



Microsoft 365
Copilot

Garantir a Segurança de Dados na Era da IA

Um Guia para Líderes de TI



E-book

Este guia foi redigido para líderes de TI que precisam de fomentar a adoção de IA enquanto mantêm os dados das suas organizações seguros. Ajudará a entender os riscos que a IA apresenta para a segurança e a privacidade de dados, ao mesmo tempo que fornece os insights necessários para liderar a transformação de IA da sua empresa com confiança.

Índice

01

As novas regras do trabalho com tecnologia de IA

02

Compreender o impacto da IA na segurança de dados

03

O desafio da IA sombra

04

A realidade BYOAI

05

O labirinto regulamentar

06

Uma estrutura que prioriza a segurança para avaliação das soluções de IA

07

Microsoft 365 Copilot: IA em que pode confiar

08

O caminho seguro para a transformação da IA

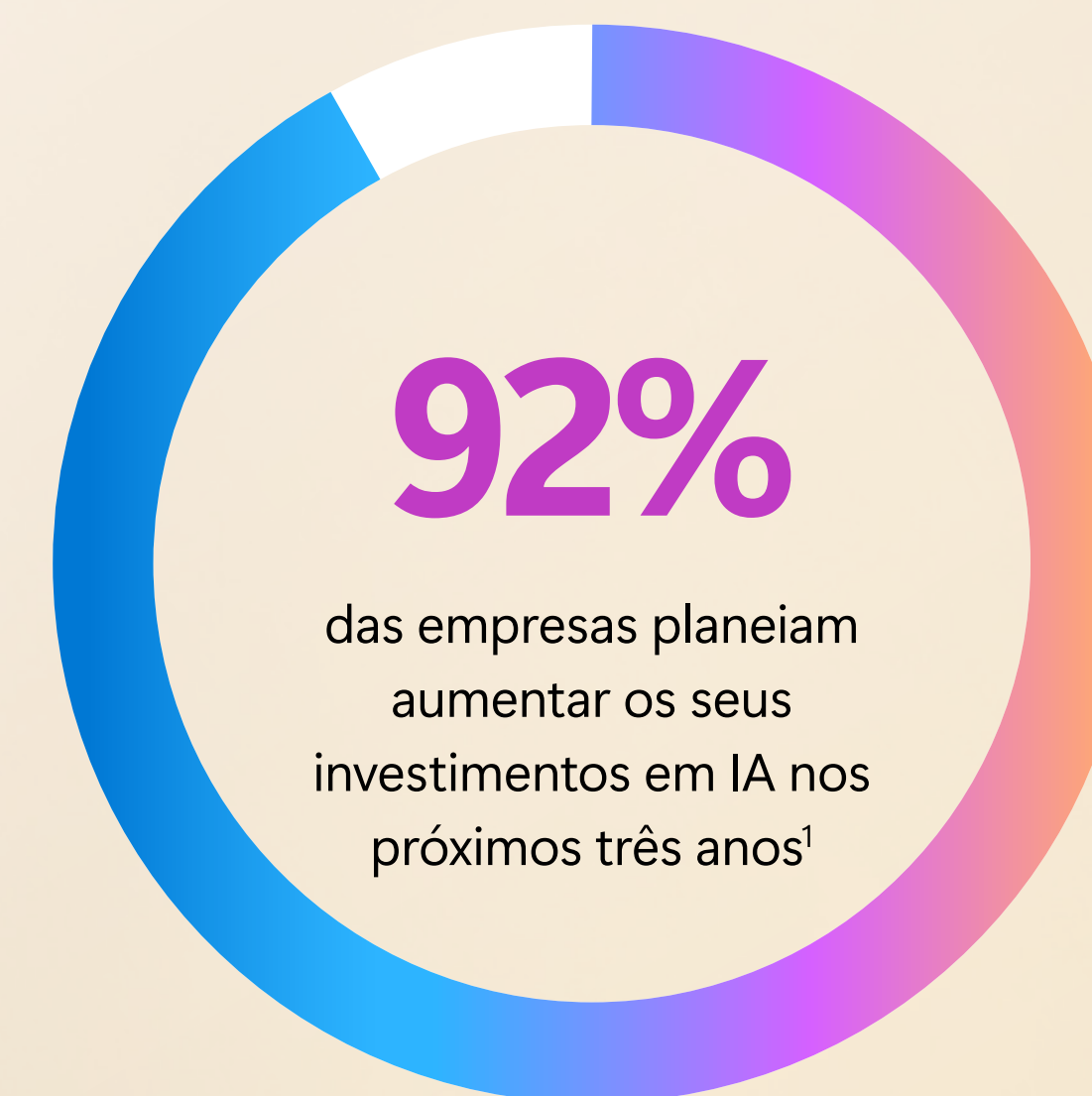
01

As novas regras do trabalho com tecnologia de IA

A IA generativa está a abrir novas portas para a inovação e a ajudar as equipas a trabalhar mais rapidamente e de forma mais inteligente do que nunca. Para organizações com visão de futuro, a IA não é apenas mais uma tendência tecnológica, mas um imperativo de negócio, essencial para a forma como operam, entregam valor e sustentam uma vantagem competitiva.

Mas esta rápida adoção traz desafios novos e ampliados que os líderes de TI devem abordar e controlar proativamente. Os sistemas de IA podem pesquisar e combinar informações ativamente em todo o ecossistema de dados, aumentando os riscos de segurança além das ferramentas tradicionais. Apesar da rápida expansão da IA, apenas **1%** das organizações relatam ter integrado totalmente a IA nos seus workflows com protocolos de segurança adequados.