centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 884A

Guía de configuración segura para Azure

Mayo 2024

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2024.05.08 18:33:07 +02'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: Pte. de asignar
Fecha de Edición: mayo de 2024

ÍNDICE

1. GUÍA SEGURA PARA AZURE

1.1 DESCRIPCIÓN DEL USO DE ESTA GUÍA

El contenido de esta guía muestra el despliegue y configuración basados en la administración de seguridad y la protección avanzada contra amenazas para cargas de trabajo en la nube pública de Microsoft Azure.

Siguiendo los pasos de configuración descritos en esta guía se puede:

a) Proteger las aplicaciones contra explotaciones y vulnerabilidades comunes con un firewall de aplicaciones.

b) Proteger los recursos de Azure de ataques por denegación de servicio.

c) Desplegar métodos de autenticación.

d) Desplegar las claves criptográficas y otros secretos usados por las aplicaciones y los servicios en la nube.

e) Seguir las recomendaciones en cuanto a la asignación de roles para la gestión y administración de tareas de Azure.

1.2 DEFINICIÓN DEL SERVICIO

Azure es una plataforma de nube completa que puede hospedar aplicaciones, simplificar el desarrollo de nuevas aplicaciones e incluso mejorar las aplicaciones locales. Azure integra los servicios en la nube que necesita para desarrollar, probar, implementar y administrar sus aplicaciones. En esta guía se tratan las configuraciones necesarias para cumplir con las medidas de protección del Esquema Nacional de Seguridad.

1.3 FUNCIONALIDADES DEL SERVICIO DE AZURE

En el portal Microsoft Azure existen diferentes servicios de infraestructura y de plataforma que se pueden configurar de la forma que se necesite de manera sencilla.

Entre los servicios, se dispone de infraestructuras denominadas:

a) IaaS (Infrastructure as a Service): almacenamiento, redes, y máquinas virtuales, entre otros.

b) PaaS (Platform as a Service): bases de datos de alta disponibilidad, servicios que permiten publicar aplicaciones web y backend para aplicaciones móviles, servicios de mensajería fiable, entre otros.

Estos servicios son compatibles con una amplia gama de tecnologías, incluyendo bases de datos Oracle, Linux, PHP, iOS, MySQL, Android, entre otras.

Además, estos servicios pueden configurarse para tener alta disponibilidad. En caso de fallo, se activaría el servicio de respaldo, garantizando así una disponibilidad superior.

Esta nube cumple con las medidas de seguridad exigidas para conseguir la certificación de conformidad del Esquema Nacional de Seguridad en categoría ALTA.

2. DESPLIEGUE SEGURO PARA AZURE

En esta guía se define una conexión segura desde la consola de Azure PowerShell que se ejecuta desde el ordenador y además desde el portal de Azure. Para ello, se deben seguir los pasos que se detallan a continuación.

2.1 USO DE LA CONSOLA DE POWERSHELL

2.1.1 AZURE POWERSHELL

El módulo **Azure PowerShell** se usa para crear y administrar recursos de Azure desde la línea de comandos o a través de scripts.

Nota: Para instalar el módulo de Azure PowerShell se puede consultar el siguiente enlace de Microsoft: https://learn.microsoft.com/es-es/powershell/azure/install-azure-powershell

Azure PowerShell admite varios métodos de autenticación. El método más directo es utilizar la misma ventana de navegador web que el portal de Azure, mediante Azure Cloud Shell, que hace uso de la misma sesión del navegador. Aunque también se puede utilizar desde su navegador. En ambos casos, la conexión siempre es segura.

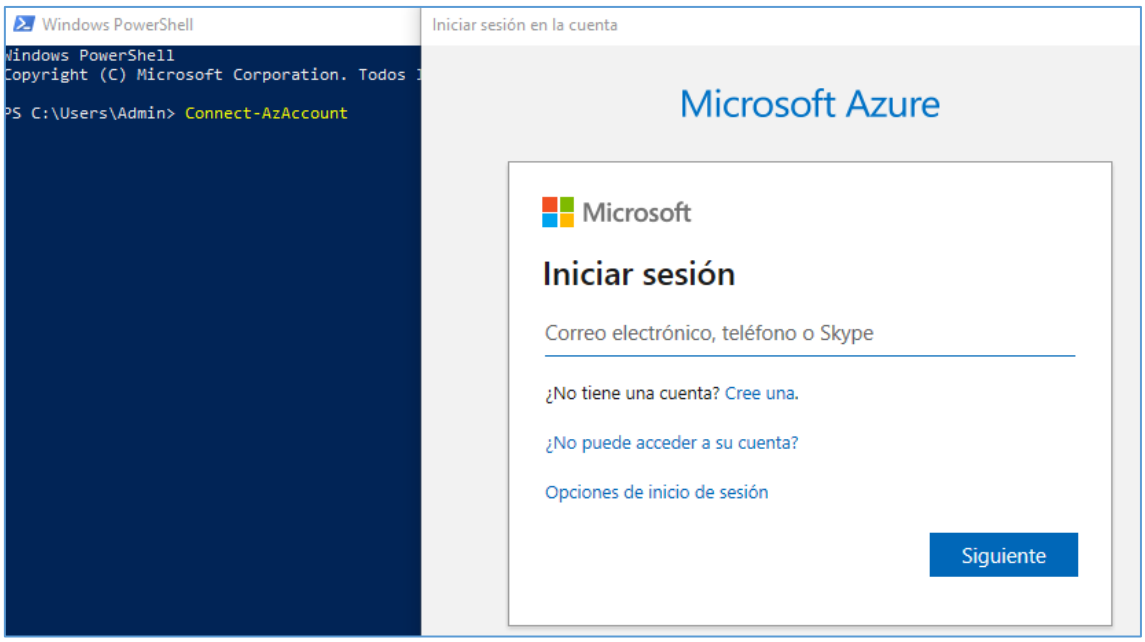
En una sesión local de PowerShell, se pide iniciar sesión interactivamente en un navegador web.

En el caso de ejecutar scripts de automatización, el enfoque recomendado es usar una Entidad de Servicio (Service Principal) con los permisos mínimos necesarios. Al restringir los permisos se protegen los recursos de Azure ante accesos no autorizados.

2.1.1.1 INICIO DE SESIÓN

a) Para iniciar sesión de forma interactiva, utilizar el cmdlet **Connect-AzAccount**.

```
#  PS C:\> Connect-AzAccount
```



b) Se solicita cuenta de correo y su contraseña del administrador del Tenant.

Nota: Se recomienda que para la gestión de Azure cree previamente una entidad de servicio. Consultar la sección *[3.1.1 Control de Acceso/Creación de cuentas de usuarios]* de la presente guía. Nota: Texto de la nota.

2.1.1.2 AUTENTICACIÓN BASADA EN CONTASEÑA

Para obtener las credenciales de la entidad de servicio utilice el comando cmdlet **Get-Credential**. Este cmdlet muestra un aviso para un nombre de usuario y una contraseña. Use el identificador de la entidad de servicio como nombre de usuario.

Desde la consola de Powershell ejecutar el siguiente comando:

```
# PS C:\> $pwshcredential = Get-Credential
# PS C:\> Connect-AzAccount -ServicePrincipal -Credential $pwshcredential -Tenant $tenantId
```

En escenarios de automatización, se puede crear las credenciales a partir de un nombre de usuario y una cadena segura (Contraseña), la sintaxis seria la siguiente:

```
# PS C:\> $password = ConvertTo-SecureString <use a secure password here> -AsPlainText -Force
# PS C:\> $pscredential = New-Object System.Management.Automation.PSCredential('service principal name/id', $password)
# PS C:\> Connect-AzAccount -ServicePrincipal -Credential $pscredential -Tenant $tenantId
```

2.1.1.3 AUTENTICACIÓN BASADA EN CERTIFICADO

La autenticación basada en certificados requiere que Azure PowerShell pueda recuperar información de un almacén de certificados local en función de una huella digital del certificado.

Para ello, ejecutar el siguiente comando Powershell.

```
# PS C:\> Connect-AzAccount -ApplicationId $applicationId -Tenant $tenantId -CertificateThumbprint <thumbprint>
```

Nota: Si usa una entidad de servicio en lugar de una aplicación registrada, agregue el argumento -ServicePrincipal y proporcione el identificador de la entidad de servicio como el valor del parámetro -ApplicationId.

```
# PS C:\> Connect-AzAccount -ServicePrincipal -ApplicationId $servicePrincipalId -Tenant $tenantId -CertificateThumbprint <thumbprint>
```

Nota: Puede encontrar más información en: https://learn.microsoft.com/es-es/powershell/azure/authenticate-noninteractive#certificate-based-authentication

2.1.1.4 CAMBIO DE LA SUSCRIPCIÓN ACTIVA

Muchas entidades cuentan con varias suscripciones. En Azure se puede identificar cada una de ellas y operar en configuraciones mediante PowerShell o desde el portal.

Para cambiar las suscripciones, primero se debe recuperar un objeto de contexto de Azure PowerShell con Get-AzSubscription y, después, cambiar el contexto actual con Set-AzContext.

En el ejemplo siguiente se muestra cómo obtener una suscripción en el Tenant activo actualmente y establecer la sesión como activa.

```
#   PS C:\> Connect-AzAccount -ServicePrincipal -ApplicationId
    $servicePrincipalId -Tenant $tenantId -CertificateThumbprint <thumbprint>
```

Para agregar un nuevo contexto después de iniciar sesión, utilice **Set-AzContext**.

```
#   PS C:\> $Context = Get-AzSubscription -SubscriptionId ...
#   PS C:\> Set-AzContext $Context
```

Para agregar un nuevo contexto después de iniciar sesión, utilice **Set-AzContext**.

```
#   PS C:\> Set-AzContext -Subscription "Suscripción 1" -Name "Dominio"
```

En relación con la seguridad es importante quitar todas las credenciales y los contextos asociados de un usuario o una entidad de servicio mediante el comando **Disconnect-AzAccount** (también conocido como **Logout-AzAccount**).

```
#   PS C:\> Disconnect-AzAccount "usuario1@dominio"
```

2.1.2 MICROSOFT GRAPH POWERSHELL

Microsoft Entra ID (anteriormente conocido como Azure AD), es un servicio de administración de identidades y acceso basado en la nube. El módulo de Microsoft Graph PowerShell contiene un conjunto de cmdlets que ayudan a administrar identidades a escala, desde la automatización de tareas hasta la administración de usuarios de forma masiva en Microsoft Entra ID.

Para instalar el módulo de Microsoft Graph PowerShell se puede consultar el siguiente enlace de Microsoft:

https://learn.microsoft.com/es-es/powershell/microsoftgraph/installation

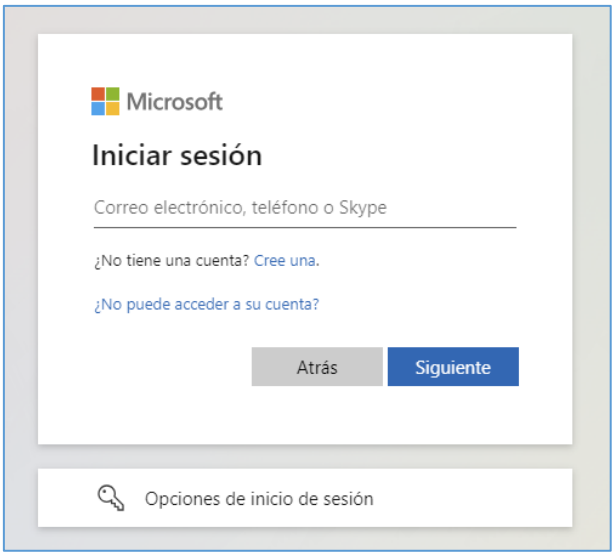
Microsoft Graph admite dos tipos de autenticación: acceso delegado y acceso solo para aplicaciones.

2.1.2.1 ACCESO DELEGADO

a) Cada API en Microsoft Graph está protegida por uno o más ámbitos de permiso. El comando **Connect-MgGraph** se utiliza para iniciar sesión en los ámbitos de permiso requeridos (en el siguiente ejemplo se utilizan los ámbitos "User.Read.All" y "Group.ReadWrite.All").

```
#   PS C:\> Connect-MgGraph -Scope "User.Read.All","Group.ReadWrite.All"
```

b) Se requerirá iniciar sesión con una cuenta de administrador. Se requerirá iniciar sesión con una cuenta de administrador.



2.1.2.2 ACCESO SOLO PARA APLICACIONES

a) Se requiere abrir una consola PowerShell y correr el siguiente comando reemplazando los valores personalizados.

```
# PS C:\> Connect-MgGraph -ClientId YOUR_APP_ID -TenantId YOUR_TENANT_ID -CertificateName YOUR_CERT_SUBJECT ## Or -CertificateThumbprint instead of -CertificateName
```

b) Si el comando es exitoso, aparecerá el mensaje: **Welcome To Microsoft Graph!**

c) Para verificar que se ha autenticado con la opción "solo para aplicaciones" se requiere ejecutar el comando **Get-MgContext**.

```
# PS C:\> Get-MgContext
```

d) La salida debería mostrar un mensaje parecido al siguiente:

```
# PS C:\> ClientId              : YOUR_APP_ID
# PS C:\> TenantId              : YOUR_TENANT_ID
# PS C:\> CertificateThumbprint :
# PS C:\> Scopes                : {Group.Read.All, User.Read.All}
# PS C:\> AuthType              : AppOnly
# PS C:\> CertificateName       : YOUR_CERT_SUBJECT
# PS C:\> Account               :
# PS C:\> AppName               : Graph PowerShell Script
# PS C:\> ContextScope          : Process
```

Nota: Puede encontrar más información en https://learn.microsoft.com/es-es/powershell/microsoftgraph/app-only

2.1.2.3 CIERRE DE SESIÓN

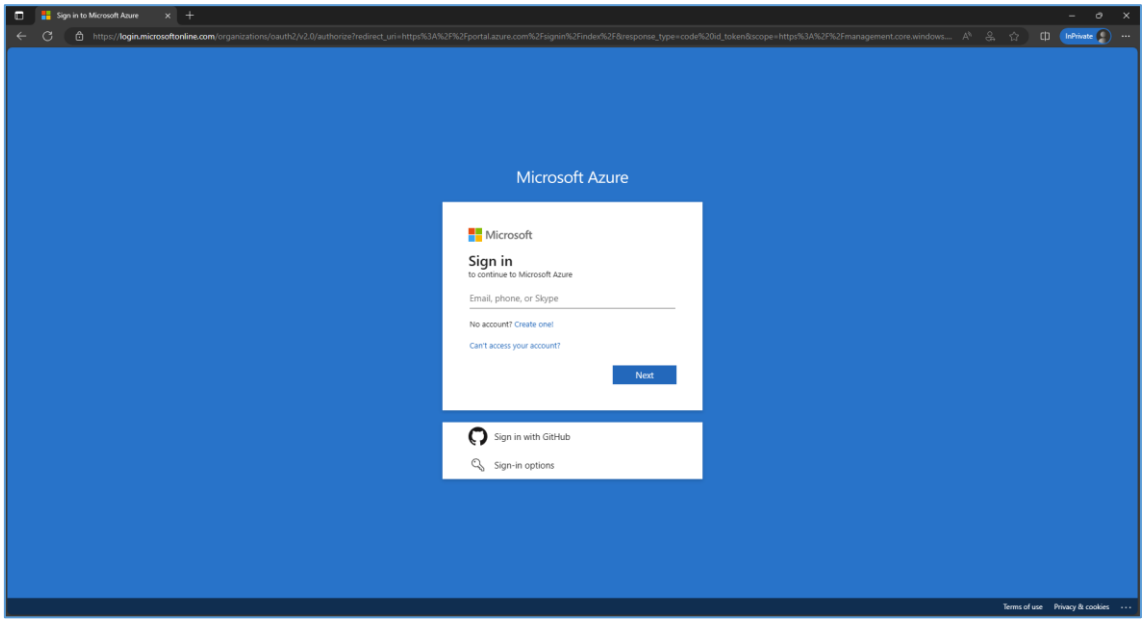
a) Utilizar el comando Disconnect-MgGraph para cerrar sesión.

```
#   PS C:\> Disconnect-MgGraph
```

Nota: Puede encontrar más información sobre el módulo de Microsoft Graph de PowerShell en https://learn.microsoft.com/es-es/powershell/microsoftgraph/

2.2 ACCESO AL PORTAL DE AZURE DESDE UN NAVEGADOR

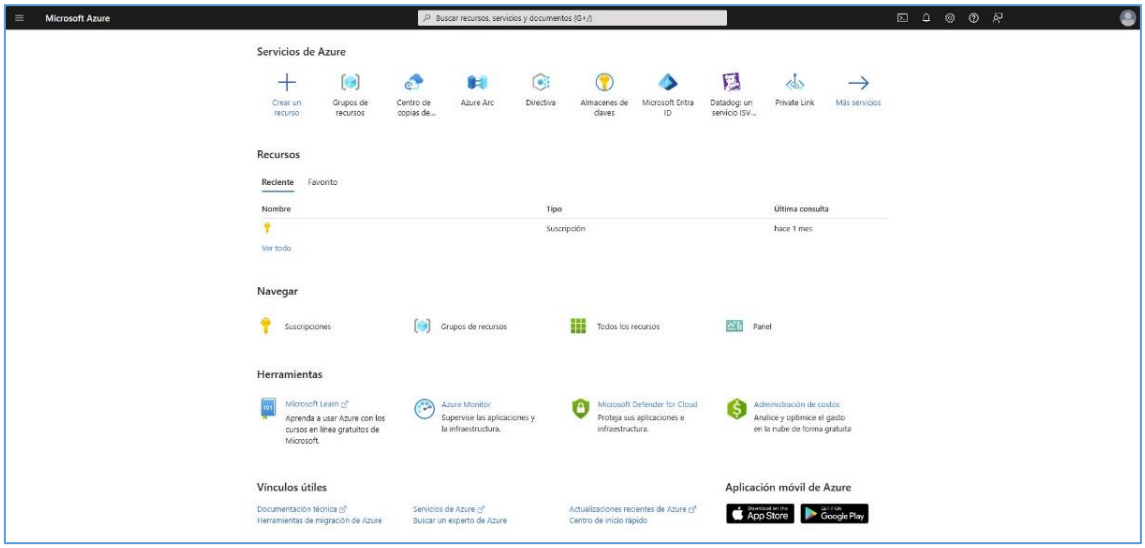
a) Se debe acceder al portal de Azure con un usuario Administrador. El usuario debe acceder al portal de Azure a través del siguiente enlace: **portal.azure.com**



Nota: Se solicita una cuenta de correo electrónico y contraseña.

2.2.1 CONFIGURACIÓN DEL PORTAL

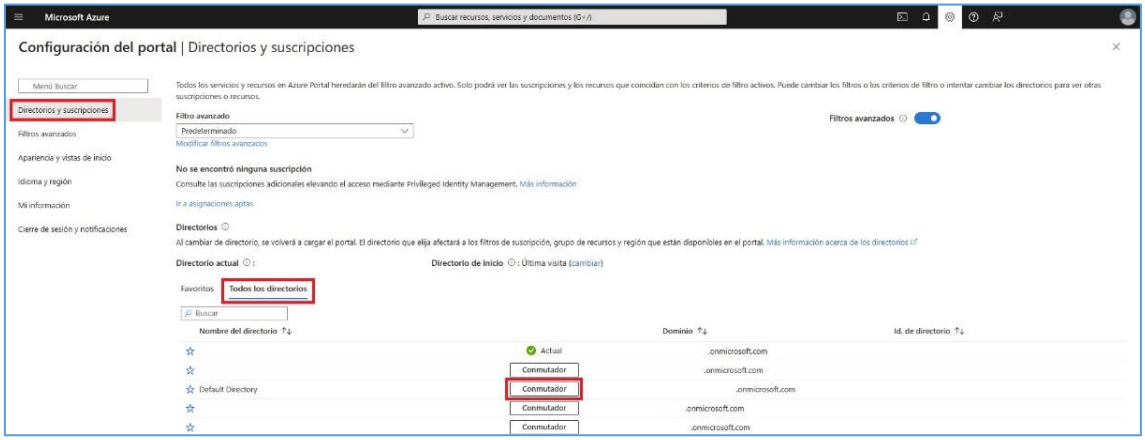
Una vez se haya iniciado sesión en el portal de Azure, se muestra una página de inicio con los iconos de todas las aplicaciones a las que tiene acceso.



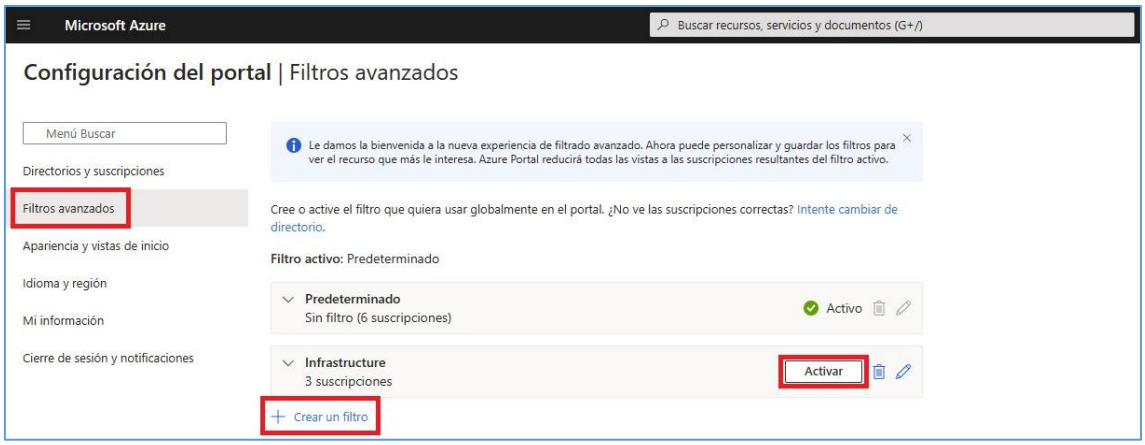
a) Pulsar sobre la rueda que se describe a continuación.

Nota: Si tiene varias suscripciones desde aquí puede cambiar las suscripciones por defecto.

b) Para cambiar de directorio, pulsar sobre [Directorios y suscripciones], en la sección de [Todos los directorios], si se dispone de acceso se podrá cambiar pulsando sobre [Conmutar].

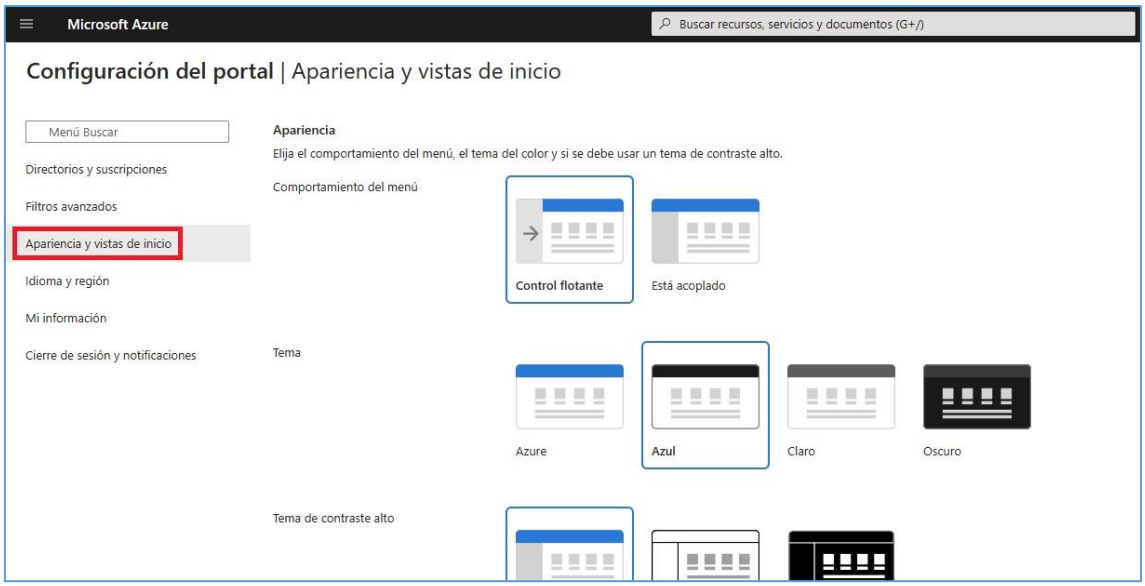


c) Si dispone de varias suscripciones dentro del mismo directorio, pulsando sobre [Filtros avanzados], podemos crear filtros pulsando sobre [Crear un filtro]. Una vez creado pulsamos sobre [Activar] para usarlo.

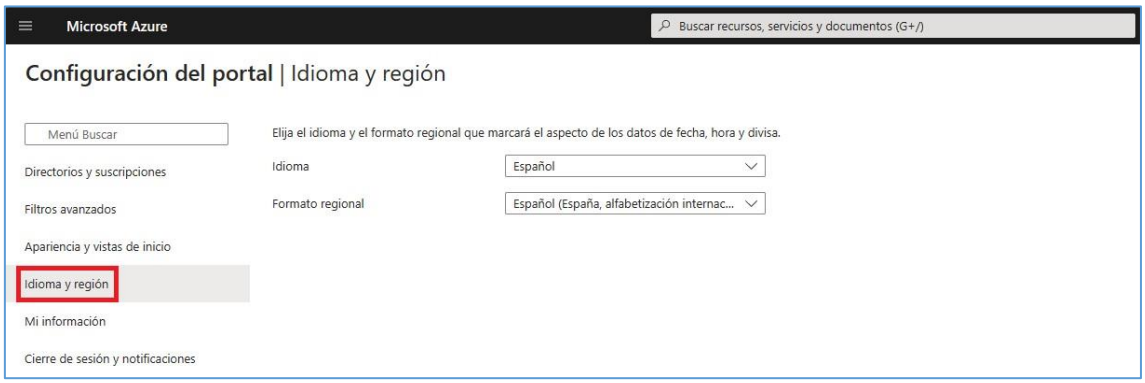


Nota: Los filtros permiten diferentes tipos de condicionales estáticos y dinámicos.

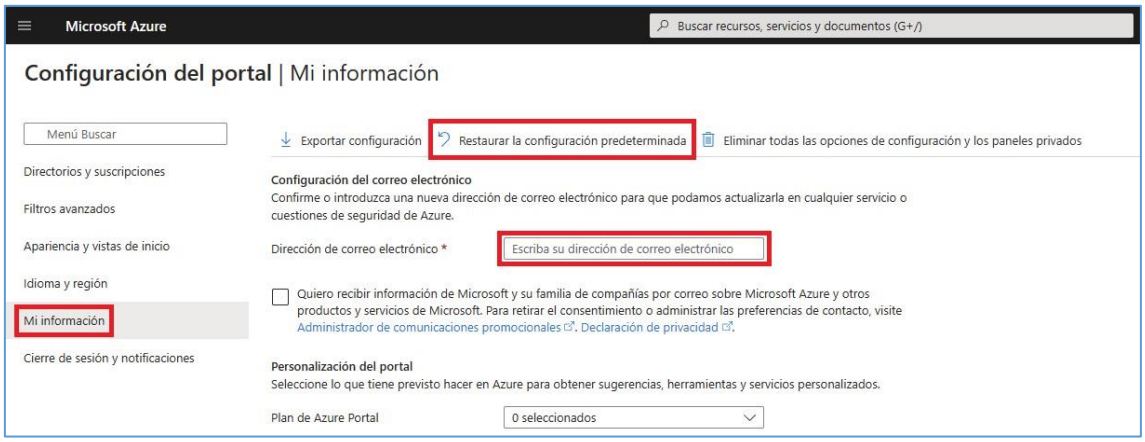
d) Si desea personalizar la vista del panel principal pulsando sobre [Apariencia y vistas de inicio].



e) Se puede modificar el idioma por defecto y el formato regional pulsando sobre [Idioma y región].

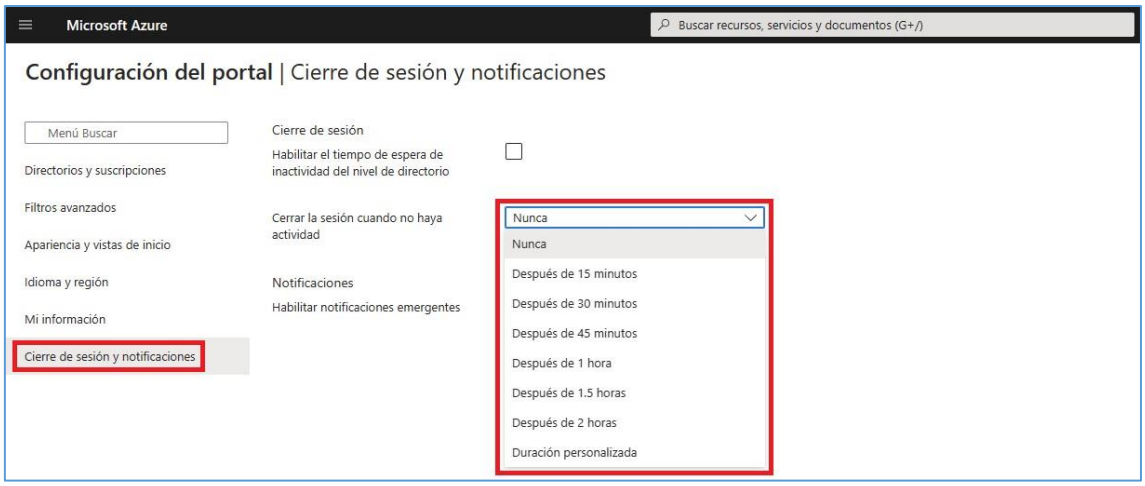


f) Si desea recibir información sobre actualizaciones de características del portal de Azure, pulsando sobre [Mi información] tenemos una sección donde podemos añadir un correo electrónico para que le envíen información.



Nota: En caso de querer restaurar toda la configuración por defecto pulsar en **Restaurar la configuración predeterminada.**

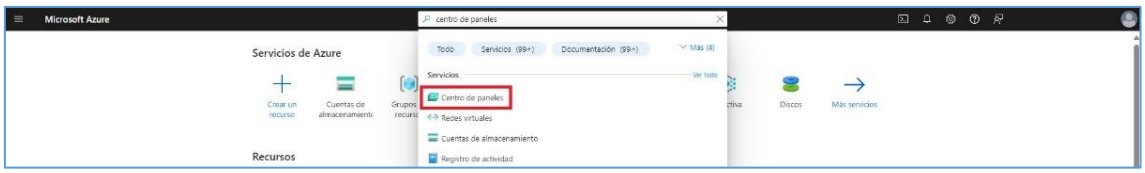
g) Si desea establecer un cierre de sesión por inactividad, desplegar la barra y elegir una duración personalizada.



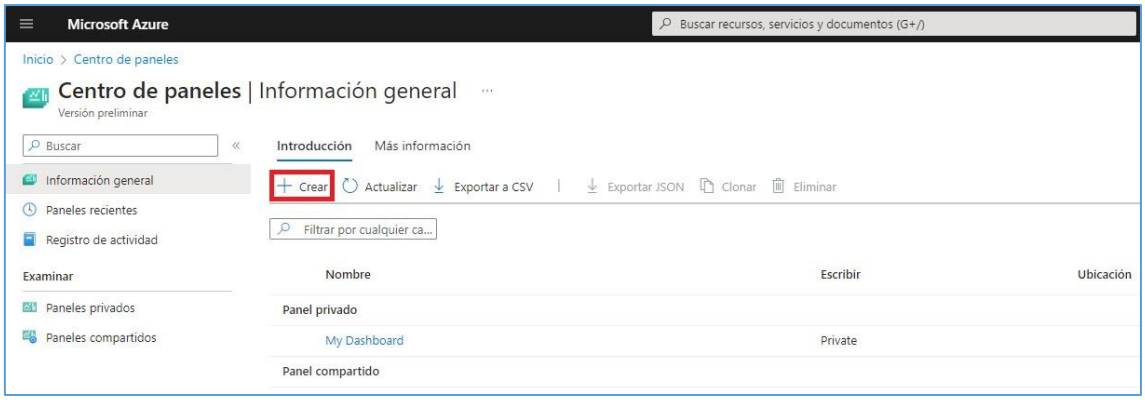
2.2.2 PANEL PERSONALIZADO

Desde el portal de Azure se puede personalizar y crear múltiples paneles creando un nuevo **Panel** (Dashboard) o editar uno existente. Para ello, se recomienda seguir estas directrices.

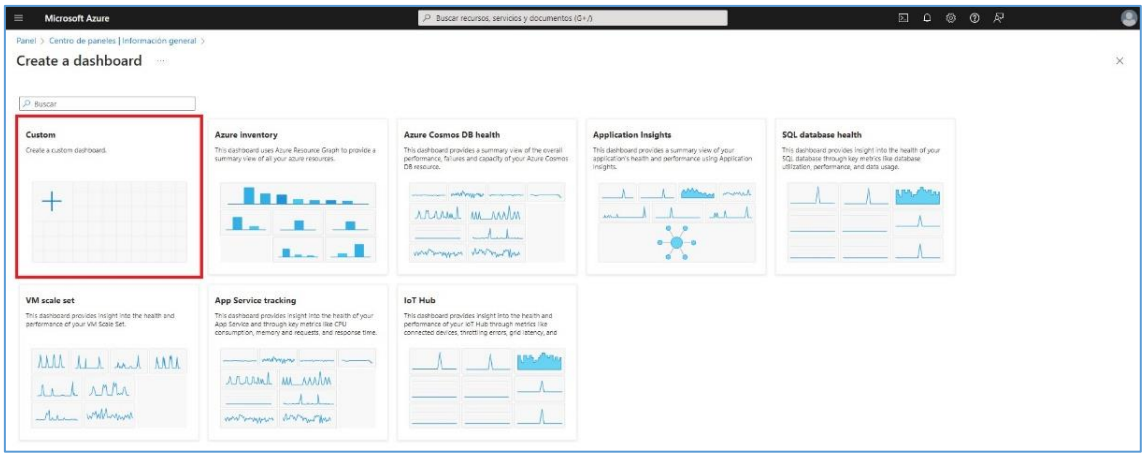
a) En el buscador escribir [Centro de paneles].



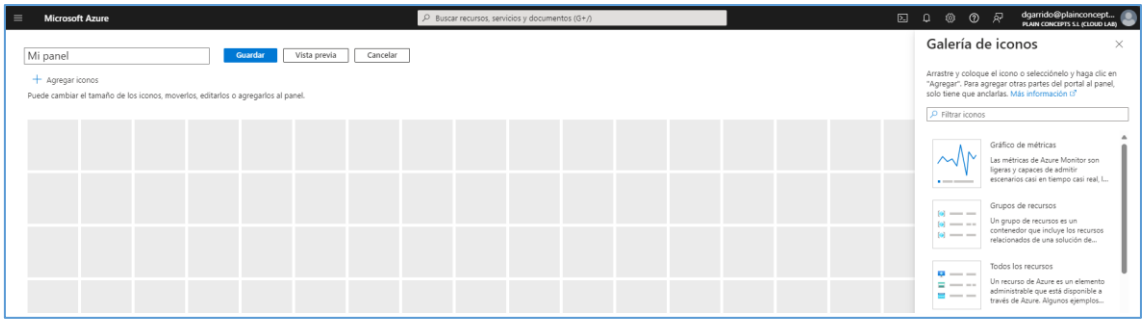
b) Pulsar sobre [Crear].



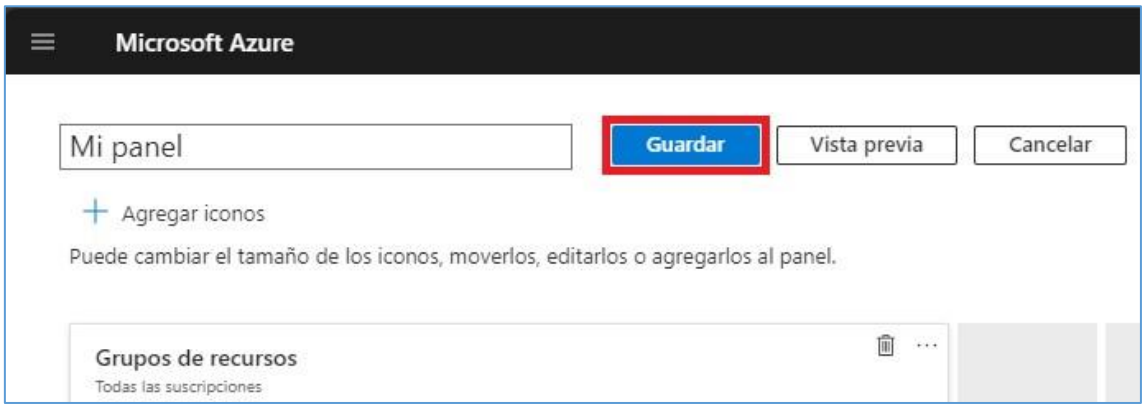
c) Hay disponibles varios tipos de paneles predefinidos. Para crear un panel personalizado pulsar sobre [Custom].



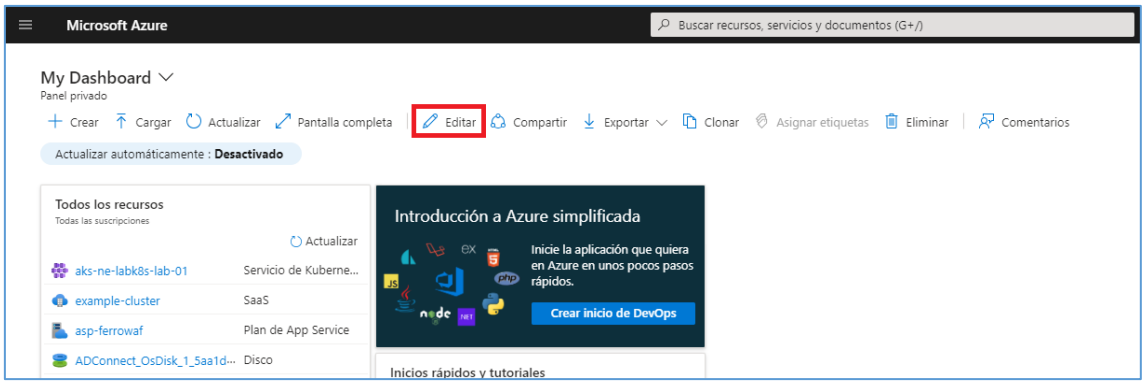
Nota: Desde aquí se puede agregar todos los servicios que se desee visualizar en el panel personalizado.



d) Para finalizar, pulsar sobre [Guardar].



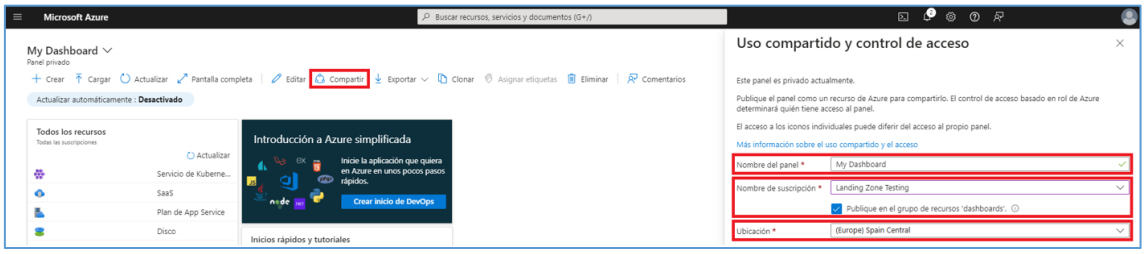
Nota: Se puede editar el panel o los paneles que tenga pulsando en editar.



2.2.3 COMPARTIR PANEL

Una vez creado un nuevo panel personalizado, se puede publicar y gestionar los accesos a los usuarios que se pueden visualizar y operar en él siguiendo estas directrices:

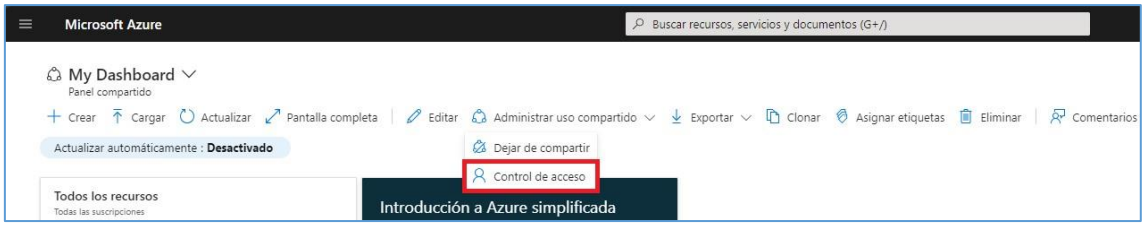
a) Desde el Panel, pulsar sobre [Compartir].



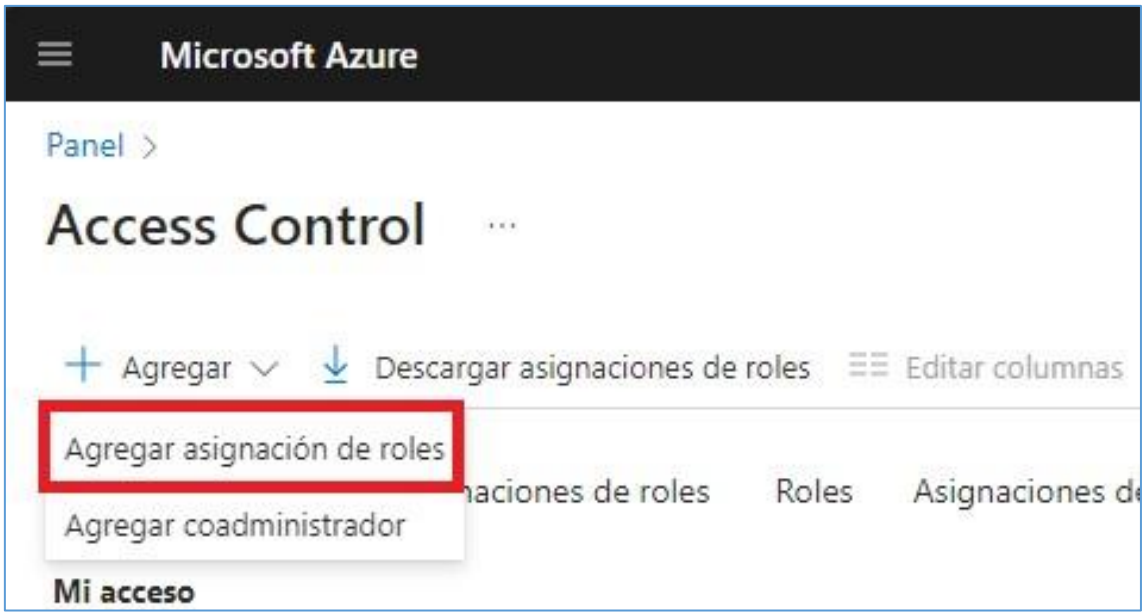
Nota: Aparece este panel donde debe definir un nombre, su suscripción y la ubicación que es Centro de España.

b) Para finalizar, pulsar en [Publicar].

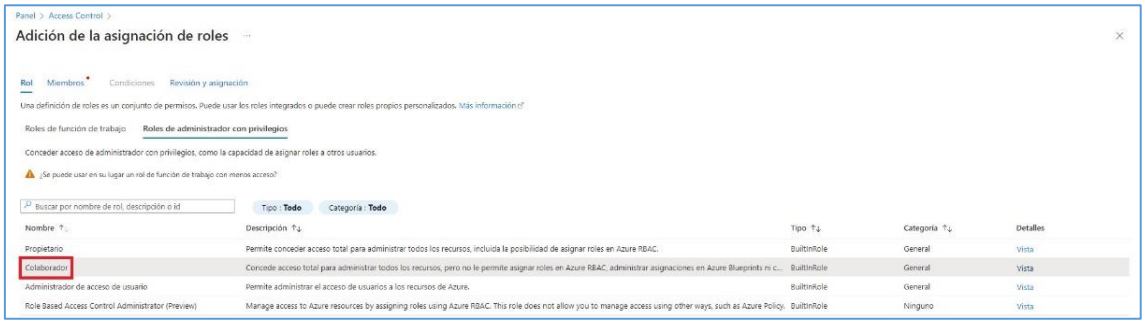
c) Una vez publicado aparece un nuevo asistente donde se debe administrar los usuarios que tienen acceso. Para ello, pulsar en [Administrar uso compartido / Control de acceso].



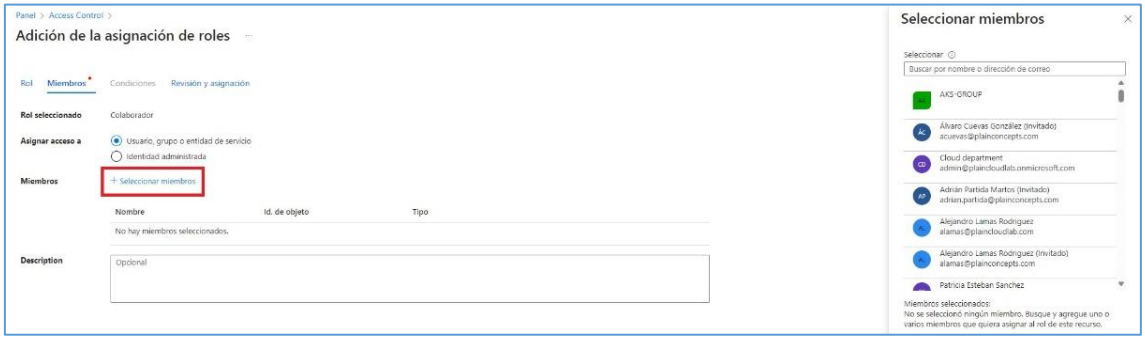
d) Pulsar en [Agregar / Agregar asignación de roles].



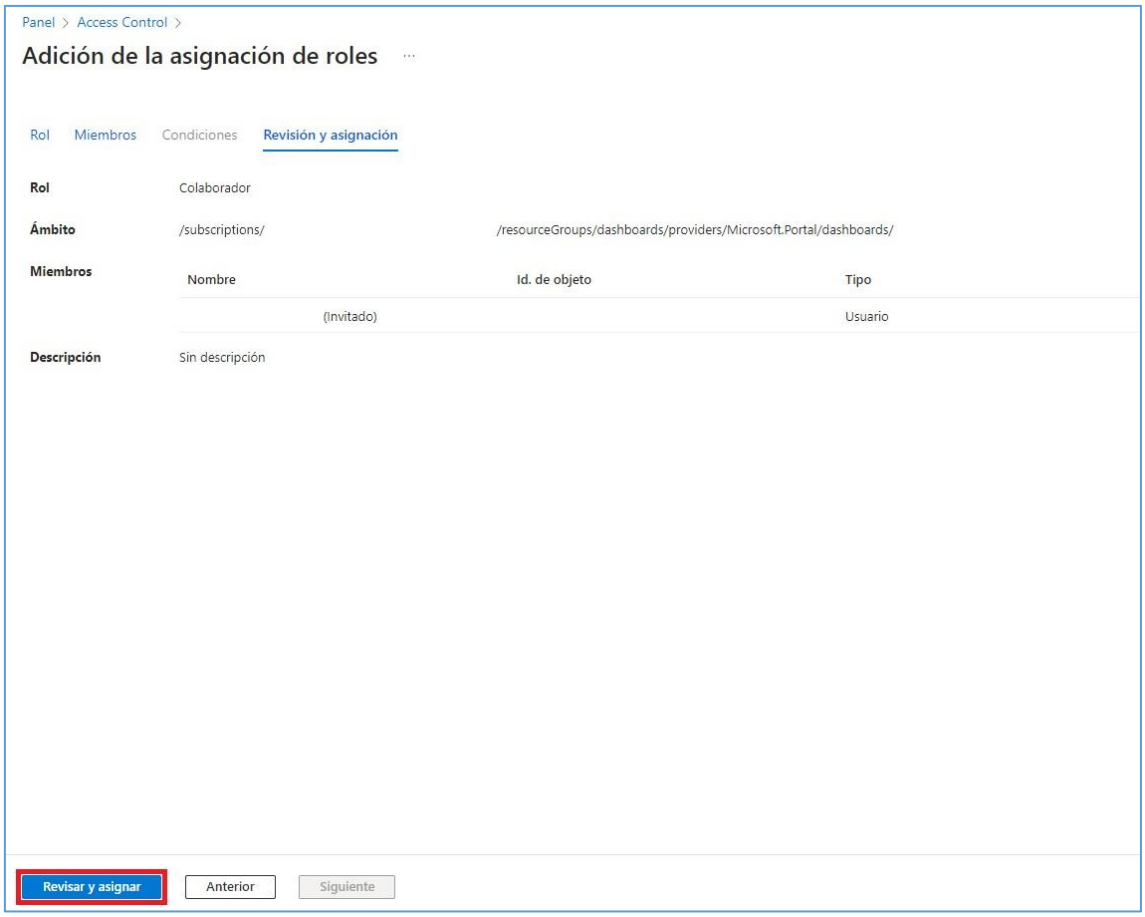
e) Seleccione el rol que va a conceder al usuario. En este ejemplo se asigna el rol de Colaborador.



f) Seleccione el usuario/s a los que se desea asignar permisos pulsando sobre [Seleccionar miembros].

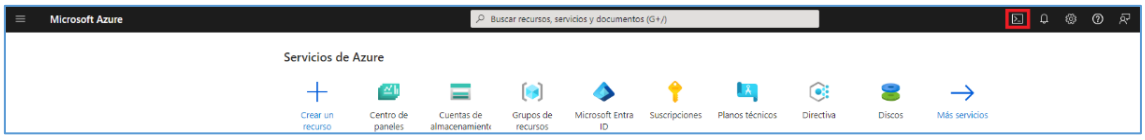


g) Para finalizar, pulsar en [Revisar y asignar].

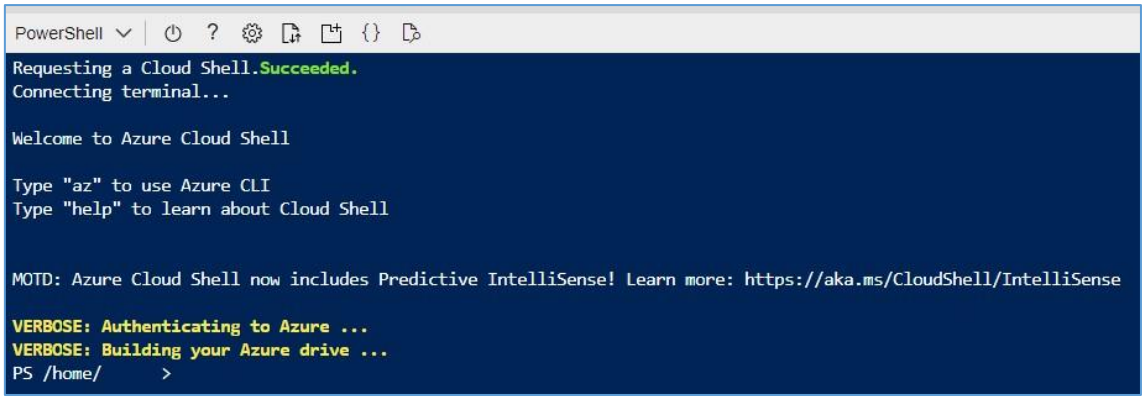


2.2.4 USO DE LA CONSOLA DE CLOUD SHELL

Desde el portal de Azure se puede utilizar Azure Cloud Shell que permite acceder desde el explorador y administrar todos los recursos de Azure. Pulsar sobre el icono que muestra la imagen.



Nota: Al pulsar el terminal validara sus credenciales.



Desde esta consola se puede ejecutar comandos de PowerShell. Por defecto tiene instalado el módulo de Azure PowerShell.

A continuación, se añaden algunos comandos recomendados para la administración de los servicios de Azure.

a) Enumerar las suscripciones a las que se tiene acceso.

```
#  PS C:\> Get-AzSubscription
```

b) Establecer una suscripción preferente

```
#  PS C:\> Set-AzContext -Subscription "{Nombre de la suscripción}"
```

Nota: Se puede consultar información sobre más comandos: https://docs.microsoft.com/es-es/azure/cloud-shell/overview

2.3 GESTIÓN DE RECURSOS EN AZURE

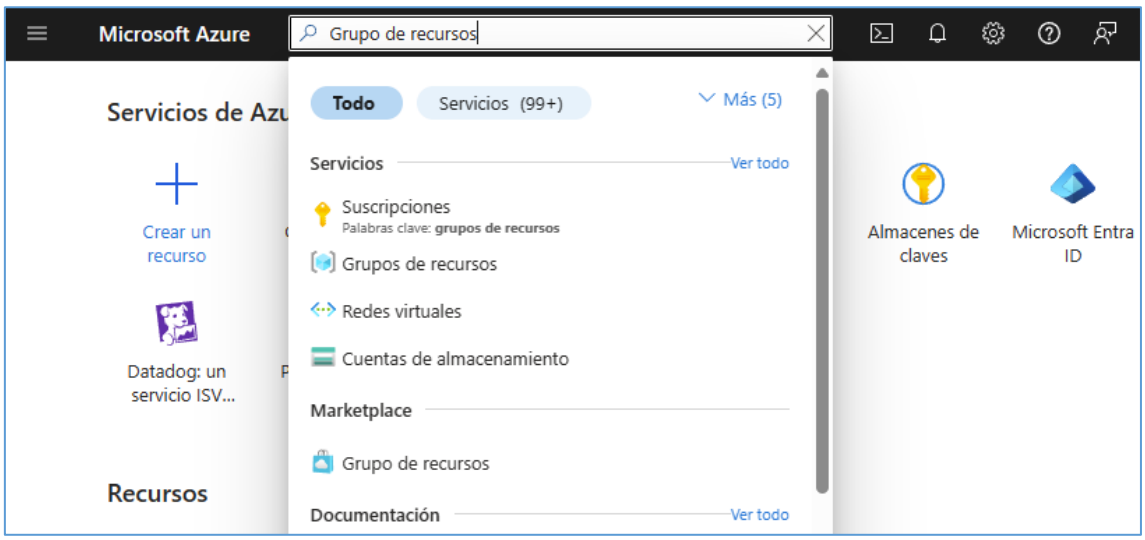
Para la administración de los recursos en Azure se utiliza Azure Resource Manager (ARM). Esto permite implementar aplicaciones y sus recursos de una forma coherente. Con ARM se facilita la administración y la visualización de los recursos. Se recomienda incluir los recursos con un mismo ciclo de vida en el mismo grupo de recursos.

2.3.1 GRUPO DE RECURSOS

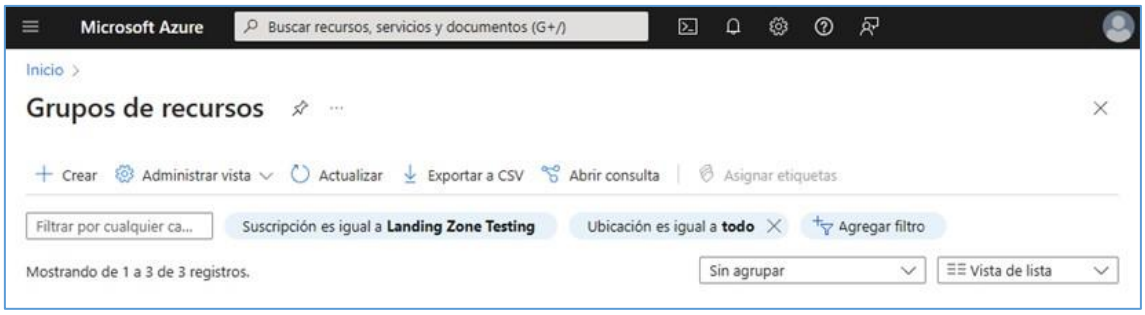
Un grupo de recursos es un contenedor donde se almacenan los recursos que se administran como grupo.

2.3.2 CREACIÓN DESDE EL PORTAL

a) En el buscador escribimos [Grupos de recursos].



b) Pulsamos sobre [Crear].

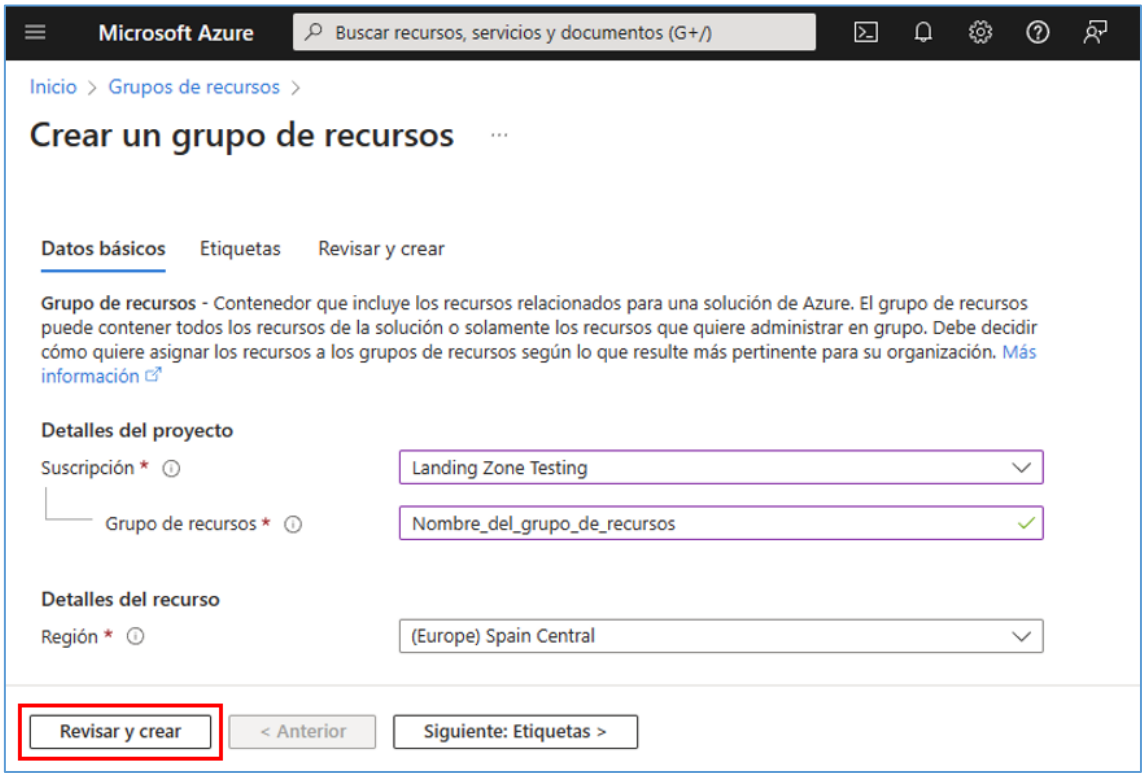


c) A continuación, se debe completar los siguientes campos.

- **Suscripción**: En la suscripción que se crea el recurso.
- **Grupo de Recursos**: Nombre que se asigna al grupo de recursos.

Nota: Al pulsar el terminal validara sus credenciales.

- **Región**: La recomendada es Centro de España.



d) Pulsar en [Revisar y crear].

2.3.3 CREACIÓN DESDE POWERSHELL

Se puede crear el grupo de recursos mediante la consola de PowerShell.

a) Copiar el contenido y ejecutar en PowerShell

```
#  PS C:\> New-AzResourceGroup -Name "{Nombre}" -Location "Spain Central"
```

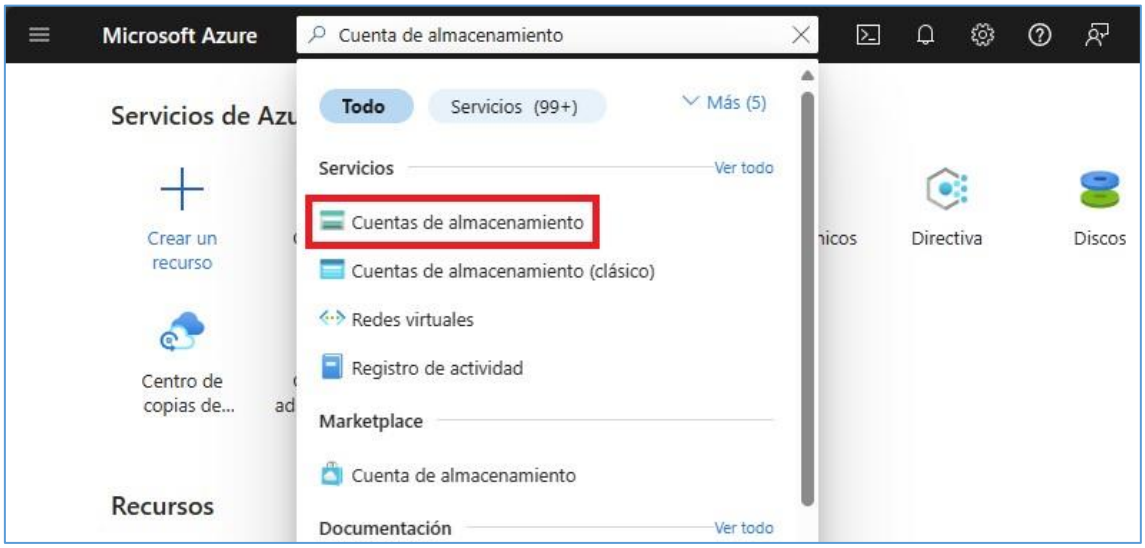
Nota: Se puede consultar la lista de comandos desde el siguiente enlace: https://learn.microsoft.com/es-es/cli/azure/resource?view=azure-cli-latest

2.3.4 CREACIÓN DE UNA CUENTA DE ALMACENAMIENTO

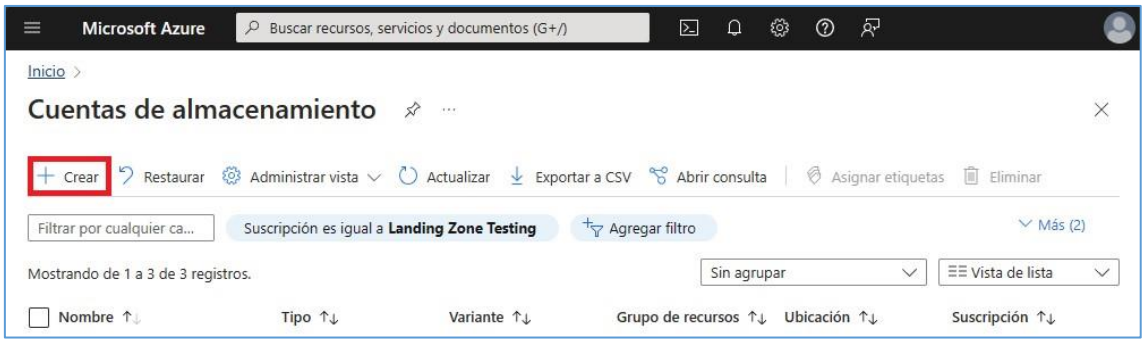
Azure Storage es la solución de almacenamiento de Microsoft para el alojamiento de los datos. Ofrece un almacén de objetos que se puede escalar de forma masiva.

A continuación, se describen los pasos que debe realizar para crear una nueva cuenta de almacenamiento.

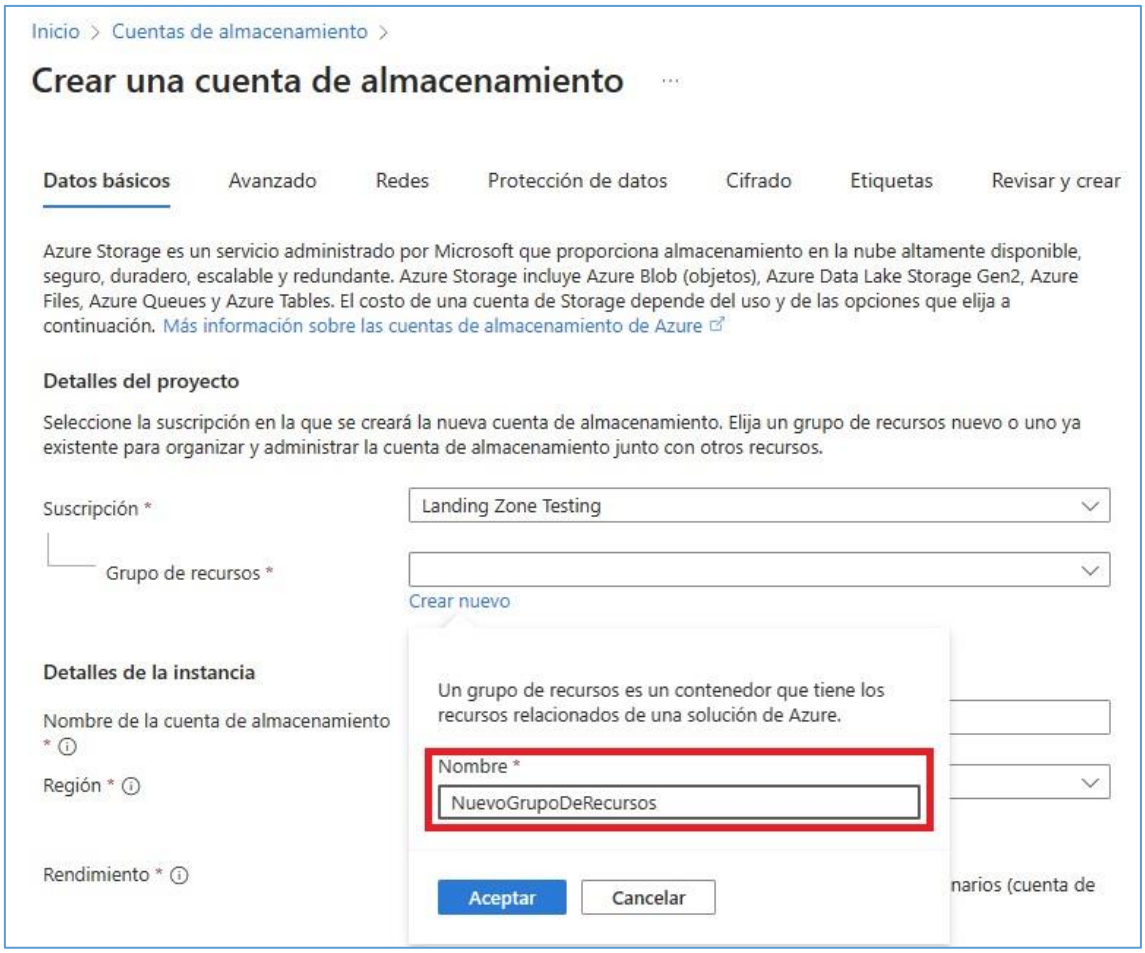
a) Desde el portal de Azure buscar [Cuenta de almacenamiento].



b) Pulsar en [Crear].



c) En grupo de recursos pulsar en [Crear nuevo]. En este momento se le asigna el nombre.



Nota: Se puede crear un nuevo grupo de recursos o desplegar y seleccionar uno existente para esta nueva cuenta de almacenamiento.

d) A continuación, se completan los siguientes campos.

a) **Nombre de cuenta**: Definir un nombre de cuenta.

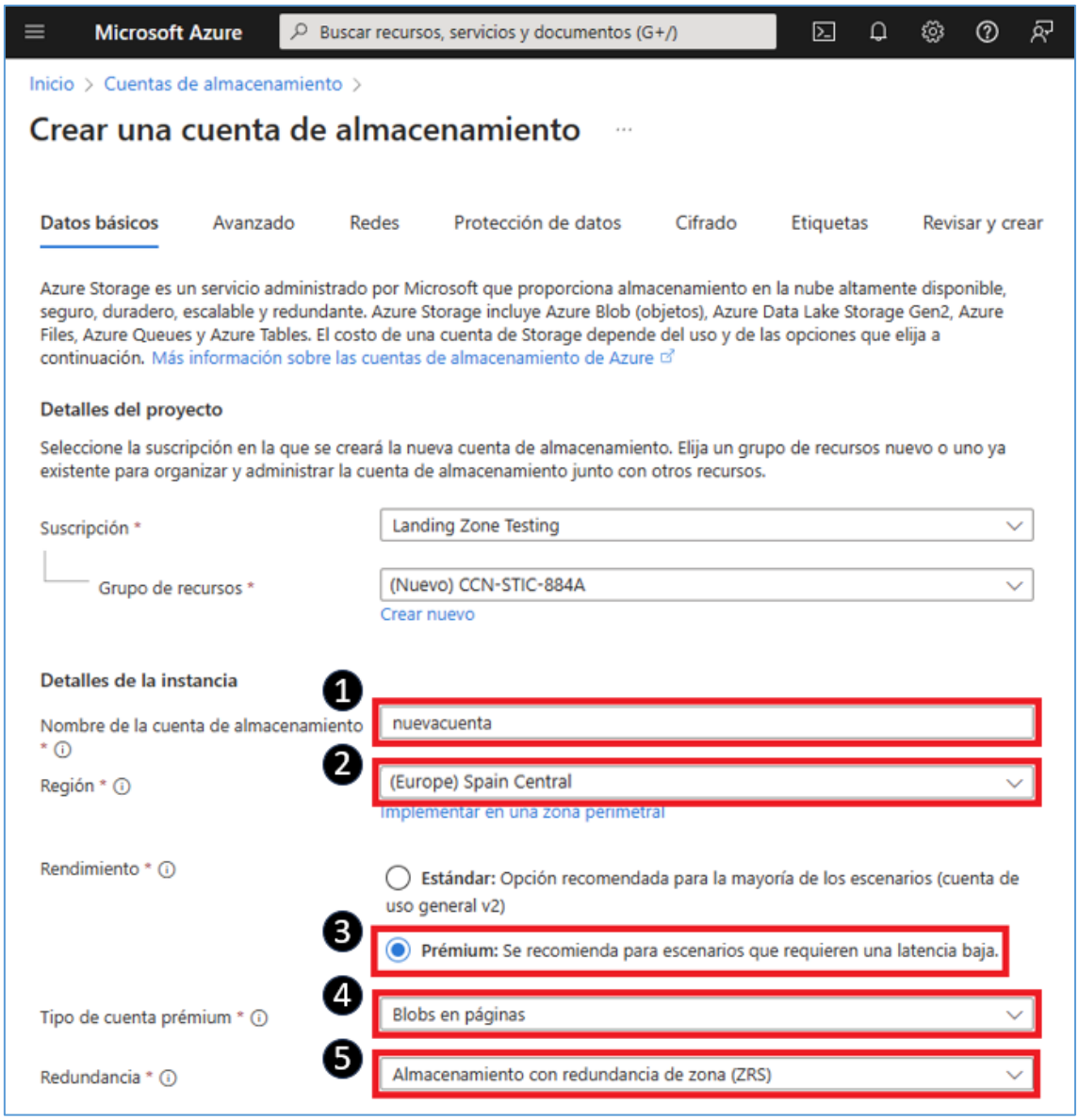
b) **Ubicación**: Seleccionar Centro de España.

c) **Rendimiento**: Se recomienda Premium.

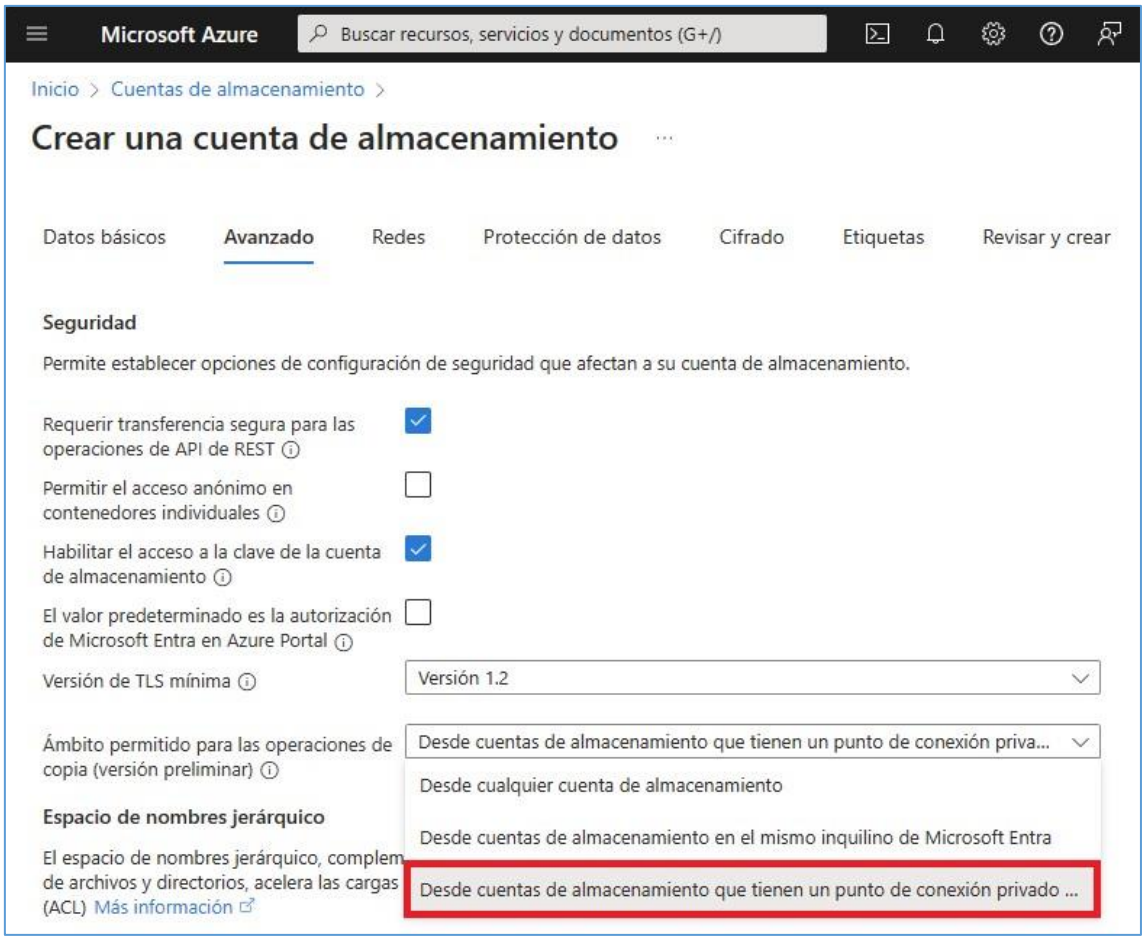
Nota: Las copias de seguridad de las cuentas de Standard Storage se realizan mediante unidades magnéticas y proporcionan un menor costo por GB. Se trata de la mejor opción para aplicaciones que requieren almacenamiento masivo o en las que el acceso a los datos es poco frecuente. Las copias de seguridad de las cuentas de Premium Storage se realizan mediante unidades de estado sólido y ofrecen un rendimiento uniforme y de latencia baja. Estas cuentas solo pueden usarse con discos de la máquina virtual y son la mejor opción para aplicaciones de E/S intensiva, como bases de datos. Asimismo, las máquinas virtuales que usan Premium Storage para todos los discos pueden acceder a un contrato de nivel de servicio del 99.9 %, incluso cuando no se ejecuten dentro de un conjunto de disponibilidad.

d) **Tipo de cuenta prémium**: Se recomienda Blob en páginas.

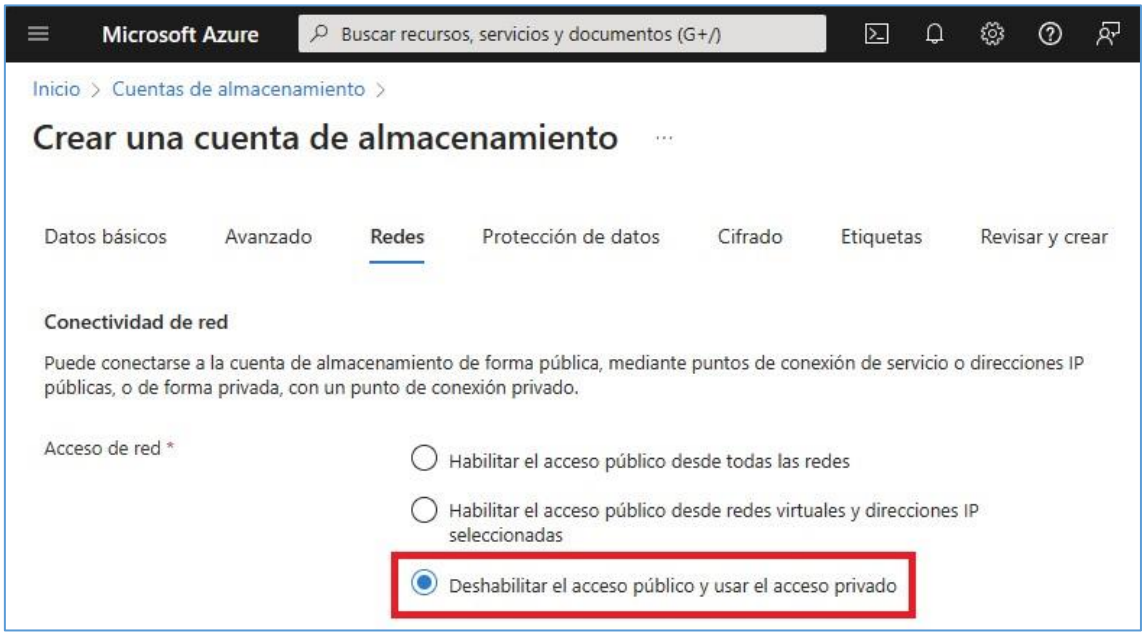
e) **Replicación**: Almacenamiento con redundancia de zona (ZRS).



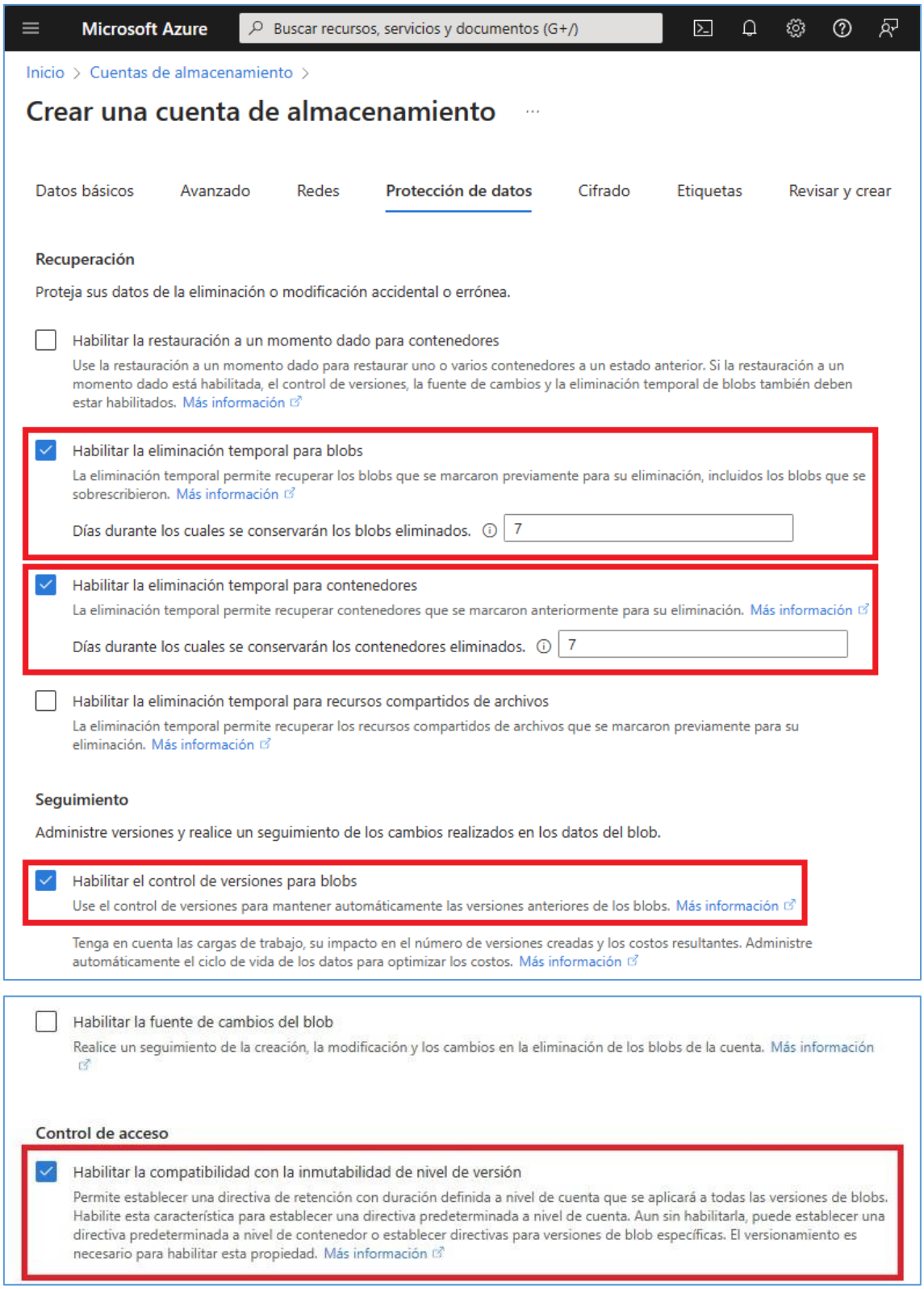
e) En la pestaña avanzado se recomienda seleccionar [Desde cuentas de almacenamiento que tienen un punto de conexión privado].



f) En la pestaña redes se recomienda seleccionar [Deshabilitar el acceso público y usar el acceso privado].



g) En la pestaña protección de datos seguir estas directrices.



a) **Habilitar la eliminación temporal para blobs**: Se recomienda un mínimo de 7 días.

Nota: En caso de borrado de un blob, permite su restauración un máximo de los días definidos en la directiva de retención.

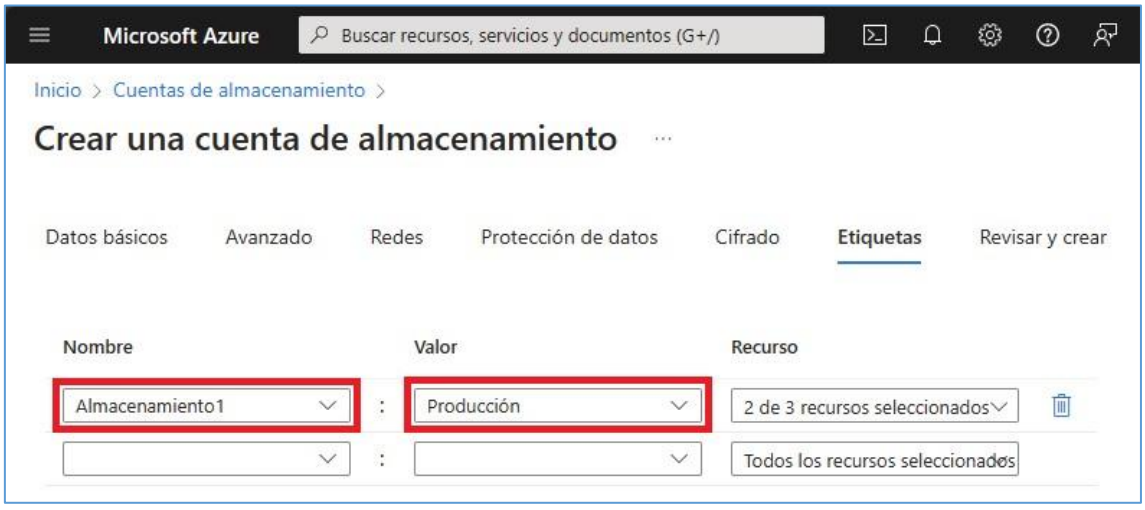
b) **Habilitar la eliminación temporal para los contenedores**: Se recomienda un mínimo de 7 días.

Nota: En caso de borrado de un contenedor, permite su restauración un máximo de los días definidos en la directiva de retención el contenedor y su contenido.

c) **Habilitar el control de versiones para blobs**: Pulsar sobre el cuadro vacío para habilitar.

d) **Habilitar la compatibilidad con la inmutabilidad de nivel de versión**: Pulsar sobre el cuadro vacío para habilitar.

h) En la pestaña Etiquetas escribir un nombre y valor que se tiene este almacenamiento.



i) Pulsar en [Revisar y crear].

j) Pulsar en [Crear].

3. CONFIGURACIÓN SEGURA PARA AZURE

En las secciones siguientes se presentan las medidas de aplicación comprendidas en los ámbitos Marco Operacional y Medidas de Protección del Esquema Nacional de Seguridad.

3.1 MARCO OPERACIONAL

3.1.1 CONTROL DE ACCESO

Microsoft Entra ID es la herramienta principal para la gestión de accesos y privilegios sobre los recursos de Azure dentro de una organización.

Si bien esta guía trata únicamente la gestión de cuentas de usuarios en la nube de Microsoft Azure con Microsoft Entra ID, también permite configuraciones hibridas.

Se puede consultar la documentación de identidades hibridas en el enlace: *https://learn.microsoft.com/es-es/entra/identity/hybrid/*

Para cumplir con los requisitos exigidos dentro del ámbito del ENS, en las siguientes secciones se trata la configuración inicial, la gestión de cuentas de usuario y la administración de Microsoft Entra ID.

Nota: En esta guía no se trata cómo administrar usuarios y objetos de **Directorio Activo de Windows Server**. Para este tipo de actividades, se recomienda consultar la guía CCN-STIC-870A Implementación del ENS en Windows Server 2012 R2.

3.1.1.1 IDENTIFICACIÓN

El proveedor de identidades es el responsable de comprobar la identidad de los usuarios y las aplicaciones que existen en el directorio de una organización y de emitir tokens de seguridad tras la autenticación correcta de dichos usuarios y aplicaciones.

Cualquier aplicación que necesite externalizar la autenticación a la plataforma de identidad de Microsoft se debe registrar en Microsoft Entra ID. Este registra la aplicación y la identifica de forma única en el directorio.

Para ello, se deben crear cuentas en Microsoft Entra ID.

También destacar que en esta guía solo se describe la gestión de cuentas Microsoft Entra ID en su *Tenant* pero no en entornos Híbridos.

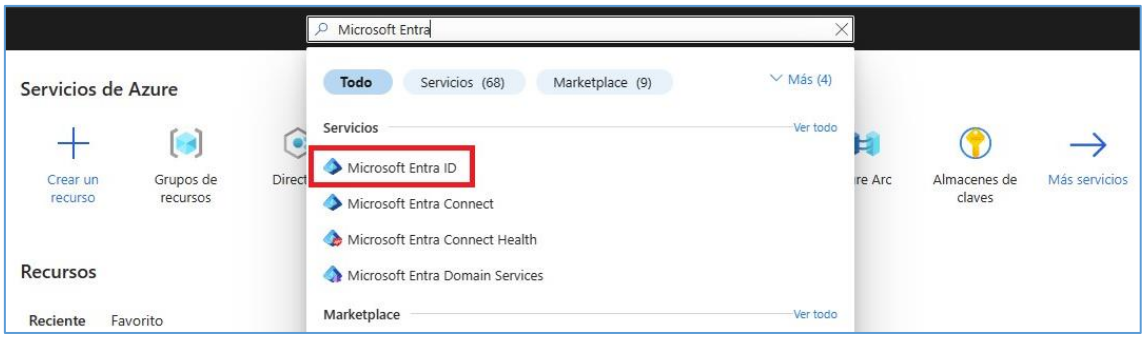
Se hace referencia a estos enlaces de Microsoft:

- *https://learn.microsoft.com/es-es/entra/identity/hybrid/whatis-hybrid-identity*
- *https://learn.microsoft.com/es-es/entra/identity/devices/how-to-hybrid-join*

A continuación, se describe cómo se realiza la gestión de cuentas de usuario y grupos de usuarios.

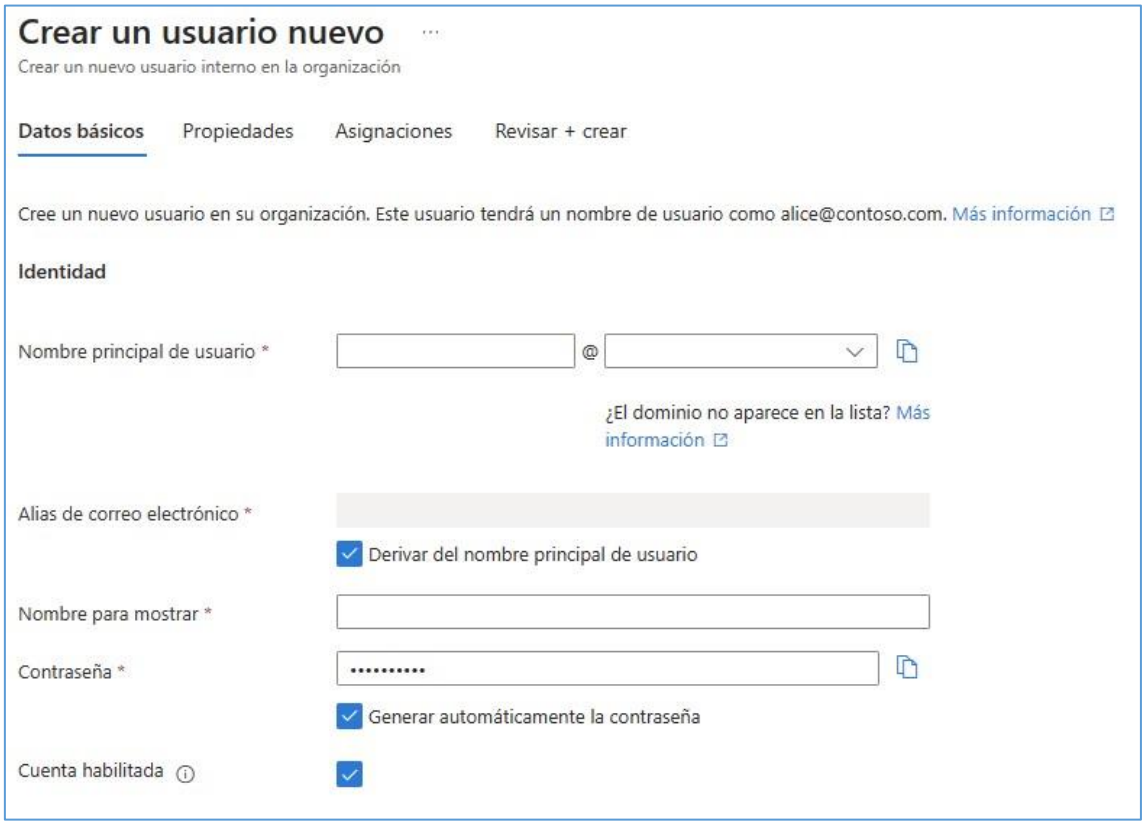
MICROSOFT ENTRA ID – ALTA, BAJA Y MODIFICACIÓN DE CUENTAS Y GRUPOS DE USUARIO

Para la gestión de usuarios/grupos, en el buscador superior escribimos [Microsoft Entra ID] y pulsamos sobre el servicio:



CREACIÓN DE CUENTAS DE USUARIOS

a) Pulsar sobre la pestaña de [Usuarios / Nuevo Usuario]. Se completan los siguientes datos:
   - **Nombre principal de usuario**: Dirección electrónica de inicio de sesión.
   - **Alias de correo electrónico** (Opcional): Dirección alternativa para el envío de correo. Es recomendable para evitar intentos de inicio de sesión no deseados.
   - **Nombre para mostrar:** Nombre de usuario**.**
   - **Contraseña:** Credencia de autenticación del usuario**.**



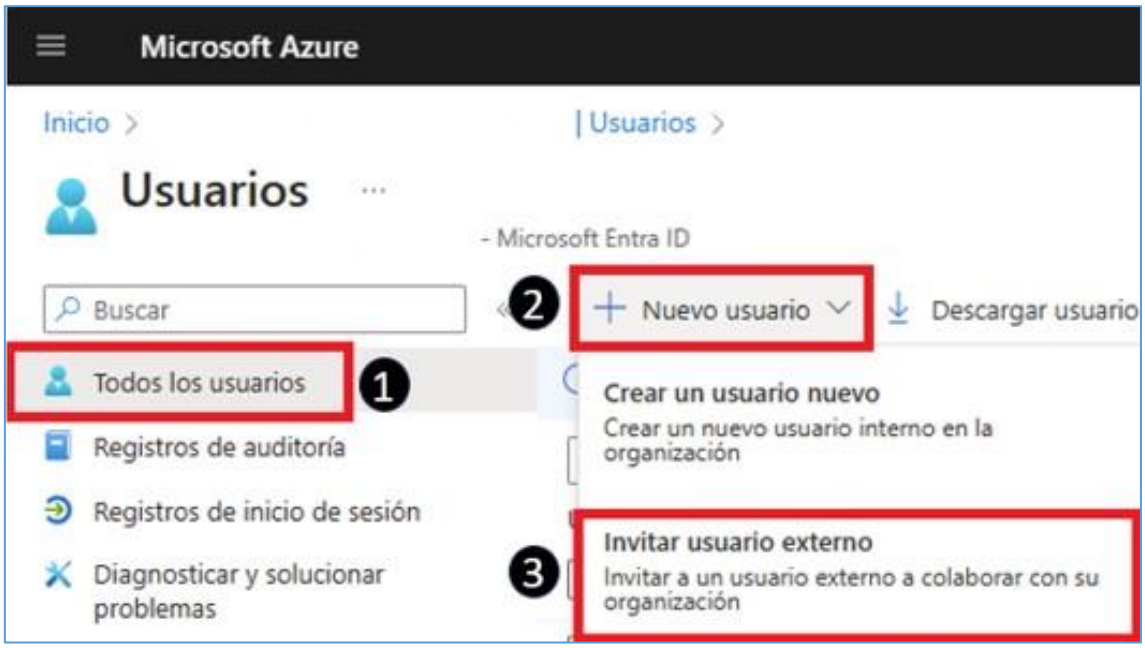
b) En la sección [Propiedades] podemos añadir metadatos del usuario correspondiente a información personal o de empresa del usuario.

c) En la sección [Asignaciones] se puede asignar al usuario unidad/es administrativa/s, grupo/s o roles del portal Microsoft Entra ID.

Nota: Opcionalmente se puede crear un usuario invitado perteneciente a otra organización. Esta misma se notifica mediante correo.

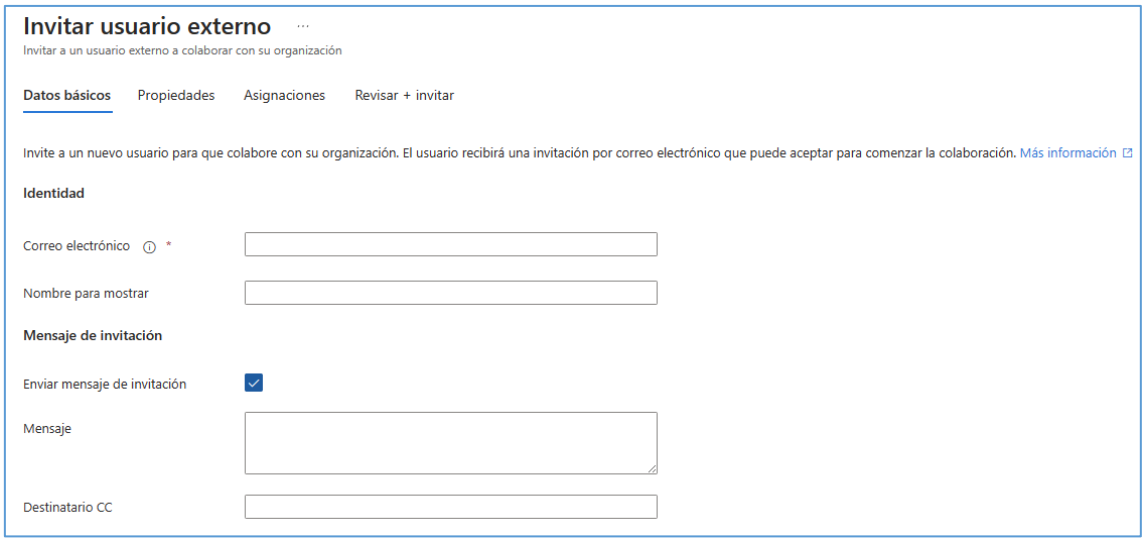
Si desea crear la cuenta de invitado, se recomienda que siga las siguientes directrices.

a) Desde el panel de Usuarios pulsar sobre Nuevo usuario invitado.



b) Se completan los siguientes datos:

a. **Correo electrónico**: Dirección de correo electrónica externa a la organización al que se desea invitar.
b. **Nombre para mostrar**: Nombre de usuario.
c. **Mensaje**: Información que acompaña al mensaje que es enviado para invitar al usuario.
d. **Destinatario CC**: Correo electrónico a quien poner en copia.

