

Aproveitando o poder da IA:

A liderança de TI na próxima
era da tecnologia empresarial

LOGICALIS GLOBAL CIO REPORT 2026

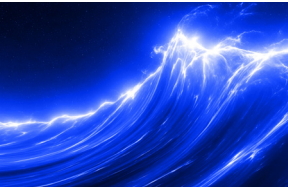


LOGICALIS
Architects of Change

Conteúdo



P 3
Prefácio
Marcio Caputo, CEO da Logicalis para a América Latina



P 4
Resumo executivo



P 6
Capítulo 1
Definindo a agenda de IA



P 12
Capítulo 2
Da confiança à capacidade



P 18
Capítulo 3
Gerenciando a segurança na era da IA



P 24
Capítulo 4
A próxima fronteira



P 30
Conclusão

Prefácio

A IA está transformando profundamente o panorama de negócios e o CIO está no centro dessa transformação. Enquanto a tecnologia avança para sistemas cada vez mais autônomos, cabe aos líderes de TI garantir o equilíbrio entre velocidade de adoção, inovação, confiança e governança. A questão central já não é se a IA deve ser adotada, mas como fazer isso de forma sustentável e alinhada aos objetivos estratégicos.

O CIO Report 2026 reflete essa efervescência. Ao mesmo tempo em que os CIOs relatam ganhos reais em iniciativas pontuais, o desafio de escalar resultados de maneira consistente permanece. Barreiras estruturais — como a falta de competências técnicas internas, desafios relacionados a dados e preocupações regulatórias e de compliance — seguem limitando o potencial de transformação. Uma realidade salta aos olhos: maturidade em IA não é apenas uma questão tecnológica. É organizacional. E, acima de tudo, é um desafio de liderança.

Outro ponto de inflexão destacado nesta edição é a transição da IA de ferramentas que apoiam a decisão para sistemas capazes de agir com crescente autonomia. Quando a tecnologia deixa de apenas recomendar e passa a executar, a responsabilidade se torna central. Sistemas que aconselham podem ser questionados; sistemas que executam precisam ser governados. Nesse contexto, o CIO assume um papel ainda mais estratégico — garantindo supervisão, controle e clareza de responsabilidades em processos críticos.



Marcio Caputo
CEO da Logicalis para a América Latina

Essa complexidade também redefine os modelos operacionais. À medida que as organizações reconhecem que não conseguirão sustentar sozinhas o ritmo de mudança, cresce a necessidade de contar com o apoio de parceiros especializados. O resultado? Mais de 90% dos CIOs esperam recorrer a provedores de Serviços Gerenciados nos próximos anos e quase metade (47%) acredita que parceiros externos entregarão serviços essenciais de TI.

Esse cenário muda a natureza da liderança em tecnologia: ela deixa de ser sobre propriedade e passa a ser, cada vez mais, sobre orquestração, gestão de riscos e capacidade de integrar pessoas, plataformas e parceiros em torno de um objetivo comum.

O CIO Report 2026 convida os líderes de tecnologia a refletirem sobre esse novo papel. Não como executores de projetos isolados, mas como arquitetos de organizações capazes de prosperar em um ambiente onde a inteligência se torna distribuída, os riscos se multiplicam e a confiança passa a ser um ativo estratégico. ●

Resumo executivo

O CIO Report deste ano captura um momento de transição para os líderes de tecnologia nas empresas. A IA deixou de crescer apenas nas periferias das corporações e passou a ocupar um papel central em como o trabalho é realizado, as decisões são tomadas e o valor é criado. Para os CIOs, isso representa uma mudança de responsabilidade que é tanto prática quanto estrutural. A questão já não é como introduzir a IA, mas como gerenciá-la, escalá-la e reduzir, ao máximo possível, os riscos organizacionais.

A pesquisa mostra um apetite avassalador por IA, acompanhado de uma consciência crescente das pressões que ela gera. Os CIOs estão navegando em um cenário definido por aceleração, fragmentação e expectativas crescentes. Espera-se que avancem mais rápido, entreguem mais valor e assumam mais responsabilidades, muitas vezes antes que a base necessária para sustentar essa responsabilidade esteja plenamente estabelecida.

Definindo a agenda de IA

Quase todas as organizações relatam entusiasmo crescente com a IA, mas muitos CIOs acreditam que a sua adoção está acontecendo rápido demais. O alinhamento estratégico permanece frágil, os roadmaps de longo prazo ainda estão em formação e a confiança nos frameworks de governança é desigual. O resultado é um desafio de liderança, mais do que técnico. Os CIOs são cobrados a ajustar o ritmo, definir prioridades e preservar a coerência em um momento em que a impulsividade avança.

