Microsoft 365 Copilot

Como garantir a segurança dos na era da IA

Um guia para líderes de TI

E-book

Este guia foi escrito para líderes de TI que precisam promover a adoção da IA, mantendo os dados de suas organizações seguros. Ele ajudará você a entender os riscos que a IA apresenta à segurança e à privacidade dos dados, ao mesmo tempo em que fornece os insights necessários para liderar a transformação da IA da sua empresa com confiança.

Índice

01

As novas regras do trabalho com a tecnologia de IA

A IA generativa está abrindo novas portas para a inovação e ajudando as equipes a trabalhar de forma mais rápida e inteligente do que nunca. Para organizações com visão de futuro, a IA não é apenas mais uma tendência tecnológica; é um imperativo empresarial, essencial para a forma como operam, entregam valor e mantêm uma vantagem competitiva.

Mas essa rápida adoção traz desafios novos e ampliados que os líderes de TI devem abordar e controlar proativamente. Os sistemas de IA podem procurar ativamente e combinar informações 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 a IA totalmente integrada em seus fluxos de trabalho com protocolos de segurança adequados.[1] Ao implementar medidas robustas de segurança e governança desde o início de sua jornada de IA, sua equipe pode proteger efetivamente dados confidenciais, manter requisitos de conformidade e proteger as informações da sua organização — tudo isso permitindo que a inovação floresça.

A onda de adoção da IA já chegou

02

Entenda o impacto da IA na segurança dos dados

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

Essa diferença é significativa por vários motivos:

- As ferramentas de IA podem descobrir conexões entre os dados que os humanos podem deixar passar
- Elas podem sintetizar informações em várias fontes automaticamente
- Elas podem gerar um novo conteúdo que contenha elementos de entradas confidenciais

Suas ferramentas de segurança tradicionais provavelmente não foram projetadas tendo esses recursos em mente. Embora o software convencional siga caminhos previsíveis ao acessar dados, a IA pode tomar rotas inesperadas por meio do seu ecossistema de informações, potencialmente expondo dados confidenciais de maneiras que você não antecipou.

Essa mudança fundamental exige novas abordagens de segurança e governança de dados que abordem especificamente como a IA interage com os ativos de informação da sua organização.

