centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 884D

Guía de configuración segura para Azure Cognitive Services

ENERO 2020

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

NIPO: 083-19-257-7

Fecha de Edición: enero de 2020

Plain Concepts ha participado en la realización y modificación del presente documento y sus anexos. Sidertia Solutions S.L. ha participado en la revisión de esta guía.

CCN centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2020.01.13 12:16:00 +01'00'

PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN) en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010 de 8 de Enero, actualizado por el Real Decreto 951/2015, de 23 de octubre, fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones (STIC) por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Julio de 2019

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. Cognitive Services

1.1 DESCRIPCIÓN DEL USO DE ESTA GUÍA

El objetivo del presente anexo es indicar los pasos a seguir necesarios para la utilización del Azure Cognitive 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 DEL SERVICIO DE Cognitive Services

Azure Cognitive Services son API, SDK y servicios disponibles para ayudar a los desarrolladores a compilar aplicaciones inteligentes sin necesidad de inteligencia artificial directa o aptitudes ni conocimientos sobre ciencia de datos.
Azure Cognitive Services permite a los desarrolladores agregar fácilmente características cognitivas en sus aplicaciones.
El objetivo de Azure Cognitive Services es ayudar a los desarrolladores a crear aplicaciones que puedan ver, oír, hablar, comprender e incluso empezar a razonar.
El catálogo de servicios de Azure Cognitive Services se puede dividir en cinco pilares principales: Vision, Voz, Lenguaje, Web Search y Decision.

3. DESPLIEGUE DE Cognitive Services

Requisitos previos

Como requisito de sistema operativo es recomendable consultar el siguiente link de Microsoft.
https://docs.microsoft.com/es-es/powershell/scripting/install/windows-powershell-system-requirements?view=powershell-6

Cognitive Services cuenta con múltiples categorías que se puede desplegar.
Se puede encontrar una lista de "tipos" de Cognitive Services disponibles con el comando az cognitiveservices list-types:

Ejecute este comando desde la consola de Azure CLI.

```
#   az cognitiveservices account list-kinds
```

Agregar un nuevo recurso al grupo de recursos

Para crear y suscribirse a un nuevo recurso de Cognitive Services, use el comando *az cognitiveservices account create*.
Este comando agrega un nuevo recurso al grupo de recursos creado anteriormente.
Al crear este nuevo recurso, se debe conocer el "tipo" de servicio que quiere usar y una ubicación de Azure:

```
# az cognitiveservices account create \
#     --name anomaly-detector-resource \
#     --resource-group cognitive-services-resource-group \
#     --kind AnomalyDetector \
#     --sku F0 \
#     --location North Europe \
#     --yes
```

Use el comando az cognitiveservices account keys list para obtener las claves de su recurso de Cognitive Services.

```
#  az cognitiveservices account keys list \
#    --name anomaly-detector-resource \
#    --resource-group cognitive-services-resource-group
```

Configuración de una variable de entorno para la autenticación

Las aplicaciones tienen que autenticar el acceso a los servicios Cognitive Services que usan. Para realizar la autenticación, se recomienda crear una variable de entorno para almacenar las claves de los recursos de Azure.

Si el despliegue utiliza una plataforma Windows escribir en la consola.

```
# setx COGNITIVE_SERVICE_KEY "your-key"
```

Si utiliza Linux

```
# export COGNITIVE_SERVICE_KEY=your-key
```

Limpieza de recursos

Se puede limpiar y eliminar un recurso de Cognitive Services, se puede eliminar el recurso o el grupo de recursos. Al eliminar el grupo de recursos también se eliminan los demás recursos incluidos en el grupo.

Para eliminar el grupo de recursos y sus recursos asociados, use el comando az group delete.

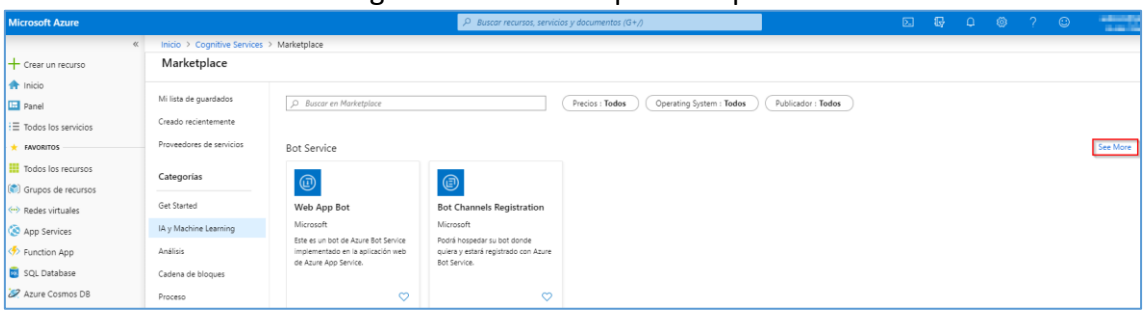
```
# az group delete --name storage-resource-group
```

Despliegue de una aplicación desde el portal de Azure

Se puede realizar los mismos pasos desde el portal de Azure para ello, siga estos pasos.

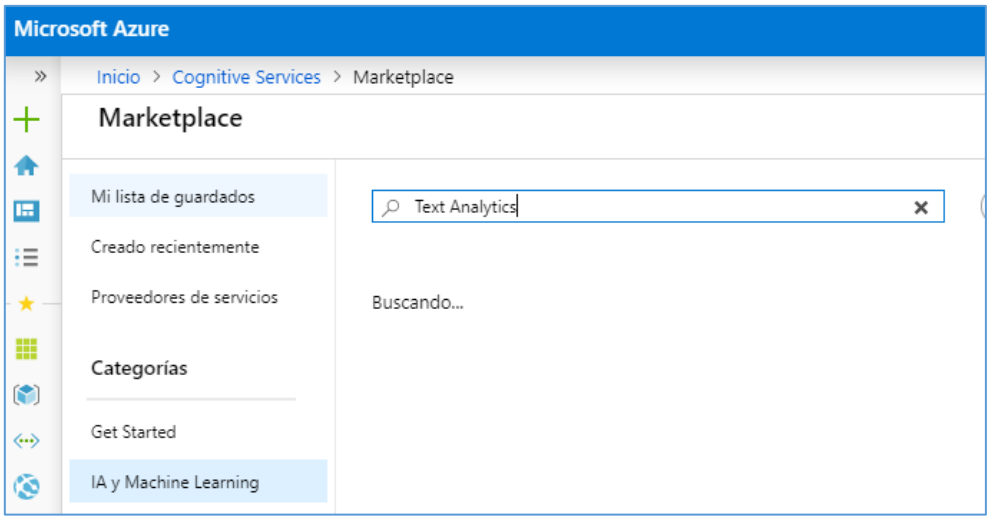
1. Desde el portal de Azure buscar Cognitive Services.

Para ver todos los Cognitive Services disponibles pulsar en más.

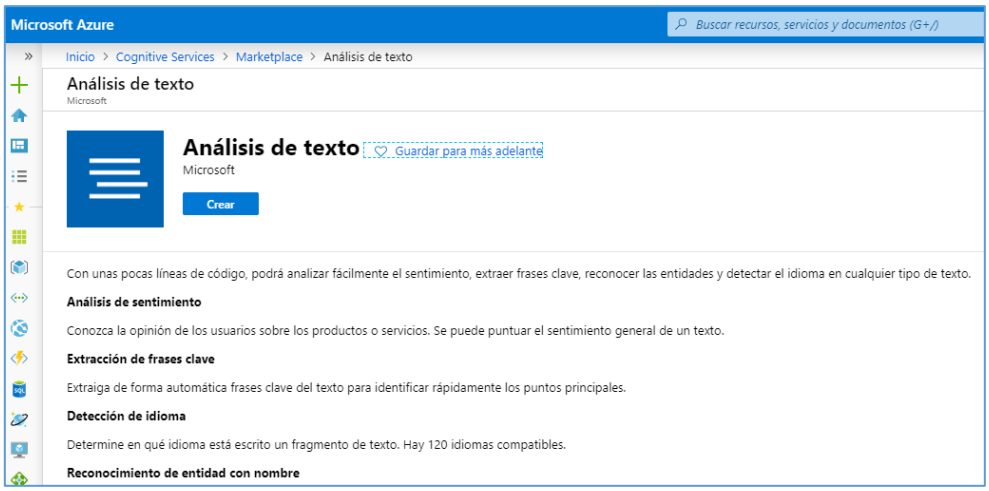


A continuación, se realiza el despliegue de una aplicación.

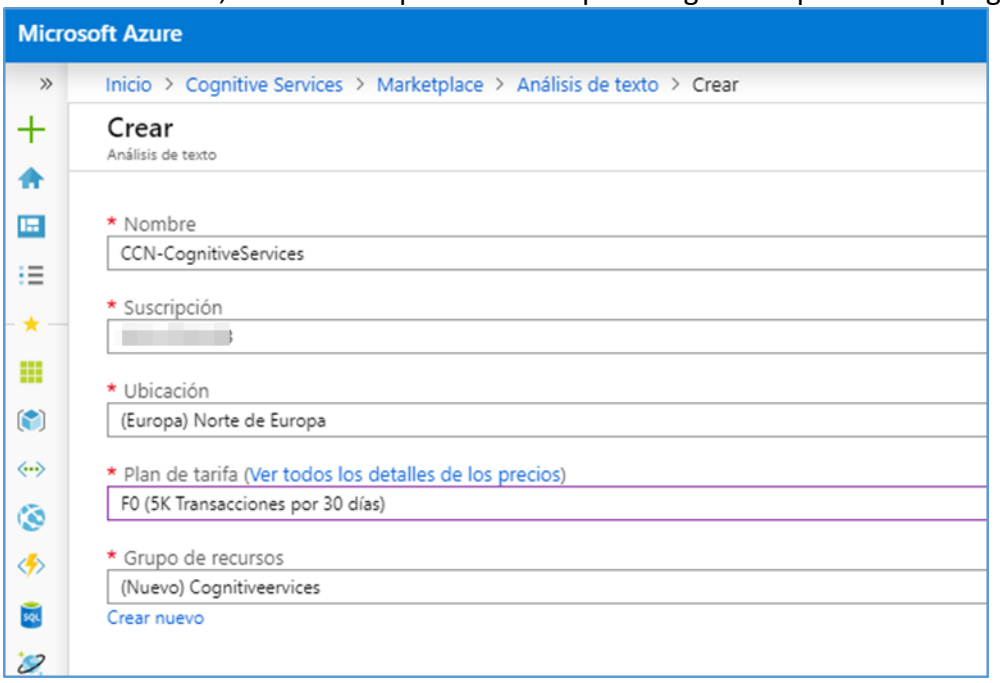
1. En el buscador buscar Text Analytics.