Da confiança à capacidade

Os CIOs demonstram confiança em relação ao seu conhecimento de IA comparado aos seus colegas, e as experimentações iniciais já estão gerando valor em áreas específicas. No entanto, escalar esse valor continua sendo um desafio. A escassez de habilidades, problemas de qualidade de dados, limitações de infraestrutura e resistência organizacional seguem freando o progresso. Este capítulo mostra que maturidade em IA não se resume a ferramentas. Trata-se de construir capacidades replicáveis e confiáveis, capazes de resistir a auditorias, análises rigorosas e demandas operacionais de longo prazo.

Gerenciando a segurança na era da IA

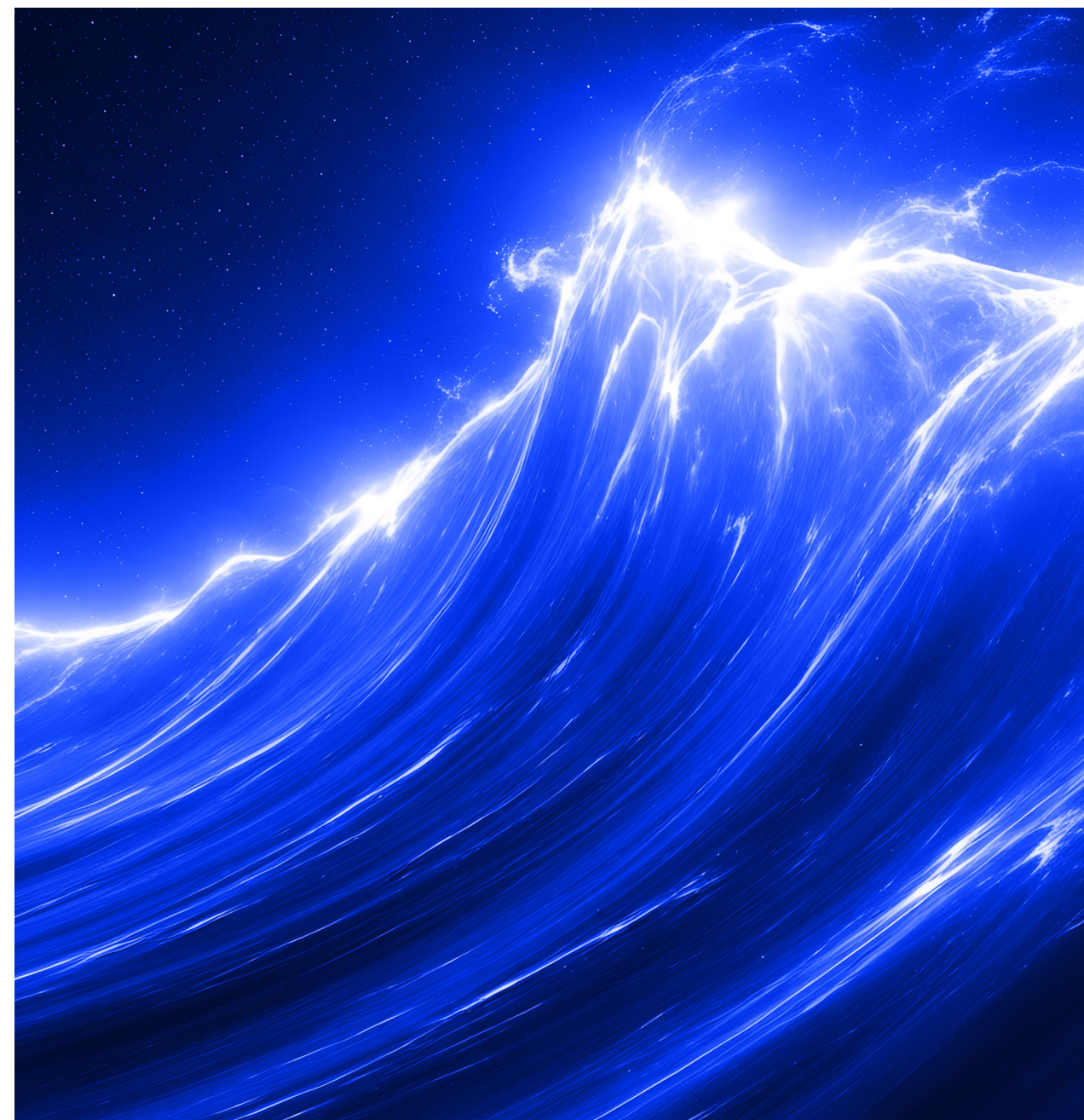
À medida que o cenário de ameaças continua a se expandir, os CIOs seguem lidando com riscos conhecidos, ao mesmo tempo em que se preparam para os desconhecidos. A IA está mudando a natureza do risco, introduzindo novas vulnerabilidades que são mais difíceis de detectar, rastrear e atribuir. Frameworks de governança existem, mas a confiança em sua eficácia é limitada. A visibilidade sobre o uso da IA é incompleta e a responsabilização é fragmentada. Cada vez mais, os CIOs tornam-se os guardiões da confiança em sistemas que operam com crescente independência, mesmo quando a autoridade está distribuída pela empresa.