¹ Ao implementar medidas robustas de segurança e governação desde o início do seu percurso de IA, a sua equipa pode proteger eficazmente dados confidenciais, manter os requisitos de conformidade e salvaguardar as informações da sua organização, tudo isto enquanto permite que a inovação floresça.

A onda de adoção de IA já chegou



02

Compreender o impacto da IA na segurança de dados

Antes de aprofundar desafios específicos, é importante compreender como a IA muda fundamentalmente o panorama da segurança de dados. Ao contrário do software tradicional que só acede a dados quando especificamente instruído, a IA generativa processa, analisa e cria conteúdo ativamente com base em todas as informações que recebe.

Esta diferença é significativa por várias razões:

- As ferramentas de IA podem descobrir ligações entre dados que os humanos podem ignorar
- Podem sintetizar informações em várias fontes automaticamente
- Podem gerar novo conteúdo que contém elementos de entradas confidenciais

As suas ferramentas de segurança tradicionais provavelmente não foram projetadas com estas funcionalidades em mente. Enquanto o software convencional segue caminhos previsíveis ao aceder a dados, a IA pode adotar rotas inesperadas através do seu ecossistema de informações, expondo potencialmente dados confidenciais de formas imprevistas.

Esta mudança fundamental requer novas abordagens à segurança e governação de dados que resolvam especificamente como a IA interage com os ativos informativos da sua organização.



