



#GlobalAzure

#GABMUGPeru

#GABMUGPeru

# Azure Policy: Guia para el cumplimiento seguridad en nube

Nelson Luis Contreras Centeno  
MBA(c), SC-100, AZ-500, CS-900



#GlobalAzure

# Agenda

- Introducción al Azure Policy
- Importancia del cumplimiento en la nube
- Creación y gestión de políticas de seguridad
- Monitoreo y cumplimiento
- Mejores prácticas y recomendaciones
- Conclusiones y recursos

#GABMUGPeru

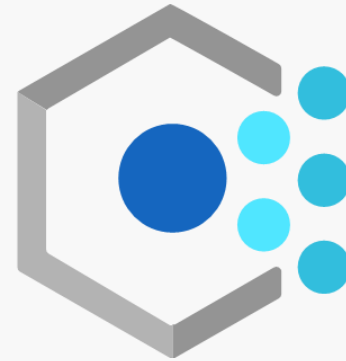
# Introducción



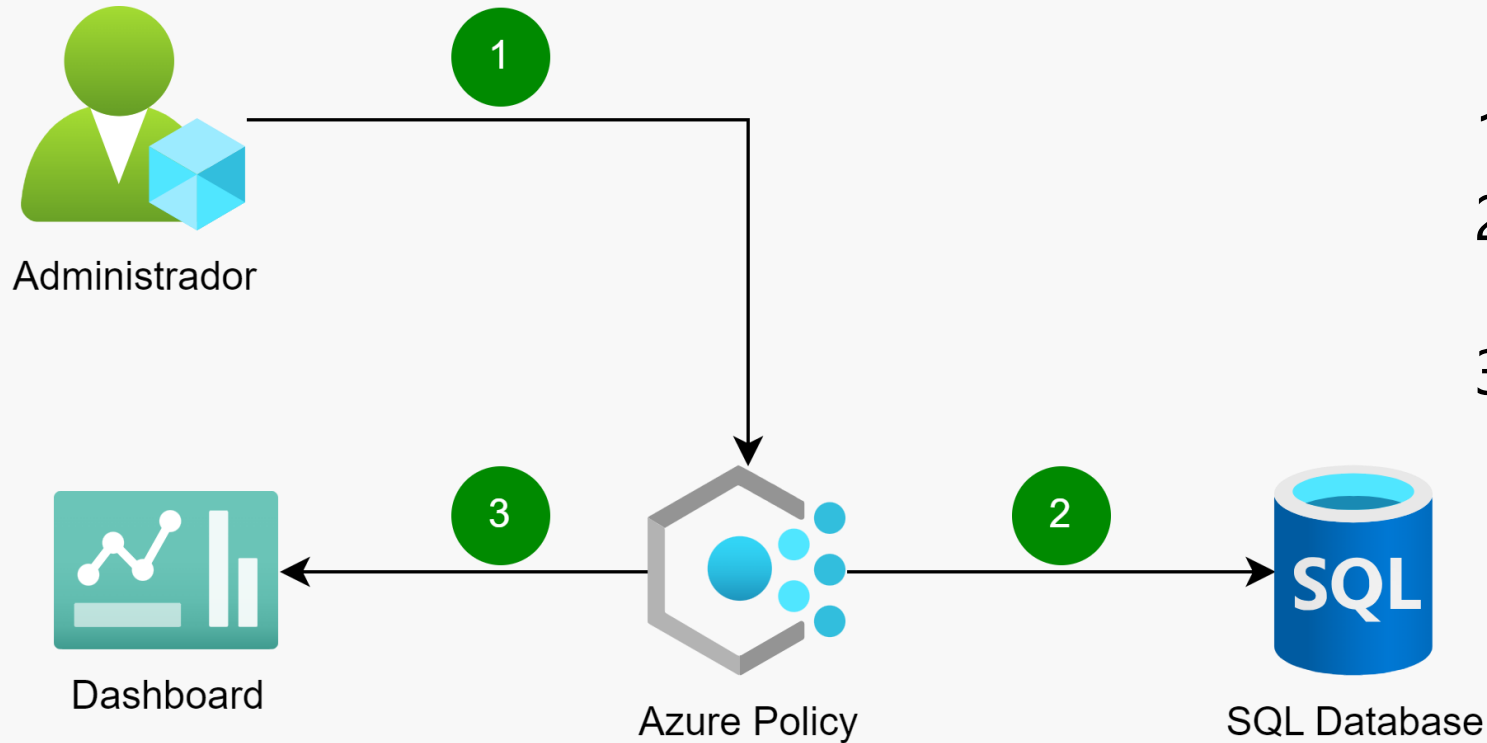
#GlobalAzure

# Azure Policy - Descripción

- Las políticas se utilizan para mantener la coherencia y aplicar el modelo de gobernanza en la nube.
- Es una herramienta permite aplicar la gobernanza que ayuda a cumplir con los estándares corporativos y de servicios.
- Los tipos de Policy son:
  - ❖ Deny
