

# Microsoft 365 Fundamentals

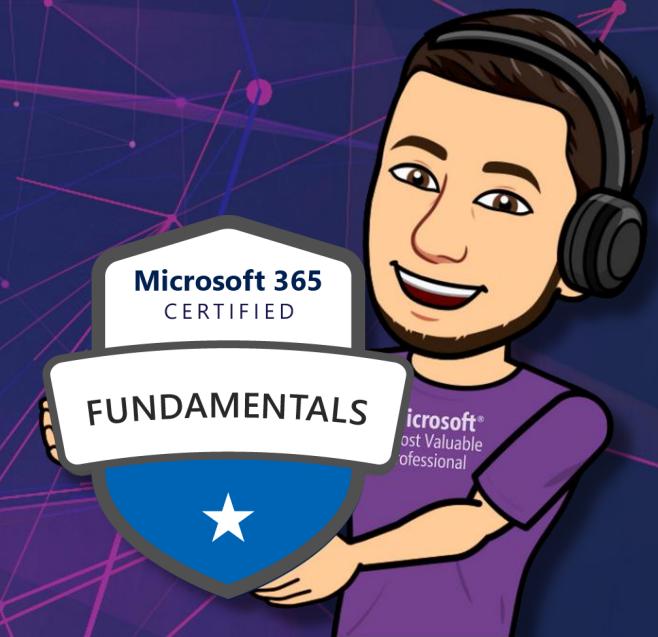


# Módulo 03

- Descrever conceitos de segurança e conformidade
- Descrever os conceitos de identidade
- Descrever a proteção contra ameaças com o Microsoft 365 Defender
- Descrever o Portal de Confiança do Serviço e a privacidade com a Microsoft



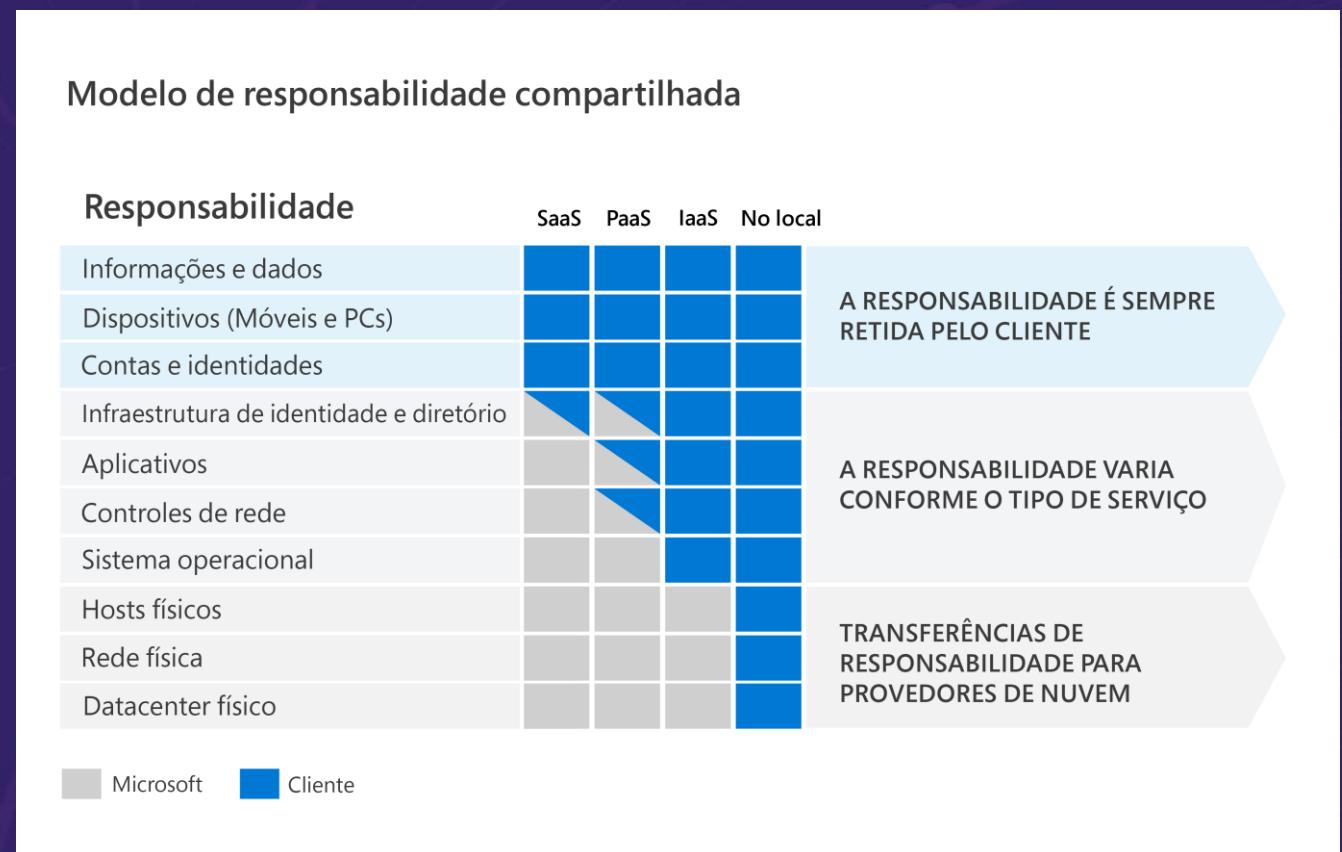
# Descrever conceitos de segurança e conformidade?

#partiu  
nuvem

# Descrever o modelo de responsabilidade compartilhada

**As responsabilidades variam dependendo de onde a carga de trabalho está hospedada:**

- SaaS (software como serviço)
- PaaS (plataforma como serviço)
- IaaS (infraestrutura como serviço)
- Datacenter local.



# Descrever a defesa em profundidade

- A defesa em profundidade usa uma abordagem em camadas de segurança, em vez de depender de um único perímetro.
- Uma estratégia de defesa em profundidade usa uma série de mecanismos para reduzir o avanço de um ataque.
- Cada camada fornece proteção para que, se uma camada for violada, uma camada subsequente impedirá que um invasor receba acesso não autorizado aos dados.



# Descrever a defesa em profundidade

**Conceito de CIA (Confidencialidade, Integridade, Disponibilidade):**

- **Confidencialidade** se refere à necessidade de manter dados confidenciais em segredo
- **Integridade** se refere a manter dados ou mensagens corretas
- **Disponibilidade** se refere a tornar os dados disponíveis para aqueles que precisam deles, quando precisam.



# Explorar o modelo de Confiança Zero

## Princípios de orientação de confiança zero

O modelo de confiança zero tem três princípios que orientam e sustentam como a segurança deve ser implementada. São eles: verificação explícita, acesso com privilégio mínimo e pressuposição de violação.

**Verificação explícita:** Sempre autentique e autorize com base nos pontos de dados disponíveis, incluindo a identidade do usuário, o local, o dispositivo, o serviço ou a carga de trabalho, a classificação de dados e as anomalias.

**Acesso com privilégio mínimo:** Limite o acesso do usuário com acesso just-in-time e just-enough (JIT/JEA), políticas adaptáveis baseadas em risco e proteção de dados para proteger os dados e a produtividade.

**Pressuposição de violação:** Segmento de acesso por rede, usuário, dispositivos e aplicativo. Use a criptografia para proteger dados e use a análise para obter visibilidade, detectar ameaças e melhorar sua segurança.

# Explorar o modelo de Confiança Zero

No modelo de confiança zero, todos os elementos funcionam em conjunto para fornecer segurança de ponta a ponta.

