



OPINIÃO

Quando o agente de IA vira funcionário: um problema de identidade

Ramon Ribeiro (\*)

Para cada identidade humana registrada nos sistemas corporativos, há entre 45 e 90 identidades não humanas operando nos mesmos ambientes, segundo dados apresentados pela IBM durante o Think 2026.

São contas de serviço, chaves de API, tokens de autenticação e, cada vez mais, agentes de IA que acessam CRMs, ERPs, bancos de dados e caixas de e-mail com autonomia para tomar decisões sem intervenção humana.

A proporção não é nova, mas o que mudou nos últimos meses é qualitativo: os agentes de IA não são credenciais passivas. Eles raciocinam, planejam, executam sequências de ações em dezenas de sistemas e podem solicitar novas permissões em tempo de execução. E a infraestrutura de gerenciamento de identidade e acesso da maioria das empresas foi desenhada para um mundo em que apenas pessoas faziam login.

Em uma pesquisa do IANS Research com CISOs, a garantia de identidade para um mundo de IA foi classificada como a segunda maior prioridade para este ano, com nota 4,46 de 5, atrás apenas do uso de IA nas próprias equipes de segurança. Uma das maiores consultorias globais de tecnologia incluiu a adaptação do gerenciamento de identidade e acesso a agentes de IA entre as seis principais tendências de cibersegurança para 2026, alertando que a incapacidade de resolver o problema levará a um aumento de incidentes de segurança relacionados a acesso à medida que agentes autônomos se tornem mais prevalentes.

O que torna essa questão particularmente difícil é que os sistemas de IAM existentes foram construídos sobre premissas que não se aplicam a agentes autônomos. Pessoas fazem login em horários previsíveis, mantêm sessões de duração limitada, passam por revisões periódicas de acesso e podem ser submetidas a autenticação multifator.

Agentes de IA operam 24 horas por dia, em velocidade de máquina, sem padrões comportamentais que sirvam como linha de base para detecção de anomalias, e não podem responder a um desafio de MFA. A IBM identificou que 92% das empresas não confiam nas próprias ferramentas legadas de IAM para gerenciar os riscos associados a identidades não humanas e agentes de IA. Não se trata de uma limitação incremental: é uma incompatibilidade estrutural entre a arquitetura de segurança vigente e a realidade operacional que as empresas estão criando ao adotar agentes autônomos.

Proliferação de agentes autônomos

A Deloitte, em seu relatório State of AI in the Enterprise de 2026, identificou que o acesso de trabalhadores a ferramentas de IA cresceu 50% apenas em 2025, mas apenas uma em cada cinco empresas possui um modelo maduro de governança para supervisionar esse uso. Do lado dos agentes, a proliferação é ainda mais intensa. Cada novo agente

implantado pode gerar múltiplas identidades derivadas, tokens de acesso e conexões com APIs externas. Um único agente de atendimento ao cliente configurado para resolver chamados pode, em uma operação rotineira, gerar centenas de sub-agentes, cada um com suas próprias credenciais e escopos de acesso. Se um desses agentes começa a emitir reembolsos fora da política ou a acessar dados de clientes sem autorização, a pergunta que emerge é simples, mas frequentemente sem resposta: quem configurou esse agente, quais permissões recebeu e quem é responsável pelo que ocorreu?

Uma análise da CSA de 2026 sobre a proliferação de tokens revelou que mais de 16% das empresas sequer rastreiam a criação de identidades associadas a agentes de IA, o que significa que o inventário básico simplesmente não existe.

Credenciais de serviço não são a mesma coisa

Contas de serviço tradicionais executam tarefas predefinidas em fluxos determinísticos. Agentes de IA, por definição, agem de forma probabilística: interpretam contexto, decidem sequências de ação e podem solicitar acesso a recursos que seus criadores não anteciparam. Um whitepaper publicado pela Cloud Security Alliance em 2026 descreveu essa dinâmica como uma aquisição autônoma de credenciais em tempo de execução, algo para o qual nenhuma geração anterior de identidades não humanas estava preparada.

A credencial que um agente possui não é apenas uma chave passiva, mas a identidade principal de um ator capaz de encadear ações em múltiplos sistemas com resultados que podem ser imprevisíveis.

O conceito de Zero Trust, amplamente adotado para proteger o acesso humano, precisa ser estendido de forma nativa para identidades não humanas e agentes de IA. Isso implica tratar cada agente como uma entidade de primeira classe no sistema de identidade, com provisionamento dinâmico que crie e retire identidades por tarefa, autorização baseada em políticas verificadas a cada invocação, rastreabilidade completa de cada ação vinculada a uma cadeia de delegação auditável e isolamento de fluxos de trabalho para limitar o raio de impacto em caso de comprometimento.