  - ❖ Audit
  - ❖ DeployIfNotExists
  - ❖ AuditIfNotExists



# Arquitectura Azure Policy



1. Definición de las políticas
2. Asignación de políticas a recursos
3. Reporte y monitoreo

- Motor de evaluación
- Verificación de Cumplimiento
- Acciones de Cumplimiento

#GABMUGPeru

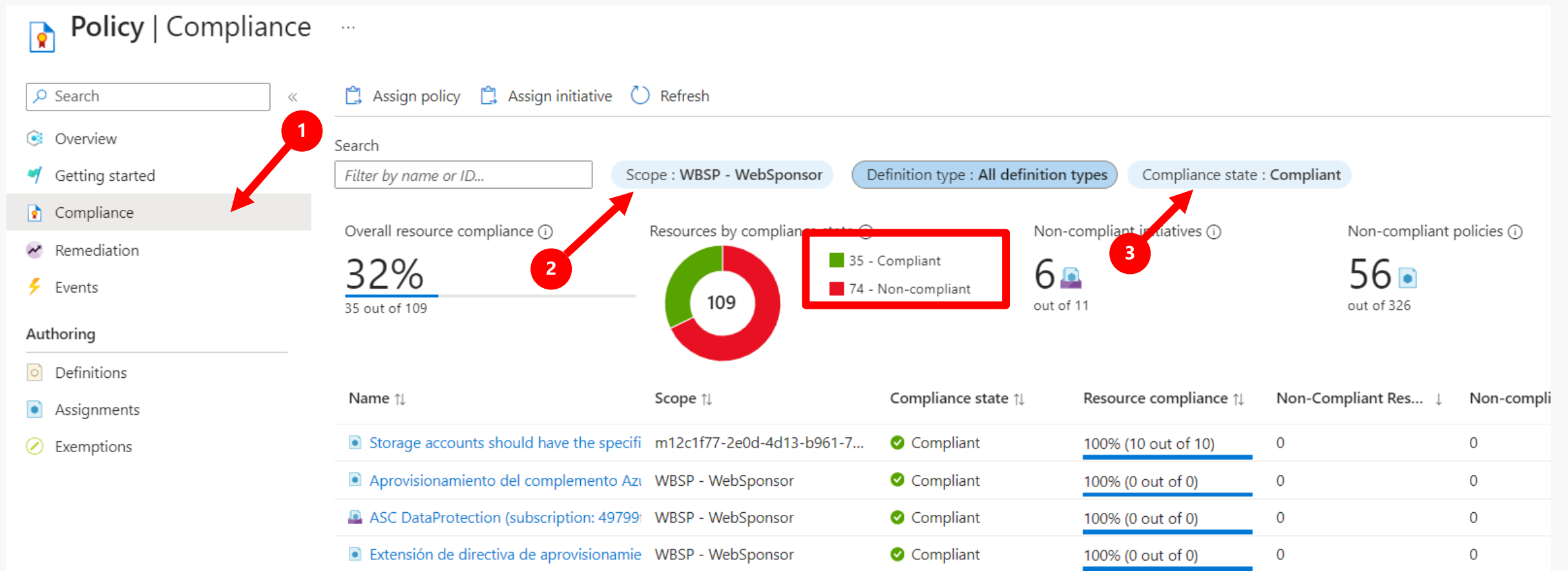
# Importancia del cumplimiento en la nube



#GlobalAzure



- El cumplimiento ayuda a asegurar que los recursos de Azure operen de manera segura y de acuerdo con las políticas de la organización, buena práctica o benchmark de seguridad.





## Riesgos reducidos

- El incumplimiento puede llevar a multas significativas, daños en la reputación y riesgos legales.
- Implementar políticas de cumplimiento ayuda a mitigar estos riesgos y asegura la integridad y confidencialidad de los datos.



## Eficiencia operativa

- Asegura que los recursos se utilicen de manera óptima y que los procesos de negocio sigan las mejores prácticas recomendadas por regulaciones y estándares.

#GABMUGPeru

# Creación y gestión de Políticas



#GlobalAzure

# Definición de una política

[Home](#) > [Policy | Definitions](#) >  

## Policy definition

New Policy definition

BASICS

Definition location \*

Mngr-Tribus

Name \*

Asegurar la configuración de TLS 1.2 en Base de Datos

Description

El servidor SQL admite conexiones cifradas mediante conexiones de capa de transporte (TLS). Se rechazará cualquier intento de inicio de sesión de clientes que utilicen una versión de TLS inferior a la versión mínima de TLS. Para obtener información sobre la versión y los certificados de TLS, consulte cómo conectarse con TLS/SSL.

Category

☒ Create new ☐ Use existing

Category

POLICY RULE

↓ [Import sample policy definition from GitHub](#)

↗ [Learn more about policy definition structure](#)

1

### Definition location

Management Group

- ✓ Tenant Root Group (m3dc1f77-2e0d-4d13-b961-7c2e63aa376b)
  - ✓ Tenant P (m4dc1f77-2e0d-4d13-b961-7c2e63aa376b)
    - ✓ Mngr-Agile Azure (m2dc1f77-2e0d-4d13-b961-7c2e63aa376b)
      - Mngr - Salud (m36c1f77-2e0d-4d13-b961-7c2e63aa376b)
      - > Mngr-Tribus (m4dc1f77-2e0d-4d13-b961-7c2e63aa376b)
      - Mngr-Networking (m17c1f77-2e0d-4d13-b961-7c2e63aa376b)
      - Mngr-Seguridad (m15c1f77-2e0d-4d13-b961-7c2e63aa376b)
    - ✓ Mngr-Servicios Compartidos (m11c1f77-2e0d-4d13-b961-7c2e63aa376b)
      - Mngr - Certificación (m11c1f77-2e0d-4d13-b961-7c2e63aa376b)
      - Mngr - Desarrollo (m10c1f77-2e0d-4d13-b961-7c2e63aa376b)
      - Mngr - Produc (m10c1f77-2e0d-4d13-b961-7c2e63aa376b)
      - Mngr-Temporal (m24c1f77-2e0d-4d13-b961-7c2e63aa376b)
      - Mngr-Waterfall (m3dc1f77-2e0d-4d13-b961-7c2e63aa376b)

Subscription

Optionally choose a Subscription

Select Cancel Clear All Selections


# Asignación de una política


[Home](#) > [Policy | Assignments](#) >


## Assign policy ...

**Basics** Parameters Remediation Non-compliance messages Review + create

**Scope**

Scope \*   **1**


[Learn more about setting the scope](#) 

Exclusions   **2**

Resource selectors [\(Expand\)](#)


Using resource selectors, you can further refine this assignment's applicability by targeting specific subsets of resources. Expand to learn more.

**Basics**


Policy definition \*   **3**

Overrides [\(Expand\)](#)

Using overrides, you can change the effects or referenced versions of definitions for all or a subset of resources evaluated by this assignment. Expand to learn more.

Assignment name \* 

Description

Policy enforcement  ☒ Enabled

# Asignación de una política

Home > Policy | Assignments >

## Assign policy ...

Basics **Parameters** Remediation Non-compliance messages Review + create

☒ Only show parameters that need input or review

No parameters found matching the current filters.

## Assign policy ...

Basics Parameters **Remediation** Non-compliance messages Review + create

By default, this assignment will only take effect on newly created resources. Existing resources can be updated via a remediation task after the policy is assigned. For `deployIfNotExists` policies, the remediation task will deploy the specified template. For `modify` policies, the remediation task will edit tags on the existing resources.

**Managed Identity**  
Policies with the `deployIfNotExists` and `modify` effect types need the ability to deploy resources and edit tags on existing resources respectively. To do this, choose between an existing user assigned managed identity or creating a system assigned managed identity. [Learn more about Managed Identity.](#)

Create a Managed Identity ⓘ ☐

**Permissions**

ⓘ This policy does not contain any role definitions. Policies must specify role definitions in order to create the correct role assignments for the managed identity.

# Iniciativas de políticas

[Home](#) > [Policy | Definitions](#) >


## Initiative definition

New Initiative definition

**Basics** Policies Groups Initiative parameters Policy parameters Review + create

An initiative definition is a collection of policy definitions that are tailored towards achieving a singular overarching goal. Initiative definitions simplify managing and assigning policy definitions by grouping them as a single assignable object.

Initiative location \* ⓘ

WBSP - WebSponsor ✓  **1**

Name \* ⓘ

Validación TLS 1.2 SQL Server ✓

Description ⓘ

Category ⓘ

☒ Create new ☐ Use existing

Category

# Iniciativas de políticas

[Home](#) > [Policy | Definitions](#) >

## Initiative definition

New Initiative definition

[Basics](#) [Policies](#) [Groups](#) [Initiative parameters](#) [Policy parameters](#) [Review + create](#)


Add one or more policies to this initiative. Reference ID can be used as a friendly display name but must be unique within the initiative.

Add policy definition(s)

1 Add selected policies to a group

1 policies are not part of any group

Group : 1 selected

<input type="checkbox"/>	Policy definition	Reference ID	Group
<input type="checkbox"/>	 [LBS SQL] 4. Habilitar versión mínima de TLS en los SQL server	[LBS SQL] 4. Habilitar versión mínima de TLS en los SQL server_1	2 0 groups



# Policy TLS 1.2 SQL Server

```
    "version": "1.0.0",
    "parameters": {
      "minimalTlsVersionEffect": {
        "type": "String",
        "metadata": {
          "description": "Enable or disable the execution of the policy",
          "displayName": "Effect"
        },
        "allowedValues": [
          "Audit",
          "Disabled",
          "Deny"
        ],
        "defaultValue": "Audit"
      }
    },
    "policyRule": {
      "if": {
        "allOf": [
          {
            "equals": "Microsoft.Sql/servers",
            "field": "type"
          },
          {
            "anyOf": [
              {
                "exists": false,
                "field": "Microsoft.Sql/servers/minimalTlsVersion"
              },
              {
                "field": "Microsoft.Sql/servers/minimalTlsVersion",
                "less": "1.2"
              }
            ]
          }
        ]
      },
      "then": {
        "effect": "[parameters('minimalTlsVersionEffect')]"
      }
    }
  }
}
```

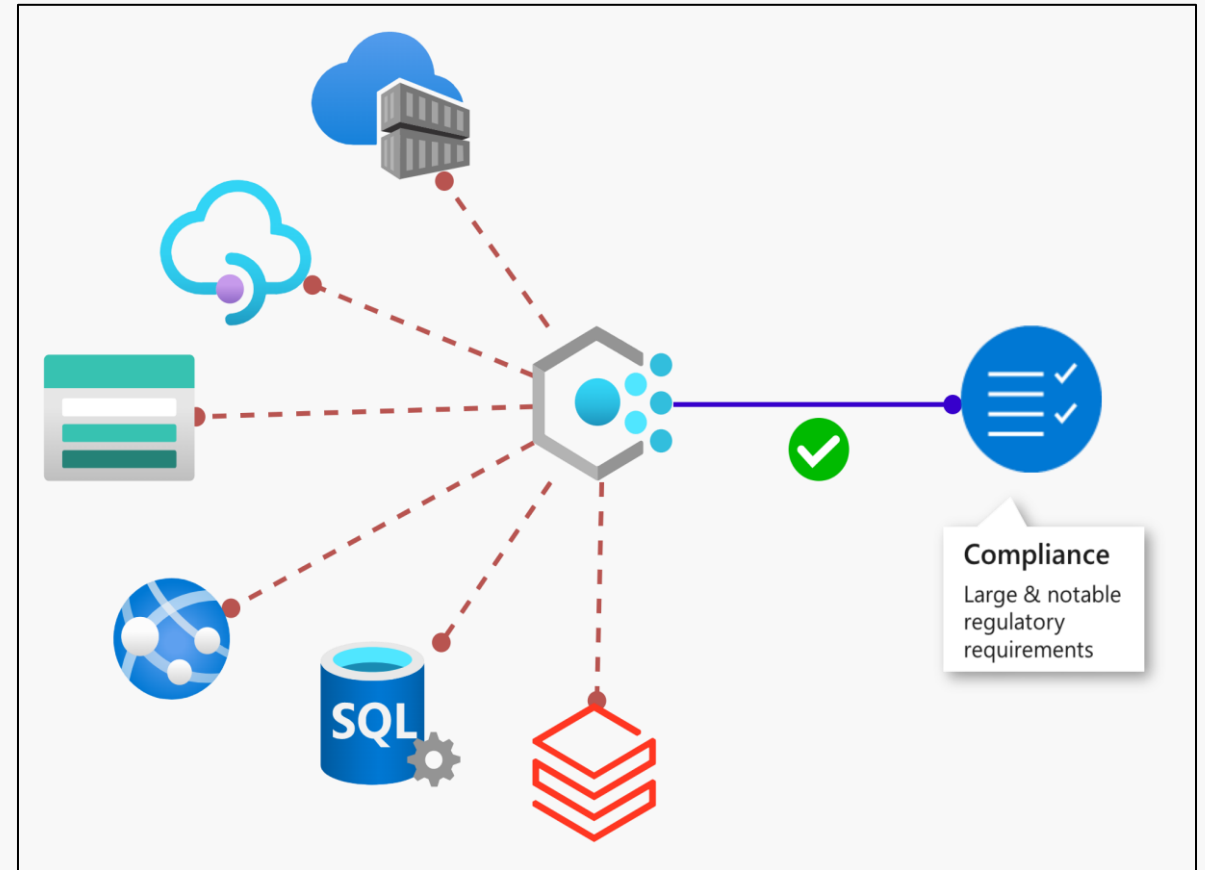
# Caso de usos

Asociar un Subscriptions Key a un API Product

Validar el cifrado en reposo TDE en almacenamiento de datos

Aplicación de etiquetas en recursos

Verificar la versión mínima de TLS 1.2 en los SQL server



#GABMUGPeru

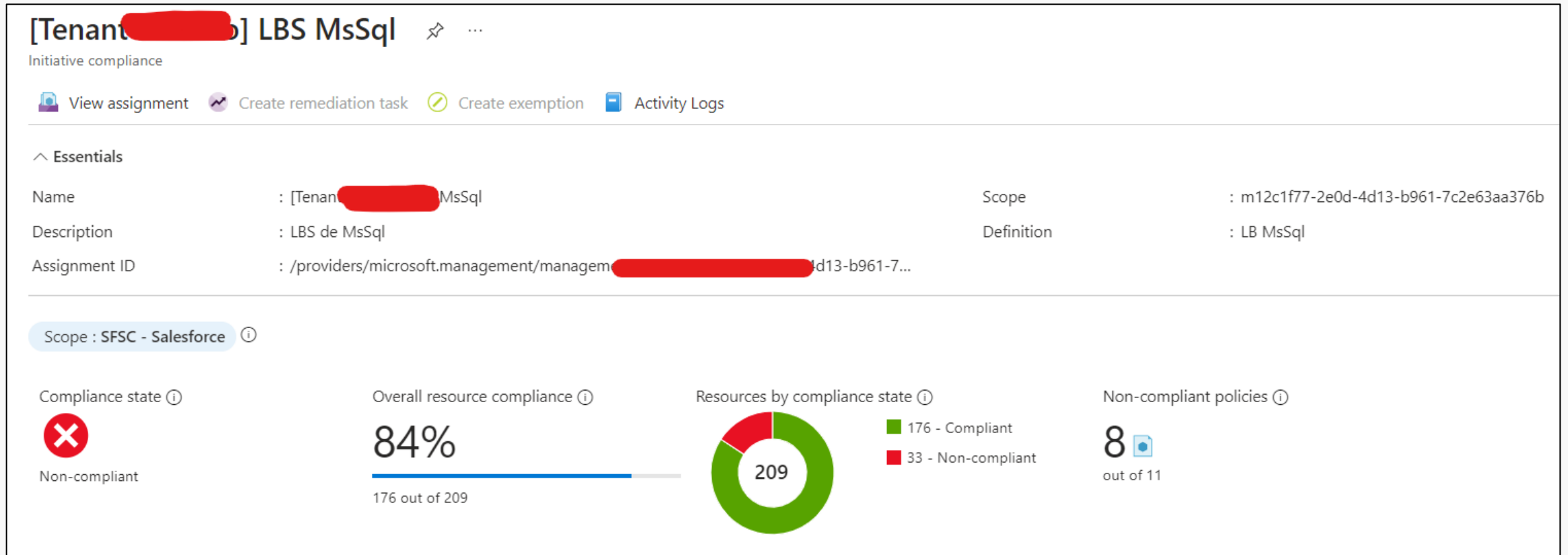
# Monitoreo y cumplimiento



#GlobalAzure

# Monitoreo

- Informes de cumplimiento
- Alertas
- Integración con herramientas externas



Name ↑↓	Effect Type ↑↓	Compliance state ↑↓	Non-Compliant Resources ↓
[LBS SQL] 10. Asegurar SQL Database deben tener resueltos los hallazgos	Audit	✗ Non-compliant	21
[LBS SQL] 9. Asegurar la activación del Defender for Cloud y configuración	AuditIfNotExists	✗ Non-compliant	6
[LBS SQL] 6. Deshabilitar el acceso desde los servicios de Azure hacia e	Audit	✗ Non-compliant	6
[LBS SQL] 5. Restringir el tráfico desde redes públicas a los SQL server	Audit	✗ Non-compliant	6
[LBS SQL] 11. Configurar la encriptación TDE con una llave administrada	Audit	✗ Non-compliant	5
[LBS SQL] 2. Establecer la retención de auditoría en 6 meses	AuditIfNotExists	✗ Non-compliant	2
[LBS SQL] 1. Habilitar la auditoría en las bases de datos	AuditIfNotExists	✗ Non-compliant	2
[LBS SQL] 8. Asegurar el uso de conexión por Private Link para la conexión	Audit	✗ Non-compliant	1
[LBS SQL] 3. Habilitar el cifrado de datos en las bases de datos	AuditIfNotExists	✓ Compliant	0
[LBS SQL] 7. Asegurar el uso de la Autenticación con Azure AD	Audit	✓ Compliant	0
[LBS SQL] 4. Habilitar versión mínima de TLS en los SQL server	Audit	✓ Compliant	0



### [LBS SQL] 4. Habilitar versión mínima de TLS en los SQL server

Policy compliance

[View assignment](#)
[Create remediation task](#)
[Create exemption](#)
[Activity Logs](#)

Compliant

100%

6 out of 6

6 - Compliant  
0 - Non-compliant

Effect Type **Audit**  
Parent Initiative

**LBS MsSql**

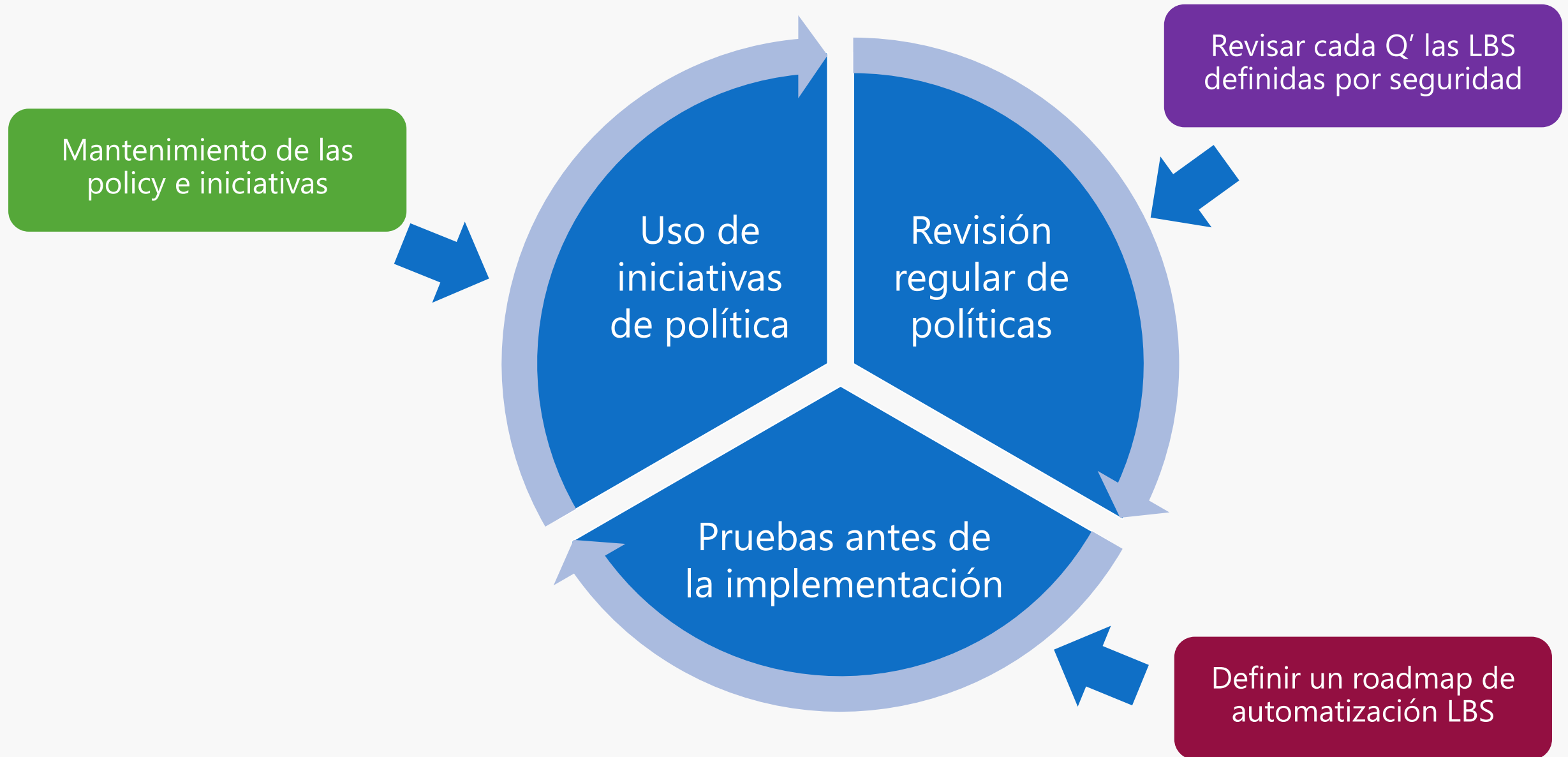
#### Resource Compliance

Compliance state : All compliance states
Resource type : microsoft.sql/servers
Location : East US 2

Name ↑↓	Compliance state ↑↓	Compliance reason ↑↓	Resource Type ↑↓	Location ↑↓	Scope ↑↓	Last evaluated ↑↓
msqlsfsc2c02	✓ Compliant	<a href="#">Details</a>	microsoft.sql/servers	East US 2	SFSC - Salesforce/RSGRFSCEU2...	4/18/24, 11:55:06 PM...
msqlsfsc2c01	✓ Compliant	<a href="#">Details</a>	microsoft.sql/servers	East US 2	SFSC - Salesforce/RSGRFSCEU2...	4/18/24, 11:55:06 PM...
msqlsfsc2d01	✓ Compliant	<a href="#">Details</a>	microsoft.sql/servers	East US 2	SFSC - Salesforce/RSGRFSCEU2...	4/18/24, 11:55:07 PM...
msqlsfsc2d02	✓ Compliant	<a href="#">Details</a>	microsoft.sql/servers	East US 2	SFSC - Salesforce/RSGRFSCEU2...	4/18/24, 11:55:07 PM...
msqlsfsc2p01	✓ Compliant	<a href="#">Details</a>	microsoft.sql/servers	East US 2	SFSC - Salesforce/RSGRFSCEU2...	4/18/24, 11:55:08 PM...
msqlsfsc2p02	✓ Compliant	<a href="#">Details</a>	microsoft.sql/servers	East US 2	SFSC - Salesforce/RSGRFSCEU2...	4/18/24, 11:55:08 PM...



# Mejores Prácticas



#GABMUGPeru

# Conclusiones



#GlobalAzure



**1** Asegura de que los recursos cumplen con los estándares, línea base de seguridad y otros requisitos de la organización.

**2** Es crucial un compromiso continuo con la actualización y revisión de políticas.

**3** Automatización del cumplimiento.

**4** Visibilidad y control.

**5** Impacto cultural de seguridad.



# Recursos Técnicos

- [Directivas recomendadas para los servicios de Azure - Azure Policy | Microsoft Learn](#)
- [Azure Policy: administración de la nube y el cumplimiento normativo | Microsoft Azure](#)
- [Introducción a Azure Policy - Azure Policy | Microsoft Learn](#)



# Patrocinadores



Microsoft



25 mibanco

años



Colabora



nuvem