A próxima fronteira

O investimento em IA agêntica sinaliza a transição dos sistemas de apoio à decisão para os autônomos. Os modelos de força de trabalho tornam-se mais fluidos. Os provedores de serviços gerenciados assumem um papel cada vez mais central. A tecnologia deixa de ser um conjunto de projetos a serem entregues e passa a ser uma condição permanente, em torno da qual as organizações orbitam. Os CIOs evoluem para arquitetos de ambientes nos quais humanos, máquinas e parceiros

externos precisam coexistir sem comprometer a responsabilidade ou o controle.

A liderança em tecnologia já não é definida pela propriedade dos sistemas, mas pela gestão das consequências. Os CIOs são chamados a equilibrar velocidade com estabilidade, ambição com prudência e inovação com responsabilidade. ●



CAPÍTULO 1

Definindo a agenda de IA



A inteligência artificial está avançando em um ritmo diferente de qualquer outra tecnologia corporativa anterior. O que começou como experimentação, tornou-se expectativa. Os conselhos já não discutem se a IA deve fazer parte da organização, mas sim com que rapidez ela pode ser incorporada e quais vantagens competitivas podem ser alcançadas. Para os CIOs, essa mudança deslocou o centro de gravidade de sua função. O desafio já não é introduzir uma nova capacidade, mas manter o equilíbrio entre impulso e capacidade de gestão.

O apetite pela adoção de IA cresceu de forma significativa ao longo do último ano, com quase todos os entrevistados (94%) relatando aumento. As demandas por inovação continuam sendo o principal motor, citadas por 48% dos CIOs, enquanto 38% apontam a gestão de riscos e compliance — refletindo, provavelmente, o aumento das pressões regulatórias e de setor. Os primeiros sucessos em provas de conceito também atuaram como catalisadores, com 37% afirmando que estão sendo mais ousados em suas iniciativas de IA com base nos resultados iniciais.

Essa combinação de ambição e urgência coloca os CIOs no centro de um novo exercício de equilíbrio. Espera-se que avancem rápido o suficiente para acompanharem o ritmo da competição, ao mesmo tempo em que garantem que governança, resiliência e disciplina comercial não fiquem para trás. A agenda de IA deixou de ser apenas sobre identificar oportunidades, e passou a ser sobre regular a velocidade em um contexto no qual a tecnologia avança mais rápido do que as estruturas organizacionais conseguem absorver.