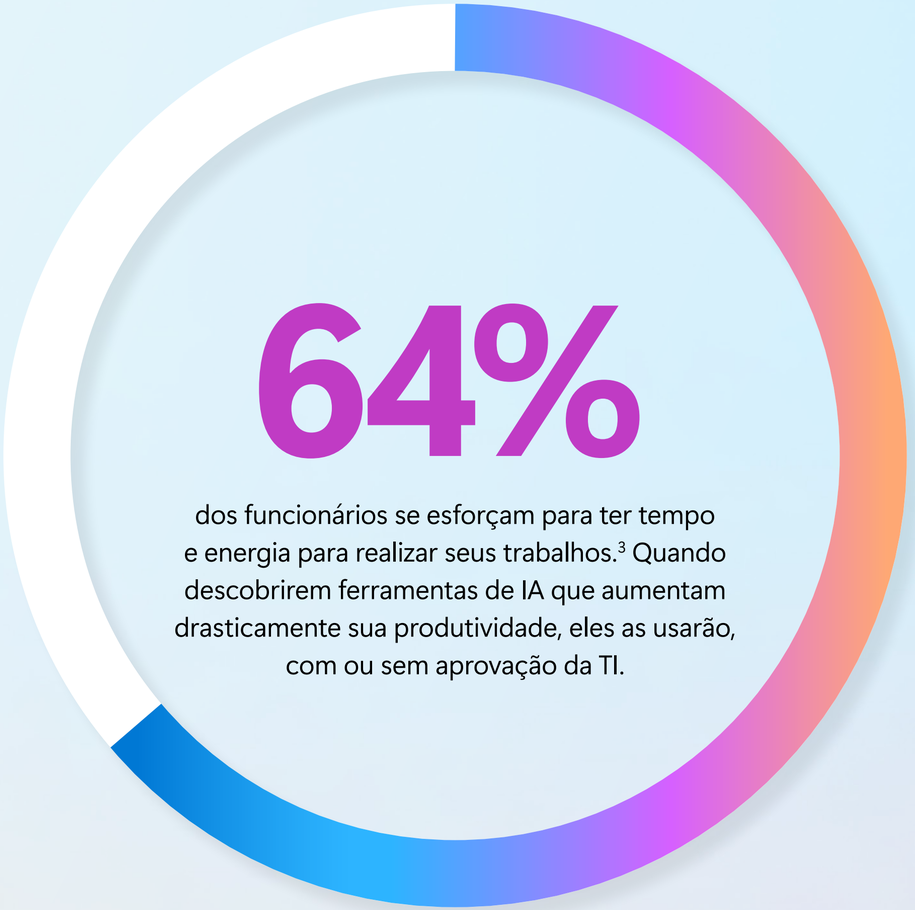
03

O desafio da shadow AI

Onde quer que você esteja em sua jornada de adoção da IA, seus funcionários já estão encontrando suas próprias soluções, criando o que é conhecido como “shadow AI”.

Esse uso não autorizado cria pontos cegos significativos em sua postura de segurança. Quando os funcionários compartilham dados da empresa com sistemas externos de IA, eles ignoram os controles de segurança existentes e criam vulnerabilidades que a maioria das organizações não está preparada para abordar.

Shadow AI não é apenas um problema de segurança— pode ser um sintoma de necessidades de produtividade não atendidas em sua organização. Quando os funcionários recorrem a ferramentas não sancionadas, eles sinalizam onde seus sistemas oficiais não estão atendendo aos seus requisitos. Lidar com a shadow AI requer governança mais forte e soluções de produtividade aprimoradas.



Por que surge a shadow AI:

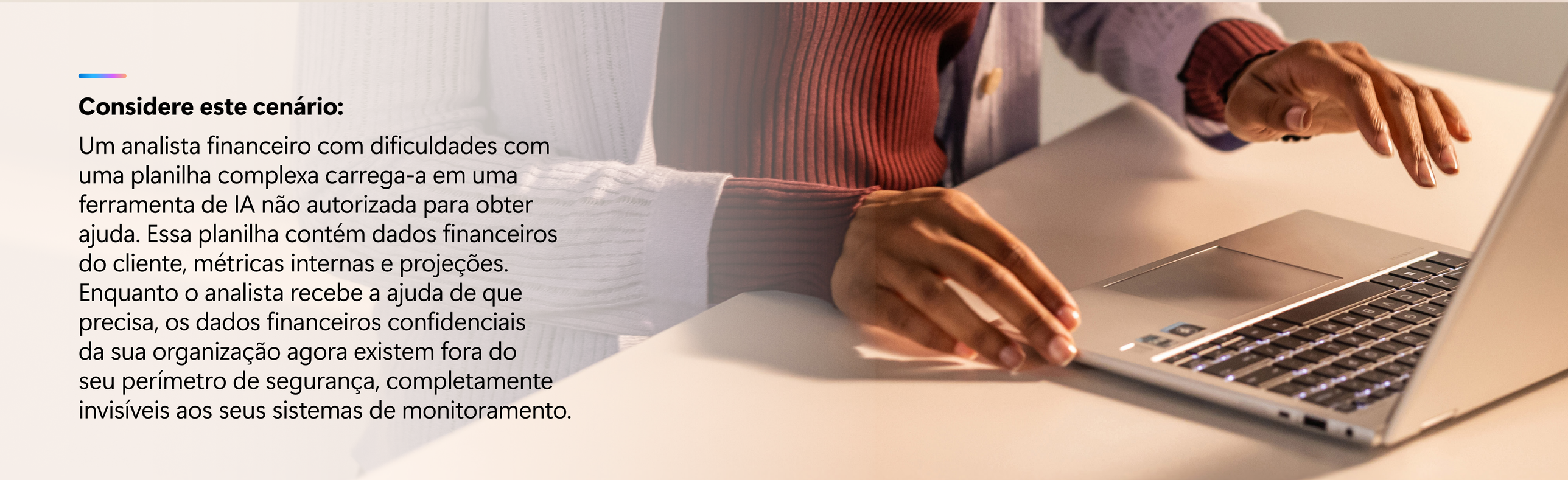
- Os funcionários estão ansiosos para aumentar a produtividade por meio dos impressionantes recursos da IA
- Os workloads diários excedem cada vez mais o tempo e a energia disponíveis
- As equipes enfrentam uma pressão crescente para entregar mais com os mesmos recursos
- As ferramentas de IA de consumo oferecem soluções imediatas sem barreiras de aprovação
- Os processos oficiais de aquisição de TI não correspondem ao ritmo da inovação

Os riscos da shadow AI:

- Nenhuma visibilidade sobre quais dados da empresa estão sendo processados por sistemas externos de IA
- Não há garantia de que informações confidenciais não estão sendo mantidas
- Nenhum padrão de segurança consistente em diferentes plataformas de IA
- Nenhuma capacidade de auditoria para fins de conformidade
- Nenhuma integração com sua infraestrutura de segurança existente

Considere este cenário:

Um analista financeiro com dificuldades com uma planilha complexa carrega-a em uma ferramenta de IA não autorizada para obter ajuda. Essa planilha 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 agora existem fora do seu perímetro de segurança, completamente invisíveis aos seus sistemas de monitoramento.



