OPINIÃO

IA agêntica: três prioridades inegociáveis para CISOs

James Robinson (*)

As ameaças relacionadas à IA evoluíram mais rápido ao longo do último ano do que a maioria das empresas consegue acompanhar, e não há muito tempo para recuperar esse atraso. Não estamos nos preparando para um mundo agêntico, nós já estamos vivendo nele.

Os agentes de IA já atuam dentro dos ambientes corporativos, alguns desenvolvidos por nossas próprias equipes, outros operados ou manipulados por invasores. Eles tomam decisões em velocidade e escala sem precedentes. Ainda estamos começando a compreender essas ameaças, enquanto tentamos administrá-las com um modelo de segurança concebido para um cenário anterior à IA agêntica.

Agora, precisamos substituir esse modelo por uma abordagem que reflita como os agentes – tanto os utilizados pelas empresas quanto os explorados por cibercriminosos – operam, falham e quais recursos podem acessar. É hora de construir as bases de segurança adequadas para um mundo que já é impulsionado por agentes de IA. E, para isso, vejo três prioridades que devem orientar os CISOs durante essa transição.

#1: Construir uma estratégia de segurança para a economia agêntica

Os agentes já estão operando dentro das empresas, muitas vezes sem serem percebidos, e a maioria das equipes ainda não sabe onde nem como a IA agêntica está sendo utilizada. Isso precisa mudar. A segurança na economia agêntica começa pelo conhecimento de todos os agentes presentes no ambiente: o que podem acessar, sob qual identidade operam e quais decisões estão autorizados a tomar. Sem esse inventário, não há como proteger o ambiente de forma eficaz.

No entanto, assim que atingem essa visibilidade, surge um novo desafio: a velocidade. Os agentes são criados, modificados e implementados na mesma velocidade do desenvolvimento de software, geralmente em questão de minutos. Isso significa que a segurança não pode mais atuar apenas após o processo de desenvolvimento. As equipes de segurança precisam incorporar controles diretamente às etapas de criação, testes e implementação dos agentes.

As estruturas tradicionais de governança deixaram de acompanhar esse ritmo. Por isso, as equipes de segurança precisam adotar um modelo automatizado, integrado e contínuo, com aplicação de políticas em tempo real e monitoramento capaz de detectar imediatamente qualquer desvio de comportamento.

#2: Criar um modelo de resposta a incidentes para violações conduzidas por agentes

Historicamente, a maioria das violações de segurança envolvia engenharia social e algum elo humano na cadeia de ataque. Por isso, os processos de resposta a incidentes (IR) foram estruturados em torno do comportamento humano: alguém clicando em um link indevido, acessando um recurso inadequado ou realizando uma alteração que não deveria.

Mas quando um agente executa essas ações, segue uma instrução equivocada ou interpreta um contexto de forma incorreta, esse modelo deixa de funcionar. As empresas precisam de uma abordagem de resposta a incidentes que trate os agentes como atores autônomos, e não como simples extensões dos usuários.

Hoje, nenhuma organização possui um manual completo para lidar com esse cenário. O trabalho começa pela definição de quais evidências são relevantes em uma investigação envolvendo agentes: a cadeia de instruções recebidas, as respostas produzidas pelo modelo, a janela de contexto utilizada, as permissões concedidas e os limites de decisão que foram ultrapassados. Sem registrar essas informações, fica impossível explicar por que um agente se comportou de determinada maneira.

Além disso, os agentes falham de formas diferentes. Eles podem alucinar etapas de um processo, agir com base em contexto incompleto, seguir instruções elaboradas por invasores, extrapolar sua finalidade original ou encadear ações de maneiras que nenhum ser humano faria. Esses comportamentos criam uma categoria inédita de incidentes.

Por isso, os CISOs precisam redefinir o que significa uma resposta eficaz a incidentes. Isso envolve identificar quais pressupostos deixaram de fazer sentido, como reconstruir o comportamento dos agentes e de que forma priorizar incidentes cuja intenção foi gerada por uma máquina, e não por uma pessoa. Ainda não existe um modelo maduro para responder a incidentes envolvendo IA agêntica, mas não podemos esperar que ele apareça. É preciso começar a construí-lo agora.

#3: Incorporar red teaming para IA

As equipes de segurança não conseguem improvisar uma mentalidade voltada para ataques envolvendo inteligência artificial. A maioria dos profissionais de defesa foi treinada para proteger sistemas, e não para pensar como invasores que dedicam seu tempo a descobrir formas de manipular agentes, explorar prompts ou levar sistemas além dos limites para os quais foram projetados.

Por isso, se uma empresa não dispõe de especialistas com experiência real em segurança ofensiva aplicada à IA, deve buscar parceiros que possuam esse conhecimento.