94% das empresas dizem que o seu interesse pela IA aumentou nos últimos 12 meses

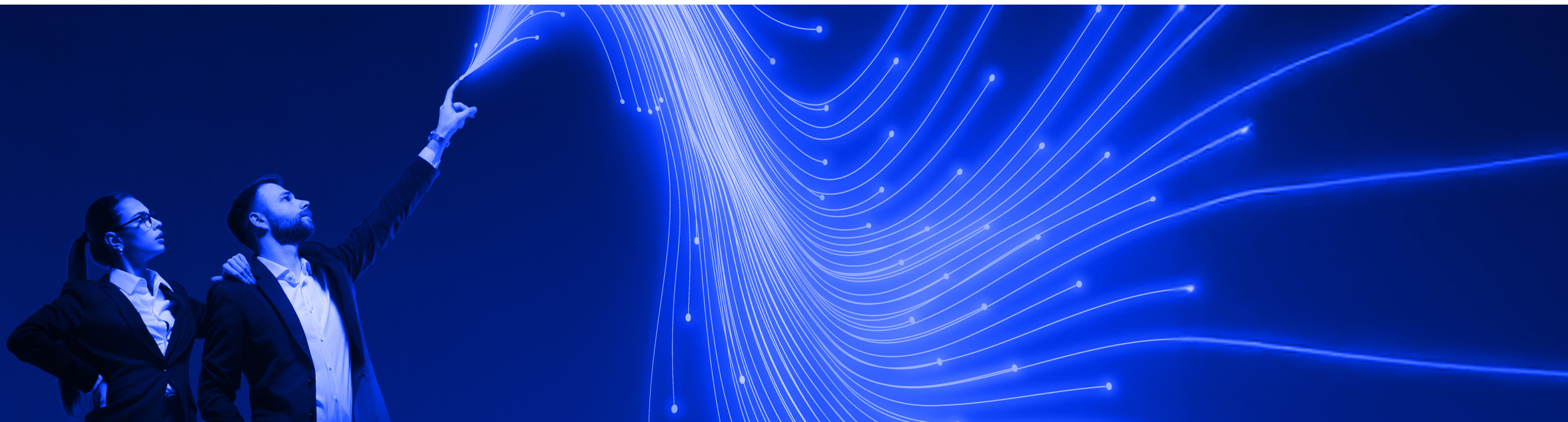
No entanto, 51% acreditam que a sua implementação está acontecendo rápido demais

No entanto, a clareza estratégica não acompanhou o entusiasmo. Menos da metade das corporações (46%) afirma que sua estratégia de IA está totalmente alinhada ao plano de negócios mais amplo ou aos principais indicadores de desempenho. Na prática, isso significa que os CIOs frequentemente operam em uma zona cinzenta, em que as iniciativas de IA avançam sem um framework plenamente maduro para mensurar valor, priorizar investimentos ou definir sucesso.

Esse desalinhamento gera exposição. Quando a atividade em IA avança à frente da governança de negócios, o CIO tem o compromisso de reconciliar ambição com responsabilidade. O risco não é investir em IA, mas em fazê-lo sem uma linha clara de conexão entre experimentação, valor corporativo e modelos operacionais de longo prazo.

A responsabilidade pelas decisões relacionadas à IA está cada vez mais concentrada na função de tecnologia. No que diz respeito à implementação, 59% dos participantes afirmam ser o decisor final. Isso reflete a ampliação do escopo





do cargo: exigem dos CIOs não apenas a entrega, mas também a integridade estratégica da IA em toda a sua organização.

Ainda assim, a confiança nas estruturas que sustentam essas decisões permanece desigual. Apenas um em cada três CIOs (36%) afirma estar extremamente confiante de que dispõe de orientações abrangentes e boas práticas para liderar iniciativas de IA de forma eficaz.

Os CIOs estão sendo posicionados como a autoridade máxima na implementação da IA, ao mesmo tempo em que se reconhece que os modelos de governança necessários para sustentar essa autoridade ainda estão em amadurecimento.

As preocupações com o ritmo reforçam essa tensão. Pouco mais da metade dos respondentes (51%) acredita que a imple-

mentação de IA em suas empresas está acontecendo rápido demais. Isso não sinaliza resistência ou ceticismo, mas reflete a percepção de que o impulso começa a superar a infraestrutura disponível. Mais da metade dos CIOs (55%) não tem forte confiança de que sua organização possua um roadmap de IA coerente para os próximos dois a três anos, e 58% afirmam que as unidades de negócio e a liderança central de TI não estão totalmente alinhadas quanto às prioridades e à direção da IA.

Para os CIOs, trata-se de um desafio de liderança, mais do que técnico. Prioridades pouco claras e falta de alinhamento dificultam o estabelecimento de padrões corporativos, governança de riscos consistente e a escalabilidade de iniciativas bem-sucedidas para além de equipes isoladas. Sem coerência, a

adoção de IA corre o risco de tornar-se desigual, reativa e cada vez mais difícil de controlar.

Os pontos sobre sustentabilidade acrescentam uma nova dimensão a essa responsabilidade. À medida que o uso de IA se expande, suas demandas energéticas e seu impacto ambiental tornam-se mais difíceis de ignorar. Ainda assim, a confiança permanece limitada: apenas 39% dos CIOs estão extremamente confiantes de que suas empresas medem e gerenciam o impacto ambiental das iniciativas de IA, e somente 41% expressam o mesmo nível de confiança de que a eficiência de energia é priorizada na implementação da IA.