04

A realidade do BYOAI

Sem uma orientação clara da liderança, os funcionários estão cada vez mais tomando a adoção da IA em suas próprias mãos — **78%** dos usuários de IA estão adotando a abordagem "traga sua própria IA" (BYOAI) para o trabalho.[2] Essa tendência é ainda mais pronunciada nas pequenas e médias empresas, onde **80%** dos funcionários se envolvem em práticas de BYOAI.[2]

Essa abordagem não sancionada vem com desvantagens significativas. Os funcionários muitas vezes mantêm o uso da IA em segredo — **52%** estão relutantes em admitir o uso da IA para tarefas importantes e **53%** se preocupam que o uso da IA os faça parecer substituíveis.[2] Esse segredo não só impede as organizações de concretizarem todos os benefícios da implementação estratégica da IA, como também cria sérias vulnerabilidades de segurança num ambiente onde os líderes citam a cibersegurança e a privacidade dos dados como a preocupação nº **1**.[2]

Considerando o uso generalizado e o crescimento inevitável da IA, a questão não é se é preciso permitir a IA em sua organização — é como fornecer uma solução segura que atenda às necessidades de seus funcionários e, ao mesmo tempo, mantenha os dados da sua organização protegidos.

05

O labirinto dos regulamentos

Estruturas e leis em torno da privacidade e da segurança dos dados criam outra camada de complexidade ao adotar a IA. Embora algumas estruturas sejam projetadas especificamente para governança de IA, outras têm aplicações mais amplas que ainda afetam a maneira como você lida com informações — e as penalidades por violações continuam severas.

Quando seus funcionários usam ferramentas de IA sem supervisão adequada, eles podem criar involuntariamente violações de conformidade. A IA aumenta esse risco porque pode acessar, combinar e expor informações regulamentadas de maneiras que as tecnologias tradicionais não podem.

Principais regulamentos que afetam o uso da IA:

GDPR

O Regulamento Geral sobre a Proteção de Dados da União Europeia dá às pessoas controle sobre seus dados pessoais e requer consentimento claro para processá-los

Lei de IA da UE

O quadro abrangente da União Europeia concebido especificamente para regular os sistemas de inteligência artificial com base nos seus níveis de risco

HIPAA

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

NIST AI Risk Management Framework

Essa orientação voluntária dos EUA ajuda as organizações a abordar os riscos no design, no desenvolvimento e na implantação de sistemas de IA

Os riscos de conformidade com a IA:

- Dados do cliente sendo processados em servidores fora de regiões aprovadas
- Informações pessoais sendo usadas sem o devido consentimento
- Dados confidenciais persistem em sistemas sem controles de retenção apropriados
- Nenhuma trilha de auditoria de como as informações protegidas estão sendo acessadas e usadas
- Conteúdo gerado por IA que viola requisitos de conformidade específicos do setor

Essas violações podem levar a graves consequências:

- Grandes penalidades financeiras (as multas do GDPR podem atingir **4%** de sua receita global)[4]
- Requisitos para notificar as partes afetadas sobre violações de dados
- Ação judicial dos afetados
- Danos à reputação da sua empresa e à confiança do cliente