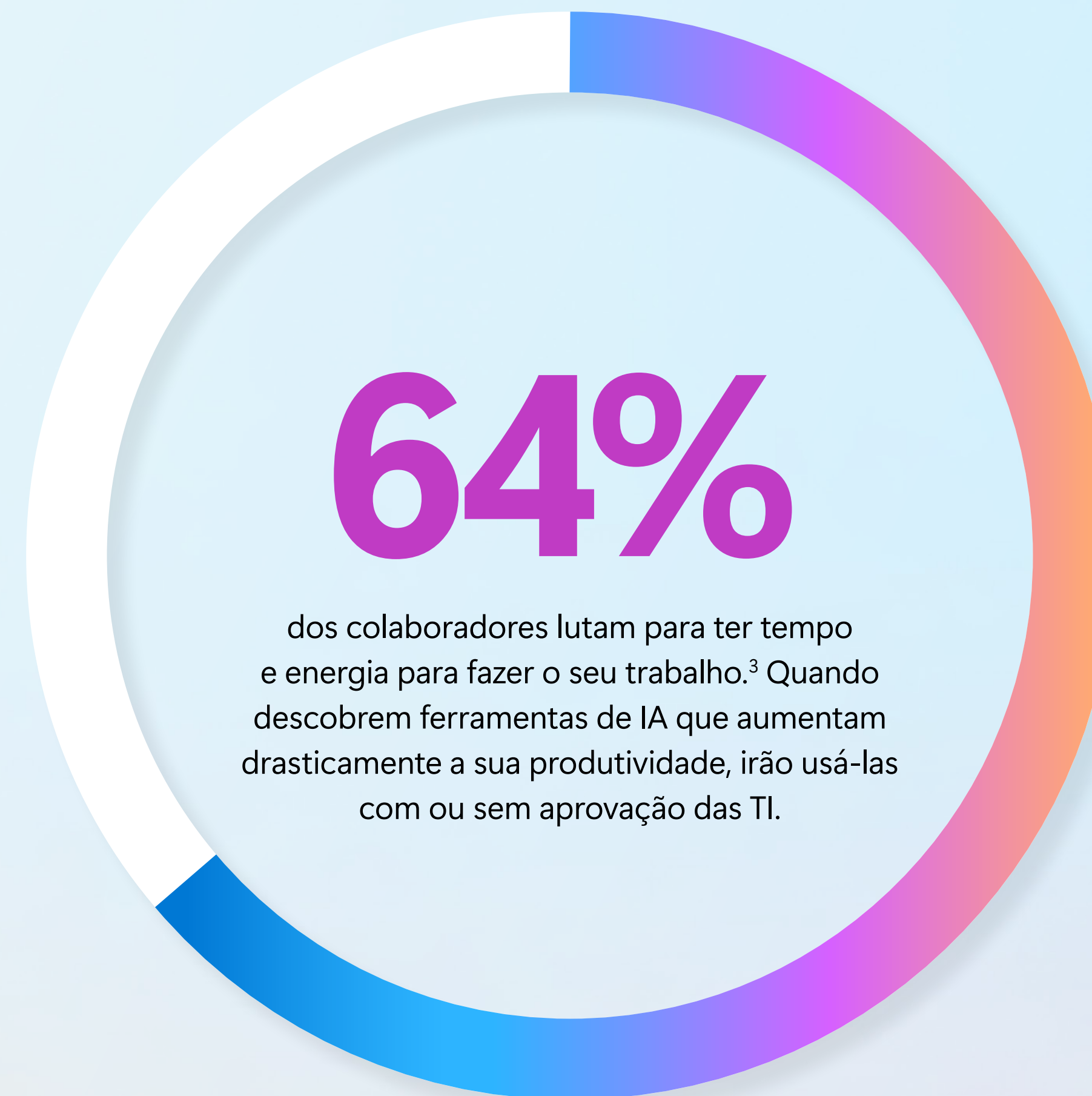
03

O desafio da IA sombra

Onde quer que se encontre no seu percurso de adoção de IA, os seus colaboradores já estão a encontrar as suas próprias soluções, criando o que é conhecido como "IA sombra".

Esta utilização não autorizada cria ângulos mortos relevantes na sua postura de segurança. Quando os colaboradores partilham dados da empresa com sistemas de IA externos, ignoram os controlos de segurança existentes e criam vulnerabilidades que a maioria das organizações não está preparada para resolver.

A IA sombra não é apenas uma questão de segurança, na medida em que pode ser um sintoma de necessidades de produtividade não satisfeitas na sua organização. Quando os colaboradores recorrem a ferramentas não sancionadas, estão a sinalizar onde os seus sistemas oficiais não estão a cumprir os seus requisitos. Resolver a IA sombra exige uma governação mais forte e soluções de produtividade avançadas.

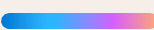


Motivos do surgimento da IA sombra:

- Os colaboradores anseiam aumentar a produtividade através dos impressionantes recursos da IA
- As workloads diárias excedem cada vez mais o tempo e a energia disponíveis
- As equipas enfrentam uma pressão crescente para entregar mais com os mesmos recursos
- As ferramentas de IA do consumidor oferecem soluções imediatas sem barreiras de aprovação
- Os processos oficiais de aquisição de TI não conseguem acompanhar o ritmo da inovação

