centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 884D

Guía de configuración segura para servicios de IA

JUNIO 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

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
2024.07.23 13:09:04 +02'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-24-247-3
Fecha de Edición: junio de 2024

ÍNDICE

1. Guía segura para los servicios de IA de Azure (Azure AI Services)

1.1 Descripción del uso de esta guía

El objetivo del presente anexo es indicar los pasos a seguir necesarios para la utilización de los servicios de **IA de Azure, en adelante "Azure AI Services"**, cumpliendo con los requisitos necesarios del Esquema Nacional de Seguridad en su categoría ALTA.

Esta guía debe usarse en conjunto con la guía de **Configuración segura para Azure** para cubrir las dependencias con otros servicios.

2. Funcionalidades de los servicios de IA de Azure

Los servicios de IA de Azure (Azure AI Services) son los servicios y herramientas de **I**nteligencia **A**rtificial de Azure (IA) que permiten crear rápidamente aplicaciones con cargas de trabajo basadas en modelos de Inteligencia Artificial previamente compilados y listos para usar sin necesidad de inteligencia artificial directa o aptitudes ni conocimientos sobre ciencia de datos.

Los servicios de Azure AI están disponibles a través de **API REST** y pueden ser explotados mediante llamadas a estas APIs o integrándolos en código mediante las diferentes SDK de bibliotecas de clientes en los lenguajes de programación modernos como C#, Java, Python, JavaScript y otros lenguajes de programación populares.

Algunos de los servicios incluidos en *Azure AI Services* son:

- **Azure AI Anomaly Detector:** Identifica posibles problemas en una fase temprana.
- **Azure AI Search:** Agrega funcionalidad de búsqueda basada en IA a aplicaciones web y móviles.
- **Azure OpenAI:** Realiza tareas de procesamiento del lenguaje natural.
- **Azure AI Bot Service:** Crea bots y los conecta a diferentes canales.
- **Azure AI Content Safety:** Detecta contenido no deseado.
- **Azure AI Custom Vision:** Personaliza el reconocimiento de imágenes para adaptarlo a tu empresa.
- **Azure AI Document Intellige:** Convierte documentos en soluciones inteligentes controladas por datos.
- Face: Detecta e identifica personas y emociones en imágenes.
- **Azure AI Immersive Reader:** Ayuda a los usuarios a leer y comprender el texto.
- **Azure AI Language**: Crea aplicaciones con funcionalidades de reconocimiento del lenguaje natural líderes del sector.
- **Azure AI Translator**: Utiliza la traducción asistida por IA para más de 100 lenguas y dialectos.
- Video Indexer: Extrae información útil de videos.
- **Azure AI Vision:** Proporciona capacidades de visión por computadora.
- **Azure AI Speech:** Ofrece capacidades de voz para aplicaciones habilitadas para voz.

- **Azure AI Audio & Video (Video Indexer):** Ofrece características de voz excepcionales para aplicaciones habilitadas para voz, así como la capacidad de extraer información relevante de vídeos almacenados.
- **Azure AI Personalizer:** Permite que las aplicaciones tomen decisiones más inteligentes a gran escala mediante el aprendizaje por refuerzo.
- **Azure AI Metrics Advisor:** Permite supervisar datos de series temporales y detectar anomalías.

3. Despliegue de los servicios de IA de Azure

3.1 Introducción

Los servicios de Azure AI pueden ser creados y explotados mediante dos tipos de recursos distintos:

- Recurso de varios servicios de IA: Permite acceder a varias instancias de servicios de Azure AI con una sola clave y un punto de conexión. Consolida la facturación de los servicios que usa.
- Recurso de servicio único de IA: Permite acceder a un servicio concreto de Azure AI con una clave y un punto de conexión únicos para ese servicio.

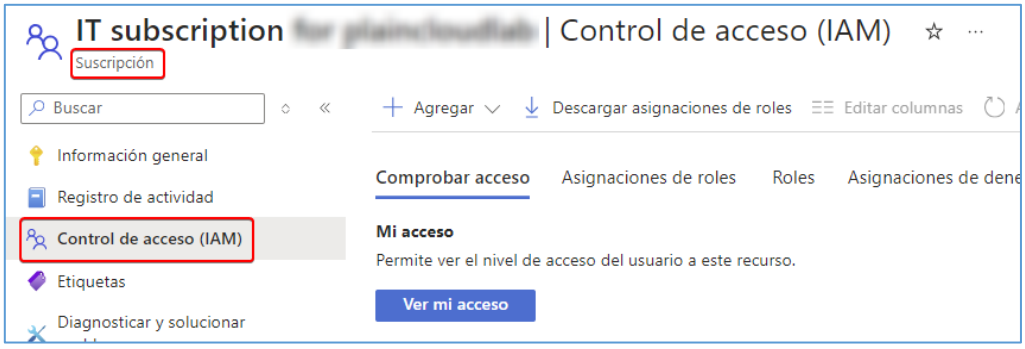
Nota: Con el objetivo de facilitar la lectura de esta guía y debido a la gran cantidad de servicios de Azure AI disponibles y teniendo en cuenta que las normas incluidas en este documento afectan a todos los servicios por igual, hemos seleccionado para los ejemplos de configuración el servicio de *Azure OpenAI* y el *Recurso de Varios Servicios de IA*.

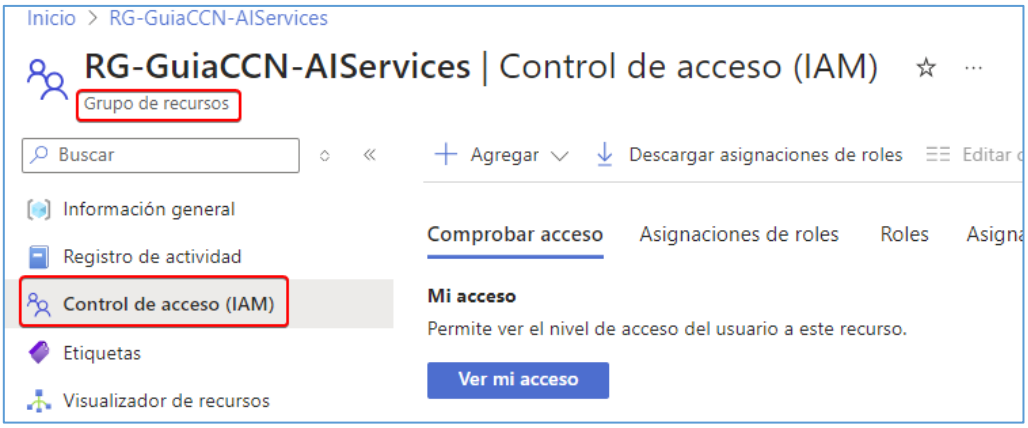
3.2 Requisitos previos

3.2.1 Permisos

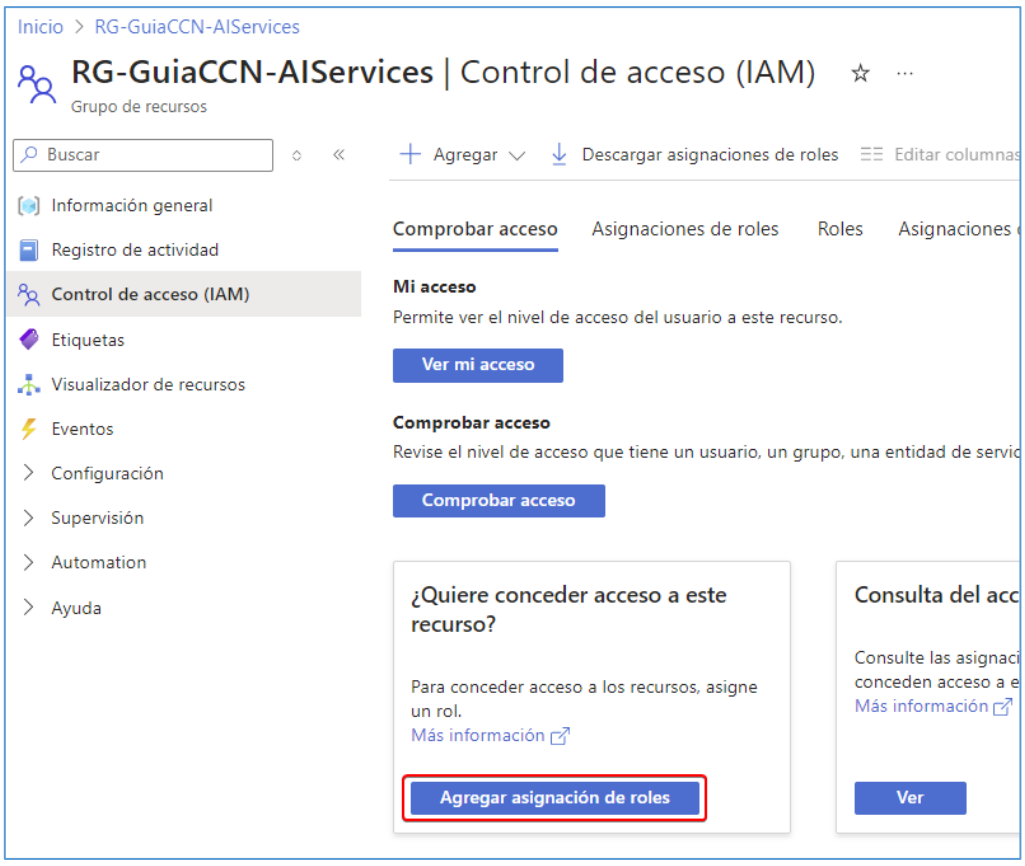
Para poder desplegar los servicios de IA, es necesario tener el permiso de "Colaborador" sobre el grupo de recurso o subscripción donde se va a desplegar él recurso y además tener el permiso de "Colaborador de Cognitive Services".
Para ello:

1. Sobre la subscripción o el grupo de recursos, pulsamos sobre "Acceso control IAM"

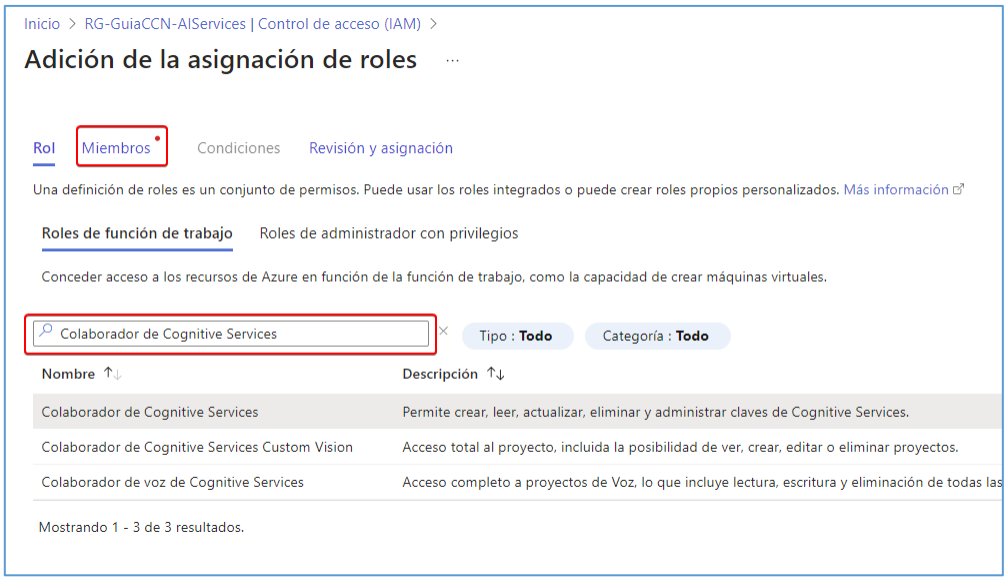




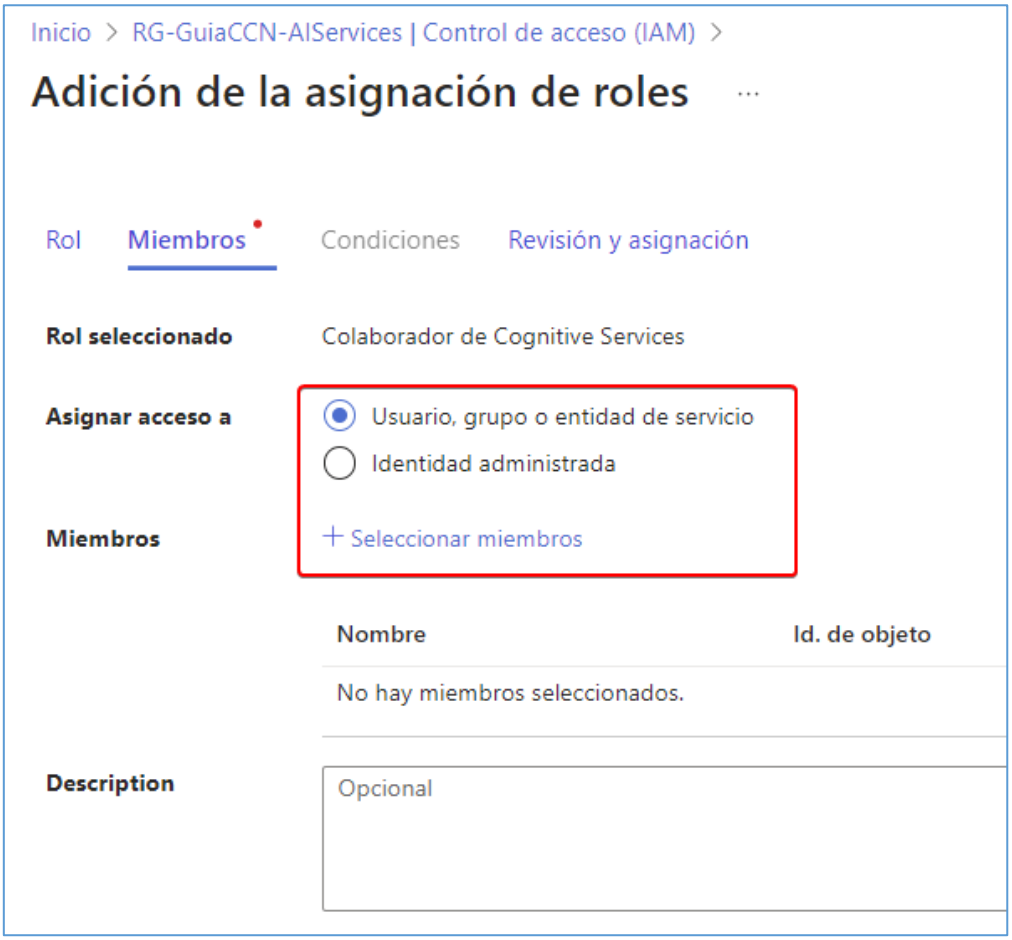
2. Pulsaremos sobre “Agregar asignación de roles”



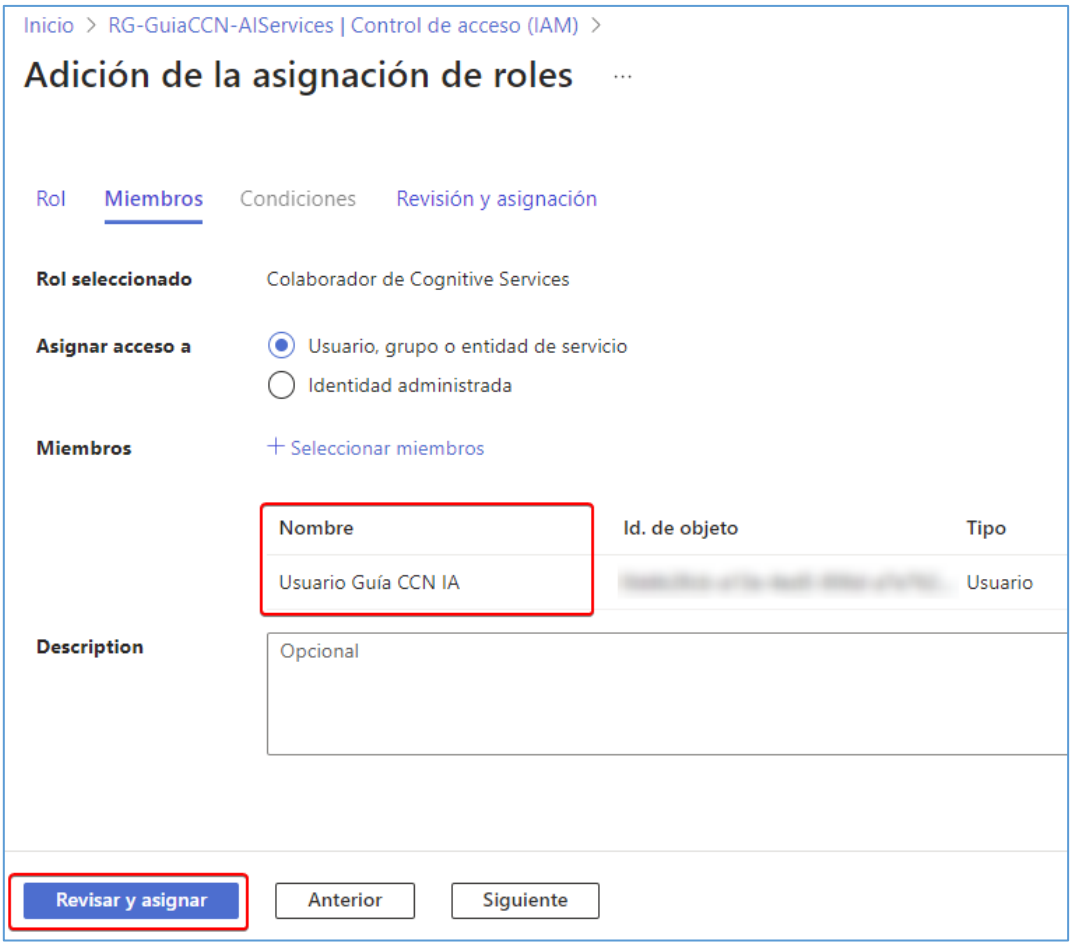
3. Buscamos y seleccionamos el rol y pulsamos sobre “Miembros” o “Siguiente”



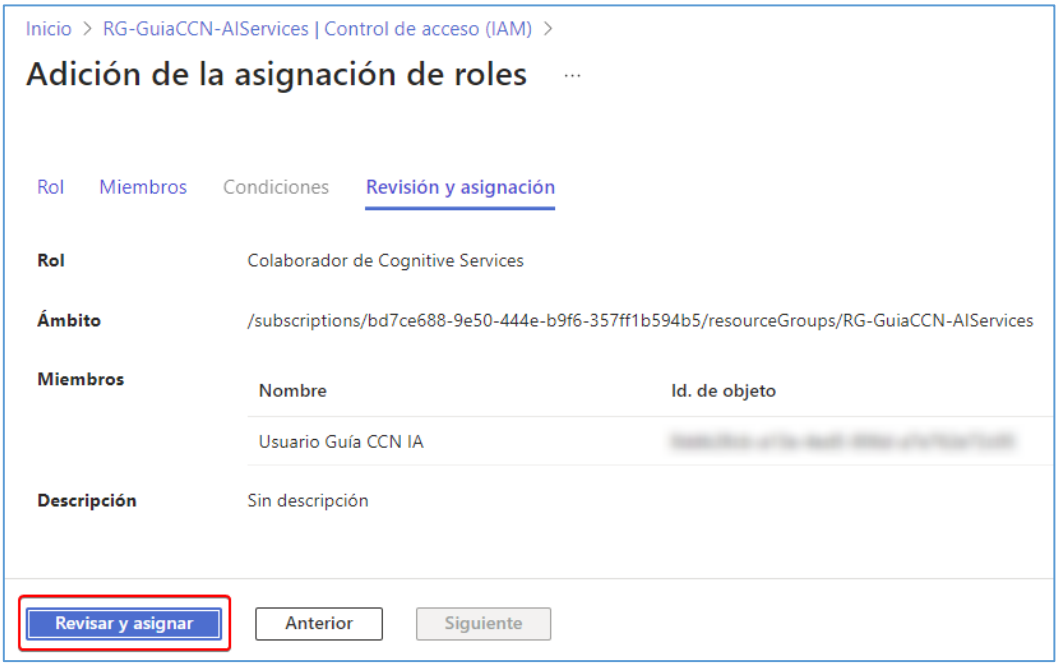
4. Seleccionamos Usuario, grupo, entidad de servicio o Identidad administrada y Seleccionar Miembros



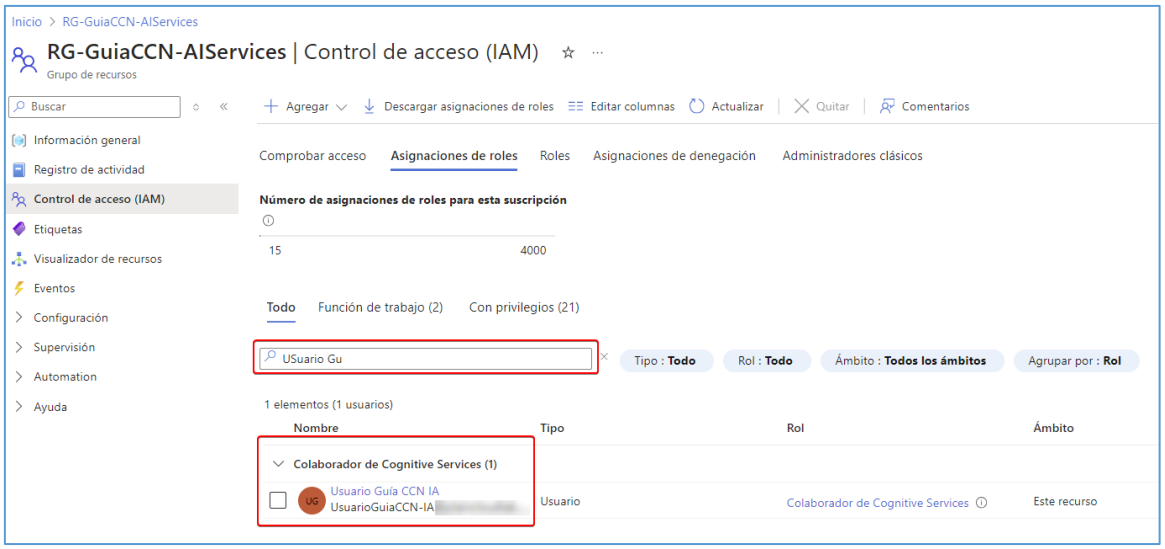
5. Una vez seleccionado comprobar que se ha incluido correctamente y pulsar sobre “Revisar y asignar”



6. Volvemos a verificar que la asignación es correcta y pulsamos sobre “Revisar y asignar”



7. Verificar en “Asignación de Roles” la correcta asignación del permiso



3.2.2 Herramientas

Azure AI Services se puede desplegar desde el ***portal de Azure*** o desde línea de comandos con ***Azure CLI* o *Azure Powershell***, también es compatible con varias herramientas de *Infraestructura como Código (**IaC**)*. Ambas herramientas pueden ser desplegadas en los sistemas operativos Linux, Windows y macOS. Se puede encontrar información detallada para su instalación en los siguientes enlaces:

- Azure Command-Line Interface (CLI)
- Azure Powershell

Para este documento usaremos Azure Powershell. Para una introducción al uso de Azure Powershell revisar el punto 2 de la guía de **Configuración segura para Azure.**

Nota: Los procedimientos incluidos en esta guía no tienen en cuenta el proceso de Inicio de Sesión ni la creación del grupo de recursos. Para información de las opciones de inicio de sesión y la creación de un grupo de recursos consultar el punto 2 de la guía de configuración segura para Azure.