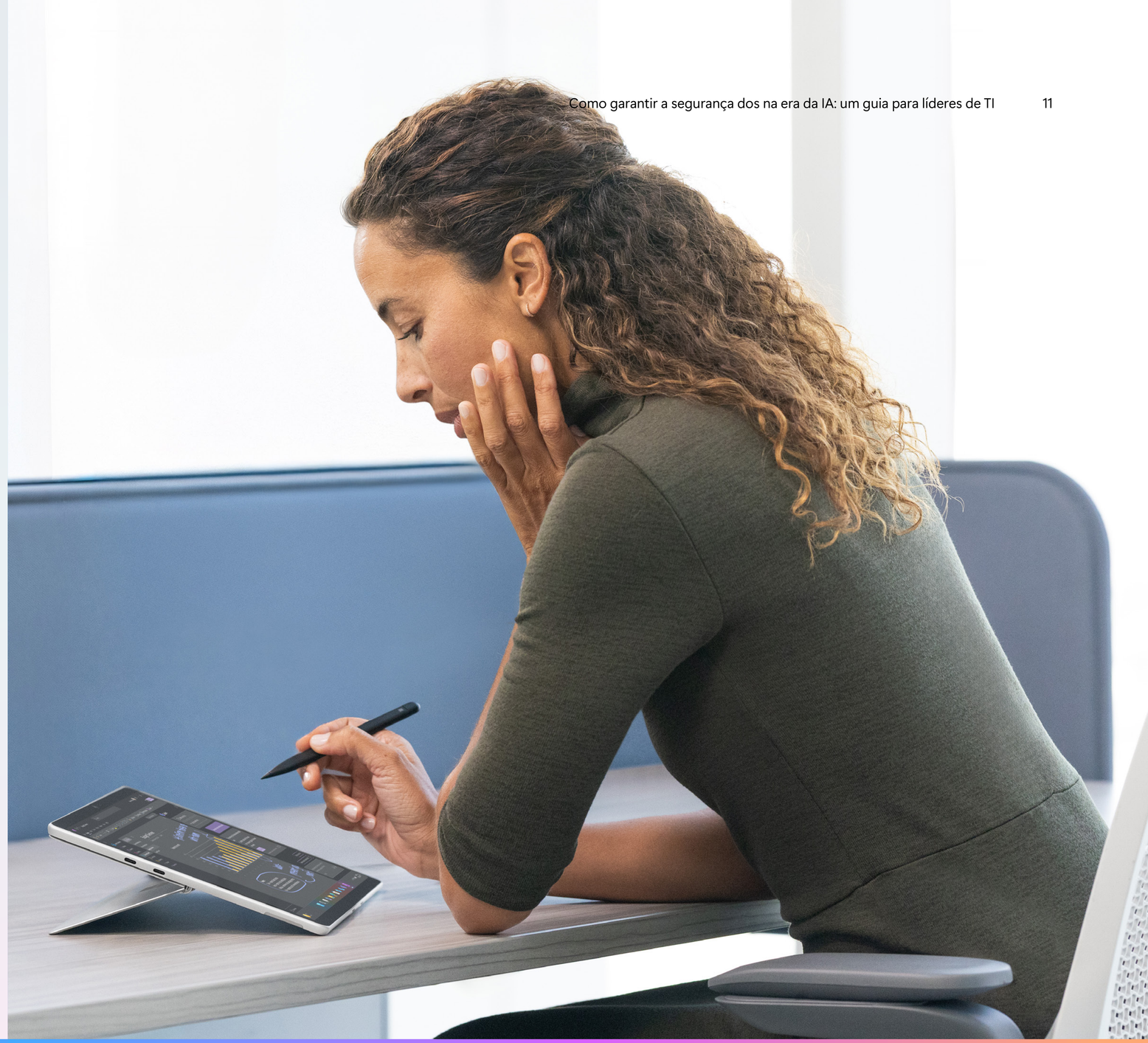
À medida que o uso da IA cresce em toda a sua organização, você precisa de governança que ajude as pessoas a trabalhar de forma eficiente, mantendo sua organização em conformidade com os regulamentos que afetam sua empresa e seus clientes.

06

Uma estrutura que prioriza a segurança para avaliar soluções de IA

Com a shadow AI, o BYOAI e os regulamentos criando riscos significativos, você precisa de uma abordagem estruturada para avaliar soluções de IA que garantam que elas possam ajudar sua organização a impulsionar a inovação, além de proteger dados confidenciais e garantir a conformidade com os requisitos regulamentares em evolução.

A estrutura a seguir fornece seis perguntas simples para avaliar se uma plataforma de IA oferece resultados em ambas as frentes.



Pergunta 1

Isso oferece segurança de nível empresarial desde o início?

Com a solução certa, sua segurança deixa de ser apenas reagir aos problemas depois que eles acontecem e passa a buscar 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 eles se tornem incidentes
- Protejam informações confidenciais em todos os níveis

Pergunta 2

Isso pode adotar e aprimorar facilmente os controles de segurança existentes?

As políticas de segurança da sua organização devem funcionar perfeitamente com a IA. Seu provedor de soluções de IA deve respeitar e integrar suas estruturas de segurança existentes, e não exigir que você crie estruturas totalmente novas.