2. Pulsar en crear.

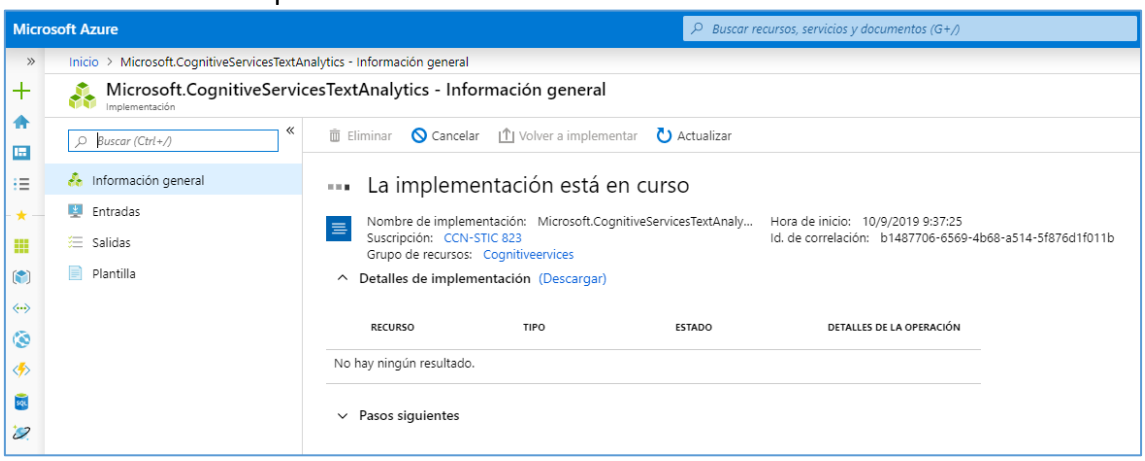


3. A continuación, se debe completar los campos obligatorios para el despliegue.

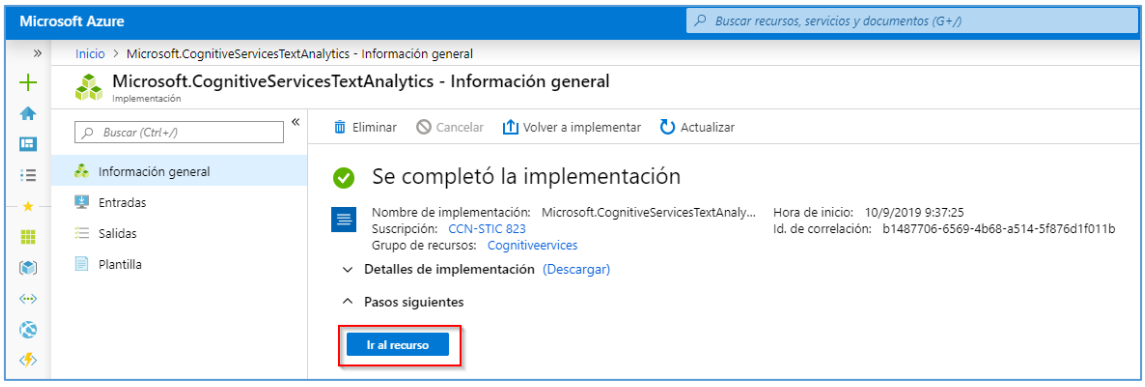


Nota: Se recomienda crear un nuevo grupo de recursos. Para más información puede consultar la guía de configuración segura para Azure [ANEXO 2.3 Elementos comunes en Azure]

4. Para finalizar pulsar en crear.



5. Al finalizar, pulsar en ir al recurso.



4. CONFIGURACIÓN DE Cognitive Services

4.1 Marco operacional

4.1.1 Control de acceso

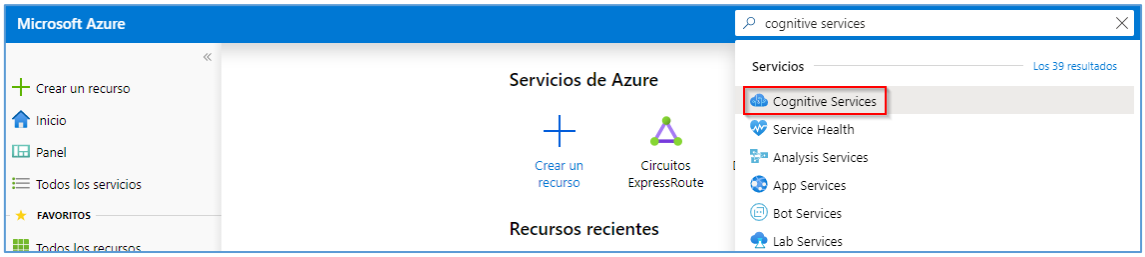
4.1.1.1 Requisitos de acceso

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]

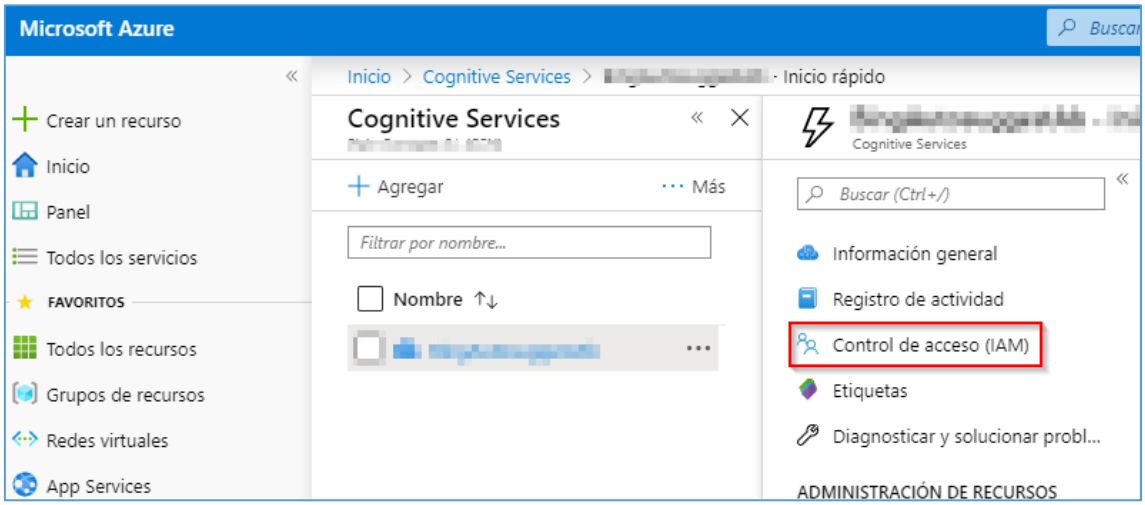
A continuación, se describen los roles que podrá asignar mediante el portal de Azure.

Lista de Roles

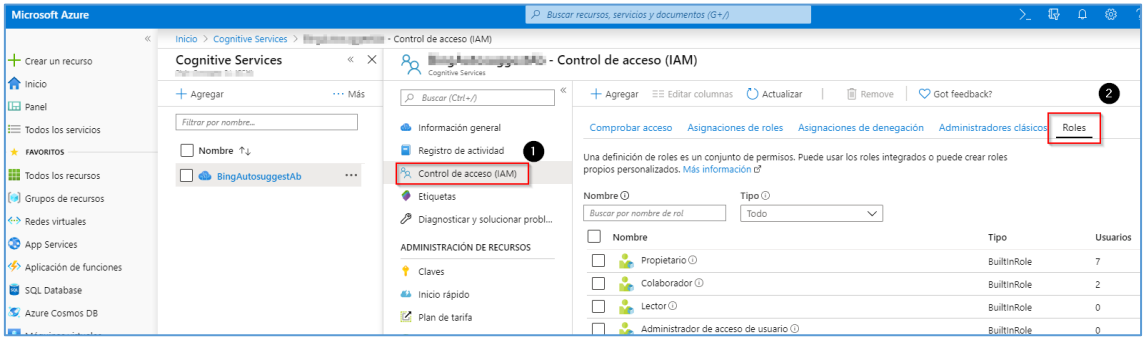
1. Desde el buscador del portal escriba Cognitive Services.



2. Pulsar en Control de acceso (IAM).



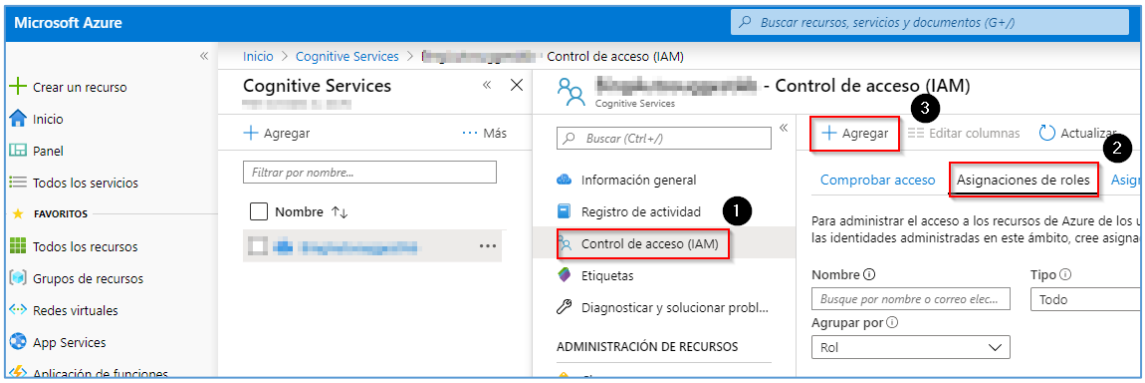
3. A continuación, en Roles.



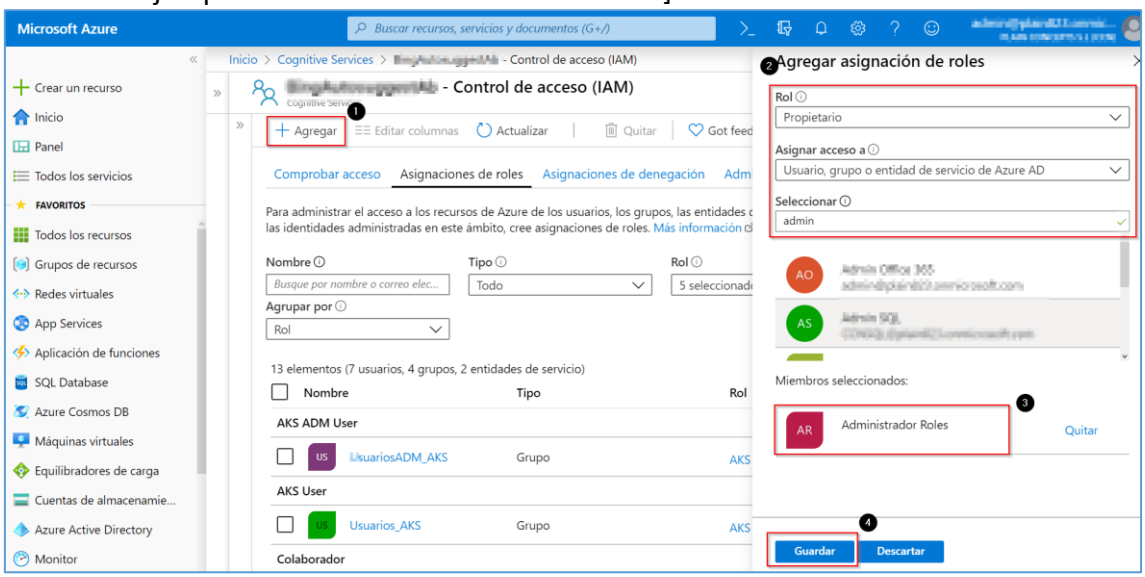
Nota: Desde aquí, podrá ver todos los roles por defecto que trae el portal cuando realiza el despliegue de una API de Cognitive services.

