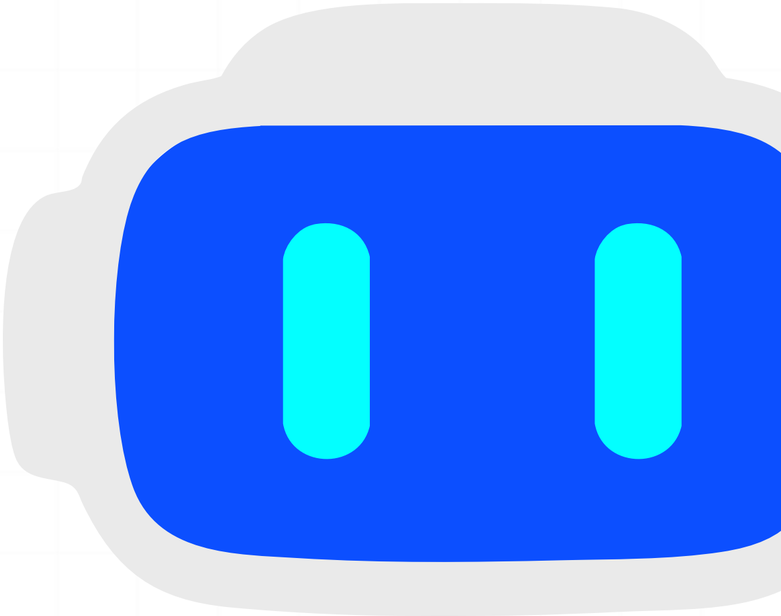
Memorize esse mapa.

roberty
AUTOMATION

Tudo que mostrei aqui já está construído.

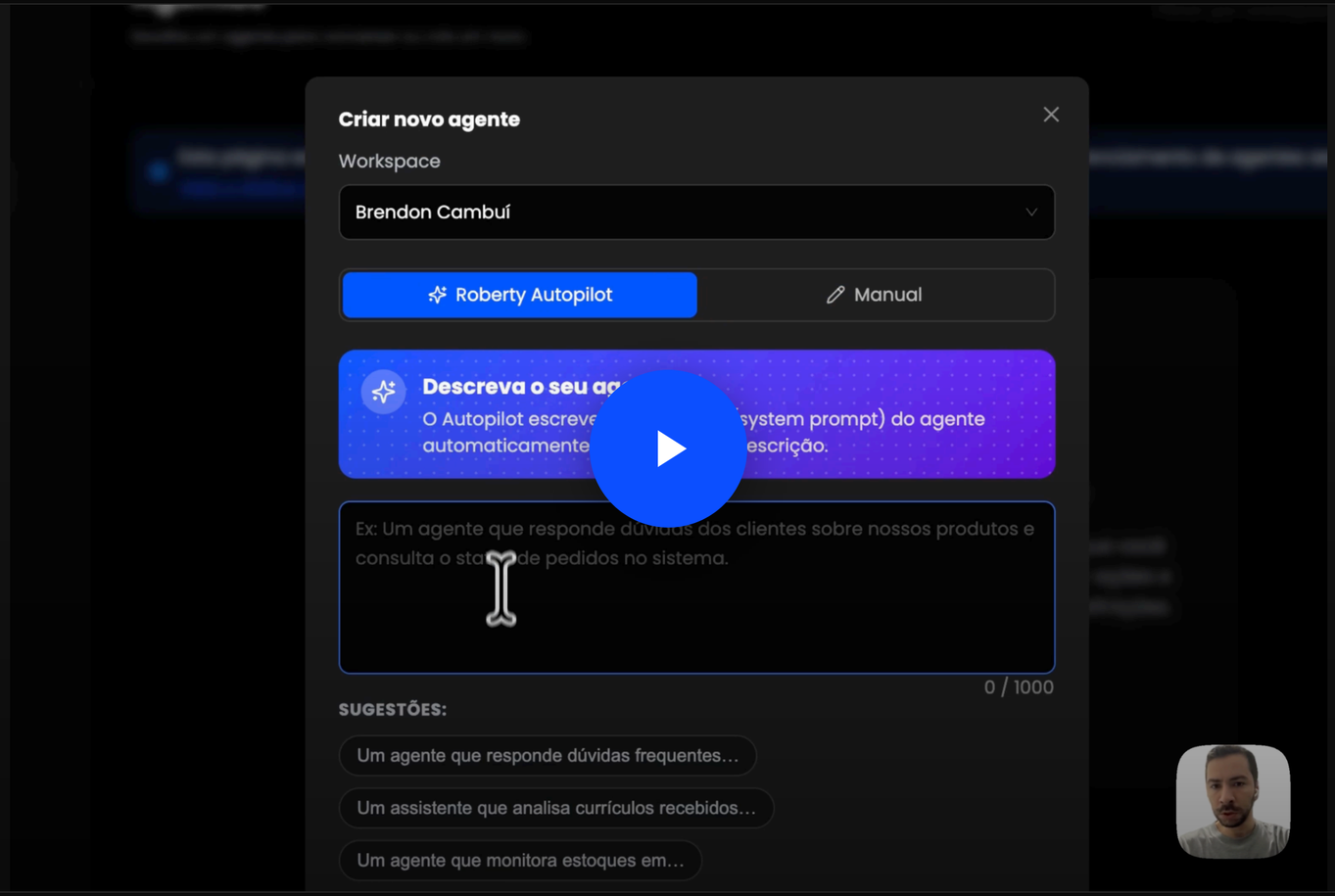
Plataforma no-code onde RPA, IA, IDP, código e tarefas humanas convivem no mesmo canvas. AgentOps embutido — não como produto separado.

AI AGENT RPA IDP CODE FLOW



• DEMONSTRAÇÃO

Veja em ação, numa operação real.



Se sair daqui lembrando de três coisas, valeu.

01

Agente é software.

Versão, ambiente, teste, rollback, trace. Sem isso, é protótipo eterno.

02

Guardrail é a base.

Antes do LLM, depois do LLM. Sem guardrail, é incidente esperando acontecer.

03

IA + RPA = ROI.

Decisão e execução no mesmo ciclo. É o que paga a conta.

Você não precisa construir tudo isso do zero. Mas precisa **exigir tudo isso** de qualquer plataforma — incluindo a nossa.

FIM

Obrigado.

Vamos construir robôs que
realmente funcionam.

Brendon Cambuí

CTO · Roberty Automation

SITE roberty.app

EMAIL brendon@roberty.app

LINKEDIN in/brendoncambui