Guía de Seguridad de las TIC
CCN-STIC 884C

Guía de configuración segura para Azure SQL Database

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
2024.05.13 10:10:39 +02'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-24-170-2
Fecha de Edición: mayo de 2024

ÍNDICE

1. GUÍA DE CONFIGURACIÓN SEGURA PARA AZURE SQL DATABASE

1.1 DESCRIPCIÓN DEL USO DE ESTA GUÍA

El objetivo del presente guía es seguir las recomendaciones de seguridad en la utilización del servicio Azure SQL Database cumpliendo con los requisitos necesarios del Esquema Nacional de Seguridad en su categoría ALTA.

Azure SQL Database es una base de datos relacional de propósito general como servicio (DBaaS) basada en la última versión estable de Microsoft SQL Server Database Engine, de alto rendimiento, fiable y segura que puede utilizar para crear aplicaciones y sitios web basados en datos en el lenguaje de programación de su elección, sin necesidad de gestionar la infraestructura.

2. DESPLIEGUE DE AZURE SQL DATABASE

2.1 PRERREQUISITOS PARA EL DESPLIEGUE MEDIANTE POWERSHELL

A continuación, se detallan los prerrequisitos para el despliegue de la instalación de SQL Database.

Requisitos de sistema:

Como requisito de sistema operativo es recomendable que consulte el siguiente link de Microsoft.

https://learn.microsoft.com/es-es/powershell/scripting/install/installing-powershell-on-windows?view=powershell-7.4

Instalación PowerShell:

1. Se debe conectar al módulo de PowerShell.
2. Instalar el módulo desde Powershell.

```
Install-Module -Name Az -AllowClobber -Scope CurrentUser
```

2.2 DESPLIEGUE DE AZURE SQL DATABASE MEDIANTE POWERSHELL

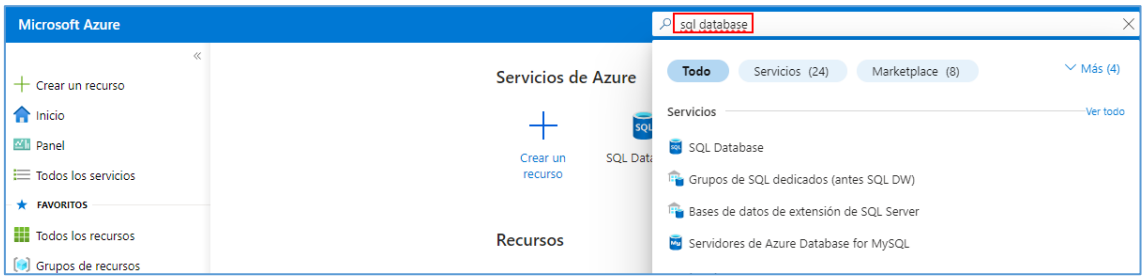
El despliegue de Azure SQL se puede realizar desde el portal de Azure o bien desde el script que se comenta a continuación.

Nota: Es importante que en el script se definan los diferentes parámetros/variables que son necesarios para el despliegue del servidor y de la base de datos.

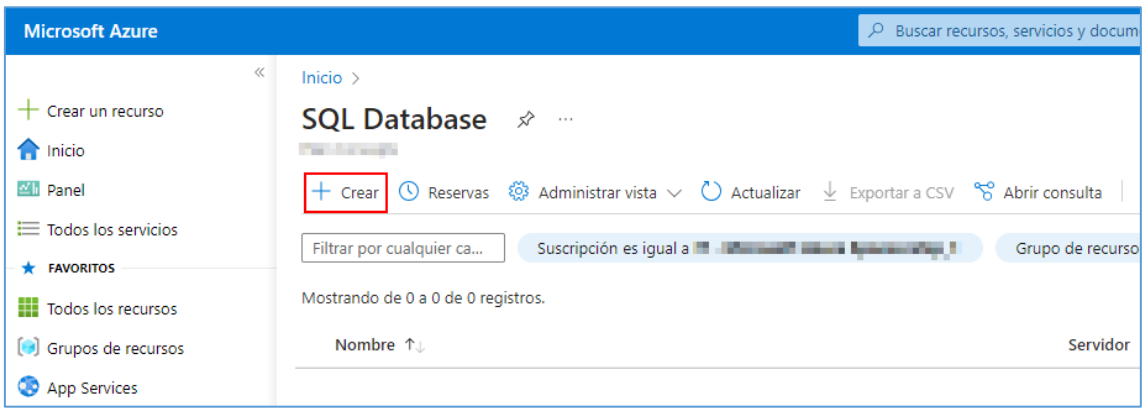
```
#   ## Se declaran las variables que son necesarias para la ejecución del script.
#   $ServerName= "Nombre del Servidor"
#   $Location= "Nombre de localización Ej. "North Europe""
#   $ResourceGroupName= "Nombre del Grupo de Recursos donde se creará el servidor"
#   $DatabaseName = "Nombre de la base de datos"
#   $ExternalAdminName = "Nombre del grupo de Administradores de la base de datos de Entra
    ID"
#
#   ##Creamos el servidor en Azure con los parámetros definidos previamente
#     $server = New-AzSqlServer -ResourceGroupName $ResourceGroupName `
#         -Location $Location `
#         -ServerName $ServerName `
#         -ServerVersion "12.0" `
#         -ExternalAdminName $ExternalAdminName `
#         -EnableActiveDirectoryOnlyAuthentication
#
#   ## Creamos la base de de datos en el servidor creado previamente
#         $database = New-AzSqlDatabase  -ResourceGroupName $resourceGroupName `
#         -ServerName $ServerName `
#         -DatabaseName $DatabaseName
```

2.3 DESPLIEGUE DE AZURE SQL DATABASE POR EL PORTAL

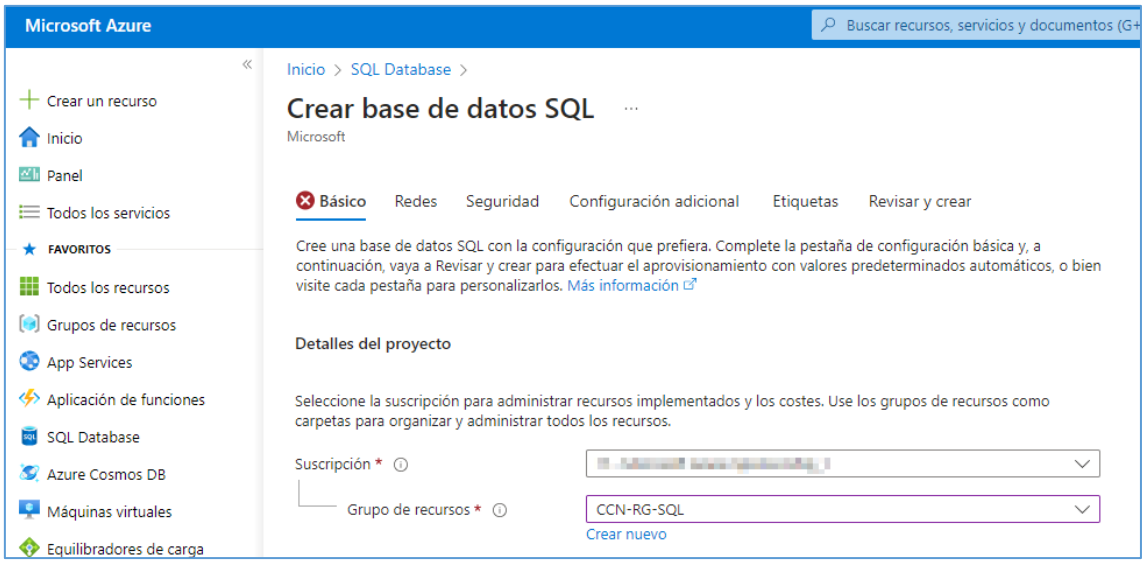
1. Desde el portal de Azure, ir a la barra de búsqueda y buscar SQL Database.



2. Pulsar en [Crear].



3. Se debe seguir el asistente de configuración.

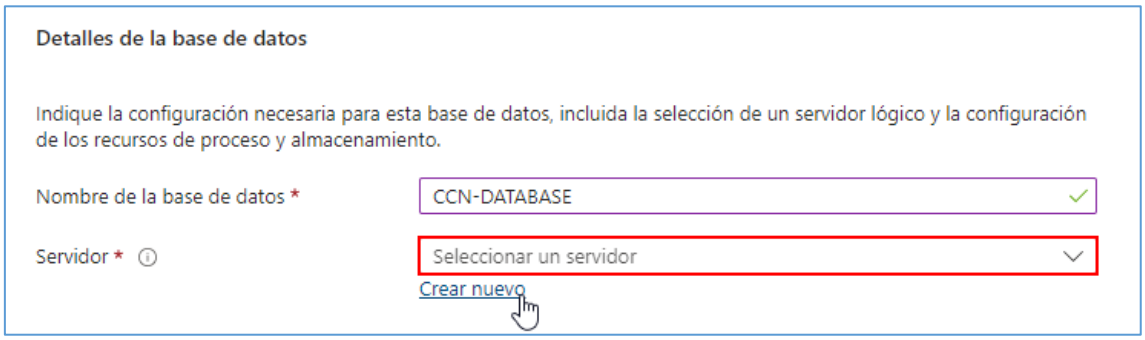


4. Se debe crear un nuevo grupo de recursos. En caso de tener ya creado el grupo de recursos previamente, seleccionar el grupo de recursos deseado.

Nota: Para una gestión más avanzada hay que recurrir al apartado *[2.3.1 Gestión de recursos Azure/Grupo de recursos]* de la guía. *[CCN-STIC-884A - Guía de configuración segura para Azure].*

Nombre de la base de datos: Definir un nombre para la base de datos.

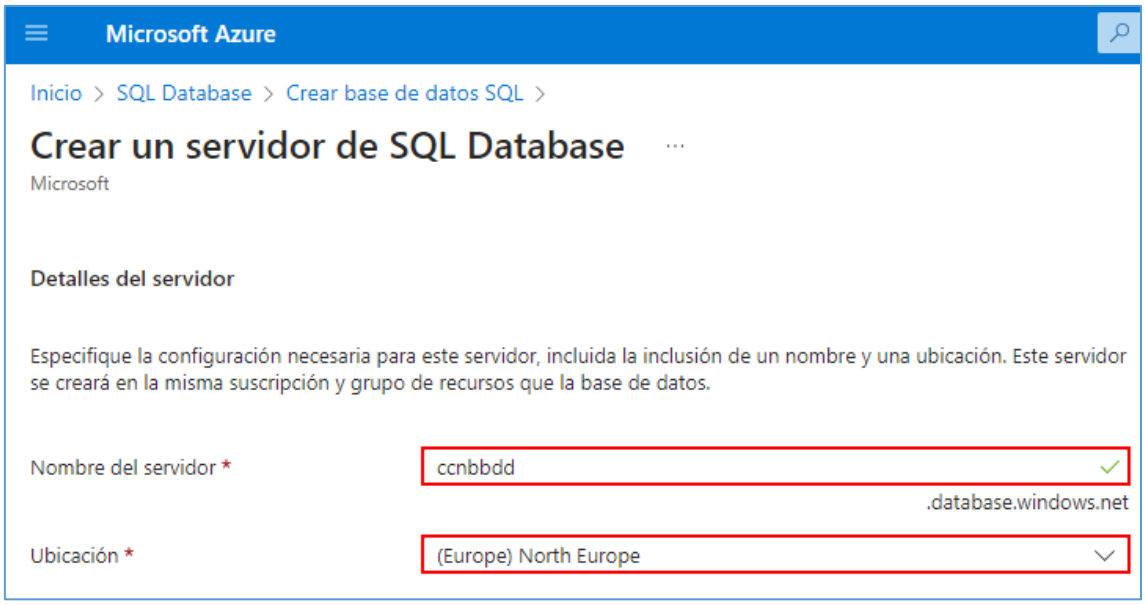
5. **Servidor**: Pulsar en [Crear nuevo].



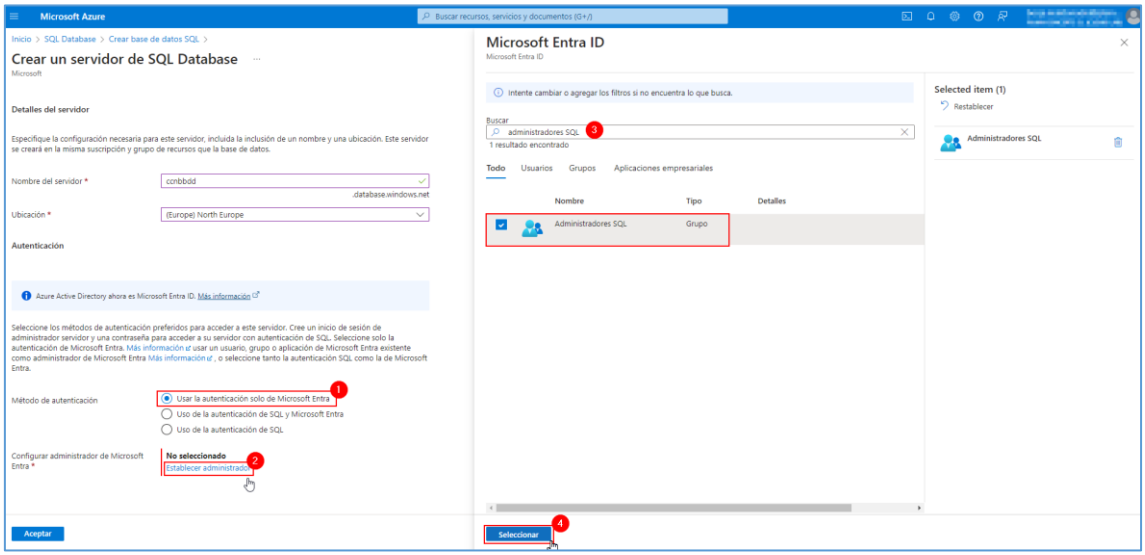
6. Se abrirá una nueva ventana donde se deben rellenar los campos que se solicita para el nuevo servidor.

Nombre del servidor: Definir un nombre para el servidor de la base de datos.

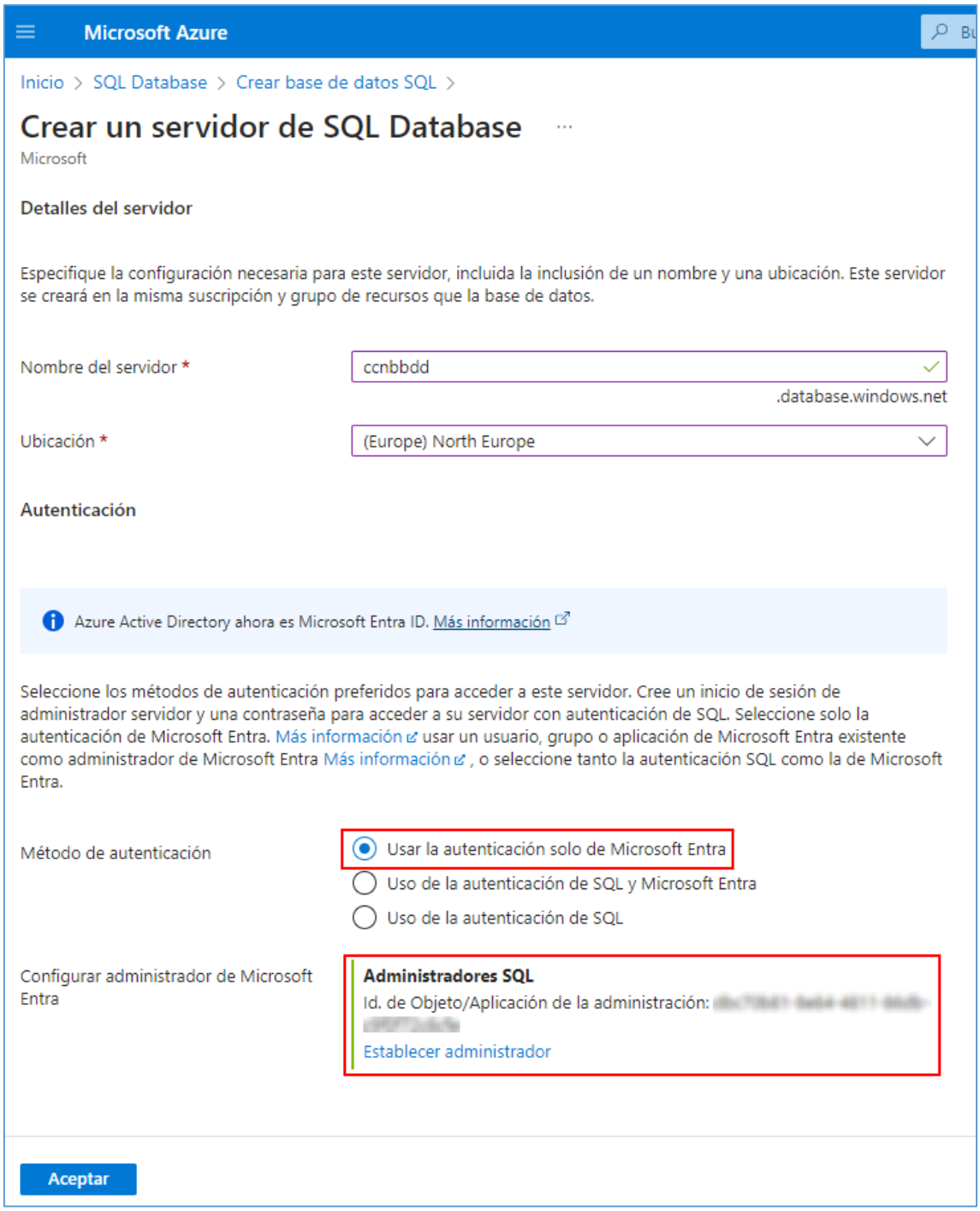
Ubicación: Se seleccionará la región donde se ubicará el servidor, como por ejemplo "North Europe" (Norte de Europa).