Isso marca uma mudança significativa no escopo da liderança em IA. Os CIOs já não são responsáveis apenas pelos custos

financeiros e de segurança da IA, mas também, cada vez mais, por suas implicações em sustentabilidade. À medida que as expectativas regulatórias e a rigorosidade dos conselhos aumentam, a responsabilidade ambiental passará a fazer parte do que significa liderar uma IA corporativa responsável.

Em conjunto, esses achados apontam para uma redefinição do papel do CIO. A liderança na era da IA está se tornando menos sobre a rapidez do avanço das corporações e mais sobre o quão deliberadamente elas conseguem fazê-lo.

A capacidade de desacelerar determinadas decisões para acelerar um progresso sustentável está se tornando uma das competências definidoras do CIO moderno. ●

CAPÍTULO 2

Da confiança à capacidade



Há um forte sentimento de confiança na forma como os CIOs avaliam a posição de suas organizações em relação à IA. Em comparação com seus pares, muitos acreditam já estar à frente em capacidades generativas, preditivas e agênticas — e essa percepção é relevante. Ela sinaliza impulso, investimento e intenções firmes. No entanto, estar à frente dos outros não significa, necessariamente, estar pronto para operar a IA em escala corporativa.

Essa distinção torna-se clara quando os CIOs passam da comparação para a capacidade. A IA já está gerando valor em áreas específicas, especialmente onde dados, responsabilidades e processos estão relativamente bem estabelecidos. O maior impacto é observado em analytics preditivo e previsões (56%), seguido por melhorias na experiência do cliente e na entrega de serviços (ambos com 45%) e no apoio à inovação e à geração de ideias (43%). Esses são ganhos relevantes e demonstram que a IA já superou a fase puramente experimental. O que eles ainda não demonstram é consistência. Esses sucessos tendem a estar concentrados em funções específicas ou equipes mais engajadas, em vez de fazerem parte de um modelo corporativo replicável. A IA funciona, mas ainda não está incorporada de forma estrutural.

É nesse ponto que a confiança começa a se abalar. Quando os CIOs avaliam sua capacidade de avançar dos primeiros sucessos para um impacto de grande magnitude, quase dois terços não estão fortemente confiantes de

Dois terços dos CIOs não estão totalmente confiantes de que conseguem evoluir a IA para além de projetos pilotos

89% dizem que estão “aprendendo enquanto fazem”

que conseguem escalar a IA além de pilotos e provas de conceito (65%). Uma proporção semelhante não demonstra forte confiança de que os investimentos em IA já tenham gerado valor de negócio mensurável (62%). Esse número praticamente não mudou desde 2025, sugerindo que, após um ano, não houve garantia de que o investimento em IA teve retorno efetivo para o negócio.

Esses dados apontam para um padrão conhecido. A IA já provou seu potencial,

mas ainda não provou sua confiabilidade. Para os CIOs, este é o momento em que a liderança deixa de incentivar apenas a experimentação e passa a construir uma capacidade de negócio confiável.

Parte do desafio está na forma como a IA cresceu. A maioria das empresas descreve sua abordagem como “Aprendemos enquanto fazemos” (89%). Essa mentalidade impulsionou avanços rápidos, reduziu barreiras de entrada e estimulou a inovação. Porém, também

significa que muitas iniciativas de IA se desenvolveram sem modelos operacionais estáveis por trás. O que funciona em um ambiente de aprendizado nem sempre resiste às exigências de escala, auditabilidade ou análise regulatória.

As barreiras identificadas pelos CIOs reforçam esse ponto. A restrição mais citada não é orçamento, mas habilidades. A falta de capacidade técnica interna está limitando as ambições em IA em quase nove de cada dez organizações (88%). Os



As maiores barreiras para a adoção da IA

- Falta de competências técnicas internas - **(88%)**
- Questões regulatórias e de compliance - **(88%)**
- Desafios relacionados a dados - **(87%)**

desafios relacionados a dados vêm logo em seguida (87%), acompanhados por limitações de infraestrutura (84%).

Não se trata de problemas operacionais menores, mas problemas que determinam se a IA pode ou não ser escalada.

Sem habilidades suficientes, a IA permanece dependente de um pequeno grupo de especialistas. Sem bases de dados robustas, os resultados continuam difíceis de confiar.

Sem infraestrutura escalável, o sucesso permanece limitado. Em conjunto, essas fragilidades impedem que a IA se torne um alicerce organizacional, em vez de uma série de projetos isolados.

O que a pesquisa sugere é que a maturidade em IA tem menos a ver com tecnologia e mais com desenho organizacional.