Esses seis elementos são os pilares fundamentais do modelo de confiança zero:

- Identidades
- Dispositivos
- Aplicativos
- Dados
- Infraestrutura
- Redes

[Video Zero Trust](#)



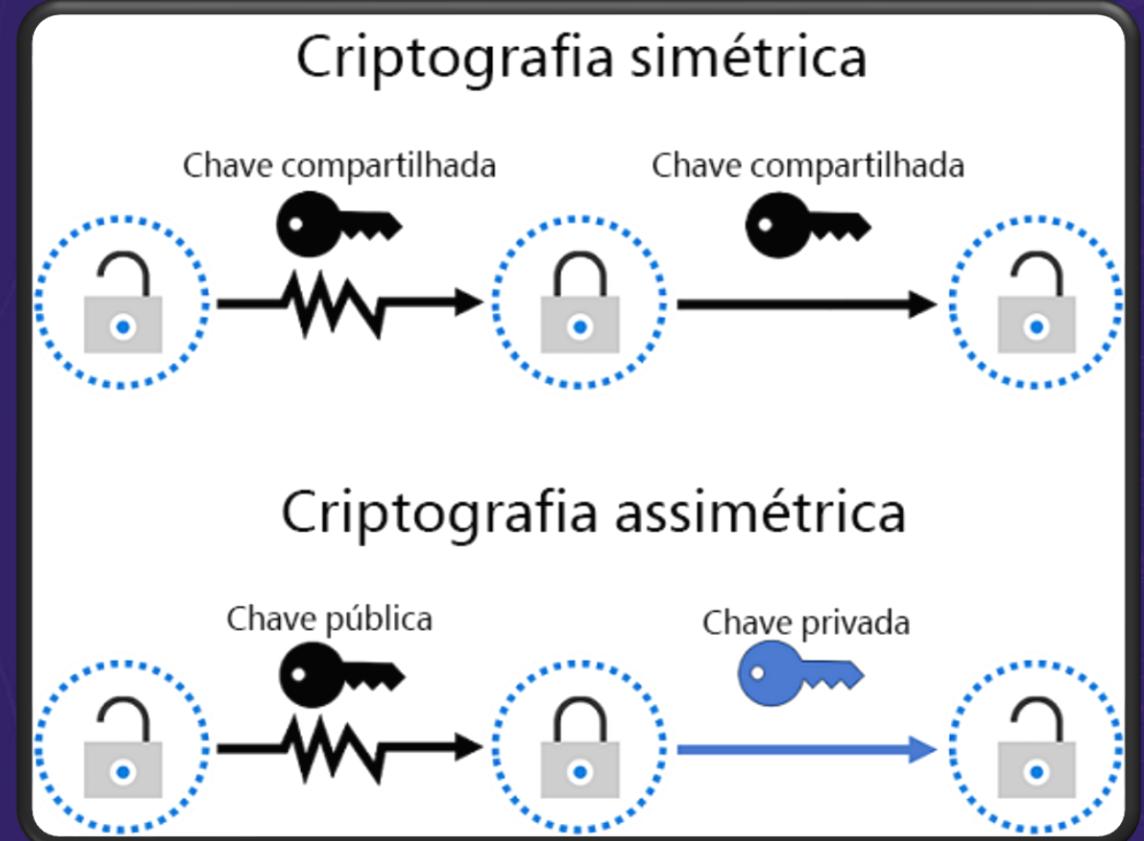
# Descrever criptografia e hash

**Criptografia é o processo de tornar dados ilegíveis e inutilizáveis para visualizadores não autorizados.**

**Há dois tipos de níveis superiores de criptografia:**

- Simétrica – usa a mesma chave para criptografar e descriptografar os dados
- Assimétrica – usa um par de chaves pública e privada.

**A criptografia pode proteger dados inativos, em uso ou em trânsito.**



# Descrever criptografia e hash

- O hash usa um algoritmo para converter texto em um valor exclusivo de comprimento fixo chamado hash.
- O hash não usa chaves e o valor com hash não é descriptografado posteriormente para o original.
- O hash é usado para armazenar senhas.





# OBRIGADO

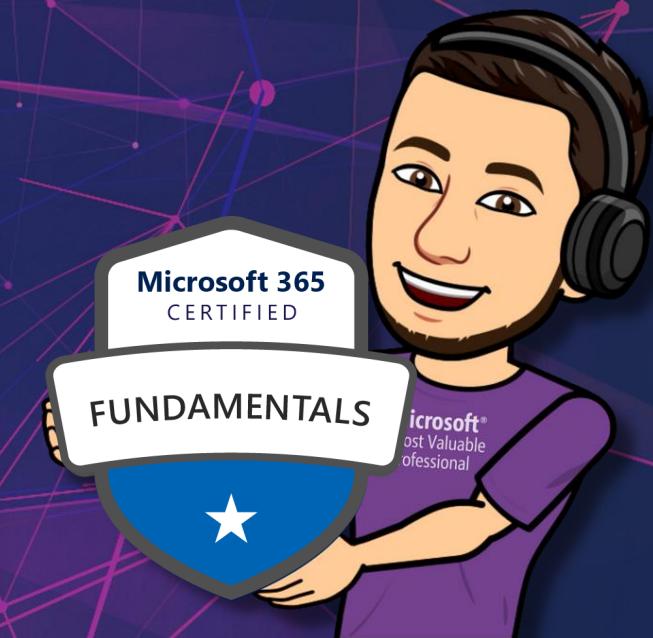
---

#partiu  
nuvem



# Descrever os conceitos de identidade

#partiu  
nuvem





# Definir autenticação e autorização

## Autenticação

- É o processo de provar que uma pessoa é quem ela afirma ser.
- Às vezes, a autenticação é abreviada para AuthN.

## Autorização

- Após autenticar um usuário, você precisará decidir onde ele pode ir e o que ele tem permissão para ver e tocar. Esse processo é chamado de autorização.
- Em termos de segurança cibernética, a autorização determina o nível de acesso ou as permissões que uma pessoa autenticada tem aos seus dados e recursos.
- Às vezes, a autorização é abreviada para AuthZ.

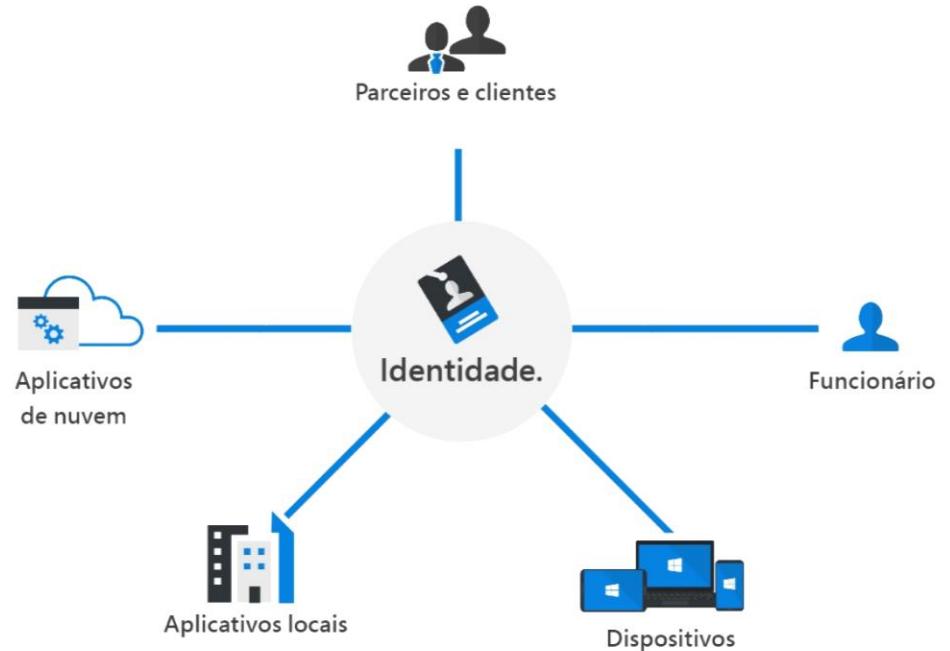
# Definir a Identidade como o perímetro de segurança primário