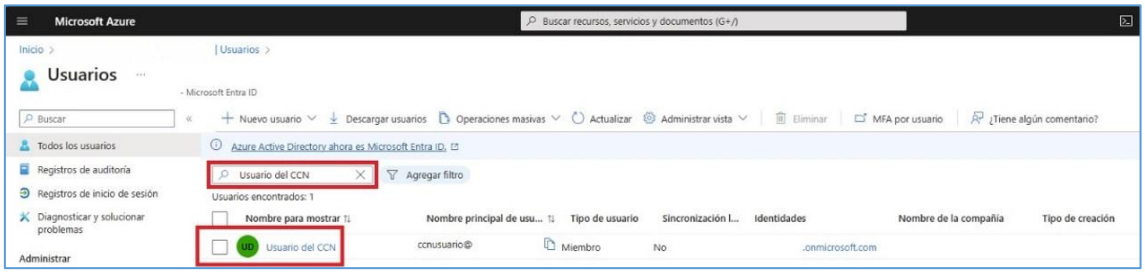


c) Se completan los mismos procesos que para un usuario normal.

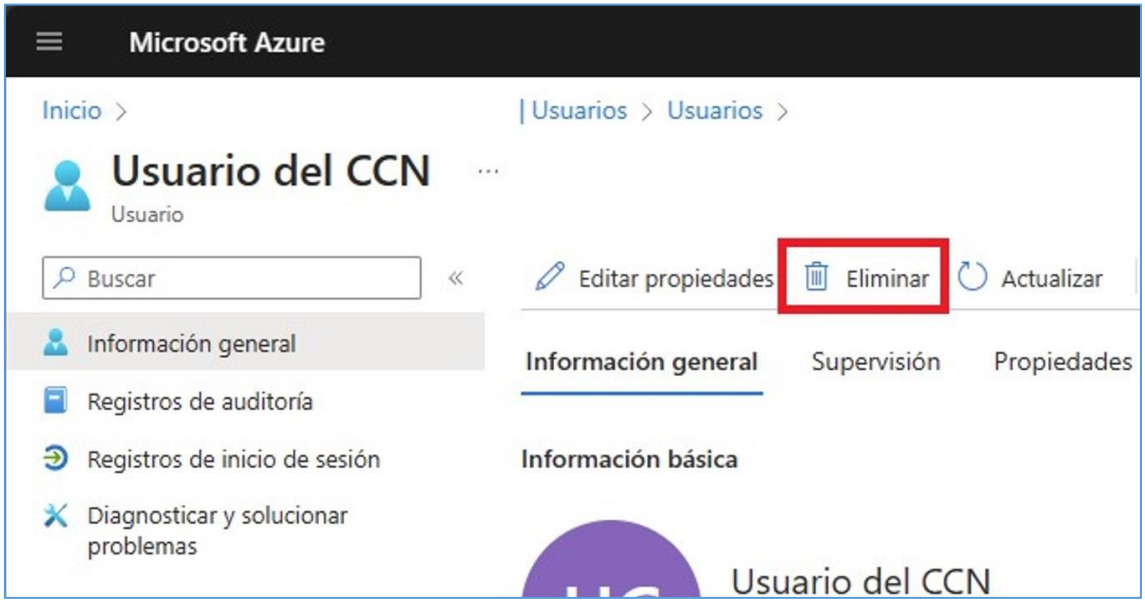
Nota: Se envía una notificación a la cuenta invitada.

BAJAS DE CUENTAS DE USUARIOS

a) Para gestionar la baja de una cuenta, se debe seleccionar el usuario al que se desea gestionar. Se dispone del buscador de usuarios para localizarlo.

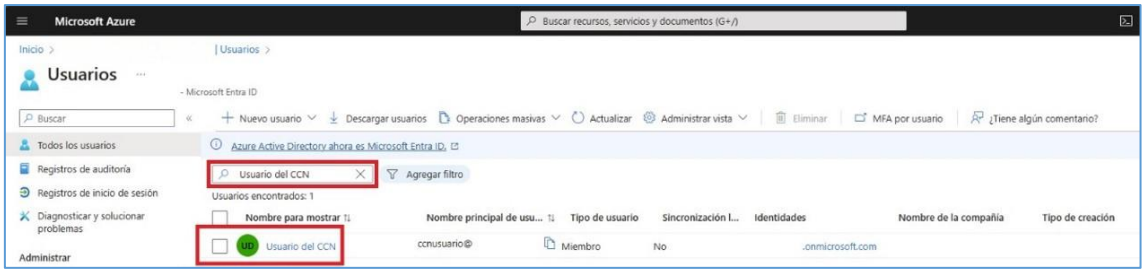


b) A continuación, pulsar sobre [Eliminar].

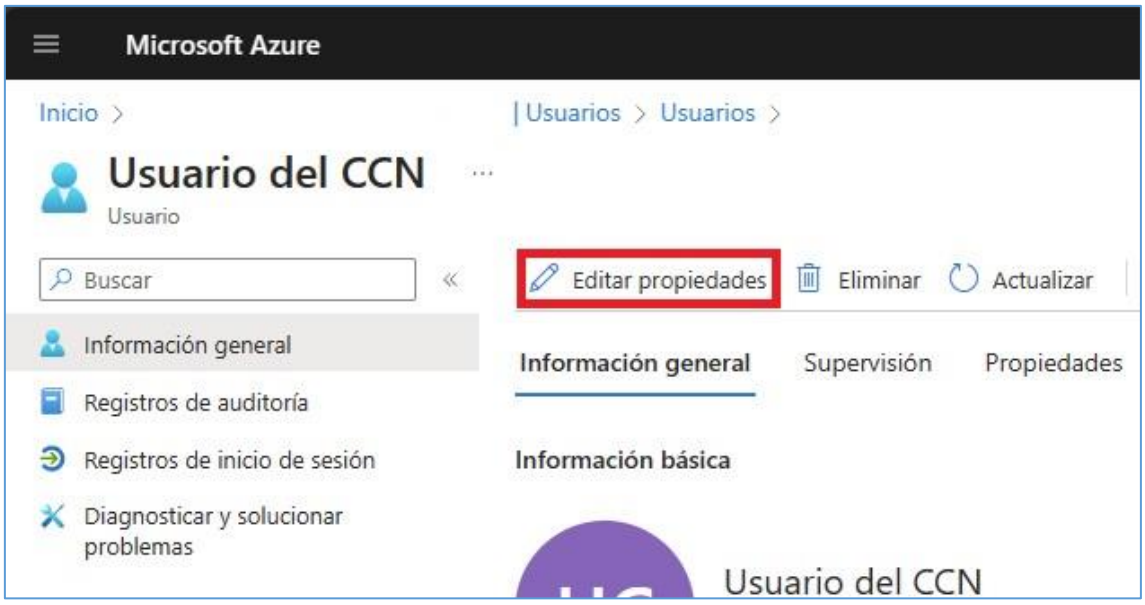


EDITAR PERFIL DE CUENTA DE USUARIO

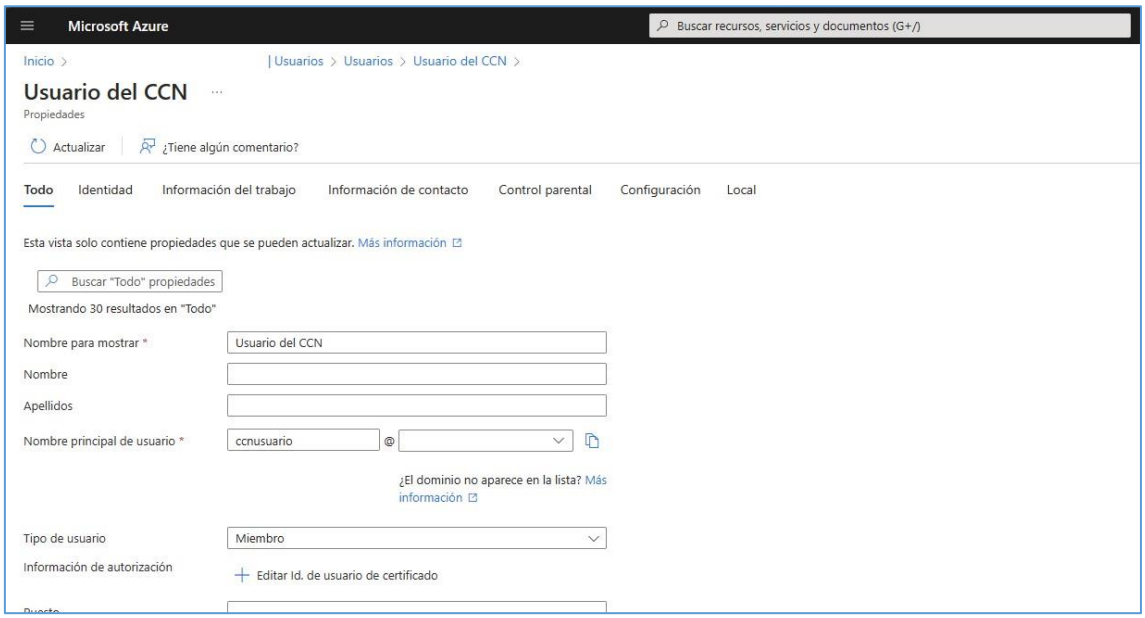
a) Desde el portal de [Microsoft Entra ID/Usuarios] pulsar en el usuario que desea modificar.



b) A continuación, pulsar sobre [Editar propiedades].

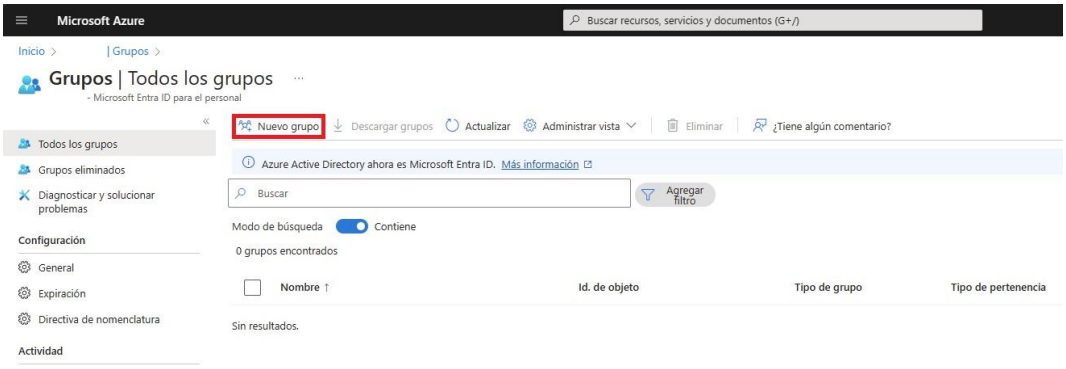


c) Desde este panel se puede modificar las propiedades de la cuenta y añadir información adicional.



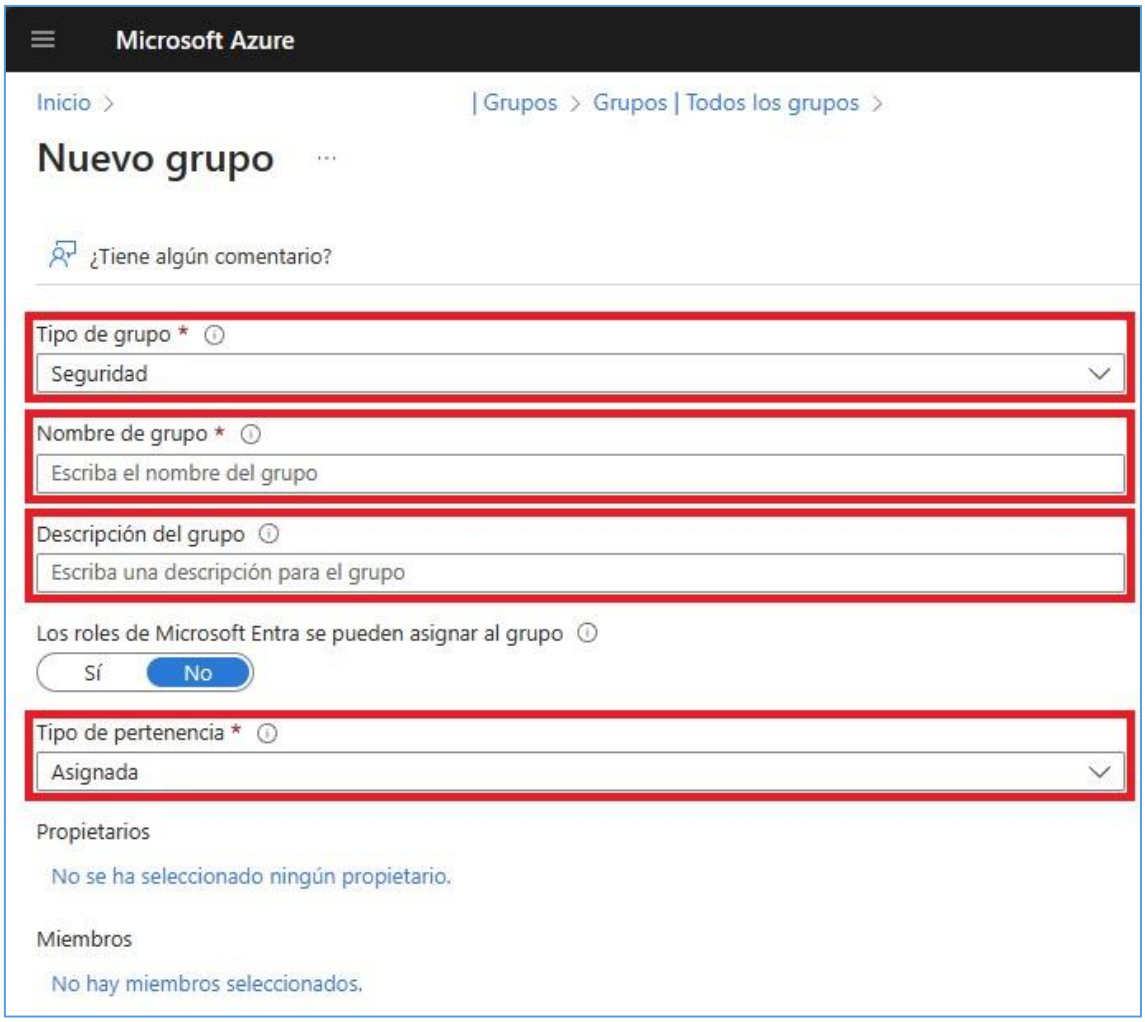
CREACIÓN DE GRUPOS MICROSOFT ENTRA ID

a) Desde el menú de ***Microsoft Entra ID*** pulsar en [Grupos/Nuevo Grupo].



b) En este apartado completar los datos para su creación.

- **Tipo de grupo:** Pueden ser de dos tipos:
  - **Seguridad:** Se usa para administrar el acceso de miembros y del equipo a los recursos compartidos de un grupo de usuarios.
  - **Office365:** Ofrece oportunidades de colaboración al conceder acceso a los miembros a un correo compartido, calendarios, archivos, el sitio de SharePoint, etc.
- **Nombre del Grupo:** El nombre que tiene este nuevo grupo.
- **Descripción del grupo:** Nombre identificativo.
- **Tipo de pertenencia:** Pueden ser de los siguientes tipos:
  - **Asignado:** Le permite agregar usuarios específicos para que sean miembros de este grupo y para que tengan permisos exclusivos.
  - **Usuario dinámico:** Permite usar reglas de pertenencia dinámicas para agregar y quitar miembros automáticamente. Si los atributos de un miembro cambian, el sistema examina las reglas del grupo dinámico del directorio para ver si el miembro cumple los requisitos de la regla (se agrega) o ya no cumple los requisitos de las reglas (se elimina).
  - **Dispositivo dinámico:** Le permite usar reglas de grupo dinámico para agregar y quitar dispositivos automáticamente. Si los atributos de un dispositivo cambian, el sistema examina las reglas del grupo dinámico del directorio para ver si el dispositivo cumple los requisitos de la regla (se agrega) o ya no cumple los requisitos de las reglas (se elimina).
- **Propietarios:** Usuarios que gestionen el grupo.
- **Miembros:** Usuarios que pertenecen a este grupo.



d) Para finalizar pulsar en [Crear].

ELIMINACIÓN DE GRUPOS

Para eliminar un grupo, seleccionar el grupo y luego pulsar sobre [Eliminar].

ADMINISTRACIÓN POR POWERSHELL

También se puede crear los usuarios y grupos mediante **PowerShell**. Para ello, ejecutar estos comandos.

- Creación de usuario.

```
# PS C:\> $PasswordProfile = @{ Password = 'P4$$w0rd1234' }
# PS C:\> New-MgUser -DisplayName "Administrador_SQL" -AccountEnabled -
  MailNickName "NotSet" -UserPrincipalName "ReneMagi@contoso.com"
```

- Creación de grupo.

```
# PS C:\> New-MgGroup -DisplayName "Administrador_SQL" -MailEnabled $false -
  SecurityEnabled $true -MailNickName "NotSet"
```

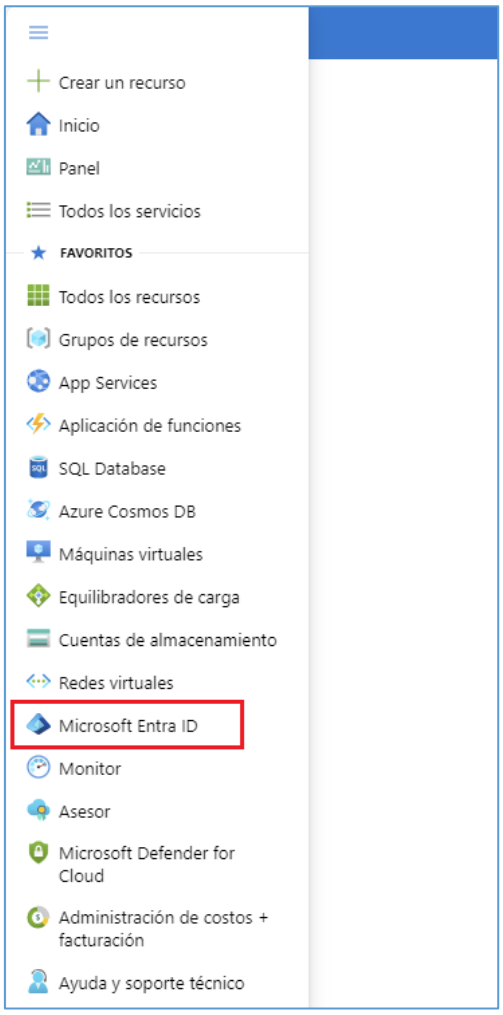
Nota: Se puede encontrar más información sobre comandos PowerShell en el enlace: *https://learn.microsoft.com/es-es/entra/identity/users/groups-settings-v2-cmdlets*

3.1.1.2 REQUISITOS DE ACCESO

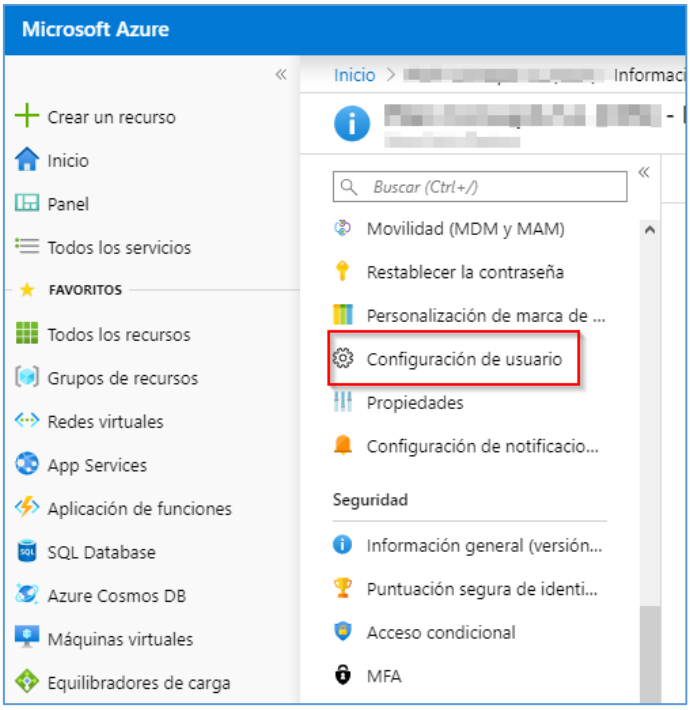
RESTRICCIÓN DE ACCESO AL PORTAL DE AZURE.

Es recomendable restringir el acceso al portal de Azure a todos aquellos usuarios que no disponen de privilegios administrativos. Esta característica limita la posibilidad de fuga de información sensible de los usuarios, como pueden ser cuentas de correo electrónico, números de teléfono y direcciones personales.

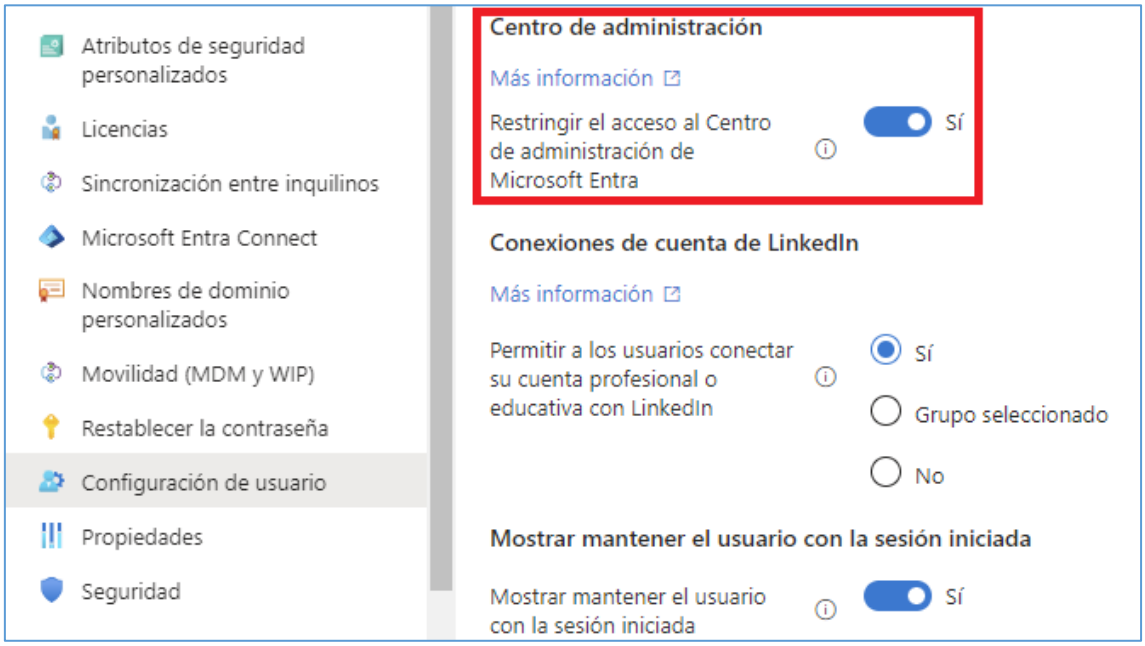
a) Desde el portal de Azure pulsar en [Microsoft Entra ID].



b) Pulsar en [configuración de usuario].



c) Pulsar en **SI** en restringir el acceso.



La opción **"No"** permite que un usuario que no sea administrador use esta experiencia con el Centro de administración de Microsoft Entra a fin de acceder a los recursos de Microsoft Entra ID para los que tenga permiso de lectura, o bien administrar sus propios recursos.

La opción **"Sí"** limita el acceso a los datos del Centro de administración de Microsoft Entra a todos los usuarios que no sean administradores, pero no limita el acceso si se usa PowerShell o algún otro cliente, como Visual Studio.

ACCESO CONDICIONAL

INTRODUCCIÓN ACCESO CONDICIONAL

El acceso condicional es la herramienta que utiliza Microsoft Entra ID para unificar señales, tomar decisiones y forzar la aplicación de las directivas de la organización. El acceso condicional se sitúa en el centro de la estrategia de control de acceso basado en identidades.

El perímetro de seguridad moderno ahora se extiende más allá de la red de una organización, incluye tanto la identidad del usuario como la del dispositivo. Las organizaciones pueden usar estas señales de identidad como parte de sus decisiones de control de acceso.

Las directivas más comunes que se pueden configurar:

a) **Pertenencia a un usuario o grupo:** Las directivas se pueden dirigir a usuarios y grupos concretos, lo que proporciona a los administradores un mayor control sobre el acceso.
b) **Información de la ubicación de la IP:** Se puede crear intervalos de direcciones IP de confianza que se pueden usar al tomar decisiones sobre directivas.

Nota: Los administradores pueden especificar que se bloquee o se permita el tráfico de intervalos de IP de países completos.

c) **Dispositivo: L**os usuarios con dispositivos de plataformas concretas o marcados con un estado concreto se pueden usar al aplicar directivas de acceso condicional.
d) **Aplicación:** Los usuarios que intentan acceder a aplicaciones específicas pueden activar diferentes directivas de acceso condicional.
e) **Detección de riesgo calculado y en tiempo real:** La integración de señales con Microsoft Entra ID Protection permite que las directivas de acceso condicional identifiquen y corrijan a los usuarios y comportamientos de inicio de sesión peligrosos.
f) **Microsoft Defender para aplicaciones en la nube:** Permite supervisar y controlar en tiempo real el acceso a las aplicaciones y las sesiones de los usuarios. Esta integración aumenta la visibilidad y el control sobre el acceso y las actividades realizadas en el entorno de la nube.

Las directivas que se recomienda configurar son las siguientes:

a) Requerir la autenticación multifactor a los usuarios con roles administrativos.
b) Requerir la autenticación multifactor para las tareas de administración de Azure.
c) Bloquear los inicios de sesión a los usuarios que intenten usar protocolos de autenticación heredados
d) Requerir ubicaciones de confianza para el registro de información de seguridad
e) Bloquear o conceder el acceso desde ubicaciones concretas.
f) Bloquear comportamientos de inicio de sesión peligrosos.

g) Requerir dispositivos administrados por la organización para aplicaciones concretas.

Nota: Recordar que, para el uso de directivas de acceso condicional, se requiere un licenciamiento **Microsoft Entra ID P1 o licencias de Microsoft 365 Empresa Premium.** Las directivas basadas en riesgo requieren acceso a Identity Protection, que requiere **licencias P2**. Consulte el siguiente enlace: *https://www.microsoft.com/es-es/security/business/microsoft-entra-pricing*

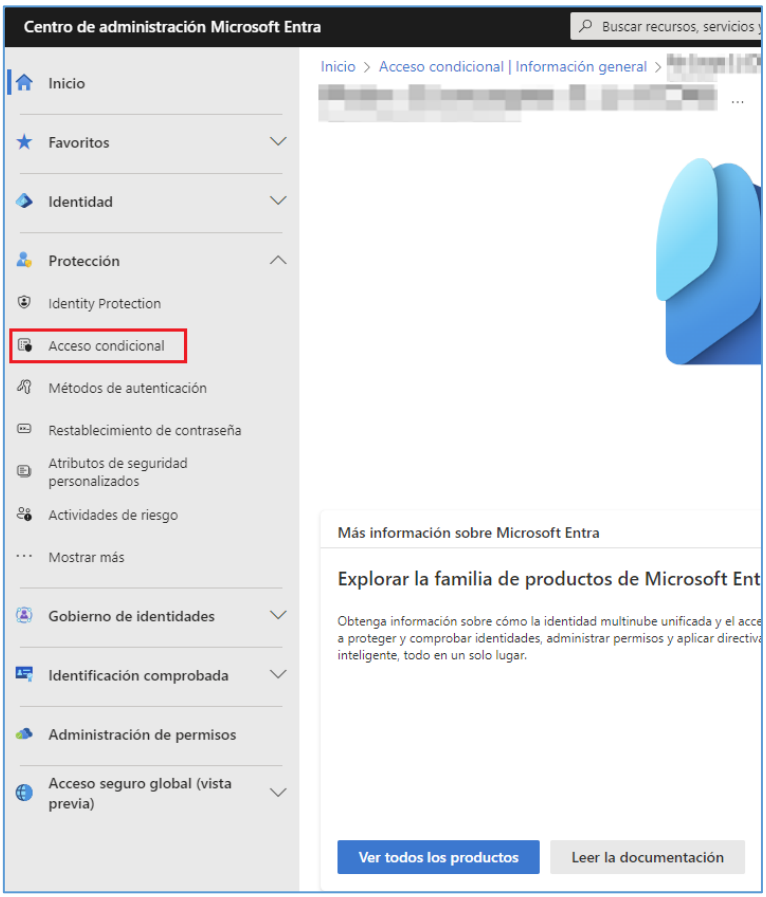
CONFIGURACIÓN ACCESO CONDICIONAL

La primera medida de acceso condicional que se recomienda aplicar es la definición de las ubicaciones desde donde se van a conectar los usuarios.

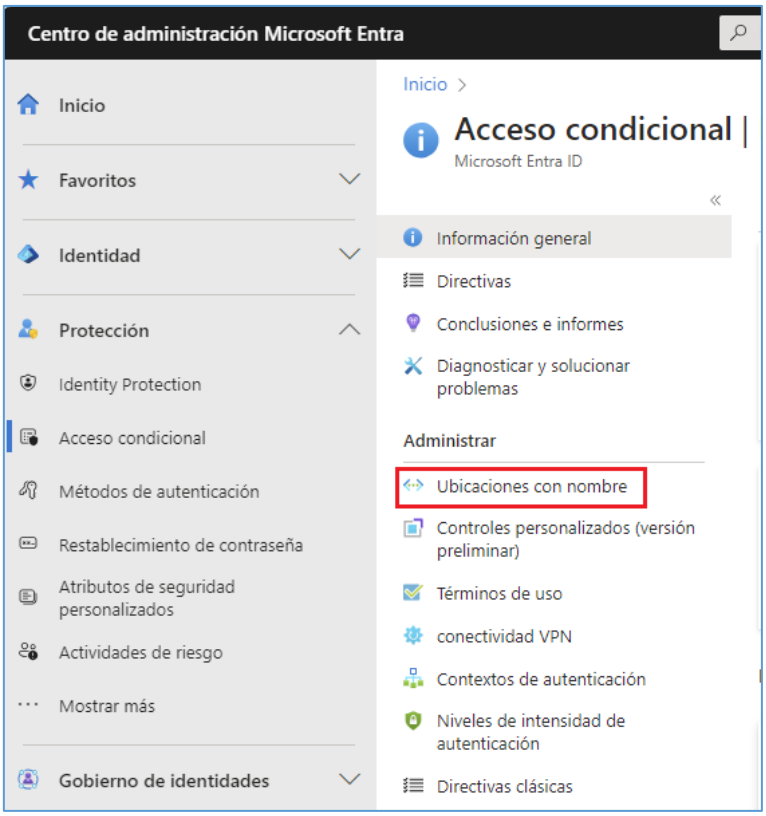
La configuración del Acceso condicional se puede realizar desde el portal de Azure desde el servicio de "Azure AD Identity Protection" > Acceso condicional, o bien desde el Centro de administración de Microsoft Entra.

A continuación, se proporcionarán las instrucciones a seguir utilizando el Centro de administración de Microsoft Entra:

a) Acceder al Centro de administración Microsoft Entra a través de la siguiente URL: *https://entra.microsoft.com/.*
b) Pulsar en [Protección/Acceso condicional].

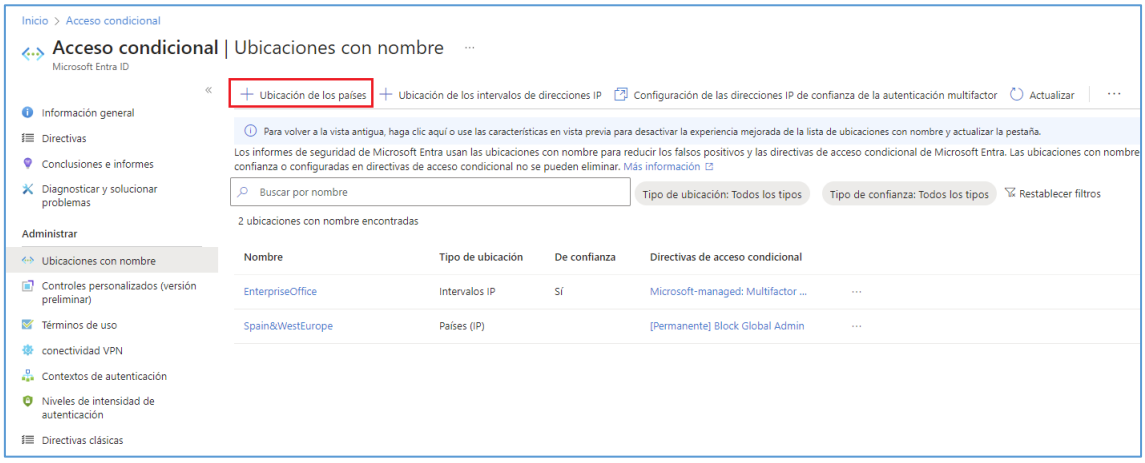


c) Pulsar en [Ubicaciones con nombres].

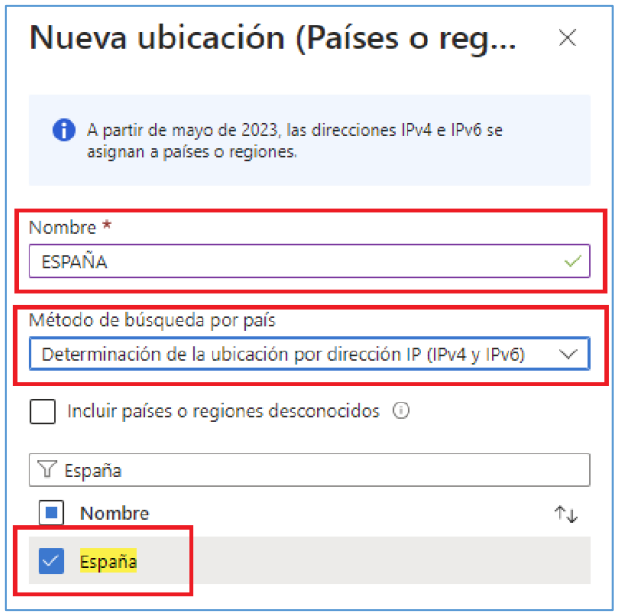


Nota: En este apartado se pueden definir las ubicaciones geográficas y configurar IP de confianza.

d) Pulsar en [Ubicación de los países].

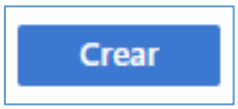


e) Debe definir un nombre y una o varias ubicaciones geográficas, en este caso seleccionar ESPAÑA. Además, debe elegir determinar la ubicación por dirección IP o coordenadas de GPS.

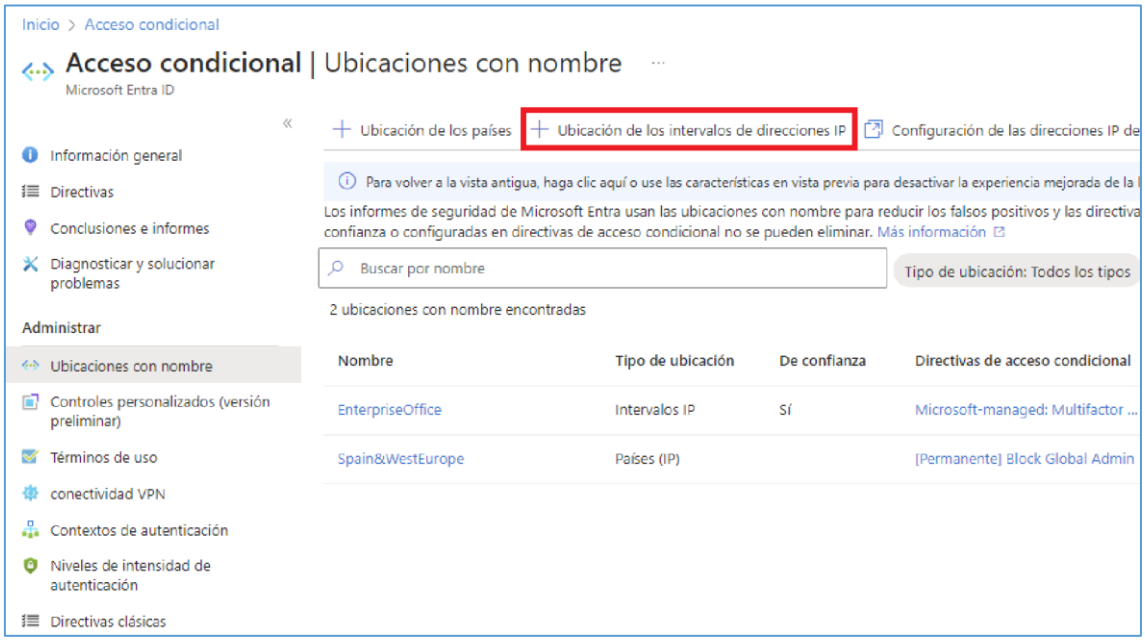


La casilla ***Incluir países o regiones desconocidas*** define direcciones IP que no se pueden asignar a ningún país o región.

f) Para finalizar pulsar en [Crear].

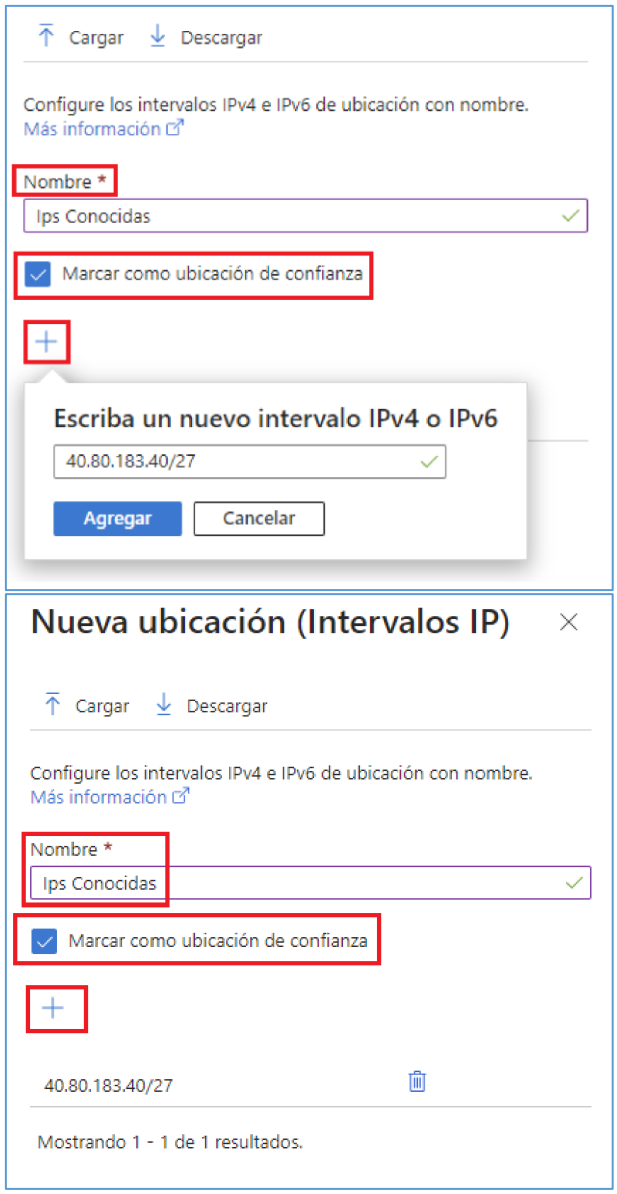


Para ello, acceder a Ubicación de los intervalos de direcciones IP.

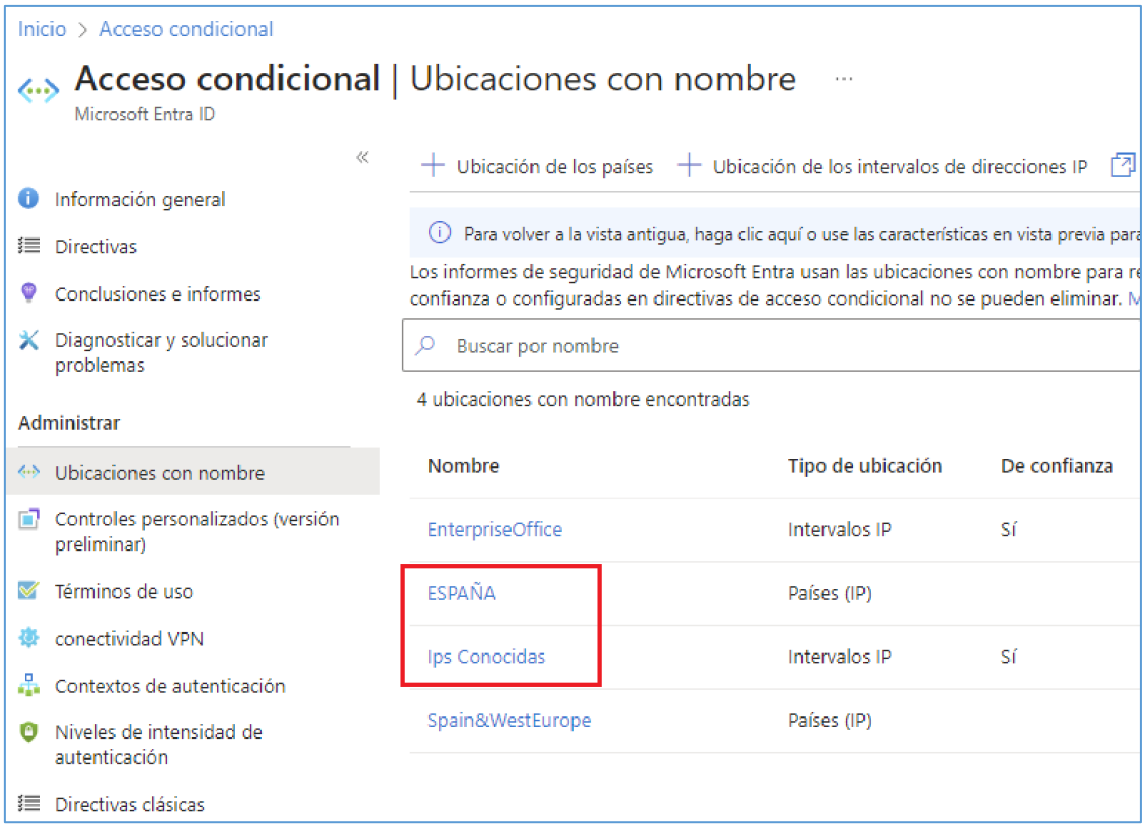


Nota: Se recomienda agregar una directiva de ubicación geográfica en intervalos de IP´S.

a) Definir un nombre
b) Pulsar en Agregar intervalo IP
c) Pulsar la casilla Marcar como ubicación de confianza
d) Definir las ips públicas en las que confía.

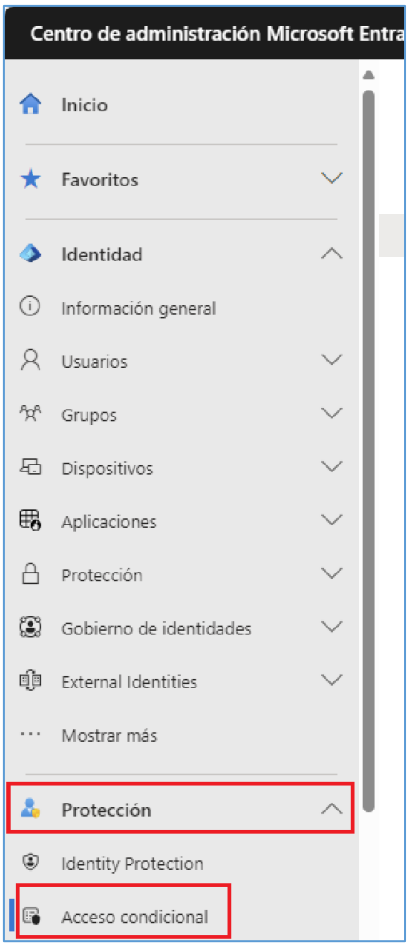


Al finalizar el panel de ubicación de nombre se muestra las dos ubicaciones creadas.

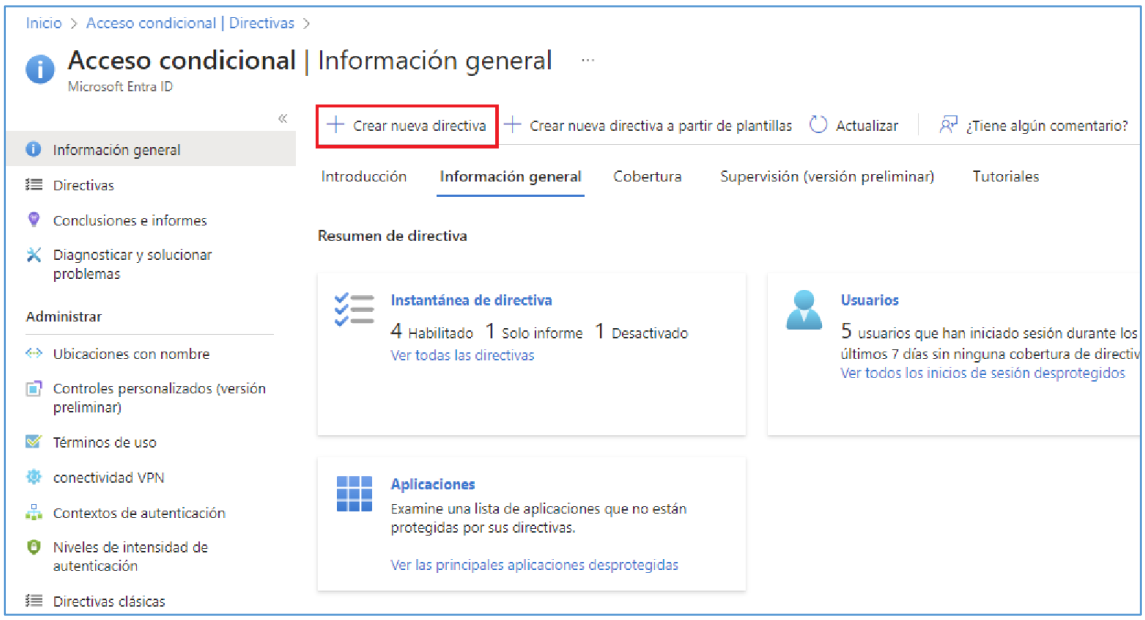


Para que estas ubicaciones creadas estén online, se crea una directiva en la que se define a quién aplica esta condición. Para ello, seguir las siguientes directrices.

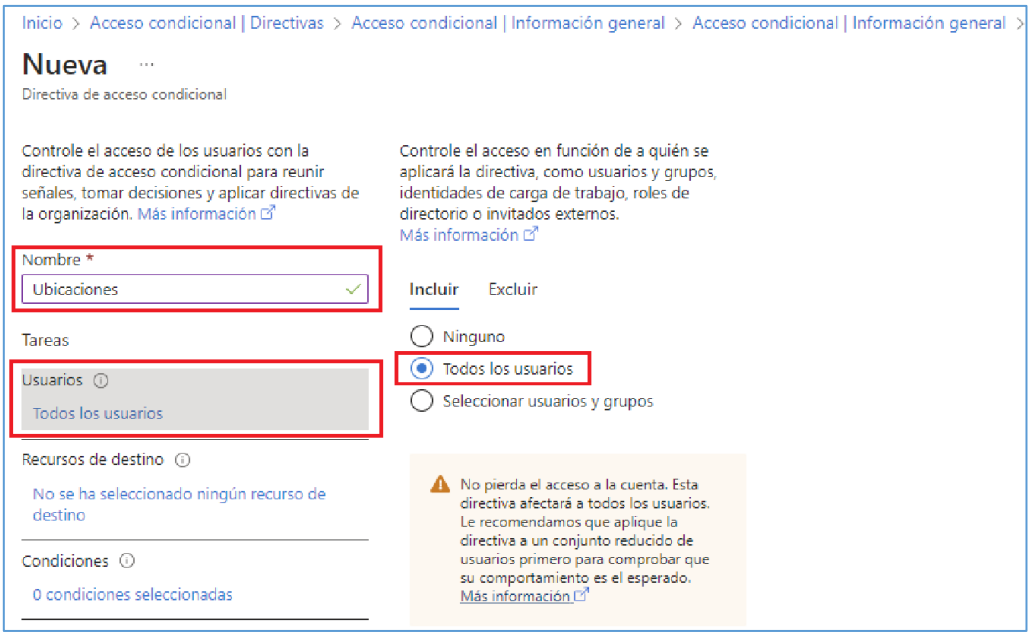
a) Desde el Centro de administración Microsoft Entra pulsar en [Protección/Acceso condicional].



b) Pulsar en [Crear nueva directiva].



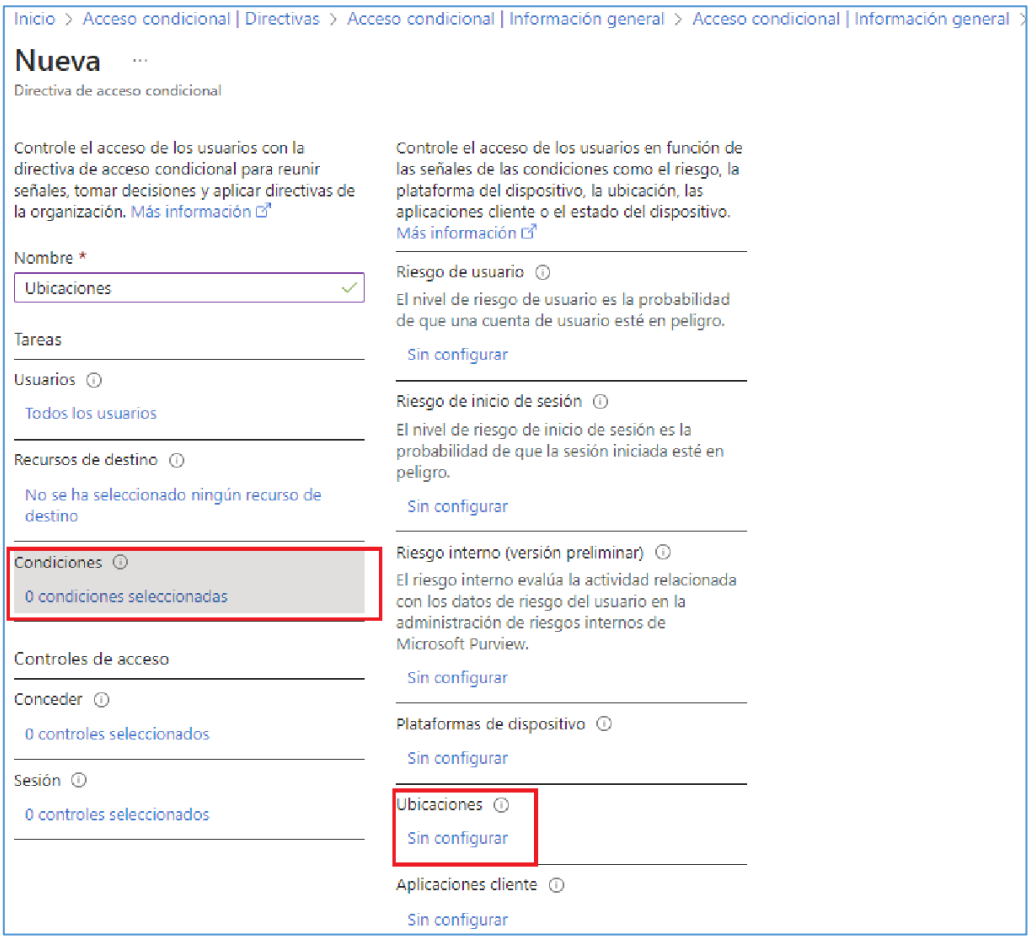
c) Definir el nombre de la directiva y pulsar en [Usuarios].



d) Pulsar en [Todos los usuarios].

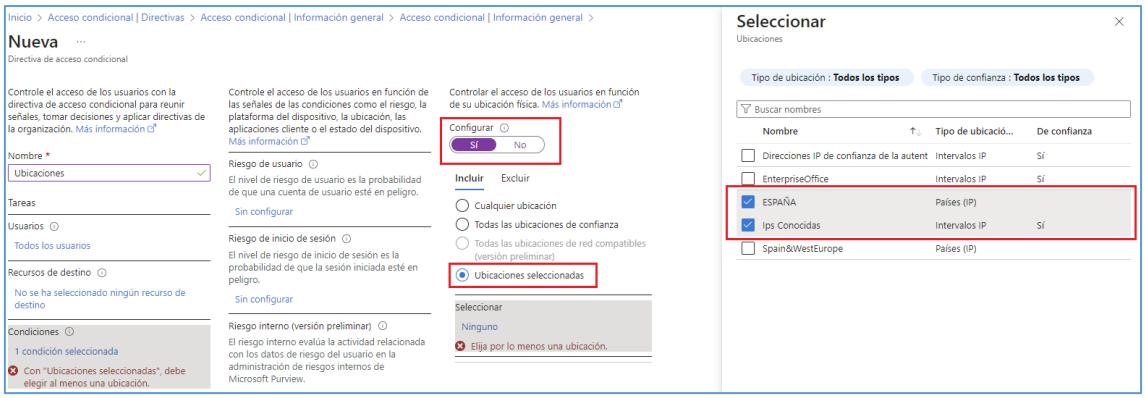
Nota: En este apartado se puede definir si esta política se aplicará a Usuarios/Grupos/Roles o excluir Usuarios/Grupos/Roles que no requiera esta condición.

e) Pulsar en [Condiciones].

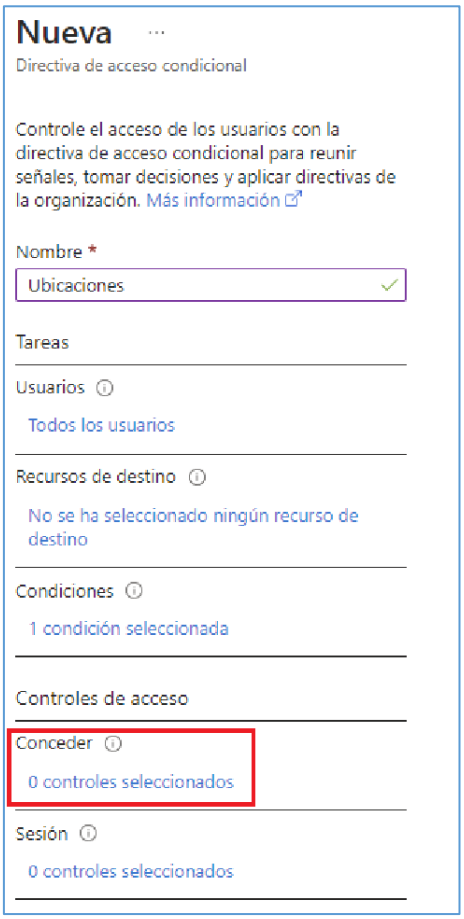


f) Pulsar en [Ubicaciones].

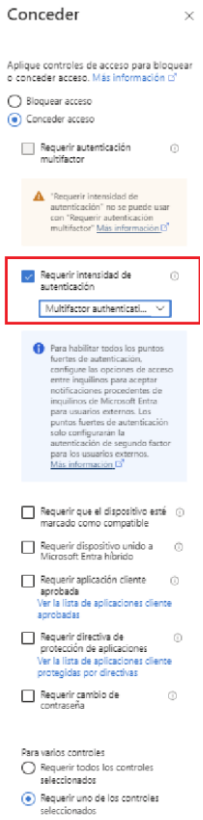
g) Seleccionar las dos ubicaciones.



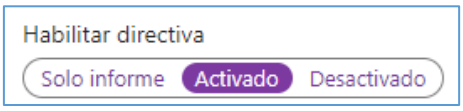
h) Para finalizar, pinchar en [Controles de acceso / Conceder].



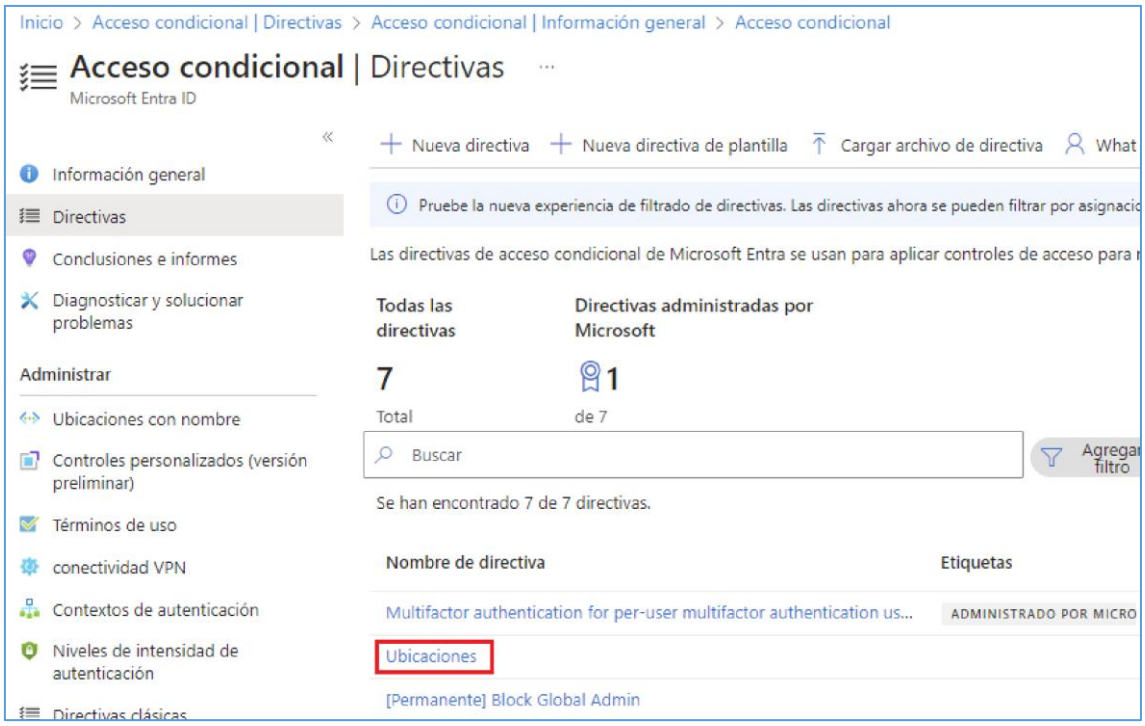
i) Se debe seleccionar *'Requerir intensidad de autenticación' y elegir un nivel de intensidad de autenticación integrada, como, por ejemplo, Autenticación Multifactor.* El servicio Autenticación multifactor de Microsoft Entra se puede consultar en el apartado [3.1.1.4 Mecanismos de autenticación] de la presente guía.



j) Para finalizar, pulsar en [Activado en habilitar directiva].



k) Pulsar en [Crear].



A continuación, se describen las distintas condiciones que se pueden crear.

- **Riesgo de usuario.**

El nivel de riesgo de usuario es la probabilidad de que una cuenta de usuario esté en peligro, pudiendo configurar los niveles de riesgo necesarios para aplicar la directiva.

- **Riesgo de Inicio de sesión.**

El riesgo del inicio de sesión es un indicador de la probabilidad (alta, media o baja) de que el legítimo propietario de una cuenta de usuario no haya realizado un inicio de sesión.

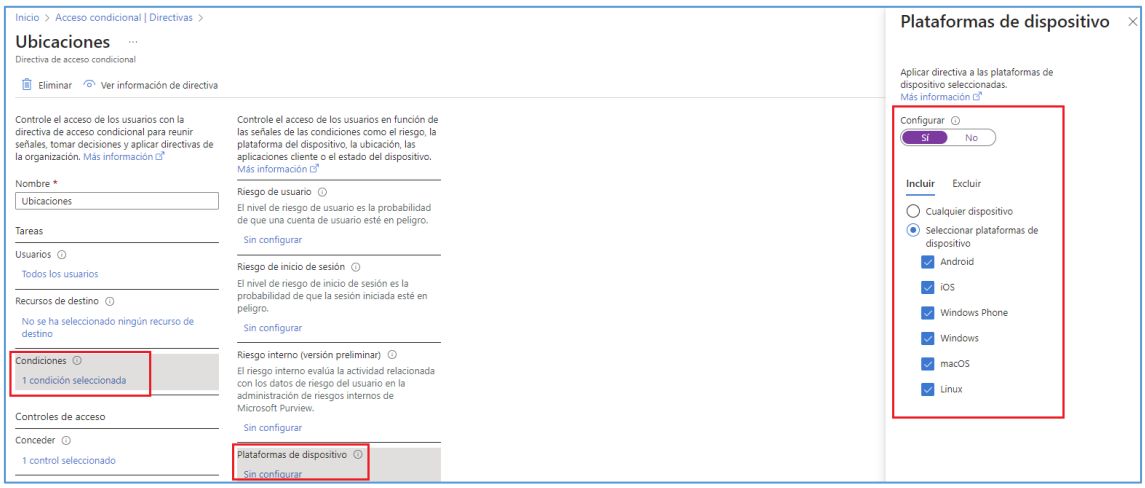
Microsoft Entra ID calcula el nivel de riesgo durante el inicio de sesión de un usuario. Se puede utilizar el nivel calculado de riesgo de inicio de sesión como condición en una directiva de acceso condicional.

Nota: Para habilitar esta condición, es necesario que tenga **Microsoft Entra ID Protection.**

Se puede consultar la documentación en el enlace: https://docs.microsoft.com/es-es/azure/active-directory/identity-protection/howto-sign-in-risk-policy#what-is-the-sign-in-risk-policy

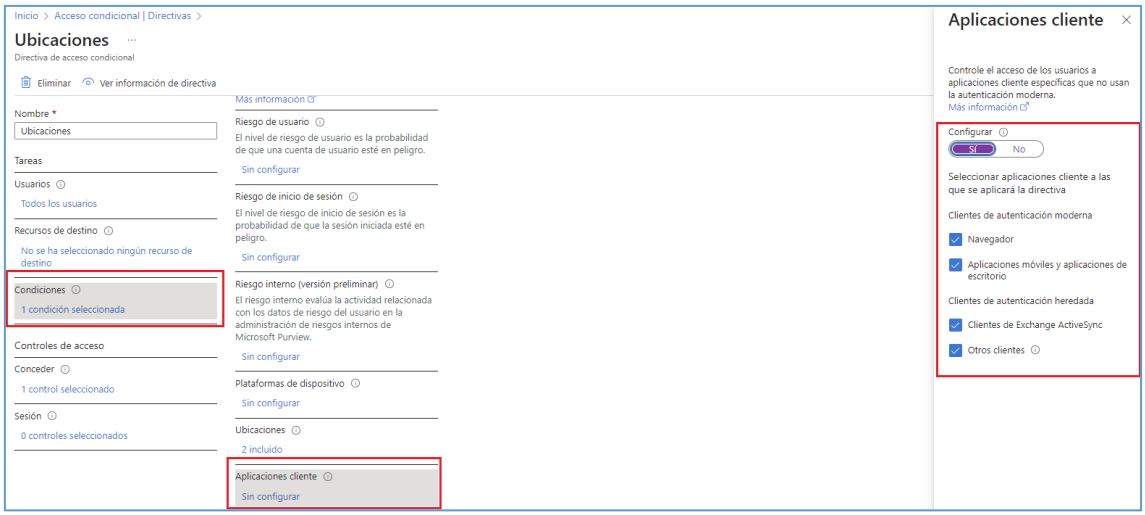
- **Plataformas de dispositivos.**

La plataforma de dispositivo es el sistema operativo que se ejecuta en el dispositivo. Microsoft Entra ID identifica la plataforma mediante el uso de la información proporcionada por el dispositivo, como el agente de usuario. Se recomienda que todas las plataformas tengan una directiva aplicada a ellas.



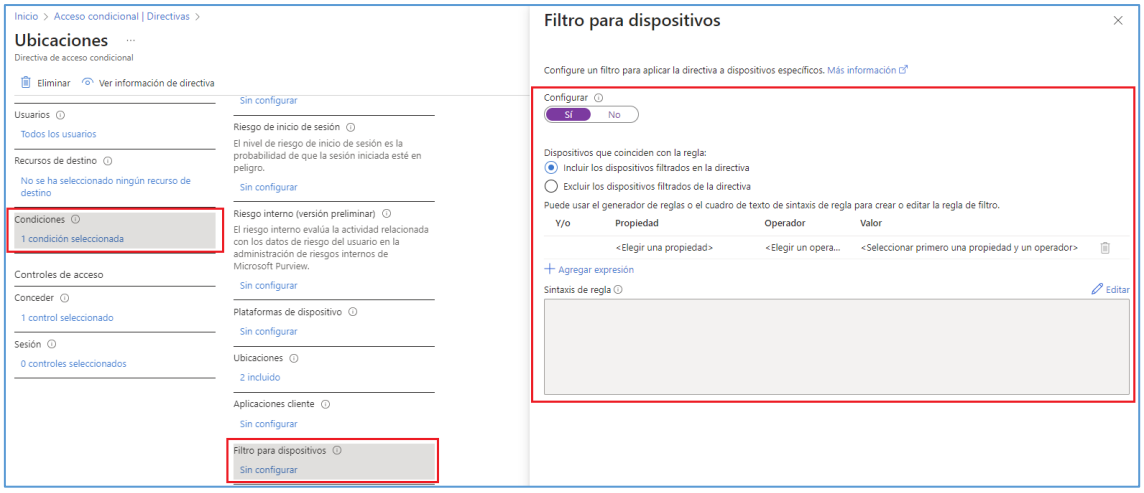
- **Aplicaciones cliente.**

De manera predeterminada, todas las directivas de acceso condicional recién creadas se aplican a todos los tipos de aplicaciones cliente. Cuando el botón de alternancia 'Configurar' está establecido en Sí, se aplica a los elementos seleccionados.



- **Filtro para dispositivos**

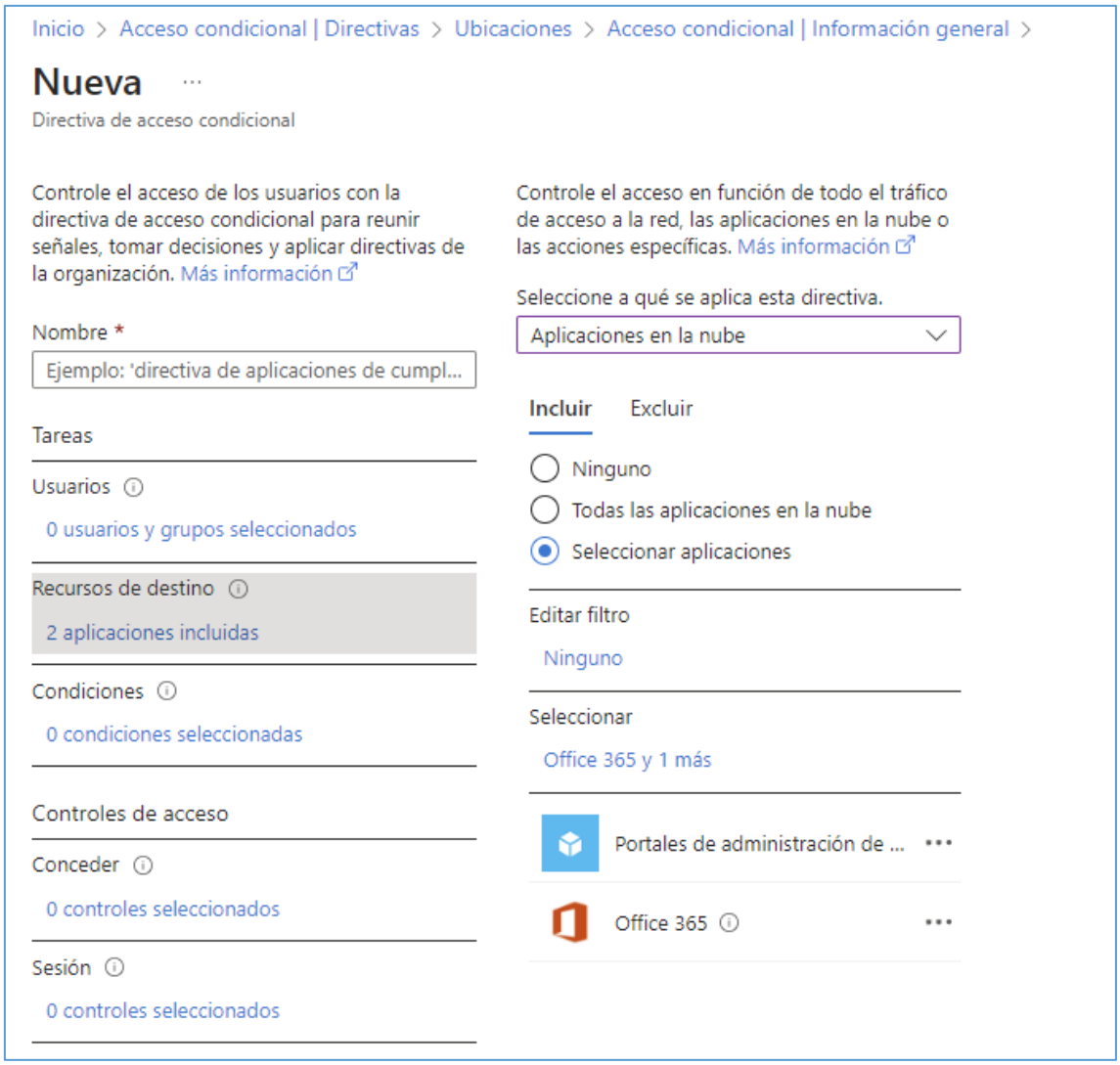
La condición de filtro para dispositivos proporciona la funcionalidad de dirigirse a dispositivos específicos o excluirlos.



En las directivas de acceso condicional se puede controlar el acceso en función del tráfico de acceso a la red, las aplicaciones en la nube o las acciones específicas. Los recursos de destino son señales clave en una directiva de acceso condicional.

- **Aplicaciones en la nube.**

Con las directivas de acceso condicional, se controla la forma en que los usuarios acceden a las aplicaciones y servicios en la nube. Los administradores pueden elegir de la lista de aplicaciones o servicios que incluyen aplicaciones incorporadas de Microsoft y cualquier Aplicaciones integradas de Microsoft Entra.



Todas las aplicaciones en la nube al aplicar las directivas de base de referencia que se aplican a todo el Tenant. La aplicación de una directiva de acceso condicional a todas las aplicaciones en la nube da como resultado que se aplique la directiva para todos los tokens emitidos a sitios web y servicios. Esta opción incluye aplicaciones que no pueden destinarse individualmente en la directiva de acceso condicional, como Microsoft Entra ID. En algunos casos, una directiva *'Todas las aplicaciones en la nube'* podría bloquear accidentalmente el acceso de los usuarios.

Seleccionar aplicaciones para dirigir servicios específicos por su directiva. Por ejemplo, para requerir que los usuarios tengan un dispositivo compatible para acceder a SharePoint Online. Esta directiva también se aplica a otros servicios cuando se accede al contenido de SharePoint. Un ejemplo es Microsoft Teams.

CONTROL DE ACCESO BASADO EN ROLES (RBAC)

El Control de Acceso Basado en Roles (RBAC) ayuda a administrar quién puede acceder a los recursos de Azure, qué se puede hacer con esos recursos y a qué áreas se pueden acceder.

¿Qué se puede hacer con RBAC?

Estos son algunos ejemplos de lo que se puede realizar con RBAC:

a) Permitir que un usuario administre las máquinas virtuales de una suscripción y que otro usuario administre las redes virtuales
b) Permitir que un grupo de DBA administre bases de datos SQL en una suscripción
c) Permitir que un usuario administre todos los recursos de un grupo de recursos, como las máquinas virtuales, los sitios web y las subredes
d) Permitir que una aplicación acceda a todos los recursos de un grupo de recursos

FUNCIONAMIENTO DE RBAC

La manera en que se controla el acceso a los recursos mediante RBAC es mediante las asignaciones de roles. Este es un concepto clave: Trata de cómo se aplican los permisos y su alcance. Una asignación de roles consta de tres elementos: entidad de seguridad, definición de rol y ámbito.

Deberá aplicarse el principio de mínimo privilegio para que los usuarios puedan realizar únicamente las operaciones necesarias dentro del alcance de sus funciones.

Azure permite el uso de varios roles integrados. A continuación, se enumeran cuatros roles fundamentales. Los tres primeros se aplican a todos los tipos de recursos.

a) **Propietario:** Tiene acceso total a todos los recursos, incluido el derecho a delegar este acceso a otros.
b) **Colaborador:** Tiene permisos para crear y administrar todos los tipos de recursos de Azure, pero no se puede conceder acceso a otros.
c) **Lector:** Tiene permisos para ver los recursos existentes de Azure.
d) **Administrador de acceso de usuario:** Tiene permisos para administrar el acceso de los usuarios a los recursos de Azure.

Además, de estos roles también existen otros enfocados a servicio ya creados en Azure, como puede ser "*Colaborador de Base de Datos SQL*", "*Administrador de seguridad SQL*", etc.

Nota: Todos estos roles se pueden encontrar en la documentación oficial de Microsoft:

https://docs.microsoft.com/es-es/azure/role-based-access-control/built-in-roles

ROLES PERSONALIZADOS RBAC

En el punto anterior se han mencionado los roles ya incluidos en Azure. En el caso de que estos roles no se adapten a las necesidades, se puede crear roles en los que se definan de manera personalizada el conjunto de permisos que van a tener los usuarios a los que se les asignen.

La única manera de definir roles es a través de plantillas **JSON**, que pueden ser creadas desde cero o basándose en un rol ya creado y modificarlo según las necesidades.

El **JSON** para definir el rol tiene la siguiente estructura:

```
#  {
#      "Name": "Operador de Roles",
#      "Id": null,
#      "IsCustom": true,
#      "Description": "Puede crear, modificar y eliminar roles",
#      "Actions": [
#        "Microsoft.Authorization/*/read",
#        "Microsoft.Authorization/roleDefinitions/write",
#        "Microsoft.Authorization/roleDefinitions/delete"
#      ],
#      "NotActions": [],
#      "DataActions": [],
#      "NotDataActions": [],
#      "AssignableScopes": [
#        "/subscriptions/00000000-0000-0000-0000-00000000000"
#      ]
#  }
```

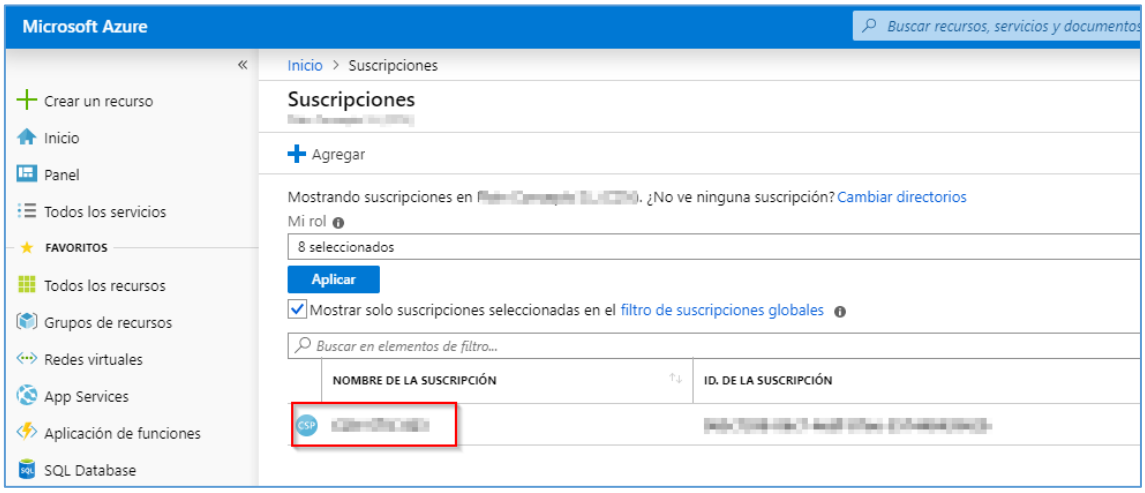
a) **Name:** Nombre del rol.
b) **Id**: Id del rol, al ser un rol personalizado se deja siempre como **null**.
c) **Description:** Descripción del rol.
d) **Actions:** Permisos del rol. Para ver todas las actions existentes en Azure consultar la siguiente documentación https://docs.microsoft.com/es-es/azure/role-based-access-control/resource-provider-operations
e) **NotActions:** Acciones a las que se deniega explícitamente el permiso.
f) **DataActions:** Especifica las acciones del plano de datos que el rol permite realizar en los datos dentro de ese objeto. Si crea un rol personalizado con DataActions, ese rol no se puede asignar en el ámbito del grupo de administración. Para más información, consultar la siguiente documentación: *https://learn.microsoft.com/es-es/azure/role-based-access-control/role-definitions#dataactions*
g) **NotDataActions:** Especifica las acciones del plano de datos que se excluyen de las DataActions permitidas. Para más información, consultar la siguiente documentación: *https://learn.microsoft.com/es-es/azure/role-based-access-control/role-definitions#notdataactions*
h) **AssignableScopes:** Se asigna el ámbito en el que se aplica el rol. Puede ser:
    a. A nivel de suscripción.
    b. A nivel de grupo de recursos.

REQUISITOS PREVIOS

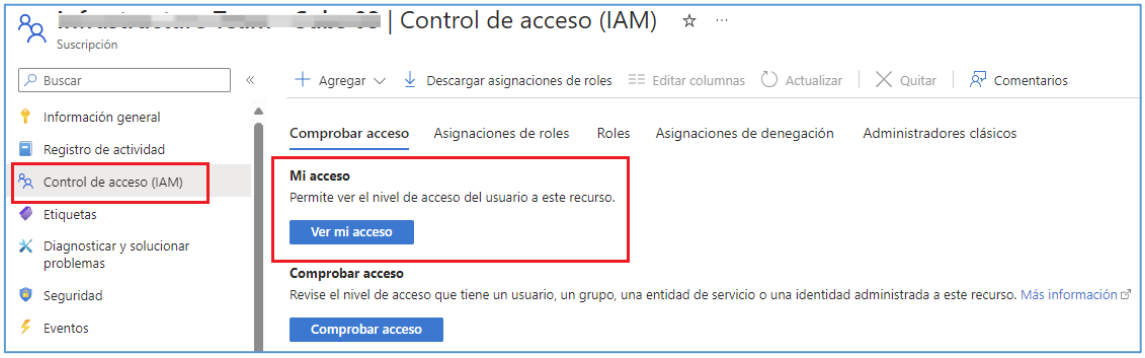
Es necesario que el usuario administrador que se conecte al portal de Azure tenga los permisos adecuados para la gestión de roles RBAC. Para ello, realizar las siguientes comprobaciones:

a) Desde el portal de Azure buscar suscripciones.

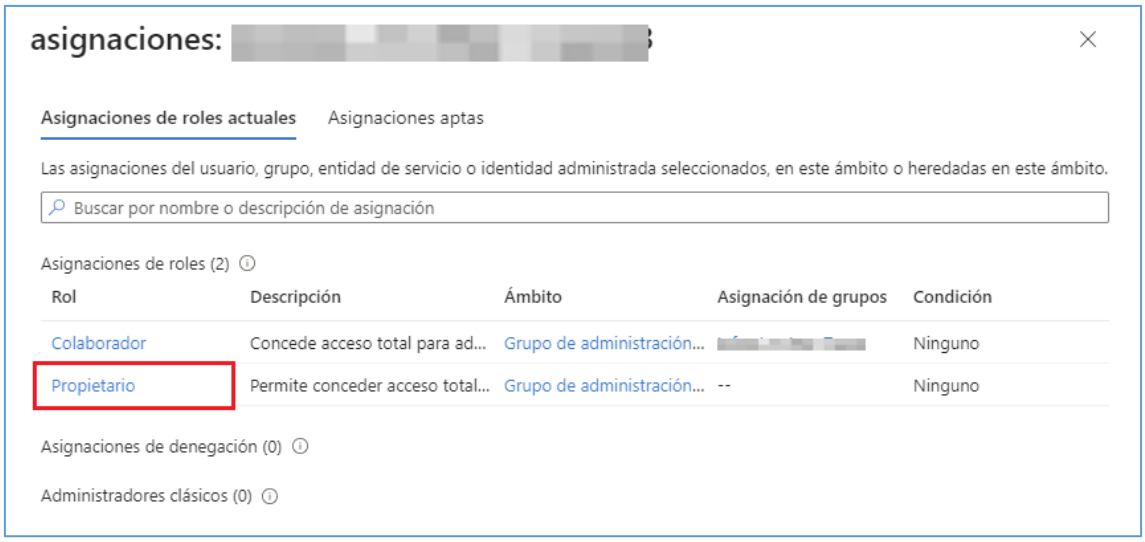
b) Pulsar en [Suscripciones] y elegir la suscripción deseada.



c) Pulsar en [control de acceso (IAM)/Ver mi acceso].



d) Verificar que dispones del rol Propietario.



DESPLIEGUE DE UN ROL PERSONALIZADO

Una vez creado el JSON con el rol, explicado en el apartado anterior, se debe desplegar para que pueda ser utilizado en Azure.

El método para poder desplegar el rol es a través de PowerShell, a través del siguiente comando:

```
# PS C:\> New-AzRoleDefinition -InputFile ".\RBAC\OperadorRoles.json"
```

Nota: La ruta del archivo del parámetro -InputFile puede ser tanto una ruta absoluta como una ruta relativa.

ASIGNAR A UNA ENTIDAD UN ROL

A continuación, se asigna a una entidad de seguridad un rol. Utilizar el ejemplo de rol personalizado creado en dicho apartado.

a) Primero debe conectarse al *Tenant* de Azure.

```
# PS C:\> Connect-AzAccount
```

b) Insertar las credenciales de administrador del *Tenant*.

c) En el siguiente paso debe obtener el ID de la entidad a la que aplica el rol, con el siguiente comando se obtiene el identificador del grupo. También puede ser un usuario, aplicación empresarial.

Nota: Recordar que es un usuario de aplicación empresarial es definido como un usuario de cuenta de servicio para una aplicación.

```
# PS C:\> $grupo = Get-AzADGroup -SearchString "Administrador Roles"
```

d) En el caso que se trate de un usuario se utiliza este comando, con el usuario deseado.

```
# PS C:\> $usuario = Get-AzADUser -DisplayName "ccn-user"
```

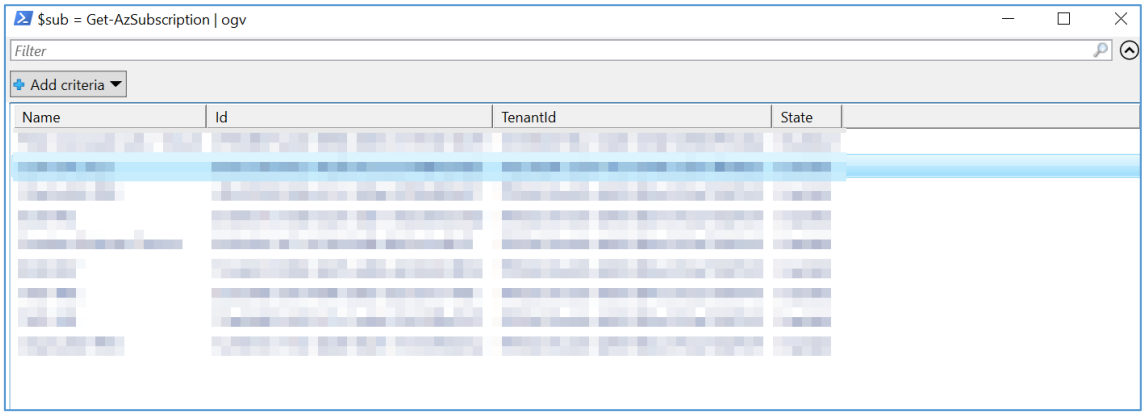
e) En el caso de que se trate de un usuario de servicio se utilizad este comando, con el nombre de usuario de servicio deseado.

```
# PS C:\> $usuarioservicio = Get-AzADServicePrincipal -DisplayName "OperationsServicePrincipal"
```

f) También se puede saber la suscripción de Azure en la que se va a aplicar el rol. Para ello, se utiliza el siguiente comando:

```
# PS C:\> $sub = Get-AzSubscription | ogv
```

Se abre una nueva ventana donde seleccionar la suscripción en la que desea aplicar el rol.



g) A continuación, debe crear la variable $scope con el formato que necesita el despliegue. Para ello, concatene la cadena /suscriptions/ y el ID de la suscripción.

```
# PS C:\> $scope = "/subscriptions/" + $sub.id
```

h) Para finalizar debe asignar el rol a la entidad, que en este caso es el grupo llamado “Administrador Roles”

- En el caso de que se trate de un grupo se utiliza el siguiente comando:

```
# PS C:\> New-AzRoleAssignment -ObjectId $grupo.ObjectId -RoleDefinitionName "Operador de Roles" -Scope $scope
```

- En el caso de que se trate de un usuario se utiliza el siguiente comando:

```
# PS C:\> New-AzRoleAssignment -ObjectId $usuario.Id -RoleDefinitionName "Operador de Roles" -Scope $scope
```

- En el caso de que se trate de un usuario de servicio se utiliza el siguiente comando:

```
# PS C:\> New-AzRoleAssignment -ObjectId $usuarioservicio.Id -RoleDefinitionName "Operador de Roles" -Scope $scope
```

Notas: Para más información ver documentación https://learn.microsoft.com/es-es/azure/role-based-access-control/role-assignments-powershell

COMANDOS RECOMENDADOS RBAC

A continuación, se recomiendan unos comandos útiles para trabajar con roles. Para los ejemplos en los comandos se utiliza el ejemplo del rol personalizado creado en dicho apartado.

- Obtener información del rol creado:

```
# PS C:\> Get-AzRoleDefinition -Name "Operador de Roles"
```

Nota: En el parámetro name poner el nombre del rol.

- Actualizar un rol, una vez el JSON haya sido actualizado.

```
# PS C:\> Set-AzRoleDefinition -Name "Operador de Roles"
```

- Borrar un rol.

```
# PS C:\> Get-AzRoleDefinition -Name "Log Analytics operator" | Remove-AzRoleDefinition
```

MICROSOFT ENTRA ID PROTECTION

Microsoft Entra ID Protection es una solución de seguridad que utiliza aprendizaje automático avanzado para identificar riesgos de inicio de sesión y comportamientos inusuales de los usuarios. Su objetivo es bloquear, desafiar, limitar o permitir el acceso según el nivel de riesgo detectado.

Esta herramienta ayuda a las organizaciones a detectar, investigar y corregir los riesgos relacionados con las identidades. Algunas de sus capacidades incluyen:

a) **Detección de riesgos:** Microsoft Entra ID Protection puede detectar comportamientos de riesgo como el uso de una dirección IP anónima, ataques de difusión de contraseña, credenciales con fugas, entre otros.

b) **Investigación:** Proporciona informes para que los administradores investiguen los riesgos y tomen medidas.

c) **Corrección de riesgos:** Automatiza la corrección de riesgos y evita apropiaciones de cuentas.

d) **Identificación de usuarios de alto riesgo:** Permite identificar a los usuarios de alto riesgo y los inicios de sesión con conclusiones prácticas.

Microsoft Entra ID Protection está disponible con una suscripción a Microsoft Entra ID P2. Microsoft recomienda migrar las directivas de riesgo de usuario y de riesgo de inicio de sesión al acceso condicional. Las directivas de riesgo heredadas configuradas en Microsoft Entra ID Protection se retirarán el 1 de octubre de 2026.

Para crear una directiva de acceso condicional se pueden seguir las instrucciones detalladas en el capítulo "1.1.1.1 Requisitos de acceso/Acceso condicional".

Notas: Se puede encontrar más información en: *https://learn.microsoft.com/es-es/entra/id-protection/howto-identity-protection-configure-risk-policies*

RECOMENDACIONES

A continuación, se detallan algunos servicios recomendados que se pueden configurar.

MICROSOFT ENTRA PRIVILEGED IDENTITY MANAGEMENT

Microsoft Entra Privileged Identity Management (PIM) es un servicio que permite administrar, controlar y supervisar el acceso a recursos importantes dentro de la organización. Esto incluye el acceso a los recursos de Microsoft Entra ID, los recursos de Azure y otros servicios de Microsoft Online Services, como Office 365 o Microsoft Intune.

Nota: *Se puede encontrar más información en: https://learn.microsoft.com/es-es/entra/id-governance/privileged-identity-management/pim-configure*

ACCESO JUST IN TIME EN MÁQUINAS VIRTUALES

Se puede usar el acceso Just-In-Time (JIR) de Microsoft Defender for Cloud para restringir el acceso a las máquinas virtuales a nivel de red, bloqueando el tráfico entrante a puertos específicos.

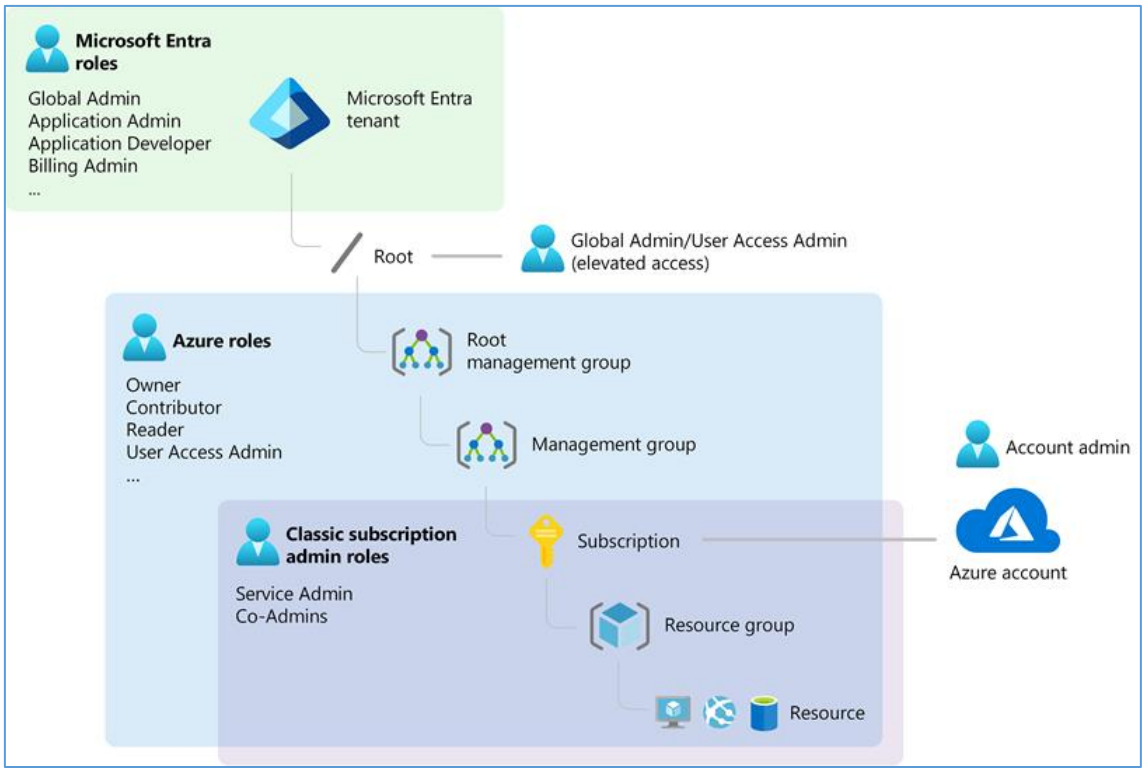
Cuando se habilita el acceso JIT, Microsoft Defender for Cloud restringe el tráfico entrante a las máquinas virtuales mediante la creación de una regla de NSG. Es necesario seleccionar los puertos de la máquina virtual cuyo tráfico entrante se va a bloquear. El control de estos puertos lo gestiona la solución de acceso JIT.

Nota: Se puede encontrar más información en: https://learn.microsoft.com/es-es/azure/defender-for-cloud/just-in-time-access-usage

3.1.1.3 SEGREGACIÓN DE FUNCIONES Y TAREAS

Para la segregación de funciones y tareas se asignan roles a los usuarios de su *Tenant* mediante RBAC. Se podrán asignar roles personalizados para los grupos de administración y suscripciones.

El siguiente diagrama muestra un ejemplo de creación de una jerarquía que se recomienda para los grupos de administración.



Se recomienda la previa creación de grupos asignados mediante roles a distintas funciones dentro del *Tenant*.

Se puede consultar la gestión de roles **RBAC** en el apartado [3.1.1.1 Despliegue de un rol personalizado] de la presente guía.

3.1.1.4 PROCESO DE GESTIÓN DE DERECHOS DE ACCESO

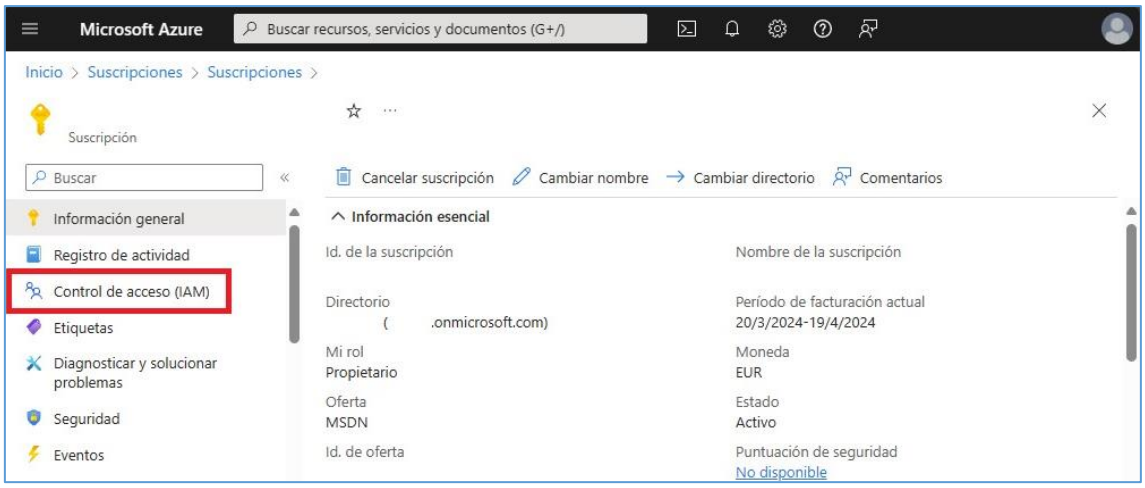
Azure implementa operaciones de datos que permiten conceder acceso a los datos dentro de un objeto.
Se puede especificar un ámbito en varios niveles: grupo de administración, suscripción, grupo de recursos o recurso.
A continuación, se describen los roles que se recomienda aplicar desde el punto de vista de seguridad.

- **Propietario:** Acceso total a todos los recursos, incluido el derecho a delegar este acceso a otros.
- **Colaborador:** Tiene permisos para crear y administrar todos los tipos de recursos de Azure, pero no puede conceder acceso a otros.
- **Lector:** Tiene permisos para ver los recursos existentes de Azure.
- **Administrador de acceso de usuario:** Tiene permisos para administrar el acceso de los usuarios a los recursos de Azure.

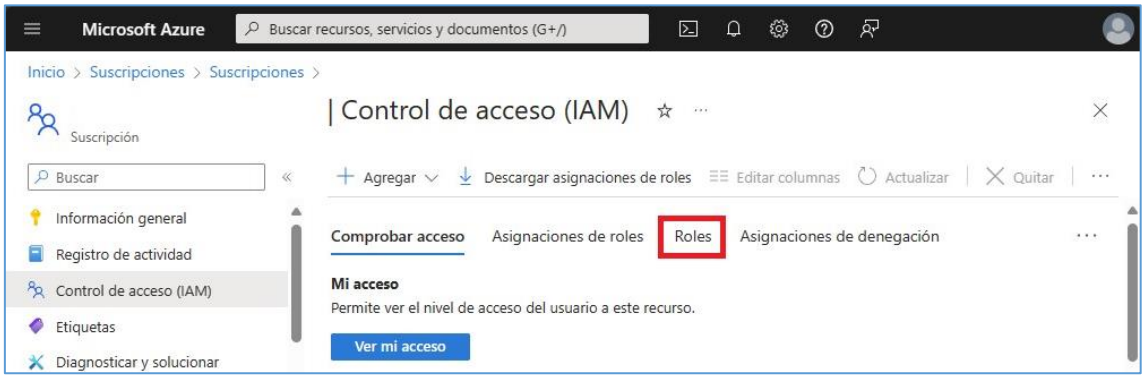
Para ello, seguir estas instrucciones:

a) En el buscador escribimos [Suscripciones].

