

# Fundamentos do Azure AZ-900

## **Capítulo 1: Introdução à Computação em Nuvem**

- O que é computação em nuvem?
- Modelos de serviço: IaaS, PaaS, SaaS
- Modelos de implantação: Pública, Privada, Híbrida

## **Capítulo 2: Conceitos Principais do Azure**

- Regiões e zonas de disponibilidade
- Recursos e assinaturas
- Grupos de recursos e gerenciamento

## **Capítulo 3: Serviços Principais do Azure**

- Máquinas Virtuais (VMs)
- Armazenamento no Azure (Blob, Disk, File)
- Banco de dados no Azure (SQL, Cosmos DB)
- Rede Virtual e conectividade

## **Capítulo 4: Segurança e Conformidade no Azure**

- Azure Active Directory (AAD)
- Controle de acesso baseado em função (RBAC)
- Políticas e governança no Azure

## **Capítulo 5: Preços e Suporte**

- Modelos de precificação do Azure
- Calculadora de custos do Azure
- Suporte e SLA

# **Capítulo 1: Introdução à Computação em Nuvem**

## **O que é computação em nuvem?**

A computação em nuvem revolucionou a maneira como empresas e indivíduos acessam e gerenciam tecnologia. Em sua essência, a computação em nuvem refere-se à entrega de recursos de TI — como servidores, armazenamento, redes e aplicativos — pela internet. Em vez de depender de infraestruturas locais e servidores físicos, a nuvem oferece um modelo flexível e escalável onde os usuários podem consumir recursos conforme a necessidade.

Os benefícios da computação em nuvem são variados e impactam diretamente a eficiência e os custos operacionais. Um dos principais aspectos é a escalabilidade: empresas podem aumentar ou reduzir o uso de recursos de acordo com a demanda. Além disso, a alta disponibilidade e a redundância dos servidores distribuídos garantem que os serviços estejam acessíveis a qualquer momento e em qualquer lugar. Outro benefício é a economia de custos, já que as organizações podem eliminar investimentos em hardware físico e reduzir gastos com manutenção e energia.

A segurança também é uma preocupação na computação em nuvem, e os provedores investem fortemente em medidas como criptografia, autenticação de múltiplos fatores e controles de acesso avançados. No entanto, as empresas ainda precisam adotar boas práticas para proteger seus dados, como a implementação de políticas de segurança e monitoramento contínuo.

## Modelos de serviço: IaaS, PaaS, SaaS

A computação em nuvem pode ser classificada em três principais modelos de serviço: **Infraestrutura como Serviço (IaaS)**, **Plataforma como Serviço (PaaS)** e **Software como Serviço (SaaS)**.

- **IaaS (Infrastructure as a Service)** O modelo IaaS fornece a infraestrutura essencial de TI por meio da nuvem. Com IaaS, empresas podem acessar servidores virtuais, armazenamento, redes e outras funcionalidades sem a necessidade de adquirir hardware físico. Esse modelo é ideal para organizações que precisam de controle total sobre seus ambientes de TI e desejam gerenciar sistemas operacionais, aplicativos e configurações personalizadas. Exemplos de IaaS incluem **Microsoft Azure Virtual Machines, Amazon EC2 e Google Compute Engine**.
- **PaaS (Platform as a Service)** O PaaS oferece um ambiente completo para desenvolvimento, teste e implantação de aplicativos sem a necessidade de gerenciar infraestrutura subjacente. Ele inclui ferramentas, bancos de dados, serviços de middleware e sistemas operacionais pré-configurados, facilitando o trabalho dos desenvolvedores. Com PaaS, as empresas podem acelerar a criação de software sem se preocupar com manutenção de servidores ou escalabilidade. Exemplos incluem **Microsoft Azure App Services, Google App Engine e AWS Elastic Beanstalk**.
- **SaaS (Software as a Service)** O SaaS é o modelo de serviço mais acessível para os usuários finais, pois oferece software pronto para uso diretamente pela internet, sem necessidade de instalação local. Aplicações SaaS são gerenciadas e mantidas pelo provedor de serviços, garantindo atualizações automáticas e suporte técnico. Exemplos populares incluem Microsoft 365, Google Workspace, Salesforce e plataformas de streaming como Netflix.