**Uma identidade pode ser associada a um usuário, um aplicativo, um dispositivo ou outra coisa.**

**Quatro pilares de uma infraestrutura de identidade:**

- Administração
- Autenticação
- Autorização
- Auditoria

A identidade é o novo perímetro de segurança



# Descrever a função do provedor de identidade

## A função do provedor de identidade

- Autenticação moderna é um termo abrangente que se refere aos métodos de autenticação e autorização entre um cliente e um servidor.
- Com a autenticação moderna, todos os serviços, incluindo todos os serviços de autenticação, são fornecidos por um provedor de identidade central.
- Com um provedor de identidade central, as organizações podem estabelecer políticas de autenticação e autorização, monitorar o comportamento do usuário, identificar atividades suspeitas e reduzir ataques mal-intencionados.

## Logon único

- O suporte para SSO (logon único) é outro recurso essencial de um provedor de identidade e "autenticação moderna"
- Com o SSO, o usuário faz logon uma vez e essa credencial é usada para acessar vários aplicativos ou recursos.
- Quando você configura o SSO para trabalhar entre vários provedores de identidade, isso é chamado de federação

[Video Autorização - Autenticação](#)

# Descrever o conceito de serviços de diretório e Active Directory



Um serviço de diretório armazena dados de diretório e os disponibiliza para os usuários de rede, administradores, serviços e aplicativos.



AD (Active Directory) é um conjunto de serviços de diretório desenvolvido pela Microsoft como parte do Windows 2000 para redes locais baseadas em domínio.



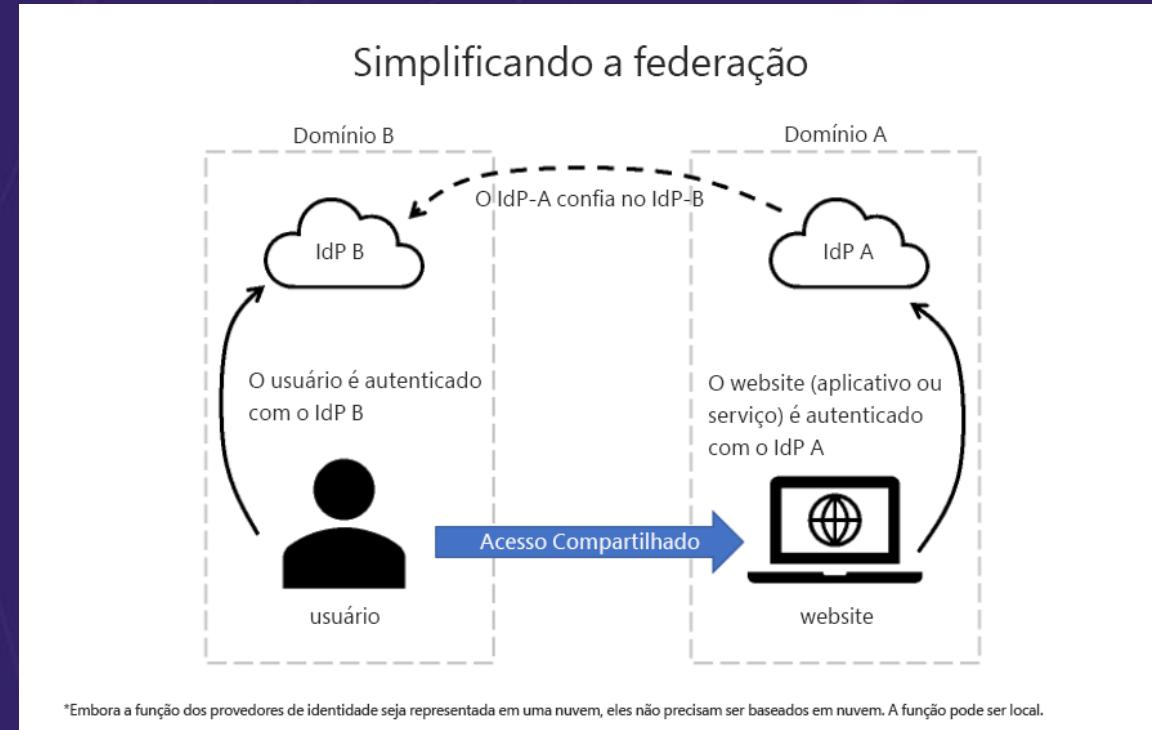
O AD DS (Active Directory Domain Services) armazena informações sobre os membros do domínio, incluindo dispositivos e usuários, verifica as credenciais e define os direitos de acesso.



O Azure Active Directory é a próxima evolução das soluções de gerenciamento de identidade e acesso. Ele fornece às organizações uma solução de IDaaS (identidade como serviço) para todos os aplicativos na nuvem e no local.

# Descrever o conceito de federação

- A federação permite o acesso de serviços através dos limites da organização ou do domínio, estabelecendo relações de confiança com o provedor de identidade do respectivo domínio.
- Com a federação, não é necessário que um usuário mantenha nome de usuário e senha diferentes ao acessar recursos em outros domínios.





# OBRIGADO

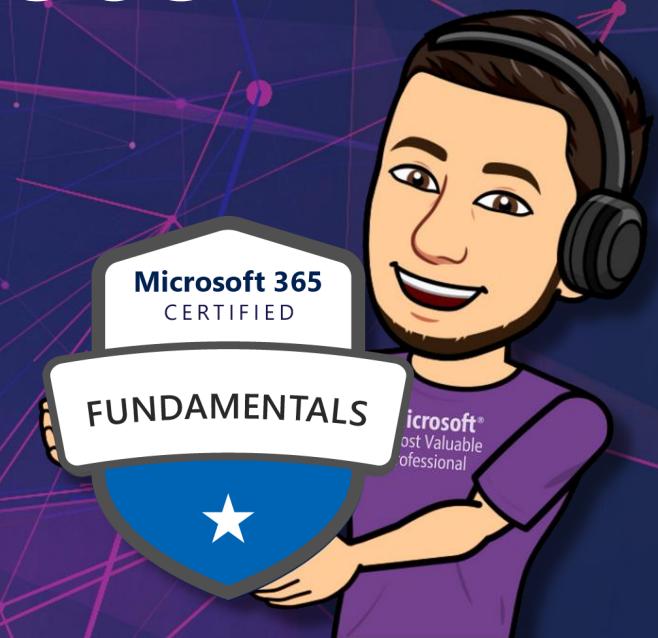
---

#partiu  
nuvem



# Descrever as soluções de colaboração no Microsoft 365

#partiu  
nuvem



# Cargas de trabalho de colaboração do Teams e o valor que elas fornecem

Estes são os muitos recursos e funcionalidades que vêm com o Teams.

