**Explorar termos e requisitos de conformidade**

Nesta unidade, você aprenderá sobre os tipos de ofertas de conformidade disponíveis no Azure.

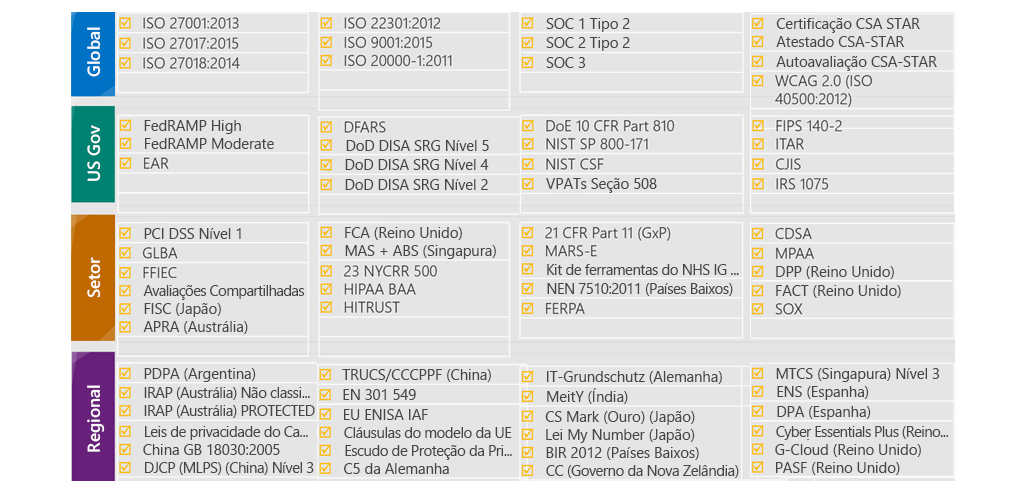
Conforme passa a executar seus aplicativos na nuvem, a Tailwind Traders quer saber como o Azure segue as estruturas de conformidade regulatória aplicáveis. A empresa pergunta:

* O quanto o Azure mantém a conformidade com relação à manipulação de dados pessoais?
* O quanto cada um dos serviços individuais do Azure se mantém em conformidade?

Os serviços online da Microsoft são baseados em um conjunto comum de controles regulatórios e de conformidade. Considere um controle como um bom padrão conhecido com o qual você pode comparar sua solução para garantir a segurança. Esses controles tratam das regulamentações atuais e se adaptam conforme as regulamentações evoluem.

## Quais categorias de conformidade estão disponíveis no Azure?

Embora haja muitas outras, a imagem a seguir mostra algumas das ofertas de conformidade mais populares disponíveis no Azure. Essas ofertas são agrupadas em quatro categorias: Global, Governo dos EUA, Setor e Regional.



Para ter uma ideia da variedade de ofertas de conformidade disponíveis no Azure, vamos examinar algumas delas com mais detalhes.

Embora nem todas essas ofertas de conformidade sejam relevantes para você ou para sua equipe, elas mostram que o compromisso da Microsoft com a conformidade é amplo, contínuo e testado e comprovado de maneira independente.

### Serviço de Informações de Justiça Criminal

Qualquer agência estadual ou local dos EUA que deseja acessar o banco de dados dos CJIS (Serviços de Informações de Justiça Criminal) do FBI precisa aderir à Política de Segurança dos CJIS.

Entre os principais provedores de nuvem, o Azure é o único que se compromete contratualmente com a conformidade com a política de segurança do CJIS. A Microsoft segue os mesmos requisitos que as entidades de justiça e de segurança pública devem atender.

### Certificação STAR da Cloud Security Alliance

O Azure, o Intune e o Microsoft Power BI obtiveram a certificação STAR da CSA (Cloud Security Alliance), que envolve uma avaliação rigorosa de terceiros independentes da postura de segurança de um provedor de nuvem.