Procure soluções que:

- Adotem perfeitamente suas políticas de segurança, rótulos de sensibilidade e configurações de proteção de informações existentes
- Apliquem controles de acesso granular no nível individual para que nenhum usuário tenha acesso aos dados que não deveria
- Sinalizem ativamente tentativas de subverter os controles de acesso

Pergunta 3

Isso inclui controles internos de governança e privacidade?

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

Procure soluções que:

- Centralizem a governança da IA com a aplicação automatizada de políticas em todas as atividades
- Incluam a detecção precoce de possíveis compartilhamentos excessivos de dados
- Alinhem-se com as estruturas regulatórias para garantir o uso da IA em conformidade

Pergunta 4

Isso pode ser implantado consistentemente em toda a organização?

Seus funcionários têm seus próprios estilos de trabalho, seus próprios horários e podem estar localizados em todo o mundo. A IA deve beneficiar a todos.

Procure soluções que:

- Ofereçam configuração perfeita e fácil adoção da IA em fluxos de trabalho diários
- Forneçam acesso flexível, desde chat de IA gratuito até soluções de agentes escaláveis
- Ajudem os funcionários a criar fluência em IA e integrá-la em seu trabalho

Pergunta 5

Isso se integra perfeitamente em as estruturas existentes?

Seu negócio opera atualmente com sua própria infraestrutura digital de programas de software, aplicativos e muito mais.

Procure soluções que:

- Combinam perfeitamente com suas ferramentas e programas para minimizar interrupções
- Forneçam uma experiência contínua de IA em todos os aplicativos para que o trabalho possa fluir perfeitamente entre as ferramentas
- Automatizam e otimizam tarefas dentro de fluxos de trabalho existentes

Pergunta 6

Os usuários estão capacitados para inovar?

Essencialmente, a IA deve transformar a maneira como o trabalho é feito. Não se trata apenas de automação, mas de aumentar a produtividade e impulsionar a inovação.

Procure soluções que:

- Transformem processos demorados em processos simplificados
- Automatizem tarefas repetitivas
- Capacitem os trabalhadores a recuperar tempo e se concentrar nas prioridades

07

Microsoft 365 Copilot: IA em que você pode confiar

O Microsoft 365 Copilot é a solução de IA generativa criada para fornecer controles robustos de segurança, governança e acesso, garantindo a implantação segura e a inovação sustentada. Ele aumenta a produtividade com ferramentas intuitivas como o Copilot Chat, que funciona onde você trabalha, e o Copilot Studio, onde sua equipe pode criar agentes de IA personalizados sem habilidades de codificação.

O Copilot integra-se perfeitamente ao seu ambiente do Microsoft 365, herdando permissões de usuário, rótulos de confidencialidade, políticas de prevenção contra perda de dados e requisitos de residência de dados geográficos, sem configuração extra. Ao incorporar a IA nas ferramentas que seus funcionários já usam, o Copilot atenua os riscos de segurança, mantendo os dados em seu ambiente confiável do Microsoft 365.

Os compromissos da Microsoft garantem que sua organização permaneça no controle:

- Seus dados estão seguros em repouso e em trânsito
- Seus dados não são usados para treinar os modelos de IA
- Você escolhe quais informações vão para a nuvem
- Você está protegido contra riscos de segurança e direitos autorais da IA

Ferramentas de governança criadas com finalidade específica, como o Copilot Control System e o SharePoint Advanced Management, dão às equipes de TI a visibilidade, os controles e os logs de auditoria necessários para manter a conformidade.

Com o Microsoft 365 Copilot, você não precisa escolher entre inovação e segurança — você pode ter os dois.

08

O caminho seguro para a transformação da IA

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

Ao implementar ferramentas de IA seguras, como o Microsoft 365 Copilot, você capacitará os funcionários com ferramentas para maior produtividade, ao mesmo tempo que elimina os riscos da shadow AI. O próximo passo é possibilitar a inovação com segurança. Sua liderança na adoção segura da IA posicionará a TI como um facilitador da transformação, ajudando sua organização a prosperar nesta nova era, mantendo os dados seguros e em conformidade.

Comece a usar 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 já chegou. Agora vem a parte difícil". Relatório Anual do Índice de Tendências de 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 consertará o trabalho?" Relatório anual do Índice de Tendência de 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 sobre a proteção das pessoas naturais no que diz respeito ao processamento de dados pessoais e à livre circulação desses dados, e revogação da Diretiva 95/46/EC (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