



OPINIÃO

Por que a governança de IA se tornou o maior desafio dos CTOs?

Fernando Carniel (*)

O hype em torno da Inteligência Artificial no desenvolvimento de software costuma focar no 'autocomplete mágico' da promessa sedutora de que ela escreverá sistemas inteiros enquanto o time toma café, multiplicando a produtividade de forma exponencial.

No entanto, para líderes de TI e engenharia de software que lidam com sistemas críticos corporativos, a realidade nas trincheiras é bem menos glamourosa.

A constatação que começa a ecoar nos corredores das grandes empresas de tecnologia é clara: dar acesso à IA para um time de desenvolvimento sem um processo estabelecido é como liberar deploy em produção sem testes. A sensação inicial é de velocidade, mas a conta chega rapidamente em forma de retrabalho, decisões inconsistentes e um perigoso débito técnico.

A popularização de ferramentas baseadas em agentes fez com que a IA deixasse de ser apenas assistiva, passando a influenciar diretamente decisões de implementação e arquitetura. O problema é que, sem governança, modelos genéricos passam a tomar decisões técnicas importantes sem qualquer alinhamento com a estratégia do produto ou os padrões do time.

Para evitar que a adoção de IA se transformasse em um passivo arquitetural, é necessário formalizar etapas que costumam ser ignoradas na pressa do dia a dia. A conclusão que tive, ao longo da minha experiência na Qive, é: a IA não deveria decidir arquitetura sozinha, mas operar dentro de um fluxo onde contexto, revisão e execução fossem claramente separados.

Esse novo framework operacional baseia-se em três pilares fundamentais que servem de modelo para o mercado:

1. A regra de ouro: não gerar código antes do alinhamento

A primeira fase do fluxo estruturado proíbe que qualquer linha de código seja gerada antes de um alinhamento técnico humano. Em vez de atuar como uma mera geradora de scripts, a IA é utilizada inicialmente como uma parceira de system design. Ela conduz o time em um brainstorming para levantar dependências, identificar riscos e gerar uma especificação.

Apenas após a aprovação desta especificação técnica, a execução do código é autorizada. O racional é simples: uma especificação rejeitada custa minutos, mas um código reescrito por falta de alinhamento custa horas ou dias.

2. Criação da memória operacional do projeto

Sem contexto, qualquer IA responde de forma genérica. Para resolver isso, a governança exige a criação de uma "memória operacional do projeto". E isso pode ser feito através de arquivos de contrato (como o AGENTS.md) que ditam a arquitetura de diretórios, padrões internos e, sobretudo, os antipadrões e o que explicitamente não deve ser feito pela IA.

Além disso, a adoção de servidores MCP (Model Context Protocol) permite que os agentes consultem automaticamente dados estruturados e em tempo real em ferramentas como Jira e Notion, garantindo que o robô já inicie a sessão compreendendo as regras de negócio.

3. O humano como guardião absoluto

Um detalhe inegociável na era da IA é que o fluxo não elimina a etapa de revisão final humana. Quando a inteligência artificial absorve a digitação do código a partir de um plano validado, o Code Review deixa de ser uma caça a erros de sintaxe e passa a focar no que realmente importa: a segurança, a legibilidade e a qualidade da implementação. A IA escreve, mas o time continua sendo o guardião absoluto do que vai para produção.

Com esses três insights, é possível dizer que a IA não está substituindo o pensamento crítico; paradoxalmente, ela está elevando o nível técnico das discussões humanas ao forçar os times a formalizarem decisões, criarem documentações vivas e exigirem clareza arquitetural.

Para as empresas que ainda estão patinando na adoção de IA, a lição mais valiosa do mercado atual é: pare de buscar o prompt perfeito e comece a desenhar o fluxo de trabalho. Ferramentas e modelos evoluirão a cada trimestre, mas processos de engenharia bem desenhados continuam sendo o principal fator que separa a verdadeira velocidade do caos. A maior mudança trazida pela IA não é a automação do código em si, mas a necessidade inadiável de amadurecer os processos de engenharia corporativos.

(*) Staff Engineer na Qive.

Carros elétricos vendem cada vez mais na Alemanha

Pela primeira vez, em junho passado, os carros totalmente elétricos foram os campeões de vendas na Alemanha.

Vivaldo José Breternitz (*)

Naquele mês, foram vendidos 84.057 veículos desse tipo, um salto de 78,2% em relação ao mesmo mês do ano anterior, garantindo um market share de 28,4%. Os híbridos tradicionais ficaram logo atrás, com 83.315 unidades (28,1%), seguidos pelos movidos a gasolina (60.796, 20,5%), diesel (33.862, 11,4%) e híbridos plug-in (32.212, 10,9%).