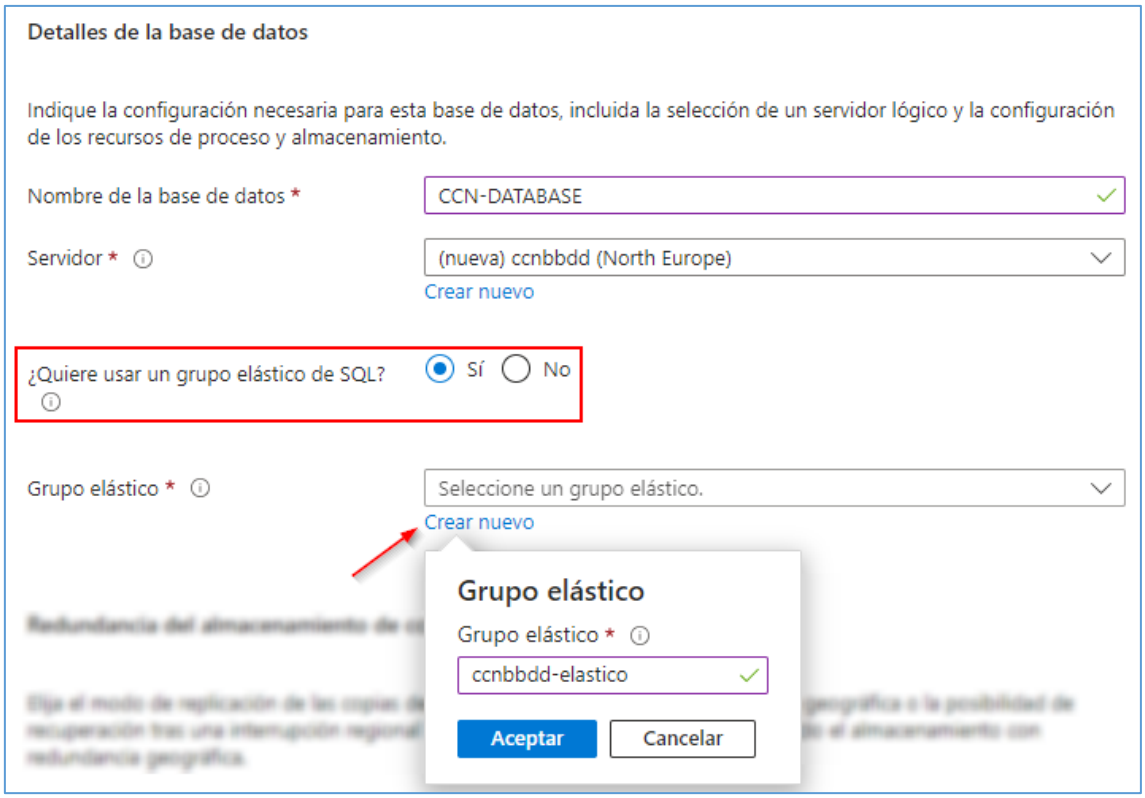
Autenticación: Se seleccionará la opción de autenticación mediante Microsoft Entra (anteriormente llamado Azure Active Directory) y se seleccionará el grupo de Administradores SQL:



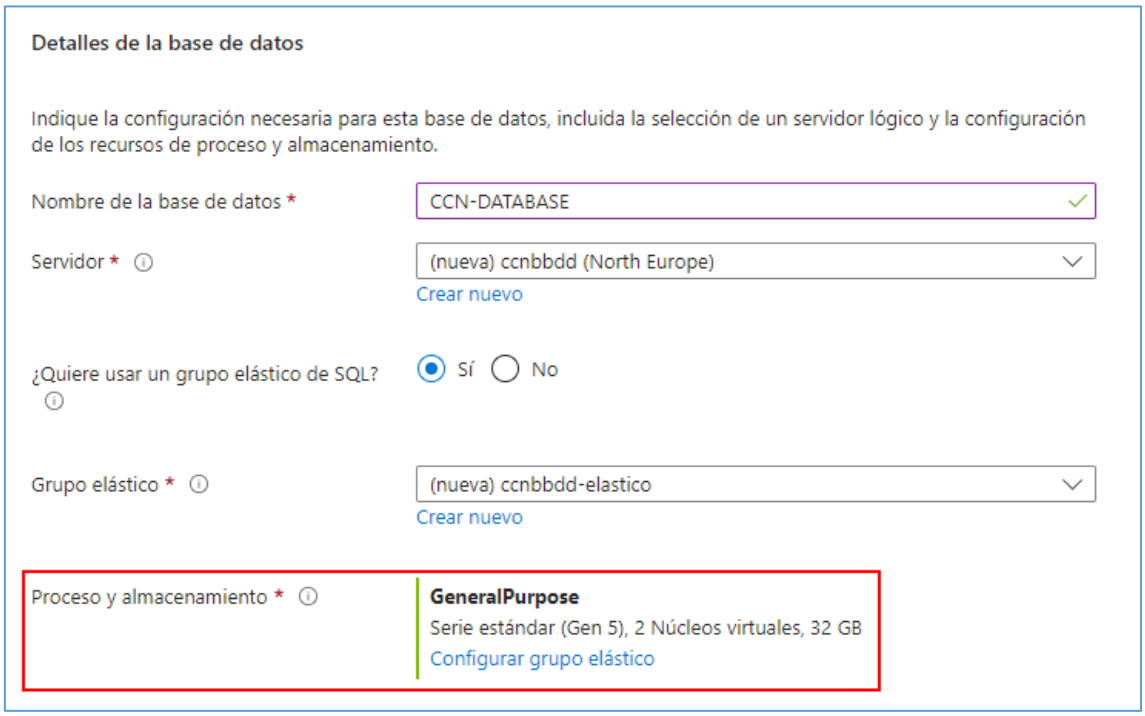
Nota: Este grupo se deberá haber creado con anterioridad en Entra ID, para ello recurrir al apartado *[3.1.1 Control de acceso/Microsoft Entra ID - Alta, baja y modificación de cuentas y grupos]* de la guía. *[CCN-STIC-884A - Guía de configuración segura para Azure].*



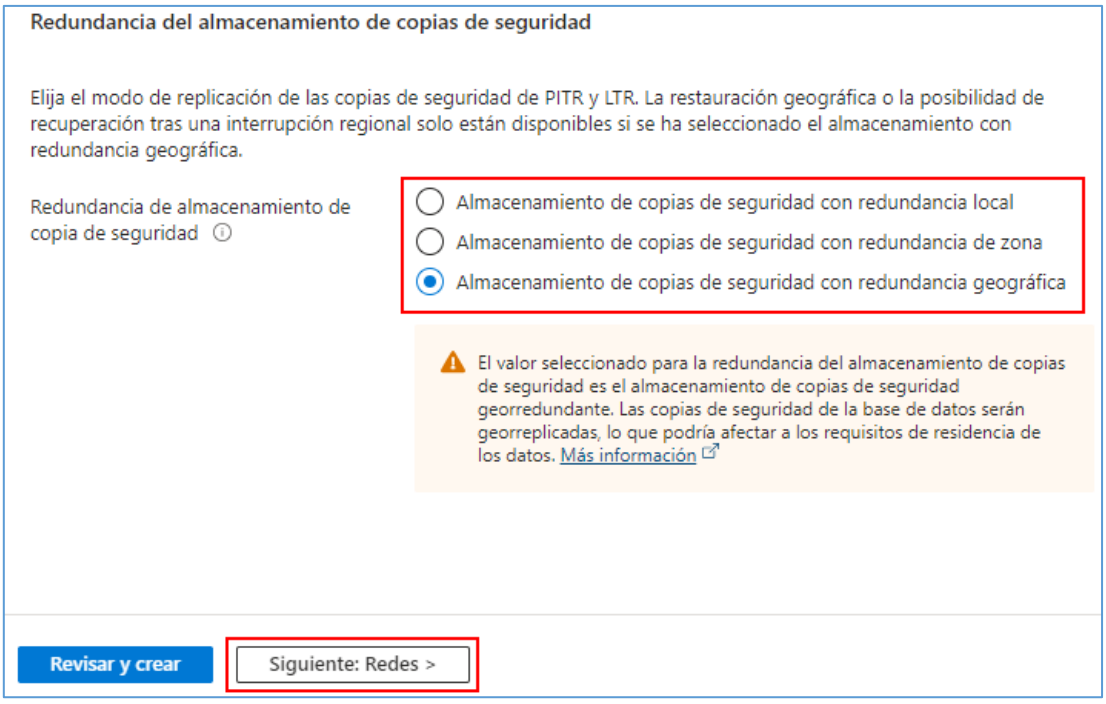
Quiere usar un grupo elástico de SQL: Es recomendable seleccionar el grupo elástico que le permite administrar el rendimiento de múltiples bases de datos y almacenamiento compartido configurando límites. Se especificará un nombre para el grupo elástico:

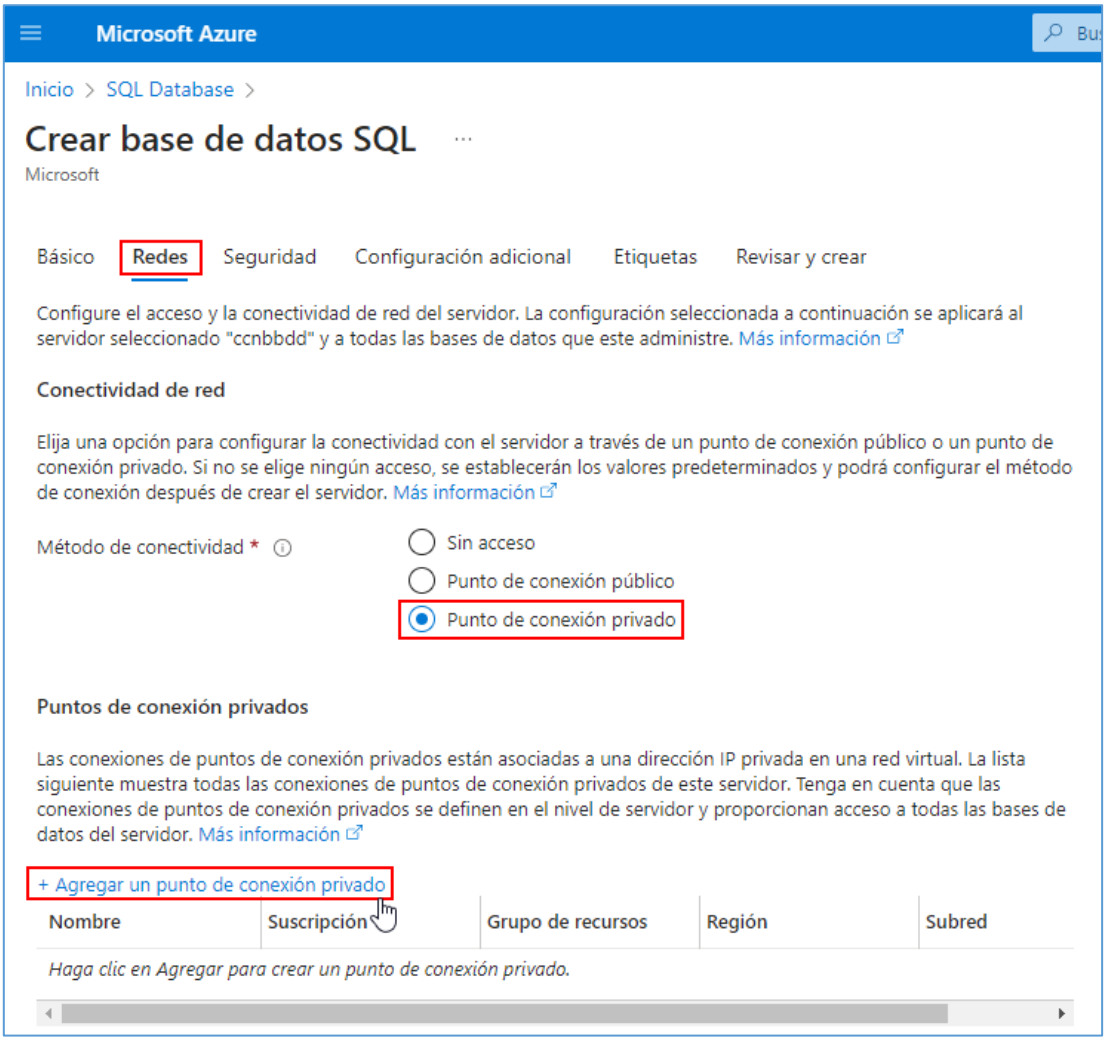


Proceso y almacenamiento: Se elegirá la configuración que más se ajuste a las necesidades de uso de la base de datos.

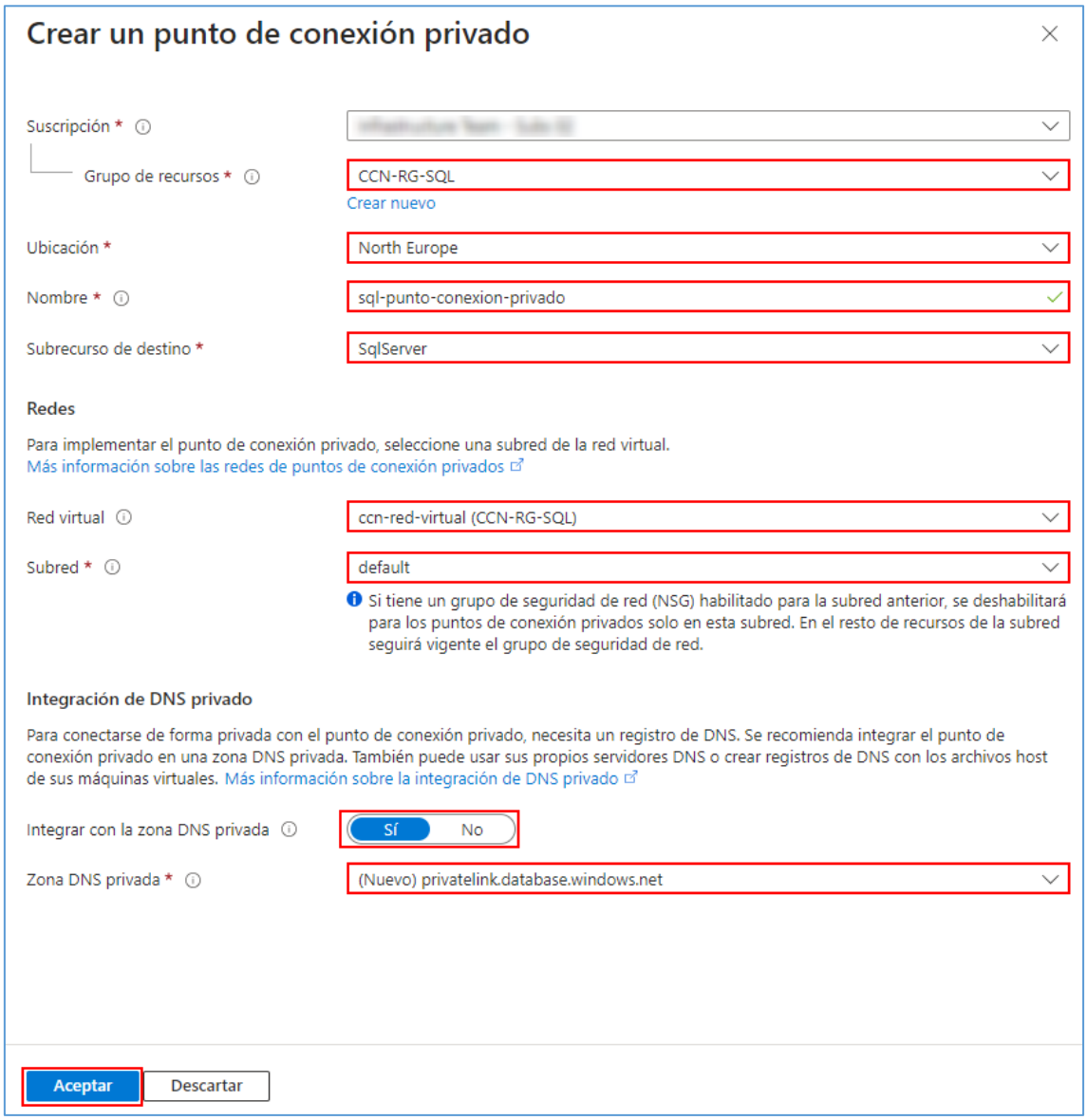


Redundancia de almacenamiento de copia de seguridad: Se seleccionará la redundancia que se desee establecer y se continuará al apartado de "redes":


Redundancia del almacenamiento de copias de seguridad
Elija el modo de replicación de las copias de seguridad de PITR y LTR. La restauración geográfica o la posibilidad de recuperación tras una interrupción regional solo están disponibles si se ha seleccionado el almacenamiento con redundancia geográfica.
Redundancia de almacenamiento de copia de seguridad
Almacenamiento de copias de seguridad con redundancia local
Almacenamiento de copias de seguridad con redundancia de zona
Almacenamiento de copias de seguridad con redundancia geográfica
El valor seleccionado para la redundancia del almacenamiento de copias de seguridad es el almacenamiento de copias de seguridad georredundante. Las copias de seguridad de la base de datos serán georreplicadas, lo que podría afectar a los requisitos de residencia de los datos. Más información
Revisar y crear
Siguiente: Redes >


Microsoft Azure
Inicio > SQL Database >
Crear base de datos SQL
Microsoft
Básico
Redes
Seguridad
Configuración adicional
Etiquetas
Revisar y crear
Configure el acceso y la conectividad de red del servidor. La configuración seleccionada a continuación se aplicará al servidor seleccionado "ccnbbdd" y a todas las bases de datos que este administre. Más información
Conectividad de red
Elija una opción para configurar la conectividad con el servidor a través de un punto de conexión público o un punto de conexión privado. Si no se elige ningún acceso, se establecerán los valores predeterminados y podrá configurar el método de conexión después de crear el servidor. Más información
Método de conectividad *
Sin acceso
Punto de conexión público
Punto de conexión privado
Puntos de conexión privados
Las conexiones de puntos de conexión privados están asociadas a una dirección IP privada en una red virtual. La lista siguiente muestra todas las conexiones de puntos de conexión privados de este servidor. Tenga en cuenta que las conexiones de puntos de conexión privados se definen en el nivel de servidor y proporcionan acceso a todas las bases de datos del servidor. Más información
+ Agregar un punto de conexión privado
Nombre
Suscripción
Grupo de recursos
Región
Subred
Haga clic en Agregar para crear un punto de conexión privado.