Esses parceiros adotam uma abordagem diferente, passam o tempo tentando comprometer modelos, testando agentes de formas que os defensores normalmente não considerariam e identificando comportamentos que só surgem sob pressão adversária. Compreendem como os invasores pensam porque testam essas técnicas diariamente, de forma segura e controlada.

O red teaming para IA (prática que simula ataques para identificar vulnerabilidades em modelos e agentes antes que sejam exploradas por invasores) também precisa caminhar lado a lado com a resposta a incidentes. Se uma empresa tem dificuldade para entender o comportamento de um agente, a melhor forma de evoluir é simular falhas reais: ataques por injeção de prompts, instruções maliciosas, uso indevido de privilégios, desvios de escopo ou agentes executando ações que ninguém havia previsto. As equipes de segurança devem submeter esses cenários a testes de estresse regularmente, porque, embora muitos deles ainda não tenham ocorrido em larga escala, certamente farão parte da realidade.

E esse trabalho não pode ser pontual. As empresas precisam transformar essa capacidade em uma competência permanente, estabelecendo um processo contínuo para testar o comportamento dos agentes, compreender suas falhas e avaliar se as defesas continuam eficazes quando algo sai do esperado.

Da conscientização à ação

A IA agêntica já está transformando a forma como os ataques acontecem, como os sistemas se comportam e o que se espera das equipes de segurança. A resiliência só virá se deixarmos de esperar por respostas definitivas e começarmos desde já a desenvolver essas capacidades.

As empresas precisam de um modelo de segurança que ofereça aos CISOs visibilidade sobre seus agentes, de uma estratégia de resposta a incidentes capaz de lidar com novos comportamentos e de iniciativas de red teaming para IA que revelem vulnerabilidades antes que elas cheguem aos ambientes de produção.

Nada disso é opcional. A IA agêntica já deixou de ser uma tendência para se tornar parte da realidade das empresas. A discussão já não é mais se essa transformação vai acontecer, mas como preparar a segurança para acompanhá-la. As decisões tomadas pelos CISOs definirão a forma como as empresas vão adotar e governar esses agentes.

(*) CISO da Netskope.

Irlanda: data centers consomem quase tanta energia quanto todas as residências

Os data centers responderam por 23% de todo o consumo de eletricidade da Irlanda em 2025, segundo dados divulgados na semana passada pelo Central Statistics Office (CSO).

Vivaldo José Breternitz (*)

PhonlamaiPhotos_Images_CANVA

O relatório mostra que o gasto energético dessas instalações subiu para 7.663 GWh em 2025, contra 6.973 GWh em 2024, um aumento de 10% em apenas um ano. No mesmo período, o consumo do restante do país cresceu apenas 2%.

Em um espaço maior de tempo, o salto é ainda mais impressionante: em 2015, os data centers representavam apenas 5% do consumo nacional; em dez anos, houve uma escalada de 360%. No quarto trimestre de 2025, o consumo chegou a 1.991 GWh, contra 291 GWh no primeiro trimestre de 2015, uma alta de 584%.

O consumo dos data centers (23%) já se aproxima do gasto residencial, que inclui casas urbanas e rurais e ficou em 28% do total. A rápida expansão dos data centers, impulsionada pelo boom da inteligência artificial, tem alimentado um debate global: críticos apontam vários problemas, dentre os quais o mais visível é que sua demanda gigantesca de energia pressiona as tarifas dos usuários domésticos

A Irlanda, com cerca de cinco milhões de habitantes, abriga 89 data centers, concentrados principalmente na capital, Dublin, e arredores. A maioria pertence a gigantes como Microsoft, AWS, Google e Meta.

O crescimento acelerado do consumo levou o governo a impor, em novembro de 2021, uma espécie de moratória sobre novas conexões à rede elétrica. Desde então, novos projetos só podem avançar se garantirem geração própria ou se forem instalados fora da região de Dublin.

Mesmo com a medida, o consumo continuou a subir. Em 2024, a Agência Internacional de Energia previu que os data centers poderiam chegar a um terço do consumo nacional até 2026, cenário que parece possível.

No fim de 2025, o governo substituiu a moratória por uma nova política de conexão para os novos data centers, exigindo coisas como uso de energia renovável de fontes próprias.

O caso irlandês não é isolado. Pesquisas indicam que o consumo global de eletricidade por data centers deve crescer 26% em 2026. Além da energia, há preocupações com uso intensivo de água e poluição sonora. Nos Estados Unidos, a resistência popular já levou ao cancelamento de mais de 75 projetos de data centers apenas no primeiro trimestre de 2026.

Devemos estar atentos para o fato de que o Brasil vem sendo considerado como um lugar interessante para instalação de novos data centers, especialmente em função de nossos preços de energia serem, ao menos por enquanto, baixos em relação aos praticados no exterior, além de termos legislação ambiental aplicada de forma não muito rigorosa.

Além disso, há muitos políticos apoiando esses novos data centers, colocando-se como arautos do progresso mas não levando em conta que essas estruturas, além dos problemas que causam, geram pouquíssimos empregos de qualidade.