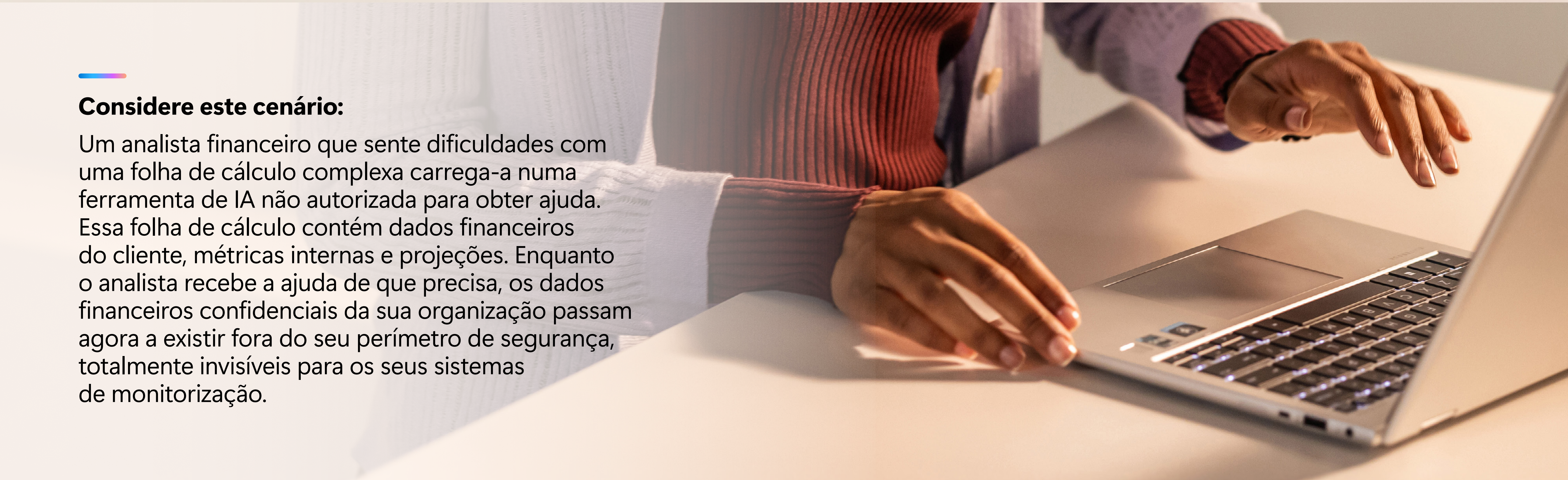
Riscos da IA sombra:

- Nenhuma visibilidade sobre os dados da empresa que estão a ser processados por sistemas externos de IA
- Nenhuma garantia de que as informações confidenciais não estão a ser retidas
- Sem padrões de segurança consistentes em diferentes plataformas de IA
- Inexistência de capacidade de auditoria para fins de conformidade
- Inexistência de integração com a sua infraestrutura de segurança existente



Considere este cenário:

Um analista financeiro que sente dificuldades com uma folha de cálculo complexa carrega-a numa ferramenta de IA não autorizada para obter ajuda. Essa folha de cálculo contém dados financeiros do cliente, métricas internas e projeções. Enquanto o analista recebe a ajuda de que precisa, os dados financeiros confidenciais da sua organização passam agora a existir fora do seu perímetro de segurança, totalmente invisíveis para os seus sistemas de monitorização.



04

A realidade BYOAI

Sem uma orientação clara da liderança, os colaboradores estão cada vez mais a adotar a IA pelas suas próprias mãos: **78%** dos utilizadores de IA estão a adotar a abordagem "traga a sua própria IA" (BYOAI) para o trabalho.² Esta tendência é ainda mais evidente nas pequenas e médias empresas, onde **80%** dos colaboradores se envolvem em práticas BYOAI.²

Esta abordagem não sancionada apresenta desvantagens significativas. Os colaboradores mantêm geralmente a sua utilização de IA em segredo: **52%** sentem relutância em admitir que utilizam IA para tarefas importantes e **53%** preocupam-se que a utilização de IA os faça parecer substituíveis.² Este sigilo não só impede que as organizações compreendam todos os benefícios da implementação estratégica da IA, mas também cria graves vulnerabilidades de segurança num ambiente onde os líderes citam a segurança e a privacidade de dados como a sua preocupação **n.º 1**.²

Dada a utilização generalizada e o inevitável crescimento da IA, a questão não é se deve permitir IA na sua organização, mas como fornecer uma solução segura que dê resposta às necessidades dos seus colaboradores, mantendo os dados da sua organização protegidos.