Para los ejemplos incluidos en esta guía se utilizará un grupo de recursos llamado:

RG-GuiaCCN-AIServices y la región **Europa del Oeste (West Europe)** por defecto.

Para los despliegues de red se ha creado una red virtual **vnet-guiasccn-weu** con dos subredes: **ai-multiservicios-snet y ai-openai-snet** .

3.3 Recurso de Varios Servicios de IA

Un ***Recurso de Varios Servicios de IA*** permite acceder a varios recursos de IA creando un solo recurso y por lo tanto utilizando un único punto de acceso, una única llave de seguridad (Key) o con un rol RBAC común a todos los recursos y agrupando el coste en este único recurso.

Un Recurso de Varios Servicios permite el acceso a uno de los siguientes subrecursos de IA:

- Decisión:
  - Azure AI Content Safety (Reemplaza a Content Moderator)
- Lenguaje:
  - Azure AI Language
  - Azure AI Translator
- Voz:
  - Azure AI Speech
- Visión:
  - Azure AI Custom Vision
  - Azure AI Face
  - Azure AI Computer Vision
- Document Intelligence:
  - Azure AI Document Intelligence

  Metrics Advisor:
  - Azure AI Metrics Advisor

Un Recurso de Varios Servicios se puede desplegar usando Azure CLI, Azure Powershell, el portal de Azure o con la utilización de los siguientes lenguajes de programación: C#, Java, JavaScript y Python.

En esta guía se incluyen instrucciones de despliegue para Azure Powershell y portal de Azure. Ver https://learn.microsoft.com/en-us/azure/ai-services/multi-service-resource para ver como desplegar este recurso usando uno de los lenguajes de programación soportados.

3.3.1 Despliegue con Azure Powershell

Nota: El siguiente procedimiento de despliegue no tiene en cuenta el proceso de Inicio de Sesión ni la creación del grupo de recursos. Para información de las opciones de inicio de sesión y la creación de un grupo de recursos consultar el punto 2 de la guía de configuración segura para Azure.

Para poder desplegar el recurso de varios servicios de IA mediante Powershell se deben seguir los siguientes pasos:

Seleccionar la suscripción donde se encuentre el grupo de recursos donde se va a desplegar el servicio:

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

Ejecutar el siguiente comando de Powershell para crear un recurso de varios servicios de IA especificando:

a. **Grupo de recursos**: Se especificará con la opción “-ResourceGroupName” el grupo de recursos donde se desplegará el servicio. En el ejemplo se ha considerado “RG-GuiaCCN-AIServices”.

b. **Nombre del recurso**: Se especificará con la opción "-Name" el nombre que se quiera dar al recurso. En el ejemplo se ha considerado "CCN-Multi-Service-Account".

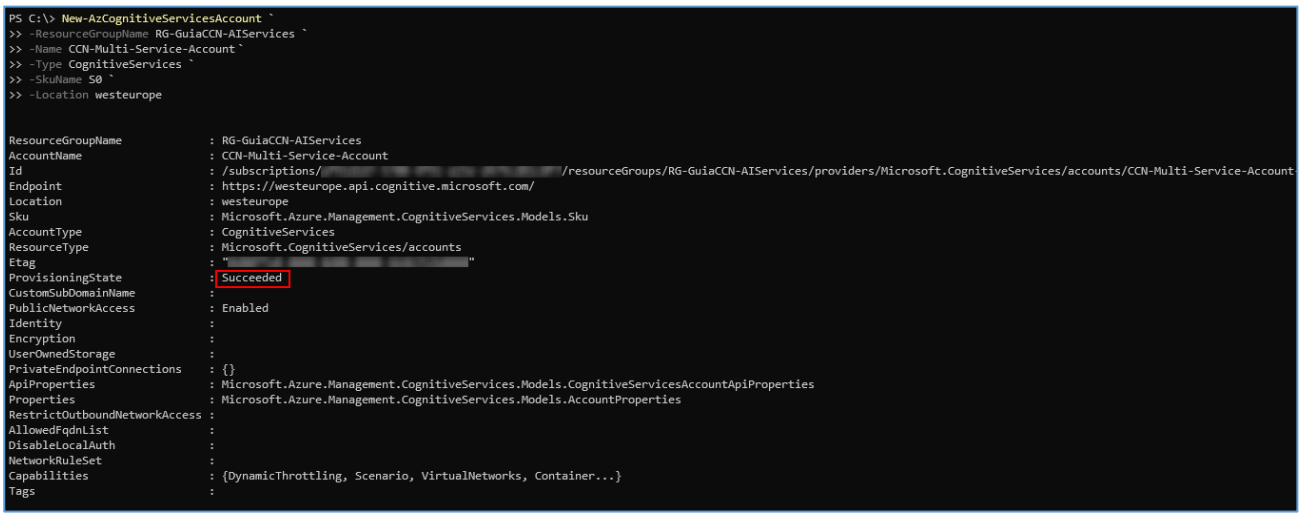
c. **Tipo de servicio**: Para el recurso de varios servicios de IA se tendrá que especificar con la opción "-Type CognitiveServices".

d. **Plan de tarifa**: Se especificará con la opción "-SkuName S0" para la creación del recurso con la tarifa "Standard S0".

e. **Región**: Se especificará con la opción "-Location" la región donde se quiera desplegar el recurso, en este caso "West Europe".

```
#  PS C:\> New-AzCognitiveServicesAccount `
     -ResourceGroupName RG-GuiaCCN-AIServices `
     -Name CCN-Multi-Service-Account `
     -Type CognitiveServices `
     -SkuName S0 `
     -Location westeurope
```

Una vez ejecutado el comando de Powershell, la consola mostrará una salida como la que se muestra a continuación indicando que el despliegue se ha realizado correctamente ("ProvisioningState: Succeeded"):

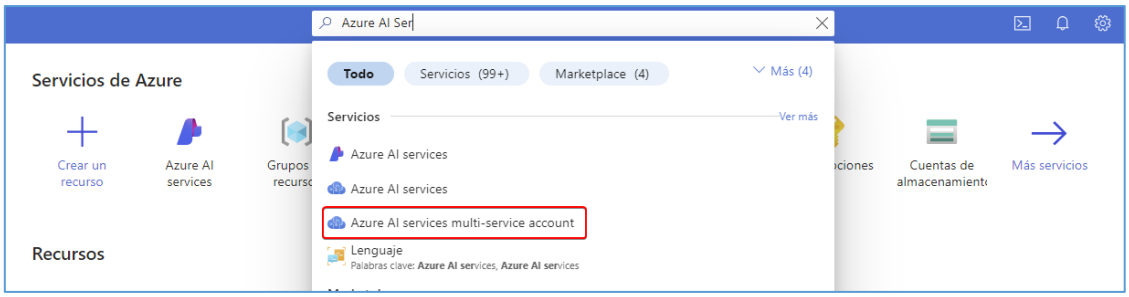


3.3.2 Despliegue con el portal de Azure

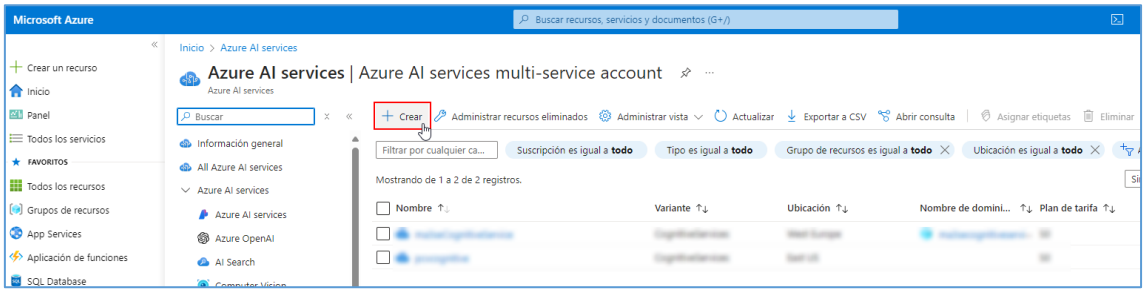
Nota: El siguiente procedimiento de despliegue no tiene en cuenta el proceso de Inicio de Sesión ni la creación del grupo de recursos. Para información de las opciones de inicio de sesión y la creación de un grupo de recursos consultar el punto 2 de la guía de configuración segura para Azure.

Para poder desplegar el recurso de varios servicios de IA desde el portal de Azure se deben seguir los siguientes pasos:

1. En la barra de búsqueda central del portal de Azure, buscar “Azure AI services” y seleccionaremos “Azure AI services multi-service account”



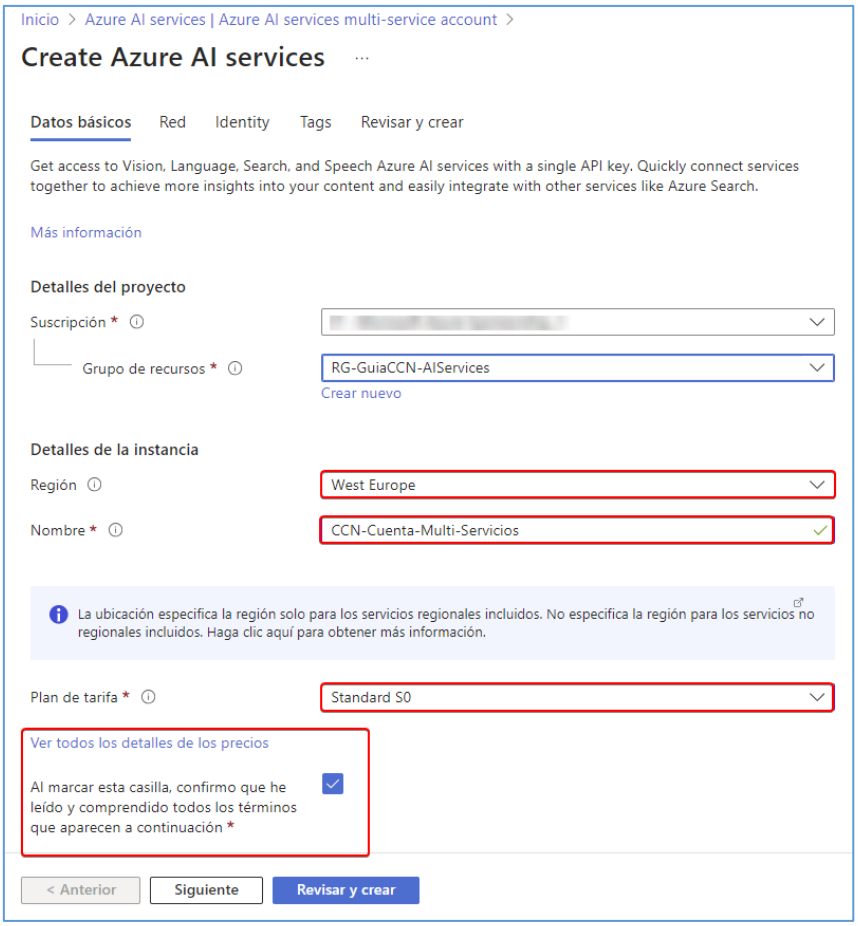
Posteriormente pulsar en “Crear”.



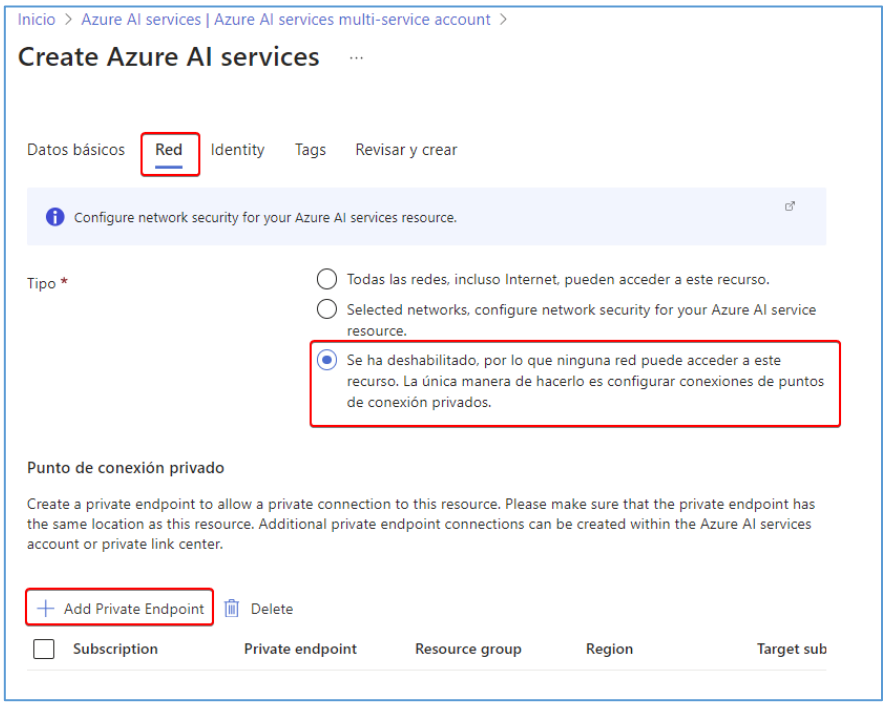
Rellenar los campos del asistente de configuración y pulsar en “Revisar y Crear”.

a. **Suscripción**: Por defecto aparecerá la suscripción que se esté empleando.
b. **Grupo de recursos**: Seleccionar el grupo de recursos donde se vaya a desplegar el servicio.
c. **Región**: Seleccionar la región donde ser desplegará el servicio.
d. **Nombre**: Introducir el nombre que se quiera dar al recurso.
e. **Plan de tarifa**: Seleccionar el plan de tarifa, en este caso “Standard S0”.
f. **Marcar la casilla** de los términos de uso

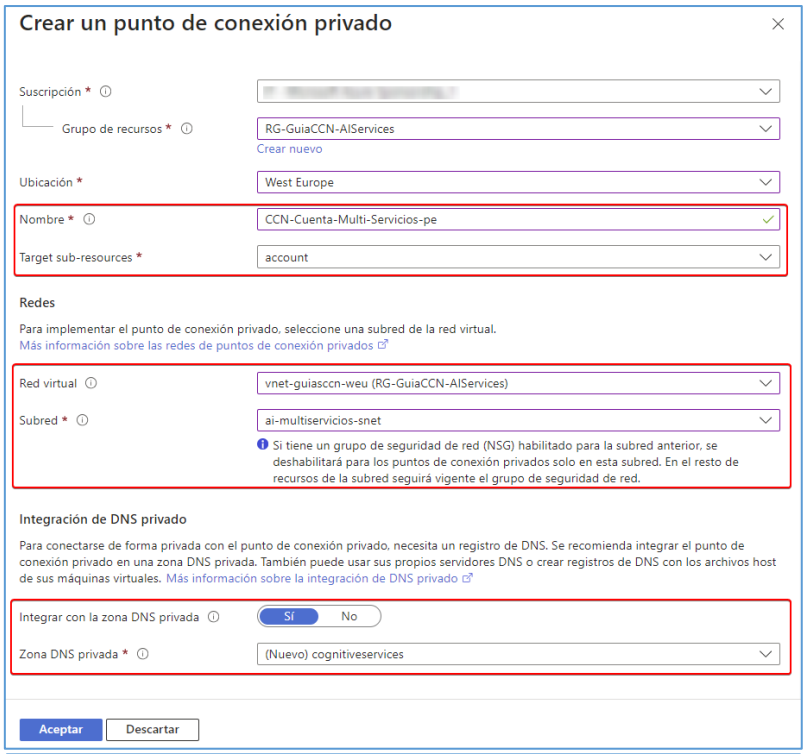
Nota: Para poder marcar la casilla será necesario que el usuario tenga permisos de “Colaborador de Cognitive Services” en la suscripción / grupo de recursos actual y que la asignación de denegación no esté establecida para registrar una característica. *[Ver 3.2.1 Permisos]*.

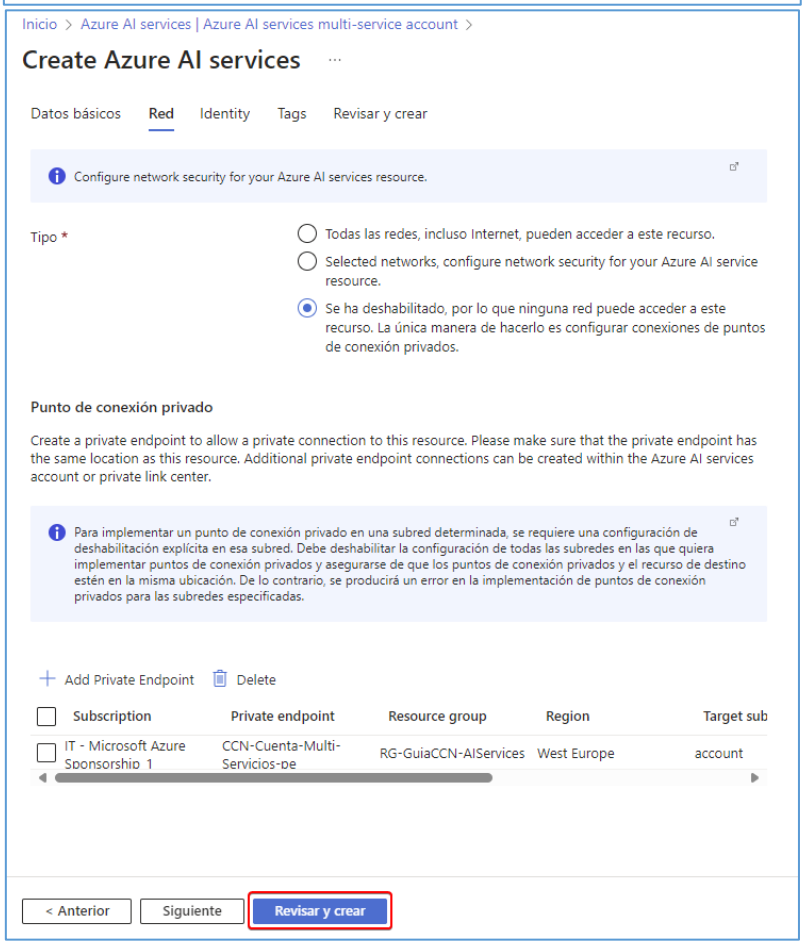


En la pestaña “Red” deshabilitaremos la conexión pública y añadiremos un “Punto de conexión privado” ya que uno de los requisitos es que nuestra infraestructura de IA debe estar privada:



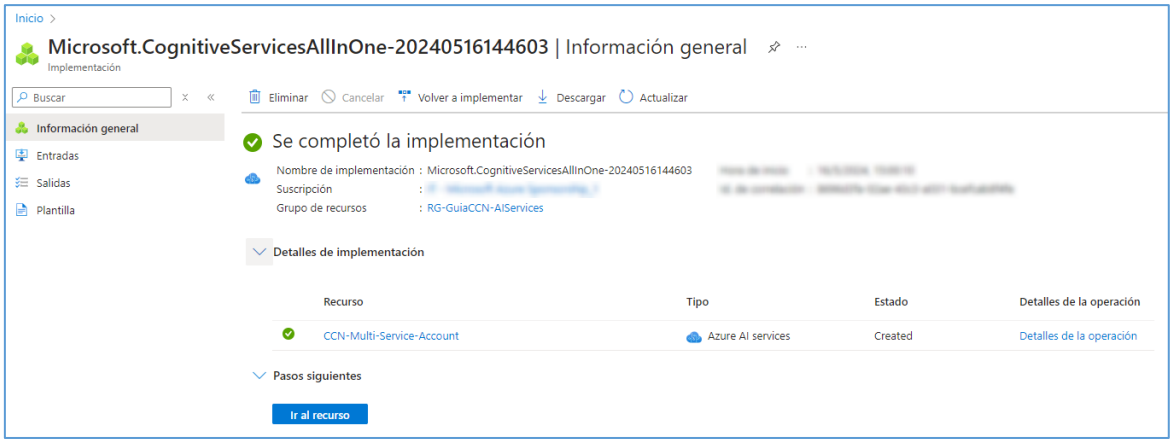
Al pulsar sobre “Add Private Endpoint” se nos abrirá la ventana de configuración del “Punto de Conexión Privado”





La configuración de la zona privada DNS es fundamental para el correcto funcionamiento de la infraestructura y se puede adaptar en función de la topología de red.

