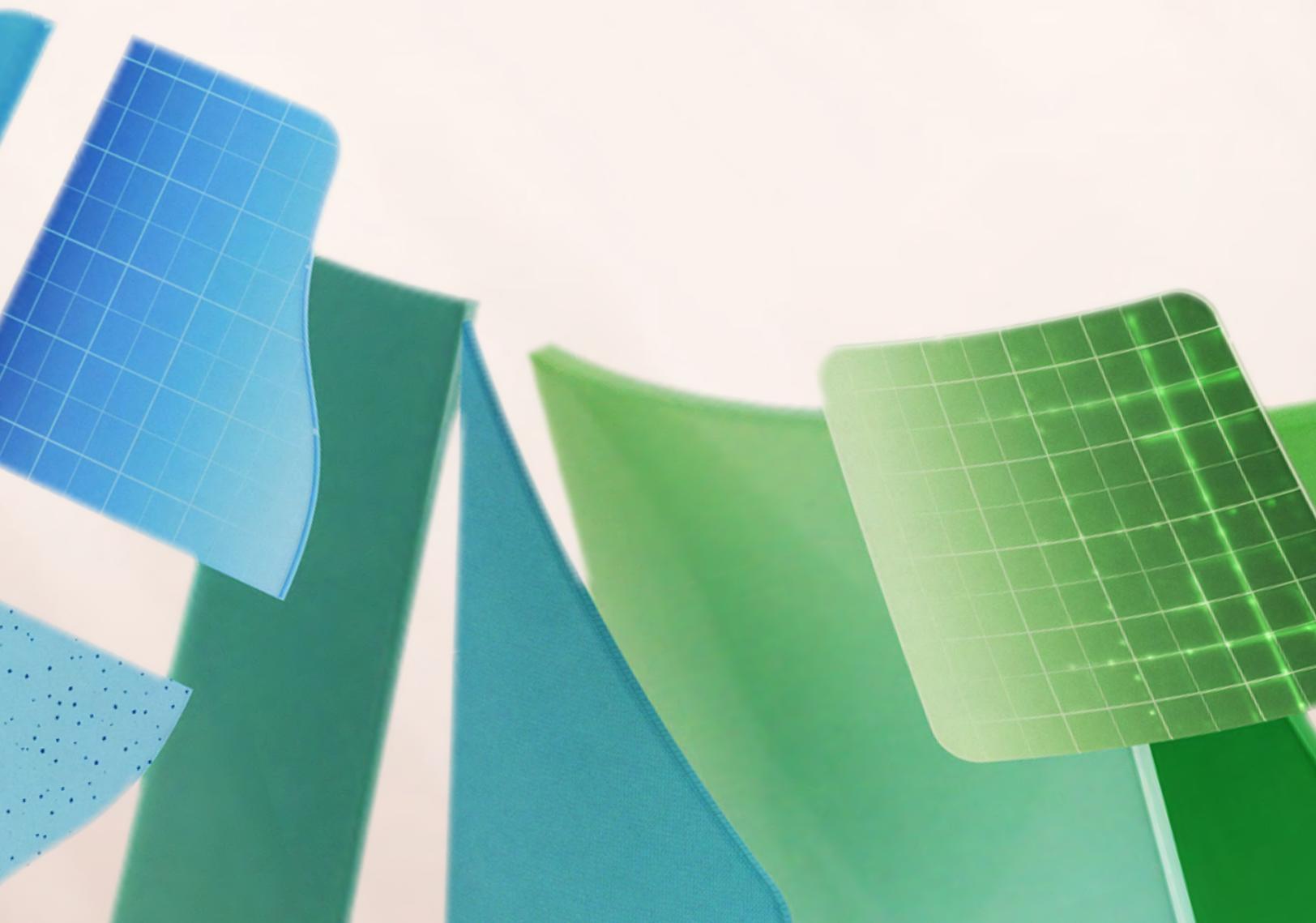


# Dados sob controlo

Dominar a governação de dados  
para o sucesso da IA



# Índice



## Introdução

# A governação de dados é o pilar da adoção segura de IA

A IA generativa é uma promessa de transformação empresarial, mas para concretizar esse potencial, é necessário garantir a qualidade e a disponibilidade dos seus dados empresariais.