Asignación de Roles

1. Desde el control de acceso (IAM), pulsar en [Asignación de Roles/Agregar].



2. A continuación, debe seleccionar un [Rol que tendrá este usuario/En este caso de Ejemplo serán Administradores de Roles].



3. Por último, pulsar en Guardar.

4.1.1.2 Identificación

Al tratarse de una API de Cognitive Services, existen varios métodos de autenticación. Se recomienda que utilice de forma centralizada **Azure Active Directory.**
Puede consultar en la guía de configuración segura para Azure el [Apartado 3.1.1 Control de acceso/Identificación] donde le ayudara a utilizar este método de autenticación.

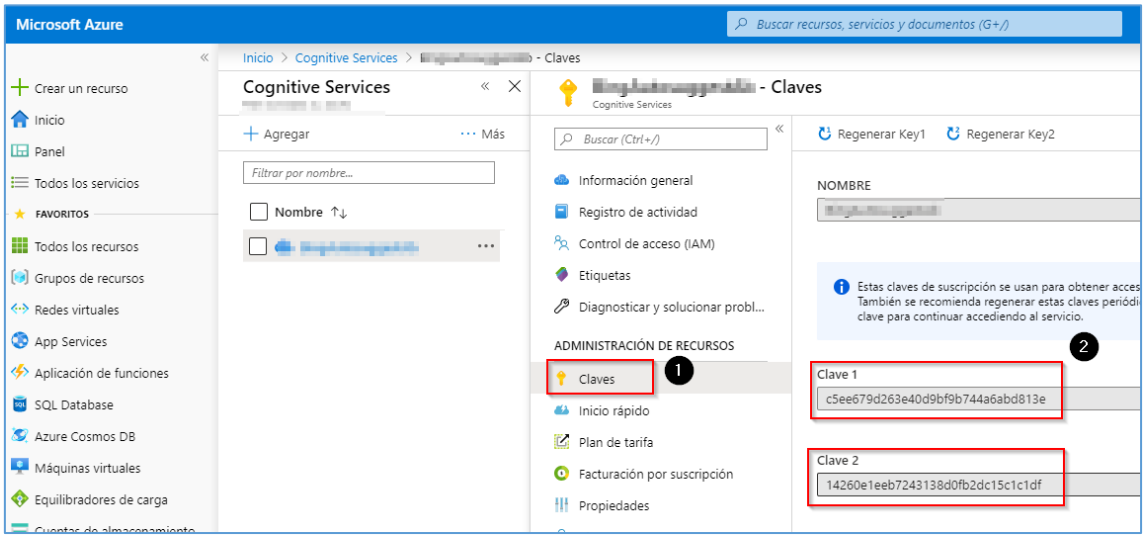
A continuación, se detallan otros métodos de autenticación que también podrá emplear.

- Autenticación con una clave de suscripción a un servicio único
- Autenticación con una clave de suscripción a varios servicios
- Autenticación con un token

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

Esta primera y la segunda es utilizando las API's claves que se proporcionan desde el portal de Azure.

Puede encontrar las claves de suscripción, desde la propria API desplegada pulsando en Claves.



El siguiente método es ***Autenticación con un token*** que puede realizarlo powershell.

Un ejemplo que se puede ejecutar:

Autorización de Token.

```
#   $FetchTokenHeader = @{
#     'Content-type'='application/x-www-form-urlencoded';
#     'Content-Length'= '0';
#     'Ocp-Apim-Subscription-Key' = 'Clave de su API'
#   }
#
#   $OAuthToken = Invoke-RestMethod -Method POST -Uri
    https://api.cognitive.microsoft.com/sts/v1.0/issueToken -Headers $FetchTokenHeader
#
#   # show the token received
#   $OAuthToken
```

Nota: Puede encontrar más información en los link https://docs.microsoft.com/en-us/azure/cognitive-services/authentication#authenticate-with-an-authentication-token https://docs.microsoft.com/en-us/azure/cognitive-services/authentication#authenticate-with-an-authentication-token

4.1.2 Explotación

4.1.2.1 Registro de la actividad de los usuarios

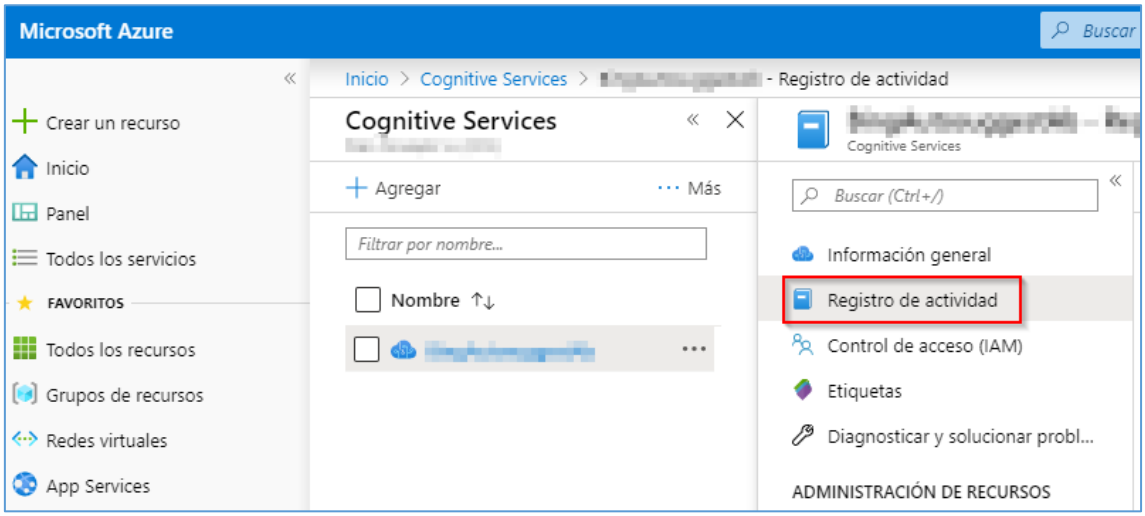
Puede consultar el registro de actividad de los usuarios desde la propia API desplegada.

Este registro de actividad le permite saber la actividad sobre los usuarios que consultan la aplicación.

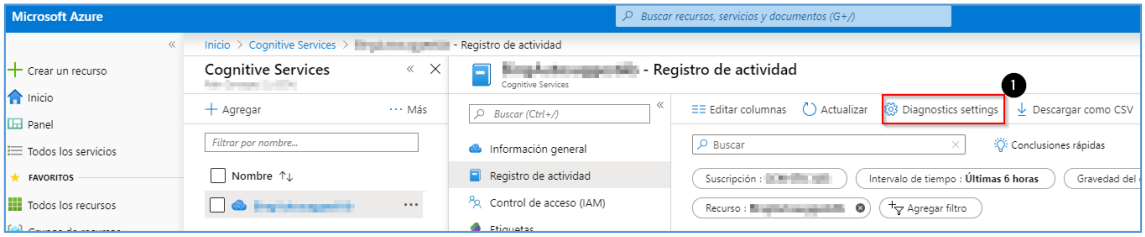
Como requisito previo, debe habilitar la configuración de diagnostico la que le permite recopilar toda la información de su aplicación.

A continuación, siga estas instrucciones.

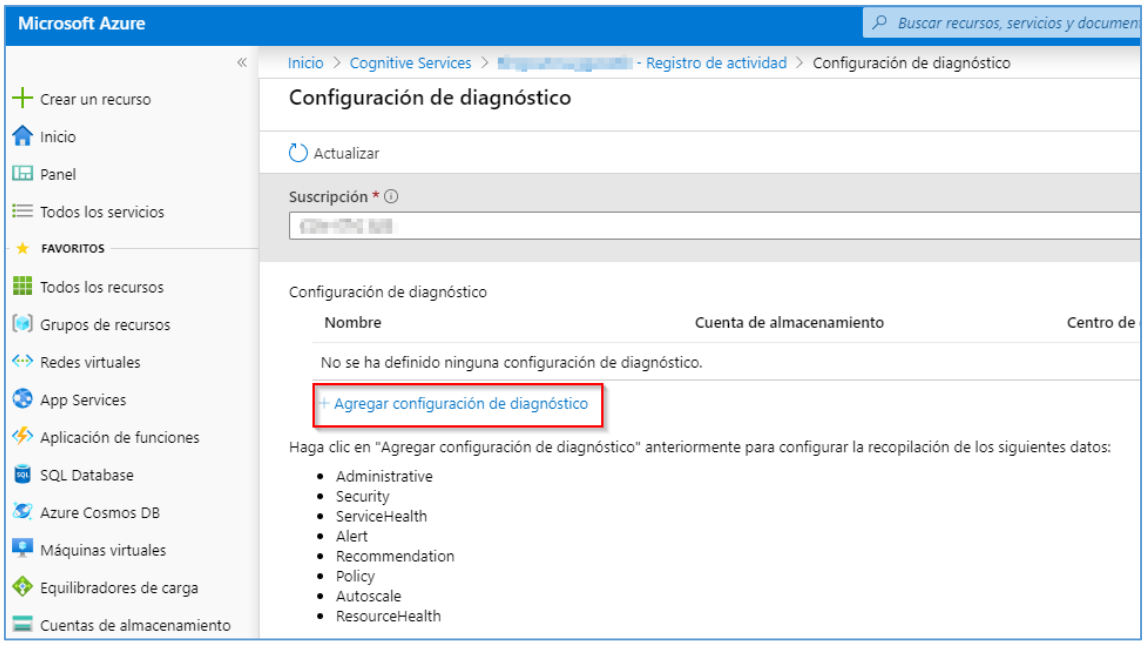
1. Pulsar en Registro de actividad.