A Certificação STAR baseia-se na obtenção da certificação ISO/IEC (Organização Internacional de Normalização/Comissão Eletrotécnina Internacional) 27001 e na adesão aos critérios especificados na CCM (Matriz de Controles de Nuvem). Essa certificação demonstra que um provedor de serviços de nuvem:

* Está em conformidade com os requisitos aplicáveis do ISO/IEC 27001.
* Tratou de problemas críticos para a segurança da nuvem, conforme descrito na CCM.
* Foi avaliado em relação ao Modelo de Maturidade de Capacidade STAR para o gerenciamento de atividades em áreas de controle da CCM.

### Cláusulas Modelo da União Europeia

A Microsoft oferece aos clientes as Cláusulas Contratuais Padrão da UE (União Europeia), que fornecem garantias contratuais com relação às transferências de dados pessoais fora da UE.

A Microsoft é a primeira empresa a receber aprovação conjunta do Grupo de Trabalho do Artigo 29º da UE para que as proteções de privacidade contratuais do Azure oferecidas aos seus clientes de nuvem empresarial atendam aos padrões atuais da UE para transferências internacionais de dados. Atender a esse padrão garante que os clientes do Azure possam usar os serviços da Microsoft para mover dados livremente pela da nuvem da Microsoft da Europa para o resto do mundo.

### Lei Health Insurance Portability and Accountability dos EUA

A lei HIPAA (Health Insurance Portability e Accountability) é uma lei federal dos EUA que regula as PHI (informações de saúde protegidas) dos pacientes.

O Azure oferece aos clientes um BAA (contrato de associado corporativo)do HIPAA, que estipula a adesão a determinadas provisões de privacidade e segurança da HIPAA e da lei HITECH. Para ajudar os clientes em seus esforços de conformidade individuais, a Microsoft oferece um contrato de associado empresarial aos clientes do Azure como um adendo do contrato.

### Organização Internacional de Normalização/Comissão Eletrotécnina Internacional 27018

A Microsoft é o primeiro provedor de nuvem a adotar o código de conduta ISO/IEC 27018, que abrange o processamento de informações pessoais por provedores de serviço de nuvem.

### Multi-Tier Cloud Security – Singapura

Após rigorosas avaliações realizadas pelo órgão de certificação de MTCS (Multi-Tier Cloud Security), os serviços em nuvem da Microsoft receberam a certificação MTCS 584:2013 em todas as três classificações de serviço:

* IaaS (infraestrutura como serviço)
* PaaS (plataforma como serviço)
* SaaS (software como serviço)

A Microsoft é o primeiro provedor de soluções de nuvem global a receber essa certificação em todas as três classificações.

### Controles de Organização de Serviço 1, 2 e 3

Os serviços de nuvem cobertos pela Microsoft são auditados pelo menos uma vez ao ano em relação à estrutura de relatório SOC (Controles de Organização de Serviço) por auditores terceirizados independentes.

A auditoria dos serviços em nuvem da Microsoft aborda os controles de segurança, disponibilidade, processamento, integridade e confidencialidade dos dados, conforme aplicável aos princípios de confiança em escopo de cada serviço.

### National Institute of Standards and Technology Cybersecurity Framework

O NIST (National Institute of Standards and Technology ) CSF (Cybersecurity Framework) é uma estrutura voluntária que consiste em padrões, diretrizes e melhores práticas para gerenciar riscos de segurança cibernética.

Os serviços em nuvem da Microsoft passaram por auditorias independentes de terceiros de Linhas de Base Alta e Moderada do FedRAMP (Federal Risk and Authorization Management Program). Os serviços em nuvem da Microsoft são certificados de acordo com os padrões do FedRAMP.

Além disso, por meio de uma avaliação validada realizada pela HITRUST (Health Information Trust Alliance), uma organização líder em desenvolvimento e capacitação de padrões de privacidade e segurança, o Office 365 foi certificado para os objetivos especificados na CSF do NIST.

### Government G-Cloud do Reino Unido

O Government G-Cloud do UK (Reino Unido) é uma certificação de computação em nuvem para serviços usados por entidades governamentais no Reino Unido. O Azure recebeu credenciamento oficial do governo do Reino Unido.

# Acessar a Política de Privacidade, os Termos dos Serviços Online e o Adendo de Proteção de Dados da Microsoft

Nesta seção, você verá como a Política de Privacidade, os Termos dos Serviços Online e o Adendo de Proteção de Dados da Microsoft explicam os dados pessoais coletados pela Microsoft, como ela os utiliza e para quais finalidades.

