**Criar uma estratégia de governança de nuvem no Azure**

Saiba como acessar políticas, bloqueios de recursos e marcas, além de descobrir como os serviços do Azure, como o Azure Policy e o Azure Blueprints, podem ajudar você a criar uma estratégia de governança de nuvem abrangente.

## Objetivos de aprendizagem

Depois de concluir este módulo, você poderá:

* Tomar decisões organizacionais sobre seu ambiente de nuvem usando o Cloud Adoption Framework para Azure.
* Definir quem pode acessar recursos de nuvem usando o controle de acesso baseado em função do Azure.
* Aplique um bloqueio de recurso para evitar a exclusão acidental dos recursos do Azure.
* Aplique marcas aos recursos do Azure para ajudar a descrever a finalidade deles.
* Controle e audite como os recursos são criados usando o Azure Policy.
* Habilite a governança em escala em várias assinaturas do Azure usando o Azure Blueprints.

# Introdução

O termo *governança* descreve o processo geral de estabelecer regras e políticas e garantir que elas sejam impostas.

Durante a execução na nuvem, uma boa estratégia de governança ajuda você a manter o controle sobre os aplicativos e os recursos que você gerencia na nuvem. Manter o controle sobre o seu ambiente garante que você permaneça em conformidade com:

* Padrões do setor, como o [PCI DSS](https://docs.microsoft.com/pt-br/microsoft-365/compliance/offering-pci-dss).
* Padrões corporativos ou organizacionais, como a garantia de que os dados da rede são criptografados.

A governança é mais benéfica quando você tem:

* Várias equipes de engenharia trabalhando no Azure.
* Várias assinaturas a serem gerenciadas.
* Requisitos regulatórios que precisam ser impostos.
* Padrões que precisam ser seguidos para todos os recursos de nuvem.

## **Conheça a Tailwind Traders**

A [Tailwind Traders](https://www.tailwindtraders.com/" \t "az-portal) é um varejista fictício de materiais para reforma e construção. A empresa opera lojas de varejo de ferragens em todo o mundo e online.

Os diferenciais da Tailwind Traders são os preços competitivos, as entregas rápidas e a ampla gama de itens. Eles estão examinando as tecnologias de nuvem para aprimorar as operações de negócios e dar suporte à expansão para novos mercados. Ao migrar para a nuvem, a empresa pretende aprimorar a experiência de compra para se diferenciar ainda mais dos concorrentes.

## Como a Tailwind Traders aumentará a agilidade mantendo o controle?

A Tailwind Traders continua a migração para a nuvem. Para seu datacenter existente, as equipes de desenvolvimento e teste precisam enviar tíquetes de suporte a fim de solicitar acesso aos componentes de rede, armazenamento e máquinas virtuais. Para comprar, provisionar e configurar esses componentes, a equipe de TI pode levar de duas semanas a dois meses.

Ao trabalhar na nuvem, você tem, essencialmente, acesso imediato aos componentes de computação, armazenamento e rede. Muitos tipos de grupos e usuários, incluindo pessoas de desenvolvimento, teste, operações e equipes de segurança, têm o potencial de receber acesso direto aos recursos de nuvem.

No futuro, a Tailwind Traders pode impor processos semelhantes que impedem que as equipes criem ou configurem recursos diretamente no Azure, de maneira semelhante à abordagem existente em que a TI central provisiona a infraestrutura. Mas a empresa sabe que essas restrições reduzem a agilidade da equipe e a capacidade de inovação. Como ela pode promover a inovação e ainda manter o controle?

Neste módulo, você ajudará a empresa a explorar as maneiras pelas quais ela pode impor padrões, capacitando as equipes a criar e gerenciar os recursos de nuvem de que precisam.

## Objetivos de aprendizagem

Depois de concluir este módulo, você poderá:

* Tomar decisões organizacionais sobre seu ambiente de nuvem usando o Cloud Adoption Framework para Azure.
* Definir quem pode acessar recursos de nuvem usando o controle de acesso baseado em função do Azure.
* Aplique um bloqueio de recurso para evitar a exclusão acidental dos recursos do Azure.
* Aplique marcas aos recursos do Azure para ajudar a descrever a finalidade deles.
* Controle e audite como os recursos são criados usando o Azure Policy.
* Habilite a governança em escala em várias assinaturas do Azure usando o Azure Blueprints.

# Controlar o acesso a recursos de nuvem usando o controle de acesso baseado em função do Azure

Quando você tem várias equipes de TI e engenharia, como é possível controlar o acesso que eles têm aos recursos no seu ambiente de nuvem? É uma boa prática de segurança conceder aos usuários apenas os direitos de que precisam para executar o trabalho e somente aos recursos relevantes.

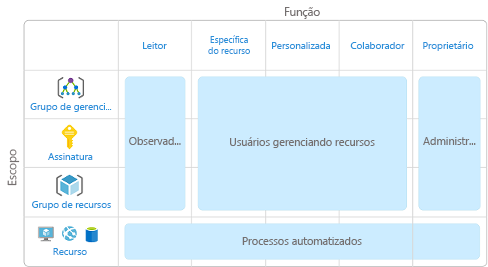
Em vez de definir os requisitos de acesso detalhados para cada indivíduo e atualizar os requisitos de acesso quando outros recursos são criados, o Azure permite controlar o acesso por meio do [RBAC do Azure](https://docs.microsoft.com/pt-br/azure/role-based-access-control/overview) (controle de acesso baseado em função do Azure).

O Azure fornece funções internas que descrevem regras de acesso comuns para os recursos de nuvem. Você também pode definir suas funções. Cada função tem um conjunto associado de permissões de acesso relacionadas a essa função. Quando você atribui indivíduos ou grupos a uma ou mais funções, eles recebem todas as permissões de acesso associadas.

## Como o controle de acesso baseado em função é aplicado aos recursos?

O controle de acesso baseado em função é aplicado a um escopo, que é um recurso ou um conjunto de recursos ao qual esse acesso se aplica.

Este é um diagrama que mostra a relação entre as funções e os escopos.



Os escopos incluem:

* Um grupo de gerenciamento (uma coleção de várias assinaturas).
* Uma assinatura única.
* Um grupo de recursos.
* Um recurso individual.

Os Observadores, os Usuários que gerenciam recursos, os Administradores e os Processos automatizados ilustram os tipos de usuários ou contas que normalmente são atribuídos a cada uma das várias funções.