Escalar a IA exige os mesmos elementos necessários para escalar qualquer capacidade corporativa: padronização, governança, responsabilização e mensuração. Exige clareza sobre quem é responsável pelos sistemas quando entram em produção, como o desempenho é monitorado e como o risco é absorvido.

É por isso que a diferença entre confiança e capacidade é tão relevante. Confiança reflete otimismo e ímpeto. Capacidade reflete disciplina e preparação.

Para os CIOs, o desafio é transformar o sucesso inicial em algo mais duradouro. Agora, o trabalho real não é provar o que a IA pode fazer, mas torná-la confiável o suficiente para ser escalada com segurança e gerar um benefício líquido para o negócio. ●

CAPÍTULO 3

Gerenciando a segurança na era da IA





34% dizem que a IA criou novos pontos cegos na segurança

A cibersegurança já operava sob pressão constante muito antes de a IA entrar em cena. Os investimentos aumentaram, as ferramentas se multiplicaram e o volume de ameaças continuou a crescer. Ainda assim, a confiança não evoluiu no mesmo ritmo.

O relatório do ano passado destacou o paradoxo do “buraco negro dos investimentos em segurança”: gastos crescentes acompanhados de incidentes persistentes. Essa tensão não desapareceu. A maioria das organizações ainda relata ter sofrido algum incidente de cibersegurança nos últimos 12 meses (77%) e, embora esse número tenha atingido o pico de 88% em 2025, o desafio está longe de estar sob controle.

Malware e ransomware continuam sendo as ameaças dominantes (33%), seguidos de perto por phishing (30%). O ambiente básico de risco permanece imprevisível, intensivo em recursos e estruturalmente exigente.

O que mudou foi o próprio cenário de ameaças. A IA deixou de ser apenas uma ferramenta utilizada pelas equipes de segurança para melhorar a detecção ou automatizar respostas. Ela passou a fazer parte da superfície de ataque.

Mais de um quarto dos CIOs agora classifica a própria IA como uma fonte significativa de risco (28%), colocando-a no mesmo patamar de vetores de ataque cibernético mais tradicionais.

As equipes de segurança já não protegem apenas sistemas e dados. Cada vez mais, são chamadas a governar comportamentos, automações e tomadas de decisão que operam com certo grau de autonomia.

Ao mesmo tempo, os fundamentos da aptidão de segurança seguem sob pressão. Os CIOs continuam apontando a escassez de habilidades especializadas em cibersegurança como uma fraqueza relevante (30%), assim como a falta de conscientização dos colaboradores, que expõe as organizações a riscos desnecessários (32%). Esses não são problemas novos, mas a IA amplia seu impacto. À medida que os sistemas se tornam mais complexos, as consequências de erros

humanos, interpretações equivocadas e usos inadequados tornam-se mais graves.

O treinamento tem dificuldade em acompanhar esse ritmo. Quase dois terços dos CIOs acreditam que suas organizações ainda não oferecem educação suficiente sobre o uso responsável da IA e os riscos associados ao seu uso (66%). Mais da metade afirma que os colaboradores estão colocando a segurança dos dados em risco pela forma como utilizam ferramentas de IA (57%).

Em nível operacional, as equipes de segurança já sentem os efeitos. Mais de um terço dos CIOs afirma que a IA criou novos pontos cegos de segurança (34%), enquanto uma proporção semelhante

acredita que ela reduziu a capacidade da organização de detectar violações e ataques cibernéticos de forma eficaz (35%). Ainda mais preocupante, dois em cada cinco relatam que os tempos de resposta a incidentes pioraram (41%).

Esses são sinais de alerta iniciais. A IA está aumentando a complexidade das operações de segurança mais rapidamente do que processos, habilidades e ferramentas conseguem se adaptar. Os sistemas estão se tornando mais difíceis de observar, interpretar e de controlar com confiança.

Apenas 27% dos CIOs dizem ter visibilidade total das ferramentas e serviços de IA em suas empresas

A maioria das organizações reconhece a necessidade de governança específica para IA, e quase todas afirmam ter algum tipo de controle implementado. No entanto, apenas cerca de um terço dos CIOs está extremamente confiante de que seus controles de governança de IA conseguem acompanhar o ritmo de implantação (34%), e pouco mais de um terço acredita ter visibilidade total sobre todas as ferramentas e serviços de IA em uso na organização (37%).