05

O labirinto regulamentar

As estruturas e leis relacionadas com a privacidade e a segurança de dados criam outra camada de complexidade ao adotar IA. Enquanto algumas estruturas são projetadas especificamente para a governação de IA, outras têm aplicações mais amplas que ainda afetam a forma como lida com as informações, e as penalidades por violações permanecem severas.

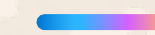
Quando os seus colaboradores usam ferramentas de IA sem supervisão adequada, podem, sem querer, criar violações de conformidade. A IA aumenta este risco porque pode aceder, combinar e expor informações regulamentadas de formas que as tecnologias tradicionais não conseguem fazer.

Regulamentações-chave que afetam a utilização de IA:



RGPD

O Regulamento Geral sobre a Proteção de Dados da União Europeia confere às pessoas controlo sobre os seus dados pessoais e exige consentimento claro para o seu processamento



Lei de IA da UE

A estrutura abrangente da União Europeia especificamente concebida para regular os sistemas de inteligência artificial com base nos seus níveis de risco



HIPAA

Esta lei federal dos EUA para cuidados de saúde estabelece padrões rigorosos para lidar com informações protegidas de saúde



Estrutura de Gestão de Riscos de IA do NIST

Esta orientação voluntária dos EUA ajuda as organizações a resolver os riscos no projeto, desenvolvimento e implementação de sistemas de IA

Os riscos de conformidade com a IA:

- Dados do cliente a serem processados em servidores fora das regiões aprovadas
- Informações pessoais a serem usadas sem o devido consentimento
- Dados confidenciais que persistem nos sistemas sem controlos de retenção apropriados
- Inexistência de registos de auditoria sobre a forma como as informações estão a ser acedidas e usadas
- Conteúdo gerado por IA que viola os requisitos de conformidade específicos do setor

Estas violações podem gerar consequências graves:

- Grandes penalidades financeiras (as multas do RGPD podem atingir **4%** da sua receita global)⁴
- Requisitos para notificar as partes afetadas sobre violações de dados
- Ações judiciais por parte dos afetados
- Danos à reputação da sua empresa e à confiança do cliente

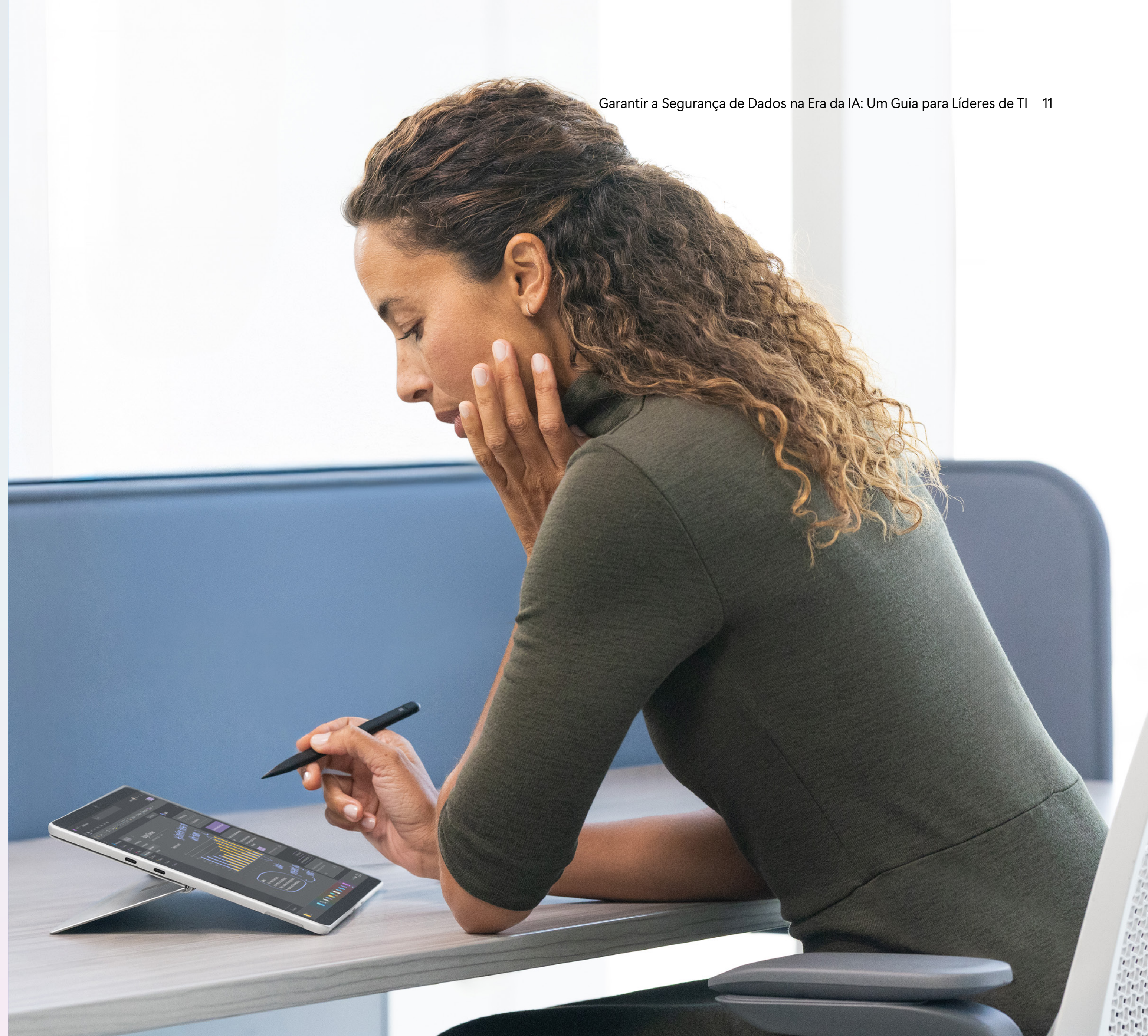
À medida que a utilização de IA aumenta na sua organização, precisa de governação que ajude as pessoas a trabalhar de forma eficiente, mantendo a sua organização em conformidade com as regulamentações que afetam a sua empresa e os seus clientes.