Quando você permite acesso a um escopo pai, essas permissões são herdadas por todos os escopos filho. Por exemplo:

* Quando você atribui a função [Proprietário](https://docs.microsoft.com/azure/role-based-access-control/built-in-roles#owner) a um usuário no escopo do grupo de gerenciamento, esse usuário pode gerenciar tudo em todas as assinaturas dentro do grupo de gerenciamento.
* Quando você atribui a função [Leitor](https://docs.microsoft.com/azure/role-based-access-control/built-in-roles#reader) a um grupo no escopo da assinatura, os membros desse grupo podem ver todos os grupos de recursos e os recursos na assinatura.
* Quando você atribui a função [Colaborador](https://docs.microsoft.com/azure/role-based-access-control/built-in-roles#contributor) a um aplicativo no escopo do grupo de recursos, o aplicativo pode gerenciar os recursos de todos os tipos nesse grupo de recursos, mas não outros grupos de recursos na assinatura.

## Quando devo usar o RBAC do Azure?

Use o RBAC do Azure quando precisar:

* Permitir que um usuário gerencie VMs em uma assinatura e outro usuário gerencie redes virtuais.
* Permitir que um grupo de Administradores de Banco de Dados gerencie bancos de dados SQL em uma assinatura.
* Permitir que um usuário gerencie todos os recursos em um grupo de recursos, como máquinas virtuais, sites e sub-redes.
* Permitir que um aplicativo acesse todos os recursos em um grupo de recursos.

Esses são apenas alguns exemplos. Você encontrará a lista completa de funções internas no final deste módulo.

## Como o RBAC do Azure é imposto?

O RBAC do Azure é imposto em qualquer ação iniciada em um recurso do Azure que passa pelo Azure Resource Manager. O Resource Manager é um serviço de gerenciamento que fornece um modo de organizar e proteger seus recursos de nuvem.

Normalmente, você acessa o Resource Manager no portal do Azure, no Azure Cloud Shell, no Azure PowerShell e na CLI do Azure. O RBAC do Azure não impõe permissões de acesso no nível do aplicativo nem dos dados. A segurança do aplicativo precisa ser realizada pelo aplicativo.

O RBAC usa um modelo de permissão. Quando você recebe uma função, o RBAC permite que você execute determinadas ações, como leitura, gravação ou exclusão. Se uma atribuição de função conceder a você permissões de leitura em um grupo de recursos e outra atribuição de função conceder a você permissões de gravação no mesmo grupo de recursos, você terá permissões de gravação e leitura nesse grupo de recursos.

## A quem o RBAC do Azure se aplica?

Você pode aplicar o RBAC do Azure a uma pessoa ou a um grupo. Você também pode aplicar o RBAC do Azure a outros tipos de identidades especiais, como entidades de serviço e identidades gerenciadas. Esses tipos de identidade são usados por aplicativos e serviços para automatizar o acesso aos recursos do Azure.

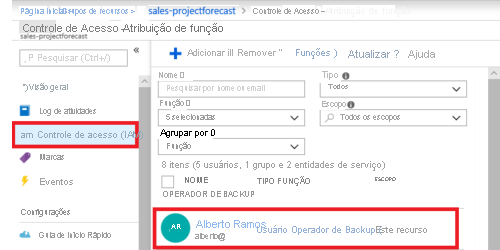
A Tailwind Traders tem as seguintes equipes com interesse em alguma parte do ambiente de TI geral:

* Administradores de TI Essa equipe tem a propriedade máxima dos ativos de tecnologia, tanto localmente quanto na nuvem. A equipe requer controle total de todos os recursos.
* Backup e recuperação de desastre Essa equipe é responsável por gerenciar a integridade de backups regulares e invocar as recuperações de dados ou de sistemas.
* Custos e cobrança As pessoas da equipe acompanham e relatam gastos relacionados à tecnologia. Elas também gerenciam os orçamentos internos da organização.
* Operações de segurança Essa equipe monitora e responde a incidentes de segurança relacionados à tecnologia. A equipe requer acesso contínuo aos arquivos de log e aos alertas de segurança.

## Como fazer para gerenciar as permissões do RBAC do Azure?

Gerencie as permissões de acesso no painel **Controle de Acesso (IAM)** no portal do Azure. Esse painel mostra quem tem acesso a qual escopo e quais funções se aplicam. Você também pode permitir ou remover o acesso nesse painel.

A captura de tela a seguir mostra um exemplo do painel **Controle de acesso (IAM)** para um grupo de recursos. Neste exemplo, Carlos Lima recebeu a função **Operador de Backup** no grupo de recursos.



# Impedir alterações acidentais usando bloqueios de recursos

Um [bloqueio de recurso](https://docs.microsoft.com/pt-br/azure/azure-resource-manager/management/lock-resources) impede que os recursos sejam excluídos ou alterados acidentalmente.

Mesmo com as políticas do controle de acesso baseado em função do Azure (RBAC do Azure) em vigor, ainda há um risco de que as pessoas com o nível correto de acesso possam excluir recursos de nuvem críticos. Imagine um bloqueio de recurso como um sistema de aviso que lembra você de que um recurso não deve ser excluído nem alterado.

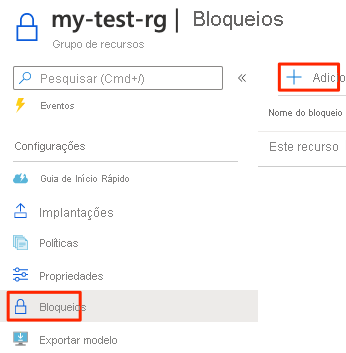
Por exemplo, na Tailwind Traders, um administrador de TI estava executando a limpeza de rotina de recursos não utilizados no Azure. O administrador excluiu acidentalmente recursos que pareciam não ser utilizados. Mas esses recursos eram críticos para um aplicativo que é usado para promoções sazonais. Como os bloqueios de recursos podem ajudar a evitar que esse tipo de incidente ocorra no futuro?

## Como fazer para gerenciar os bloqueios de recursos?

Gerencie os bloqueios de recursos no portal do Azure, no PowerShell, na CLI do Azure ou em um modelo do Azure Resource Manager.

Para ver, adicionar ou excluir bloqueios no portal do Azure, acesse a seção **Configurações** do painel **Configurações** de um recurso no portal do Azure.

