

## Creación de una estrategia de gobernanza en la nube en Azure

### Control del acceso a los recursos en la nube por medio del control de acceso basado en roles de Azure

Cuando tenemos varios equipos de TI e ingeniería, ¿cómo podemos controlar el acceso que tienen a los recursos del entorno de nube? Una buena práctica de seguridad consiste en conceder a los usuarios únicamente los derechos que necesitan para realizar su trabajo, y solo a los recursos pertinentes.

En vez de definir los requisitos de acceso detallados de cada individuo y, posteriormente, ir actualizándolos a medida que se vayan creando más recursos, Azure permite controlar el acceso a través del [control de acceso basado en roles de Azure](#) (RBAC de Azure).

Azure proporciona roles integrados que describen las reglas de acceso comunes de los recursos en la nube. También podemos definir nuestros propios roles. Cada rol tiene un conjunto asociado de permisos de acceso que tienen que ver con ese rol. Cuando se asignan usuarios o grupos a uno o varios roles, reciben todos los permisos de acceso asociados correspondientes.

#### ¿Cómo se aplica el control de acceso basado en roles a los recursos?

El control de acceso basado en roles se aplica a un *ámbito*, que es un recurso o un conjunto de recursos en los que este acceso se permite.

En este diagrama se muestra la relación entre roles y ámbitos.



Los ámbitos pueden ser lo siguiente:

- Un grupo de administración (una colección de varias suscripciones)
- Una sola suscripción
- Un grupo de recursos.
- Un solo recurso

En el diagrama, los *observadores*, los *usuarios que administran recursos*, los *administradores* y los *procesos automatizados* denotan los tipos de usuarios o cuentas que se suelen asignar a cada uno de los distintos roles.

Si se otorga acceso a un ámbito primario, esos permisos se heredan en todos los ámbitos secundarios. Por ejemplo:

- Cuando asignamos el rol [Propietario](#) a un usuario en el ámbito del grupo de administración, dicho usuario podrá administrar todo el contenido de todas las suscripciones dentro de ese grupo de administración.
- Cuando asignamos el rol [Lector](#) a un grupo en el ámbito de suscripción, los miembros de dicho grupo podrán ver todos los grupos de recursos y recursos dentro de esa suscripción.
- Cuando asignamos el rol [Colaborador](#) a una aplicación en el ámbito del grupo de recursos, dicha aplicación podrá administrar los recursos de cualquier tipo dentro de ese grupo de recursos específico, pero no los otros grupos de recursos dentro de esa suscripción.

### ¿Cuándo conviene usar RBAC de Azure?

Usaremos RBAC de Azure cuando necesitemos:

- Permitir que un usuario administre las VM en una suscripción y que otro usuario administre las redes virtuales.
- Permitir a un grupo de administradores de base de datos que administren bases de datos SQL de una suscripción
- Permitir que un usuario administre todos los recursos de un grupo de recursos, como las máquinas virtuales, los sitios web y las subredes
- Permitir que una aplicación acceda a todos los recursos de un grupo de recursos.

Estos son solo algunos ejemplos. Al final de este módulo hay una lista completa de roles integrados.

### ¿Cómo se aplica RBAC de Azure?

RBAC de Azure se aplica a cualquier acción que se inicie en un recurso de Azure que pasa por Azure Resource Manager. Resource Manager es un servicio de administración que proporciona una forma de organizar y proteger nuestros recursos en la nube.

Normalmente, se accede a Resource Manager a través de Azure Portal, Azure Cloud Shell, Azure PowerShell y la CLI de Azure. RBAC de Azure no aplica permisos de acceso en el nivel de aplicación ni de datos. La seguridad de la aplicación debe controlarla la propia aplicación.

RBAC emplea un *modelo de permisos*, es decir, cuando se nos asigna un rol, RBAC *nos permite* realizar determinadas acciones, como leer, escribir o eliminar. Si una asignación de roles nos concede permisos de lectura a un grupo de recursos y otra asignación de roles nos concede permisos de escritura al mismo grupo de recursos, tendremos permisos tanto de lectura como de escritura en ese grupo de recursos.

## ¿A quién se aplica RBAC de Azure?

RBAC de Azure se puede aplicar a una persona individual o a un grupo. También se puede aplicar a otros tipos de identidad especiales, como entidades de servicio e identidades administradas. Las aplicaciones y los servicios usan estos tipos de identidad para automatizar el acceso a los recursos de Azure.

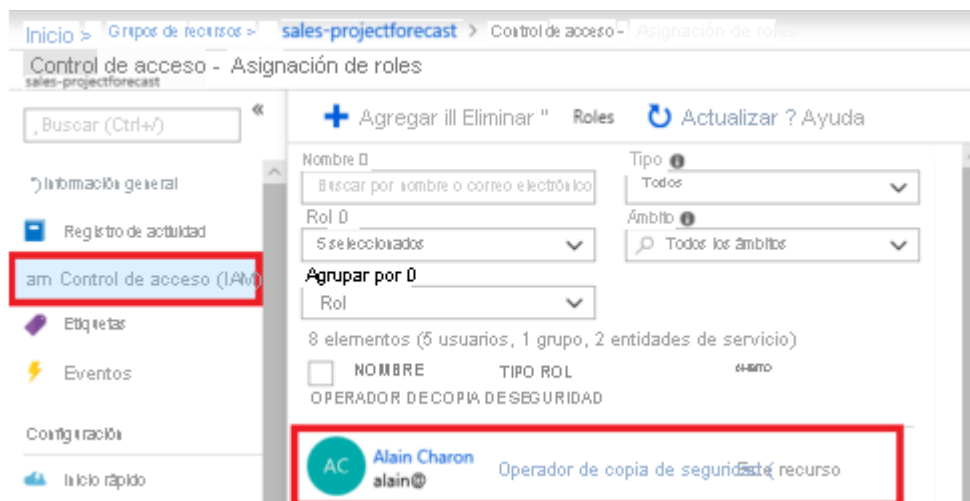
Tailwind Traders tiene los siguientes equipos implicados en alguna parte de su entorno de TI general:

- **Administradores de TI:** este equipo tiene la propiedad definitiva de los recursos tecnológicos, tanto locales como en la nube. El equipo requiere un control completo de todos los recursos.
- **Copia de seguridad y recuperación ante desastres:** este equipo es responsable de administrar el estado de las copias de seguridad periódicas y de invocar cualquier recuperación de datos o del sistema.
- **Coste y facturación:** los miembros de este equipo realizan un seguimiento e informan sobre los gastos relacionados con la tecnología. También administran los presupuestos internos de la organización.
- **Operaciones de seguridad:** este equipo supervisa los incidentes de seguridad relacionados con la tecnología y responde a estos. El equipo requiere acceso continuo a los archivos de registro y a las alertas de seguridad.

## ¿Cómo se administran los permisos de RBAC de Azure?

Los permisos de acceso se administran en el panel **Control de acceso (IAM)** de Azure Portal. En este panel se muestra quién tiene acceso a qué ámbito y qué roles se aplican. En él también puede conceder o quitar cualquier tipo de acceso.

En la siguiente captura de pantalla se muestra un ejemplo del panel **Control de acceso (IAM)** de un grupo de recursos. En este ejemplo, Alain Charon tiene asignado el rol **Operador de copias de seguridad** en ese grupo de recursos.



## Uso de bloqueos de recursos para evitar cambios inintencionados

Los [bloqueos de recursos](#) impiden que se eliminen o modifiquen recursos por error.

Aun cuando haya directivas de control de acceso basado en roles de Azure (RBAC de Azure) en vigor, sigue existiendo el riesgo de que alguien con el nivel de acceso adecuado elimine recursos de nube críticos. Podríamos pensar en un bloqueo de recursos como un sistema de aviso que nos recuerda que un recurso no se debe eliminar o cambiar.