Método de conectividad: Se seleccionará Punto de conexión privado y a continuación se agregará un nuevo punto de conexión privado. Se abrirá una nueva ventana donde se configurará dicho punto de conexión:



Grupo de recursos: Se seleccionará el grupo de recursos donde se vaya a crear la base de datos.

Ubicación: Se seleccionará la misma región que se haya definido para la base de datos.

Nombre: Se dará un nombre al punto de conexión privado, como por ejemplo "sql-punto-conexión-privado".

Subrecurso de destino: Se seleccionará "SqlServer" (especificado por defecto).

Red virtual: Se debe seleccionar una red virtual que exista previamente. (*Ver apartado [3.2.1.1 Segregación de redes] de la guía. [CCN-STIC-884A - Guía de configuración segura para Azure]*).

Subred: Se seleccionará la subred de la cual se quiera obtener la IP privada para el punto de conexión.

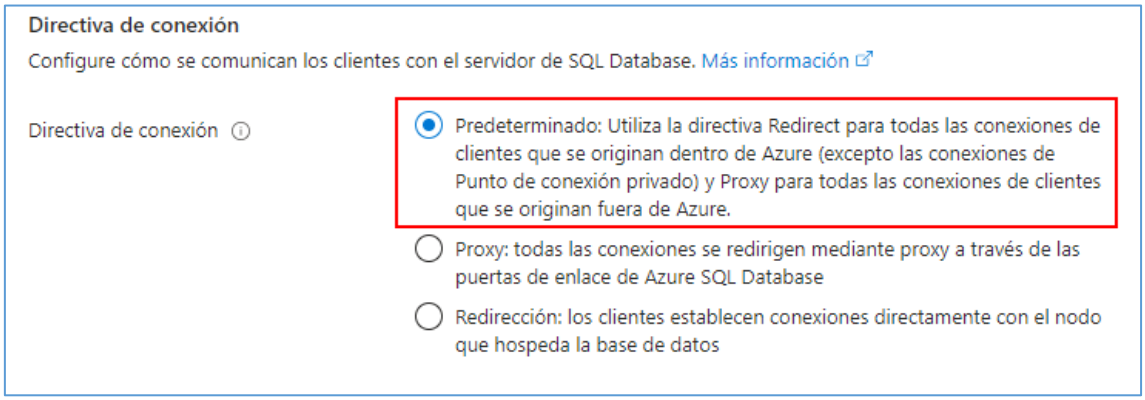
Integrar con la zona DNS privada: Se seleccionará "Sí".

Zona DNS privada: dejar el valor predeterminado que aparece "privatelink.database.windows.net".

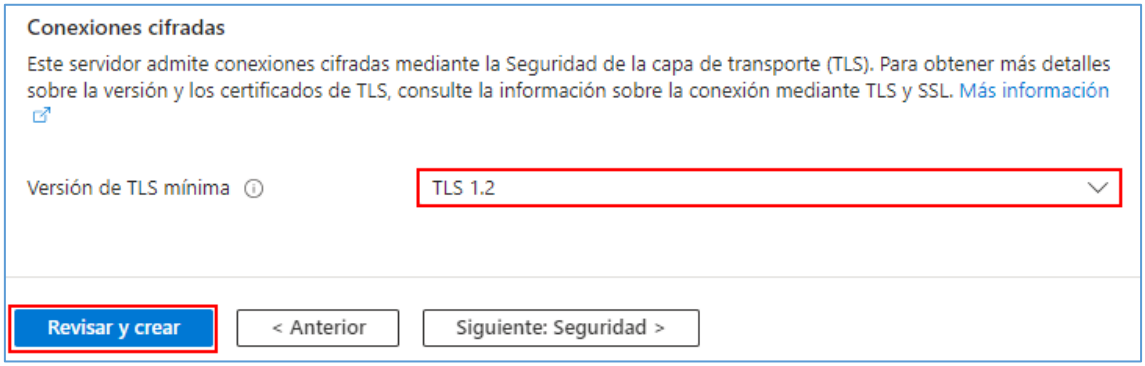
Pulsar en [Aceptar].

Continuar con la configuración la base de datos:

Directiva de conexión: Se seleccionará la opción "Predeterminado".

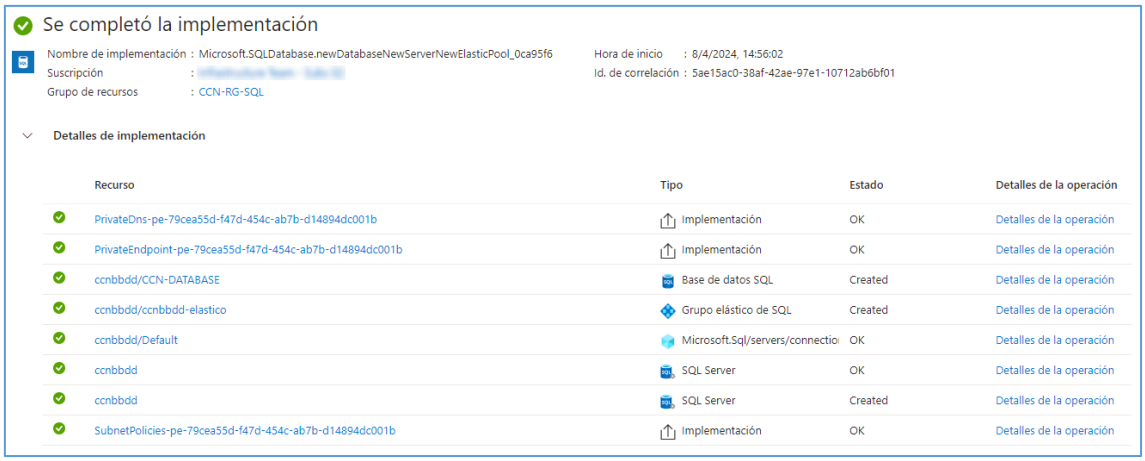


Conexiones cifradas: Se seleccionará la versión de TLS 1.2.



Finalmente se pulsará en [Revisar y crear].

Nota: La implementación del recurso puede tardar varios minutos hasta su finalización. Una vez haya finalizado verá la siguiente información.



3. CONFIGURACIÓN DE AZURE SQL DATABASE

3.1 MARCO OPERACIONAL

3.1.1 CONTROL DE ACCESO

3.1.1.1 IDENTIFICACIÓN

Microsoft Entra ID (anteriormente llamado Azure Active Directory) proporciona la administración de identidades basada en la nube y permite usar una identidad única en todo su *Tenant* y las aplicaciones de acceso en Azure.

Se recomienda que para la gestión de los administradores se utilice Entra ID en la gestión de cuentas de administradores y delegación en base de datos.

Nota: Para una gestión más avanzada hay que recurrir al apartado *[3.1.1 Control de acceso/Microsoft Entra ID - Alta, baja y modificación de cuentas y grupos]* de la guía. *[CCN-STIC-884A - Guía de configuración segura para Azure].*

3.1.1.2 REQUISITOS DE ACCESO

En esta guía se trata la seguridad en el acceso a los servidores de Azure SQL Database.

En cuanto a los requisitos de red, para poder acceder a la base de datos de Azure SQL Database es necesario hacerlo mediante conexión privada (dentro de la misma red de Azure donde se encuentre la base de datos o bien mediante un túnel VPN) ya que la conexión publica se encuentra deshabilitada.

En cuanto a los permisos de los usuarios, se debe aplicar una capa de seguridad mediante RBAC creando un nuevo rol personalizado, permitiendo dar un privilegio de administración a los servidores de SQL.

Los permisos son:

Microsoft.Authorization/roleDefinitions/write
Microsoft.Authorization/roleDefinitions/delete

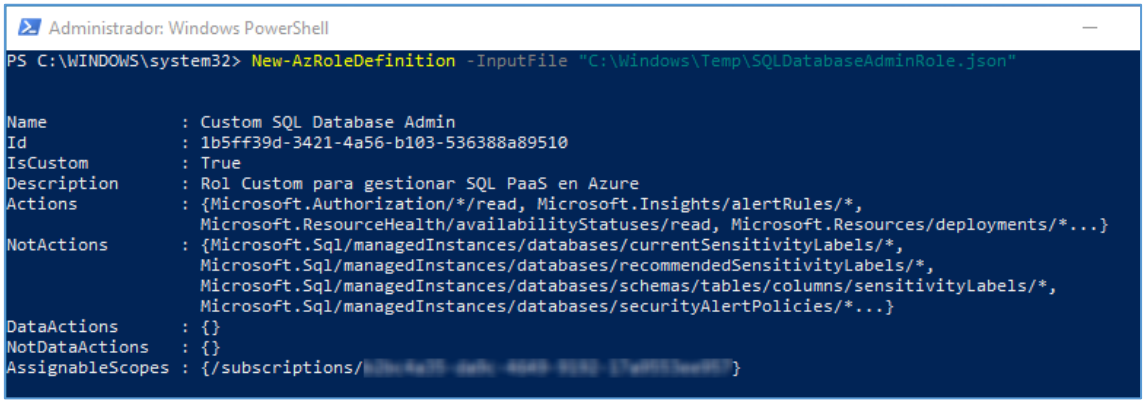
Creación de rol personalizado

Desde Powershell ejecutar:

```
#    New-AzRoleDefinition -InputFile "c:\temp\SQLDatabaseAdminRole.json"
```

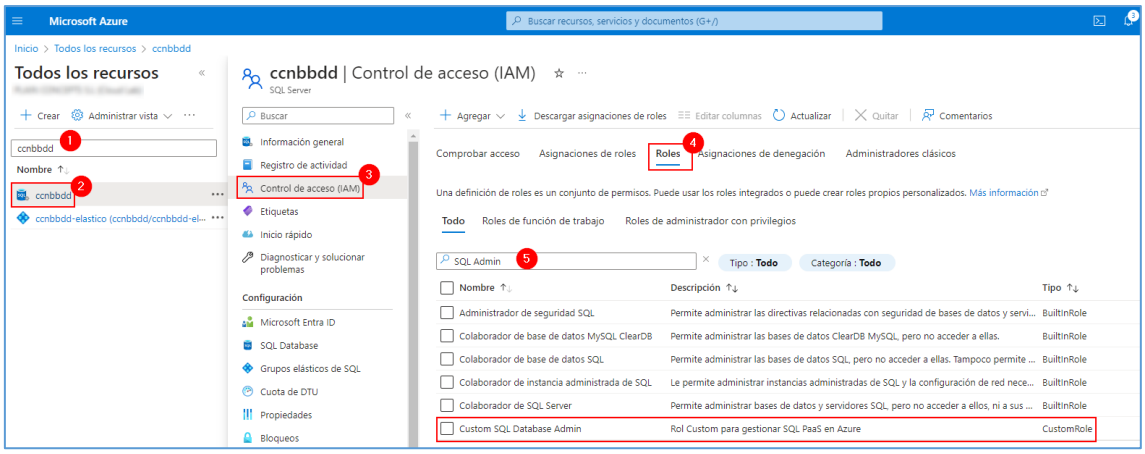
Nota: El fichero SQLDatabaseAdminRole.Json se puede encontrar adjunto en el apartado de Scripts de Configuración de la presente guía.

Al ejecutar este comando devuelve esta información.



Nota: Recordar que puede comprobar este nuevo ROL desde el portal tal y como se indica a continuación.

1. Pulsar en todos los recursos.
2. Buscar el nuevo servidor de SQL.
3. Pulsar en [Control de acceso (IAM)/Roles].

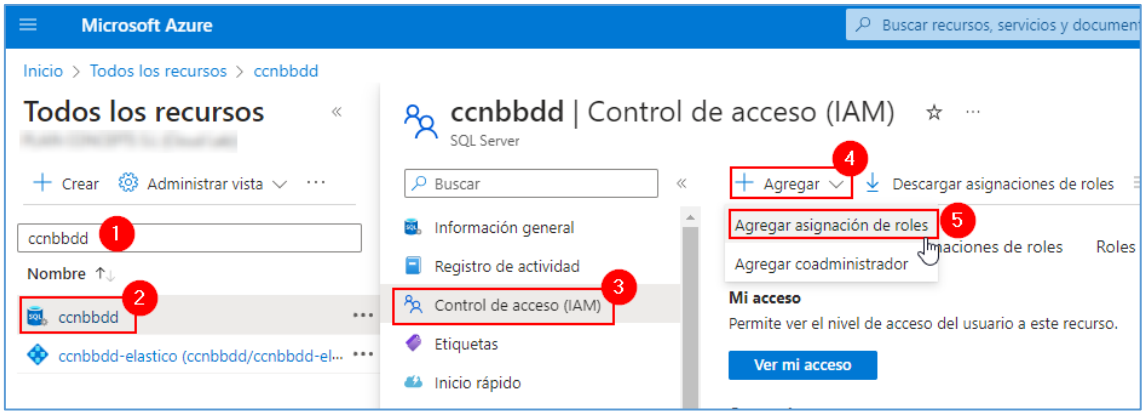


Desde ahí se puede ver el rol.

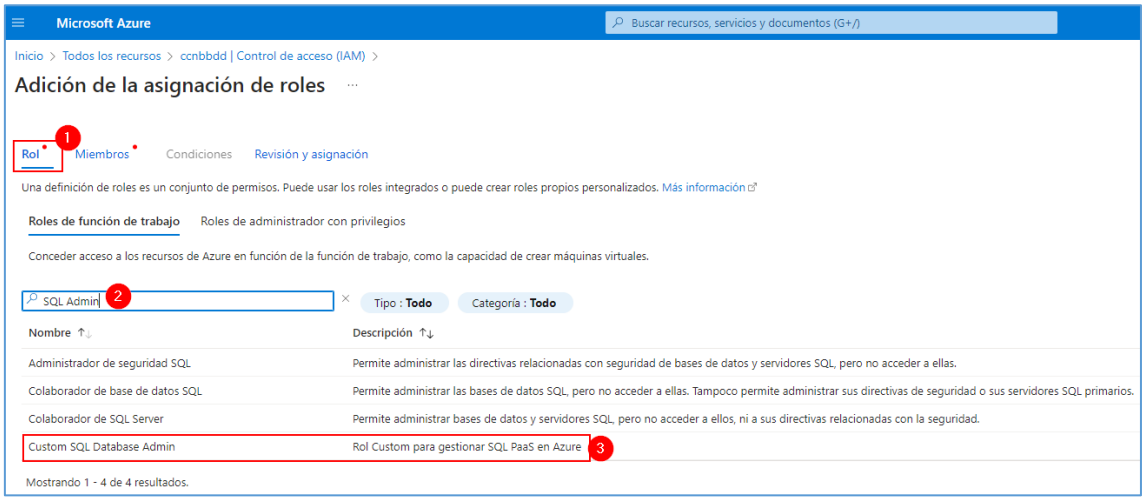
Asignación del nuevo rol

1. Pulsar en [todos los recursos].
2. Seleccionar la base de datos.

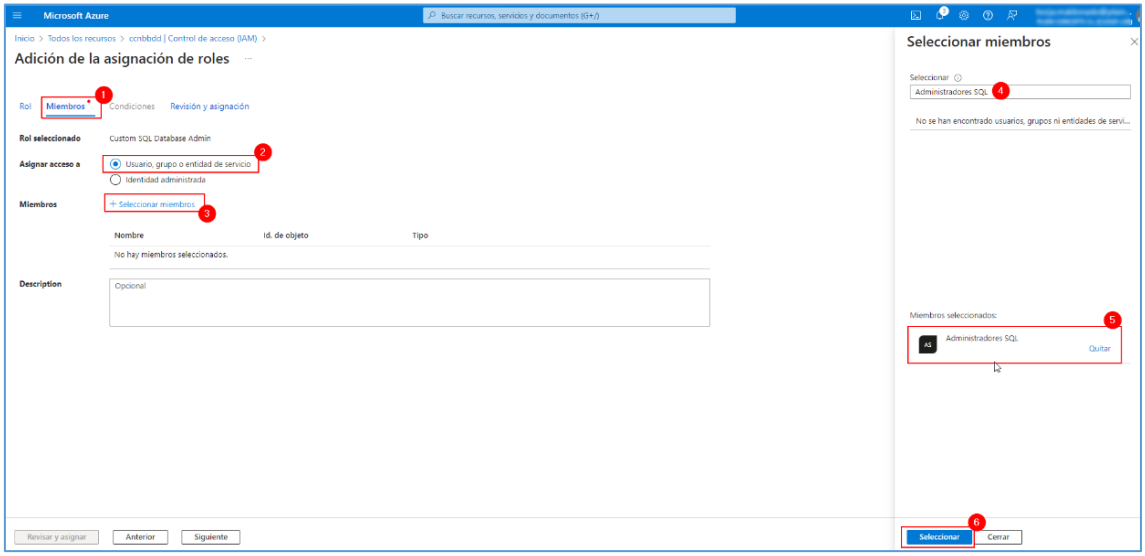
3. Pulsar en [Control de acceso (IAM)/Agregar] y [Agregar asignación de roles].



4. En la nueva ventana emergente, en el apartado de [Rol] buscar y seleccionar el Rol correspondiente.

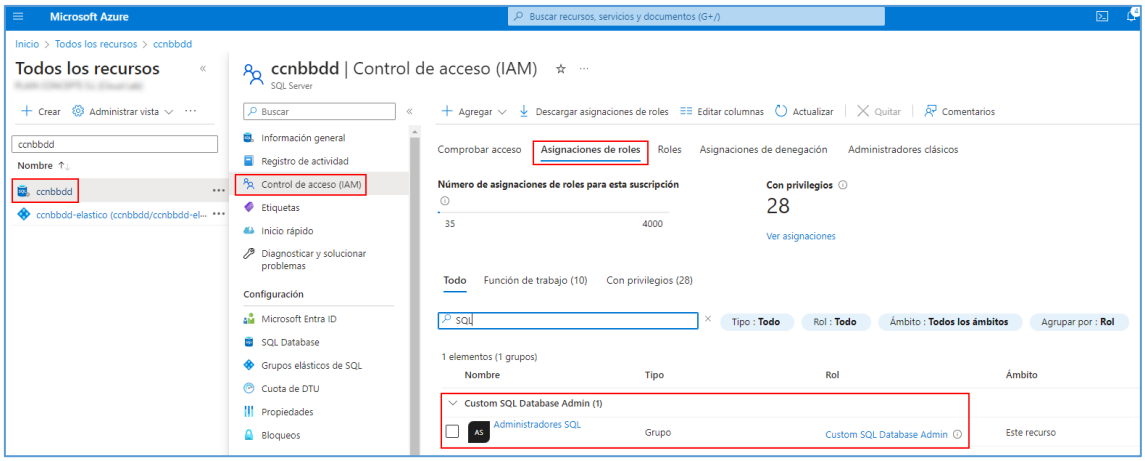


5. En el apartado de [Miembros], seleccionar el grupo de “Administradores SQL”.



6. Finalmente, pulsar en [Revisar y asignar].

Puede consultar los roles en la pestaña [Asignación de roles].