## **Modelos de implantação: Pública, Privada e Híbrida**

Além dos modelos de serviço, a computação em nuvem pode ser classificada em três principais formas de implantação: Nuvem Pública, Nuvem Privada e Nuvem Híbrida.

### **Nuvem Pública**

A nuvem pública é um ambiente compartilhado onde os serviços são disponibilizados a vários clientes por meio de um provedor externo. Toda a infraestrutura — servidores, armazenamento, redes e serviços — é gerenciada pelo provedor de nuvem.

Características:

Recursos altamente escaláveis e sob demanda

Acesso global via internet

Modelo de pagamento conforme o uso

Sem necessidade de manutenção física por parte do cliente

Exemplos de provedores: Microsoft Azure, Amazon Web Services (AWS). Google Cloud Platform (GCP)

Casos de uso comuns:

Startups que precisam escalar rapidamente

Empresas que desejam reduzir custos com infraestrutura

Projetos com alta variabilidade de demanda

Vantagem principal: Agilidade e economia — ideal para empresas que desejam começar rápido e com baixo investimento inicial.

## **Nuvem Privada**

A nuvem privada é uma infraestrutura de nuvem dedicada exclusivamente a uma única organização. Ela pode ser hospedada no próprio datacenter da empresa ou por um provedor terceirizado, mas o acesso é restrito e controlado.

Características:

Maior controle sobre segurança e conformidade

Personalização de hardware e software

Isolamento completo de outros usuários

Casos de uso comuns:

Organizações com requisitos rigorosos de segurança (como bancos e órgãos governamentais)

Empresas que precisam atender a normas regulatórias específicas

Ambientes que exigem desempenho previsível e dedicado

Vantagem principal: Controle total sobre os dados e a infraestrutura.

## **Nuvem Híbrida**

A nuvem híbrida combina elementos da nuvem pública e privada, permitindo que dados e aplicativos sejam compartilhados entre os dois ambientes. Isso oferece maior flexibilidade e opções de implantação.

Características:

Integração entre recursos locais e na nuvem

Possibilidade de manter dados sensíveis localmente e usar a nuvem pública para cargas variáveis

Suporte à continuidade de negócios e recuperação de desastres

Casos de uso comuns:

Empresas que desejam migrar gradualmente para a nuvem

Organizações que precisam manter parte da infraestrutura local

Situações que exigem escalabilidade rápida sem abrir mão do controle

Vantagem principal: Flexibilidade — o melhor dos dois mundos.

## Capítulo 2: Conceitos Principais do Azure

### Regiões e Zonas de Disponibilidade

#### Distribuição geográfica do Azure e como escolher a melhor região para sua aplicação

O Microsoft Azure possui uma rede global de data centers distribuídos estrategicamente ao redor do mundo. Cada região do Azure é composta por um ou mais data centers e representa um local geográfico onde os serviços da nuvem são oferecidos. A escolha da região para hospedar aplicações no Azure deve levar em consideração fatores como latência, conformidade regulatória e requisitos de desempenho.

Empresas que operam globalmente precisam de baixa latência para garantir a melhor experiência para os usuários. Nesse sentido, escolher uma região próxima aos clientes reduz os tempos de resposta. Além disso, a conformidade regulatória é essencial para determinadas indústrias, como o setor financeiro e de saúde, que possuem regras específicas sobre armazenamento e processamento de dados. O Azure oferece regiões que atendem a essas exigências, garantindo que empresas sigam as regulamentações locais.