2. Pulsar en Diagnostics Settings.

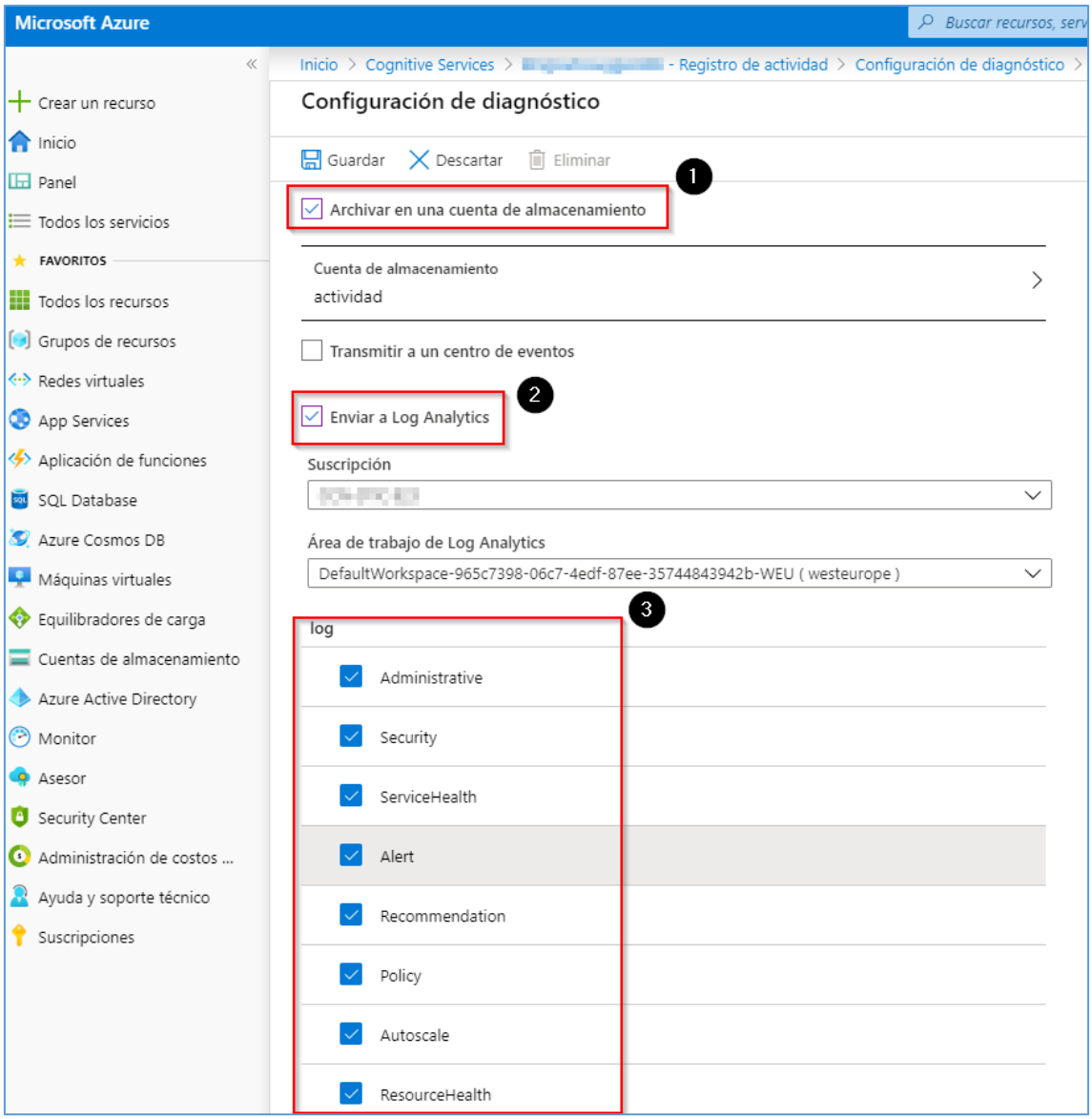


3. Pulsar en agregar configuración de diagnóstico.



Nota: El archivado de diagnóstico utiliza una cuenta de almacenamiento. Para ello, deberá consultar la guía de configuración segura para Azure [Apartado 2.3 Elementos comunes/creación de una cuenta de almacenamiento].

Además, todos estos registros se almacenan y se procesan en Log Analytics. Para ello, consulte la guía de configuración segura para Azure Apartado 3.1.6 Monitorización del sistema/Log Analytics]



4. Para finalizar, pulsar en guardar.

Registro de diagnóstico

Azure Cognitive Services cuenta con un registro de diagnóstico que proporciona un registro del estado de salud de sus aplicaciones y datos sobre el funcionamiento de los recursos y aplica una depuración en caso que se detecten problemas.

Necesitará estos requisitos previos:

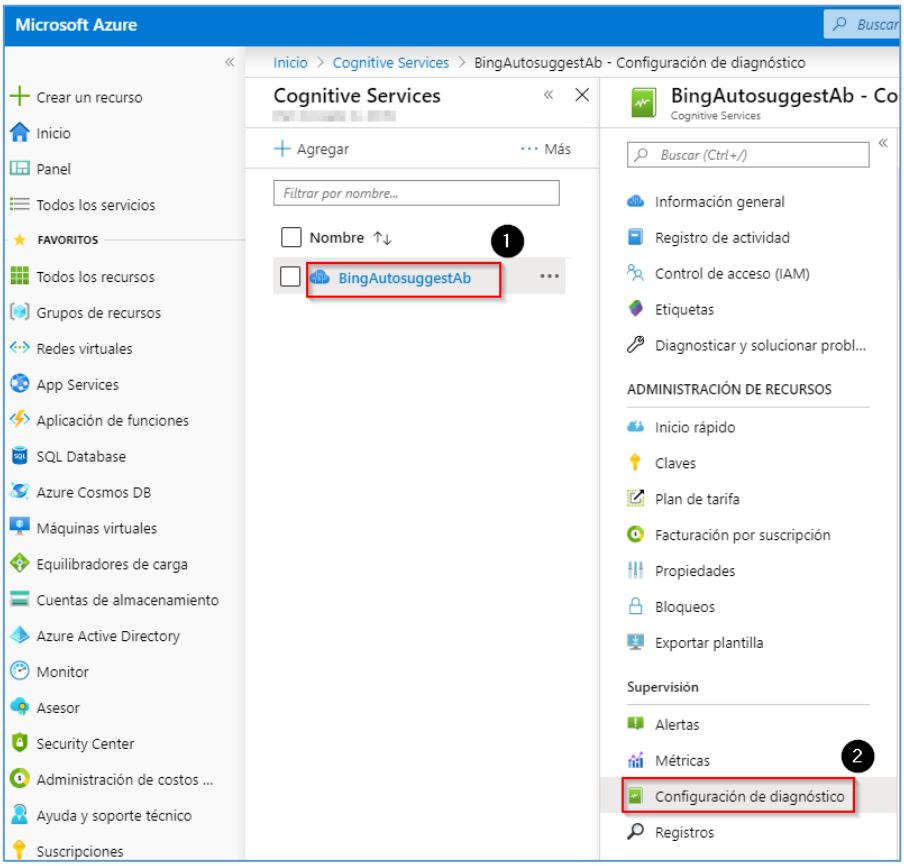
Para habilitar el registro de diagnóstico, necesitará un lugar donde almacenar los datos de registro.

Azure Storage: conserva los registros de diagnóstico para auditorías de directivas.
Nota: Para la creación de una cuenta de almacenamiento consulte la guía de configuración segura para Azure [Apartado 2.3 Elementos comunes/Creación de una cuenta de almacenamiento]

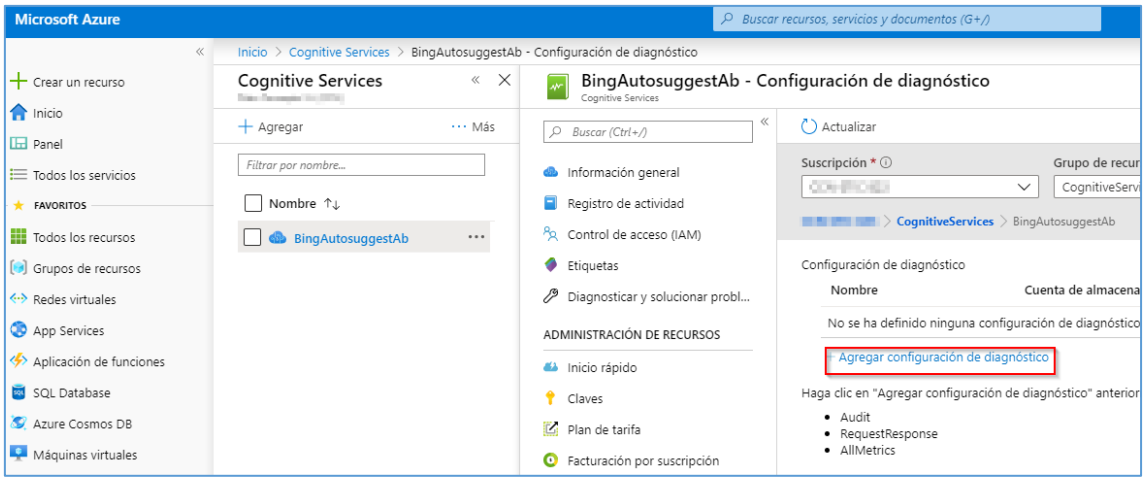
Log Analytics: una herramienta flexible de búsqueda y de análisis de registros que permite el análisis de los registros
Nota: Para habilitar Log Analtytics consulte la guía de configuración segura para Azure [Apartado 3.1.6.2 Sistemas de Métricas]

Una vez que tenga estos pre requisitos deberá seguir estas directrices:

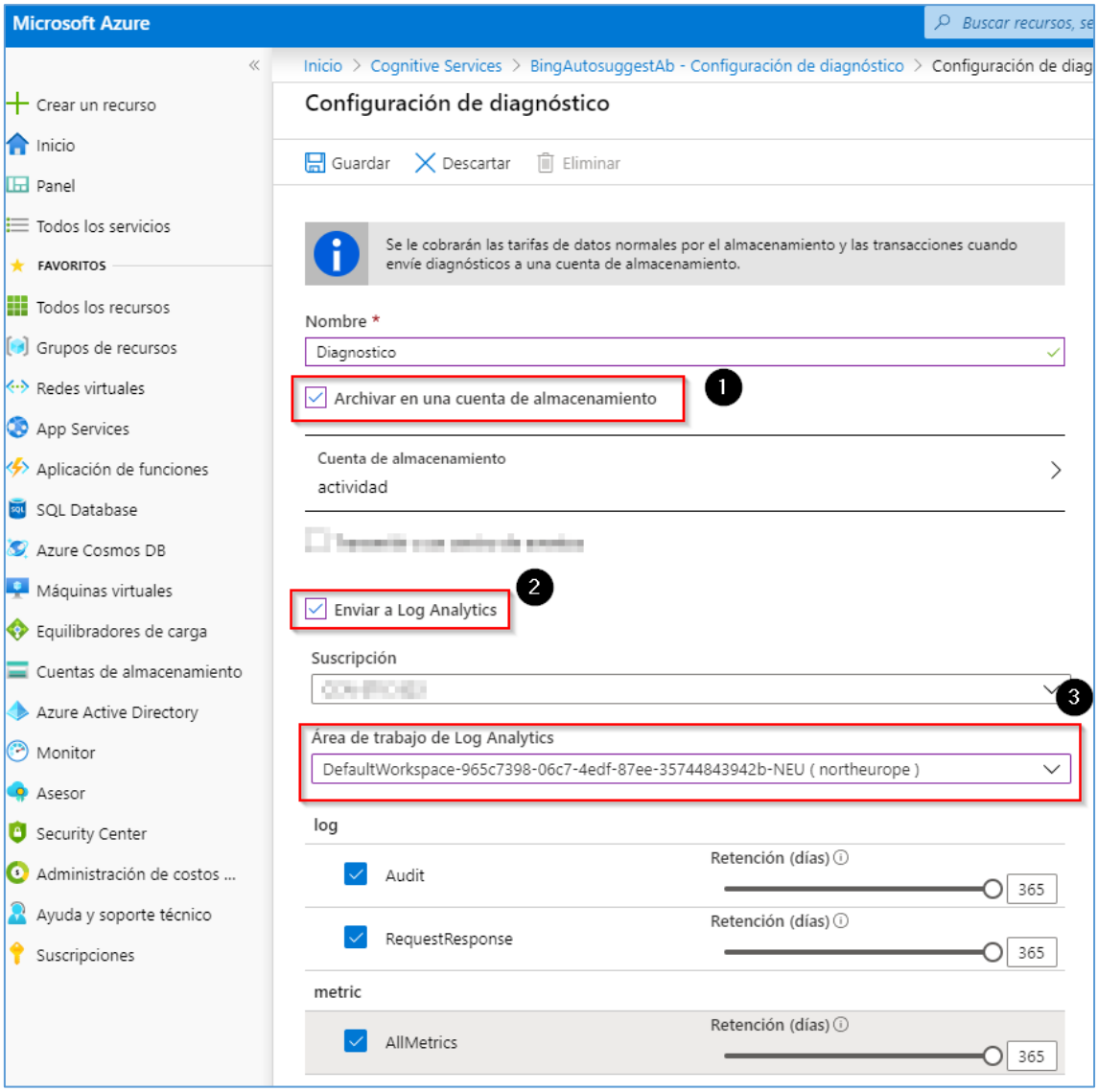
1. Acceda a Azure Portal. Busque y seleccione un recurso de [Cognitive Services/Configuración de diagnóstico].