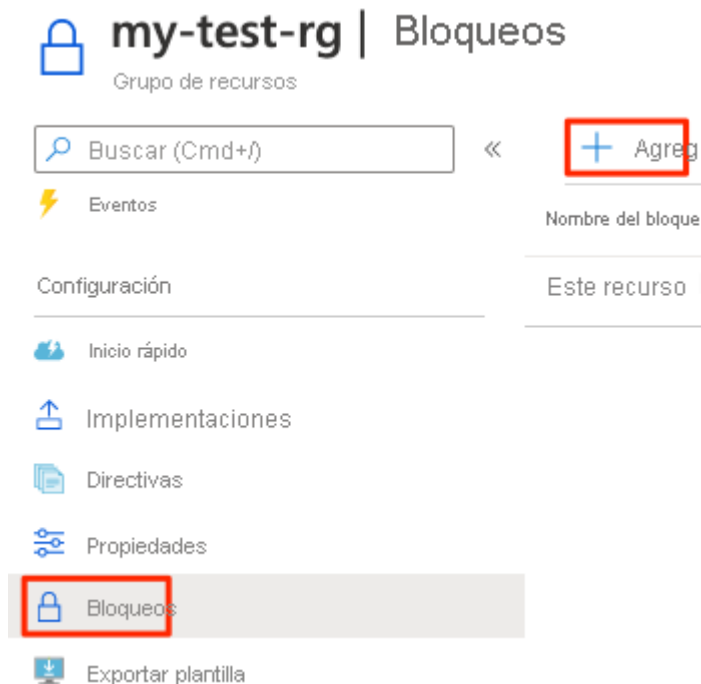
Por ejemplo, en Tailwind Traders, un administrador de TI se encuentra realizando una limpieza rutinaria de recursos no utilizados en Azure y, por error, elimina unos recursos que parecen no estar usándose, pero en realidad son recursos fundamentales en una aplicación que se emplea para promociones estacionales. ¿Cómo impiden los bloqueos de recursos que se produzca este tipo de incidentes en el futuro?

### ¿Cómo se administran los bloqueos de recursos?

Los bloqueos de recursos se pueden administrar en Azure Portal, PowerShell, la CLI de Azure o con una plantilla de Azure Resource Manager.

Para ver, agregar o eliminar bloqueos en Azure Portal, vaya a la sección **Configuración** del panel **Bloqueos** de cualquier recurso en Azure Portal.

En este ejemplo se muestra cómo agregar un bloqueo de recurso desde Azure Portal. En la siguiente unidad pondremos en práctica un bloqueo de recurso similar.



### ¿Qué niveles de bloqueo hay disponibles?

Podemos aplicar bloqueos a una suscripción, a un grupo de recursos o a un recurso individual. Puede establecer el bloqueo de nivel en **CanNotDelete** o **ReadOnly**.

- **CanNotDelete** significa que las personas autorizadas pueden seguir leyendo y modificando un recurso, pero no eliminarlo sin quitar primero el bloqueo.
- **ReadOnly** significa que las personas autorizadas pueden leer un recurso, pero no eliminarlo ni cambiarlo. Aplicar este bloqueo es como restringir a todos los usuarios autorizados a los permisos concedidos por el rol **Lector** en RBAC de Azure.

### ¿Cómo se elimina o cambia un recurso bloqueado?

Aunque los bloqueos impiden que se produzcan cambios por error, se pueden seguir realizando cambios realizando un proceso de dos pasos.

Para modificar un recurso bloqueado, primero hay que quitar el bloqueo. Tras quitarlo, podemos aplicar cualquier acción que podamos realizar de acuerdo a nuestros permisos. Este paso adicional nos permite llevar a cabo la acción, e impide que cualquier administrador pueda hacer algo de manera accidental.

Los bloqueos de recursos se aplican con independencia de los permisos RBAC. Es decir, aun siendo el propietario del recurso, tendremos que quitar el bloqueo antes de poder realizar la actividad bloqueada.

### Combinación de bloqueos de recursos con Azure Blueprints

¿Qué ocurre si un administrador de la nube elimina un bloqueo de recurso por error? Si el bloqueo de recurso se quita, los recursos asociados correspondientes se podrán cambiar o eliminar.

Para que el proceso de protección sea más riguroso, podemos combinar bloqueos de recursos con Azure Blueprints. Azure Blueprints nos permite definir el conjunto recursos estándar de Azure que la organización necesita. Así, por ejemplo, podemos definir un plano técnico que especifique que debe haber un bloqueo de recursos determinado. Azure Blueprints puede reemplazar automáticamente el bloqueo de recursos si dicho bloqueo se quita.

Posteriormente en este módulo hablaremos más sobre Azure Blueprints.

### Ejercicio: Uso de un bloqueo de recursos para impedir que una cuenta de almacenamiento se elimine por error

En este ejercicio, veremos cómo usar bloqueos de recursos para evitar que se eliminen recursos de Azure por error.

Para ello, crearemos un grupo de recursos desde Azure Portal (pensemos en un grupo de recursos como un contenedor de recursos de Azure relacionados). Después, agregaremos un bloqueo a ese grupo de recursos y confirmaremos que el grupo no se puede eliminar.

Por último, agregaremos una cuenta de almacenamiento a nuestro grupo de recursos y veremos cómo el bloqueo del grupo de recursos primario impide que esa cuenta de almacenamiento se elimine. Una cuenta de almacenamiento es un contenedor que agrupa un conjunto de servicios de almacenamiento de Azure.

### Importante

Para completar los ejercicios de este módulo se necesita una [suscripción de Azure](#) propia. Si no la tiene, puede seguir leyendo.

### Creación del grupo de recursos

Aquí crearemos un grupo de recursos denominado **my-test-rg**.

1. Abra [Azure Portal](#) e inicie sesión.
2. En la parte superior de la página, seleccione **Grupos de recursos**.
3. Seleccione **+ Nuevo**. Aparece la página **Crear un grupo de recursos**.
4. En la pestaña **Aspectos básicos**, rellene los campos siguientes.

#### Configuración

##### Valor

##### Detalles del proyecto

Suscripción

*Su suscripción de Azure*

Resource group

**my-test-rg**

##### Detalles del recurso

Region

**(EE. UU.) Este de EE. UU.**

También puede seleccionar una región más cercana a la suya.

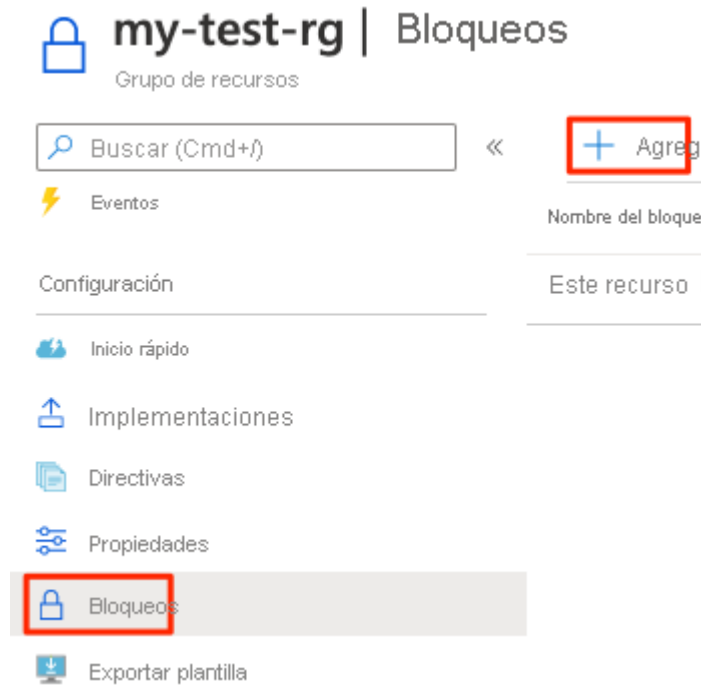
5. Seleccione **Revisar y crear** y, luego, **Crear**.

### Adición de un bloqueo al grupo de recursos

Agregue un bloqueo de recurso al grupo de recursos. Para ello:

1. En Azure Portal, seleccione el grupo de recursos, **my-test-rg**.

2. En **Configuración**, seleccione **Bloqueos** y, luego, seleccione **Agregar**.



3. Rellene estos campos.

#### Configuración

##### Valor

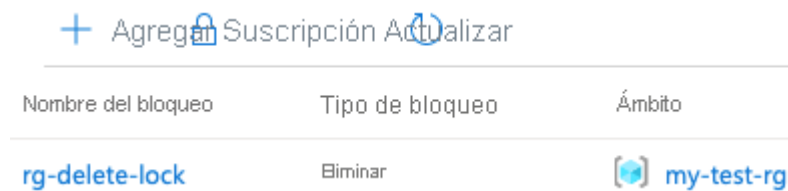
Nombre del bloqueo

**rg-delete-lock**

Tipo de bloqueo

##### Eliminar

4. Seleccione **Aceptar**. Vemos que el bloqueo de recurso se aplica al grupo de recursos.



#### Confirmación de que el grupo de recursos está protegido frente a eliminaciones

Aquí intentaremos eliminar el grupo de recursos para confirmar que está protegido.

1. En la parte superior de la página, seleccione **my-test-rg** para ir a la página de información general del grupo de recursos.