As organizações que dão prioridade a uma boa governação de dados estão mais bem posicionadas para obter uma vantagem competitiva com a IA. A governação de dados ajuda a garantir que os dados consultados e gerados pela IA são corretos, seguros, controlados e compatíveis.

**Qualidade e disponibilidade dos dados:** os sistemas de IA baseiam-se em grandes conjuntos de dados de alta qualidade para oferecer a melhor resposta possível com o contexto adequado a partir dos workflows exclusivos da sua organização. Uma melhor qualidade dos dados permite obter insights e previsões de IA mais eficazes.

**Conformidade:** uma governação de dados sólida garante o cumprimento dos requisitos regulamentares, reduzindo o risco de problemas legais e multas.

**Segurança:** a etiquetagem e a gestão adequadas dos dados protegem as informações confidenciais contra o acesso não autorizado, a partilha indevida e as falhas de segurança.

**Confiança:** a governação fiável dos dados reforça a confiança dos intervenientes nos resultados da IA, promovendo uma maior adoção e apoio às iniciativas de IA.

Este e-book apresenta práticas fundamentais de governação de dados que preparam uma organização para a IA. Explica como estabelecer boas normas de qualidade de dados, garantir a conformidade com os requisitos regulamentares e implementar medidas de segurança e proteção de dados. Quer se trate de impedir que o conteúdo confidencial de uma reunião seja partilhado externamente ou de se proteger contra falhas de segurança de dados, aprenderá estratégias para fomentar a confiança nos sistemas de IA e tornar os dados facilmente acessíveis para obter insights acionáveis. Ao adotar essas práticas, a sua organização poderá tirar partido de todo o potencial da IA para promover a inovação contínua e criar uma vantagem competitiva.

## Casos de utilização de IA generativa

**Acelerar a comunicação:** elabore conteúdo personalizado mais rapidamente, para ter mais tempo para desenvolver relações e colaborar.

**Aumentar a eficiência:** reduza o tempo gasto em tarefas de rotina, aumente a produtividade e reduza os custos.

**Facilitar a inovação:** ajude a gerar ideias e propostas para novos produtos e serviços.

**Personalizar as experiências dos clientes:** adapte o conteúdo e as recomendações para promover a fidelização e o envolvimento.

# 1

# Reforçar a governação de dados para a transformação da IA

**Todas as empresas têm políticas e processos que regem a utilização de dados. As estruturas de governação de dados variam em termos de maturidade e abrangência, mas poucas foram totalmente otimizadas para a IA. Apesar de muitas das melhores práticas de governação de dados permanecerem as mesmas, como garantir a precisão e a consistência dos dados, há outros aspetos que precisam de ser atualizados para maximizar os investimentos em IA. Vejamos algumas áreas-chave.**

## Visibilidade dos dados

O conhecimento detalhado do fluxo de dados nos sistemas de IA permite encontrar e reduzir a utilização não autorizada ou inadequada. Esta visibilidade ajuda a dar suporte à segurança e à conformidade, protegendo os dados confidenciais para maximizar o valor da IA.

A governação de dados tradicional tem se centrado na identificação do local onde os dados residem e no controlo do acesso. No entanto, com a crescente integração da IA nas operações empresariais, a governação de dados tem de acompanhar a evolução das necessidades de segurança. Por exemplo, com o lançamento de um produto altamente

sensível, a governação tem agora de abarcar a gestão do conteúdo gerado pela IA, garantindo que os documentos relacionados com o projeto, as comunicações e os insights produzidos pela IA são seguros. Isso significa implementar medidas de segurança para que apenas os membros autorizados da equipa possam aceder à IA e utilizá-la para analisar ou resumir as informações do projeto.

Além disso, ao gerir os volumes de processamento e armazenamento de dados, as organizações podem controlar melhor os custos operacionais associados à IA.