Veja a seguir um exemplo que mostra como adicionar um bloqueio de recurso no portal do Azure. Você aplicará um bloqueio de recurso semelhante na próxima parte.



## Quais níveis de bloqueio estão disponíveis?

Você pode aplicar bloqueios a uma assinatura, a um grupo de recursos ou a um recurso individual. É possível definir o nível de bloqueio como **CanNotDelete** ou **ReadOnly**.

* **CanNotDelete** significa que as pessoas autorizadas ainda podem ler e modificar um recurso, mas não podem excluir o recurso sem antes remover o bloqueio.
* **ReadOnly** significa que pessoas autorizadas podem ler um recurso, mas não podem excluir nem alterar o recurso. A aplicação desse bloqueio é como restringir todos os usuários autorizados às permissões concedidas pela função **Leitor** no RBAC do Azure.

## Como fazer para excluir ou alterar um recurso bloqueado?

Embora o bloqueio ajude a evitar alterações acidentais, você ainda poderá fazer alterações seguindo um processo de duas etapas.

Para modificar um recurso bloqueado, primeiro, você precisará remover o bloqueio. Depois de remover o bloqueio, aplique qualquer ação que você tenha permissões para executar. Essa etapa adicional permite que a ação seja executada, mas ajuda a proteger os administradores de fazer algo não pretendido.

Os bloqueios de recursos se aplicam independentemente das permissões de RBAC. Mesmo que você seja o proprietário do recurso, ainda precisará remover o bloqueio para realizar a atividade bloqueada.

## Combinar bloqueios de recursos com o Azure Blueprints

E se um administrador de nuvem excluir acidentalmente um bloqueio de recurso? Se o bloqueio de recurso for removido, os recursos associados a eles poderão ser alterados ou excluídos.

Para tornar o processo de proteção mais robusto, você pode combinar bloqueios de recursos com o Azure Blueprints. O Azure Blueprints permite que você defina o conjunto de recursos padrão de recursos do Azure necessário para a sua organização. Por exemplo, você pode definir um blueprint que especifica que determinado bloqueio de recurso precisa existir. O Azure Blueprints poderá substituir automaticamente o bloqueio de recurso se esse bloqueio for removido.

Você aprenderá mais sobre o Azure Blueprints mais adiante neste módulo.

# Organizar seus recursos do Azure usando marcas

À medida que o seu uso de nuvem aumenta, passa a ser cada vez mais importante manter-se organizado. Uma boa estratégia de organização ajuda você a entender o seu uso da nuvem e pode ajudar a gerenciar os custos.

Por exemplo, conforme a Tailwind Traders cria maneiras de implantar aplicativos no Azure, ela precisa encontrar uma forma de marcar os ambientes de teste para identificar e excluir com facilidade os recursos nesses ambientes quando eles não são mais necessários.

Uma forma de organizar os recursos relacionados é colocá-los nas próprias assinaturas. Use também grupos de recursos para gerenciar os recursos relacionados. As *marcas* de recursos são outra maneira de organizar os recursos. As marcas fornecem informações extras ou metadados sobre os recursos. Esses metadados são úteis para:

* **Gerenciamento de recursos** As marcas permitem que você localize em recursos associados a cargas de trabalho, ambientes, unidades de negócios e proprietários específicos e realize ações nesses recursos.
* **Gerenciamento e otimização de recursos** As marcas permitem agrupar os recursos para que você possa relatar custos, alocar centros de custos internos, acompanhar orçamentos e prever o custo estimado.
* **Gerenciamento de operações** As marcas permitem que você agrupe os recursos de acordo com o grau de importância da disponibilidade deles para os seus negócios. Esse agrupamento ajuda você a formular SLAs (Contratos de Nível de Serviço). Um SLA é uma garantia de tempo de atividade ou desempenho acordada entre você e seus usuários.
* **Segurança** As marcas permitem que você classifique os dados pelo nível de segurança, como *público* ou *confidencial*.
* **Governança e conformidade regulatória** As marcas permitem que você identifique recursos que se alinham com os requisitos de conformidade regulatória ou de governança, como a ISO 27001. Elas também podem fazer parte dos seus esforços de imposição de padrões. Por exemplo, você pode exigir que todos os recursos sejam marcados com um proprietário ou um nome de departamento.
* **Automação e otimização de carga de trabalho** As marcas podem ajudar você a visualizar todos os recursos que participam de implantações complexas. Por exemplo, você pode marcar um recurso com o nome da carga de trabalho ou do aplicativo associado e usar um software como o Azure DevOps para executar tarefas automatizadas nesses recursos.

## Como fazer para gerenciar marcas de recursos?

Você pode adicionar, modificar ou excluir marcas de recursos por meio do PowerShell, da CLI do Azure, dos modelos do Azure Resource Manager, da API REST ou do portal do Azure.

Você também pode gerenciar marcas usando o Azure Policy. Por exemplo, você pode aplicar marcas a um grupo de recursos, mas essas marcas não são aplicadas automaticamente aos recursos nesse grupo de recursos. Você pode usar o Azure Policy para fazer com que um recurso herde as mesmas marcas do grupo de recursos pai. Você aprenderá mais sobre o Azure Policy mais adiante neste módulo.

Use também o Azure Policy para impor regras e convenções de marcação. Por exemplo, exija que determinadas marcas sejam adicionadas aos novos recursos à medida que eles forem provisionados. Defina também regras que reaplicam as marcas removidas.

## Um exemplo de estrutura de marcação

Uma marca de recurso consiste em um nome e um valor. Você pode atribuir uma ou mais marcas a cada recurso do Azure.

Depois de examinar os próprios requisitos de negócios, a Tailwind Traders decide usar as marcas a seguir.

**Nome**

**Valor**

**AppName**

O nome do aplicativo do qual o recurso faz parte.

**CostCenter**

O código do centro de custo interno.

**Proprietário**

O nome do proprietário de negócios responsável pelo recurso.

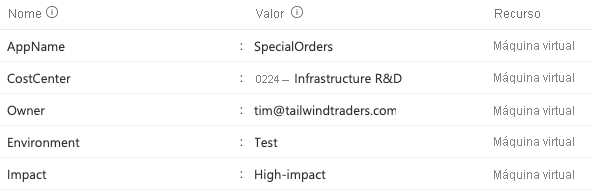
**Ambiente**

Um nome de ambiente, como "Prod", "Dev" ou "Test".