Para a Tailwind Traders, entender o compromisso da Microsoft com a privacidade ajuda a garantir que os dados de seus clientes e aplicativos estarão protegidos.

Vamos continuar com uma breve visão da Política de Privacidade da Microsoft e onde encontrá-la.

## O que está contido na Política de Privacidade da Microsoft?

A [Política de Privacidade da Microsoft](https://privacy.microsoft.com/privacystatement) explica quais dados pessoais a Microsoft coleta, como a Microsoft os utiliza e para quais fins.

A política de privacidade abrange todos os serviços, sites, aplicativos, softwares, servidores e dispositivos da Microsoft. Essa lista inclui desde produtos corporativos e de servidor até dispositivos que você usa em casa, passando pelos softwares que os alunos usam na escola.

A política de privacidade da Microsoft também fornece informações relevantes para produtos específicos, como o Windows e o Xbox.

## O que está contido nos Termos dos Serviços Online?

O [OST](https://www.microsoft.com/licensing/terms/product/ForallOnlineServices) (Termos dos Serviços Online) é um contrato legal entre a Microsoft e o cliente. O OST detalha as obrigações das duas partes em relação ao processamento e à segurança de dados de clientes e dados pessoais. O OST se aplica especificamente ao serviços online da Microsoft que você licencia por meio de uma assinatura, incluindo o Azure, o Dynamics 365, o Office 365 e o Bing Mapas.

## O que é o Adendo de Proteção de Dados?

O DPA (Adendo de Proteção de Dados) define com mais profundidade os termos de segurança e processamento de dados dos serviços online. Esses termos incluem:

* Conformidade com as leis.
* Divulgação de dados processados.
* Segurança de Dados, que inclui políticas e práticas de segurança, criptografia de dados, acesso a dados, responsabilidades do cliente e conformidade com auditorias.
* Transferência, retenção e exclusão de dados.

Para acessar o DPA:

1. Acesse a [Documentação e os Termos de Licenciamento](https://www.microsoftvolumelicensing.com/DocumentSearch.aspx).
2. Na barra de pesquisa, insira **DPA**.
3. Nos resultados da pesquisa, localize o link para o DPA no idioma de sua preferência. Como alternativa, na barra de pesquisa que aparece, insira o idioma de sua preferência para filtrar os resultados. Veja um exemplo que recupera a versão em inglês do DPA.