## Qualidade dos dados

A IA acentua a importância de a qualidade dos dados ser elevada, uma vez que uma má qualidade dos dados afeta diretamente os resultados da IA. Ao aplicar ferramentas de IA para consultar os dados da sua empresa, convém ter a certeza de que os dados são atuais e fiáveis. Igualmente importante é compreender a proveniência e a qualidade dos dados que as suas equipas utilizam para criar os seus próprios modelos e aplicações de IA. As auditorias regulares aos dados, os processos de validação rigorosos e uma gestão proativa ajudam a garantir a integridade dos dados. Ao centrarem-se nestas áreas, as organizações podem obter resultados fiáveis da IA que melhoram a tomada de decisões e estimulam a inovação.

## Gestão de utilizadores

Com a IA, os utilizadores interagem com os dados de maneiras sofisticadas. Comunicam com os sistemas de IA, como o Microsoft 365 Copilot, através de pedidos em linguagem natural. Com a permissão e as proteções implementadas, a IA pode aceder ao contexto relevante dos dados, como ficheiros, chats e e-mails, juntamente com fontes externas através de plug-ins para gerar uma resposta.

É crucial monitorizar os dados utilizados nestes processos para garantir que a IA fornece respostas corretas e fundamentadas. Proporcionar transparência através de notas de rodapé ou ligações às fontes originais ajuda os utilizadores a verificar as informações, reduzindo o risco de utilização indevida dos dados e garantindo a conformidade com os regulamentos.

## Conformidade e Deteção de Dados Eletrónicos

A ascensão da IA traz consigo novos desafios em matéria de conformidade e Deteção de Dados Eletrónicos (ou seja, o tratamento de dados para casos jurídicos), nomeadamente em termos de gestão de dados gerados pela IA e de adaptação à evolução dos requisitos legais. A atualização das estruturas de governação de dados para enfrentar estes desafios envolve o desenvolvimento de políticas que abranjam o conteúdo gerado por IA, como garantir a monitorização, a categorização e o armazenamento seguro de comunicações ou documentos produzidos pela IA. Por exemplo, pode ser necessário atualizar as políticas para garantir que os e-mails ou relatórios gerados por IA são etiquetados e arquivados corretamente para obtenção futura.

A melhoria das capacidades de Deteção de Dados Eletrónicos incluiria a integração de ferramentas de IA capazes de pesquisar e identificar conteúdo gerado por IA em várias plataformas. Por exemplo, durante uma consulta de carácter jurídico, as ferramentas de Deteção de Dados Eletrónicos devem ser capazes de localizar e obter documentos específicos gerados por IA, resumir comunicações relevantes e fornecer registos de auditoria claros para provar a conformidade. Ao atualizar estas capacidades, as organizações podem melhorar a gestão dos dados no decorrer de auditorias ou investigações legais, garantindo que todas as informações relevantes geradas por IA podem ser acedidas e defendidas em tribunal.

## Segurança de dados

A proteção das operações orientadas por IA deve envolver princípios de Confiança Zero ao nível da identidade, o que minimiza o risco de acesso não autorizado. As atualizações regulares dos endpoints, incluindo dispositivos e aplicações, reduzem as vulnerabilidades que podem ser exploradas. Um bom conhecimento das ferramentas de IA generativa utilizadas na organização permite bloquear aplicações não autorizadas ou inseguras, evitando assim potenciais falhas de segurança. Ao limitar o acesso aos dados e às ferramentas de IA apenas a elementos de confiança, as organizações podem alcançar uma maior integridade dos dados e proteger as suas operações de IA contra potenciais ameaças.



## O que é a Confiança Zero?

A Confiança Zero é um modelo de segurança centrado na verificação de cada pedido como se fosse proveniente de uma rede não fidedigna. Em vez de partir do princípio de que tudo o que está dentro da firewall da empresa é seguro, esta abordagem adota o princípio "nunca confiar, verificar sempre".