Nota: Esto es solo un ejemplo de la asignación de roles mediante **RBAC** desde el portal de Azure.

Nota: Para una gestión más avanzada hay que recurrir al apartado *[3.1.1.2 Requisitos de acceso/Control de acceso basado en roles]* de la guía. *[CCN-STIC-884A - Guía de configuración segura para Azure].*

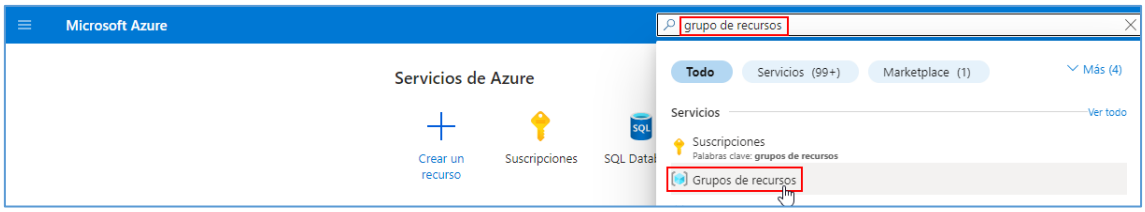
3.1.1.3 SEGREGACIÓN DE FUNCIONES Y TAREAS

Para la segregación de funciones y tareas se recomienda que se aplique un control de acceso basado en rol **(RBAC)** como se ha mencionado anteriormente ya que tiene varios roles integrados para recursos de Azure que se pueden asignar a usuarios, grupos, entidades de servicio e identidades administradas.

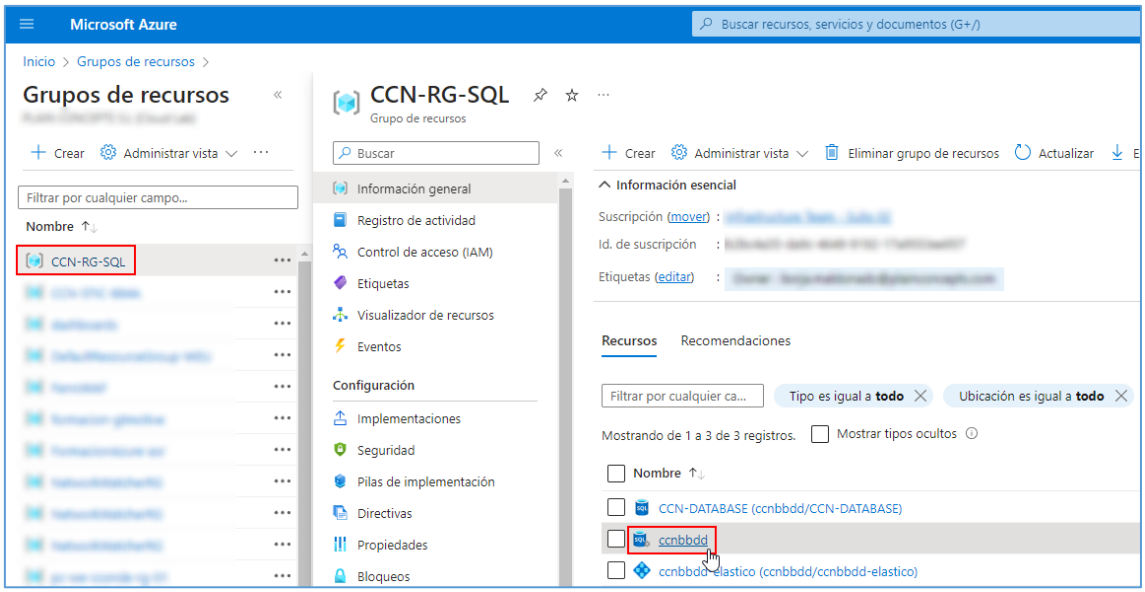
Las asignaciones de roles sirven para controlar el acceso a los recursos de Azure. Si los roles integrados no cumplen las necesidades específicas de su organización, puede crear sus propios roles personalizados para los recursos de Azure.

A continuación, algunos ejemplos que puede aplicar para delegar las funciones y tareas.

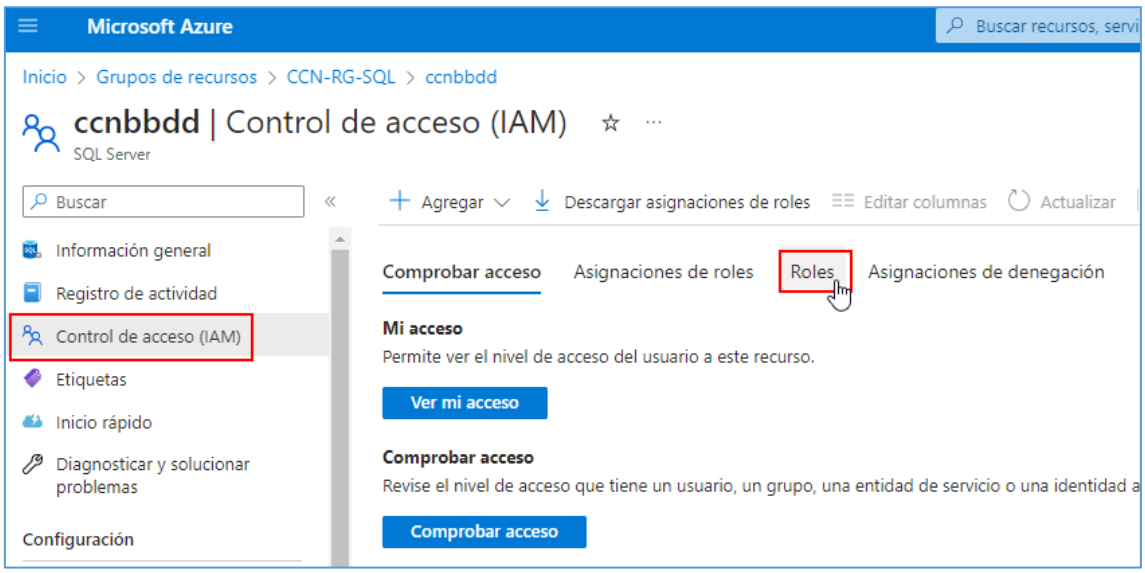
1. Desde el portal de Azure, en el buscador de la parte superior, escribir “grupo de recursos” y pulsar en la opción del desplegable:



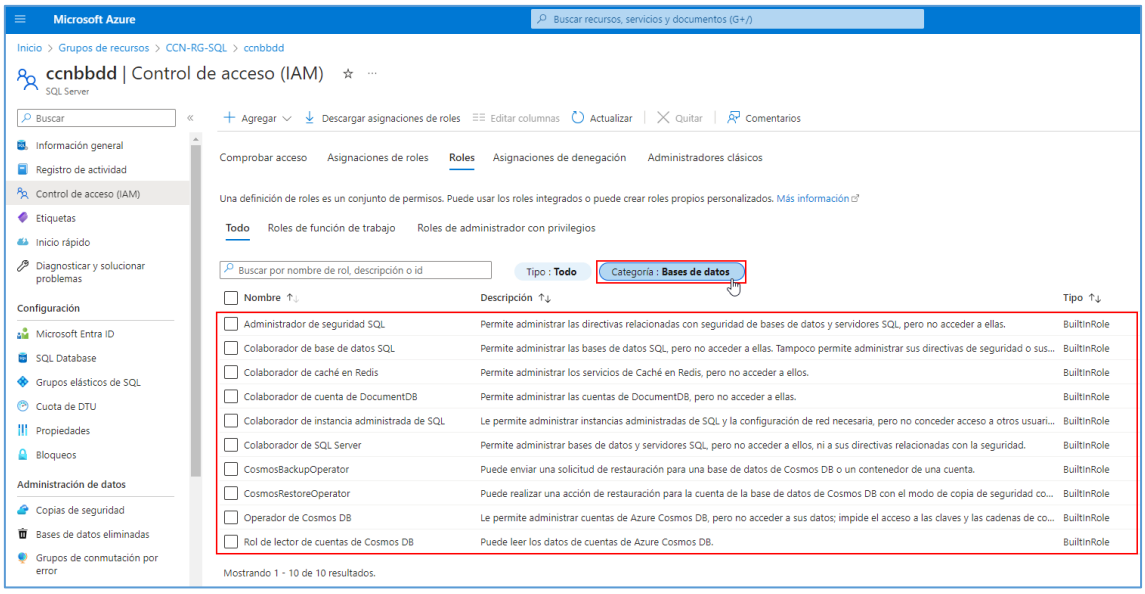
2. Seleccionar el grupo de recursos donde se encuentre la base de datos y pulsar el servidor de la base de datos:



3. Pulsar en [Control de acceso (IAM)] en el apartado de [Roles]:



4. Pulsar en [Categoría] y seleccionar "Base de datos".



Nota: Desde esta pestaña puede ver todos los roles que puede asignar desde el portal de Azure. Se ha seleccionado la categoría de "base de datos" pero se puede explorar otros roles.

Nota: Para una gestión más avanzada hay que recurrir al apartado *[3.1.1.2 Requisitos de acceso/Control de acceso basado en roles]* de la guía. *[CCN-STIC-884A - Guía de configuración segura para Azure*].

Nota: También se recomienda seguir el siguiente enlace de Microsoft: https://learn.microsoft.com/es-es/azure/role-based-access-control/role-assignments-portal

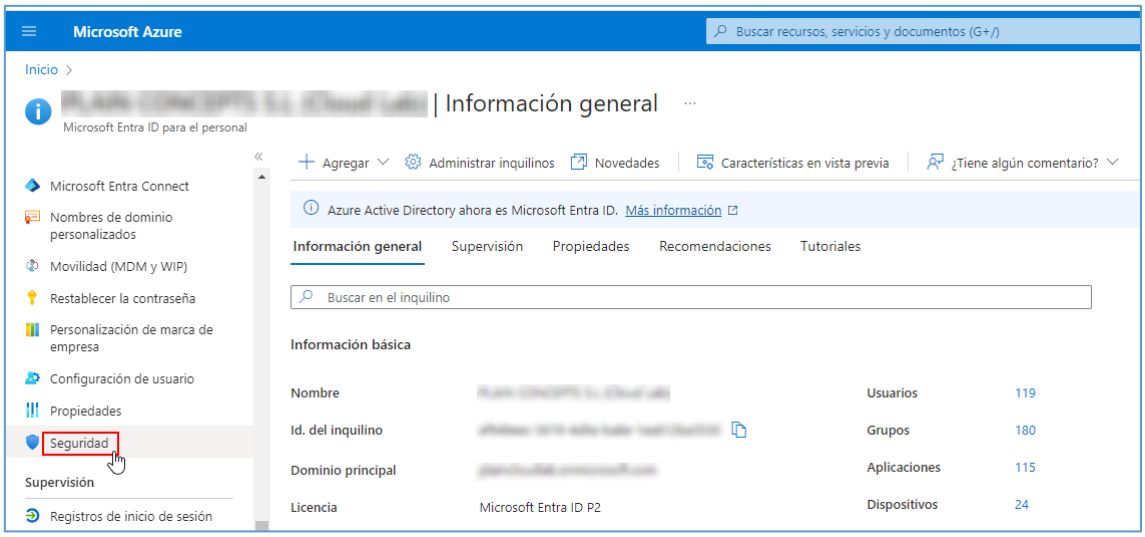
3.1.1.4 MECANISMO DE AUTENTICACIÓN (USUARIOS EXTERNOS)

Es importante destacar la integración de Azure Multi-Factor como un mecanismo seguro de autenticación. A su vez se recomienda crear una directiva de acceso condicional para los administradores de SQL.

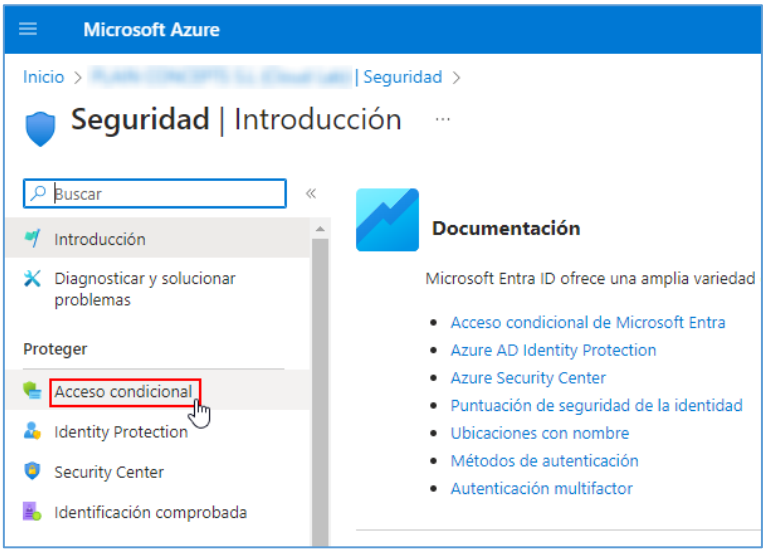
Para ello, debe seguir estas directrices:

1. Desde el buscador de la parte superior del portal de Azure, buscar "Microsoft Entra ID".

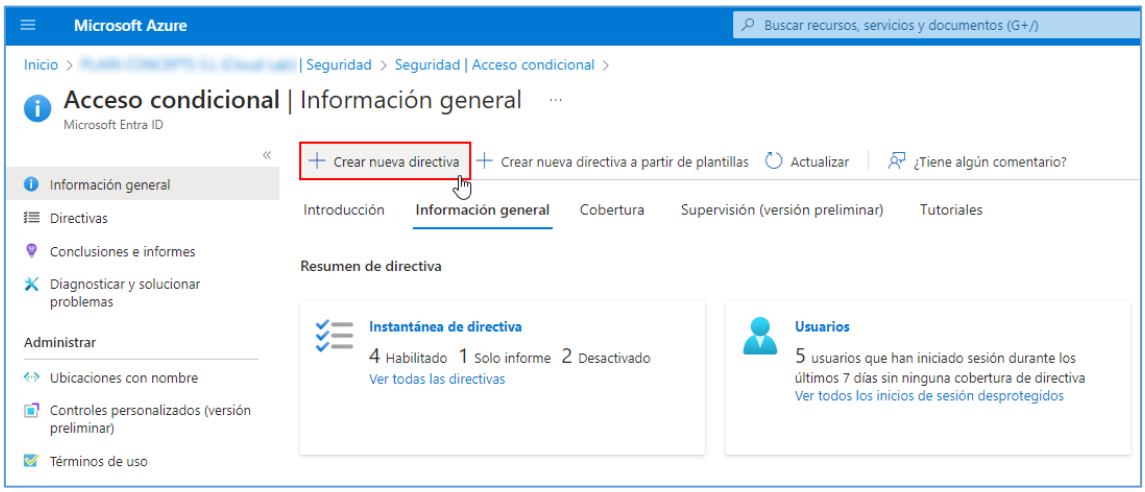
2. Ir al apartado de [Seguridad] del menú lateral izquierdo.



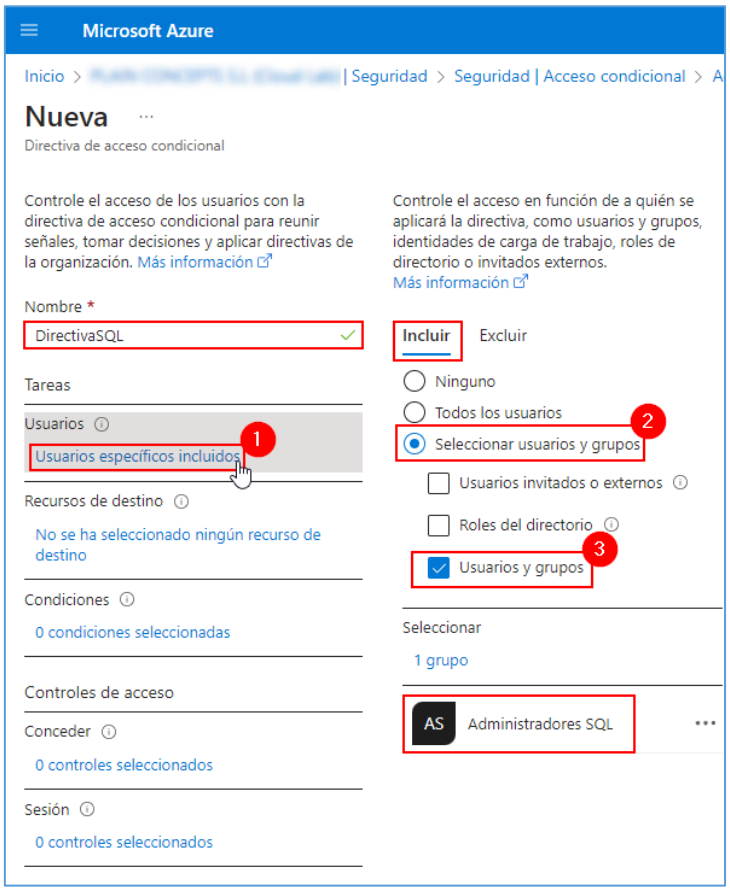
3. En la nueva ventana, ir al apartado de [acceso condicional] del menú lateral izquierdo.