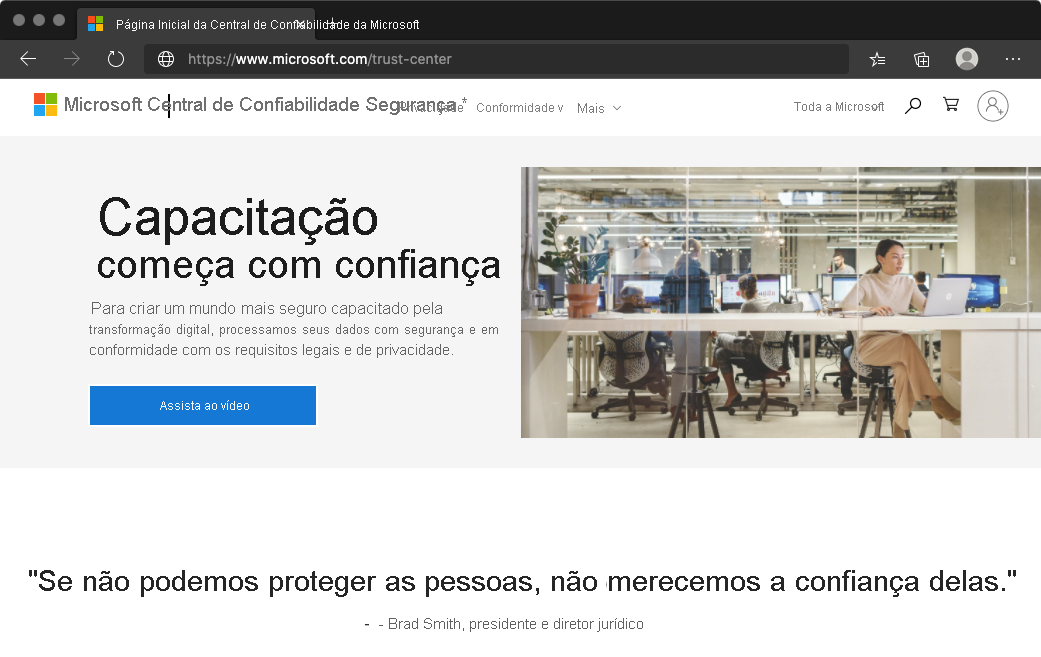


A transparência é importante quando se trata de como um provedor de nuvem comunica suas políticas de privacidade e de como ele trata seus dados. O DPA, o OST e a Política de Privacidade da Microsoft detalham o compromisso da Microsoft com a proteção de dados e da privacidade na nuvem.

# Explorar a Central de Confiabilidade

A Tailwind Traders precisa se manter atualizada com relação aos padrões de segurança mais recentes para proteger seus dados. Hoje, a equipe de segurança precisa verificar se o Azure atende ao ISO 27001, um padrão de segurança de informações amplamente utilizado. Onde a empresa pode acessar essas informações?

A [Central de Confiabilidade](https://www.microsoft.com/trust-center?rtc=1%3Fazure-portal%3Dtrue) demonstra os princípios da Microsoft para manutenção da integridade dos dados na nuvem e como a Microsoft implementa e dá suporte à segurança, à privacidade, à conformidade e à transparência em todos os seus produtos e serviços em nuvem. A Central de Confiabilidade é uma parte importante da iniciativa de Nuvem Confiável da Microsoft e dá suporte e fornece recursos para a comunidade jurídica e de conformidade.



A Central de Confiabilidade fornece:

* Informações detalhadas sobre segurança, privacidade, ofertas de conformidade, políticas, recursos e práticas recomendadas em todos os produtos de nuvem da Microsoft.
* Recursos adicionais sobre cada tópico.
* Links para os blogs de segurança, privacidade e conformidade e eventos futuros.

A Central de Confiabilidade é um excelente recurso para outras pessoas de sua organização que podem desempenhar funções de segurança, privacidade e conformidade. Essas pessoas incluem gerentes de negócios, profissionais de avaliação de risco e privacidade e equipes de conformidade jurídica.

## Explorar a Central de Confiabilidade

Como um exercício opcional, vamos olhar rapidamente a entrada na Central de Confiabilidade referente ao ISO 27001.

O acesso à Central de Confiabilidade não requer uma assinatura do Azure nem uma conta Microsoft.

1. Vá até a [Central de Confiabilidade](https://www.microsoft.com/trust-center?rtc=1%3Fazure-portal%3Dtrue).
2. Localize a seção **Recursos adicionais** na página. Em **Ofertas de conformidade**, selecione **Saiba mais**.

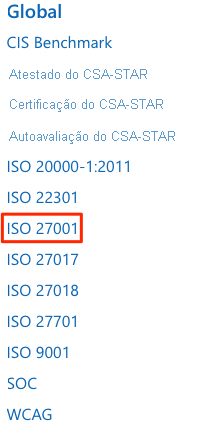


Na seção Conformidade do setor regulatório &, clique em **Ofertas de conformidade da Microsoft**.

Você será levado para [Ofertas de conformidade da Microsoft](https://docs.microsoft.com/pt-br/microsoft-365/compliance/offering-home).

Essas ofertas são agrupadas em quatro categorias: **Global**, **Governo dos EUA**, **Setor** e **Regional**.

1. Em **Global**, selecione **ISO 27001**.



A página dos Padrões de Gerenciamento de Segurança da Informação ISO 27001 é típica do tipo de informações de conformidade que fornecemos.

1. Examine rapidamente a documentação do ISO/IEC 27001.

Você verá:

* + Uma visão geral do padrão.
  + Quais serviços de nuvem fazem parte do escopo.
  + Uma visão geral do ciclo de auditoria e links para relatórios de auditoria.
  + Respostas para perguntas frequentes.
  + White papers e recursos adicionais.

As áreas de documentação de outras ofertas de conformidade variam, mas esse é o formato típico que você encontrará.