Ainda mais revelador é o grau de concessão. Quase dois terços (62%) admitem ter flexibilizado padrões de governança devido à limitação de

62% admitem ter flexibilizado padrões de governança devido à limitação de entendimento ou capacidade

entendimento ou capacidade. Isso não representa uma falha de intenção, mas sim um sinal de que a governança de IA está avançando mais rápido do que a capacidade institucional.

Os dados revelam um desequilíbrio estrutural. A propriedade da IA está distribuída por toda a organização, mas a responsabilidade por suas consequências está cada vez mais concentrada no CIO.

Isso torna o risco da IA diferente da maioria dos riscos tecnológicos anteriores. Ele não é apenas técnico — é organizacional. Ele se instala nas lacunas entre papéis, equipes e direitos de decisão.

A dependência de fornecedores adiciona outra camada de fragilidade. Muitas organizações reconhecem que estão cada vez mais dependentes de um único fornecedor de IA para funções críticas (59%). Ao mesmo tempo, a preocupação com uma “bolha da IA” é generalizada (67%), refletindo inseguranças quanto à estabilidade e à maturidade do mercado. Apesar disso, uma parcela significativa ainda não possui planos de continuidade caso um fornecedor-chave se torne indisponível (16%).

Para os CIOs, isso amplia o conceito de segurança para além de sistemas e dados, incluindo cadeias de suprimentos, resiliência comercial e flexibilidade estratégica.



A resposta até agora tem sido pragmática. Muitas organizações estão recorrendo a suporte externo, seja terceirizando elementos da cibersegurança (32%), seja contratando profissionais temporários e especialistas para suprir lacunas urgentes (31%). Essas medidas trazem capacidade e expertise, mas também reforçam uma verdade mais profunda: a governança de riscos de IA está se tornando uma característica permanente da liderança, e não uma resposta temporária a uma nova tecnologia.

O que está emergindo é uma responsabilidade mais silenciosa e complexa. Os CIOs são requisitados a tornar a IA segura

o suficiente para ser confiável antes que se torne poderosa o suficiente para ser perigosa. Eles atuam em um ambiente onde a visibilidade é imperfeita, as habilidades são escassas e a responsabilidade é compartilhada.

Nesse contexto, governança deixa de ser apenas uma questão de políticas e passa a ser uma questão de julgamento.

O papel do CIO é cada vez mais definido por sua capacidade de manter a organização estável enquanto seus sistemas se tornam mais autônomos, mais interconectados e mais difíceis de controlar. ●

CAPÍTULO 4

A próxima fronteira



**60% das empresas planejam
investir em agentes de IA
nos próximos 12 meses**

questões de identidade, autoridade e rastreabilidade se tornam mais complexas. Quem é responsável quando um processo orientado por IA toma uma decisão equivocada? Como as ações são auditadas? Como distinguir intenção de erro? Essas não são questões abstratas de governança. Elas moldam o quanto as organizações estão dispostas a delegar responsabilidade às máquinas em fluxos de trabalho críticos.

As implicações para a força de trabalho são igualmente incertas. Algumas organizações esperam que a IA reduza o número de colaboradores (40%), enquanto outras acreditam que ele aumentará (31%). A diferença entre essas posições sugere que o impacto da IA não seguirá um único padrão. Provavelmente, ela remodelará funções em vez de simplesmente eliminá-las ou criá-las.

Para os CIOs, isso torna o desenho da força de trabalho parte da estratégia de IA. A questão passa a ser como estruturar ambientes nos quais humanos e sistemas de IA trabalhem juntos, como a autoridade é compartilhada e como a responsabilização é mantida quando o trabalho é distribuído entre pessoas e máquinas.

Além da IA, os CIOs também são chamados a pensar em múltiplos horizontes simultaneamente. Mais da metade acredita que a IA generativa e a agêntica irão romper com os modelos de negócios existentes nos próximos dois anos (53%). Ao mesmo tempo, a computação quântica já aparece nos roadmaps estratégicos, com quase um terço esperando que ela tenha impacto semelhante (30%).

A medida que a IA passa da posição de apoiar o trabalho para a de moldá-lo ativamente, a natureza da tecnologia corporativa volta a se transformar. A IA generativa ganhou destaque por ser visível e imediata, mas ela é apenas o primeiro passo de uma mudança mais longa em direção a sistemas que atuam com crescente independência. Para os CIOs, é nesse ponto que a conversa deixa de ser sobre ferramentas e passa a ser sobre comportamento. O que acontece quando a

tecnologia deixa de ser apenas algo que a organização utiliza e passa a participar de como ela opera?