2. Pulsar en Agregar configuración de diagnóstico.



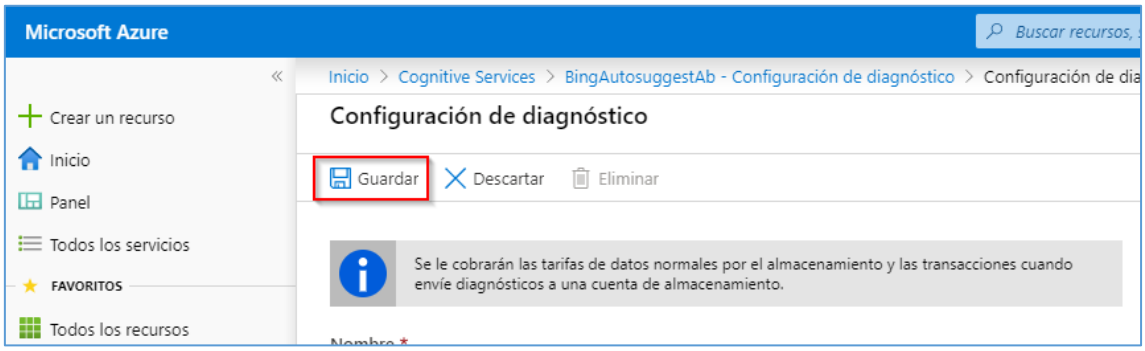
3. A continuación de describen los campos que deberá completar.



Nombre: Defina un nombre para esta configuración de diagnóstico.
Archivar en una cuenta de almacenamiento: Active la casilla y selecciones una cuenta de almacenamiento.

Enviar a Log Analytics: Active la casilla.
Área de trabajo de Log Analytics: Seleccione un área de trabajo.
Log: Active Audit, RequestResponse y AllMetrics y defina una retención de 365

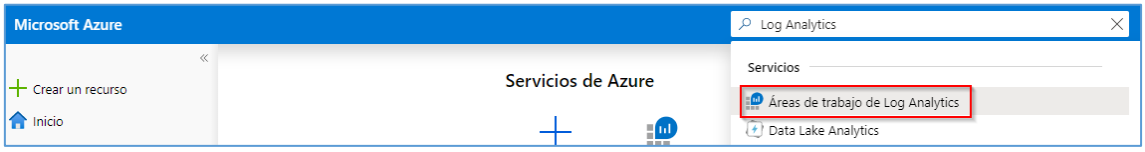
4. Por último, pulsar en guardar.



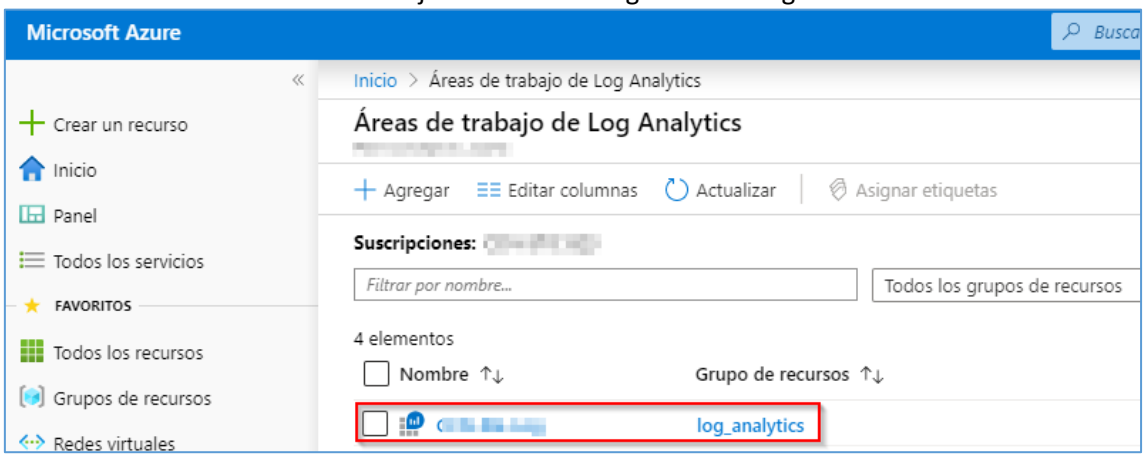
Nota: Una vez realizadas estas configuraciones podrá ver desde Log Analytics los registros y hacer consultas.

A continuación, se describen algunos ejemplos:

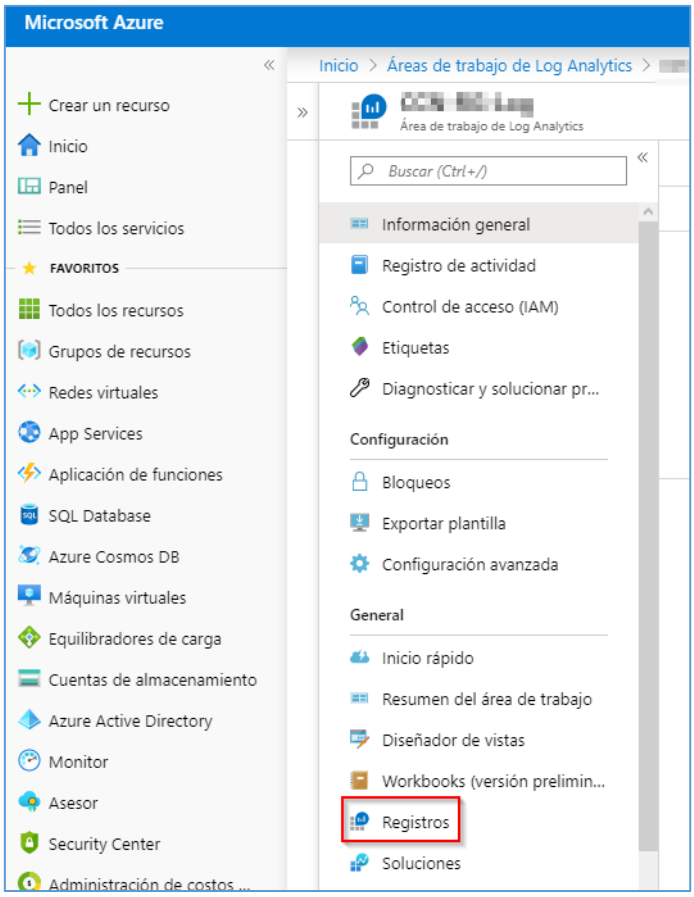
1. En Azure Portal, localice y seleccione Log Analytics en el menú de navegación izquierdo.



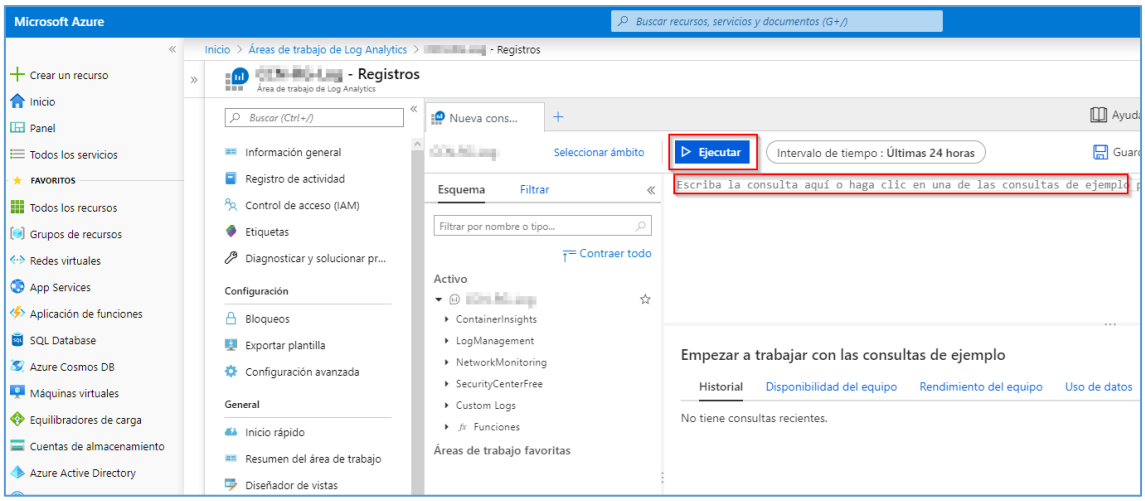
2. Seleccione el área de trabajo donde ha configurado los registros.



3. Pulsar en registros.



4. Escriba la consulta.



Algunos ejemplos que podrá consultar:

Ejecute esta consulta para todos los registros de diagnóstico de Azure Cognitive Services durante el período de tiempo especificado:

Kusto

```
#   AzureDiagnostics
#   | where ResourceProvider == "MICROSOFT.COGNITIVESERVICES"
```

Ejecute esta consulta para ver los 10 registros más recientes:

```
#   AzureDiagnostics
#   | where ResourceProvider == "MICROSOFT.COGNITIVESERVICES"
#   | take 10
```

Ejecute esta consulta para agrupar las operaciones por recurso:

```
#   AzureDiagnostics
#   | where ResourceProvider == "MICROSOFT.COGNITIVESERVICES" |
#   summarize count() by Resource
```

Ejecute esta consulta para buscar el promedio de tiempo que se tarda en realizar una operación:

```
#   AzureDiagnostics
#   | where ResourceProvider == "MICROSOFT.COGNITIVESERVICES"
#   | summarize avg(DurationMs)
#   by OperationName
```

Ejecute esta consulta para ver el volumen de operaciones a lo largo del tiempo dividido por el nombre de la operación con recuentos agrupados por decenas.

```
#   AzureDiagnostics
#   | where ResourceProvider == "MICROSOFT.COGNITIVESERVICES"
#   | summarize count()
#   by bin(TimeGenerated, 10s), OperationName
#   | render areachart kind=unstacked
```

Podrá consultar métricas y registros de diagnóstico de Azure Storage desde el link https://docs.microsoft.com/es-es/azure/storage/blobs/storage-quickstart-blobs-dotnet#download-blobs

Podrá consultar Descripción de las búsquedas de registros en los registros de Azure Monitor desde el link https://docs.microsoft.com/es-es/azure/azure-monitor/log-query/log-query-overview