Alguns analistas já utilizam o termo "guardian agents", agentes de supervisão cuja função é monitorar se outros agentes estão operando dentro dos limites definidos, como uma camada necessária de governança.

Empresas que estão implantando agentes de IA sem antes resolver a questão de identidade estão construindo automação sobre alicerces que não foram projetados para sustentá-la. A próxima grande falha de segurança corporativa provavelmente não virá de um invasor externo sofisticado, mas de um agente de IA com permissões excessivas que ninguém lembra de ter configurado, acessando dados que ninguém autorizou, em um sistema que ninguém sabia que estava conectado.

(\*) Diretor Comercial da Solo Network.

SAP aperta o cinto para investir em inteligência artificial

A maior empresa de software da Europa anunciou a suspensão da maioria das contratações e a paralisação de viagens não essenciais, como forma de liberar recursos destinados ao desenvolvimento de IA.

Vivaldo José Breternitz (\*)

As medidas foram comunicadas aos funcionários no início deste mês, por e-mail ao qual a agência Bloomberg teve acesso. A empresa informou que a partir de agora "novas contratações serão exclusivamente focadas em perfis selecionados, principalmente em funções centrais de IA". Viagens sem relação com projetos de IA também estão suspensas. Além disso, a SAP pretende reduzir gastos com fornecedores.

A lógica é simples: economizar em algumas áreas para investir em outras. A SAP não está sozinha nesse movimento. Outras empresas de grande porte, da área de tecnologia, como Microsoft, Oracle e Salesforce também têm cortado custos, com o mesmo objetivo, mas quase sempre recorrendo a demissões: o padrão é claro: transformar folha de pagamento em orçamento para inteligência artificial.

O mercado mostra como mudanças são urgentes: as ações da SAP já caíram cerca de 33% neste ano, diante do temor de que a IA reduza a demanda por softwares tradicionais, como os ERPs fornecidos pela empresa.

A SAP está destinando parte de seu orçamento de IA para aquisições, mas nem sempre a empresa consegue fechar os negócios



Funtap\_CANVA

pelos quais se interessa. Há alguns dias perdeu a disputa pela Cognite, companhia de inteligência artificial industrial e dados, que fechou acordo de US\$ 3,1 bilhões com a Schneider Electric. Para uma empresa que busca adquirir rapidamente expertise, uma derrota dessas pesa.

Em 2025 a SAP concluiu um processo de reestruturação que custou mais de € 3 bilhões e resultou na eliminação de 10 mil empregos; recentemente a empresa sinalizou que pretende continuar reduzindo seu quadro de funcionários entre 1% e 2% ao ano.

A grande dúvida é se a aposta em IA vai trazer resultados, pois alguns clientes e parceiros têm questionado o custo-benefício das primeiras ferramentas de IA lançadas pela SAP.

Para o campeão europeu do software, vale o antigo dito: a sorte está lançada - mas ainda é preciso esperar os resultados.

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

O erro que toda empresa comete antes de adotar IA

Existe uma diferença enorme entre usar inteligência artificial e operar orientado por ela. Eu vejo essa confusão acontecer todos os dias — e no setor de saúde, onde atuo, ela tem consequências que vão muito além de um projeto mal executado.

A maioria das empresas que diz ser "AI First" ainda aplica IA de forma fragmentada. Uma automação aqui, um chatbot ali, um modelo de linguagem plugado num processo que ninguém documentou direito. Segundo a McKinsey, 88% das empresas globais já usam IA em alguma função de negócio. Mas usar não é o mesmo que transformar. E a diferença está, quase sempre, antes do algoritmo.

O que sustenta uma aplicação de IA não é o modelo em si. É a fundação embaixo dele: documentação organizada, arquitetura coerente, regras de negócio bem estruturadas, dados utilizáveis. Sem isso, você não está sendo AI First, você está empilhando sofisticação sobre um terreno instável.

Hospitais operam 24 horas por dia. Não há janela de manutenção conveniente, não há margem para comportamento imprevisível, não há tolerância para rastreabilidade zero. Quando começo a falar de IA nesse contexto, a primeira pergunta que faço não é "qual modelo vamos usar?", é "seus dados estão organizados o suficiente para que qualquer IA faça sentido com eles?"

Há alguns anos, eu diria que a resposta da maioria seria não.

O que mudou na minha visão de construir produtos em ambientes críticos foi entender que a adoção de IA precisa ser tratada como uma transformação cultural,



Divulgação

Michael Cortez

não como uma funcionalidade nova no roadmap. Isso significa capacitar pessoas em diferentes áreas para pesquisar, documentar, questionar e construir com IA como parte do método de trabalho. Quando isso acontece, o efeito não é de automação: é de amplificação. A empresa pensa melhor, documenta melhor, entrega melhor.