Equipes e canais



Chat e mensagens instantâneas



Reuniões online



Telefonia do Microsoft Teams



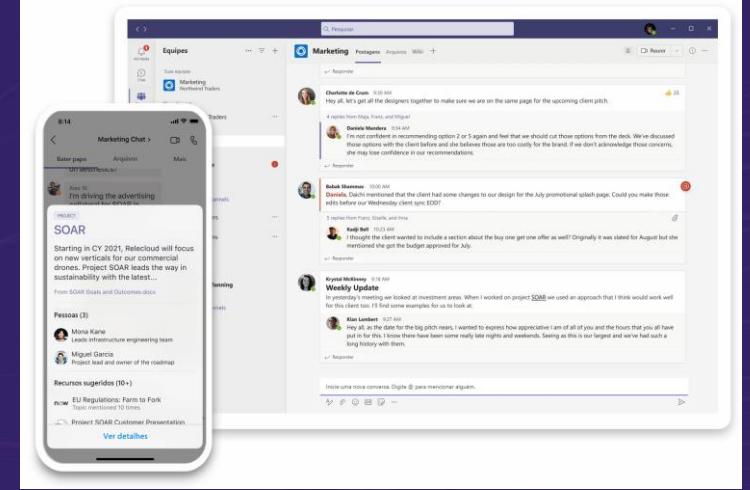
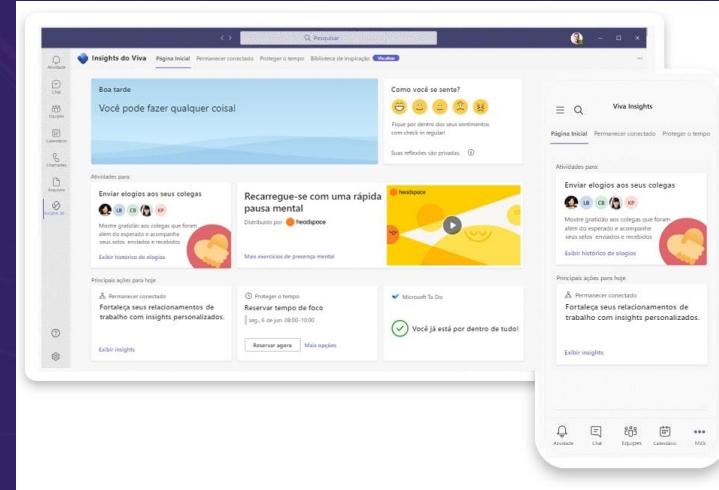
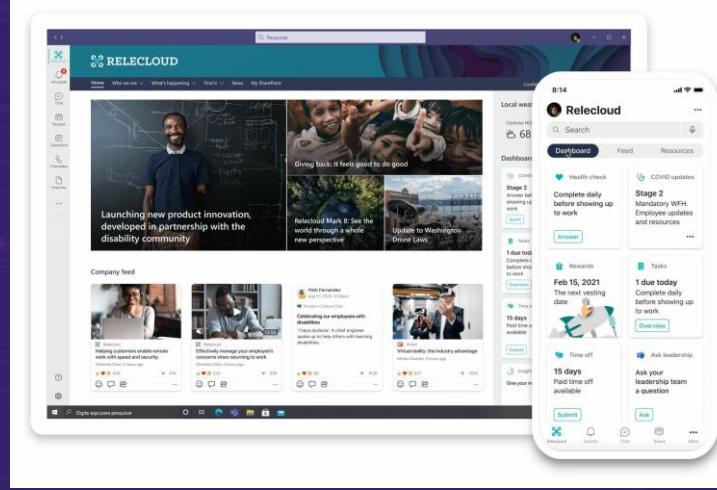
Estender o Teams usando aplicativos colaborativos



Segurança e conformidade



# Principais recursos de experiência do funcionário no Microsoft Viva



## Conexões do Viva

As Conexões do Viva foram criadas para manter todos na força de trabalho conectados uns aos outros. Os funcionários podem ter acesso fácil a ferramentas e recursos.

## Insights do Viva

Os Insights do Viva fornecem insights com proteção de privacidade e recomendações acionáveis que ajudam todos na organização a trabalhar de modo mais inteligente e alcançar o equilíbrio.

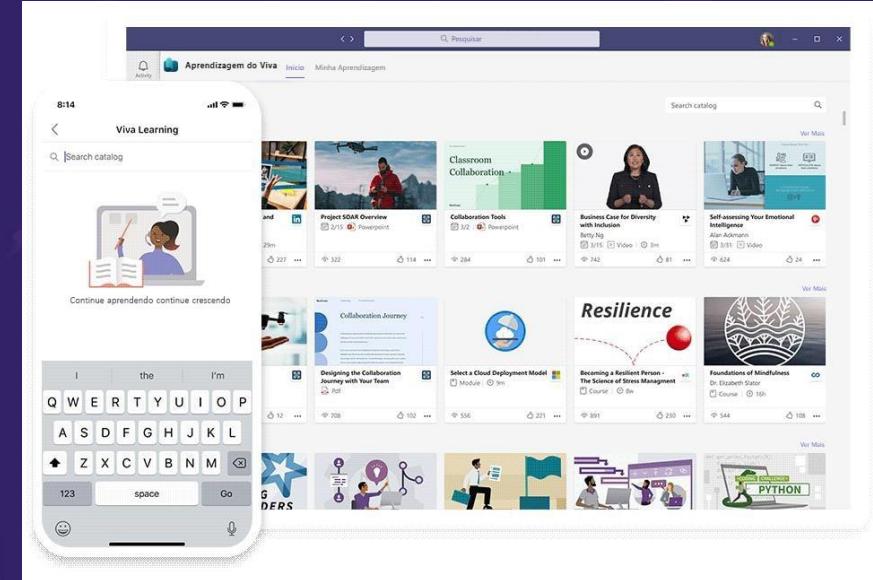
## Tópicos do Viva

Os Tópicos do Viva se concentram no conhecimento e na experiência. As informações são fornecidas aos funcionários por meio de páginas de tópicos.

# Principais recursos de experiência do funcionário no Microsoft Viva

## Aprendizagem do Viva:

A Aprendizagem do Viva é um hub de aprendizagem centralizado que permite integrar perfeitamente a aprendizagem e a criação de habilidades ao seu dia. Os funcionários podem descobrir, compartilhar, recomendar e aprender com bibliotecas de conteúdo.



# Recursos do SharePoint e do OneDrive promovem a colaboração

## SharePoint

- O SharePoint, a intranet inteligente, pode ajudar você a transformar as comunicações e as experiências digitais dos funcionários.
- O SharePoint fornece três tipos principais de sites:
  - Sites de equipe
  - Sites de comunicação
  - Sites do hub