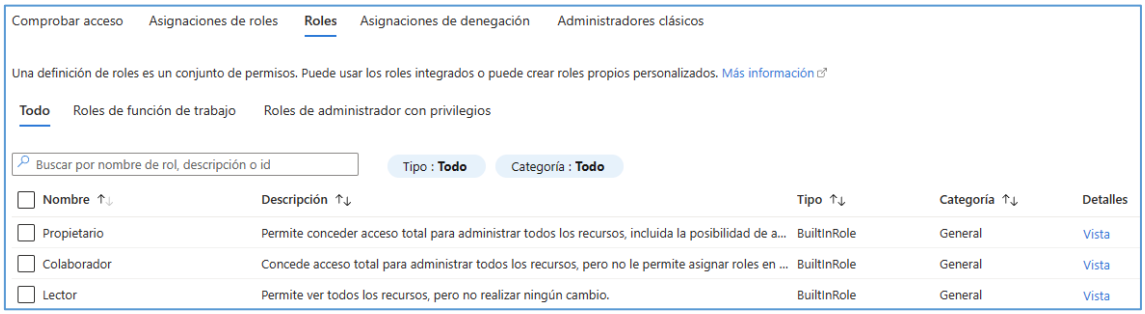
b) Seleccionar una suscripción, pulsar sobre [Control de acceso IAM].



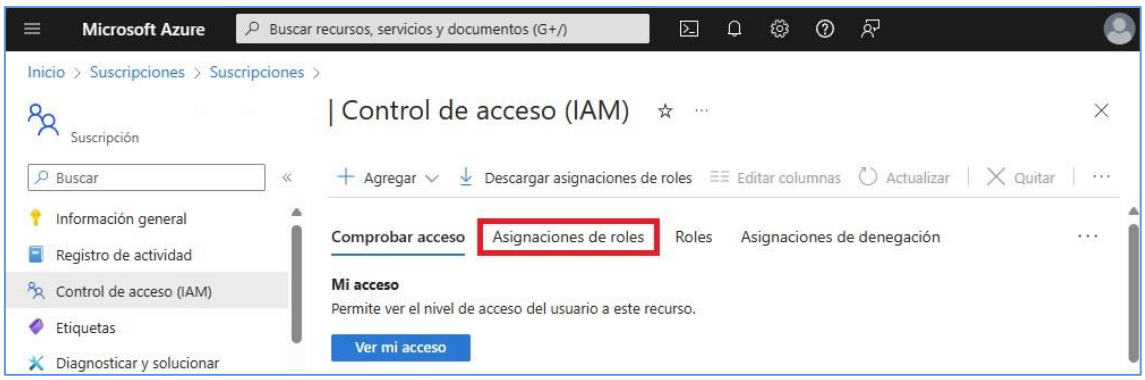
c) Pulsar en [Roles].



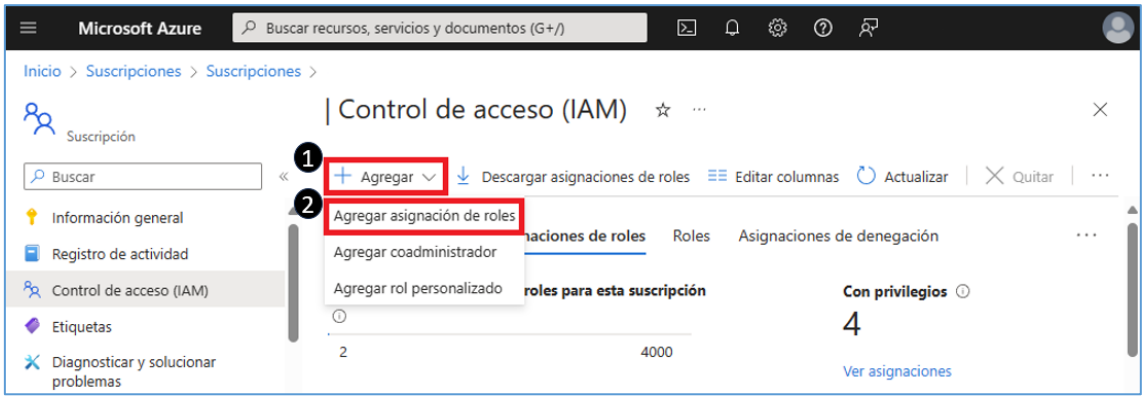
d) Aquí se puede ver los usuarios que tienen los roles mencionados.



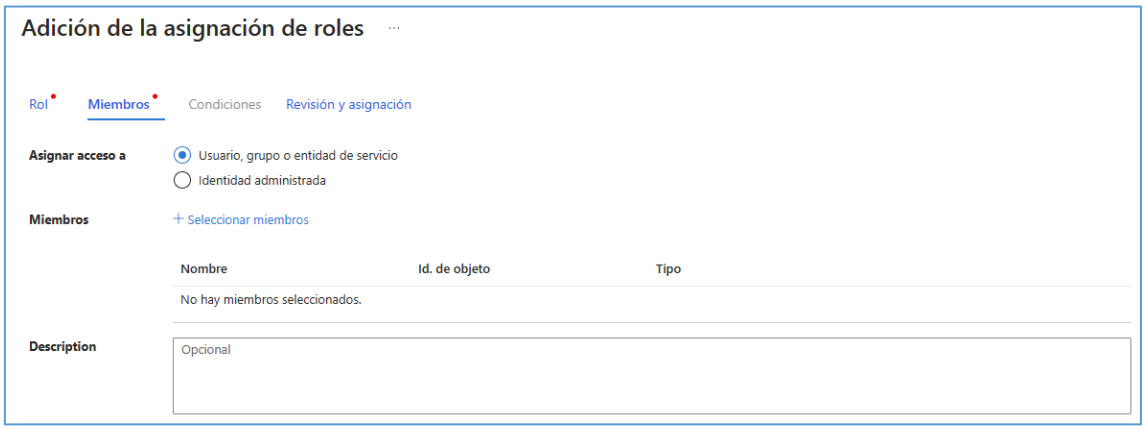
e) Para asignar un rol, se debe pulsar sobre [Asignaciones de roles].



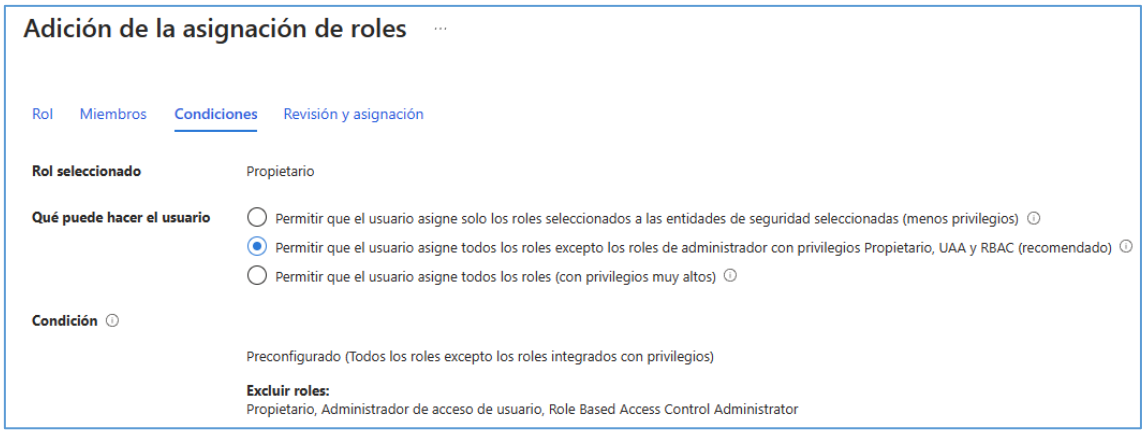
f) Pulsar en [Agregar/Agregar asignación de roles].



g) Se seleccionar un rol.
h) Se selecciona un usuario / grupo / identidad administrada.



i) Dependiendo del rol, si este tiene capacidades de asignación de permisos, se puede limitar el ámbito donde se pueden aplicar dichos permisos.



j) Para finalizar pulsar en [Revisar y asignar].

Nota: *Recuerde que en Azure se puede asignar distintos roles, tanto desde este panel como en un servicio específico.*

Se recomienda, que utilice roles personalizados RBAC. Para ello, consultar en el apartado [3.1.1.1 Despliegue de un rol personalizado] de la presente guía.

3.1.1.5 MECANISMOS DE AUTENTICACIÓN (USUARIOS EXTERNOS)

Los mecanismos de autenticación aplicables para usuarios externos son los mismos que para usuarios de la organización. Para más información ver el apartado [3.1.1.6 Mecanismos de autenticación (usuarios de la organización)].

3.1.1.6 MECANISMOS DE AUTENTICACIÓN (USUARIOS DE LA ORGANIZACIÓN)

La autenticación multifactor (MFA) de Microsoft Entra protege el acceso a los datos y aplicaciones, y al mismo tiempo mantiene la simplicidad para los usuarios. Proporciona más seguridad, ya que requiere una segunda forma de autenticación y ofrece autenticación segura a través de una variedad de métodos de autenticación.

CONSIDERACIONES DE LA IMPLEMENTACIÓN

La autenticación multifactor (MFA) de Microsoft Entra se puede implementar sin necesidad de aplicar directivas de acceso condicional. En esta guía se recomienda que cuando este implantado MFA se utilice una directiva de acceso condicional con el objetivo de que los usuarios realicen la autenticación multifactor y **considerar varios criterios para determinar quién debe usarla. Estos son algunos de los ejemplos**:

a) **Pertenencia a un grupo:** miembros específicos de un grupo.
b) **Roles de usuario:** ciertos roles dentro de la organización que por ejemplo manejen información confidencial.
c) **Ubicación de inicio de sesión:** ubicaciones desconocidas o no confiables (Requiere Microsoft Entra ID Protection).
d) **Tipo de dispositivo:** usuarios que se conectan desde dispositivos que no son de la empresa o que no cumplen con las políticas de seguridad de la empresa.

e) **Acceso a aplicaciones específicas:** acceso a aplicaciones específicas que contienen información sensible.
f) **Comportamiento de inicio de sesión sospechoso**: Si se detecta un comportamiento de inicio de sesión sospechoso, como inicios de sesión a horas inusuales o desde ubicaciones geográficas inusuales (Requiere Microsoft Entra ID Protection).
g) **Tipo de red:** usuarios que se conectan desde redes no seguras o públicas.
h) **Nivel de acceso:** usuarios que necesitan acceder a niveles más altos de información.
i) **Historial de seguridad del usuario:** Si ha sido víctima de un ataque de seguridad o ha demostrado comportamientos de seguridad pobres (Requiere Microsoft Entra ID Protection).
j) **Tipo de aplicación**: usuarios que intentan acceder a aplicaciones críticas o sensibles.

MÉTODOS DE AUTENTICACIÓN

MFA de Microsoft Entra permite configurar varios métodos de autenticación. Para ello, se debe configurar una política que defina el método con el que se van a registrar los usuarios.

A continuación, se describen los métodos que se recomiendan desde el punto de vista de seguridad **considerando los métodos más seguros los que utilizan la autenticación sin contraseña,** además de ser los más difíciles de duplicar o robar proporcionando una capa de seguridad más allá de una simple contraseña.

a) **Windows Hello para empresas**: Este método utiliza datos biométricos o un PIN para autenticar a los usuarios.
b) **Aplicación Microsoft Authenticator**: Esta aplicación genera códigos de verificación únicos, o permite la autenticación mediante notificaciones push.
c) **Clave de seguridad FIDO2**: Las claves de seguridad FIDO2 son dispositivos físicos que se utilizan para la autenticación.

ACTIVACIÓN MFA EN LOS USUARIOS DE MICROSOFT ENTRA ID

Para activar el MFA de Microsoft se deben seguir las directrices descritas a continuación.

Como se menciona anteriormente, la Autenticación multifactor de Microsoft Entra se puede habilitar sin necesidad del acceso condicional, utilizando un método obligado de doble factor de autenticación para los usuarios.

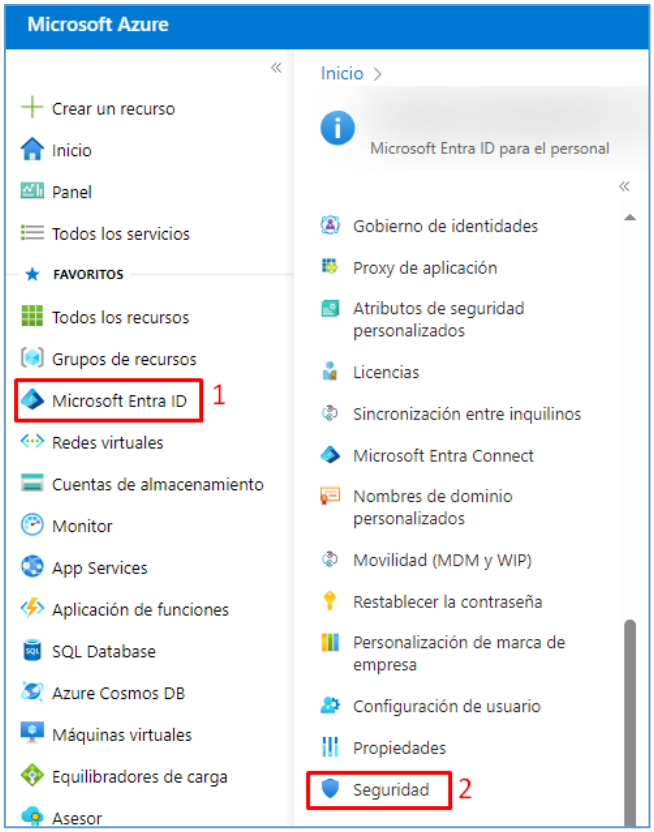
Elegiremos los métodos que queremos habilitar y su configuración, tal y como se indicó en puntos anteriores se recomiendan los métodos de:

- Microsoft Authenticator.
- Clave de seguridad FIDO2.

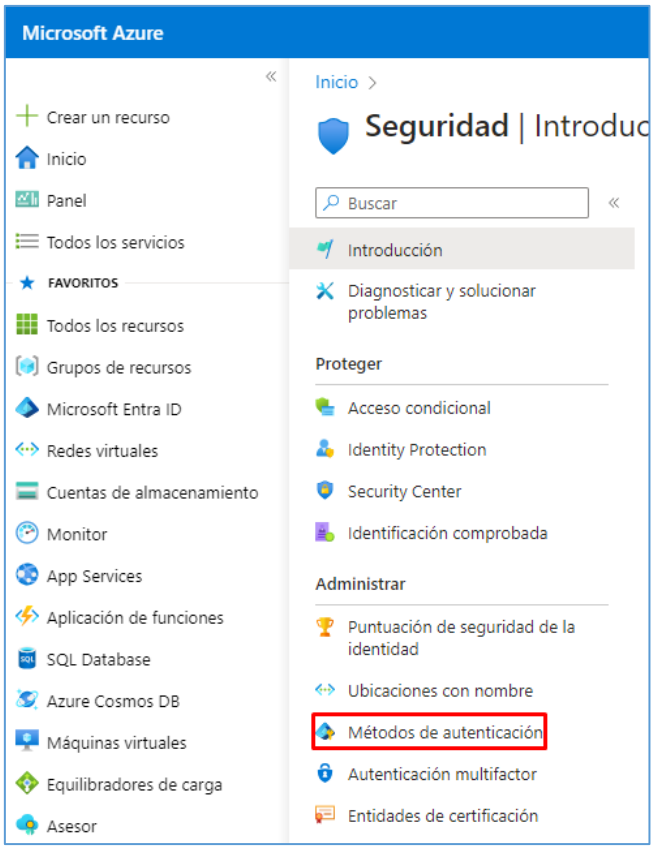
Siga estas instrucciones:

a) Desde el portal de Azure, pulsar en [Microsoft Entra ID]

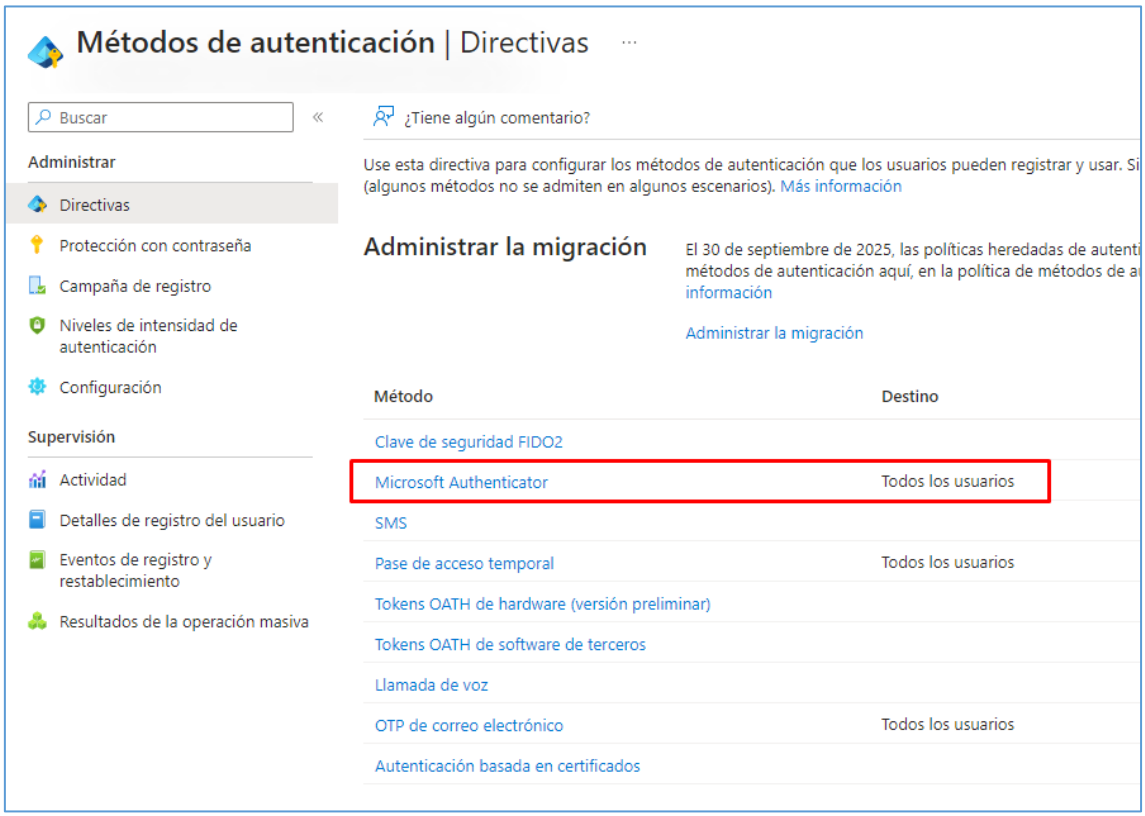
b) Pulsar en el apartado de [Seguridad]



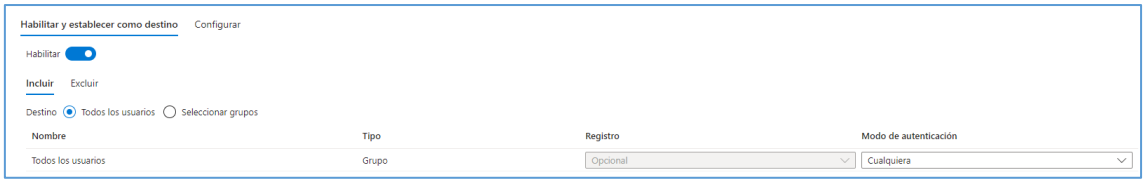
c) Una vez allí, elegir la opción de **[Métodos de autenticación]**.



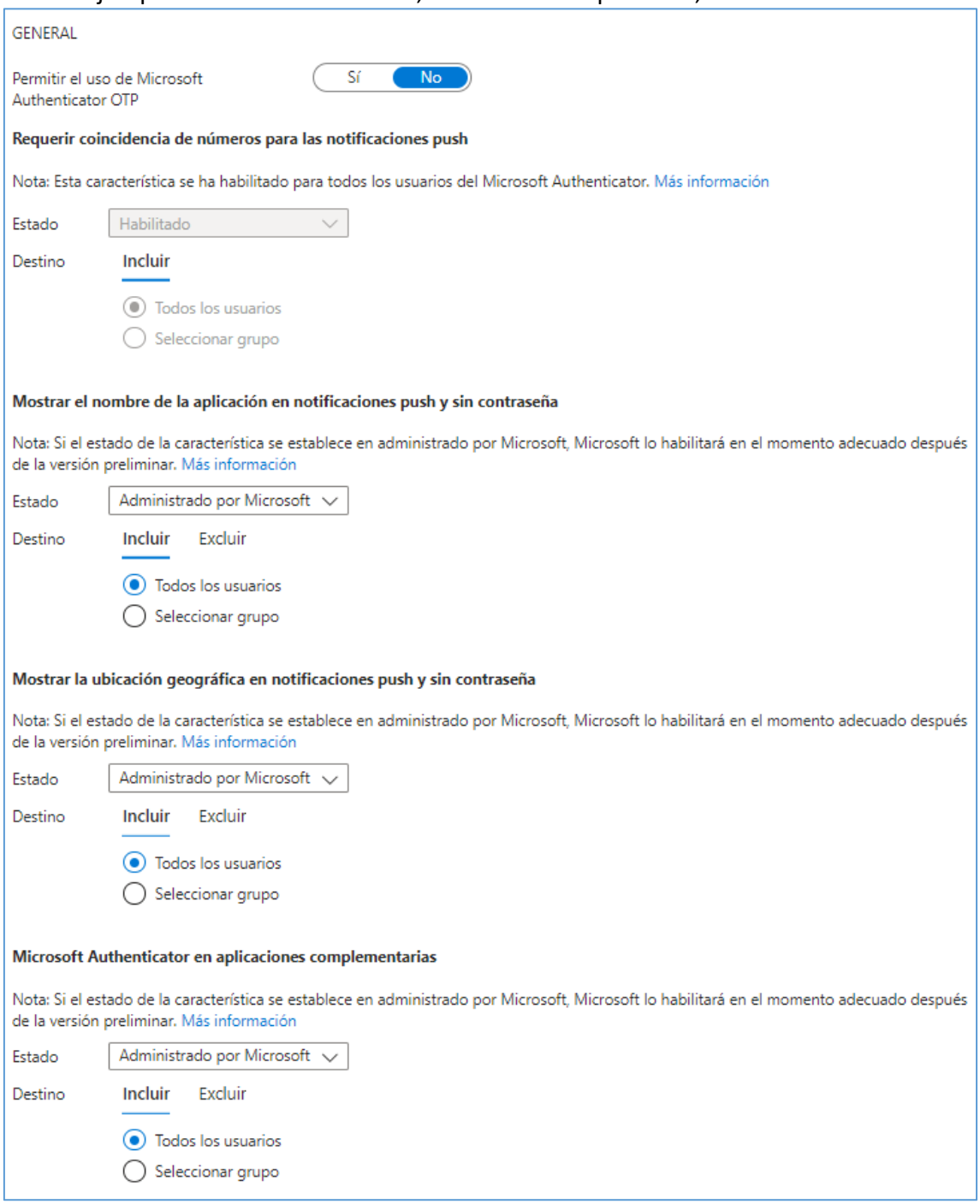
d) Pulsar en la configuración que se quiera editar. En este caso [Microsoft Authenticator].



e) Habilitamos el método y en este caso elegiremos que se incluya a todos los usuarios.



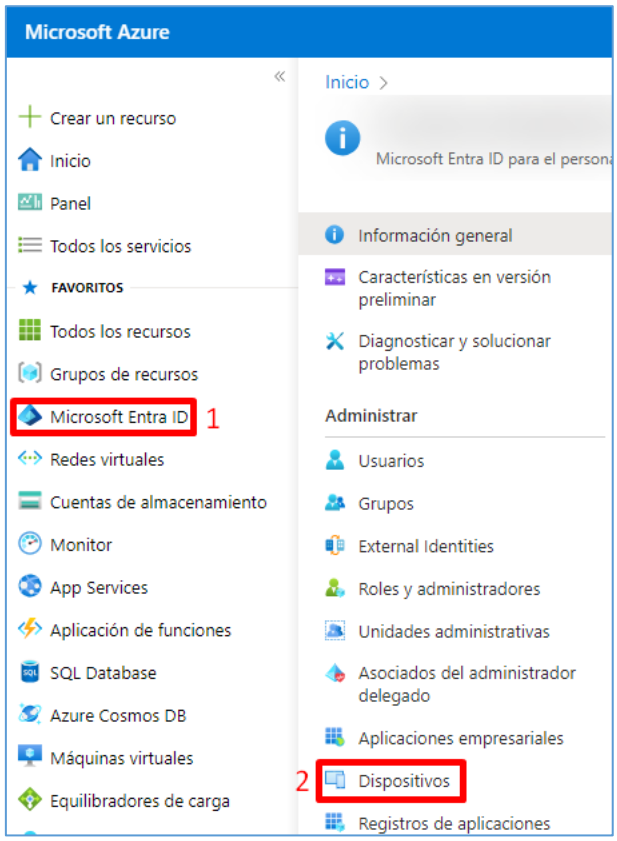
f) Dentro de este mismo apartado, pero en la pestaña Configurar se pueden cambiar los diferentes parámetros para mostrar en Microsoft Authenticator, por ejemplo: Mostrar la ubicación, nombre de la aplicación, etc.



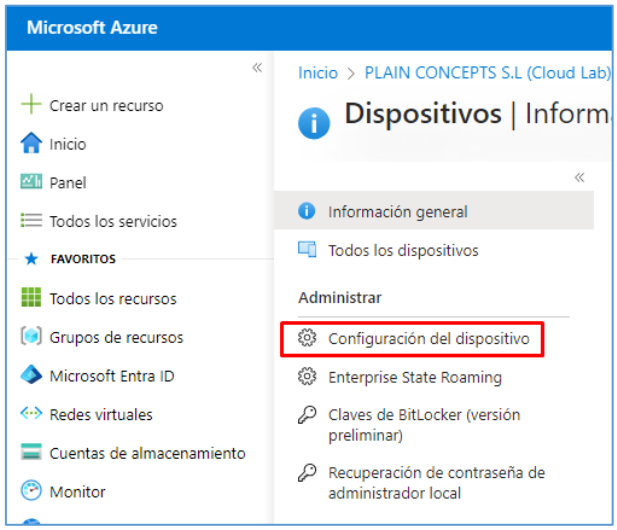
HABILITAR AUTENTICACIÓN MULTIFACTOR EN DISPOSITIVOS

Se puede habilitar el multifactor en los dispositivos, para ello hay que seguir estas directrices.

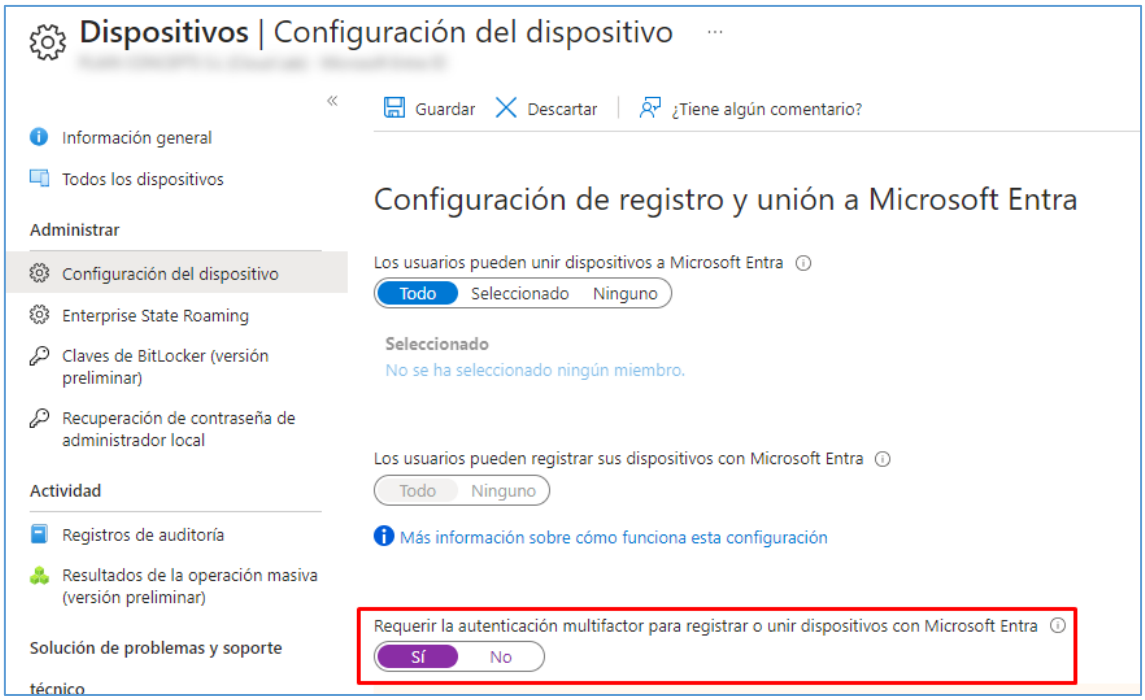
a) Desde el portal de Azure, pulsar en [Microsoft Entra ID/Dispositivos].



b) Pulsar en configuración de dispositivos.



c) Marcar con la opción en SI de Requerir la autenticación multifactor para registrar o unir dispositivos con Microsoft Entra y pulsar el botón de Guardar en la parte superior.



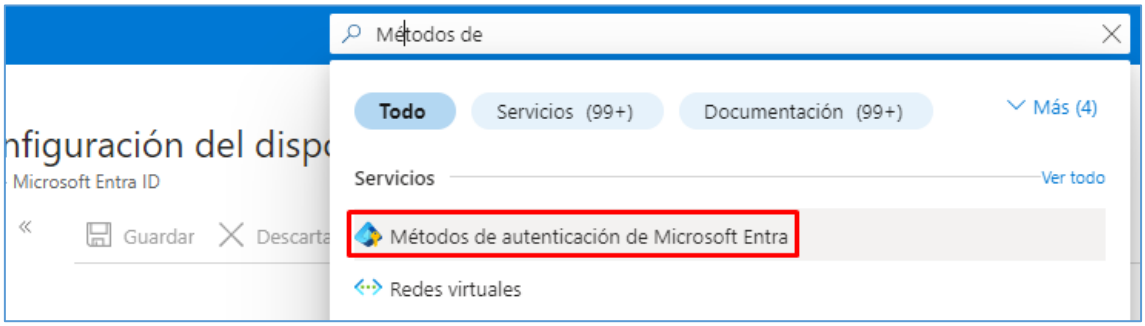
Nota: Recuerde que esta configuración es aplicada para todos los dispositivos. Desde el mismo panel se puede seleccionar los usuarios y los grupos que pueden unir dispositivos a Azure AD en caso de que desee limitarlo.

MÉTODOS DE AUTENTICACIÓN

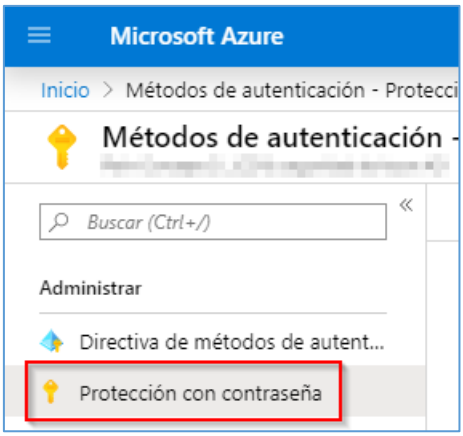
Otra medida recomendada en esta guía es la protección a través de la configuración de contraseñas de Microsoft Entra, tanto en el umbral de intentos como en bloqueos y auditoria.

Para ello, se recomienda seguir estas directrices.

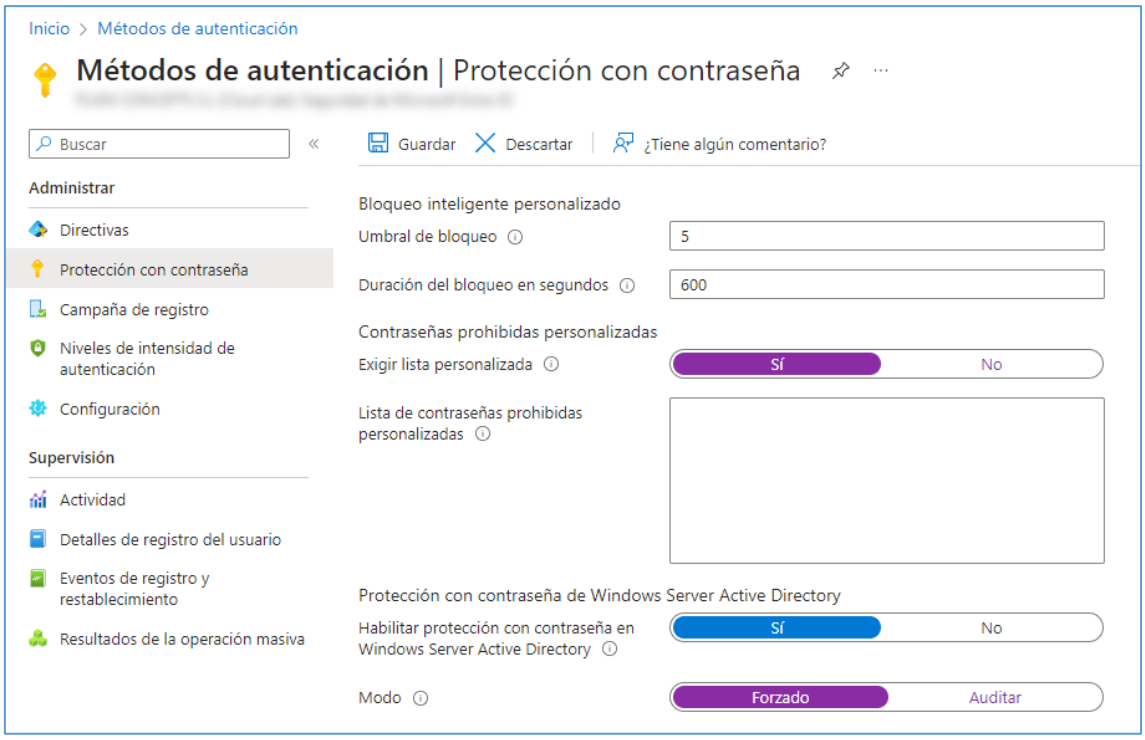
a) Desde el portal de Azure, buscar Métodos de autenticación.



b) Pulsar en [Protección de contraseñas].



c) Seguir las instrucciones recomendadas.



Se debe personalizar el bloqueo de cuentas en múltiples intentos, para ello siga estas instrucciones.

- **Umbral de bloqueo:** Es aconsejable que el valor sea como máximo de 5 intentos.
- **Duración de bloqueo en segundos:** Recomendado en 60 segundos.
- **Contraseñas prohibidas:** Cuando se habilita, las palabras de la lista siguiente se usan en el sistema de contraseñas prohibidas para evitar el uso de contraseñas fáciles de averiguar.
- **Protección de contraseñas:** Se debe activar para la protección de contraseñas en los controladores de dominio de Active Directory.
  Nota: *Puede consultar más información sobre protección de contraseñas en este artículo.*
  https://docs.microsoft.com/es-es/azure/active-directory/authentication/howto-password-ban-bad-on-premises-deploy

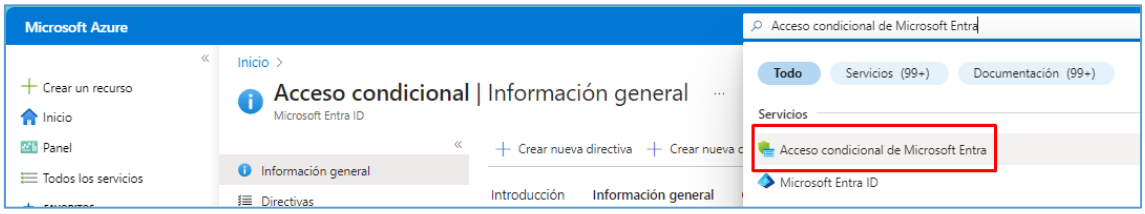
- **Método:** Se debe seleccionar Forzado. De esta forma, los usuarios no pueden configurar contraseñas prohibidas y el intento se registra.

d) Para finalizar, pulsar en [guardar].

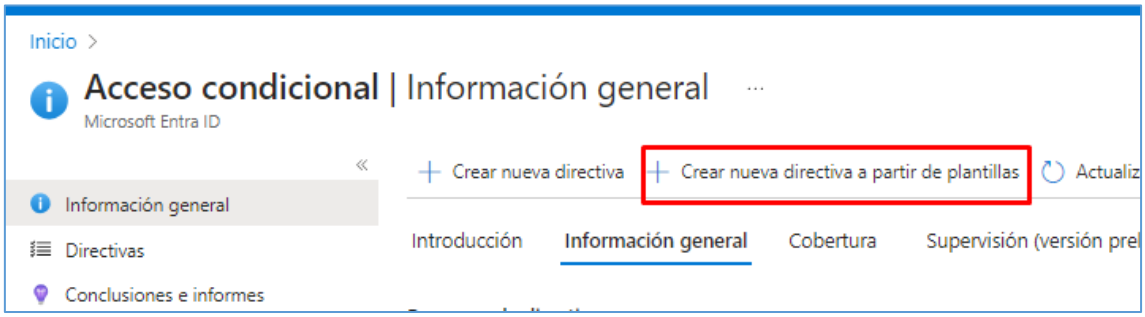
REQUERIR AUTENTICACIÓN MULTIFACTOR MEDIANTE *POLÍTICAS DE ACCESO CONDICIONAL*

Se pueden configurar políticas de acceso condicional para multitud de opciones. Vamos a configurar el Requerimiento de autenticación multifactor para todos los usuarios creando una directiva a partir de una plantilla definida.

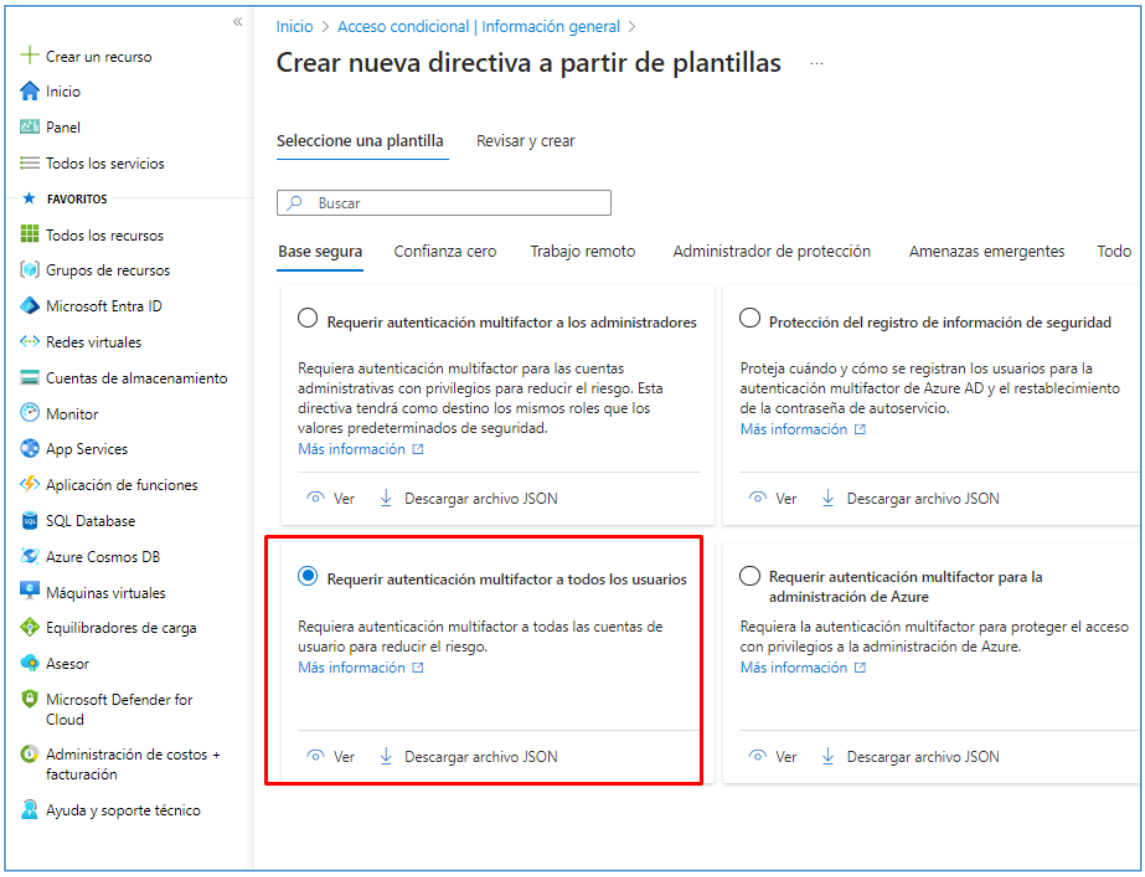
a) Entrar en [Acceso condicional de Microsoft Entra]



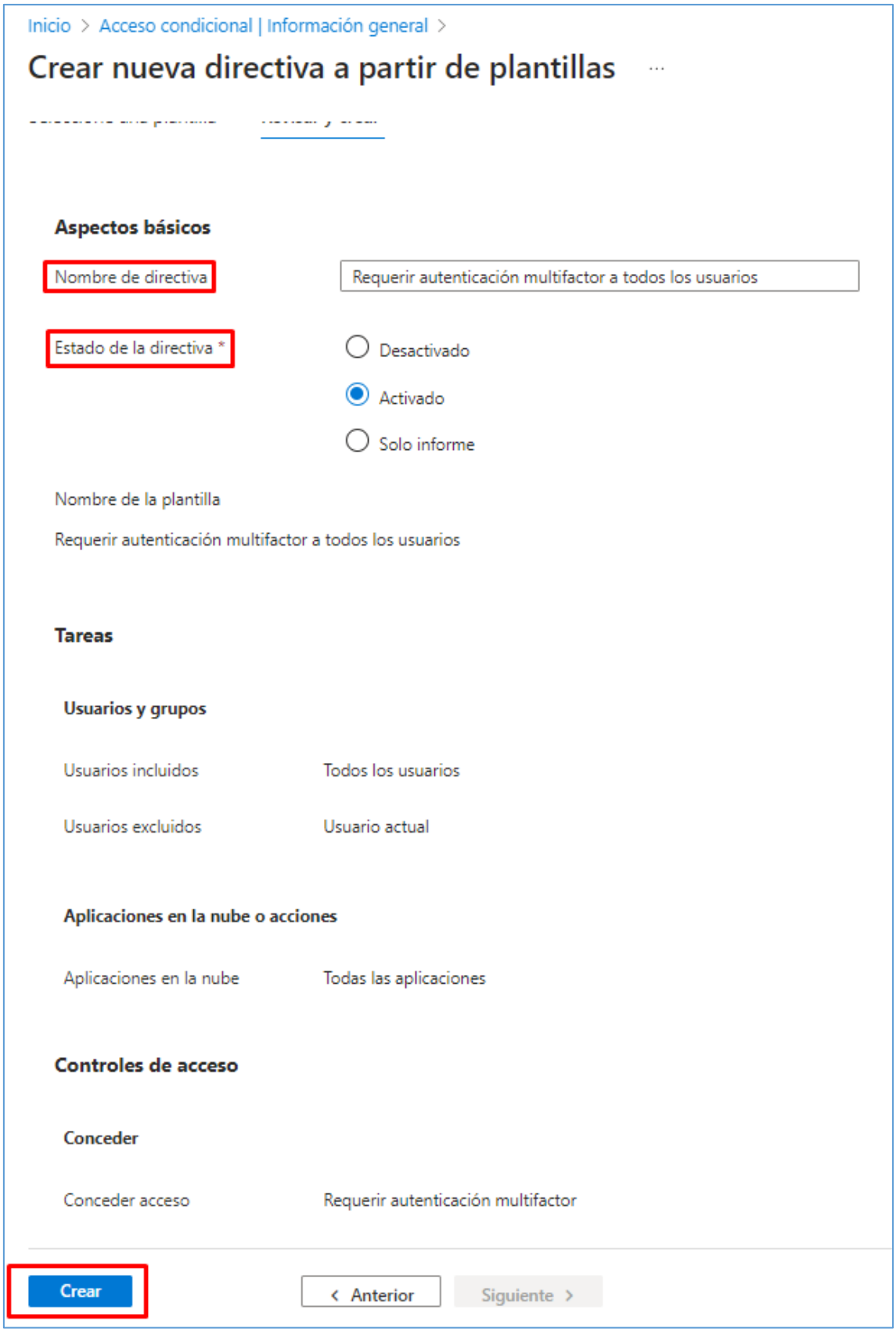
b) Pulsamos en [Crear una nueva directiva a partir de plantillas]



c) Bajo la pestaña **Base segura** pulsamos en Requerir autenticación multifactor a todos los usuarios o bien lo buscamos y pulsamos sobre el botón en la parte inferior de Revisar y crear.



d) Indicamos el nombre y la activamos. Pulsamos en el botón crear.


Inicio > Acceso condicional | Información general >
Crear nueva directiva a partir de plantillas
Aspectos básicos
Nombre de directiva
Requerir autenticación multifactor a todos los usuarios
Estado de la directiva *
Desactivado
Activado
Solo informe
Nombre de la plantilla
Requerir autenticación multifactor a todos los usuarios
Tareas
Usuarios y grupos
Usuarios incluidos
Todos los usuarios
Usuarios excluidos
Usuario actual
Aplicaciones en la nube o acciones
Aplicaciones en la nube
Todas las aplicaciones
Controles de acceso
Conceder
Conceder acceso
Requerir autenticación multifactor
Crear
Anterior
Siguiente

MICROSOFT ENTRA ID - CREACIÓN DE APLICACIÓN EMPRESARIAL

Una *aplicación empresarial* hace uso principalmente de las siguientes características:

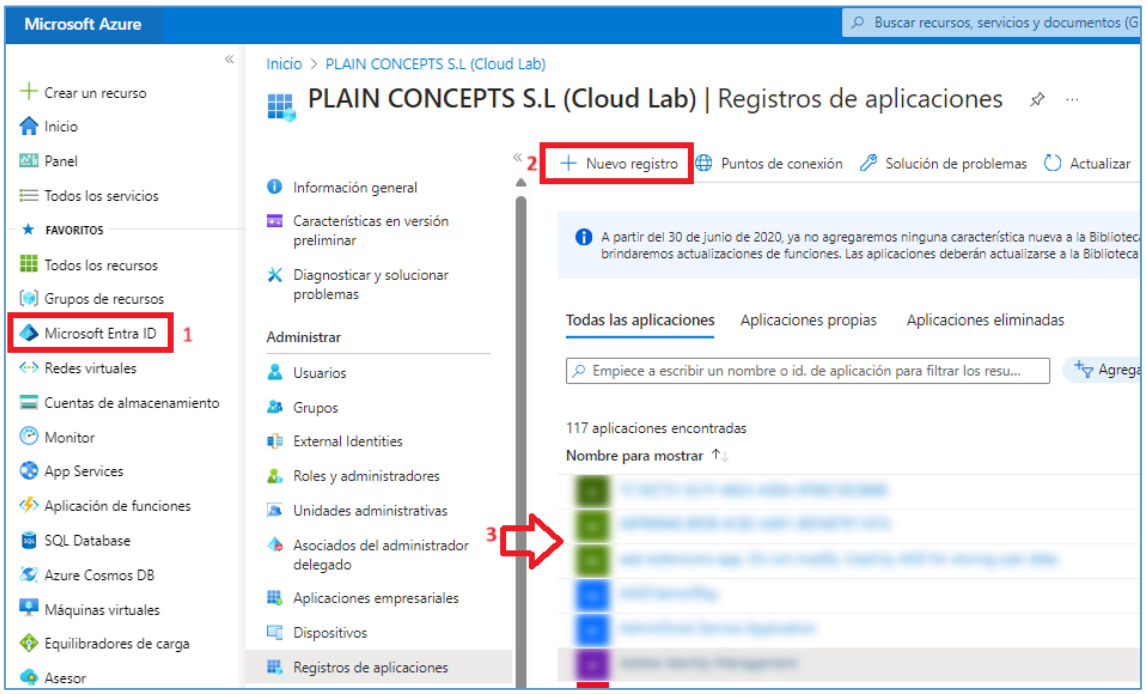
a) **Integración de Aplicaciones**: Microsoft Entra ID permite a las empresas integrar sus aplicaciones internas y externas. Los empleados pueden acceder a todas las aplicaciones que necesitan para su trabajo desde un solo lugar, lo que mejora la productividad y la eficiencia.

b) **Inicio de Sesión Único (SSO)**: Con el inicio de sesión único, los usuarios pueden acceder a todas sus aplicaciones con un solo conjunto de credenciales. Esto no solo mejora la experiencia del usuario, sino que también aumenta la seguridad al reducir la necesidad de recordar múltiples contraseñas.

c) **Gestión de Acceso a Aplicaciones**: Microsoft Entra ID permite a las empresas controlar quién tiene acceso a qué aplicaciones. Esto es crucial para proteger los datos sensibles y garantizar que solo las personas adecuadas tengan acceso a las aplicaciones correctas.

Se recomienda utilizar las credenciales de tipo federadas siempre que sea posible, aunque existen las opciones de crear credenciales con certificados y de tipo clave.

Para crear una aplicación pulse en [Microsoft Entra ID/Registros de aplicaciones] > Nuevo Registro. Una vez creada, la puedes ver en el listado y buscarla usando la caja de texto destinada para ello.



ACCESO LOCAL (LOCAL LOGON)

Se recomienda usar un acceso condicional para discriminar los accesos locales permitidos desde la oficina u otro acceso que se requiera autorizado, teniendo en cuenta, por ejemplo, la dirección IP de origen o los dispositivos utilizados.
La configuración del MFA se describe en el *apartado* [3.1.1.2 Requisitos de acceso] de la presente guía.

3.1.2 EXPLOTACIÓN

3.1.2.1 REGISTRO DE LA ACTIVIDAD

Con esta funcionalidad, se puede enviar registros de auditoría y de inicios de sesión de Microsoft Entra ID a una cuenta de almacenamiento de Azure, a un centro de eventos, también a Azure Monitor o a una solución personalizada.

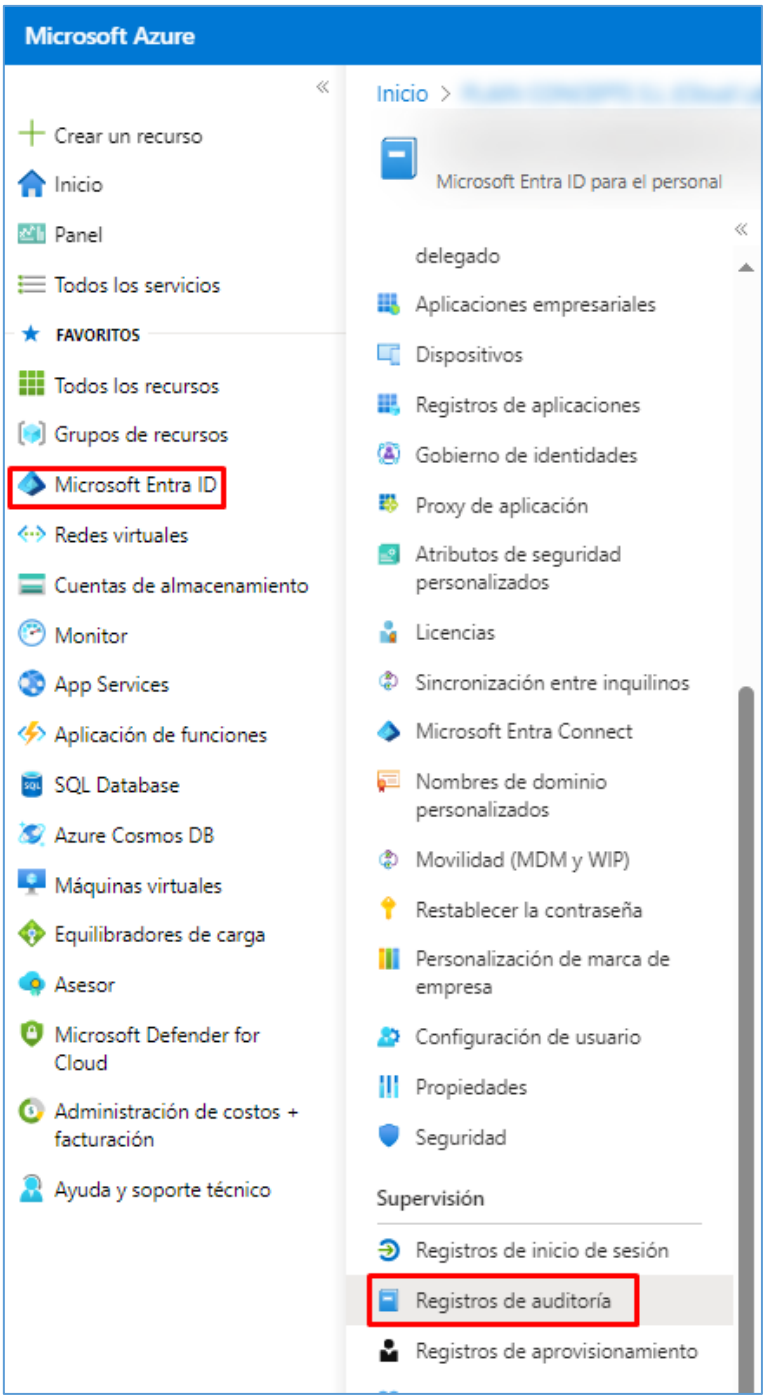
A continuación, se describen los tipos de registro relacionados con la actividad de los usuarios:

- **Registros de auditoría:** El informe de actividad de registros de auditoría proporciona acceso al historial de todas las tareas llevadas a cabo en el *Tenant*.
- **Registros de inicio de sesión:** El informe de actividad de inicios de sesión, determina quién ha realizado las tareas incluidas en el informe de registros de auditoría.

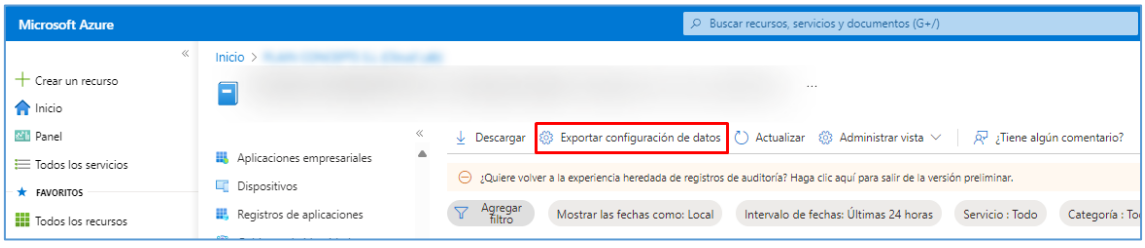
Nota: Para acceder a este registro se debe disponer de los permisos necesarios.

Para consultar los registros pulse en:

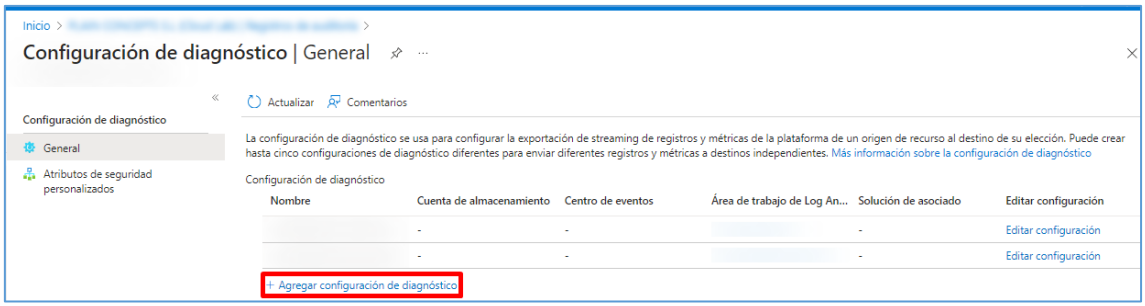
a) **[Microsoft Entra ID/Registros de auditoria].**



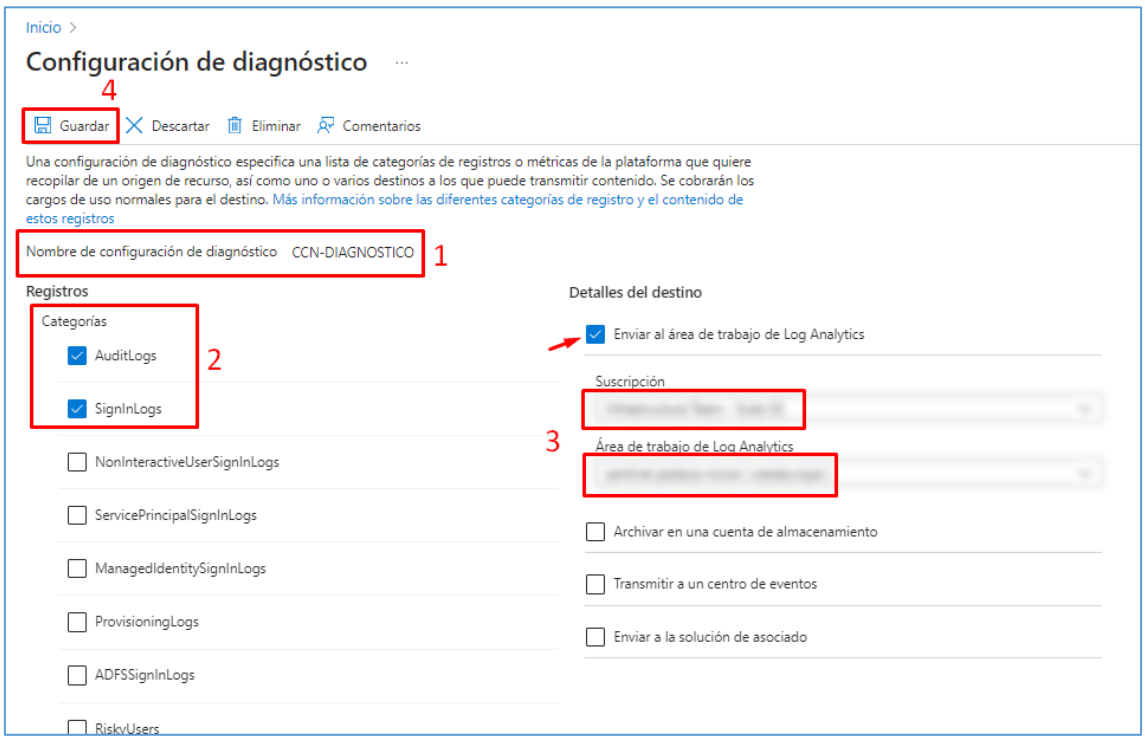
b) Pulsar en [Exportar configuración de datos].



c) Pulsar en [Agregar configuración de diagnóstico].

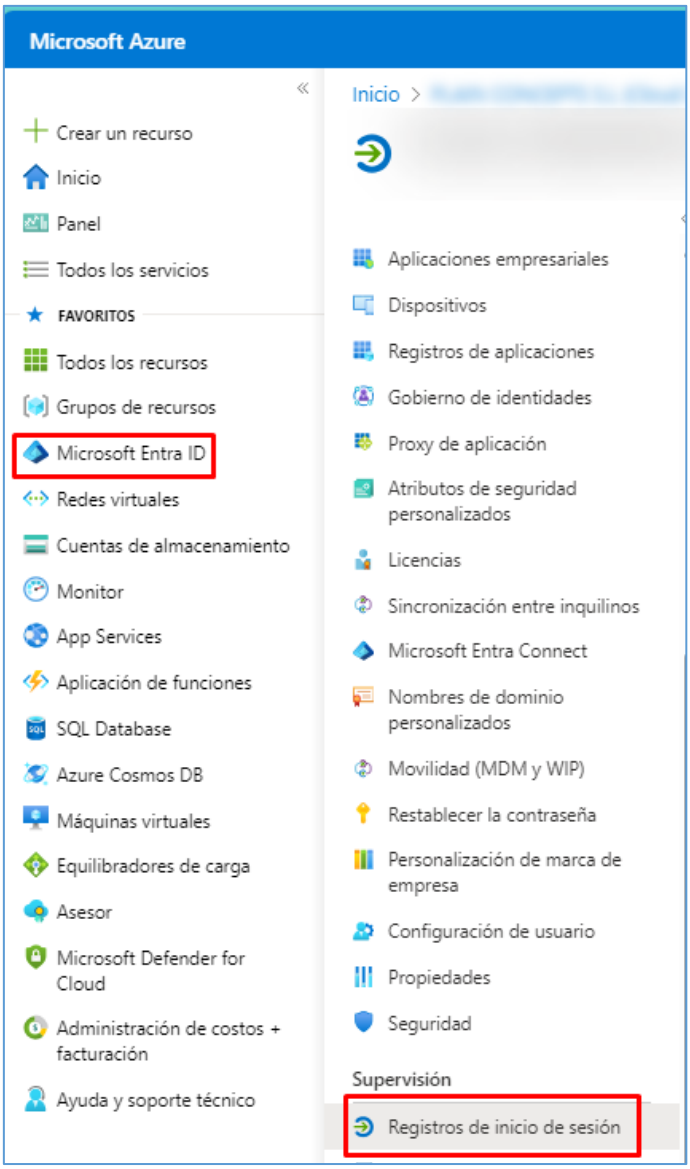


d) Definir un nombre y marcar la opción de Enviar al área de trabajo de Log Analytics. En este caso marcar las categorías de registros, las Categorías de "AuditLogs" y "SignInLogs" y enviar los detalles al Log Analytics aunque se podría enviar a una cuenta de almacenamiento u otras opciones.

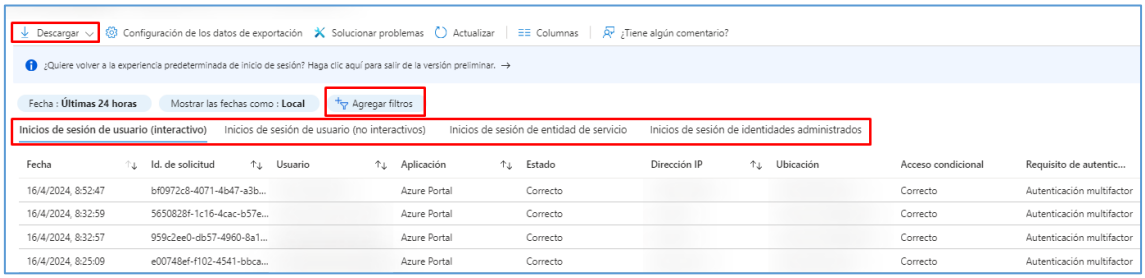


Una vez guardado desde la ventana anterior de Registros de auditoria se pueden consultar los resultados y descargar en formato CSV o JSON.

También se puede visualizar los inicios de sesión de los usuarios. Para ello, desde el portal de [Microsoft Entra ID/Registros de inicio de sesión].



Se puede filtrar por tipo de inicios de sesión, agregar filtros personalizados y modificar las columnas.



3.1.2.2 PROTECCIÓN DE CLAVES CRIPTOGRÁFICAS

Azure Key Vault es un servicio en la nube que se usa para administrar claves criptográficas, secretos y certificados.

Key Vault también permite almacenar de forma segura claves y secretos protegidos con un HSM[1]. Los HSM utilizados han sido certificados conforme a las normas FIPS 140-2 Nivel 3 y eIDAS Common Criteria EAL4+.

Además, Key Vault registra los intentos de acceso y el uso de sus secretos para disponer de una traza de auditoría completa para el cumplimiento.

Azure Key Vault le ayudara a solucionar los problemas siguientes:

a) **Administración de secretos**: Azure Key Vault se puede utilizar para almacenar de forma segura y controlar de manera estricta el acceso a los tokens, contraseñas, certificados, claves de API y otros secretos.

b) **Administración de claves**: también se puede usar Azure Key Vault como una solución de administración de claves. Azure Key Vault facilita la creación y control de las claves de cifrado utilizadas para cifrar los datos.

c) **Administración de certificados**: Azure Key Vault también es un servicio que le permite aprovisionar, administrar e implementar fácilmente certificados públicos y privados de la Capa de sockets seguros y de Seguridad de la capa de transporte (SSL/TLS) para su uso con Azure y sus recursos internos conectados.

d) **Almacenamiento de secretos basado en módulos de seguridad de hardware**: las claves y secretos se pueden proteger mediante software o mediante dispositivos HSM.

TÉRMINOS KEY VAULT

A continuación, se describen una serie de aspectos importantes que es necesario conocer:

Propietario del almacén: Un propietario del almacén puede crear un almacén de claves y obtener acceso completo y control sobre él. El propietario del almacén también puede configurar una auditoría para registrar quién accede a los secretos y claves. Los administradores del *Tenant* pueden controlar el ciclo de vida de la clave, revertir a una nueva versión de la clave, realizar copias de seguridad de ella y efectuar otras tareas relacionadas.

Identidades administradas: Azure Key Vault proporciona una manera de almacenar de forma segura las credenciales y otras claves y secretos, pero el código tiene que autenticarse en Key Vault para recuperarlos. El uso de una identidad administrada permite solucionar este problema más fácilmente, al proporcionar a los servicios de Azure una identidad administrada automáticamente en Azure AD. Puede usar esta identidad para autenticarse Key Vault o en cualquier servicio que admita la autenticación de Microsoft Entra ID, sin necesidad de tener credenciales en el código.

[1] *Hardware Security Module*

MÉTODOS DE AUTENTICACIÓN

Para realizar cualquier operación con Key Vault, es necesario autenticarse. Se recomienda que utilice el siguiente método.

Identidades administradas de recursos de Azure: Cuando implementa una aplicación en una máquina virtual en Azure, puede asignar una identidad a la máquina virtual que tiene acceso a Key Vault. También puede asignar identidades a otros recursos de Azure. La ventaja de este enfoque es que la aplicación o el servicio no administran la rotación del primer secreto.

ROLES DE KEY VAULT

Con una suscripción a Azure se puede crear y usar instancias de Key Vault. Aunque Key Vault beneficia a los desarrolladores y los administradores de seguridad, el administrador de un *Tenant* que administra otros servicios de Azure puede implementarlo y administrarlo.

- Crear o importar una clave o un secreto
- Revocar o eliminar una clave o un secreto
- Autorizar usuarios o aplicaciones para acceder al almacén de claves para que puedan administrar o usar sus claves y secretos
- Configurar el uso de claves (por ejemplo, para firmar o cifrar)
- Supervisar el uso de claves

REDUNDANCIA Y DISPONIBILIDAD

Azure Key Vault tiene varias capas de redundancia para garantizar la disponibilidad de las claves y los secretos para su aplicación, aunque se produzcan errores de componentes individuales del servicio.

El contenido del almacén de claves se replica dentro de la región y en una región secundaria que se encuentre a una distancia mínima de 241 km pero dentro de la misma ubicación geográfica. Así se mantiene la disponibilidad de las claves y los secretos.

Si se produce un error en algún componente individual dentro del servicio del almacén de claves, los componentes alternativos de la región se encargan de atender la solicitud para garantizar que no se pierde funcionalidad. No es necesario realizar ninguna acción para ello. Se lleva a cabo automáticamente y es transparente para el usuario.

En el caso excepcional de que toda una región de Azure pase a estar no disponible, las solicitudes efectuadas a Azure Key Vault de esa región se envían automáticamente (un proceso conocido como conmutación por error) a una región secundaria. Cuando la región primaria vuelva a estar disponible, las solicitudes se enrutan a ella nuevamente (conmutación por recuperación). Conviene insistir en que no es necesaria ninguna acción, ya que este proceso se realiza automáticamente.

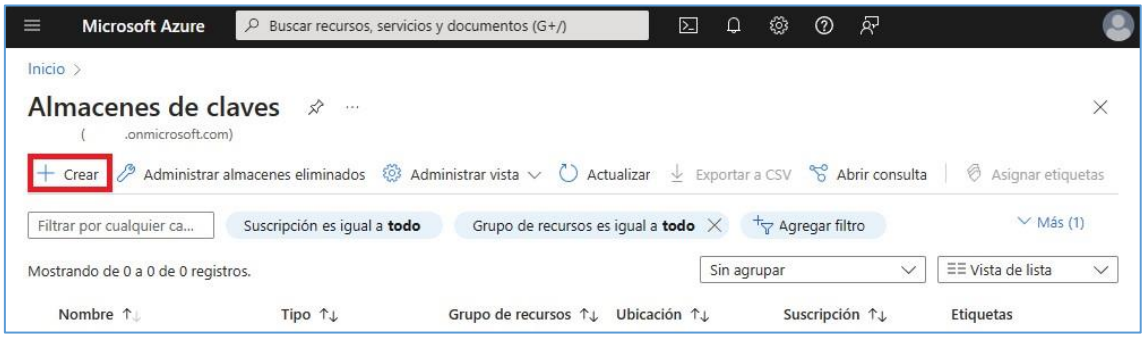
En este diseño de alta disponibilidad, Azure Key Vault no requiere ningún tiempo de inactividad para las actividades de mantenimiento.

A continuación, se indican las instrucciones que se debe seguir.

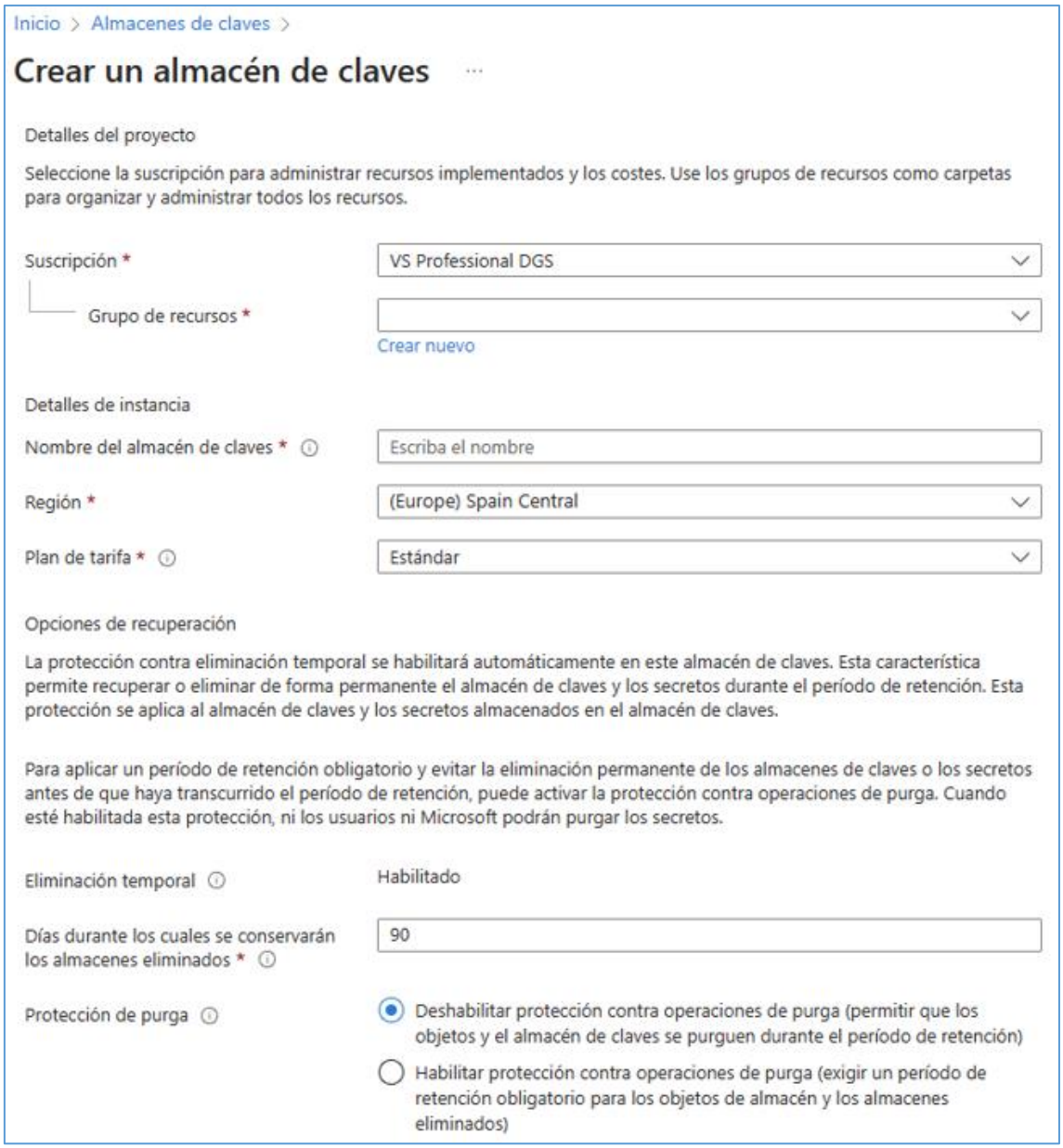
CREACIÓN DE AZURE KEY VAULT DESDE EL PORTAL.

a) En el buscador escribir [Almacenes de claves]

b) Pulsar en [Crear].

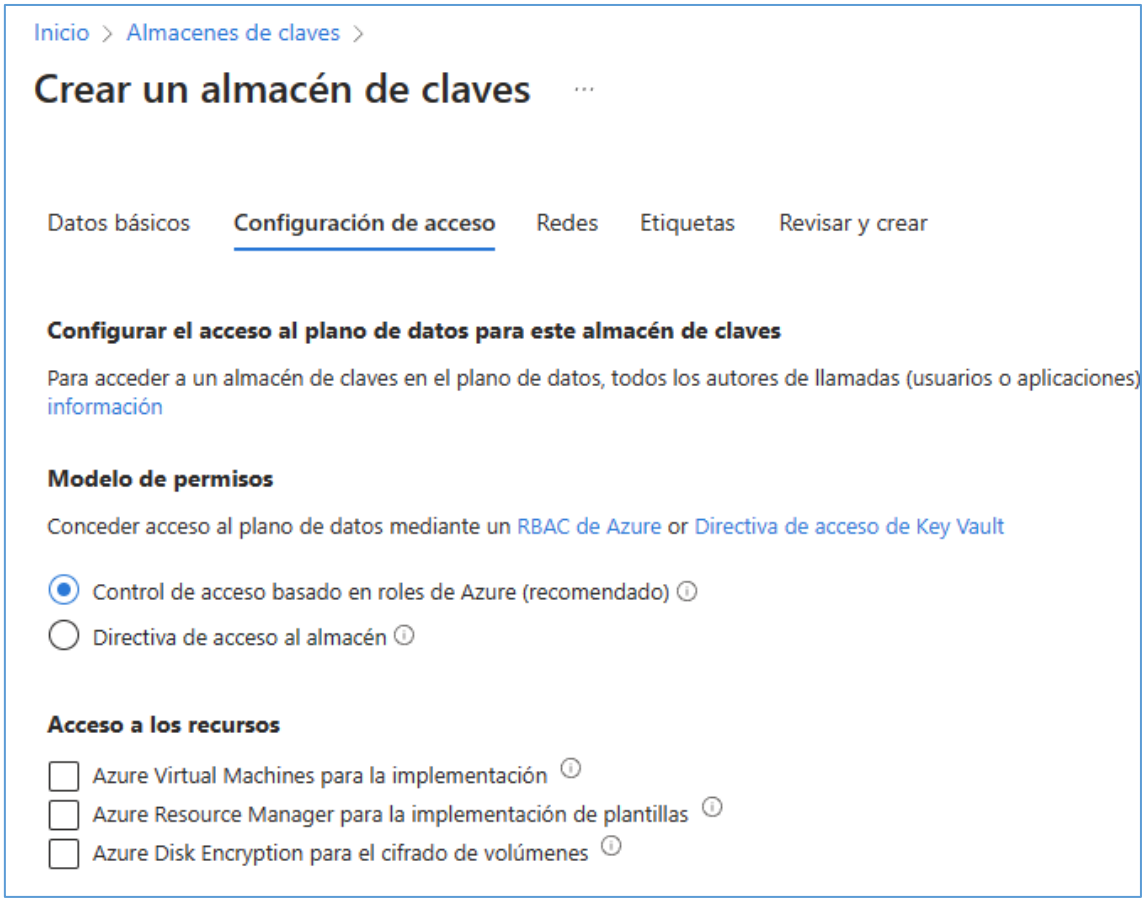


c) En la pestaña general completar la siguiente información:



- **Suscripción**: Suscripción donde se desea desplegar el Key Vault.
- **Grupo de recursos**: Es recomendable crear un nuevo grupo de recursos. Al pulsar en crear, le solicitara que lo defina con un nombre.
- **Nombre del almacén de claves**: Definir un nombre para el almacén.
- **Región**: Es recomendable desplegarlo en la región de Spain Central.
- **Plan de tarifa**: Es recomendable seleccionar "Premium" que incluye la compatibilidad con HSM.
- **Días durante los cuales se conservarán los almacenes eliminados**: Es recomendables dejarlo en 90.
- **Protección de purga**: Es recomendable habilitar esta opción para proteger el borrado del almacén de claves.

d) Pulsar en la pestaña de [Configuración de acceso].



e) Definir modelo de permisos.

a) Control de acceso basado en roles (Recomendado): Permisos basado en RBAC. Los roles disponibles se pueden encontrar en:

- https://learn.microsoft.com/es-es/azure/key-vault/general/rbac-guide?tabs=azure-cli#azure-built-in-roles-for-key-vault-data-plane-operations

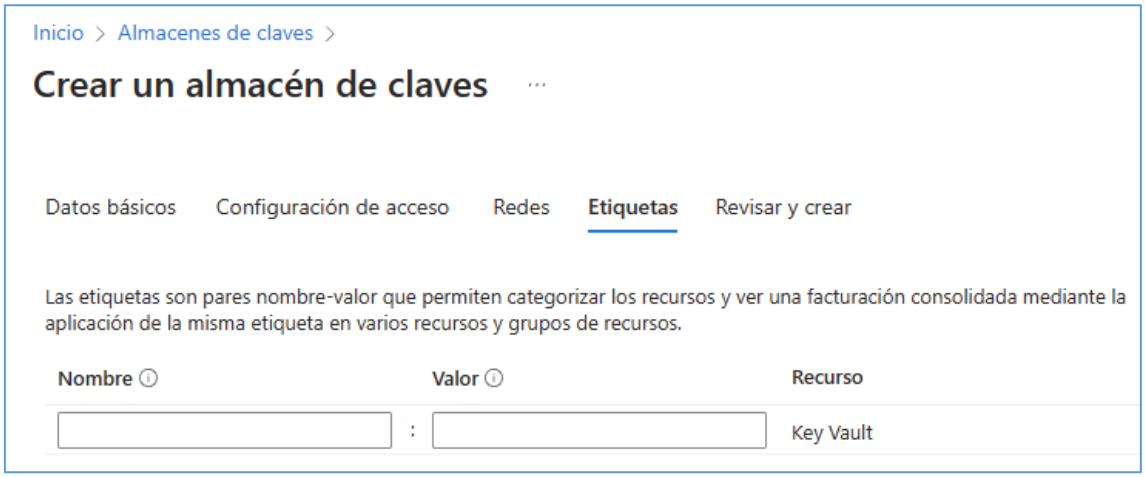
b) Directiva de acceso al almacén: Antiguo modelo de permisos del almacén de claves que en algún caso todavía puede ser necesario por limitaciones de la plataforma de Azure.

f) Habilitar los tres accesos.

- **Azure virtual machines para la implementación:** Especifica si se permite que las Azure Virtual Machines recuperen certificados almacenados como secretos del almacén de claves.
- **Azure Resource Manager para la implementación de plantillas:** Especifica si se permite que Azure Resource Manager recupere secretos del almacén de claves.
- **Azure Disk Encryption para el cifrado de volúmenes:** Especifica si se permite el Azure Disk Encryption para recuperar secretos del almacén.

g) Pulsar en la pestaña [Redes / Disabled].

h) Pulsar en la pestaña [Etiquetas].



Nombre: Definir un nombre para todo el almacén de Key Vault.

Valor: El valor que se debe usar es Producción.

i) Pulsar en [Revisar y crear].

CREACIÓN DE AZURE KEY VAULT DESDE POWERSHELL

a) Desde la consola de Powershell.

```
#  PS C:\> Connect-AzAccount
```

En la ventana emergente del explorador, escribir el nombre de usuario y la contraseña de su cuenta de Azure. Azure PowerShell obtiene todas las suscripciones asociadas a esta cuenta. PowerShell utiliza la primera de forma predeterminada.

Es posible que se deba especificar la suscripción que se usó para crear el almacén de claves. Para ver las suscripciones de su cuenta, escribir el siguiente comando:

```
# PS C:\> Get-AzSubscription
```

b) Después, para especificar la suscripción asociada al almacén de claves que se va a registrar, escribir:

```
# PS C:\> Set-AzContext -SubscriptionId "<subscription ID>"
```

Nota: Hacer que PowerShell trabaje en la suscripción correcta es un paso importante, especialmente si tiene varias suscripciones asociadas a su cuenta.

c) Se crea el Key Vault con configuración de red pública deshabilitada.

```
# PS C:\> New-AzKeyVault -ResourceGroupName "CNN-ResourceGroup" -Name
  "cnnkeyvault" -Location "Spain Central" -PublicNetworkAccess "Disabled"
```

d) Aunque se puede usar una cuenta de almacenamiento existente para sus registros, se debe crear una cuenta de almacenamiento que se dedica a los registros de Key Vault.

```
# PS C:\> $sa = New-AzStorageAccount -ResourceGroupName "CNN-ResourceGroup"
  -Name "cnnkeyvaultlogs" -Type Standard_LRS -Location "Spain Central"
```

e) A continuación, ejecutar.

```
# PS C:\> $kv = Get-AzKeyVault -VaultName "ccnKeyVault"
```

f) Habilitar el registro. Para ello, utilizar el cmdlet **Set-AzDiagnosticSetting**, junto con las variables que se han creado para la nueva cuenta de almacenamiento y el almacén de claves. También se debe establecer la marca **-Enabled** en **$true** y establecer la categoría en **AuditEvent.**

```
# PS C:\> Set-AzDiagnosticSetting -ResourceId $kv.ResourceId -
  StorageAccountId $sa.Id -Enabled $true -Category "AuditEvent"
```

De manera opcional se puede establecer una directiva de retención para los registros, de forma que los registros más antiguos se eliminen automáticamente.

Por ejemplo, establecer la directiva de retención mediante la configuración de la marca **-RetentionEnabled** en **$true** y establecer el parámetro **-RetentionInDays** nº días, Microsoft recomienda 90, con el fin de que los registros que tengan más de 90 días se eliminen automáticamente.

```
# PS C:\> Set-AzDiagnosticSetting -ResourceId $kv.ResourceId -
  StorageAccountId $sa.Id -Enabled $true -Category "AuditEvent" -
  RetentionEnabled $true -RetentionInDays 90
```

ACCESO A LOS REGISTROS

Los registros de Key Vault se almacenan en el contenedor **insights-logs-auditevent** de la cuenta de almacenamiento proporcionada. En estos registros se almacenan todos los accesos e intentos de acceso a Azure Key Vault. Para ver los registros, se tiene que descargar los blobs.

Los blobs almacenan texto y datos binarios, hasta unos 4,7 TB. Los blobs se componen de bloques de datos que se pueden administrar de forma individual.

En primer lugar, se crea una variable para el nombre del contenedor. Esta variable se usa en el resto de esta guía.

a) Desde la consola de PowerShell.

```
# PS C:\> $container = "insights-logs-auditevent"
```

b) Para mostrar una lista de todos los blobs de este contenedor, escriba:

```
# PS C:\> Get-AzStorageBlob -Container $container -Context $sa.Context
```

c) Crear una carpeta para descargar los blobs

```
# PS C:\> New-Item -Path "C:\Users\username\CcnKeyVaultLogs" -ItemType
"Directory" -Force
```

d) A continuación, obtener una lista de todos los blobs

```
# PS C:\> $blobs = Get-AzStorageBlob -Container $container -Context
$sa.Context
```

e) Canalizar esta lista mediante **Get-AzStorageBlobContent** para descargar los blobs en la carpeta de destino

```
# PS C:\> $blobs | Get-AzStorageBlobContent -Destination
"C:\Users\username\CcnKeyVaultLogs"
```

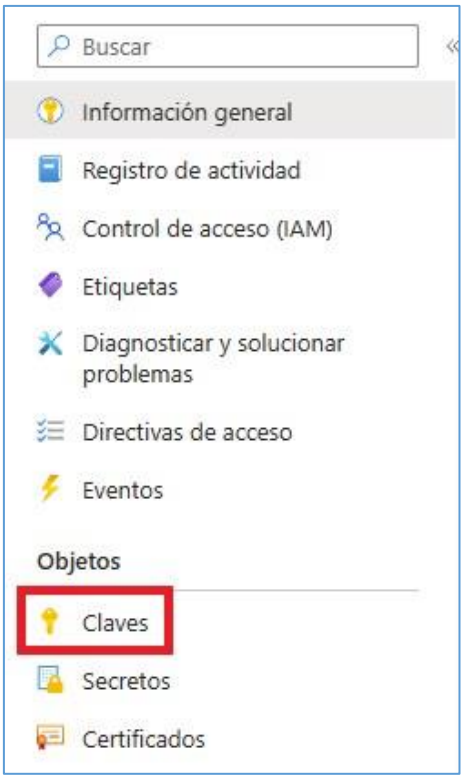
USO DEL PANEL KEY VAULT

a) En el buscador escribir [Almacenes de claves].

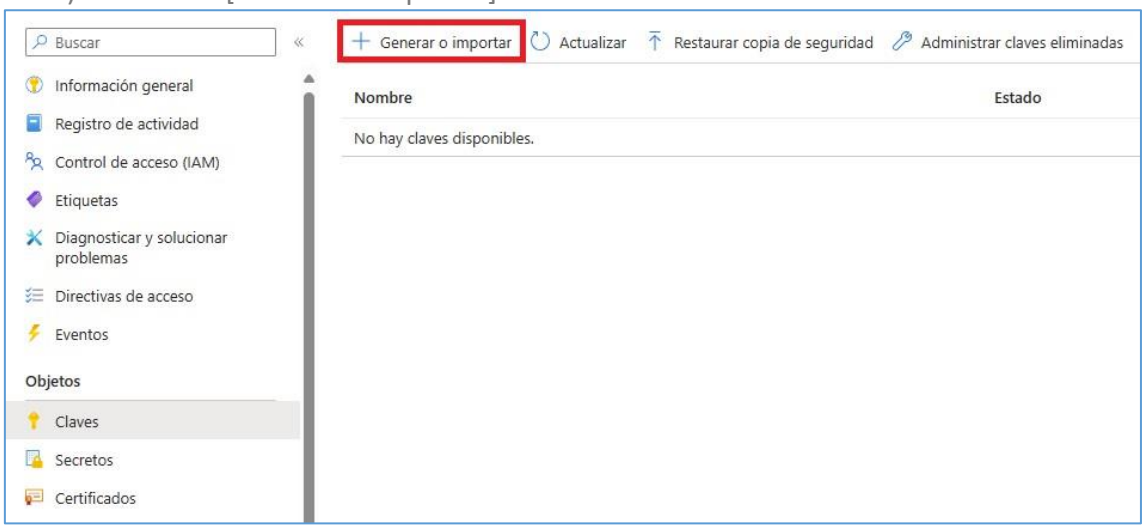
b) A continuación, seleccionar un Almacén de claves.

CREACIÓN DE CLAVES

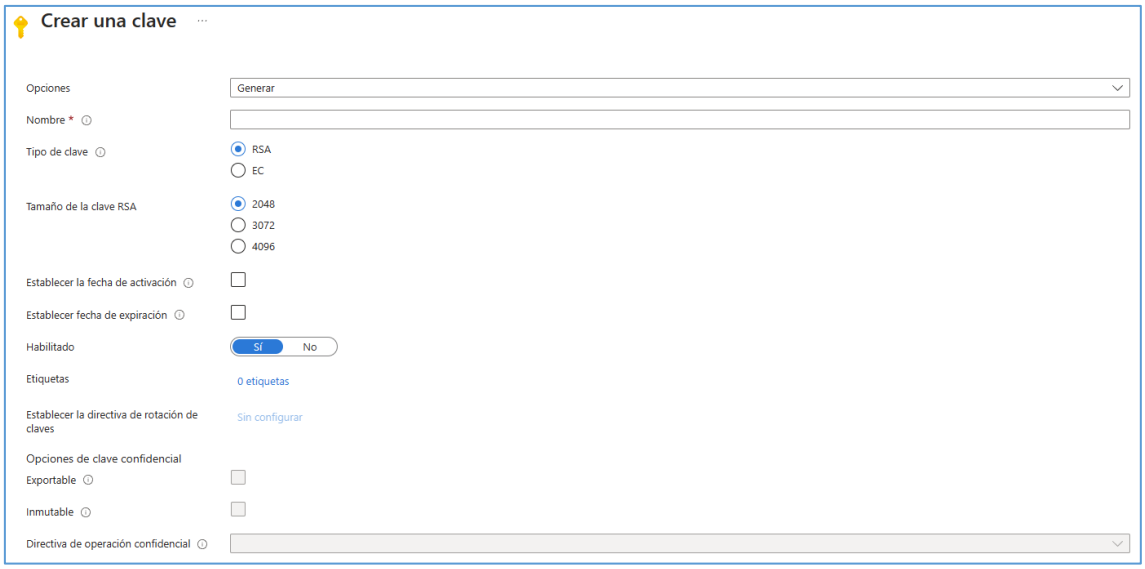
a) Pulsar en [Claves].



b) Pulsar en [Generar o importar].



- **Opciones:** Se puede generar, importar o restaurar copia de seguridad.
- **Nombre:** Definir un nombre para la nueva clave.



- **Tipo de clave:** Key Vault admite solo tipos de claves
    - **RSA**: Tamaños disponibles 2048, 3072 y 4096.
    - **EC** (Curva elíptica): Nombres disponibles P-256, P-384, P-521 y P-256K

Para la selección de los tipos de clave y su tamaño, se debe cumplir con los requisitos especificados en la guía *CCN-STIC-807 Criptología de Empleo en el Esquema Nacional de Seguridad.* Por este motivo, para sistemas de información categorizados como ENS Alto no se permite la utilización de tamaños de clave RSA-2048, ya que presentan una fortaleza criptológica de 112 bits, menor que los 128 exigidos.

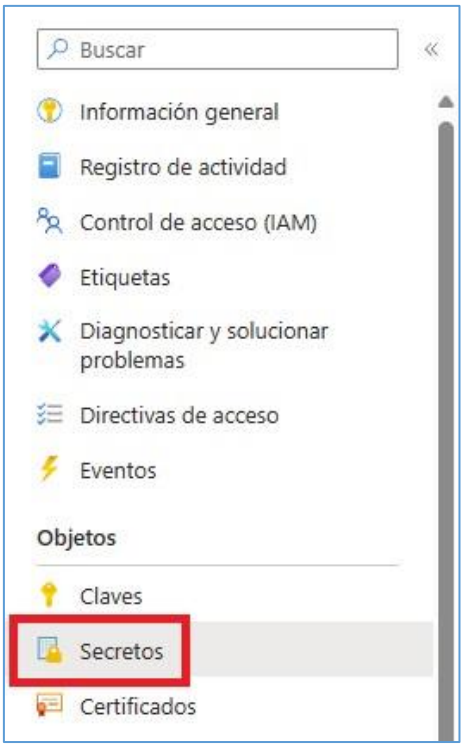
De forma opcional, se puede establecer una fecha de activación y expiración.

Nota: Se puede consultar más los tipos de claves: *https://docs.microsoft.com/es-es/azure/key-vault/about-keys-secrets-and-certificates*

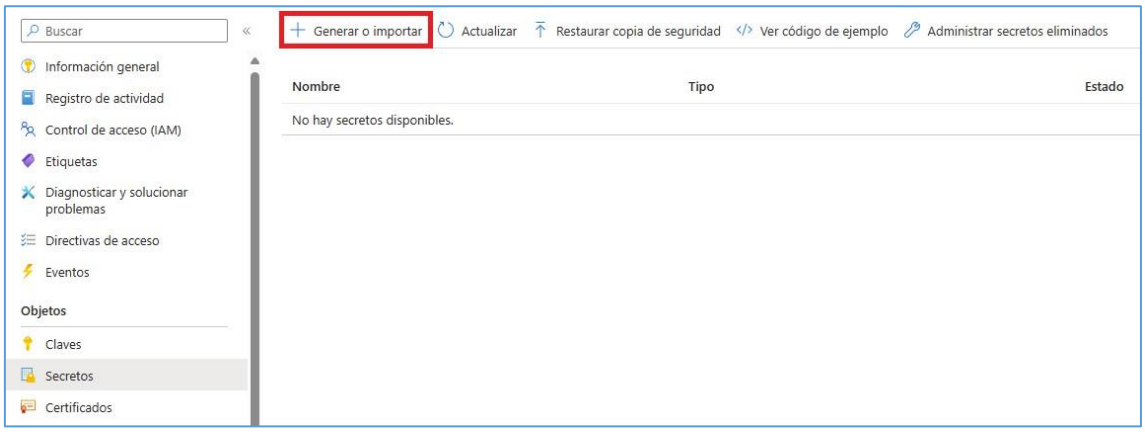
c) Por último, pulsar en [crear].

CREACIÓN DE SECRETOS

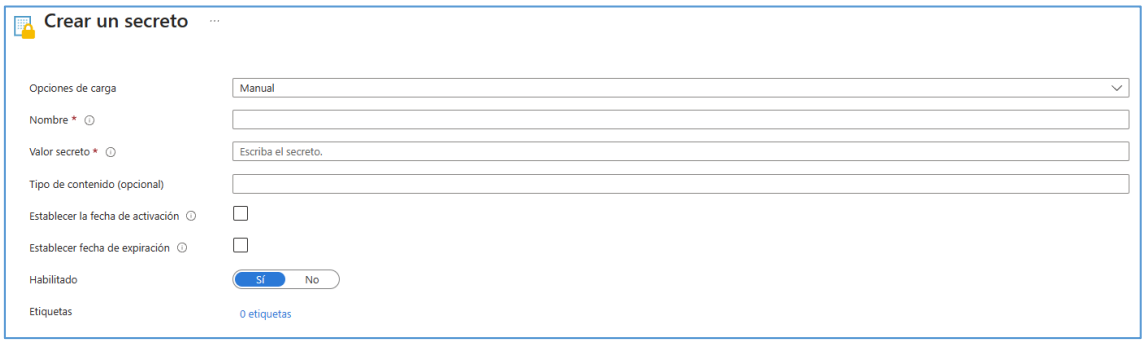
a) Pulsar en [Secretos].



b) Pulsar en [Generar o importar].



c) A continuación, completar los siguientes campos.



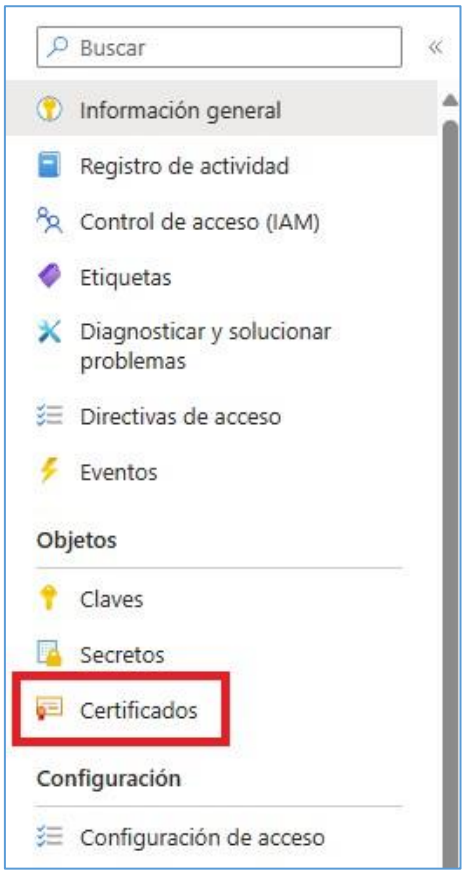
- **Nombre:** Escribir un nombre para este secreto.
- **Valor secreto:** Establezca un valor. Ejemplo: **Pa$$hVFkk965BuUv**.
- **Tipo de contenido:** Defina un nombre de uso para este secreto.