**Impacto**

O grau de importância do recurso para as operações de negócios, como "Crítico", "De alto impacto" ou "De baixo impacto".

Este é um exemplo que mostra essas marcas conforme elas são aplicadas a uma máquina virtual durante o provisionamento.



A equipe da Tailwind Traders pode executar consultas, por exemplo, no PowerShell ou na CLI do Azure, para listar todos os recursos que contêm essas marcas.

Tenha em mente que não é necessário impor a presença de uma marca específica em todos os recursos. Por exemplo, você pode decidir que apenas os recursos críticos tenham a marca **Impact**. Em seguida, todos os recursos não marcados não serão considerados críticos.

# Controlar e auditar seus recursos usando o Azure Policy

Em um exercício anterior deste módulo, você identificou seus requisitos de governança e de negócios. Como garantir que seus recursos permaneçam em conformidade? Você poderá receber um alerta se a configuração de um recurso for alterada?

O [Azure Policy](https://azure.microsoft.com/services/azure-policy) é um serviço do Azure que permite criar, atribuir e gerenciar políticas que controlam ou auditam os recursos. Essas políticas impõem regras diferentes sobre as configurações dos recursos, de modo que essas configurações permaneçam em conformidade com os padrões corporativos.

## Como o Azure Policy define as políticas?

O Azure Policy permite que você defina políticas individuais e grupos de políticas relacionadas, conhecidas como iniciativas. O Azure Policy avalia seus recursos e realça os que não estão em conformidade com as políticas criadas por você. Ele também pode impedir a criação de recursos sem conformidade.

O Azure Policy vem com definições de iniciativa e política internas para Armazenamento, Rede, Computação, Central de Segurança e Monitoramento. Por exemplo, se você definir uma política que permita que apenas um determinado tamanho de SKU (unidade de manutenção de estoque) para VMs (máquinas virtuais) seja usado em seu ambiente, essa política será invocada quando você criar VMs e sempre que você redimensionar as VMs existentes. O Azure Policy também avalia e monitora todas as VMs atuais do ambiente.

Em alguns casos, ele pode corrigir automaticamente os recursos e as configurações sem conformidade para garantir a integridade do estado dos recursos. Por exemplo, se todos os recursos de determinado grupo de recursos precisarem ser marcados com **AppName** e um valor igual a "SpecialOrders", o Azure Policy reaplicará automaticamente essa marca se ela estava ausente.

Além disso, o Azure Policy se integra ao Azure DevOps aplicando as políticas de pipeline de entrega e integração contínua que se pertencem às fases pré e pós-implantação dos seus aplicativos.

## Azure Policy em ação

A implementação de uma política no Azure Policy envolve três tarefas:

1. Criar uma definição da política.
2. Atribuir a definição aos recursos.
3. Examinar os resultados da avaliação.

Vamos examinar cada etapa mais detalhadamente.

### Tarefa 1. Criar uma definição da política

Uma definição de política expressa o que avaliar e qual ação será tomada. Por exemplo, você pode impedir que as VMs sejam implantadas em determinadas regiões do Azure. Você também pode auditar suas contas de armazenamento para confirmar se elas só aceitam conexões de redes permitidas.

Cada definição de política tem condições sob as quais ela é imposta. Uma definição de política também tem um efeito de acompanhamento que ocorre quando as condições são atendidas. Estes são alguns exemplos de definições de política:

* **SKUs de máquina virtual permitidos** Esta política permite que você especifique um conjunto de SKUs de VM que sua organização pode implantar.
* **Locais permitidos** Esta política permite que você restrinja os locais que sua organização pode especificar quando implanta recursos. Seu efeito é usado para impor seus requisitos de conformidade geográfica.
* **A MFA deve ser habilitada nas contas com permissões de gravação na assinatura** Essa política exige que a MFA (autenticação multifator) esteja habilitada em todas as contas de assinaturas com privilégios de gravação, a fim de impedir uma violação de contas ou de recursos.
* **O CORS não deve permitir que todos os recursos tenham acesso aos seus aplicativos Web** O CORS (compartilhamento de recurso entre origens) é um recurso HTTP que permite que um aplicativo Web em execução em um domínio acesse recursos em outro domínio. Por motivos de segurança, os navegadores da Web modernos restringem o cross-site scripting por padrão. Essa política permite que só os domínios necessários interajam com o aplicativo Web.
* **As atualizações do sistema devem ser instaladas em seus computadores** Essa política permite que a Central de Segurança do Azure recomende atualizações ausentes do sistema de segurança nos seus servidores.

### Tarefa 2. Atribuir a definição aos recursos

Para implementar suas definições de política, atribua definições aos recursos. Uma atribuição de política é uma definição de política que ocorre em um escopo específico. Esse escopo pode ser um grupo de gerenciamento (uma coleção de várias assinaturas), uma assinatura única ou um grupo de recursos.

As atribuições de política são herdadas por todos os recursos filho no escopo. Se uma política for aplicada a um grupo de recursos, ela será aplicada a todos os recursos desse grupo de recursos. Você poderá excluir um subescopo da atribuição de política se houver recursos filho específicos que você precisará isentar da atribuição de política.

### Tarefa 3. Examinar os resultados da avaliação

Quando uma condição é avaliada em relação aos recursos existentes, cada recurso é marcado como em conformidade ou sem conformidade. Você pode examinar os resultados da política sem conformidade e executar qualquer ação necessária.

A avaliação de política ocorre uma vez por hora. Se você fizer alterações na definição de política e criar uma atribuição de política, essa política avaliará seus recursos dentro da próxima hora.

## O que são iniciativas do Azure Policy?

Uma iniciativa do Azure Policy é uma forma de agrupar políticas relacionadas. A definição de iniciativa contém todas as definições de política para ajudar a acompanhar seu estado de conformidade para atingir uma meta maior.

Por exemplo, o Azure Policy inclui uma iniciativa chamada **Habilitar o Monitoramento na Central de Segurança do Azure**. A meta dela é monitorar todas as recomendações de segurança disponíveis para todos os tipos de recursos do Azure na Central de Segurança do Azure.