## OneDrive

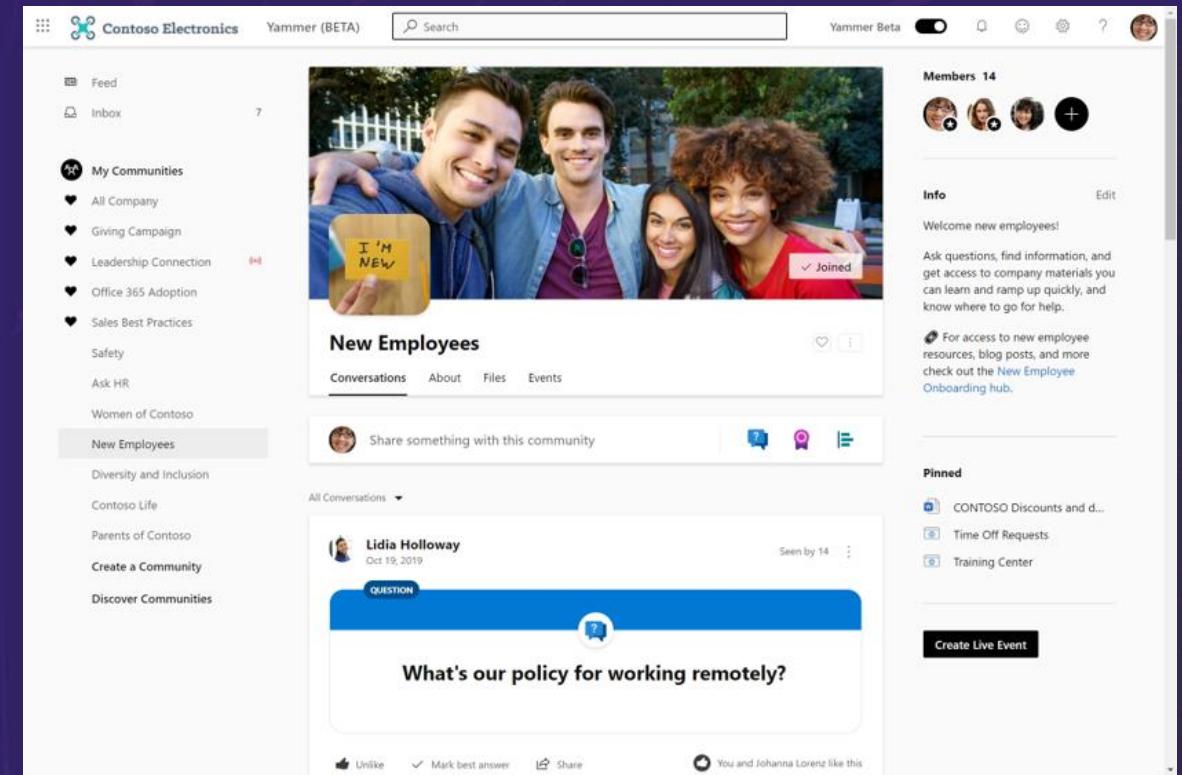
- A seguinte lista descreve como o OneDrive capacita você e sua equipe a colaborar em tempo real para entregar os resultados certos:
  - Acesse arquivos de todos seus dispositivos
  - Gerencie arquivos em qualquer lugar
  - Colaboração contínua com arquivos
  - Compartilhe dentro ou fora da sua organização
  - Encontre rapidamente os arquivos que mais importam
  - Proteja seus arquivos com segurança de nível empresarial

# Descrever como o Yammer ajuda comunidades a se conectarem e crescerem

**A seguinte lista descreve como o Yammer ajuda comunidades a se conectarem e crescerem:**

- Participação de líderes
- Modernização da comunicação dos funcionários
- Compartilhamento de conhecimento
- Envolvimento de seus funcionários
- Capacitação das comunidades no Microsoft 365

**À direita, há uma captura de tela mostrando a interface do Yammer.**





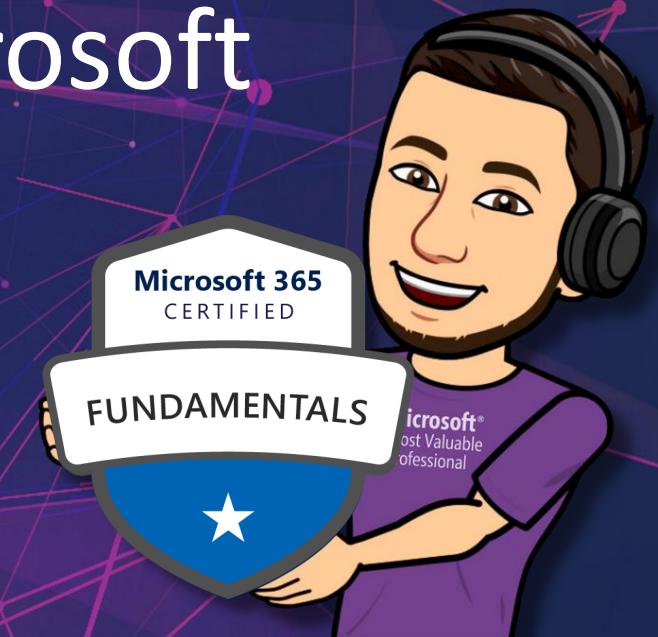
# OBRIGADO

---

#partiu  
nuvem



Descrever a modernização do ponto de extremidade (endpoint), os conceitos de gerenciamento e as opções de implantação no Microsoft 365



# Descrever os recursos de gerenciamento de endpoint do Microsoft 365



**O Microsoft Endpoint Manager inclui o seguinte serviço e funcionalidades:**

- Microsoft Intune
- Configuration Manager
- Cogerenciamento
- Análise de Área de Trabalho
- Windows Autopilot
- Azure Active Directory
- Centro de administração do Endpoint Manager

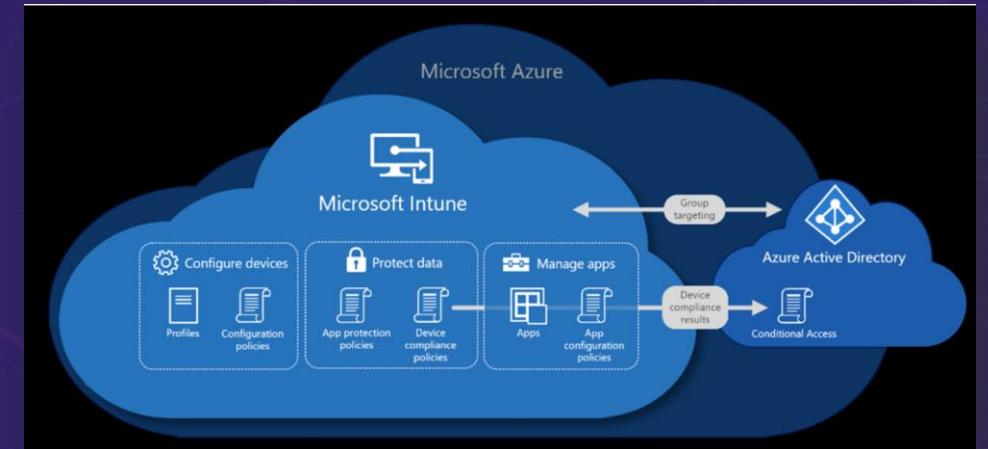
# Microsoft Intune

**Microsoft Intune é um provedor MDM e MAM para seus dispositivos**

O Microsoft Intune é um serviço baseado em nuvem que se concentra no gerenciamento de dispositivos móveis (MDM) e no gerenciamento de aplicativos móveis (MAM). O Intune é integrado como parte do Microsoft Endpoint Manager no Microsoft 365, e permite que os usuários sejam produtivos, mantendo os dados da sua organização protegidos.

Ele se integra a outros serviços, incluindo o Microsoft 365 e o Azure Active Directory (Azure AD) para controlar quem tem acesso e o que eles têm acesso e proteção de informações do Azure para proteção de dados.

Quando você usá-lo com o Microsoft 365, você pode permitir que sua força de trabalho seja produtiva em todos os seus dispositivos, mantendo as informações da sua organização protegidas.



# Cogerenciamento

O cogerenciamento permite que você dispositivos Windows 10/11 use o Configuration Manager e o Microsoft Intune simultaneamente.