De manera opcional se puede establecer una fecha de activación.

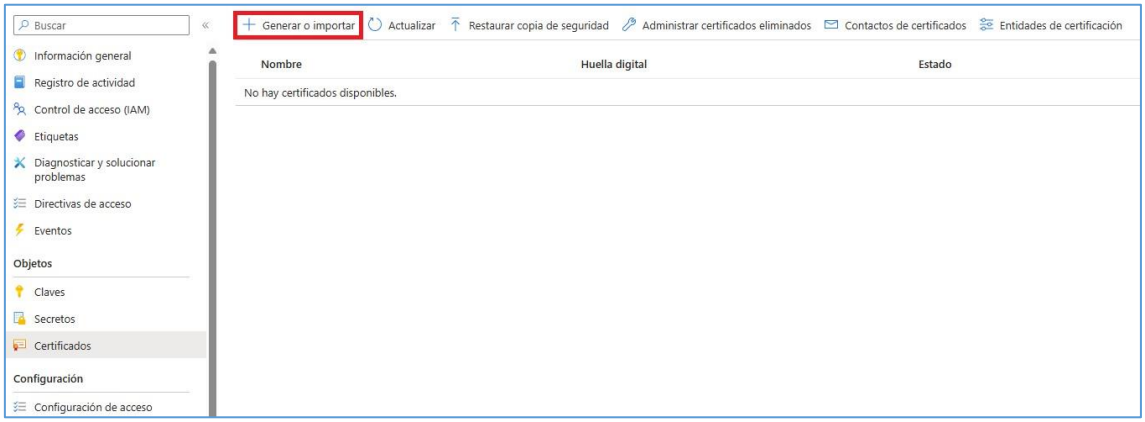
d) Pulsar en [Crear].

CREACIÓN DE CERTIFICADOS

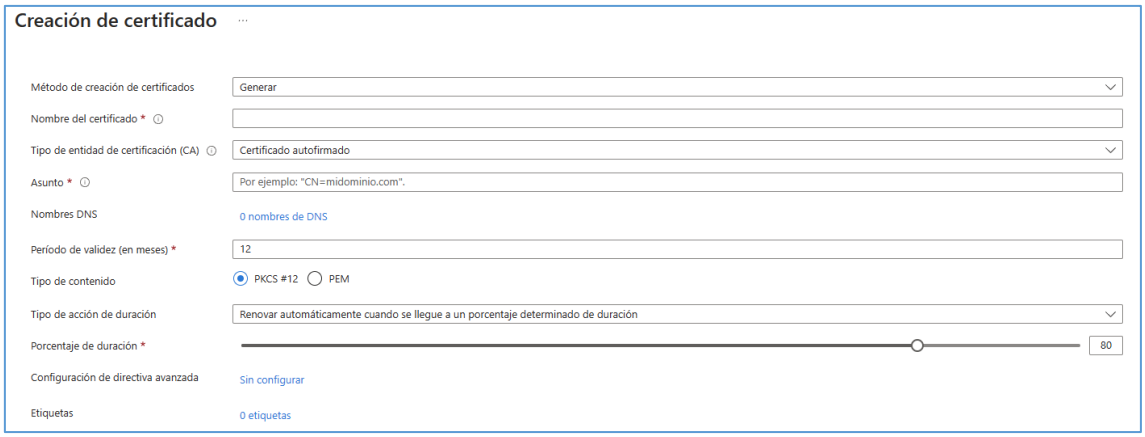
a) Pulsar en [Certificados].



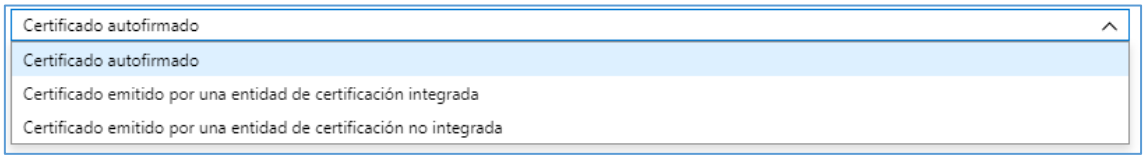
b) Pulsar en [Generar o importar].



c) A continuación, completar estos campos.

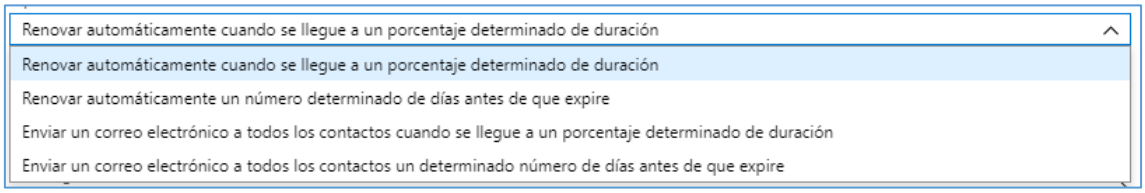


- **Método de creación de certificados:** Se puede ser generar o importar.
- **Nombre del certificado:** Definir el nombre del certificado.
- **Tipo de entidad de certificación (CA):** En este caso seleccione Auto firmado. [En el menú cuenta con dos opciones más]

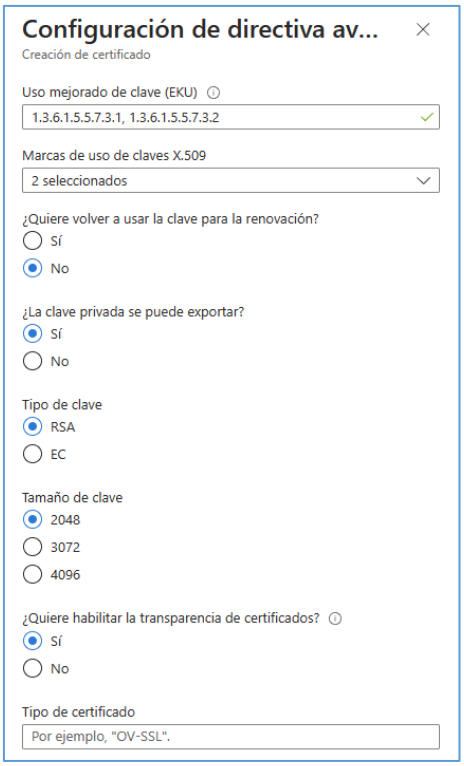


- **Asunto:** Nombre distintivo de X.500. Ejemplo CN=midominio.com
- **Nombre de DNS:** Los nombres alternativos del firmante (SAN) se pueden especificar como nombres DNS.
- **Periodo de validez en meses:** Por defecto 12 meses.
- **Tipo de contenido:** En la combinación de certificados se admiten dos formatos basados en PEM. O bien se puede combinar un único certificado codificado en PKCS #8 o un archivo P7B codificado en base64. -----BEGIN CERTIFICATE----- -----END CERTIFICATE-----
- **Tipo de acción de duración:** Seleccionar renovar automáticamente.

  [Dispone de más opciones]



- **Porcentaje de duración:** Varía el porcentaje dependiendo de la opción de renovación. En este caso se define en 80.
- **Configuración de directivas avanzadas:** De manera opcional se puede definir una directiva para este certificado.



d) Pulsar en [Crear].

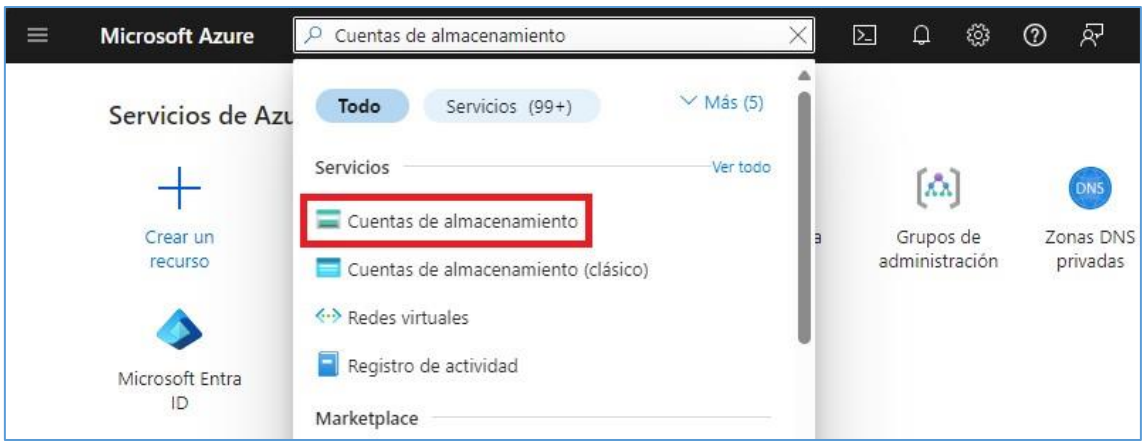
CIFRADO EN CUENTAS DE ALMACENAMIENTO

El cifrado del servicio **Cuenta de almacenamiento** protege los datos en reposo. El servicio Azure Storage cifra los datos tal como están escritos en los centros de datos y los descifra automáticamente cuando accede a ellos.

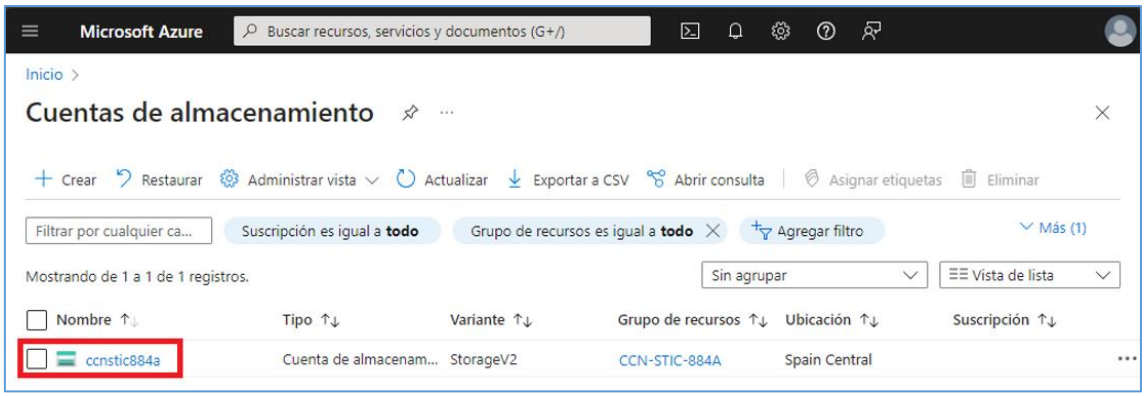
Su cuenta de almacenamiento está cifrada de forma predeterminada con una clave administrada de Microsoft. Deberá utilizarse Key Vault para generar las claves del cifrado gestiona por el usuario.

Para ello realizar estos pasos.

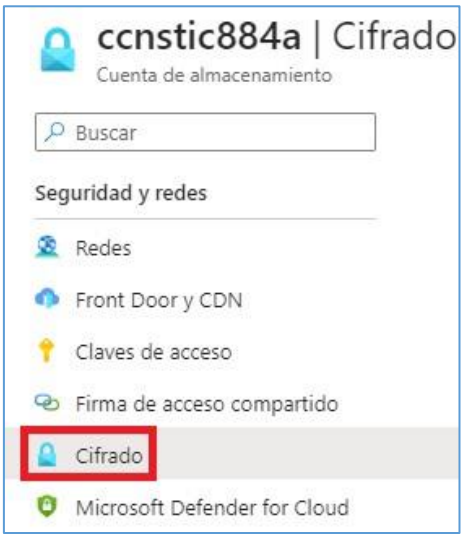
a) En el buscador escribir [Cuentas de almacenamiento].



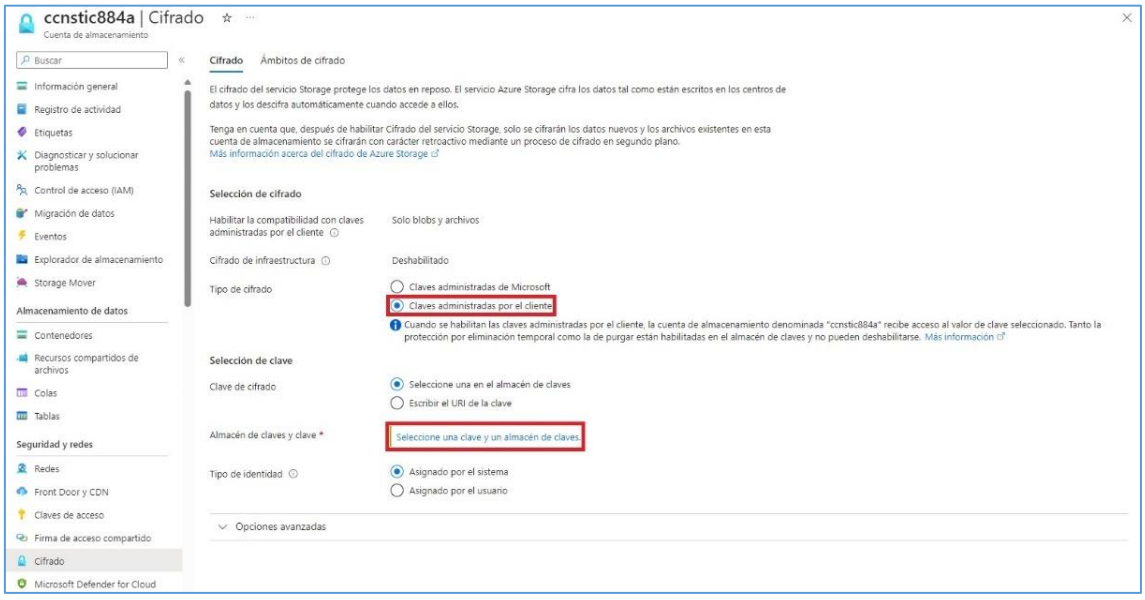
b) Elegir la cuenta de almacenamiento de alguna aplicación o máquina virtual que tenga desplegada.



c) Pulsar sobre [Cifrado].



d) Pulsar sobre [Claves administradas por el cliente] y luego pulsar en [Seleccione una clave y un almacén de claves].



Nota: El usuario que asigna la configuración debe tener permisos de administración sobre el Key Vault.

e) Se crea un nuevo almacén que se usa de forma centralizada para todas las cuentas de almacenamiento.

- **Suscripción:** Suscripción donde encontrar el Key Vault.
- **Tipo de almacenamiento:** Podemos escoger entre el modelo estándar o un HSM administrado por Microsoft.
- **Almacén de claves:** Key Vault donde encontrar la clave de encriptación.
- **Clave:** Clave gestionada por el usuario que se usara para encriptar el recurso.

Nota: *La identidad administrada de la cuenta de almacenamiento deberá tener el permiso de* ***Usuario criptográfico de Key Vault*** *o uno superior para poder continuar con el proceso.*

f) Por último, pulsar sobre [Seleccionar / Guardar].

LIMITACIONES

La tabla que presentamos a continuación representa el número de transacciones clave, el número máximo de transacciones permitidas en 10 segundos por almacén y región.

Los límites de servicio en Key Vault sirven para evitar el uso incorrecto de los recursos y garantizar la calidad de servicio para todos los clientes de Key Vault. Cuando se supera un umbral de servicio, Key Vault limita las solicitudes sucesivas de ese cliente durante un período de tiempo. Cuando esto sucede, Key Vault devuelve el código de estado HTTP 429 (demasiadas solicitudes) y un error en las solicitudes. Además, las solicitudes con error que devuelven un código 429 cuentan para la limitación cuyo seguimiento realiza Key Vault.

En el código de error HTTP 429, comience la limitación del cliente mediante un enfoque de retroceso exponencial:

a) Espere 1 segundo, reintente la solicitud.

b) Si todavía está limitado, espere 2 segundos, reintente la solicitud.

c) Si todavía está limitado, espere 4 segundos, reintente la solicitud.

d) Si todavía está limitado, espere 8 segundos, reintente la solicitud.

e) Si todavía está limitado, espere 16 segundos, reintente la solicitud.

Tipo de Clave	Clave HSM	Clave HSM	Clave de Software	Clave de Software
	Clave Create	Las restantes transacciones	Clave Create	Las restantes transacciones
2048 bits de RSA	10	2000	20	4000
3072 bits de RSA	10	500	20	1000
4096 bits de RSA	10	250	20	250
ECC P-256	10	2000	20	4000
ECC P-384	10	2000	20	4000
ECC P-521	10	2000	20	4000
ECC SECP256K1	10	2000	20	4000
2048 bits de RSA	10	2000	20	4000
3072 bits de RSA	10	500	20	1000
4096 bits de RSA	10	250	20	250
ECC P-256	10	2000	20	4000
ECC P-384	10	2000	20	4000
ECC P-521	10	2000	20	4000
ECC SECP256K1	10	2000	20	4000
2048 bits de RSA	10	2000	20	4000

3.1.3 CONTINUIDAD DEL SERVICIO

3.1.3.1 PLAN DE CONTINUIDAD

Azure Site Recovery (ASR) garantiza la continuidad del servicio manteniendo las aplicaciones en funcionamiento durante las interrupciones.

Se replican cargas de trabajo que se ejecutan en máquinas físicas y virtuales desde un sitio principal a una ubicación secundaria. Cuando se produce una interrupción en el sitio principal, se conmuta por error a la ubicación secundaria. Una vez la ubicación principal vuelve a estar en ejecución, se puede realizar la conmutación por recuperación.

Con Site Recovery se puede administrar la replicación de:

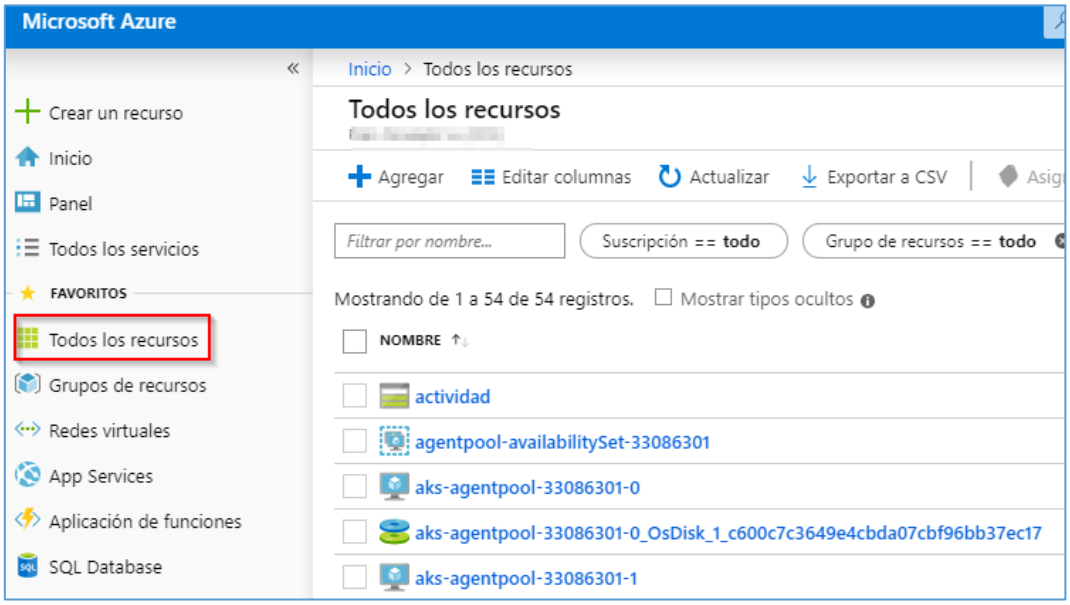
- Máquinas virtuales de Azure que se replican entre distintas regiones.
- Máquinas virtuales locales, máquinas virtuales de Azure Stack y servidores físicos.

En los siguientes pasos se explica como configurar ASR para algunos recursos.

REPLICACIÓN DE MÁQUINAS VIRTUALES

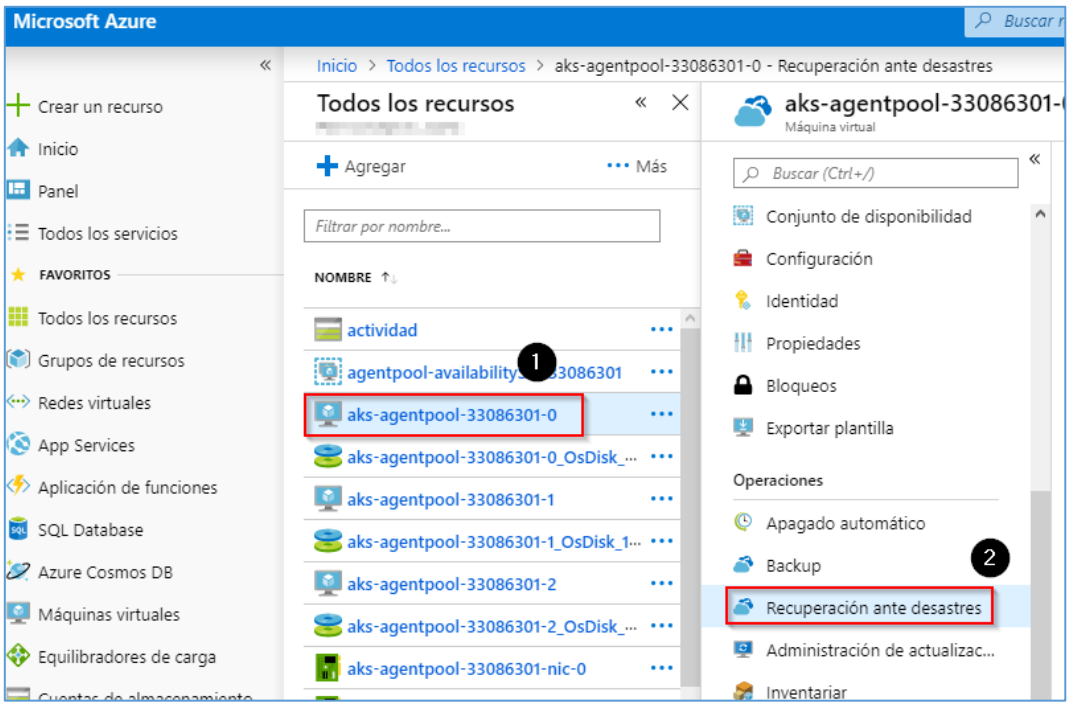
Antes de crear un plan de recuperación ante desastres, se debe hacer una replicación de la máquina virtual. Para ello, realizar los siguientes pasos:

a) Desde el panel de Azure pulsar en [todos los recursos].



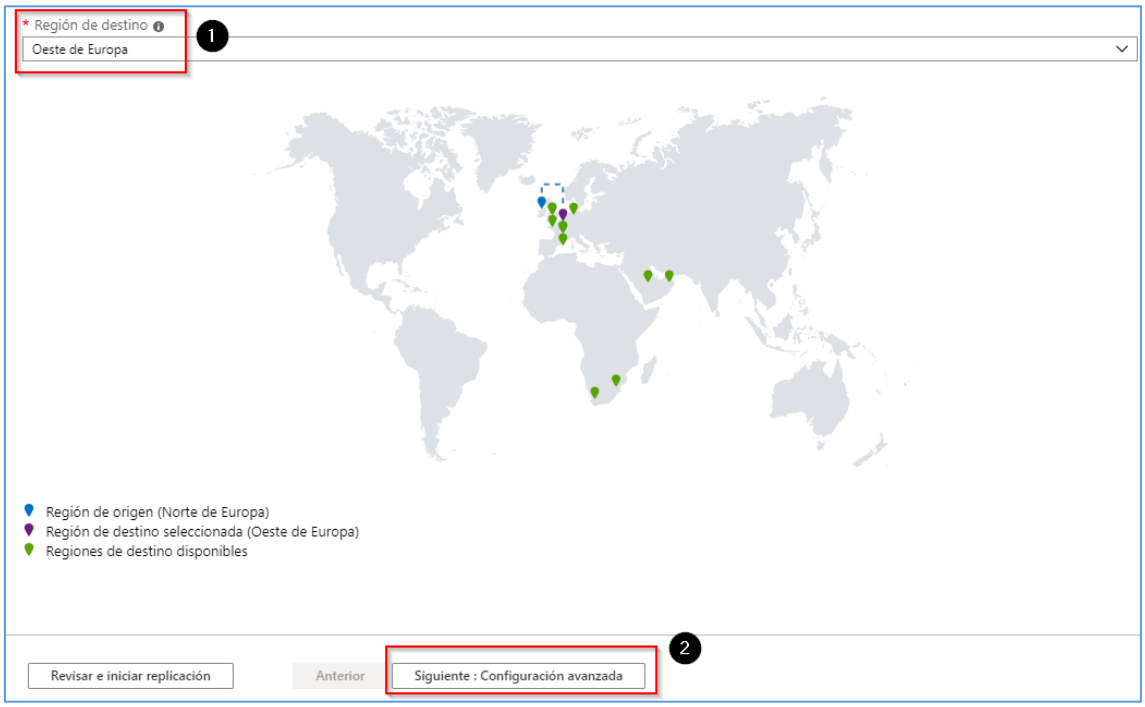
b) Pulsar en una máquina virtual.

c) Pulsar en [recuperación ante desastres].

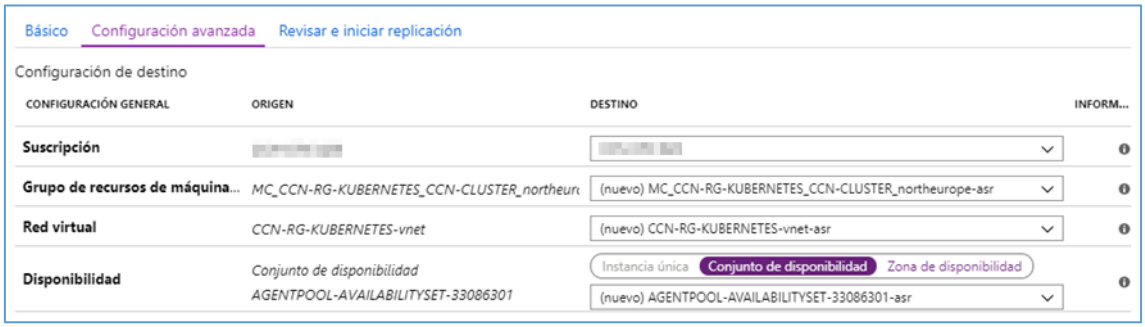


Nota: Las máquinas virtuales se pueden replicar en otra región de Azure para cubrir sus necesidades de continuidad y recuperación ante desastres. Se recomienda realizar exploraciones periódicas de recuperación ante desastres para asegurarse de que satisface las necesidades de cumplimiento. La VM se replica con la configuración especificada en la región seleccionada, de forma que se puede recuperar sus aplicaciones en caso de interrupciones en la región de origen.

d) Seleccionar la región donde quiere realizar la replicación.
e) Pulsar en [configuración avanzada]. Y rellenar los siguientes campos:



- **Grupo de recursos de máquina virtual:** Este nuevo grupo se utiliza para realizar la conmutación por error.
- **Red virtual:** Se crea una nueva red virtual para la conmutación por error.
- **Disponibilidad:** Seleccionar el tipo de disponibilidad en la región de destino. Solo se puede seleccionar "Zona de disponibilidad" si la región de destino admite las zonas de disponibilidad. Si el tipo de disponibilidad de destino es "Conjunto de disponibilidad" y si protege una VM con discos administrados, solo se puede ver y seleccionar un conjunto de disponibilidad administrado para VM con discos administrados y un conjunto de disponibilidad no administrado para VM sin discos administrados.



- **Grupo con ubicación por proximidad:** Se puede seleccionar opcionalmente un grupo con ubicación por proximidad en la región de destino. En caso de conmutación por error, se intentaría activar la VM de destino en el grupo con ubicación por proximidad seleccionado.

CONFIGURACIÓN DE RESERVA DE CAPACIDAD

- **Grupos de reserva de capacidad:** Opcionalmente se puede seleccionar un grupo de reserva de capacidad. La reserva de capacidad a petición permite reservar la capacidad de proceso en una región de Azure o una zona de disponibilidad durante cualquier período de tiempo.

CONFIGURACIÓN DE ALMACENAMIENTO

- **Renovación de la VM:** Azure Site Recovery admite la renovación (tasa de cambio de datos) de hasta 100 MB/s por máquina virtual. Las máquinas virtuales de Azure que tengan cargas de trabajo de renovación elevadas (como bases de datos) se pueden proteger mediante la opción de alta renovación de Azure Site Recovery, que es compatible con renovación de hasta 100 MB/s por máquina virtual.
- **Cuenta de almacenamiento en caché:** La cuenta de almacenamiento en caché se encuentra en la región de origen. Se utiliza como un almacén de datos temporal antes de replicar los cambios a la región de destino. De forma predeterminada, se crea una cuenta de almacenamiento en caché por depósito y se vuelve a utilizar. Se puede seleccionar una cuenta de almacenamiento en caché diferente si se desea personalizar la cuenta de almacenamiento en caché que se utiliza para esta máquina virtual.
- **Disco administrado de origen:** Los datos que se replican desde la VM de origen se almacenan en los discos administrados de réplica en la región de destino. Para cada disco administrado en la VM de origen, se crea un disco administrado de réplica y se utiliza en la región de destino.

CONFIGURACIÓN DE REPLICACIÓN

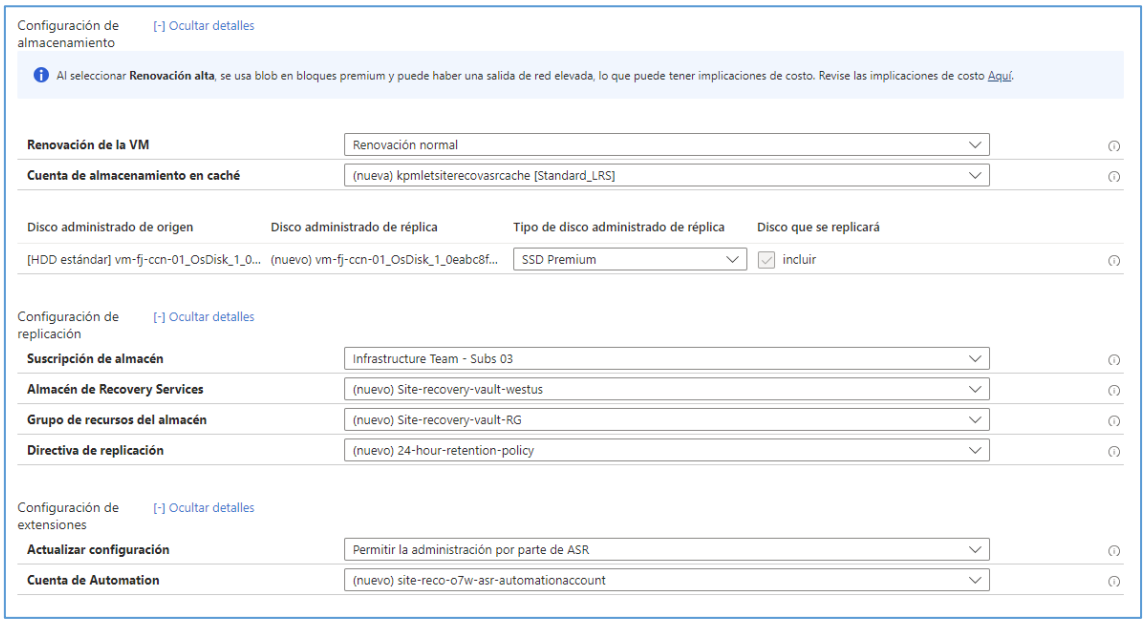
- **Suscripción de almacén:** Seleccionar la suscripción de Azure en la que existe el almacén de Recovery Services. Solo se almacenan en este almacén los metadatos correspondientes a las VM. Los datos reales de los discos nunca dejan las regiones de origen y de destino.
- **Almacén de Recovery Services:** El almacén de Recovery Services contiene la configuración de la máquina virtual de destino y organiza la replicación. En el caso de que se produzca una interrupción y la máquina virtual de origen no esté disponible, se puede hacer una conmutación por error desde el almacén de Recovery Services.
- **Grupo de recursos del almacén:** Grupo de recursos del almacén de Recovery Services.

- **Directiva de replicación:** La directiva de replicación define la configuración del historial de retención de puntos de recuperación y la frecuencia de instantáneas coherentes con la aplicación.

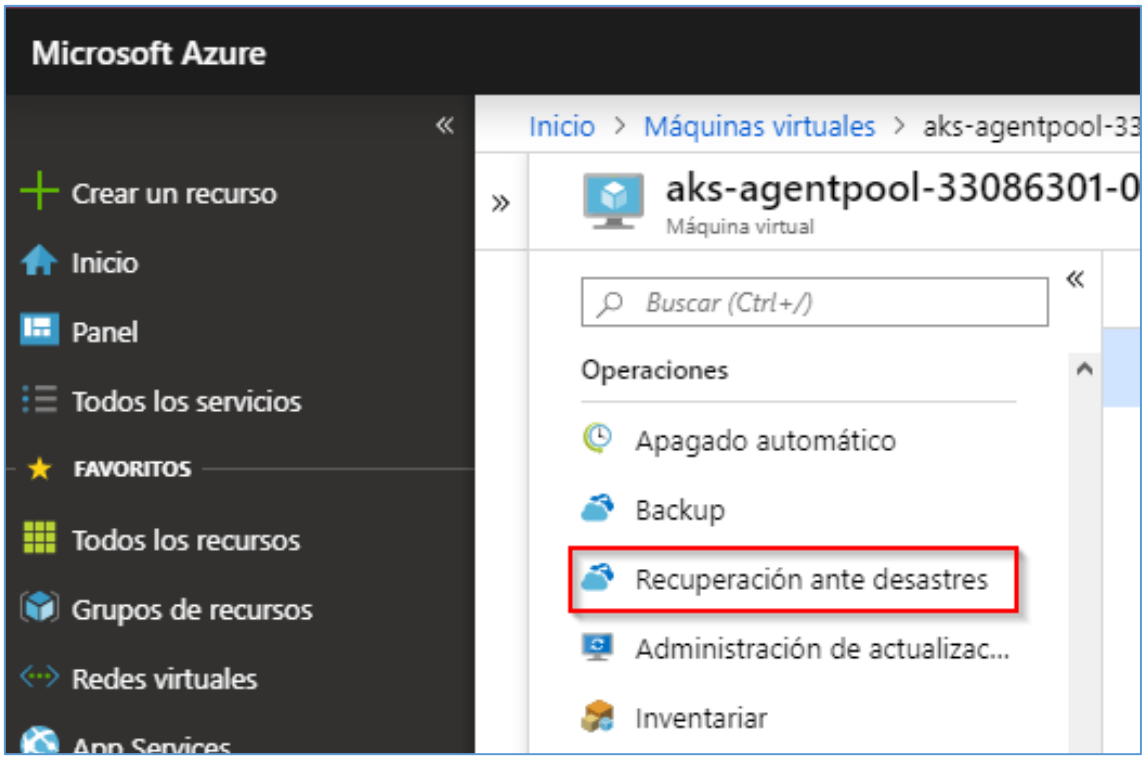
CONFIGURACIÓN DE EXTENSIONES

Las extensiones de máquina virtual (VM) de Azure son pequeñas aplicaciones que proporcionan tareas de configuración y automatización tras la implementación en máquinas virtuales de Azure.

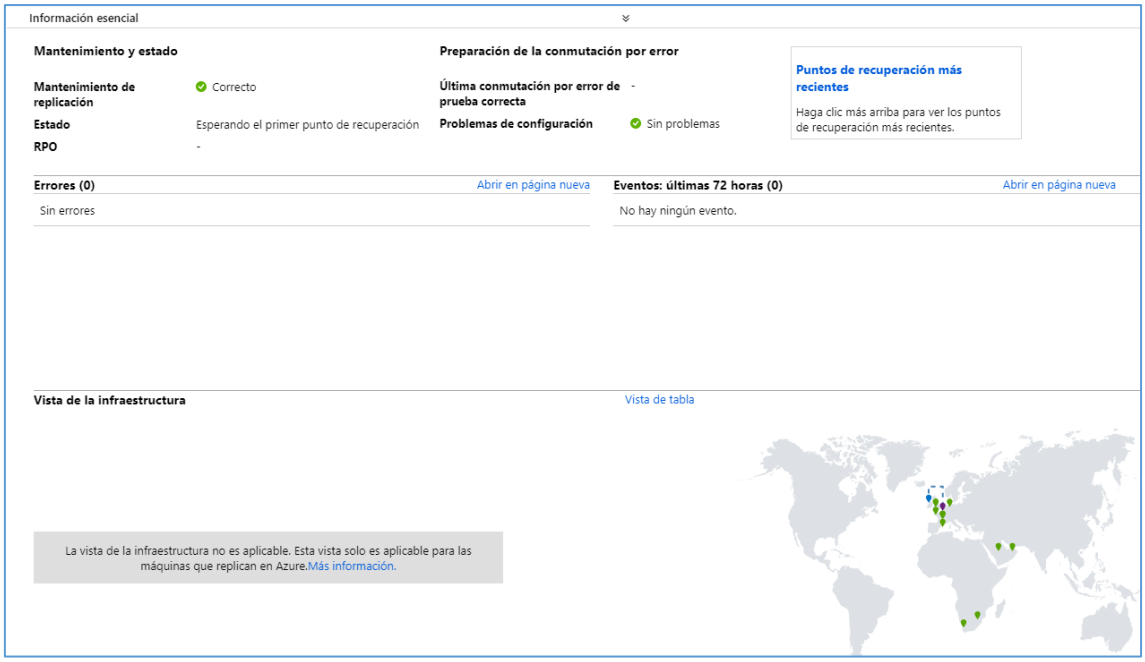
- **Actualizar configuración:** Site Recovery administra las extensiones de todos los elementos replicados asociados con el almacén y los mantiene actualizados. También se puede elegir actualizar las extensiones manualmente. Esto no requiere ningún reinicio ni afecta a la replicación en curso de las máquinas virtuales.
- **Cuenta de Automation:** Site Recovery usa esta cuenta de automatización para actualizar la extensión de Site Recovery en todas las máquinas replicadas asociadas con el almacén.



f) Pulsar en [revisar e iniciar replicación].
g) Se puede comprobar la replicación desde la propia máquina virtual en la opción de [recuperación ante desastres].



Ahí se encuentra el panel con el estado de sincronización.

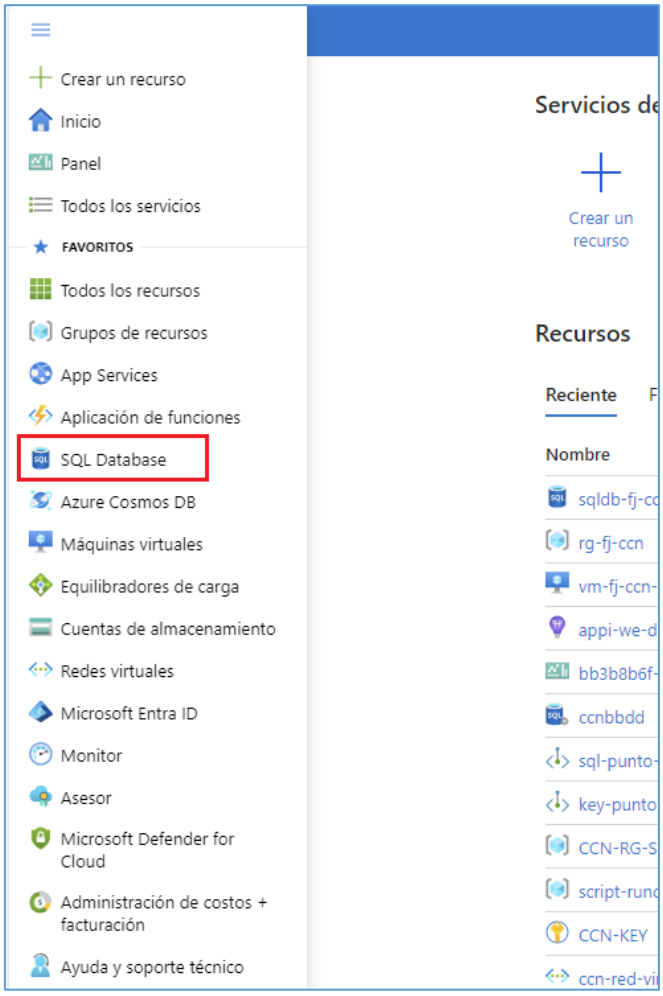


REPLICACIÓN EN BASE DE DATOS

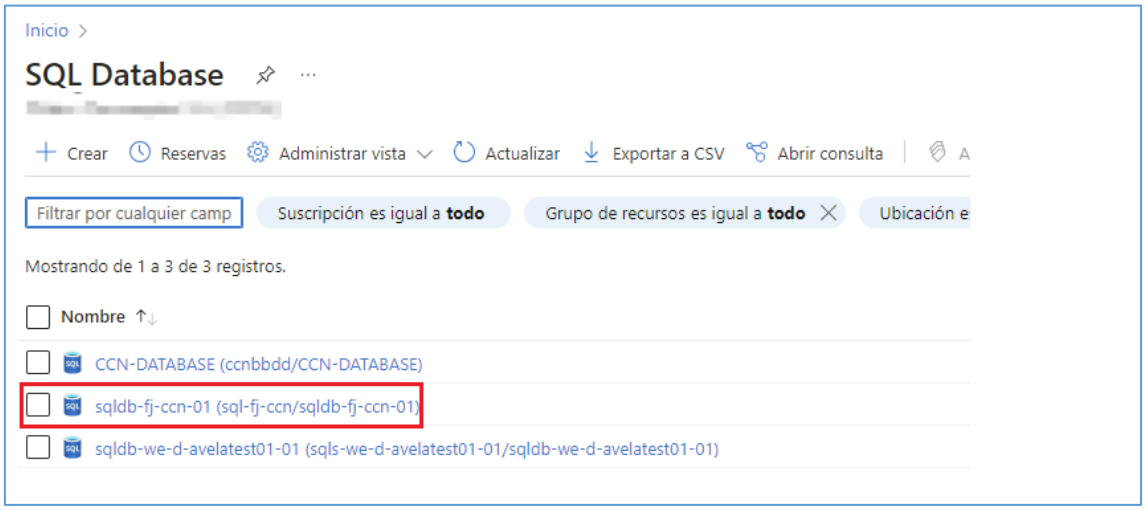
La replicación geográfica activa es la característica de Azure SQL Database que permite crear bases de datos secundarias en un servidor de SQL Database en el mismo centro de datos u otro diferente (región).

Los pasos siguientes crean otra base de datos secundaria replicada en otra región geográfica de Azure.

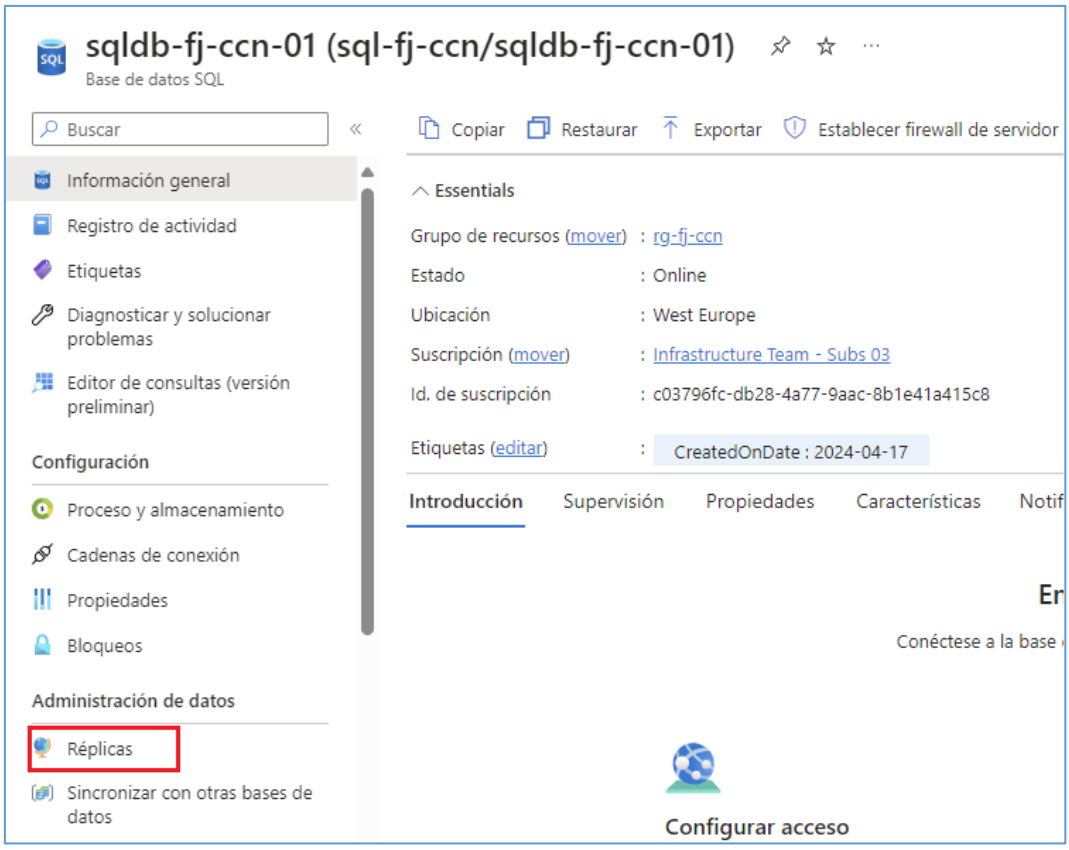
a) Pulsar desde el portal de Azure en [SQL Database].



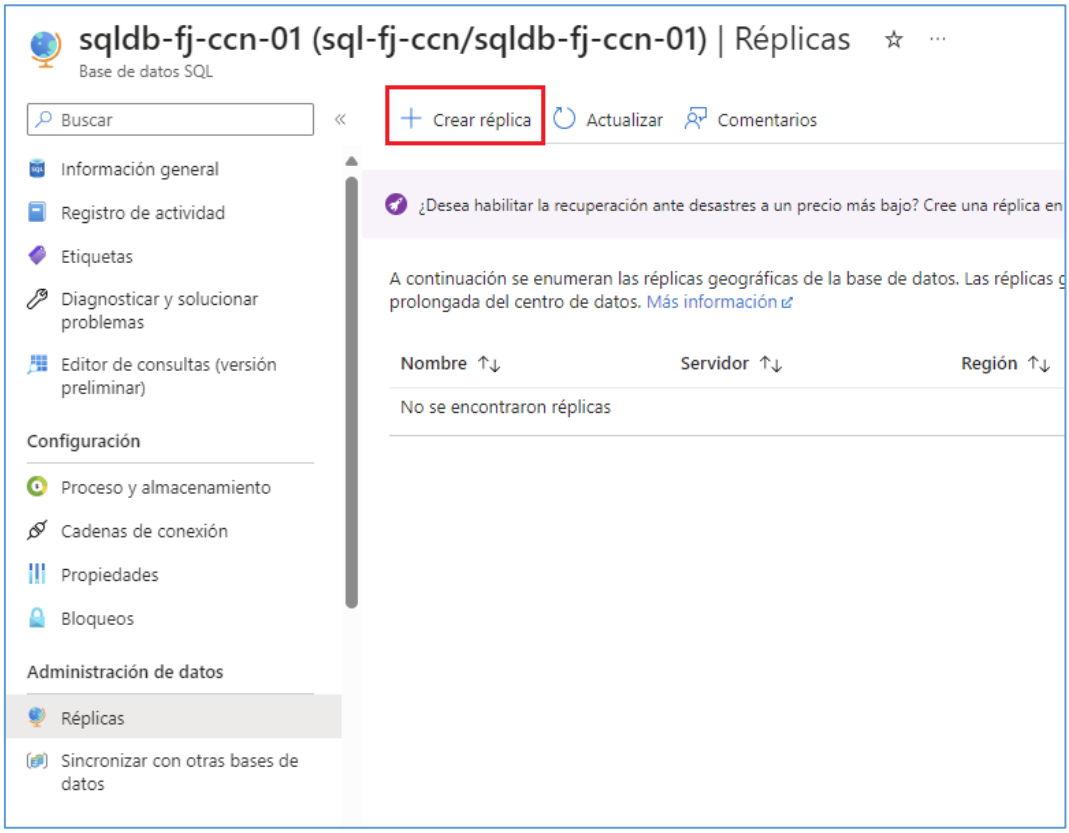
b) Seleccionar su base de datos.



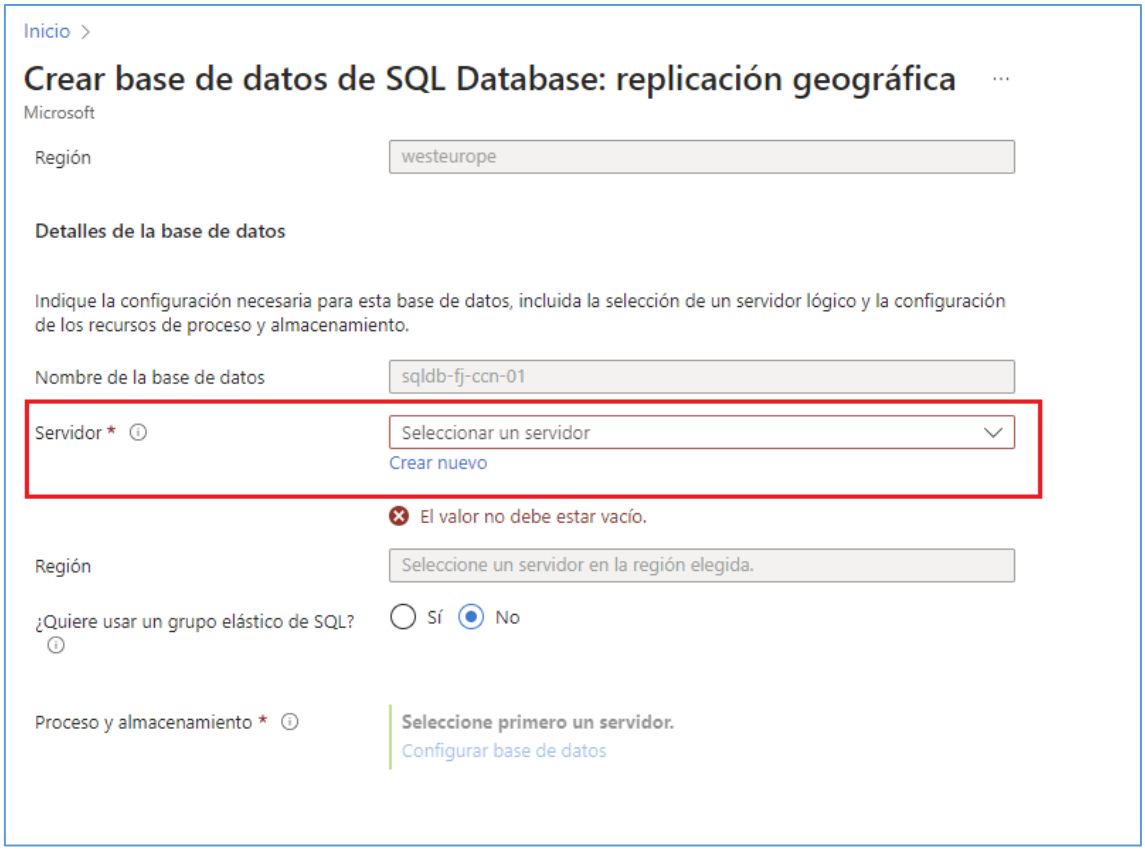
c) Pulsar en [Réplicas].

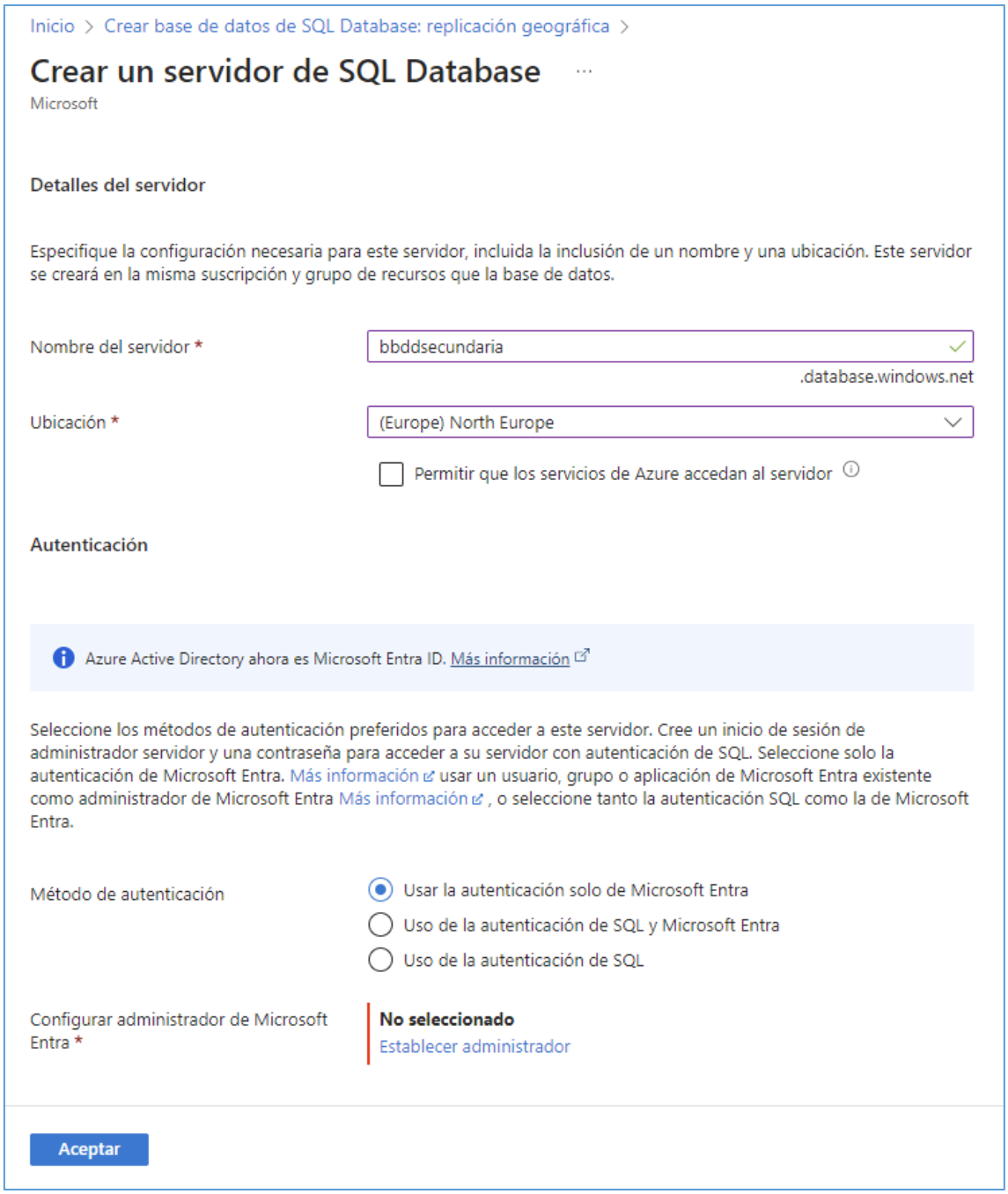


d) Pulsar en [Crear réplica].



e) Pulsar en [Servidor/Crear nuevo].





f) Definir un nombre para este servidor y Ubicación. Se recomienda utilizar la autenticación solo de Microsoft Entra en la medida de lo posible y quitar la opción de permitir que otros servidores Azure accedan al servidor. Pulsar en [aceptar].

g) Elegir si utilizar o no un grupo elástico de SQL. En caso contrario, elegir un nivel de servicio SQL y el nivel de rendimiento que se adapte mejor a las necesidades de la aplicación.

h) Configurar la clave de nivel de bases de datos si se está utilizando una clave de encriptación diferente a la proporcionada por Azure.

i) Seleccionar la redundancia de almacenamiento de copia de seguridad deseada y pulsar en [Revisar y crear].

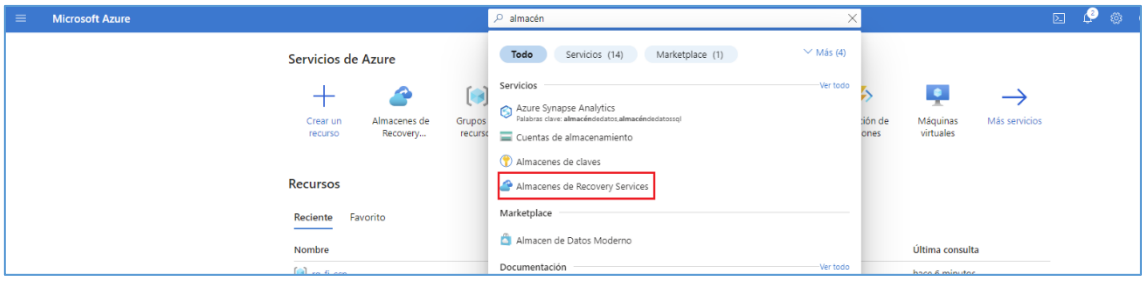
REPLICACIÓN DEL SERVICIO

Para ello, se utiliza el servicio **Site Recovery**: Site Recovery garantiza la continuidad de servicio manteniendo las aplicaciones y cargas de trabajo empresariales en funcionamiento durante las interrupciones. Replica las cargas de trabajo que se ejecutan en máquinas físicas y virtuales desde un sitio principal a una ubicación secundaria.

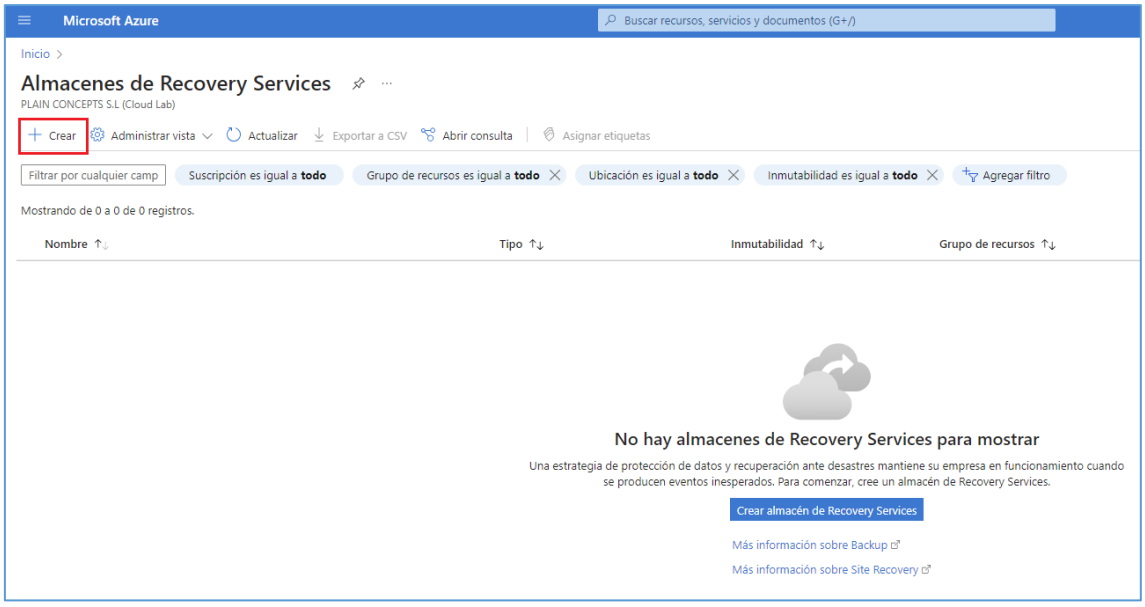
Cuando se produce una interrupción en el sitio principal, se conmuta por error a la ubicación secundaria y se accede desde allí a las aplicaciones. Cuando la ubicación principal vuelva a estar disponible, se puede realizar la conmutación por recuperación en ella.

Lo primero que se debe hacer es crear un almacén de Recovery Services.

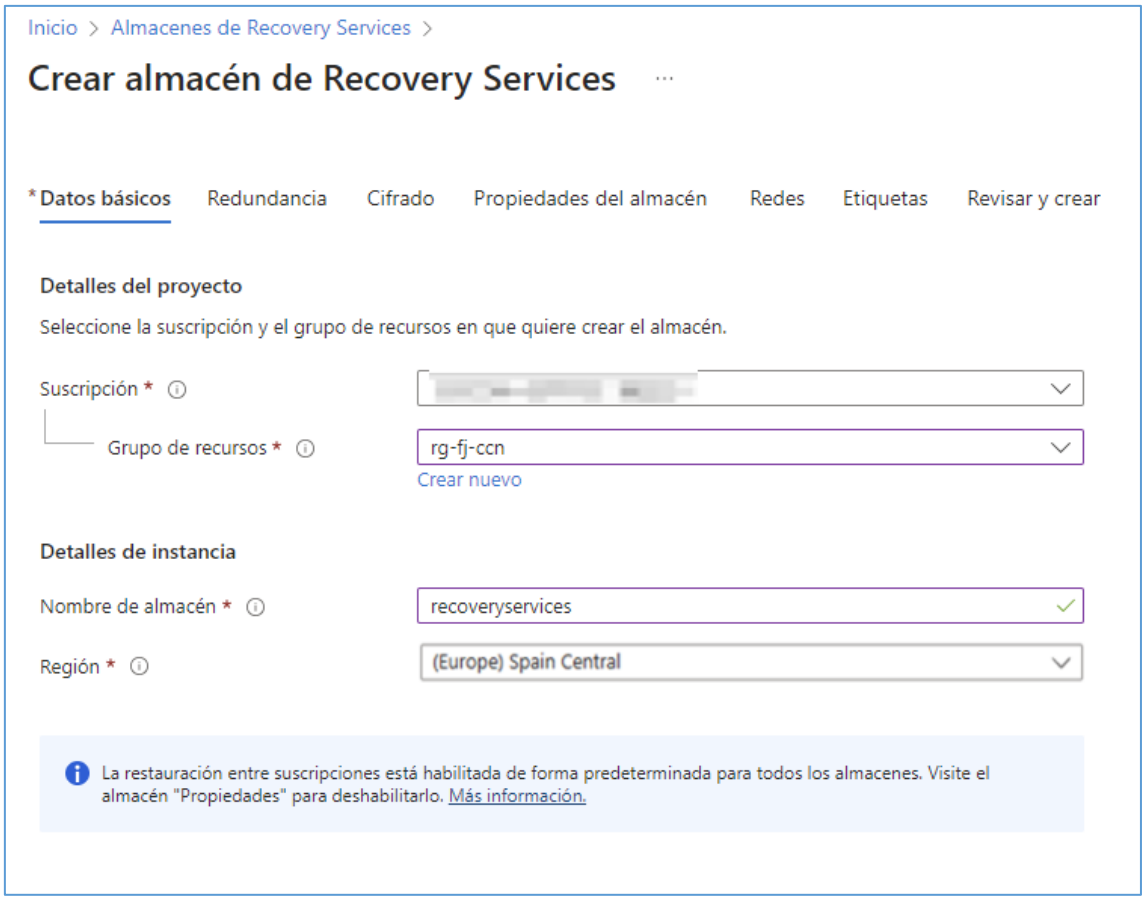
a) Desde el portal de Azure buscar almacenes de Recovery Services.



b) Pulsar en [Crear].

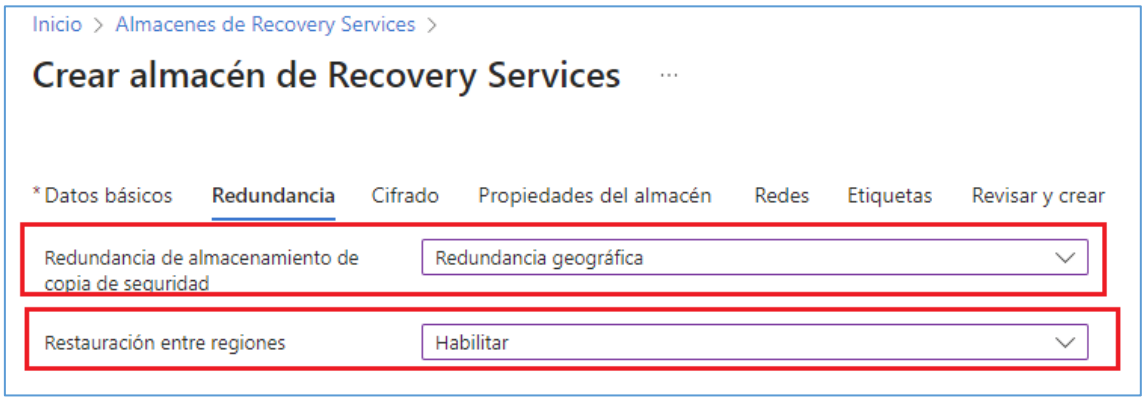


c) A continuación, se debe completar los campos de Datos básicos:



- Suscripción: Seleccionar su suscripción.
- Grupo de recursos: Crear un nuevo grupo de recursos.
- Detalles de la instancia
- Nombre del almacén: Crear un nombre para el nuevo almacén.
- Región: Seleccionar Spain Central.

d) A continuación, se debe completar los campos de **Redundancia** que solicita la creación del almacén bajo la pestaña con el mismo nombre:



- **Redundancia de almacenamiento de copia de seguridad:** Elegir el tipo de redundancia deseada, por ejemplo, Redundancia geográfica y habilitar la restauración entre regiones si procede.

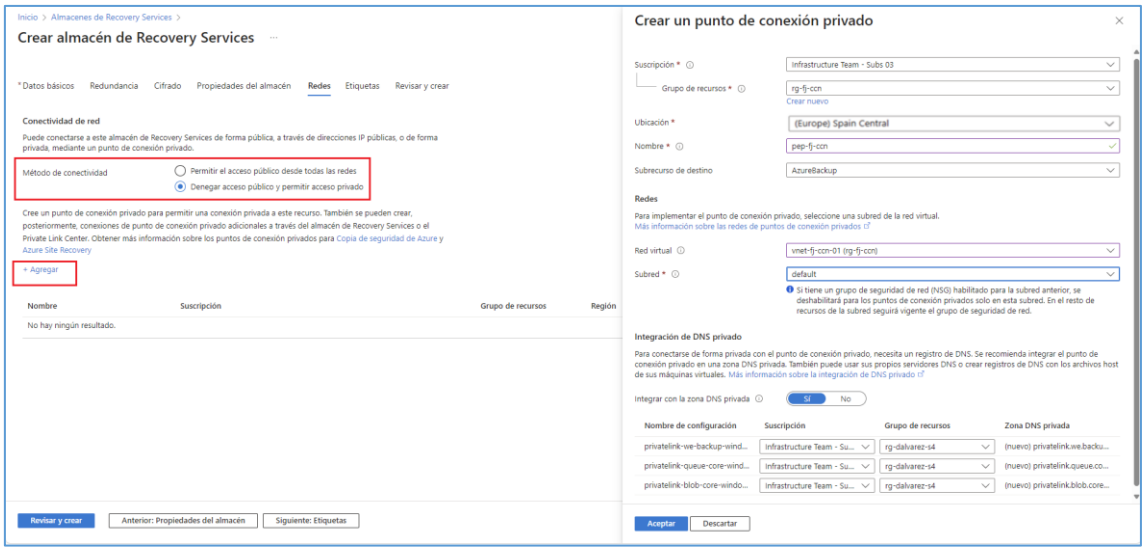
e) **A continuación, se debe completar los campos de Cifrado** que solicita la creación del almacén bajo la pestaña con el mismo nombre:

- **Tipo de cifrado:** Se puede utilizar una clave propia o gestionada por Microsoft. La clave administrada por el cliente es la opción más segura, pero a su vez la más costosa a nivel de mantenimiento.

f) A continuación, se deben completar los campos de **Propiedades del almacén** que solicita la creación.

- **Habilitar inmutabilidad:** Opcionalmente se puede habilitar la inmutalidad. El almacén inmutable impide que realice algunas operaciones en el almacén que podrían provocar la pérdida de datos.

g) A continuación, se debe completar los campos de **Redes** del almacén que solicita la creación.



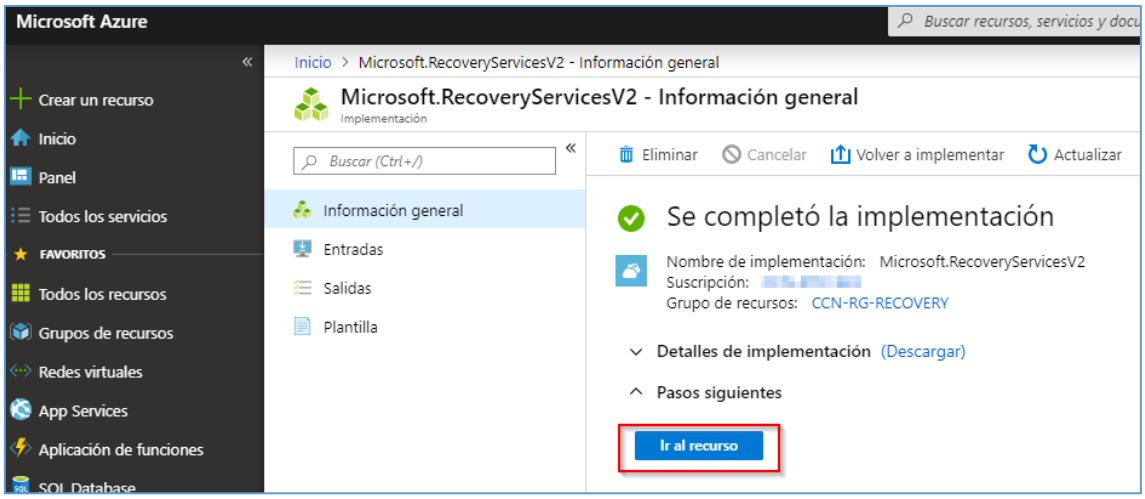
- Restringir la conectividad de red permitiendo solamente el acceso privado y configurar un punto de conexión privado para permitir la conexión privada al recurso.

h) Identificar este servicio bajo la pestaña **Etiquetas** haciendo uso de las y pulsar [Revisar y crear]

Etiquetas

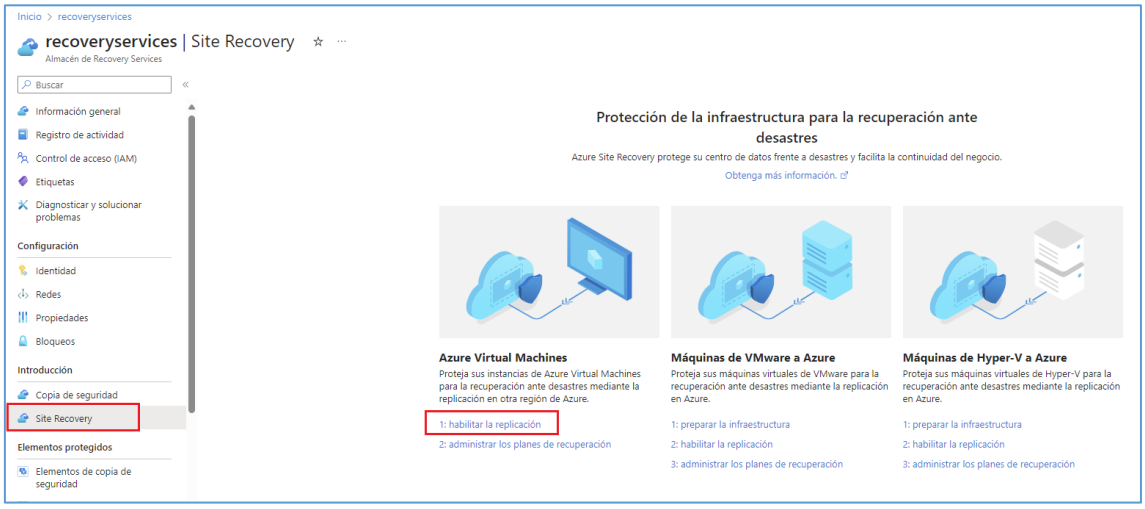
Nota: Una vez que tenemos creado el almacén, configurar el plan de continuidad para sus aplicaciones.

i) Pulsar en [ir al recurso].

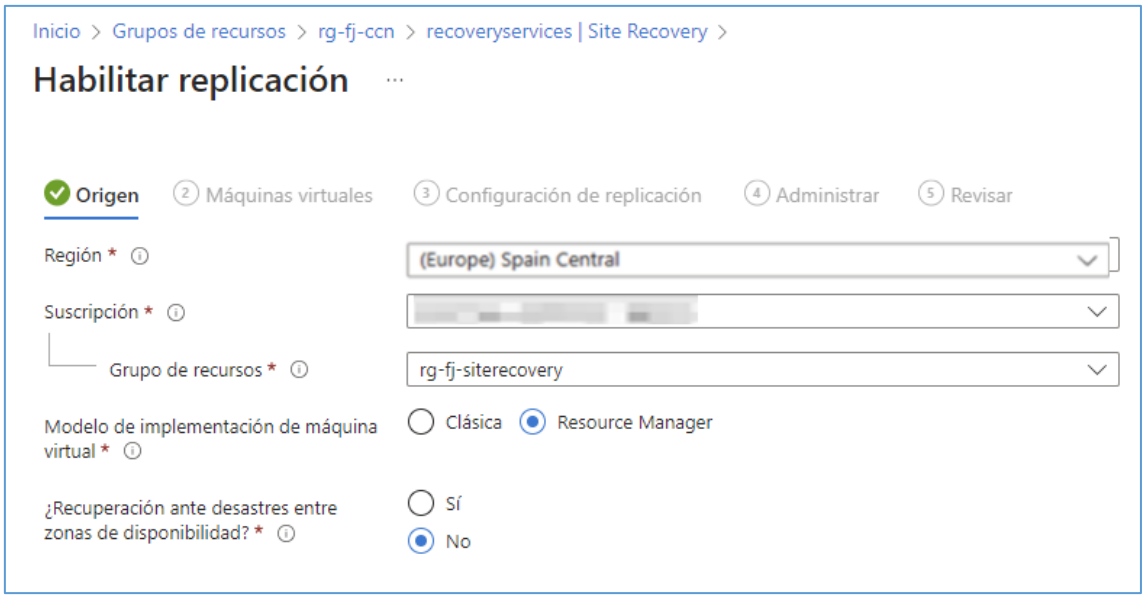


En este panel general se debe crear los planes de recuperación ante desastres.

j) Pulsar [Site recovery/habilitar la replicación].



k) Pulsar [replicar la aplicación].



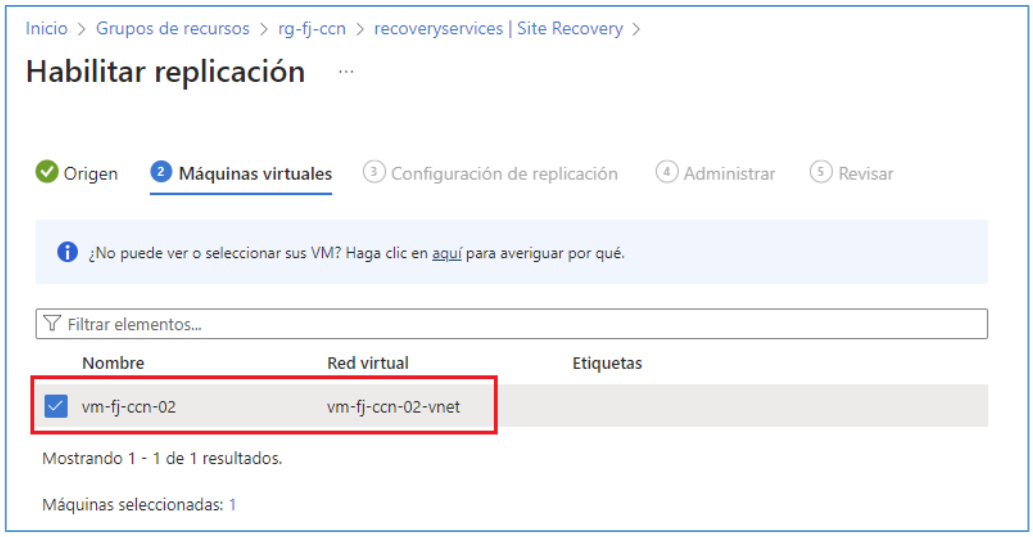
- **Región:** Seleccionar la ubicación en la que se ejecutan las máquinas virtuales de Azure.
- **Suscripción:** Seleccionar la suscripción de origen donde se encuentran las VM de origen.
- **Grupo de recursos:** Elegir el grupo de recursos donde se encuentra la máquina virtual.
- **Modelo de implementación de máquina virtual:** En este caso elegimos Resource Manager.

Nota: Se puede encontrar más información sobre modelos de implementación en el siguiente enlace: https://learn.microsoft.com/es-es/azure/azure-resource-manager/management/deployment-models

- **Recuperación ante desastres entre zonas de disponibilidad:** Solo las máquinas virtuales implementadas en una zona se pueden aplicar a la recuperación ante desastres de zona.

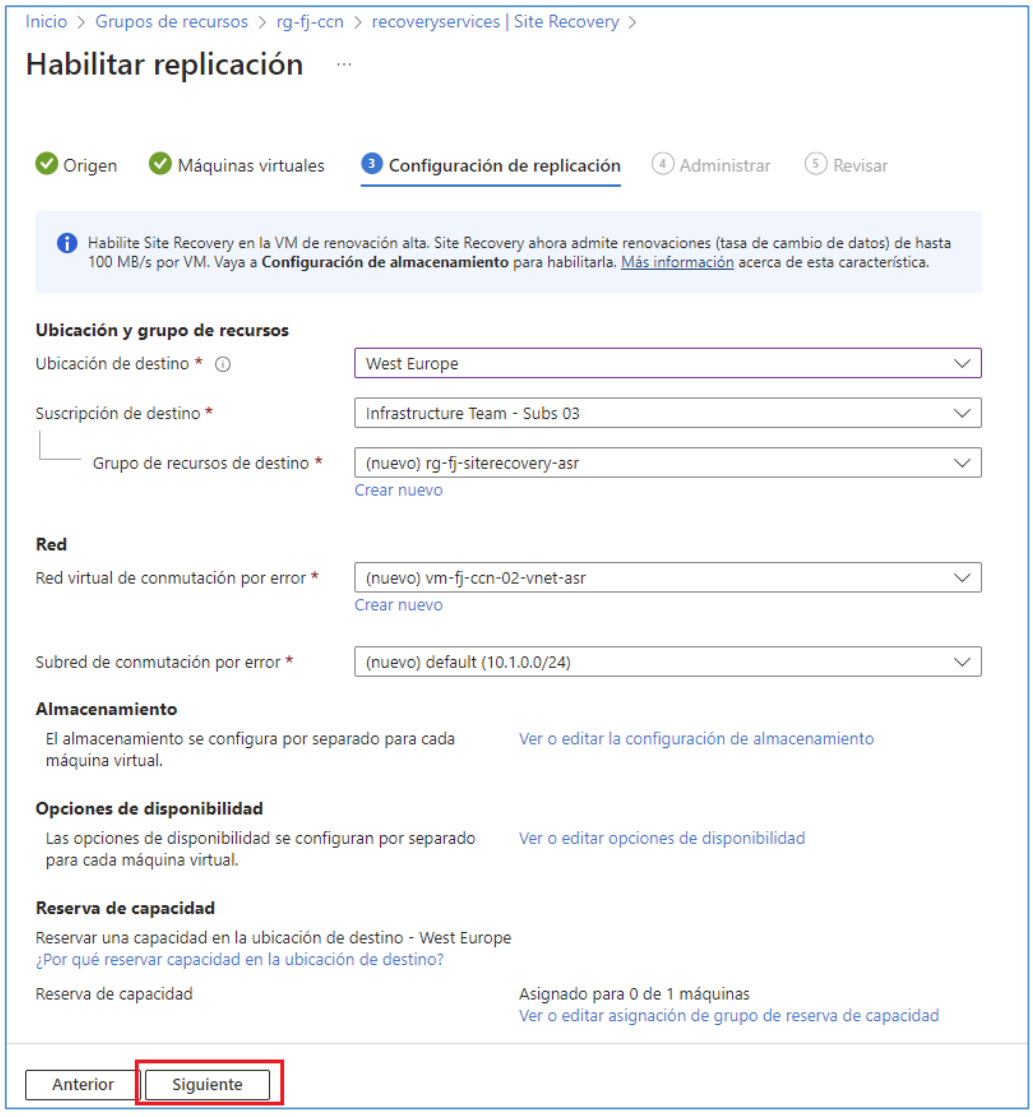
a) Pulsar en [Siguiente].

b) Seleccionar la máquina virtual y pulsar en [Siguiente].

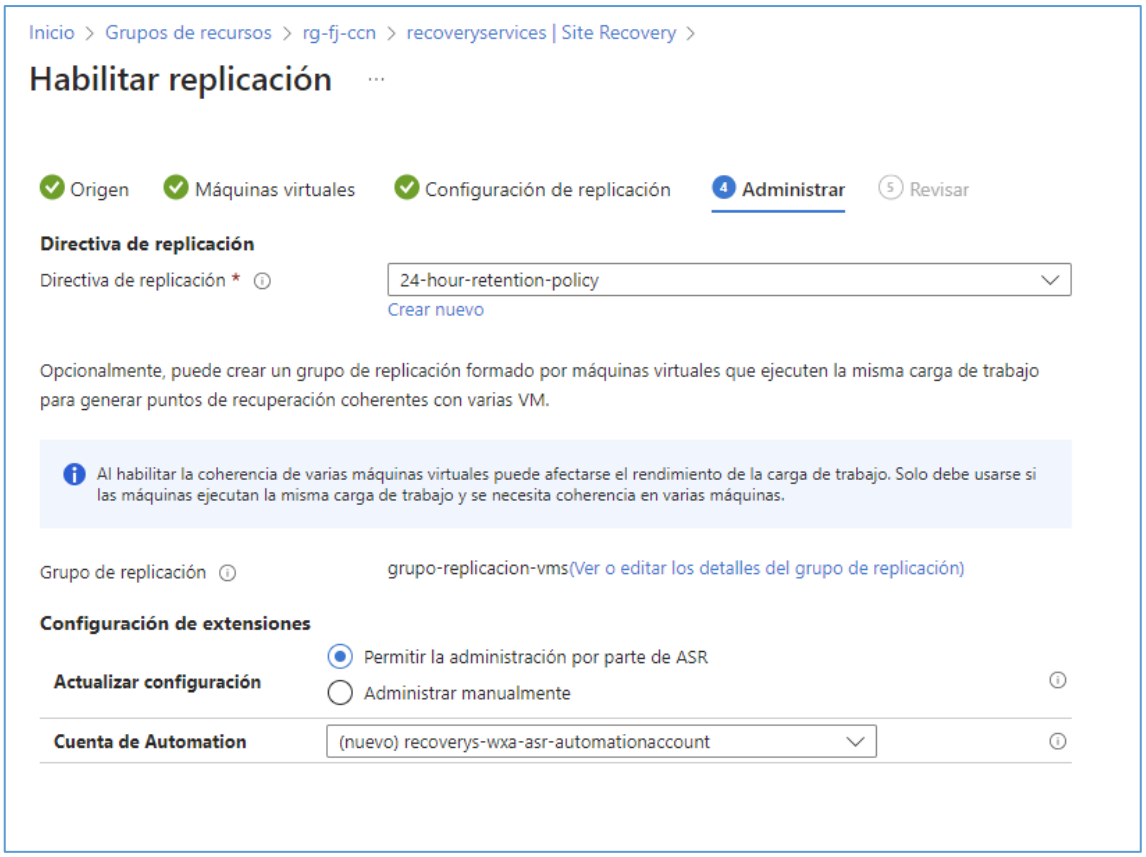


c) Se puede personalizar la configuración de replicación.

d) Pulsar en [Siguiente].



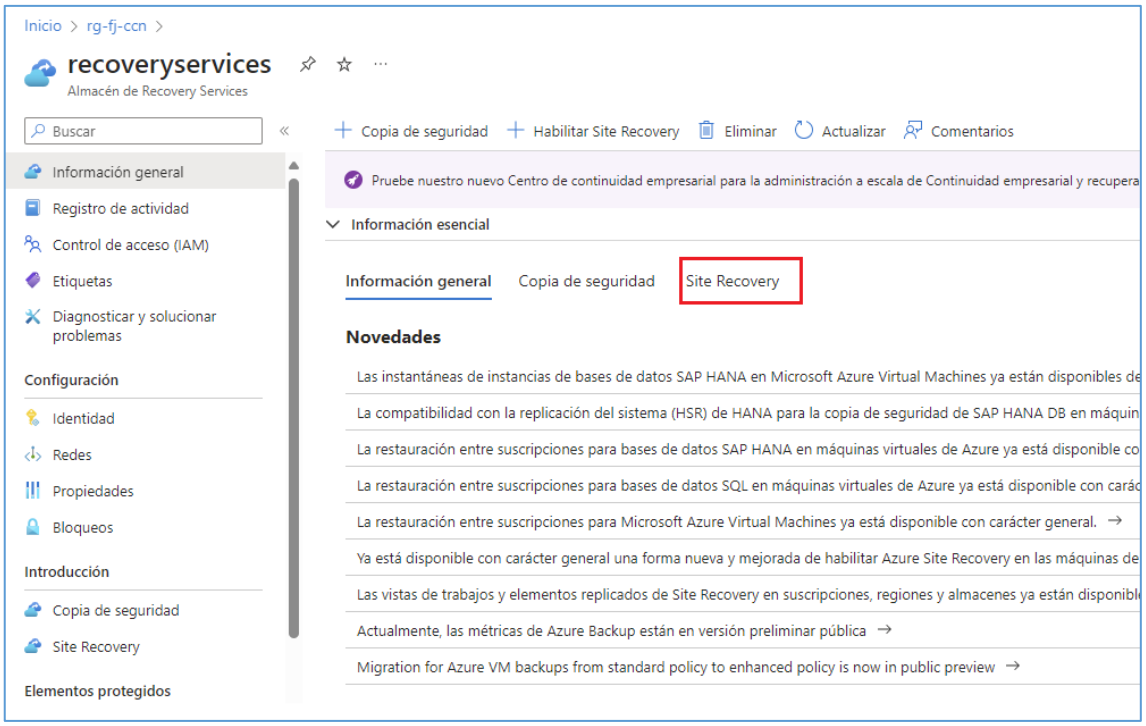
e) Se puede personalizar la directiva de replicación, crear un grupo de replicación y configurar las extensiones.



f) Pulsar en [Habilitar la replicación].

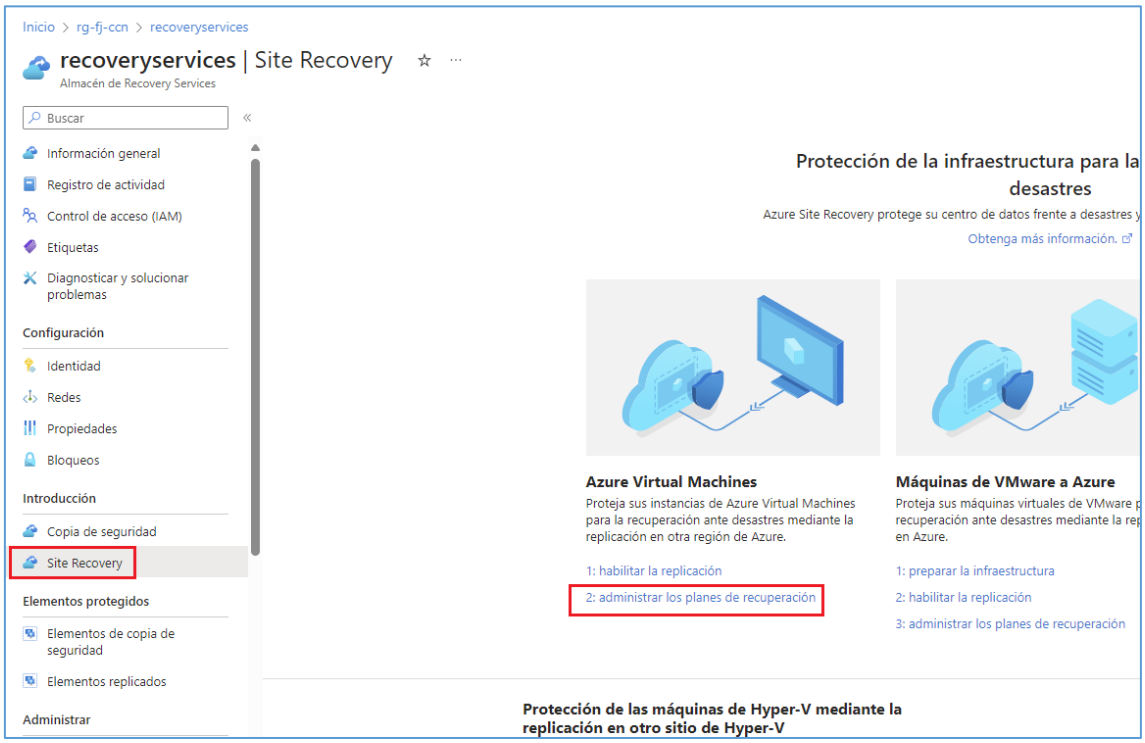
Nota: *Inicialmente es un proceso que suele tardar hasta que queda la replicación habilitada*.

g) Se puede consultar el estado de replicación desde el panel pulsando en [Site Recovery].



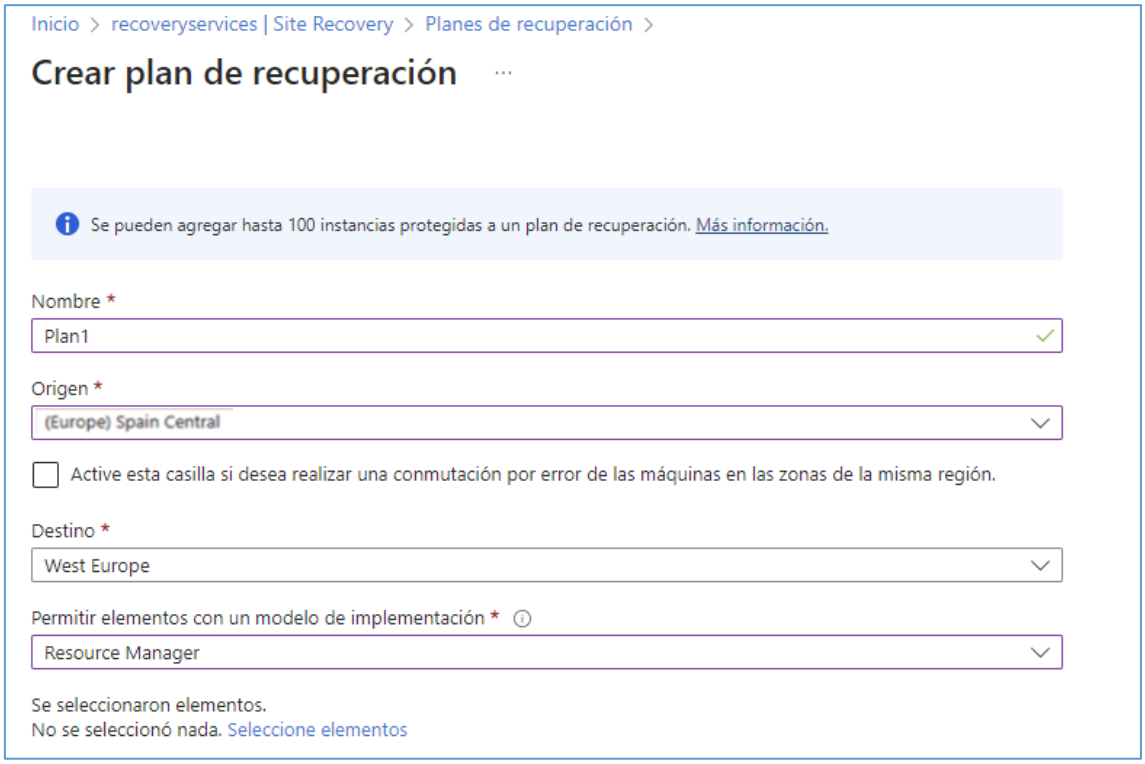
PLANES DE RECUPERACIÓN

a) Accedemos al menú [Site Recovery / Administrar los planes de recuperación]



b) Pulsar en [Plan de recuperación].

c) En este paso elegir la región origen y destino que se crea el plan de recuperación.



- **Nombre:** Elegir un nombre para el plan de recuperación.
- **Origen:** Seleccionar el origen de la máquina virtual.
- **Destino:** Seleccionar el destino donde se encuentra la réplica.
- **Permitir elementos con un modelo de implementación:** Seleccionar Resource Manager.
- **Seleccionar elementos:** Seleccionar la máquina virtual que se va a replicar geográficamente.

d) Pulsar en [Crear].

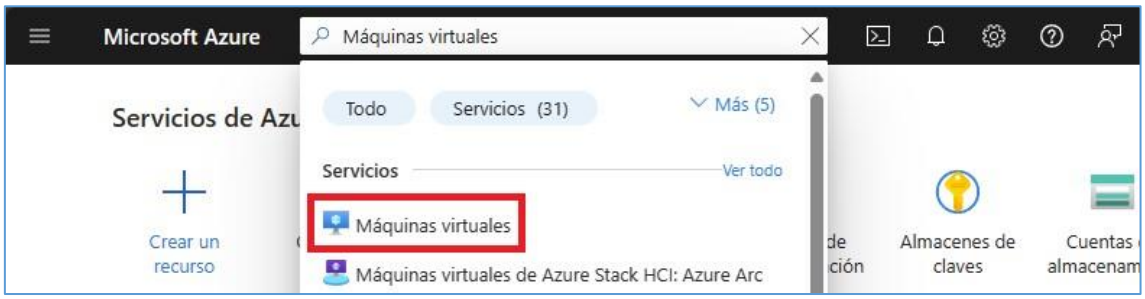
3.1.3.2 PRUEBAS PERIÓDICAS

COMPROBACIÓN DE CONMUTACIÓN POR ERROR

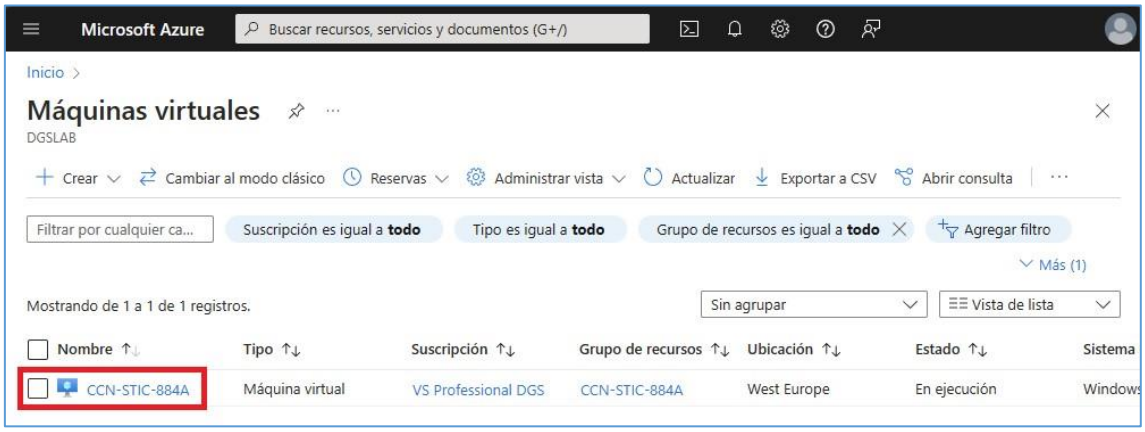
Desde Azure se pueden realizar pruebas periódicas de los servicios replicados en diferentes regiones.

La conmutación por error de prueba se ejecuta para validar la estrategia de replicación y recuperación ante desastres sin perder datos ni tiempo de actividad. La conmutación por error de prueba no afecta a la replicación en curso ni al entorno de producción.

a) En el buscador escribimos [Máquinas virtuales].