Dentre os elétricos, o Tesla Model Y liderou com 6.023 unidades vendidas, conquistando o terceiro lugar geral. O Volkswagen ID.3 ficou em segundo entre os elétricos (3.514), seguido pelo Skoda Enyaq (3.383). No total, o mercado alemão recebeu 296.378 novos carros em junho, uma alta de 15,7% na comparação com junho de 2025.

A Volkswagen manteve a liderança absoluta com 51.058 unidades, seguida por BMW e Skoda. Apesar da entrada acelerada de montadoras chinesas na Europa, os elétricos mais vendidos no país ainda são de marcas europeias e americanas.

Esses números são significativos, pois a Alemanha é o maior mercado automotivo da Europa e o berço do motor a combustão. É a terra das Autobahnen e de gigantes como Volkswagen, BMW e Mercedes-Benz, que construíram uma reputação baseada em combustíveis fósseis; ver os elétricos assu-



PhonlmaiPhotos_Images_CANVA

miem a dianteira, ainda que por margem estreita sobre os híbridos, mostra que a transição chegou ao coração da cultura automotiva europeia.

Apesar do avanço, apenas 4,1% dos veículos que rodam na Alemanha são elétricos. A maioria esmagadora, 59,3%, ainda é movida a gasolina. Custos crescentes de baterias e de componentes pressionam a indústria e retardam a queda de preços dos elétricos.

O resultado de junho revela que os alemães não rejeitam a eletricidade ao

comprar novos carros, mas a eletrificação da frota será lenta.

No Brasil, os elétricos vivem um cenário diferente: a liderança, por ampla margem, é da BYD. No primeiro semestre de 2026 foram vendidos cerca de 90,6 mil veículos totalmente elétricos, um crescimento de quase 200% em relação ao mesmo período de 2025. O mercado de híbridos somou 215 mil unidades, totalizando 16% das vendas nacionais de veículos leves.

(*) Doutor em Ciências pela Universidade de São Paulo, é professor, consultor e diretor do Fórum Brasileiro de Internet das Coisas – vjnit@gmail.com.

Primeiro ataque de ransomware conduzido por um agente de IA acende alerta

Um ataque identificado pela empresa de cibersegurança Sysdig, neste mês de julho, acendeu um novo alerta para especialistas em segurança digital. Batizada de JADEPUFFER, a campanha é descrita pela Sysdig como o primeiro caso documentado de ransomware conduzido por um agente de inteligência artificial. Segundo os pesquisadores, o agente foi capaz de executar de forma amplamente autônoma diversas etapas técnicas da invasão após receber objetivos definidos por um operador humano. A descoberta representa uma mudança importante na evolução das ameaças cibernéticas, ao indicar que agentes baseados em modelos de linguagem já podem coordenar, de forma automatizada, diferentes etapas de ataques complexos em velocidade de máquina.

Segundo a Sysdig, o agente explorou uma instância vulnerável do framework Langflow por meio da falha CVE-2025-3248, coletou credenciais, movimentou-se lateralmente pelo ambiente, estabeleceu persistência e chegou ao banco de dados de produção da vítima, onde executou a extorsão. Durante toda a operação, os próprios códigos utilizados continham descrições em linguagem natural explicando o raciocínio adotado pelo modelo, além de demonstrarem capacidade de adaptação em tempo real. Em uma das etapas, o sistema corrigiu sozinho uma tentativa de acesso malsucedida em apenas 31 segundos.

Embora nenhuma das técnicas utilizadas seja inédita isoladamente, pesquisadores apontam que o diferencial está na capacidade de um único agente de IA coordenar automaticamente grande parte das fases técnicas da operação, reduzindo significativamente a necessidade de conhecimento técnico por parte dos criminosos e acelerando ataques que antes dependiam de intensa atuação humana.



newrrp CANVA

Para o especialista em cibersegurança Rodolfo Almeida, COO da ViperX, startup do Grupo Dfense Security, o episódio representa uma mudança de paradigma na forma como ataques de ransomware passam a ser executados. "O mais preocupante não é uma nova técnica, mas a capacidade da IA conectar diferentes etapas em uma única operação. Isso reduz a barreira de entrada para criminosos e encurta o tempo de reação das equipes de segurança."