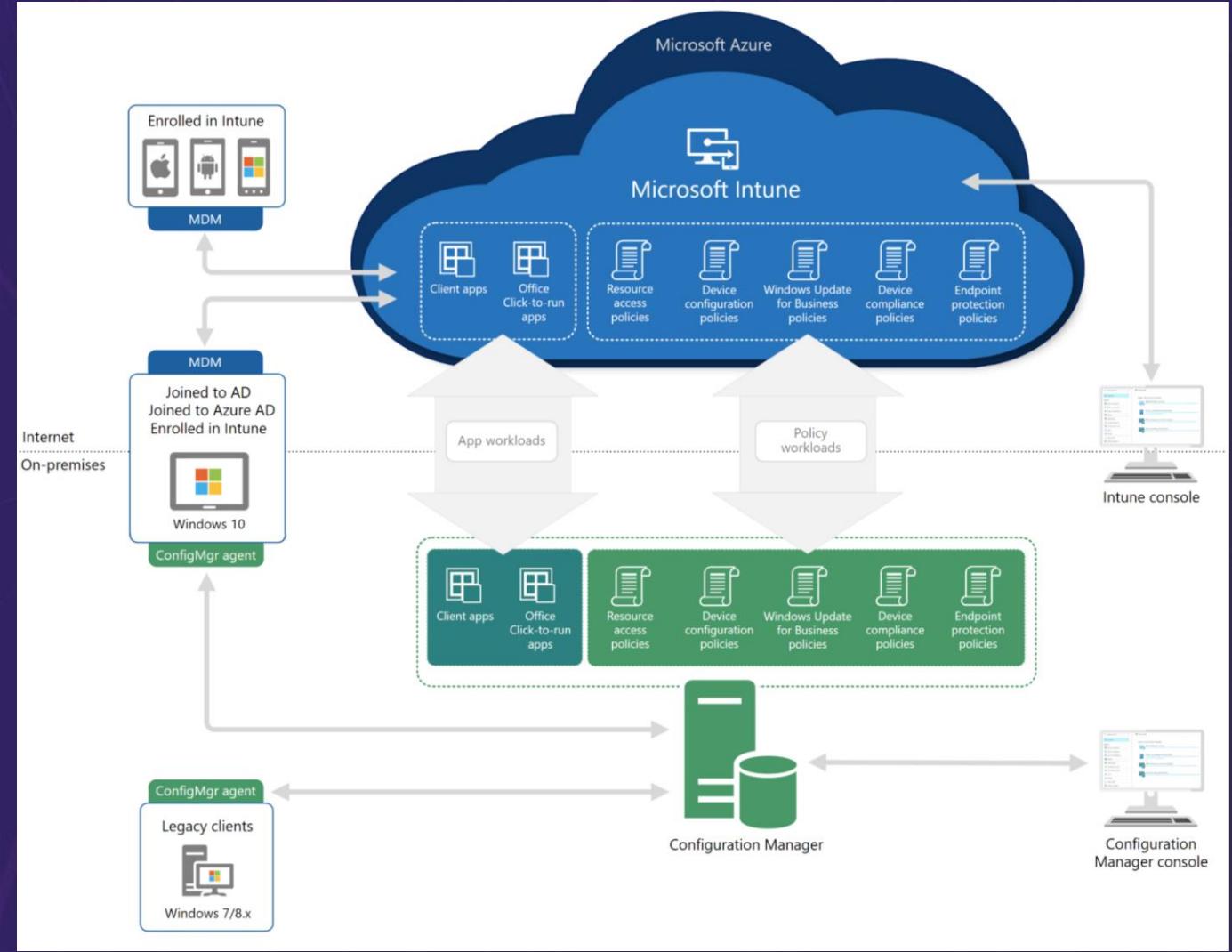
Existem dois caminhos principais para alcançar a cogestão:

## **Cientes existentes do Configuration Manager:**

Você tem dispositivos Windows 10/11 que já são clientes do Configuration Manager.

Você criou o Híbrid Azure AD e registra-os no Intune.

**Novos dispositivos baseados na internet:** você tem novos dispositivos Windows 10/11 que se juntam ao Azure AD e se inscrevem automaticamente no Intune. Você instala o Configuration Manager client para chegar ao estado de cogerenciamento.



# Comparar os recursos do Windows 365 e da Área de Trabalho Virtual do Azure

## Windows 365:

- O Windows 365 é um serviço baseado em nuvem que cria automaticamente um tipo de máquina virtual do Windows, conhecida como PC na nuvem, para seus usuários finais.
  - PCs na nuvem do Windows 365 personalizados em diferentes dispositivos
  - Transmitir de qualquer dispositivo
  - Implantar e gerenciar em um só console
  - Provisionado automaticamente
  - Integração nativa a outros produtos da Microsoft

## Área de Trabalho Virtual do Azure:

- A AVD (Área de Trabalho Virtual do Azure) é uma solução moderna e segura de virtualização de aplicativos e área de trabalho no Azure.
  - Configurar a implantação do cliente Windows de várias sessões
  - Executar o Microsoft 365 Apps em cenários virtuais de vários usuários
  - Atualizações de segurança estendida gratuitas
  - Trazer aplicativos e áreas de trabalho existentes do RDS e do Windows Server
  - Gerenciar áreas de trabalho e aplicativos com uma experiência de gerenciamento unificada



# Descrever os modelos de implantação e versão do WaaS (Windows como serviço)



**Podemos aprender sobre os modelos de implantação e lançamento do WaaS (Windows como serviço) nos seguintes:**

- Tipos de versão – Atualizações de recursos e de qualidade
- Canais de serviço – Programa Windows Insider, Canal de Disponibilidade Geral e Canal de Serviço de Longo Prazo
- Anéis de implantação – Versão prévia, Limitado e Amplo
- Métodos de implantação para Windows – métodos de implantação Moderno, Dinâmico e Tradicional
- Gerenciar o Windows como serviço – Configuration Manager

# Anéis de implantação – Prévia (visualização)



Os usuários do anel de visualização são as pessoas mais experientes e resilientes de tecnologia, que não perderão a produtividade se algo der errado. Em geral, esses usuários são profissionais de TI e talvez algumas pessoas na organização de negócios.

Durante as fases de planejamento e preparação, você deve se concentrar nas seguintes atividades:

- Trabalhe com Windows Insider Preview builds.
- Identifique os recursos e a funcionalidade que sua organização pode ou deseja usar.
- Estabeleça quem usará os recursos e como eles se beneficiarão.
- Entenda por que você está colocando a atualização.
- Planeje os comentários de uso.

# Anéis de implantação – Limitado

A finalidade do anel Limitado é validar a atualização em dispositivos representativos em toda a rede. Durante esse período, os dados e os comentários são gerados para permitir que a decisão de avançar para uma implantação mais ampla. Análise de Área de Trabalho pode ajudar a definir um bom anel limitado de dispositivos representativos e ajudar a monitorar a implantação.

Se possível, todos os hardwares e todos os aplicativos devem ser representados e é importante que as pessoas selecionadas para esse anel estejam usando seus dispositivos regularmente para gerar os dados necessários para tomar uma decisão para uma implantação mais ampla em toda a sua organização.

Durante o piloto e as fases de validação, você deve se concentrar nas seguintes atividades:

- Implantar inovações.
- Avalie e aja se forem encontrados problemas.
- Avançar, a menos que bloqueado.

# Anéis de implantação – Amplo

Na maioria das empresas, o anel Amplo inclui o restante da sua organização. Devido ao trabalho no anel anterior para verificar a estabilidade e minimizar a interrupção (com dados de diagnóstico para dar suporte à sua decisão), uma implantação ampla pode ocorrer relativamente rapidamente.

Durante a fase de implantação ampla, você deve se concentrar nas seguintes atividades:

- **Implante em todos os dispositivos na organização.**
- Trabalhe em todos os problemas incomuns finais que não foram detectados em seu anel Limitado.
- Avalie e aja se forem encontrados problemas.
- Avançar, a menos que bloqueado.