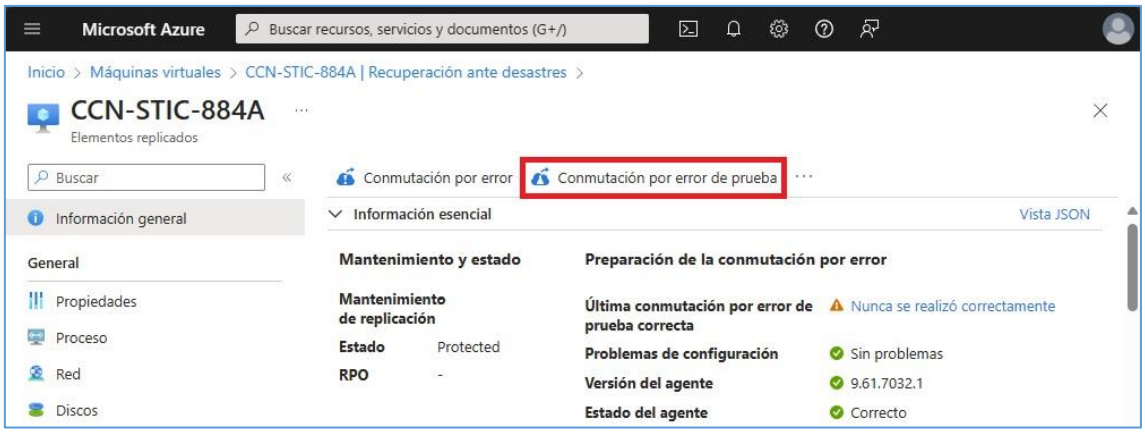


b) Pulsar sobre una máquina virtual.

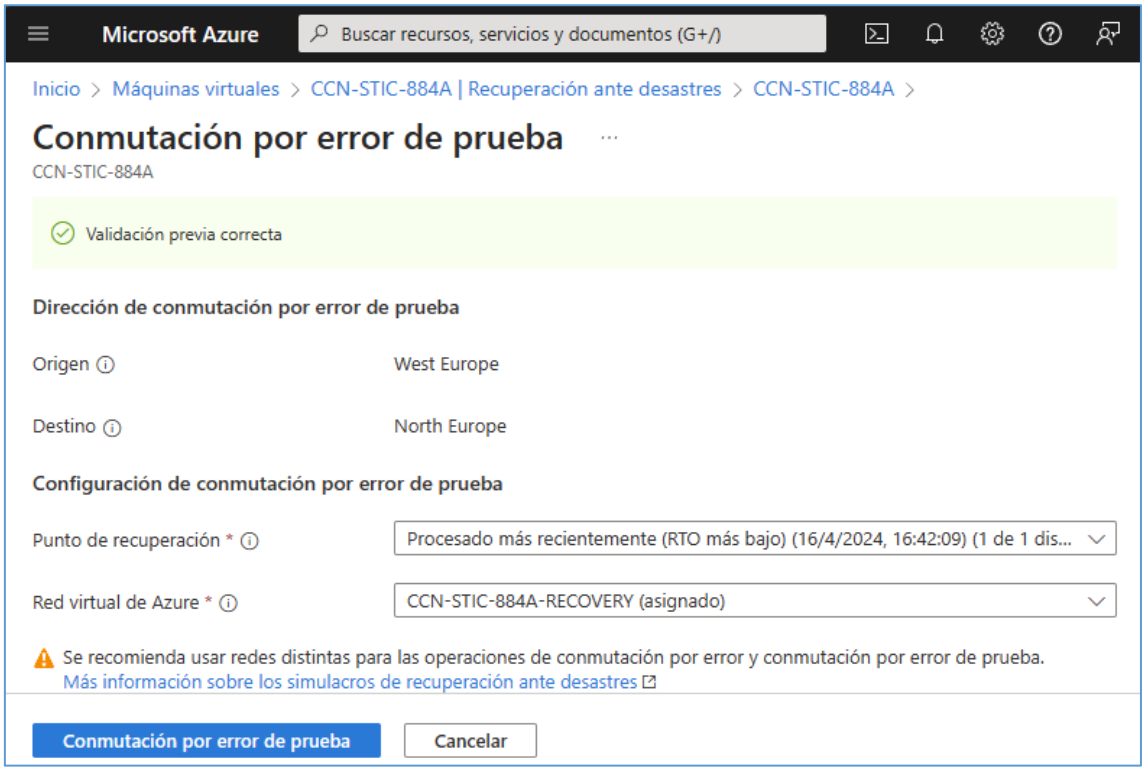


c) En las opciones de la máquina virtual, pulsar sobre [Copia de seguridad y recuperación ante desastres / Recuperación ante desastres]

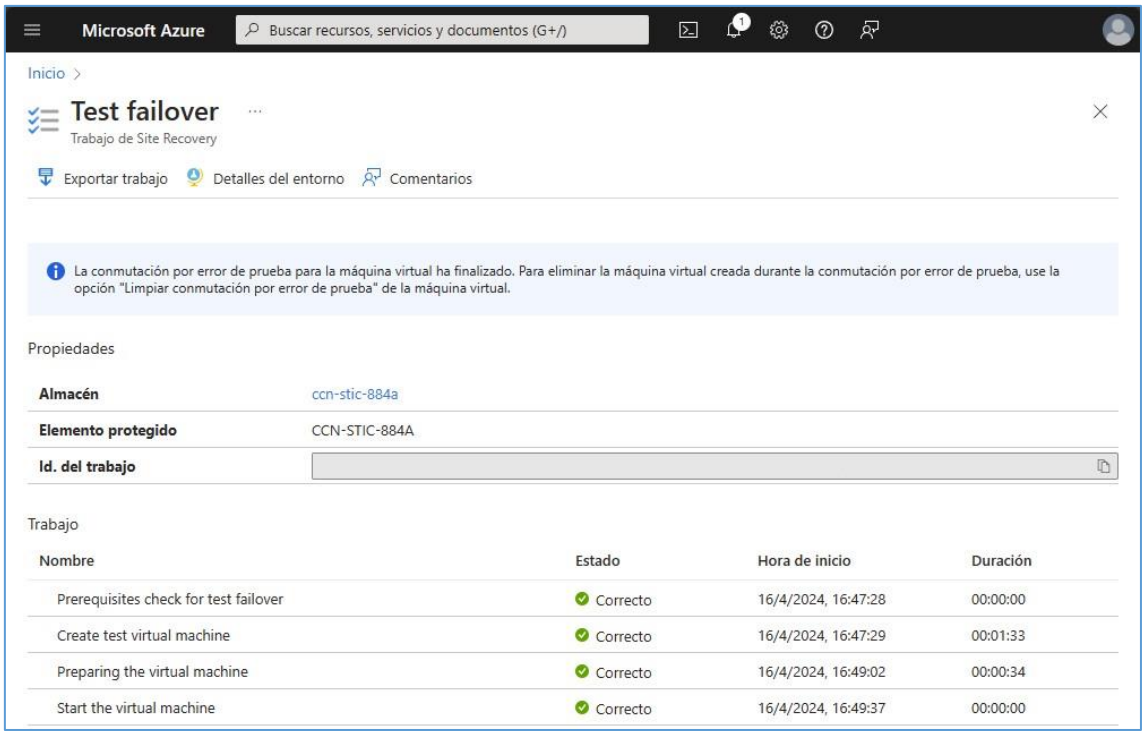
d) Pulsar sobre [Conmutación por error de prueba].



e) A continuación, definir la simulación de conmutación y pulsar sobre [Conmutación por error de prueba].



Nota: Al finalizar, se muestra el resultado de la prueba de conmutación por error entre regiones.



COMPROBACION DE CONMUTACION POR ERROR MEDIANTE POWERSHELL

Se puede realizar las mismas comprobaciones mediante la consola de PowerShell.

Para ello, realizar los siguientes pasos:

a) Desde la consola de PowerShell.

```
# PS C:\> $RecoveryPlan = Get-AzRecoveryServicesAsrReplicationProtectedItem
-Name "AzureDemoVM" -ProtectionContainer $PrimaryProtContainer

# PS C:\> $TFOJob = Start-AzRecoveryServicesAsrTestFailoverJob -RecoveryPlan
$RecoveryPlan -AzureVMNetworkId $TFONetwork -Direction PrimaryToRecovery
```

b) Esperar a que finalice la operación de conmutación por error de prueba.

```
# PS C:\> Get-ASRJob -Job $TFOJob
```

c) Una vez la prueba haya finalizado en la máquina virtual conmutada por error de prueba, limpie la copia de prueba mediante una operación de conmutación por error de prueba de limpieza. Esta operación elimina la copia de prueba de la máquina virtual que se creó con la conmutación por error de prueba.

```
#   PS C:\> $Job_TFOCleanup = Start-
    AzRecoveryServicesAsrTestFailoverCleanupJob -ReplicationProtectedItem
    $ReplicationProtectedItem

#   PS C:\> Get-ASRJob -Job $Job_TFOCleanup | Select-Object State
```

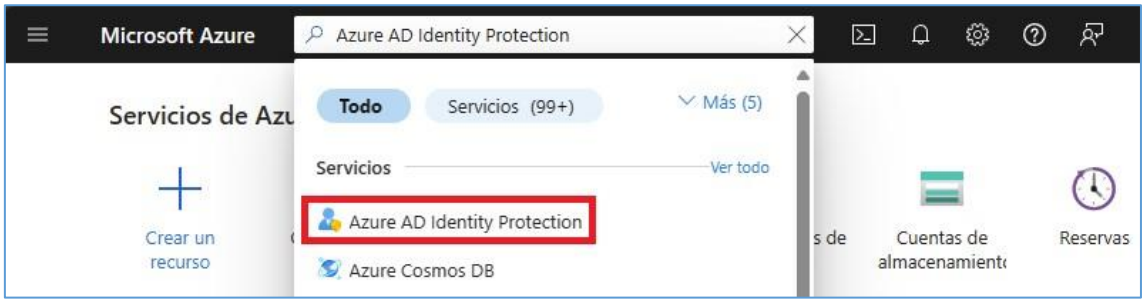
3.1.4 MONITORIZACIÓN DEL SISTEMA

3.1.4.1 DETECCIÓN DE INTRUSIÓN

Para la detección de intrusos se recomienda utilizar **Microsoft Entra ID Protection**. Este servicio permite crear directivas de riesgo de inicio de sesión de los usuarios de Microsoft Entra ID.

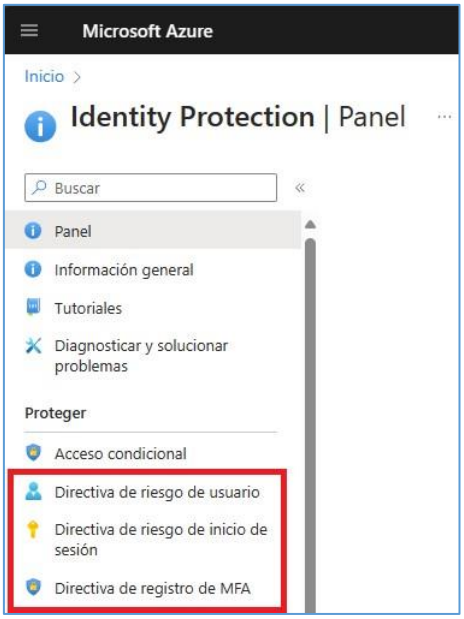
Seguir estas instrucciones.

a) En el buscador escribimos [Identity Protection].



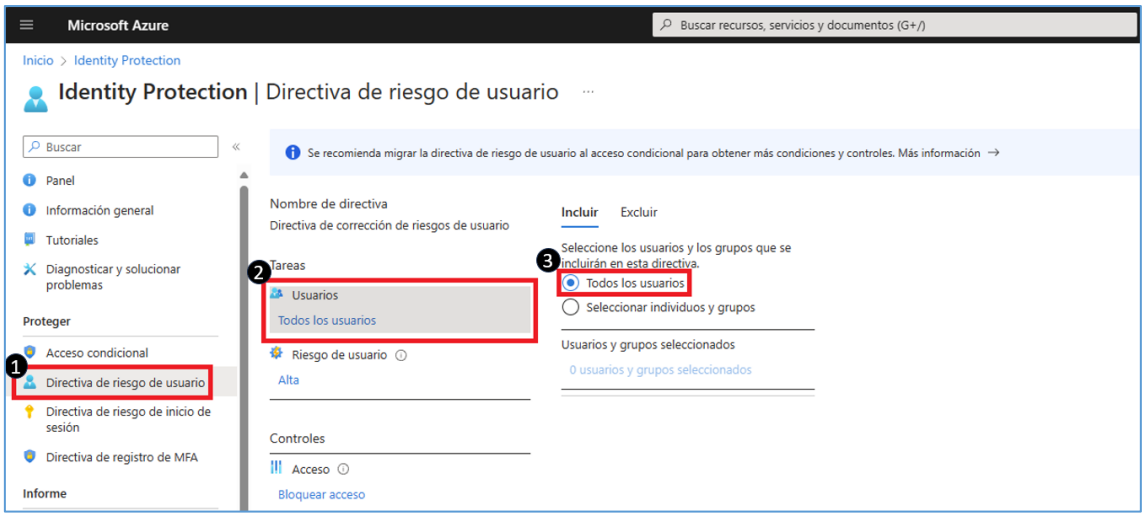
En este panel se deben configurar tres directivas.

- Directiva de riesgo de usuario.
- Directiva de riesgo de inicio de sesión.
- Directiva de registro de MFA.

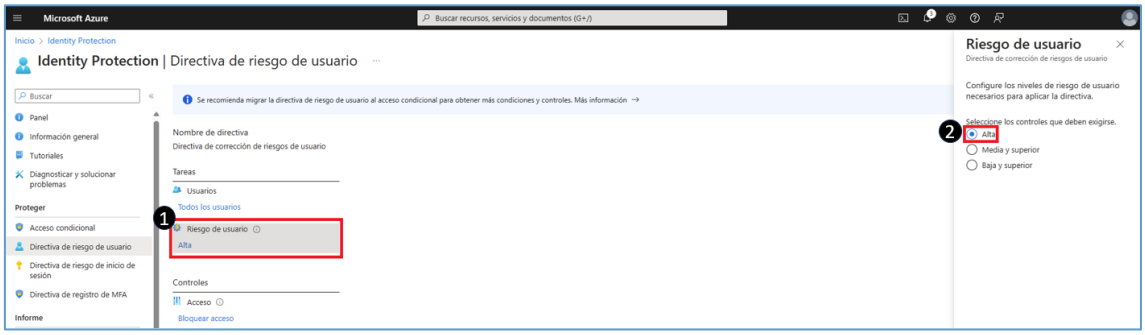


DIRECTIVA DE RIESGO DE USUARIO

a) Pulsar en [Usuarios / Todos los usuarios].

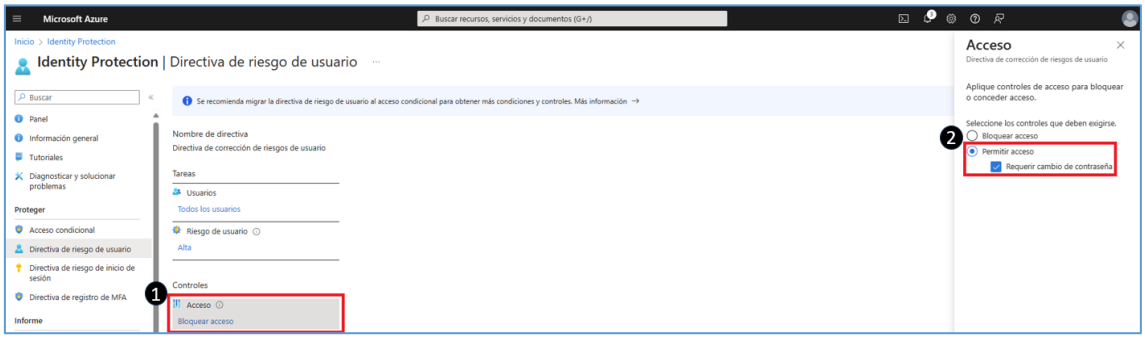


b) Pulsar en [Riesgos de usuario / Alto].

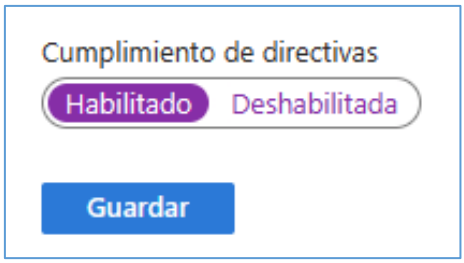


Nota: Se puede encontrar más información sobre los niveles de riesgos de usuarios en el enlace: https://learn.microsoft.com/en-us/entra/id-protection/overview-identity-protection#what-is-a-user-risk-level

c) Pulsar en [Controles / Permitir acceso] y [Requerir cambio de contraseña].

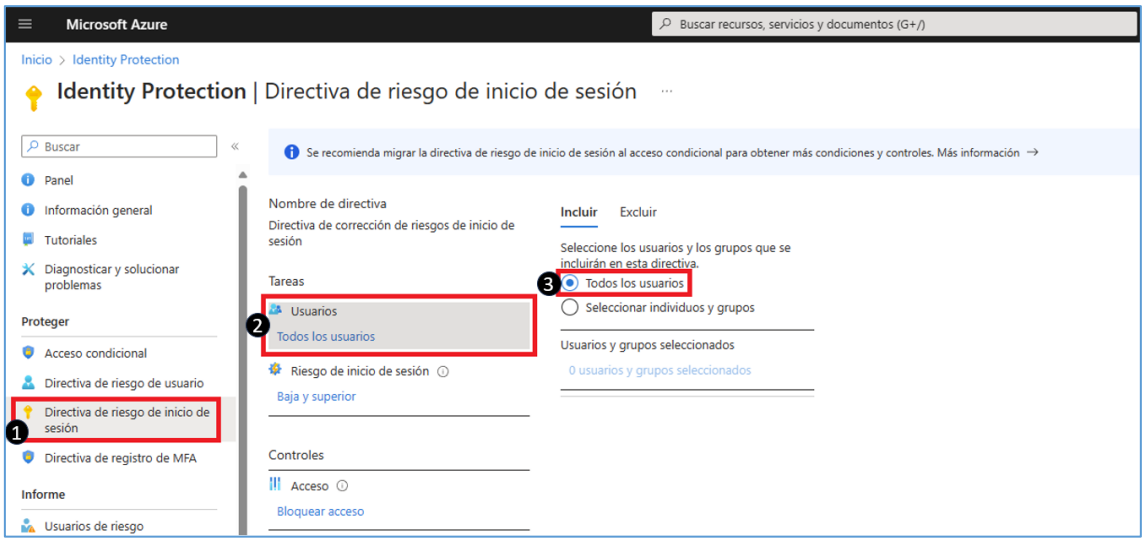


d) Para finalizar, en **Cumplimiento de directivas** pulsar en [Habilitar / Guardar].

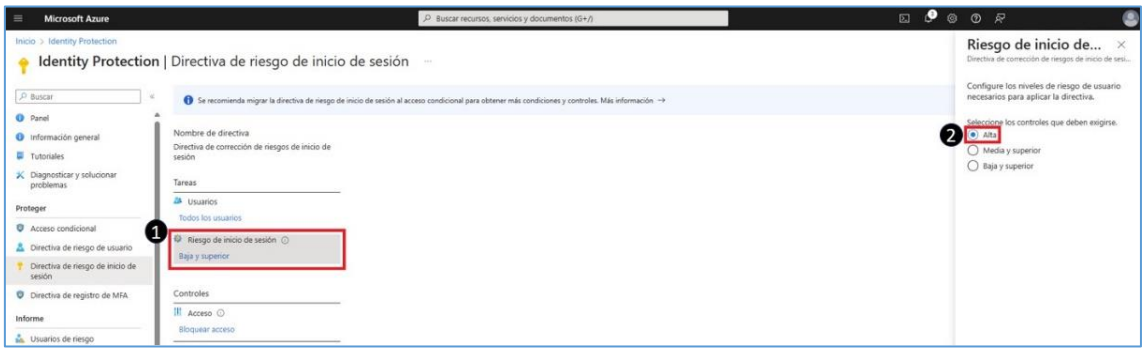


DIRECTIVA DE RIESGO DE INICIO DE SESIÓN

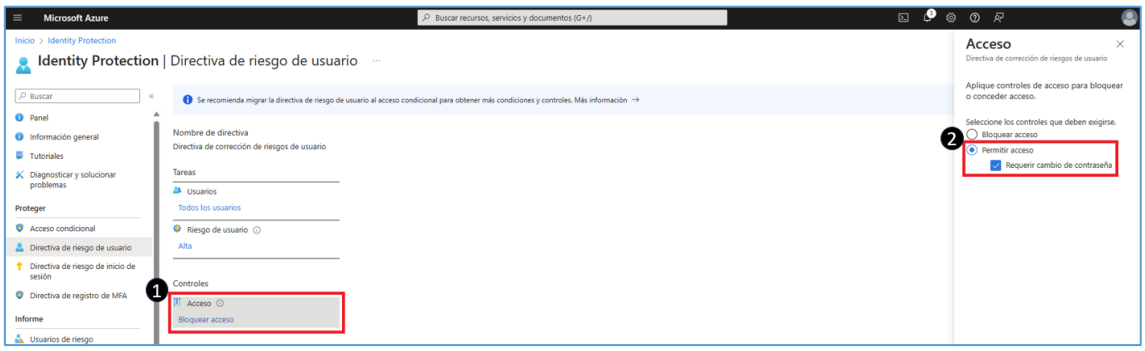
a) Pulsar en [Usuarios / Todos los usuarios].



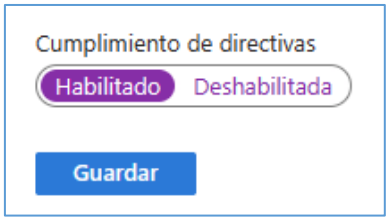
b) Pulsar en [Riesgo de inicio de sesión / Alto].



e) Pulsar en [Acceso / Permitir acceso] y [Requerir cambio de contraseña].

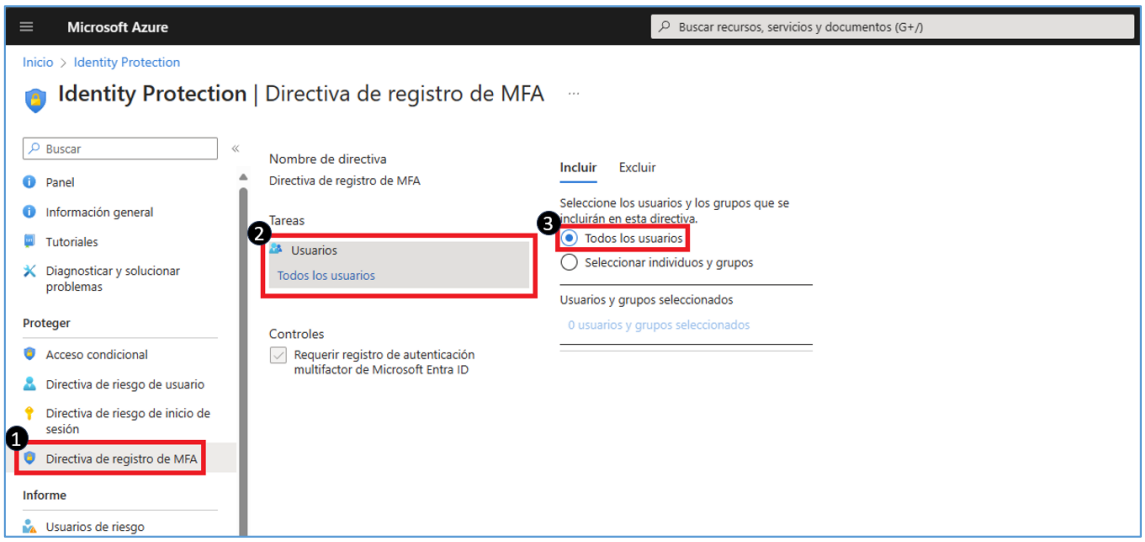


c) Para finalizar, en **Cumplimiento de directivas** pulsar en [Habilitar / Guardar].

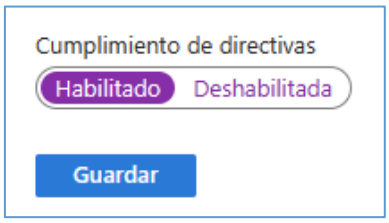


DIRECTIVA DE REGISTRO DE MFA

a) Pulsar en [Usuarios / Todos los usuarios].

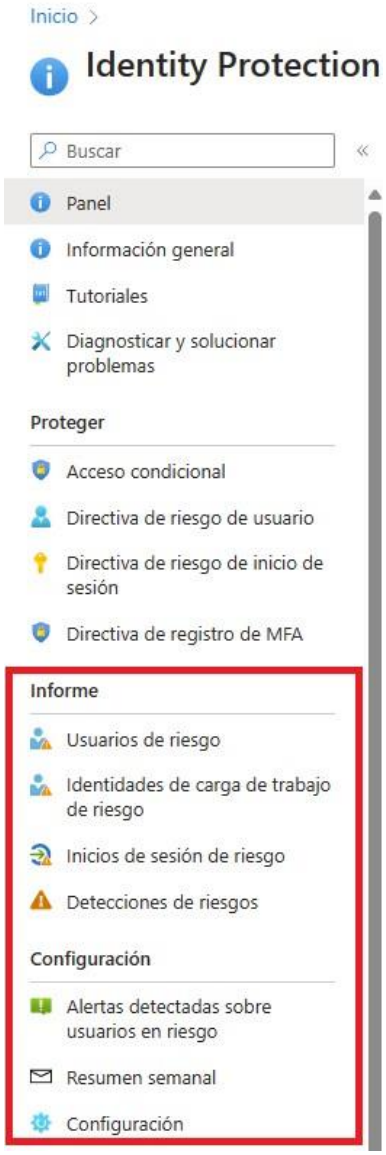


b) Para finalizar, en **Cumplimiento de directivas** pulsar en [Habilitar / Guardar].



INFORMES Y CONFIGURACIÓN

Desde el panel se puede visualizar en tiempo real Informes de riesgos en inicios de sesión o detecciones de riesgos.



Al final del panel se puede configurar alertas que llegaran vía email o un resumen semanal con las detecciones encontradas.

Además, se puede consultar los Mecanismos de autenticación en el apartado [3.1.1.4 Directivas de acceso condicional] de la presente guía.

Para encontrar más información: *https://learn.microsoft.com/es-es/entra/id-protection/overview-identity-protection*

3.1.4.2 SISTEMA DE MÉTRICAS

Para definir métricas dentro de Azure se debe configurar Azure monitor.

Estas métricas pueden ser métricas de plataforma, personalizadas, registros populares de Azure Monitor convertidos en métricas y de Application Insights.

Las alertas de métricas se evalúan a intervalos regulares para comprobar si las condiciones de una o varias series temporales para las métricas son verdaderas y recibir

una notificación cuando se cumplan las evaluaciones. Como las alertas de métricas tienen un estado, solo envían notificaciones cuando cambia ese estado.

AZURE MONITOR

Permite identificar de manera proactiva los problemas que les afectan y los recursos de los que dependen.

Azure Monitor almacena datos en almacenes de datos para cada uno de los tres pilares de observabilidad, más uno adicional: métricas, logs, traces (seguimientos distribuidos) y cambios. Las métricas son valores numéricos que describen un aspecto de un sistema en un momento dado. Los logs son eventos del sistema registrados. El seguimiento distribuido permite ver la ruta de acceso de una solicitud a medida que viaja a través de diferentes servicios y componentes. Los cambios son una serie de eventos en la aplicación y los recursos.

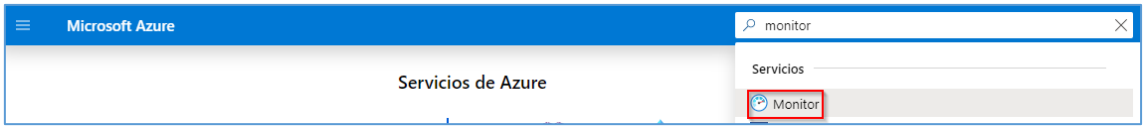
Los datos de registro recopilados por Azure Monitor se pueden analizar con consultas que recuperan, consolidan y analizan rápidamente los datos recopilados.

Azure Monitor recopila datos de cada uno de los siguientes niveles:

- Datos de supervisión de aplicaciones: datos sobre el rendimiento y la funcionalidad del código que ha escrito, independientemente de la plataforma.
- Datos de supervisión del sistema operativo invitado: datos sobre el sistema operativo en el que se ejecuta la aplicación. La aplicación se puede ejecutar en Azure, en otra nube o en el entorno local.
- Supervisión de recursos con DMV: datos sobre el funcionamiento de un recurso de Azure.
- Datos de supervisión de la suscripción de Azure: datos sobre el funcionamiento y la administración de una suscripción de Azure, así como sobre el estado y el funcionamiento del propio Azure.
- Datos de supervisión de inquilino de Azure: datos sobre el funcionamiento de los servicios de Azure en el nivel del inquilino, como Azure Active Directory.

Los datos de registro recopilados por Azure Monitor se pueden analizar con consultas que recuperan, consolidan y analizan rápidamente los datos recopilados. Se puede crear y probar consultas usando Log Analytics.

Se puede acceder Azure monitor utilizando el buscador y escribiendo Azure monitor



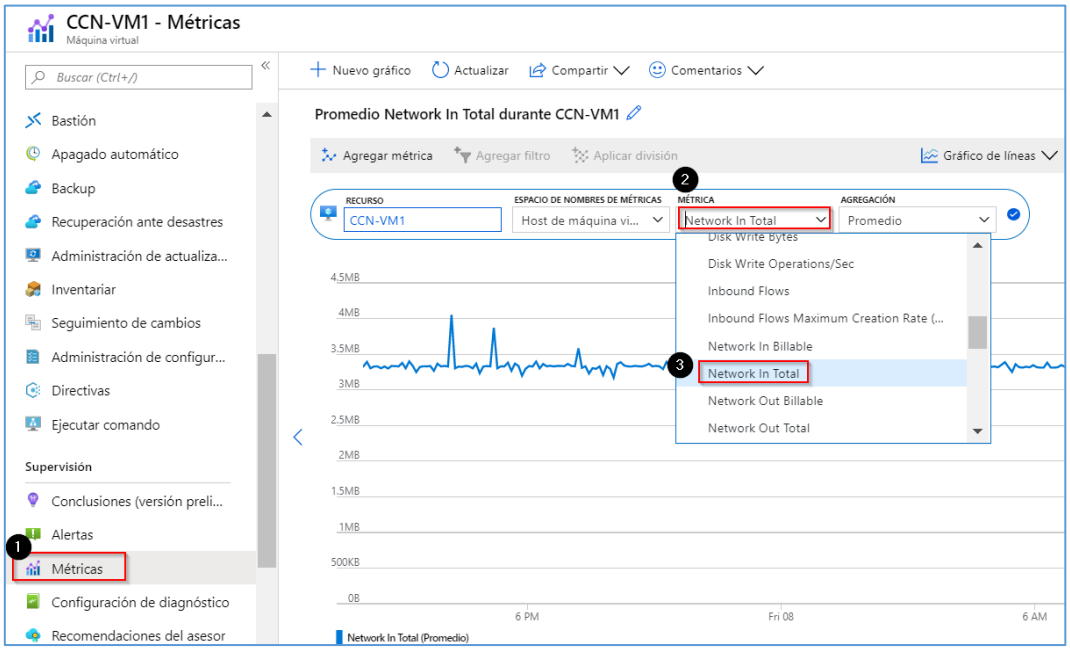
Nota: Se puede consultar la documentación en el enlace *https://docs.microsoft.com/es-es/azure/azure-monitor/overview*

EXPLORADOR DE MÉTRICAS DE AZURE

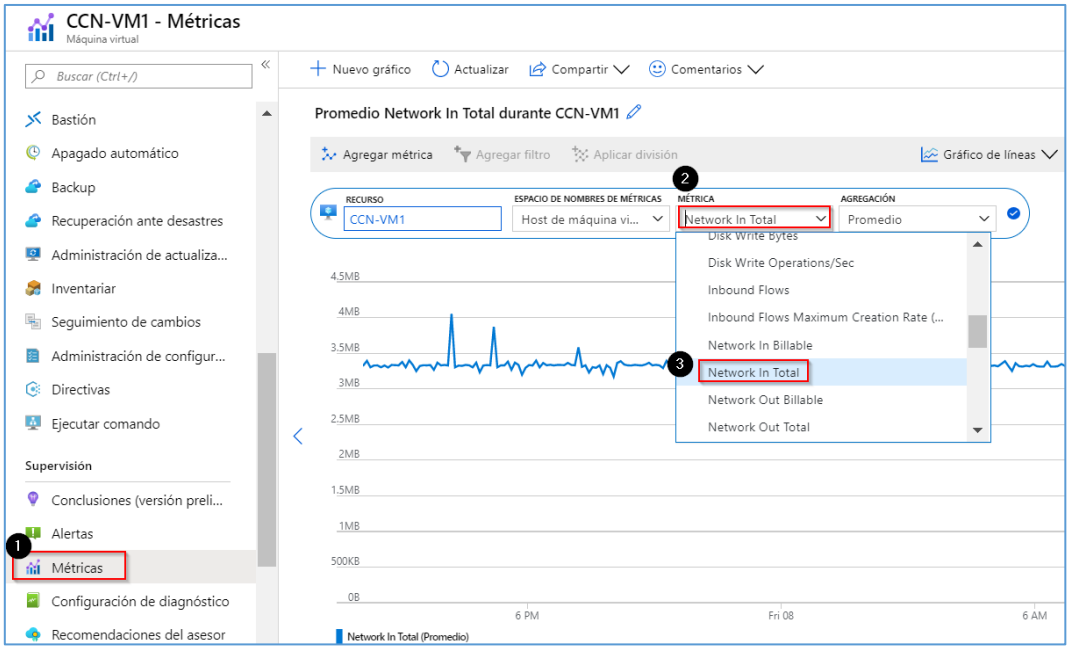
El explorador de métricas de Azure Monitor es un componente de Microsoft Azure Portal que permite trazar los gráficos, correlacionar visualmente las tendencias e investigar crestas y valles en valores de las métricas. Utilice el Explorador de métricas para investigar el estado y la utilización de recursos.

Para ello realizar los siguientes pasos:

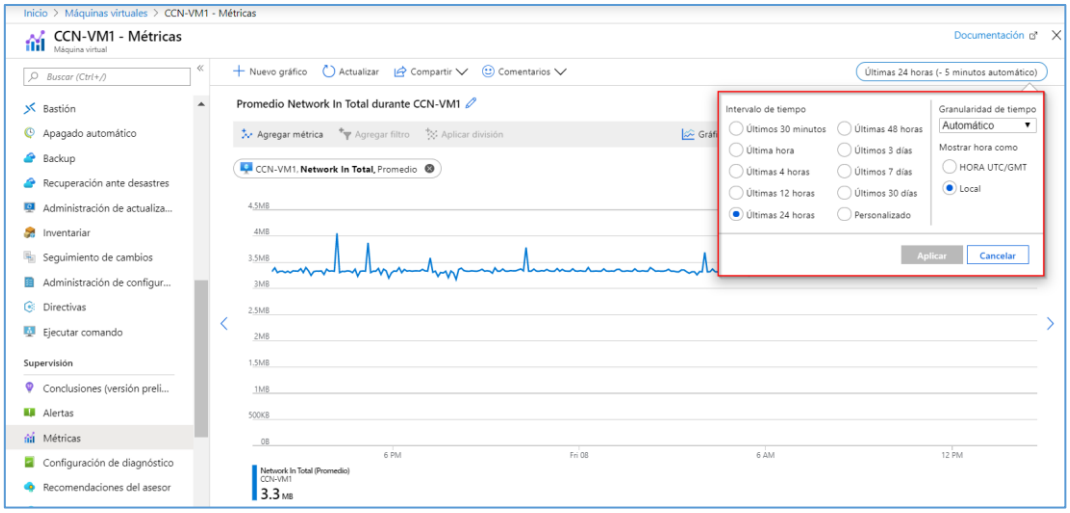
a) Seleccionar un recurso y una métrica para visualizar un gráfico básico. El intervalo de tiempo se puede modificar. Para el ejemplo se utiliza las métricas de una máquina virtual.



b) Se puede cambiar el intervalo de tiempo, para ello pulsar en:



c) Seleccionar el rango de tiempo adecuado y pulsar en [Aplicar].



ALERTAS

Las alertas permiten identificar y solucionar los problemas antes de que los usuarios puedan verlos.

Los atributos clave de las reglas de alertas son:

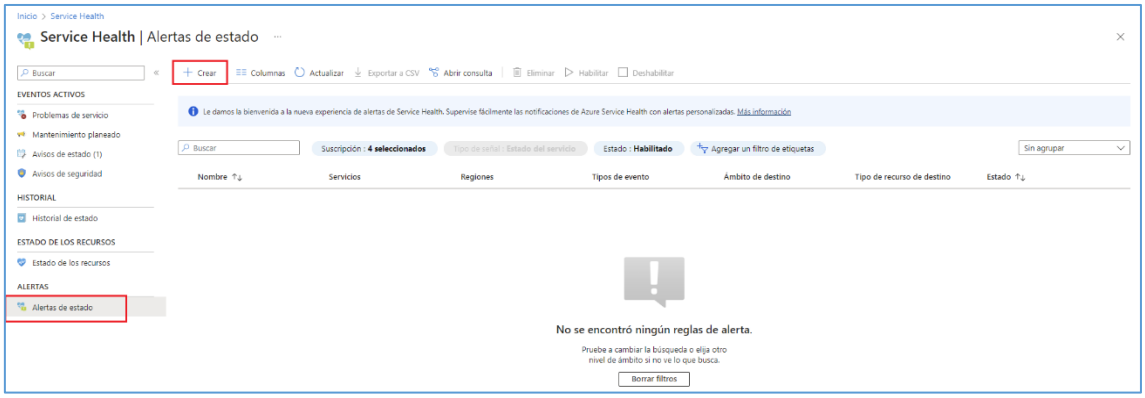
- **Recurso destino**: Define el ámbito y las señales disponibles para las alertas. Un destino puede ser cualquier recurso de Azure, como por ejemplo una máquina virtual o un área de trabajo de log analytics.
- **Señal**: Es emitida por el recurso de destino. Las señales pueden ser de los siguientes tipos:
    - **Métrica**: Para consultar más información consultar la sección [3.1.4.2 Sistemas de métricas/Azure Monitor/ Explorador de métricas]
    - **Registro de Actividad**: Se tratan de alertas que se activan cuando un evento del registro de actividad cumple con las condiciones especificadas en la alerta.
      Por norma general se crean alertas del registro de actividad cuando:
        - Se producen operaciones específicas en recursos de Azure.
        - Se produce un evento de mantenimiento del servicio.

      Cuando se activa una alerta del registro de actividad se usa un grupo de acciones para generar acciones o notificaciones. Un grupo de acciones es un conjunto reutilizable de destinatarios de notificación.

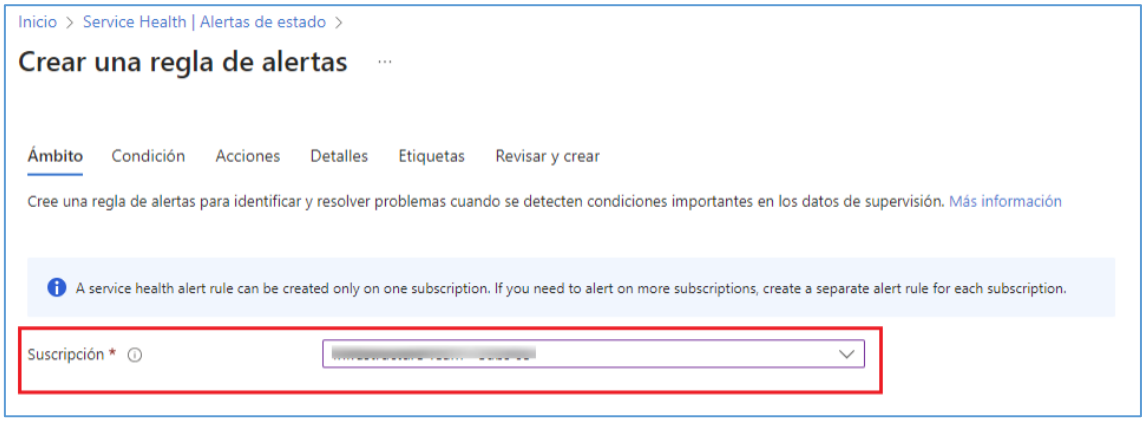
    - **Registro**: Las alertas de registro consisten en reglas creadas para los registros de Azure Monitor o Application Insights, para ejecutar automáticamente consultas de registros especificadas a intervalos regulares. Si los resultados de la consulta coinciden con determinados criterios se crea un registro de alertas.

Como ejemplo se crea una alerta que envíe una notificación por correo cuando haya algún evento en Service Health. Para crear la alerta realizar los siguientes pasos:

a) Buscar Service Health, pulsar en [Alertas de estado/Crear].



b) Selecciona la suscripción.

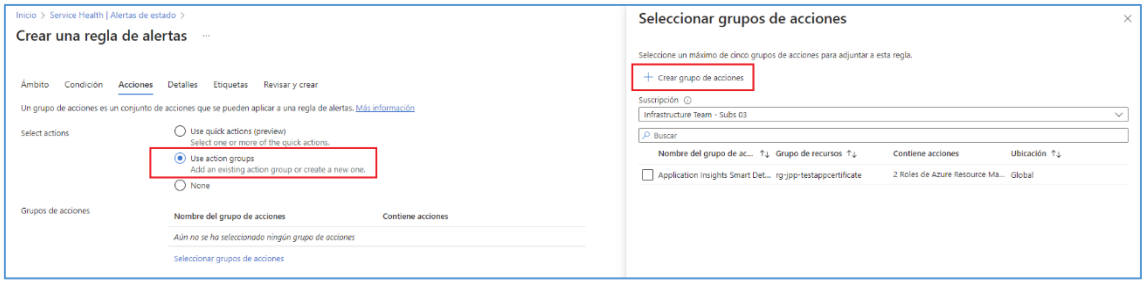


c) Seleccionar servicios, regiones y tipo de evento. Regiones seleccionad solo en las que haya algún recurso creado.

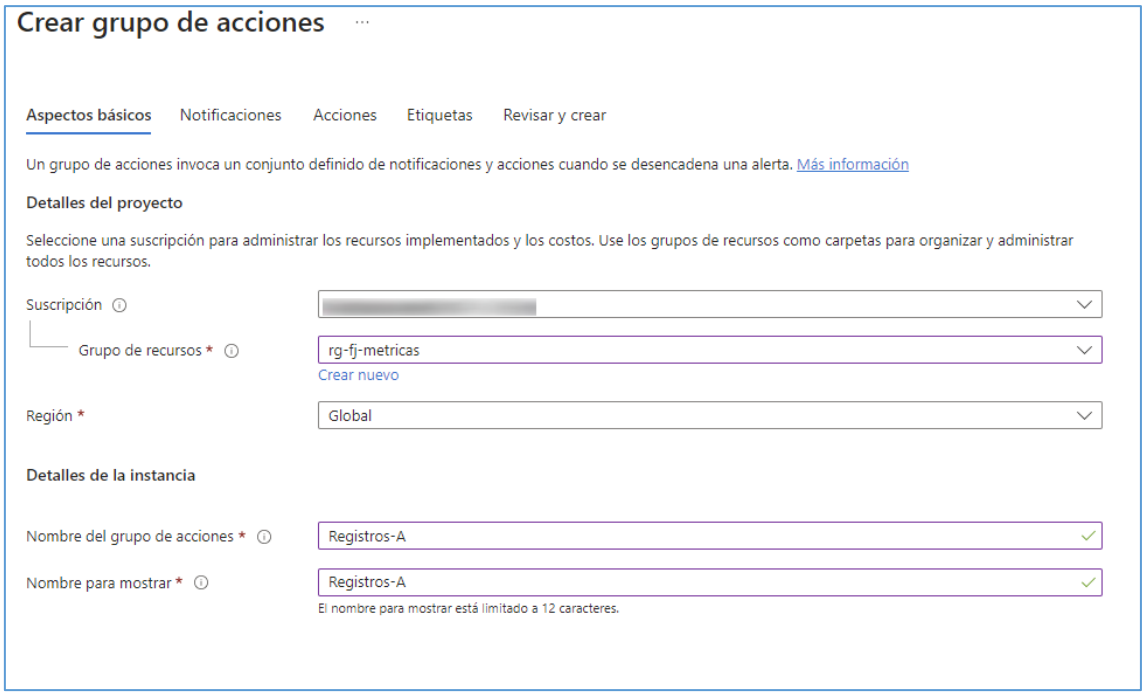
El Tipo de evento puede ser:

- Problema de servicio
- Mantenimiento planeado
- Avisos de estado
- Aviso de seguridad

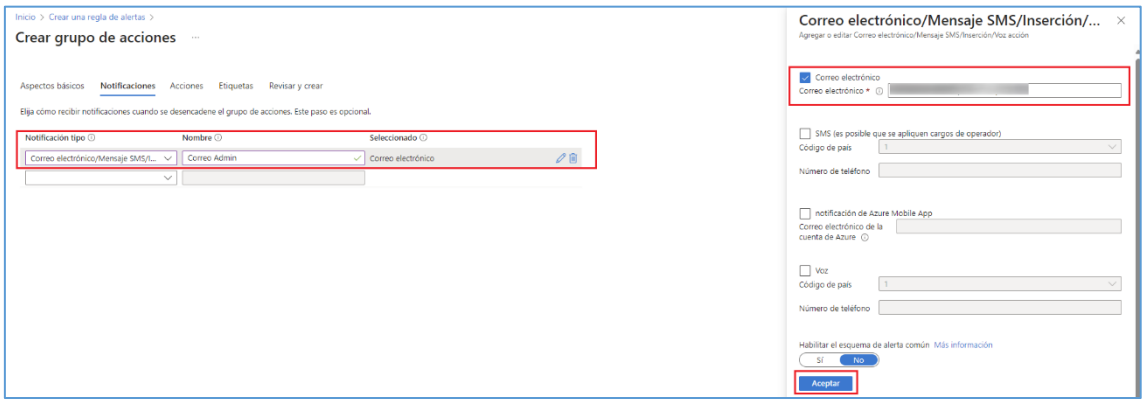
Una vez seleccionado, en acciones pulsar en "Use action groups" y crear grupo de acciones.



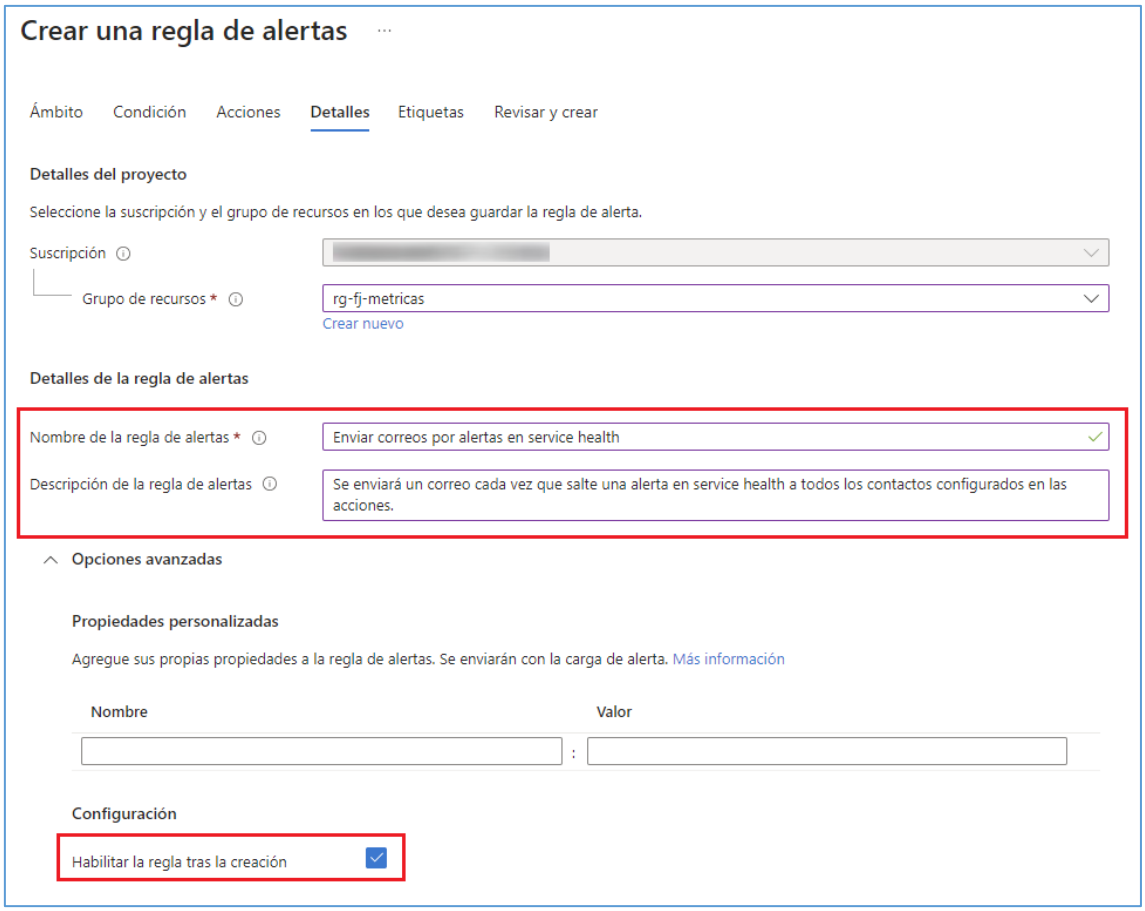
d) Dar nombre al grupo de acciones, dar un nombre corto que forma parte del correo cuando salte la alerta, seleccionar suscripción, grupo de recursos donde se guarda el grupo de acciones y la región.



e) En notificación tipo seleccionar correo electrónico, y añadir el correo electrónico deseado, sólo se permite uno por acción. En el caso de desear mandarlo a más destinatarios añadir más acciones.



f) Una vez definidas las acciones se completa la sección *Detalles* en la regla de alertas. Seleccionar la suscripción y el grupo de recursos donde se desea guardar la regla de alerta. Dar nombre a la alerta, descripción (opcional) y en *Opciones avanzadas* habilitar la regla tras la creación.



3.1.4.3 VIGILANCIA

NETWORK WATCHER

Network Watcher proporciona un conjunto de herramientas para monitorear, diagnosticar, ver métricas y habilitar o deshabilitar registros de recursos de IaaS (infraestructura como servicio) de Azure. De esta manera, Network Watcher permite supervisar y reparar el estado de red de productos IaaS constando de tres herramientas y funcionalidades: supervisión, herramientas de diagnóstico de red y tráfico.

Al crear una red virtual en una suscripción se habilita de forma automática en la región de la red virtual (VNET). Esto no afecta a los recursos ni a los cargos asociados.

SUPERVISIÓN

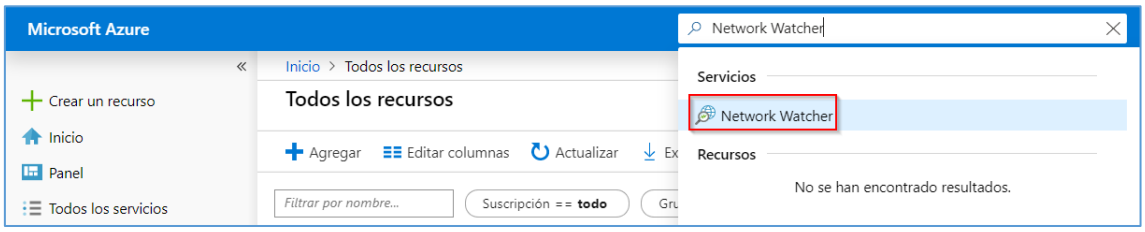
SUPERVISIÓN DE LA COMUNICACIÓN ENTRE UNA MÁQUINA

Network Watcher supervisa la comunicación a intervalos regulares informando de los cambios en la disponibilidad, latencia y topología entre una máquina virtual y otro punto de conexión, como puede ser otra máquina virtual.

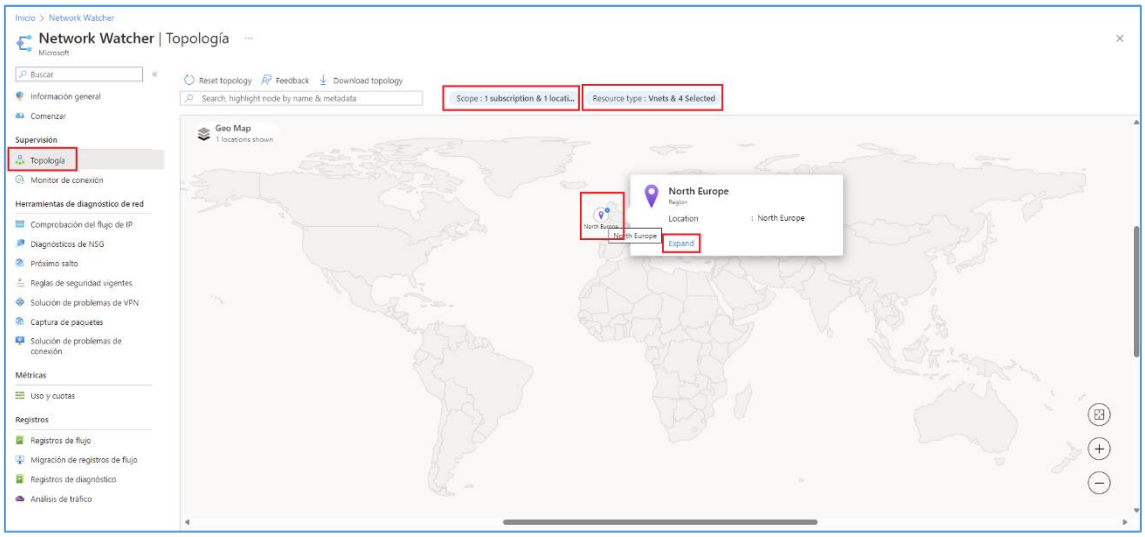
VISUALIZACIÓN DE RECURSOS EN UNA RED VIRTUAL

Network Watcher genera un diagrama de los recursos que contienen una red virtual y las relaciones existentes entre los distintos recursos. Para generar el diagrama se realizan los siguientes pasos:

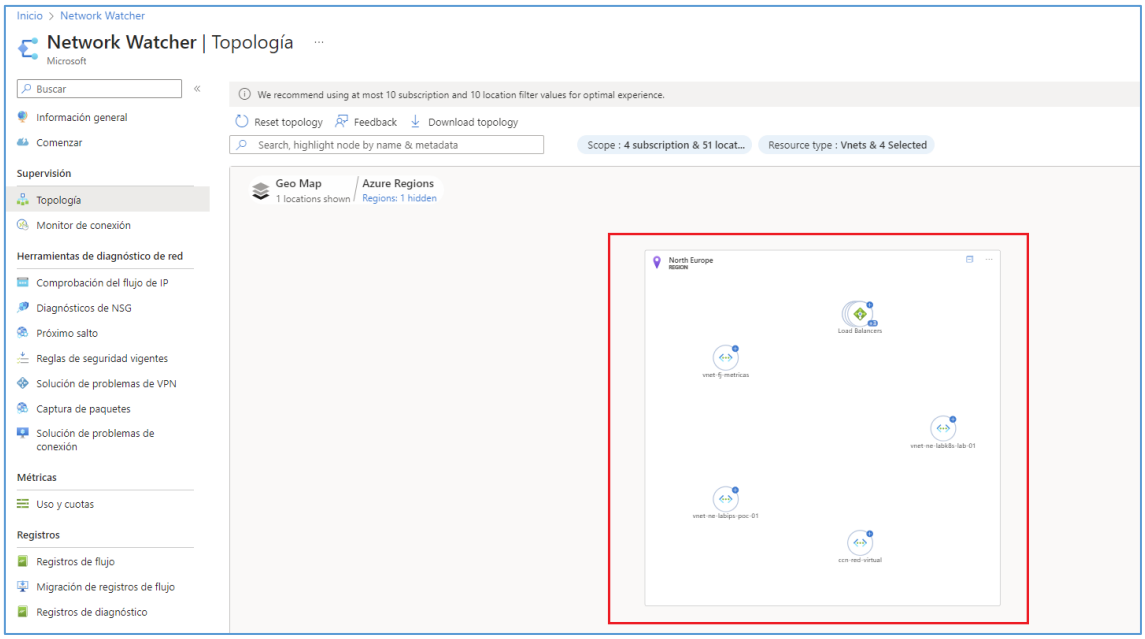
a) Buscar [Network Watcher].



b) Pulsar en [Topología], aplica los filtros deseados para generar el diagrama. Puedes seleccionar la Suscripción, grupo recursos, localización o tipo de recurso si lo deseas. Después desplaza el puntero del ratón sobre la región y selecciona [Expandir].



c) A continuación, se mostrará la topología de red de la región seleccionada tras haber aplicado los filtros deseados.



DIAGNÓSTICO

Network Watcher permite detectar problemas en los siguientes escenarios:

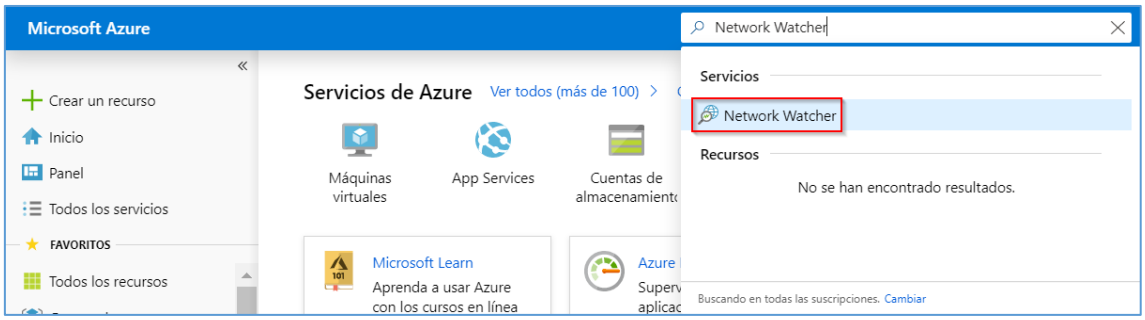
- En el tráfico de red hacia una máquina virtual o hacia una puerta de enlace
- En el enrutamiento de red desde una máquina virtual
- En conexiones de salida desde una máquina virtual
- Determinar latencias entre distintas regiones de Azure y proveedores de Internet.

Además, permite capturar paquetes desde y hacia una máquina virtual.

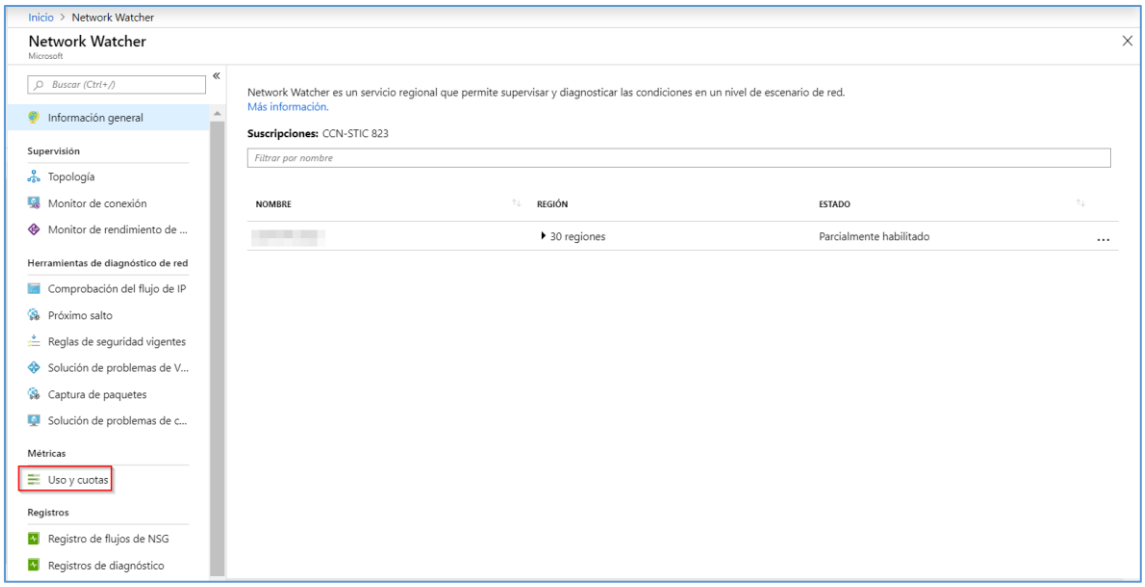
MÉTRICAS

La opción de métricas le permite controlar los límites en Azure para todos los recursos. Para verlo hay que seguir los siguientes pasos:

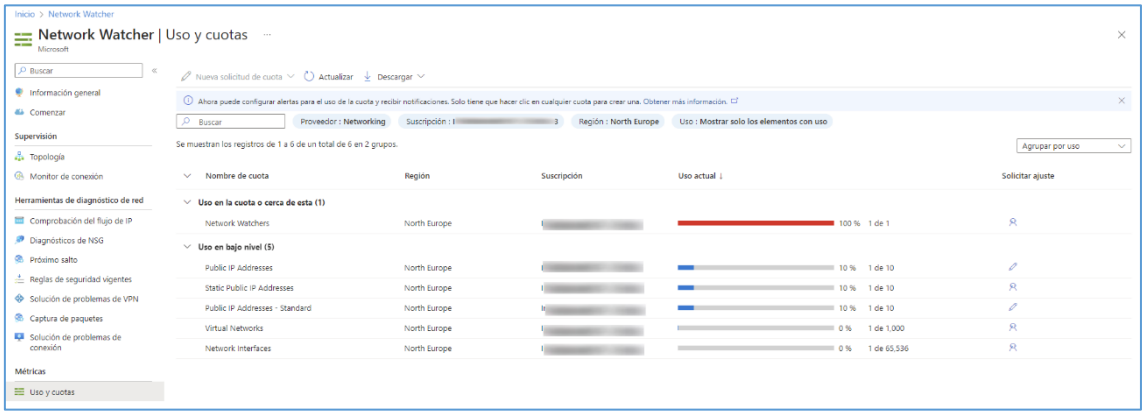
a) Buscar Network watcher.



b) Pulsar en [Uso y cuotas].



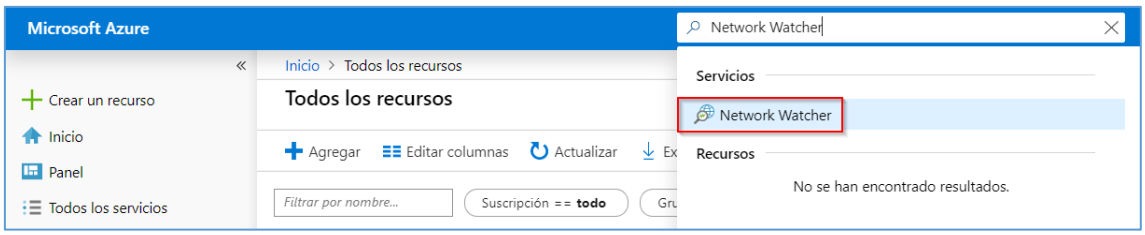
c) Puedes filtrar por proveedor, suscripción, región y uso para visualizar el uso y cuotas deseados en el Tenant. En el ejemplo se muestran las cuotas de todos los elementos de red en uso de una suscripción en la región del Centro de España:



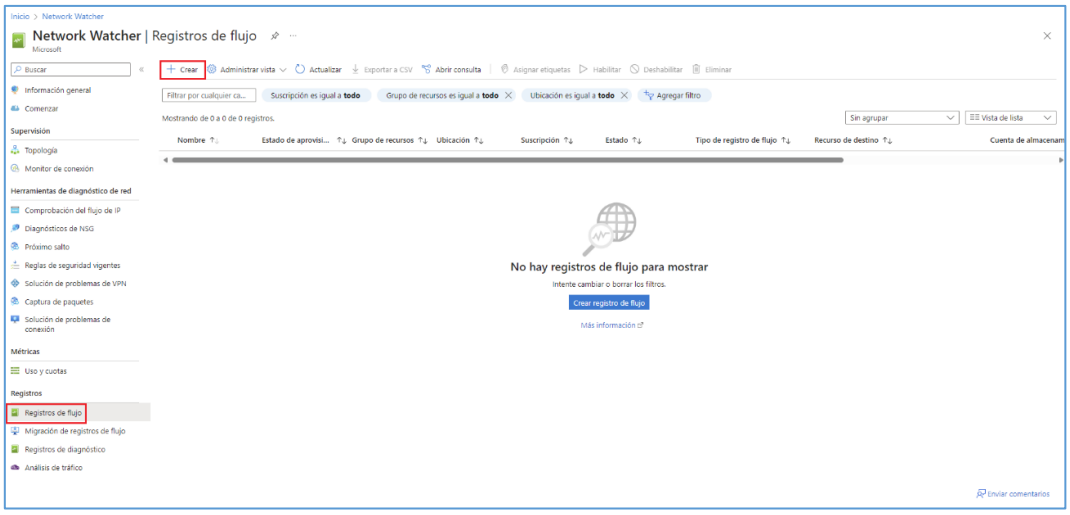
REGISTROS DE FLUJO

Network watcher permite realizar un análisis del tráfico que haya pasado por un NSG o una red virtual. Para ello, se debe realizar la siguiente configuración:

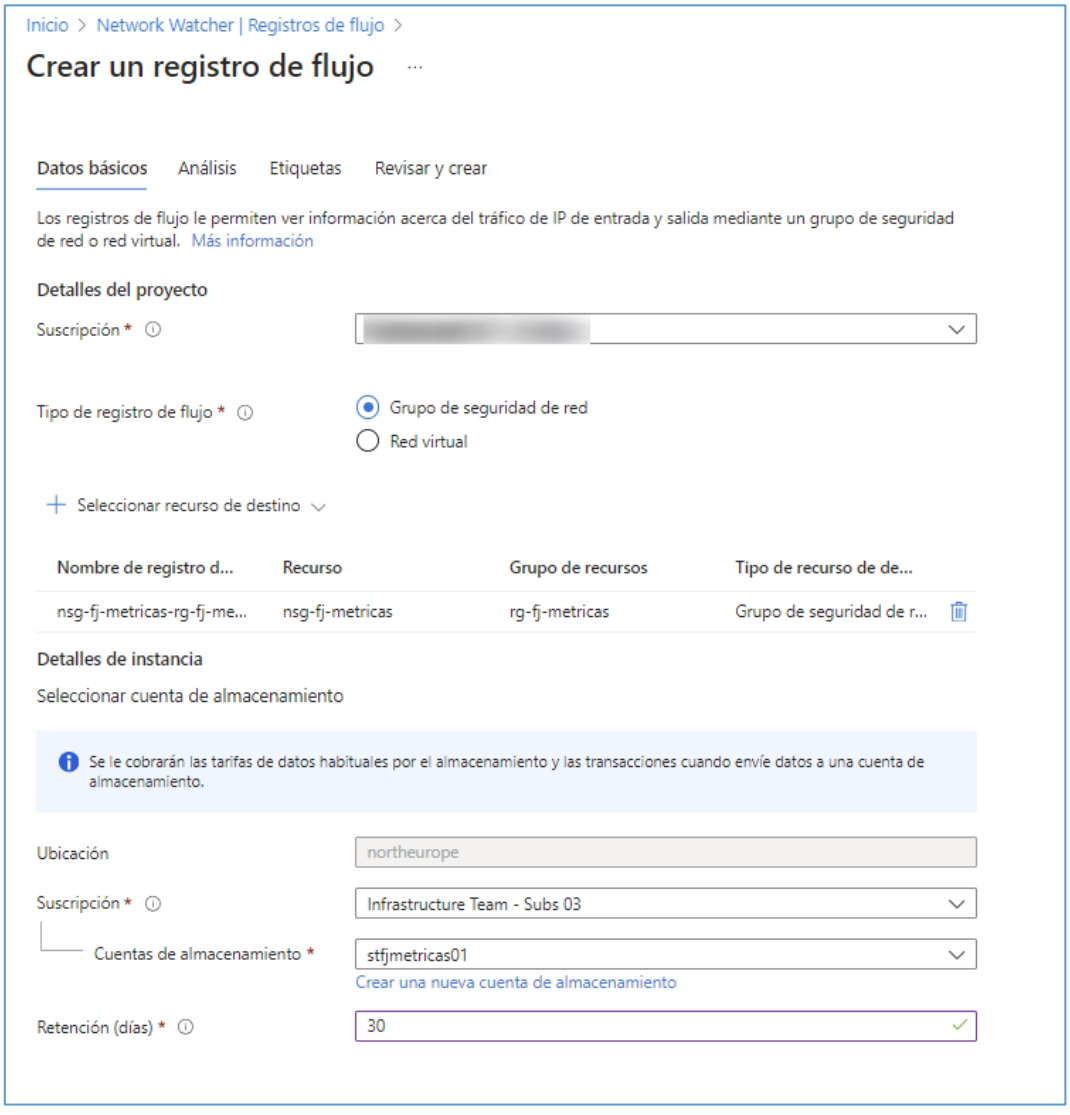
a) Buscar Network Watcher



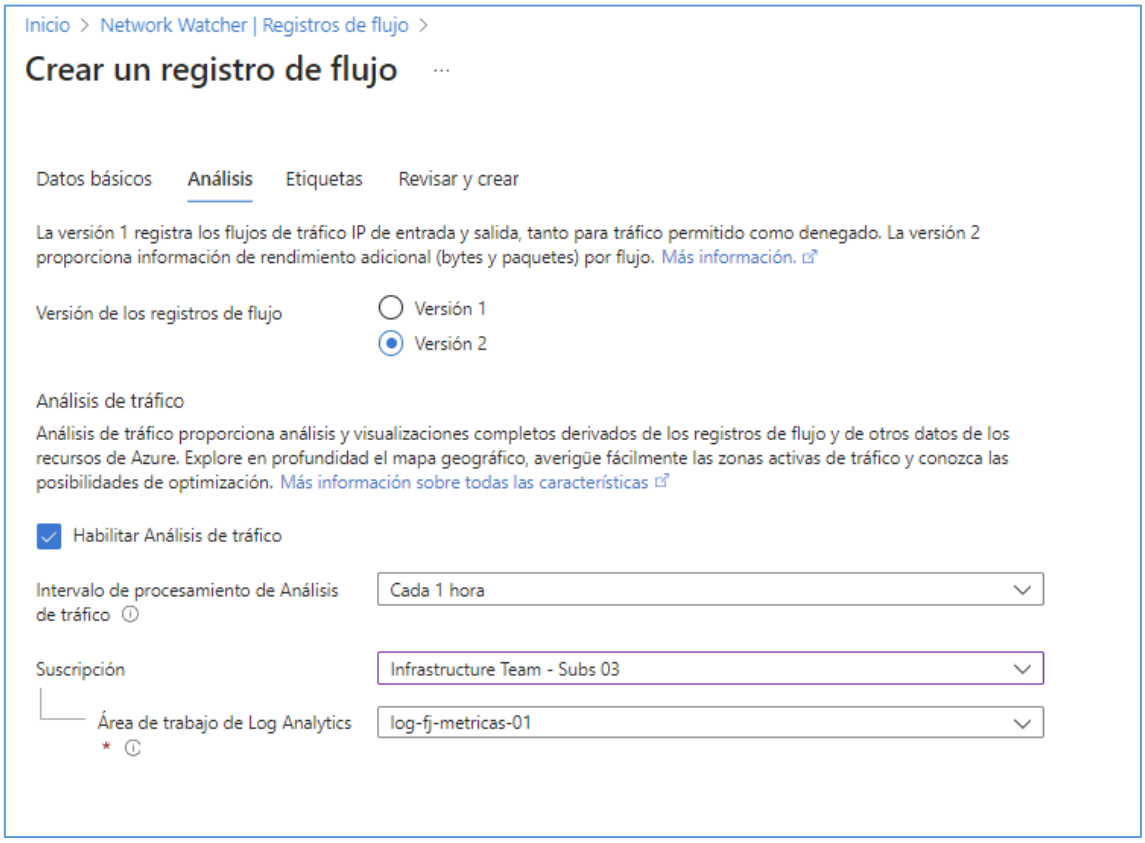
b) Pulsar en [Registros de flujo / Crear].



c) Seleccionar el recurso de Azure cuya conectividad desees registrar, en este ejemplo elegimos un grupo de seguridad. Se debe disponer de una cuenta de almacenamiento creada exclusivamente para guardar los logs.



d) Dependiendo de la cantidad de información que sea necesaria, es posible utilizar la versión 1 o la versión 2 de los registros de flujos. La versión 1 muestra todos los flujos de tráfico por IP de entrada y salida. La versión 2, además, aporta bytes y paquetes transmitidos. También se pide un área de trabajo para *log analytics* cuya creación se explica en el apartado de *log analytics.* Además, es necesario definir el intervalo de procesamiento del análisis de tráfico. Se puede poner cada 10 minutos o cada hora. Por defecto, se configurará para que sea cada hora, a no ser que se tenga que hacer un análisis muy exhaustivo.

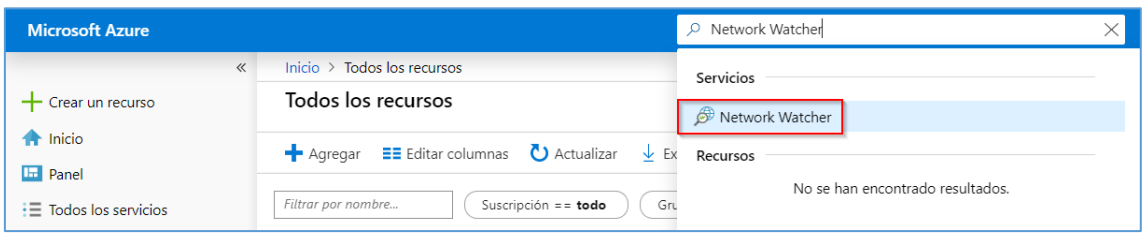


CAPTURA DE PAQUETES

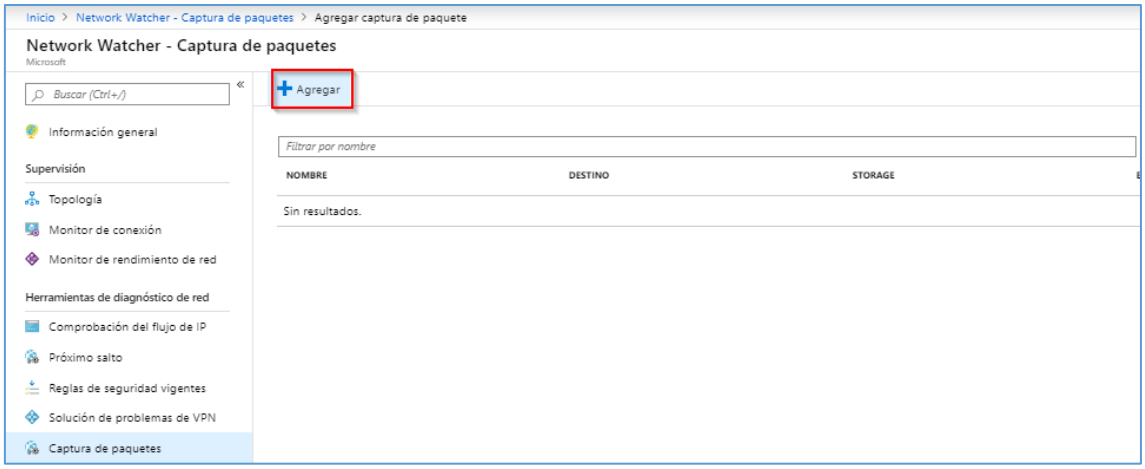
En el caso de que sea necesario capturar todo el tráfico de red que pasa por una máquina específica se puede utilizar el capturador de paquetes de Network Watcher.

Para la configuración, se realizan los siguientes pasos:

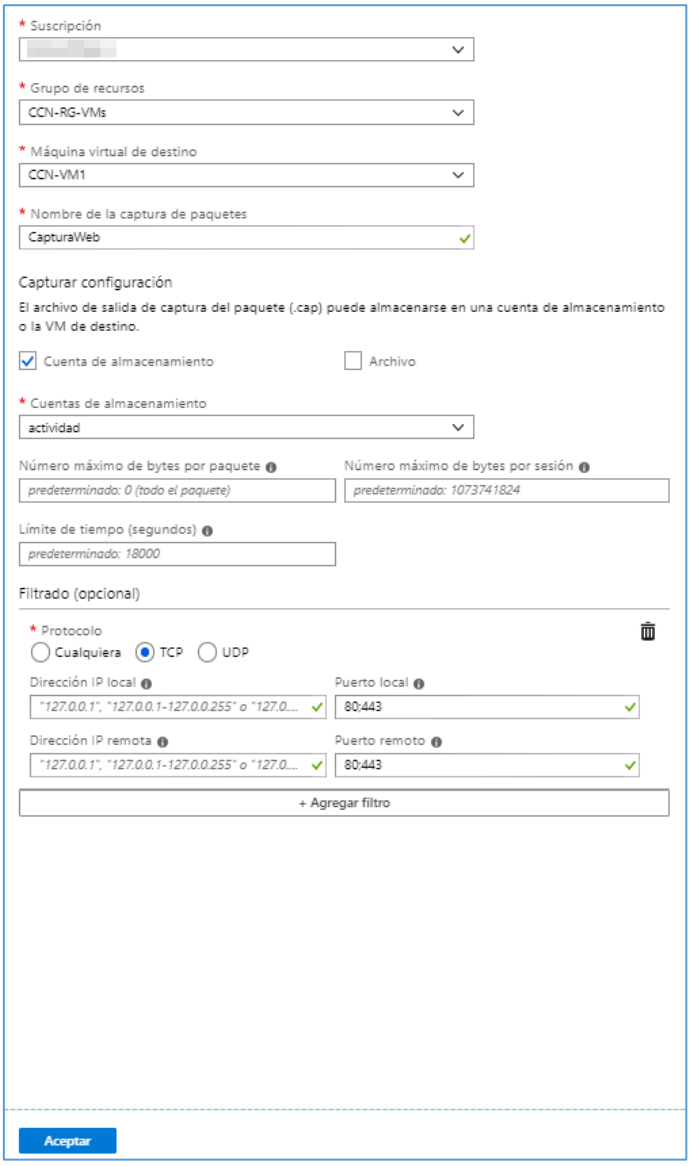
a) Buscar Network Watcher



b) Pulsar [Capturar paquetes/Agregar]



c) Rellenar los siguientes campos:



- **Suscripción** en la que se encuentra la máquina.
- **Grupo de recursos** en el que se encuentra la máquina.
- **Máquina virtual de destino** en la que desea analizar el tráfico.
- **Nombre** de la captura de paquetes.
- **Captar configuración**: Donde se guarda el archivo, se utiliza la cuenta de almacenamiento para logs.
- Nº máximo de bytes por paquetes/por sesión y límite de tiempo se deja por defecto.
- Filtrado: Además se puede filtrar por el origen de los paquetes, el puerto por el que llega el tráfico. Esta parte es opcional

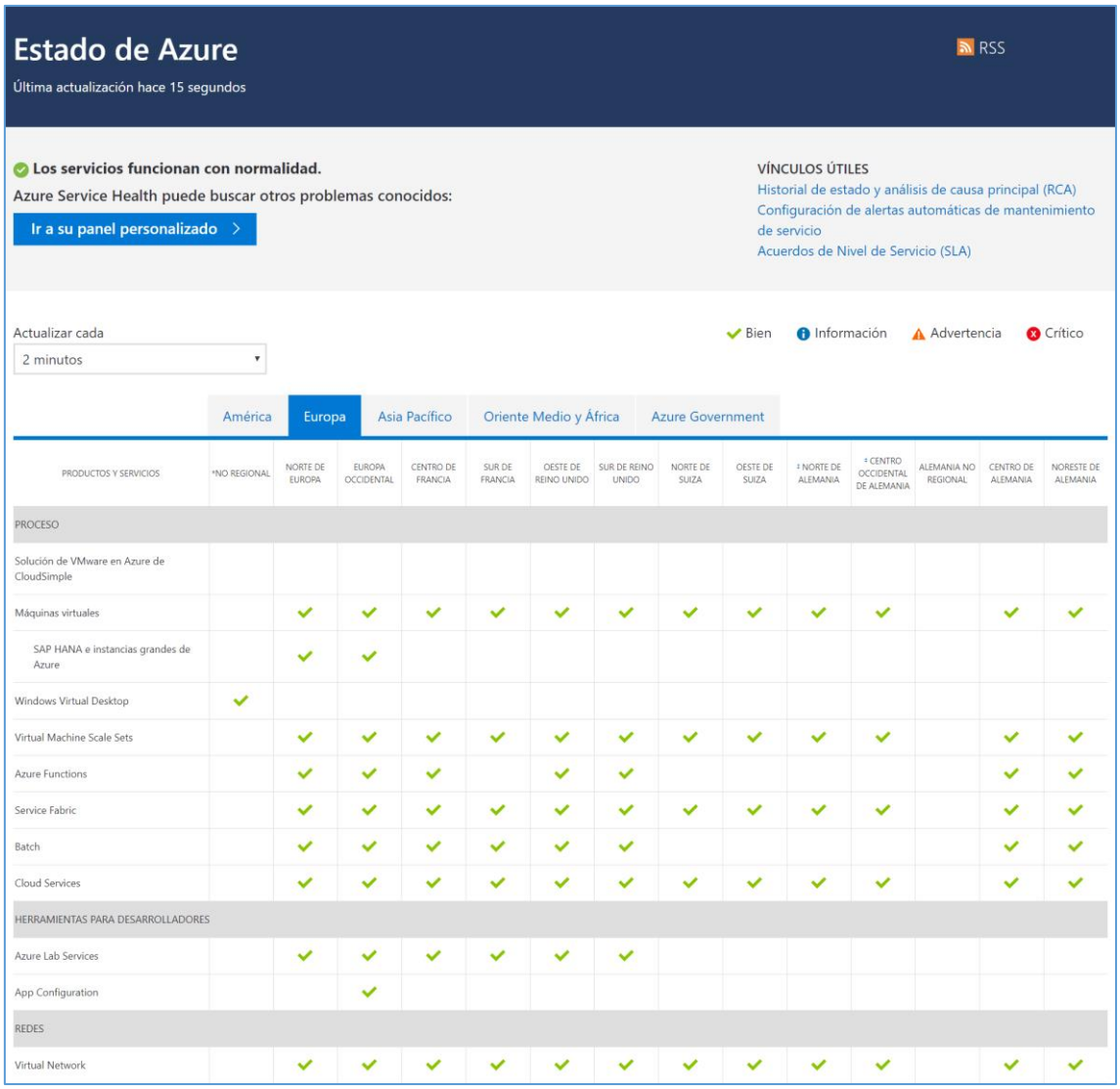
SERVICE HEALTH

Proporciona un estado de los servicios de Azure, proporcionando guía y soporte técnico personalizados cuando aparecen problemas.

Se conforma de tres servicios independientes más pequeños:

- **Estado de Azure:** Informa sobre las interrupciones de servicio en Azure. Es una vista global del estado de todos los servicios y regiones de Azure.

Nota: Para visitar el estado de Azure se utiliza este link: *https://status.azure.com/es-es/status*



Estado de Azure

Última actualización hace 15 segundos

RSS

Los servicios funcionan con normalidad.

Azure Service Health puede buscar otros problemas conocidos:

Ir a su panel personalizado >

VÍNCULOS ÚTILES

Historial de estado y análisis de causa principal (RCA)

Configuración de alertas automáticas de mantenimiento de servicio

Acuerdos de Nivel de Servicio (SLA)

Actualizar cada

2 minutos

Bien Información Advertencia Crítico

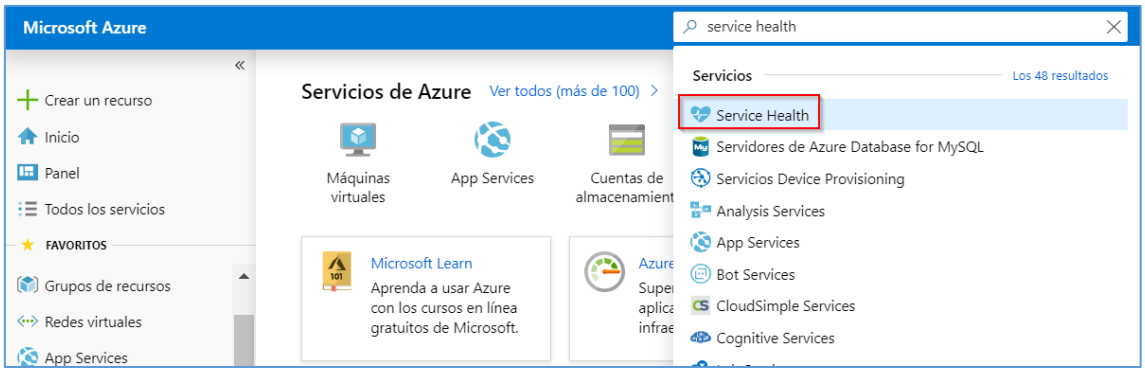
América | Europa | Asia Pacífico | Oriente Medio y África | Azure Government

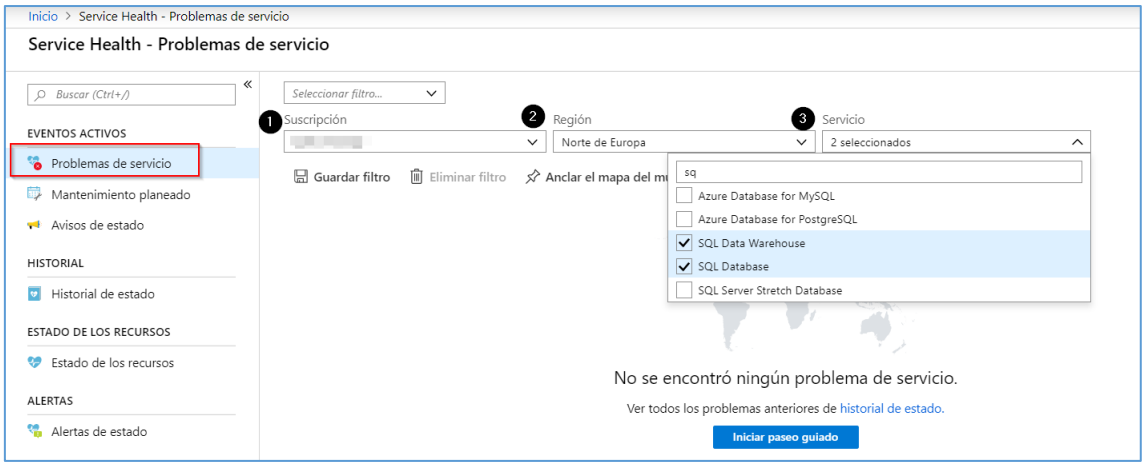
PRODUCTOS Y SERVICIOS	*NO REGIONAL	NORTE DE EUROPA	EUROPA OCCIDENTAL	CENTRO DE FRANCIA	SUR DE FRANCIA	OESTE DE REINO UNIDO	SUR DE REINO UNIDO	NORTE DE SUIZA	OESTE DE SUIZA	‡ NORTE DE ALEMANIA	‡ CENTRO OCCIDENTAL DE ALEMANIA	ALEMANIA NO REGIONAL	CENTRO DE ALEMANIA	NORESTE DE ALEMANIA
PROCESO														
Solución de VMware en Azure de CloudSimple														
Máquinas virtuales		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓
SAP HANA e instancias grandes de Azure		✓	✓											
Windows Virtual Desktop	✓													
Virtual Machine Scale Sets		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓
Azure Functions		✓	✓	✓		✓	✓						✓	✓
Service Fabric		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓
Batch		✓	✓	✓	✓	✓	✓						✓	✓
Cloud Services		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓
HERRAMIENTAS PARA DESARROLLADORES														
Azure Lab Services		✓	✓	✓	✓	✓	✓							
App Configuration			✓											
REDES														
Virtual Network		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓

- **Service Health:** Proporciona una vista personalizada del estado de los servicios y regiones de Azure que están siendo utilizadas.
- **Resource Health (Estado de los recursos):** Proporciona información sobre el estado de los recursos en la nube de forma individual, como podría ser una instancia de máquina virtual, un firewall, etc.

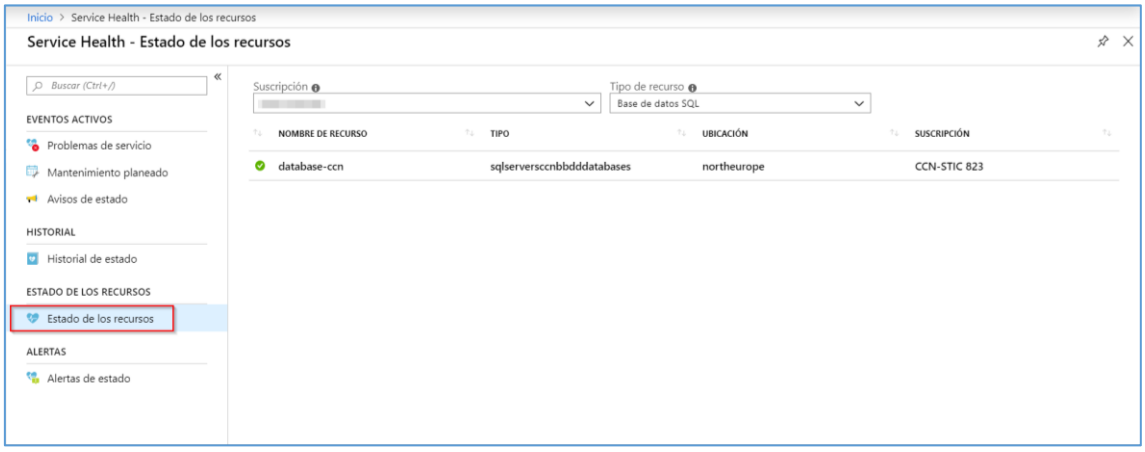
Se puede consultar el Service Health así cómo Resource Health:

a) Buscar Service Health. Pulsar en [Problemas de servicio], seleccionar suscripción, región y el servicio que queremos comprobar. En el ejemplo se comprueba SQL.





b) Para Resource Health pulsar en [Estado de recursos]. Seleccionar suscripción y tipo de recurso.



MICROSOFT DEFENDER FOR CLOUD

Microsoft Defender for Cloud es una plataforma de protección de aplicaciones nativas de la nube (CNAPP) que se compone de medidas y prácticas de seguridad diseñadas para proteger las aplicaciones basadas en la nube frente a diversas amenazas cibernéticas y vulnerabilidades. Defender for Cloud combina las funcionalidades de:

- Una solución de operaciones de seguridad de desarrollo (DevSecOps) que unifica la administración de seguridad en el nivel de código en entornos multinube y varias canalizaciones.

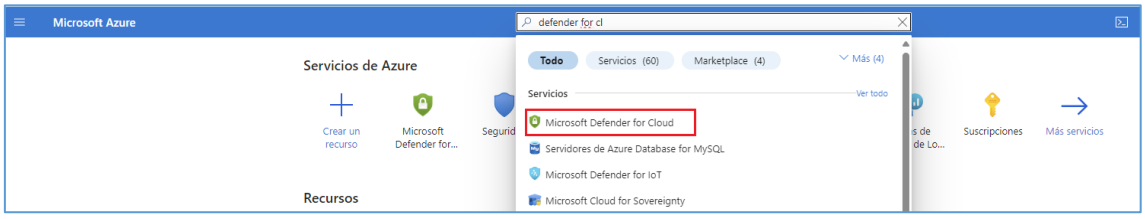
- Una solución de administración de posturas de seguridad en la nube (CSPM) que muestra las acciones que puede realizar para evitar infracciones.
- Una plataforma de protección de cargas de trabajo en la nube (CWPP) con protecciones específicas para servidores, contenedores, almacenamiento, bases de datos y otras cargas de trabajo.

EVALUACIONES CONTINUAS

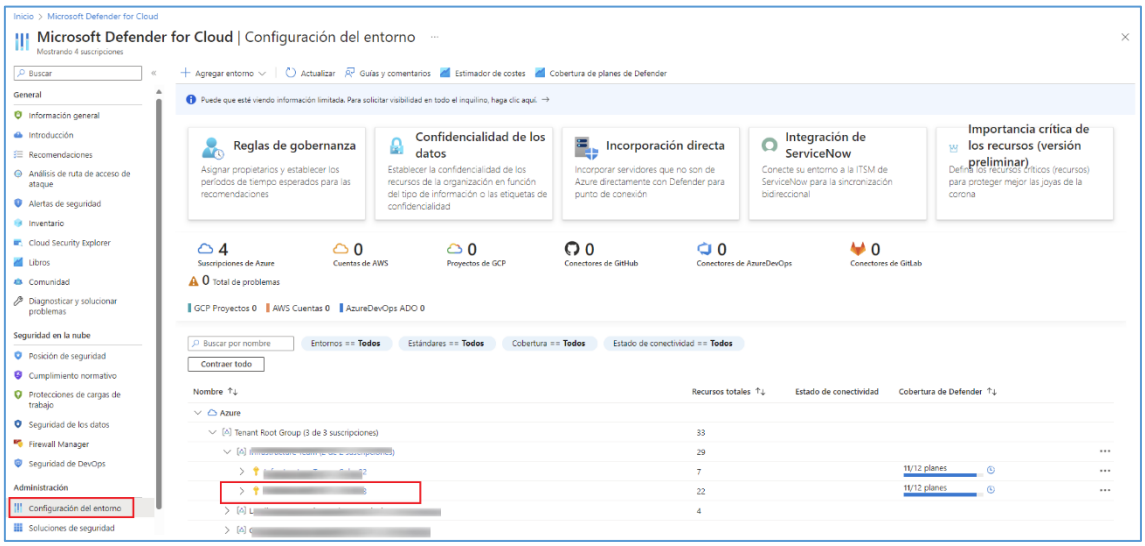
Azure Defender for Cloud siempre está detectando los recursos nuevos que se implementan en las cargas de trabajo y evalúa si están configurados según los procedimientos recomendados de seguridad. Si no es así, se marcan y el usuario recibe una lista de recomendaciones clasificadas por orden de prioridad de lo que debe corregir con el fin de proteger sus servicios.

HABILITACIÓN DE PLANES DE PAGO EN LA SUSCRIPCIÓN

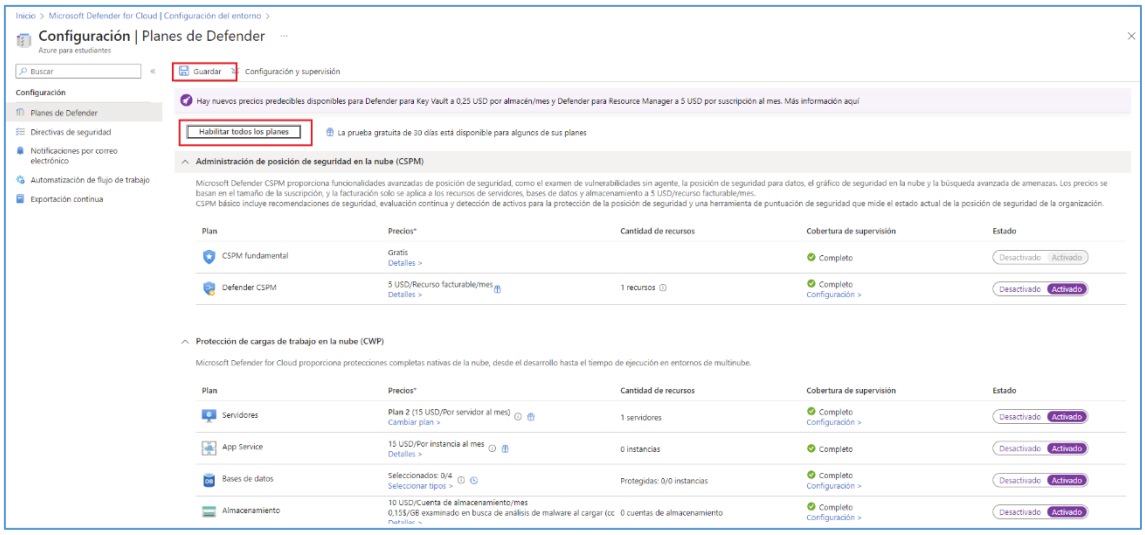
a. Desde el portal de Azure buscar [Microsoft Defender for Cloud].



b. A continuación, pulsar en [Configuración del entorno] y selecciona la suscripción que deseas monitorizar.



c. Seleccionar [Habilitar todos los planes] y [Guardar]. También es posible habilitar los planes individuales deseados como Defender para servidores o Bases de datos.