06

Uma estrutura que prioriza a segurança para avaliação das soluções de IA

Com a IA sombra, a BYOAI e as regulamentações que criam riscos significativos, precisa de uma abordagem estruturada para avaliar soluções de IA que garanta ajuda à sua organização a impulsionar a inovação, ao mesmo tempo que protege dados confidenciais e assegura a conformidade com os requisitos regulamentares em evolução.

A estrutura seguinte fornece seis perguntas simples para avaliar se uma plataforma de IA dá resposta a ambas as frentes.



Pergunta 1

Oferece segurança de nível empresarial desde o início?

Com a solução certa, a sua segurança passa de apenas reagir aos problemas depois de acontecerem para procurar proativamente vulnerabilidades nos dados da sua organização, antes que se tornem problemas maiores.

Procure soluções que:

- Forneçam visibilidade em tempo real em todo o seu ecossistema de dados
- Identifiquem automaticamente potenciais riscos de dados antes que se tornem incidentes
- Protejam informações confidenciais em todos os níveis

Pergunta 2

Pode facilmente adotar e melhorar os controlos de segurança existentes?

As políticas de segurança da sua organização devem funcionar perfeitamente com a IA. O seu fornecedor de soluções de IA deve respeitar e integrar-se nas suas estruturas de segurança existentes, não exigir que crie estruturas totalmente novas.

Procure soluções que:

- Adotem facilmente as suas políticas de segurança, etiquetas de confidencialidade e definições de proteção de informações existentes
- Apliquem controlos de acesso granular ao nível individual, para que nenhum utilizador tenha acesso aos dados que não deve
- Sinalizem ativamente tentativas de subversão dos controlos de acesso

Pergunta 3

Inclui controlos integrados de governação e privacidade?

Como as ferramentas de IA funcionam de forma mais proativa, as suas medidas de segurança também devem ser proativas. A implementação de uma forte governação de dados cria limites claros onde os seus colaboradores podem inovar com segurança sem colocar informações confidenciais em risco.

Procure soluções que:

- Centralizem a governação de IA com a aplicação automatizada de políticas em todas as atividades
- Incluam a deteção precoce de potencial excesso de partilha de dados
- Estejam em linha com as estruturas regulamentares para garantir a utilização em conformidade da IA

Pergunta 4

Pode ser implementada de forma consistente em toda a organização?

Os seus colaboradores têm os seus próprios estilos de trabalho, os seus próprios horários e podem estar localizados em todo o mundo. A IA deve beneficiar todos.