# Acessar a documentação de conformidade do Azure

Concluído100 XP

* 4 minutos

Aqui, você aprende a acessar a documentação detalhada sobre a conformidade e os padrões legais e regulatórios no Azure.

O comércio eletrônico é uma parte importante da estratégia de vendas da Tailwind Traders. A [loja de varejo online](https://www.tailwindtraders.com/) deles permite que os clientes naveguem e façam pedidos de produtos com facilidade. Normalmente, os clientes pagam com cartão de crédito, de modo que a Tailwind Traders é responsável por cumprir o DSS (Data Security Standard) do PCI (Payment Card Industry). Esse padrão global, conhecido como PCI DSS, busca evitar fraudes por meio do aumento do controle de dados de cartão de crédito. O padrão se aplica a qualquer organização que armazene, processe ou transmita dados de pagamento e de titulares de cartão.

Você tem a tarefa de investigar se, hospedando o aplicativo de comércio eletrônico da empresa no Azure, a Tailwind Traders manteria a conformidade com o PCI DSS. Você começa pela documentação de conformidade do Azure.

## O que é a documentação de conformidade do Azure?

A [documentação de conformidade do Azure](https://docs.microsoft.com/pt-br/azure/compliance/) fornece uma documentação detalhada sobre a conformidade e os padrões legais e regulatórios no Azure.

Aqui, você encontra ofertas de conformidade nestas categorias:

* Global
* Governo dos EUA
* Serviços financeiros
* Saúde
* Mídia e manufatura
* Regional

Também há recursos de conformidade adicionais, como relatórios de auditoria, informações de privacidade, mapeamentos e implementações de conformidade e white papers e relatórios de analistas. Diretrizes de privacidade e de conformidade de países e regiões também estão incluídas. Alguns recursos podem exigir que você esteja conectado ao serviço de nuvem para acessá-los.

## Examinar a conformidade com o PCI DSS

A equipe jurídica da Tailwind Traders quer saber mais sobre como o PCI DSS está relacionado ao aplicativo de comércio eletrônico da empresa no Azure.

Acompanhe o processo a seguir como um exercício opcional.

1. Vá até a [documentação de conformidade do Azure](https://docs.microsoft.com/pt-br/azure/compliance/).
2. Em **Serviços financeiros**, selecione **PCI DSS**.



Lá, você vê:

* + Uma visão geral do padrão PCI DSS.
  + Como o PCI DSS se aplica à Microsoft.
  + Quais serviços de nuvem fazem parte do escopo.
  + Uma visão geral do ciclo de auditoria.
  + Respostas para perguntas frequentes.
  + White papers e recursos adicionais.

### Acessar recursos de conformidade adicionais

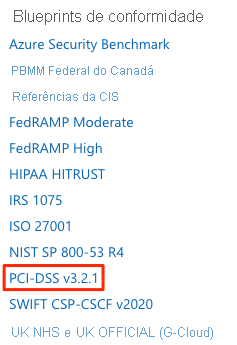
Na [documentação de conformidade do Azure](https://docs.microsoft.com/pt-br/azure/compliance/), você pode acessar recursos de conformidade adicionais.

Por exemplo, na seção **Relatórios de auditoria**, você encontra um link para os relatórios de auditoria do [PCI DSS](https://servicetrust.microsoft.com/ViewPage/MSComplianceGuideV3?docTab=7027ead0-3d6b-11e9-b9e1-290b1eb4cdeb_PCI_DSS%3Fazure-portal%3Dtrue).



Nessa seção, você pode acessar vários arquivos diferentes, incluindo os relatórios de Atestado de Conformidade e a Matriz de Responsabilidades Compartilhadas do PCI DSS.

Em **Blueprints de conformidade**, você encontra blueprints de referência, ou definições de política, para padrões comuns que podem ser aplicados à sua assinatura do Azure. O blueprint do [PCI DSS](https://docs.microsoft.com/pt-br/azure/governance/blueprints/samples/pci-dss-3.2.1/) implanta um conjunto principal de políticas que são mapeadas para a conformidade com o PCI DSS e ajudam você a controlar suas cargas de trabalho do Azure com relação a esse padrão.

