

Seu Caminho para a IA Segura em Escala



Seu caminho para a IA segura em grande escala

Este relatório baseia-se em um estudo independente realizado com 300 líderes de tecnologia e negócios dos setores de serviços financeiros, saúde, governo, manufatura e tecnologia. Os entrevistados incluem tomadores de decisão seniores com responsabilidade direta por dados, segurança, risco e estratégia de tecnologia. As descobertas refletem especificamente as respostas de líderes C-suite de diversos setores, pois são os mais próximos das decisões que determinam se a IA escala com segurança ou estagna.



Há uma lacuna significativa entre implantar IA e estar pronto para o que essa implantação exige. Em todo o mundo, as empresas se classificam de maneiras muito diferentes em termos de sua preparação para a implantação de IA e tudo o que isso implica.

Nosso relatório de pesquisa Modelo de Maturidade de Confiança em Dados e IA dividiu as organizações em cinco níveis diferentes, classificando sua implantação, implementação e preparação. Nossa pesquisa descobriu que **95%** das organizações implantaram IA em seus ambientes. No entanto, implantar IA de forma segura e eficaz está se mostrando mais difícil, porque as bases operacionais necessárias para confiar na IA em larga escala exigem mais tempo para serem estabelecidas do que a adoção da própria tecnologia.



A IA está avançando rapidamente — mas os contratempos também estão

A adoção de IA entre as organizações desses respondentes já está em andamento. Cerca de 70% dos entrevistados relatam que a IA já está integrada em diversas funções de negócios ou é essencial para suas operações e estratégia competitiva. Ainda assim, o mesmo grupo relata um padrão de contratempos que é difícil de conciliar com esse nível de maturidade.

Cerca de **52%** dos entrevistados dizem que pelo menos uma iniciativa de IA teve seu escopo reduzido nos últimos 18 meses. 4 em cada 10 entrevistados relatam que iniciativas foram atrasadas além dos cronogramas originais. Mais de 1 em cada 4 (**28%**) relatam que uma iniciativa foi totalmente descontinuada, enquanto cerca de 1 em cada 3 dizem que suas iniciativas prosseguiram conforme planejado.

Esses contratempos estão ocorrendo em organizações onde a IA já está em produção, o que significa que têm menos a ver com a adoção em estágio inicial e mais com o que a adoção exige quando atinge escala.

A Velocidade Expõe as Lacunas

As barreiras identificadas pelos líderes ajudam a explicar as razões por trás disso. A restrição mais frequentemente citada é a falta de talentos especializados em IA e aprendizado de máquina (**43%**), seguida pela dificuldade de integrar IA aos fluxos de trabalho e sistemas existentes (**33%**). A incerteza regulatória (**25%**), as limitações de qualidade dos dados (**20%**) e as preocupações com a transparência dos modelos (**19%**) aumentam ainda mais a pressão.

Esses desafios não são isolados entre si. Na verdade, eles se intensificam em organizações que avançam rapidamente para a implantação de IA antes que a governança, as estruturas de responsabilidade e a infraestrutura de dados estejam devidamente preparadas para apoiá-la. A lista de barreiras, nesse sentido, é menos um conjunto de problemas pontuais do que uma descrição do que fica para trás quando a velocidade tem prioridade.

Notavelmente, poucos executivos citam a tecnologia em si como o fator limitante, reforçando que a maturidade em IA agora está mais restrita pela prontidão operacional do que pela velocidade da inovação.

Onde a IA encontra seus limites: competências, sistemas e padrões

A confiança dos executivos, na superfície, conta uma história mais otimista. Cerca de **80%** dos executivos dizem estar confiantes na capacidade de sua organização de escalar a IA com segurança e responsabilidade nos próximos dois anos. A pesquisa, porém, revela uma distinção crítica: quase metade de todos os entrevistados reconhece que sua confiança é impulsionada mais pela intuição do que por evidências que poderiam demonstrar prontamente a terceiros. Entre os executivos cuja confiança se baseia em um plano definitivo, três fatores têm quase o mesmo peso:



55%

Estrutura formal
de governança

55%

Compromisso Visível
da Liderança

53%

Função dedicada
de risco de IA

No entanto, os números começam a cair quando o assunto é validação externa. Apenas **31%** relatam ter passado por uma revisão regulatória ou auditoria envolvendo IA, e somente **20%** mencionam benchmarking em relação a empresas do mesmo setor. Para a maioria das organizações, a confiança é gerada internamente em vez de testada externamente. Ela representa as estruturas projetadas pelos líderes, as equipes que eles construíram e as prioridades que definiram — todas precisam ser testadas externamente para comprovar que são capazes de resistir em uma emergência.

Essa distinção importa à medida que as expectativas para a governança de IA evoluem. Reguladores e conselhos estão cada vez menos preocupados com a existência da governança em princípio e mais focados em saber se ela pode ser demonstrada sob demanda.

Quase 9 em cada 10 executivos relatam que existem políticas formais de governança de IA de alguma forma. No entanto, apenas cerca de 1 em cada 3 afirma que conseguiria apresentar evidências de auditoria abrangentes imediatamente, caso solicitado. A maioria reconhece que a evidência existe, mas seria necessário um esforço substancial para reuni-la. Políticas escritas e governança auditável são recursos distintos e a lacuna entre elas representa uma fonte significativa de exposição.