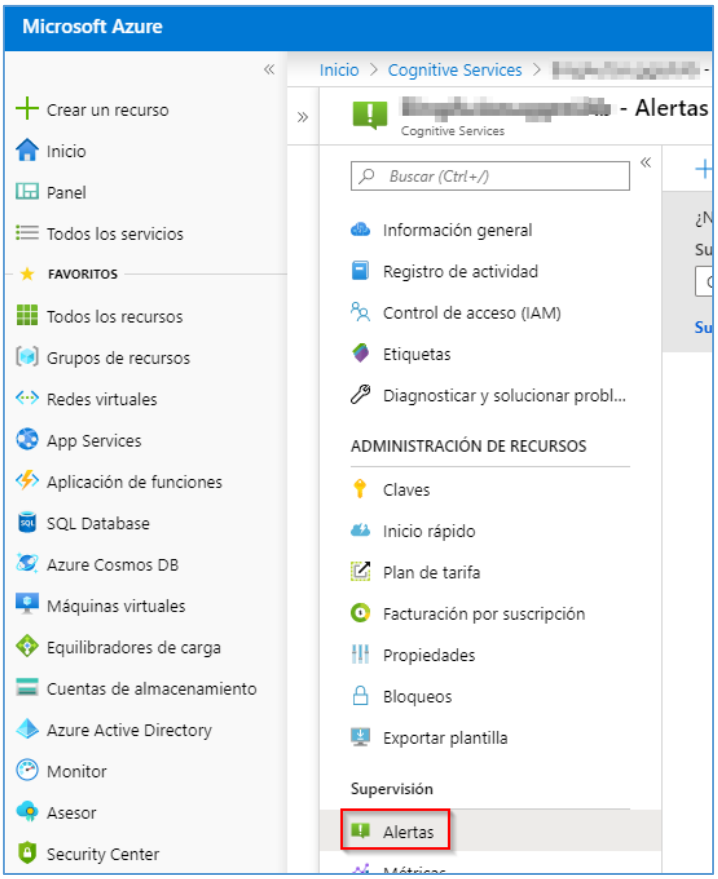
4.1.2.2 Monitorización del sistema

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

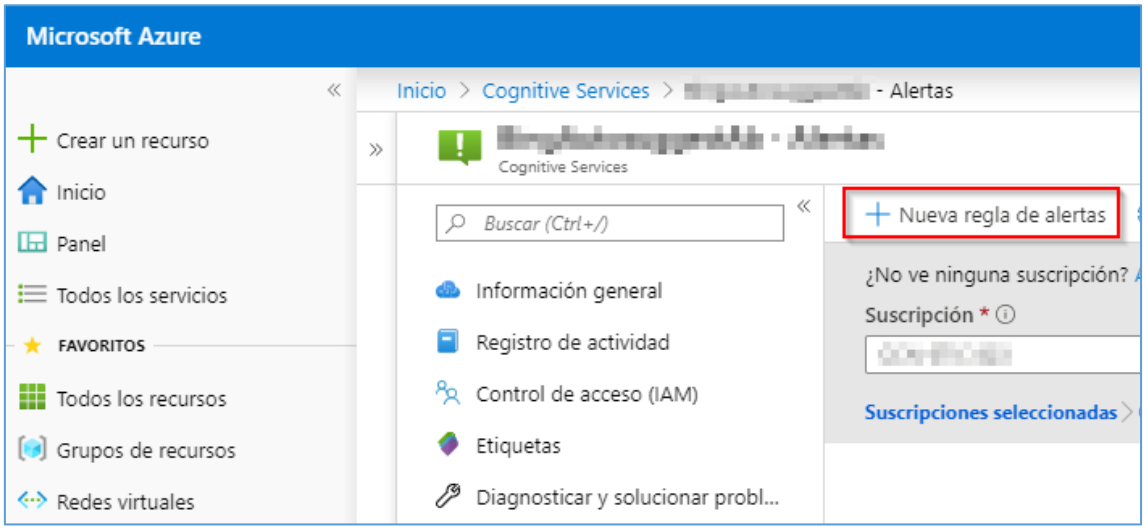
A continuación, siga las instrucciones para la creación de Alertas.

Personalización de Alertas

1. Desde la API pulsar en Alertas.

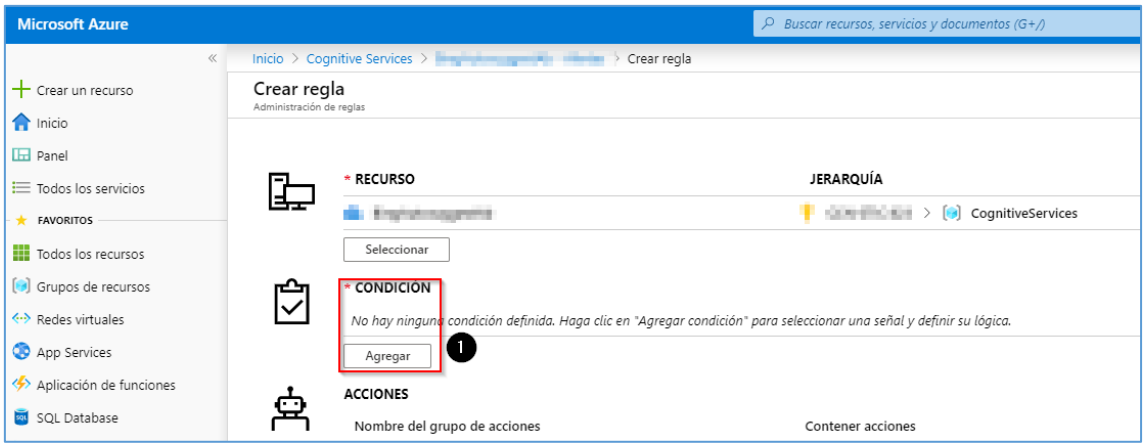


2. Pulsar en nueva regla de alertas.



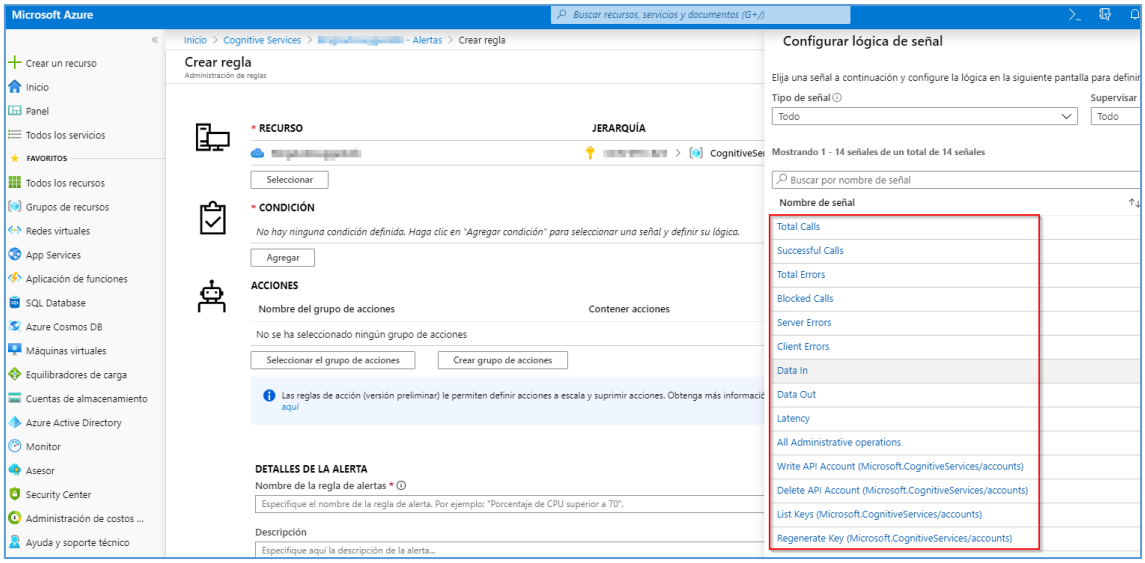
Nota: En este asistente deberá definir una condición y una acción.

3. Pulsar en Agregar.

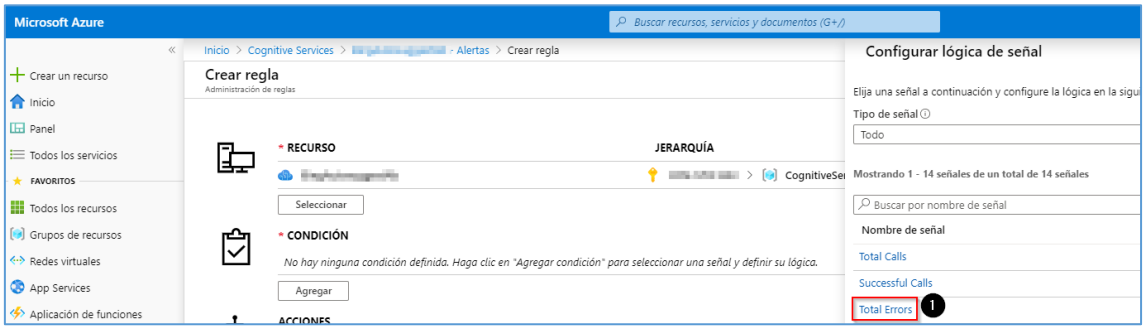


Nota: Podrá definir distintos tipos de métricas.

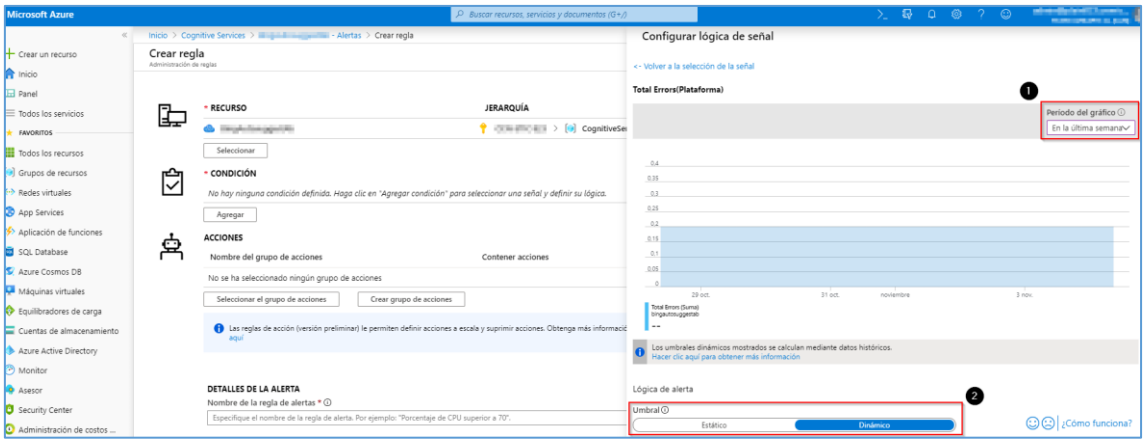
Algunos Ejemplos:



En este ejemplo definiremos Total Errors.