## Princípios de Confiança Zero

**Verificar explicitamente:** autenticar e autorizar sempre com base em todos os pontos de dados disponíveis.

**Utilizar o acesso com privilégios mínimos:** limite o acesso dos utilizadores com acessos do tipo Just-In-Time e Just-Enough-Access (JIT/JEA), políticas adaptáveis baseadas no risco e proteção de dados.

**Antecipar as falhas de segurança:** limite os danos, controle o acesso, garanta a encriptação e utilize dados para detetar ameaças e reforçar as defesas.

## 2

# O papel da administração de dados na transformação da IA: origens, qualidade e fiabilidade

**À medida que as organizações adotam a IA para ajudar nas decisões empresariais, têm de garantir que estes sistemas podem fornecer resultados corretos e fiáveis. Os dados que fundamentam as respostas de IA devem estar disponíveis, ser consistentes e estar bem documentados.**

A administração de dados suporta uma IA fiável através da implementação de políticas de governação que monitorizam a origem dos dados, verificam a sua qualidade e asseguram a sua fiabilidade e precisão. Estas práticas criam as bases para sistemas de IA que fornecem insights fiáveis, permitindo tomar decisões fundamentadas com confiança.

## Linhagem de dados: compreender as origens e as alterações das informações

A linhagem de dados acompanha o percurso dos dados dentro de uma organização. Documenta as origens, as transformações e os destinos dos dados. Para as empresas com tecnologia de IA, compreender a linhagem de dados é vital por várias razões:

- **Transparência:** saber qual é a proveniência dos dados e como mudam ajuda a confirmar a precisão dos resultados gerados pela IA e garante a conformidade regulamentar, proporcionando uma compreensão clara do histórico dos dados.
- **Rastreabilidade:** a linhagem de dados permite às organizações localizar os erros ou as inconsistências até à sua origem, simplificando a resolução de problemas e a correção de dados.
- **Análise do impacto:** compreender a forma como os dados são utilizados pelas ferramentas de IA generativa ajuda a avaliar o potencial impacto das alterações nas origens de dados ou nos métodos de processamento em termos de precisão da saída e resultados empresariais.

## Qualidade dos dados: a qualidade está na base do valor das respostas de IA

A qualidade dos dados afeta diretamente a fiabilidade das saídas de IA. Os dados de alta qualidade fornecem o contexto para os modelos de IA darem respostas corretas e valiosas às entradas dos utilizadores. Os principais aspetos da qualidade dos dados incluem:

- **Precisão:** os dados devem representar corretamente as condições reais.
- **Integralidade:** todos os dados necessários devem estar presentes e ser tidos em conta.
- **Consistência:** os dados devem ser consistentes nos diferentes sistemas e ao longo do tempo.
- **Oportunidade:** os dados devem estar atualizados e disponíveis quando necessário.

## Fiabilidade dos dados: garantir dados fiáveis

Dados fiáveis são aqueles que cumprem sistematicamente os padrões de qualidade e estão disponíveis quando necessário. Para as empresas com tecnologia de IA, os dados fiáveis são cruciais para promover a confiança nas ferramentas de IA e nas decisões que estes fundamentam. Garantir a fiabilidade dos dados envolve:

- **Redundância de dados:** implementar sistemas de cópia de segurança que evitam perdas e aumentam a disponibilidade.
- **Cópias de segurança regulares:** realizar cópias de segurança frequentes para se proteger contra a perda de dados ou danos em dados.
- **Monitorização e alertas:** configurar sistemas de monitorização para detetar e alertar os intervenientes para problemas de dados em tempo real.
- **Planos de recuperação após desastre:** desenvolver e testar planos para recuperar os dados e retomar rapidamente as operações após interrupções.

# 3

## A relação entre governação, segurança e IA responsável

**Em conjunto, a governação e a segurança de dados constituem o pilar da utilização responsável da IA. Os dados seguros e de alta qualidade garantem que a IA funciona de forma ética e eficaz. As principais áreas a serem avaliadas incluem a classificação de dados, os controlos de acesso, a encriptação, a resposta a incidentes e a conformidade regulamentar.**

### Classificação de dados

A classificação de dados é uma parte fundamental para controlar a forma como as ferramentas de IA processam as informações confidenciais. Normalmente, os dados e as reuniões são classificados como gerais, confidenciais ou altamente confidenciais. A classificação adequada garante que a IA só acede às informações adequadas, reduzindo o risco de expor dados confidenciais a utilizadores não autorizados.