El proceso de creación puede tardar unos minutos. Finalmente aparecerá un resumen de la implementación del servicio tal y como se muestra a continuación:



3.4 Recurso de servicio único de IA (OpenAI)

3.4.1 Despliegue con Azure Powershell

Nota: El siguiente procedimiento de despliegue no tiene en cuenta el proceso de Inicio de Sesión ni la creación del grupo de recursos. Para información de las opciones de inicio de sesión y la creación de un grupo de recursos consultar el punto 2 de la guía de configuración segura para Azure.

Para poder desplegar el recurso de OpenAI mediante Powershell se deben seguir los siguientes pasos:

1. Seleccionar la suscripción donde se encuentre el grupo de recursos donde se va a desplegar el servicio:

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

Ejecutar el siguiente comando de Powershell para crear el recurso de OpenAI especificando:

a) Grupo de recursos: Se especificará con la opción “-ResourceGroupName” el grupo de recursos donde se desplegará el servicio. En el ejemplo se ha considerado “RG-GuiaCCN-AIServices”.

b) Nombre del recurso: Se especificará con la opción “-Name” el nombre que se quiera dar al recurso. En el ejemplo se ha considerado “CCN-OpenAI”.

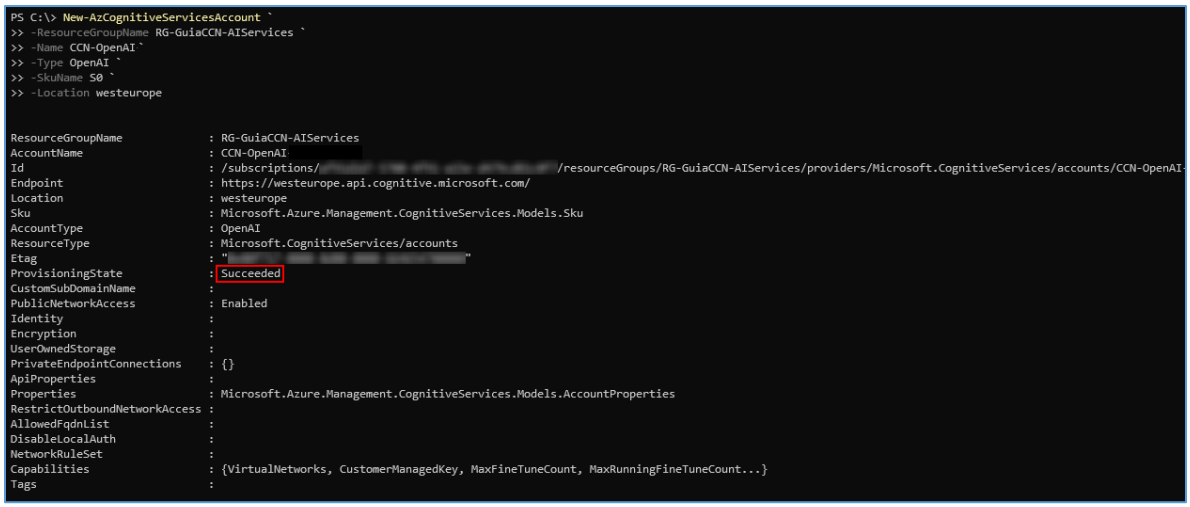
c) Tipo de servicio: Para el recurso de OpenAI se tendrá que especificar con la opción “-Type OpenAI”.

d) Plan de tarifa: Se especificará con la opción “-SkuName S0” para la creación del recurso con la tarifa “Standard S0”.

e) Región: Se especificará con la opción “-Location” la región donde se quiera desplegar el recurso, en este caso “West Europe”.

```
#  PS C:\> New-AzCognitiveServicesAccount `
     -ResourceGroupName RG-GuiaCCN-AIServices `
     -Name CCN-OpenAI `
     -Type OpenAI `
     -SkuName S0 `
     -Location westeurope
```

Una vez ejecutado el comando de Powershell, la consola mostrará una salida como la que se muestra a continuación indicando que el despliegue se ha realizado correctamente (“ProvisioningState: Succeeded”):



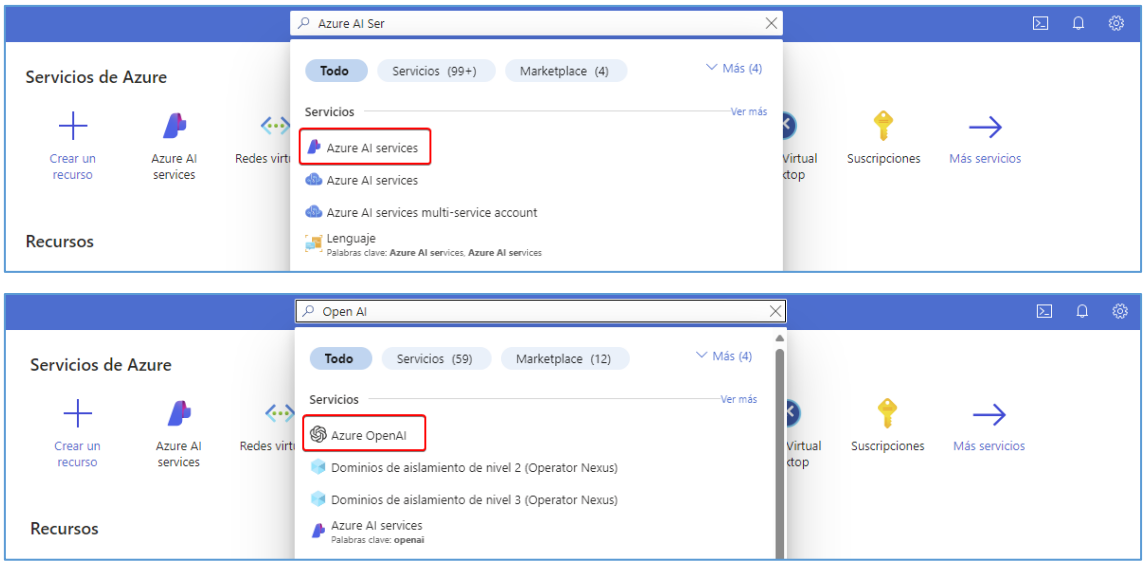
Nota: Para ver el listado de los diferentes tipos de recursos de servicios de IA que se pueden desplegar mediante Powershell se puede consultar la tabla del siguiente enlace: https://learn.microsoft.com/es-es/azure/ai-services/multi-service-resource?tabs=windows&pivots=azpowershell#create-an-azure-ai-services-resource

3.4.2 Despliegue con el portal de Azure

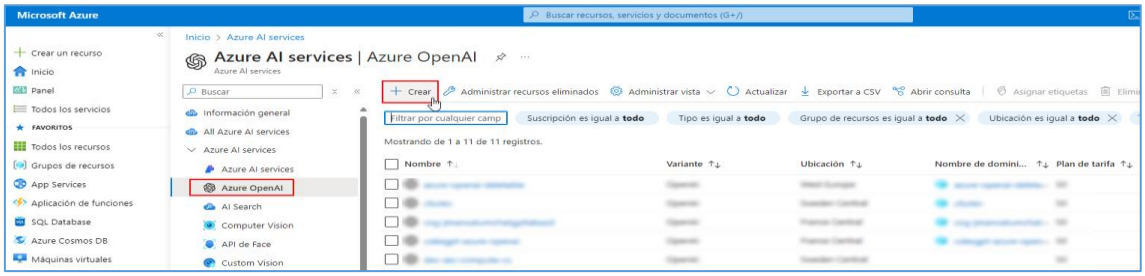
Nota: El siguiente procedimiento de despliegue no tiene en cuenta el proceso de Inicio de Sesión ni la creación del grupo de recursos. Para información de las opciones de inicio de sesión y la creación de un grupo de recursos consultar el punto 2 de la guía de configuración segura para Azure.

Para poder desplegar el recurso de OpenAI desde el portal de Azure se deben seguir los siguientes pasos:

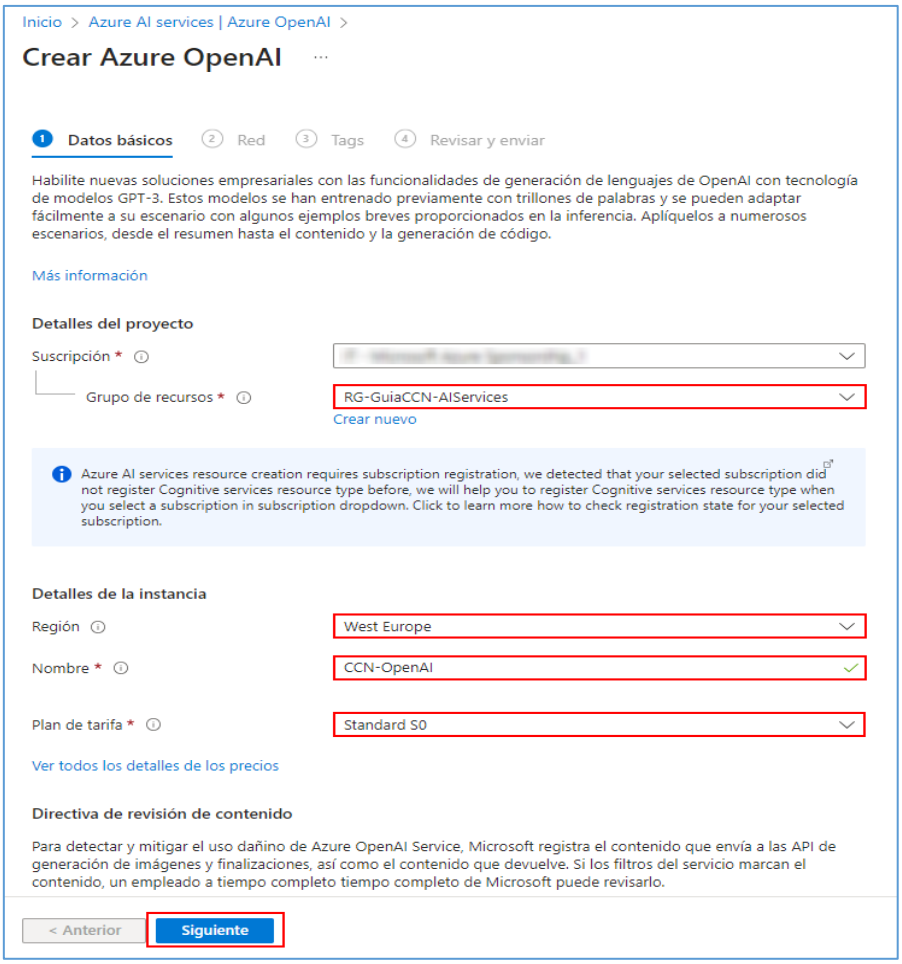
1. En la barra de búsqueda central del portal de Azure, buscar “azure ai services” u “Open AI”.



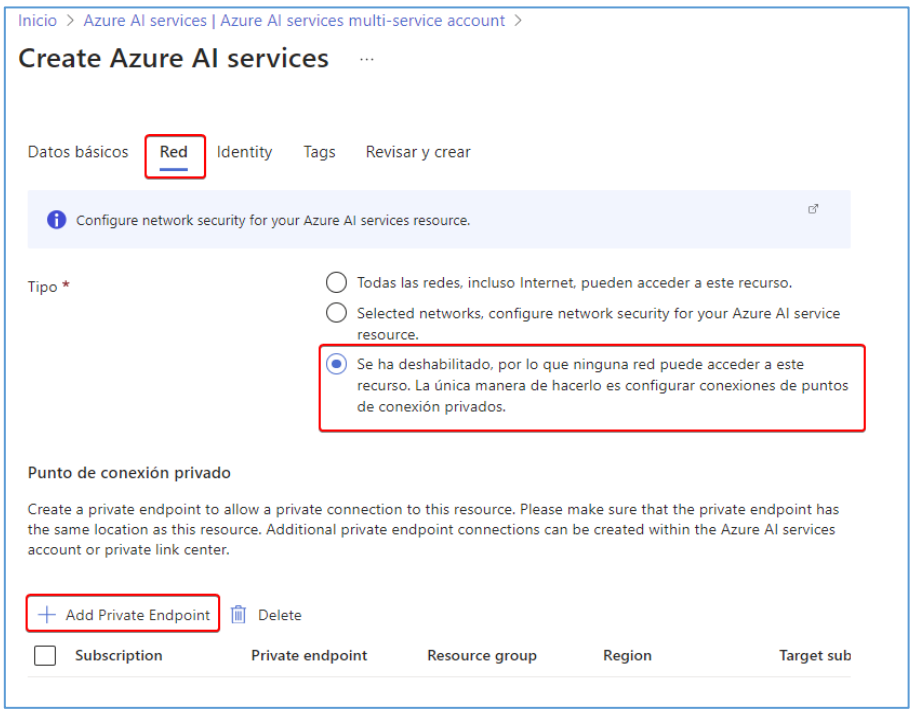
2. En el menú lateral izquierdo, pulsar sobre el apartado de “Azure OpenAI” y posteriormente pulsar en “Crear”.



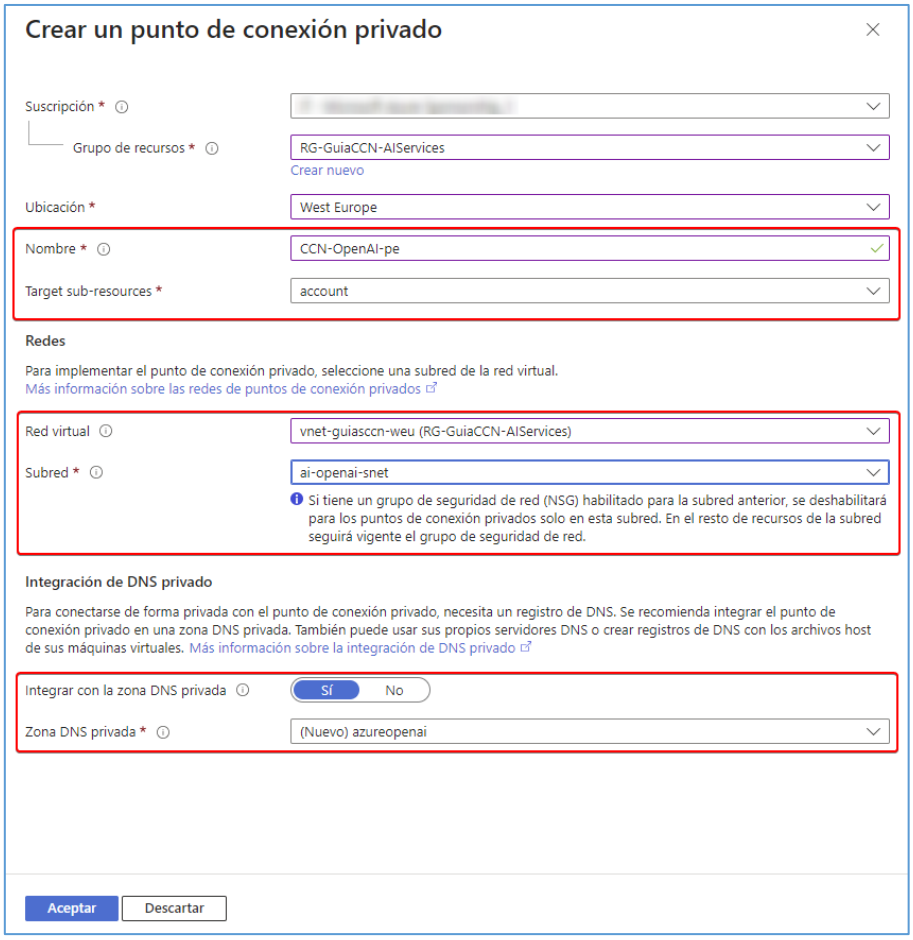
3. Rellenar los campos del asistente de configuración y pulsar en “Siguiente”.
    a. **Suscripción**: Por defecto aparecerá la suscripción que se esté empleando.
    b. **Grupo de recursos**: Seleccionar el grupo de recursos donde se vaya a desplegar el servicio.
    c. **Región**: Seleccionar la región donde ser desplegará el servicio.
    d. **Nombre**: Introducir el nombre que se quiera dar al recurso.
    e. **Plan de tarifa**: Seleccionar el plan de tarifa, en este caso “Standard S0”.



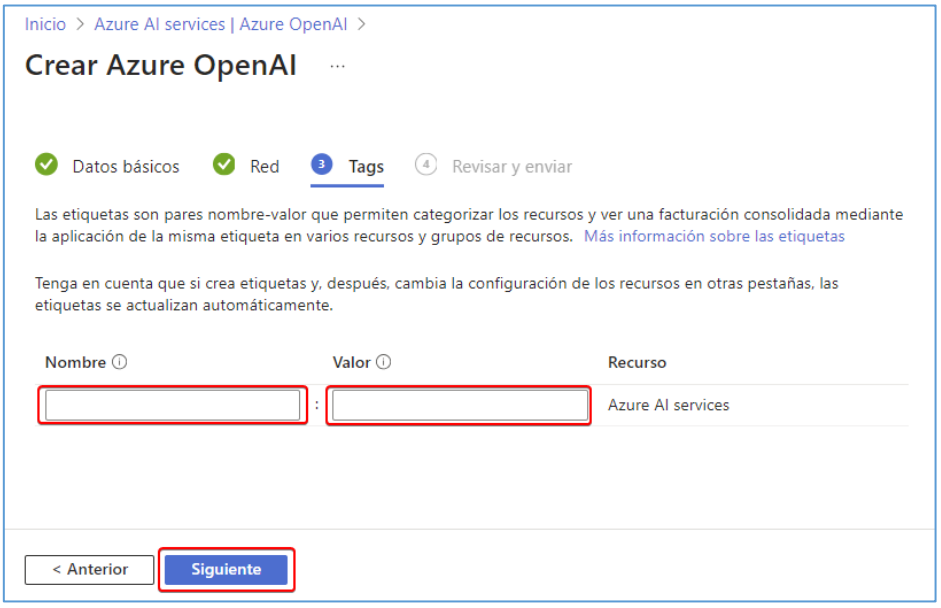
4. En la pestaña “Red” añadiremos un deshabilitaremos la conexión pública y añadiremos un “Punto de conexión privado”:



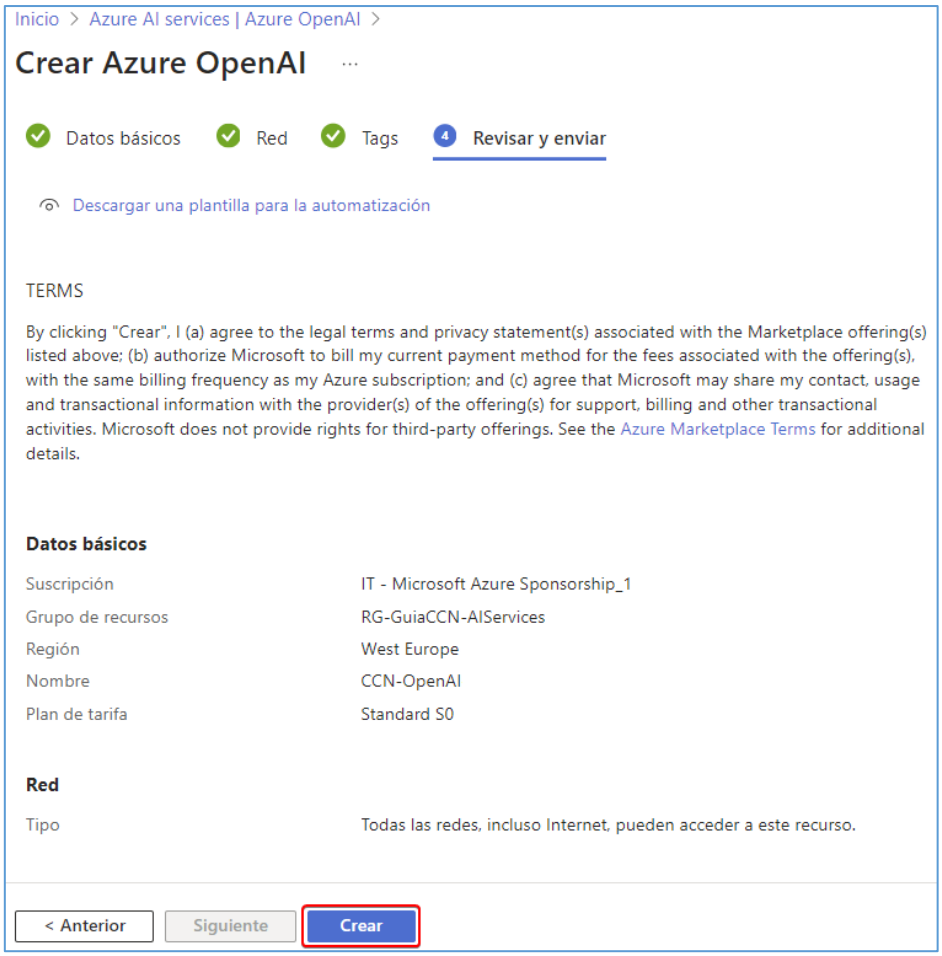
Al pulsar sobre “Add Private Endpoint” se abrirá la ventana de configuración:



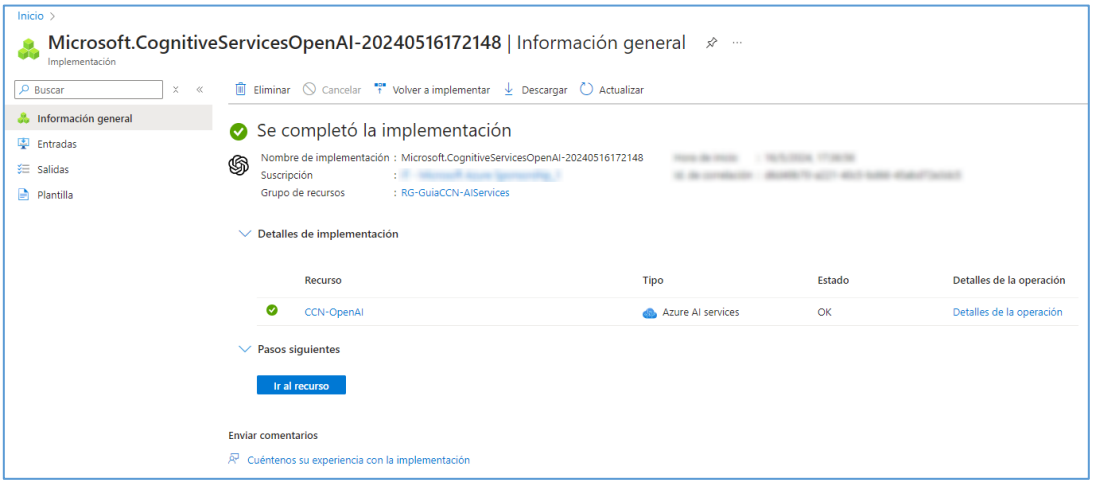
5. En el apartado de “Tags”, introducir las etiquetas que se quieran asociar al recurso y pulsar en “Siguiente”.