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



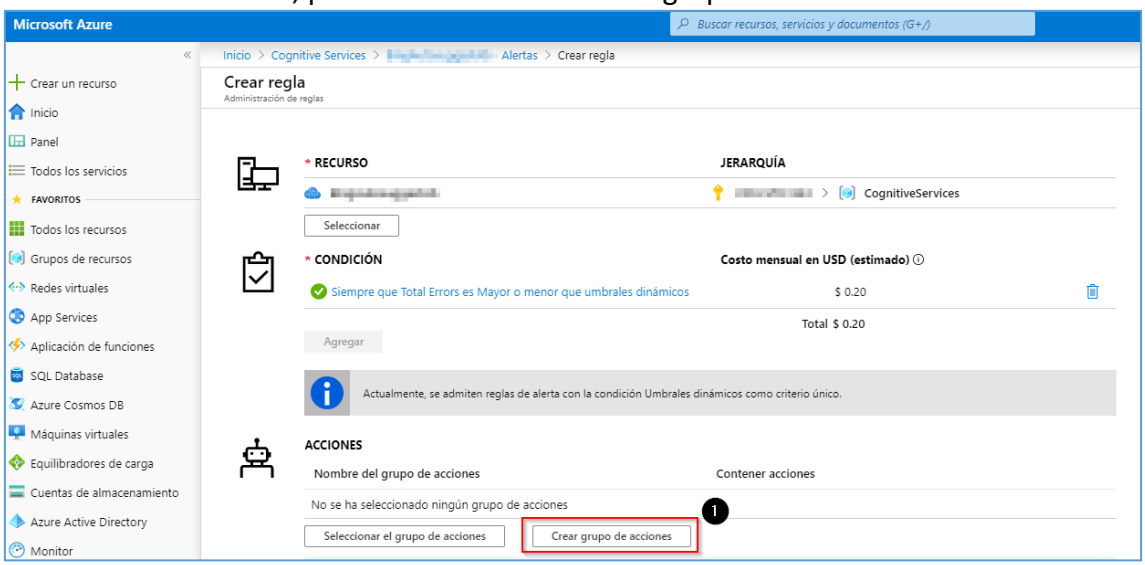
Lógica de Alerta.

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.

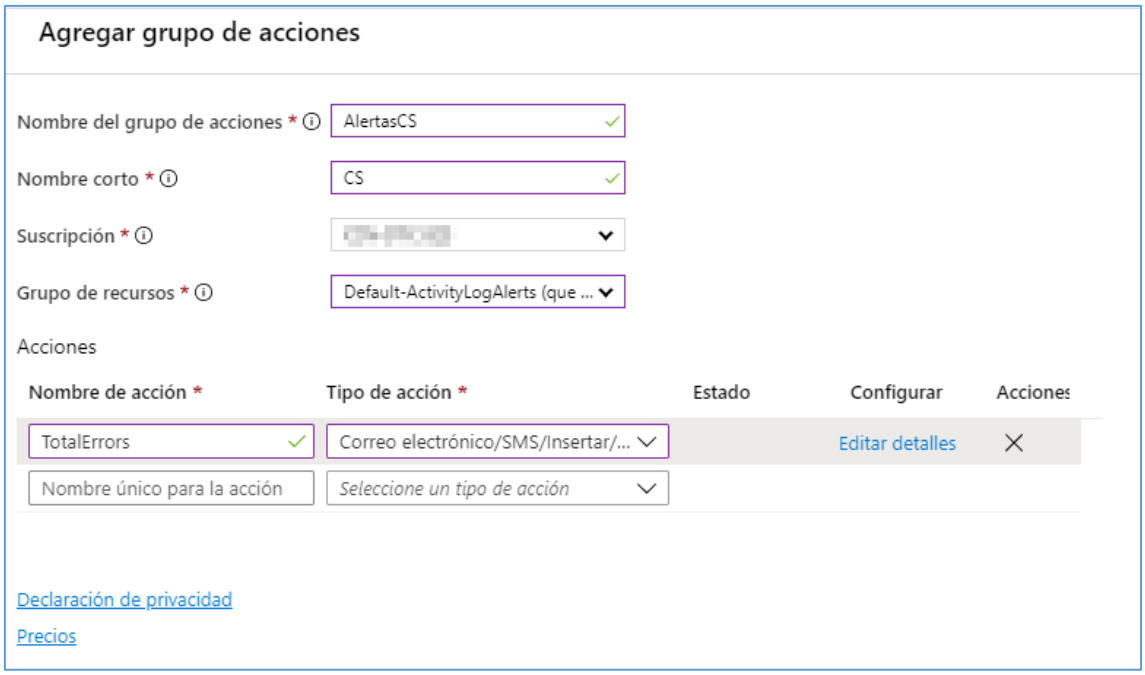
Podrá encontrar más información en el link: https://docs.microsoft.com/es-es/azure/azure-monitor/platform/alerts-dynamic-thresholds

4. Una vez definido el Umbral, pulsaren Listo.

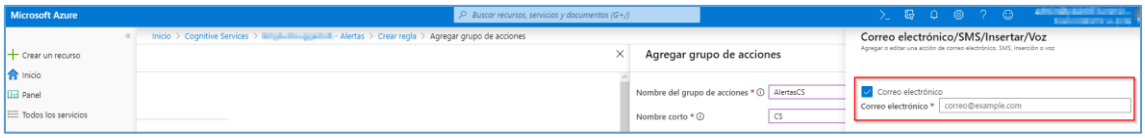
5. A continuación, pulsar en seleccionar crear grupo de acciones.



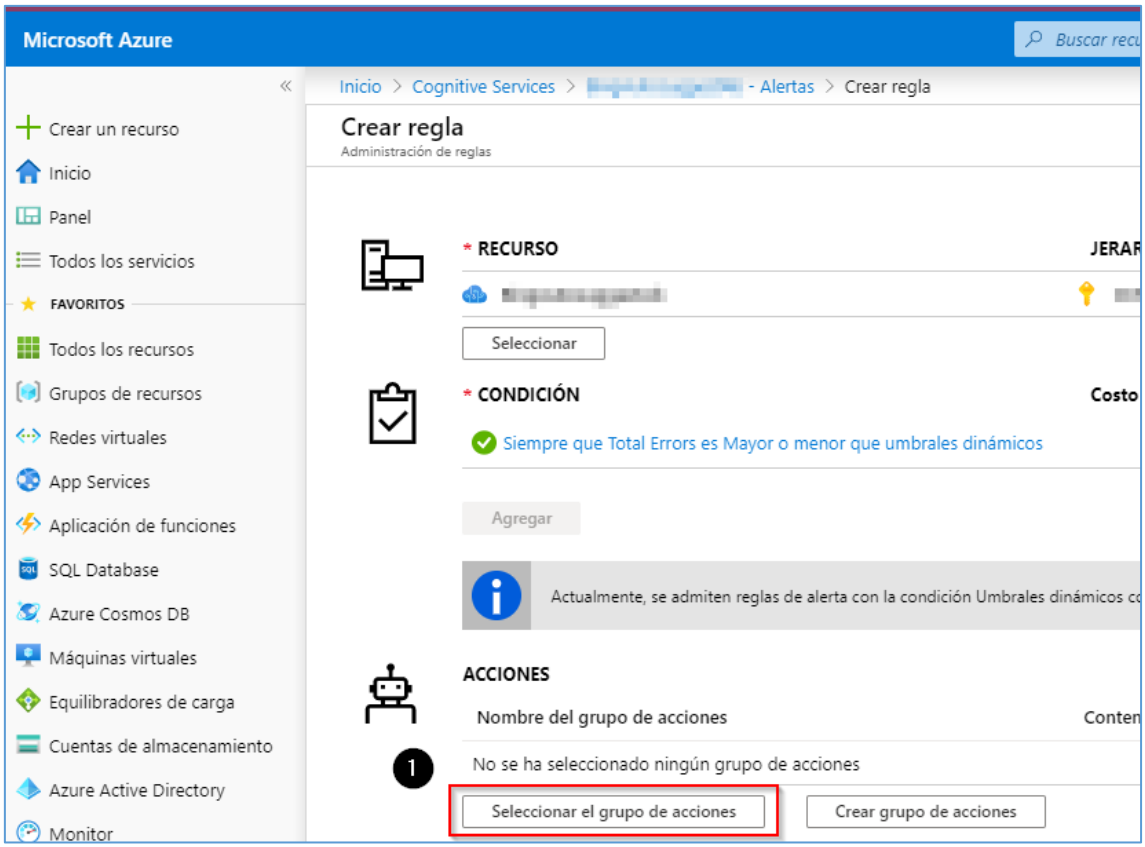
6. Deberá completar los siguientes campos.



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 enviar esta alerta. En este caso seleccionamos Correo Electrónico. Al elegir esta opción deberá rellenar estos campos.



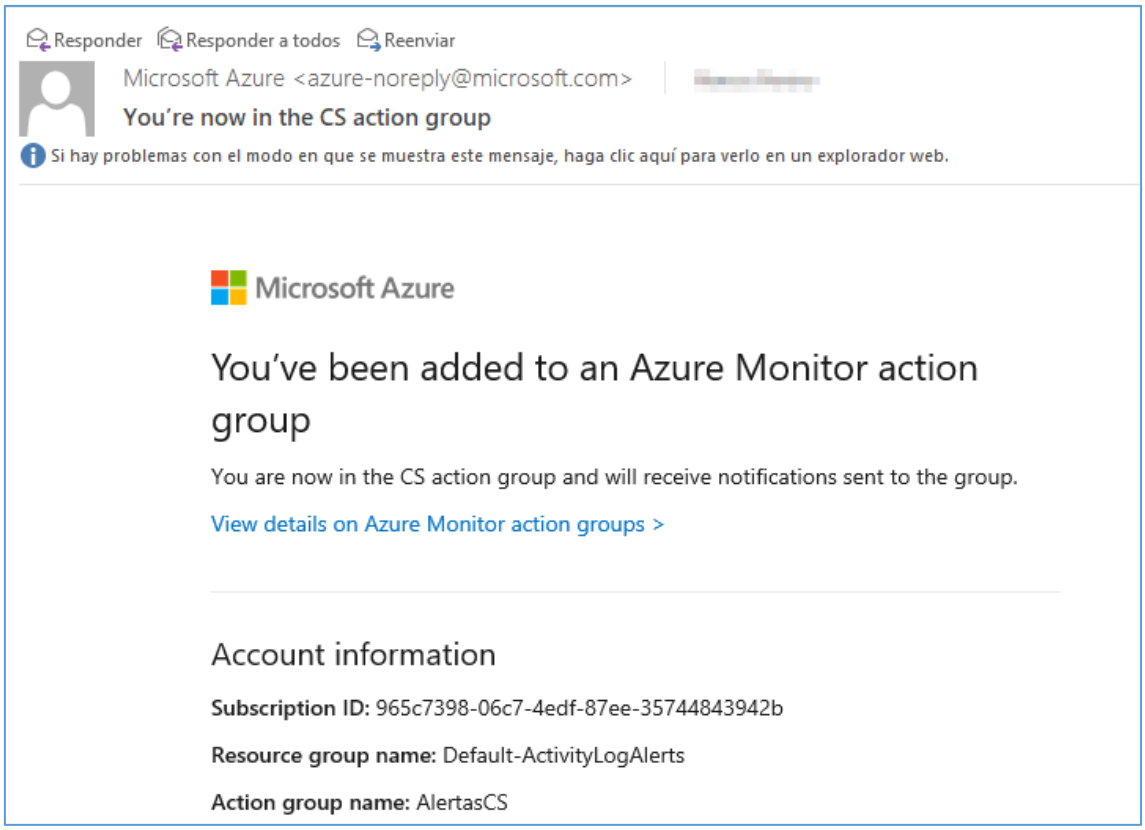
7. Una vez agregada la dirección de correo electrónico, pulsar en crear.
8. A continuación, pulsar en Seleccionar grupo de acciones.



