



Mercado Digital

Patricia Knebel

patricia.knebel@jornaldocomercio.com.br

Confira, diariamente, no blog Mercado Digital, conteúdos sobre tecnologia e inovação. Para acessar, aponte a câmera do seu celular para o QR Code.

jornaldocomercio.com/mercadodigital



Talentos e cibersegurança são desafios da IA

Em apenas três anos, o número de vagas que exigem conhecimentos em Inteligência Artificial no Brasil quase quadruplicou. Em 2021, eram 19 mil, em 2024, chegaram a 73 mil. Os dados fazem parte do Voa Brasil, relatório da Microsoft sobre os impactos da empresa no País.

Depois de anos medindo o avanço da Inteligência Artificial pela evolução de modelos, pelo processamento e infraestrutura, agora, o ativo mais importante, para além de toda a tecnologia em si, é a disponibilidade de pessoas capazes de transformar essa tecnologia em vantagem competitiva.

O levantamento mostra que um dos maiores desafios no Brasil atualmente é formar profissionais capazes de acompanhar essa transformação. Segundo dados da Anatel, apenas cerca de 30% da população brasileira possui habilidades digitais básicas e menos de um quinto alcança um nível intermediário. Ao mesmo tempo, a demanda do mercado cresce em ritmo acelerado. Ou seja, a tecnologia avança mais rápido do que a formação de profissionais capazes de utilizá-la.

Essa preparação, segundo o relatório, deve começar cada vez mais cedo. Além dos programas voltados à qualificação de profissionais já ativos no mercado de trabalho, a Microsoft alerta para a importância de iniciativas nas escolas, com estudantes e educadores. Um levantamento da Associação Nova Escola (ANE), realizado em 2025 com 845 educadores, mostra que 94% dos professores já ouviram falar em inteligência artificial. Ainda assim, quase metade (47%) nunca utilizou esse tipo de ferramenta em sala de aula. Entre os principais obstáculos apontados estão a falta de formação e de conhecimento técnico sobre o tema (35%).

Essa realidade explica por que a capacitação passou a ocupar espaço tão estratégico quanto os investimentos em infraestrutura. A Microsoft afirma ter treinado mais de 3,7 milhões de brasileiros em IA por meio do programa ConectAI e estabeleceu a meta de chegar a 5 milhões de pessoas até 2027. Em paralelo, ampliou a parceria com a Escola do Trabalhador 4.0 para disponibilizar 10 milhões de vagas gra-

tuitas em cursos de tecnologia e IA até 2030. O objetivo, de acordo com a gigante da tecnologia, é reduzir um gargalo que pode limitar a competitividade das empresas brasileiras nos próximos anos.

O relatório também chama atenção para outro aspecto que tende a ganhar cada vez mais peso nas organizações, a cibersegurança. À medida que agentes de IA passam a executar tarefas mais complexas e a operar grandes volumes de dados, crescem igualmente as ameaças digitais.

A própria inteligência artificial passa a desempenhar um papel duplo, sendo utilizada tanto por criminosos para automatizar ataques quanto por empresas para identificar essas situações e responder com maior velocidade.

A Microsoft afirma bloquear diariamente cerca de 4,5 bilhões de ameaças de malware, analisar 35 milhões de detecções de riscos de identidade e verificar 5 bilhões de e-mails. Hoje, mais de 34 mil engenheiros da companhia atuam exclusivamente em iniciativas de cibersegurança. E a procura por profissionais especializados em ciberseguran-



ADOBESTOCK/DIVULGAÇÃO/JC

Barreira é formar pessoas que acompanhem a transformação com a IA

ça também tem aumentado. O estudo mostra que o número de profissionais empregados em segurança da informação cresce 16,1% ao ano.

Segundo o Microsoft Digital Defense Report 2025, 80% dos incidentes investigados envolveram tentativas de roubo de dados, motivadas principalmente por ganhos financeiros (52%) ou espionagem (4%). Setores como saúde, pesquisa, educação e transporte aparecem entre os mais visados por concentrarem grandes volumes de informa-

ções sensíveis.

Cerca de 63% dos brasileiros relataram ter enfrentado ao menos um episódio significativo de ameaça digital nos últimos 12 meses, dado que só deve aumentar à medida que mais pessoas utilizam a tecnologia. Os dados brasileiros apresentados pela Microsoft também mostram que o acesso às tecnologias de IA permanece desigual. Enquanto 69% das pessoas da classe A já utilizam inteligência artificial, esse percentual cai para 16% entre as classes D e E.