# Implantação Moderna



AZURE CLOUD  
COMPUTING

Cenário	Descrição	Mais informações
<a href="#"><u>Windows Autopilot</u></a>	Personalizar a OOB (experiência inicial) para sua organização e implantar um novo sistema com aplicativos e configurações já definidas	<a href="#"><u>Visão geral do Windows Autopilot.</u></a>
<a href="#"><u>Upgrade in-loco (In-Place)</u></a>	Use a Instalação do Windows para atualizar seu sistema operacional e migrar aplicativos e configurações. Dados de reversão são salvos em Windows.old.	<a href="#"><u>Realizar um upgrade in-loco para o Windows 10 com o MDT</u></a> <a href="#"><u>Realizar um upgrade in-loco para o Windows 10 usando o Configuration Manager</u></a>

# Implantação Dinâmica

Cenário	Descrição	Mais informações
<a href="#"><u>Ativação de assinatura</u></a>	Alternar do Windows 10 Pro para o Enterprise quando um usuário inscrito entrar.	<a href="#"><u>Ativação de assinatura do Windows 10</u></a>
<a href="#"><u>AAD / MDM</u></a>	O dispositivo é ingressado automaticamente Azure Active Directory e configurado pelo MDM.	<a href="#"><u>Integração do Azure Active Directory com o MDM</u></a>
<a href="#"><u>Pacotes de provisionamento</u></a>	Usando a ferramenta Designer de Configuração e Imagens do Windows, crie pacotes de provisionamento que possam ser aplicados a dispositivos.	<a href="#"><u>Configurar dispositivos sem MDM</u></a>



# Implantação Tradicional

Cenário	Descrição	Mais informações
<a href="#">Bare-metal</a>	Implante um dispositivo novo ou limpe um dispositivo existente e implante com uma imagem nova.	<a href="#">Implantar uma imagem do Windows 10 com o MDT</a> <a href="#">Implantar o Windows 10 usando o PXE e o Configuration Manager</a>
<a href="#">Atualizar</a>	Também chamado de limpar e carregar. Reimplante um dispositivo salvando o estado do usuário, apagando o disco e, em seguida, restaurando o estado do usuário.	<a href="#">Atualizar um computador Windows 7 com Windows 10</a> <a href="#">Atualizar um cliente do Windows 7 SP1 com Windows 10 usando o Configuration Manager</a>
<a href="#">Substituir</a>	Substitua um dispositivo existente por um novo salvando o estado do usuário no dispositivo antigo e, em seguida, restaurando-o no novo dispositivo.	<a href="#">Substituir um computador Windows 7 por um computador Windows 10</a> <a href="#">Substitua um cliente do Windows 7 SP1 pelo Windows 10 com o Configuration Manager</a>

# Identificar métodos de implantação e manutenção do Microsoft 365 Apps



Para implantar o Office, primeiro escolha qual ferramenta de implantação usar e se você instalará os arquivos do Office diretamente da nuvem ou de uma fonte local na rede.

## **Quatro métodos para executar implantações de grande escala do Microsoft 365 Apps:**

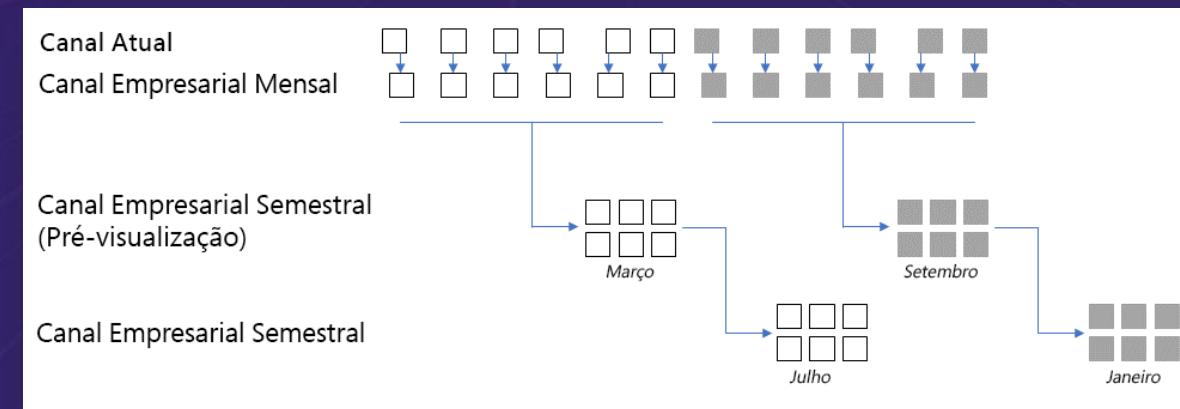
- **Implantar de uma fonte local com o Configuration Manager:** gerencie sua implantação com o Configuration Manager e baixe e implante o Office a partir de pontos de distribuição na sua rede.
- **Implantar da nuvem com a Ferramenta de Implantação do Office:** gerencie sua implantação com a ODT e instale o Office em dispositivos cliente diretamente da CDN do Office.
- **Implantar de uma fonte local com a Ferramenta de Implantação do Office:** gerencie sua implantação com a ODT e baixe e implante o Office de uma fonte local na sua rede.
- **Instalar por conta própria da nuvem:** gerencie sua implantação pelo portal do Office e peça que seus usuários instalem o Office nos dispositivos cliente deles diretamente do portal.

# Métodos de implantação e manutenção do Microsoft 365 Apps

## Tipos de canais de atualizações para o Microsoft 365 Apps:

- **Canal Atual:** Oferece aos usuários os recursos mais recentes do Office assim que eles estiverem prontos, mas sem cronogramas.
- **Canal Empresarial Mensal:** Fornece aos usuários os recursos mais recentes do Office somente uma vez por mês e em um cronograma previsível (a segunda terça-feira do mês)
- **Canal Empresarial Semestral:** Oferece aos usuários os novos recursos do Office a cada seis meses, em Janeiro e julho.

Todos os canais de atualização receberão atualizações por questões de segurança e não segurança, quando necessário. Essas atualizações geralmente ocorrem na segunda terça-feira do mês





# Gerenciar atualizações do Microsoft 365 Apps

Escolha como gerenciar atualizações:

- **Atualizar automaticamente:** dispositivos cliente são automaticamente atualizados diretamente pela CDN do Office com base no canal de atualização que você define como parte da implantação inicial.
- **Gerenciar as atualizações do Configuration Manager:** atualizações do Office são baixadas e implantadas em dispositivos cliente pelo Configuration Manager
- **Gerenciar as atualizações com a Ferramenta de Implantação do Office:** atualizações do Office são baixadas para uma fonte local pela ODT e instaladas em dispositivos cliente.

Assim como com a implantação inicial, as organizações podem usar uma combinação das opções a seguir para diferentes usuários.