Brasil já reúne condições que favorecem esse tipo de ataque

O alerta também é relevante para o cenário brasileiro. Embora o caso tenha ocorrido no exterior, o avanço de ataques cibernéticos apoiados por agentes de IA já faz parte das preocupações das autoridades nacionais. Em 2025, a Agência Brasileira de Inteligência (Abin) incluiu os ataques cibernéticos autônomos apoiados por agentes de IA entre os desafios de inteligência considerados relevantes para o Brasil em 2026.

Ao mesmo tempo, cresce o número de empresas adotando plataformas de IA generativa, agentes autônomos e frameworks como o Langflow para desenvolver aplicações corporativas. Nesse contexto, ambientes de IA expostos à internet passam a representar um novo vetor de risco quando não recebem atualizações de segurança e controles adequados de acesso.

A principal preocupação não está apenas na vulnerabilidade explorada pelo agente, mas na forma como as organizações administram credenciais privilegiadas e aplicações de IA. "Ambientes de IA frequentemente precisam acessar bancos de dados, APIs e serviços de nuvem. Se uma aplicação exposta também tiver acesso a credenciais permanentes e privilegiadas, pode acelerar toda a cadeia de ataque. Atualização, menor privilégio, cofres de senha e monitoramento deixam de ser controles opcionais", explica Almeida.

Como as empresas podem se proteger

Entre as principais recomendações dos especialistas estão:

- aplicação imediata de correções de segurança em plataformas de IA expostas à internet;
- eliminação de credenciais padrão, adoção de cofres de segredos (vaults) e rotação periódica de credenciais privilegiadas;
- implementação de acesso just-in-time e monitoramento contínuo de atividades suspeitas.

Essas medidas tornam-se ainda mais importantes diante de ataques capazes de evoluir em segundos, reduzindo significativamente a janela de resposta das equipes de segurança, enquanto o tempo médio de reação das organizações ainda costuma ser medido em horas.

News@TI

NVIDIA Agent Toolkit

A NVIDIA anuncia que o NVIDIA Agent Toolkit agora inclui as bibliotecas do NVIDIA Omniverse™, uma coleção de componentes de software que fornecem aos agentes de IA as ferramentas e habilidades necessárias para agregar recursos de IA física a aplicações existentes e preparar conteúdo 3D para simulação. Robôs, fábricas e sistemas autônomos devem ser projetados, testados e treinados por meio de simulação antes de poderem funcionar no mundo real (<https://developer.nvidia.com/omniverse>).

Inteligência artificial para reduzir em 40% o tempo de análise documental

A The House, vertical do Grupo Teddy Open Finance especializada em crédito imobiliário, colocou em operação neste mês uma solução de inteligência artificial para automatizar a pré-validação documental em operações de crédito imobiliário. Desenvolvida para reduzir um dos principais gargalos da concessão de crédito, a tecnologia deve diminuir em cerca de 40% o tempo médio de análise das pastas documentais, mantendo a decisão final sob responsabilidade dos especialistas (<https://thehouse.com.br/>).

Empresas & Negócios

José Hamilton Mancuso (1936/2017)

Responsável: Lilian Mancuso

Editorias

Economia: Nelson Tucci (nelson.tucci@netjen.com.br)
Mercado/Negócios/Tecnologia/Agronegócios/
Espaço empresarial: Ricardo Souza (ricardosouza@netjen.com.br);
Livros: Ralph Peter (ralphpeter@agenteliterarioralph.com.br)
Comercial: comercial@netjen.com.br
Publicidade Legal: lilian@netjen.com.br

Colaboradores: Ana Luisa Winckler, Carol Olival, Claudia Lazzarotto, Denise Debiasi, Fabiana Monteiro, Geraldo Nunes, Heródoto Barbeiro e Neiva Mendes

Laurinda Machado Lobato (1941-2021)

José Leonil Lobato (1939-2026)

Webmaster/TI: Fabio Nader; Editoração Eletrônica: Ricardo Souza.
Revisão: Maria Cecília Camargo; Serviço informativo: Agências Brasil, Senado, Câmara, EBC, ANSA.

Artigos e colunas são de inteira responsabilidade de seus autores, que não recebem remuneração direta do jornal.

ISSN 2595-8410

Jornal Empresas & Negócios Ltda

Administração, Publicidade e Redação: Rua Joel Jorge de Melo, 468, cj. 71 – Vila Mariana – São Paulo – SP – CEP.: 04128-080
Telefone: (11) 3106-4171 – E-mail: (netjen@netjen.com.br)
Site: (www.netjen.com.br). CNPJ: 05.687.343/0001-90
JUCESP, Nire 35218211731 (6/6/2003)
Matriculado no 3º Registro Civil de Pessoa Jurídica sob nº 103.