6. Finalmente, en el apartado de “Revisar y enviar” se puede revisar la configuración establecida y para desplegar el recurso pulsar en “Crear”.

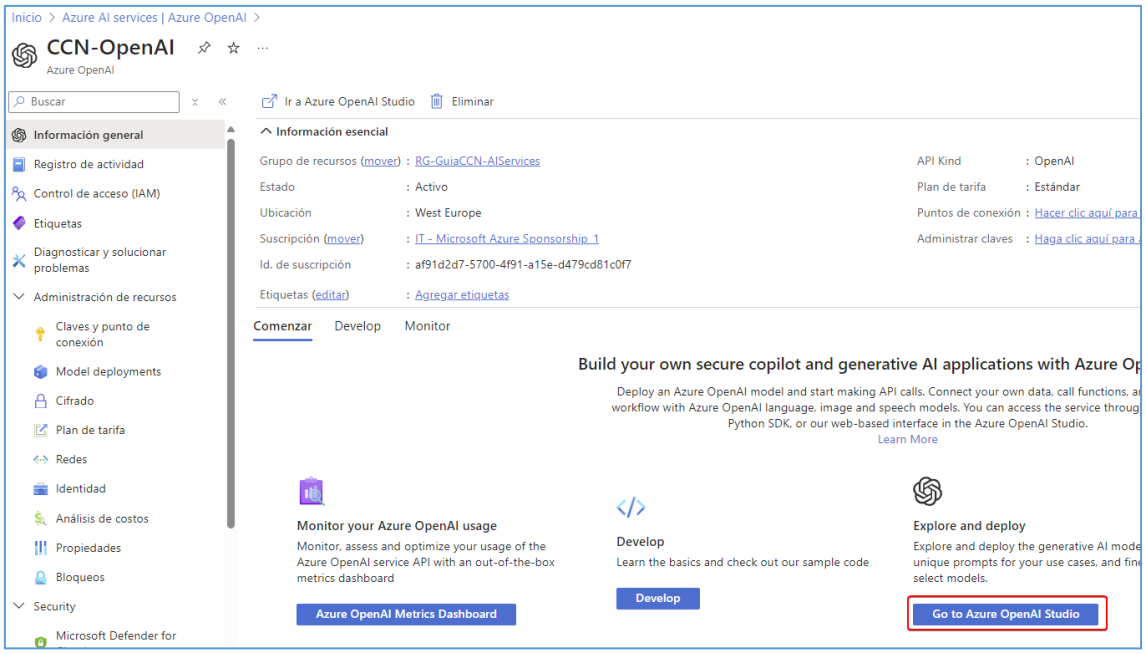


El proceso de creación puede tardar unos minutos. Finalmente aparecerá un resumen de la implementación del servicio tal y como se muestra a continuación:

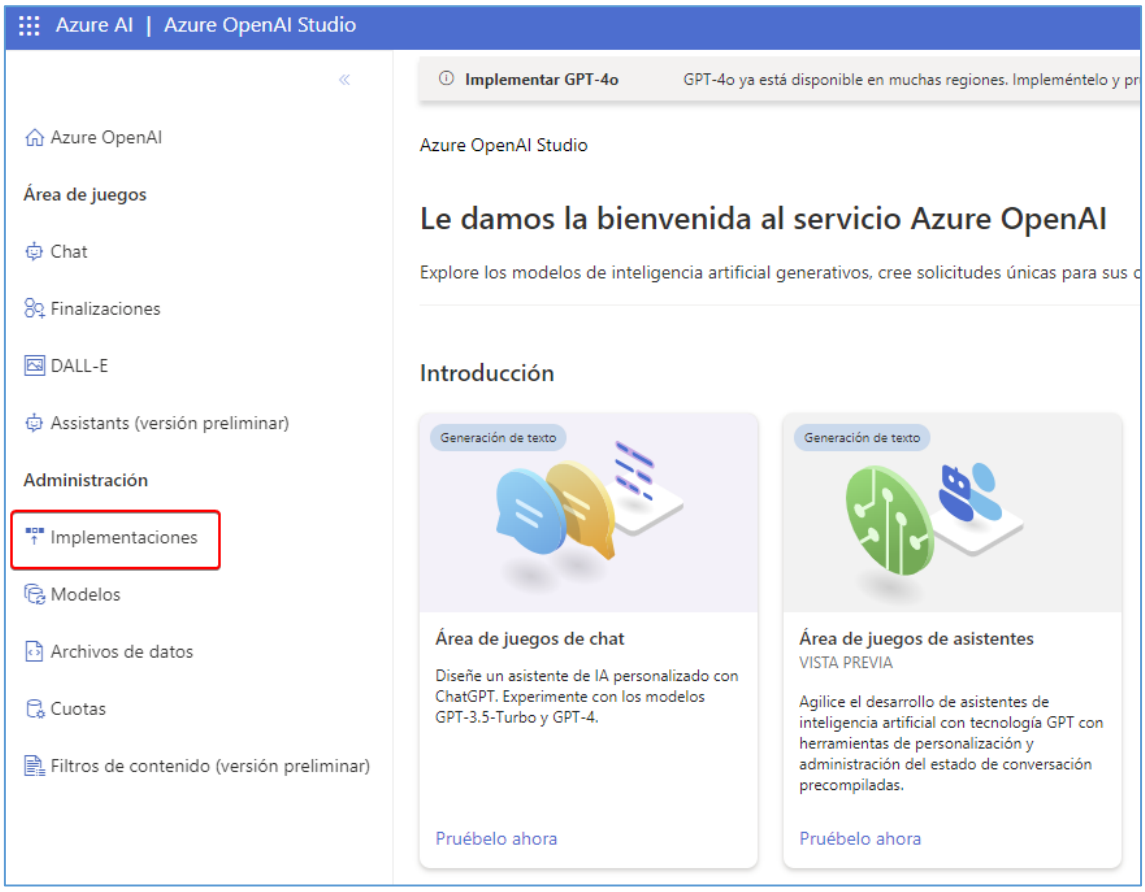


Una vez desplegado el servicio de OpenAI, hay que crear un deployment. Para ello:

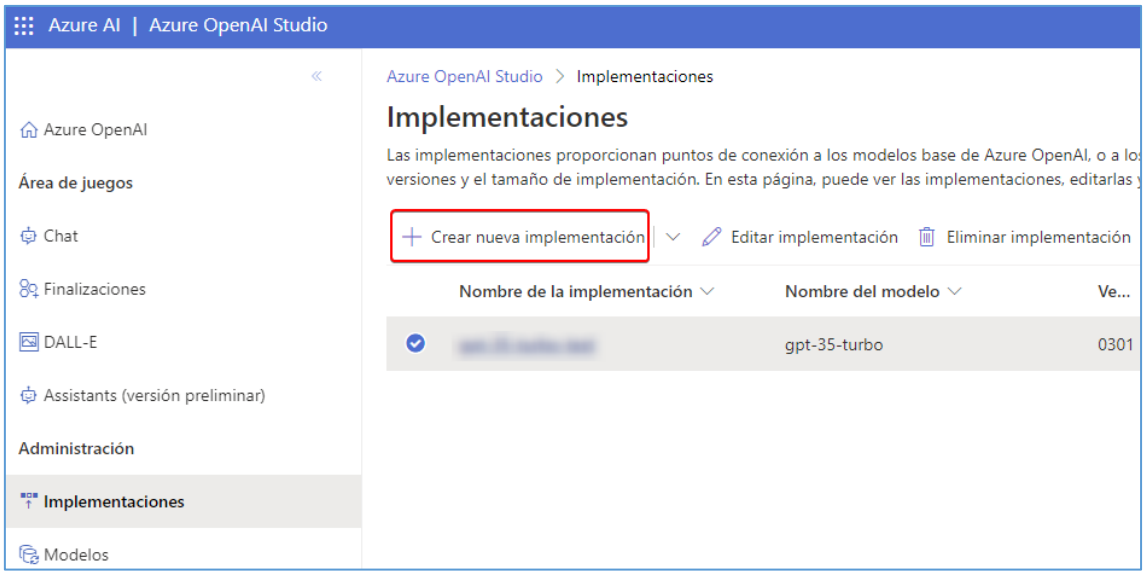
1. Abrir AI Studio: Desde el navegador https://oai.azure.com/ o desde el portal de Azure



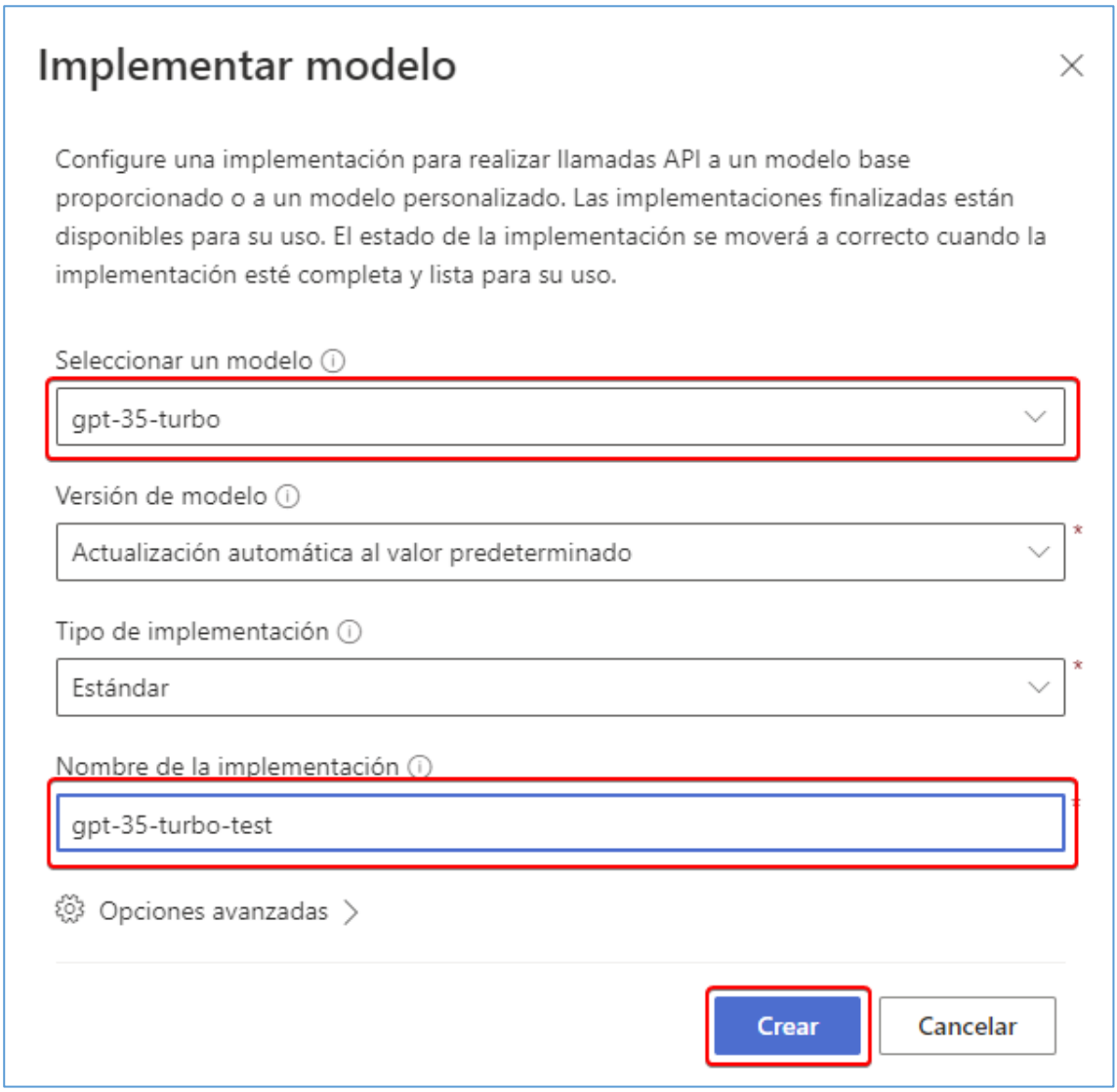
2. Ir a Implementaciones



3. Pulsar en “Crear nueva implementación”



4. Seleccionaremos el modelo, asignaremos un nombre de implementación y pulsaremos en crear.



4. Configuración segura para los servicios IA de Azure

4.1 Marco Operacional

4.1.1 Control de Acceso

4.1.1.1 Identificación

Las integraciones con los servicios de AI se realizan mediante llamadas API Rest. Existen varios métodos de autenticación, pero se recomienda utilizar **Microsoft Entra ID**.

A continuación, se detallan los métodos de autenticación que podrá emplear.

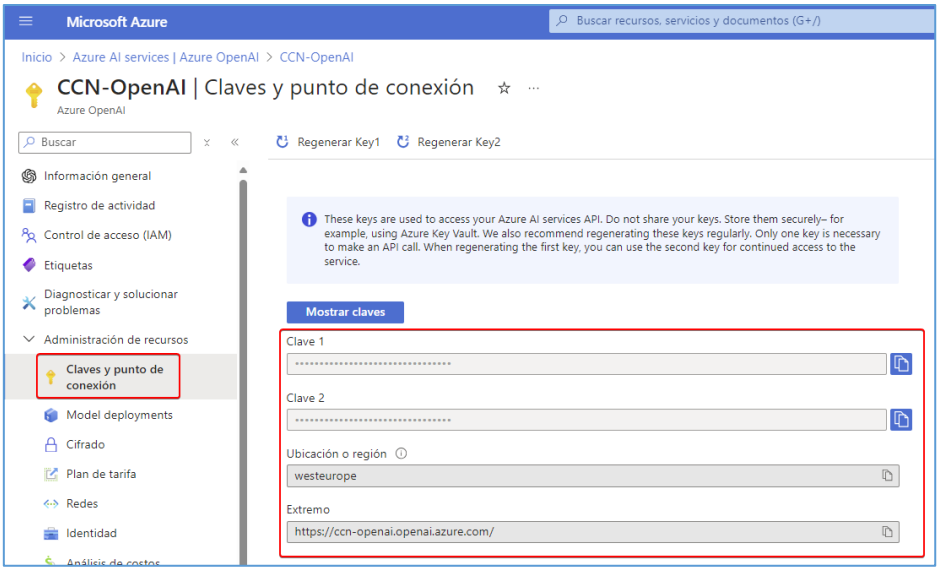
- Autenticación con una clave de recurso (API Key): Este método utiliza una clave (API Key) a modo de llave que permite conectar con los servicios de IA.
- Autenticación con Entra ID: Asigna Roles RBAC a un recurso de IA por lo que requiere autenticación previa. Puede ser utilizado por una entidad de aplicación o una Identidad Administrada entre otros modos.

Existe un tercer método "Autenticación con token" por el cual utilizando el API Key generamos un token que es enviado al recurso para la autenticación. Este método está siendo deprecado por Azure y por lo tanto no se recomienda su utilización. En algunos recursos de IA ya no es posible utilizarlos. Se comenta en la guía de su existencia a modo de información.

Nota: Se recomienda consultar este link: https://docs.microsoft.com/es-es/azure/cognitive-services/authentication

4.1.1.1.1 Identificación con API Key

Para identificarnos mediante API Key, primero obtendremos la clave en el mismo recurso de Azure, sección "Claves":



Nota: Las claves no deberán, bajo ningún concepto ser guardadas en código de la aplicación o en un almacén que no esté encriptado. Se recomienda el uso de Azure Key Vault. Consultar

[3.1.2.2 Protección de claves criptográficas] de la guía *[CCN-STIC-884A - Guía de configuración segura para Azure]*.

```
#  El siguiente código es un ejemplo de llamada con Powershell y API Key:
#  $apiKey = "54d36b53beb144268d1745d12964ea12"
#  $header = @{"api-key"  = $apiKey }
#  $deploymentName = "gpt-35-turbo-test"
#  $maxTokens = 100
#  $prompt = "What is PowerShell?"
#  $APIVersion = "2024-02-01"
#  $uri = "https://ccn-
   openai.openai.azure.com/openai/deployments/$deploymentName/completions?api
   -version=$APIVersion"
#  $body = @"
#  {
#  "prompt": "$prompt",
#  "max_tokens": $maxTokens
#  }"@
#  Invoke-RestMethod -Method POST `
#  -Uri $uri `
#  -ContentType "application/json" `
#  -Body $body  `
#  -Headers $header
```

Este script ha devuelto la siguiente respuesta:

```
PS C:\traslateapitest> Invoke-RestMethod -Method POST -Uri $uri -ContentType "application/json" -Body $body  -Headers $header

id                     : cmpl-9ZdInS9RAI7OhbhV30PuYeqjqzXl3
object                 : text_completion
created                : 1718279585
model                  : gpt-35-turbo
prompt_filter_results  : {@{prompt_index=0; content_filter_results=}}
choices                : {@{text= PowerShell is an interactive command-line shell, designed specifically for Microsoft Windows, that allows users to implement
e tasks, manage system devices, and
                         automate recurring tasks. PowerShell is ideally suited for automating and speeding up routine system administration tasks.

                         How do I start a PowerShell script? You can start PowerShell scripts by using the New-Item cmdlet or clicking the “Create New File” bu
owerShell ISE (Integrated Scripting
                         Environment).

                         What is REPL in Python? REPL stands for “Read Evaluate Print; index=0; finish_reason=length; logprobs=; content_filter_results=}}
usage                  : @{prompt_tokens=4; completion_tokens=100; total_tokens=104}
```

4.1.1.1.2 Identificación mediante EntraID (RBAC)

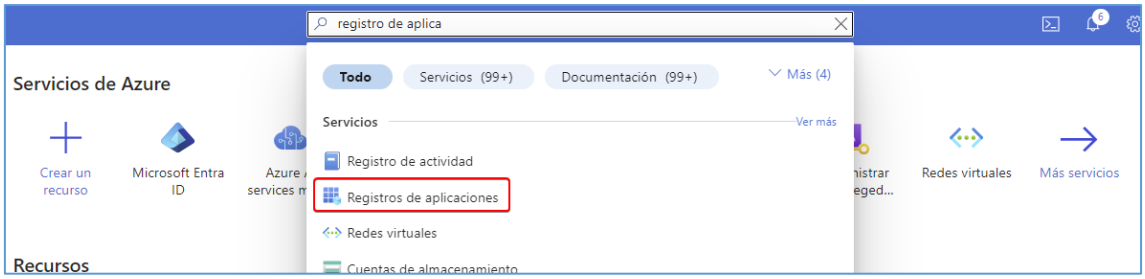
Para la identificación mediante EntraID:

- Crearemos una cuenta de aplicación o servicio principal
- Obtener un token para el “servicio principal”
- Realizar una llamada a la API del servicio de traducción de Azure mediante el recurso de varios servicios creado en el punto 3.2

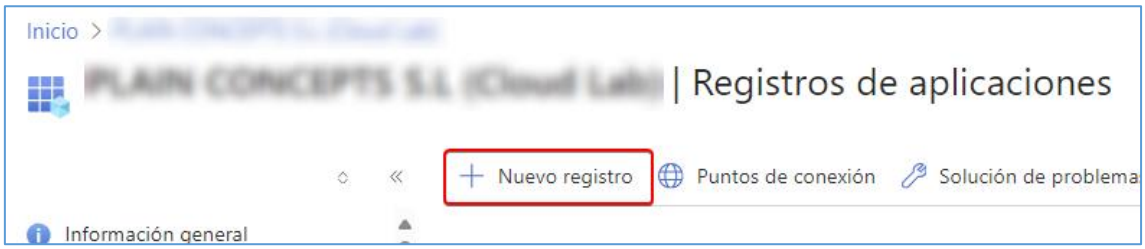
Nota: Para la creación de un usuario de aplicación necesitaremos al menos el rol RBAC en EntraID de “Administrador de aplicaciones”.