#### Zonas de disponibilidade para alta disponibilidade e tolerância a falhas

Cada região do Azure pode conter **Zonas de Disponibilidade**, que são locais fisicamente separados dentro da mesma região. Essas zonas possuem infraestrutura independente, incluindo energia, rede e refrigeração, garantindo que, mesmo em caso de falha grave em um data center, os serviços permaneçam ativos.

Ao utilizar as **Zonas de Disponibilidade**, empresas podem projetar soluções resilientes, garantindo maior disponibilidade dos sistemas e menor impacto em caso de falhas. Os serviços do Azure, como **Máquinas Virtuais**, **Banco de Dados SQL** e **Azure Kubernetes Service (AKS)**, podem ser configurados para replicação entre zonas de disponibilidade, aumentando a tolerância a falhas.

## Recursos e Assinaturas

### Organização de recursos dentro de uma assinatura do Azure

Uma assinatura do Azure é a estrutura que permite às empresas acessarem e utilizarem os serviços da plataforma. Dentro de uma assinatura, os usuários podem provisionar, gerenciar e controlar os recursos necessários para seus projetos.

Para manter uma boa organização, o **Azure Resource Manager (ARM)** facilita o agrupamento dos recursos, permitindo que sejam organizados por aplicação, equipe ou função. Essa abordagem melhora a visibilidade dos custos e facilita a governança sobre os serviços em uso.

### Diferença entre contas gratuitas, Pay-as-you-go e contratos corporativos

O Azure oferece diferentes tipos de assinaturas, cada uma voltada para necessidades específicas:

- **Conta gratuita do Azure:** Ideal para quem deseja explorar os serviços do Azure sem custos iniciais. Oferece créditos gratuitos por tempo limitado e uma seleção de serviços sempre gratuitos.
- **Pay-as-you-go:** Modelo baseado em consumo, onde os usuários pagam pelos recursos utilizados sem necessidade de contrato longo. Essa opção é flexível e adequada para pequenas empresas e startups.
- **Contratos corporativos:** Grandes organizações podem assinar contratos personalizados com a Microsoft, garantindo melhores condições de preços, suporte técnico e serviços gerenciados.

## **Grupos de Recursos e Gerenciamento**

**Grupos de Recursos**, facilitando o gerenciamento e aplicação de políticas globais. Cada grupo pode conter diversos serviços como VMs, bancos de dados, redes e funções de aplicativos.

Ao utilizar grupos de recursos, empresas podem:

Aplicar permissões e políticas de segurança centralizadas.

Monitorar custos por grupo de projeto ou equipe.

Automatizar tarefas administrativas para todos os recursos de um grupo.

## **Utilização do Azure Resource Manager (ARM) e suas principais funcionalidades**

O **Azure Resource Manager (ARM)** é o serviço de gerenciamento que permite implantar, gerenciar e organizar os recursos do Azure de forma eficiente. Entre suas funcionalidades estão:

**Templates ARM:** Definição de infraestrutura como código para padronizar implantações.

- **RBAC (Role-Based Access Control):** Controle de acesso baseado em funções, garantindo segurança na administração dos recursos.
- **Tags:** Organização de recursos através de marcações para facilitar a identificação e categorização.
- **Políticas do Azure:** Aplicação de regras de conformidade automatizadas para manter governança sobre os serviços.



## Capítulo 3: Serviços Principais do Azure

### Máquinas Virtuais (VMs)

As **Máquinas Virtuais (VMs)** do Azure oferecem uma solução flexível para executar aplicativos e sistemas operacionais na nuvem. Com o serviço de VMs, os usuários podem provisionar servidores virtuais que podem ser configurados com diferentes capacidades de CPU, memória e armazenamento, permitindo um alto nível de personalização para atender às demandas específicas de cada aplicação.

Uma das principais vantagens das VMs do Azure é a escalabilidade. Os usuários podem aumentar ou reduzir os recursos de acordo com a necessidade, sem precisar adquirir novos equipamentos físicos. Além disso, as máquinas virtuais podem ser integradas a outros serviços do Azure, como **Azure Load Balancer**, para distribuir tráfego entre várias instâncias e garantir alta disponibilidade.