Por sua vez, a classificação incorreta pode levar ao processamento de dados de IA que devem ser restritos, o que pode originar falhas de segurança ou problemas de conformidade. Uma governação de dados eficaz, seja através de ferramentas automatizadas ou de políticas de utilizador final, garante a classificação correta dos dados, protegendo as informações confidenciais e suportando a capacidade de a IA fornecer resultados fiáveis e compatíveis.

### Controlos de acesso

Estes controlos regulam quem pode aceder aos dados relevantes para a IA e quais são as aplicações ou identidades que têm permissão para interagir com esses dados. Controlos de acesso fracos podem levar à exposição não autorizada de informações confidenciais, aumentando o risco de falhas de segurança e utilização indevida.

A governação de dados desempenha um papel fundamental na imposição destes controlos, restringindo o acesso aos dados a pessoal autorizado e aplicações específicas, garantindo que os dados confidenciais são processados adequadamente. Isso não só protege a integridade dos dados, como também garante que os sistemas de IA operam em conjuntos de dados seguros e fiáveis, aumentando a sua fiabilidade e conformidade.

## Encriptação

Proteger os dados contra a intercetção e adulteração através da encriptação ajuda a garantir que essas ferramentas de IA generativa podem fundamentar as suas respostas no contexto correto, como dados relacionados com o trabalho, ficheiros, chats e e-mails, sem correr o risco de fuga de dados.

As políticas de governação de dados podem exigir práticas robustas de encriptação, protegendo os dados ao longo de todo o ciclo de vida. Esta abordagem garante que as ferramentas de IA podem fornecer respostas fiáveis, mantendo os seus dados seguros e preservando a confiança.

## Resposta a incidentes

Os dados organizacionais confidenciais podem ser expostos através de incidentes envolvendo ferramentas de IA generativa que concedem acesso não autorizado a ficheiros, e-mails ou outros dados empresariais que os sistemas utilizam para gerar respostas.

Um plano proativo de resposta a incidentes é crucial nesses cenários. Sem esse plano, a organização corre o risco não só de expor dados confidenciais, mas também de confiar em resultados comprometidos da IA. A governação de dados inclui ter protocolos de resposta detalhados para lidar rapidamente com falhas de segurança, minimizando o seu impacto e preservando a fiabilidade dos sistemas de IA.

## Conformidade regulamentar

As aplicações de IA devem cumprir as regulamentações, como o RGPD ou o CCPA, que regem a proteção de dados e a privacidade. O incumprimento pode conduzir a penalizações avultadas e minar a confiança. Também é crucial compreender onde as ferramentas de IA processam os dados, já que muitas ferramentas gratuitas podem tratar os dados globalmente ou fora das localizações de armazenamento habituais da sua empresa. A governação de dados garante que as aplicações de IA não só funcionam dentro dos quadros legais, como também mantêm os dados dentro dos limites de serviço corretos, alinhando-se com as normas de conformidade da sua organização. Esta abordagem apoia a utilização ética da IA e ajuda a promover a confiança na tecnologia de IA.



# 4

## Atualizar a sua estrutura de governação de dados para apoiar a adoção da IA

No cenário da IA em evolução, é importante identificar áreas específicas da sua estrutura de governação de dados existente que podem exigir maior atenção. Em vez de reformular toda a estrutura, pode concentrar-se nas áreas com maior probabilidade de evoluir, direcionando os seus esforços para onde irão aumentar mais o valor da IA, garantindo que os seus dados permanecem protegidos e seguros. Seguem-se alguns insights importantes a considerar:

### Adaptação de políticas e procedimentos

A IA envolve novos tipos de recolha, processamento e utilização de dados. A atualização das políticas de dados pode ajudar a dar resposta a necessidades relevantes em termos de privacidade de dados, conformidade regulamentar e utilização ética. Por exemplo, exigir a anonimização de dados em instâncias específicas pode proteger as informações pessoais, tornando a sua utilização mais segura ao longo do ciclo de vida completo da IA.