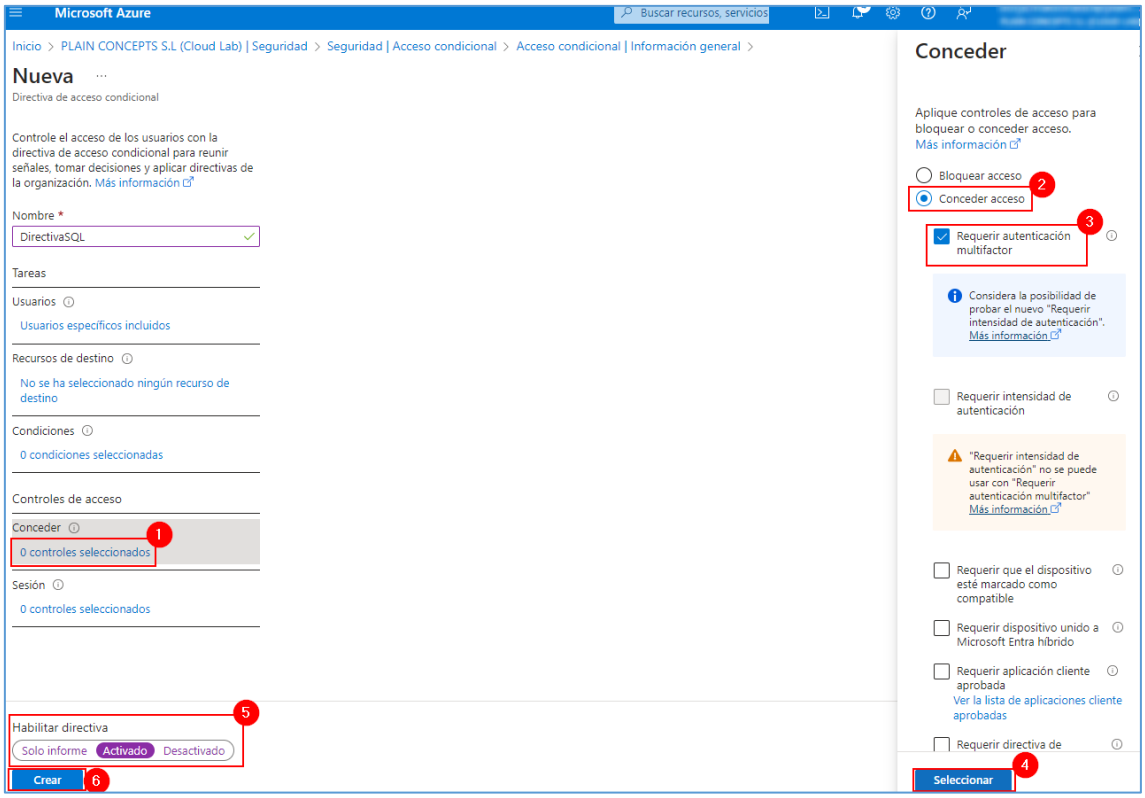
4. En la nueva ventana, pulsar en [Crear nueva directiva].



5. En la nueva ventana emergente, se dará nombre a la nueva directiva.
6. Pulsar en el apartado de [Usuarios], luego seleccionar la opción de "seleccionar usuarios y grupos", después "Usuarios y grupos".
7. En el nuevo apartado emergente, se buscará el grupo "Administradores SQL" y se seleccionará, quedando la configuración de la siguiente manera:

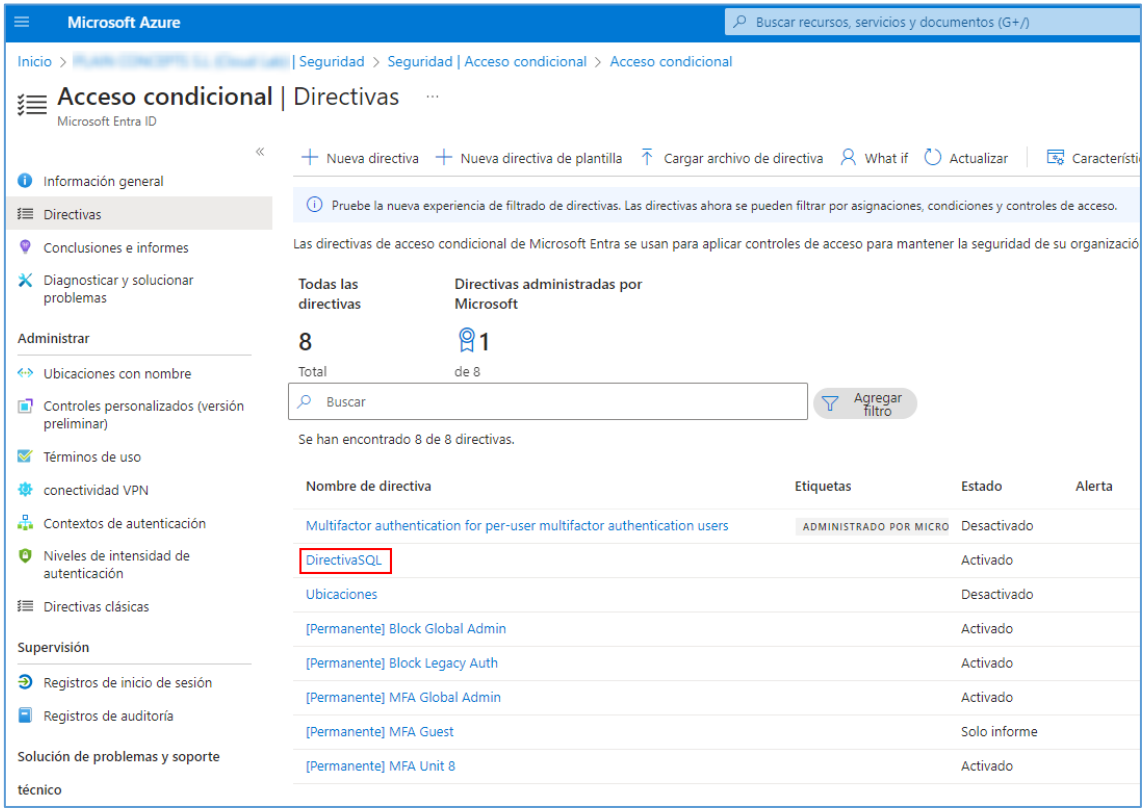


8. A continuación, pulsar en [controles seleccionados] dentro del apartado de Controles de acceso – conceder.
9. En el apartado emergente, seleccionar "Conceder acceso" y "Requerir autenticación multifactor".
10. Finalmente, habilitar la directiva seleccionando la opción de "Activado", quedando la configuración de la siguiente manera:



11. Para finalizar, pulsar en [Crear].

Aparecerá la nueva directiva de acceso condicional para los usuarios Administradores de SQL. Esto fuerza a que el grupo de Administradores de SQL utilicen doble factor de autenticación.



Es importante conocer los conceptos del acceso condicional ya que puede asignar diversas condiciones de autenticación.

Se pueden agregar distintas condiciones desde una directiva de acceso condicional. Atendiendo dispositivos autorizados, ubicaciones geográficas, rangos de ips, grupos de usuarios entre otros.

Nota: Para una gestión más avanzada hay que recurrir al apartado *[3.1.1.2 Requisitos de acceso/Acceso condicional]* de la guía. *[CCN-STIC-884A - Guía de configuración segura para Azure].*

3.1.1.5 MECANISMO DE AUTENTICACIÓN (USUARIOS DE LA ORGANIZACIÓN)

Los mecanismos de autenticación aplicables a los usuarios de la organización son los mismos que para los usuarios externos. Para más información ver el apartado *[3.1.1.4 Mecanismos de autenticación (usuarios externos)* de la presente guía.

3.1.2 EXPLOTACIÓN

3.1.2.1 REGISTRO DE LA ACTIVIDAD

El registro de actividad contiene todas las operaciones de escritura (PUT, POST, DELETE) para los recursos.

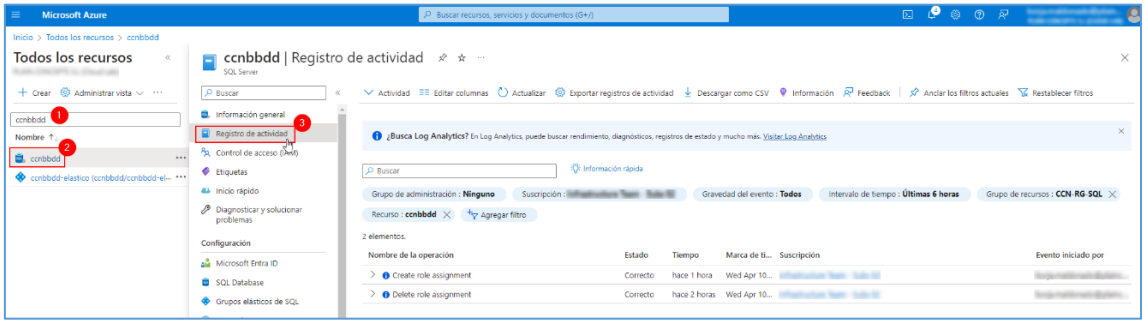
Los registros de actividad se conservan 90 días. Puede consultar cualquier intervalo de fechas, siempre que no hayan transcurrido más de 90 días desde la fecha inicial.

Mediante los registros de actividad, puede determinar:

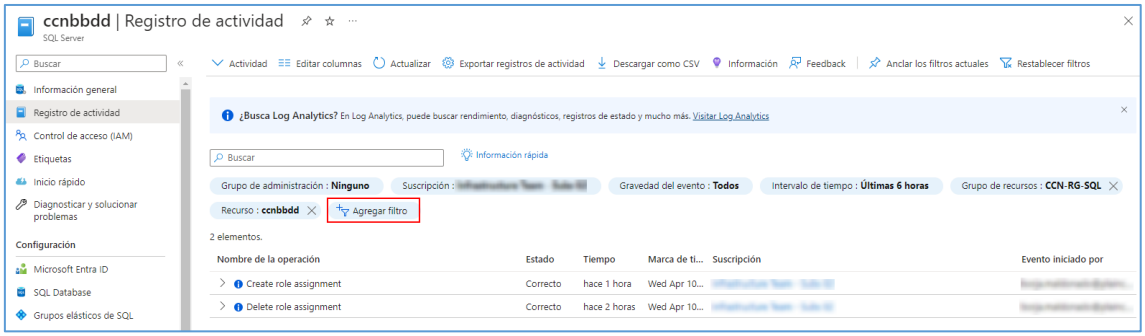
- Qué operaciones se realizaron en los recursos en la suscripción.
- Quién inició la operación.
- Cuando tuvo lugar la operación.
- El estado de la operación.
- Los valores de otras propiedades que podrían ayudarle en la investigación de la operación.

Portal de Azure

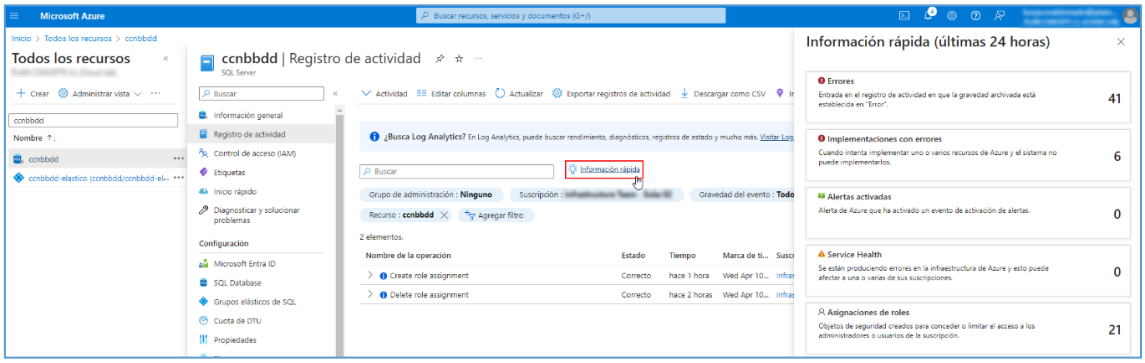
1. Para ver los registros de actividad mediante el portal, pulsar en todos los recursos.
2. Pulsar en la [base de datos].
3. Ir al apartado de [Registro de actividad].



4. En este panel se encuentran varios filtros que puede aplicar.



5. Pulsando en [Información rápida] se puede visualizar los eventos de las últimas 24 horas. Así mismo, desde este panel, se pueden personalizar filtros de búsqueda de eventos.



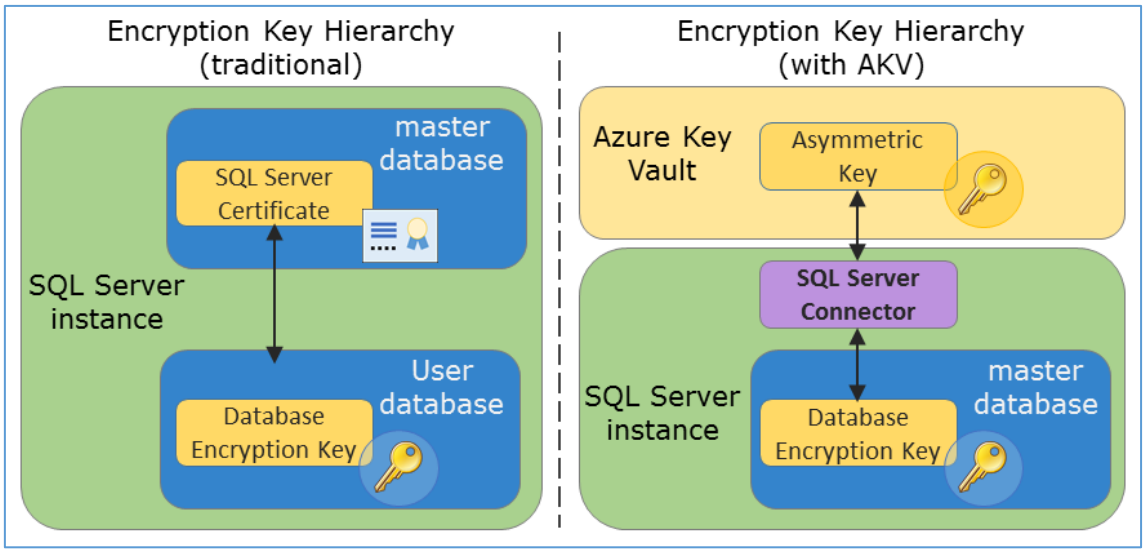
3.1.2.2 PROTECCIÓN DE CLAVES CRIPTOGRÁFICAS

Azure SQL proporciona varios tipos de cifrado que ayudan a proteger información confidencial, como cifrado de datos transparente (TDE).

El cifrado de datos transparente (TDE) de Azure SQL con clave gestionada por el cliente permite el escenario "*Bring Your Own Key*" para la protección de datos en reposo, y permite implementar la separación de funciones en la gestión de claves y datos. Con la TDE gestionada por el cliente, éste es responsable y tiene el control total de la gestión del ciclo de vida de la clave (creación, carga, rotación y eliminación de la clave), los permisos de uso de la clave y la auditoría de las operaciones realizadas con las claves.

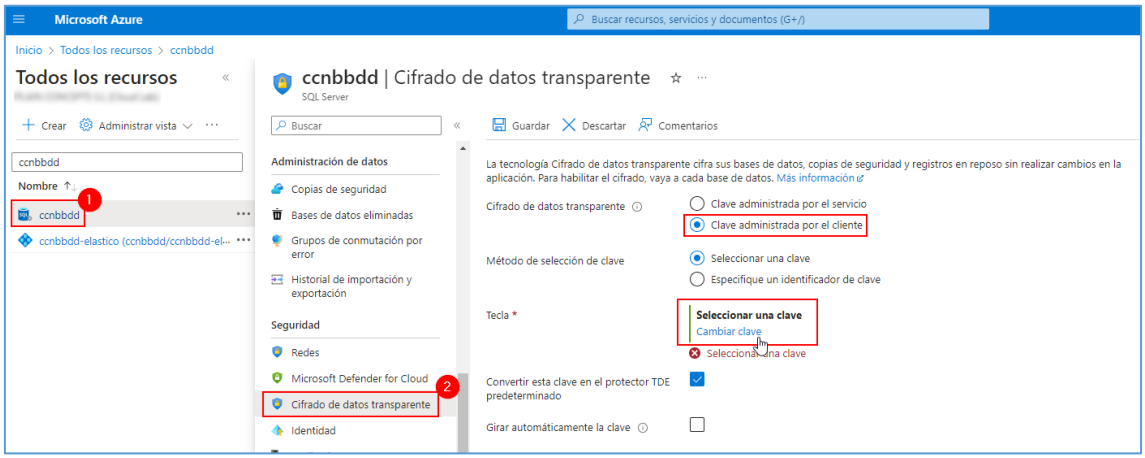
En este escenario, la clave utilizada para el cifrado de la clave de cifrado de la base de datos (DEK), denominada "protector TDE", es una clave asimétrica gestionada por el cliente y almacenada en un Azure Key Vault (AKV) propiedad del cliente y gestionada por él, un sistema externo de gestión de claves basado en la nube.

En la imagen siguiente se compara la jerarquía de claves de administración y servicio tradicional con el sistema del Almacén de claves de Azure.



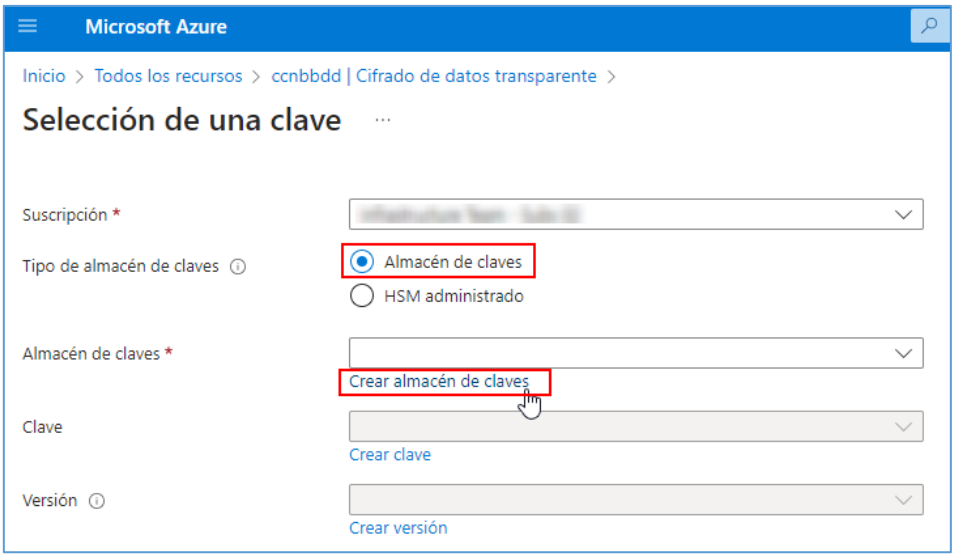
A continuación, se describen los pasos que se deben realizar para cifrar su base de datos utilizando Azure Key Vault.