Iniciativa mira adoção segura da IA agêntica na saúde

Projeto em conjunto com o Centers for Disease Control and Prevention (CDC) e com o conglomerado National Institutes of Health (NIH) busca criar uma infraestrutura segura para que agentes inteligentes acelerem descobertas científicas

A Red Hat, player global de desenvolvimento de software open source empresarial, anunciou o lançamento de um esforço conjunto com o Centers for Disease Control and Prevention (CDC) e com o conglomerado National Institutes of Health (NIH) para acelerar a adoção segura da IA agêntica na saúde pública.

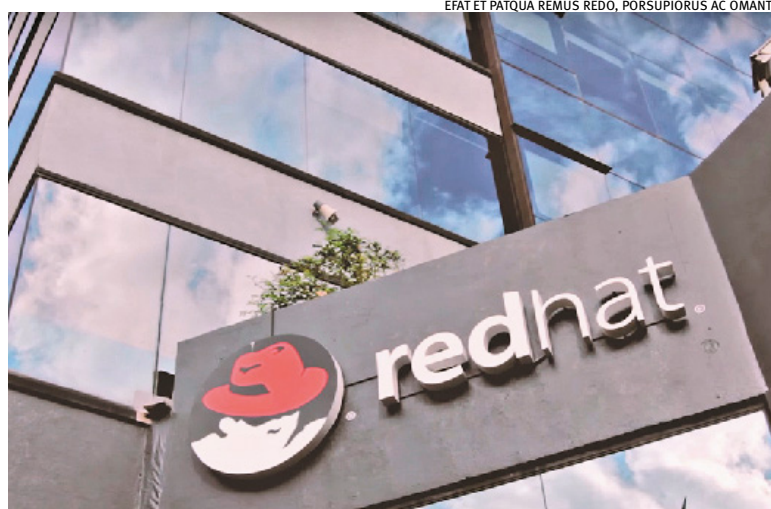
A iniciativa busca reduzir de horas para segundos o tempo necessário para transformar uma pergunta científica em uma resposta baseada em dados. O avanço pode contribuir para pesquisas mais ágeis, apoiar respostas a emergências sanitárias e ampliar a capacidade de tomada de decisão em áreas estratégicas.

Mais do que acelerar pesquisas científicas, a meta é criar uma infraestrutura capaz de tor-

nar agentes de IA confiáveis em ambientes onde decisões baseadas em dados podem impactar diretamente a saúde da população. Hoje, levar agentes inteligentes para ambientes altamente regulados, como saúde e pesquisa biomédica, ainda representa um desafio. Esses sistemas precisam acessar grandes volumes de informações sensíveis com segurança, preservar o contexto científico dos dados e operar dentro

de rígidos padrões de governança e rastreabilidade.

O projeto da Red Hat com o CDC e o NIH concentra esforços no fortalecimento do Model Context Protocol (MCP), padrão aberto que permite a comunicação entre modelos de IA e diferentes fontes de dados para criar uma infraestrutura capaz de conectar agentes inteligentes a repositórios científicos de forma segura, auditável e padronizada.



EFAT ET PATQUA REMUS REDO, PORSUPIORUS AC OMANT.

Red Hat anunciou parceria para agilizar IA agêntica na saúde pública

Governo e indústria são áreas mais visadas

O setor governamental foi o mais visado por ataques cibernéticos pelo segundo ano consecutivo, responsável por 19% de todos os incidentes de alta gravidade de 202. Os dados são do relatório global "Anatomia do mundo cibernético", da Kaspersky Security Services. O setor industrial seguiu de perto, com 17%, enquanto o setor de TI subiu para o terceiro lugar, com 15%, deslocando o financeiro dos três setores mais visados. "Anatomia do mundo cibernético" é um relatório global abrangente que utiliza dados sobre incidentes coletados pelos serviços Kaspersky Managed Detection and Response, Kaspersky Incident Response, Kaspersky Compromise Assessment e Kaspersky SOC Consulting. Com base nessas constatações, o relatório mostra que o setor governamental continuou sendo o mais visado em 2025. Uma análise detalhada das principais causas dos ataques nesse setor revela que as ameaças persistentes

avançadas (APTs) foram as mais comuns, responsáveis por 33,3% dos incidentes. Essa tendência destaca a sofisticação cada vez maior dos adversários, que aperfeiçoam continuamente suas táticas para burlar a proteção automatizada. Além disso, 18,9% das instituições públicas sofreram ataques de engenharia social, o que reforça o papel dos funcionários como uma das principais portas de entrada para ameaças cibernéticas. Essa vulnerabilidade dupla, tanto de ataques persistentes avançados quanto de campanhas de engenharia social, ressalta a necessidade de fortalecer não apenas a tecnologia, mas também a resiliência organizacional. A implementação de medidas como controle de acesso baseado em funções e restrição de privilégios pode reduzir significativamente o impacto das contas comprometidas, especialmente nos grandes ambientes distribuídos do governo.