Com essa iniciativa, as seguintes definições de política são incluídas:

* **Monitorar um banco de dados SQL não criptografado na Central de Segurança** Essa política monitora servidores e bancos de dados SQL não criptografados.
* **Monitorar vulnerabilidades de SO na Central de Segurança** Esta política monitora servidores que não atendem à linha de base de vulnerabilidade do sistema operacional configurado.
* **Monitorar o Endpoint Protection ausente na Central de Segurança** Essa política monitora servidores que não têm um agente de proteção de ponto de extremidade instalado.

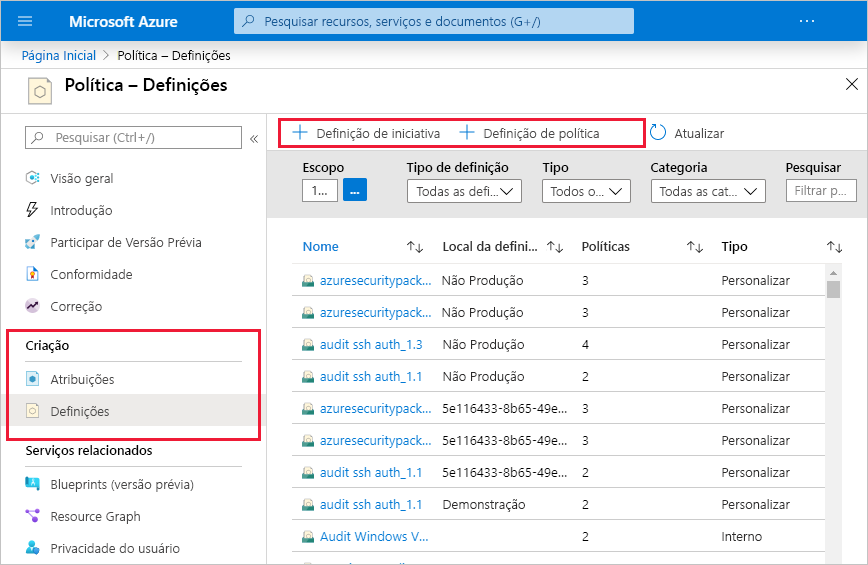
Na verdade, a iniciativa **Habilitar o Monitoramento na Central de Segurança do Azure** contém mais de 100 definições de política separadas.

O Azure Policy também inclui iniciativas que dão suporte a padrões de conformidade regulatória, como o HIPAA e a ISO 27001.

### Como fazer para definir uma iniciativa?

Você define iniciativas usando o portal do Azure ou ferramentas de linha de comando. No portal do Azure, você pode pesquisar a lista de iniciativas internas do Azure. Você também pode criar sua própria definição de política personalizada.

A imagem a seguir mostra alguns exemplos de iniciativas do Azure Policy no portal do Azure.



### Como fazer para atribuir uma iniciativa?

Assim como uma atribuição de política, uma atribuição de iniciativa é uma definição de iniciativa atribuída a um escopo específico de um grupo de gerenciamento, uma assinatura ou um grupo de recursos.

Mesmo que você tenha somente uma política, uma iniciativa permite aumentar o número de políticas ao longo do tempo. Como a iniciativa associada permanece atribuída, é mais fácil adicionar e remover políticas sem a necessidade de alterar a atribuição de política aos seus recursos.

# Controlar várias assinaturas usando o Azure Blueprints

Até agora, você explorou vários recursos do Azure que podem ajudá-lo a implementar suas decisões de governança, monitorar a conformidade dos seus recursos de nuvem e controlar o acesso e proteger recursos críticos contra a exclusão acidental.

O que acontece quando seu ambiente de nuvem começa a crescer além de apenas uma assinatura? Como você pode escalar a configuração desses recursos, sabendo que eles precisam ser impostos para os recursos em novas assinaturas?

Em vez de ter que configurar recursos como o Azure Policy para cada nova assinatura, com o [Azure Blueprints](https://azure.microsoft.com/services/blueprints), você pode definir um conjunto repetível de ferramentas de governança e de recursos padrão do Azure necessário para a sua organização. Assim, as equipes de desenvolvimento podem criar e implementar rapidamente novos ambientes, sabendo que eles estão sendo criados de acordo com as especificações da organização, com um conjunto de componentes internos que aceleram as fases de desenvolvimento e implantação.

O Azure Blueprints orquestra a implantação de vários modelos de recursos e outros artefatos, como:

* Atribuições de função
* Atribuições de política
* Modelos do Azure Resource Manager
* Grupos de recursos

## Azure Blueprints em ação

Ao formar uma equipe de centro de excelência em nuvem ou uma equipe de custodiantes da nuvem, essa equipe pode usar o Azure Blueprints para escalar as práticas de governança em toda a organização.

A implementação de um blueprint no Azure Blueprints envolve estas três etapas:

1. Criar um Azure Blueprint.
2. Atribuir o blueprint.
3. Acompanhar as atribuições de blueprint.

Com o Azure Blueprints, a relação entre a definição do blueprint (o que deve ser implantado) e a atribuição do blueprint (o que foi implantado) é preservada. Em outras palavras, o Azure cria um registro que associa um recurso ao blueprint que o define. Essa conexão ajuda você a acompanhar e auditar suas implantações.

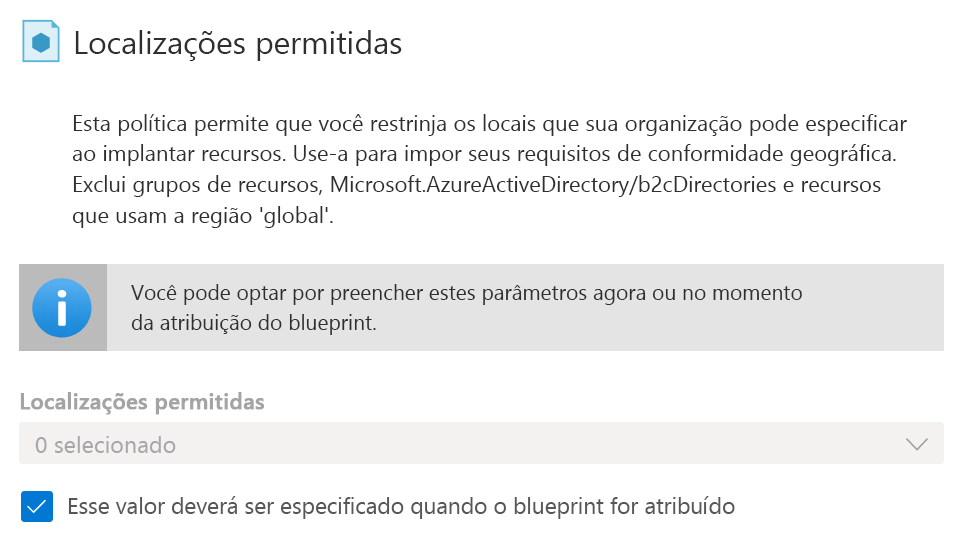
Os blueprints também têm controle de versão. O controle de versão permite que você acompanhe e comente as alterações no blueprint.