Inicio > Grupos de recursos > **my-test-rg**

## Grupos de recursos



2. Seleccione **Eliminar grupo de recursos**.

Agregar Editar columnas **Eliminación de...** Actualizar Mover

3. En el símbolo del sistema, escriba **my-test-rg** y, luego, seleccione **Aceptar**. Aparecerá un mensaje que indica que el grupo de recursos está bloqueado y no se puede eliminar.

**Error al eliminar el grupo de recursos my...** 22:03  
El grupo de recursos my-test-rg está bloqueado y no se puede eliminar. Haga clic aquí para administrar los bloqueos de este grupo de recursos.

### Protección de una cuenta de almacenamiento de eliminaciones por error

Ahora agregaremos una cuenta de almacenamiento a nuestro grupo de recursos y veremos cómo el bloqueo del grupo de recursos primario impide eliminar esa cuenta de almacenamiento. Para ello:

1. En Azure Portal, en la parte superior de la página, seleccione **Inicio** para volver a la página de inicio.
2. Seleccione **Cuentas de almacenamiento**. Luego, seleccione **+ Nuevo**. Aparece la página **Crear cuenta de almacenamiento**.
3. En la pestaña **Aspectos básicos**, rellene los campos siguientes.

#### Nota

Reemplace **NNN** por una serie de números. Los números ayudan a garantizar que el nombre de la cuenta de almacenamiento sea único.

#### Configuración

##### Valor

##### Detalles del proyecto

##### Suscripción

*Su suscripción de Azure*

Resource group

**my-test-rg**

##### Detalles de instancia



Nombre de la cuenta de almacenamiento

**mysaNNN**

Location

**(EE. UU.) Este de EE. UU.**

Rendimiento

**Estándar**

Tipo de cuenta

**StorageV2 (uso general v2)**

Replicación


**Almacenamiento con redundancia local (LRS)**

Como antes, en este caso también puede seleccionar una región más cercana a la suya.

4. Seleccione **Revisar y crear** y, luego, **Crear**. La implementación puede tardar un poco en completarse.
5. Haga clic en **Go to resource** (Ir al recurso).
6. En la parte superior de la página, seleccione **Eliminar**.

 Abrir en el...  Mover  Actualizar  **Eliminar**  Comentarios

Aparecerá un mensaje que indica que el recurso o su grupo primario está bloqueado y no se puede eliminar. En este ejemplo se muestra el mensaje de error relativo a una cuenta de almacenamiento denominada **mysa1234**.

 "mysa1234" no se puede eliminar porque este recurso o su elemento primario tiene un bloqueo de eliminación. Se deben quitar los bloqueos para poder eliminar este recurso. [Más información sobre la eliminación de bloqueos](#)

Aunque no hemos creado un bloqueo expresamente para esta cuenta de almacenamiento, el bloqueo que creamos para el grupo de recursos primario impide eliminar el recurso. En otras palabras, la cuenta de almacenamiento hereda el bloqueo del grupo de recursos primario.

### **Eliminación de un grupo de recursos y la cuenta de almacenamiento**

Ya no necesitamos el grupo de recursos o la cuenta de almacenamiento, así que ahora los eliminaremos.

Cuando un grupo de recursos se elimina, también se eliminan sus recursos secundarios, como la cuenta de almacenamiento que creamos anteriormente.

Para eliminar el grupo de recursos, primero hay que quitar el bloqueo de recurso.

1. En Azure Portal, seleccione **Inicio>Grupos de recursos>my-test-rg** para ir al grupo de recursos.

2. En **Configuración**, seleccione **Bloqueos**.
3. Busque **rg-delete-lock** y seleccione **Eliminar** en esa misma fila.
4. Seleccione **Información general** y, después, **Eliminar grupo de recursos**.
5. En el símbolo del sistema, escriba **my-test-rg** y, luego, seleccione **Aceptar**. La operación de eliminación puede tardar un poco en completarse.
6. Cuando la operación finalice, seleccione **Inicio>Grupos de recursos**. Verá que el grupo de recursos **my-test-rg** ya no está en la cuenta y que la cuenta de almacenamiento también se ha eliminado.

Buen trabajo. Ya sabemos cómo usar bloqueos de recursos para evitar que se eliminen recursos de Azure por error.

### Uso de etiquetas para organizar los recursos de Azure

A medida que el uso que hacemos de la nube va en aumento, es cada vez más importante mantenerse organizado. Una buena estrategia de organización nos ayudará a conocer cuál es nuestro uso de la nube, así como a administrar los costos.

Por ejemplo, a medida que Tailwind Traders concibe nuevas formas de implementar sus aplicaciones en Azure, necesita una manera de marcar sus entornos de prueba para poder identificar y eliminar fácilmente recursos en estos entornos cuando ya no sean necesarios.

Un método para organizar los recursos relacionados es colocarlos en sus propias suscripciones. También se pueden usar grupos de recursos para administrarlos. Las *etiquetas* de recursos son otra forma de organizar recursos. Las etiquetas proporcionan información extra, o metadatos, sobre los recursos. Estos metadatos son útiles para lo siguiente:

- **Administración de recursos:** las etiquetas permiten localizar recursos asociados a cargas de trabajo, entornos, unidades de negocio y propietarios específicos y actuar al respecto.
- **Optimización y administración de costes:** las etiquetas permiten agrupar recursos para que podamos informar sobre los costes, asignar centros de costes internos, mantener los presupuestos a raya y predecir costes estimados.
- **Administración de operaciones:** las etiquetas permiten agrupar recursos según la importancia que tiene su disponibilidad para nuestro negocio. Esta agrupación nos ayuda a formular acuerdos de nivel de servicio (SLA), que constituyen una garantía de rendimiento o de tiempo de actividad entre nosotros y nuestros usuarios.
- **Seguridad:** las etiquetas permiten clasificar los datos según su nivel de seguridad, por ejemplo, *públicos* o *confidenciales*.
- **Gobernanza y cumplimiento normativo:** las etiquetas permiten identificar los recursos que cumplen con los requisitos de gobernanza o cumplimiento normativo, como la norma ISO 27001. Las etiquetas también pueden formar parte de nuestros esfuerzos de aplicación de estándares. Así, podríamos exigir que todos los recursos se etiqueten con un nombre de departamento o propietario.

- **Automatización y optimización de las cargas de trabajo:** las etiquetas pueden servir para ver todos los recursos que participan en implementaciones complejas. Por ejemplo, podemos etiquetar un recurso con su nombre de aplicación o carga de trabajo asociado y usar un software como Azure DevOps para realizar tareas automatizadas en esos recursos.

### ¿Cómo se administran las etiquetas de recursos?

Podemos agregar, modificar o eliminar etiquetas de recursos a través de PowerShell, la CLI de Azure, plantillas de Azure Resource Manager, la API REST o Azure Portal.

Las etiquetas también se pueden administrar mediante Azure Policy. Por ejemplo, podemos usar etiquetas en un grupo de recursos, pero esas etiquetas no se aplican automáticamente a los recursos de ese grupo de recursos. Se puede usar Azure Policy para garantizar que un recurso herede las mismas etiquetas que su grupo de recursos primario. Posteriormente en este módulo hablaremos más sobre Azure Policy.

Azure Policy se puede usar también para aplicar reglas y convenciones de etiquetado. Así, podemos requerir que se agreguen determinadas etiquetas a los nuevos recursos a medida que se aprovisionan. Asimismo, podemos definir reglas que vuelvan a aplicar etiquetas que se han quitado.

### Ejemplo de una estructura de etiquetado

Una etiqueta de recurso se compone de un nombre y un valor. Podemos asignar una o más etiquetas a cada recurso de Azure.

Después de revisar los requisitos empresariales, Tailwind Traders decide usar las siguientes etiquetas.

#### **Nombre**

#### **Valor**

##### **AppName**

Nombre de la aplicación de la que forma parte el recurso

##### **CostCenter**

Código interno del centro de costes

##### **Propietario**

Nombre del propietario de empresa responsable del recurso

##### **Entorno**

Nombre de entorno, como "Prod.", "Dev." o "Prueba".

##### **Impacto**

Importancia del recurso para las operaciones empresariales, como "Crítico", "Gran impacto" o "Bajo impacto".

En este ejemplo se muestran estas etiquetas cuando se aplican a una máquina virtual durante el aprovisionamiento.

| Nombre ⓘ    | Valor ⓘ                     | Recurso         |
|-------------|-----------------------------|-----------------|
| AppName     | : SpecialOrders             | Máquina virtual |
| CostCenter  | : 0224 - Infrastructure R&D | Máquina virtual |
| Propietario | : tim@tailwindtraders.com   | Máquina virtual |
| Entorno     | : Prueba                    | Máquina virtual |
| Impacto     | : Gran impacto              | Máquina virtual |

El equipo de Tailwind Traders puede ejecutar consultas (por ejemplo, con PowerShell o la CLI de Azure) para ver todos los recursos que contienen estas etiquetas.