Os padrões de investimento já refletem essa transição. A IA generativa permanece firme na agenda, com quase três quartos das organizações (72%) planejando novos investimentos nos próximos 12 meses. No entanto, o interesse avança rapidamente para além dela. Seis em cada dez esperam investir em IA agêntica (60%), sinalizando um apetite crescente por sistemas capazes de executar tarefas,

tomar decisões e coordenar atividades com mínima intervenção humana.

A IA está migrando de uma posição de apoio para a de tomada de ação autônoma. Para os CIOs, as implicações dizem menos respeito ao desempenho e mais à responsabilização. Sistemas que aconselham podem ser questionados. Sistemas que agem precisam ser governados.

As consequências práticas disso estão apenas começando a emergir. À medida que a IA se torna mais autônoma,

Isso traz consequências para os modelos operacionais. A crescente dependência de Provedores de Serviços Gerenciados (Managed Service Providers – MSPs) reflete o reconhecimento de que poucas organizações conseguem sustentar sozinhas o ritmo de mudança. Quase todas esperam utilizar MSPs nos próximos anos (94%), e quase metade antecipa que parceiros externos entregarão serviços essenciais de TI (47%).

Isso transforma novamente o papel do CIO. A liderança em tecnologia passa a ser menos sobre propriedade e mais sobre orquestração.

A empresa passa a depender de uma rede de fornecedores, plataformas e especialistas, e gerenciar esse ecossistema torna-se tão importante quanto gerenciar equipes internas.

Para os CIOs, isso exige um tipo diferente de liderança. Menos focada em projetos de transformação e mais em desenho institucional. Menos em implantar novas ferramentas e mais em moldar ambientes nos quais sistemas autônomos, parceiros externos e equipes humanas possam coexistir sem comprometer a responsabilização.

Se os capítulos anteriores mostraram como a IA está acelerando pressão, complexidade e risco, este aponta para algo mais duradouro. O CIO está se tornando o arquiteto de uma organização que precisa permanecer no controle mesmo quando a inteligência se torna distribuída, a autonomia se torna norma e o controle se torna mais difícil de centralizar. ●



Mais da metade dos CIOs acredita que a IA vai romper com os seus modelos de negócios nos próximos dois anos

Quase todas as organizações planejam confiar em Managed Service Providers nos próximos 2 a 3 anos



Conclusão

As perspectivas compartilhadas pelos CIOs neste relatório apontam para uma mudança profunda. A IA já não é algo para o qual as empresas estão se preparando — ela está moldando decisões, ampliando riscos e redefinindo o que significa responsabilidade dentro das corporações.

Para os CIOs, o papel está se tornando menos sobre introduzir novas capacidades e mais sobre moldar as condições sob as quais essas capacidades podem prosperar de forma sustentável.

Ao longo dos quatro capítulos, uma tensão consistente atravessa os dados. A ambição é alta, o impulso é forte e a crença no potencial da IA é ampla. Ao mesmo tempo, a confiança em governança, escalabilidade e controle de longo prazo é frágil.

Os CIOs operam em um ambiente no qual o progresso avança mais rápido do que as estruturas criadas para sustentá-lo. Espera-se que ajam de forma decisiva, ao mesmo tempo em que absorvem as consequências de decisões cujas implicações ainda não são totalmente visíveis.

O que a pesquisa revela não é hesitação, mas realismo. Os CIOs entendem que a IA não pode simplesmente ser implantada e evoluir sozinha; ela precisa ser orientada, mensurada e se tornar confiável antes de realmente gerar benefícios e retorno para o negócio.

Em ciclos tecnológicos anteriores, o sucesso era frequentemente medido pela rapidez com que novas capacidades eram implementadas. Na era da IA, o sucesso será medido pela eficácia com que essas capacidades são aproveitadas e gerenciadas, pela qualidade de sua governança,

pelo grau de autonomia que se pode permitir e pela confiança com que as organizações podem depender delas sem perder de vista o julgamento humano e a responsabilização institucional.

Essa é uma responsabilidade maior do que qualquer projeto tecnológico isolado, e é exatamente isso que torna este momento um dos mais significativos da história do papel do CIO. ●

Somos arquitetos da mudança. Ajudamos organizações a prosperar em um mundo cada vez mais digital.

Na Logicalis, aproveitamos nossa experiência coletiva em tecnologia para ajudar nossos clientes a construir um plano para o sucesso, para que possam alcançar resultados sustentáveis e relevantes.

www.la.logicalis.com/pt-br/cio-report