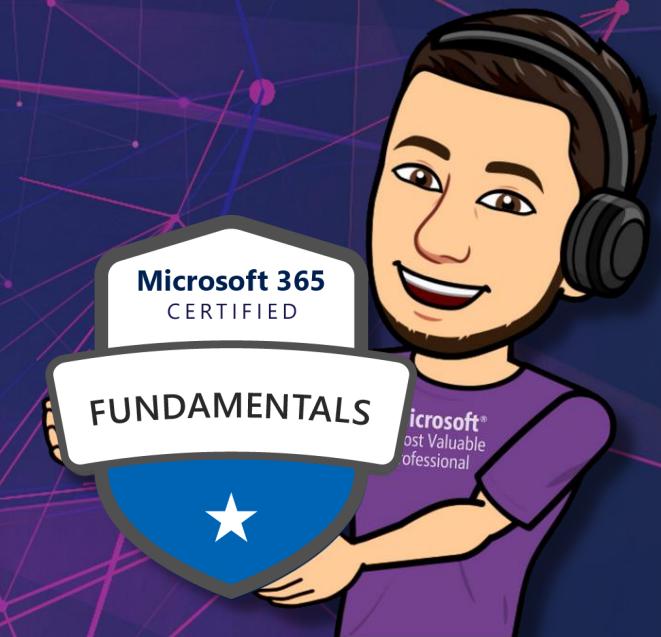
# OBRIGADO

---

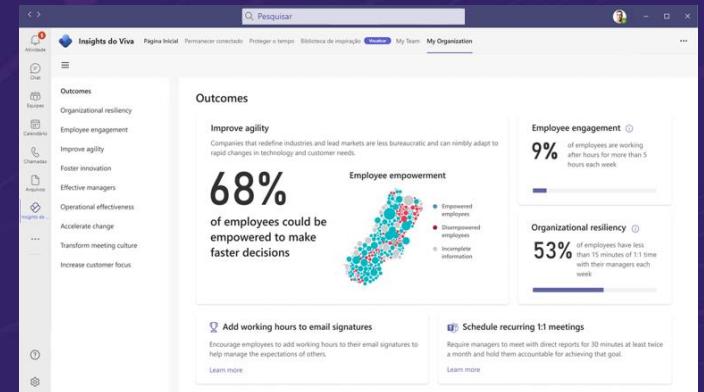
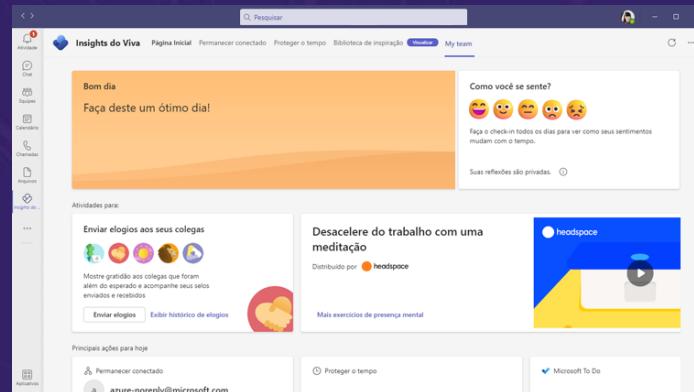
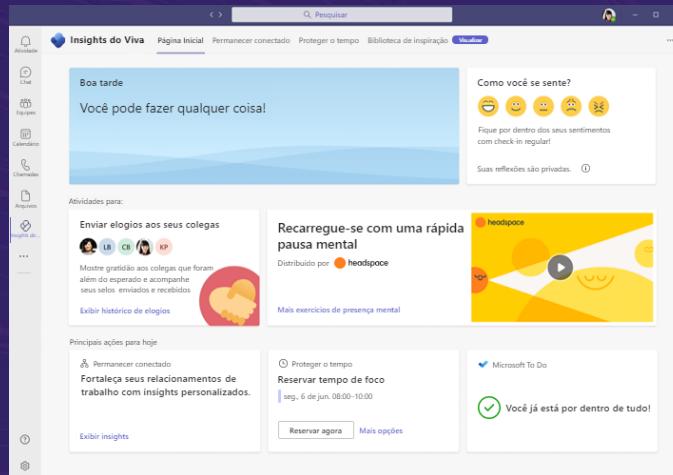
#partiu  
nuvem



# Descrever os recursos de análise no Microsoft 365



# Descrever os recursos dos Insights do Viva



## Insights pessoais

- Bem-estar pessoal
- Permanecer conectado
- Horário protegido
- Resumo diário
- Reuniões eficazes

## Insights do Gerente

- Chamar a atenção
- Insights reflexivos
- Planos de ação

## Insights Organizacionais

- Resiliência organizacional
- Participação do funcionário
- Aprimorar a agilidade
- Promover a inovação
- Gerentes eficazes
- Eficácia operacional
- Acelerar mudanças
- Transformar a cultura de reuniões
- Aumentar o foco o cliente

# Descrever os recursos do centro de administração e do portal do usuário do Microsoft 365



AZURE CLOUD COMPUTING

## Centro de administração do Microsoft 365:

- Gerenciar usuários adicionando, excluindo ou restaurando usuários.
- Gerenciar licenças adicionando e removendo licenças.
- Gerenciar um grupo do Microsoft 365 criando um grupo, excluindo um grupo e editando o nome ou a descrição.
- Gerenciar a cobrança.
- Exibir ou criar solicitações de serviço.
- Gerenciar configurações globais para aplicativos.
- Ver relatórios de atividades.
- Exibir a integridade do serviço.

[Video Portal](#)

## Portal do usuário do Microsoft 365:

- O portal do usuário do Microsoft 365 foi projetado para que os usuários acessem seus emails, calendários e documentos por meio de aplicativos do Microsoft 365, como Office, Teams, Outlook e muito mais.

# Descrever os relatórios disponíveis no centro de administração do Microsoft 365 e outros centros de administração

## Os dois tipos de relatórios disponíveis no centro de administração:

- Pontuação de produtividade
- Uso

## Outros centros de administração com relatórios:

- Azure Active Directory
- Endpoint Manager
- Exchange
- Segurança e conformidade
- SharePoint
- Teams

[Video Portal](#)

The screenshot shows the Microsoft 365 Admin Center interface. On the left, there is a navigation sidebar with categories like 'Funções', 'Recursos', 'Cobrança', 'Suporte', 'Configurações', 'Configurar', 'Relatórios', and 'Integridade'. Under 'Relatórios', two items are listed: 'Pontuação de Produtividade' and 'Uso'. Below these, a section titled 'Centros de administração' is expanded, showing 'Segurança', 'Conformidade', 'Endpoint Manager', 'Azure Active Direct...', and 'Exchange'. The main content area is titled 'Todos os centros de administração' and lists various administrative centers with their names and brief descriptions. The 'Centros de administração' section is highlighted with a red border.

Nome	Descrição
Aplicativos do Dynamics 365	Use o centro de administração do Dynamics 365 para gerenciar seu ambiente, gerenciar capacidade, monitorar uso e executar outras operações administrativas.
Azure Active Directory	Aproveite ao máximo o gerenciamento de identidades. Habilite a autenticação multifator, a redefinição de senha de autotendimento e edite a identidade visual da empresa.
Azure ATP	Identificar, detectar e investigar ameaças avançadas, identidades comprometidas e ações internas mal intencionadas direcionadas à sua organização.
Configuração do Office	Gerencie, configure e monitore a implantação de aplicativos de Microsoft 365 para sua organização.
Conformidade	Use o Microsoft Purview compliance portal para atender às suas metas de conformidade e privacidade. Você encontrará soluções integradas que ajudam a proteger informações confidenciais, gerenciar ciclos de vida de dados, reduzir riscos internos, proteger dados pessoais e muito mais.
Endpoint Manager	Uma experiência única de gerenciamento para a equipe de Computação do Usuário Final em TI para garantir que os dispositivos e aplicativos do Microsoft 365 dos funcionários estejam protegidos, gerenciados e atualizados.
Exchange	Gerencie as configurações de email avançadas, como regras de fluxo de email, criptografia e quarentena.
Fluxo	Escolha como Microsoft Stream funciona para a sua organização.



# OBRIGADO

---

#partiu  
nuvem





AZURE CLOUD  
COMPUTING

# Labs Hand On



#partiu  
nuvem



AZURE CLOUD  
COMPUTING

## LAB 01 – Explorar recursos do Microsoft 365

- Task 1: Realizar criação de um novo usuário e atribuir licença
- Task 2: Explorar recursos do Sharepoint e One Drive
- Task 3: Explorar Microsoft Planner e o Microsoft To-Do
- Task 4: Instalar o pacote Office diretamente pelo portal
- Task 5: Explorar Microsoft Teams e Microsoft Viva