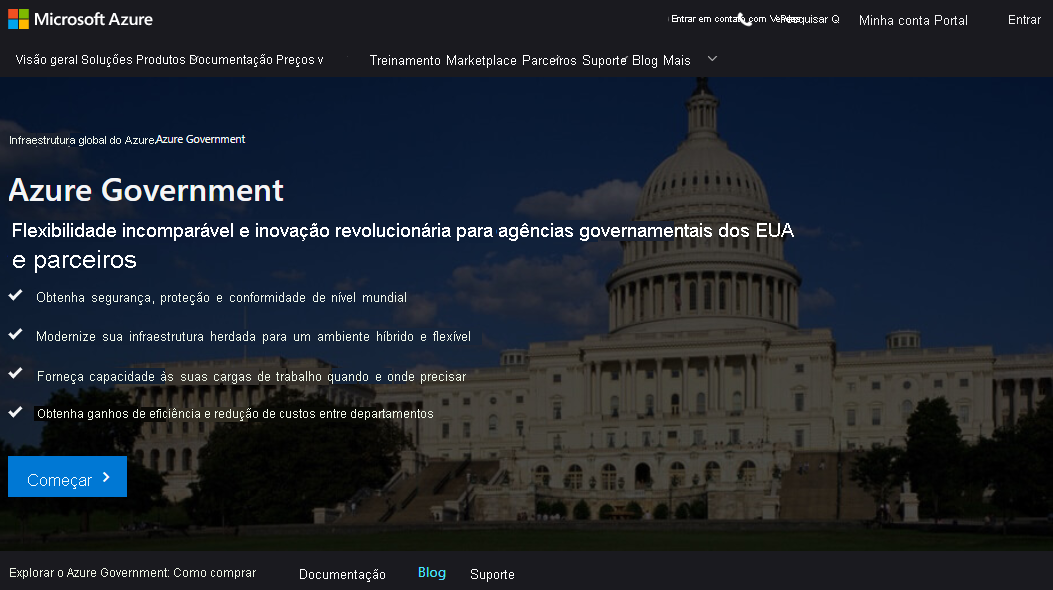


Você pode, então, ver se os recursos do Azure na arquitetura de seu aplicativo foram configurados corretamente de modo a manter a conformidade com o PCI DSS ou quais recursos você precisa corrigir.

Como os padrões evoluem, a equipe da Tailwind Traders pode verificar o relatório de auditoria periodicamente para garantir que o Azure tenha alterações recentes.

**O que é o Azure Governamental?**

O [Azure Government](https://azure.microsoft.com/global-infrastructure/government) é uma instância separada do serviço do Microsoft Azure. Ele atende às necessidades de segurança e de conformidade das agências federais dos EUA, de governos estaduais e locais e de seus provedores de soluções. O Azure Government oferece isolamento físico de implantações que não são do governo dos EUA e fornece uma equipe de TI selecionada.



Os serviços do Azure Government lidam com os dados que estão sujeitos a determinadas normas e requisitos governamentais:

* FedRAMP (Federal Risk and Authorization Management Program)
* NIST (National Institute of Standards and Technology) 800.171 DIB (Defense Industrial Base)
* ITAR (Regulamentos de Tráfego Internacional de Armas)
* IRS (Receita Federal dos Estados Unidos) 1075
* DoD (Departamento de Defesa dos Estados Unidos) L4
* CJIS (Serviço de Informações de Justiça Criminal)