Recordemos que no es necesario requerir que una etiqueta específica esté presente en todos los recursos. Por ejemplo, podemos decidir que solo los recursos críticos tengan la etiqueta **Impact**. De este modo, todos aquellos recursos que no estén etiquetados no se considerarán como críticos.

### Uso de Azure Policy para controlar y auditar recursos

En un ejercicio anterior de este módulo, ha identificado los requisitos empresariales y de gobernanza. ¿Cómo puede asegurarse de que estos recursos *mantengan* su cumplimiento? ¿Puede recibir un aviso cuando la configuración de un recurso cambie?

[Azure Policy](#) es un servicio de Azure que permite crear, asignar y administrar directivas que controlan o auditan recursos. Dichas directivas aplican distintas reglas en todas las configuraciones de los recursos para que esas configuraciones sigan cumpliendo con los estándares corporativos.

### ¿Cómo se definen directivas en Azure Policy?

Azure Policy permite definir tanto directivas individuales como *grupos* de directivas relacionadas, lo que se conoce como *iniciativas*. Azure Policy evalúa los recursos y resalta los que no cumplen las directivas que hemos creado. Azure Policy también puede impedir que se creen recursos no conformes.

Azure Policy incluye definiciones de iniciativas y directivas integradas para categorías como Almacenamiento, Redes, Proceso, Centro de Seguridad y Supervisión. Por ejemplo, si define una directiva que permite usar exclusivamente un determinado tamaño de SKU (referencia de almacén) para las máquinas virtuales (VM) en el entorno, esa directiva se invoca al crear una nueva máquina virtual y cada vez que se cambia el tamaño de las ya existentes. Azure Policy también evalúa y supervisa todas las máquinas virtuales que hay actualmente en el entorno.

En algunos casos, Azure Policy puede corregir automáticamente los recursos y configuraciones no conformes para garantizar la integridad del estado de los recursos. Por ejemplo, si todos los

recursos de un determinado grupo de recursos deben etiquetarse con la etiqueta **AppName** y un valor de "SpecialOrders", Azure Policy volverá a aplicar automáticamente esa etiqueta si se ha quitado.

Azure Policy se integra con Azure DevOps aplicando directivas de integración continua y canalización de entrega que competen a las fases de implementación anterior y posterior de las aplicaciones.

### **Azure Policy en acción**

La implementación de una directiva en Azure Policy conlleva tres tareas:

1. Crear una definición de directiva
2. Asignar la definición a los recursos
3. Revisar los resultados de evaluación

Vamos a examinar cada paso con más detalle.

#### **Tarea 1: Crear una definición de directiva**

Una definición de directiva expresa qué se debe evaluar y qué acción realizar. Por ejemplo, podemos impedir que se implementen máquinas virtuales en determinadas regiones de Azure. También podemos auditar nuestras cuentas de almacenamiento para comprobar que solo aceptan conexiones de redes permitidas.

Cada definición de directiva tiene condiciones que regulan su aplicación. Además, esta definición tiene un efecto complementario que se produce cuando se cumplen las condiciones. Estos son algunos ejemplos de definiciones de directiva:

- **SKU de máquina virtual permitidas:** esta directiva permite especificar un conjunto de SKU de máquina virtual que la organización puede implementar.
- **Ubicaciones permitidas:** esta directiva permite restringir las ubicaciones que la organización puede especificar al implementar los recursos. Su efecto se usa para exigir los requisitos de cumplimiento de replicación geográfica.
- **MFA debe estar habilitado en las cuentas con permisos de escritura de la suscripción:** esta directiva requiere que la autenticación multifactor (MFA) esté habilitada en todas las cuentas de la suscripción que tengan permisos de escritura, para evitar una vulneración de seguridad en esas cuentas o en los recursos.
- **CORS no debe permitir que todos los recursos obtengan acceso a las aplicaciones web:** el uso compartido de recursos entre orígenes (CORS) es una característica de HTTP que permite que una aplicación web que se ejecuta en un dominio acceda a recursos de otro dominio. Por motivos de seguridad, los exploradores web modernos restringen el scripting entre sitios de forma predeterminada. Esta directiva permite que solo los dominios necesarios interactúen con la aplicación web.

- **Las actualizaciones del sistema deben estar instaladas en las máquinas:** esta directiva permite a Azure Security Center recomendar las actualizaciones del sistema de seguridad que faltan en los servidores.

## Tarea 2: Asignar la definición a los recursos

Para implementar nuestras definiciones de directiva, debemos asignar definiciones a los recursos. Una *asignación de directiva* es una definición de directiva que se aplica dentro de un ámbito específico. Este ámbito puede ser un grupo de administración (esto es, una colección de varias suscripciones), una sola suscripción o un grupo de recursos.

Todos los recursos secundarios dentro de ese ámbito heredarán las asignaciones de directivas. Si una directiva se aplica a un grupo de recursos, se aplicará también a todos los recursos dentro de ese grupo. Podemos excluir un subámbito de la asignación de directiva si hay recursos secundarios específicos que deban quedar fuera de la asignación de la directiva.

## Tarea 3: Revisión de los resultados de la evaluación

Cuando una condición se evalúa con los recursos existentes, cada recurso se marca como conforme o no conforme. Esto nos permitirá revisar los resultados de directiva que no sean conformes y tomar las medidas oportunas.

La evaluación de la directiva se produce aproximadamente una vez cada hora. Si realizamos cambios en la definición de la directiva y creamos una asignación de directiva, dicha directiva se evaluará con los recursos en una hora.

## ¿Qué son las iniciativas Azure Policy?

Una iniciativa de Azure Policy es una forma de agrupar las directivas relacionadas. La definición de iniciativa contiene todas las definiciones de directiva para facilitar el seguimiento del estado de cumplimiento de cara a un objetivo mayor.

Por ejemplo, Azure Policy incluye una iniciativa denominada **Habilitar la supervisión en Azure Security Center**, cuyo objetivo es supervisar todas las recomendaciones de seguridad disponibles para todos los tipos de recursos de Azure en Azure Security Center.

En esta iniciativa se incluyen las siguientes definiciones de directiva:

- **Supervisar base de datos SQL sin cifrar en Security Center:** esta directiva supervisa servidores y bases de datos SQL sin cifrar.
- **Supervisión de los puntos vulnerables del sistema operativo en Security Center:** esta directiva supervisa los servidores que no cumplen la línea base de la vulnerabilidad del sistema operativo configurada.
- **Supervisar la falta de Endpoint Protection en Security Center:** esta directiva supervisa los servidores que no tienen instalado un agente de Endpoint Protection.

La iniciativa **Habilitar la supervisión en Azure Security Center** contiene más de 100 definiciones de directiva independientes, de hecho.

Azure Policy también incluye iniciativas que admiten normas de cumplimiento, como HIPAA e ISO 27001.

### ¿Cómo se define una iniciativa?

Las iniciativas se definen mediante Azure Portal o herramientas de línea de comandos. En Azure Portal, puede buscar en la lista de iniciativas integradas en Azure. O bien podemos crear nuestra propia definición de directiva personalizada.

En la siguiente imagen se muestran algunos ejemplos de iniciativas de Azure Policy en Azure Portal.

Microsoft Azure

Buscar recursos, servicios y documentos (G+/I)

Inicio > Directiva: definiciones

**Directiva: definiciones**

Buscar (Ctrl+/)

+ Definición de iniciativa + Definición de directiva Actualizar

Ámbito: 1... Tipo de definición: Todos los tip... Tipo: Todos lo... Categoría: Todas las cat... Buscar: Filtrar po...

| Nombre               | Ubicación de de...   | Directivas | Tipo          |
|----------------------|----------------------|------------|---------------|
| azuresecuritypack... | No de producción     | 3          | Personalizar  |
| azuresecuritypack... | No de producción     | 3          | Personalizar  |
| audit ssh auth_1.3   | No de producción     | 4          | Personalizado |
| audit ssh auth_1.1   | No de producción     | 2          | Personalizado |
| azuresecuritypack... | 5e116433-8b65-49e... | 3          | Personalizado |
| azuresecuritypack... | 5e116433-8b65-49e... | 3          | Personalizado |
| audit ssh auth_1.1   | 5e116433-8b65-49e... | 2          | Personalizado |
| audit ssh auth_1.1   | Demostración         | 2          | Personalizar  |
| Audit Windows V...   |                      | 2          | Integrado     |

### ¿Cómo se asigna una iniciativa?

Al igual que una asignación de directiva, una asignación de iniciativa es una definición de iniciativa que se asigna a un ámbito específico de un grupo de administración, una suscripción o un grupo de recursos.