### Funções e responsabilidades

É essencial incorporar a prontidão para a IA em todas as funções envolvidas com a governação de dados. Os colaboradores familiarizados com os requisitos dos dados de IA podem agir como administradores para dar suporte à qualidade e conformidade dos dados. A colaboração multifuncional entre as equipas jurídica, de TI e de ciência de dados pode ajudar a enfrentar os desafios específicos da IA de forma mais eficaz.

## Adaptação das normas e definições de dados

A uniformização dos formatos de dados, das definições e das métricas de qualidade simplifica a implementação de políticas que regem a utilização de ferramentas de IA dentro de uma organização. A existência de normas de dados explícitas facilita a decisão relativamente aos conjuntos de dados que as ferramentas de IA podem analisar para fornecer contexto empresarial, bem como aos dados que os utilizadores podem carregar para análise. Isto garante que as aplicações de IA utilizam os dados mais relevantes e fiáveis, melhorando a sua eficácia e apoiando a conformidade com as políticas organizacionais.

## Melhoria contínua

A governação de dados é um processo contínuo, especialmente no que se refere à IA. A realização de auditorias e atualizações regulares à sua estrutura de governação pode ajudar a adaptá-la a novos desenvolvimentos de IA e alterações regulamentares. A IA em si pode ser utilizada para verificar e melhorar as práticas de governação, o que pode levar à deteção de lacunas e sugestão de melhorias. Esta abordagem proativa aumenta a conformidade e a eficiência à medida que as tecnologias de IA evoluem.

## Ferramentas e técnicas para uma governação de dados eficaz

### **Alinhar-se com os objetivos**

**empresariais:** certifique-se de que a sua estratégia de governação de dados apoia os objetivos organizacionais para melhorar a tomada de decisões e a eficiência.

**Automatizar as tarefas de rotina:** utilize a automatização para as tarefas repetitivas, como a classificação de dados e a gestão do acesso, para reduzir os erros manuais e melhorar a segurança.

### **Garantir elevados padrões de precisão:**

use ferramentas de validação e limpeza para oferecer suporte à integridade dos dados ao longo do tempo.

**Formar os utilizadores:** ofereça formação em matéria de ferramentas e procedimentos de governação de dados para prevenir a má gestão e garantir o cumprimento das políticas.

**Realizar auditorias regulares:** reveja as práticas de dados com regularidade para garantir que estão a acompanhar as alterações regulamentares e organizacionais.

## Conclusão

# Governança de dados eficaz para a capacitação de IA com o Microsoft 365

Utilizar a IA de forma responsável requer uma governança de dados sólida. Uma governança de dados eficaz garante a disponibilidade, a precisão e a segurança dos dados, o que permite à IA fornecer insights fiáveis e promover a inovação. Dar prioridade à qualidade, conformidade e segurança dos dados melhora as capacidades de IA, impulsionando uma melhor tomada de decisões e mantendo uma vantagem competitiva.

## Microsoft 365: Capacitar a preparação para a IA

O Microsoft 365 oferece as melhores aplicações de produtividade da sua categoria com ferramentas incorporadas para a classificação, o controlo e a proteção de dados. Estas funcionalidades dão suporte à sua estrutura de governança de dados, facilitando uma adoção confiante da IA quando tiver tudo preparado. O Microsoft 365 ajuda a garantir aspetos como:

- **Qualidade dos dados:** dê suporte à precisão e fiabilidade dos resultados da IA.
- **Conformidade:** cumpra os requisitos regulamentares, reduzindo os riscos legais.
- **Segurança dos princípios da Confiança Zero:** proteja as informações confidenciais contra o acesso não autorizado, as falhas de segurança e as ciberameaças

**Descubra ferramentas de produtividade abrangentes melhoradas com opções de IA e proteção robusta para ajudar a sua organização a trabalhar de forma eficiente e segura.**



**Explorar o Microsoft 365**