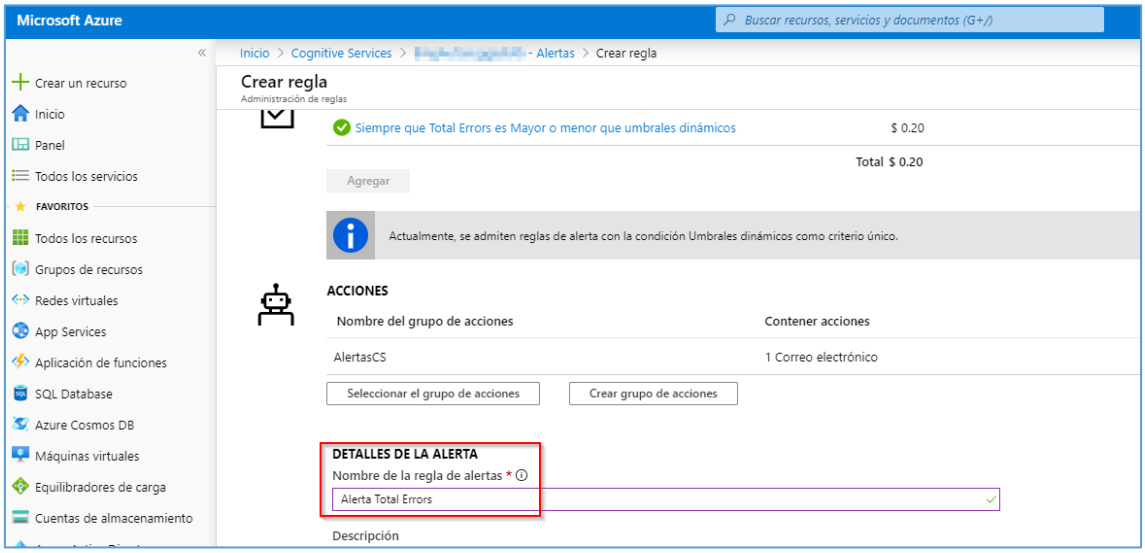
9. Pulsar en el nuevo grupo de acciones.

10. Pulsar en seleccionar.

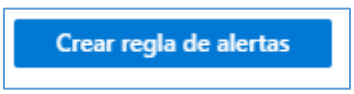
Nota: Le llegara un correo con la activación.



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



12. Pulsar en Crear regla de alerta.



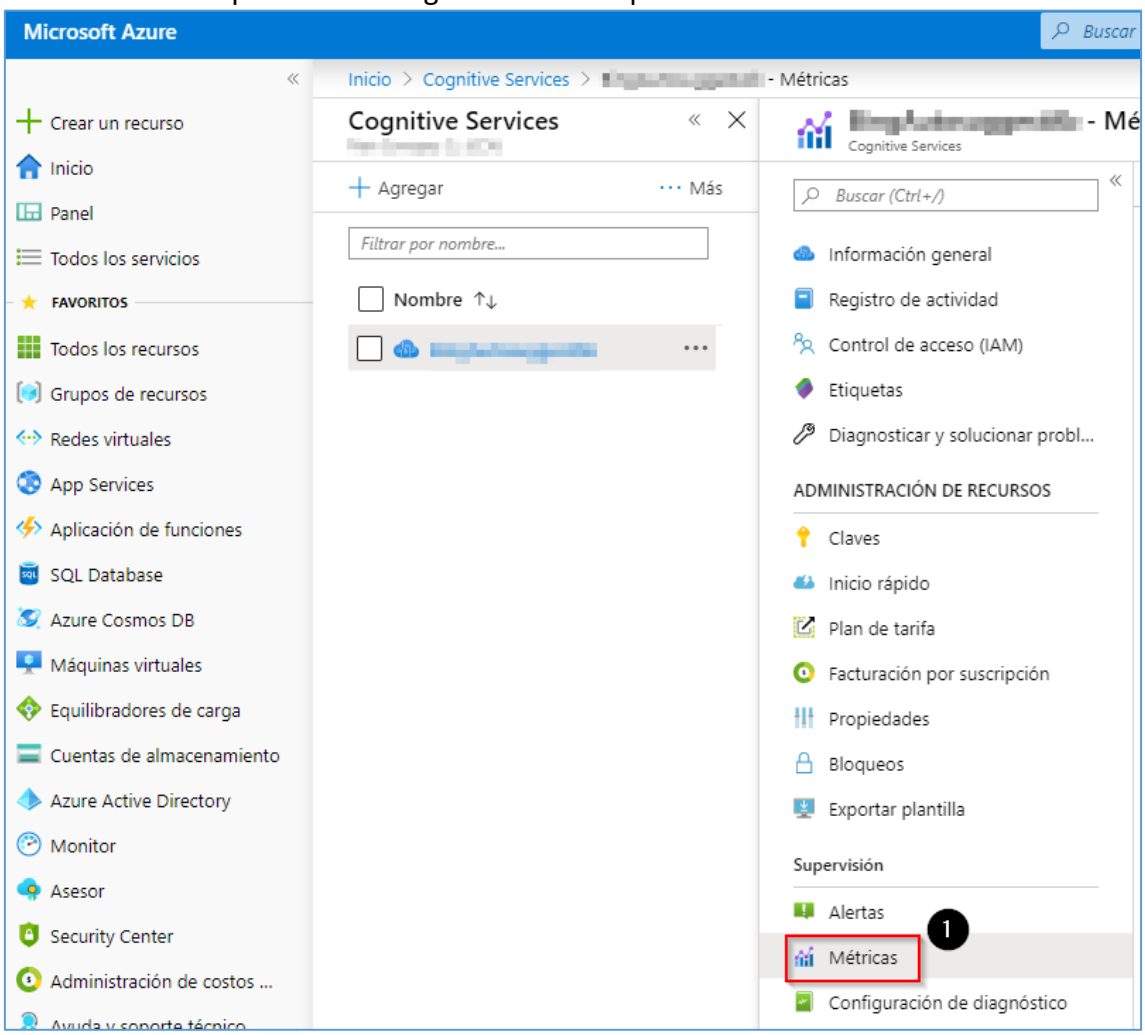
Nota: Recuerde que estas alertas están asociadas Azure monitor. Consultar la guía de configuración segura para Azure [Apartado 3.1.6 Monitorización de sistema]

Personalización de Métricas

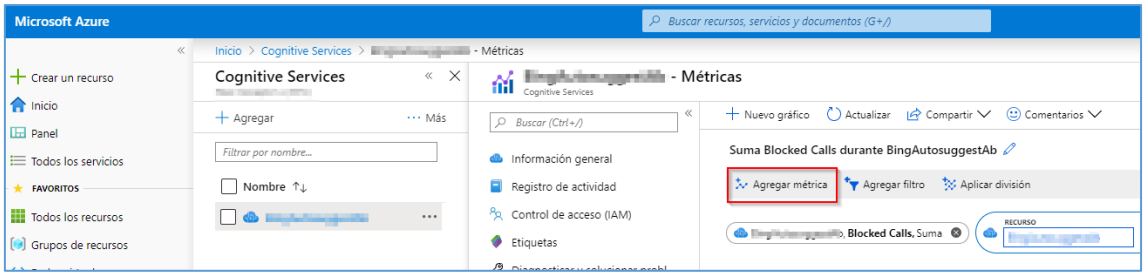
El explorador de métricas de Azure Monitor es un componente de Azure que permite trazar los gráficos, correlacionar visualmente.
Podrá configurar métricas personalizadas desde cualquier recurso que tenga en Azure.

Para ello, siga estas instrucciones:

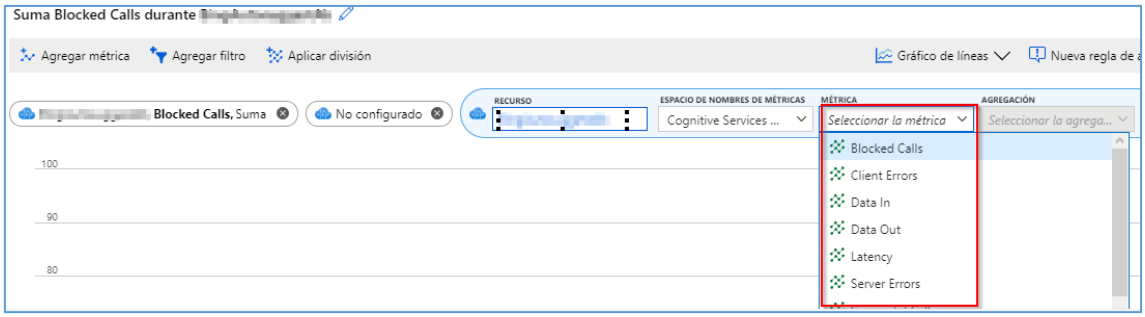
1. Desde la aplicación de cognitive services pulse en Métricas.



2. Pulsar en Agregar métrica.



3. Seleccione el tipo de métrica.



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

5. GLOSARIO Y ABREVIATURAS

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

Término	Definición
AAD	*Azure Active Directory (Directorio Activo de Azure).*
APP SERVICES	*Azure App Service le permite crear y hospedar aplicaciones web, back-ends móviles y API RESTful en el lenguaje de programación que prefiera sin tener que administrar la infraestructura.*
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.*
Azure AD	*Azure Active Directory.*
RBAC	*RBAC es un sistema de autorización basado en Azure Resource Manager que proporciona administración de acceso específico a los recursos de Azure.*
KUSTO	*Kusto es un servicio para almacenar y ejecutar análisis interactivos sobre macrodatos.* *Se basa en sistemas de administración de bases de datos relacionales, admite entidades como bases de datos, tablas y columnas, y además proporciona operadores de consulta de análisis complejos (como columnas calculadas, búsqueda y filtrado por filas, agrupar por agregados o uniones).*
ENS	*Esquema Nacional de Seguridad.*
TOKEN	*Los tokens de acceso permiten a los clientes llamar a las API protegidas por Azure de forma segura. Los tokens de acceso de la Plataforma de identidad de Microsoft son JWT, objetos JSON codificados en Base64 firmados por Azure.*
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.

6. 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 Azure Active directory para la administración del Tenant y la generación de claves.	**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 para todas las cuentas que operan en cognitive services.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No

		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
op.exp	**Explotacion**		
op.exp.8	**Registro de la actividad de los usuarios**		
	Se ha comprobado que el registro de Auditoría está activado y capturando eventos. Además, se ha utilizado las consultas recomendadas 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 cognitive services y la generación de métricas.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas:	**Observaciones:**

		☐ Si ☐ No	