No supply chain hospitalar, onde opero, isso tem impacto direto. A IA nos ajuda a aprofundar investigações de domínio, estruturar hipóteses de evolução de produto, entender dores dos usuários com mais profundidade e apoiar a codificação em escala. Mas nada disso funcionaria se a base não estivesse sólida. Dado bagunçado continua bagunçado, com ou sem modelo sofisticado por cima.

Tem outro ponto que quase ninguém fala abertamente: o diferencial competitivo está mudando de lugar. Num mundo em que a IA modifica funcionalidades, onde qualquer empresa pode implementar um recurso parecido em semanas, o que vai separar os players não é mais o que a tecnologia faz. É o quanto de especialização, serviço e conhecimento de processo está embutido junto. Modelos de licenciamento puro sofrerão pressão crescente. Quem combina tecnologia com densidade consultiva e domínio setorial tem uma vantagem que não é facilmente replicável.

Isso me leva à última questão, que é quase filosófica: inovar com responsabilidade é o oposto de inovar devagar?

Na saúde, eu defendo que não. Alucinações, automações mal calibradas e comportamentos pouco previsíveis não são apenas falhas técnicas, podem gerar impacto direto em operações assistenciais. Ser criterioso aqui não é excesso de cautela. É o que garante que a inovação dure, que escale e que gere confiança real, não apenas uma demo bonita num evento de tecnologia.

Ser AI First de verdade exige mais do que ferramentas novas. Exige revisão de processos, organização de dados, capacitação de times e uma mudança genuína no método de trabalho. Quem fizer isso vai construir melhor no curto prazo — e vai estar muito mais preparado para o que vem no médio e longo.

O algoritmo é a última peça. A fundação é o que importa.

(Fonte: Michael Cortez, Software House Manager e sócio da GTPLAN, empresa especializada em tecnologia SaaS para Supply Chain).

News@TI  
ricardosouza@netjen.com.br

Eu Entrego apresenta Ship From Store Nacional no Fórum E-Commerce Brasil 2026

@ A Eu Entrego participa da 17ª edição do Fórum E-Commerce Brasil, entre os dias 28 e 30 de julho, no Distrito Anhembi, em São Paulo, com estande próprio para apresentar suas soluções de logística inteligente e omnichannel. Localizado no estande 0141, ao lado da Plenária Tecnologia & Inovação, o espaço será dedicado à demonstração das tecnologias da

empresa, geração de negócios e encontros com varejistas, indústrias e parceiros do ecossistema. O principal destaque será o lançamento oficial do Ship From Store Nacional, solução que amplia para todo o Brasil o modelo de integração entre lojas físicas e e-commerce desenvolvido pela companhia (https://eventos.ecommercebrasil.com.br/forum).

|                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  <b>José Hamilton Mancuso (1936/2017)</b><br>Responsável: <b>Lilian Mancuso</b>                                                                                                                                                                                                        | <b>Laurinda Machado Lobato (1941-2021)</b>                                                                                                                                                                                                                                                                               | <b>José Leonil Lobato (1939-2026)</b>                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Editórias</b><br><i>Economia:</i> Nelson Tucci (nelson.tucci@netjen.com.br)<br><i>Mercado/Negócios/Tecnologia/Agronegócios/ Espaço empresarial:</i> Ricardo Souza (ricardosouza@netjen.com.br);<br><i>Livros:</i> Ralph Peter (ralphpeter@agenteliterarioralph.com.br)<br><i>Comercial:</i> comercial@netjen.com.br<br><i>Publicidade Legal:</i> lilian@netjen.com.br | <i>Webmaster/TI:</i> Fabio Nader; <i>Editoração Eletrônica:</i> Ricardo Souza.<br><i>Revisão:</i> Maria Cecília Camargo; <i>Serviço informativo:</i> Agências Brasil, Senado, Câmara, EBC, ANSA.<br><br>Artigos e colunas são de inteira responsabilidade de seus autores, que não recebem remuneração direta do jornal. | <b>Jornal Empresas &amp; Negócios Ltda</b><br>Administração, Publicidade e Redação: Rua Joel Jorge de Melo, 468, cj. 71 – Vila Mariana – São Paulo – SP – CEP.: 04128-080<br>Telefone: (11) 3106-4171 – E-mail: (netjen@netjen.com.br)<br>Site: (www.netjen.com.br). CNPJ: 05.687.343/0001-90<br>JUCESP, Nire 35218211731 (6/6/2003)<br>Matriculado no 3º Registro Civil de Pessoa Jurídica sob nº 103. |
| <b>Colaboradores:</b> Ana Luisa Winckler, Carol Olival, Claudia Lazzarotto, Denise Debiasi, Fabiana Monteiro, Geraldo Nunes, Heródoto Barbeiro e Neiva Mendes                                                                                                                                                                                                            | ISSN 2595-8410                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                         |