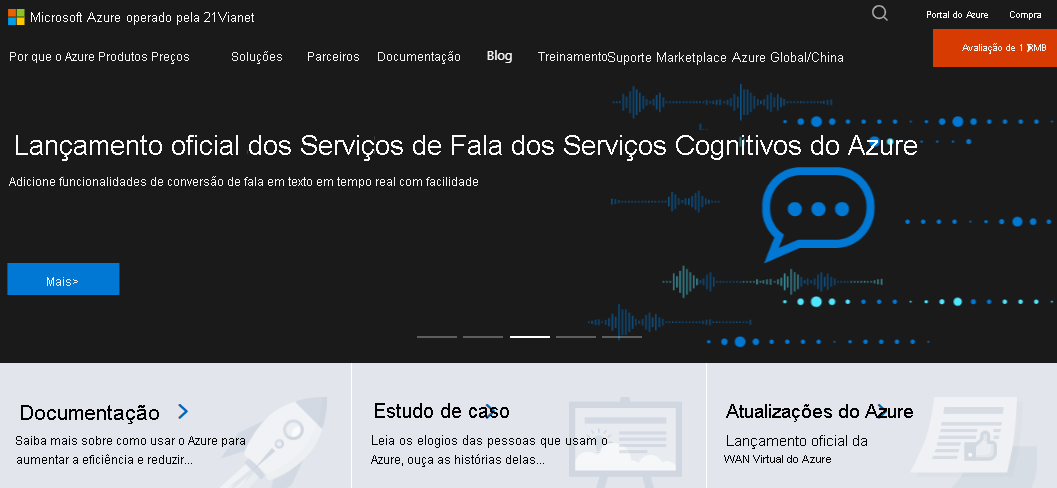
Para fornecer o mais elevado nível de segurança e conformidade, o Azure Government usa redes e data centers isolados fisicamente, localizados apenas nos EUA. Os clientes do Azure Government, como os governos locais, estaduais e federal dos EUA ou seus parceiros, estão sujeitos a uma validação quanto à elegibilidade.

O Azure Government oferece a conformidade mais ampla e tem aprovação Nível 5 do DoD dos EUA. O Azure Government está [disponível em oito geografias](https://azure.microsoft.com/global-infrastructure/geographies/#geographies?azure-portal=true) e oferece mais certificações de conformidade do que qualquer provedor de nuvem.

# O que é o Azure China 21Vianet?

A [Azure China 21Vianet](https://docs.microsoft.com/pt-br/azure/china) é operada pela 21Vianet. Trata-se de uma instância fisicamente separada dos serviços de nuvem localizados na China. O Azure China 21Vianet é operado e administrado de maneira independente pela Xangai Blue Cloud Technology Co., Ltd. ("21Vianet"), uma subsidiária de propriedade total Beijing 21Vianet Broadband Data Center Co., Ltd.

De acordo com a Regulamentação de Telecomunicação da China, os provedores de serviços de nuvem, IaaS (infraestrutura como serviço) e PaaS (plataforma como serviço) precisam ter permissões de telecomunicação de valor agregado. Somente empresas registradas localmente com menos de 50% de investimento estrangeiro se qualificam para essas permissões. Para obedecer essa regulamentação, o serviço do Azure na China é operado pela 21Vianet, com base nas tecnologias licenciadas da Microsoft.



Como o primeiro provedor de serviços de nuvem pública estrangeiro oferecido na China em conformidade com os regulamentos governamentais, o Azure China 21Vianet fornece segurança de nível mundial, conforme tratado na Central de Confiabilidade e conforme exigido pelas regulamentações chinesas, para todos os sistemas e aplicativos criados em sua arquitetura.

## Produtos e serviços do Azure disponíveis na China

Os serviços do Azure são baseados nas mesmas tecnologias do Azure, do Office 365 e do Power BI que compõem o serviço de nuvem global da Microsoft, com níveis de serviço comparáveis. Os acordos e contratos do Azure na China, onde aplicável, são assinados entre os clientes e a 21Vianet.

O Azure inclui os principais componentes de IaaS, PaaS e SaaS (software como serviço). Esses componentes incluem serviços de rede, armazenamento, gerenciamento de dados e gerenciamento de identidades, entre muitos outros.

O Azure China 21Vianet dá suporte à maioria dos mesmos serviços que o Azure global tem, como a replicação de dados geossíncrona e o dimensionamento automático. Mesmo que você já use os serviços globais do Azure, para operar na China talvez seja necessário hospedar novamente ou refatorar alguns de seus aplicativos ou serviços, ou todos eles.