Estruturas de responsabilidade reforçam esse padrão. A maioria dos executivos atribui a responsabilidade primária pela governança de IA ao CTO ou CDO, enquanto uma parcela significativa recorre a comitês multifuncionais para coordenar a supervisão. **7%** têm um líder dedicado à governança de IA.

Embora cada um desses modelos possa ser eficaz, eles dependem de propriedade e responsabilidade claramente definidas, duas condições que se tornam mais difíceis de sustentar à medida que a IA se expande entre as funções. Sem funções explicitamente definidas e caminhos claros de escalonamento, a cobertura das políticas não se traduz de forma confiável em controle operacional, especialmente quando algo dá errado em larga escala.

Pesquisas sugerem um ambiente em que a adoção de IA é generalizada e o otimismo da liderança é alto. No entanto, as bases operacionais necessárias para sustentar a adoção e o entusiasmo ainda estão tomando forma na maioria das organizações. As empresas que navegam nessa transição de forma mais eficaz compartilham uma característica definidora: confiança fundamentada na prova. Em particular, organizações classificadas nos níveis superiores deste relatório (níveis quatro e cinco) tendem a ter um programa prático de governança que foi implementado e testado sob escrutínio, não meramente projetado.



A IA em Escala Favorece a Preparação, Não a Velocidade

O Modelo de Maturidade de Confiança em Dados e IA oferece aos líderes uma metodologia estruturada e comparativa para diminuir a diferença entre percepção e realidade. Avalia com que consistência a organização governa, protege, recupera e viabiliza dados e IA em toda a corporação, medindo a realidade operacional em vez da intenção declarada. Baseado em pesquisas e melhores práticas, o modelo mede cinco níveis de maturidade, desde o ad hoc até o líder do setor. Ele transforma a prontidão de uma suposição em uma capacidade mensurável.

Para os líderes que questionam se sua confiança está à frente das evidências, isso também oferece a referência externa que, segundo a pesquisa, a maioria das organizações não possui.

As organizações mais propensas a sustentar a IA em escala não são, necessariamente, as mais rápidas a adotá-la. Em vez disso, são aquelas que investem desde cedo em governança, responsabilidade e fundamentos de dados que permitem que a IA seja escalada sem introduzir riscos que superem sua capacidade de gestão.

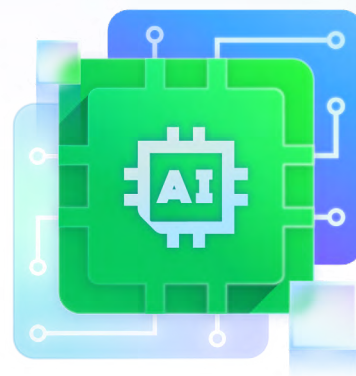
Este sumário executivo destaca dados da região dos EUA. O relatório completo da pesquisa Modelo de Maturidade de Confiança em Dados e IA expande essas descobertas para mais regiões e setores, e examina como os líderes abordam a governança, a resiliência e a prontidão da IA. Este relatório oferece aos líderes uma forma de avaliar seu posicionamento em relação a esse Standard e apresenta um caminho claro para alcançá-lo.



Métodos e Escopo

Este sumário executivo tem como base uma pesquisa encomendada pela Veeam, realizada com **300 líderes de tecnologia e de negócios** dos setores de serviços financeiros, saúde, governo, manufatura e tecnologia. Entre os entrevistados estavam tomadores de decisão seniores responsáveis pelas estratégias de dados, segurança, risco e tecnologia. As conclusões referenciadas ao longo deste documento concentram-se nos principais executivos (C-suite) dentro da população mais ampla do estudo.

A pesquisa examinou como as organizações estão adotando, governando e escalando a IA na prática, com foco na prontidão operacional, estruturas de governança e as condições que moldam a confiança da liderança. As conclusões refletem comportamentos, resultados e condições de tomada de decisão relatados, em vez de intenções futuras declaradas. Os resultados de benchmark foram obtidos a partir do estudo completo e representam as respostas reais dos líderes participantes, sendo utilizados para identificar padrões comuns entre as organizações à medida que a IA passa da implantação inicial para operações empresariais mais abrangentes.





Sobre a Veeam Software

A Veeam é a empresa líder em confiança de dados e IA, especializada em ajudar organizações a garantir que seus dados e IA sejam totalmente compreendidos, protegidos e resilientes, possibilitando a expansão segura de IA em escala. Como líder de mercado em resiliência de dados e gestão da postura de segurança de dados, a Veeam foi desenvolvida para a convergência de identidade, dados, segurança e riscos de IA.

A Veeam entrega profunda inteligência contextual em cada ativo de dados, identidade e modelo de IA. A empresa governa o acesso tanto de humanos quanto de agentes de IA, automatiza os processos de privacidade, conformidade e remediação, além de proteger e recuperar as organizações de ameaças modernas — incluindo ransomware, desastres, erros de IA e garantindo a restauração de dados limpos e confiáveis. A Veeam capacita as organizações a irem além da simples proteção de dados, permitindo que ativem e tenham todo o potencial dos dados.

Com sede em Seattle e escritórios em mais de 30 países, a Veeam protege mais de 550.000 clientes no mundo inteiro, incluindo 82% das empresas da Fortune 500, que confiam na Veeam para manter seus negócios em operação.

Saiba mais em www.veeam.com ou siga a Veeam no LinkedIn [@veeam-software](#) e X [@veeam](#).