Aun cuando solo tengamos una directiva, una iniciativa nos permite aumentar el número de directivas a lo largo del tiempo. Dado que la iniciativa asociada permanece asignada, es más fácil agregar y quitar directivas sin necesidad de cambiar la asignación de directiva de los recursos.

## Ejercicio: Uso de Azure Policy para restringir las implementaciones a una ubicación específica

En este ejercicio, crearemos una directiva en Azure Policy que restrinja la implementación de recursos de Azure a una ubicación específica. Para comprobar que la directiva funciona, intentaremos crear una cuenta de almacenamiento en una ubicación que la infrinja.

Tailwind Traders quiere limitar la ubicación en la que se pueden implementar recursos a la región **Este de EE. UU.**, Esto tiene dos motivos:

- **Mejor seguimiento de costes:** a fin de llevar un control de los costos, Tailwind Traders usa diferentes suscripciones para realizar un seguimiento de las implementaciones en cada una de sus ubicaciones regionales. La directiva garantizará que todos los recursos se implementan en la región **Este de EE. UU.**
- **Cumplimiento de la seguridad y residencia de los datos:** Tailwind Traders debe adherirse a una regla de cumplimiento que rige dónde se pueden almacenar datos de clientes. En este caso, los datos de clientes se deben almacenar en la región **Este de EE. UU.**

Recordemos que podemos asignar una directiva a un grupo de administración, a una sola suscripción o a un grupo de recursos. Aquí, asignaremos la directiva a un grupo de recursos, así no afectará a otros recursos de la suscripción a Azure.

### Importante

Para completar los ejercicios de este módulo se necesita una [suscripción de Azure](#) propia. Si no la tiene, puede seguir leyendo.

### Creación del grupo de recursos

Aquí crearemos un grupo de recursos denominado **my-test-rg**. Es el grupo de recursos al que aplicaremos la directiva de ubicación.

A efectos de aprendizaje, usaremos el mismo nombre de grupo de recursos que usamos en el ejercicio anterior. Podemos usar el mismo nombre porque eliminamos ese grupo de recursos anterior.

1. Vaya a [Azure Portal](#) e inicie sesión.
2. Seleccione **Crear un recurso**.
3. Escriba **grupo de recursos** en el cuadro de búsqueda y presione Entrar.
4. Si se le lleva a un panel de resultados de la búsqueda, seleccione **Grupo de recursos** en los resultados.
5. Seleccione **Crear**. Luego, escriba los valores siguientes para cada opción.

### Configuración

#### Valor



## Suscripción

(Su suscripción de Azure)

Suscripción > Grupo de recursos

my-test-rg

Región

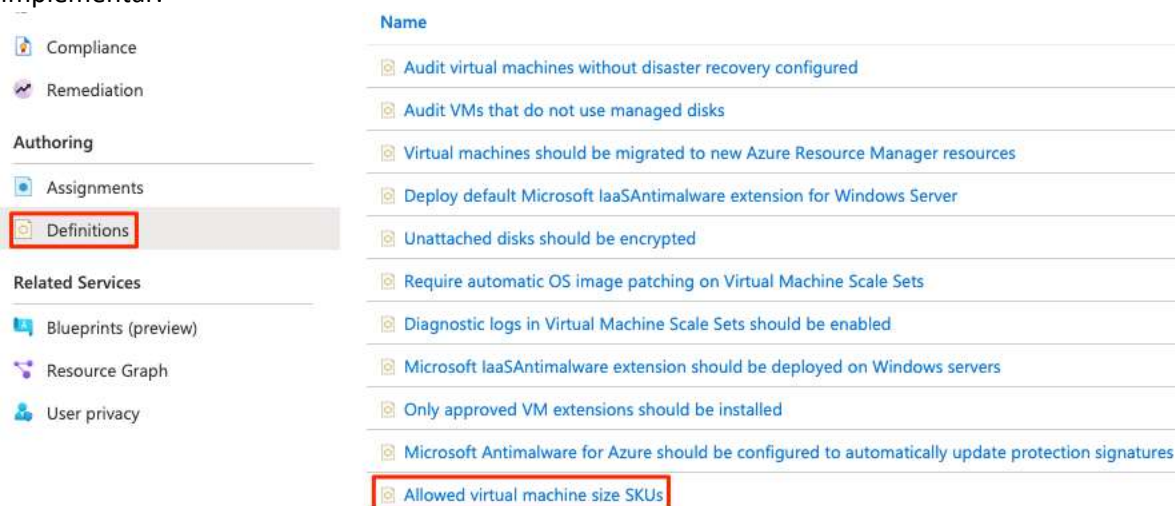
(EE. UU.) Este de EE. UU.

6. Seleccione **Revisar y crear** y, luego, **Crear**.

## Exploración de directivas predefinidas

Antes de configurar nuestra directiva de ubicación, vamos a echar un vistazo a algunas directivas predefinidas. A modo de ejemplo, nos fijaremos en las directivas relacionadas con los servicios de Azure Compute.

1. En Azure Portal, en la parte superior de la página, seleccione **Inicio** para volver a la página de inicio.
2. En la parte superior de la página, escriba **directiva** en la barra de búsqueda y, luego, seleccione **Directiva** en la lista de resultados para acceder a Azure Policy.
3. En **Creación**, seleccione **Definiciones**.
4. En la lista desplegable **Categoría**, seleccione únicamente **Proceso**. Observe que la definición **SKU de máquina virtual permitidas** nos permite especificar un conjunto de SKU de máquina virtual que la organización puede implementar.



Si lo desea, explore cualquier otra directiva o categoría que le interese.

## Configuración de la directiva de ubicación

Aquí puede configurar la directiva de ubicación permitida mediante Azure Policy. A continuación, asigne esa directiva al grupo de recursos. Para ello:

1. En el panel **Directiva**, en **Creación**, seleccione **Asignaciones**.



Una asignación es una directiva que se asignó para que se lleve a cabo dentro de un ámbito específico. Por ejemplo, una definición puede estar asignada al ámbito de suscripción.

2. Seleccione **Asignar directiva**.



Se le lleva al panel **Asignar directiva**.

3. En **Ámbito**, seleccione los puntos suspensivos.  
Establezca lo siguiente en el cuadro de diálogo que aparece:
  - a. En el campo **Suscripción**, su suscripción a Azure.
  - b. En el campo **Grupo de recursos**, **my-test-rg**.
  - c. Elija **Seleccionar**.
4. En **Definición de directiva**, seleccione los puntos suspensivos.
  - a. Seleccione la definición **Ubicaciones permitidas**.
  - b. Elija **Seleccionar**.

Tipo

Todos los tipos

Buscar

ubicación

#### Definiciones de directivas (5)

##### Ubicaciones permitidas de Azure Cosmos DB

Integrado

Esta directiva permite restringir las ubicaciones que la organización aplicará los requisitos de cumplimiento de replicación geográfica.

##### Configure copias de seguridad de las VM de una ubicación en

Integrado

Esta directiva permite configurar la protección de Azure Backup en la solo a las VM que aún no están configuradas para realizar la copia de la directiva se asigna a más de 200 VM, puede dar lugar a que se mejorará para admitir más imágenes de VM, más VM images

##### La ubicación del recurso de auditoría coincide con la del grupo de re

Integrado

Auditoría cuya ubicación de recursos coincide con la ubicación de si

##### Ubicaciones permitidas

Integrado

Esta directiva le permite restringir las ubicaciones que su organización requisitos de cumplimiento. Excluye los grupos de recursos, Microsoft región.

Esta definición de directiva especifica la ubicación en la que todos los recursos deben implementarse. Si se elige otra ubicación, se producirá un error en la implementación.

5. Seleccione **Siguiente** para ir a la pestaña **Parámetros**.
6. En la lista desplegable **Ubicaciones permitidas**, seleccione **Este de EE. UU.**
7. Seleccione **Revisar y crear** y, luego, **Crear**.

Vemos que ahora la asignación de directiva **Ubicaciones permitidas** aparece en el panel **Directiva | Asignaciones**, y que esa directiva se aplica al grupo de recursos **my-test-rg**.

| Nombre                 | T4 Ámbito                               | ↑↓ | Tipo      | T4 Directivas | TJ Categoría | ↑↓  |
|------------------------|-----------------------------------------|----|-----------|---------------|--------------|-----|
| Ubicaciones permitidas | Tailwind Traders R&D account/my-test-rg |    | Directiva | 1             | General      | ... |

#### Comprobación de la directiva de ubicación

Aquí intentaremos agregar una cuenta de almacenamiento a nuestro grupo de recursos en una ubicación que infringe la directiva de ubicación.