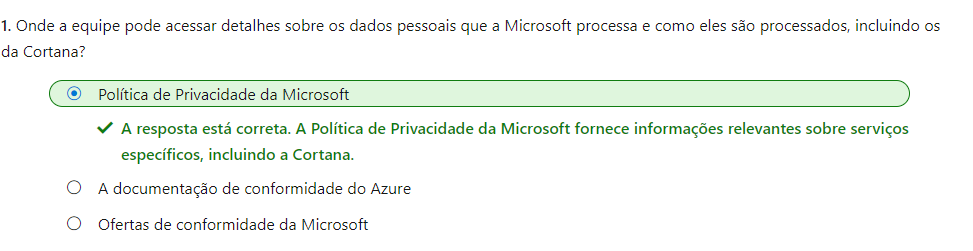
**Verificação de conhecimentos**

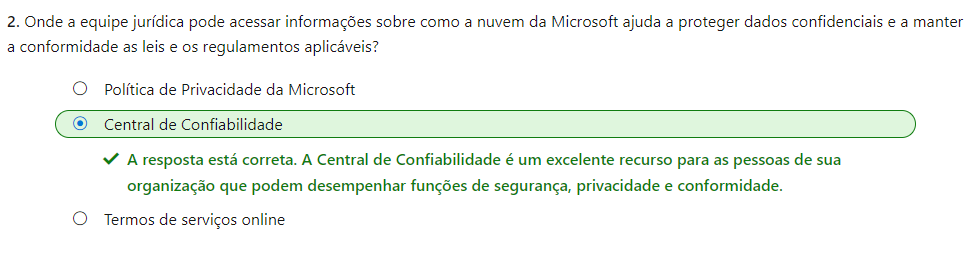
Considere este cenário.

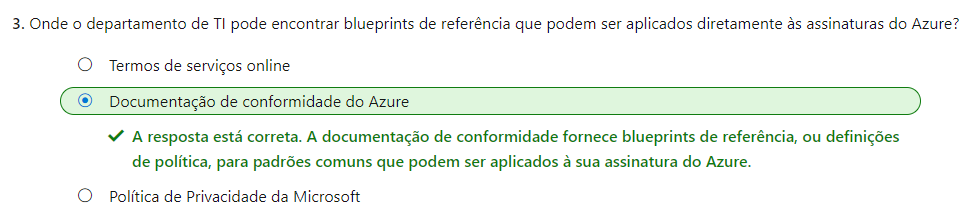
Na Tailwind Traders, os departamentos jurídico e de TI desejam entender melhor como a Microsoft lida com informações pessoais. Eles também querem entender melhor como os serviços do Azure podem ajudá-los a cumprir suas metas de conformidade.

As necessidades deles vão além do Azure. Por exemplo, os aplicativos em seus lojas de varejo usam a Cortana para ajudar os funcionários das lojas a localizar os itens rapidamente.

Escolha a melhor resposta para cada pergunta. Em seguida, selecione **Verificar suas respostas**.







**Resumo**

Neste módulo, você aprendeu sobre a abordagem da Microsoft à privacidade, à segurança e à conformidade. Você explorou recursos específicos dos serviços online, incluindo o Azure, e como governos podem usar o Azure para atender às suas necessidades específicas de segurança e conformidade.

Agora, a equipe de segurança da Tailwind Traders tem um melhor entendimento de quais recursos estão disponíveis para ajudá-los a proteger seus dados na nuvem e a manter a conformidade:

* A [Política de Privacidade da Microsoft](https://privacy.microsoft.com/privacystatement) proporciona confiança na forma como a Microsoft coleta, protege e usa dados do cliente.
* A [Central de Confiabilidade](https://www.microsoft.com/trustcenter) fornece documentação sobre padrões de conformidade e sobre como o Azure pode dar suporte à sua empresa.
* A [documentação de conformidade do Azure](https://docs.microsoft.com/pt-br/azure/compliance/) inclui informações detalhadas sobre a conformidade e os padrões legais e regulatórios no Azure.

Tenha em mente que o status de conformidade dos produtos e serviços do Azure não implica automaticamente conformidade para o serviço ou aplicativo que você cria ou hospeda no Azure. Você é responsável por garantir a conformidade com os padrões legais e regulatórios que precisa seguir.

A maioria dos serviços são os mesmos no Azure Government e no Azure global. Entretanto, há algumas diferenças das quais você deve estar ciente. Para saber mais, [compare o Azure Government e o Azure global](https://docs.microsoft.com/pt-br/azure/azure-government/compare-azure-government-global-azure).