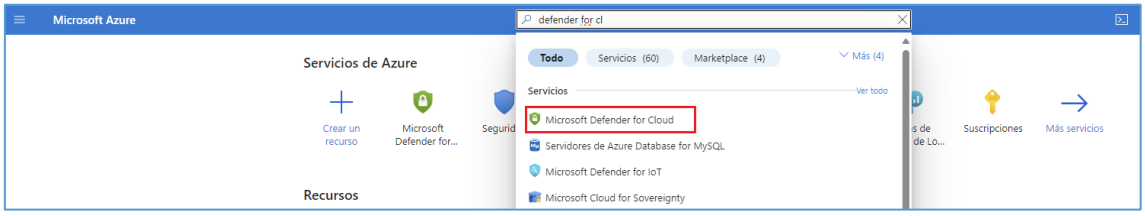
PROTECCIÓN DE LAS MÁQUINAS VIRTUALES

Para garantizar la seguridad de las máquinas virtuales, es posible habilitar el plan de Defender para servidores en Microsoft Defender for Cloud. Este plan proporciona detección de amenazas y protección avanzada para las máquinas que operan con sistemas Windows y Linux en Azure, Amazon Web Services (AWS), Google Cloud Platform (GCP), así como en entornos locales. Defender para servidores minimiza la exposición a amenazas implementando controles de acceso y de aplicación para prevenir actividades malintencionadas.

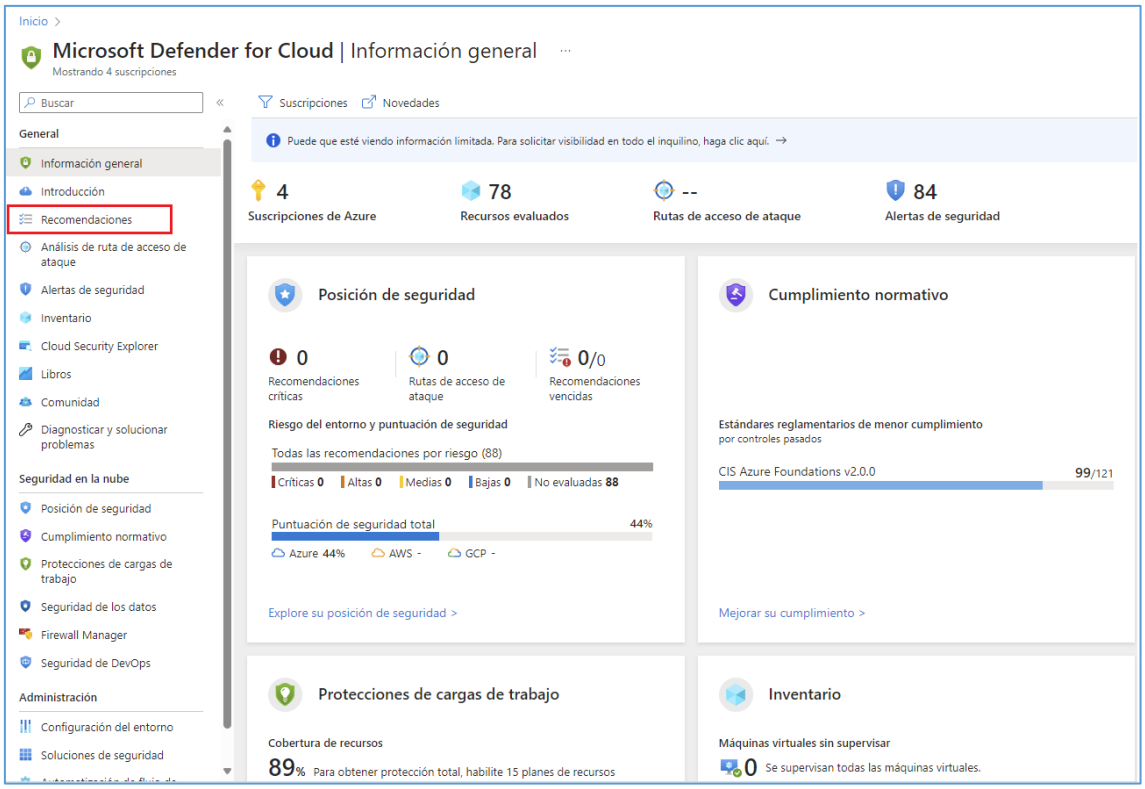
Nota: Puede obtener más información sobre cómo configurar una directiva de acceso a las máquinas virtuales Just-In-Time y una directiva de control de aplicación en el siguiente enlace: *https://learn.microsoft.com/es-es/azure/defender-for-cloud/tutorial-protect-resources*

BÚSQUEDA DE RECOMENDACIONES

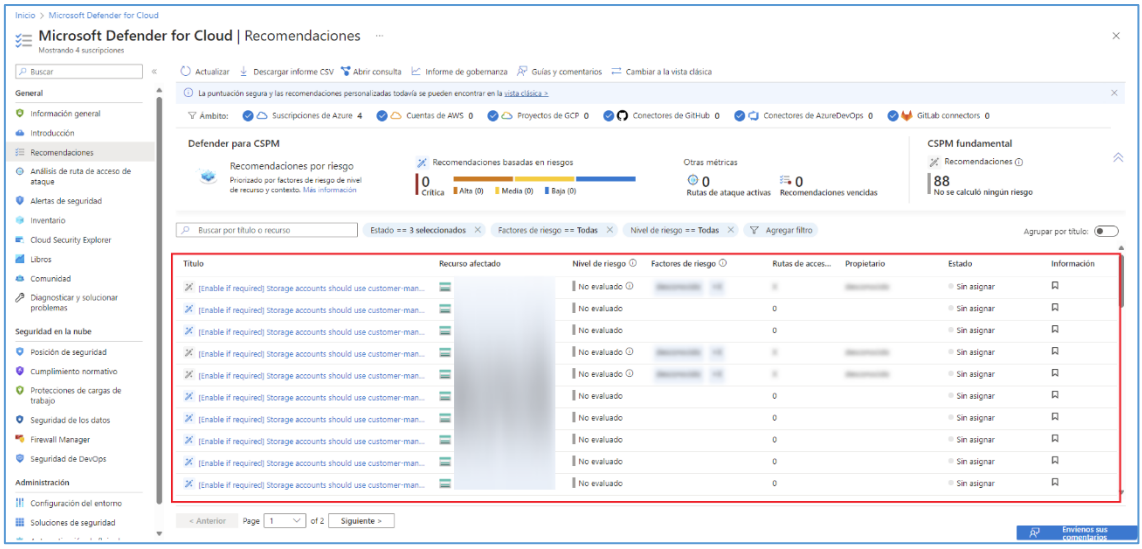
1. Buscar [Microsoft Defender for Cloud].



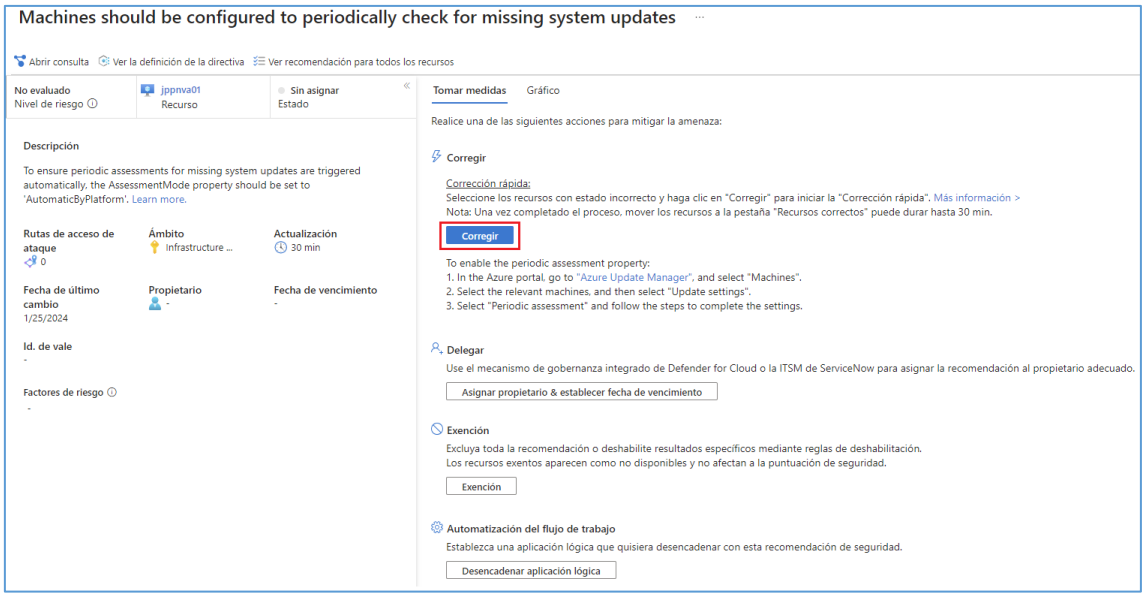
2. Pulsar en [Recomendaciones].



Nota: *En este panel se muestra todas las recomendaciones encontradas para sus servicios.*



3. Pulsar en una de las recomendaciones y [Corregir].

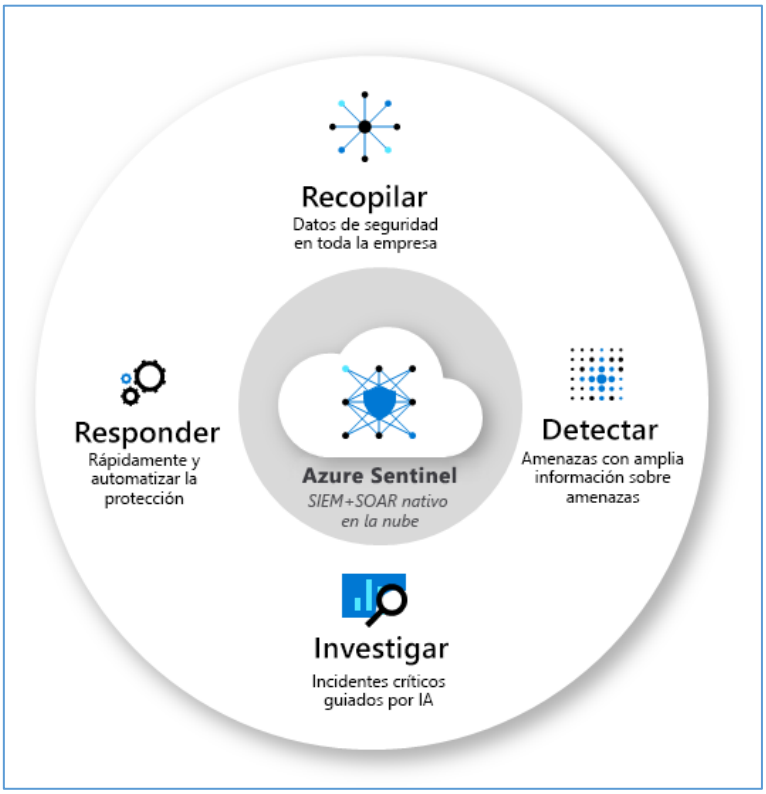


Nota: *Este proceso se puede realizar para todos sus servicios.*

MICROSOFT SENTINEL

Microsoft Sentinel es una solución de administración de información de seguridad y respuesta automatizada de orquestación de seguridad escalable y nativa en Azure. Con este servicio se proporciona un análisis de seguridad y una inteligencia frente amenazas siendo una solución que permite detectar alertas, amenazas y ofrecer una respuesta.

Microsoft Sentinel incorpora de forma nativa Log Analytics y Logic Apps.



Recopilar datos en nube: De aplicaciones, dispositivos, usuarios y de toda la infraestructura, tanto local como en distintas nubes.

Detectar amenazas y reducir falsos positivos mediante el análisis y la inteligencia de amenazas de Microsoft.

Investigar amenazas con inteligencia artificial para buscar actividades sospechosas aprovechando el trabajo de ciberseguridad de Microsoft.

Responder con la orquestación y automatización de tareas comunes integradas.

CONECTORES DE DATOS DE MICROSOFT SENTINEL

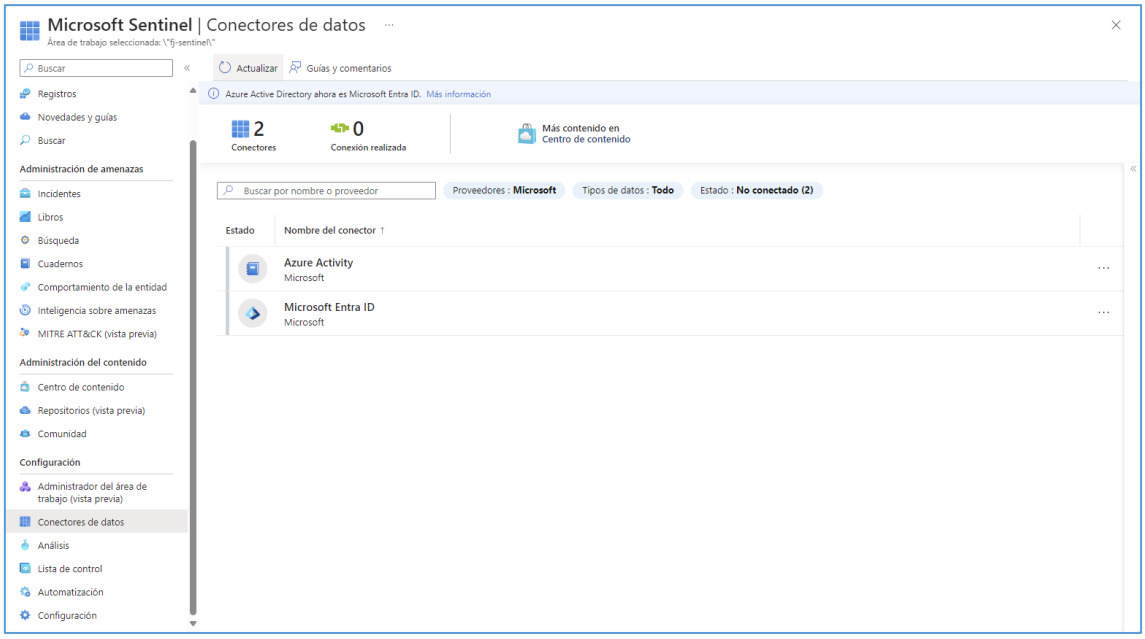
Para conectar fuentes de datos se deben conectar con los orígenes de seguridad. Se disponen de conectores para soluciones de Microsoft que se encuentran disponibles de manera inmediata y proporcionan información en tiempo real, como Microsoft Entra ID.

Además, existen conectores para soluciones que no son de Microsoft.

Para ver los conectores se realizan los siguientes pasos:

a. Buscar Microsoft Sentinel.

b. Pulsar en [Conectores de datos].



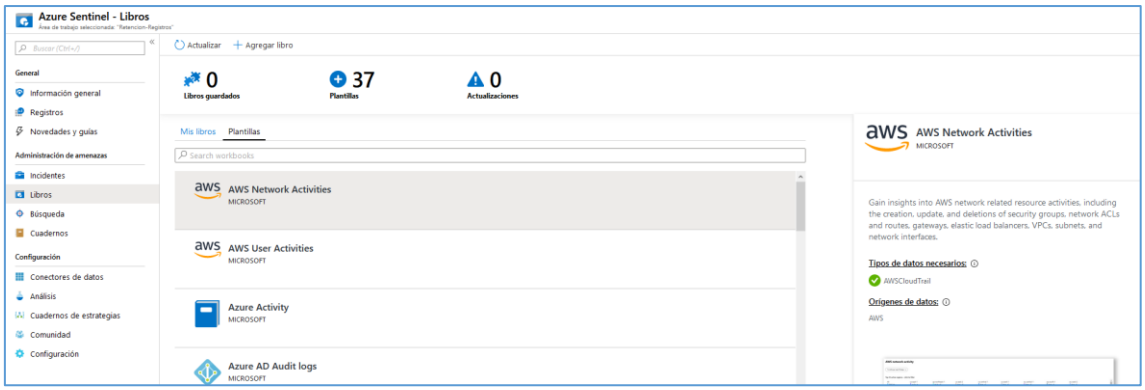
WORKBOOKS

Una vez conectados los orígenes de datos se pueden supervisar los datos mediante la integración con los libros de Azure Monitor, lo que proporciona versatilidad al crear libros personalizados.

Microsoft Sentinel permite crear libros personalizados en los datos, incluyendo también plantillas de libro integradas que permiten obtener información rápidamente de los datos.

Para ver los workbooks (Libros en el portal) se realizan los siguientes pasos:

a) Buscar Microsoft Sentinel
b) Pulsar en [Libros].



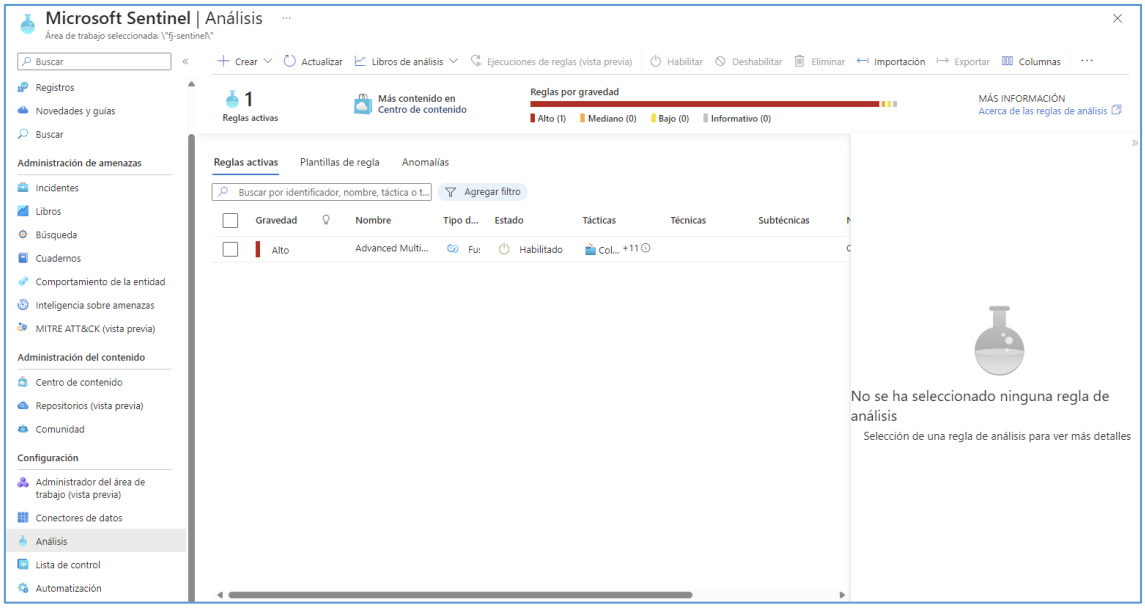
ANÁLISIS

Microsoft Sentinel analiza las alertas para que sean relacionadas con los incidentes. Los **incidentes** son grupos de alertas relacionadas, que juntas, crean una posible amenaza que se puede investigar y resolver.

Además, se proporcionan reglas de aprendizaje automático para asignar el comportamiento de red y buscar anomalías en los recursos.

Para ver las reglas de análisis se realizan los siguientes pasos:

a) Buscar Microsoft Sentinel
b) Pulsar [Análisis].



AUTOMATIZACIÓN Y ORQUESTACIÓN

Con Microsoft Sentinel se pueden automatizar las tareas con el fin de simplificar la orquestación de la seguridad con cuadernos de estrategia integrados con los servicios de Azure. Se encuentra construida sobre una Logic App lo que proporciona una

arquitectura extensible que permite la automatización escalable a medida que emergen nuevas tecnologías y amenazas.

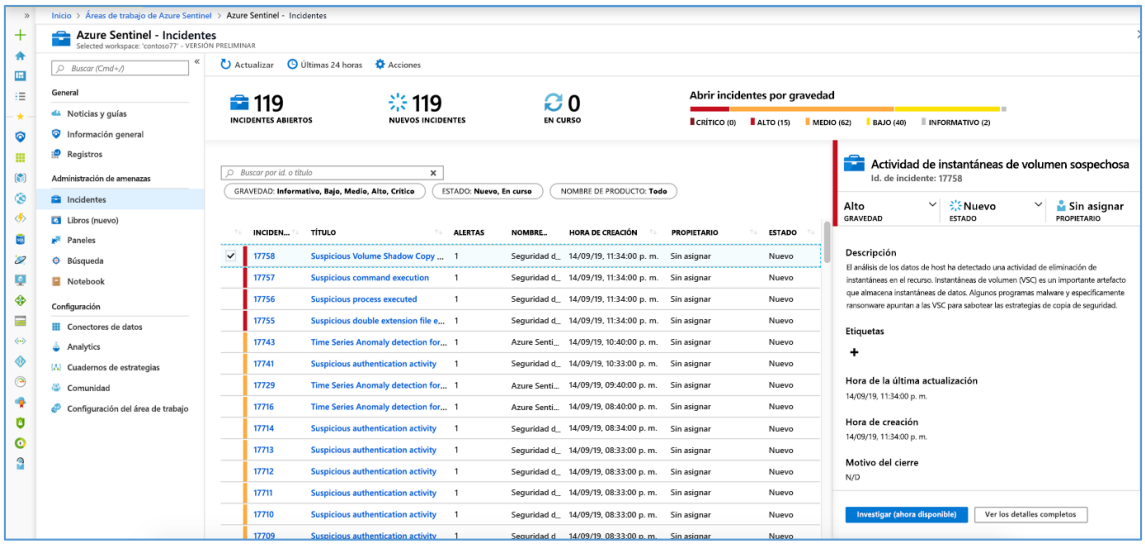
Para crear un cuaderno de estrategia se puede elegir de una galería creciente de cuadernos de estrategia integrados, que **incluyen** más de 200 conectores para los servicios de Azure.

INVESTIGACIÓN

Las herramientas de investigación profundas de Microsoft Sentinel ayudan a conocer el ámbito de una posible amenaza de seguridad. Se puede elegir una entidad en el gráfico interactivo para explorar en profundidad la entidad y sus conexiones para llegar a la causa principal de la amenaza.

Para consultar esta sección es necesario seguir los siguientes pasos:

a) Buscar Microsoft Sentinel
b) Pulsar en [Incidentes], y seleccionar el incidente para ver el análisis.



COMUNIDAD

La comunidad de Microsoft Sentinel es un recurso muy eficaz para la detección y la automatización de amenazas. Se agregan nuevos libros, cuadernos de estrategia, consultas de búsqueda en un repositorio de GitHub. (https://github.com/Azure/Azure-Sentinel)

Nota: Para más información sobre Azure Sentinel consultar: https://docs.microsoft.com/es-es/azure/sentinel/

3.2 MEDIDAS DE PROTECCIÓN

3.2.1 PROTECCIÓN DE LAS COMUNICACIONES

3.2.1.1 PERÍMETRO SEGURO

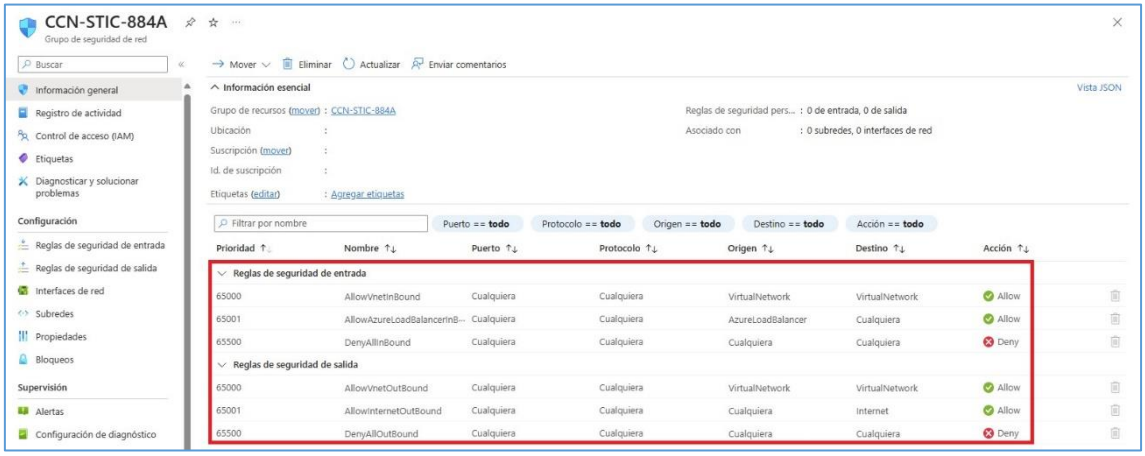
SECURIZACIÓN DE SUBREDES

INTRODUCCIÓN A LOS NSG

Los **Grupos de Seguridad de Red** (NSG) son un firewall de capa 4 que permiten filtrar los puertos de origen y destino por protocolo (TCP/UDP/ICMP), pero no por contenido. Se pueden aplicar en dos niveles:

- **Tarjeta de red (NIC):** Las reglas solo afectan a la maquina en la que se aplica el NSG. Se pueden aplicar también para máquinas con varias NICs (Multi-Hommed)
- **Subred:** Las reglas afectan a todas las máquinas que se encuentran en la subred.

Todos los NSG creados tienen creadas seis reglas por defecto, 3 inbound (tráfico de entrada), 3 outbound (tráfico de salida). Estas reglas no se pueden modificar ni eliminar. Tienen prioridades muy elevadas para que sean siempre las últimas en aplicarse.



La regla entrante con prioridad 65000 permite que las máquinas que se encuentren en la misma VNet puedan comunicarse entre sí. La regla entrante de prioridad 65001 permite el acceso a la máquina desde un balanceador de Azure, Azure Load Balancer.

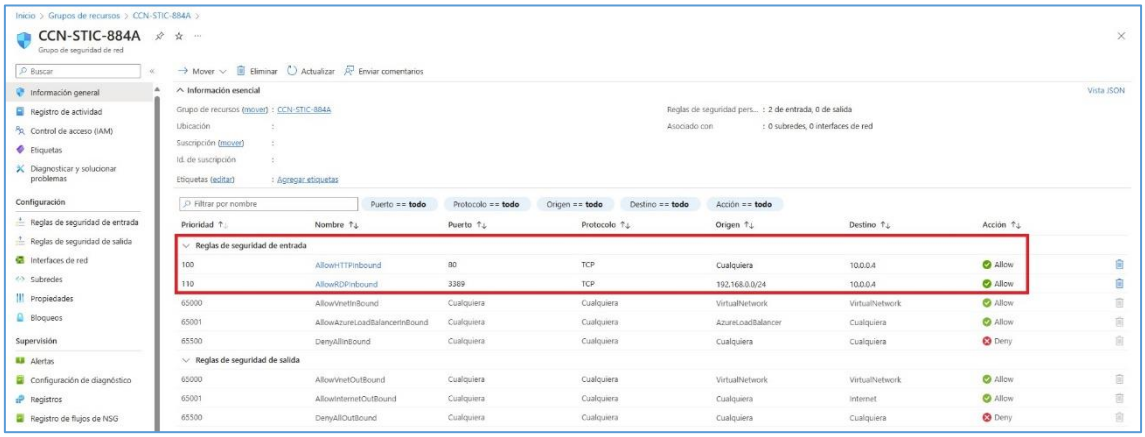
Por último, nos encontramos con una regla entrante 65500 que bloquea cualquier otro tráfico que no haya sido permitido de forma explícita en una regla con un valor de prioridad inferior.

En cuanto a las reglas salientes (outbound), está permitido el tráfico desde la máquina virtual a cualquier otra máquina en la misma VNet y también desde la máquina virtual hacia Internet.

Para ver el registro de actividad se puede consultar el apartado de monitorización.

CÓMO FUNCIONA UN NSG

Para explicar el funcionamiento se añade al ejemplo anterior dos reglas de entrada, una para permitir el tráfico por el puerto 80, y otra por el 3389.



Cuando llega un paquete al NSG se aplican las reglas en orden creciente de prioridad. La primera regla cuyas condiciones se cumplan aplica la acción y el resto de las reglas no se aplican a ese paquete.

El comportamiento de cualquier paquete que pase por el NSG sería el siguiente:

a) Si llega un paquete dirigido al puerto 80 con IP origen 10.10.0.22 y con IP destino 10.10.0.50 se permite la entrada. En caso contrario, se pasa a la siguiente regla.
b) Si el paquete va dirigido al puerto 3389 se le permite la entrada. En caso contrario, pasa a la siguiente regla.
c) Si el paquete viene de un Azure Load Balanced, se le permite la entrada. En caso contrario, se pasa a la siguiente regla.
d) Si el paquete no cumple ninguna condición de las reglas anteriores se cumple la última regla, se deniega el acceso.

En el momento en el que un paquete cumpla con una regla no sigue procesando y se cumple la regla.

REGLAS NSG

Un NSG puede tener desde cero reglas o tantas como sean necesarias siempre que estén dentro de los límites de Azure. Cada regla tiene las siguientes propiedades:

- **Nombre**: Único dentro del mismo NSG. Límite 80 caracteres. No se puede usar los caracteres guion medio, guion bajo, punto, coma.
- **Prioridad**: Valores entre 100-4096. Las reglas se procesan en orden de prioridad, desde el número con menor prioridad hasta el de mayor prioridad.
- **Origen y destino**: Puede ser cualquiera (*), una IP individual, un rango de IP o una etiqueta de servicio.
- **Protocolo**: Pueden ser TCP, UDP, ICMP u cualquiera.

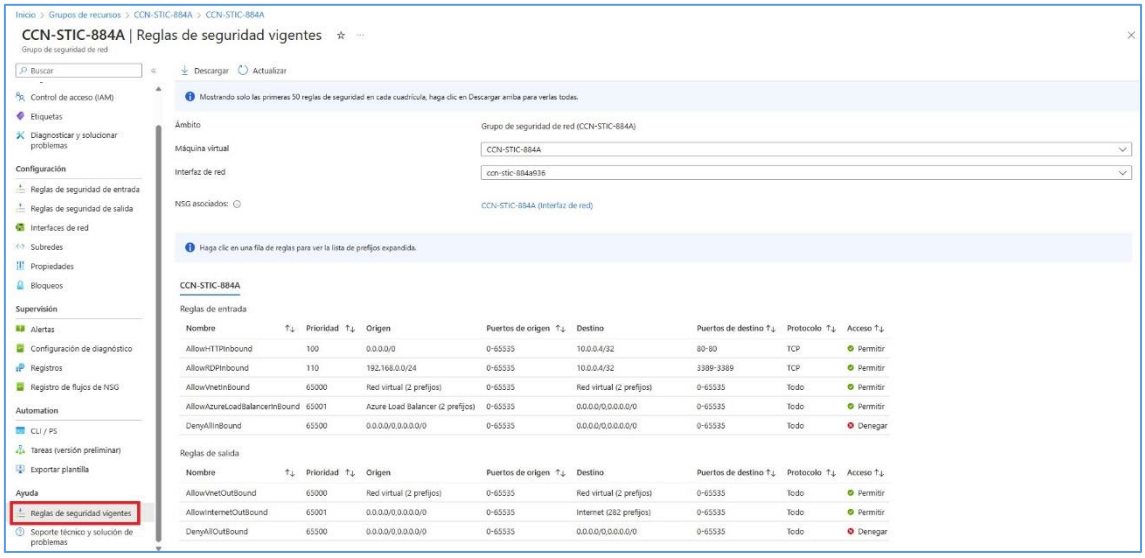
- **Dirección**: Se aplica el tráfico tanto entrante como saliente.
- **Intervalo de puertos**: Se puede especificar un puerto individual (80) o un intervalo de puertos (20-22).
- **Acción**: Se puede seleccionar como acciones Permitir o Denegar.

Nota: Para más información: https://docs.microsoft.com/es-es/azure/virtual-network/security-overview

REGLAS EFECTIVAS NSG

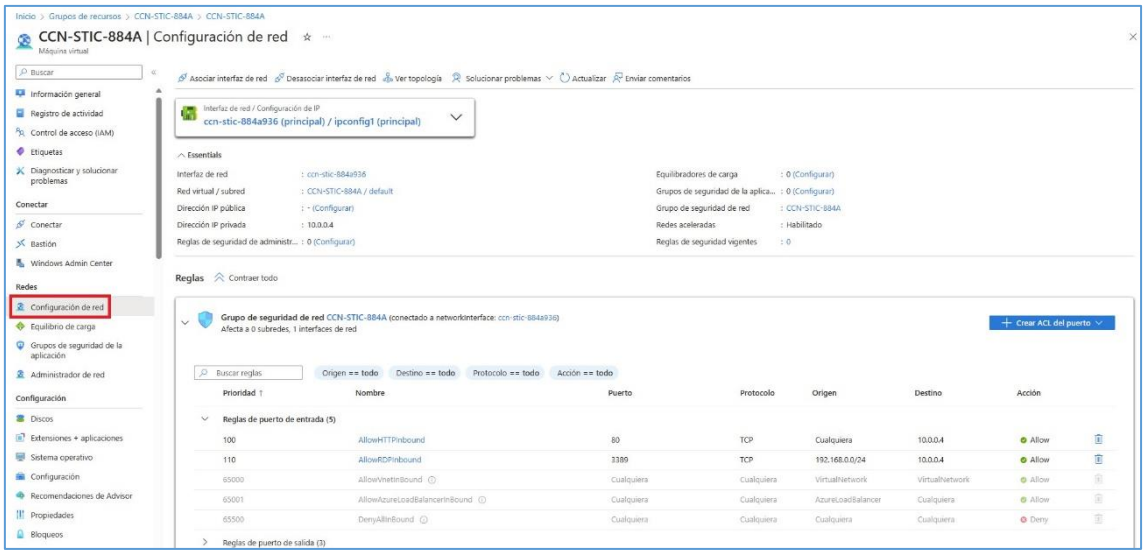
Cómo se mencionó en el apartado introductorio, un NSG puede estar vinculado a una o varias NIC y/o una o varias subredes, por lo que una máquina puede verse afectada por dos NSG al mismo tiempo.

Para ver las reglas efectivas que le afecta a un servidor puede utilizar la opción [Reglas de seguridad vigentes] dentro del NSG que se desea comprobar.



En máquinas virtuales se ven las máquinas en las que tiene aplicado este NSG, elegir lo que se va a comprobar. Para que se muestre las reglas la máquina debe estar encendida.

También se pueden ver las reglas efectivas si nos vamos a la máquina virtual, a la opción de redes, se muestran las reglas efectivas que tiene el servidor, y qué NSG se lo está aplicando.



LÍMITES NSG

Los límites por defecto que existen por suscripción son:

Recurso	Limite por defecto
Redes virtuales (vNet)	1000
Subredes por vNet	3000
Emparejamientos por vNet	100
Servidores DNS por vNet	20
IPs privadas por vNet	65536
IPs privadas por tarjeta de red (NIC)	256
IPs privadas por máquina virtuales	256
Flujos TCP o UDP por NIC	500000
Tarjetas de red	65536
Grupos de seguridad de red (NSG)	5000
Reglas por NSG	1000
IPs y rangos de IPs de origen/destino	4000
Grupos de seguridad de aplicación (ASG)	3000
Grupos de seguridad de aplicación por NIC	20
ASGs totales en reglas de un NSG	100
Tablas de rutas	200
Rutas por tabla de rutas	400
Certificados VPN Point-to-Site	20
Virtual Network TAPs	100

Nota: Para más información consultar: https://learn.microsoft.com/es-es/azure/azure-resource-manager/management/azure-subscription-service-limits#networking-limits

DESPLIEGUE DE UN NSG.

A continuación, se despliega un NSG tanto desde el portal de Azure como desde Powershell:

a) En el buscador escribimos [Grupos de seguridad de red].

b) Pulsar sobre [Crear].

c) A continuación, se debe completar los campos:

- **Suscripción**: Nombre de la suscripción donde se despliega el recurso,
- **Grupo de recursos**: Nombre del grupo del recurso donde se crea el recurso.
- **Nombre**: Apodo del recurso. No se puede modificar.
- **Región**: Localización donde se despliega el recurso. Se recomienda la región de **España Central**.

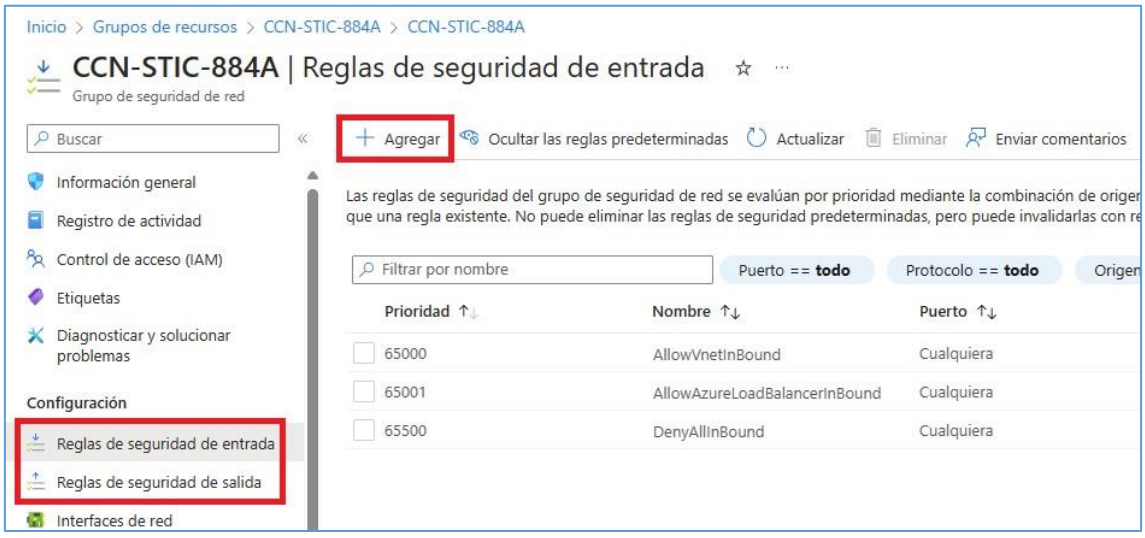
d) Pulsar sobre [Revisar y crear / Crear].

Podemos crear el grupo de seguridad de red usando comandos de consola utilizando la tecnología de PowerShell y haciendo uso de la librería de Az.

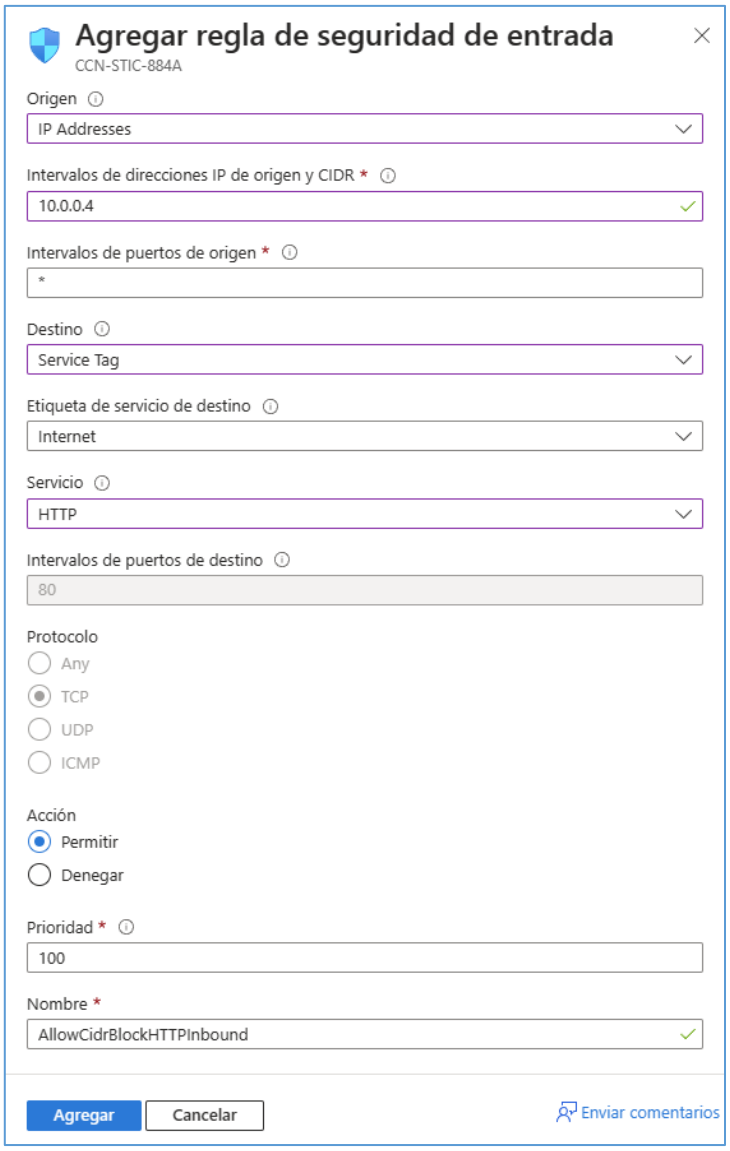
```
#  PS C:\> New-AzNetworkSecurityGroup -Name $Name -ResourceGroupName
   $ResourceGroupName -Location "Spain Central"
```

AÑADIR REGLAS A UN NSG

a) En el NSG que se desee configurar, pulsar sobre [Reglas de seguridad de entrada o de salida / Agregar]:



b) Rellenar el formulario de la definición de la regla:



Origen / Destino (Intervalo de direcciones IP, Etiqueta de servicio o Grupo de seguridad de aplicación), **intervalos de puertos** de Origen / Destino, **protocolo**, **acción**, **prioridad**, **nombre** y descripción (Opcional). Estos campos se encuentran explicados en el punto [3.2.1.1 Perímetro seguro/Securización de subredes/Reglas NSG].

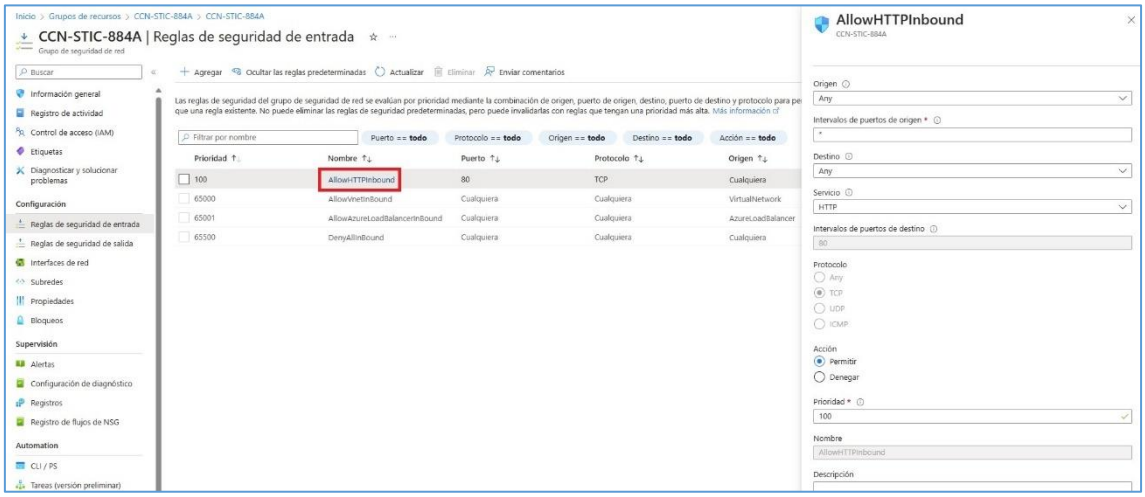
Se pueden crear nuevas reglas utilizando la tecnología de PowerShell y haciendo uso de la librería de Az.

```
#   PS C:\> $Nsg = Get-AzNetworkSecurityGroup -Name $Name -ResourceGroupName
    $ResourceGroupName

#   PS C:\> $Nsg | Add-AzNetworkSecurityRuleConfig -Name $RuleName -
    Description "Permitir puerto" -Access "Allow" -Protocol "TCP" -Direction
    "Inbound" -Priority 100 -SourceAddressPrefix "*" -SourcePortRange "*" -
    DestinationAddressPrefix "*" -DestinationPortRange "*"
```

ACTUALIZAR REGLAS NSG

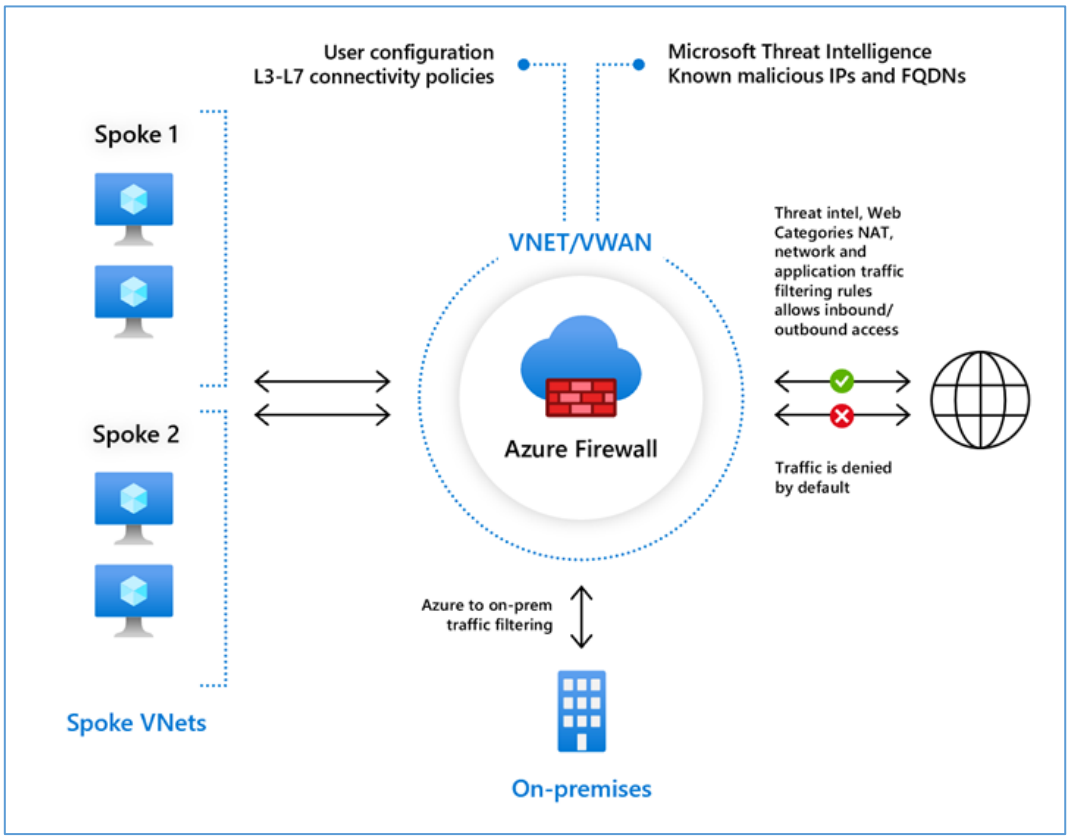
a) Pulsar sobre la regla que se desea modificar y modificar los campos.



AZURE FIREWALL

Anteriormente se ha mostrado en la guía la opción por defecto que se utiliza para controlar el tráfico entre las distintas redes.

Existe otra herramienta en Azure llamada **Azure Firewall**. A diferencia de los NSG, Azure Firewall es un firewall que se presenta como servicio que proporciona protección a nivel de red y de aplicación en todas las suscripciones y redes virtuales.

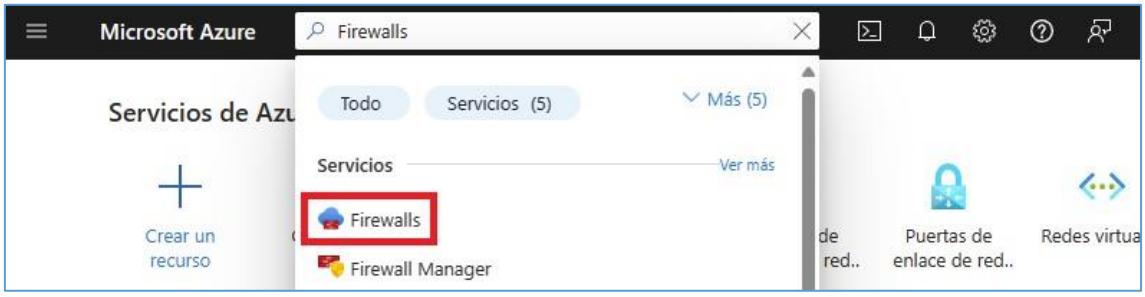


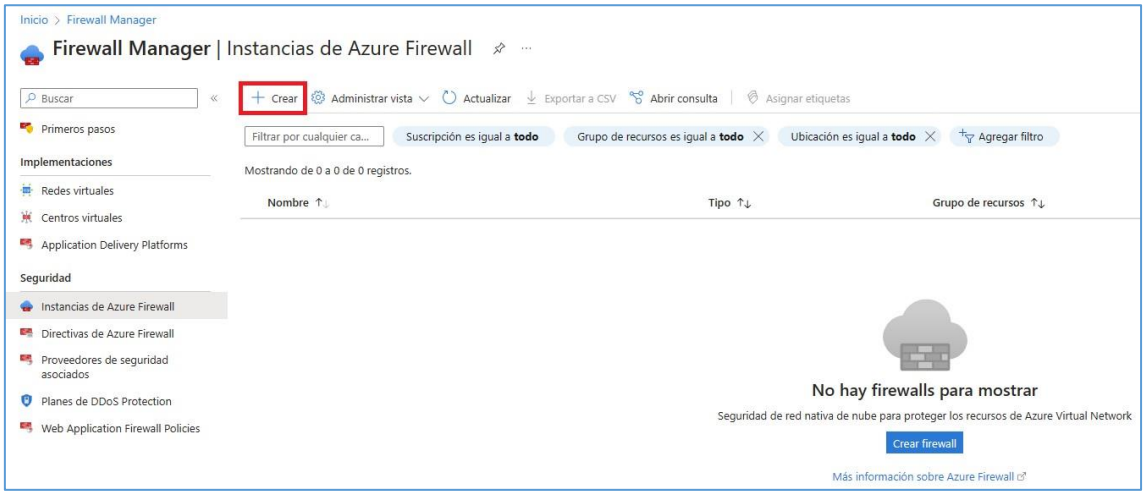
Además, incorpora las siguientes características:

- **Alta disponibilidad**: Sin configuración alguna del usuario, Microsoft asegura una disponibilidad del 99,95% del servicio, y si lo configuramos con las **zonas de disponibilidad**, aumenta hasta el 99,99%.
- **Escalabilidad**: Se puede escalar verticalmente todo lo que sea necesario para acoger los flujos de red que sean necesarios.
- **Filtrado por FQDN de aplicación**: Permite limitar el tráfico por protocolo HTTP/s en una lista de dominios.
- **Reglas de filtrado de tráfico de red**: Permite crear reglas clásicas de capa 3 y 4.
- **Información sobre amenazas**: Utilizando inteligencia sobre amenazas, se puede habilitar el alertado inteligente y que deniegue tráfico desde y hacia dominios y direcciones IP.
- **Proxy DNS**: Procesar y reenviar peticiones de DNS, fundamental para el filtrado por FQDN.
- **DNS personalizado**: Permite utilizar el servicio como servidor de DNS.
- **Tunelación forzada**: Forzar a que todo el tráfico tenga que pasar por el Firewall para poder permitirlo o restringirlo.

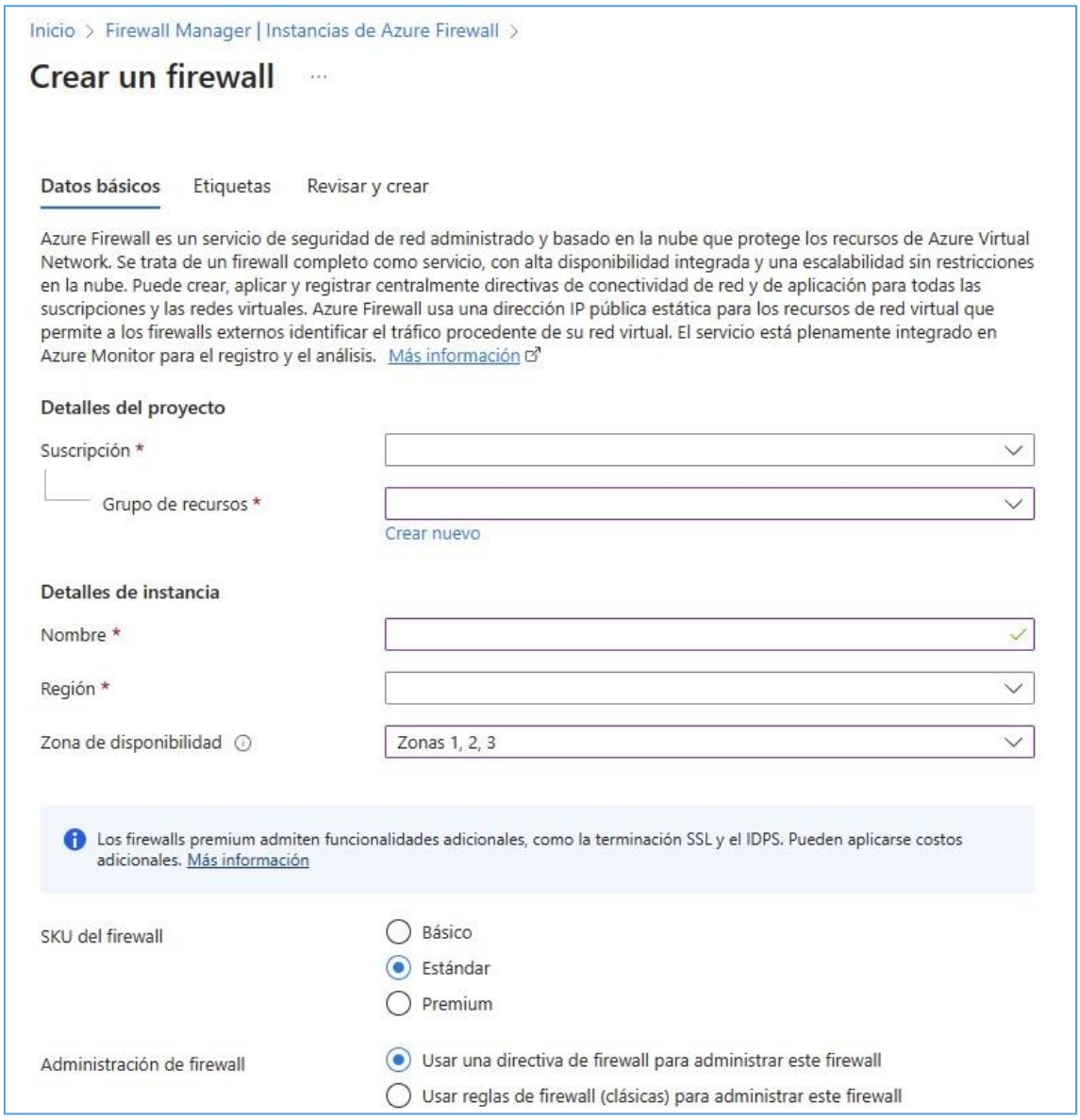
CONFIGURACIÓN

a) En el buscador escribimos [Firewalls / Crear].

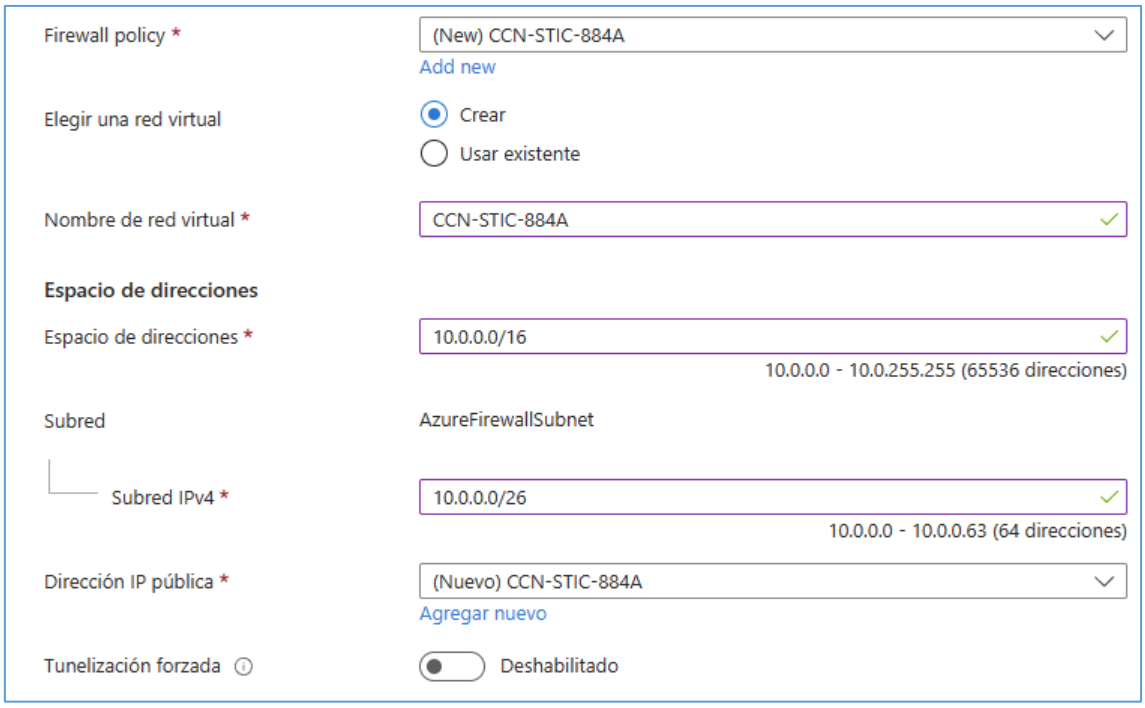




b) Rellenar el formulario de [Datos básicos].



- **Suscripción**: Nombre de la suscripción donde se despliega el recurso.
- **Grupo de recursos**: Nombre del grupo del recurso donde se crea el recurso.
- **Nombre**: Apodo del recurso. No se puede modificar.
- **Región**: Localización donde se despliega el recurso. Se recomienda la región de **España Central**.
- **Zona de disponibilidad**: Seleccionar las 3 zonas.
- **Sku del firewall**: Seleccionar el tamaño estándar.
- **Administración de firewall**: Seleccionar "Usar una directiva de firewall para administrar este firewall.



- **Firewall policy**: Nombre del recurso directiva que usara el Azure Firewall.
- **Elegir una red virtual**: Se puede crear o seleccionar una existente que cumpla con los requisitos del Azure Firewall.
- **Nombre de red virtual**: Nombre de la red virtual donde desplegar el Firewall.
- **Espacio de direcciones**: Si se decide crear la red, se le tiene que asignar un rango de direcciones.
- **Subred IPv4**: La subred virtual que usara el Azure Firewall, debe tener mínimo un rango /26.
- **Dirección IP pública**: Se puede crear o seleccionar una existente que cumpla con los requisitos del Azure Firewall.
- **Tunelación forzada**: Seleccionar “Deshabilitado”.

c) Pulsar sobre [Revisar y crear / Crear].

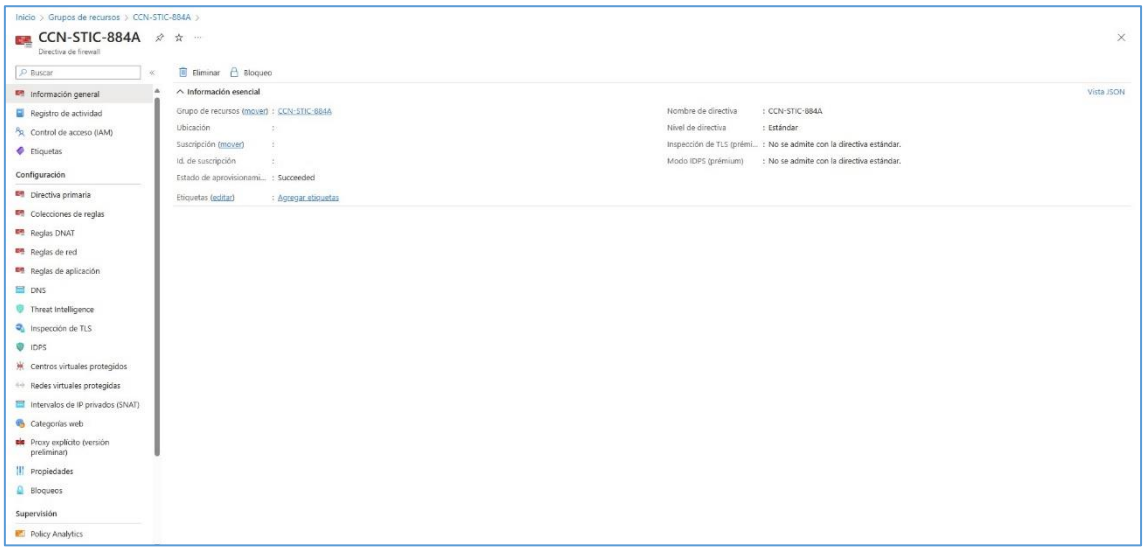
REGLAS AZURE FIREWALL

- **Reglas de red:** Reglas de filtrado de red para permitir o denegar por dirección IP de origen y destino, puerto y protocolo.
- **Reglas de aplicación:** Se realizan a través de etiquetas FQDN, que representan al servicio en Azure, permiten el tráfico desde un servicio de Azure a través del Firewall. Para consultar más información: https://docs.microsoft.com/es-es/azure/firewall/fqdn-tags
- **Reglas NAT:** Todas las direcciones IP de tráfico de red virtual salientes se convierten a direcciones IP públicas de Azure Firewall. Se puede identificar y permitir el tráfico que se origina en la red virtual y se dirige a los destinos remotos de Internet.

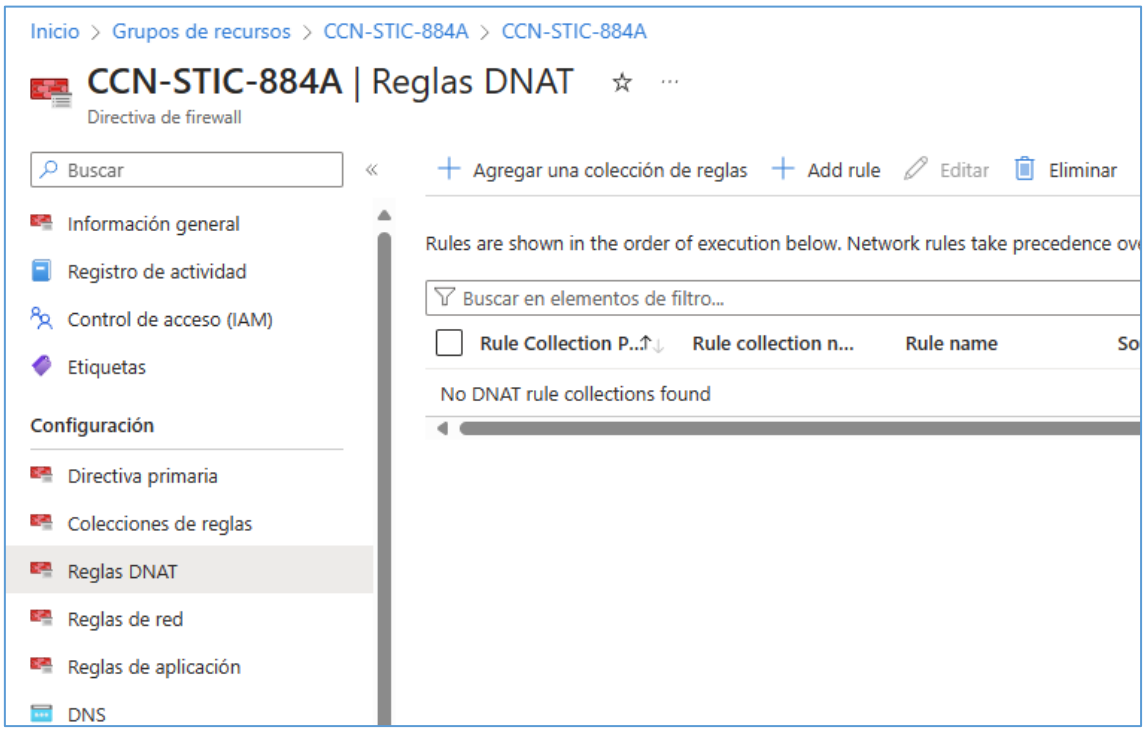
CREAR/MODIFICAR REGLAS AZURE FIREWALL

Para poder añadir o modificar las reglas de filtrado de tráfico, se debe localizar la Directiva de firewall, que es donde se gestionan las reglas.

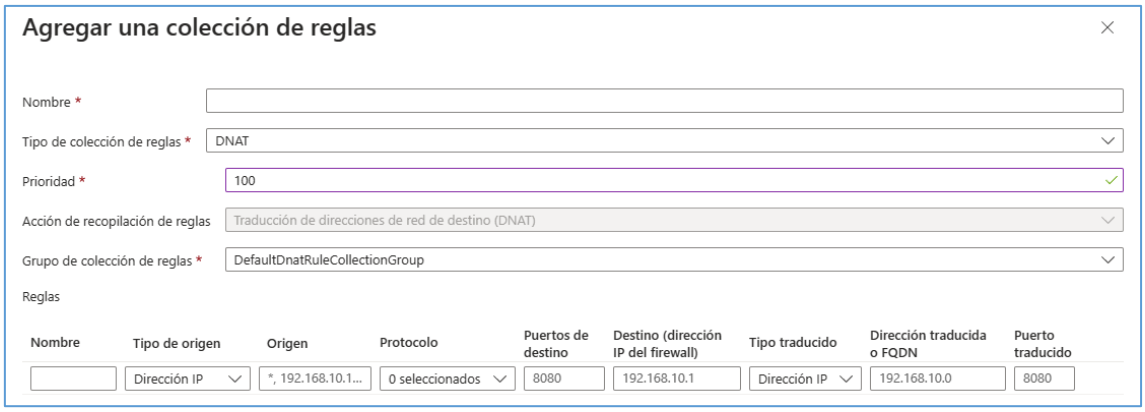
a) Seleccionar la [Directiva de firewall] que se desea configurar:



b) Pulsar sobre [Reglas DNAT, de red, de aplicación / Agregar una colección de reglas]:



c) Rellenar el formulario de la nueva regla:

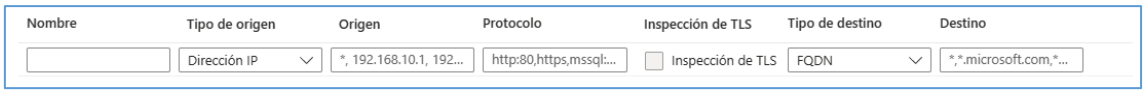


- **Nombre**: Apodo de la colección de reglas.
- **Tipo de colección de reglas**: Tipo de colección de reglas (Red, DNAT, Aplicación).
- **Prioridad**: Nivel de prioridad de la colección. Entre 100 y 65000.
- **Acción de recopilación de reglas**: Permitir o Denegar (No aplica para DNAT).
- **Grupo de colección de reglas**: Nombre del grupo de colección de reglar donde guardar la colección.

La configuración de las Reglas DNAT es:

- **Nombre**: Apodo de la regla.
- **Tipo de origen**: Definir el tipo de origen (Dirección IP y Grupo de IP)
- **Origen**: Dirección o rango IP de origen.
- **Protocolo**: Se permite TCP o UDP.
- **Puerto de destino**: Puerto que consume el cliente de origen.
- **Dirección (dirección IP del firewall)**: IP pública del firewall por la que se expone la regla de DNAT.
- **Tipo traducido**: Dirección IP o FQDN.
- **Dirección traducida o FQDN**: Dirección IP o FQDN al que se traduce.
- **Puerto traducido**: Puerto al que se traduce.

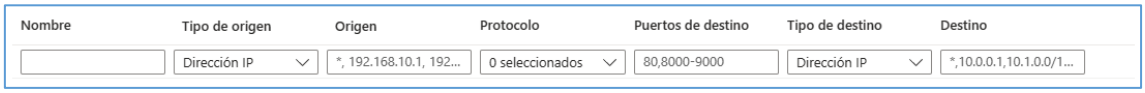
La configuración de las Reglas de aplicación es:



- **Nombre**: Apodo de la regla.
- **Tipo de origen**: Definir el tipo de origen (Dirección IP y Grupo de IP)
- **Origen**: Dirección o rango IP de origen.

- **Protocolo**: Se permite http, https o mssql.
- **Inspección de TLS:** Solo permitido en el tamaño premium.
- **Tipo de destino**: Se permite FQDN, etiqueta FQDN, URL o Categoria Web.
- **Destino**: FQDN, etiqueta FQDN, URL o Categoria Web.

La configuración de las Reglas de red es:



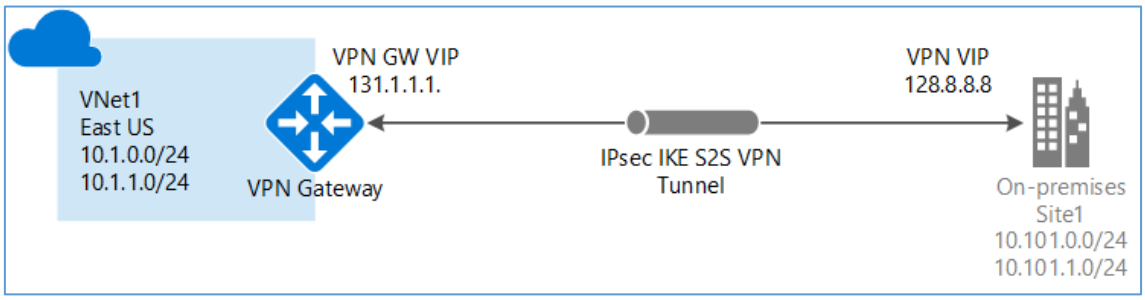
- **Nombre**: Apodo de la regla.
- **Tipo de origen**: Definir el tipo de origen (Dirección IP y Grupo de IP)
- **Origen**: Dirección o rango IP de origen.
- **Protocolo**: Se permite TCP, UDP, ICMP o todos.
- **Puertos de destino:** Puerto o rango de puertos de destino.
- **Tipo de destino**: Se permite Dirección IP, etiqueta de destino, FQDN y grupo de IP.
- **Destino**: Dirección IP, etiqueta de destino, FQDN y grupo de IP.

3.2.1.2 PROTECCIÓN DE LA CONFIDENCIALIDAD

VPN

En esta guía se explica cómo se debe crear una conexión de puerta de enlace VPN de sitio a sitio desde la red local a la red virtual.

Este tipo de conexión requiere un dispositivo VPN local que tenga una dirección IP pública asignada.



Antes de comenzar con la configuración, comprobar que se cumplen los criterios siguientes:

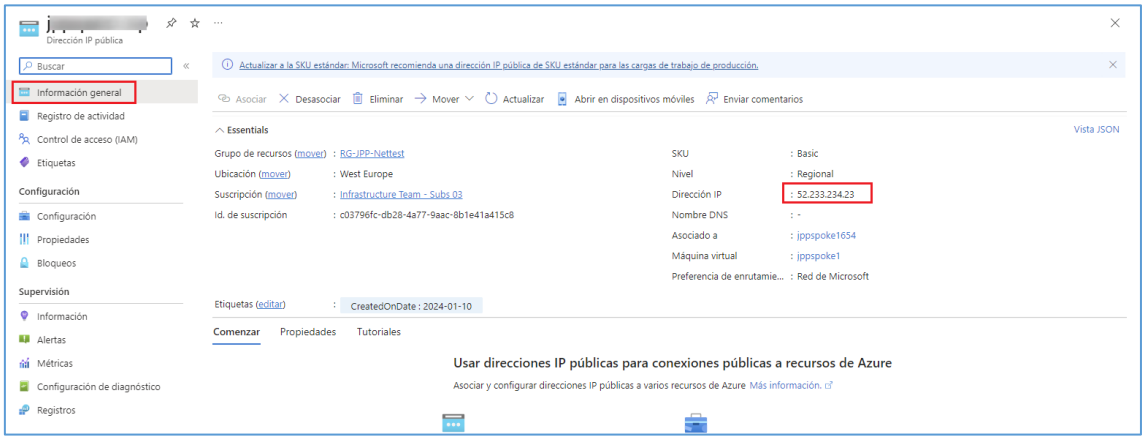
a) Tener un dispositivo VPN compatible cualificado (incluido en la familia Redes Privadas Virtuales de la guía *CCN-STIC-105 Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación*). Para ver la lista de dispositivos compatibles, se recomienda consultar https://docs.microsoft.com/es-es/azure/vpn-gateway/vpn-gateway-about-vpn-devices

b) Comprobar que tiene una dirección IPv4 pública externa para el dispositivo VPN.

Las conexiones de sitio a sitio a una red local requieren un dispositivo VPN. En este paso, se debe configurar el dispositivo VPN. Para configurar el dispositivo VPN, necesita los elementos siguientes:

- Una clave compartida. Se trata de la misma clave compartida que se especifica al crear la conexión VPN de sitio a sitio. Ver apartado [3.2.1.1 Segregación de redes / Puerta de enlace de red local y virtual].
- La dirección IP pública de la puerta de enlace de red virtual. Se puede ver la dirección IP pública, para verlo desde el portal:
  a) Escribir en el buscador el nombre de la IP pública o buscar IP pública para ver todas las existentes.

b) Pulsar en la IP pública para ver la IP asignada.



Para ver la dirección mediante PowerShell.

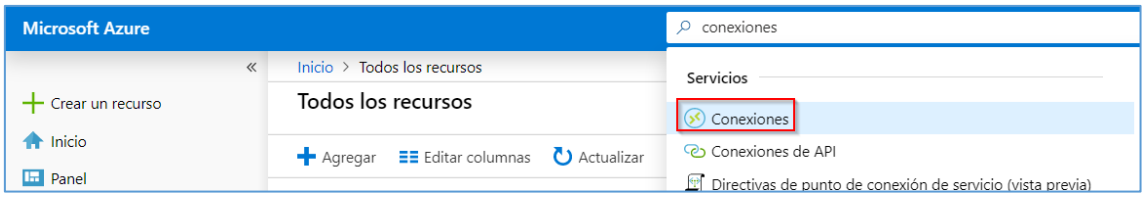
```
#   Get-AzPublicIpAddress -Name CCN-VPNCONEXION -ResourceGroupName CCNVPN
```

CREACIÓN DE LA CONEXIÓN VPN

A continuación, se debe crear la conexión VPN de sitio a sitio entre la puerta de enlace de red virtual y el dispositivo VPN.

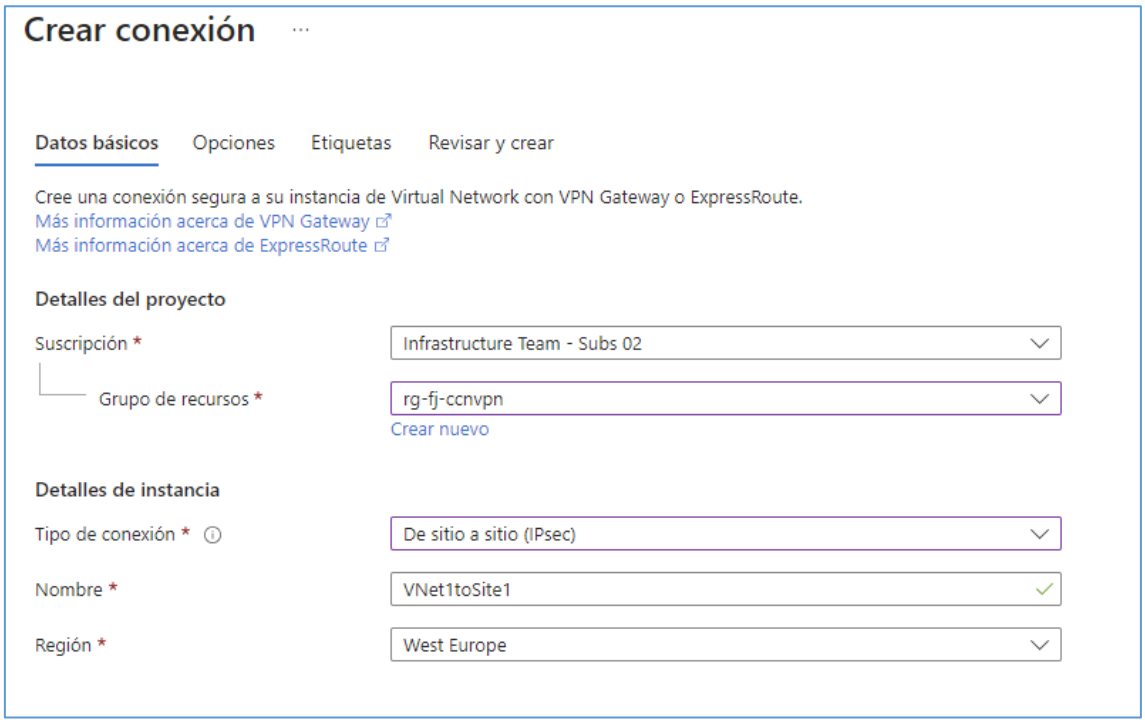
Para crear la conexión VPN desde el portal:

a) Buscar conexiones

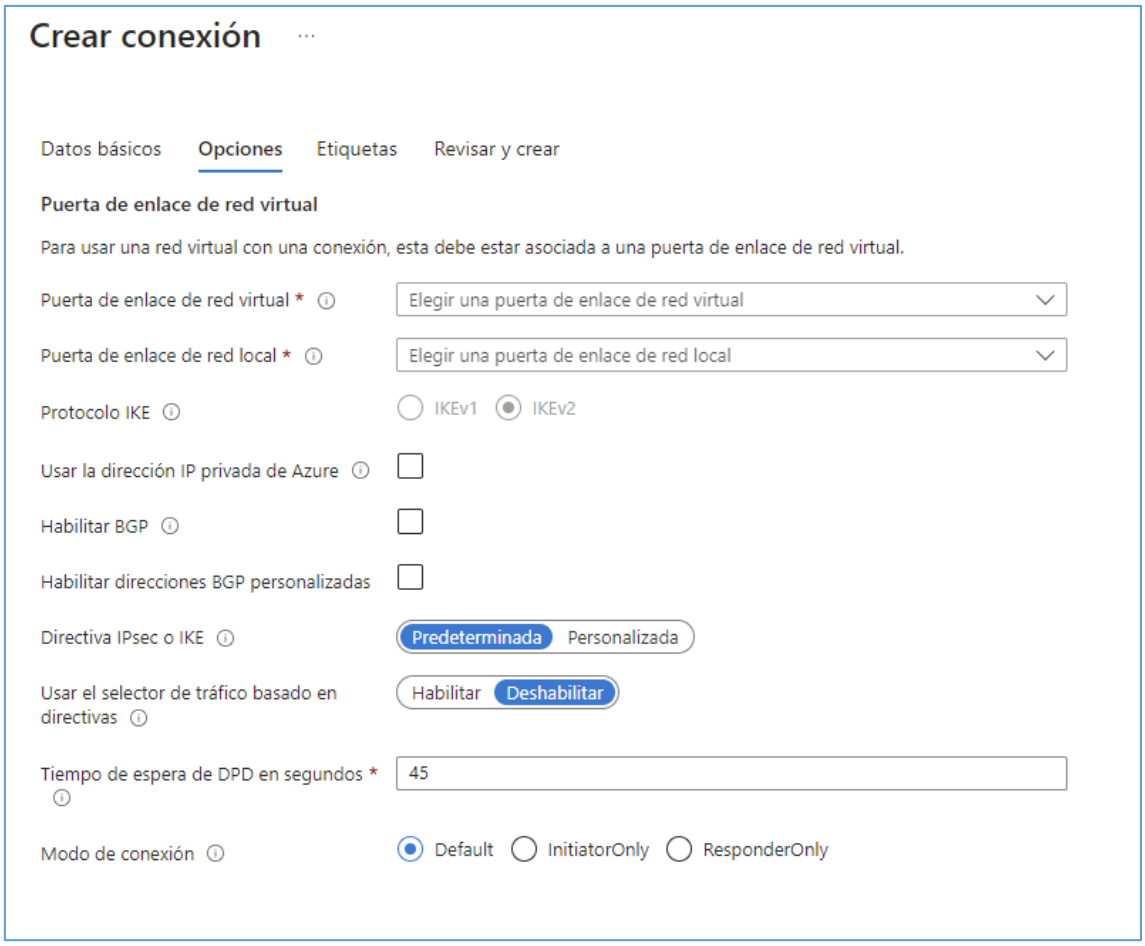


b) Crear una nueva conexión.

c) Para comenzar se pide el tipo de conexión, se debe utilizar "De sitio a sitio (IPsec)", suscripción en la que se crea la conexión, grupo de recursos, región y nombre.



d) A continuación, rellenamos los campos del formulario. Se necesita una puerta de enlace de red virtual y una puerta de enlace de red local y la clave que se creó en la puerta de enlace de red local. El resto de los parámetros se pueden dejar por defecto.



e) Crear el recurso.

Para crear la conexión desde Powershell:

a) Establecer las variables.

```
# $gateway1 = Get-AzVirtualNetworkGateway -Name VNet1GW -ResourceGroupName
  CCNVPN
# $local = Get-AzLocalNetworkGateway -Name Site1 -ResourceGroupName ccnvpn
```

b) Crear la conexión.

```
# New-AzVirtualNetworkGatewayConnection -Name VNet1toSite1 -
  ResourceGroupName CCNVPN `
# -Location 'North Europe' -VirtualNetworkGateway1 $gateway1 -
  LocalNetworkGateway2 $local `
# -ConnectionType IPsec -RoutingWeight 10 -SharedKey ' QTuKYdZi7lEZtfNT2K5U
  '
```

Comprobación de la conexión VPN

Para comprobar que la conexión se realizó correctamente se puede hacer uso del cmdlet "**Get-AzVirtualNetworkGatewayConnection**", con o sin "**-Debug**".

```
# Get-AzVirtualNetworkGatewayConnection -Name VNet1toSite1 -
ResourceGroupName CCNVPN
```

AZURE EXPRESSROUTE

Además de conectar las redes locales con Azure a través de VPN, existe la posibilidad de utilizar un ExpressRoute. ExpressRoute permite ampliar las redes locales con Azure mediante una conexión privada con la ayuda de un proveedor de conectividad. Las conexiones de ExpressRoute ofrecen más fiabilidad, más velocidad, latencia más coherente y mayor seguridad que las conexiones a Internet normales porque no se realizan a través de una conexión a Internet pública.

Nota: Para información sobre cómo conectar su red local a Azure mediante ExpressRoute puede consultar el siguiente enlace: https://learn.microsoft.com/es-es/azure/expressroute/expressroute-connectivity-models

3.2.1.3 PROTECCIÓN DE LA INTEGRIDAD Y DE LA AUTENTICIDAD

Para la protección de autenticidad y de la integridad seguir los pasos de esta guía ya que es importante que implante diversos servicios que ofrece Microsoft en su *Tenant*.

Microsoft Defender for Cloud: Unifique la administración y habilite la protección contra amenazas avanzadas para cargas de trabajo en la nube. Las recomendaciones las puede consultar en esta guía en la sección [3.1.4.3 Vigilancia / Microsoft Defender for Cloud / Búsqueda de recomendaciones].

Autenticación multifactor de Microsoft Entra: Se debe crear un método de autenticación donde se puede configurar condiciones mediante una directiva para los usuarios. Se puede consultar más información en esta guía en la sección [3.1.1.5 Mecanismo de autenticación / Métodos de Autenticación].

Azure DDoS Protection: Para proteger sus aplicaciones frente a ataques por denegación de servicio distribuido (DDoS). Se puede consultar más información en esta guía en la sección [3.2.3.1 Protección frente a la denegación de servicio].

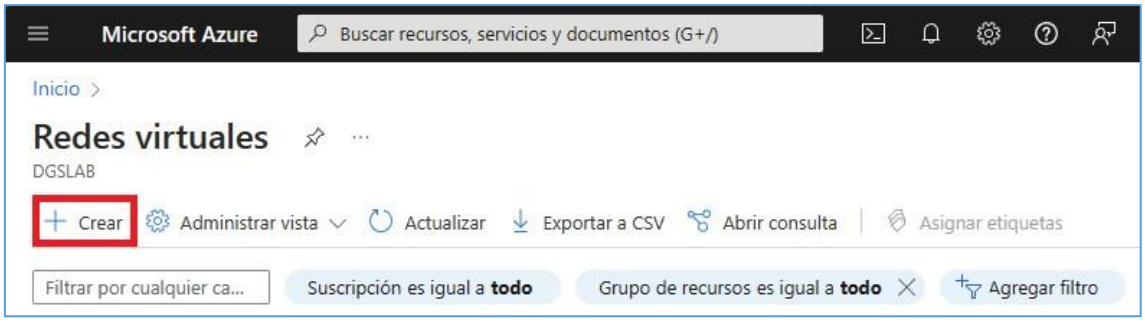
3.2.1.4 SEPARACIÓN DE FLUJOS DE INFORMACIÓN EN LA RED

Una VNET es una red privada en Azure que aporta a su vez las ventajas de la infraestructura en Azure como la escalabilidad, la disponibilidad y el aislamiento.

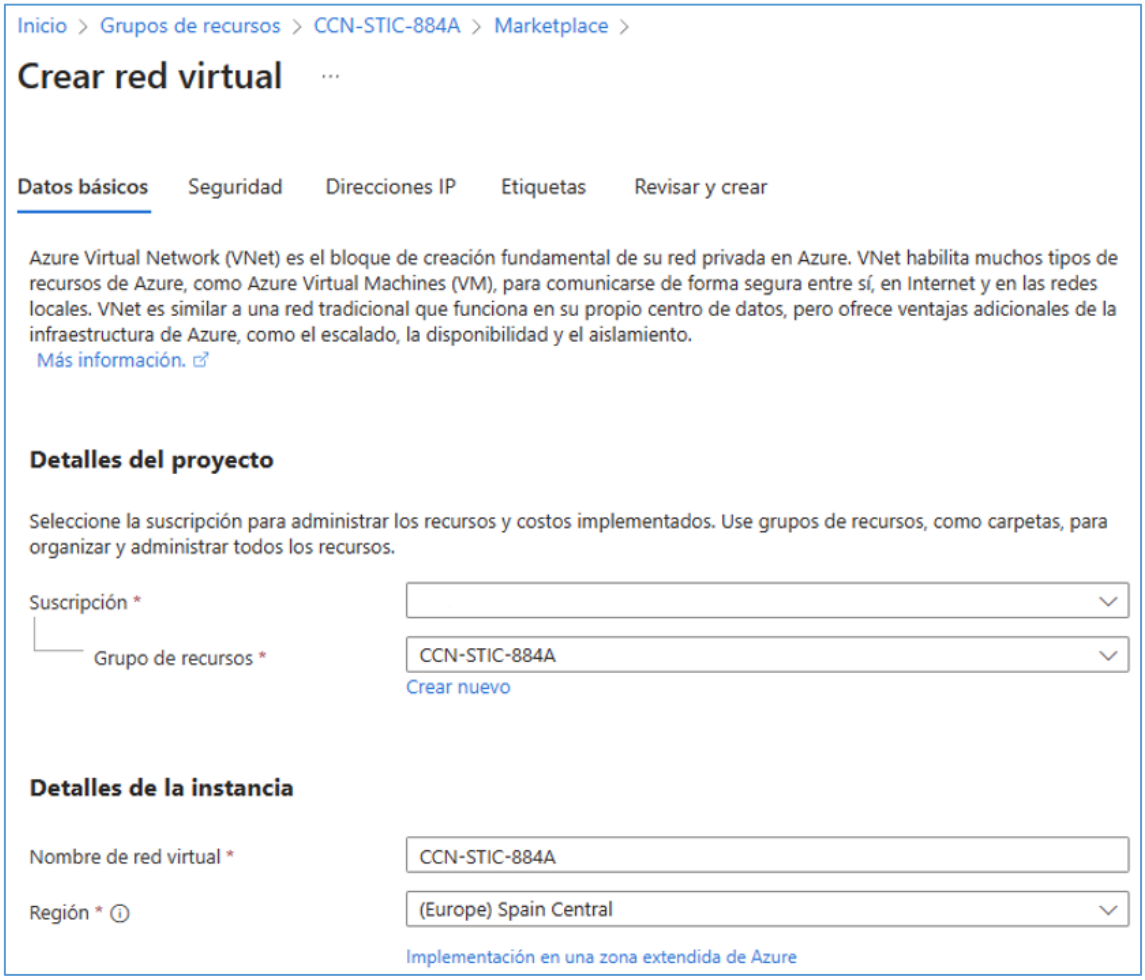
CREACIÓN DE VNET Y SUBREDES DESDE EL PORTAL DE AZURE

a) En el buscador escribir [Redes virtuales].

b) Pulsar sobre [Crear].

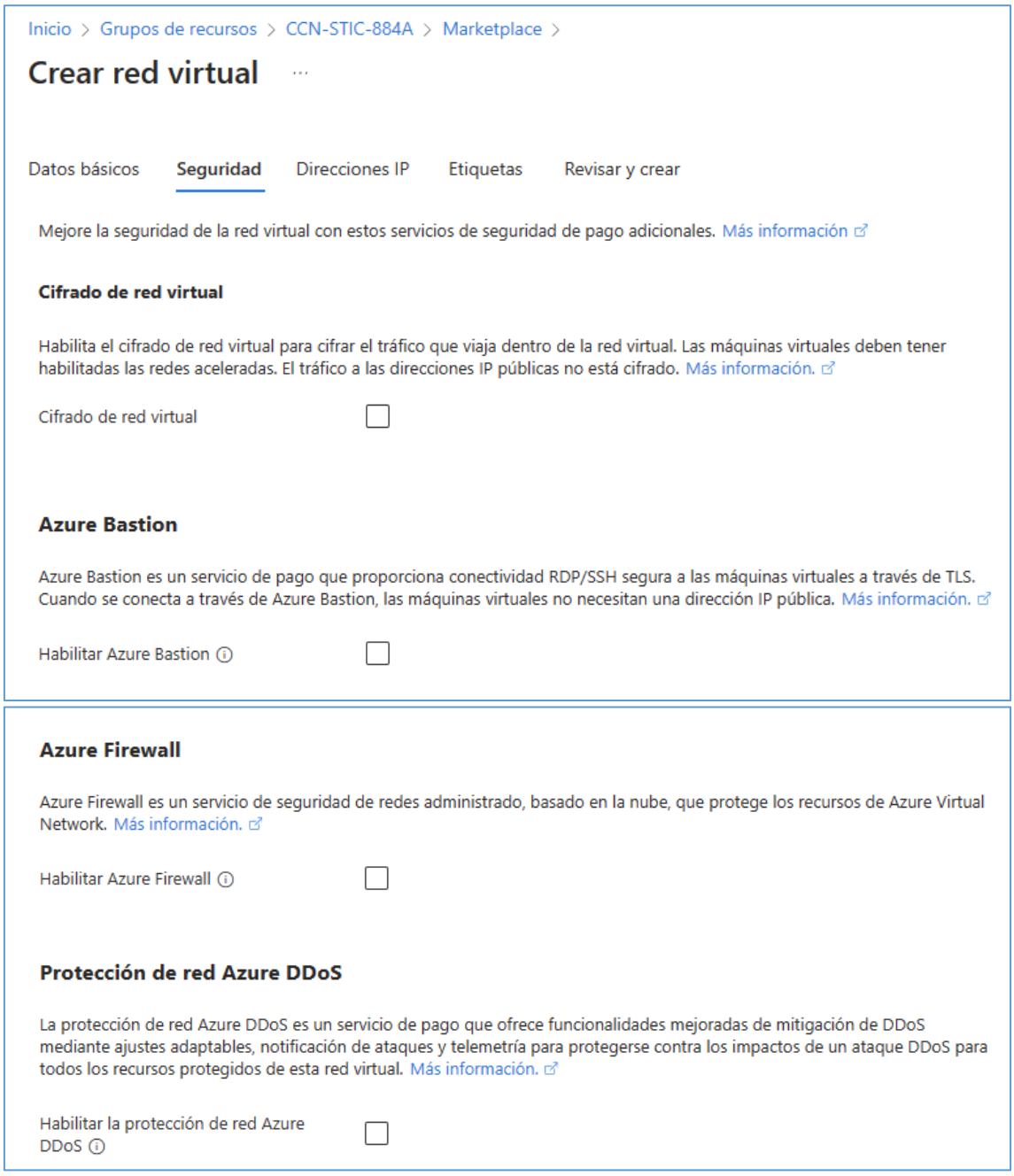


c) Rellenar los campos del formulario [Datos básicos].



- **Suscripción**: Suscripción donde gestionar los costes del recurso.
- **Grupo de recursos**: Grupo de recursos donde desplegar el recurso.
- **Nombre de red virtual**: Nombre del recurso.
- **Región**: Centro de datos donde desplegar el recurso (Se recomienda: Spain Central)

d) Rellenar los campos del formulario [Seguridad].



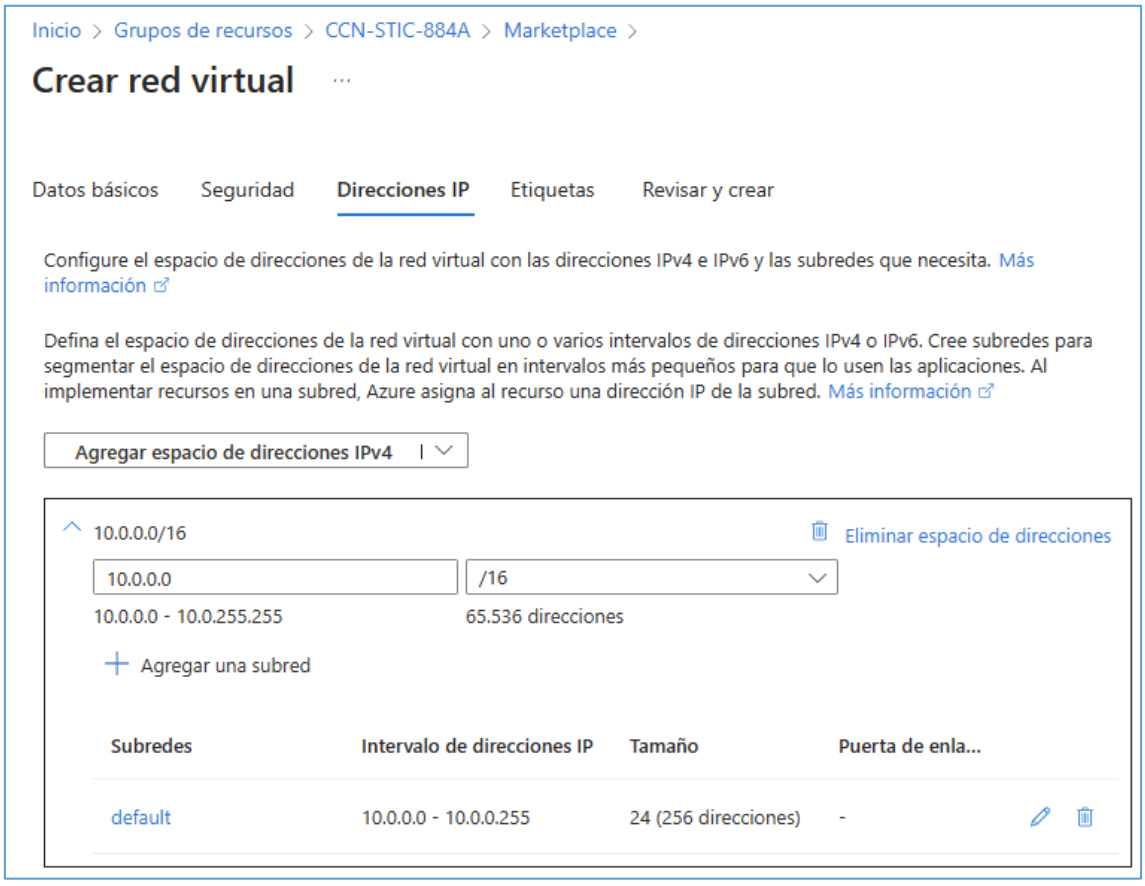
- **Cifrado de red virtual**: Cifrado de las comunicaciones de redes de Azure. Deshabilitado por defecto. No compatible con la mayoría de máquinas.

- **Azure Bastion**: Servicio gestionado con la funcionalidad de máquina de salto hacia otras máquinas virtuales en Azure. Por defecto esta deshabilitado.
- **Azure Firewall**: Por defecto deshabilitado, Azure Firewall es un servicio de seguridad de red administrado y basado en la nube que protege los recursos de Azure Virtual Network. Se trata de un firewall como servicio con estado completo que incorpora alta disponibilidad y escalabilidad a la nube sin restricciones.