1. En Azure Portal, en la parte superior de la página, seleccione **Inicio** para volver a la página de inicio.
2. Seleccione **Crear un recurso**.
3. Escriba **cuenta de almacenamiento** en el cuadro de búsqueda y presione Entrar.
4. Si se le lleva a un panel de resultados de la búsqueda, seleccione **Cuenta de almacenamiento** en los resultados.
5. Seleccione **Crear**. Luego, escriba los valores siguientes para cada opción.

#### **Nota**

Reemplace **NNN** por una serie de números. Los números ayudan a garantizar que el nombre de la cuenta de almacenamiento sea único.

#### **Configuración**

##### **Valor**

##### **Suscripción**

*(Su suscripción de Azure)*

**Suscripción > Grupo de recursos**

**my-test-rg**

**Nombre de cuenta de almacenamiento**

**mysaNNN**

**Ubicación**

**(Asia Pacífico) Este de Japón**

**Rendimiento**

**Estándar**

**Tipo de cuenta**

**StorageV2 (uso general v2)**

**Redundancia**

**Almacenamiento con redundancia local (LRS)**


**Nivel de acceso (predeterminado)**

**Acceso frecuente**

Si antes seleccionó **Este de Japón** en la directiva de ubicación, seleccione una región diferente de la lista.

6. Seleccione **Revisar y crear** y, luego, **Crear**.  
Aparecerá un mensaje que indica que se ha producido un error en la implementación debido a una infracción de la directiva. También verá los detalles de la implementación. En este ejemplo se muestran los detalles de implementación de una cuenta de almacenamiento denominada **mysa1234**.

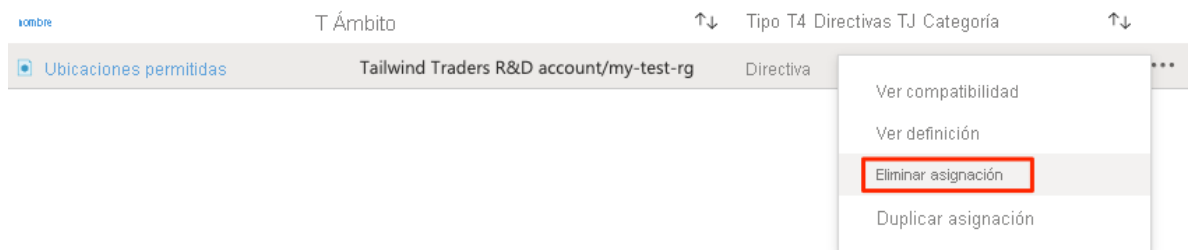
^ Detalles de la implementación (Descargar)

| Recurso                                                                                   | Tipo                              | Estado    |
|-------------------------------------------------------------------------------------------|-----------------------------------|-----------|
|  mys1234 | Microsoft.Storage/storageAccounts | Prohibido |

### Eliminación de la asignación de directiva

Ya no necesitamos la asignación de directivas, así que la quitaremos de la suscripción.

1. En Azure Portal, seleccione **Inicio>Directiva**.
2. En **Creación**, seleccione **Asignaciones**.
3. En la fila **Ubicaciones permitidas**, seleccione los puntos suspensivos y, luego, seleccione **Eliminar asignación**. Cuando se le solicite, seleccione **Sí**.



Verá que la asignación de directiva **Ubicaciones permitidas** ya no existe.

Como paso opcional, puede probar a crear la cuenta de almacenamiento una segunda vez para comprobar que la directiva ya no surta efecto alguno.

### Eliminar el grupo de recursos

Ya no necesitamos el grupo de recursos, así que lo quitaremos de la suscripción.

1. En Azure Portal, seleccione **Inicio>Grupos de recursos>my-test-rg** para ir al grupo de recursos.
2. Seleccione **Información general** y, después, **Eliminar grupo de recursos**.
3. En el símbolo del sistema, escriba **my-test-rg** y, luego, seleccione **Aceptar**. La operación de eliminación puede tardar un poco en completarse.
4. Cuando la operación finalice, seleccione **Inicio>Grupos de recursos**. Verá que el grupo de recursos **my-test-rg** ya no está en la cuenta

¡Excelente trabajo! Ha aplicado una directiva correctamente con Azure Policy para restringir la implementación de recursos de Azure en ubicaciones específicas. Ahora puede aplicar las directivas que necesite en el nivel de grupo de administración, suscripción o grupo de recursos.

### **Gobernanza de varias suscripciones con Azure Blueprints**

Hasta ahora, hemos visto una serie de características de Azure que pueden servir para poner en marcha nuestras decisiones de gobernanza, supervisar el cumplimiento de los recursos en la nube, controlar el acceso y proteger los recursos críticos frente a posibles eliminaciones accidentales.

¿Qué ocurre cuando nuestro entorno de nube empieza a crecer por encima de una sola suscripción? ¿Cómo podemos escalar la configuración de estas características, sabiendo que deben aplicarse a los recursos de las nuevas suscripciones?

En lugar de tener que configurar características como Azure Policy en cada nueva suscripción, con [Azure Blueprints](#) puede definir un conjunto repetible de herramientas de gobernanza y recursos de Azure estándar que la organización necesita. De este modo, los equipos de desarrollo pueden crear e implementar rápidamente nuevos entornos sabiendo que se crean de acuerdo con los estándares organizativos con un conjunto de componentes integrados que aceleran las fases de desarrollo e implementación.

Azure Blueprints organiza la implementación de varias plantillas de recursos y de otros artefactos, como son los siguientes:

- Asignaciones de roles
- Asignaciones de directivas
- Plantillas de Azure Resource Manager
- Grupos de recursos

### **Azure Blueprints en acción**

Cuando formamos un equipo de centro de excelencia en la nube o un equipo de administradores de nube, dicho equipo puede usar Azure Blueprints para escalar sus prácticas de gobernanza en toda la organización.

Para implementar un proyecto en Azure Blueprints hay que realizar estos tres pasos:

1. Crear una instancia de Azure Blueprints
2. Asignar ese plano técnico
3. Llevar un seguimiento de las asignaciones del plano técnico

Con Azure Blueprints, la relación entre la definición del plano técnico (lo que debe ser implementado) y su asignación (lo que se ha implementado) permanece. En otras palabras, Azure crea un registro que asocia un recurso con el plano técnico que lo define, y gracias a esta conexión podemos realizar el seguimiento y la auditoría de nuestras implementaciones.

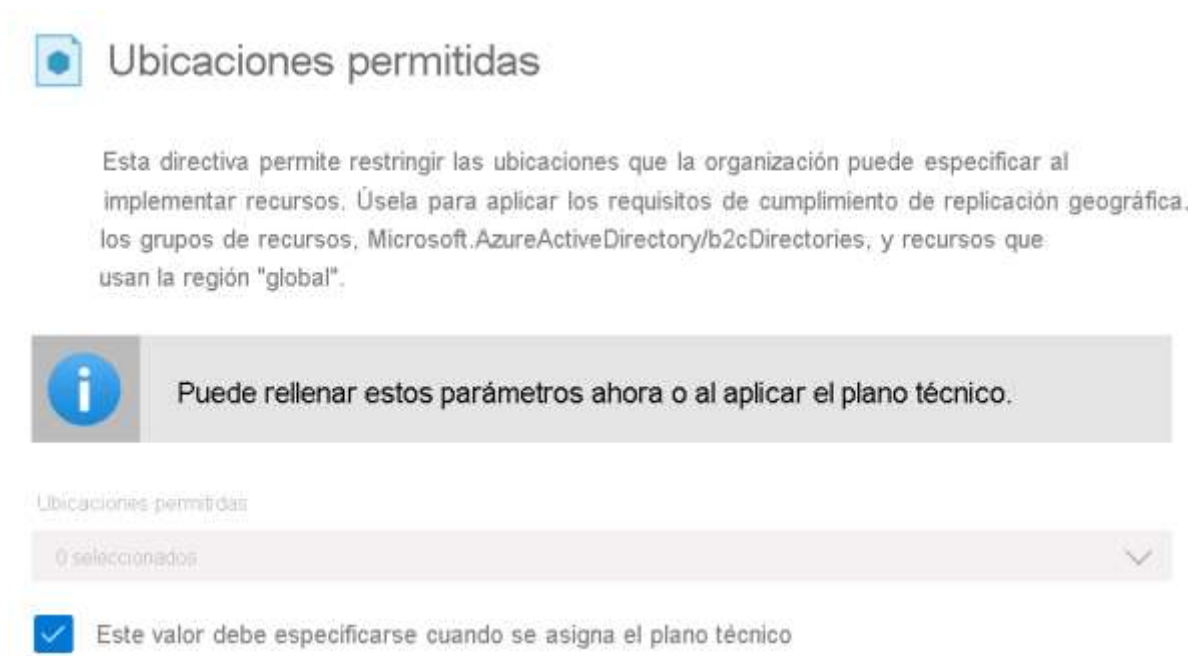
Los planos técnicos también tienen versiones. El control de versiones nos permite llevar un control de los cambios que se producen en el plano técnico y comentarlos.