Para la creación de una cuenta de aplicación desde el portal de Azure:

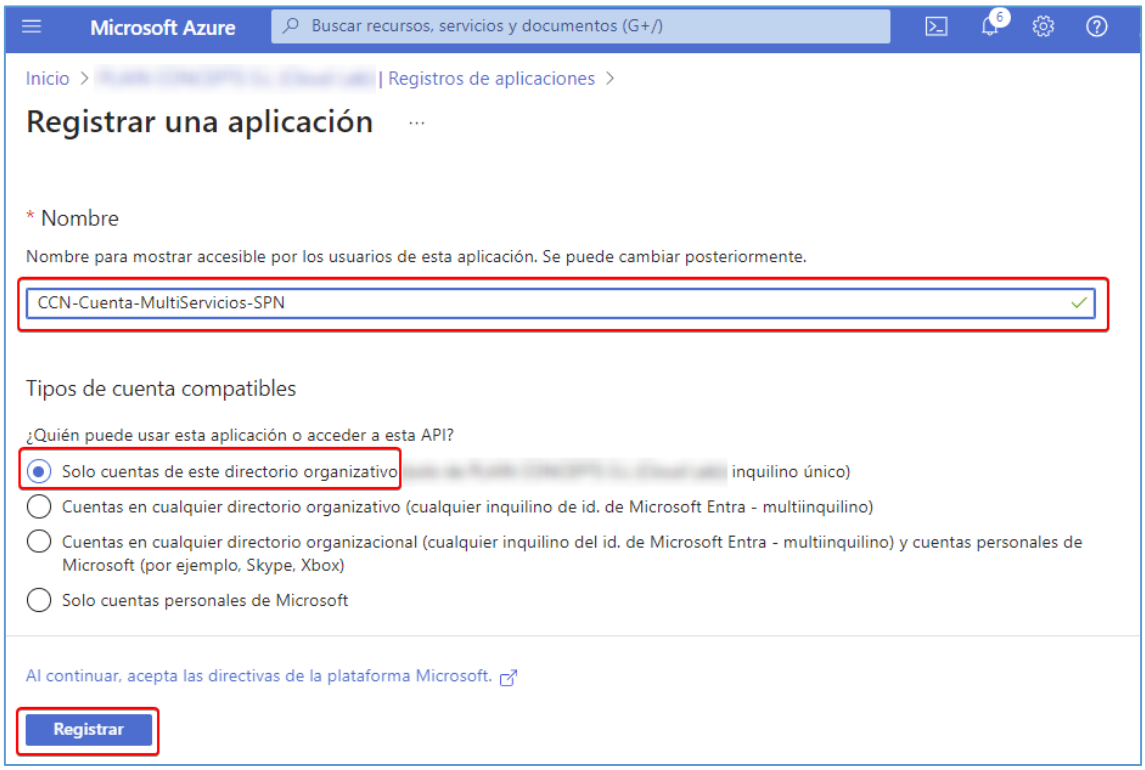
1. En el buscador de Azure, buscar “Registros de aplicaciones”



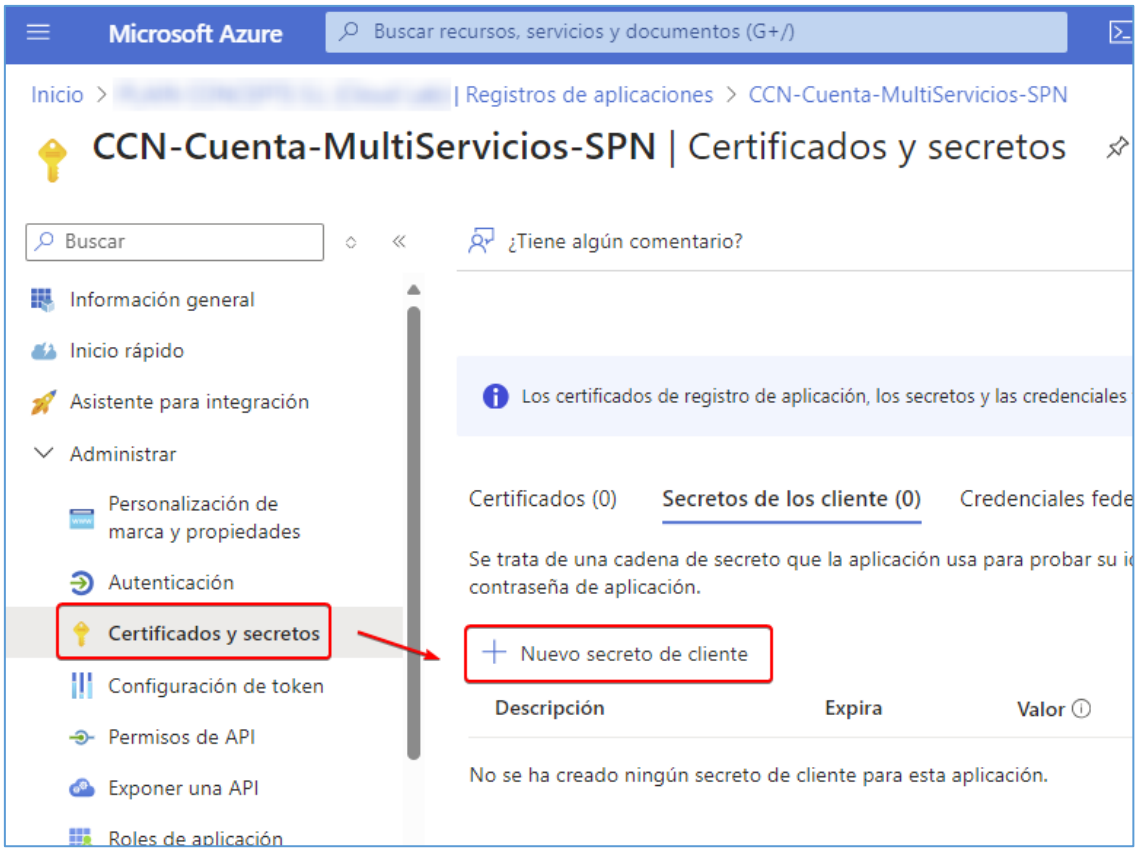
2. Pulsaremos sobre “Nuevo Registro”



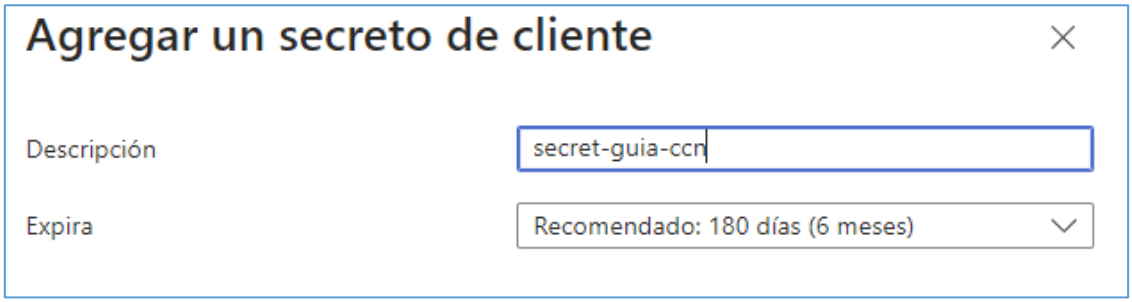
3. Asignaremos un nombre y pulsaremos en “Registrar”



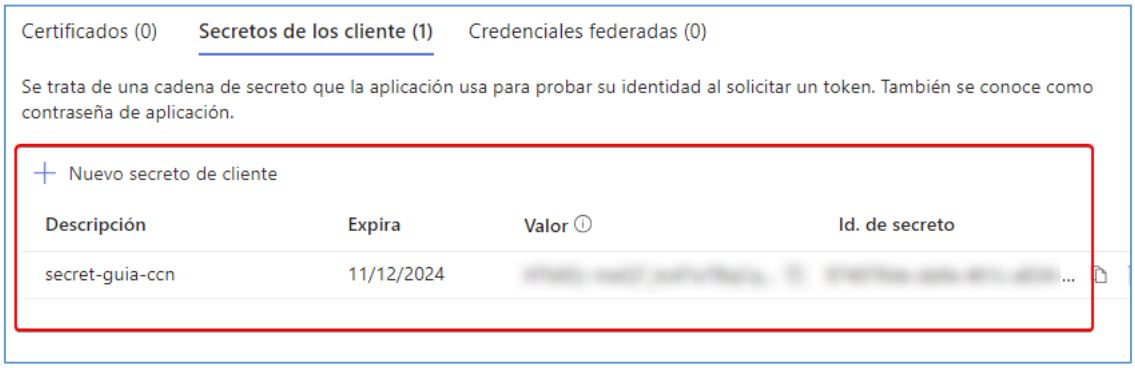
4. En el servicio principal recién creado, iremos a “Certificados y Secretos” y pulsaremos sobre “Nuevo Secreto de Cliente”.



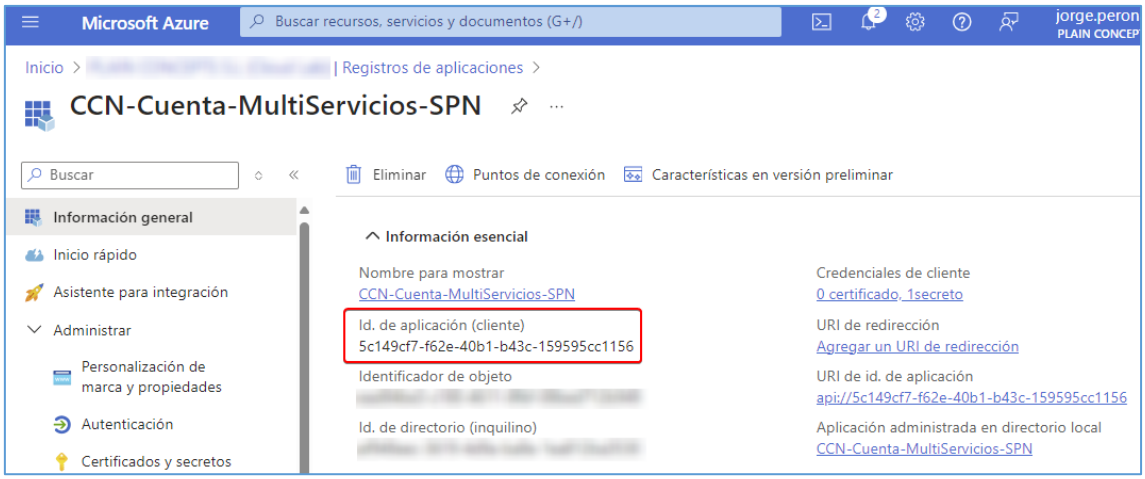
5. Agregaremos una descripción y pulsamos sobre agregar



6. Apuntad el secreto generado (campo Valor) ya que una vez salgamos de esta pantalla ya no será visible



7. Desde Información general, apuntad el ID de aplicación que lo necesitaremos junto al secreto generado anteriormente para obtener el token de acceso:



8. Asignar el rol “Usuario de Cognitive Services” en el recurso de IA “CCN-Cuenta-MultiServicios”. Ver el punto 3.2.1. Permisos o 4.1.1.2. Requisitos de Acceso para ver como asignar el permiso.

Una vez asignado, abriremos la consola de Powershell para recuperar el token y hacer la llamada API rest al recurso de IA:

```
#  Generar un Token para el servicio principal generado anteriormente
#  $tenantId = "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxx"
#  $clientId = "5c149cf7-f62e-40b1-b43c-159595cc1156"
#  $clientSecret = "5NC8Q~jOBjJ3g~3.mBzAWxQn9bbnIxX4eIgPtcr3"
#  $resourceUrl = "https://cognitiveservices.azure.com/"
#  $tokenEndpoint =
   "https://login.microsoftonline.com/$tenantId/oauth2/token"
#  $body = @{
#  grant_type    = "client_credentials"
#  client_id     = $clientId
#  client_secret = $clientSecret
#  resource      = $resourceUrl
#  }
#  $responseToken = Invoke-RestMethod `
#  -Uri $tokenEndpoint `
#  -Method Post `
#  -Body $body
#  $accessToken = $responseToken.access_token
```

La siguiente captura muestra un ejemplo de token generado:

```
token_type      : Bearer
expires_in      : 3599
ext_expires_in  : 3599
expires_on      : 1718367053
not_before      : 1718363153
resource        : https://cognitiveservices.azure.com/
access_token    : eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6IkwxS2ZLRklfam5YYndXYzIyeFp4dzFzVUhIMCIsImtpZCI6IkwxS2Z
                  LRklfam5YYndXYzIyeFp4dzFzVUhIMCJ9.eyJhdWQiOiJodHRwczovL2NvZ25pdGl2ZXNlcnZpY2VzLmF6dXJlLmNvbS8iLCJpc
                  3MiOiJodHRwczovL3N0cy53aW5kb3dzLm5ldC9hZjk0OGVlYy0zNjE5LTRkOWEtYmE4ZS0xZWE4MTJiYTM1MzAvIiwiaWF0Ijox
                  NzE4MzYzMTUzLCJuYmYiOjE3MTgzNjMxNTMsImV4cCI6MTcxODM2NzA1MywiYWlvIjoiRTJkZ1lEaTZhRXBBM2MrcC9ETmw1amd
                  jM2J6YUd3QT0iLCJhcHBpZCI6IjVjMTQ5Y2Y3LWY2MmUtNDBiMS1iNDNjLTE1OTU5NWNjMTE1NiIsImFwcGlkYWNyIjoiMSIsIm
                  lkcCI6Imh0dHBzOi8vc3RzLndpbmRvd3MubmV0L2FmOTQ4ZWVjLTM2MTktNGQ5YS1iYThlLTFlYTgxMmJhMzUzMC8iLCJpZHR5c
                  CI6ImFwcCIsIm9pZCI6ImNlOGU4YTdlLTM0ZTEtNGU2ZS1iNzFjLWNhODdhMDVmZjUxYyIsInJoIjoiMC5BWFFBN0k2VXJ4azJt
                  azI2amg2b0VybzFNSkFpTVgzSUtEeEhvTzJPVTNTYmJXM2lBQUEuIiwic3ViIjoiY2U4ZThhN2UtMzRlMS00ZTZlLWI3MWMtY2E
                  4N2EwNWZmNTFjIiwidGlkIjoiYWY5NDhlZWMtMzYxOS00ZDlhLWJhOGUtMWVhODEyYmEzNTMwIiwidXRpIjoiYkptN2pWNDBhRT
                  ZvS0prREtaNC1BQSIsInZlciI6IjEuMCIsInhtc19pZHJlbCI6IjcgMjgifQ.AvIFcBlJf-znaqOhL9zYcaOQkHZ0fBI1o2mR5P
                  CtTPCG8f8kxDxGi7kqrcamgze9XCjVzj0xBuQT7C-UucXCzziM-Y-GzQccYknzxGOUCkNyweh3NpvQhcEWizDyAbCfNLnseuDf7
                  CFjwVziDLY2Jc-sqWTlEsW13Ze53ocfRVOQuXjkGQZea3cvyhWNPBVWO8wlqjp0Ch_QEsEkxqvDk8YFMTHVEPn8ExuEmw_-k_-o
                  vTiM-_K54v-dl-pNT4iGj4IOhtxxd2FQPyfnrYCw2vCJi9X_uK2couDSXjo1784bBbWJ50MF_Dd2sqbpLLnv_cA5whDVONuxBfT
                  erR6tHQ
```

Una vez tengamos el token realizaremos la llamada a la API ajustando los parámetros $IAResourceID y $bodyRequest:

```
#   url = "https://api.cognitive.microsofttranslator.com/translate?api-
    version=3.0&to=es"
#   $IAResourceID = "/subscriptions/bd7ce688-9e50-444e-b9f6-
    357ff1b594b5/resourceGroups/RG-GuiaCCN-
    AIServices/providers/Microsoft.CognitiveServices/accounts/CCN-Cuenta-
    MultiServicios"
#   $header = @{
#       Authorization = "Bearer $accessToken"
#       "Ocp-Apim-ResourceId" = "$IAResourceID"
#       "Ocp-Apim-Subscription-Region" = "westeurope"
#       "Content-Type" = "application/json"
#   }
#   $bodyRequest = "[{'Text':'How much for the cup of coffee?'}]"
#   invoke-RestMethod -Uri $url `
#   -Method Post `
#   -Body $bodyRequest `
#   -Headers $header
```

La siguiente captura muestra la respuesta de la API:

```
PS C:\traslateapitest> invoke-RestMethod -Uri $url `
>> -Method Post `
>> -Body $bodyRequest `
>> -Headers $header

detectedLanguage        translations
----------------        ------------
@{language=en; score=1} {@{text=¿Cuánto cuesta la taza de café?; to=es}}
```

4.1.1.2 Requisitos de Acceso

Los requisitos de acceso a los servicios de IA son:

- Los elementos de Azure IA serán siempre desplegados en red privadas con un punto de conexión privada.
- Los permisos a los usuarios se deben de aplicar mediante RBAC manteniendo una política de mínimo privilegio.

El control de acceso basado en rol (RBAC) tiene varios roles integrados para recursos de Azure que se pueden ser consumidos y asignados 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 Tenant, podrá consultar la guía de configuración segura para Azure apartado [3.1.1.2 Requisitos de acceso/Roles personalizados].

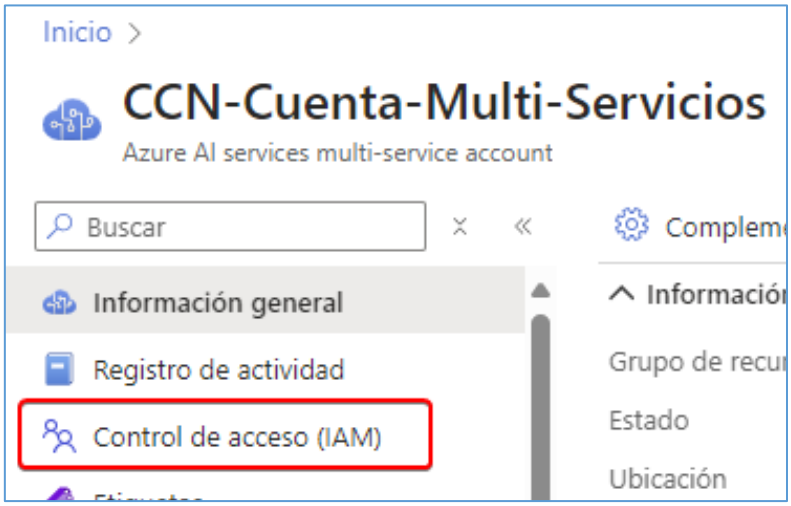
Los roles integrados se pueden agrupar en:

- **Roles generales:** Se aplican a una subscripción o a un grupo de recurso y afectan a todos los recursos contenidos. Los más comunes son: Propietario, Lector o Colaborador.
- **Roles específicos de recurso:** Asignan permiso sobre un recurso concreto. Se puede aplicar a nivel de subscripción o grupo de recursos, pero solo afectarán al recurso para el que fueron creados. Un ejemplo de este tipo de roles es "Cognitive Service OpenAI User".

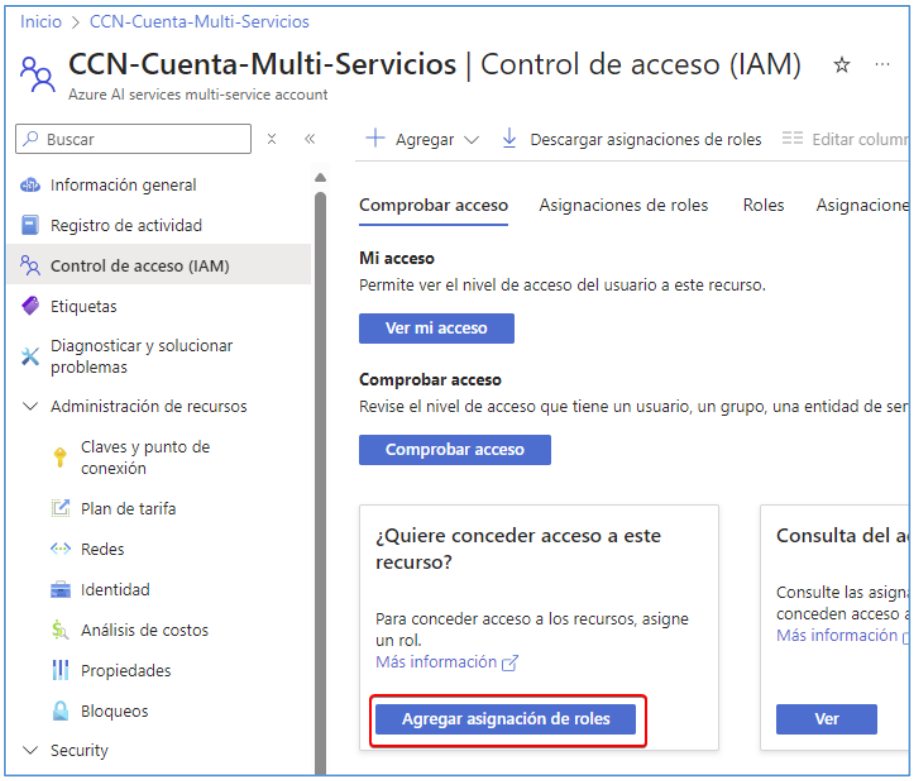
Nota: Si los roles integrados no cumplen las necesidades específicas se pueden crear roles personalizados. Ver *[3.1.1.2 Requisitos de acceso / Roles personalizados RBAC]* de la guía. *[CCN-STIC-884A - Guía de configuración segura para Azure]*

A continuación, se muestra como listar y asignar un rol integrado de Azure a una entidad de seguridad (usuario, grupo, service principal) desde el portal de Azure.