O Azure suporta diversas distribuições de sistemas operacionais, incluindo **Windows Server, Ubuntu, Red Hat Enterprise Linux, SUSE Linux** e outras. Os usuários podem também criar **Imagens Personalizadas** e armazená-las no **Azure Compute Gallery** para facilitar a implantação em larga escala. Outro benefício das VMs no Azure é a opção de **Spot VMs**, que permite acessar capacidade computacional não utilizada a um custo significativamente mais baixo. Esse modelo é útil para cargas de trabalho flexíveis, como testes e processamento de dados.

### Armazenamento no Azure (Blob, Disk, File)

O **Azure Storage** fornece serviços de armazenamento escaláveis e seguros para diversas necessidades, incluindo armazenamento de arquivos, discos virtuais e dados estruturados. Os principais tipos de armazenamento no Azure são:

#### Blob Storage

O **Blob Storage** é utilizado para armazenar grandes volumes de dados não estruturados, como vídeos, imagens e backups. Esse serviço suporta diferentes níveis de armazenamento, como **Hot, Cool e Archive**, permitindo que os usuários escolham a melhor opção com base na frequência de acesso e nos custos.

#### Disk Storage

O **Disk Storage** é projetado para fornecer armazenamento persistente para máquinas virtuais. Ele suporta **discos gerenciados**, que oferecem alta disponibilidade e redundância. Os discos podem ser **HDD, SSD Standard e SSD Premium**, dependendo das necessidades de desempenho.

#### File Storage

O **Azure File Storage** permite o armazenamento e compartilhamento de arquivos via protocolo **SMB** (Server Message Block). É uma excelente alternativa para aplicações que exigem acesso simultâneo a arquivos entre diferentes instâncias de máquinas virtuais.

## **Banco de Dados no Azure (SQL, Cosmos DB)**

O Azure oferece diversas opções de banco de dados gerenciados para diferentes necessidades:

### **Azure SQL Database**

O **Azure SQL Database** é um serviço de banco de dados relacional totalmente gerenciado, baseado no SQL Server. Ele elimina a necessidade de manutenção de infraestrutura, oferecendo **backups automáticos, alta disponibilidade e escalabilidade automática**.

### **Azure Cosmos DB**

O **Cosmos DB** é uma solução de banco de dados NoSQL distribuída, ideal para aplicações que requerem baixa latência e disponibilidade global. Ele suporta diversos modelos de dados, incluindo **documentos (MongoDB), tabelas, grafos e colunas amplas**.

Além dessas opções, o Azure também possui serviços como **Azure Database for MySQL, Azure Database for PostgreSQL e Azure Database for MariaDB**, permitindo que os usuários escolham a tecnologia mais adequada para seus projetos.

## Rede Virtual e Conectividade

O **Azure Virtual Network (VNet)** permite que usuários criem redes privadas na nuvem, conectando máquinas virtuais, bancos de dados e aplicativos de forma segura. Ele oferece suporte a diferentes configurações de rede, como:

### VPN Gateway

O **VPN Gateway** permite a conexão segura entre data centers locais e a nuvem do Azure via uma **VPN Site-to-Site** ou **Point-to-Site**, garantindo criptografia e segurança no tráfego de dados.

### ExpressRoute

O **Azure ExpressRoute** fornece uma conexão dedicada entre a infraestrutura local e o Azure, oferecendo baixa latência e maior confiabilidade do que conexões de internet tradicionais.

### Azure Load Balancer e Application Gateway

O **Azure Load Balancer** distribui o tráfego de rede entre instâncias de máquinas virtuais, garantindo disponibilidade e desempenho. Já o **Azure Application Gateway** funciona como um balanceador de carga que inclui recursos avançados, como inspeção de tráfego e proteção contra ataques.