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

Edital busca organizações para projetos que unam dados, IA e saúde mental de crianças e adolescentes

À medida que as necessidades de saúde mental de crianças e adolescentes aumentam em todo o Brasil, a organização global de saúde pública Vital Strategies lançou um desafio nacional para acelerar o uso de dados e inteligência artificial para identificação precoce de riscos e ampliar o acesso ao cuidado. A iniciativa conta com apoio do Google.org em cerca de R$ 5 milhões.

O "Desafio Dados e IA para a Promoção da Saúde Mental de Crianças e Adolescentes" é uma chamada aberta para organizações que desenvolvem soluções inovadoras e baseadas em dados para prevenir, detectar e responder a riscos de saúde mental entre crianças e adolescentes. As inscrições estão abertas até 03 de agosto, com organizações selecionadas elegíveis para apoio em duas faixas (Faixa A: R$ 300 mil a R$ 500 mil; Faixa B: R$ 600 mil a R$ 800 mil).

"A inteligência artificial pode servir como uma ferramenta importante para abordar desafios complexos de saúde pública, e acreditamos que suas verdadeiras capacidades são alcançadas quando canalizadas para a transformação social positiva, liderada por especialistas locais", disse Juliana Bueno, Relações Públicas do Google no Brasil. "Ao unir a inovação tecnológica com políticas públicas, esta iniciativa colabora com a criação de um modelo sustentável para a adoção de IA, que priorize ainda mais o bem-estar humano e a saúde mental dos jovens. O que também justifica o nosso apoio", acrescentou.

No Brasil, estima-se que 11% a 20% das crianças e adolescentes vivam com alguma condição de saúde mental, mas a dimensão real do problema pode ser ainda maior. Entre 2015 e 2019, os casos notificados de automutilação entre jovens de 10 a 19 anos aumentaram mais de oito vezes. Na Pesquisa Nacional de Saúde do Escolar (PeNSE), quase 3 em cada 10 adolescentes entrevistados relataram sentir tristeza com frequência. Entre as meninas, mais de 4 em cada 10 relatam tristeza frequente, e 1 em cada 4 disse que a vida não vale a pena ser vivida.

"Em um momento em que as necessidades de saúde mental entre crianças e adolescentes crescem mais rapidamente do que a capacidade dos sistemas de responder, precisamos repensar a forma como monitoramos mudanças, identificamos riscos precocemente e garantimos que o cuidado adequado chegue a tempo", afirmou Pedro de Paula, Vice-Presidente Sênior de Inovação Global da Vital Strategies. "A inteligência artificial está ampliando a capacidade dos sistemas de saúde pública de enxergar e agir. Quando aplicada de forma responsável e apoiada por sistemas robustos de dados, ela pode transformar informações fragmentadas em ações oportunas capazes de salvar vidas. Este desafio tem como objetivo apoiar soluções com potencial de escala e garantir que elas cheguem a quem mais precisa (https://www.vitalstrategies.org/resources/dados-e-ia-para-promocao-da-saude-mental-de-criancas-e-adolescentes/).

News @ TI

ricardosouza@netjen.com.br

João Appolinário se torna investidor do LiaHub

@João Appolinário, fundador da Polishop, acaba de se tornar sócio-investidor do LiaHub, companhia brasileira de inteligência artificial corporativa criada para ajudar empresas a estruturar, governar e escalar o uso da tecnologia em seus negócios. A entrada do empresário no quadro societário marca uma nova fase para o LiaHub e reforça o avanço da inteligência artificial como pauta estratégica para empresários, executivos e lideranças corporativas. Mais do que uma aposta financeira, o movimento conecta a experiência de Appolinário na aplicação prática de IA em produtos, operações e gestão à proposta do LiaHub de transformar a tecnologia em resultado concreto para empresas.

CBC na Shot Fair Brasil 2026

@A Companhia Brasileira de Cartuchos (CBC) estruturou uma participação robusta na Shot Fair Brasil 2026 por meio de iniciativas focadas no relacionamento e na experiência dos parceiros. Uma das principais frentes será conduzida pelo PRLO (Programa de Relacionamento com Lojistas), que promoverá homenagens exclusivas no decorrer do evento. A empresa entregará placas de reconhecimento aos três lojistas com melhor desempenho, além de troféus para o Top 10 CBC Partners – Varejo referente a 2025 e ao primeiro semestre de 2026. A Shot Fair Brasil 2026 acontece de 15 a 18 de julho de 2026, das 10h às 20h, no Distrito Anhembi (Av. Olavo Fontoura, 1209, Santana, São Paulo - SP) (https://www.cbcstore.com.br/).

Empresas & Negócios

José Hamilton Mancuso (1936/2017) | **Laurinda Machado Lobato (1941-2021)** | **José Leonil Lobato (1939-2026)**

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

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.

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

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.