Nota: Para más información consultar *https://learn.microsoft.com/es-es/azure/firewall/overview*

- **Protección de red Azure DDoS**: Seleccionar el plan deseado, DDoS está explicado en el apartado [3.2.3 Protección de los servicios] de la presente guía.

e) Rellenar los campos del formulario [Direcciones IP].



f) Pulsar sobre [Revisar y crear / Crear].

CREACIÓN DE REDES Y SUBREDES POR POWERSHELL

a. Establecer las variables que definen las subredes.

```
# $subnet1 = New-AzVirtualNetworkSubnetConfig -Name 'GatewaySubnet' -
AddressPrefix 10.1.255.0/27
# $subnet2 = New-AzVirtualNetworkSubnetConfig -Name 'Frontend' -
AddressPrefix 10.1.0.0/24
```

b. Crear la VNET con las subredes que fueron definidas en el paso anterior.

```
# New-AzVirtualNetwork -Name VNet1 -ResourceGroupName CCNVPN `
# -Location 'Spain Central' -AddressPrefix 10.1.0.0/16 -Subnet $subnet1,
$subnet2
```

c. Para agregar una subred de puerta de enlace a una red virtual que ya ha creado realizar los pasos de esta sección si ya tiene una red virtual, aunque se debe agregar una subred de puerta de enlace.

1. Seleccionar la VNET a la que se agregara la subred.

```
# $vnet = Get-AzVirtualNetwork -ResourceGroupName CCNVPN -Name VNet1
```

2. Crear la subred de la puerta de enlace.

```
# Add-AzVirtualNetworkSubnetConfig -Name 'GatewaySubnet' -
AddressPrefix 10.1.255.0/27 -VirtualNetwork $vnet
```

3. Establecer la configuración.

```
# Set-AzVirtualNetwork -VirtualNetwork $vnet
```

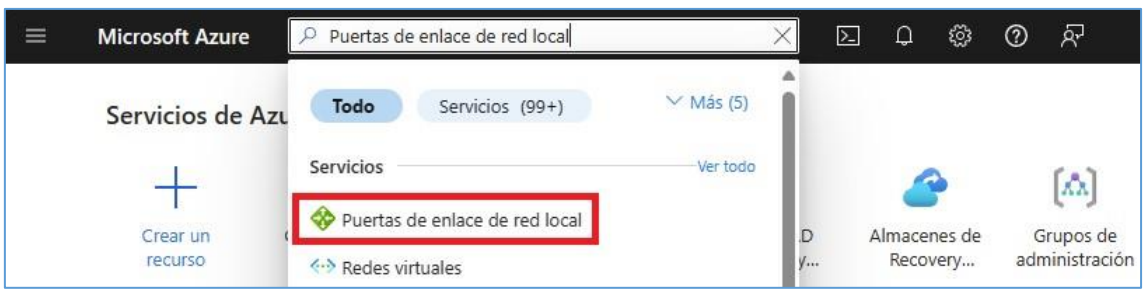
PUERTA DE ENLACE DE RED LOCAL Y VIRTUAL

La puerta de enlace de red local (LNG) suele hacer referencia a la ubicación local. No es lo mismo que una puerta de enlace de red. Asignar al sitio un nombre al que Azure pueda hacer referencia y, luego, especificar la dirección IP del dispositivo VPN local con la que crea una conexión. Especificar también los prefijos de dirección IP que se enrutan a través de la puerta de enlace VPN al dispositivo VPN.
Use los valores siguientes:

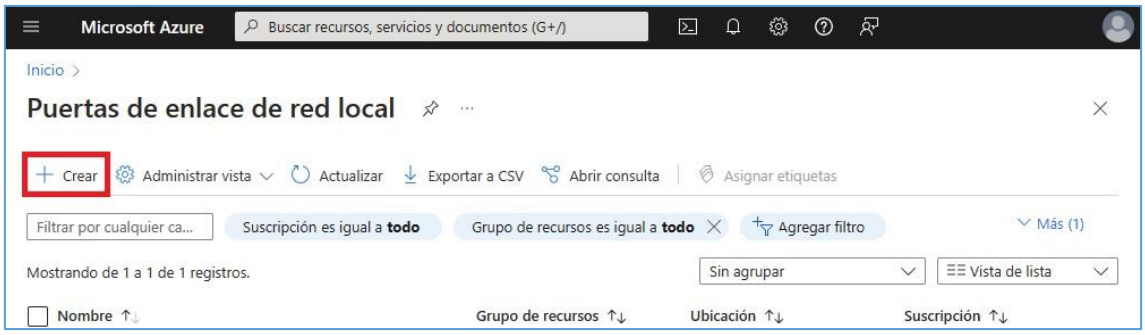
- GatewayIPAddress es la dirección IP del dispositivo VPN local.
- AddressPrefix es el espacio de direcciones local.

CREACIÓN DE PUERTAS DE ENLACE DE RED LOCAL DESDE EL PORTAL

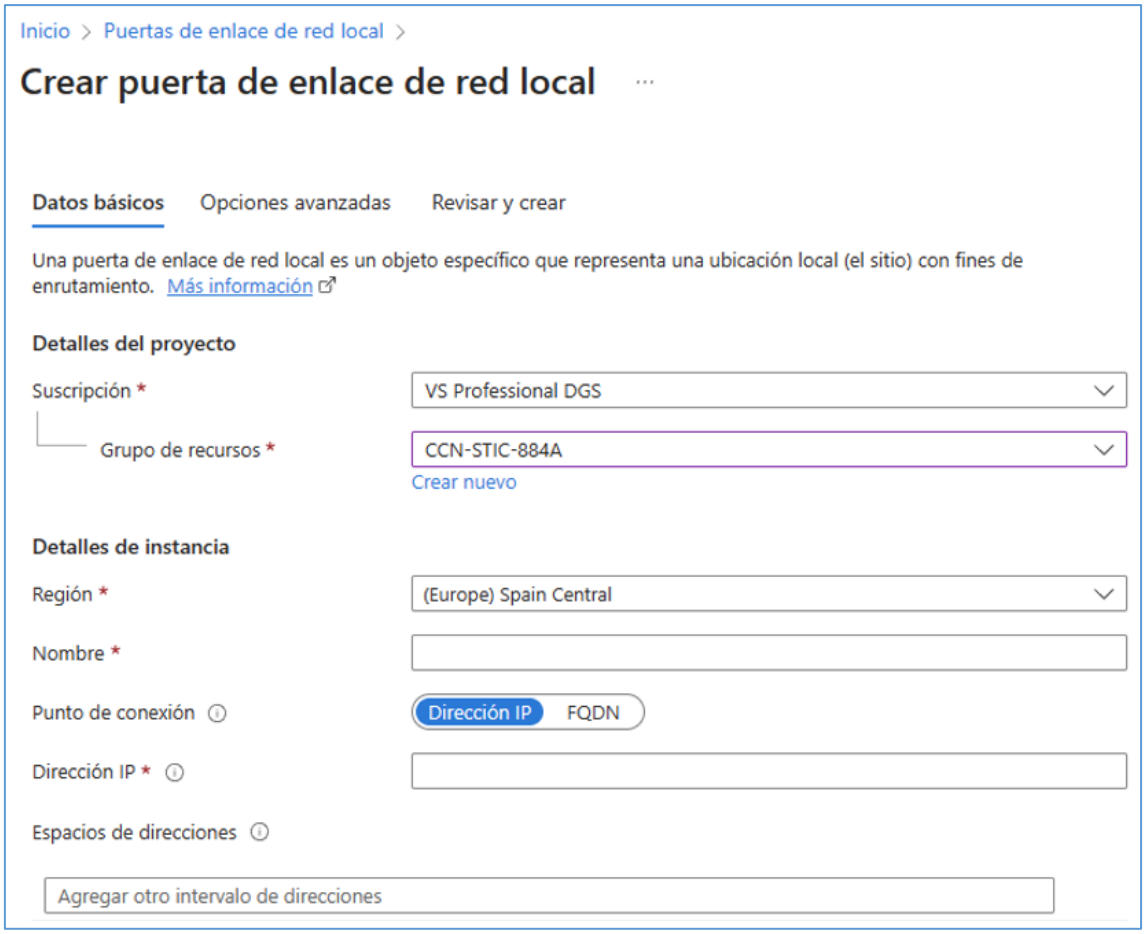
1. En el buscador escribimos [Puertas de enlace de red local].



2. Pulsamos sobre [Crear].

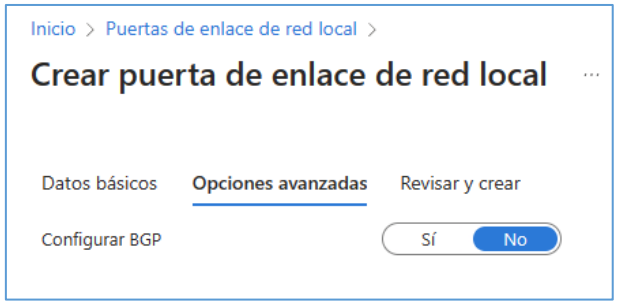


3. Rellenar formulario [Datos básico].



- **Suscripción**: Suscripción donde gestionar los costes del recurso.
- **Grupo de recursos**: Grupo de recursos donde desplegar el recurso.
- **Región**: Centro de datos donde desplegar el recurso (Se recomienda: Spain Central)
- **Nombre de red virtual**: Nombre del recurso.
- **Punto de conexión**: Definir el tipo de conexión que define el origen local.
- **Dirección IP / FQDN**: Direccionamiento local.
- **Espacio de direcciones**: Rango/s de direcciones IP que se permite durante la comunicación.

4. Rellenar formulario [Opciones avanzadas].

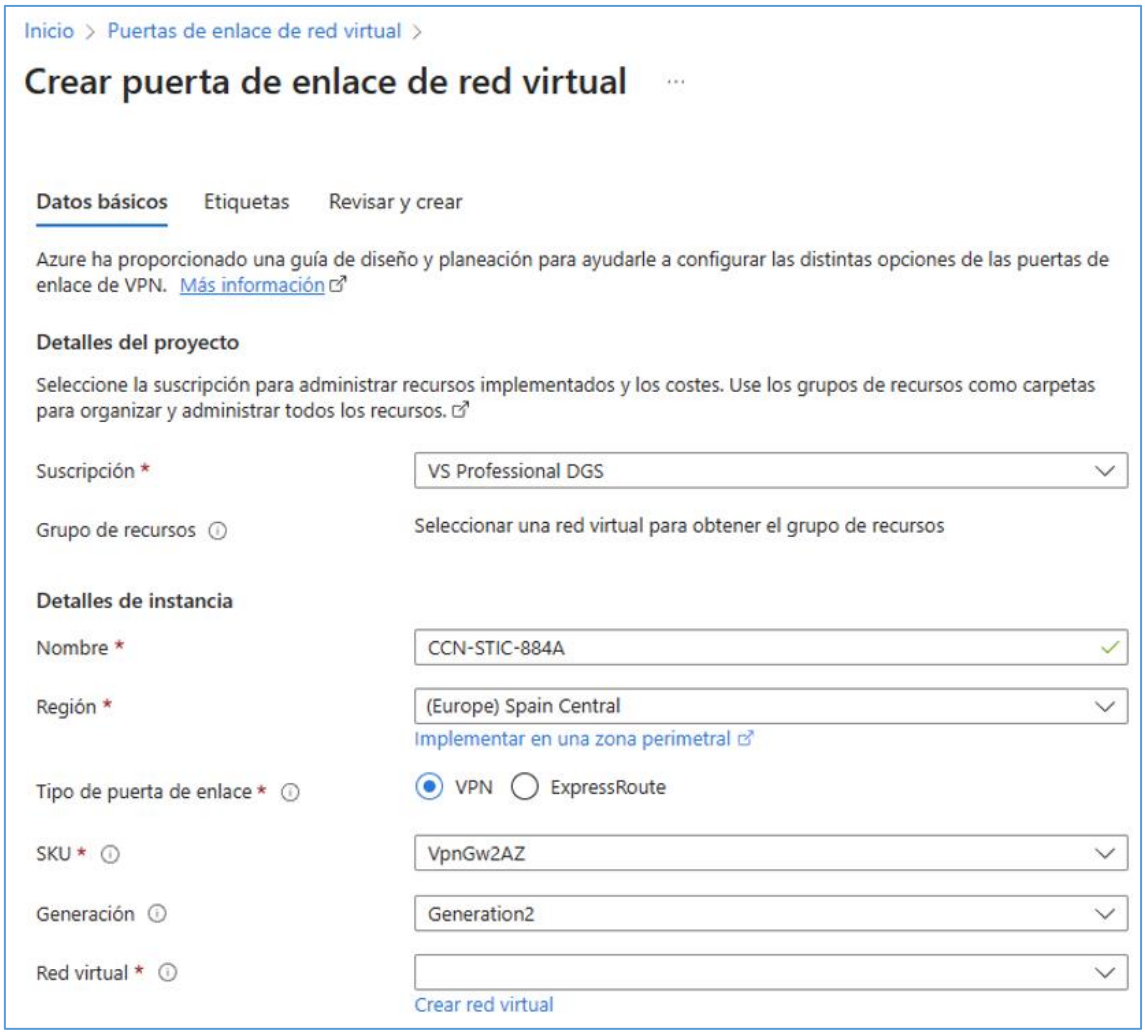


Habilitar [Configurar BGP] si se desea una configuración por BGP. Esta opción esta deshabilitada por defecto.

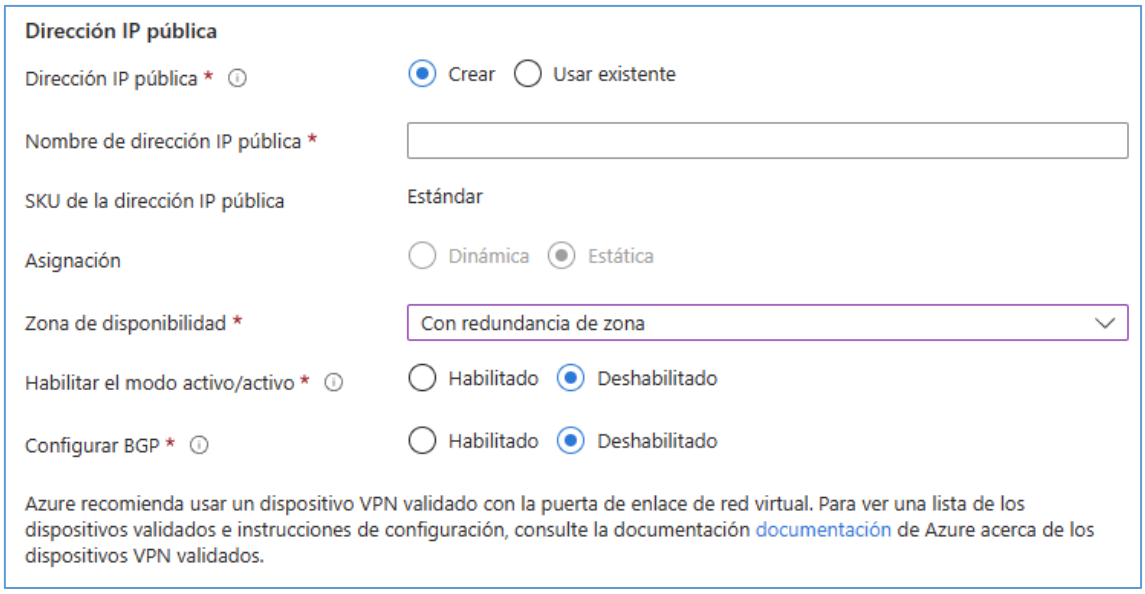
5. Pulsar sobre [Revisar y crear / Crear].
6. En el buscador escribimos [Puertas de enlace de red virtual].

7. Pulsamos sobre [Crear].

8. Rellenar el formulario [Datos básicos]



- **Suscripción**: Suscripción donde gestionar los costes del recurso.
- **Grupo de recursos**: Grupo de recursos donde desplegar el recurso.
- **Región**: Centro de datos donde desplegar el recurso (Se recomienda: Spain Central)
- **Nombre de red virtual**: Nombre del recurso.
- **Tipo de puerta de enlace**: Escoger VPN. El modo Express Route es una conexión dedicada entre los CPDs de Azure y el proveedor de servicio de Internet. Esta conexión es dedicada en exclusiva para el cliente.
- **SKU:** Se recomienda VpnGw2AZ para asegurar la alta disponibilidad y un ancho de banda lo suficientemente grande para no producir cuellos de botella.
- **Generación:** Si está disponible, escoger la generación 2.
- **Red virtual**: Red sobre la que ira montada la VPN. Más información de cómo crear una red virtual en el punto [3.2.1.1 Segregación de redes].

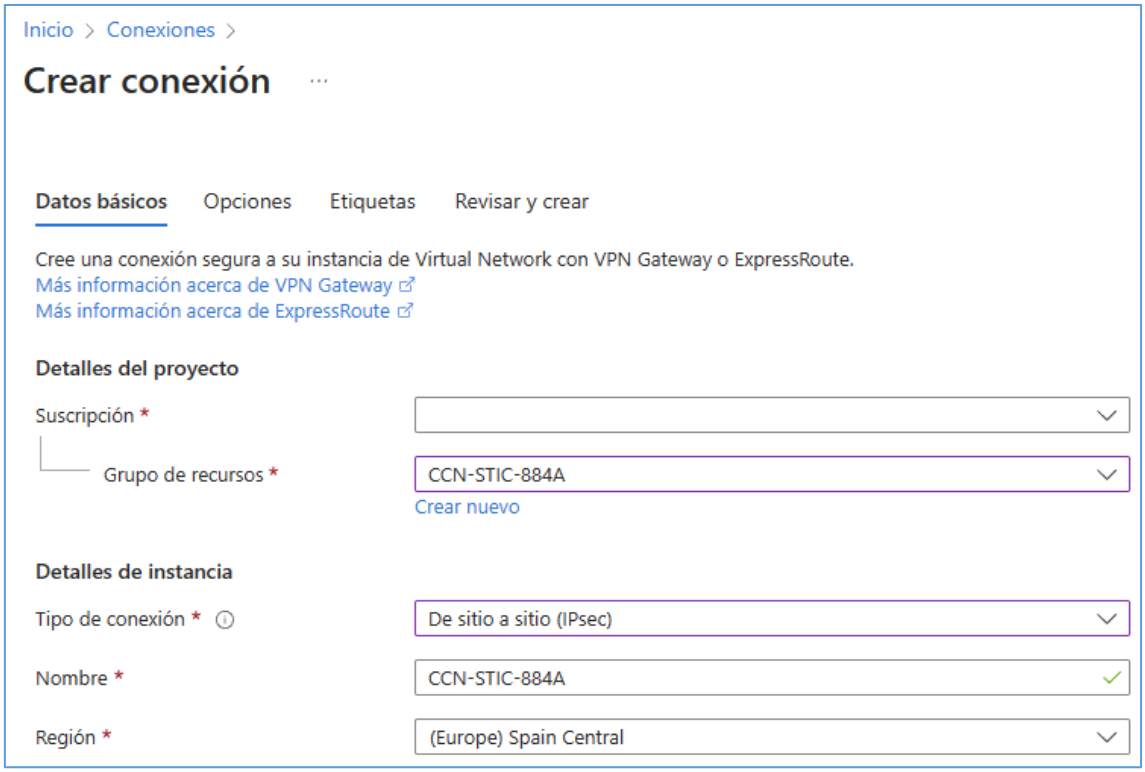


- **Dirección IP pública**: Seleccionar Crear.
- **Nombre de dirección IP pública**: Nombre del recurso.
- **SKU de la dirección IP pública**: Solo permite Estándar.
- **Asignación**: Solo permite Estática
- **Zona de disponibilidad**: Seleccionar Con redundancia de zona.
- **Habilitar el modo activo / activo:** Seleccionar Deshabilitado.
- **Configurar BGP:** Seleccionar Deshabilitado.

9. Pulsar sobre [Revisar y crear / Crear].
10. En el buscador escribimos [Puertas de enlace de red local].

11. Pulsamos sobre [Crear].

12. Rellenamos el formulario [Datos básicos].



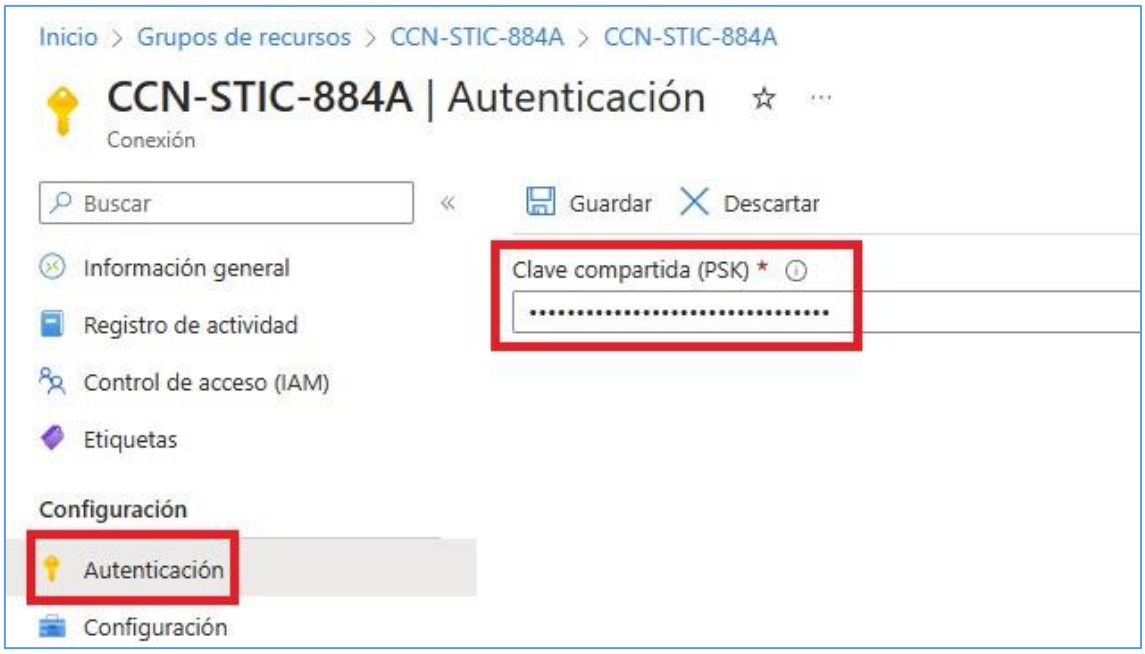
- **Suscripción**: Suscripción donde gestionar los costes del recurso.
- **Grupo de recursos**: Grupo de recursos donde desplegar el recurso.
- **Tipo de conexión**: Seleccionamos la opción de sitio a sitio (Ipsec).
- **Nombre**: Nombre del recurso.
- **Región**: Centro de datos donde desplegar el recurso (Se recomienda: Spain Central)

13. Rellenamos el formulario [Opciones].

- **Puerta de enlace de red virtual**: Seleccionar una puerta de enlace de red virtual creada con anterioridad.
- **Puerta de enlace de red local**: Seleccionar una puerta de enlace de red local creada con anterioridad.

Nota: El resto de la configuración se puede personalizar en base a las necesidades de la red corporativa.

14. Pulsar sobre [Revisar y crear / Crear].
15. Una vez creado el recurso, pulsar sobre la sección de [Autenticación] y en [Clave compartida (PSK)] añadir la clave para habilitar la comunicación.



Nota: Las claves compartidas deben tener un nivel de entropía suficiente para presentar el nivel de fortaleza exigido de acuerdo con lo establecido en la CCN-STIC-807 Criptología de empleo en el ENS.

CREACIÓN DE UNA PUERTA DE ENLACE DE RED LOCAL DESDE POWERSHELL

1. Para agregar una puerta de enlace de red local con un único prefijo de dirección ejecutar:

```
# New-AzLocalNetworkGateway -Name Site1 -ResourceGroupName CCNVPN `
# -Location 'Spain Central' -GatewayIpAddress 'IpVPNLocal' -
AddressPrefix '10.101.0.0/24
```

2. Para agregar una puerta de enlace de red local con varios prefijos de dirección ejecutar:

```
# New-AzLocalNetworkGateway -Name Site1 -ResourceGroupName CCNVPN `
# -Location ' Spain Central' -GatewayIpAddress 'IpVPNLocal' -
AddressPrefix @('10.101.0.0/24','10.101.1.0/24')
```

3. Crear la configuración de direccionamiento IP de la puerta de enlace.

```
# $vnet = Get-AzVirtualNetwork -Name VNet1 -ResourceGroupName CCNVPN
# $subnet = Get-AzVirtualNetworkSubnetConfig -Name 'GatewaySubnet' -
VirtualNetwork $vnet
# $gwipconfig = New-AzVirtualNetworkGatewayIpConfig -Name gwipconfig1
-SubnetId $subnet.Id -PublicIpAddressId $gwpip.Id
```

4. Crear la puerta de enlace VPN.

```
# New-AzVirtualNetworkGateway -Name VNet1GW -ResourceGroupName ccnvpn
`
# -Location 'Spain Central' -IpConfigurations $gwipconfig -GatewayType
Vpn `
# -VpnType RouteBased -GatewaySku VpnGw2AZ
```

3.2.2 PROTECCIÓN DE LA INFORMACIÓN

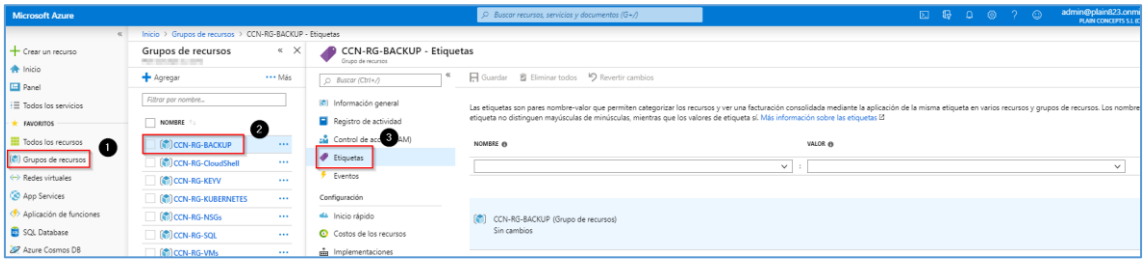
3.2.2.1 CALIFICACIÓN DE LA INFORMACIÓN

Las etiquetas de los recursos de Azure están estrechamente vinculadas con los estándares de nomenclatura y clasificación de los recursos. A medida que se agregan recursos a las suscripciones, cada vez resulta más importante clasificarlos de forma lógica para fines de facturación, administración y operativos.

Después de aplicar las etiquetas, se pueden recuperar todos los recursos de la suscripción que tengan ese nombre y valor de etiqueta. Las etiquetas le permiten recuperar los recursos relacionados que se encuentran en distintos grupos de recursos.

Es importante que al desplegar cualquier aplicación sea relacionada con una etiqueta. Para ello, realizar estas instrucciones.

a) Desde el portal de Azure pulsar en Grupo de recursos y seleccionar el grupo de recursos deseado.

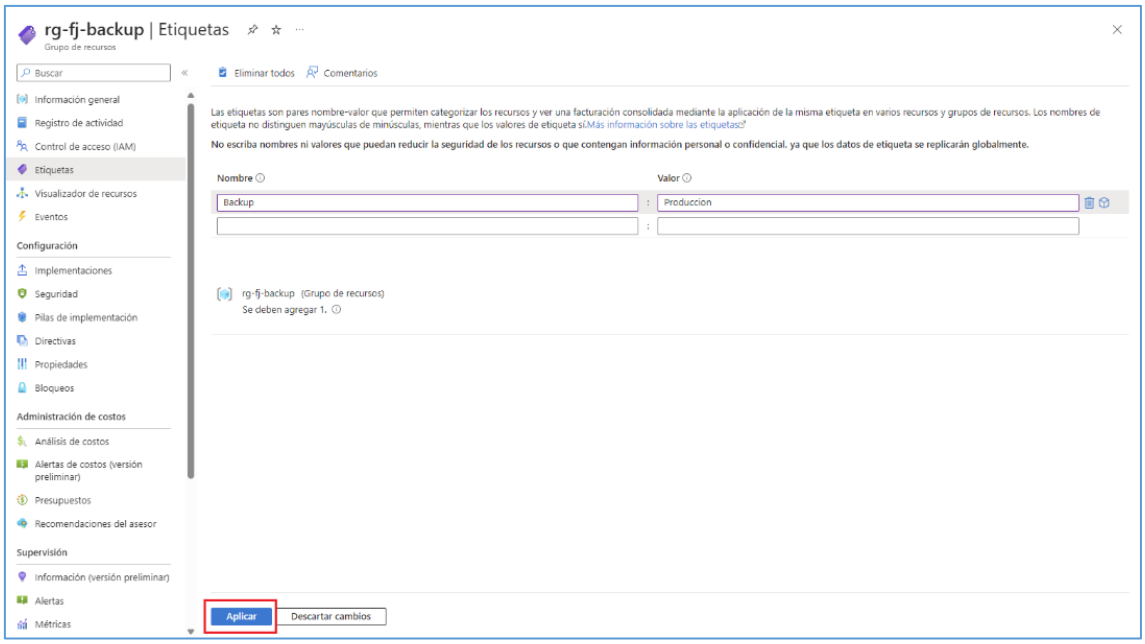


b) A continuación, pulsar en [Etiquetas].

Nota: Por ejemplo, en nombre se puede definir como el servicio.

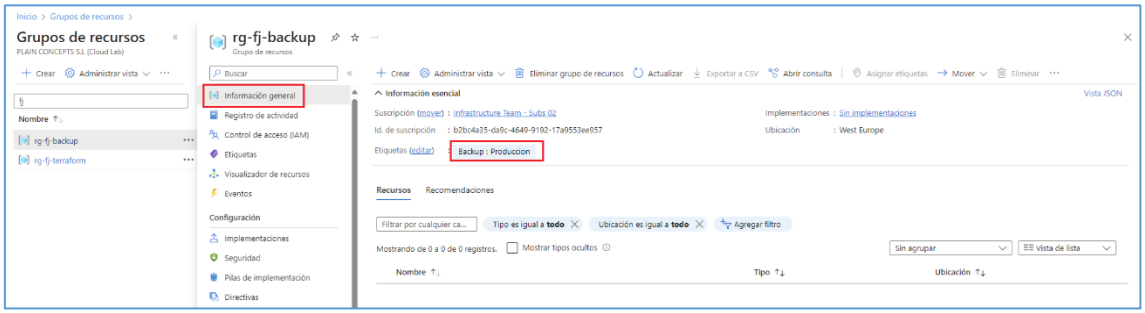
Nombre: Backup

Valor: Producción

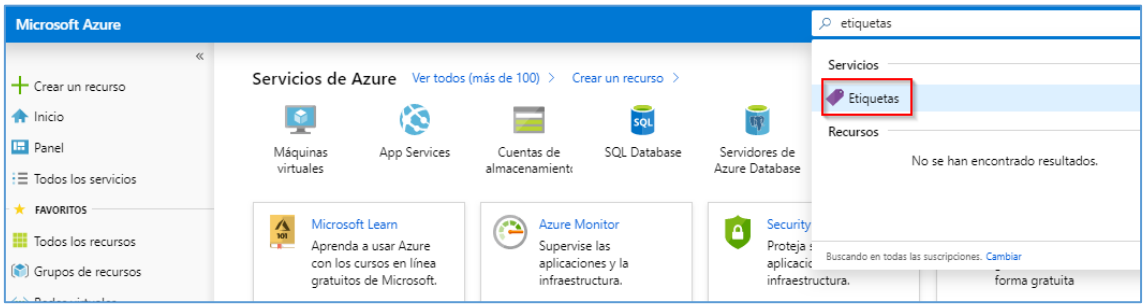


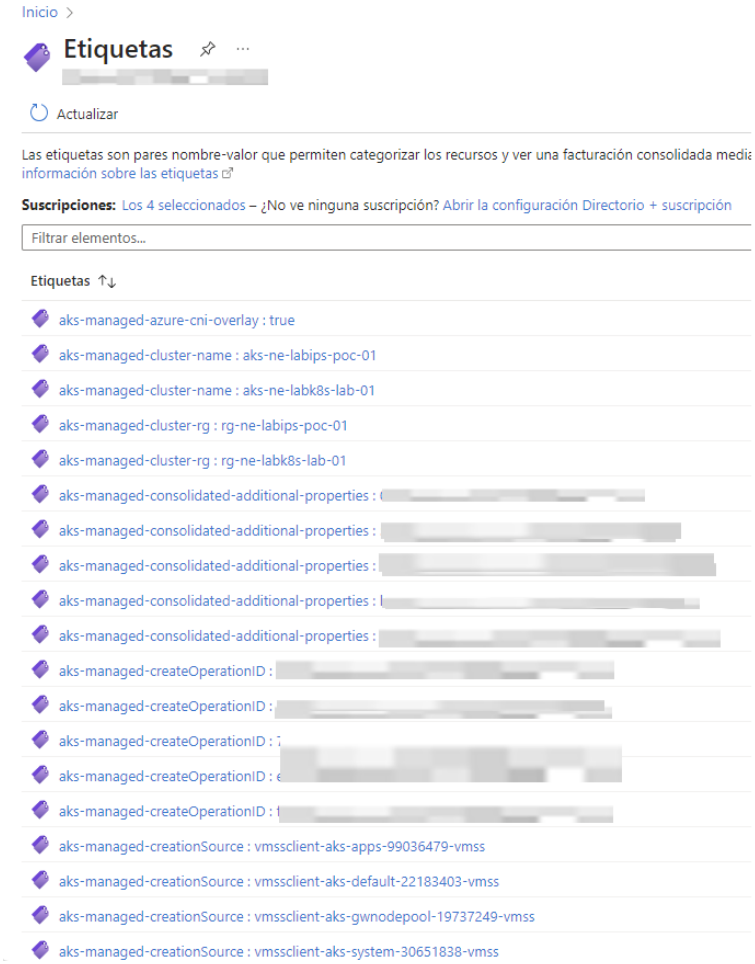
c) Para finalizar pulsar en [Aplicar].

Desde Información general se puede pulsar en Backup: Producción y se muestran todos los recursos que tienen la etiqueta definida.



Además, se pueden ver todas las etiquetas desde buscador de Azure escribiendo [Etiquetas].





A continuación, se detallan algunas directrices que se pueden seguir mediante la consola de Powershell.

Para ver las etiquetas existentes de un grupo de recursos, use:

```
#   (Get-AzResourceGroup -Name examplegroup).Tags
```

Para ver las etiquetas existentes de un recurso que tiene un identificador de recurso especificado, use:

```
#   (Get-AzResource -ResourceId /subscriptions/<subscription-
    id>/resourceGroups/<rg-
    name>/providers/Microsoft.Storage/storageAccounts/<storage-name>).Tags
```

O bien, para ver las etiquetas existentes para un recurso que tiene un nombre y un grupo de recursos especificados, use:

```
#   (Get-AzResource -ResourceName examplevnet -ResourceGroupName
    examplegroup).Tags
```

Para obtener grupos de recursos que tengan una etiqueta específica, use:

```
#   (Get-AzResourceGroup -Tag @{ Dept="Finance" }).ResourceGroupName
```

Para obtener recursos que tengan una etiqueta específica, use:

```
#   (Get-AzResource -Tag @{ Dept="Finance"}).Name
```

Para agregar etiquetas a un grupo de recursos sin etiquetas existentes, use:

```
#   Set-AzResourceGroup -Name examplegroup -Tag @{ Dept="IT";
    Environment="Test" }
```

Para agregar etiquetas a un grupo de recursos que ya tiene etiquetas, recupere las etiquetas existentes, agregue la nueva y vuelva a aplicar todas:

```
#   $tags = (Get-AzResourceGroup -Name examplegroup).Tags
#   $tags.Add("Status", "Approved")
#   Set-AzResourceGroup -Tag $tags -Name examplegroup
```

Para agregar etiquetas a un recurso sin etiquetas, use:

```
#   $r = Get-AzResource -ResourceName examplevnet -ResourceGroupName
    examplegroup
#   Set-AzResource -Tag @{ Dept="IT"; Environment="Test" } -ResourceId
    $r.ResourceId -Force
```

3.2.2.2 COPIAS DE SEGURIDAD

En Azure el servicio ofrecido por Microsoft que permite realizar copias de seguridad de sus datos y restaurarlos de manera segura y eficiente es Azure Backup. Este se compone de dos entidades de almacenamiento:

- Almacenes de copia de seguridad (Backup Vault).
- Almacenes de Recovery Services (Recovery Service Vault).

ESCENARIOS DE COPIAS DE SEGURIDAD

a. **Entorno local**: Realiza copias de seguridad de archivos, carpetas y el estado del sistema en tu entorno local mediante el agente de Microsoft Azure Recovery Services (MARS).

b. **Máquinas virtuales de Azure**: Copia de seguridad de máquinas virtuales Windows o Linux completas (mediante extensiones de copia de seguridad) o de archivos, carpetas y estados del sistema mediante el agente de MARS.

c. **Azure Managed Disks**: Copia de seguridad de Azure Managed Disks.

d. **Recursos compartidos Azure Files**: Copia de seguridad de recursos compartidos de archivos de Azure en una cuenta de almacenamiento.

e. **SQL Server en máquinas virtuales de Azure**: Copia de seguridad de bases de datos de SQL Server que se ejecutan en las máquinas virtuales de Azure.

f. **Bases de datos de SAP HANA en máquinas virtuales de Azure**: Copia de seguridad de las bases de datos de SAP HANA.

g. **Servidores de Azure Database for PostgreSQL**: Copia de seguridad de bases de datos de Azure Database for PostgreSQL.

h. **Blobs de Azure**: Copia de seguridad operativa para blobs de Azure.

i. **Azure DB para PostgreSQL:** Para servidor flexible (versión preliminar).

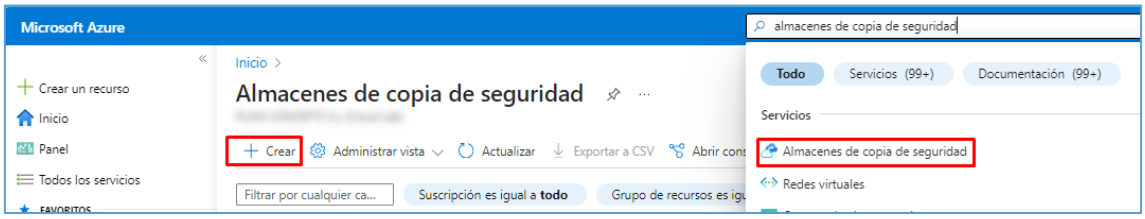
j. **Azure Kubernetes Service (AKS)**: Copia de seguridad de AKS.

ALMACENES DE COPIA DE SEGURIDAD

Los almacenes de copias de seguridad son entidades de almacenamiento que contienen los datos de las copias de seguridad de varias cargas de trabajo recientes que admite **Azure Backup**. Algunos de los puntos clave sobre ellos son:

a) Creación de un almacén de copia de seguridad.
b) Administración centrada en el origen de datos
c) Experiencias conectadas

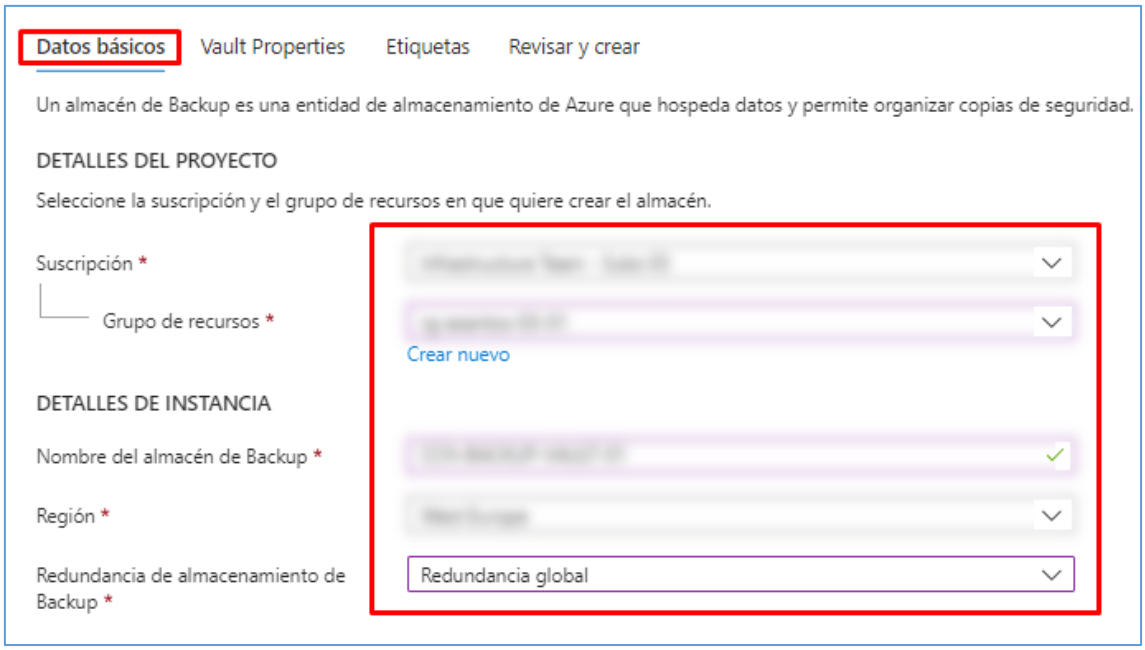
Para crear un almacén de copia de seguridad utilizamos el buscador con **almacenes de copia de seguridad.** Una vez allí, pulsamos sobre el botón Crear.



En la ventana de Crear un almacén de backup, nos movemos sobre las diferentes pestañas rellenando la información que nos piden.

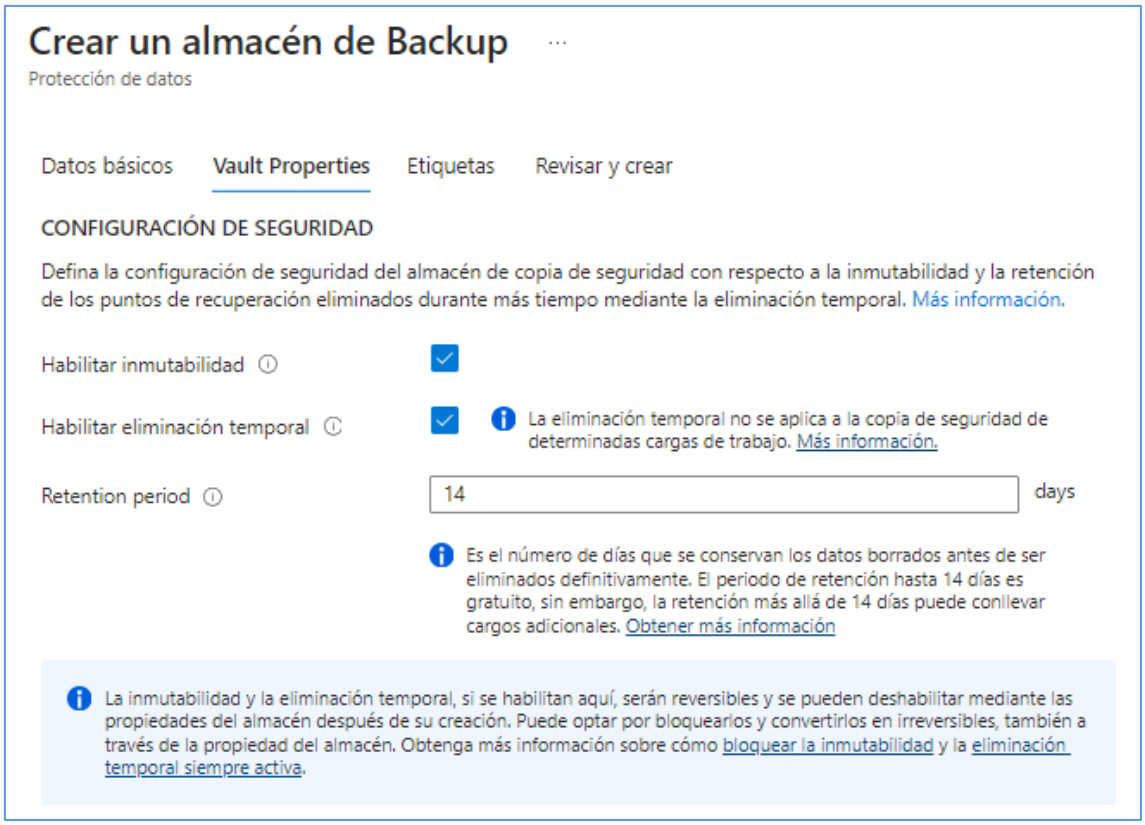
a) Datos Básicos:

- Suscripción
- Grupo de recursos
- Nombre del almacén de Backup
- Región
- Redundancia de almacenamiento de Backup: Elegiremos una redundancia global. Si quiere elegir entre otras opciones puede consultar el siguiente enlace: Información general de los almacenes de Backup - Azure Backup | Microsoft Learn

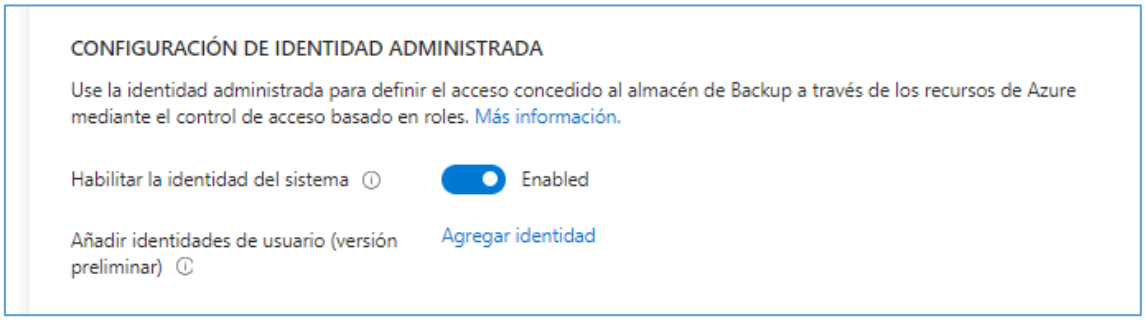


b) Vault Properties: En este apartado se define la configuración del almacén con respecto a la inmutabilidad y retención, configurar una identidad administrada y el tipo de cifrado de los datos.

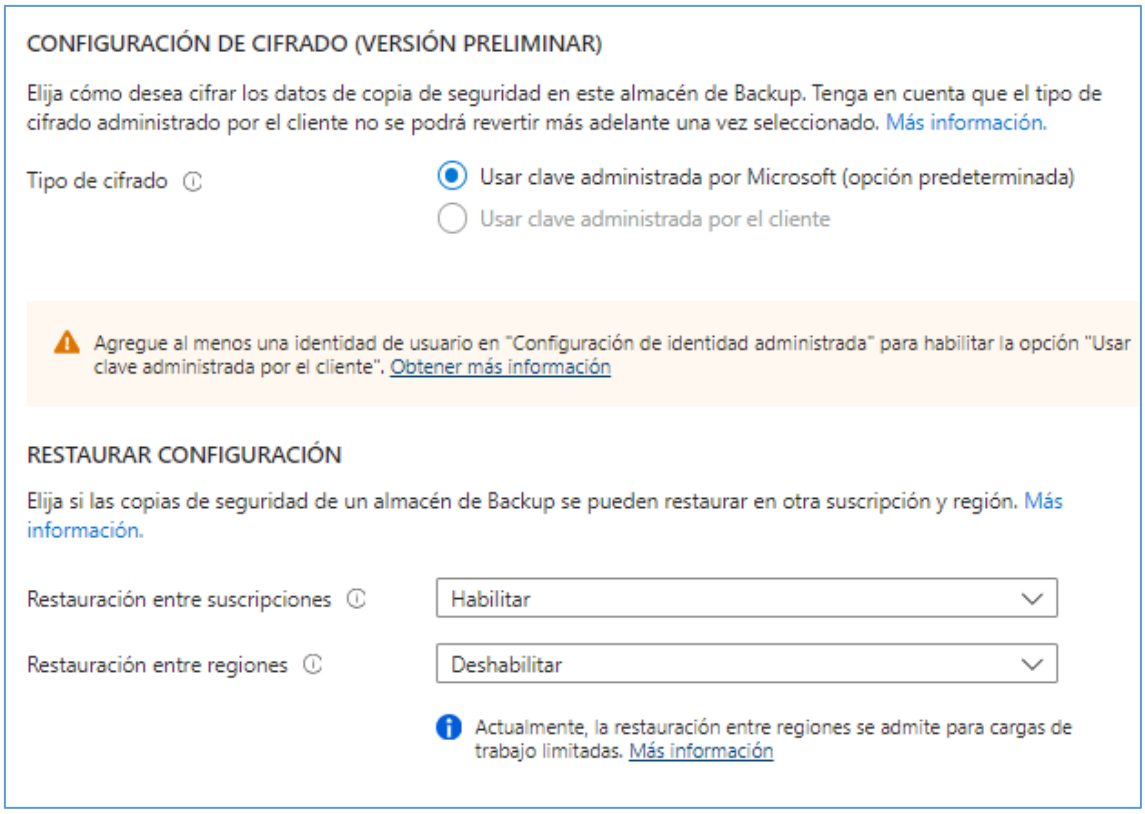
- Habilitamos la inmutabilidad para proteger los datos contra la eliminación o modificación, bloquear operaciones que provoquen pérdida de puntos de recuperación y evitar actores malintencionados. Este valor se aplica a todos los datos del almacén excepto a las copias de seguridad operativas (blobs, archivos y discos).
- Marcamos la eliminación temporal.
- Periodo de retención indicado por nuestra organización de manera interna. Indica el número de días que se conservan los datos borrados antes de eliminarse definitivamente.



- Se habilitará una identidad del sistema para definir el acceso al almacén a través de los recursos de Azure. Teniendo así un ciclo de vida controlado.



- Tipo de cifrado: Utilizaremos clave administrada por Microsoft ya que para usar una clave administrada por el cliente se debe añadir una identidad de usuario que está en versión preliminar.
- Habilitaremos la restauración entre suscripciones y regiones.



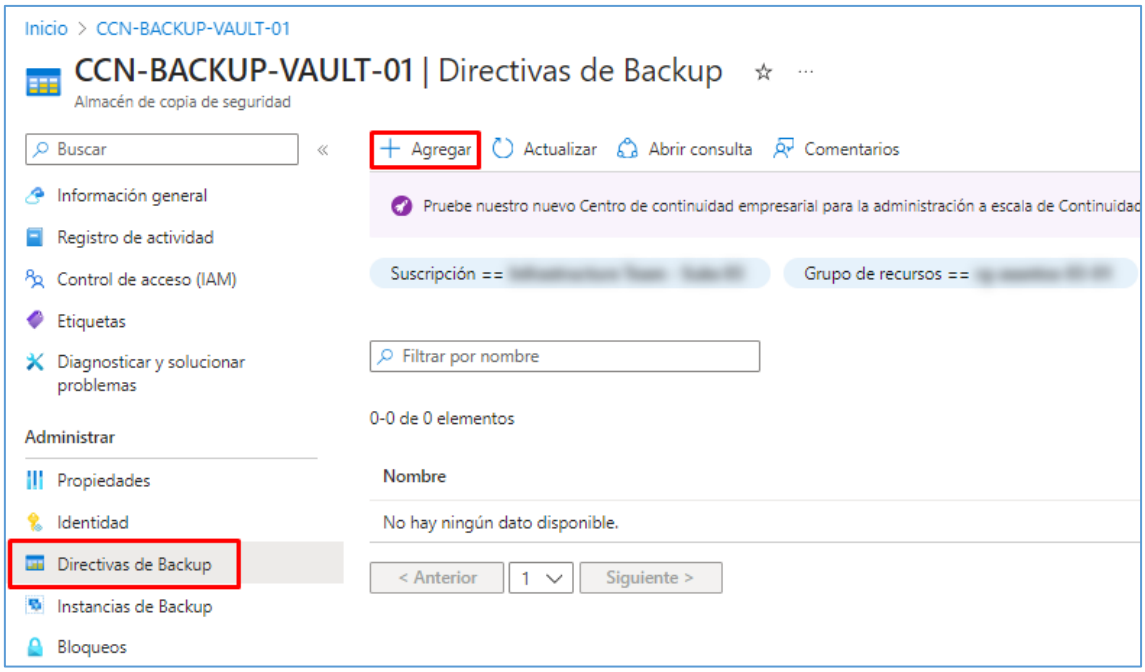
c) Con estos datos, pulsamos en el botón de Revisar y crear de la parte inferior de la pantalla.

d) Una vez creado, podemos pulsar en el botón de ir al recurso o acceder a él desde el listado de Almacenes de copias de seguridad usando el buscador.

CREAR DIRECTIVAS DE BACKUP

Para crear directivas de backup necesitamos previamente tener creado un Almacén de copias de seguridad, en este caso lo hemos creado en el apartado anterior.

Buscamos nuestro almacén mediante el buscador Almacenes de copia de seguridad, allí tendremos un listado con ellos y elegimos el que corresponda. Una vez dentro del almacén pulsamos sobre la opción Directivas de Backup de la columna izquierda y pulsamos sobre el botón de Agregar.



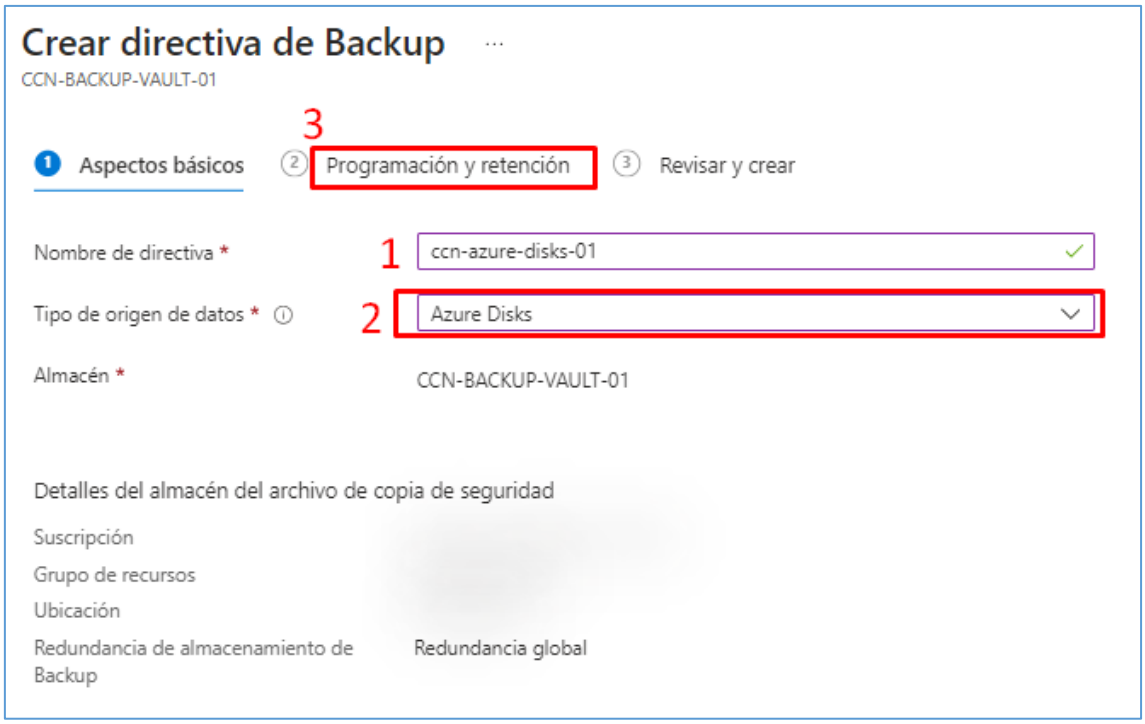
En la siguiente ventana tenemos que rellenar el Nombre de la directiva y el tipo de origen de datos y dependiendo de esta sección, la siguiente pestaña de programación y retención nos ofrecerá diferentes opciones que vamos a mostrar a continuación.

En esta guía no se explicará cómo crear directivas de Backup para los orígenes de datos de **Servidores flexibles de Azure Database for PostgreSQL** ni de **Azure Database for MySQL** ya que actualmente se encuentran en su versión preliminar.

ORIGEN DE DATOS: AZURE DISKS

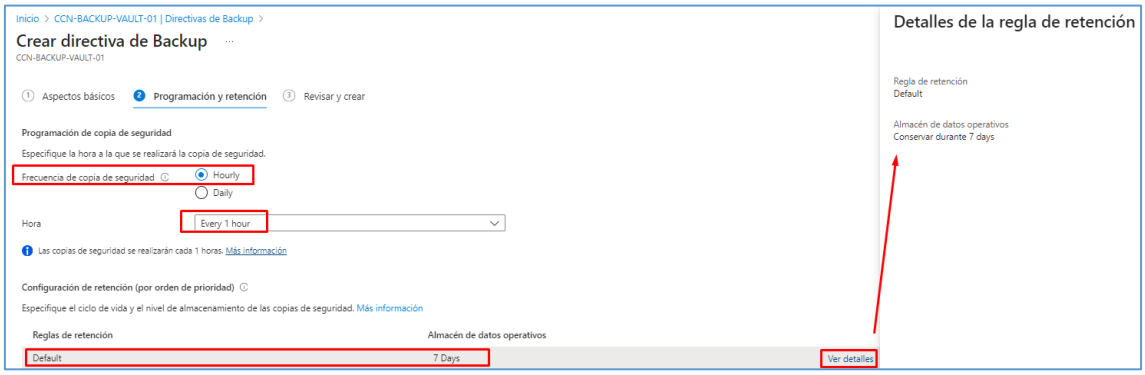
Para crear una directiva de backup de Azure Disk realizamos la siguiente configuración:

a) En la sección de **Aspectos Básicos** elegimos el origen de datos que corresponde a Azure Disks y asignamos un nombre a la directiva.

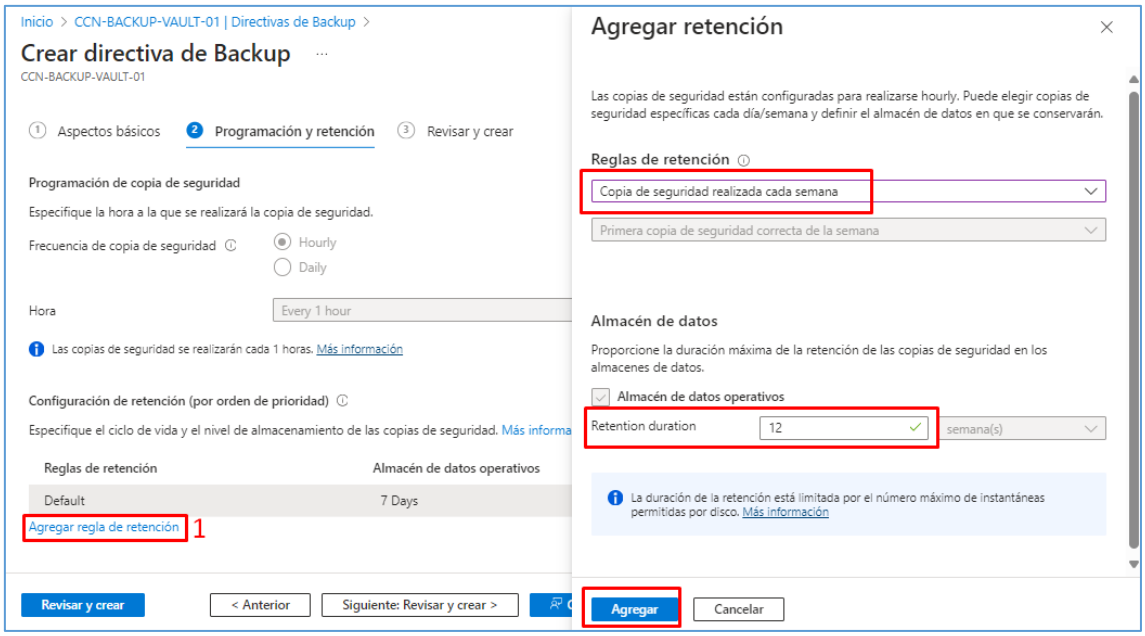


b) Sobre la pestaña **Programación y retención** elegimos la frecuencia de la copia de seguridad.

c) También podemos crear más reglas de retención además de la de por defecto, en este caso, la regla por realizará una copia de seguridad cada día y configura una retención de 7 días.

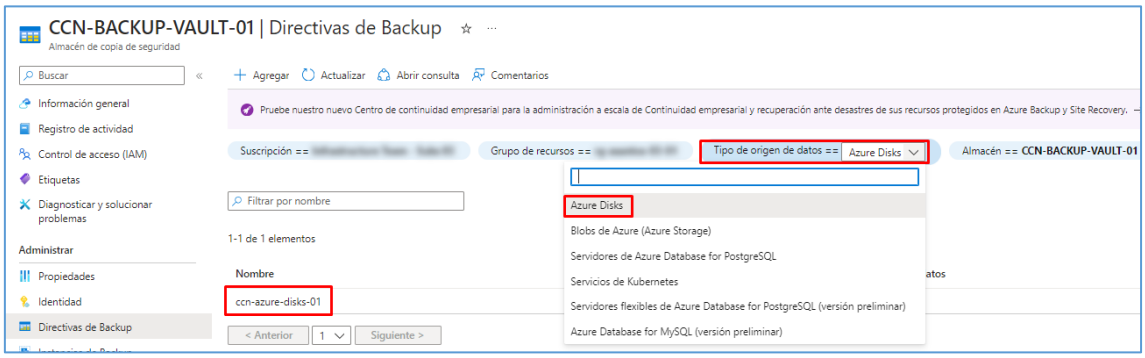


d) Crearemos una regla para una copia realizada cada semana que tendrá una retención de 12 semanas. Pulsamos en el botón Agregar.



e) Una vez creada la regla, pulsamos en revisar y crear y después en crear.

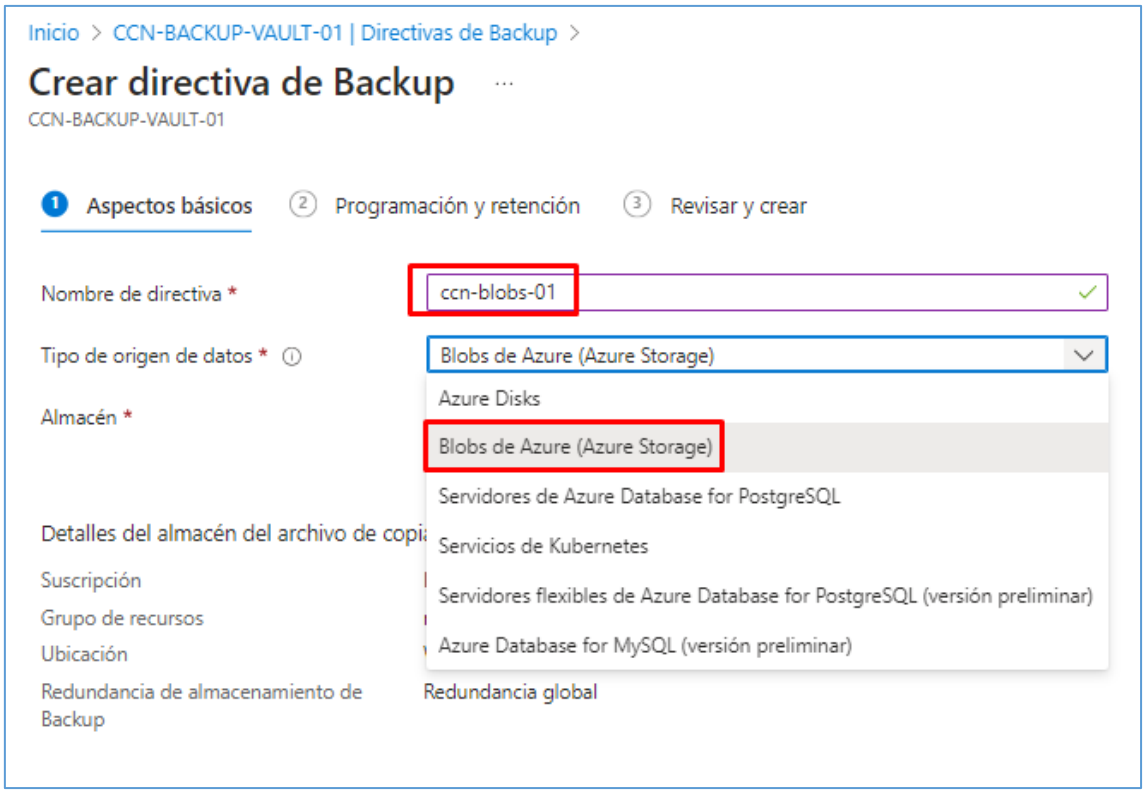
Para ver la directiva creada, podemos hacerlo desde el aparado Directivas de Backup y utilizar el filtro de **Tipo de origen de datos correcto.**



ORIGEN DE DATOS: BLOBS DE AZURE

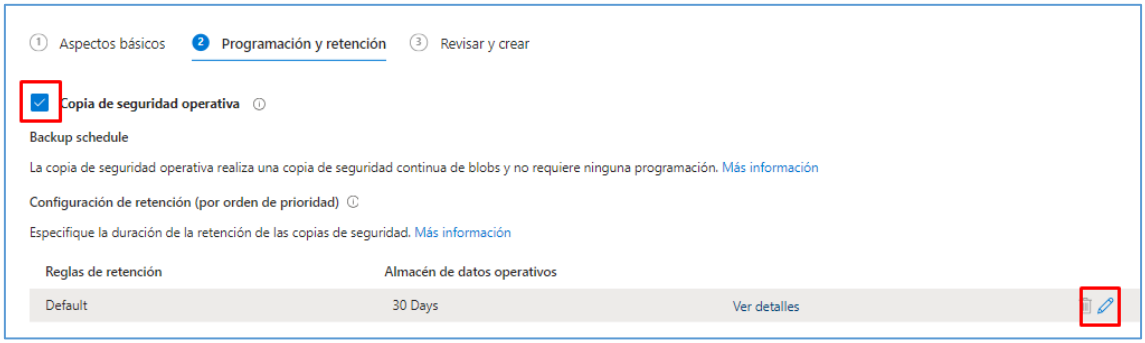
Para crear una directiva de Blobs de Azure realizamos la siguiente configuración:

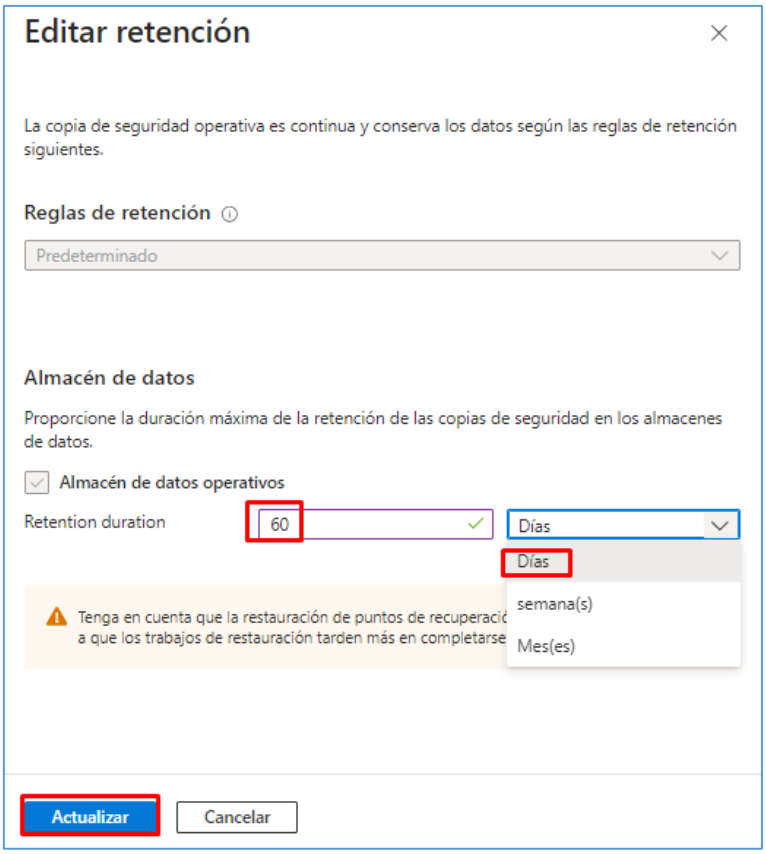
a) En la sección de **Aspectos Básicos** elegimos el origen de datos que corresponde a Blobs de Azure y asignamos **un nombre a la directiva**.



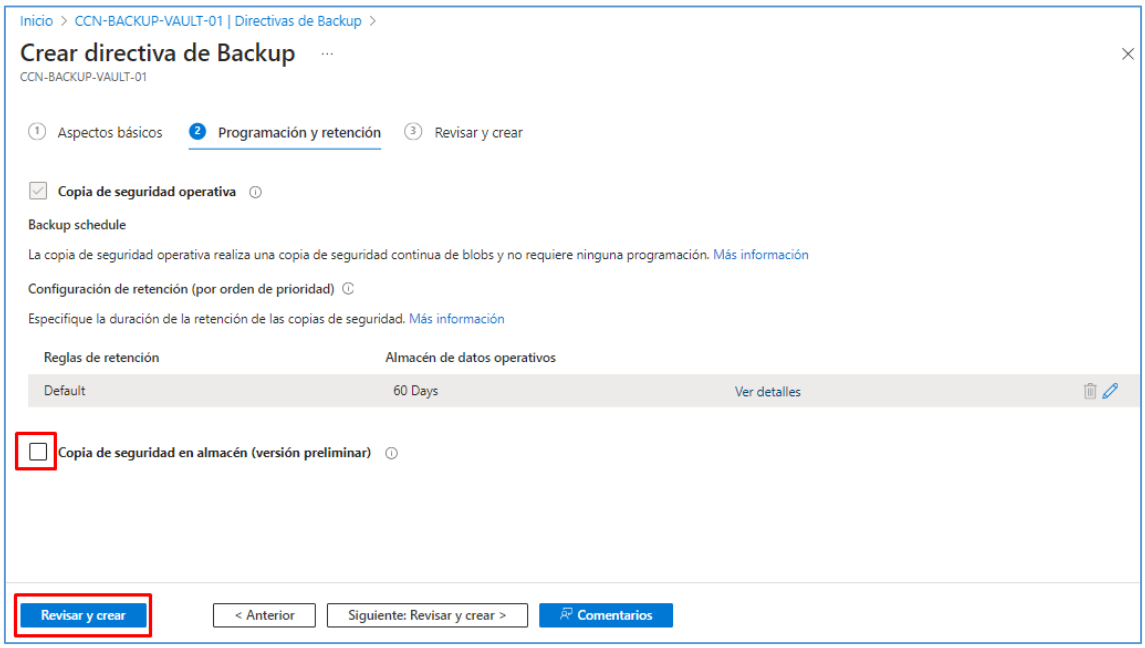
b) Sobre la pestaña **Programación y retención.** Marcamos la copia de seguridad operativa. Las copias de seguridad operativas se almacenan localmente y protegen los datos de origen contra la eliminación o modificación accidental. La redundancia del almacén no se aplica a las copias de seguridad operativas. Más información.

c) Modificamos la regla de retención por defecto a en vez de 30 días, 60, pero esto puede estar definido por la organización de manera interna. Para ello, utilizamos el icono del lápiz.

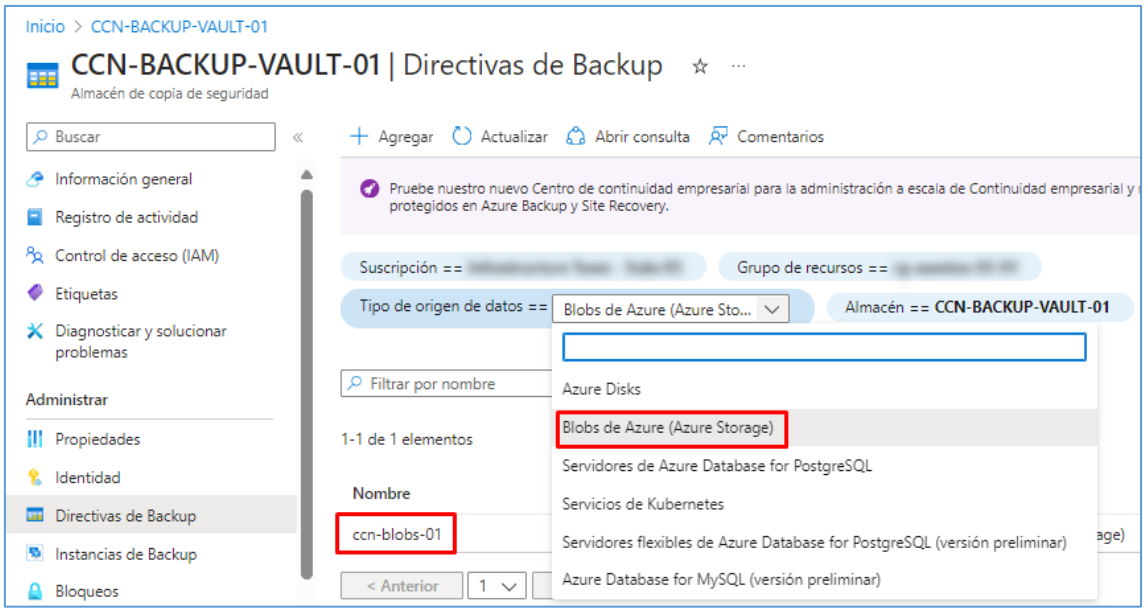




d) Por el momento desmarcamos la Copia de seguridad en almacén que, aunque es una opción muy interesante, por el momento se mantiene en su versión preliminar. Pulsamos en el botón de Revisar y crear y finalmente en Crear.



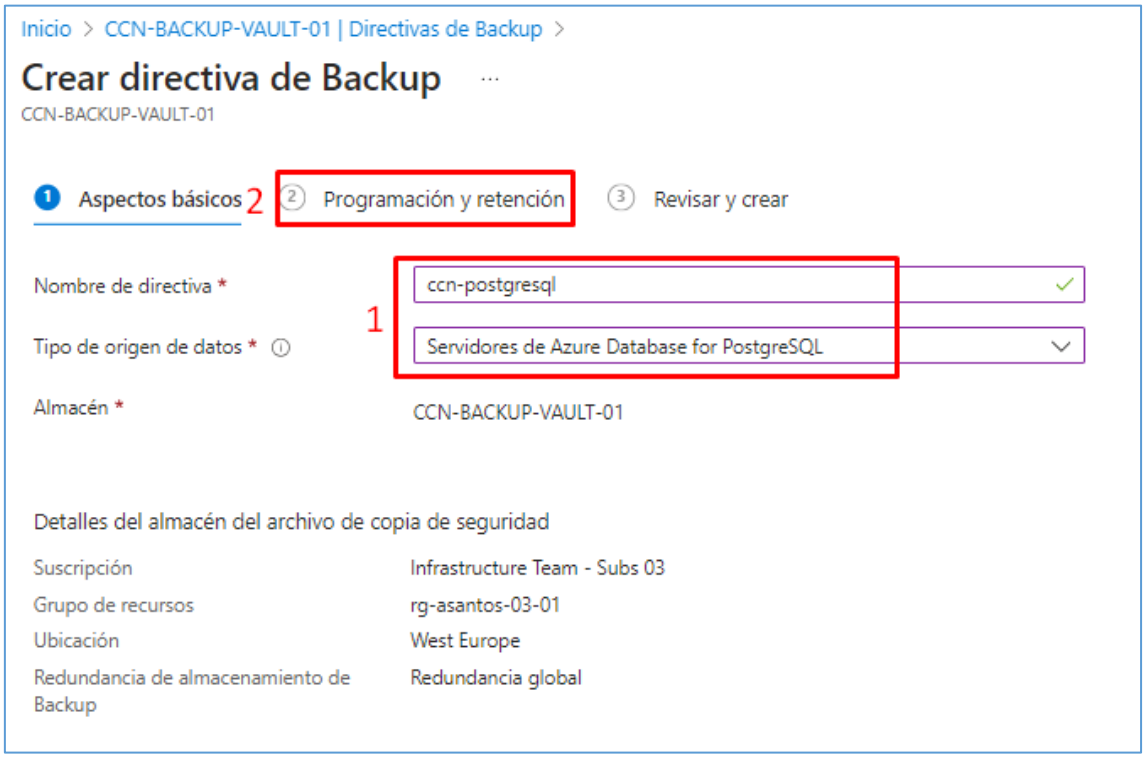
Para ver la directiva creada, podemos hacerlo desde el aparado Directivas de Backup y utilizar el filtro de **Tipo de origen de datos correcto.**



ORIGEN DE DATOS: SERVIDORES DE AZURE DATABASE FOR POSTGRESQL

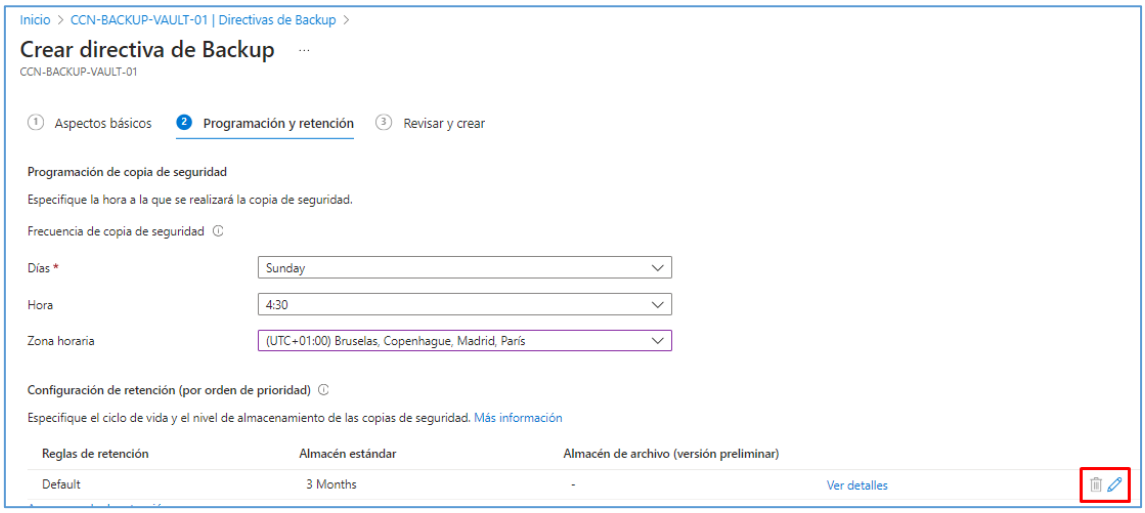
Para crear una directiva de Servidores de Azure Database para PostgreSQL realizamos la siguiente configuración:

a) En la sección de **Aspectos Básicos** elegimos el origen de datos que corresponde a Servidores de Azure Database para PostgreSQL y asignamos **un nombre a la directiva**.

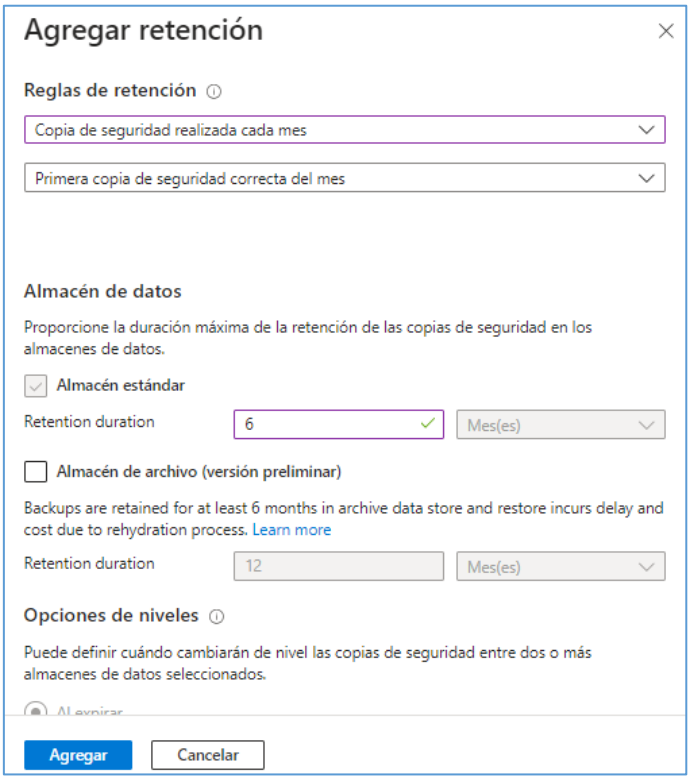


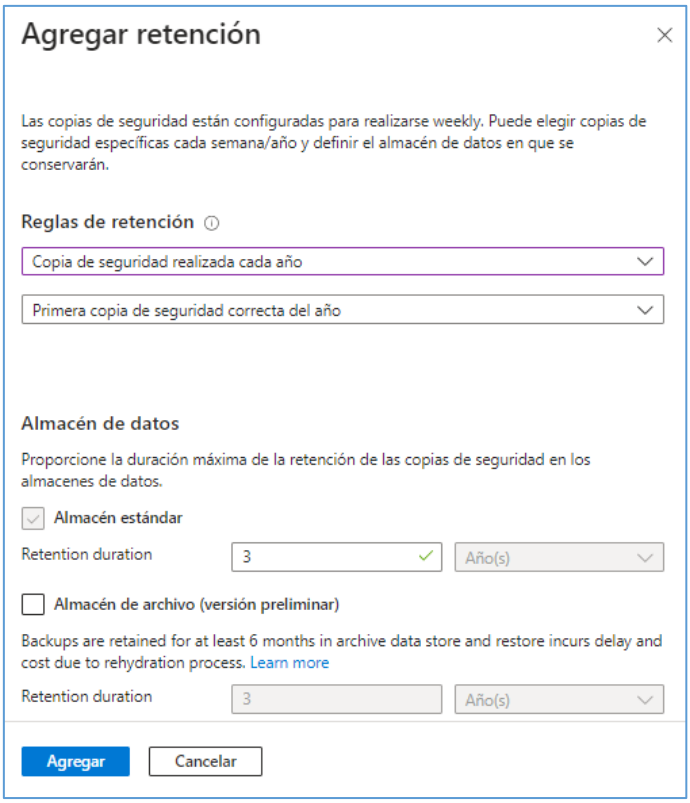
b) Sobre la pestaña **Programación y retención.** Elegimos los días que realizarán las copias de seguridad, siendo todos los días de la semana o días concretos. Elegiremos los domingos a las 4:30 de la zona horaria perteneciente a UTC+1.

La regla de retención por defecto utiliza el almacén estándar y una retención de 3 meses. Se puede editar como se muestra en la imagen.

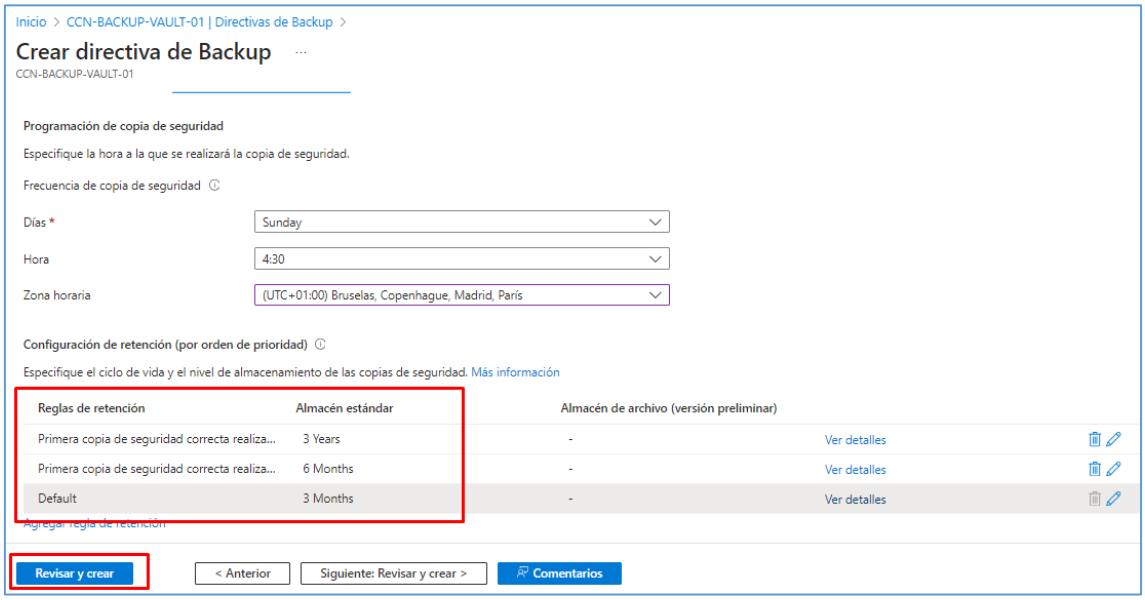


c) Además de esa regla, vamos a crear otra **regla mensual con una retención de 6 meses** y otra **anual con una retención de 3 años**, como se muestra en las siguientes imágenes:

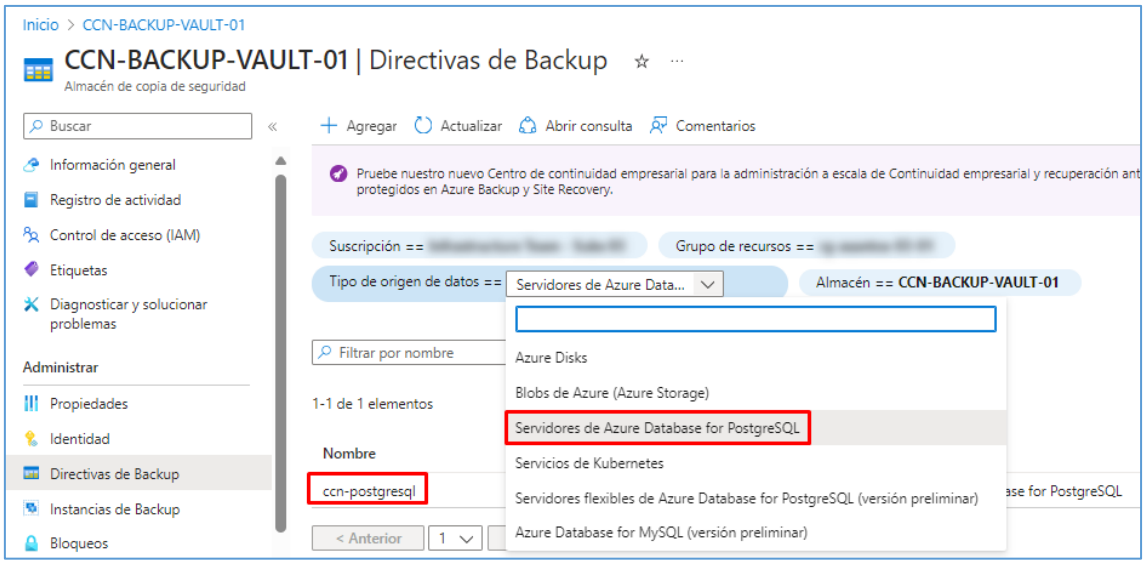




d) Podemos ver la configuración de las 3 reglas y pulsamos en el botón de revisar y crear y finalmente en Crear.



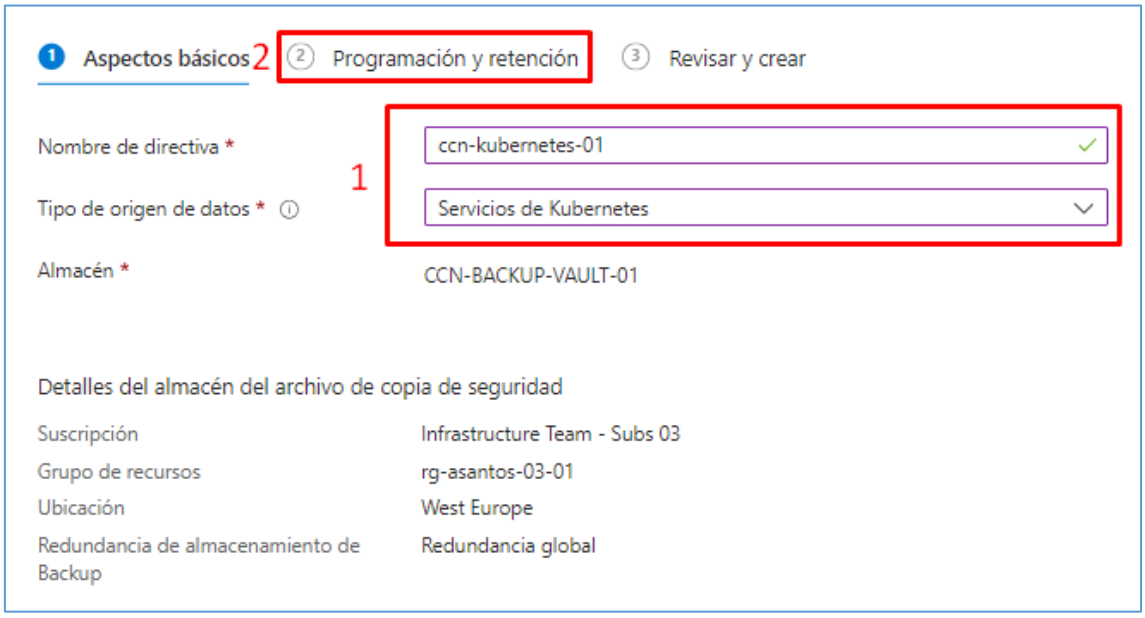
Para ver la directiva creada, podemos hacerlo desde el aparado Directivas de Backup y utilizar el filtro de **Tipo de origen de datos correcto.**



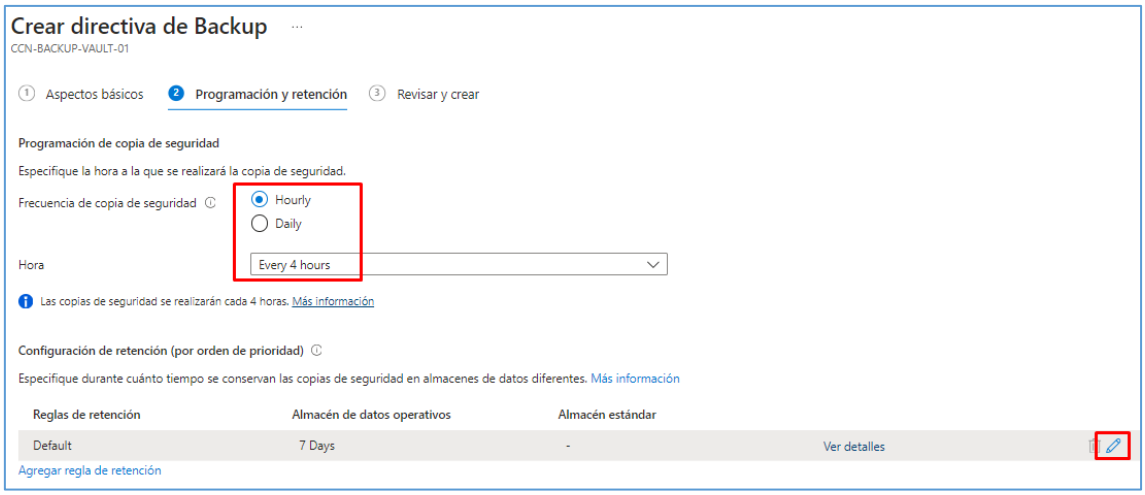
ORIGEN DE DATOS: SERVICIOS DE KUBERNETES

Para crear una directiva de Servicios de Kubernetes realizamos la siguiente configuración:

a) En la sección de **Aspectos Básicos** elegimos el origen de datos que corresponde a Servicios de Kubernetes y asignamos un nombre a la directiva.



b) Sobre la pestaña **Programación y retención** elegimos la frecuencia de la copia de seguridad. Y podemos editar o ver la regla de retención por defecto.

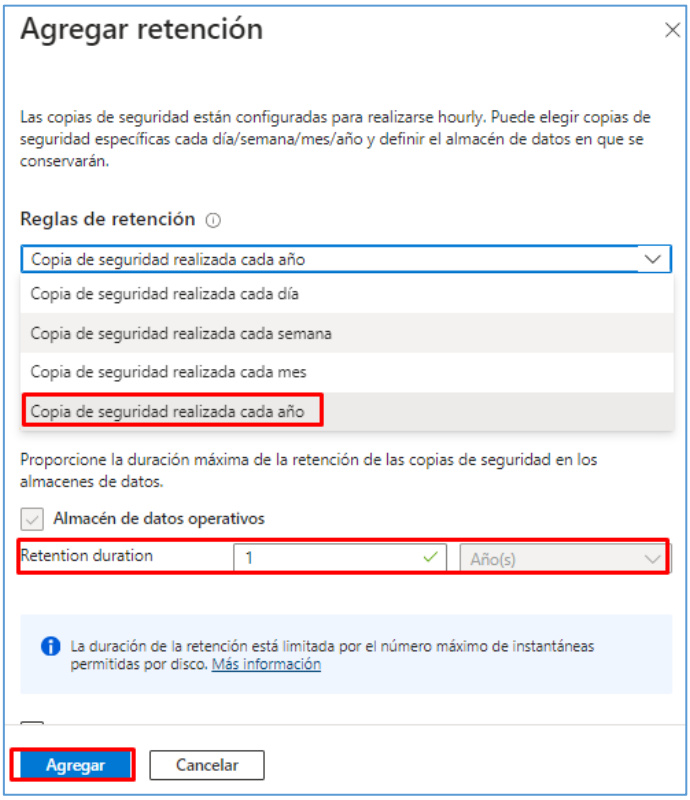


c) Vamos a crear más reglas de retención en este caso, crearemos:

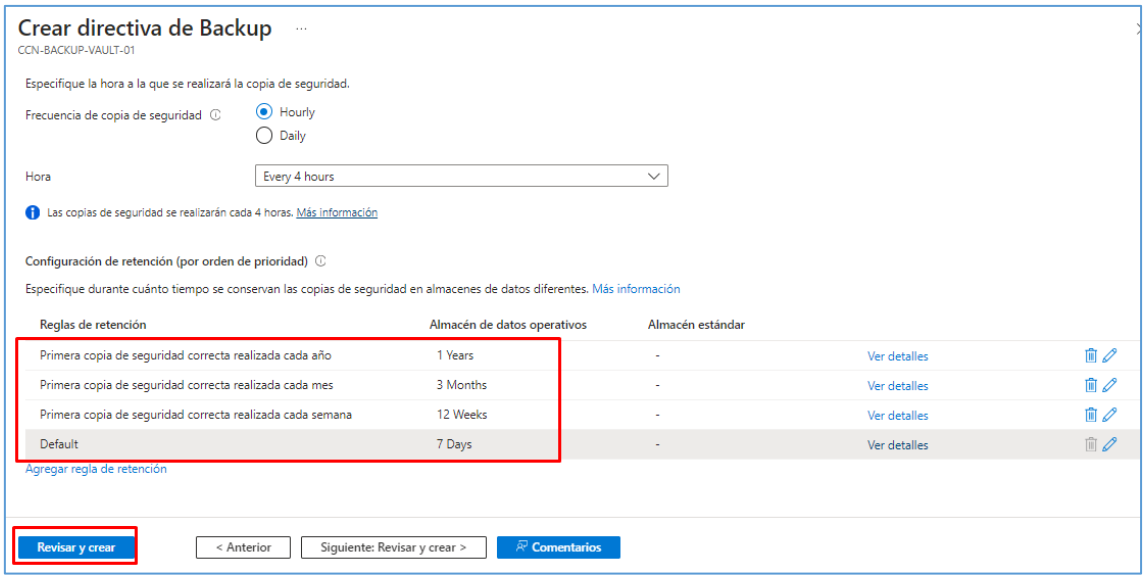
   a. Una copia de seguridad realizada cada semana con una retención de 12 semanas.

   b. Una copia de seguridad realizada cada mes con una retención de 3 meses

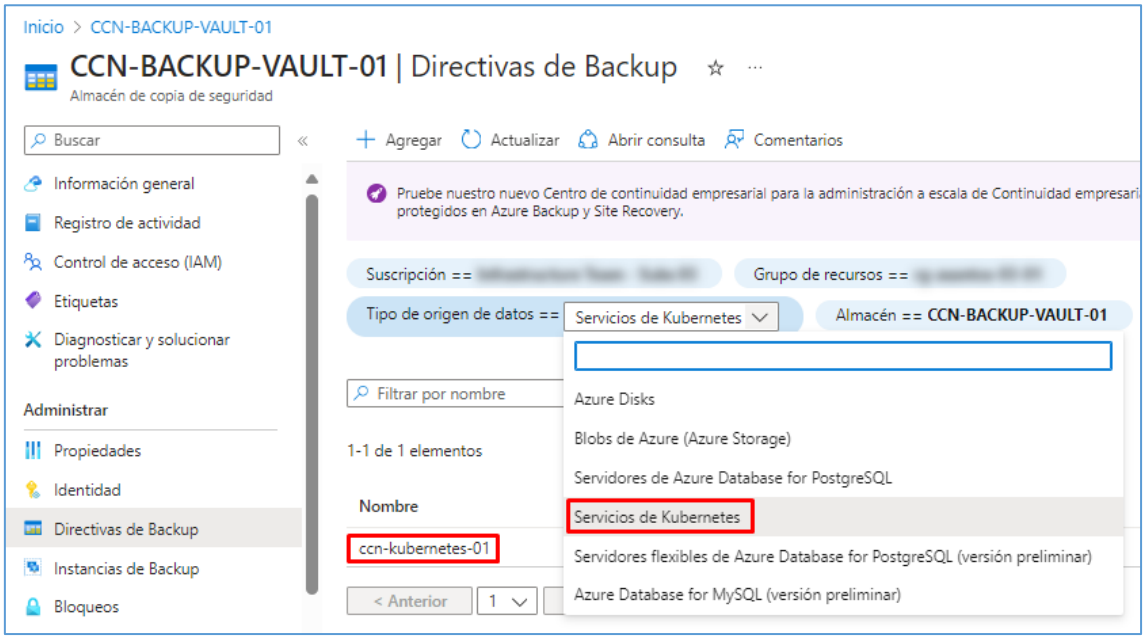
   c. Una copia de seguridad realizada cada año con una retención de 1 años.



d) Podemos ver la configuración de las 3 reglas y pulsamos en el botón de Revisar y crear y finalmente en Crear.