### ¿Qué son los artefactos de plano técnico?

Cada componente de la definición de un plano técnico se denomina *artefacto*.

Es posible que los artefactos no tengan parámetros adicionales (configuraciones). Un ejemplo es la directiva **Implementar la detección de amenazas en servidores SQL Server**, que no requiere ninguna configuración adicional.

Los artefactos también pueden contener uno o más parámetros que se pueden configurar. En la siguiente captura de pantalla se muestra la directiva **Ubicaciones permitidas**, que incluye un parámetro que especifica las ubicaciones que se pueden usar.



Puede especificar el valor de un parámetro al crear la definición del plano técnico o al asignar la definición del plano a un ámbito. De este modo, puede mantener un plano técnico estándar, pero con la flexibilidad suficiente para especificar los parámetros de configuración pertinentes en cada ámbito en el que se asigne la definición.

### ¿Cómo usarán Azure Blueprints en Tailwind Traders para cumplir con la norma ISO 27001?

[ISO 27001](#) es una norma publicada por la Organización internacional de normalización, que rige la seguridad de los sistemas de tecnologías de la información (TI). Como parte de su proceso de calidad, Tailwind Traders quiere certificar que cumple con esta norma. Azure Blueprints cuenta con varias definiciones de plano técnico integradas relacionadas con ISO 27001.

Como administradores de TI, decidimos investigar la definición de la norma **ISO 27001 de plano técnico de servicios compartidos**. El esquema del plan es el siguiente:

1. Definir un grupo de administración llamado **PROD-MG** Recordemos que un grupo de administración se encarga de administrar el acceso, las directivas y el cumplimiento en varias suscripciones de Azure. Cada nueva suscripción de Azure que se cree se agregará a este grupo de administración.
2. Crear una definición de plano técnico según la norma **ISO 27001 de plano técnico de servicios compartidos**. A continuación, publique el plano técnico.
3. Asignar el plano técnico al grupo de administración **PROD-MG**

En la siguiente imagen se muestran los artefactos que se crean al ejecutar un plano técnico ISO 27001 a partir de una plantilla.

### Crear plano técnico

|                                                                                                                                                |                                     |                              |
|------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------|------------------------------|
|  Forzar el cifrado en las cuentas de Data Lake Store          | Asignación de directiva             | Ninguno                      |
|  Requerir el cifrado de blob de las cuentas de almacenamiento | Asignación de directiva             | Ninguno                      |
| + Agregar artefacto.                                                                                                                           |                                     |                              |
|  Grupo de recursos de Log Analytics                           | Grupo de recursos                   | 2 de 2 parámetros rellenados |
|  Plantilla de Log Analytics                                   | Plantilla de Azure Resource Manager | 0 de 4 parámetros rellenados |
| + Agregar artefacto.                                                                                                                           |                                     |                              |
|  Grupo de recursos de red                                     | Grupo de recursos                   | 2 de 2 parámetros rellenados |
|  Plantilla de Azure Firewall                                 | Plantilla de Azure Resource Manager | 0 de 3 parámetros rellenados |
|  Plantilla de Virtual Network y de la tabla de rutas        | Plantilla de Azure Resource Manager | 0 de 9 parámetros rellenados |

Como se aprecia en la imagen, la plantilla de plano técnico contiene asignaciones de directivas, plantillas de Resource Manager y grupos de recursos. El plano técnico implementa estos artefactos en las suscripciones existentes dentro del grupo de administración **PROD-MG**. También implementará estos artefactos en todas las suscripciones nuevas a medida que se vayan creando y agregando al grupo de administración.

### Aceleración del uso de la nube con Cloud Adoption Framework para Azure

[Cloud Adoption Framework para Azure](#) sirve como guía consolidada para ayudar en el recorrido para la adopción de la nube. Cloud Adoption Framework ayuda a crear e implementar las estrategias empresariales y tecnológicas necesarias para usar la nube correctamente.

Tailwind Traders necesita controlar su entorno de nube de manera que cumpla con varios estándares del sector, pero no tiene muy claro por dónde empezar. Tienen diversos requisitos empresariales, y son conscientes de que estos requisitos están ligados a sus cargas de trabajo locales. También las cargas de trabajo que se ejecuten en la nube deben cumplir con estos requisitos.

Se nos ha asignado la tarea de investigar qué hay disponible en Azure y de definir e implementar una estrategia de gobernanza para Tailwind Traders. Decidimos empezar con Cloud Adoption Framework.

### ¿Qué se incluye en Cloud Adoption Framework?



Como se ha mencionado en el vídeo, Cloud Adoption Framework se compone de diversas herramientas, documentación y procedimientos de eficacia probada. Cloud Adoption Framework incluye estas fases:

1. Definir la estrategia.
2. Crear un plan.
3. Preparar la organización.
4. Adoptar la nube.
5. Controlar y administrar los entornos de nube.

## Plataforma de adopción de Microsoft Cloud para Azure



La fase de control se centra en la gobernanza en la nube. Cloud Adoption Framework se puede consultar como referencia para obtener instrucciones recomendadas mientras traza su estrategia de gobernanza en la nube.

A modo de ayuda para crear la estrategia de adopción, Cloud Adoption Framework desglosa cada fase en una serie de ejercicios y pasos. Echemos un vistazo a cada una de estas fases.

### Definición una estrategia

En esta fase abordaremos los motivos por los que estamos trasladándonos a la nube y qué queremos obtener con la migración a la nube. ¿Necesitamos escalar para satisfacer la demanda o llegar a nuevos mercados? ¿Se reducirán los costes o aumentará la agilidad empresarial? Al definir la estrategia empresarial en la nube, conviene comprender aspectos como la [economía de la nube](#), así como sopesar el impacto empresarial, el tiempo de respuesta, el alcance global, el rendimiento, etc.

Estos son los pasos de esta fase.



1

**Definir y documentar nuestras motivaciones:** nos reuniremos con las partes interesadas y con la dirección para responder a la pregunta de por qué nos trasladamos a la nube.



2

**Documentar los resultados empresariales:** nos reuniremos con la dirección de los grupos de finanzas, marketing, ventas y recursos humanos como ayuda para documentar nuestros objetivos.



3

**Evaluación de las consideraciones financieras:** mida los objetivos e identifique la rentabilidad esperada de una inversión específica.



4

**Comprensión de las consideraciones técnicas:** evalúe esas consideraciones técnicas mediante la selección y la finalización del primer proyecto técnico.

#### **Creación un plan**

En esta fase crearemos un plan que establece una correspondencia entre los objetivos que aspiramos alcanzar y acciones concretas. Un buen plan nos puede ayudar a garantizar que nuestros esfuerzos se corresponden con los resultados empresariales que buscamos.

Estos son los pasos de esta fase.

**Bienes digitales:** crearemos un inventario de las cargas de trabajo y activos digitales existentes que tenemos previsto migrar a la nube.



1

**Alineación inicial de la organización:** garantizaremos que se van a centrar en los esfuerzos de migración las personas adecuadas, tanto desde un punto de vista técnico como desde un punto de vista de la gobernanza en la nube.



**Plan de preparación de aptitudes:** elaboraremos un plan que ayude a los usuarios a desarrollar las aptitudes que necesitan para usar la nube.



**Plan de adopción de la nube:** elaboraremos un plan completo que encamine a los equipos de desarrollo, operaciones y empresarial hacia un objetivo compartido de adopción de la nube.



#### **Preparación de la organización**

En esta fase crearemos una *zona de aterrizaje*, dicho de otro modo, un entorno en la nube donde empezar a hospedar nuestras cargas de trabajo.

Estos son los pasos de esta fase.



**Guía de instalación de Azure:** Revise la guía de instalación de Azure para familiarizarse con las herramientas y los enfoques necesarios para crear una zona de aterrizaje.



**Zona de aterrizaje de Azure:** empezaremos a crear las suscripciones de Azure que van a asimilar cada una de las áreas principales de nuestro negocio. Una zona de aterrizaje engloba una infraestructura en la nube, así como capacidades de gobernanza, cuentas y seguridad.



**Expansión de la zona de aterrizaje:** optimizaremos la zona de aterrizaje para asegurarnos de que satisface las necesidades de operaciones, gobernanza y seguridad.



**Procedimientos recomendados:** comenzaremos con procedimientos recomendados de eficacia probada para garantizar que los esfuerzos de migración a la nube son escalables y fáciles de mantener.

#### **Adopción de la nube**

En esta fase empezaremos a migrar nuestras aplicaciones a la nube. A lo largo del proceso, probablemente encontremos formas de modernizar nuestras aplicaciones y crear soluciones innovadoras que usen servicios en la nube.

Cloud Adoption Framework divide esta fase en dos partes: migrar e innovar.

**Migrar:** estos son los pasos de la parte de migración de esta fase.

**Migrar la primera carga de trabajo:** usaremos la guía de migración de Azure para implementar nuestro primer proyecto en la nube.



**Escenarios de migración:** usaremos guías más detalladas para explorar escenarios de migración de mayor complejidad.



**Procedimientos recomendados:** consultaremos los procedimientos recomendados de migración a la nube de Azure para confirmar que estamos siguiendo los procedimientos recomendados adecuados.

3

**Mejoras del proceso:** identificaremos distintas maneras de escalar el proceso de migración y, al mismo tiempo, requerir menos esfuerzo.

4

**Innovar:** estos son los pasos de la parte de innovación de esta fase.

1

**Consenso en torno al valor empresarial:** confirmaremos que las inversiones en nuevas innovaciones aportan un valor a la empresa y satisfacen las necesidades de los clientes.

2

**Guía de innovación de Azure:** usaremos esta guía para acelerar el desarrollo y crear un producto mínimo viable de nuestra idea.

3

**Procedimientos recomendados:** confirmaremos que nuestros avances casan con los procedimientos recomendados antes de continuar.

4

**Bucles de comentarios:** nos comunicaremos a menudo con nuestros clientes para confirmar que lo que estamos creando es lo que necesitan.

**Control y administración de los entornos de nube**

En esta fase empezaremos a trazar nuestras estrategias de administración y gobernanza en la nube. A medida que el patrimonio de la nube cambia con el tiempo, también lo hacen los procesos y las directivas de gobernanza de la nube. Deberemos crear soluciones resistentes que se optimicen constantemente.

**Gobernanza:** estos son los pasos de la parte de gobernanza de esta fase.

**Metodología:** evaluaremos nuestra solución de estado final. Después, definiremos una metodología que nos lleve gradualmente de los pasos iniciales a la gobernanza en la nube completa.



**Banco de pruebas:** usaremos la [herramienta de banco de pruebas de gobernanza](#) para valorar el estado actual en el que estamos y el estado futuro para establecer un panorama para aplicar el marco de trabajo.



**Base de gobernanza inicial:** crearemos un producto mínimo viable que capture los primeros pasos de nuestro plan de gobernanza.



**Mejora de la base de gobernanza inicial:** iremos agregando iterativamente controles de gobernanza que solucionen riesgos tangibles a medida que vayamos avanzando hacia la solución de estado final.



**Administración:** estos son los pasos de la parte de administración de esta fase.



**Establecer una línea base de administración:** definiremos nuestro compromiso mínimo con la administración de operaciones. Una línea base de administración es el conjunto mínimo de herramientas y procesos que se debe aplicar a todos los recursos de un entorno.



**Definición de los compromisos empresariales:** Documente las cargas de trabajo admitidas para establecer los compromisos operativos con la empresa y acordar las inversiones en administración de la nube para cada carga de trabajo.



**Expandir la línea base de administración:** pondremos en marcha procedimientos recomendados para iterar en la línea base de administración inicial.



**Operaciones y principios de diseño avanzados:** en el caso de aquellas cargas de trabajo que requieran un mayor nivel de compromiso empresarial, revisaremos la arquitectura más profundamente para satisfacer los compromisos de resistencia y confiabilidad.

#### **Creación de una estrategia de gobernanza de suscripciones**

Al comienzo de cualquier implementación de gobernanza en la nube, se debe identificar una estructura de la organización en la nube que cubra las necesidades empresariales. A menudo, este paso implica la conformación de un *equipo centro de excelencia en la nube* (también denominado *equipo de habilitación de la nube* o *equipo de custodia de la nube*). Este equipo está capacitado para implementar prácticas de gobernanza desde una ubicación centralizada para toda la organización.

A menudo, los equipos inician su estrategia de gobernanza de Azure en el nivel de suscripción. Hay tres aspectos principales que deben considerarse al crear y administrar suscripciones: facturación, control de acceso y límites de suscripción.

Vamos a echar un vistazo a cada uno de ellos con más detalle.

#### **Facturación**

Se puede crear un informe de facturación por suscripción. Si tenemos varios departamentos y necesitamos realizar un "contracargo" de costes en la nube, una posible solución es organizar las suscripciones por departamento o por proyecto.

Las etiquetas de recursos también pueden ser de ayuda. Las etiquetas se explorarán más adelante en este módulo. Al definir cuántas suscripciones se necesitan y cómo denominarlas, debemos tener en cuenta los requisitos de facturación internos.

### **Control de acceso**

Una suscripción es un límite de implementación de los recursos de Azure. Cada suscripción está asociada a un inquilino de Azure Active Directory. Cada inquilino proporciona a los administradores la capacidad de configurar un acceso granular a través de roles definidos por medio del control de acceso basado en roles de Azure.

Al diseñar la arquitectura de suscripciones, hay que tener en cuenta el factor de límite de la implementación, por ejemplo, ¿necesitamos suscripciones independientes para los entornos de desarrollo y producción? Con suscripciones independientes, es posible controlar el acceso a cada una de ellas por separado y aislar los recursos entre sí.

### **Límites de suscripción**

Las suscripciones también tienen algunas limitaciones de recursos. Por ejemplo, el número máximo de circuitos Azure ExpressRoute de red por cada suscripción es de 10. Estos límites se deben tener en cuenta durante la fase de diseño. Si necesitamos superar estos límites, puede que tengamos que agregar más suscripciones. Si alcanzamos un límite máximo estricto, no hay flexibilidad para aumentarlo.

Los grupos de administración también están disponibles para ayudar a administrar las suscripciones. Un grupo de administración se encarga de administrar el acceso, las directivas y el cumplimiento en varias suscripciones de Azure. Nos adentraremos en los grupos de administración más adelante en este módulo.



1. ¿Qué debe hacer Tailwind Traders para permitir a algunos usuarios controlar las máquinas virtuales en cada entorno, pero impedirles al mismo tiempo modificar recursos de red y de otro tipo en el mismo grupo de recursos o en la misma suscripción de Azure?

- ☒ Crear una asignación de roles mediante el control de acceso basado en roles de Azure (RBAC de Azure)

✓ Correcto. RBAC de Azure permite crear roles que definen permisos de acceso. Así, podríamos crear un rol que limite el acceso solo a las máquinas virtuales, y un segundo rol que proporcione acceso a todo a los administradores.

- ☐ Crear una directiva en Azure Policy que audite el uso de recursos
- ☐ Dividir el entorno en grupos de recursos independientes

2. ¿Qué debe hacer Tailwind Traders para asegurarse de que el equipo solo implementa tamaños de SKU de máquina virtual rentables?

- ☒ Crear una directiva en Azure Policy que especifique los tamaños de SKU permitidos

✓ Correcto. Cuando esta directiva se habilite, se aplicará cuando se creen más máquinas virtuales o se cambie el tamaño de las ya existentes. Azure Policy también evalúa todas las máquinas virtuales que hay actualmente en el entorno.

- ☐ Inspeccionar la implementación manualmente con regularidad para ver qué tamaños de SKU se usan
- ☐ Crear un rol de RBAC de Azure que defina los tamaños de SKU de máquina virtual permitidos

3. ¿Cuál es probablemente la mejor forma de que Tailwind Traders sepa a qué departamento de facturación pertenece cada recurso de Azure?

- ☐ Llevar seguimiento del uso de recursos en una hoja de cálculo
- ☐ Dividir la implementación en suscripciones de Azure independientes, donde cada suscripción pertenece a su propio departamento de facturación

- ☒ Usar una etiqueta en cada recurso que incluya el departamento de facturación asociado

✓ Correcto. Las etiquetas proporcionan información extra, o metadatos, sobre los recursos. Así, el equipo podría crear una etiqueta llamada DeptFactur cuyo valor sería el nombre del departamento de facturación. Se puede usar Azure Policy para garantizar que se asignan las etiquetas adecuadas cuando se aprovisionen recursos.