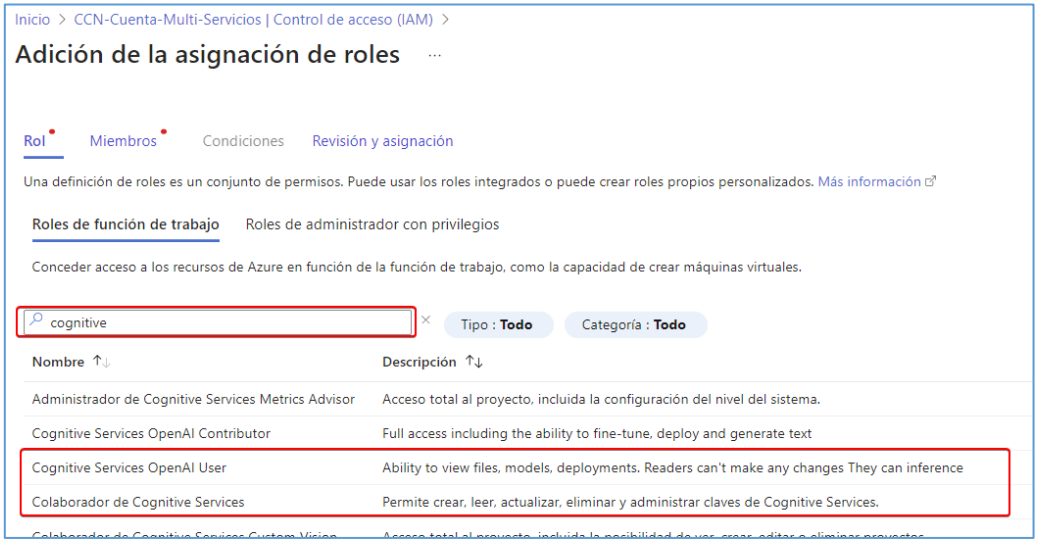
1. En el servicio de IA al que queramos asignar un permiso, pulsaremos sobre *"Control de acceso (IAM)":*



2. En la pantalla principal de *Control de Acceso IAM* pulsaremos sobre "Agregar asignación de roles":

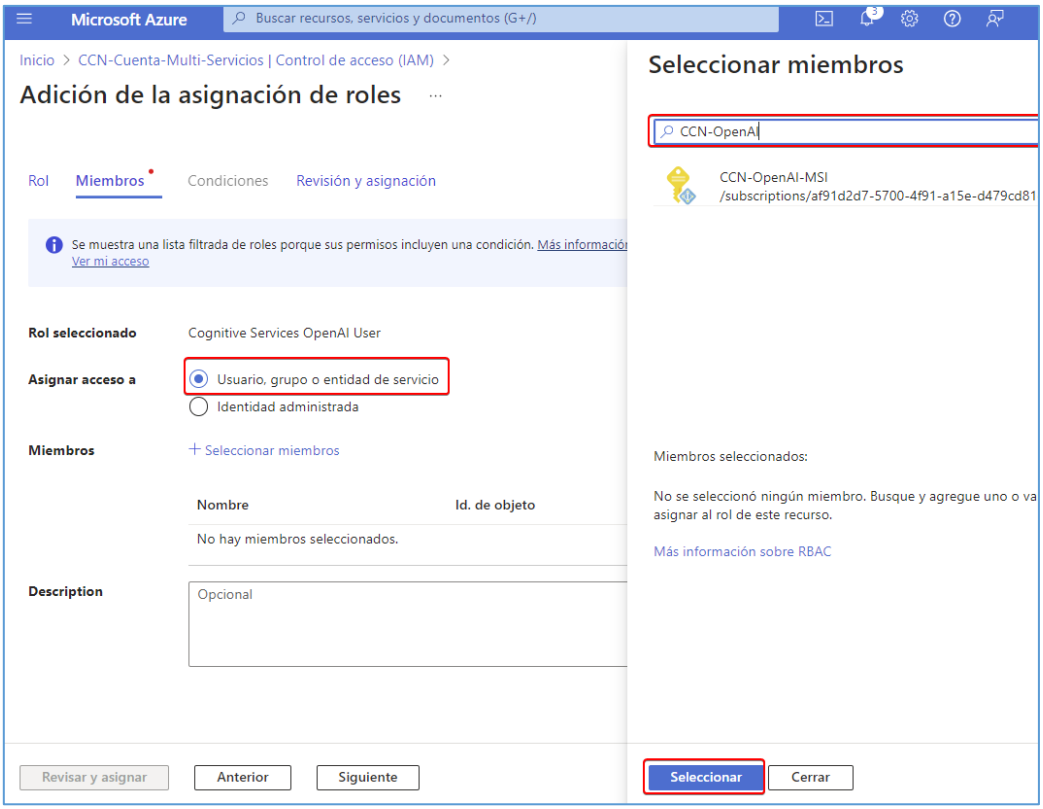


Sobre la lupa de búsqueda escribiremos "Cognitive" y nos mostrara el nombre del rol, una breve descripción, el tipo de rol y la categoría del rol entre otras opciones de todos los servicios de IA. Seleccionamos el rol y pulsamos sobre siguiente o sobre miembros para pasar a la pestaña *Miembros*.

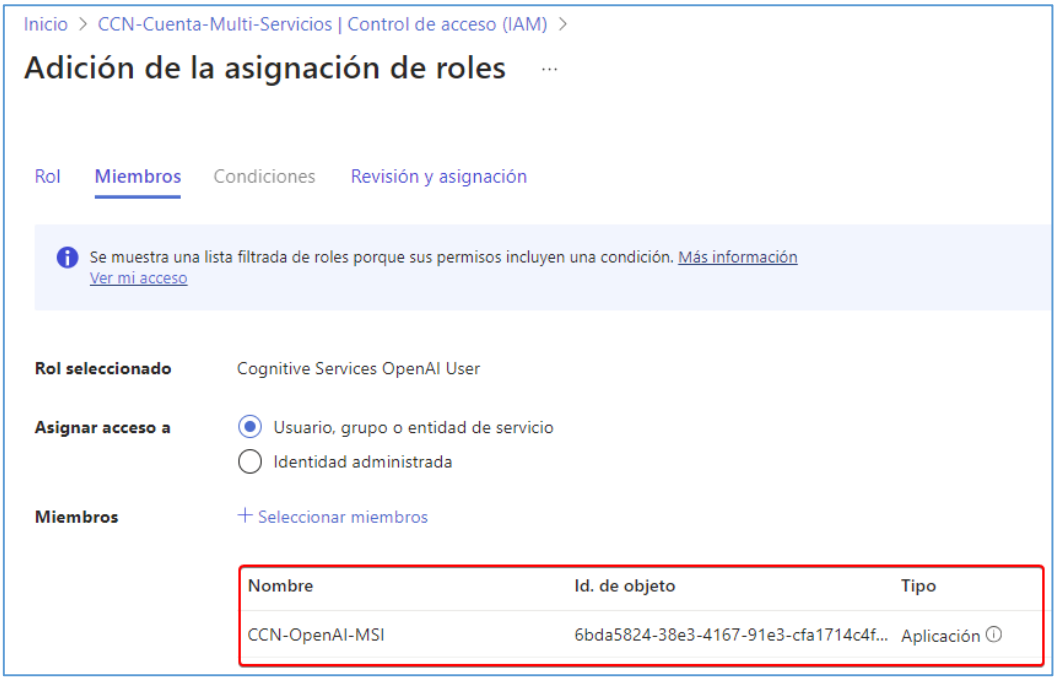


En esta captura se ha resaltado un rol genérico como es *Colaborador de Cognitive Services* y un rol exclusivo de OpenAI *Cognitive Services OpenAI User*.

3. En la pestaña Miembros seleccionaremos el usuario, grupo, entidad de servicio o identidad administrada al que queremos asignar permisos. En nuestro ejemplo seleccionaremos una Entidad de Servicio llamada *CCN-OpenAI-MSI:*



Confirmamos en miembros que la asignación es la correcta:



Una vez seleccionada pulsaremos sobre Siguiente y Revisar y asignar

4.1.1.3 Segregación de funciones y tareas

En los servicios de Azure IA se pueden clasificar los usuarios en al menos cuatro roles según sus tareas, si bien es verdad que algunos usuarios pueden tener más de un rol:

- **Usuarios Finales:** Estos usuarios explotaran los servicios de IA mediante una capa de presentación, como puede ser una aplicación web o aplicación clásica de escritorio. Nunca necesitaran acceso a herramientas de desarrollo, configuración o a modelos de entrenamiento. La seguridad de estos usuarios vendrá dada por la misma aplicación si fuera necesaria.
- **Usuarios Administradores:** Son los usuarios encargados de gestionar los servicios de Azure para realizar cambios de configuración sobre los servicios de AI, redes, etc.., bien mediante línea de comandos o mediante el portal de Azure. Estos usuarios no entrenarán los modelos que serán posteriormente explotados por los usuarios finales.
- **Usuarios Desarrolladores:** Son los usuarios encargados de integrar las diferentes aplicaciones con los servicios de IA mediante llamadas a las API. Como veremos más adelante estas integraciones se realizan mediante autenticación basada en API KEY almacenada en un servicio de claves como es "Azure Key Vault".
- **Usuario Administrador de IA:** Son los usuarios encargados de entrenar y configurar los diferentes modelos de IA.

Para la segregación de funciones y tareas para estos roles de usuarios aplicara un control de acceso basado en **roles RBAC**

Para los servicios de IA están predefinidos los siguientes roles. Estos roles se pueden asignar en un Grupo Administrado, subscripción, grupo de recursos o a un recurso directamente:

- **Colaborador de Cognitive Services:** Normalmente, a este rol se le concede acceso en el nivel de grupo de recursos para un usuario junto con roles adicionales. Por sí solo, este rol permitiría a un usuario realizar las siguientes tareas:
  ✅ Crear recursos de Azure OpenAI en el grupo de recursos asignado.
  ✅ Ver los recursos del grupo de recursos asignado en Azure Portal.
  ✅ Ver el punto de conexión de recursos en Claves y punto de conexión
  ✅ Ver, copiar o regenerar claves en Claves y punto de conexión
  ✅ Posibilidad de ver los modelos disponibles para la implementación en Azure OpenAI Studio
  ✅ Usar las experiencias de área de juegos de Chat, Finalizaciones y DALL-E (versión preliminar) para generar texto e imágenes con los modelos que ya se han implementado en este recurso de Azure OpenAI
  ✅ Crear filtros de contenido personalizados
  ✅ Agregar un origen de datos para el uso de la característica de datos
  ✅ Crear nuevas implementaciones de modelos o editar implementaciones de modelos existentes (via API)
  ✅ Creación de modelos personalizados de ajuste preciso
  ✅ Carga de conjuntos de datos de ajuste preciso

✅Creación de nuevas implementaciones de modelos o edición de implementaciones de modelos existentes (mediante Azure OpenAI Studio)

- **Lector de usos de Cognitive Services:** La visualización de la cuota requiere el rol Lector de usos de Cognitive Services. Este rol proporciona el acceso mínimo necesario para ver el uso de la cuota en una suscripción de Azure. Este rol se debe de aplicar a nivel de subscripción.

Los roles integrados del recurso de OpenAI son dos y pueden ser complementados con los roles predefinidos de IA:

- **Usuario de OpenAI de Cognitive Services:**
  ✅Ver el recurso en Azure Portal
  ✅Ver el punto de conexión de recursos en Claves y punto de conexión
  ✅Posibilidad de ver los recursos y las implementaciones de modelos asociadas en Azure OpenAI Studio.
  ✅Posibilidad de ver qué modelos están disponibles para la implementación en Azure OpenAI Studio.
  ✅Usar las experiencias de área de juegos Chat, Finalizaciones y DALL-E (versión preliminar) para generar texto e imágenes con los modelos que ya se han implementado en este recurso de Azure OpenAI.
  ✅Realizar llamadas API de inferencia con Microsoft Entra ID.

- **Colaborador de OpenAI de Cognitive Services: Reúne los permisos de Usuario de OpenAI y añade:**
  ✅Crear modelos personalizados con ajuste preciso
  ✅Cargar conjuntos de datos para el ajuste preciso
  ✅Creación de nuevas implementaciones de modelos o edición de implementaciones de modelos existente.

4.1.1.4 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.

Nota: Se puede obtener información más detallada ver *[3.1.1.4 Proceso de gestión de derechos de acceso]* de la guía. *[CCN-STIC-884A - Guía de configuración segura para Azure]*.

4.1.1.5 Mecanismo de autenticación (Usuarios Externos)

La autenticación multifactor (MFA) de Microsoft Entra ID 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.

Nota: Para la configuración de la autenticación multifactor 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].*

4.1.1.6 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 *[4.1.1.5 Mecanismos de autenticación (Usuarios Externos)]* de la presente guía.

4.1.2 Explotación

4.1.2.1 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.

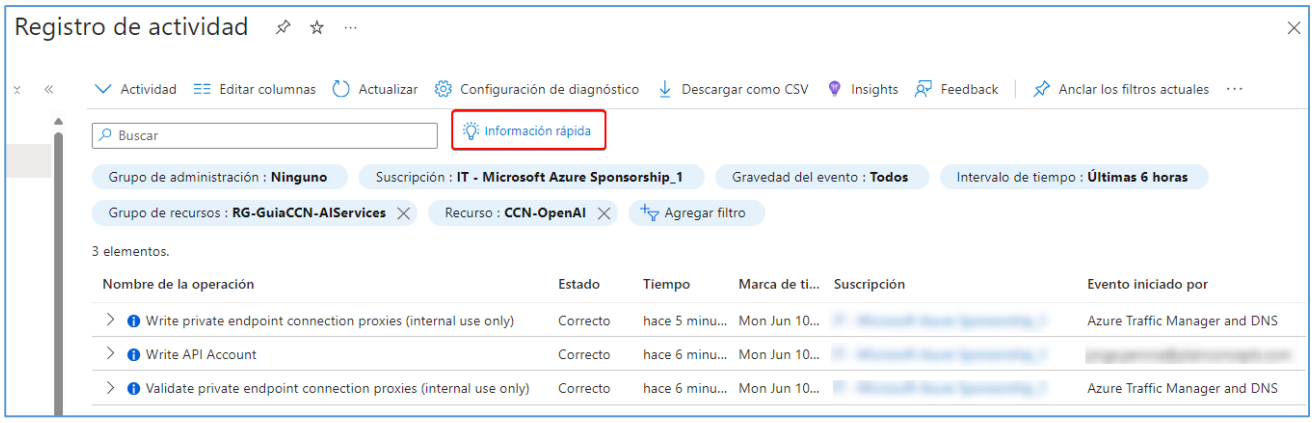
Las entradas en el registro de actividad son generadas por el sistema **y no se pueden cambiar ni eliminar**. Los logs de actividad tienen un **periodo de retención de 90 días** tras lo cual deberán ser exportadas para preservarlas. **Todas las actividades en Azure Monitor son registradas y pueden ser auditadas** por defecto.

Nota: Cualquier usuario con un rol de Lector puede acceder al registro de actividad, pero solo estarán disponibles los registros de los recursos sobre los que tenga permiso. Si aplicamos el rol de Lector a nivel de subscripción tendrá acceso a los registros de actividad de todos los recursos o si lo asignamos a nivel de grupo de recursos tendrá acceso a los registros de

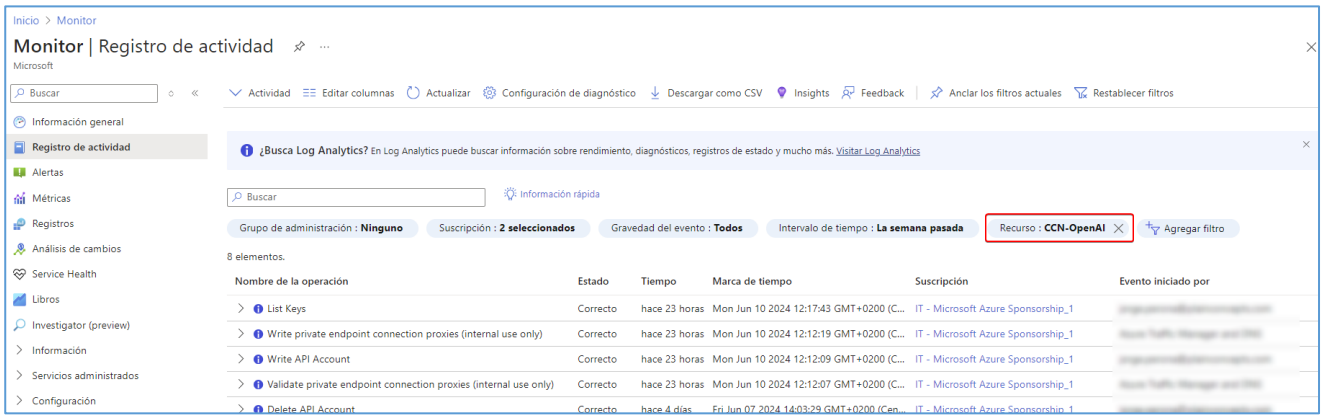
Para ver los registros de actividad mediante el portal de Azure:

1. pulsar en todos los recursos.

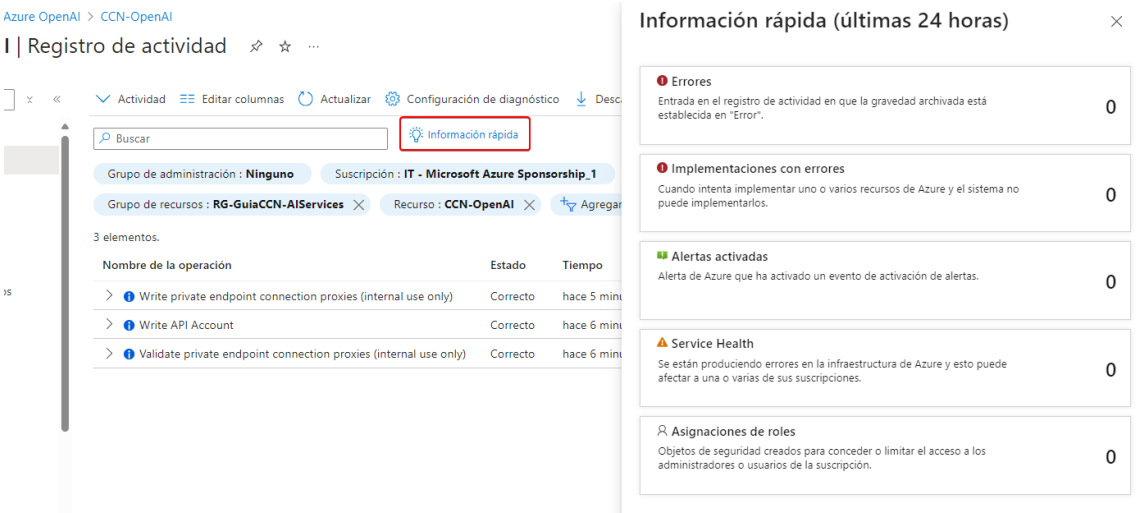
2. Pulsar en el servicio AI que queramos consultar.
3. Ir al apartado de [Registro de actividad].



