EVSOLID · CONTEÚDOS

O agente de IA vai virar commodity. Quem controla o agente, não.

Agentes de IA estão ficando mais fáceis de criar, mais baratos de operar e cada vez mais parecidos nas tarefas que executam. Isso não torna a tecnologia irrelevante. Muda o lugar onde está o valor: a vantagem duradoura tende a sair do agente isolado e migrar para o sistema que define sua identidade, suas permissões, suas alçadas e sua responsabilidade.

RESPOSTA DIRETA

O valor está na governança da execução

Um agente é capaz de agir; uma camada de controle decide quem ele é, o que pode fazer, quanto pode gastar, quando deve pedir aprovação e como suas ações serão auditadas. É essa camada que transforma uma demonstração de IA em operação empresarial.

Neste artigo

1. Por que o agente tende a virar commodity
2. A lição do ERP
3. O problema não é só capacidade
4. Sete perguntas da camada de controle
5. Exemplo: um agente de cobrança

6. O que muda para quem compra e constrói

Por que o agente tende a virar commodity

Toda semana surge um agente novo: para atendimento, conciliação, código, compras ou análise de documentos. A barreira técnica para criar uma dessas experiências está caindo porque modelos, conectores e ferramentas de automação se tornam mais disponíveis.

Quando uma capacidade fica simples de replicar, ela não desaparece — mas deixa de concentrar sozinha o valor. O diferencial passa a ser o contexto que ninguém copia de um dia para o outro: regras de negócio, dados confiáveis, integração com processos, responsabilidade e confiança operacional.

Essa é a tese de **Keoma Cherulli**, CEO & Founder da EVSolid: o agente é a capacidade de executar; o sistema que governa essa capacidade é o que permite operar em escala.

A lição do ERP: executar é diferente de governar

O software empresarial já passou por uma transformação parecida. Nas décadas de 1980 e 1990, armazenar dados era caro e complexo. Com o amadurecimento da infraestrutura, bancos de dados se tornaram uma base indispensável, mas amplamente disponível.

O valor do ERP nunca esteve apenas em guardar uma informação. Ele está em fazer a regra da empresa acontecer: definir quem lança uma nota, quem aprova um pagamento, até qual valor, com quais documentos e para onde uma exceção é escalada.

Com agentes, o paralelo é útil. O modelo e o agente executam. A empresa ainda precisa da camada que define quando podem executar, em nome de quem e com quais limites. Em nosso artigo sobre cargo, gestor e limite de alçada, explicamos por que dar uma função operacional a um agente não é burocracia: é clareza de responsabilidade.

O problema raramente é o que o agente sabe fazer

Um agente pode ter uma tarefa legítima e ainda cruzar uma fronteira de negócio. Isso acontece quando regras ficam espalhadas entre prompts, credenciais excessivas, conhecimento informal e integrações que não registram contexto.

Os sinais aparecem rápido: permissões maiores que a tarefa exige; custo de API sem orçamento; decisões sem trilha de autorização; dificuldade para separar ações humanas de ações automatizadas; e ausência de um ponto claro para pausar a operação.

Em 2025, a Gartner projetou que mais de 40% dos projetos de IA agêntica seriam cancelados até o fim de 2027, citando custos crescentes, valor de negócio pouco claro e controles de risco inadequados. Os três fatores apontam menos para uma limitação de inteligência e mais para uma limitação de gestão.



Um agente útil precisa operar com permissão mínima, alçada definida e evidências para auditoria.

Sete perguntas que a camada de controle precisa responder

O sistema que controla agentes fica entre pessoas, agentes e sistemas corporativos. Ele não precisa executar toda tarefa; precisa tornar a execução governável.

1. **Quem é este agente?** Identidade própria, cargo, departamento e um gestor humano responsável — nunca a senha de uma pessoa reutilizada.
2. **O que ele acessa?** Sistemas, dados e permissões mínimas necessárias para cumprir a tarefa.
3. **Até onde decide sozinho?** Alçadas por valor, volume, tipo de ação e risco. Acima disso, o fluxo escala para uma pessoa.
4. **Quanto pode gastar?** Limites para tokens, chamadas de API, recursos de infraestrutura e transações financeiras, com alertas e bloqueios.
5. **O que fez e por quê?** Registro da ação, do contexto usado, das regras aplicadas e da justificativa.
6. **Está entregando resultado?** Metas e indicadores por agente: qualidade, prazo, taxa de exceção, economia ou recuperação de receita.
7. **Como ele para?** Um ponto único para pausar, revogar acesso ou desligar o agente sem depender de quem o configurou.

Essas perguntas também tornam o software mais seguro para agentes externos. Como discutimos em software para agentes de IA, não basta expor uma API: é preciso oferecer contexto, contratos claros, permissões e rastreabilidade.

Exemplo prático: um agente de cobrança

Imagine um agente de cobrança em uma empresa de médio porte. Sem uma camada de controle, ele recebe uma instrução vaga para reduzir inadimplência, acesso ao ERP e ao e-mail. A automação pode funcionar até conceder um desconto não autorizado ou cobrar um cliente que já negociou diretamente com o gerente.

Identidade

Analista de Cobrança Digital, na área Financeira, com gestor humano.

Permissões

Consulta títulos e envia mensagens pelo canal oficial; não altera cadastro ou títulos.

Alçada

Propõe parcelamentos até R$ 2.000; acima disso, encaminha para aprovação.

Orçamento

Limite mensal de consumo de API, com alerta antecipado e bloqueio configurável.

Auditoria

Mensagens e propostas ficam no histórico do cliente, identificadas como ação do agente.

Indicador

Redução da inadimplência acima de 30 dias, com qualidade e exceções acompanhadas.

O modelo de IA pode ser exatamente o mesmo. O que muda é a gestão em volta dele — e é isso que permite ampliar a automação sem ampliar o risco na mesma proporção.

O que muda para quem compra e para quem constrói software

Para quem compra tecnologia, a pergunta evolui de “qual agente é mais inteligente?” para “como vamos administrar dez, cinquenta ou cem agentes?”. Um agente brilhante sem controle pode virar um risco; um agente suficiente, bem governado, pode se tornar uma operação confiável.

Antes de colocar qualquer agente em produção, vale perguntar ao fornecedor ou ao time interno: ele tem identidade própria? Onde estão as regras e quem pode alterá-las? É possível auditar o último mês de ações? Existem limites de gasto e alçada? O desligamento leva segundos ou depende de uma intervenção técnica?

Para quem constrói software, a oportunidade é justamente a camada que conecta agentes às regras, aos processos e às pessoas de cada empresa. Criar agentes tende a ficar mais acessível; administrar trabalhadores digitais dentro de uma operação real continua específico e difícil de copiar.

PERSPECTIVA DE KEOMA CHERULLI

“Na era dos sistemas, quem tinha só o banco de dados tinha infraestrutura. Quem tinha o ERP tinha a operação. Na era dos agentes, quem tiver o sistema que os controla terá a operação.”

A pergunta que fica

Agentes de IA não substituem governança; eles tornam a governança mais urgente. A empresa que apenas conecta ferramentas e amplia credenciais pode ganhar velocidade no início, mas perde visibilidade quando a operação cresce.

Por isso, como propõe Keoma Cherulli, a pergunta estratégica não é apenas quais agentes criar. É quem — ou o que — vai mandar neles.

Artigos recomendados

Continue a leitura com estes conteúdos:

- Agentes de IA precisam de cargo, gestor e limite de alçada
- Software para agentes de IA: como pensar além da experiência humana
- O que o Ozempic pode ensinar sobre o futuro da inteligência artificial