## O que são artefatos de blueprint?

Cada componente na definição de blueprint é conhecido como um artefato.

É possível que os artefatos não tenham parâmetros adicionais (configurações). Um exemplo é a política **Implantar detecção de ameaças nos servidores SQL**, que não requer nenhuma configuração adicional.

Os artefatos também podem conter um ou mais parâmetros que você pode configurar. A captura de tela a seguir mostra a política **Localizações permitidas**. Essa política inclui um parâmetro que especifica as localizações permitidas.



Você pode especificar o valor de um parâmetro ao criar a definição de blueprint ou atribuí-la a um escopo. Com isso, você pode manter um blueprint padrão, mas ter a flexibilidade de especificar os parâmetros de configuração relevantes em cada escopo no qual a definição é atribuída.

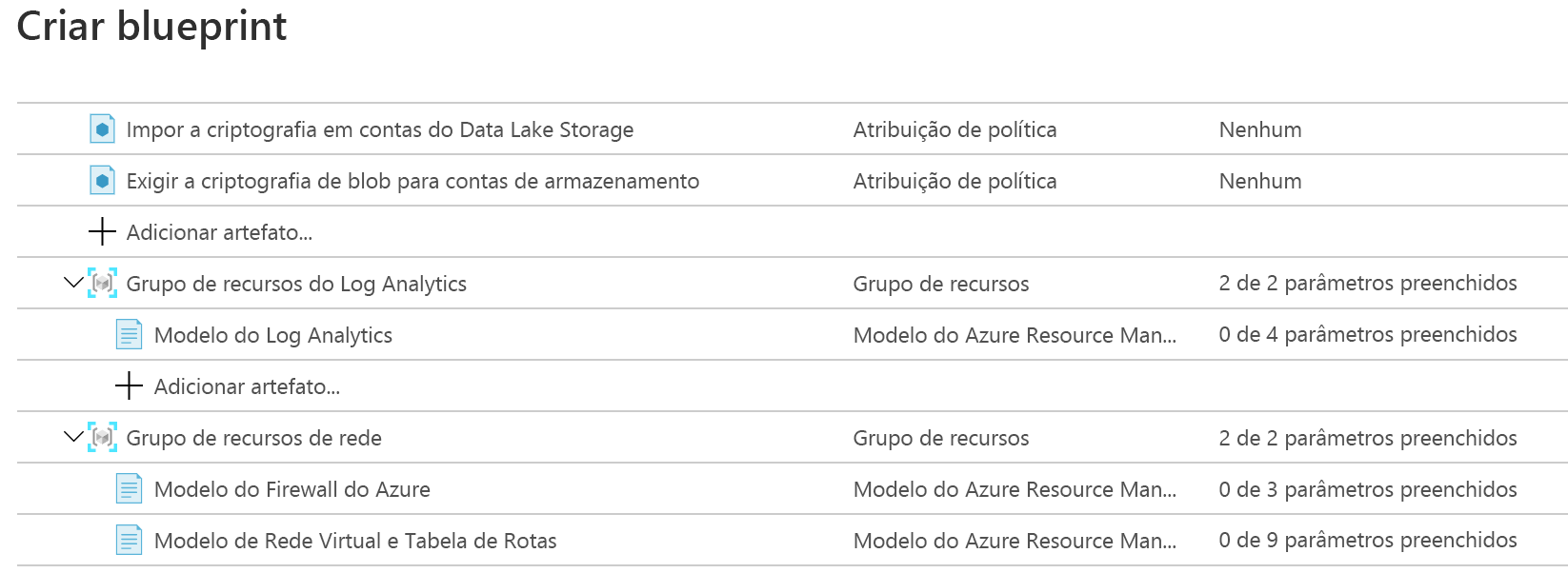
## Como a Tailwind Traders usará o Azure Blueprints para ficar em conformidade com a ISO 27001?

A [ISO 27001](https://www.iso.org/isoiec-27001-information-security.html) é um padrão que se aplica à segurança de sistemas de TI publicado pela Organização Internacional de Normalização. Como parte do processo de qualidade, a Tailwind Traders deseja se certificar que está em conformidade com esse padrão. O Azure Blueprints tem várias definições de blueprint internas relacionadas à ISO 27001.

Como administrador de TI, você decide investigar a definição da **ISO 27001: Blueprint de Serviços Compartilhados**. Esta é uma estrutura do seu plano.

1. Definir um grupo de gerenciamento chamado **PROD-MG**. Lembre-se de que um grupo de gerenciamento gerencia o acesso, as políticas e a conformidade em várias assinaturas do Azure. Cada nova assinatura do Azure é adicionada a esse grupo de gerenciamento no momento da criação.
2. Criar uma definição de blueprint com base no modelo **ISO 27001: Modelo**Serviços compartilhados do Blueprint. Em seguida, publique o blueprint.
3. Atribuir o blueprint ao grupo de gerenciamento **PROD-MG**.

A imagem a seguir mostra os artefatos que são criados quando você executa um blueprint ISO 27001 com base em um modelo.



Você verá que o modelo de blueprint contém atribuições de política, modelos do Resource Manager e grupos de recursos. O blueprint implanta esses artefatos nas assinaturas existentes do grupo de gerenciamento **PROD-MG**. Ele também implanta esses artefatos nas novas assinaturas, à medida que elas são criadas e adicionadas ao grupo de gerenciamento.

**Acelere sua jornada de adoção da nuvem usando o Cloud Adoption Framework para Azure**

Concluído100 XP

* 3 minutos

O [Cloud Adoption Framework para Azure](https://docs.microsoft.com/pt-br/azure/cloud-adoption-framework/) fornece diretrizes comprovadas para ajudar com a sua jornada de adoção da nuvem. O Cloud Adoption Framework ajuda você a criar e implementar as estratégias de negócios e de tecnologia necessárias para ter sucesso na nuvem.