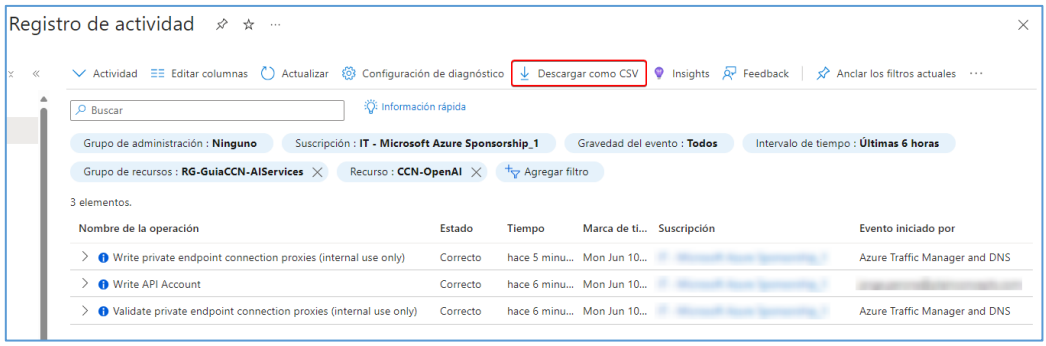
4. Otra alternativa para acceder al registro de actividad es hacerlo desde el Monitor de Azure pero en este caso habrá que aplicar un filtro por recurso



5. Aquí se pueden aplicar diferentes filtros o incluso obtener un resumen rápido con la opción “Información Rápida”:

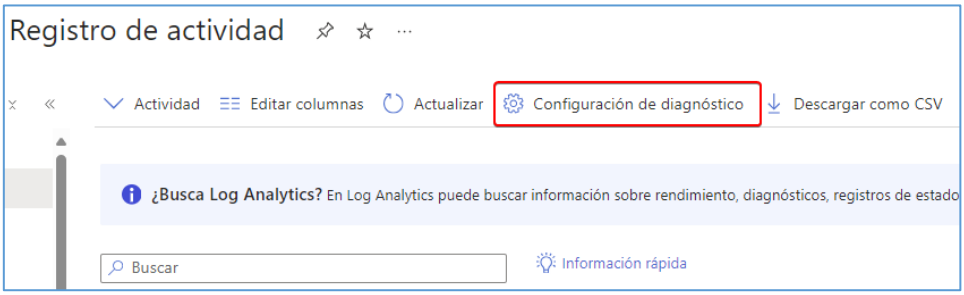


6. Los datos pueden ser exportados en csv mediante la opción “Descargar como CSV”

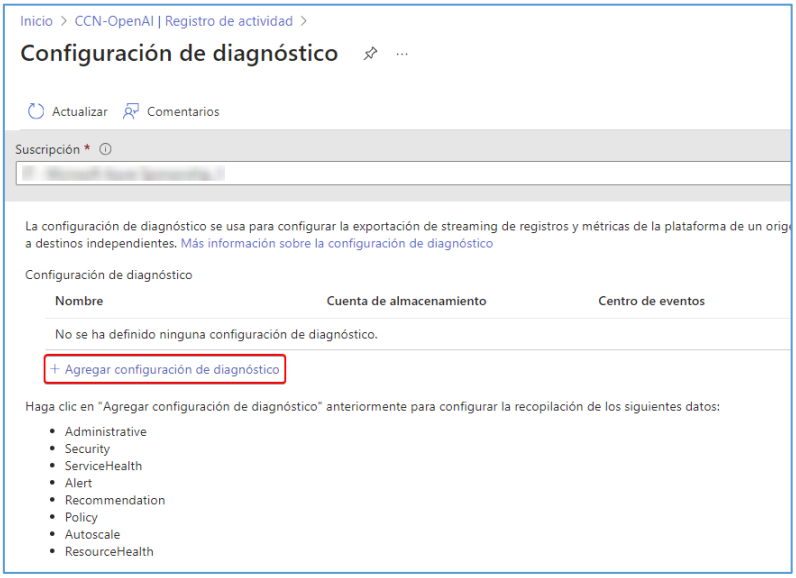


Ejemplo de CSV descargado:

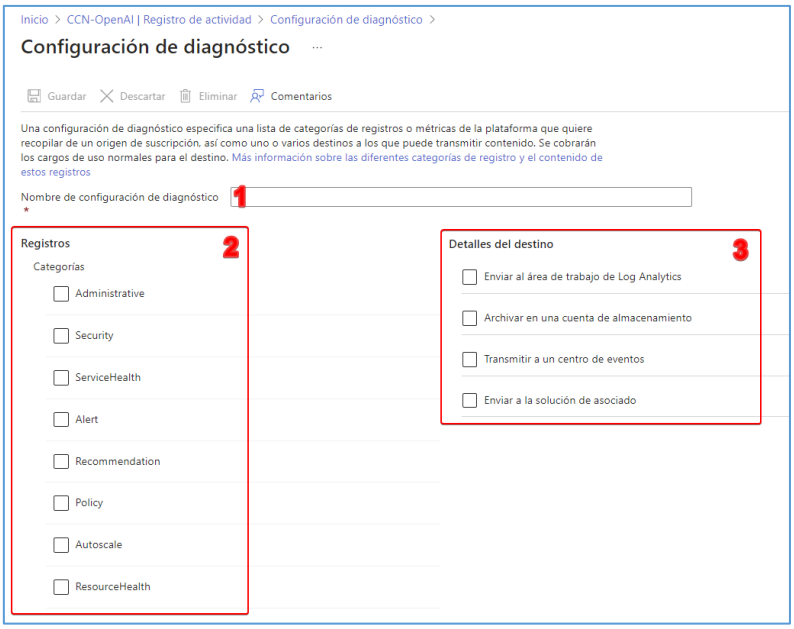
7. Adicionalmente se pueden integrar con “Loga Analytics”, exportar a una Storage Account o exportar a una aplicación de logs de terceros mediante el uso de “Configuración de Diagnostico”:



Para configura los logs de diagnóstico:



Indicaremos Nombre (1), Registro (2) y Detalle del destino (3)



4.1.3 Continuidad del Servicio

Los servicios de IA de Azure son un servicio PaaS por lo que según la matriz de responsabilidad la continuidad del servicio es responsabilidad de Azure. Ver Responsabilidad compartida en la nube - Microsoft Azure | Microsoft Learn. Esto no quita de un posible fallo del servicio en el proveedor por lo que será necesario contar con un plan de Continuidad del Servicio.

La disponibilidad de un servicio PaaS de Azure vendrá dada por su SLA. Las SLA de Azure pueden ser consultadas en Licensing Documents (microsoft.com).

La siguiente imagen muestra un ejemplo de SLA para OpenAI:

Servicio Azure OpenAI

Definiciones adicionales:
"**Recurso de Azure OpenAI**" hace referencia a un recurso de Azure de tipo Azure OpenAI que se crea en una región de Azure en una suscripción de Microsoft Azure.
"**Implementación**" hace referencia a un punto de conexión modelo implementado en un recurso de Azure OpenAI.
"**Solicitud**" es una llamada API a una Implementación.
"**Máximo de Minutos Disponibles**" se refiere al número total de minutos que un Cliente implementa una determinada Implementación en un recurso de Azure OpenAI durante un Periodo Aplicable.
"**Tiempo de Inactividad**" hace referencia al número total de minutos dentro del Máximo de Minutos Disponibles durante los cuales una Implementación no está disponible. Un minuto se considera tiempo no disponible si >0,01 % de las Solicitudes realizadas a la implementación durante ese minuto devuelven un Código de Error. Si no se realizan Solicitudes durante un determinado minuto, se supone que ese minuto está 100 % disponible.
El "**Porcentaje de Tiempo de Actividad**" se representa a través de la siguiente fórmula

$$\frac{\textit{Máximo de Minutos Disponibles} - \textit{Tiempo de Inactividad}}{\textit{Máximo de Minutos Disponibles}} \; x \; 100$$

Crédito de Servicio:

Porcentaje de Tiempo de Actividad	Crédito de Servicio
<99,9 %	10 %
<99 %	25 %

4.1.3.1 Análisis de impacto

Aunque el cloud provider es responsable de la disponibilidad del servicio y nos da por contrato unos SLA de disponibilidad altos, este no está exento de una falla en algunos de los servicios, por lo que es importante contar con un análisis de impacto que

determine en caso de falla como actuar teniendo en cuenta toda la infraestructura implicada, no solo en los elementos de IA.

Este análisis de impacto deberá de contener al menos:

- Disponibilidad deseada del servicio (100%, 99.9%...)
- Definición de RPO de la infraestructura
- Definición de RTO de la infraestructura
- SLA global de la infraestructura (teniendo en cuenta todos los recursos, no solo los recursos de IA).
- Identificación y mitigación de riesgos

Una vez contemos con esta información se procederá a elaborar un plan de continuidad.

4.1.3.2 Plan de continuidad

Como se ha comentado anteriormente, la disponibilidad de un servicio de IA vendrá dado por su SLA. Este SLA es el mismo para todas las regiones, pero la perdida de servicio por parte del proveedor de cloud en una región no implica la pérdida del servicio en otras regiones. Se puede consultar el listado de disponibilidad de recursos por regiones en Productos de Azure por región | Microsoft Azure.

Adicionalmente, hay que tener en cuenta que los servicios de IA no actúan solos, sino que actúan en serie con otros servicios de Azure. Es decir, tienen procesos de entrada y salida que interactúan con otros servicios. A la hora de generar el plan habrá que tener en cuenta la continuidad de todos los servicios implicados en la infraestructura.

Si está utilizando los modelos base de un recurso de IA, debe configurar su código de cliente para supervisar los errores y, si estos persisten, estar preparado para redirigir a otra región de su elección en la que disponga de una suscripción habilitada para los recursos de IA.

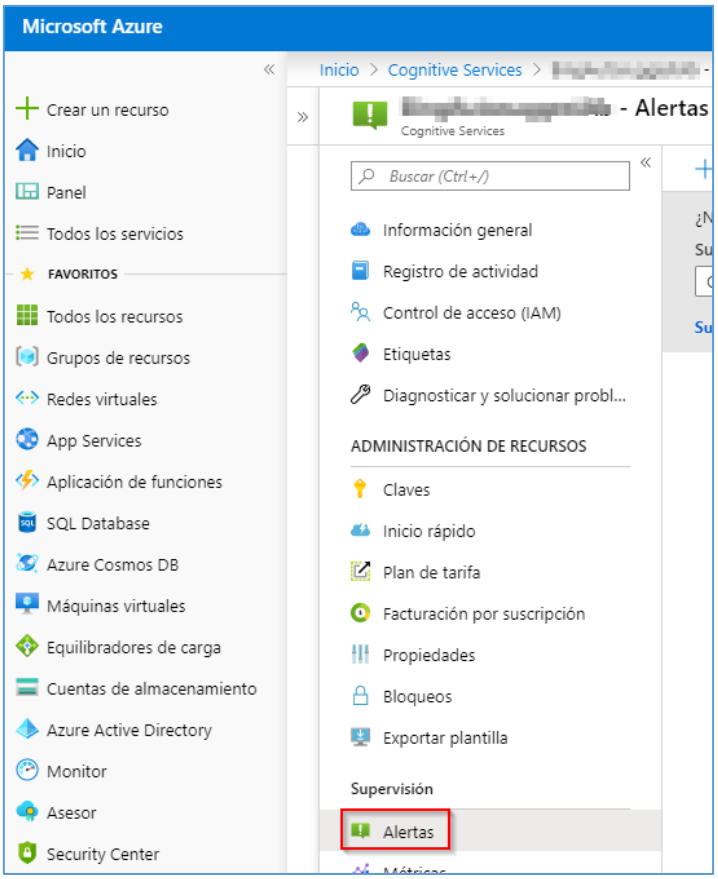
Nota: Para más información ver Continuidad empresarial y recuperación ante desastres (BCDR) con Azure OpenAI Service - Azure OpenAI | Microsoft Learn

4.1.4 Monitorización del sistema

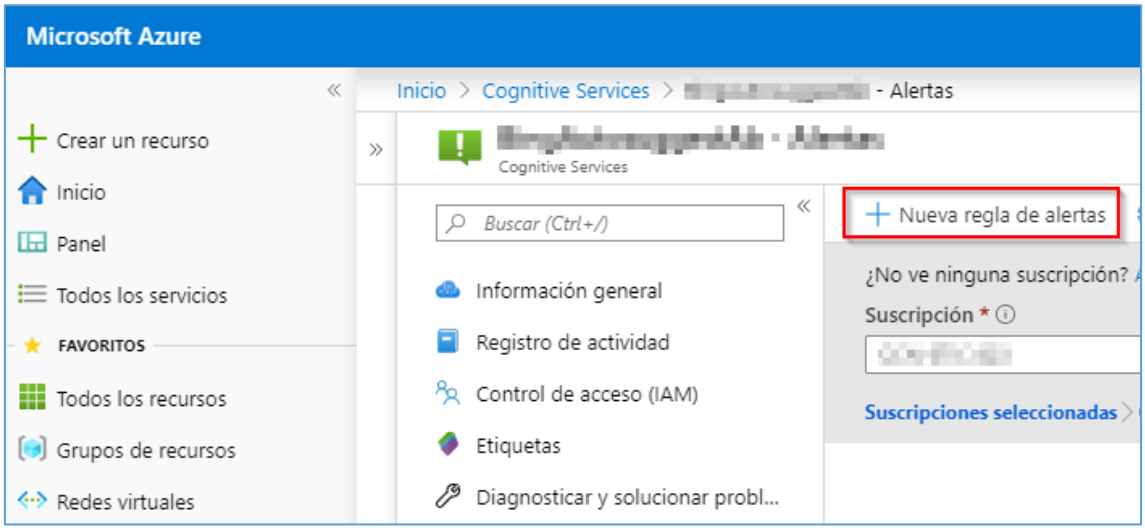
Una vez desplegada la API, congnitive services cuenta con una supervisión de Alertas y métricas que serán alojadas en Log Analitycs.

Personalización de Alertas

1. Desde la API pulsar en Alertas.

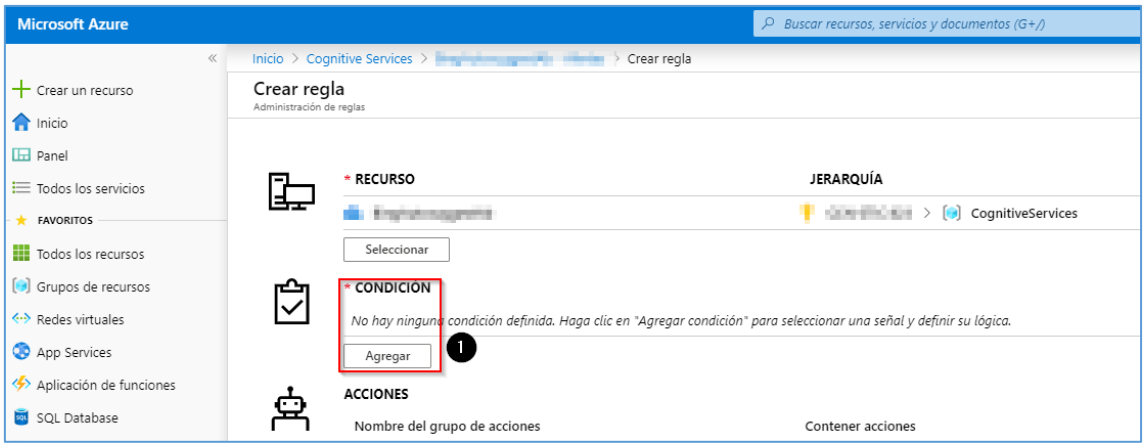


2. Pulsar en nueva regla de alertas.



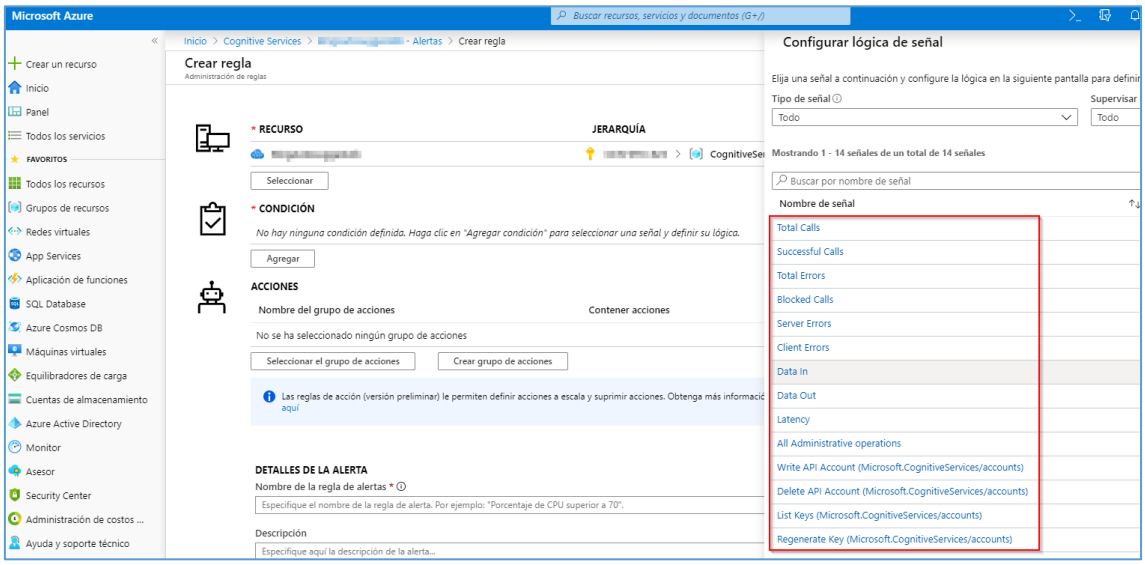
Nota: En este asistente deberá definir una condición y una acción.

3. Pulsar en Agregar.

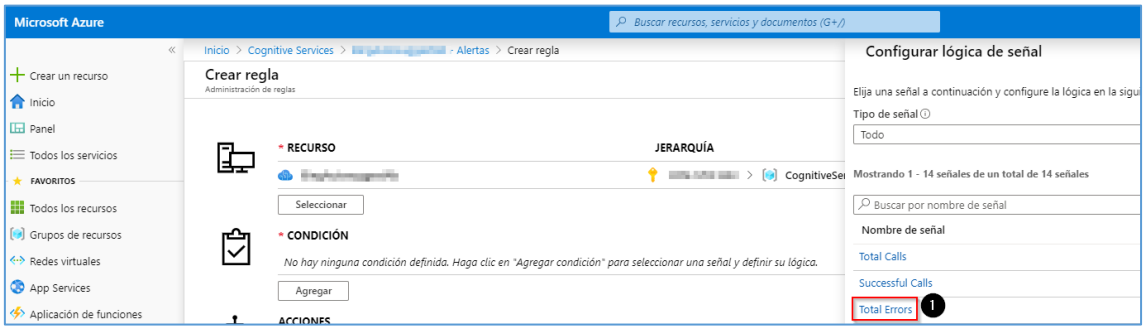


Nota: Podrá definir distintos tipos de métricas.

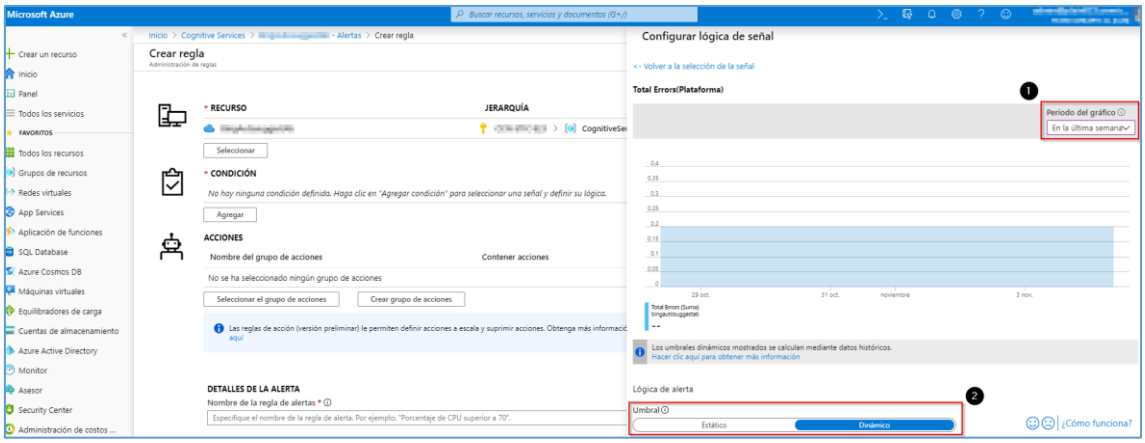
Algunos Ejemplos:



En este ejemplo definiremos Total Errors.



Nota: Deberá definir el periodo del gráfico, el umbral y un valor.



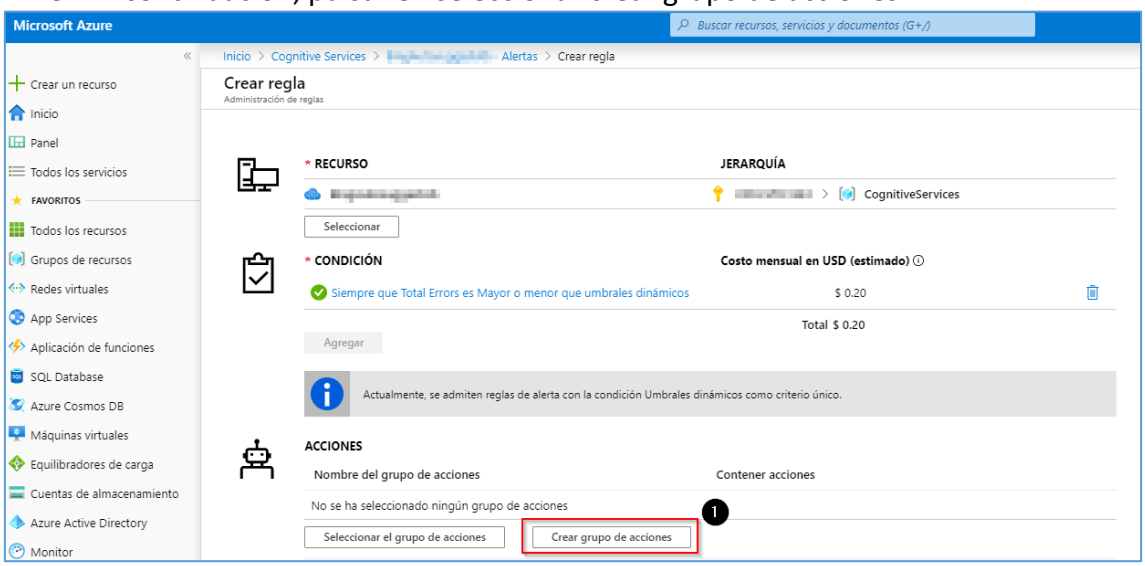
Lógica de Alerta.