1. Desde el portal de Azure pulsar en [todos los recursos] y seleccionar su servidor de [base de datos].
2. En el menú lateral izquierdo, en el apartado de seguridad, pulsar en [Cifrado de datos transparente].
3. Seleccionar la opción de [Clave administrada por el cliente].
4. Para seleccionar una clave, pulsar en [Cambiar clave].



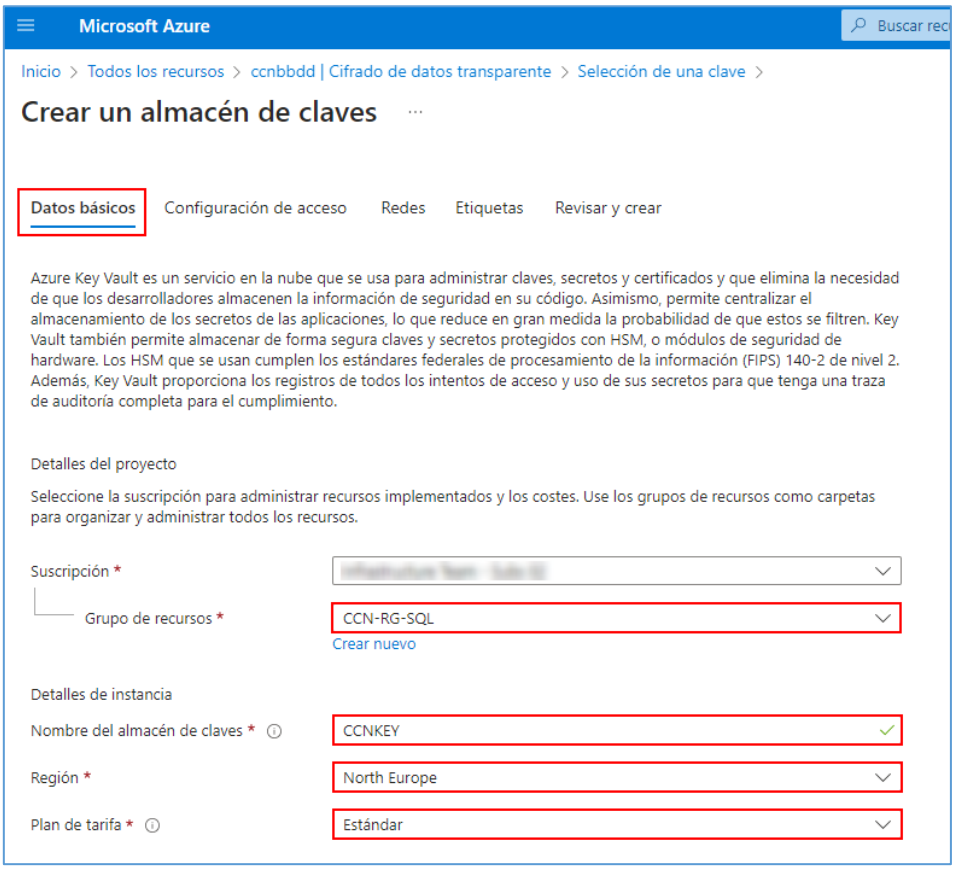
Se abrirá una ventana nueva donde se seleccionará la opción de [Almacén de Claves] (Key Vault). En este apartado de la configuración se podrá seleccionar un Almacén de Claves que previamente estuviera creado y donde se almacena la clave a utilizar para el cifrado o bien se podrá crear uno nuevo. A continuación, se muestra la opción de crear uno nuevo:

1. Pulsar en [Crear almacén de claves].

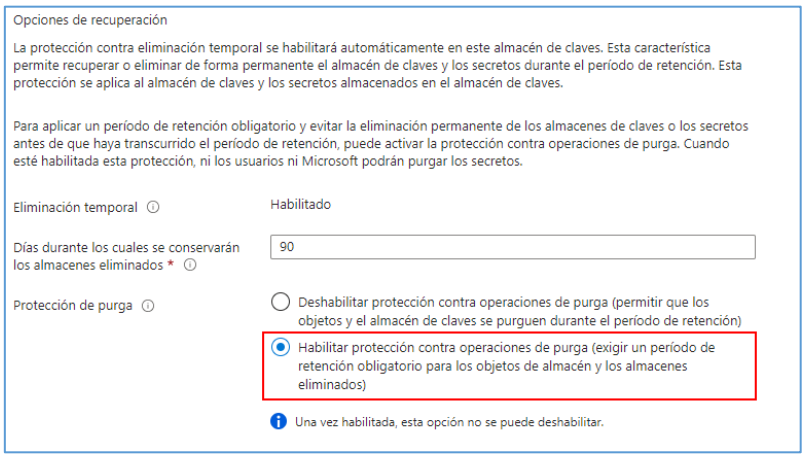


2. Se abrirá una ventana nueva donde se especificarán los siguientes campos:

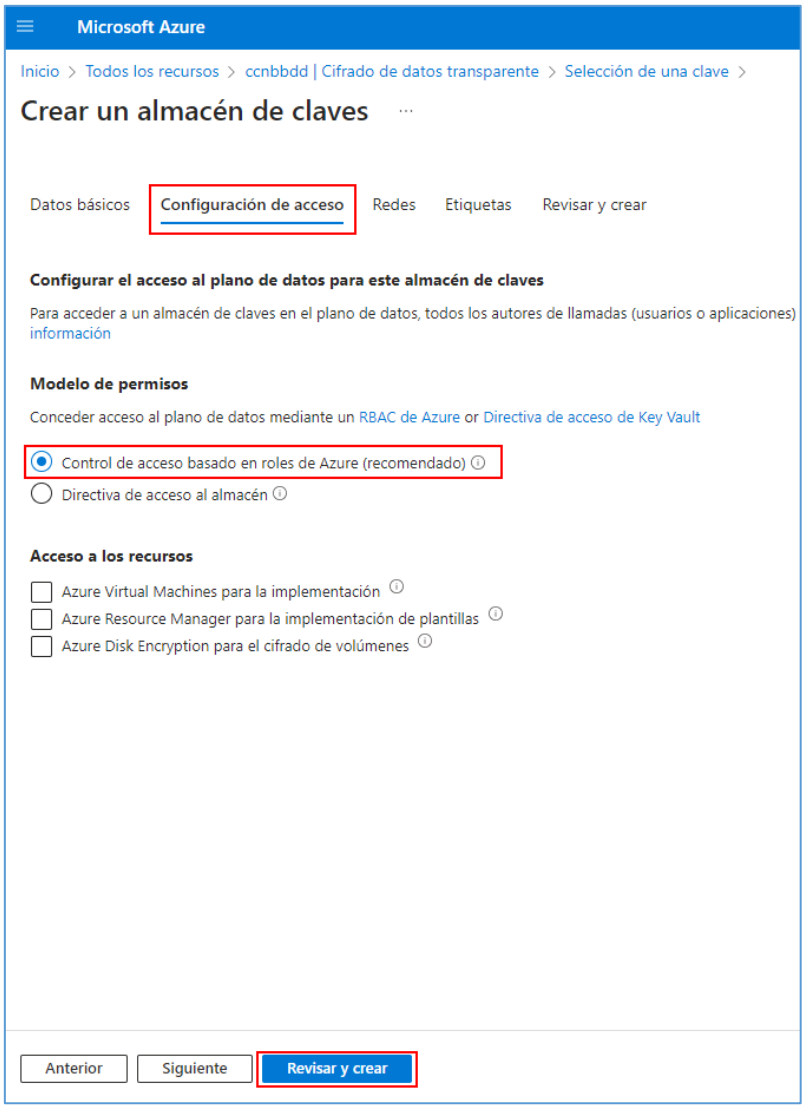
- **Suscripción**: Seleccionar su suscripción.
- **Grupo de recursos**: Se recomienda crear un nuevo grupo que estará dedicado para este Almacén. Solo le pedirá un nombre para definirlo.
- **Nombre del almacén de claves**: Definir el nombre que se va a utilizar para el nuevo almacén.
- **Región**: Seleccionar Norte de Europa.
- **Plan de tarifa**: Seleccionar tarifa Estándar.



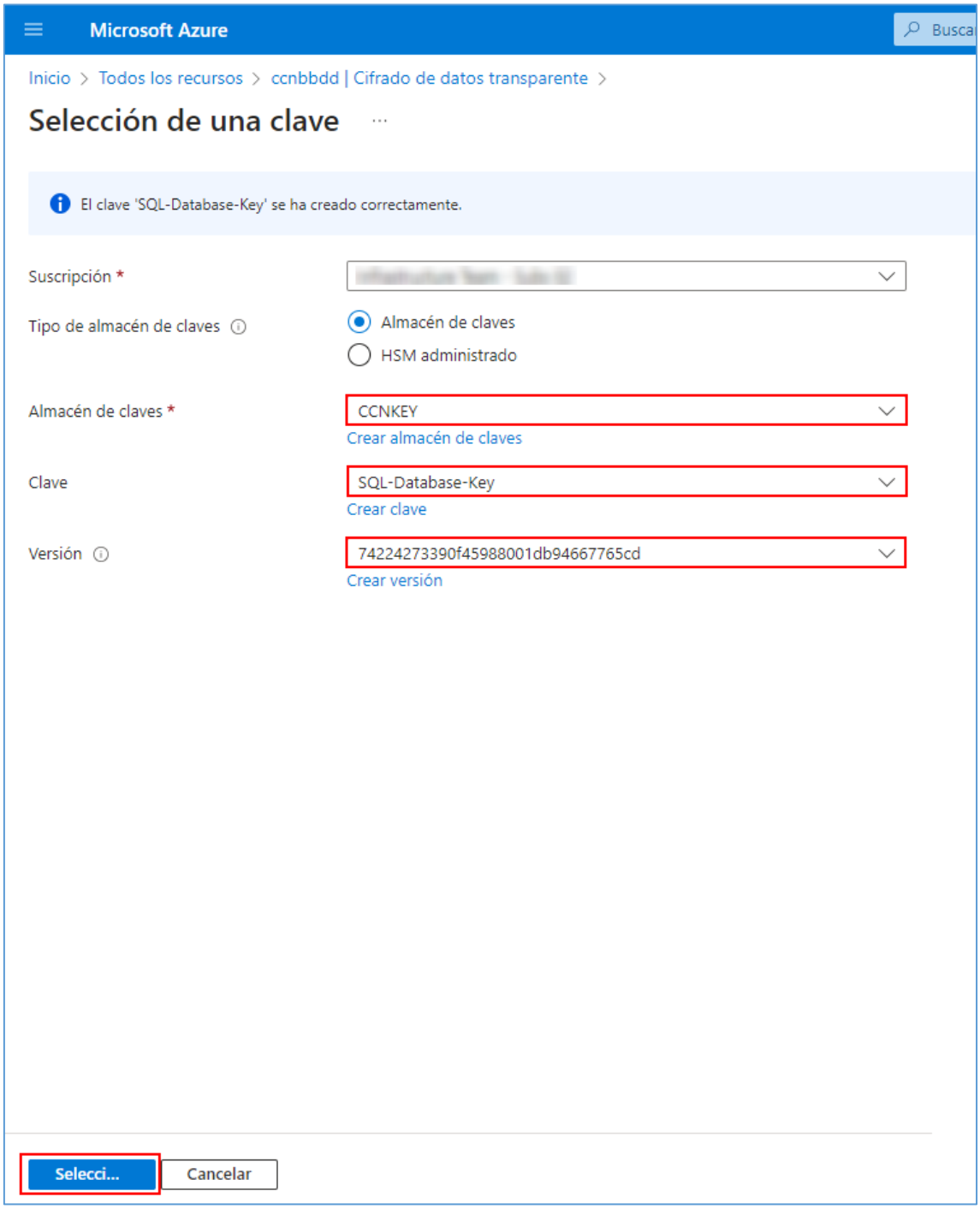
- **Protección de purga**: Habilitar protección contra operaciones de purga.



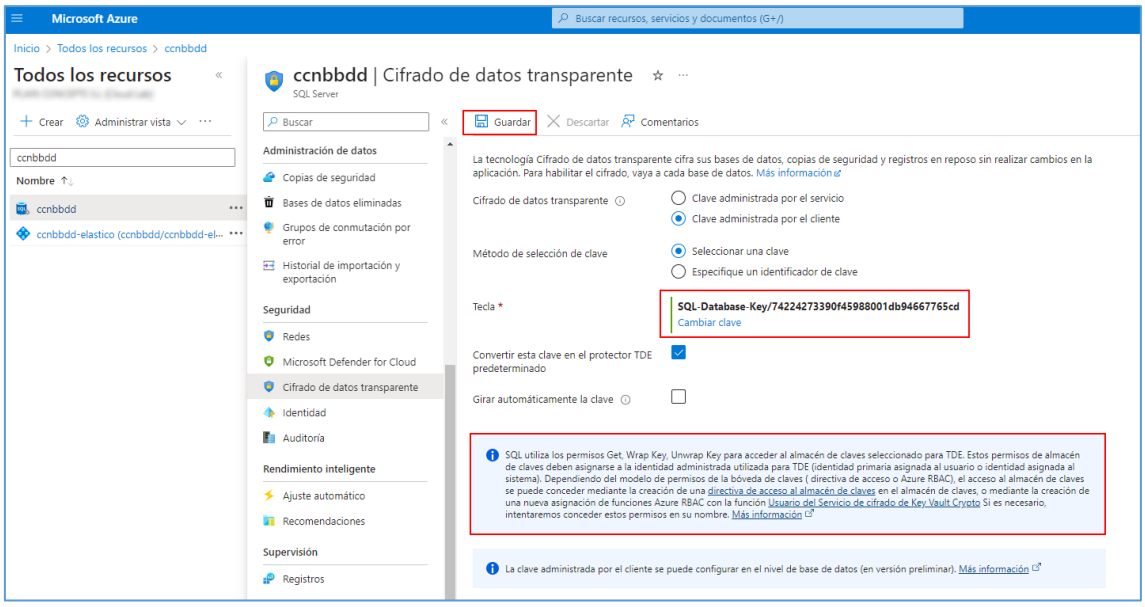
3. Ir al apartado de [Configuración de acceso].
   - **Modelo de permisos**: Seleccionar Control de acceso basado en roles.
4. Finalmente pulsar en [Revisar y crear].



Una vez creado el almacén de claves, se seleccionará la clave correspondiente con la que se encriptará tanto las bases de datos como copias de seguridad. Dicha clave se generará por parte de los responsables de creación de claves que para cumplir con los requisitos de seguridad tendrá que ser un equipo independiente de los administradores de la base de datos. Una vez seleccionada la clave de encriptación y su versión, pulsar en [Seleccionar].

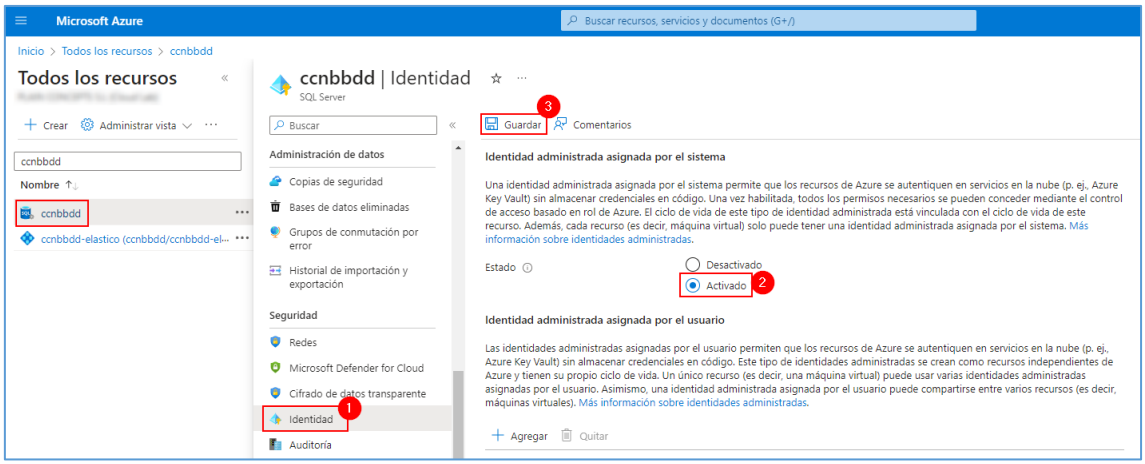


Tras el proceso de selección de la clave de encriptación, se deberán guardar los cambios realizados pulsando en [Guardar] tal y como se muestra en la siguiente imagen.



Para permitir al servidor de la base de datos poder acceder al Key Vault, será necesario habilitar la identidad administrada del servidor y posteriormente darle los permisos necesarios en el Key Vault. Para ello:

1. Ir al apartado de [Identidad] del menú de Seguridad.
2. Activar la identidad administrada asignada por el sistema
3. Guardar los cambios



Los permisos se darán a la identidad recién generada que tendrá el nombre del servidor de la base de datos. Tal y como muestra la primera imagen, los permisos que se han de dar son los de "*Usuario del Servicio de cifrado de Key Vault Crypto*".