Procure soluções que:

- Ofereçam configuração sem falhas e fácil adoção de IA em workflows diários
- Forneçam acesso flexível, desde chat de IA gratuito até soluções escaláveis de agentes
- Ajudem os colaboradores a desenvolver fluência em IA e a integrá-la no seu trabalho

Pergunta 5

Integra-se perfeitamente nas estruturas existentes?

A sua empresa opera atualmente com a sua própria infraestrutura digital de programas de software, aplicações e muito mais.

Procure soluções que:

- Se integrem perfeitamente com as suas ferramentas e programas para minimizar interrupções
- Forneçam uma experiência contínua de IA em todas as aplicações para que o trabalho possa fluir perfeitamente entre as ferramentas
- Automatizem e otimizem tarefas nos workflows existentes

Pergunta 6

Os utilizadores estão capacitados a inovar?

Na sua essência, a IA deve transformar a forma como o trabalho é feito. Não se trata apenas de automatização, mas de aumentar a produtividade e impulsionar a inovação.

Procure soluções que:

- Convertam o desperdício de tempo em processos simplificados
- Automatizem tarefas repetitivas
- Capacitem os trabalhadores a recuperarem tempo e se concentrarem nas prioridades

07

Microsoft 365 Copilot: IA em que pode confiar

O Microsoft 365 Copilot é a solução de IA generativa criada para oferecer segurança, governação e controlos de acesso robustos, garantindo implementação segura e inovação sustentada. Aumenta a produtividade com ferramentas intuitivas como o Copilot Chat, que trabalha consigo e o Copilot Studio, onde a sua equipa pode criar agentes de IA personalizados sem competências de codificação.

O Copilot integra-se perfeitamente no seu ambiente do Microsoft 365, herdando permissões de utilizador, etiquetas de sensibilidade, políticas de prevenção de perda de dados e requisitos de residência de dados geográficos, sem configuração adicional. Ao incorporar a IA nas ferramentas que os seus colaboradores já usam, o Copilot reduz os riscos de segurança enquanto mantém os dados no seu ambiente fidedigno do Microsoft 365.

Os compromissos da Microsoft garantem que a sua organização mantém o controlo:

- Os seus dados estão protegidos, quer sejam inativos ou em circulação
- Os seus dados não são usados para treinar modelos de IA
- Escolhe que informações vão para a cloud
- Está protegido contra riscos de segurança de IA e de direitos de autor

As ferramentas de governação criadas especificamente para este fim, como o Sistema de Controlo do Copilot e a gestão Avançada do SharePoint oferecem às equipas de TI a visibilidade, os controlos e os registos de auditoria necessários para manter a conformidade.

Com o Microsoft 365 Copilot, não precisa de escolher entre inovação e segurança, pois pode ter ambos.



O caminho seguro para a transformação da IA

A revolução da IA apresenta uma oportunidade única para os líderes de TI fornecerem valor estratégico, equilibrando inovação e segurança.

Ao implementar ferramentas de IA seguras, como o Microsoft 365 Copilot, irá capacitar os colaboradores com ferramentas para maior produtividade, ao mesmo tempo que elimina os riscos da IA sombra. O caminho a seguir passa por permitir a inovação de forma segura. A sua liderança na adoção segura de IA irá posicionar as TI como um facilitador de transformação, ajudando a sua organização a prosperar nesta nova era, mantendo os dados seguros e em conformidade.



Começar a utilizar o Microsoft 365 Copilot

Fontes:

¹ "Superagency in the workplace: Empowering people to unlock AI's full potential," McKinsey & Company, 28 de janeiro de 2025. <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/superagency-in-the-workplace-empowering-people-to-unlock-ais-full-potential-at-work>.

² "A IA no Trabalho Está Aqui. Agora vem a Parte Difícil." Índice de Tendências do Trabalho da Microsoft, 8 de maio de 2024. <https://www.microsoft.com/en-us/worklab/work-trend-index/ai-at-work-is-here-now-comes-the-hard-part>.

³ "A IA Vai Reparar o Trabalho?", Índice de Tendências do Trabalho da Microsoft, 9 de maio de 2023. <https://www.microsoft.com/en-us/worklab/work-trend-index/will-ai-fix-work>.

⁴ «Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)», Parlamento Europeu e Conselho da União Europeia, 27 de abril de 2016 <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>.