## Capítulo 4: Segurança e Conformidade no Azure

A segurança na nuvem é um dos principais desafios para empresas que adotam serviços como o Microsoft Azure. Para garantir proteção de dados e controle de acesso eficiente, o Azure oferece uma ampla gama de ferramentas e serviços que ajudam a implementar práticas seguras e a manter a conformidade com regulamentações internacionais.

**Azure Active Directory (AAD)** O **Azure Active Directory (Azure AD)** é o serviço de gerenciamento de identidade e acesso na nuvem da Microsoft. Ele permite que empresas protejam informações sensíveis, controlando quem pode acessar recursos e dados.

### **Autenticação e Gerenciamento de Identidade**

O **Azure AD** permite que usuários e aplicativos se autenticuem de forma segura, reduzindo riscos de acesso não autorizado. Entre seus principais recursos estão:

**Autenticação Multifator (MFA)** – Exige um segundo fator de autenticação, como um código enviado ao celular, para aumentar a segurança.

**Single Sign-On (SSO)** – Permite que os usuários acessem múltiplos aplicativos e serviços com uma única credencial, reduzindo a necessidade de múltiplos logins.

**Gerenciamento de Identidades Híbridas** – Integra identidades locais do **Active Directory** com o Azure, facilitando a transição de empresas para a nuvem.

## Proteção Contra Ameaças

O Azure AD usa inteligência artificial e análises avançadas para identificar e prevenir ataques cibernéticos. Recursos como **Identity Protection** monitoram riscos em tempo real, detectando acessos suspeitos e atividades incomuns.

## Controle de Acesso Baseado em Função (RBAC)

O **Role-Based Access Control (RBAC)** é um mecanismo de gerenciamento de permissões que define quais ações usuários podem executar dentro de um ambiente do Azure. Com RBAC, empresas podem restringir acessos para garantir que apenas usuários autorizados possam modificar ou visualizar determinados recursos.

## Princípios do RBAC

**Menor Privilégio Possível** – Os usuários recebem apenas as permissões mínimas necessárias para realizar suas tarefas.

**Papéis Predefinidos** – O Azure inclui funções como **Leitor**, **Contribuidor** e **Administrador**, facilitando o gerenciamento de permissões.

**Papéis Personalizados** – As empresas podem criar papéis específicos para suas necessidades, garantindo um controle mais preciso.

Além de proteger contra acessos indevidos, o RBAC melhora a governança organizacional, ajudando a manter ambientes seguros e bem estruturados.

## Políticas e Governança no Azure

Para garantir conformidade e governança na nuvem, o Azure oferece diversas ferramentas que permitem a aplicação de normas de segurança e regulamentos.

## Azure Policy

O **Azure Policy** permite que empresas definam regras e padrões para garantir que os recursos estejam em conformidade com políticas internas e externas. Com ele, é possível:

Aplicar **restrições automáticas**, como impedir a criação de VMs em regiões específicas.

Monitorar o **cumprimento de políticas**, garantindo que todos os recursos sigam boas práticas de segurança.

Implementar **correções automáticas**, ajustando configurações para atender requisitos de conformidade.

## Microsoft Defender for Cloud

O **Microsoft Defender for Cloud** fornece recomendações de segurança, identificando vulnerabilidades e sugerindo melhorias para proteger os dados armazenados no Azure.

## Compliance Manager

O Azure também conta com o **Compliance Manager**, um serviço que ajuda as empresas a atenderem regulamentações como **GDPR**, **ISO 27001** e **HIPAA**. Ele fornece relatórios detalhados sobre o nível de conformidade e sugestões para melhorar a segurança.

## Capítulo 5: Preços e Suporte

O Microsoft Azure oferece diferentes modelos de precificação para atender às necessidades de empresas e indivíduos. A transparência e a flexibilidade nos custos permitem que os usuários escolham a melhor estratégia de investimento para suas cargas de trabalho na nuvem. Além disso, a plataforma disponibiliza ferramentas como a **Calculadora de Custos do Azure**, que ajuda a prever gastos antes da implementação de serviços. No quesito suporte, o Azure conta com **Service Level Agreements (SLAs)** que garantem a disponibilidade dos serviços e opções de suporte técnico conforme a demanda dos clientes.