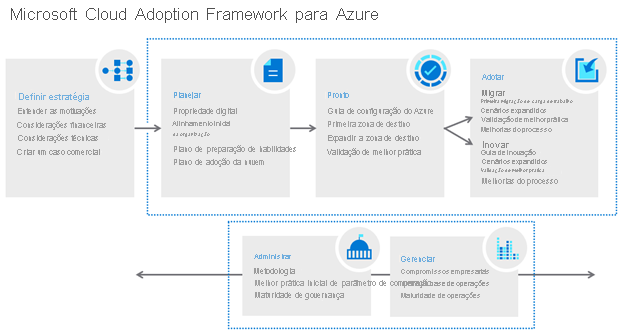
A Tailwind Traders precisa controlar o ambiente de nuvem para ficar em conformidade com vários padrões do setor, mas não tem certeza de onde começar. Ela tem requisitos de negócios e sabe como esses requisitos se relacionam com suas cargas de trabalho locais. Esses requisitos também devem ser atendidos por todas as cargas de trabalho que ela executa na nuvem.

Você recebeu a tarefa de investigar o que está disponível no Azure e definir e implementar a estratégia de governança da Tailwind Traders. Você decide começar com o Cloud Adoption Framework.

## O que há no Cloud Adoption Framework?

Conforme mencionado no vídeo, o Cloud Adoption Framework consiste em ferramentas, documentação e práticas comprovadas. O Cloud Adoption Framework inclui estas fases:

1. Definir sua estratégia.
2. Criar um plano.
3. Preparar sua organização.
4. Adotar a nuvem.
5. Controlar e gerenciar seus ambientes de nuvem.



A fase de controle tem como foco a governança de nuvem. Veja o Cloud Adoption Framework novamente para obter diretrizes recomendadas durante a criação da sua estratégia de governança de nuvem.

Para ajudar a criar sua estratégia de adoção, o Cloud Adoption Framework divide cada fase em exercícios e etapas adicionais. Vamos dar uma olhada rápida em cada estágio.

### Definir sua estratégia

Aqui, você explicará por que está migrando para a nuvem e indicará o que deseja obter com a migração. Você precisa escalar seus negócios para atender à demanda ou alcançar novos mercados? Isso reduzirá os custos ou aumentará a agilidade dos negócios? Ao definir sua estratégia de negócios de nuvem, entenda a [economia de nuvem](https://azure.microsoft.com/overview/cloud-economics), o impacto nos negócios, o tempo de retorno, o alcance global, o desempenho, entre outros.

Aqui estão as etapas desta fase.



**Definir e documentar suas motivações**: reunir-se com os stakeholders e a liderança pode ajudar você a explicar por que está migrando para a nuvem.



**Documentar os resultados dos negócios**: reúna-se com a liderança dos grupos de finanças, marketing, vendas e recursos humanos para ajudar você a documentar suas metas.



**Avalie as considerações financeiras**: avalie os objetivos e identifique o retorno esperado de um investimento específico.



**Entenda as considerações técnicas**: avalie as considerações técnicas por meio da seleção e da conclusão do seu primeiro projeto técnico.

### Criar um plano

Aqui, você criará um plano que mapeia suas metas ambiciosas para ações específicas. Um bom plano ajuda a garantir que os seus esforços sejam mapeados para os resultados de negócios desejados.

Aqui estão as etapas desta fase.

**Propriedade digital**: crie um inventário dos ativos digitais e das cargas de trabalho existentes que você pretende migrar para a nuvem.



**Alinhamento organizacional inicial**: verifique se as pessoas certas estão envolvidas nos seus esforços de migração, do ponto de vista técnico e da governança de nuvem.



**Plano de preparação de habilidades**: crie um plano que ajude os indivíduos a criar as habilidades de que precisam para operar na nuvem.



**Plano de adoção da nuvem**: crie um plano abrangente que reúne as equipes de desenvolvimento, operações e negócios em direção a uma meta de adoção da nuvem compartilhada.



### Preparar sua organização

Aqui, você criará uma zona de destino ou um ambiente na nuvem para começar a hospedar suas cargas de trabalho.

Aqui estão as etapas desta fase.



**Guia de configuração do Azure**: Examine o Guia de Configuração do Azure para se familiarizar com as ferramentas e as abordagens necessárias para criar uma zona de destino.



**Zona de destino do Azure**: comece a criar as assinaturas do Azure que dão suporte a cada uma das principais áreas do seu negócio. Uma zona de destino inclui a infraestrutura de nuvem, bem como funcionalidades de governança, contabilidade e segurança.



**Expandir a zona de destino**: refine sua zona de destino para garantir que ela atende às suas necessidades de operações, governança e segurança.



**Melhores práticas**: comece com as práticas recomendadas e comprovadas para ajudar a garantir que seus esforços de migração para a nuvem sejam escalonáveis e possam ser mantidos.

### Adotar a nuvem

Aqui, você começará a migrar seus aplicativos para a nuvem. Ao longo do caminho, você poderá encontrar maneiras de modernizar seus aplicativos e criar soluções inovadoras que usam os serviços de nuvem.

O Cloud Adoption Framework divide essa fase em duas partes: migração e inovação.

**Migrar**: Aqui estão as etapas na parte de migração desta fase.

**Migrar sua primeira carga de trabalho**: use o guia de migração do Azure para implantar seu primeiro projeto na nuvem.



**Cenários de migração**: use guias detalhados adicionais para explorar cenários de migração mais complexos.



**Melhores práticas**: dê uma olhada na lista de verificação de melhores práticas de migração para a nuvem do Azure para confirmar se você está seguindo as práticas recomendadas.



**Aprimoramentos de processo**: identifique maneiras de escalar o processo de migração, exigindo menos esforço.



**Inovar**: Aqui estão as etapas na parte de inovação desta fase.



**Consenso do valor comercial**: confirme se os investimentos em inovações agregam valor aos negócios e atendem às necessidades dos clientes.



**Guia de inovação do Azure**: use esse guia para acelerar o desenvolvimento e criar um MVP (produto mínimo viável) para a sua ideia.



**Melhores práticas**: confirme se o seu progresso é mapeado para as práticas recomendadas antes de prosseguir.



**Loops de comentários**: pergunte frequentemente aos seus clientes se você está criando algo de que eles precisam.

### Controlar e gerenciar seus ambientes de nuvem

Aqui, você começará a formar suas estratégias de governança e gerenciamento de nuvem. À medida que o estado da nuvem se altera ao longo do tempo, o mesmo ocorrerá com os processos e as políticas de governança da nuvem. Você precisará criar soluções resilientes que sejam constantemente otimizadas.