Nota: Para una gestión más avanzada hay que recurrir al apartado *[3.1.2.2 Protección de claves criptográficas]* de la guía. *[CCN-STIC-884A - Guía de configuración segura para Azure].*

3.1.3 MONITORIZACIÓN DEL SISTEMA

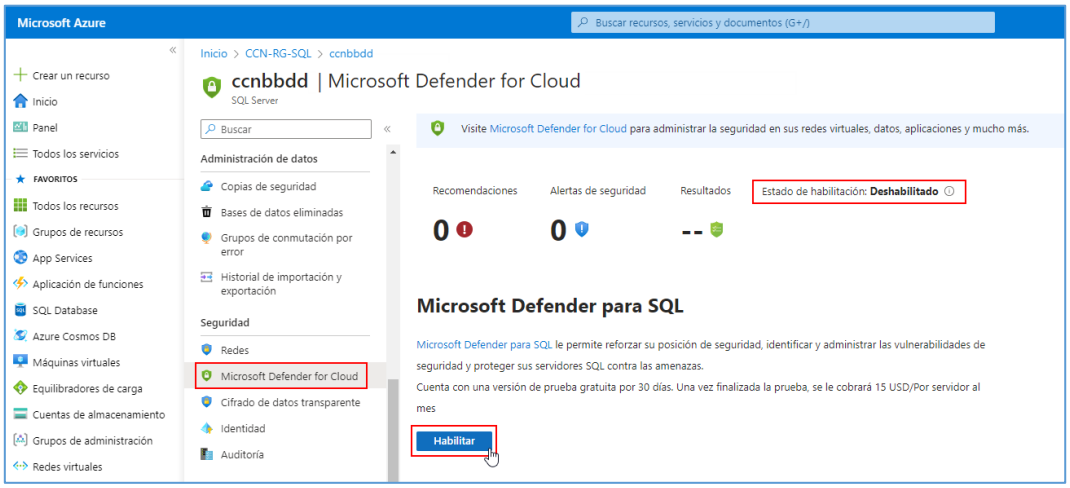
3.1.3.1 DETECCIÓN DE LA INTRUSIÓN

Microsoft Defender para SQL es un plan de Defender en Microsoft Defender for Cloud. Azure Defender para SQL incluye funcionalidades para buscar y mitigar las posibles vulnerabilidades de la base de datos, así como para detectar actividades anómalas que puedan indicar una amenaza para ella. Proporciona una ubicación única para habilitar y administrar estas funcionalidades.

Este servicio proporciona una funcionalidad llamada “Advanced Thread Protection” (Protección avanzada contra amenazas) que permite detectar actividades anómalas de intentos inusuales y posiblemente dañinos de acceder a las bases de datos. Supervisa continuamente la base de datos en busca de actividades sospechosas y proporciona alertas de seguridad inmediatas sobre posibles vulnerabilidades, ataques de inyección Azure SQL y patrones anómalos de acceso a la base de datos.

Para poder activar activar Microsoft Defender para SQL se deben seguir los suiguentes pasos:

1. Desde el portal de Azure, buscar y seleccionar el Servidor de la base de datos.
2. En el menú lateral izquierdo, en el apartado de seguridad, pulsar en [Microsoft Defender for Cloud]
3. Selección la opción de [Habilitar].



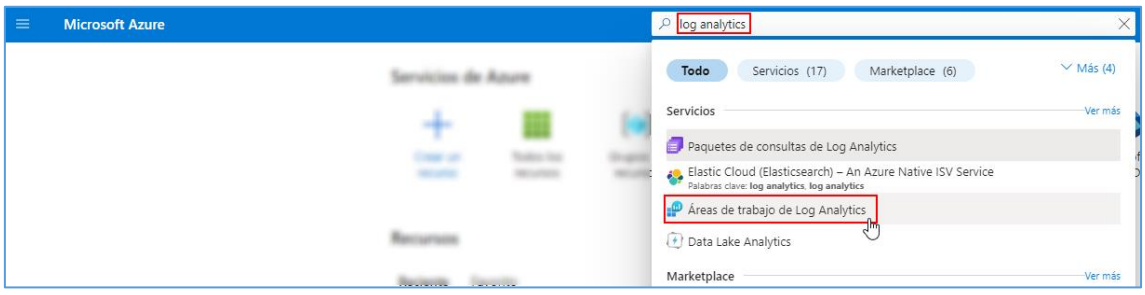
Una vez habilitado el servicio, se verá un vínculo [Configurar] a lado del estado de habilitación donde se podrá editar la configuracion:

3.1.3.2 SISTEMA DE MÉTRICAS

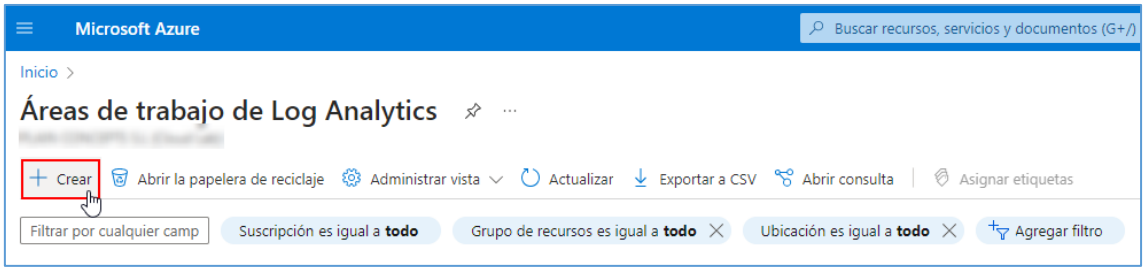
Log Analytics de Azure Monitor es una herramienta que se debe usar para obtener información detallada de los registros de Azure Monitor.

Para ello, debe seguir estas instrucciones de configuración:

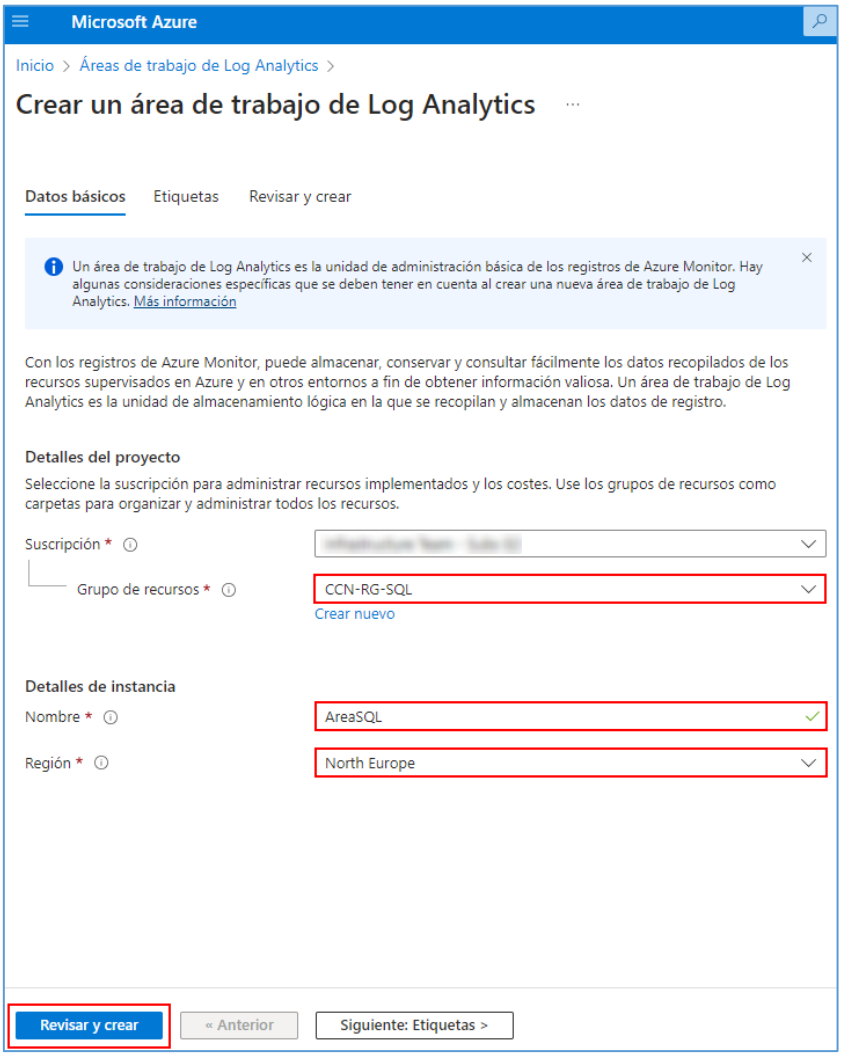
1. Desde el portal de Azure, ir a la barra de búsqueda y buscar “log analytics”.



1. Pulsar en [Crear].



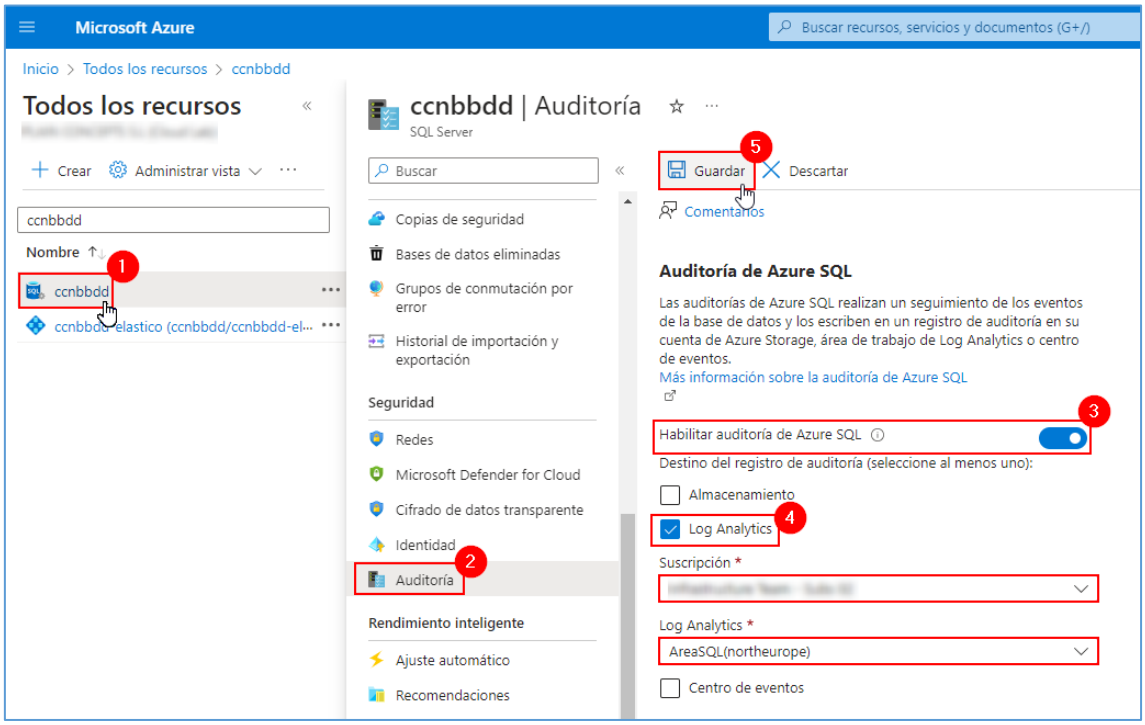
2. Se abre una ventana nueva donde se debe rellenar la siguiente información:
   - **Grupo de recursos**: Se puede seleccionar el grupo de recursos donde se encuentre la propia base de datos o elegir uno nuevo.
   - **Nombre**: Proporcionar un nombre al área de trabajo de Log Analytics.
   - **Región**: Localización donde se quiera ubicar el recurso (Norte de Europa).
3. Finalmente pulsar en [Revisar y crear].



Nota: Este proceso puede tardar unos minutos.

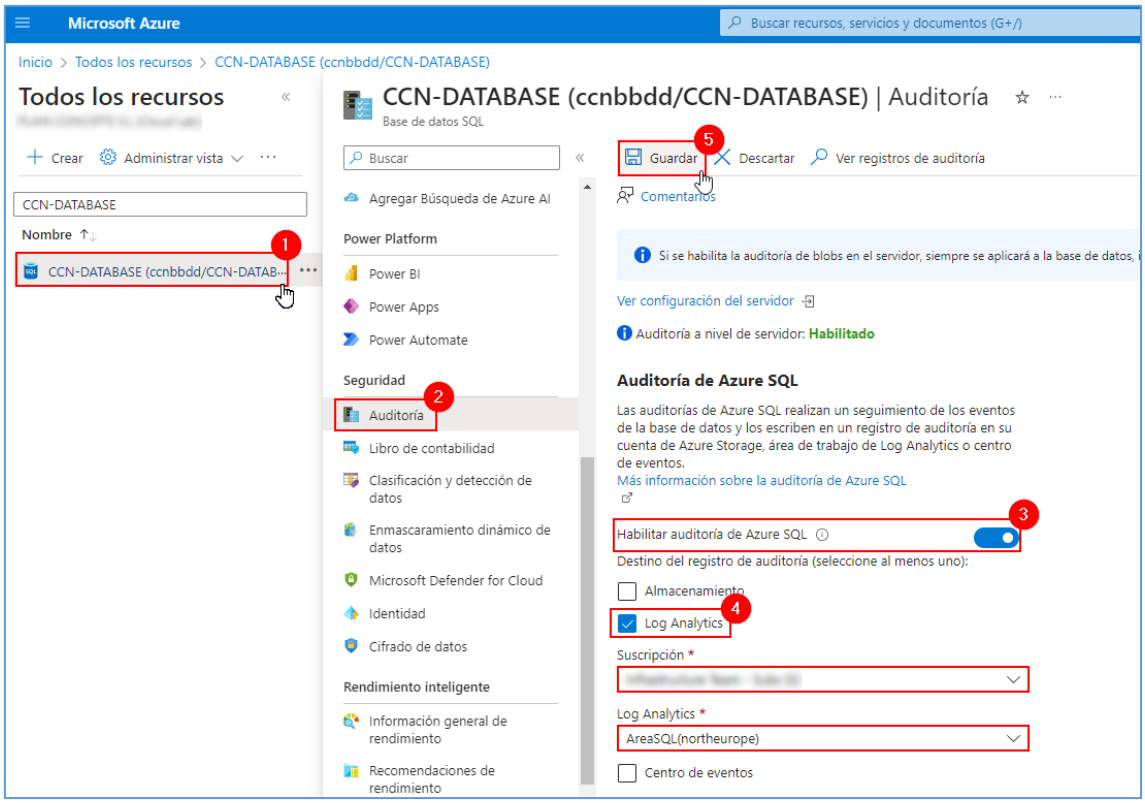
Una vez creado el área de trabajo de Log Analytics, se procederá a la configuración de la monitorización del servidor y de la base de datos.

4. Desde el portal de Azure, buscar y seleccionar el Servidor de la base de datos.
5. En el menú lateral, en el apartado de Seguridad, pulsar en [Auditoría].
6. Habilitar la función de [auditoría de Azure SQL].
7. Seleccionar la opción de [Log Analytics] y seleccionar el área de trabajo anteriormente creado.
8. Finalmente pulsar en [Guardar].



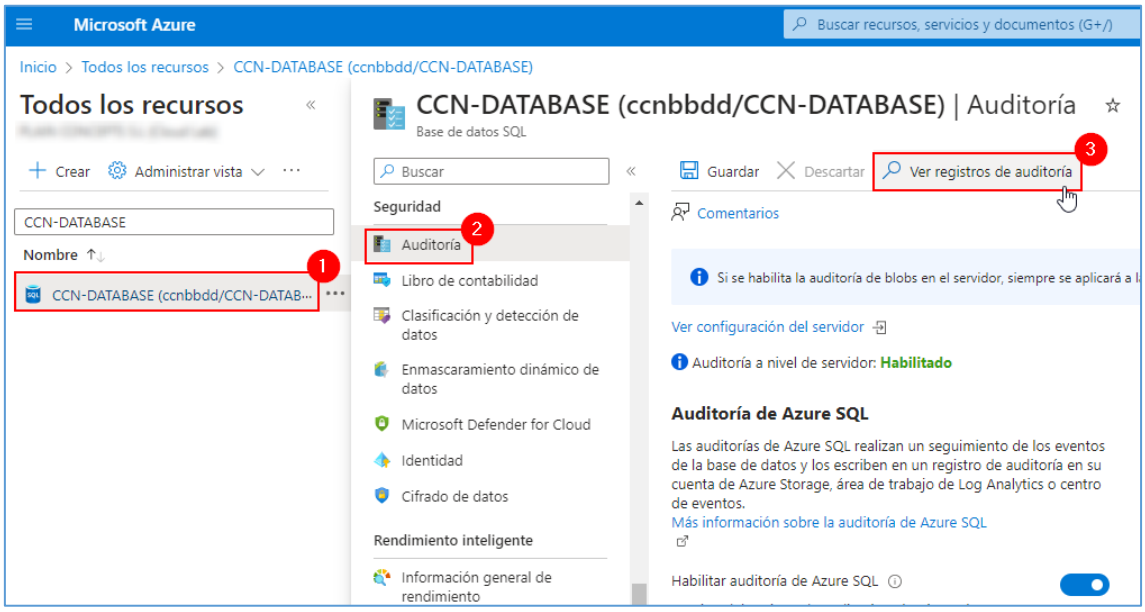
Este proceso se realizará también a nivel de base de datos, para ello se debe seguir un proceso análogo al llevado a cabo para el Servidor:

1. Desde el portal de Azure, buscar y seleccionar el Base de Datos.
2. En el menú lateral, en el apartado de Seguridad, pulsar en [Auditoría].
3. Habilitar la función de [auditoría de Azure SQL].
4. Seleccionar la opción de [Log Analytics] y seleccionar el área de trabajo anteriormente creado.
5. Finalmente pulsar en [Guardar].