### Modelos de Precificação do Azure

O Azure possui diversas opções de preços que variam conforme o consumo e o tipo de serviço utilizado. Os principais modelos de precificação incluem:

**Pay-as-you-go (Pagamento conforme o uso)** Esse modelo permite que os usuários paguem apenas pelos recursos consumidos, sem necessidade de contratos longos ou compromissos financeiros prévios. O Pay-as-you-go é ideal para startups e empresas que precisam de escalabilidade e flexibilidade, ajustando os custos conforme o crescimento do negócio.

### Reserva de instâncias (Reserved Instances)

Para workloads previsíveis e de longa duração, o Azure oferece descontos significativos para instâncias reservadas, onde os usuários podem contratar recursos por períodos de um ou três anos com preços reduzidos. Esse modelo é vantajoso para empresas que sabem suas necessidades computacionais com antecedência.

## Spot Instances

As **Spot VMs** oferecem preços reduzidos para cargas de trabalho que podem ser interrompidas, utilizando capacidade computacional não utilizada pelo Azure. Esse modelo é útil para tarefas como processamento de dados e testes de aplicações.

## Azure Hybrid Benefit

A Microsoft disponibiliza o **Azure Hybrid Benefit**, que permite que clientes que já possuem licenças do Windows Server e SQL Server utilizem esses produtos no Azure sem custos adicionais, reduzindo significativamente os gastos operacionais.

## Calculadora de Custos do Azure

O **Azure Pricing Calculator** é uma ferramenta essencial para planejamento financeiro, permitindo que os usuários façam estimativas detalhadas sobre os custos de seus serviços na nuvem. Com essa calculadora, é possível:

- **Escolher serviços específicos** e configurar parâmetros como armazenamento,
- **Comparar diferentes regiões** para entender variações de preços em diferentes data centers do Azure.
- **Estimar custos mensais e anuais**, facilitando o planejamento de orçamento para TI.
- **Adicionar descontos e benefícios**, como Reserved Instances e Azure Hybrid Benefit, para obter estimativas mais precisas.
- A ferramenta pode ser acessada pelo site oficial do Azure e ajuda empresas a evitar surpresas financeiras, garantindo previsibilidade nos custos operacionais.



## Suporte e SLA

O suporte técnico do Azure está disponível em diferentes planos, permitindo que usuários escolham o nível de atendimento ideal para suas necessidades. Entre as opções de suporte, estão:

### Plano Gratuito

Todos os usuários do Azure têm acesso ao suporte básico, que inclui documentação oficial, fóruns de discussão e acesso ao status dos serviços.

### Planos Pagos (Standard, Professional Direct, Premier)

Para empresas que precisam de um suporte mais avançado, o Azure oferece planos pagos que incluem:

**Suporte técnico 24/7** para incidentes críticos.

**Tempo de resposta reduzido**, garantindo atendimento prioritário.

**Consultoria especializada** e recomendações para otimização de recursos.

### Service Level Agreement (SLA)

O **SLA do Azure** define os níveis de garantia de disponibilidade dos serviços. Cada serviço tem um SLA específico, e alguns exemplos incluem:

**Máquinas Virtuais** – Garantia de **99,9%** de disponibilidade em instâncias individuais e **99,99%** em instâncias distribuídas em várias zonas de disponibilidade.

**Banco de Dados SQL** – Disponibilidade garantida de **99,99%**, com opções de redundância em várias regiões.

**Armazenamento Azure** – SLA de **99,9%** para operações de leitura e gravação.

Caso a Microsoft não cumpra os SLAs estabelecidos, os clientes podem solicitar **créditos de serviço**, reduzindo os custos das faturas em compensação pela indisponibilidade.

Material de estudo para Certificação  
AZ-900.

Conteúdo gerado por IA para fins  
didáticos