**Controlar**: Aqui estão as etapas na parte de controle desta fase.

**Metodologia**: considere sua solução de estado final. Em seguida, defina uma metodologia que leve você incrementalmente das primeiras etapas à governança de nuvem completa.



**Parâmetro de comparação**: use a [ferramenta de parâmetro de comparação de governança](https://cafbaseline.com/) para avaliar o estado atual e o estado futuro e estabelecer uma visão para a aplicação da estrutura.



**Base de governança inicial**: crie um MVP que capture as primeiras etapas do plano de governança.



**Aprimorar a base de governança inicial**: adicione iterativamente controles de governança que resolvam os riscos tangíveis à medida que você progride rumo à solução de estado final.



**Gerenciar**: Aqui estão as etapas na parte de gerenciamento desta fase.



**Estabelecer uma linha de base de gerenciamento**: defina seu compromisso mínimo com o gerenciamento de operações. Uma linha de base de gerenciamento é o conjunto mínimo de ferramentas e processos que devem ser aplicados a todos os ativos em um ambiente.



**Definir compromissos empresariais**: Documente as cargas de trabalho compatíveis para estabelecer compromissos operacionais com o negócio e entre em acordo sobre investimentos em gerenciamento de nuvem para cada carga de trabalho.



**Expandir a linha de base de gerenciamento**: aplique as práticas recomendadas para iterar pela linha de base de gerenciamento inicial.



**Operações avançadas e princípios de design**: para cargas de trabalho que exigem um nível mais alto de compromisso de negócios, execute uma análise mais profunda da arquitetura para cumprir seus compromissos de resiliência e confiabilidade.

# Criar uma estratégia de governança de assinatura

No início de qualquer implementação de governança de nuvem, você identifica uma estrutura de organização em nuvem que atende às suas necessidades de negócios. Esta etapa geralmente envolve a formação de uma equipe do centro de excelência na nuvem (também chamada de equipe de habilitação de nuvem ou uma equipe custodiante de nuvem). Essa equipe está capacitada para implementar práticas de governança de um local centralizado para toda a organização.

As equipes costumam iniciar a estratégia de governança do Azure no nível da assinatura. Há três aspectos principais a serem considerados ao criar e gerenciar assinaturas: cobrança, controle de acesso e limites de assinatura.

Vamos examinar cada um desses aspectos mais detalhadamente.

## Cobrança

Você pode criar um relatório de cobrança por assinatura. Caso você tenha vários departamentos e precise fazer um "estorno" dos custos da nuvem, uma solução possível é organizar as assinaturas por departamento ou por projeto.

As marcas de recurso também podem ajudar. Você explorará as marcas mais adiante neste módulo. Quando você define quantas assinaturas são necessárias e como nomeá-las, leve em consideração seus requisitos internos de cobrança.

## Controle de acesso

Uma assinatura é um limite de implantação para os recursos do Azure. Cada assinatura é associada a um locatário do Azure Active Directory. Cada locatário fornece aos administradores a capacidade de configurar o acesso granular por meio de funções definidas usando o controle de acesso baseado em função do Azure.

Quando projetar a arquitetura da assinatura, leve em conta o fator de limite de implantação. Por exemplo, você precisa ter assinaturas separadas para ambientes de desenvolvimento e produção? Com assinaturas separadas, você pode controlar o acesso a cada um separadamente e isolar os recursos uns dos outros.

## Limites de assinatura

As assinaturas também têm algumas limitações de recursos. Por exemplo, o número máximo de circuitos do Azure ExpressRoute na rede por assinatura é 10. Esses limites devem ser considerados durante a fase de design. Se você precisar exceder esses limites, talvez seja necessário adicionar mais assinaturas. Se você atingir um limite rígido máximo, não haverá flexibilidade para aumentá-lo.

Os grupos de gerenciamento também estão disponíveis para auxiliar no gerenciamento de assinaturas. Um grupo de gerenciamento gerencia o acesso, as políticas e a conformidade em várias assinaturas do Azure. Você aprenderá mais sobre os grupos de gerenciamento mais adiante neste módulo.

# Verificação de conhecimentos

Considere este cenário.

A Tailwind Traders criou ambientes para desenvolvimento e teste para seu sistema de comércio eletrônico.

Este é um diagrama que mostra os componentes básicos de computação, de banco de dados e de rede encontrados em cada ambiente.

Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente

Esses ambientes oferecem uma forma para a equipe criar e testar novos recursos de aplicativos. Se você concluiu o módulo [Planejar e gerenciar seus custos do Azure](https://docs.microsoft.com/pt-br/learn/modules/plan-manage-azure-costs/), já viu esse layout.

Embora as equipes de desenvolvimento e teste sejam subordinadas a diferentes departamentos, os dois ambientes existem na mesma assinatura do Azure.

O gerente de TI deseja implementar controles de governança para ajudar a garantir que apenas os usuários autorizados possam acessar esses sistemas. Ter esses controles em vigor também ajudará a acompanhar e gerenciar os custos operacionais.

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

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente  
Uma imagem contendo Linha do tempo

Descrição gerada automaticamente

**Resumo**

Você recebeu a tarefa de definir e implementar a estratégia de governança da Tailwind Traders.

A governança de nuvem exige uma boa coleta de requisitos e análise. A boa notícia é que o Cloud Adoption Framework para Azure pode ajudar você a definir e implementar sua estratégia de governança. Há vários serviços e recursos no Azure que dão suporte a esses esforços:

* O RBAC do Azure (controle de acesso baseado em função do Azure) permite que você crie funções que definem permissões de acesso.
* Os bloqueios de recursos impedem que os recursos sejam excluídos ou alterados acidentalmente.
* As marcas de recursos fornecem informações extras ou metadados sobre os recursos.
* O Azure Policy é um serviço do Azure que permite criar, atribuir e gerenciar políticas que controlam ou auditam os recursos.
* O Azure Blueprints permite que você defina um conjunto repetível de ferramentas de governança e de recursos padrão do Azure necessário para a sua organização.

Com esses pontos em mente, você está pronto para realizar a próxima etapa para a criação de uma boa estratégia de governança de nuvem.