Umbral: El umbral estático usa un valor de umbral definido por el usuario para evaluar la regla, mientras que los umbrales dinámicos usan algoritmos de aprendizaje automático para aprender continuamente el patrón de comportamiento métrico y calcular los umbrales automáticamente.

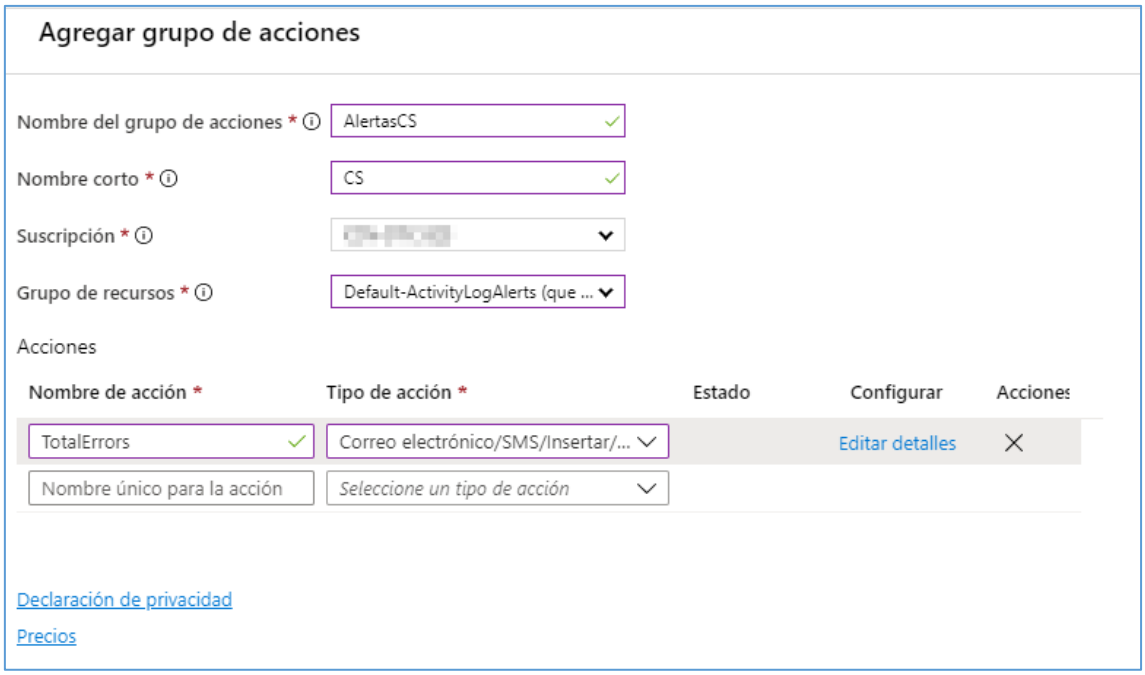
Podrá encontrar más información en el link: https://learn.microsoft.com/es-es/azure/azure-monitor/alerts/alerts-dynamic-thresholds

4. Una vez definido el Umbral, pulsaren Listo.

5. A continuación, pulsar en seleccionar crear grupo de acciones.



6. Deberá completar los siguientes campos.



Nombre del grupo de acciones: Defina el nombre de la acción.

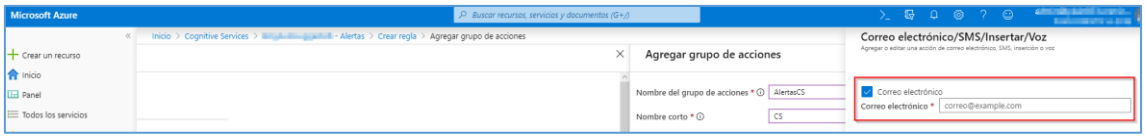
Nombre corto: Defina un nombre corto.

Suscripción: Seleccione su suscripción.

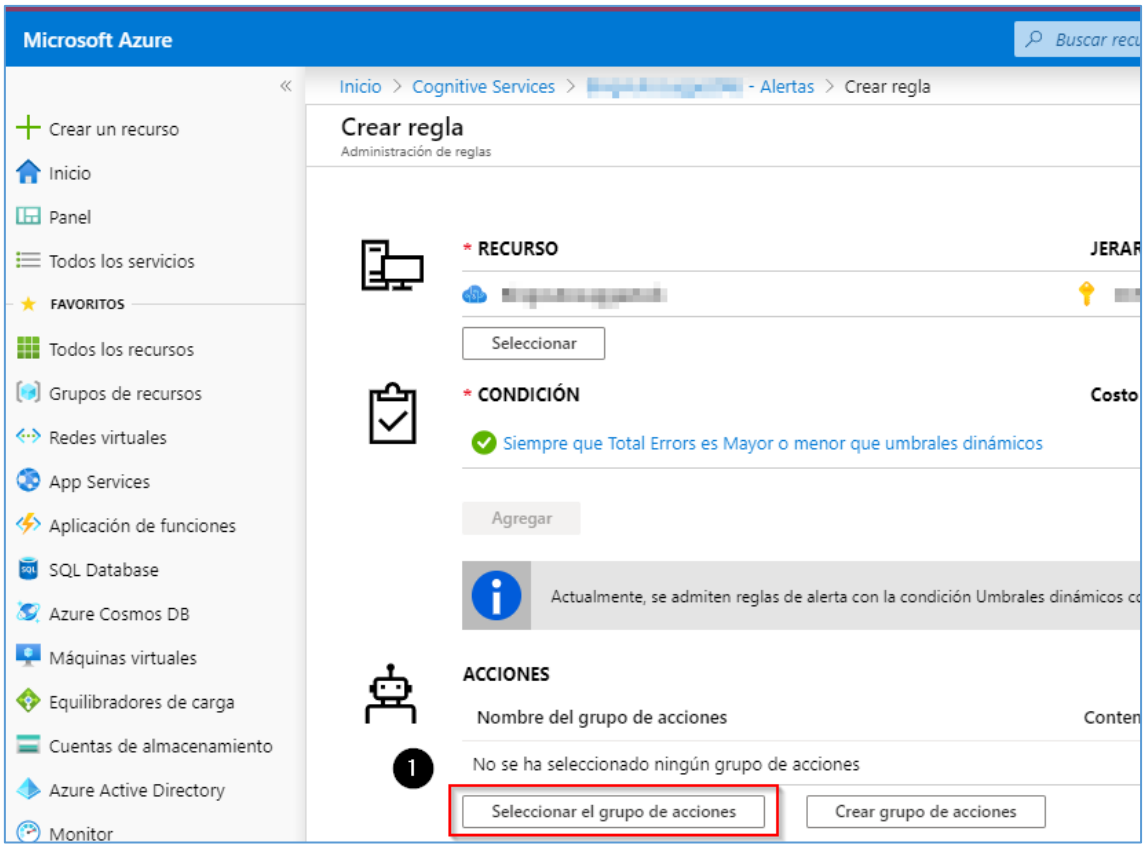
Grupo de recursos: Despliegue y elija en que grupo de recursos se registrara esta alerta.

Nombre de acción: Defina un nombre para la acción. En este caso se recomienda usar nombres que hagan referencia a la alerta.

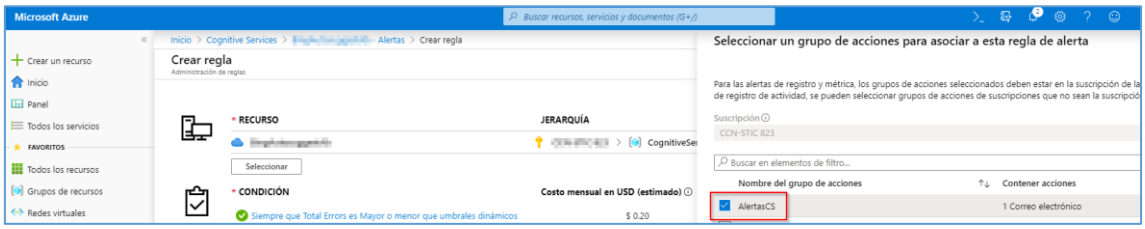
Tipo de acción: Se define a que método se va a enviar esta alerta. En este caso seleccionamos Correo Electrónico. Al elegir esta opción deberá rellenar estos campos.



7. Una vez agregada la dirección de correo electrónico, pulsar en crear.
8. A continuación, pulsar en Seleccionar grupo de acciones.

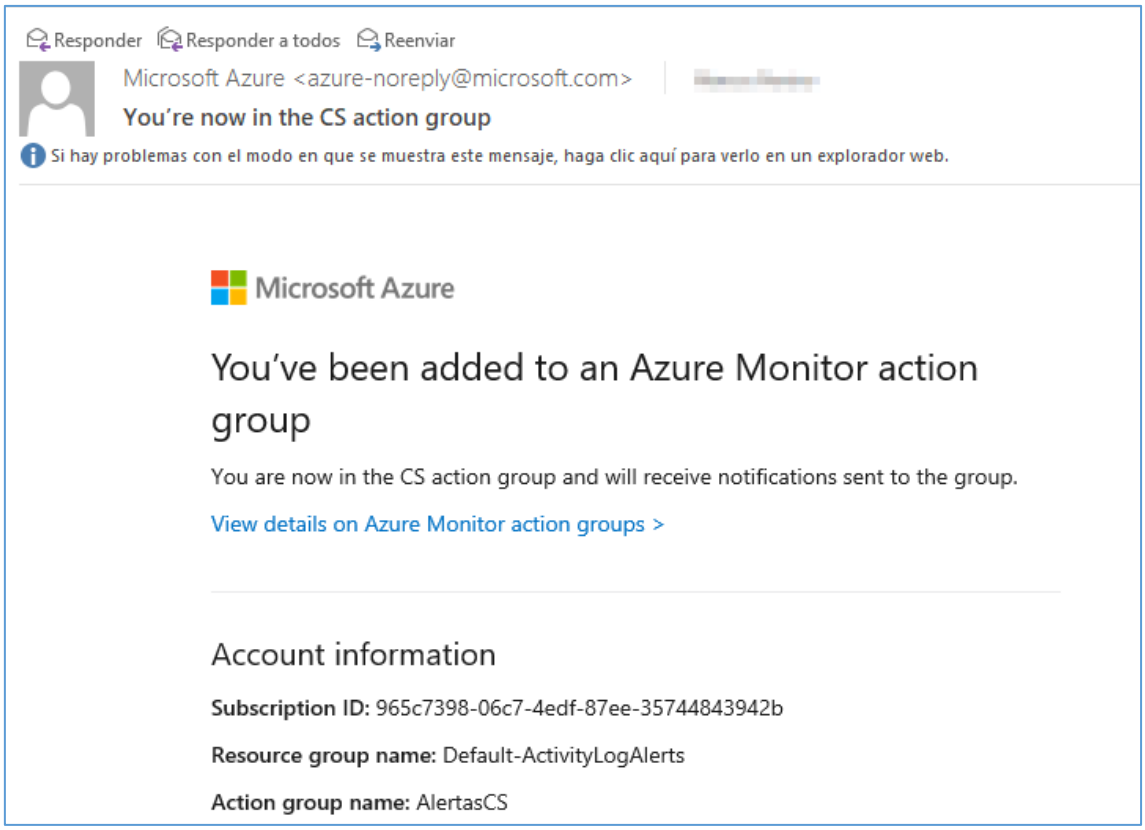


9. Pulsar en el nuevo grupo de acciones.

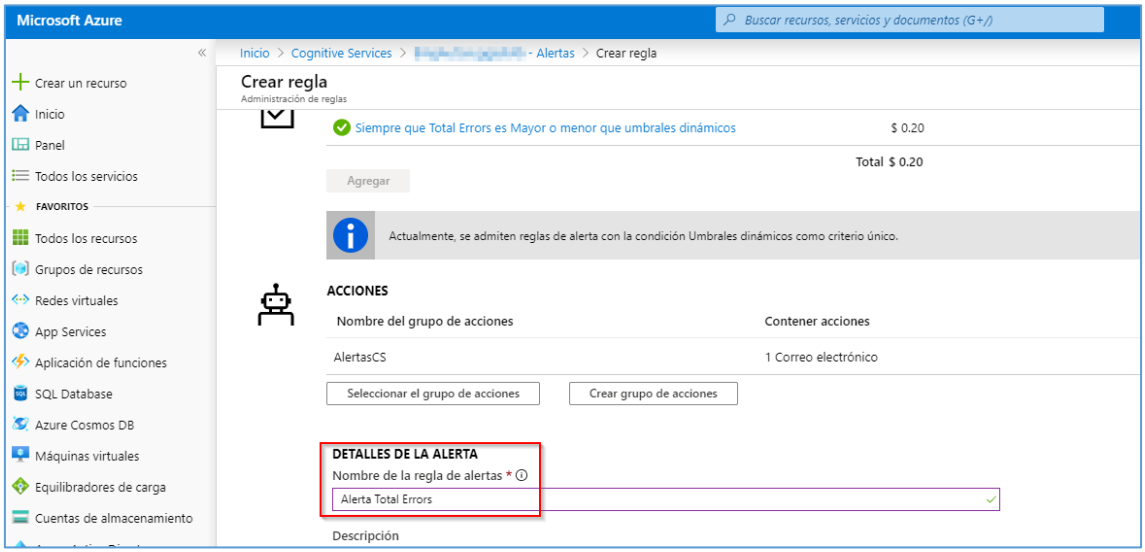


10. Pulsar en seleccionar.

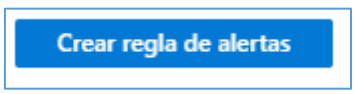
Nota: Le llegara un correo con la activación.



11. Para finalizar la creación de la regla debe definir un nombre que detalle la alerta.



12. Pulsar en Crear regla de alerta.



Nota: Recuerde que estas alertas están asociadas Azure monitor. Consultar la guía de configuración segura para Azure [Apartado 3.1.6 Monitorización de sistema]

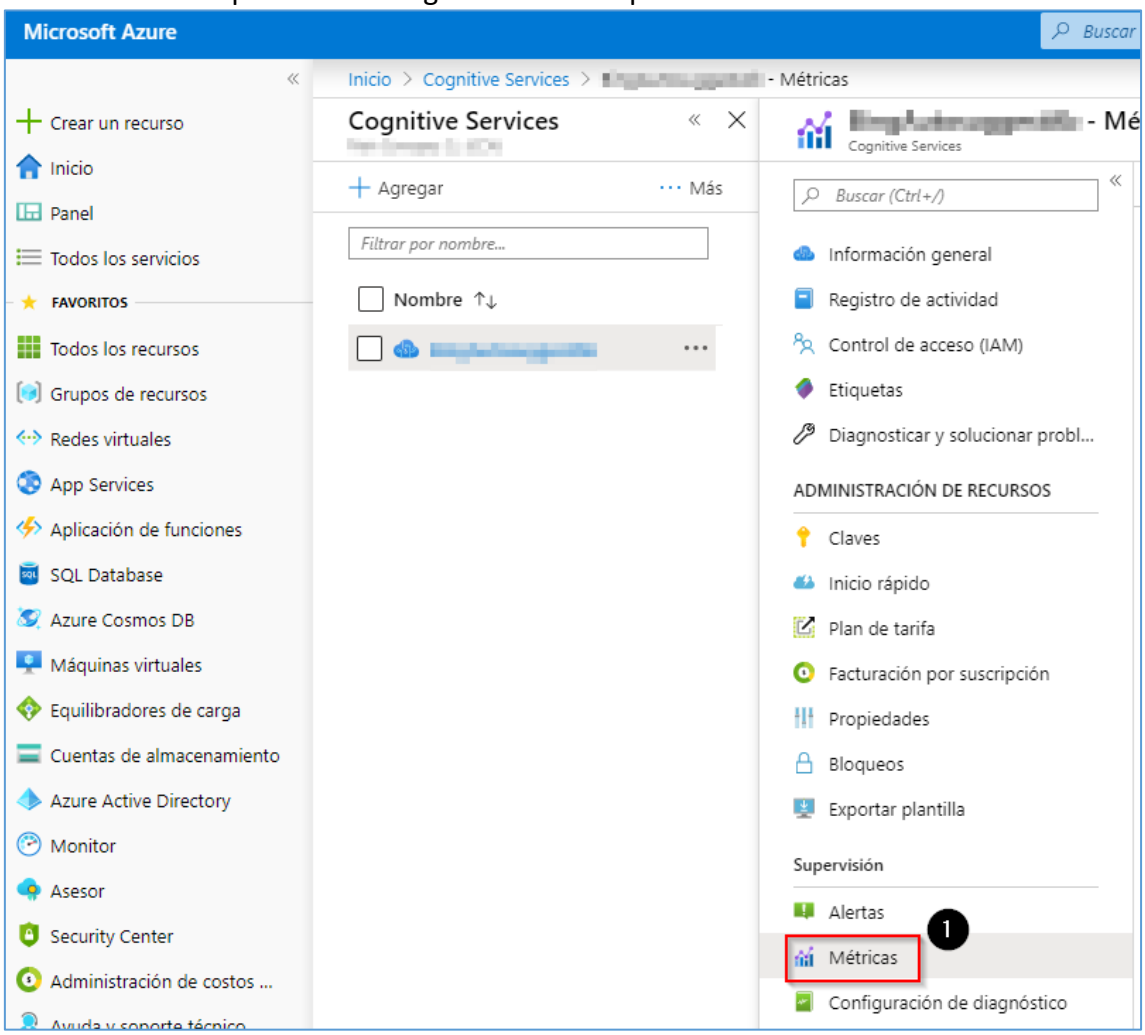
4.1.4.1 Sistema de métricas

El explorador de métricas de Azure Monitor es un componente de Azure que permite trazar los gráficos, correlacionar visualmente.

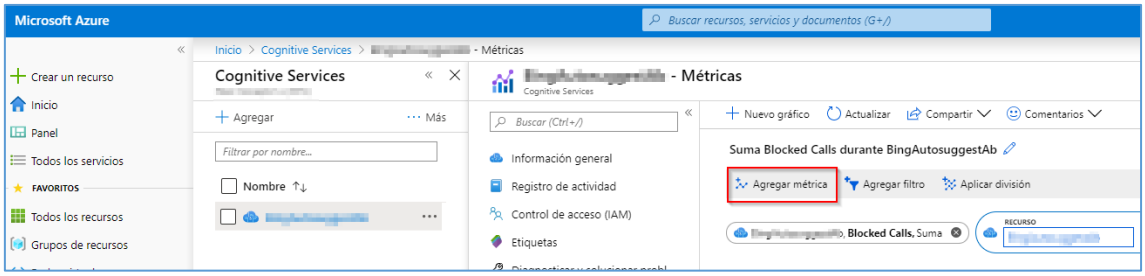
Podrá configurar métricas personalizadas desde cualquier recurso que tenga en Azure.

Para ello, siga estas instrucciones:

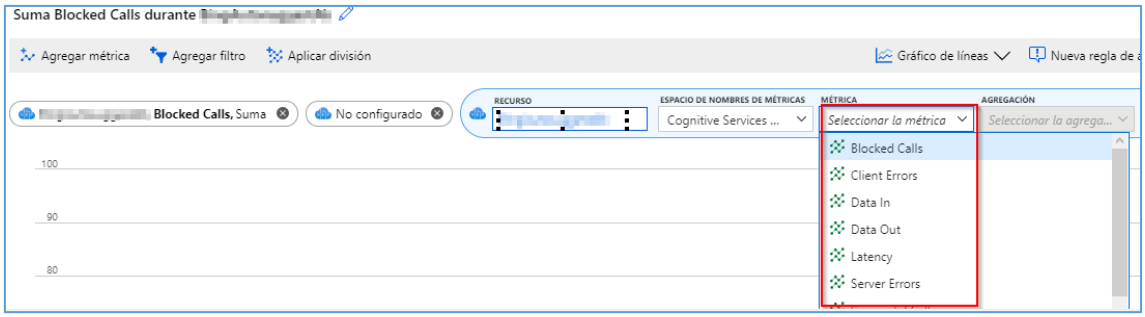
1. Desde la aplicación de cognitive services pulse en Métricas.



2. Pulsar en Agregar métrica.



3. Seleccione el tipo de métrica.



Puede consultar tantas métricas desee. Para ello, consulte el siguiente link: https://learn.microsoft.com/es-es/previous-versions/azure/storage/common/storage-analytics-metrics

5. Glosario y abreviaturas

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.
Endpoint	Endpoint es una Punto de acceso, una IP, FQDN o URL que permite invocar un servicio para su consumo.
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

Término	Definición
	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
RPO	Punto Objetivo de recuperación: En caso de una caída indica a qué momento podremos restaurara
RTO	Tiempo Objetivo de Recuperación: En caso de pérdida del servicio, indica el tiempo máximo que podemos tardar en recuperar la infraestructura.

6. 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.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No

	Se ha configurado el acceso condicional delimitando zonas geográficas y/o rangos de IPs. (importante y/o) 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	**Explotación**		
op.exp.8	**Registro de la actividad**		
	Se ha comprobado que el registro de Auditoría está activado y capturando eventos habilitando una nueva área de trabajo y aplicando consulta a los registros de diagnóstico mediante KUSTO.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: Si No	**Observaciones:**

		☐ ☐	
Op.mon	**Monitorizacion de sistema**		
Op.mon.2	**Sistema de métricas**		
	Se ha configurado Azure monitor aplicando los registros / alertas populares haciendo referencia a las recomendaciones mencionadas en la monitorización de los servicios de IA.	**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