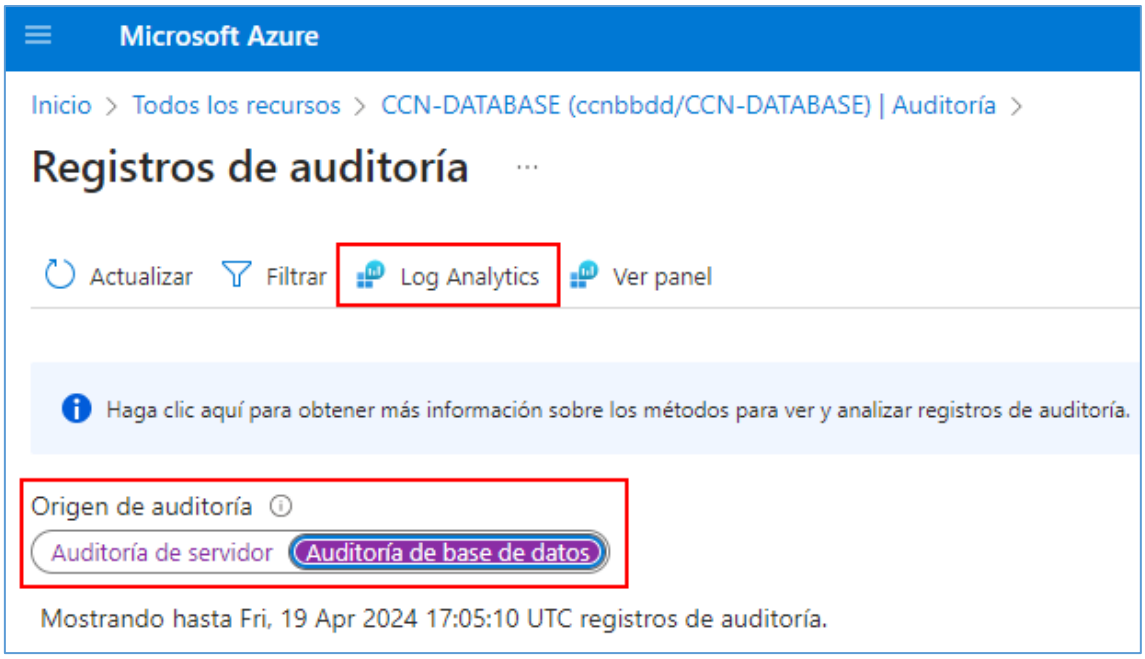


Una vez configurada la monitorización, los diferentes registros contenidos en el área de trabajo de Log Analytics se pueden consultar bien desde el propio recurso de Log Analytics o bien de la siguiente manera:

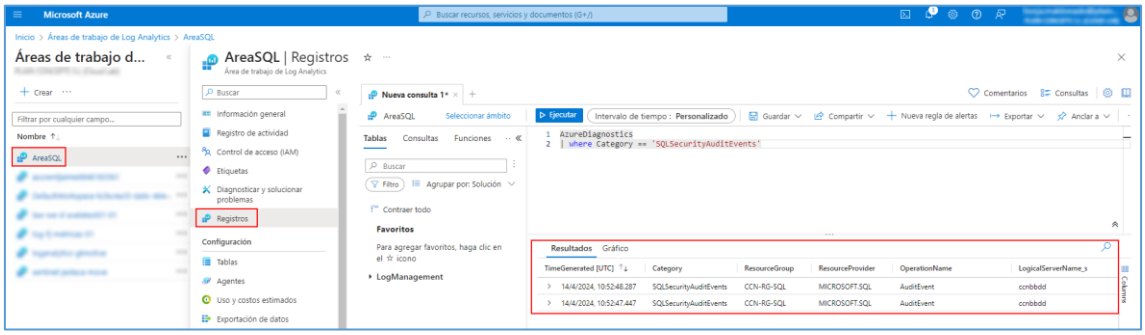
1. Desde el portal de Azure, buscar y seleccionar el Base de Datos.
2. En el menú lateral, en el apartado de Seguridad, pulsar en [Auditoría].
3. Ir al apartado de [Ver registros de auditoría].



4. En la nueva ventana, seleccionar [auditoría de servidor] o [auditoría de base de datos] y pulsar sobre [Log Analytics].



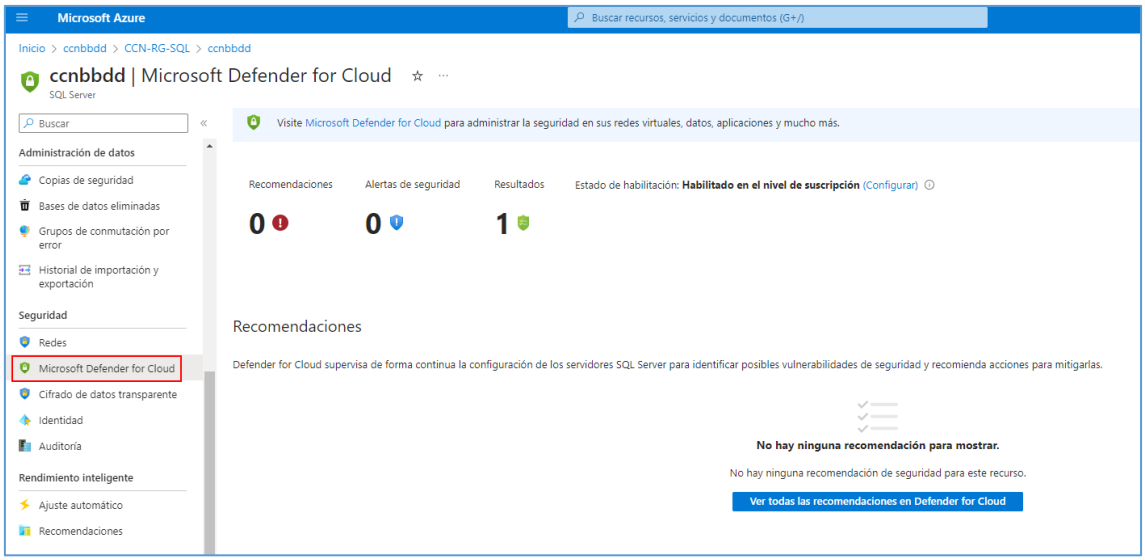
5. Aparecerá un área de consulta donde se mostrarán los diferentes registros en función del intervalo de tiempo que se establezca. También se pueden aplicar diferentes filtros mediante la consulta.



Nota: Para una gestión más avanzada hay que recurrir al apartado *[3.1.4 Monitorización de sistema]* de la guía. *[CCN-STIC-884A - Guía de configuración segura para Azure].*

3.1.3.3 VIGILANCIA

El servicio de Microsoft Defender para SQL, comentado en el apartado 3.1.3.1, proporciona herramientas de vigilancia gracias a las continuas comprobaciones de seguridad que realiza sobre los servidores de bases de datos en los que esté habilitado. Los diferentes hallazgos y recomendaciones que se encuentren se mostrarán en el apartado de Defender for Cloud del servidor:



Nota: Para más información sobre Microsoft Defender for Cloud recurrir al apartado *[3.1.4.3 Monitorización del sitema / Vigilancia]* de la guía. *[CCN-STIC-884A - Guía de configuración segura para Azure].*

3.2 MEDIDAS DE PROTECCIÓN

3.2.1 PROTECCIÓN DE LAS COMUNICACIONES

3.2.1.1 PERÍMETRO SEGURO

Azure SQL permite varias formas de conectividad con la base de datos, dependiendo de las características de configuración de red. Para tener una base de datos protegida dentro de un perímetro seguro, la configuración que se establece para la conectividad de Azure SQL es mediante un punto de conexión privado el cual solo será accesible a través de red interna, estando el acceso público deshabilitado.

Para poder establecer conexión con el servidor de la base de datos de Azure SQL será necesario que el origen de la conexión esté dentro de la misma red donde se encuentre la base de datos en Azure, o bien tener conectividad establecida con dicha red, bien mediante “peering” con otra red virtual dentro si es dentro de Azure o bien mediante túnel VPN o Express Route si se trata de entornos locales (on-premises).

Es importante destacar que, a parte de tener la conectividad establecida, también será necesario tener la comunicación habilitada, es por ello que se tendrán que revisar las reglas de Firewall del entorno local para que pueda haber una correcta comunicación entre el origen de la conexión y la base de datos de Azure SQL.

Existen otros tipos de recomendaciones para el aislamiento de la base de datos, así como la configuración de Azure firewall y NSG.

Nota: Para una gestión más avanzada, hay que recurrir al apartado *[3.2.1.2 Protección de las comunicaciones/Perímetro seguro]* de la guía. *[CCN-STIC-884A - Guía de configuración segura para Azure].*

3.2.2 PROTECCIÓN DE LA INFORMACIÓN

3.2.2.1 CALIFICACIÓN DE LA INFORMACIÓN

Para la clasificación de la información se recomienda el uso de etiquetas.

Se componen de clave-valor definidos por el usuario, se pueden colocar directamente en un recurso o un grupo de recursos.

Actualmente, Azure admite un máximo de 15 etiquetas por recurso y grupo de recursos.

Las etiquetas se pueden colocar en un recurso en el momento de su creación, o bien se pueden agregar a un recurso existente.

En Azure SQL se recomienda el uso de estas etiquetas que se deben emplear en las máquinas virtuales, grupo de recursos, base de datos.

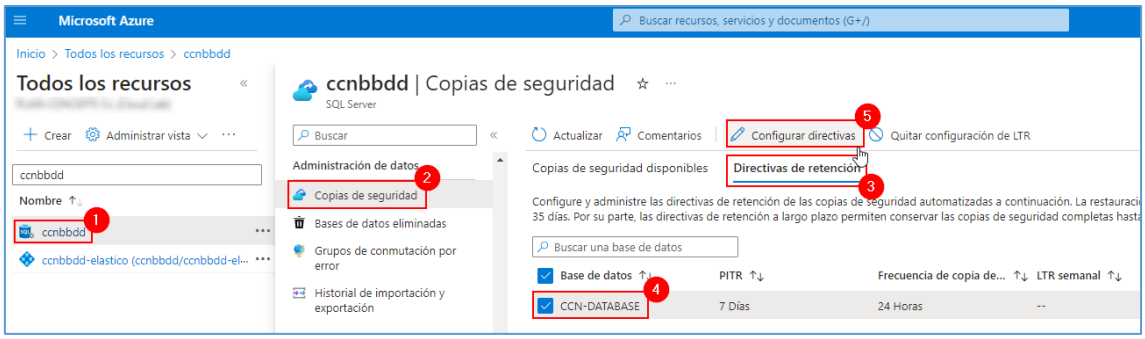
Nota: Para para conocer más el uso de etiquetas y su configuración hay que recurrir al apartado *[3.2.2.1 Protección de la información/Clasificación de la información]* de la guía. *[CCN-STIC-884A - Guía de configuración segura para Azure].*

3.2.2.2 COPIAS DE SEGURIDAD

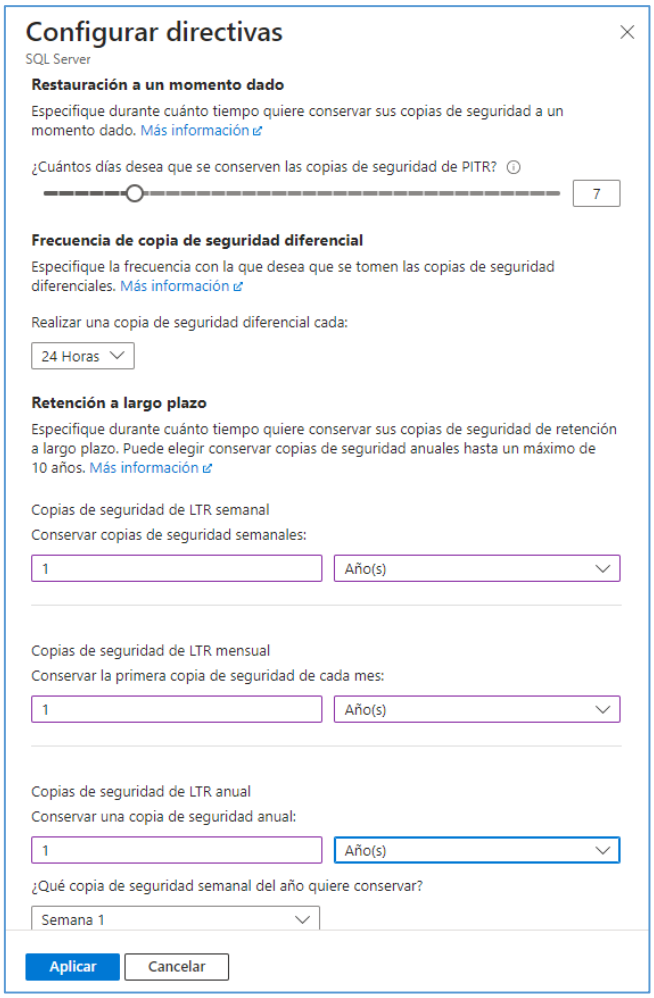
En el caso de las bases de datos de Azure SQL, las copias de seguridad se crean automáticamente. En el apartado de "Copias de seguridad" del servidor SQL se pueden ver las diferentes copias de seguridad que hay disponibles para cada una de las bases de datos del servidor, así como poder administrar las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

A continuación, se describe las instrucciones que debe seguir para configurar la retención en sus bases de datos.

1. Desde el portal de Azure pulsar en [Todos los recursos]
2. Buscar y seleccionar el servidor SQL de la base de datos.
3. Ir al menú del lateral izquierdo y pulsar [Copias de seguridad].
4. Ir al apartado de [Directivas de retención].
5. Seleccionar la base de datos y finalmente pulsar en [Configurar directivas].



Aparecerá un nuevo apartado donde se puede configurar la “Restauración a un momento dado”, la “Frecuencia de copia de seguridad diferencial” y la “Retención a largo plazo”.



- **Restauración a un momento dado:** Se puede seleccionar de 1 a 35 días.
- **Frecuencia de copia de seguridad diferencial:** Cada 12 ó 24 horas.
- **Retención a largo plazo:**
  - Copias de seguridad de LTR semanal: Debe asignar el tiempo que se conserven las copias de seguridad semanales.
  - Copias de seguridad de LTR mensual: Debe asignar el tiempo que se conserven las copias de seguridad mensuales.
  - Copias de seguridad de LTR anual: Debe asignar el tiempo que se conserven las copias de seguridad anuales.

Una vez definida la configuración pulsar en [Aplicar].

Nota: Puede consultar más información en el enlace https://docs.microsoft.com/es-es/azure/sql-database/sql-database-automated-backups

3.3 SCRIPTS DE CONFIGURACIÓN

Se adjunta el script en formato JSON para la creación de un nuevo rol personalizado para los administradores de SQL.

Puede consultar sobre mas roles en los siguientes links.

- https://learn.microsoft.com/es-es/azure/azure-sql/database/logins-create-manage?view=azuresql
- https://learn.microsoft.com/es-es/sql/relational-databases/security/authentication-access/application-roles?view=sql-server-ver15
- https://learn.microsoft.com/es-es/sql/relational-databases/security/authentication-access/database-level-roles?view=sql-server-ver15

4. GLOSARIO DE ABREVIATURAS

A continuación de describen una serie de términos, acrónimos y abreviaturas en materia de seguridad utilizados en esta guía:

Entra ID	*Microsoft Entra ID, anteriormente llamado Azure Active Directory*
RBAC	*"Role Based Access Control", es un sistema de autorización basado en Azure Resource Manager que proporciona administración de acceso específico a los recursos de Azure.*
JSON	*Acrónimo de "JavaScript Object Notation", (notación de objeto de JavaScript) es un formato de texto sencillo para el intercambio de datos.*
ENS	*Esquema Nacional de Seguridad*
MFA	*"Multifactor Authentication" (Autenticación Multifactor). Sistema de seguridad que requiere más de una forma de autenticarse, por ejemplo, a través de una app, sms, etc.*
AKV	*"Azure Key Vault", solución de administración de claves, secretos y certificados en Azure.*
BYOK	*"Bring Your Own Key", término que se utiliza para indicar que la clave es proporcionada por el usuario.*
DEK	*"Data Encryption Key", clave de cifrado de la base de datos.*
Grupo de Recursos	*Contenedor que almacena los recursos relacionados con una solución de Azure. El grupo de recursos incluye los recursos que se desean administrar como grupo.*

Log Analytics	*Azure Log Analytics, anteriormente conocido como Microsoft Monitoring Agent (MMA) o agente Linux de OMS, se desarrolló para lograr una administración completa en las máquinas locales, en los equipos que supervisaba System Center Operations Manager y en las máquinas virtuales de cualquier nube. Los agentes de Windows y Linux se asocian a Azure Monitor y almacenan los datos de registro recopilados de diferentes orígenes en el área de trabajo de Log Analytics.*
Cifrado de datos transparente	*El Cifrado de datos transparente (TDE) cifra los archivos de datos de SQL Server, Base de datos SQL de Azure y Azure Synapse Analytics (SQL DW), lo que se conoce como cifrado de datos en reposo.*

5. CUADRO RESUMEN DE 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 Entra ID (anteriormente llamado Azure Active Directory) 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 y el acceso mediante conexión privada.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		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. Mínimo han de aplicarse los roles Propietario, colaborador, lector y Administrador de acceso de usuario y administradores de bases de datos SQL, siguiendo la referencia de la guía de configuración segura de Azure.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**

<table>
<tr><td>op.acc.5
op.acc.6</td><td colspan="3">Mecanismo de autenticación (usuarios externos y usuarios de la organización)</td></tr>
<tr><td rowspan="2"></td><td rowspan="2">Se ha habilitado Multi-Factor Authentication (MFA) para los usuarios administradores de SQL utilizando una directiva de acceso condicional.</td><td>Aplica:
☐ Si ☐ No</td><td>Cumple:
☐ Si ☐ No</td></tr>
<tr><td>Evidencias Recogidas:
☐ Si ☐ No</td><td>Observaciones:</td></tr>
<tr><td>op.exp</td><td colspan="3">Explotacion</td></tr>
<tr><td>op.exp.8</td><td colspan="3">Registro de la actividad</td></tr>
<tr><td rowspan="2"></td><td rowspan="2">Se ha comprobado que el registro de Auditoría está activado y capturando eventos habilitando una nueva área de trabajo.</td><td>Aplica:
☐ Si ☐ No</td><td>Cumple:
☐ Si ☐ No</td></tr>
<tr><td>Evidencias Recogidas:
☐ Si ☐ No</td><td>Observaciones:</td></tr>
</table>

op.exp.10	**Protección de claves criptográficas**		
	Se ha configurado Key Vault, límitando el acceso tan sólo a usuarios administradores y a la identidad administrada asignada por el sistema del Servidor de la base de datos.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
op.mon	**Monitorizacion de sistema**		
op.mon.1	**Detección de intrusión**		
	Se ha habilitado Microsoft Defender for SQL a nivel de suscripción o a nivel de servidor de base de datos.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**

op.mon.2	**Sistema de métricas**		
	Se ha configurado Azure monitor aplicando los registros populares haciendo referencia a las recomendaciones de Azure SQL Database.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
op.mon.3	**Vigilancia**		
	Se ha habilitado Microsoft Defender for SQL a nivel de suscripción o a nivel de servidor de base de datos.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**

mp	**Medidas de protección**		
mp.com	**Protección de las comunicaciones**		
mp.com.1	**Perímetro seguro**		
	Se ha configurado el acceso a la base de datos mediante punto de conexión privado.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
mp.info	**Protección de la información**		
mp.info.2	**Clasificacion de la informacion**		
	Se han utilizado etiquetas para diferenciar los servicios que compone las bases de datos de SQL, Maquinas virtuales, grupos de recursos.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**

mp.info.6	**Copias de seguridad**		
	Se ha configurado un politica de retencion de copias de seguridad.	**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