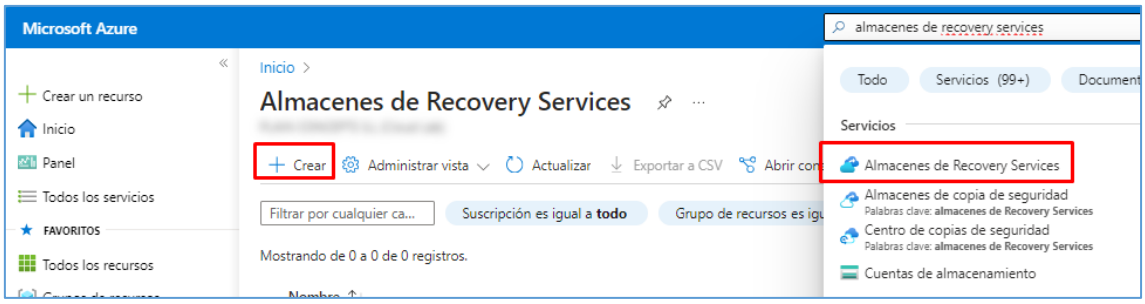


Para ver la directiva creada, podemos hacerlo desde el aparado Directivas de Backup y utilizar el filtro de **Tipo de origen de datos correcto.**



ALMACENES DE RECOVERY SERVICE

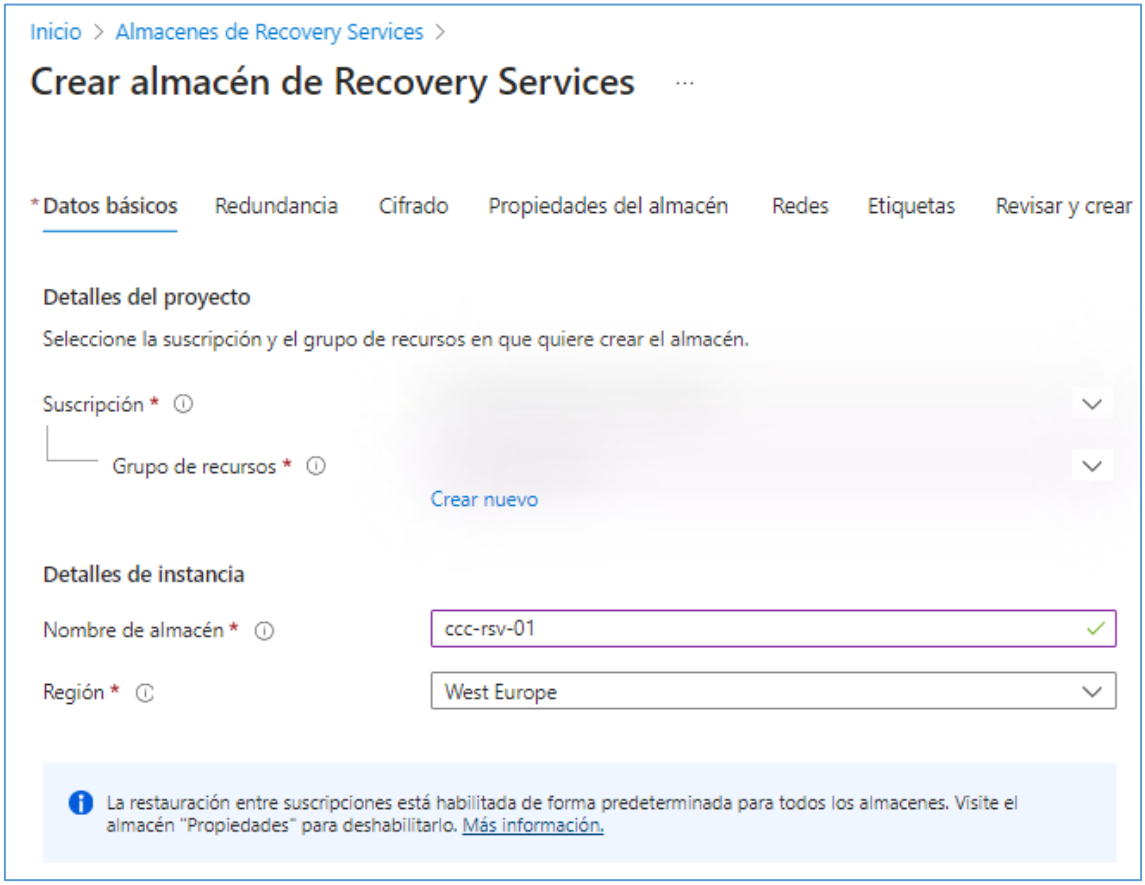
Para crear un almacén de Recovery Services utilizamos el buscador con **almacenes de copia de seguridad.** Una vez allí, pulsamos sobre el botón Crear.



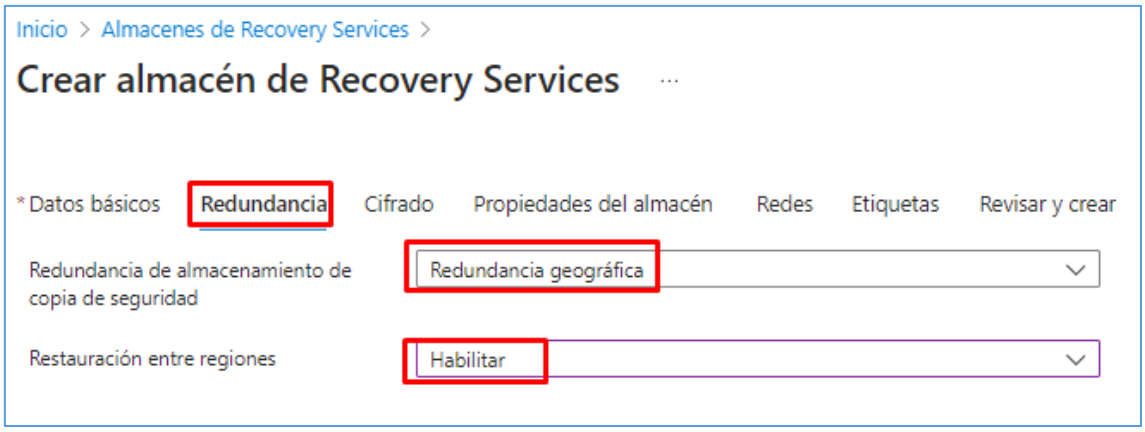
En la ventana de Crear un almacén de Recovery Services, nos movemos sobre las diferentes pestañas rellenando la información que nos piden.

a) Datos Básicos:

- Suscripción
- Grupo de recursos
- Nombre del almacén
- Región

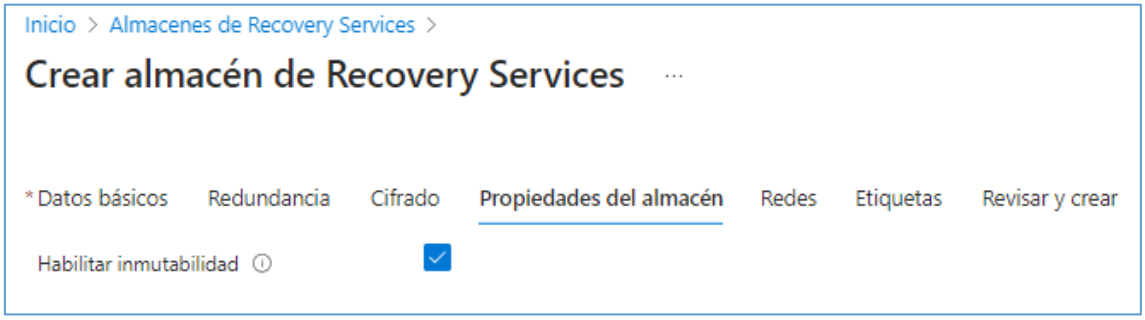


b) Redundancia: Elegiremos una redundancia geográfica. Si quiere elegir entre otras opciones puede consultar el siguiente enlace: Información general de los almacenes de Backup - Azure Backup | Microsoft Learn y habilitaremos la restauración entre regiones.

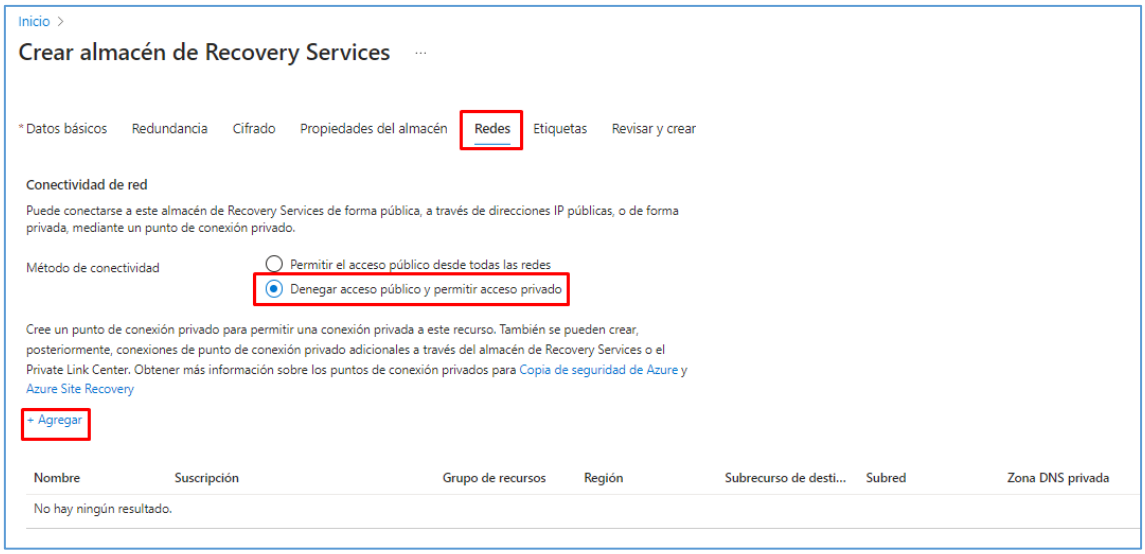


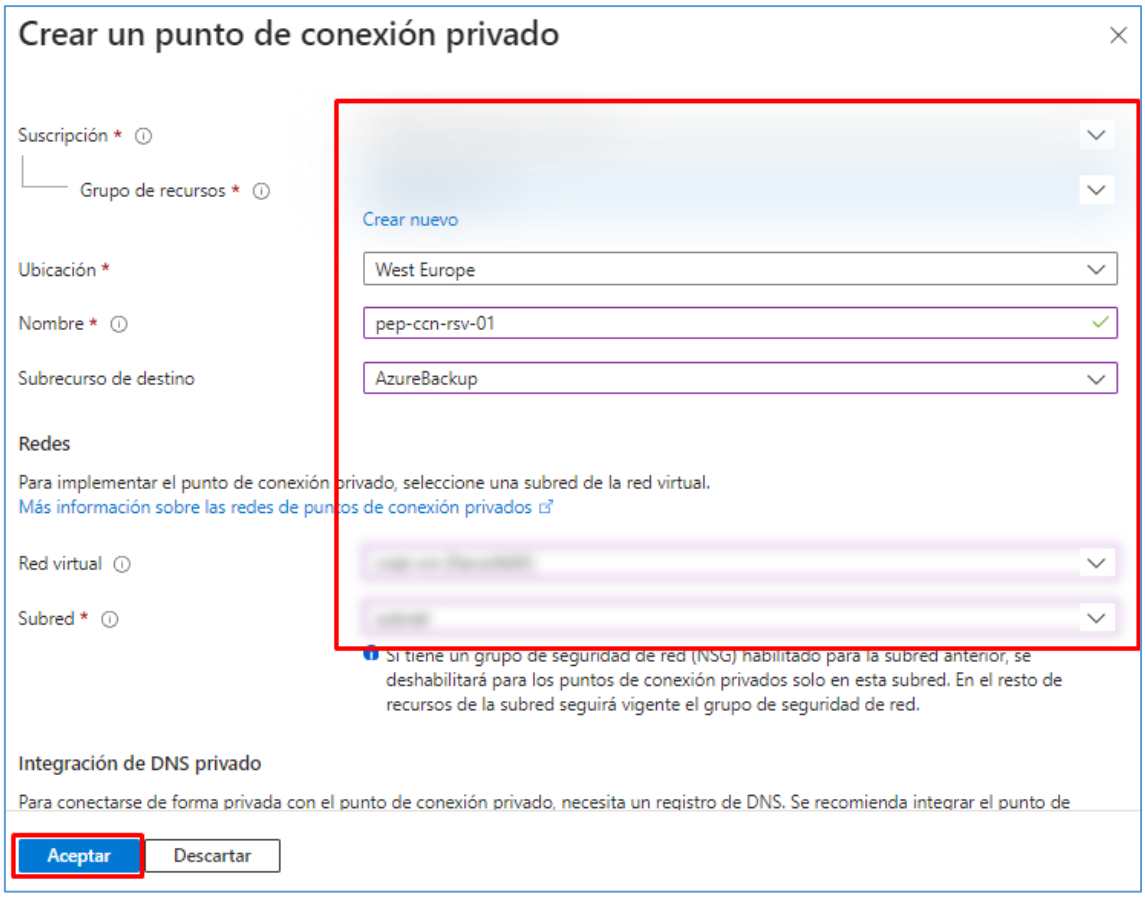
c) Cifrado: Utilizaremos la opción de Usar clave administrada por Microsoft, para tener más información sobre este punto puede visitar: Cifrado de datos de copia de seguridad mediante claves administradas por el cliente - Azure Backup | Microsoft Learn

d) Propiedades del almacén: Habilitamos la inmutabilidad para impedir realizar ciertas operaciones en el almacén que podrían provocar perdida de datos. Más información en Concepto de almacén inmutable de Azure Backup - Azure Backup | Microsoft Learn.

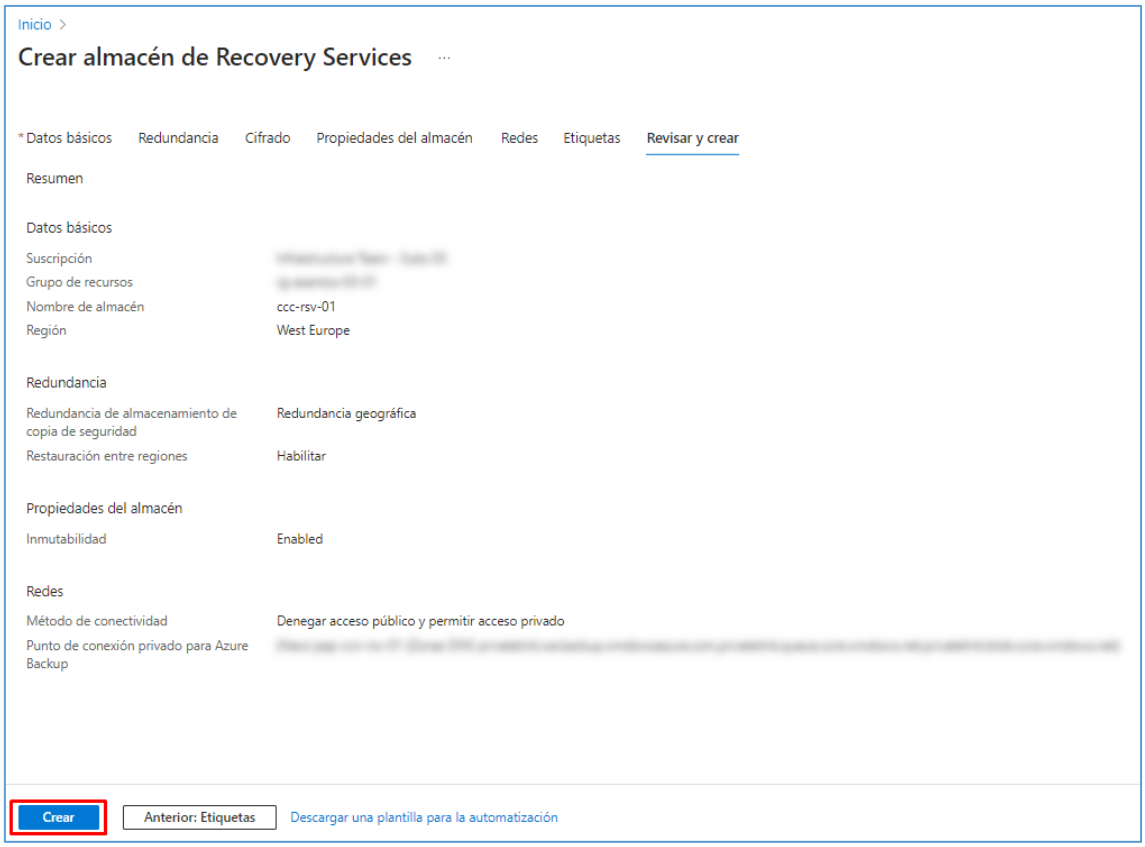


e) Redes: El método de conectividad será **Denegar acceso público y permitir acceso privado** y al denegar el acceso debemos crear un punto de conexión privado. Para ello hay que elegir la red virtual y la subred, que debe ser creada con anterioridad a la creación del almacén.





f) Con estos datos, podemos revisar lo elegido anteriormente, pulsando en el botón inferior de Revisar y Crear y finalmente Crear.



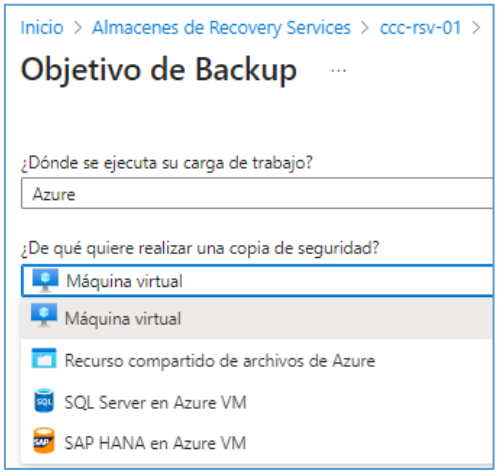
Una vez creado podremos realizar copias de seguridad de desde la opción de navegación [Copia de seguridad].

a) Máquinas Virtuales.

b) Recursos compartidos de archivos de Azure.

c) SQL Server en Azure VM.

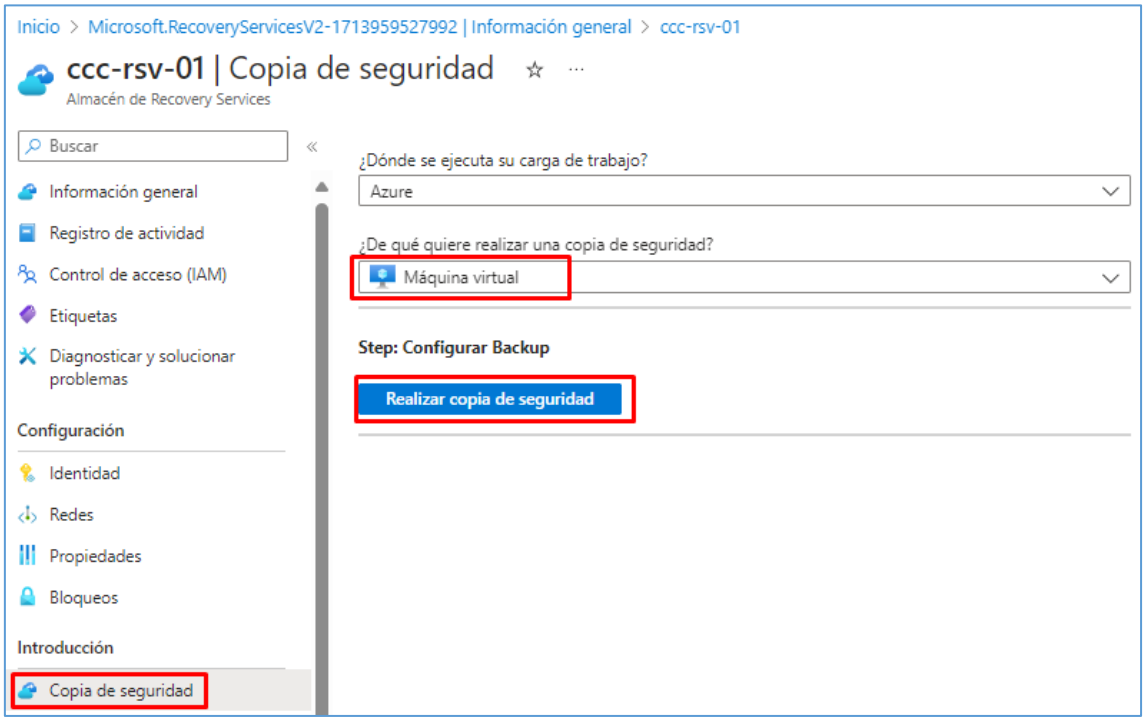
d) SAP HANA en Azure VM.



CONFIGURACIÓN DE COPIAS DE SEGURIDAD EN MÁQUINAS VIRTUALES

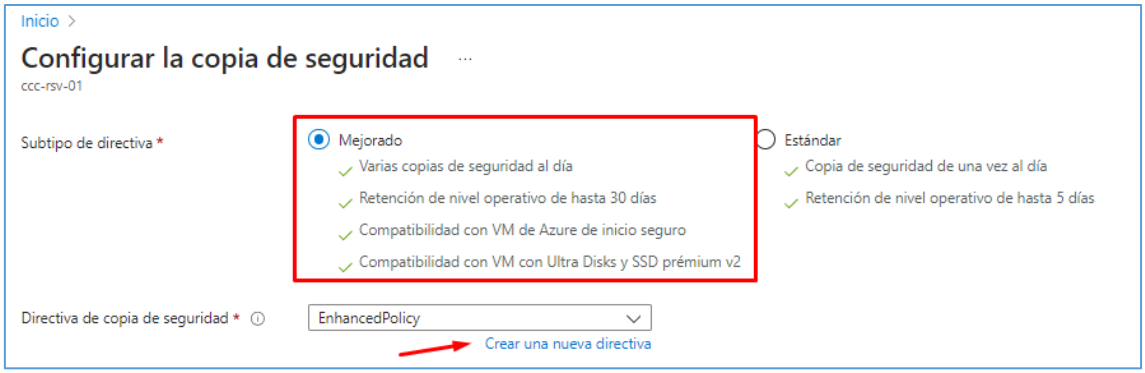
Para configurar copias de seguridad en máquinas virtuales accedemos al almacén buscando [Almacenes de Recovery Services].

a) Accedemos al Almacén de Recovery Services y navegamos a la opción [Copia de seguridad]. Vamos a realizar una copia de una Máquina Virtual y pulsamos en [Realizar copia de seguridad].

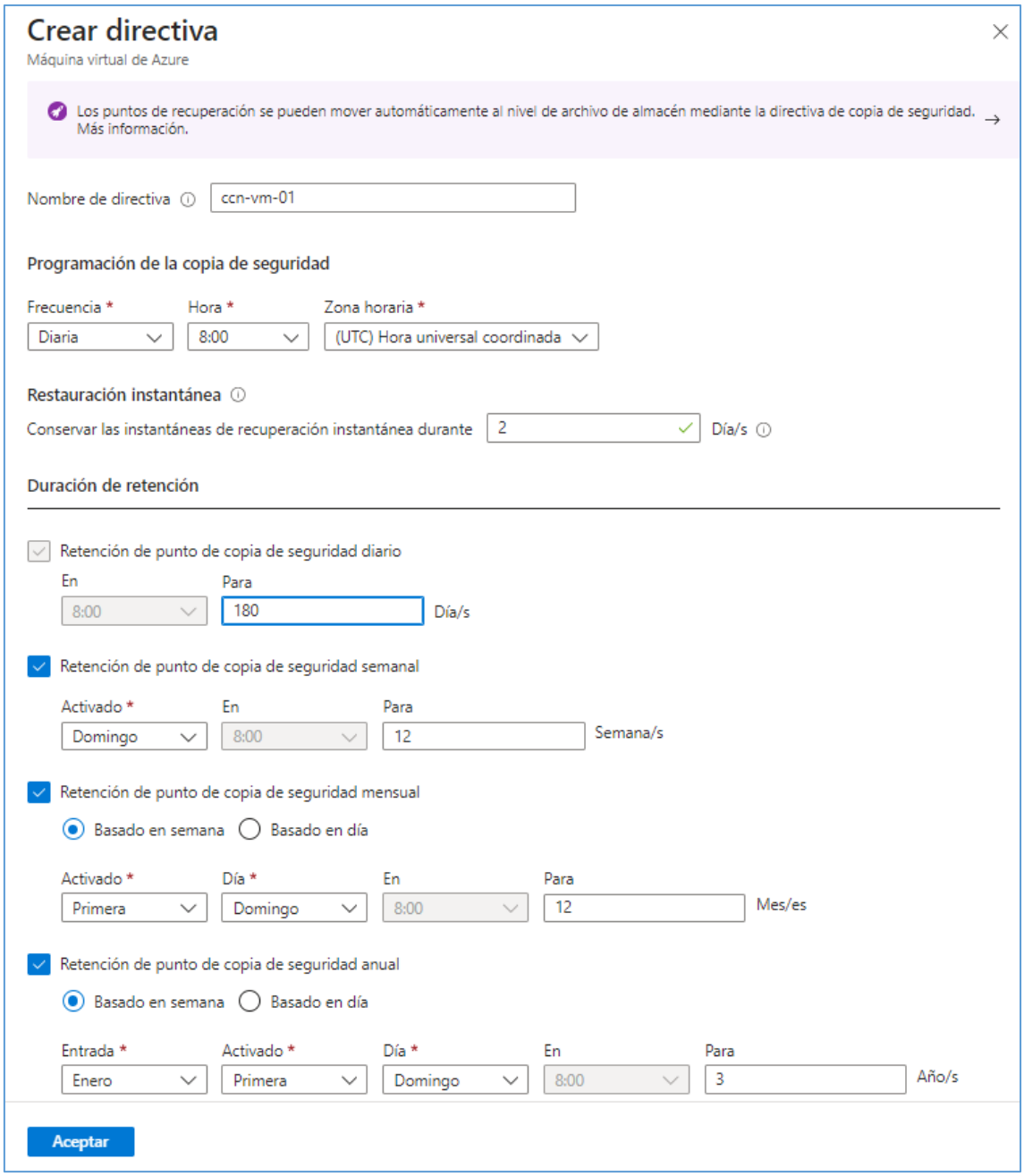


b) Elegiremos el subtipo de directiva Mejorado, ya que ofrece compatibilidad con VM de Azure de inicio seguro y Ultra Disks y SSD prémium v2.

c) Creamos una directiva de copia de seguridad pulsando sobre [Crear una nueva directiva].



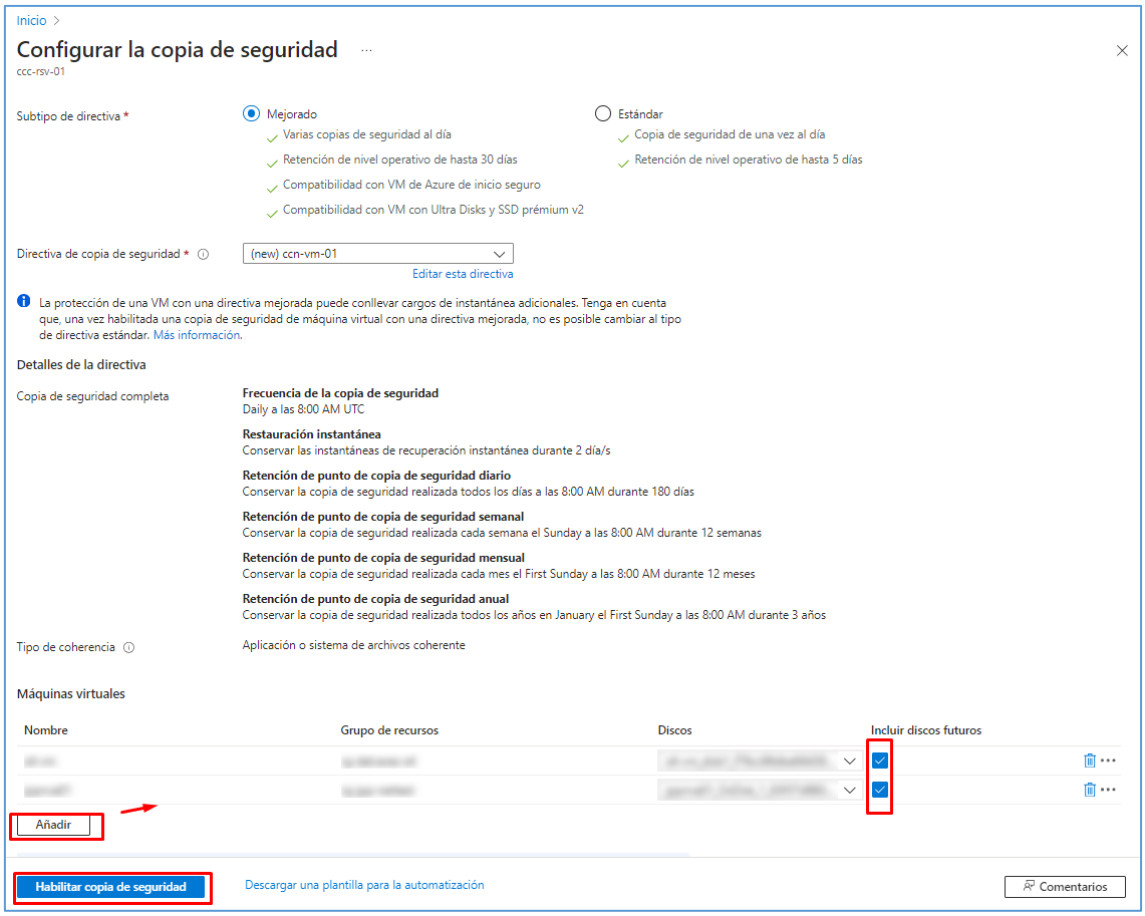
d) Configuramos una copia semanal con una retención de 12 semanas, una copia mensual con una retención de 12 meses y una anual para 3 años. Y conservamos las instantáneas durante 2 días y una retención de 180 días.



e) Añadimos las máquinas virtuales de las que queremos realizar backups pulsando el botón de [Añadir] del apartado [Máquinas virtuales]. Se ofrece un listado de máquinas virtuales con un campo para filtrar por nombre, podemos elegir varias VMs del listado.

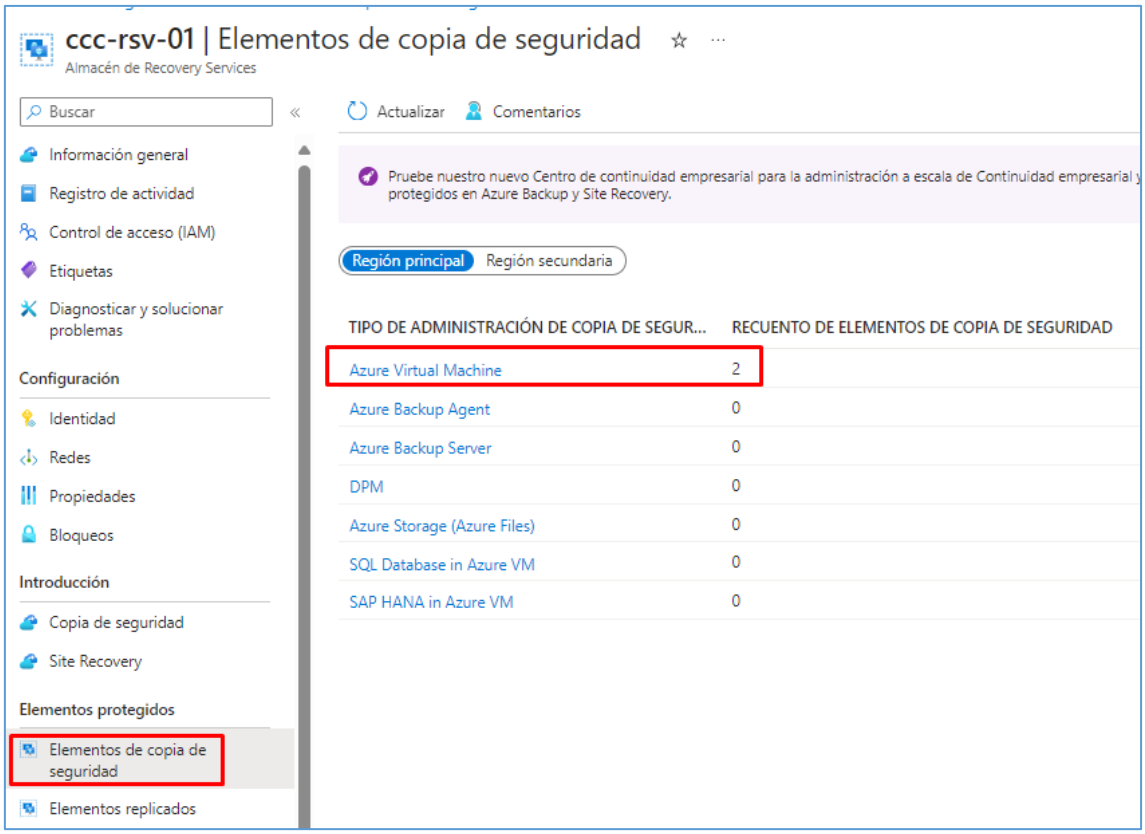
f) Confirmamos que dejamos marcada la opción de [Incluir discos futuros].

g) Pulsamos el botón de la parte inferior de [Hablitar copia de seguridad]. Estos parámetros pueden venir definidos por su Organización de manera interna.

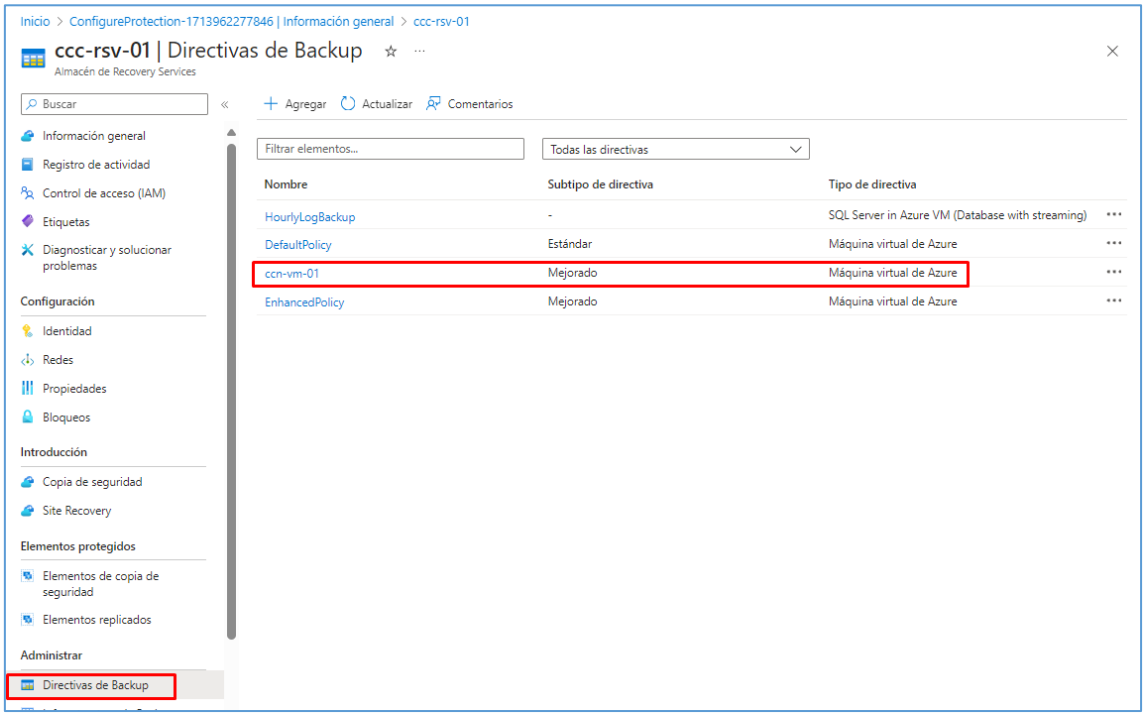


Para comprobar si una máquina está protegida por Azure Backup podemos realizar los siguientes pasos:

a) En el apartado de Elementos de copia de seguridad del Almacén de Recovery Services podemos ver un listado de las copias configuradas. Al pulsar sobre el apartado, se encuentra más información y detalles al respecto.

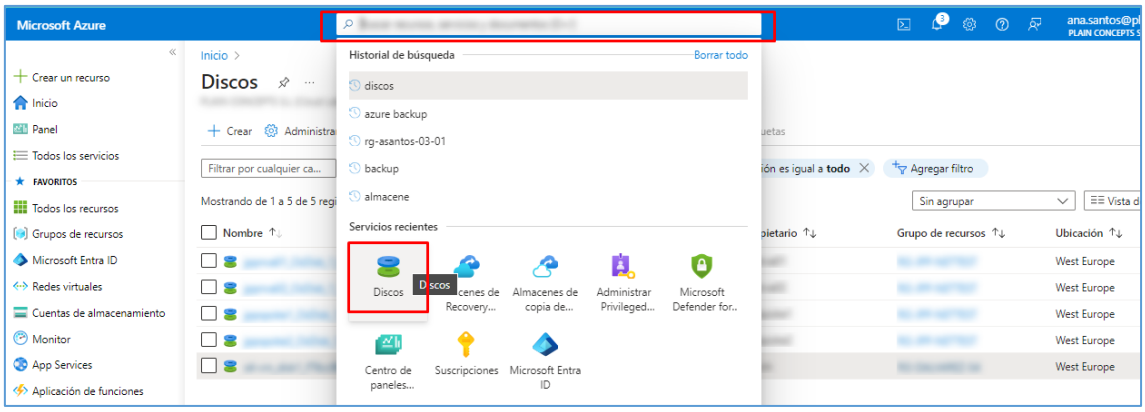


También se pueden ver las directivas que se han creado desde [Directivas Backup].



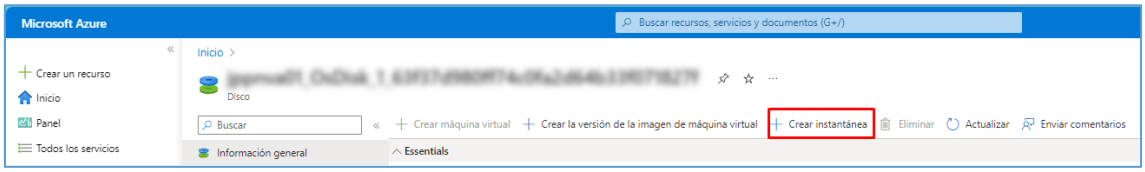
CREACIÓN DE COPIAS INSTANTÁNEAS EN DISCOS VIRTUALES

Se pueden realizar copias instantáneas de los discos, para ello escribimos en el buscador [Discos].



a) Pulsamos sobre el disco que nos interese, se abre una pestaña y accedemos al disco correspondiente.

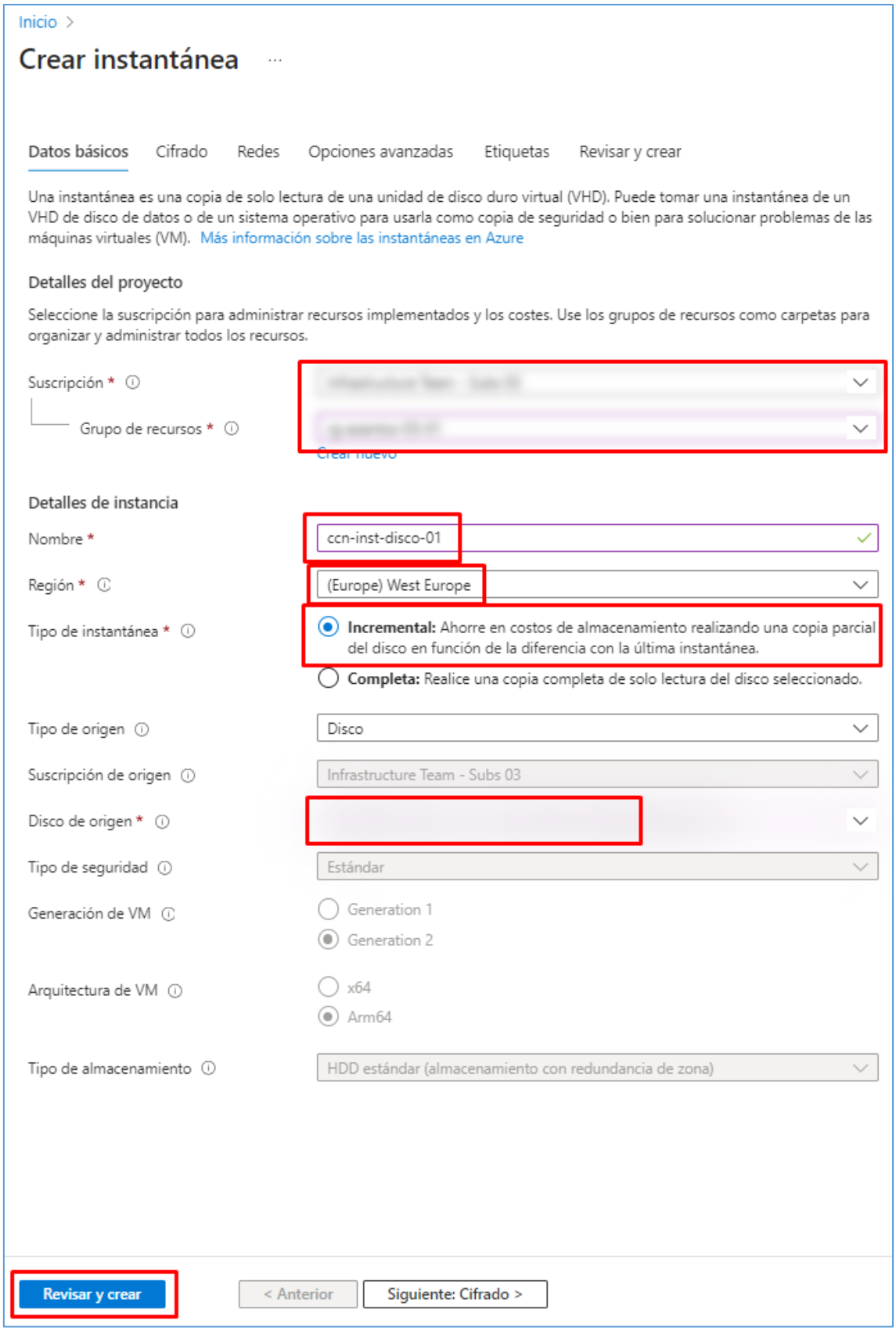
b) Pulsamos sobre [Crear instantánea].



c) Rellenamos con la información que se solicita:

   a. Suscripción
   b. Grupo de recurso
   c. Nombre de la instancia
   d. Región
   e. Tipo de Instantánea
   f. Origen
   g. Disco de Origen

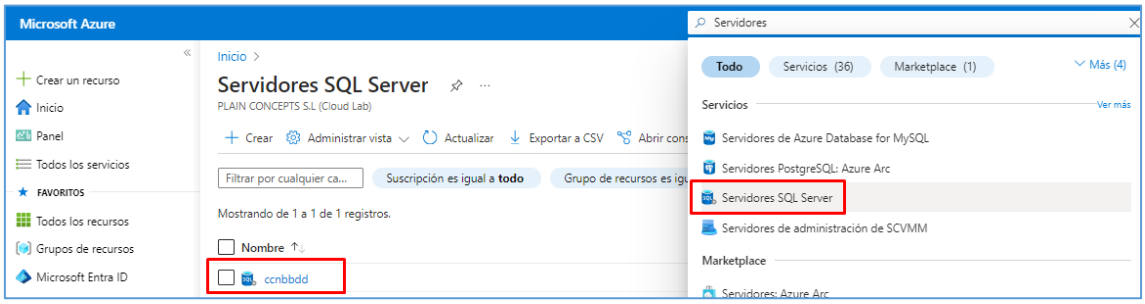
d) Pulsamos el botón de revisar y crear. Finalmente pulsamos sobre el botón crear.


Inicio >
Crear instantánea
Datos básicos
Cifrado
Redes
Opciones avanzadas
Etiquetas
Revisar y crear
Una instantánea es una copia de solo lectura de una unidad de disco duro virtual (VHD). Puede tomar una instantánea de un VHD de disco de datos o de un sistema operativo para usarla como copia de seguridad o bien para solucionar problemas de las máquinas virtuales (VM). Más información sobre las instantáneas en Azure
Detalles del proyecto
Seleccione la suscripción para administrar recursos implementados y los costes. Use los grupos de recursos como carpetas para organizar y administrar todos los recursos.
Suscripción *
Grupo de recursos *
Crear nuevo
Detalles de instancia
Nombre *
ccn-inst-disco-01
Región *
(Europe) West Europe
Tipo de instantánea *
Incremental: Ahorre en costos de almacenamiento realizando una copia parcial del disco en función de la diferencia con la última instantánea.
Completa: Realice una copia completa de solo lectura del disco seleccionado.
Tipo de origen
Disco
Suscripción de origen
Infrastructure Team - Subs 03
Disco de origen *
Tipo de seguridad
Estándar
Generación de VM
Generation 1
Generation 2
Arquitectura de VM
x64
Arm64
Tipo de almacenamiento
HDD estándar (almacenamiento con redundancia de zona)
Revisar y crear
< Anterior
Siguiente: Cifrado >

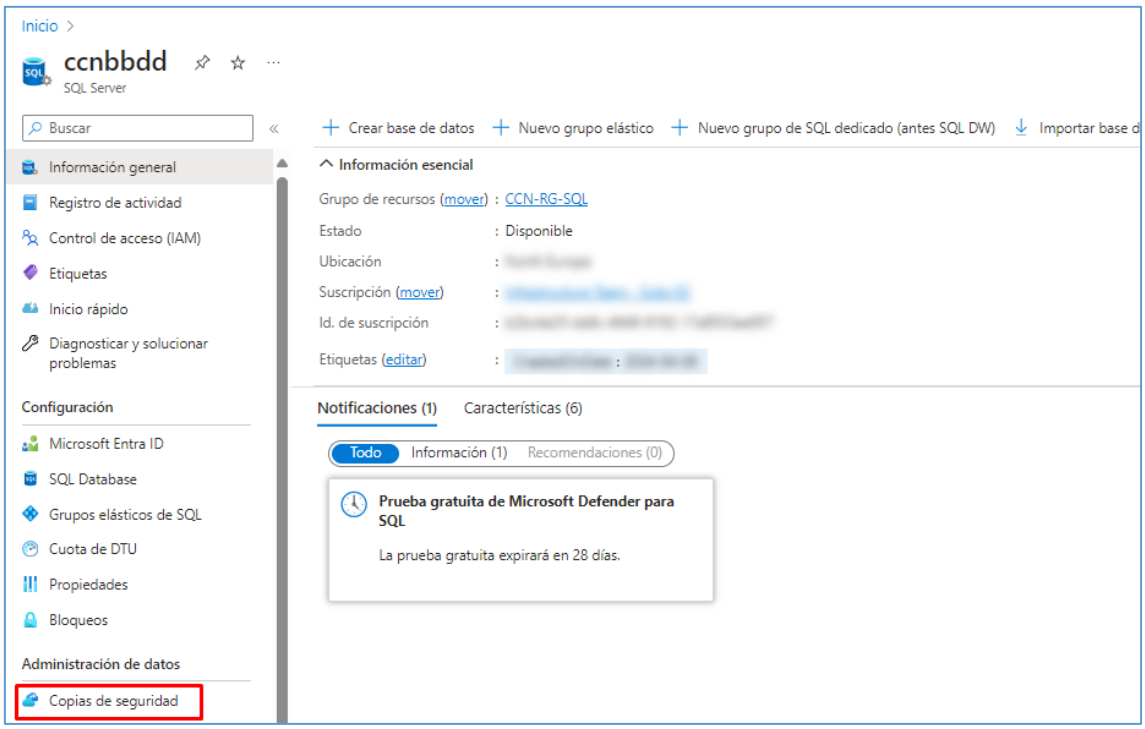
COPIAS DE SEGURIDAD EN BASES DE DATOS

En el caso de las bases de datos de Azure SQL, las copias de seguridad se crean automáticamente. En el apartado de "Copias de seguridad" del servidor SQL se pueden ver las diferentes copias de seguridad que hay disponibles para cada una de las bases de datos del servidor, así como poder administrar las copias de seguridad de retención a largo plazo (LTR). Desde este apartado también se puede restaurar una base de datos si así fuera necesario.

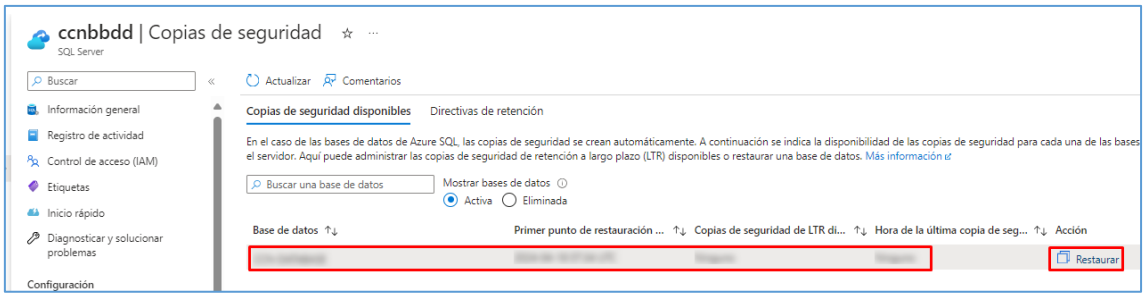
Utilizamos el buscador y escribimos Servidores SQL. Accedemos al servidor del que queremos restaurar o modificar los periodos de retención.



e) Pulsamos sobre el apartado [Copias de seguridad]

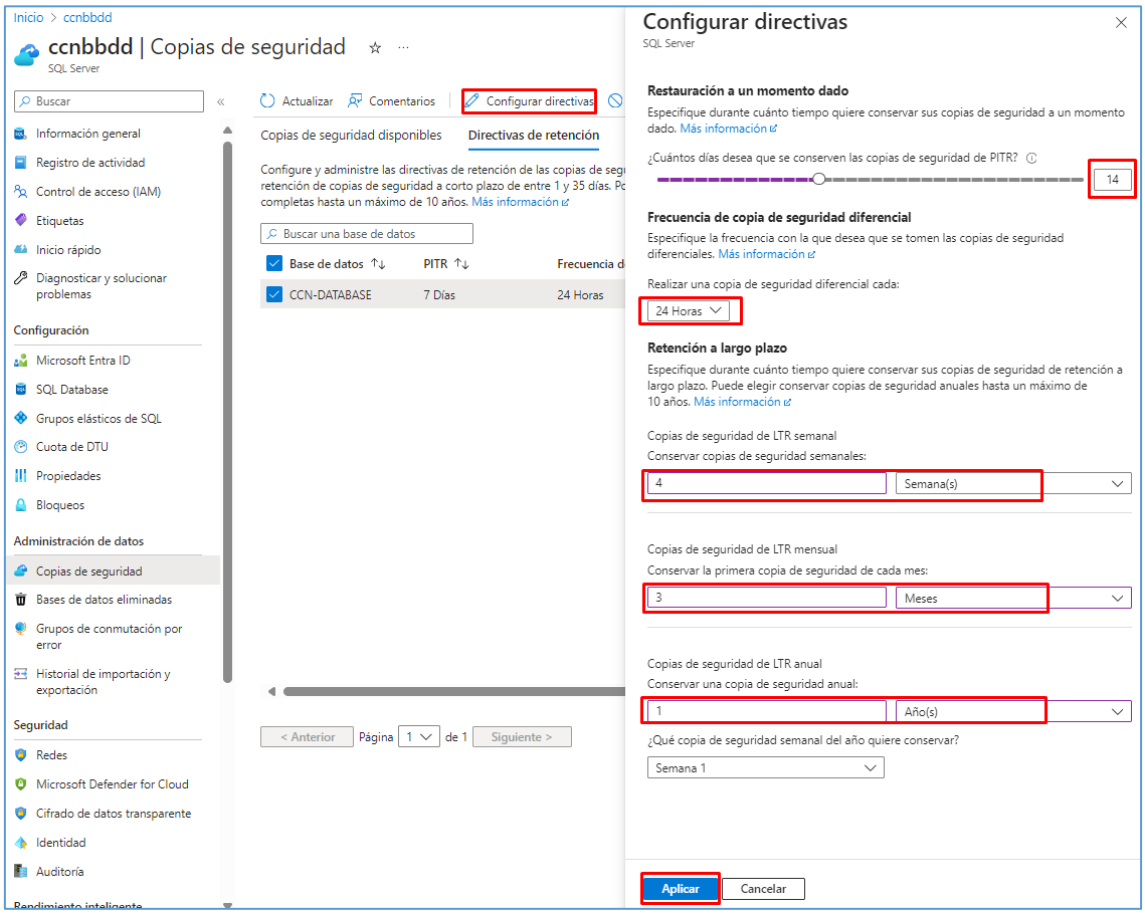


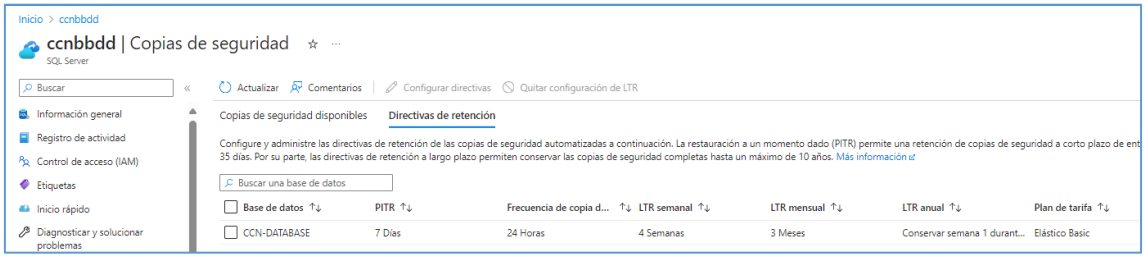
f) Una vez allí veremos la configuración de las copias disponibles y el botón restaurar en caso de querer realizar esa operación.



g) Sobre la pestaña [Directivas de retención] podemos modificar las directivas de retención o quitar la configuración de LTR (long term retention).

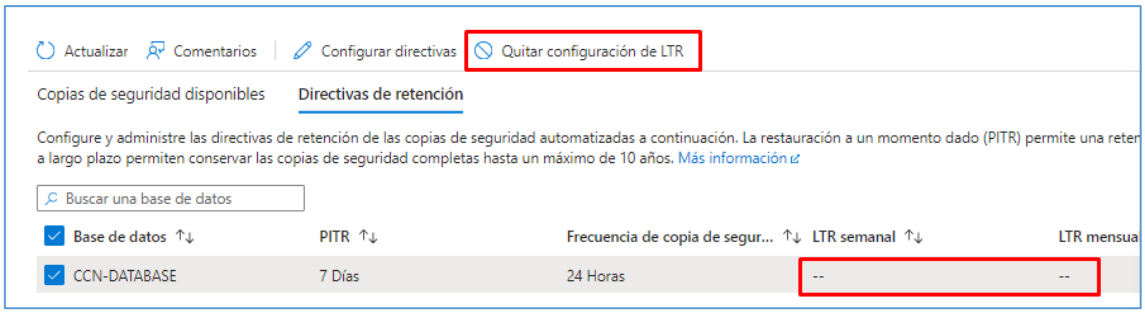
a. Configurar directivas: Se pueden configurar los días y conservar las copias semanal, mensual y anualmente.





Nota: Recomendamos configurar las LRT semanal, mensual y anualmente.

b. En caso de querer eliminar la configuración de LTR, puede realizarlo pulsando sobre la base de datos y después con el botón [Quitar configuración de LTR]



A continuación, se detallan las opciones de retención.

a) **Copias de seguridad LTR semanales:** Todas las copias de seguridad se guardan durante el período de retención establecido.
b) **Copias de seguridad LTR mensuales:** La primera copia de seguridad de cada mes se guarda durante el período de retención establecido
c) **Copias de seguridad LTR anuales:** La copia de seguridad creada durante la semana del año especificado se guarda durante el período de retención establecido.

3.2.3 PROTECCIÓN DE LOS SERVICIOS

3.2.3.1 PROTECCIÓN FRENTE A DENEGACIÓN DE SERVICIO

Azure proporciona protección continua contra los ataques de denegación de servicio. Esta protección se integra en la plataforma Azure mediante Azure DDoS Protection

DDoS Protection aprovecha la escalabilidad y la elasticidad de la red global de Microsoft para aportar una funcionalidad de mitigación de DDoS masiva en todas las regiones de Azure. El servicio DDoS Protection de Microsoft limpia el tráfico en la red perimetral de Azure antes de que pueda afectar a la disponibilidad del servicio, a fin de proteger las aplicaciones de Azure.

Hay dos niveles de DDoS Protection:

a) Protección de red contra DDoS (Azure DDoS Network Protection): Junto con los procedimientos recomendados de diseño de aplicaciones, proporciona características mejoradas de mitigación DDoS para protegerse de los ataques DDoS. Se ajusta automáticamente para proteger los recursos específicos de Azure de una red virtual.

b) Protección de IP de Azure contra DDoS: Es un modelo de IP de pago por protección. Protección de IP de Azure contra DDoS contiene las mismas características de ingeniería principales que Protección de red contra DDoS, pero variará en los siguientes servicios de valor añadido: compatibilidad con respuesta rápida de DDoS, protección de costos y descuentos en WAF.

Durante el proceso de creación de una red virtual se ofrece la posibilidad de asociar la VNET con un Plan de protección contra DDoS.

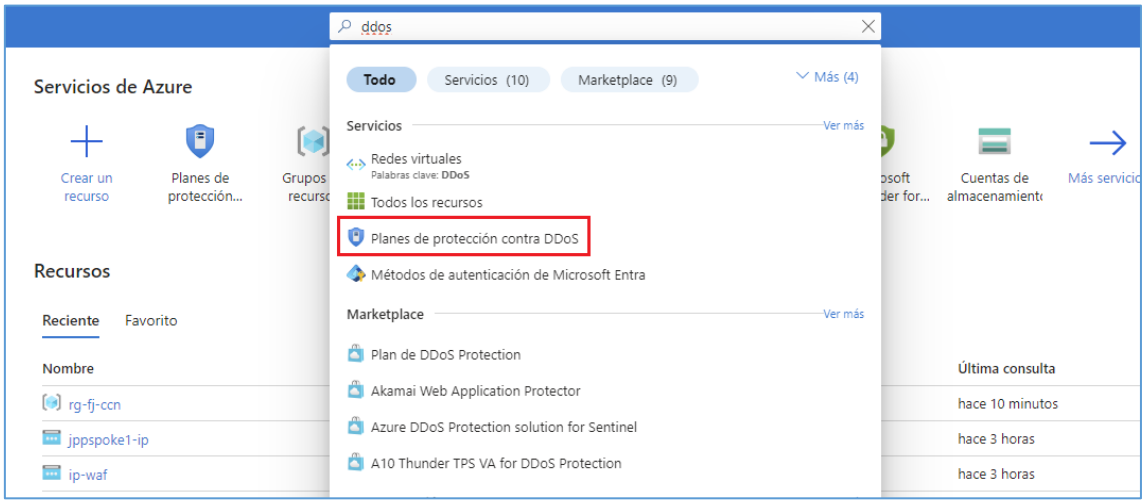
Durante el proceso de creación de una IP pública se ofrece la posibilidad de especificar el tipo de protección DDoS: protección de red (hereda la protección contra DDoS de la red virtual), dirección IP (específico de la IP) o deshabilitar.

Nota: *Para más información consultar la documentación oficial de Microsoft:* https://learn.microsoft.com/es-es/azure/ddos-protection/ddos-protection-overview

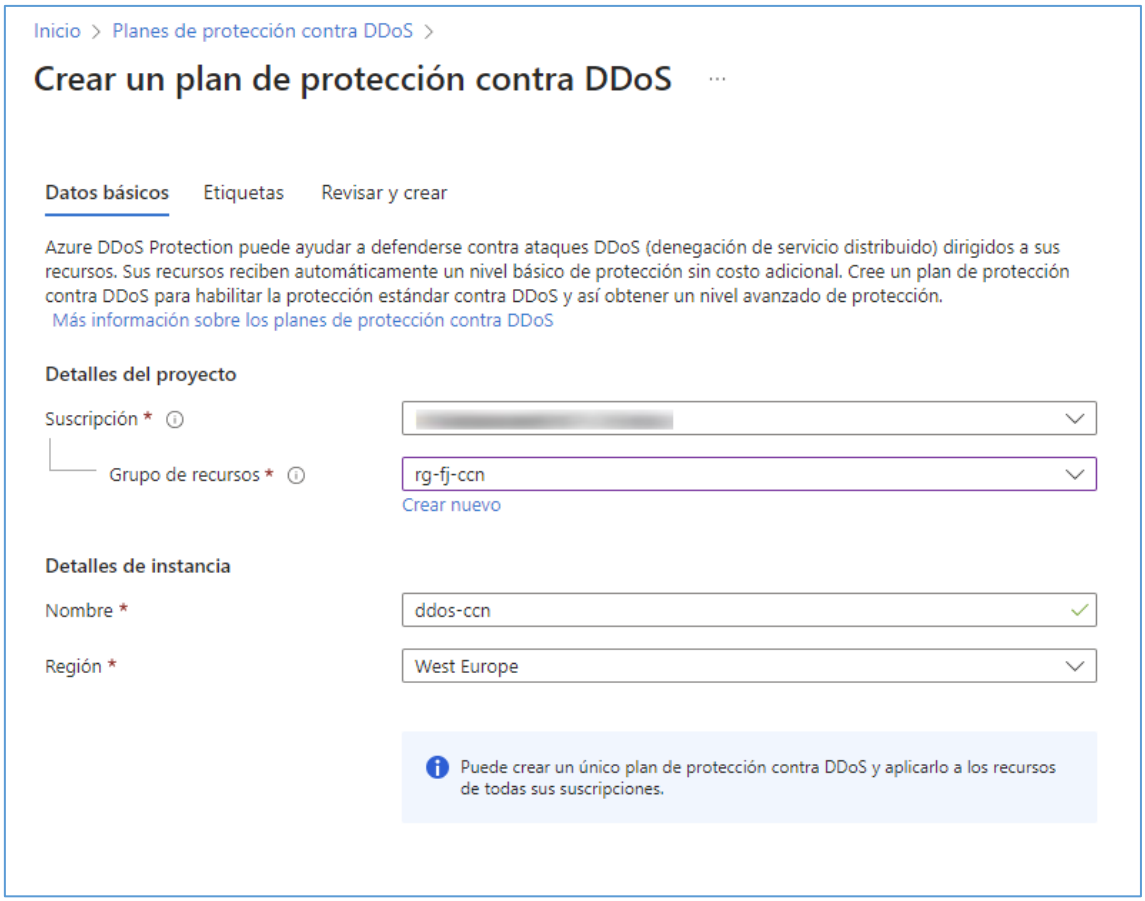
CREACIÓN Y CONFIGURACIÓN DE AZURE DDOS NETWORK PROTECTION

CREACIÓN DE UN PLAN DE PROTECCIÓN CONTRA DDOS

a) En el buscador de Azure escribir DDoS, elegir la opción de Planes de protección contra DDoS y seleccionar Crear.

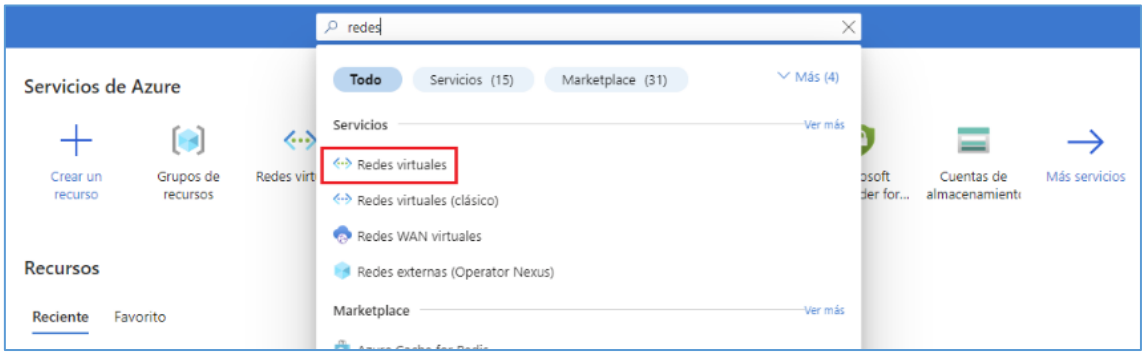


b) Se rellena el formulario introduciendo los parámetros de suscripción, grupo de recursos, nombre y región. Para finalizar pulsar sobre [Revisar y crear / Crear].

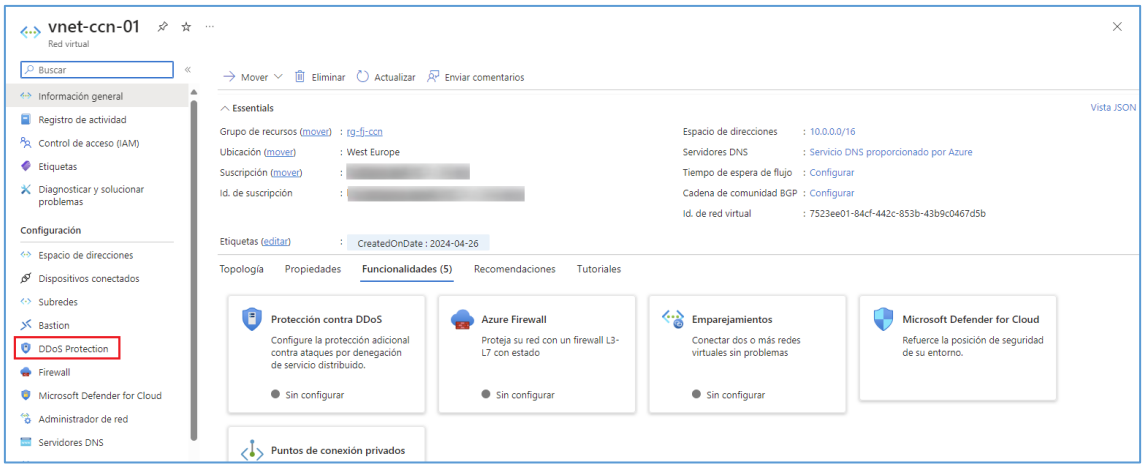


HABILITACIÓN DE LA PROTECCIÓN CONTRA DDOS EN UNA RED VIRTUAL EXISTENTE

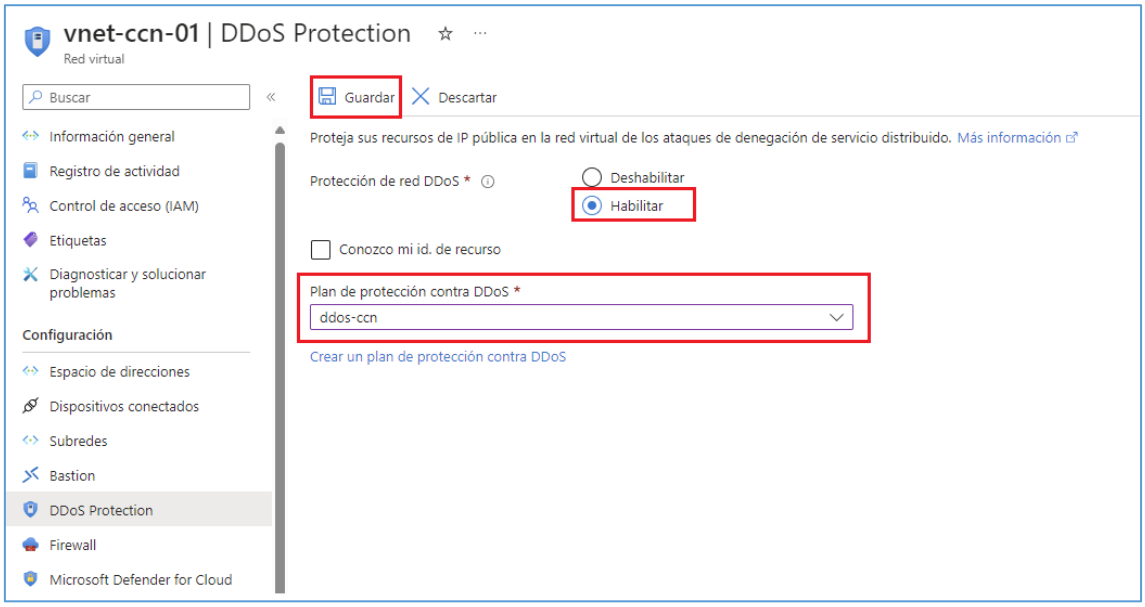
a) En el buscador de Azure escribir redes y seleccionar Redes virtuales. De las redes disponibles elegir la red donde queremos habilitar la protección contra DDoS.



b) En el menú de configuración seleccionar [DDoS Protection].



c) Seleccionar la opción de Habilitar en la Protección de red DDoS, elegir el plan de protección deseado y Guardar.

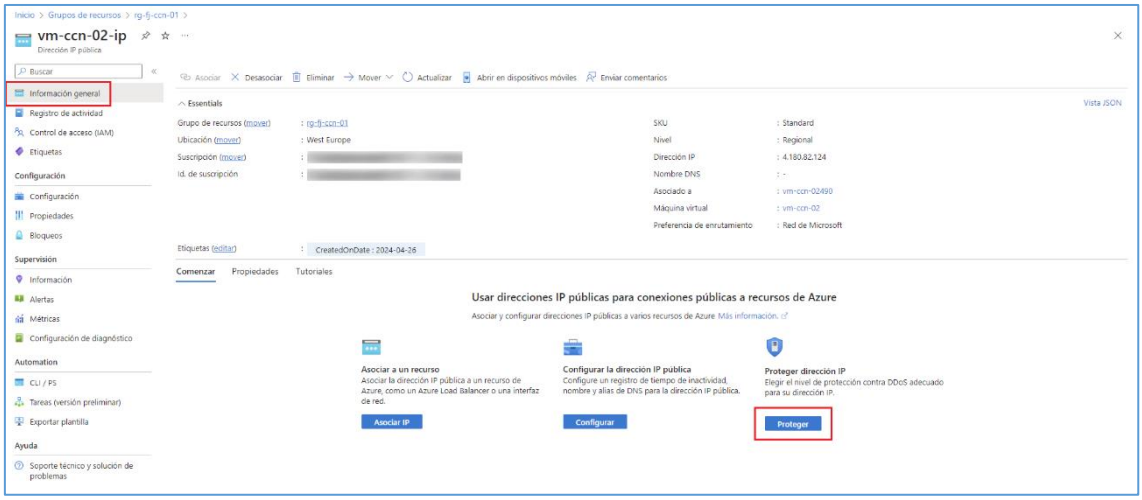


CREACIÓN Y CONFIGURACIÓN DE PROTECCIÓN DE IP DE AZURE DDOS

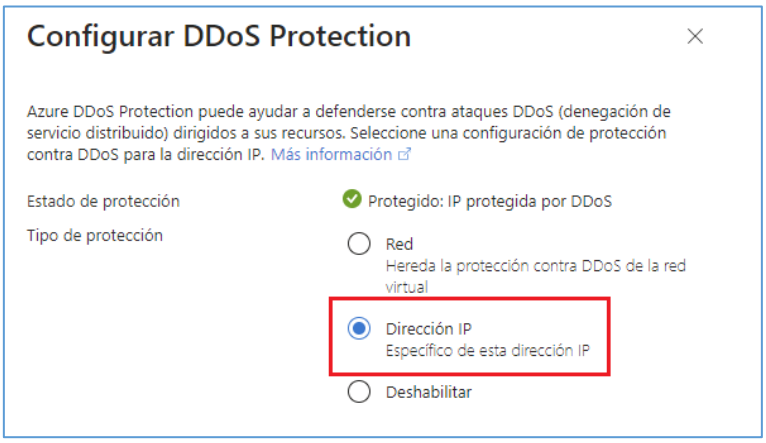
HABILITACIÓN DE LA PROTECCIÓN CONTRA DDOS EN UNA IP PÚBLICA EXISTENTE

a) En el buscador de Azure escribir ip pública y seleccionar Direcciones IP públicas. De las IPs públicas disponibles elegir la IP donde queremos habilitar la protección contra DDoS.

b) En la opción de menú de Información general pulsar el botón Proteger.



c) En el tipo de protección, si previamente hemos vinculado la protección contra DDoS en la red virtual donde está ubicada la IP pública se recomienda dejar seleccionada la opción de Red. En el caso de que solamente se desee proteger la IP pública seleccionada se puede elegir la opción de Dirección IP y Guardar.

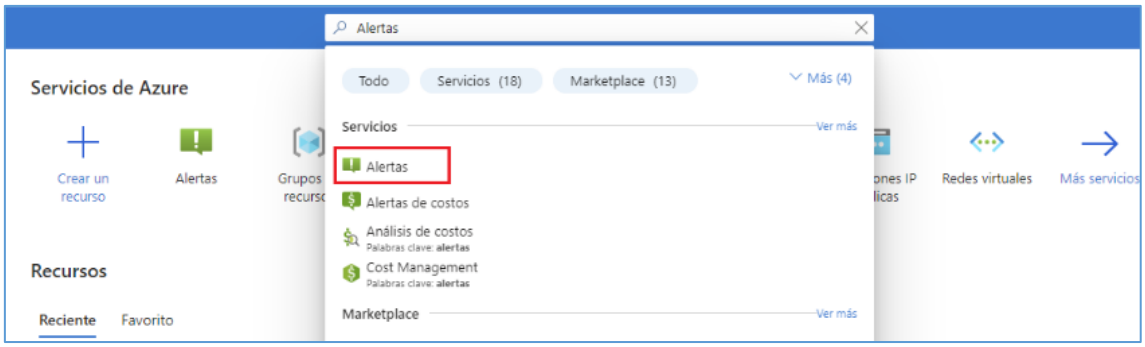


CONFIGURACIÓN DE ALERTAS DE MÉTRICAS DE AZURE DDOS PROTECTION

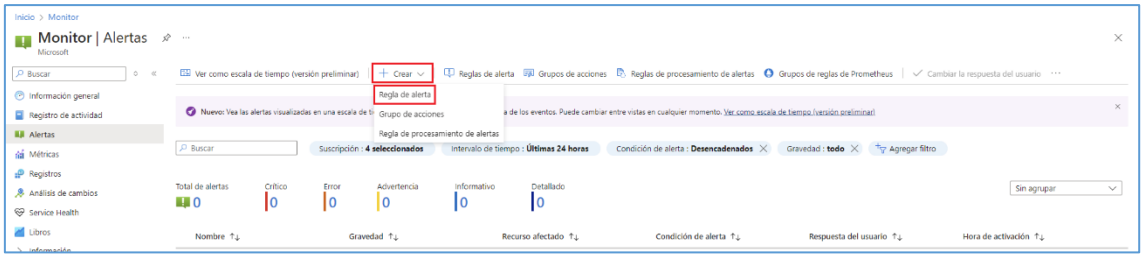
Azure DDoS Protection proporciona información detallada y visualización de análisis de ataques DDoS. Los usuarios que protegen sus redes virtuales frente a ataques DDoS disponen de visibilidad detallada sobre el tráfico de ataques y las acciones llevadas a cabo para mitigarlos mediante informes de mitigación de ataques y registros de flujo de mitigación. La telemetría enriquecida se expone a través de Azure Monitor, incluidas las métricas detalladas mientras dure un ataque DDoS. Las alertas se pueden configurar para cualquiera de las métricas de Azure Monitor que expone DDoS Protection.

Para configurar las alertas de métricas puede seguir los siguientes pasos:

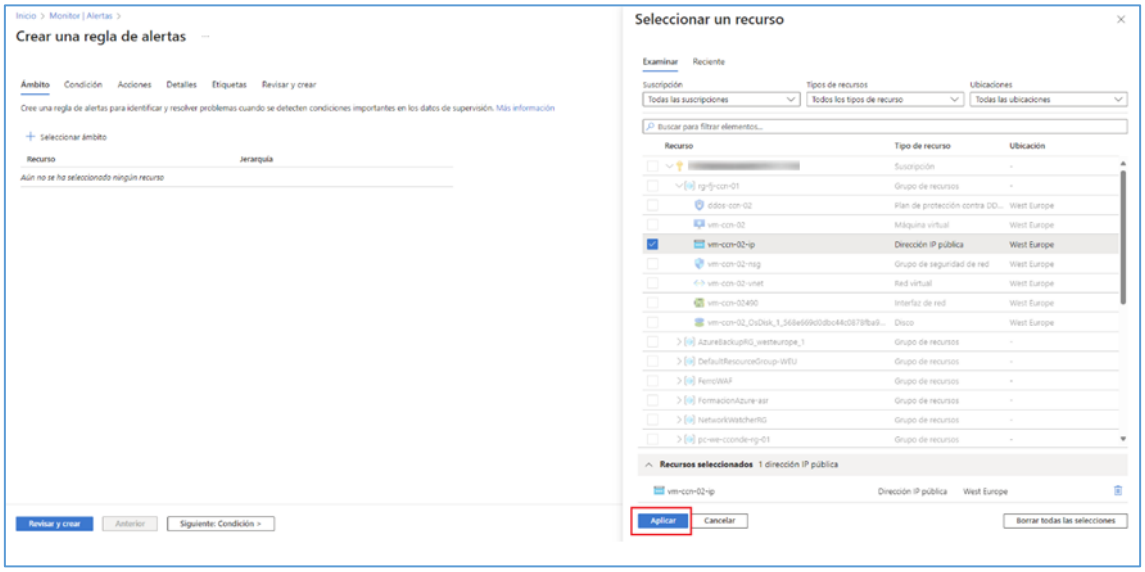
a) En el cuadro de búsqueda escribe Alertas y selecciona la opción de [Alertas]:



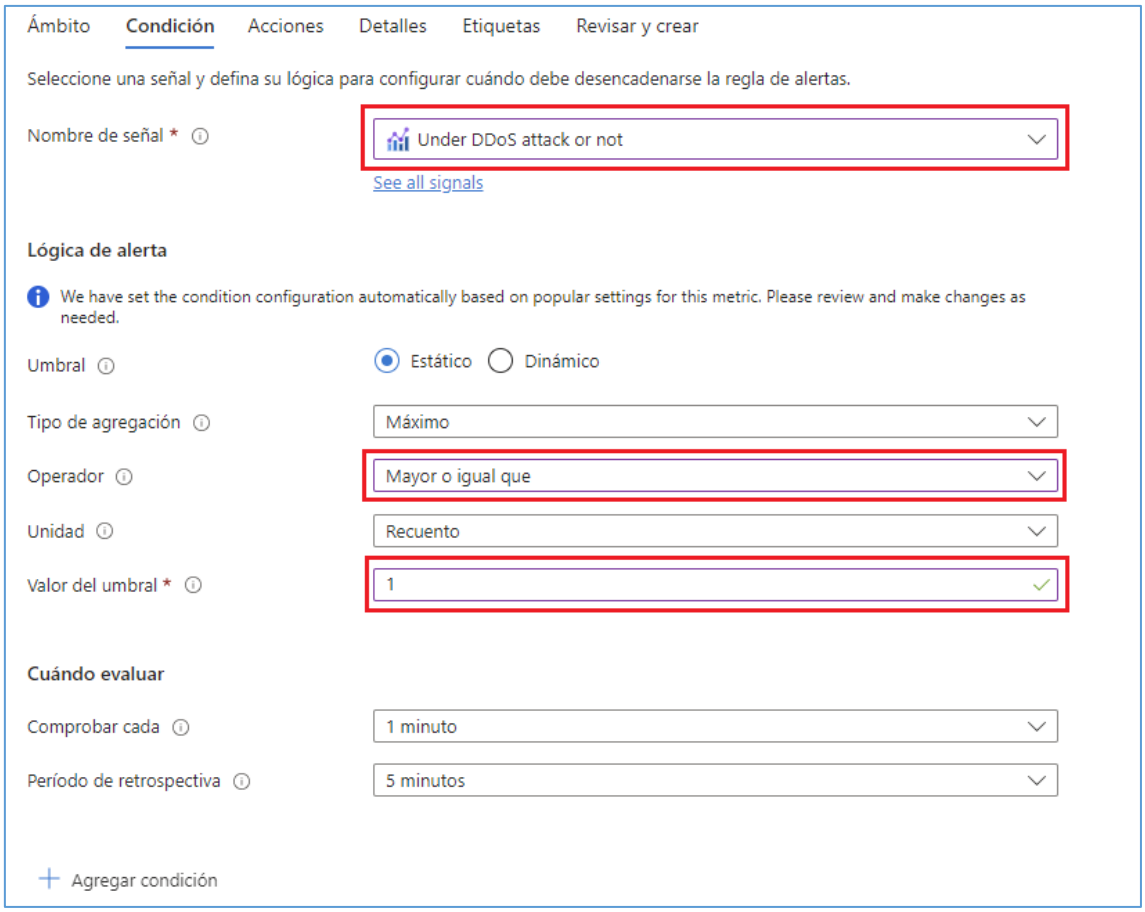
b) Pulsar en Crear/Regla de alerta.



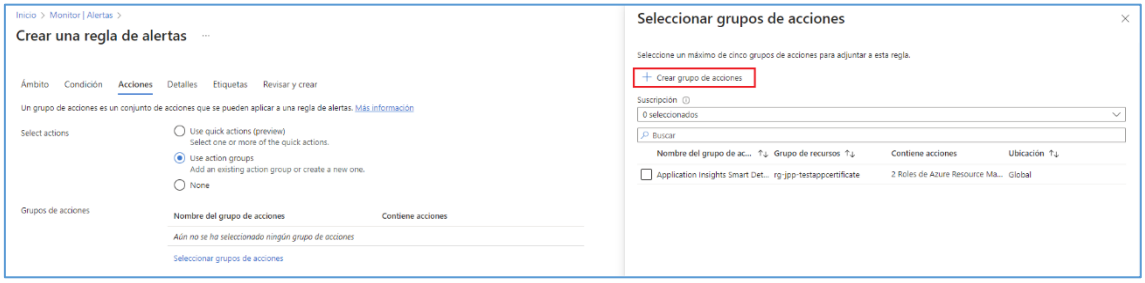
c) Seleccionar el ámbito de monitorización, por ejemplo, la IP pública a monitorizar, y seleccionar Aplicar.

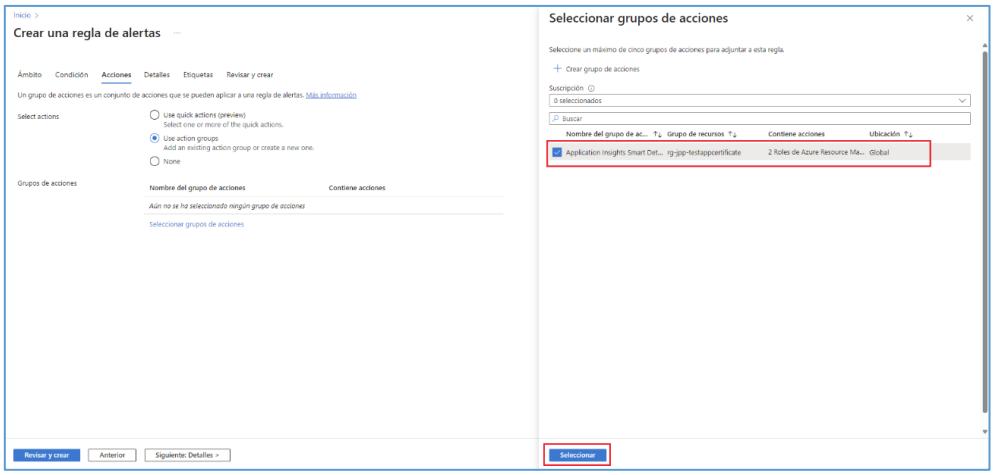


d) Seleccionar Agregar condición y elegir la opción “Under DDoS attack or not”. Dejar los parámetros por defecto modificando solamente el operador a “Mayor o igual que” y especificar 1 en el valor del umbral.

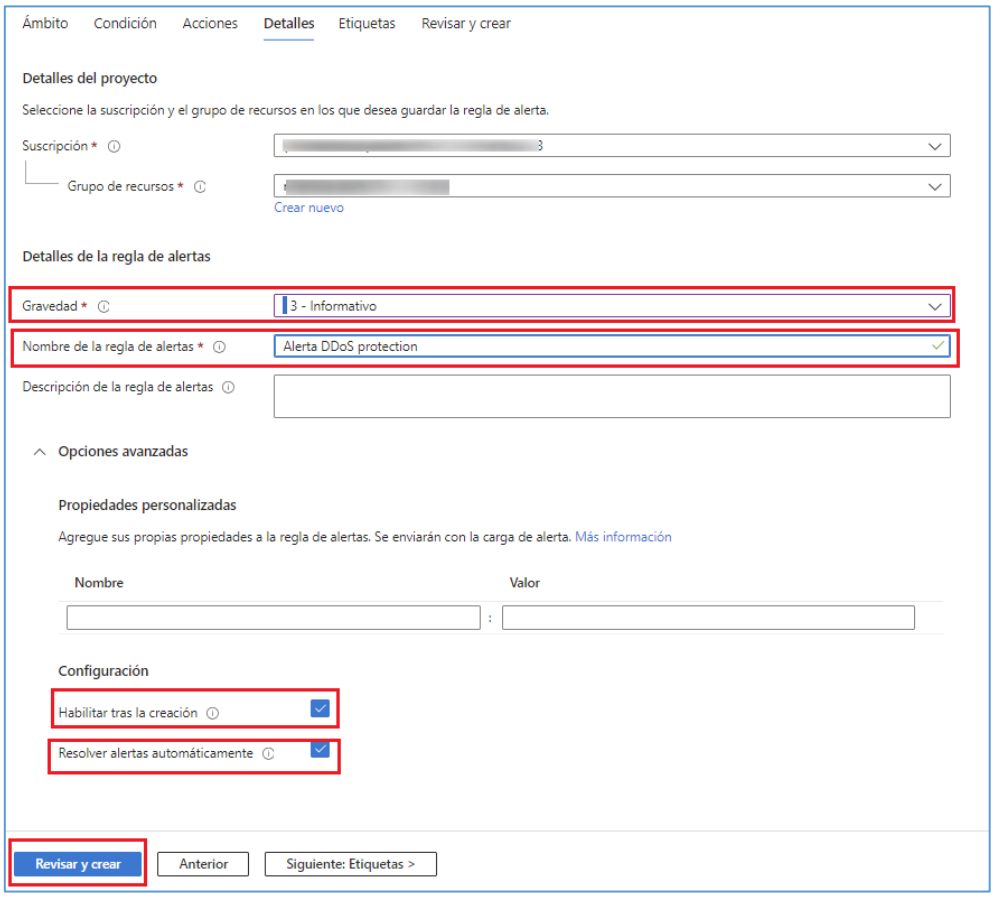


e) En la página de Acciones, pulsar el Crear un grupo de acciones y seguir los pasos que se explican en el apartado [3.1.4.2 Sistema de métricas / Azure Monitor / Alertas] referente a la creación del grupo de acciones. También es posible utilizar un grupo de acciones creado con anterioridad seleccionándolo en el listado del grupo de acciones.





f) En la pestaña Detalles, seleccionar la Gravedad de la alerta, como por ejemplo "Informativo", agregar opcionalmente una descripción y seleccionar las opciones de configuración de "Habilitar tras la creación" y "Resolver alertas automáticamente", después "Revisar y crear" y "Crear" para finalizar.



4. GLOSARIO Y ABREVIATURAS

A continuación de describen una serie de términos, acrónimos y abreviaturas en materia de seguridad utilizados en esta guía:

Término	Definición
AAD o Azure AD	**Azure Active Directory (AAD o Azure AD),** ahora conocido como Microsoft Entra ID, es una solución integral de identidad y acceso en la nube. Su objetivo es conectar a empleados, clientes y socios con aplicaciones, dispositivos y datos de manera segura.
AD DS	Active Directory Domain Services (Servicios de dominio de Directorio Activo).
ASR	**Azure Site Recovery** es un servicio que ayuda a garantizar la continuidad empresarial manteniendo las aplicaciones y cargas de trabajo empresariales en funcionamiento durante interrupciones planeadas o imprevistas.
DDoS	**DDoS (Distributed Denial of Service).** Un ataque DDoS (denegación de servicio distribuido) tiene como objetivo desactivar o derribar un sitio web, aplicación web, servicio en la nube u otro recurso en línea sobrecargándolo con solicitudes de conexión sin sentido, paquetes falsos u otro tráfico malicioso.
ENS	Esquema Nacional de Seguridad.
Grupo de Recursos	Un **grupo de recursos** en Azure es un contenedor lógico que almacena los recursos relacionados con una solución de Azure. Puede incluir todos los recursos de la solución o solo aquellos que se desean administrar como grupo.
IaaS	La **Infraestructura como servicio (IaaS)** es un tipo de servicio de computación en la nube que ofrece recursos esenciales de procesamiento, almacenamiento y redes.
JSON	Acrónimo de **JavaScript Object Notation**, es un formato de texto que forma parte del sistema de JavaScript. Aunque se deriva de la sintaxis de JavaScript, su objetivo no es la creación de programas, sino el acceso, almacenamiento e intercambio de datos.
LNG	Un **Local Network Gateway (LNG)** es un recurso específico en Azure que representa la ubicación local para fines de enrutamiento.
Log Analytics	**Azure Log Analytics** es una herramienta en el portal de **Azure** que se utiliza para **editar y ejecutar consultas de registro** en los datos almacenados en el almacén de registros de **Azure Monitor**. Puedes escribir consultas para recuperar registros específicos y luego utilizar las funciones de Log Analytics para ordenar, filtrar y analizar esos registros.

LTR	Retención a largo plazo o **Long Term Retention.** Es ua característica usada para las copias de Azure **SQL Database y Azure SQL Managed Instance** que permite almacenar copias de seguridad completas con una política de redundancia configurables. Retención de copia de seguridad a largo plazo
MFA	La **autenticación multifactor (MFA)** es una tecnología que se utiliza para incrementar el nivel de seguridad en las transacciones o inicios de sesión. En lugar de depender únicamente de la clásica combinación de nombre de usuario y contraseña, la MFA incorpora uno o más factores de autenticación adicionales.
NSG	Puede usar el **grupo de seguridad de red** o **Network Security Group (NSG)** para filtrar el tráfico de red entre los recursos de una red virtual de Azure. Un grupo de seguridad de red contiene reglas de seguridad que permiten o deniegan el tráfico de red entrante o el tráfico de red saliente de varios tipos de recursos de Azure.
RBAC	El Control de Acceso Basado en Roles (RBAC) es un modelo de seguridad que permite asignar funciones y autorizaciones en la infraestructura informática de una organización
TIC	TIC (Tecnologías de la Información y la Comunicación) son un conjunto de tecnologías desarrolladas para una información y comunicación más eficiente. Estas tecnologías han modificado la forma de acceder al conocimiento y las relaciones humanas

5. CUADRO RESUMEN DE LAS MEDIDAS DE SEGURIDAD

Se facilita a continuación un cuadro resumen de configuraciones a aplicar para la protección del servicio, donde la organización puede valorar qué medidas de las propuestas se cumplen.

Control ENS	Configuracion	Estado	
op	**Marco Operacional**		
op.acc	**Control de Acceso**		
op.acc.1	**Identificación**		
	*Se ha configurado el uso de cuentas y grupos de **Microsoft Entra ID** para la administración del Tenant.*	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
op.acc.2	***Requisitos de Acceso***		
	Se ha configurado el requisito de acceso mediante la aplicación de roles RBAC. *Se ha configurado el acceso condicional delimitando zonas geográficas y/o rangos de IPs. (importante y/o)*	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No

	Recomendable: - *Restricción de acceso al portal de Azure* - *Microsoft Entra ID Protection*	**Evidencias Recogidas:** ☐ Si ☐ No	**Observaciones:**
op.acc.3	**Segregación de funciones y tareas**		
	Se han diseñado, creado y aplicado los roles a los grupos de usuarios. *Se han de aplicarse los roles Propietario, colaborador, lector y Administrador de acceso de usuario.*	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
op.acc.5	**Mecanismo de autenticación (usuarios externos)**		
	Se ha habilitado Multi-Factor Authentication (MFA) para los usuarios externos.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**

op.acc.6	**Mecanismo de autenticación (usuarios de la organización)**		
	Se ha habilitado Multi-Factor Authentication (MFA) para los usuarios de la organización.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
op.exp	**Explotacion**		
op.exp.8	**Registro de la actividad**		
	Se ha comprobado que los registros de Auditoría y de inicio de sesión están activados y capturando eventos.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
		Aplica: ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**

op.exp.10	**Protección de claves criptográficas**		
	Se ha configurado Key Vault, limitando el acceso tan solo a usuarios administradores.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
op.cont.2	**Plan de continuidad**		
	Se ha configurado Azure Site Recovery replicando las maquinas virtuales y base de datos para poder crear un plan de recuperacion.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
op.cont.3	**Pruebas periódicas**		
	Para las maquinas virtuales se ha realizado una conmutacion por error.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
op.mon.1	**Detección de intrusión**		

	Se ha configurado Microsoft Entra ID Protection creando directivas de riesgo de inicio de sesión de los usuarios de Microsoft Entra ID.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
op.mon.2	**Sistema de métricas**		
	Se ha configurado Azure monitor creando alertas de los servicios de producción.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
op.mon.3	**Vigilancia**		
	Se ha configurado Network Watcher creando captura de paquetes. Se han habilitado planes de pago en Microsoft Defender for Cloud para los recursos más utilizados. Se ha configurado Microsoft Sentinel.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**

mp.com.1	**Perímetro seguro**		
	Se ha configurado el despliegue de NSG / Azure Firewall aplicando las reglas recomendadas para los servicios de Azure.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
mp.com.2	**Protección de la confidencialidad**		
	Se ha desplegado el servicio de VPN (Site to site) y/o ExpressRoute.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
mp.com.3	**Protección de la integridad y de la autenticidad**		
	Se cumple con las siguientes medidas de seguridad: Vigilancia [op.mon.3]; Mecanismo de autenticación (usuarios de la organización) [op.acc.6] y Protección frente a denegación de servicio [mp.s.4]	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**

mp.com.4	**Separación de flujos de información en la red**		
	Se han configurado VNETS para el aislamiento de redes.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
mp.info.2	**Calificación de la información**		
	Se ha configurado etiquetas para todos los servicios de Azure.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
mp.info.6	**Copias de seguridad**		
	Se ha configurado un plan de backup para los servicios de Azure.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No

		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
mp.s.4	**Protección frente a denegación de servicio**		
	Se ha configurado DDOS en aquellas VNET expuestas a potenciales ataques externos.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL