centro criptológico nacional

Guía de Seguridad de las TIC

CCN-STIC 884E

Guía de configuración segura para Microsoft Sentinel

Mayo 2024

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

cpage.mpr.gob.e

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2024.05.23 11:46:23 +02'00'

Pº de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2024

NIPO: 083-24-182-5
Fecha de Edición: mayo de 2024

LIMITACIÓN DE RESPONSABILIDAD
El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL
Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1. GUIA SEGURA PARA MICROSOFT SENTINEL 4

1.1 DESCRIPCIÓN DEL USO DE ESTA GUÍA 4

1.2 DEFINICIÓN DEL SERVICIO 4

1.3 PROTECCIÓN DEL PUESTO DE TRABAJO 5

1.3.1 CONEXIÓN A MICROSOFT DEFENDER XDR 6

1.4 FUNCIONALIDADES DEL SERVICIO MICROSOFT SENTINEL 13

1.5 PRERREQUISITOS 14

1.6 LICENCIAMIENTO Y PRECIOS 14

2. DESPLIEGUE SEGURO PARA MICROSOFT SENTINEL 15

2.1 ACCESO AL PORTAL AZURE DESDE UN NAVEGADOR 15

2.2 CONFIGURACIÓN DEL SERVICIO MICROSOFT SENTINEL 27

2.2.1 CONECTAR LOS ORÍGENES DE DATOS 35

3. CONFIGURACIÓN SEGURA PARA MICROSOFT SENTINEL 68

3.1 MARCO OPERACIONAL 68

3.1.1 CONTROL DE ACCESO 68

3.1.2 EXPLOTACIÓN 75

3.1.3 MONITORIZACIÓN DEL SISTEMA 85

3.2 MEDIDAS DE PROTECCIÓN 92

3.2.1 PROTECCIÓN DE LAS COMUNICACIONES 92

3.2.2 PROTECCIÓN DE LA INFORMACIÓN 95

3.2.3 PROTECCIÓN DE LOS SERVICIOS 97

4. GLOSARIO Y ABREVIATURAS 100

5. CUADRO RESUMEN DE MEDIDAS DE SEGURIDAD 102

1. GUIA SEGURA PARA MICROSOFT SENTINEL

1.1 DESCRIPCIÓN DEL USO DE ESTA GUÍA

El objetivo de la presente guía es indicar los pasos a seguir para la configuración y despliegue de Microsoft Sentinel cumpliendo con los requisitos del Esquema Nacional de Seguridad.

1.2 DEFINICIÓN DEL SERVICIO

Microsoft Sentinel es una solución de administración de eventos de información de seguridad (*Security Information and Event Management* SIEM) y respuesta automatizada de orquestación de seguridad (*Security Orchestration*, *Automation and Response* SOAR) que es escalable y nativa de la nube. Microsoft Sentinel ofrece un análisis de seguridad inteligente e integra inteligencia frente a amenazas en toda la organización. De esta forma se proporciona una única solución para la detección de ataques, visibilidad de amenazas, búsquedas proactivas y respuestas contra amenazas. Microsoft Sentinel es un SIEM cloud diseñado para integrar eventos y señales procedentes de la nube y del entorno local (on premise).

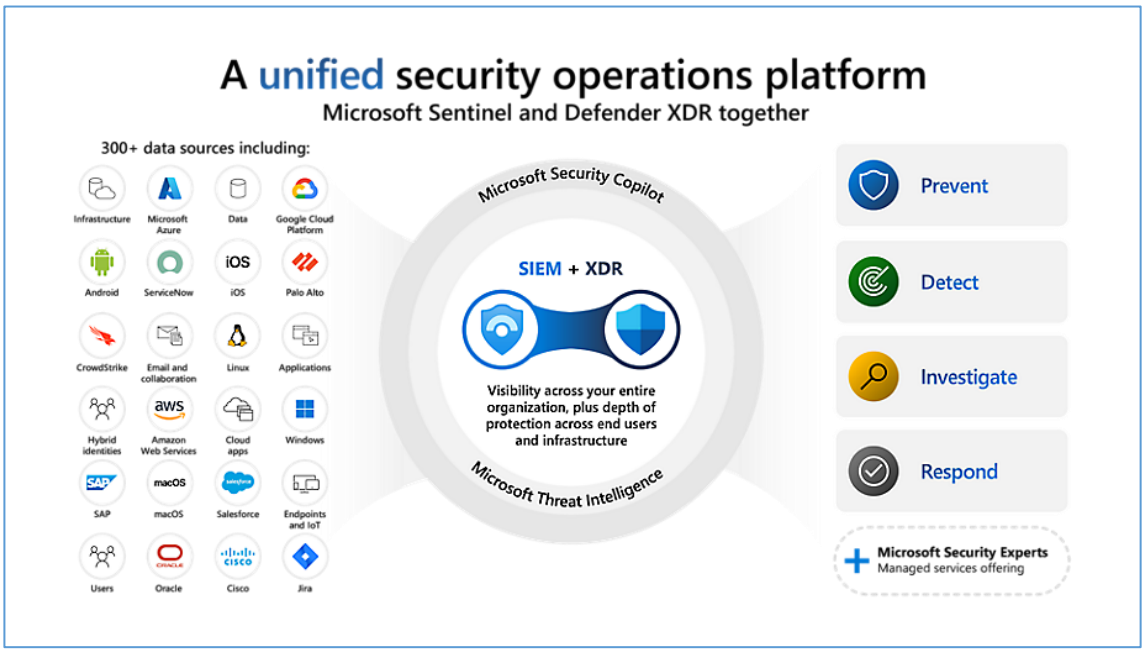
Microsoft Sentinel se integra con los productos de seguridad de Microsoft Defender XDR, Microsoft Defender for Cloud y otras fuentes de terceros para unificar la recopilación y análisis de logs en un único servicio. Se detalla e informa de otro producto en el apartado de protección de puesto de trabajo, como es Microsoft Defender XDR, siendo un servicio diferente a Microsoft Sentinel.

1.3 PROTECCIÓN DEL PUESTO DE TRABAJO

Microsoft cuenta con la suite de seguridad integrada ***Microsoft Defender XDR*** para la protección del puesto de trabajo.

Microsoft Defender XDR es un conjunto de servicios unificado de defensa empresarial previa y posterior a la vulneración que coordina de forma nativa la detección, prevención, investigación y respuesta entre extremos, identidades, correo electrónico y aplicaciones para proporcionar protección integrada contra ataques sofisticados.

Con la solución Microsoft Defender XDR integrada, los profesionales de seguridad pueden relacionar las señales de amenaza que cada uno de estos productos recibe y determinar el alcance completo y el impacto de la amenaza; cómo entró en el entorno, lo que está afectado y cómo está afectando actualmente a la organización. Microsoft Defender XDR realiza acciones automáticas para evitar o detener el ataque y recuperar automáticamente los buzones, puntos de conexión e identidades de usuario afectados.



El conjunto de servicios de *Microsoft Defender XDR* protege:

- **Endpoints** con ***Microsoft Defender for Endpoint***: Microsoft Defender for Endpoint es una plataforma de extremo unificada para la protección preventiva, la detección posterior a la infracción, la investigación automatizada y la respuesta.
- **Correo electrónico y colaboración** con ***Microsoft Defender for Office 365***: Defender para Office 365 protege su organización contra las amenazas malintencionadas que suponen los mensajes de correo electrónico, los vínculos (URL) y las herramientas de colaboración.

- **Identidades** con ***Microsoft Defender for Identity*** y ***Microsoft Entra ID Protection***: Microsoft Defender para identidad usa señales de Active Directory para identificar, detectar e investigar amenazas avanzadas, identidades comprometidas y acciones malintencionadas dirigidas contra una organización.
- **Aplicaciones** con seguridad de ***Microsoft Defender for Cloud Apps***: Es una solución de seguridad que protege las aplicaciones de software como servicio (SaaS) y los datos que se almacenan en la nube. Ofrece funcionalidades fundamentales de un Cloud Access Security Broker (CASB), gestión de la postura de seguridad de SaaS, protección de información, protección contra amenazas y protección entre aplicaciones.

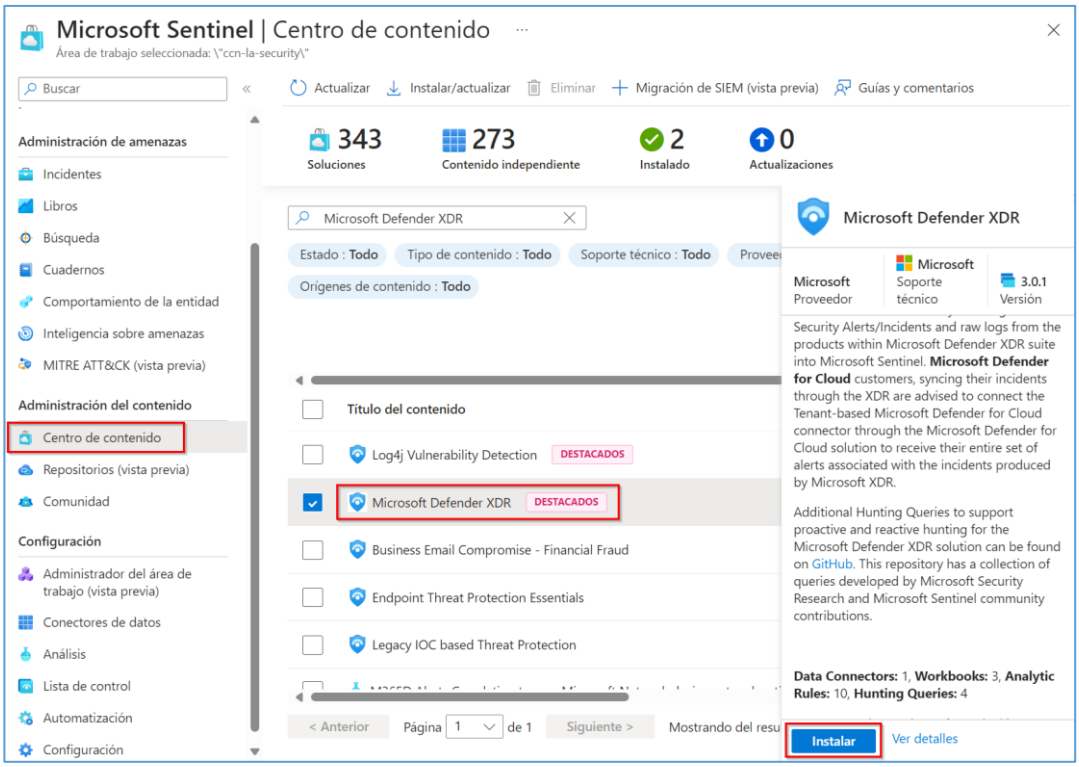
Microsoft Sentinel es una solución de seguridad que proporciona detección avanzada, investigación y respuesta automatizada a amenazas en el entorno corporativo. En esencia, es un Sistema de Gestión de Información y Eventos de Seguridad (SIEM) y Automatización de Orquestación, Análisis y Respuesta de Seguridad (SOAR) basado en la nube.

1.3.1 CONEXIÓN A MICROSOFT DEFENDER XDR

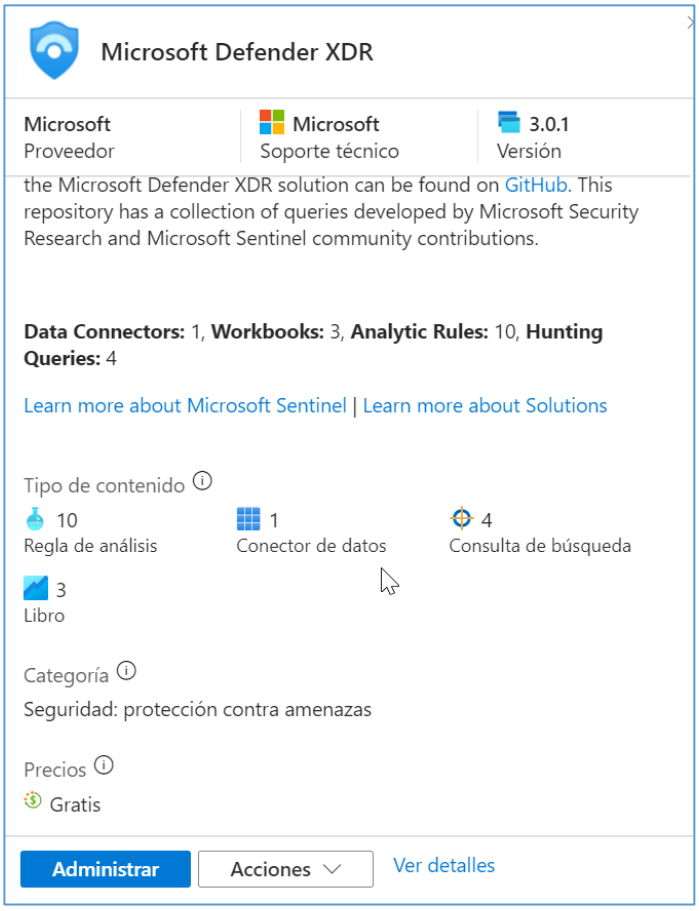
El conector **Microsoft Defender XDR** de Microsoft Sentinel permite alimentar alertas e incidentes de seguridad de la suite Microsoft Defender XDR a Microsoft Sentinel y mantiene los incidentes sincronizados de manera segura entre ambos portales. Los incidentes de Microsoft Defender XDR incluyen todas sus alertas, entidades y otra información relevante, y se completan y agrupan las alertas de los otros servicios de Microsoft Defender XDR como *Microsoft Defender for Endpoint*, *Microsoft Defender for Identity*, *Microsoft Defender for Office 365* y *Microsoft Defender for Cloud Apps*.

Conexión a Microsoft Defender XDR

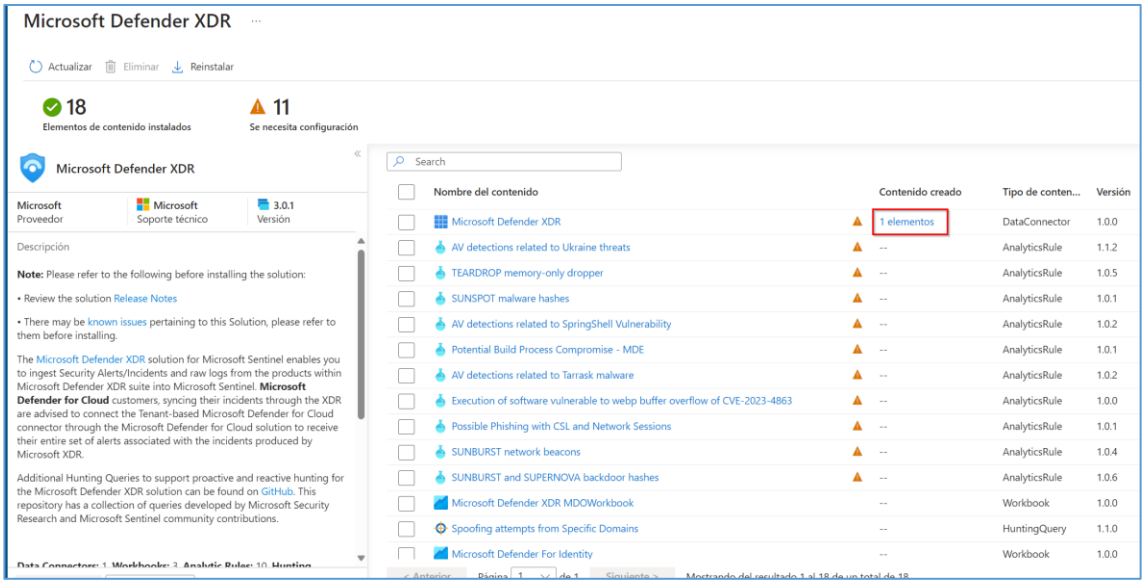
1. En Microsoft Sentinel, seleccionar *Content Hub* (Centro de contenido), elegir Microsoft Defender XDR en la galería y seleccionar Instalar.



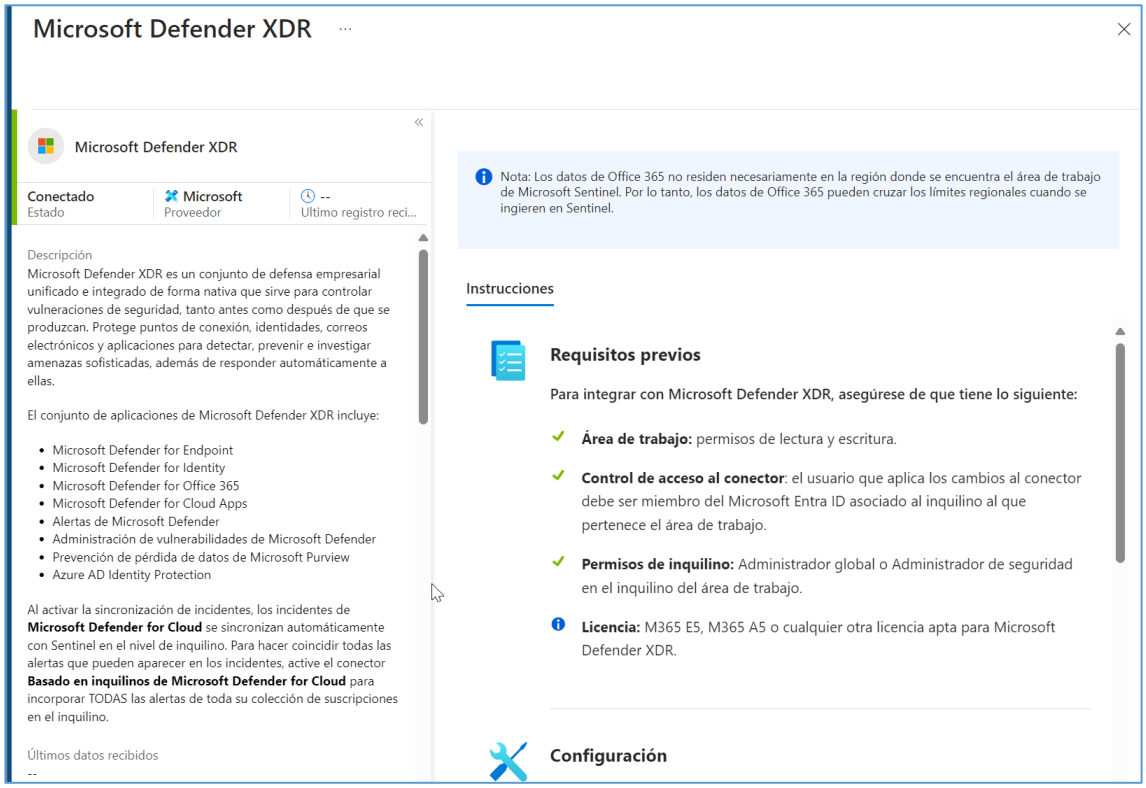
2. Una vez instalada la solución se debe configurar el conector, para ello se pulsará Administrar.



3. A continuación, se accede a los elementos instalados:

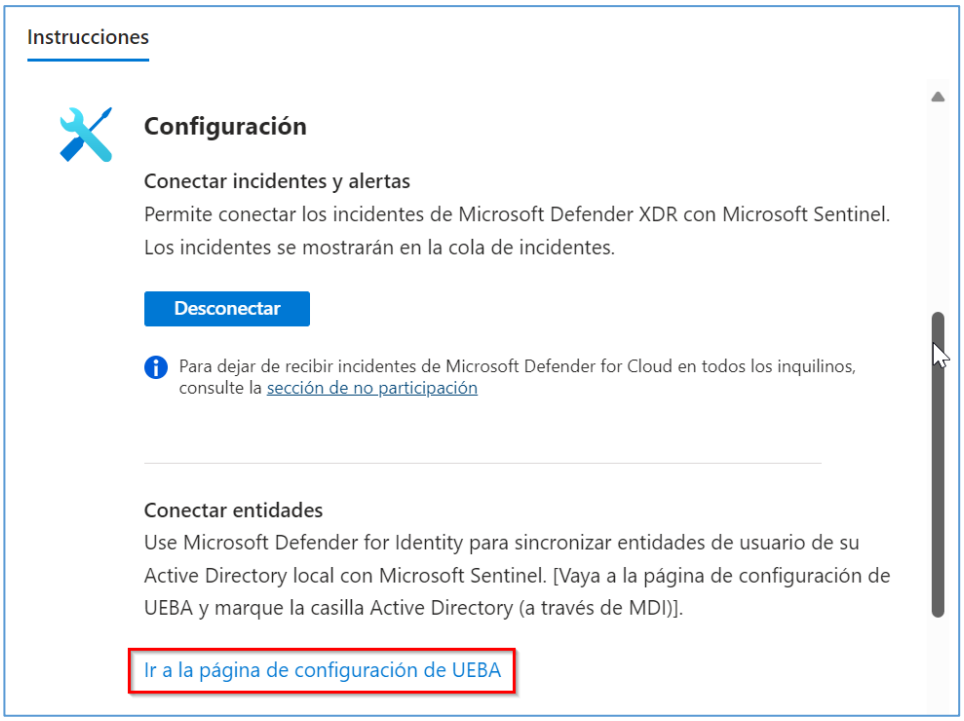


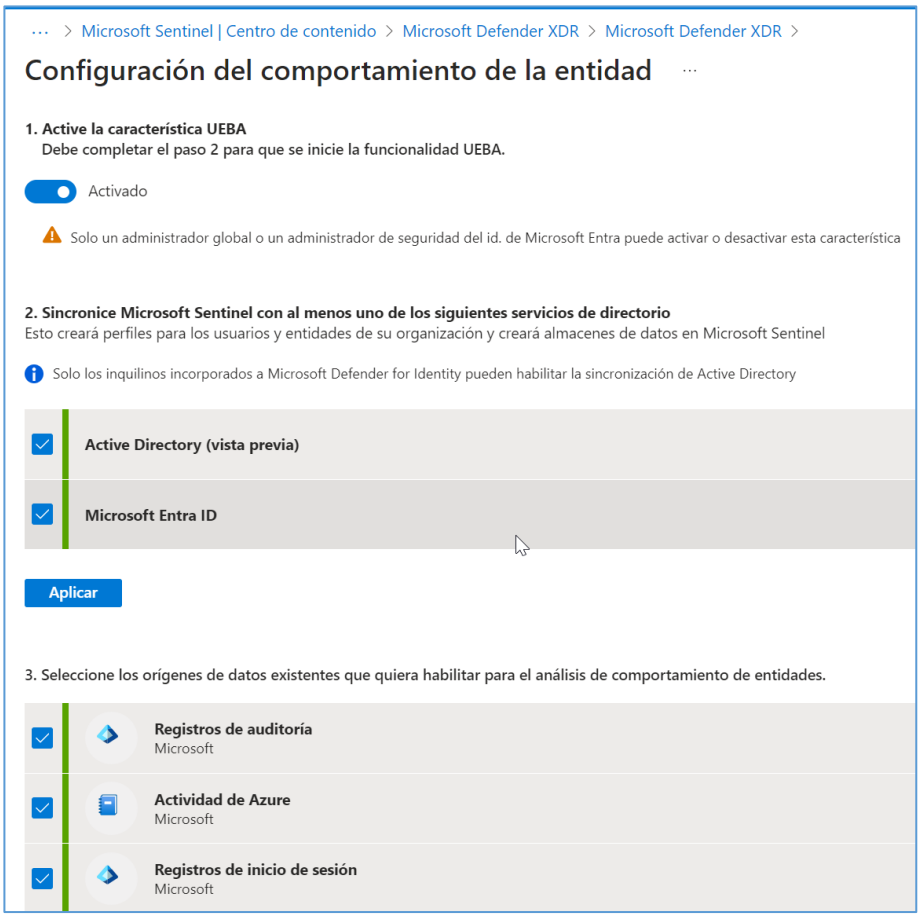
4. Se abre la configuración del conector seleccionando el tipo DataConector:



5. Se recomienda habilitar la configuración de UEBA (User and Event Behavioral Analytics). Utiliza el aprendizaje automático y el aprendizaje profundo para modelar el comportamiento de los usuarios y dispositivos en las redes corporativas. UEBA puede identificar comportamientos anómalos de los empleados o grupos de empleados, lo que podría indicar actividades deshonestas o intentos de robo de datos utilizando su propio acceso. Puede analizar el comportamiento de las cuentas, y alertar sobre posibles cuentas comprometidas

antes de que se produzcan daños significativos, además de, detectar ataques de fuerza bruta, detectar cambios en permisos y creación de usuarios con privilegios y detectar violación de datos protegidos.

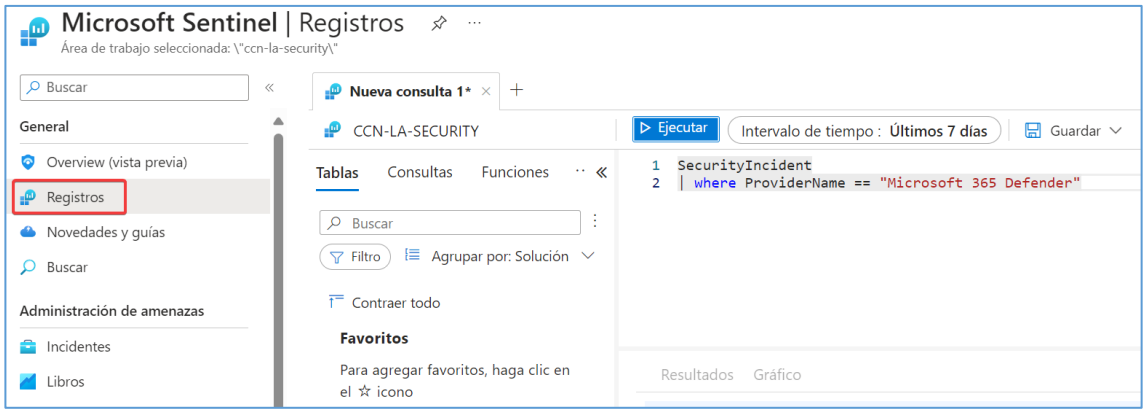




6. Por último, se deben conectar todas las fuentes de la suite de Defender que estén activas en el tenant:

7. Para consultar los datos de incidentes de Microsoft Defender XDR, puede usarse la siguiente sentencia de KQL en la ventana de consulta:

```
SecurityIncident
| where ProviderName == "Microsoft 365 Defender"
```



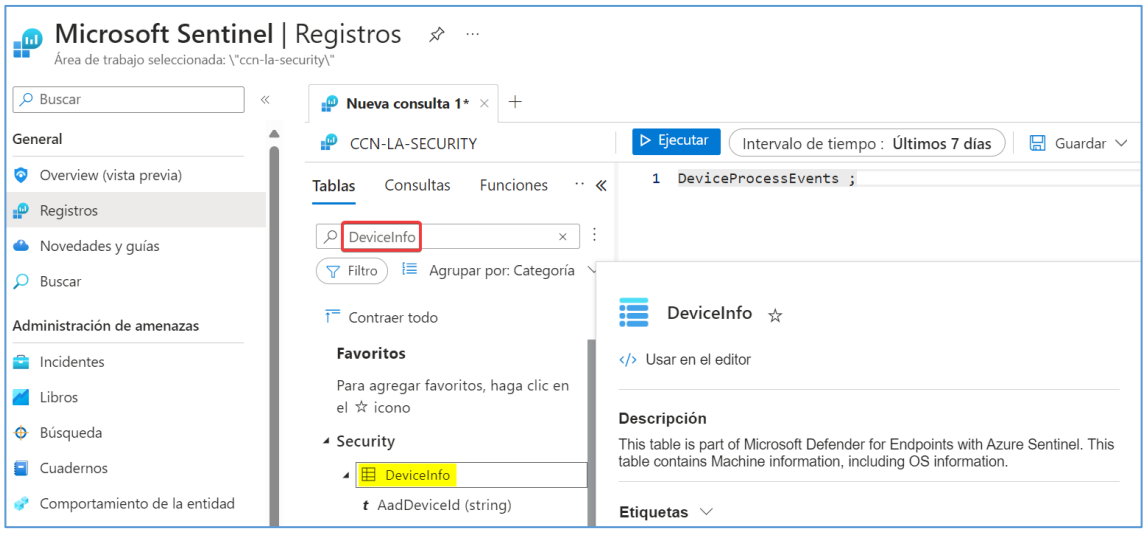
8. Para recopilar eventos de búsqueda avanzada de *Microsoft Defender for Endpoint*, se pueden recopilar los siguientes tipos de eventos de sus tablas de búsqueda avanzada correspondientes.

   a. Marcar las casillas de las tablas con los tipos de evento que se quiera recopilar:

Nombre de la tabla	Tipo de eventos
DeviceInfo	Información del equipo (incluida la información del sistema operativo)
DeviceNetworkInfo	Propiedades de red de dispositivos, incluyendo adaptadores físicos, direcciones IP y MAC, así como redes y dominios conectados
DeviceProcessEvents	Creación de procesos y eventos relacionados
DeviceNetworkEvents	Conexión de red y eventos relacionados
DeviceFileEvents	Creación y modificación de archivos, y otros eventos del sistema de archivos
DeviceRegistryEvents	Creación y modificación de entradas del Registro
DeviceLogonEvents	Inicios de sesión y otros eventos de autenticación en dispositivos
DeviceImageLoadEvents	Eventos de carga de DLL
DeviceEvents	Varios tipos de eventos
DeviceFileCertificateInfo	Información de certificado de archivos firmados

   b. Hacer clic en Aplicar cambios.

   c. Para consultar las tablas de búsqueda avanzada en Log Analytics, escribir el nombre de la tabla de la lista anterior en la ventana de consulta.

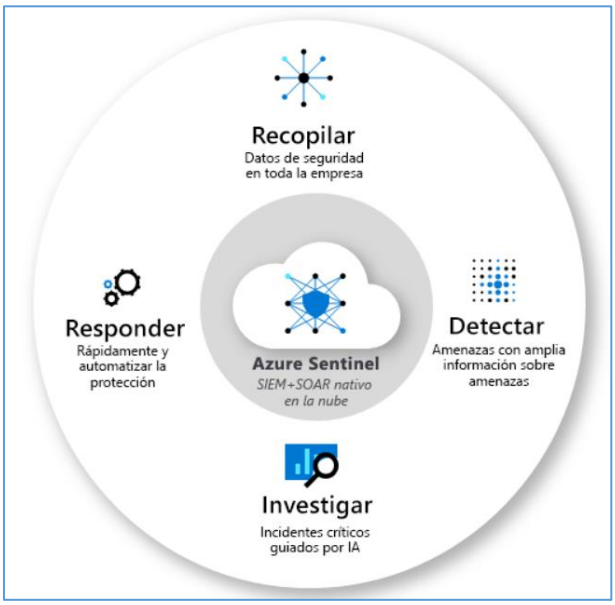


* Más información sobre agregación de conectores en el apartado [2.2 Configuración del servicio Microsoft Sentinel].

1.4 FUNCIONALIDADES DEL SERVICIO MICROSOFT SENTINEL

Microsoft Sentinel permite obtener una vista general de toda la empresa, lo que suaviza la tensión provocada por ataques cada vez más sofisticados, volúmenes de alertas cada vez mayores y plazos de resolución largos.

- Recopila datos a escala de nube de todos los usuarios, dispositivos, aplicaciones y de toda la infraestructura, tanto en el entorno local como en diversas nubes.
- Detecta amenazas que antes no se detectaban y minimiza los falsos positivos mediante el análisis y la inteligencia frente a amenazas sin precedentes de Microsoft.
- Investiga amenazas con inteligencia artificial y busca actividades sospechosas a escala, aprovechando el trabajo de ciberseguridad que ha llevado a cabo Microsoft durante décadas.
- Responde a los incidentes con rapidez con la orquestación y la automatización de tareas comunes integradas.



Creado sobre la gama completa de servicios de Azure existentes, Microsoft Sentinel incorpora de forma nativa bases contrastadas, como Log Analytics y Logic Apps.

Microsoft Sentinel enriquece la investigación y la detección con IA al proporcionar el servicio de inteligencia frente a amenazas de Microsoft y permite aportar su propia inteligencia frente a amenazas.

Microsoft Sentinel se asienta sobre la base del área de trabajo de Log Analytics. La disponibilidad de Microsoft Sentinel depende del SLA de Log Analytics. Para un Área de Trabajo de Log Analytics determinada, Microsoft garantiza que la disponibilidad de consulta no será inferior al 99,9 %, exceptuando el modelo free que proporciona Log Analytics de Azure que no incorpora un SLA.

1.5 PRERREQUISITOS

Para poder habilitar Microsoft Sentinel antes se deben comprobar los siguientes requisitos:

- Suscripción activa de Azure.
- Área de trabajo de Log Analytics. Un área de trabajo de Log Analytics es un entorno único destinado a la recogida logs.
- Para habilitar Microsoft Sentinel, se necesita permisos de colaborador en la suscripción en la que reside el área de trabajo de Microsoft Sentinel.
- Para usar Microsoft Sentinel, se necesita permisos de colaborador o lector de Microsoft Sentinel en el grupo de recursos al que pertenece el área de trabajo.
- Para instalar o administrar soluciones en el centro de contenido, se necesita el rol Colaborador de Microsoft Sentinel en el grupo de recursos al que pertenece el área de trabajo.
- Microsoft Sentinel es un servicio de pago. Para más información sobre precios, consultar el siguiente punto de este documento.

1.6 LICENCIAMIENTO Y PRECIOS

Microsoft Sentinel no necesita una licencia específica. Sí será necesario asegurarse de que se disponen de las licencias necesarias para los servicios que van a suministrar los datos que se quieran conectar con Microsoft Sentinel. Por ejemplo, para exportar los datos de Entra ID, se necesitará una licencia Microsoft Entra ID P1, P2 o Governance. Por este motivo, como mínimo, es aconsejable una licencia Microsoft 365 E3 la cual ya incluye Microsoft Entra ID P1.

Microsoft Sentinel se puede habilitar sin coste adicional en un área de trabajo de Log Analytics durante los primeros 31 días. Si el uso se prolonga más de 31 días se cobrará según los precios enumerados anteriormente. Los cobros relacionados con el área de trabajo de Log Analytics por la ingesta de datos y las funcionalidades adicionales para la automatización y el aprendizaje automático siguen aplicándose durante la evaluación gratuita.

Para calcular el coste, Microsoft proporciona una calculadora que permitirá estimar con bastante precisión la facturación mensual del servicio. Se puede encontrar el detalle en el siguiente enlace:

https://azure.microsoft.com/es-es/pricing/calculator/?service=azure-sentinel

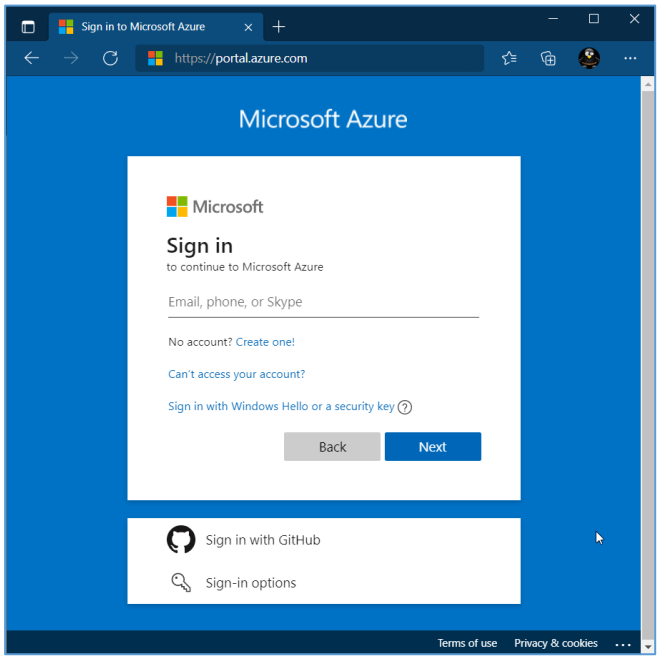
2. DESPLIEGUE SEGURO PARA MICROSOFT SENTINEL

Microsoft Sentinel es un servicio cloud accesible desde el portal de Azure con cualquier navegador web moderno. Para ello, se deben seguir los pasos que se detallan a continuación.

2.1 ACCESO AL PORTAL AZURE DESDE UN NAVEGADOR

1. Se debe acceder al portal de Azure con un usuario Administrador.

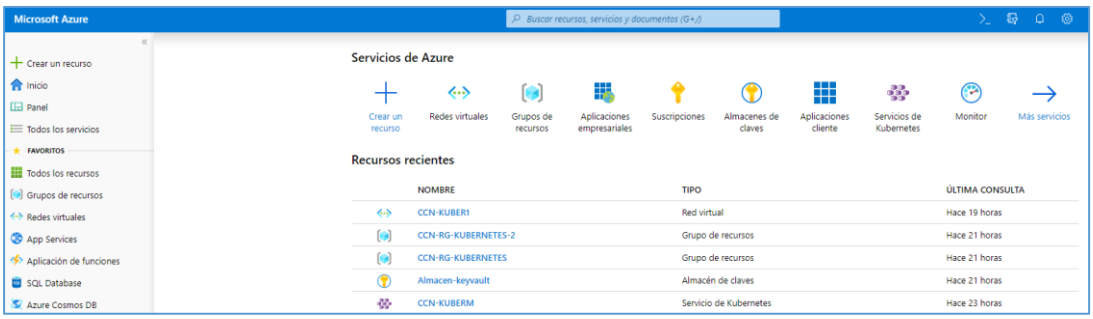
   El usuario *administrador* debe acceder al portal de Azure a través del siguiente enlace: **portal.azure.com**



Nota: *Se solicita la cuenta de correo electrónico y contraseña.*

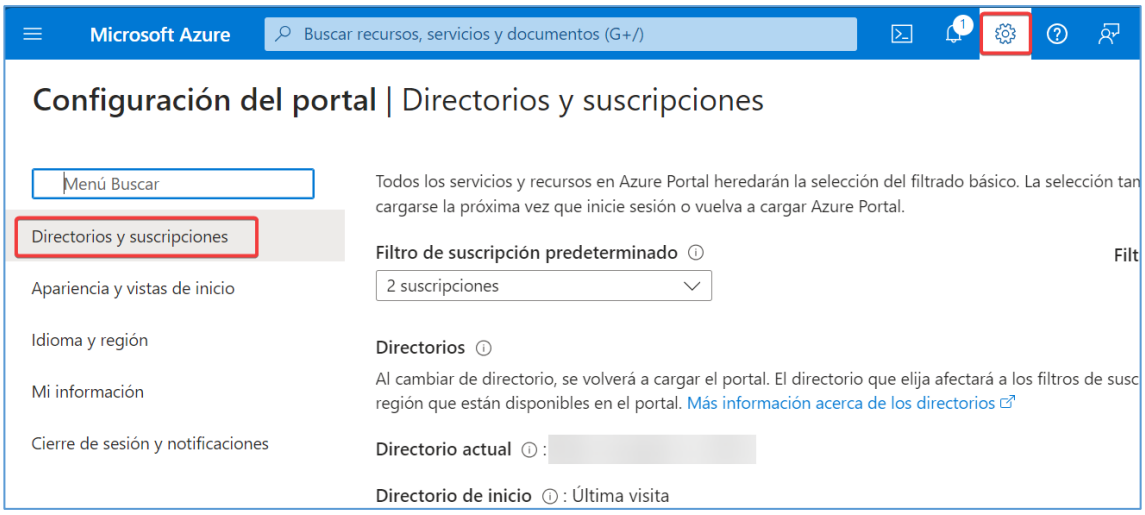
Configuración del portal

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

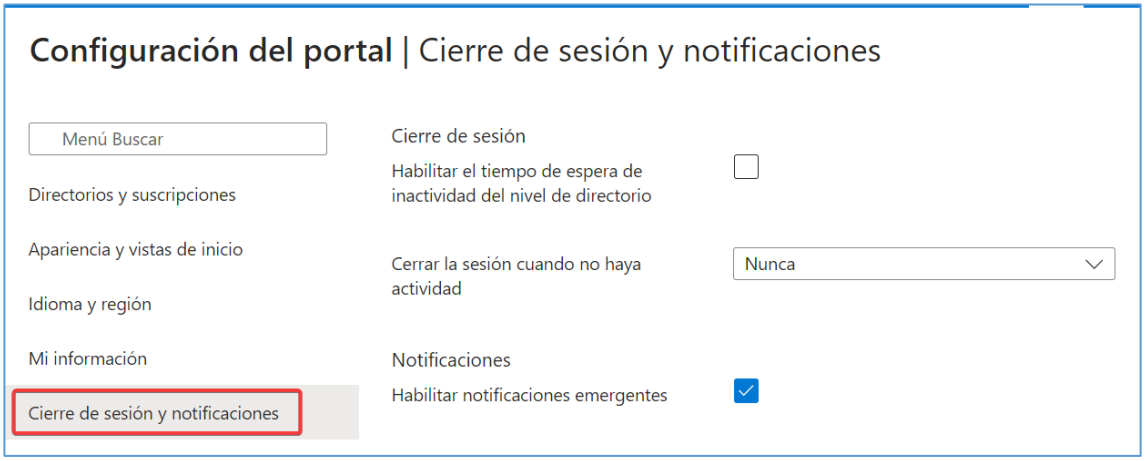


1. Pulsar sobre la rueda que se describe a continuación.

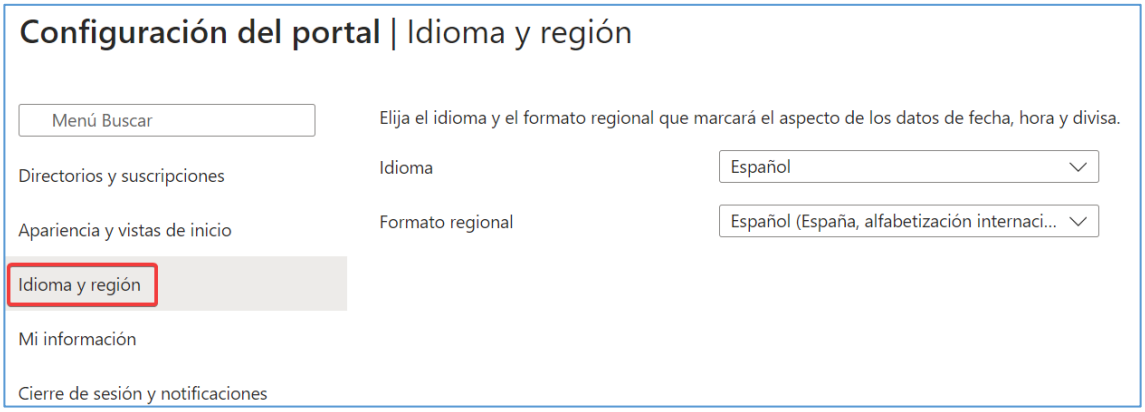
Nota: En caso de tener varias suscripciones, desde aquí se puede seleccionar la adecuada.



2. En la misma sección de configuración, para establecer un cierre de sesión por inactividad, clicar en la sección Cierre de sesión y notificaciones.

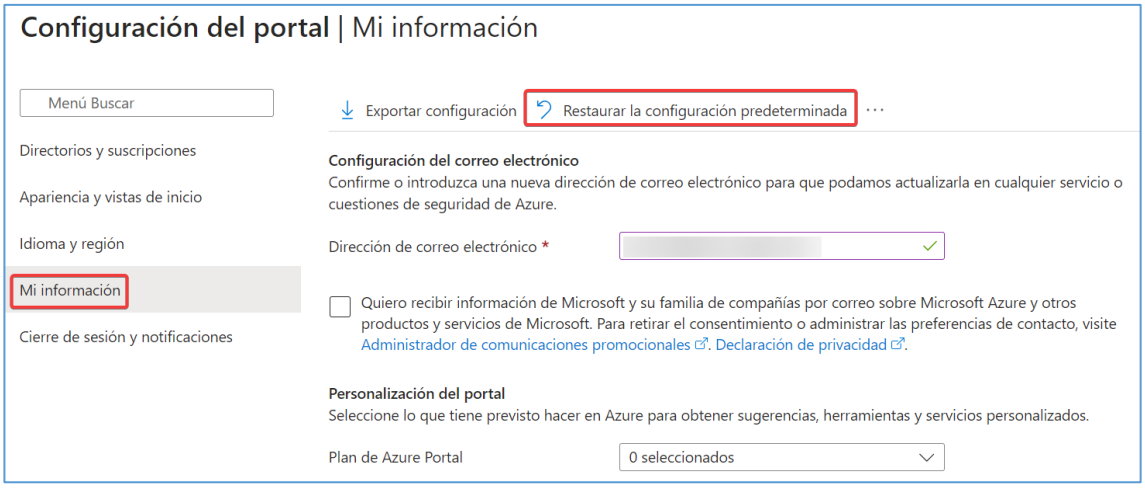


3. Establecer el idioma y región.



4. Se puede personalizar la vista del panel principal.

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



Protección de acceso al portal

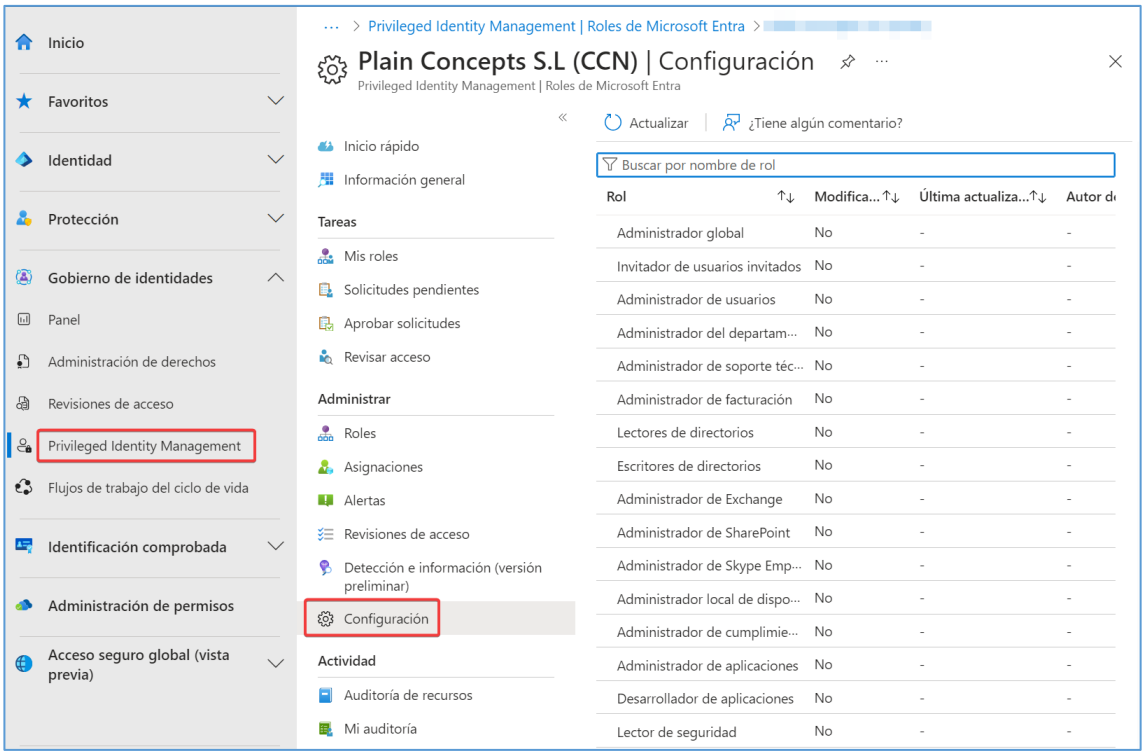
Los últimos estudios realizados por Microsoft indican que una cuenta tiene un 99.9% menos de probabilidades de ser comprometida si usa la autenticación multifactor. Para habilitar MFA en Entra ID se pueden usar dos métodos:

1. Habilitar en las características del rol el uso de MFA utilizando la administración privilegiada de identidad (Privileged Identity Management).
2. Utilizando el acceso condicional.

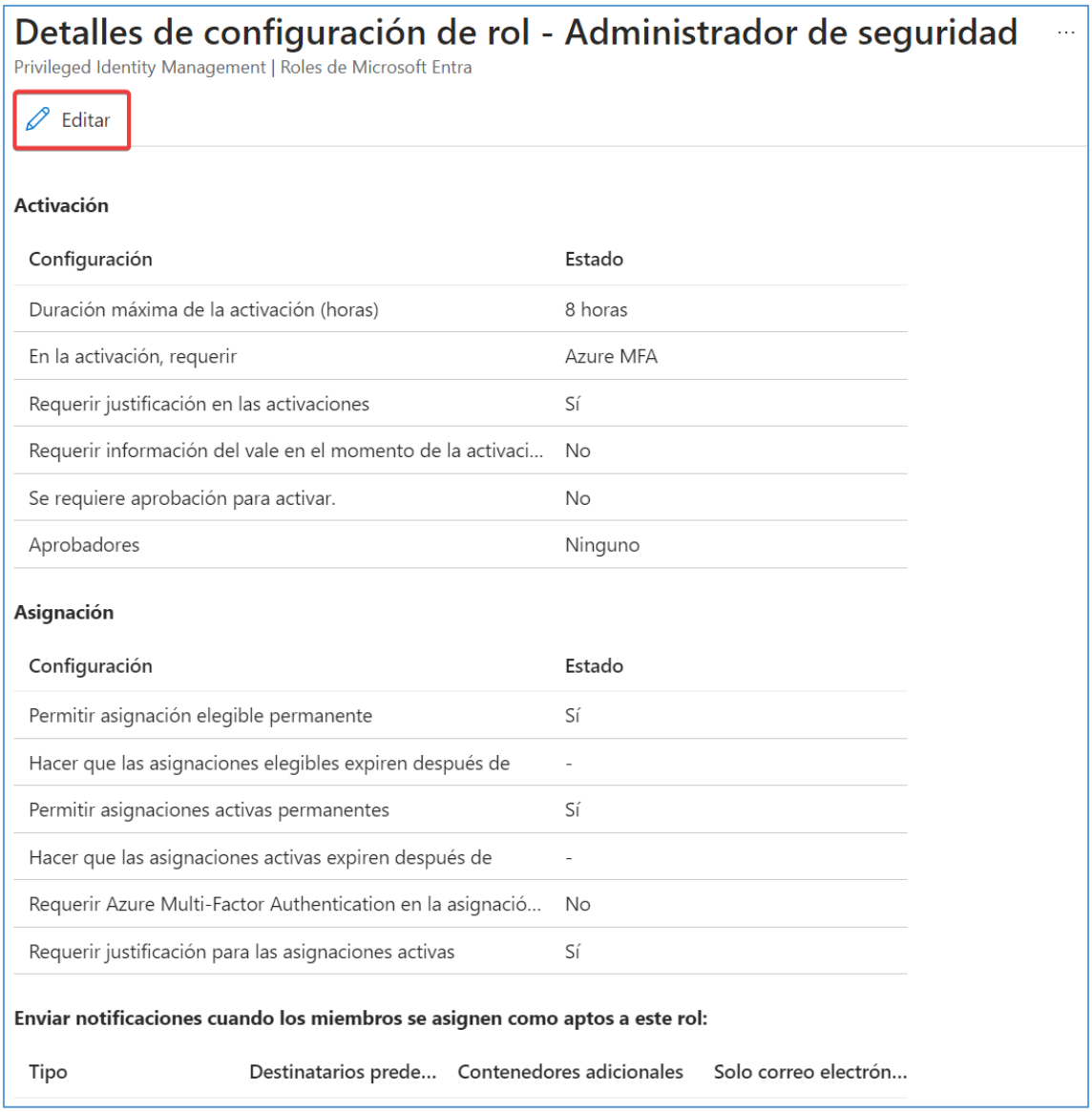
Habilitar MFA utilizando PIM (Privileged Identity Management)

Se puede configurar un rol de Microsoft Entra ID utilizando el portal de PIM para habilitar el MFA. Será necesario realizar los siguientes pasos para habilitarlo:

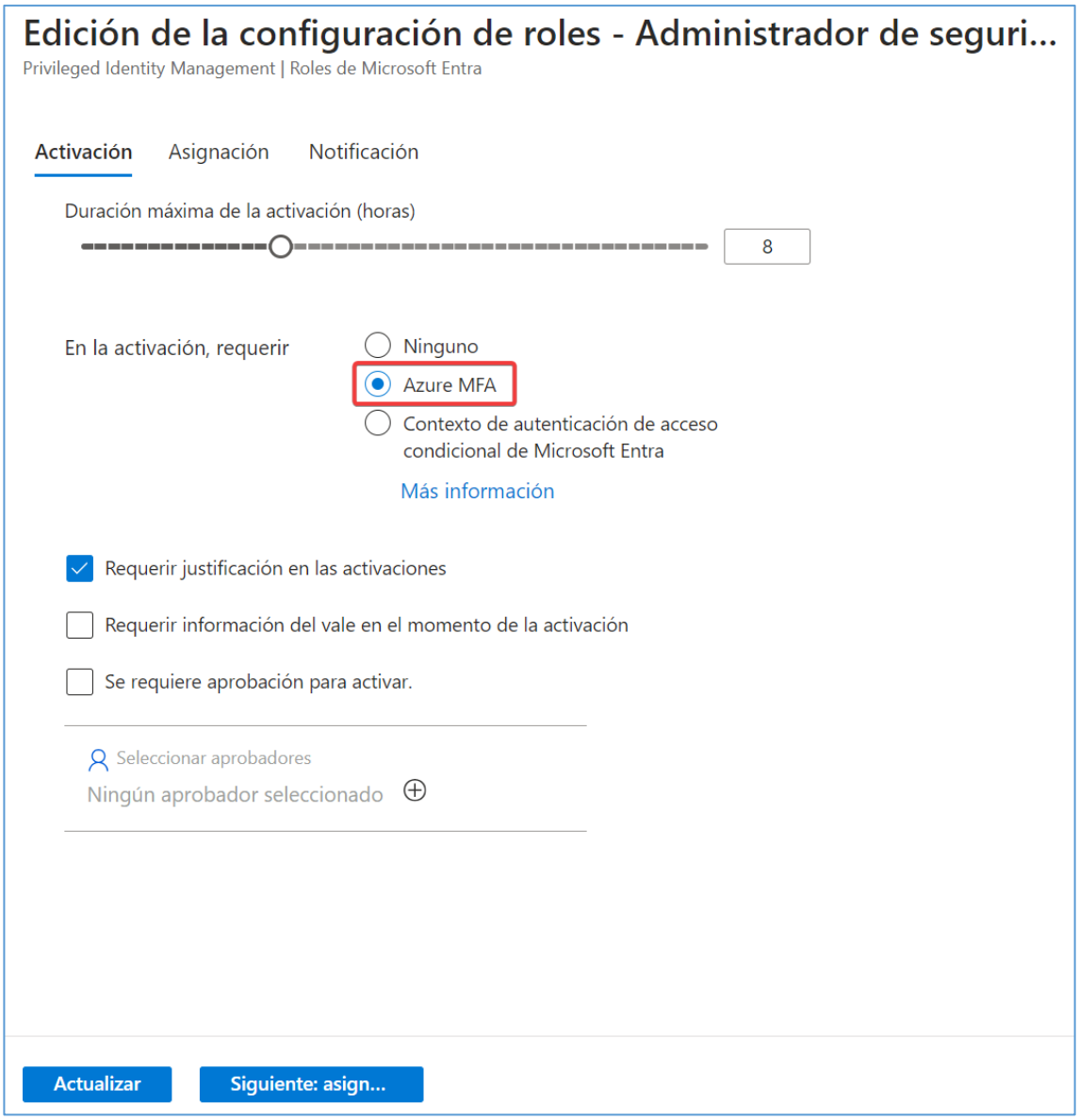
1. Iniciar sesión en el centro de administración de Microsoft Entra con un usuario en el rol Administrador de roles con privilegios.
2. Abrir Gobierno de identidades → Privileged Identity Management → Roles de Microsoft Entra → Configuración.



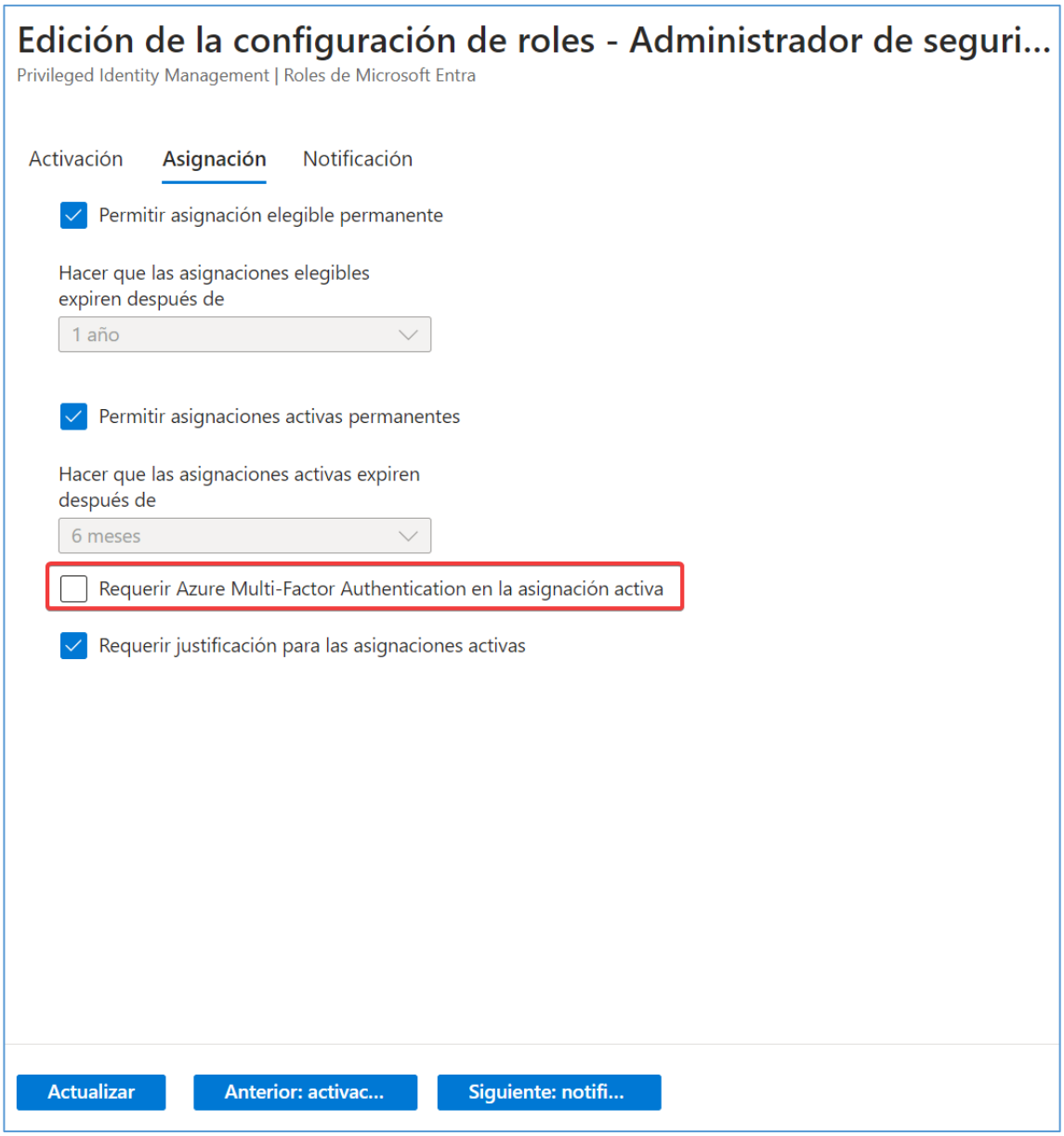
3. Seleccionar el rol cuya configuración se desea configurar. Por ejemplo, uno de los roles que se utilizará es el de Administrador de Seguridad:



4. Seleccionar **Editar** para abrir la página Configuración de roles. En la pestaña de activación se puede configurar que requiera Azure MFA.



También es posible configurar MFA en la asignación:

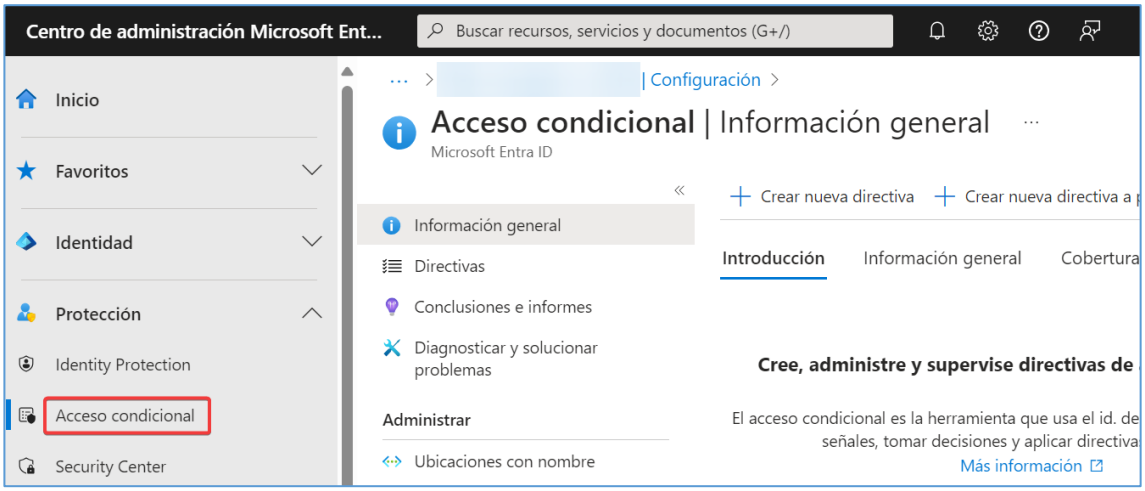


Privileged Identity Management proporciona la obligatoriedad de la autenticación multifactor de Microsoft Entra ID en la activación y en la asignación activa.

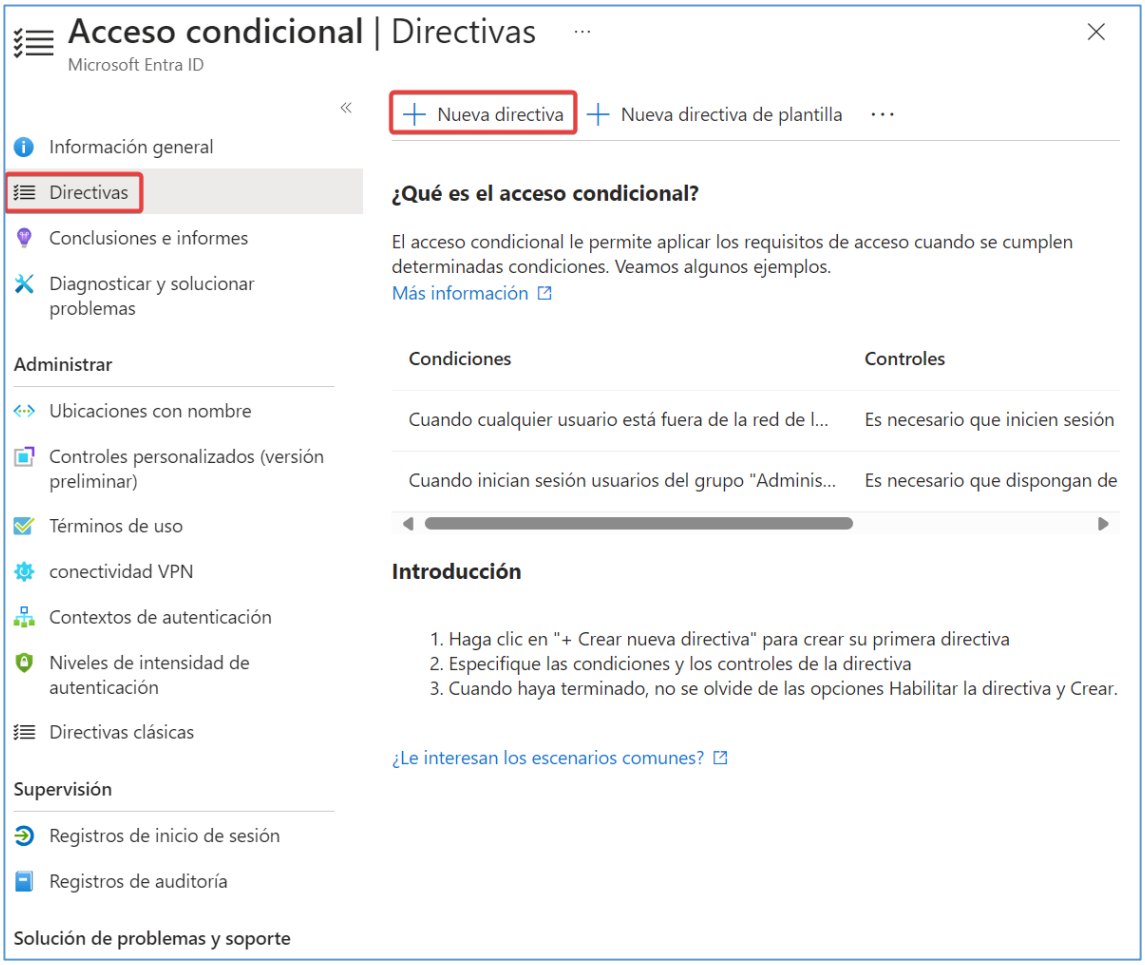
Habilitar MFA utilizando Acceso Condicional

Los administradores de seguridad es uno de los grupos a los que Microsoft recomienda habilitar el MFA. El motivo es que las cuentas con privilegios en Microsoft Entra ID son objetivo de los atacantes y de esta forma se consigue reducir el riesgo de que estas cuentas se vean comprometidas. Estos son los pasos que seguir para crear una directiva de acceso condicional que exija que el rol administrativo administrador de seguridad realice la autenticación multifactor.

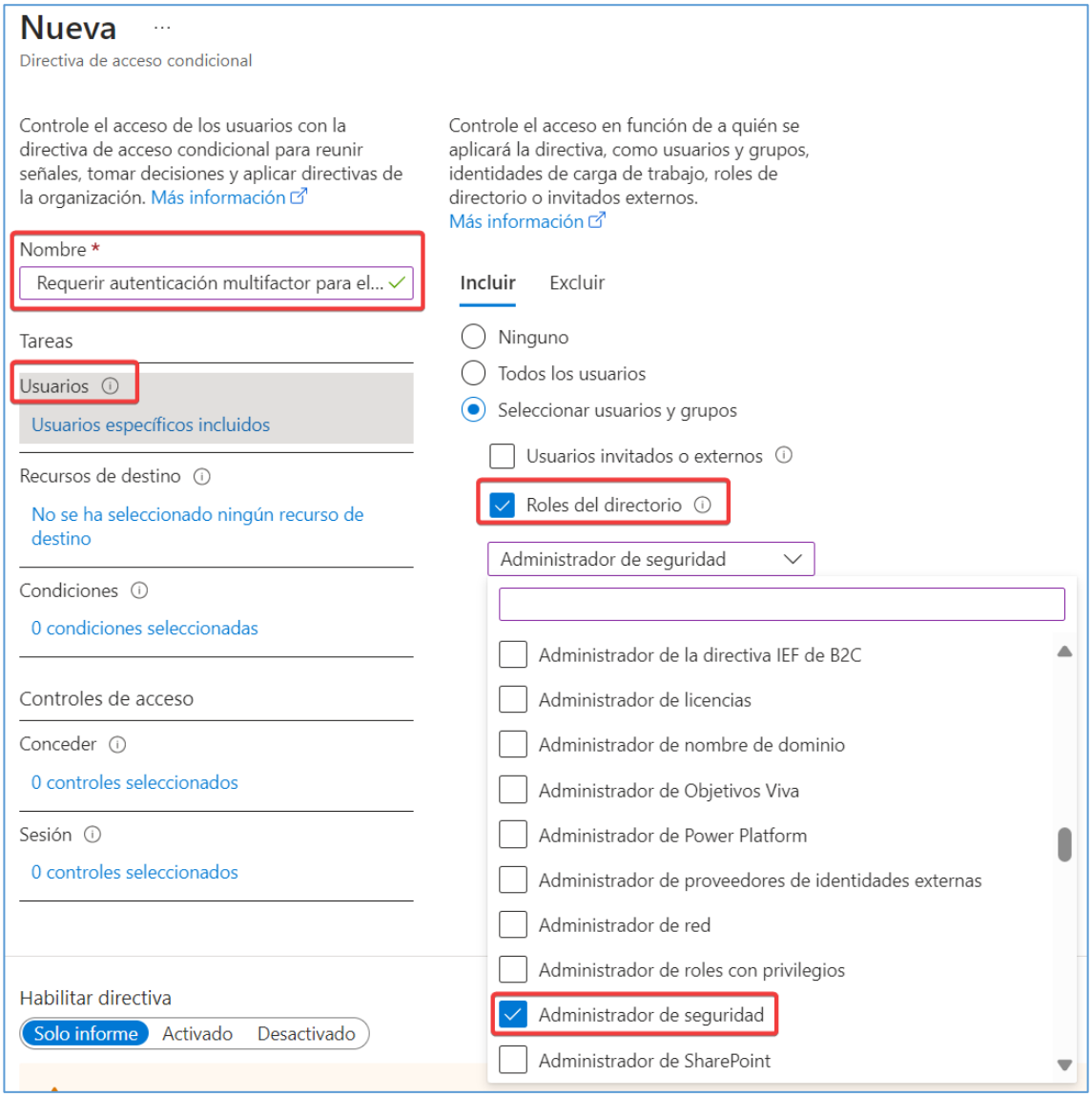
1. Iniciar sesión en el centro de administración de Microsoft Entra como administrador global, administrador de seguridad o administrador de acceso condicional.
2. Ir a Protección → **Acceso condicional**.



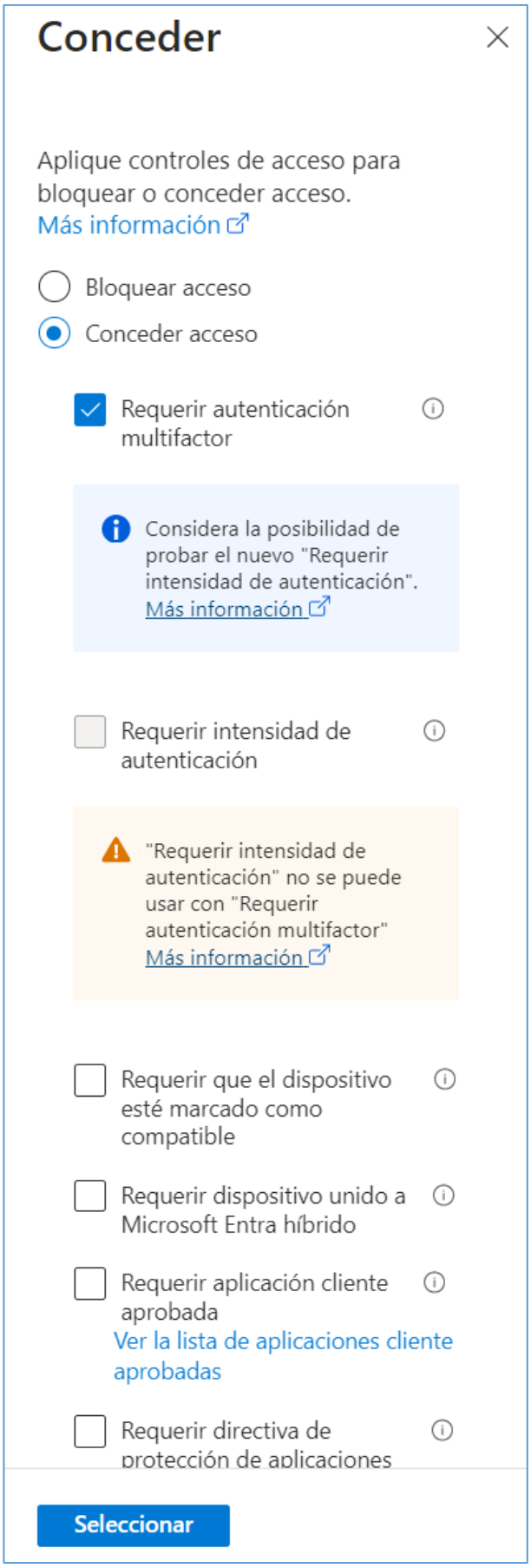
3. Seleccionar **Nueva directiva.**



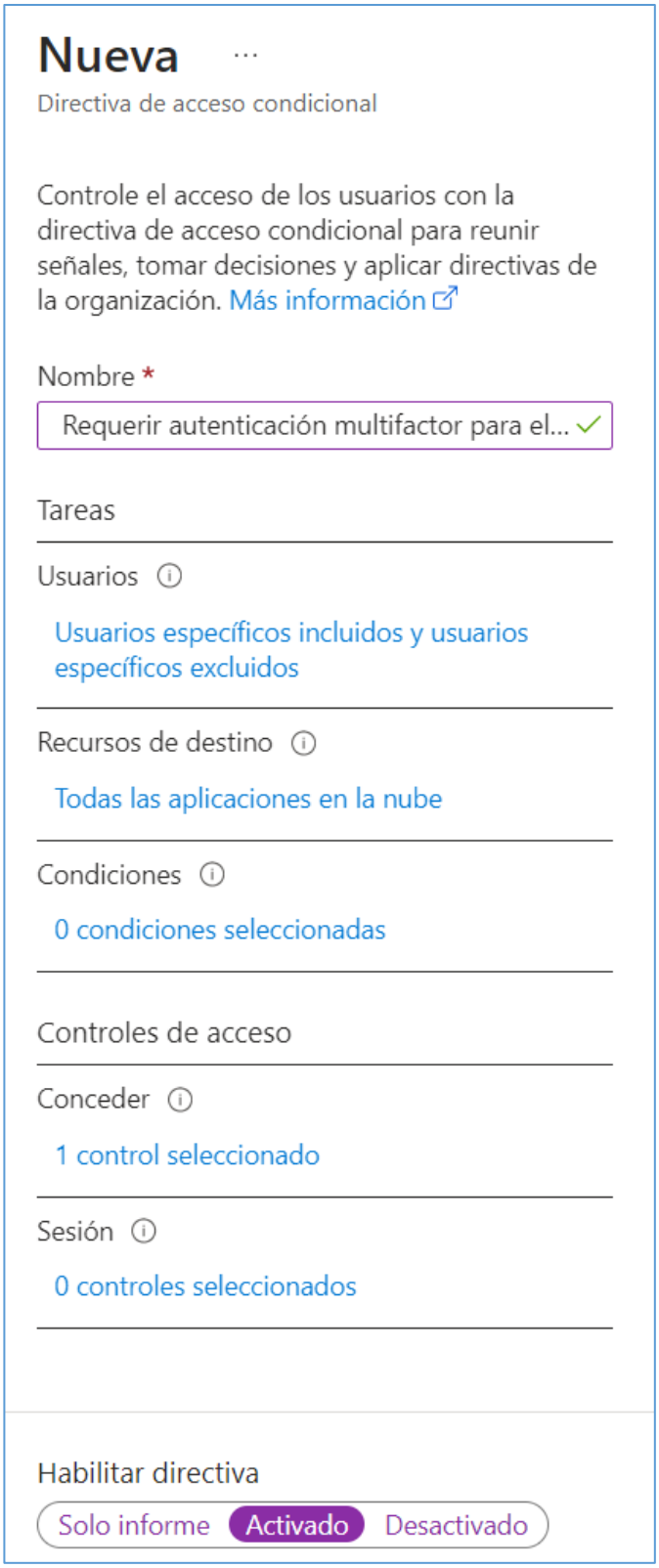
4. Asignar un nombre a la directiva. Se recomienda que las organizaciones creen un estándar significativo para los nombres de sus directivas.
5. En **Asignaciones**, seleccionar **Usuarios y grupos**. En **Incluir**, seleccionar **Roles del directorio** y elegir el rol **Administrador de seguridad:**



6. En **Excluir**, seleccionar **Usuarios y grupos** y, luego, elegir las cuentas de acceso de emergencia de la organización. Seleccionar **Listo**.
7. En **Recursos de destino → Aplicaciones en la nube → Incluir**, seleccionar **Todas las aplicaciones en la nube.**
8. En **Controles de acceso** > Conceder, seleccionar Conceder acceso, Requerir autenticación multifactor y Seleccionar.


Conceder
Aplique controles de acceso para bloquear o conceder acceso.
Más información
Bloquear acceso
Conceder acceso
Requerir autenticación multifactor
Considera la posibilidad de probar el nuevo "Requerir intensidad de autenticación".
Más información
Requerir intensidad de autenticación
"Requerir intensidad de autenticación" no se puede usar con "Requerir autenticación multifactor"
Más información
Requerir que el dispositivo esté marcado como compatible
Requerir dispositivo unido a Microsoft Entra híbrido
Requerir aplicación cliente aprobada
Ver la lista de aplicaciones cliente aprobadas
Requerir directiva de protección de aplicaciones
Seleccionar

9. Confirmar la configuración y establecer **Habilitar directiva en Activado**.



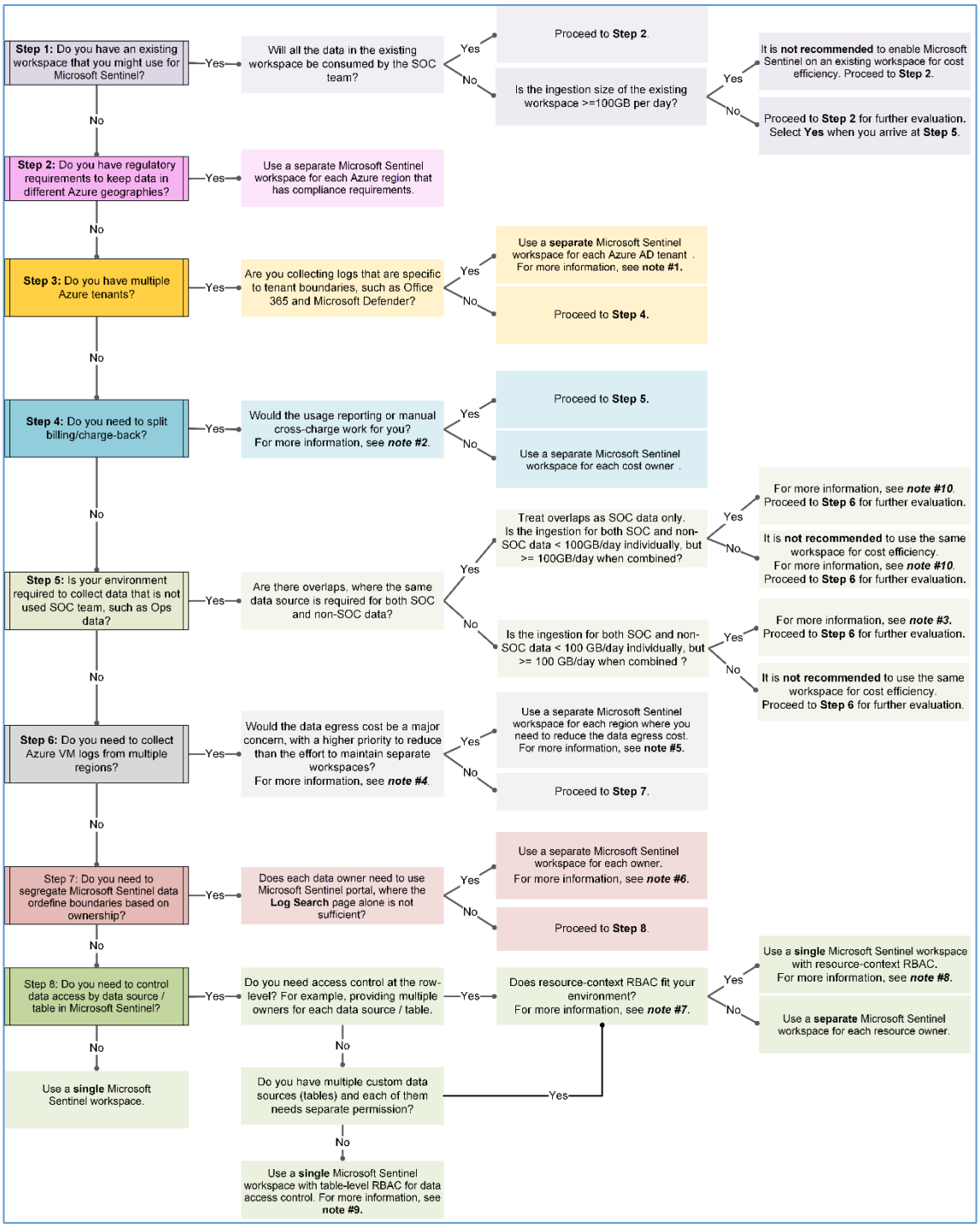
Además de configurar MFA como se ha visto, se recomienda habilitar protección del acceso al centro de administración de Microsoft Entra, etc. Esta configuración se

encuentra descrita en la guía: [CCN-STIC-884A - Guía de Configuración segura para Azure].

2.2 CONFIGURACIÓN DEL SERVICIO MICROSOFT SENTINEL

Para poder utilizar Microsoft Sentinel, primero se debe habilitar y, después, conectar sus orígenes de datos. Microsoft Sentinel incluye varios conectores para soluciones de Microsoft, que están disponibles inmediatamente y proporcionan integración en tiempo real, entre las que se incluyen las soluciones de Microsoft Defender XDR, orígenes de Microsoft 365 (como Office 365), Microsoft Entra ID, Microsoft Defender for Identity, Defender for Cloud Apps, alertas de Microsoft Defender for Cloud y más. Además, hay conectores integrados al amplio ecosistema de seguridad para soluciones que no son de Microsoft. También puede usar el formato de evento común (Common Event Format CEF), Syslog o la API de REST para conectar los orígenes de datos con Microsoft Sentinel.

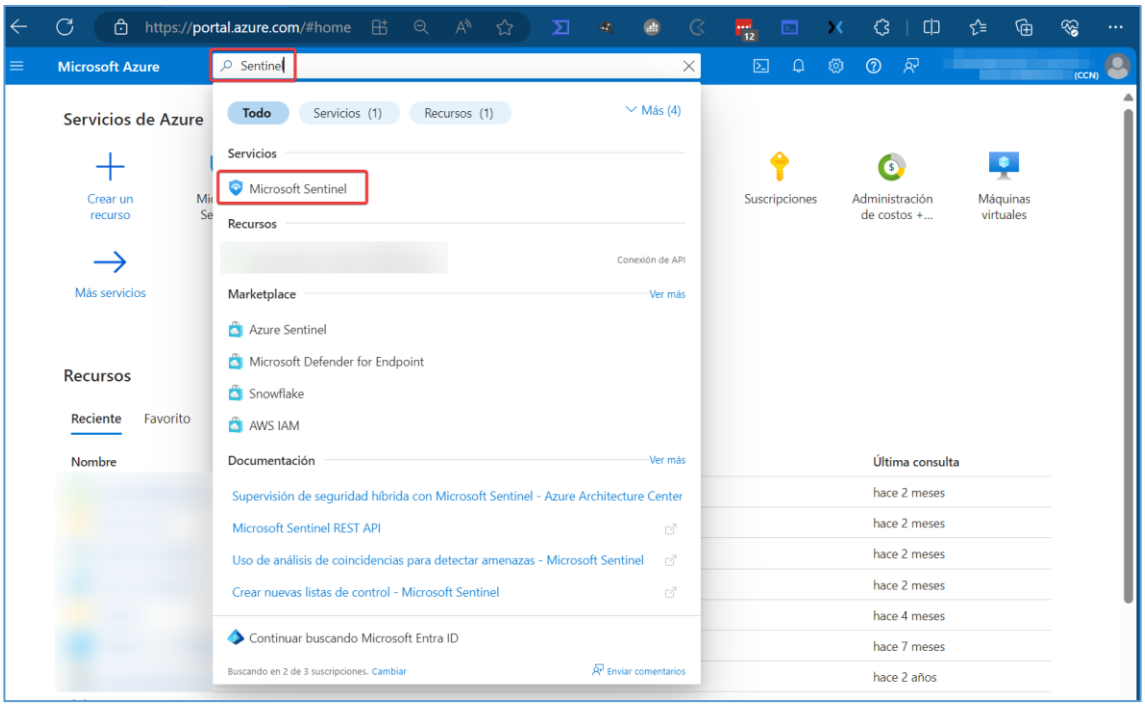
A continuación, se muestra un árbol de decisión que ayudará a definir las diferentes áreas de trabajo que se pueden establecer para Microsoft Sentinel.



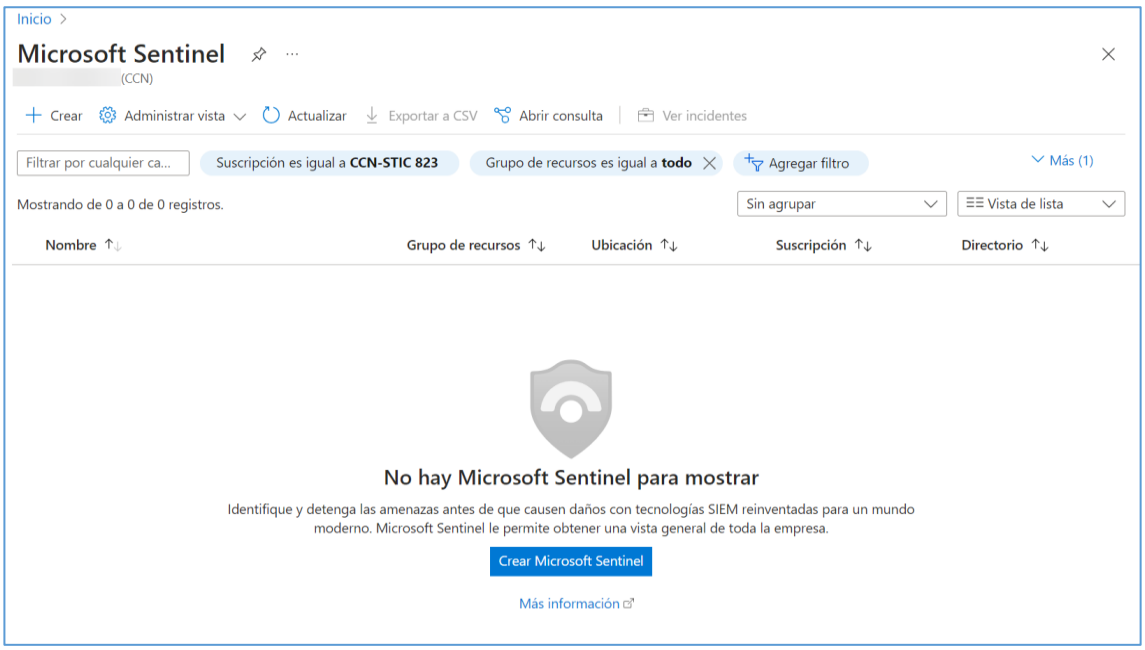
* Acceso al gráfico de flujo de árbol de decisión completo: https://docs.microsoft.com/es-es/azure/sentinel/design-your-workspace-architecture#decision-tree

Para esta guía se utilizará el modelo de un único tenant en Azure donde residen conjuntamente el servicio de Microsoft Sentinel y Logs Analytics.

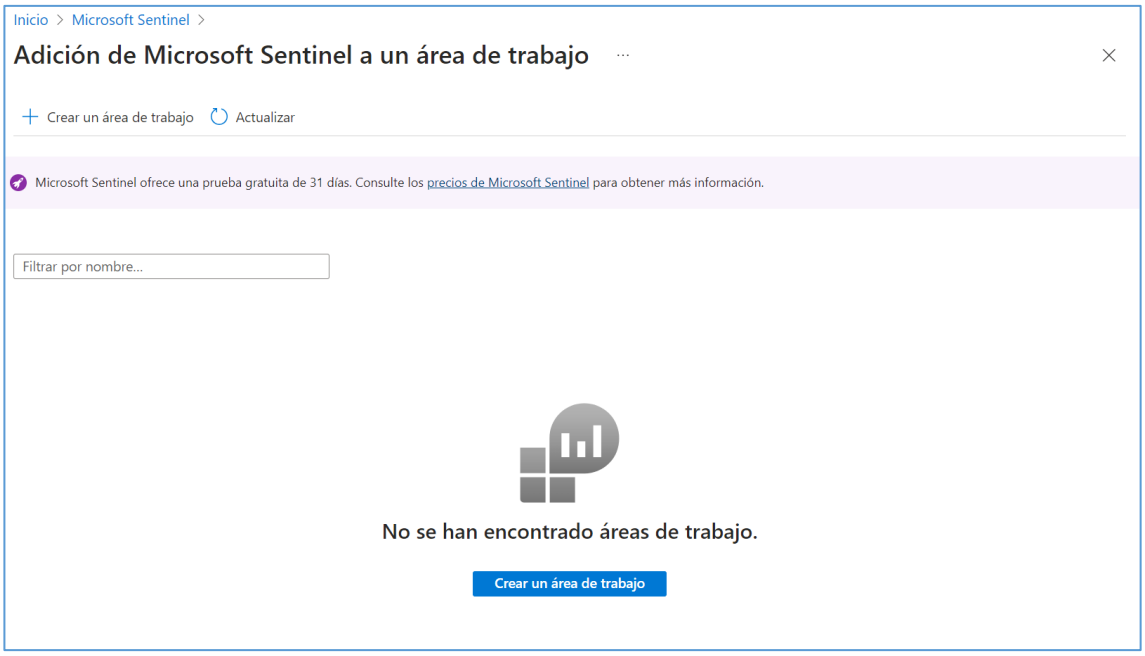
Una vez validados los prerrequisitos definidos en el apartado Prerrequisitos. En el portal de Azure www.portal.azure.com, se seleccionará Microsoft Sentinel.



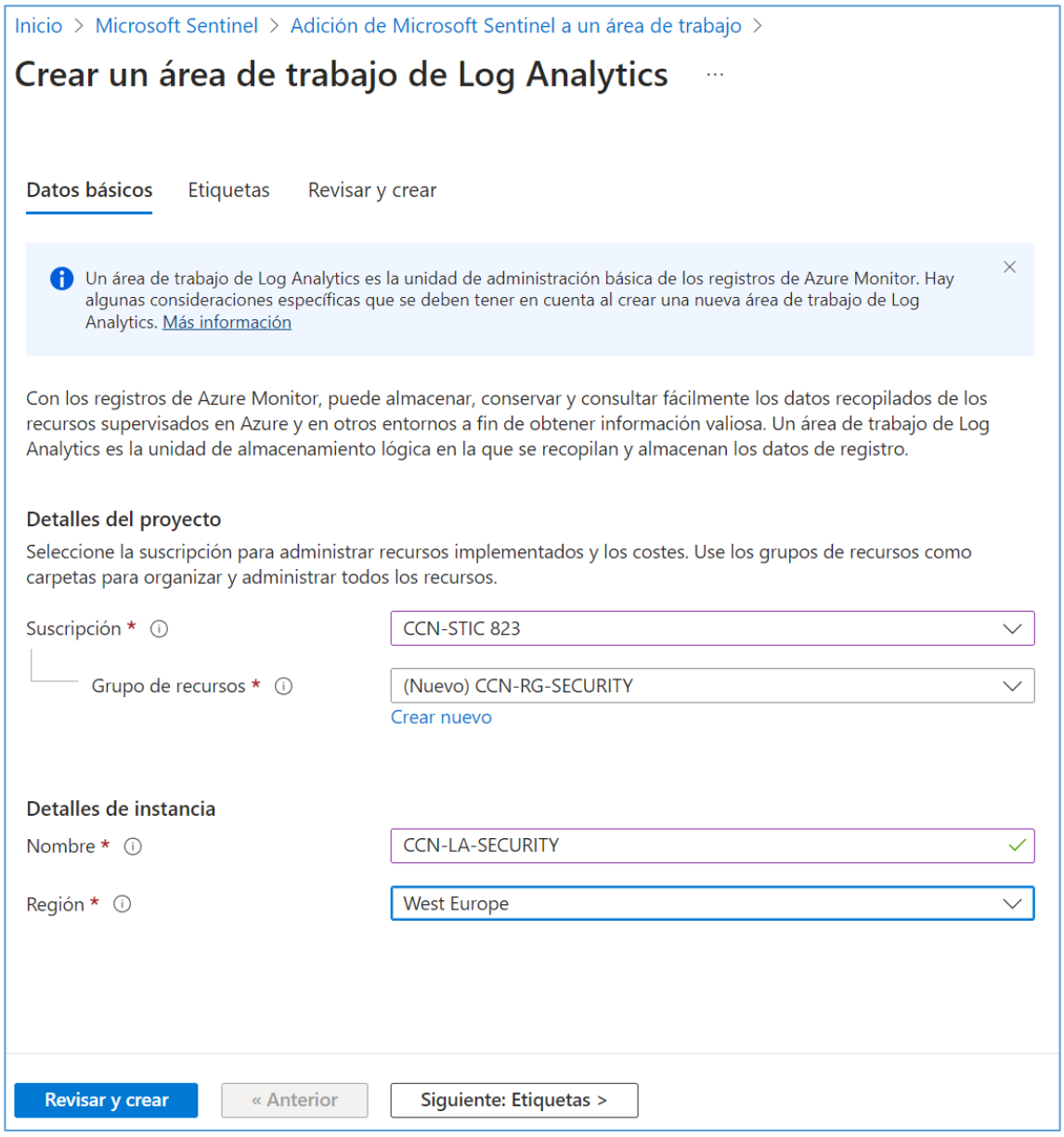
1. En Microsoft Sentinel se seleccionará *Crear* Microsoft Sentinel:



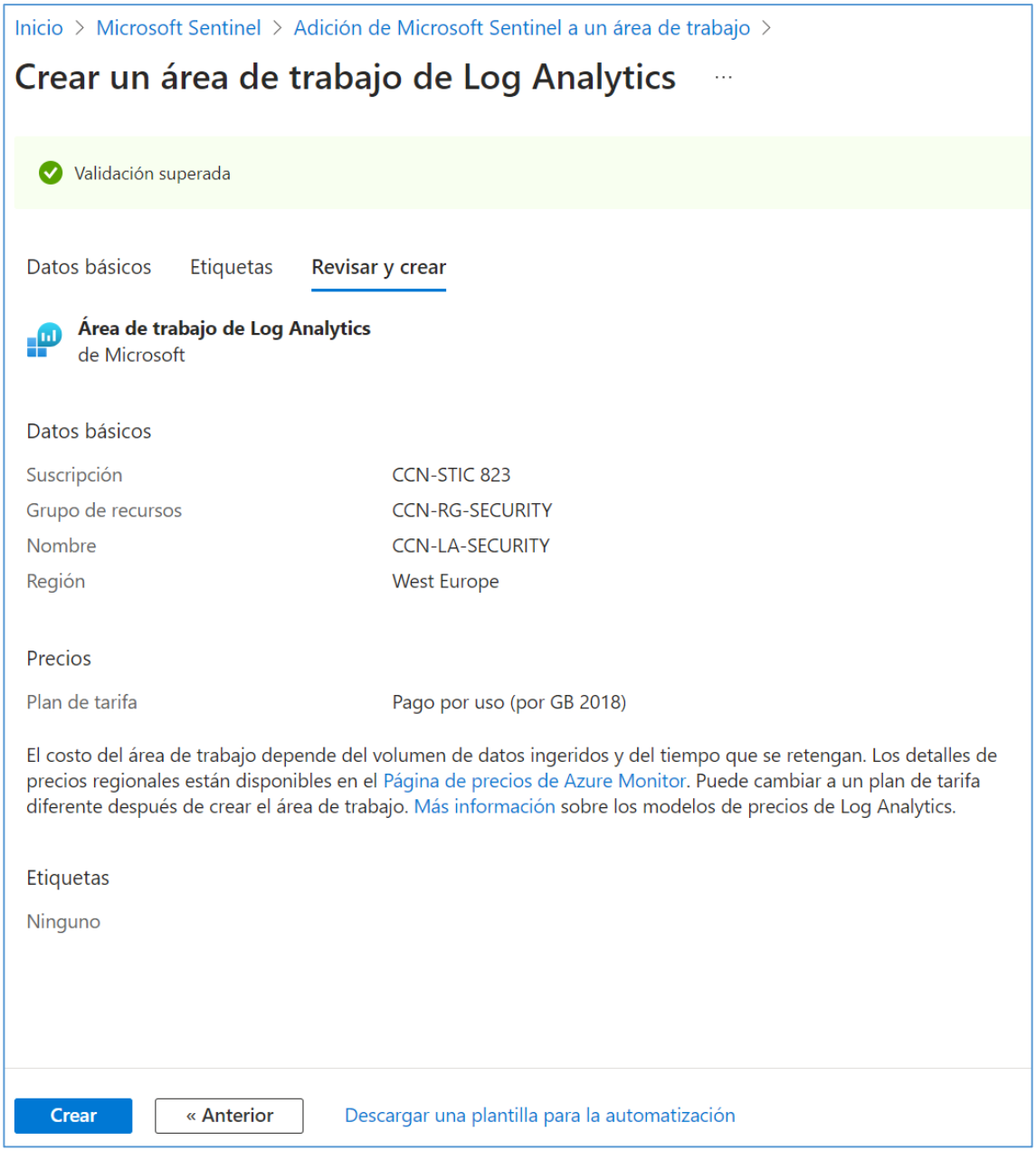
2. Se seleccionará el área de trabajo que se quiere usar o se creará un área nueva. Microsoft Sentinel se puede ejecutar en más de un área de trabajo, pero los datos se aíslan en un área de trabajo. Una vez implementado en un área de trabajo, Microsoft Sentinel no admite actualmente el movimiento de esa área de trabajo a otros grupos de recursos o suscripciones. Las áreas de trabajo predeterminadas creadas por Microsoft Defender for Cloud no aparecerán en la lista; no se puede instalar Microsoft Sentinel en ellas.


Inicio > Microsoft Sentinel >
Adición de Microsoft Sentinel a un área de trabajo
Crear un área de trabajo
Actualizar
Microsoft Sentinel ofrece una prueba gratuita de 31 días. Consulte los precios de Microsoft Sentinel para obtener más información.
Filtrar por nombre...
No se han encontrado áreas de trabajo.
Crear un área de trabajo

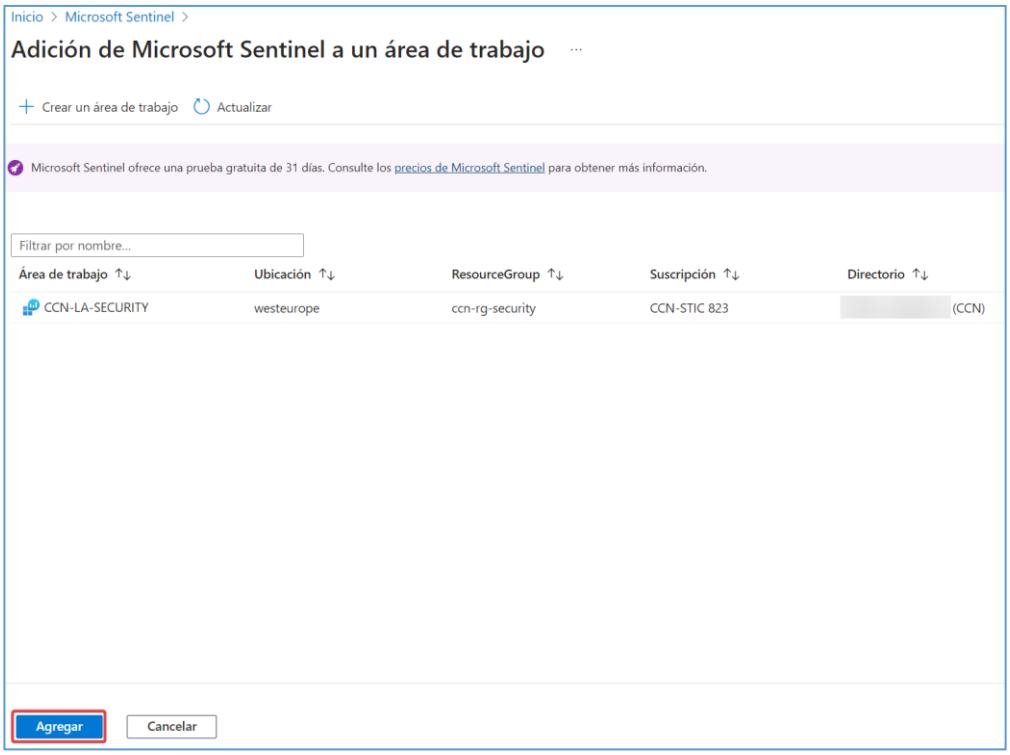
3. El área de trabajo se creará dentro de un grupo de recursos que se destinará para albergar todos los recursos relacionados con la seguridad, de esta manera, es más sencillo administrar la gestión de acceso a los mismos. Es recomendable utilizar una nomenclatura que defina el propósito al que está destinado el recurso.



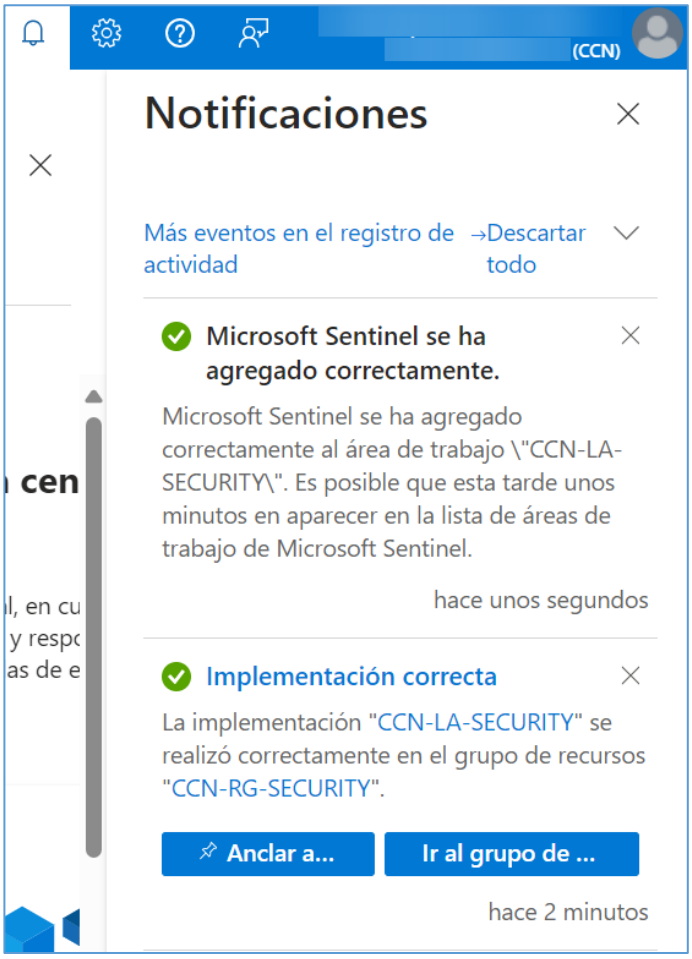
4. Superada la validación, seleccionar *Crear* para finalizar la creación del nuevo espacio de trabajo de Log Analytics.



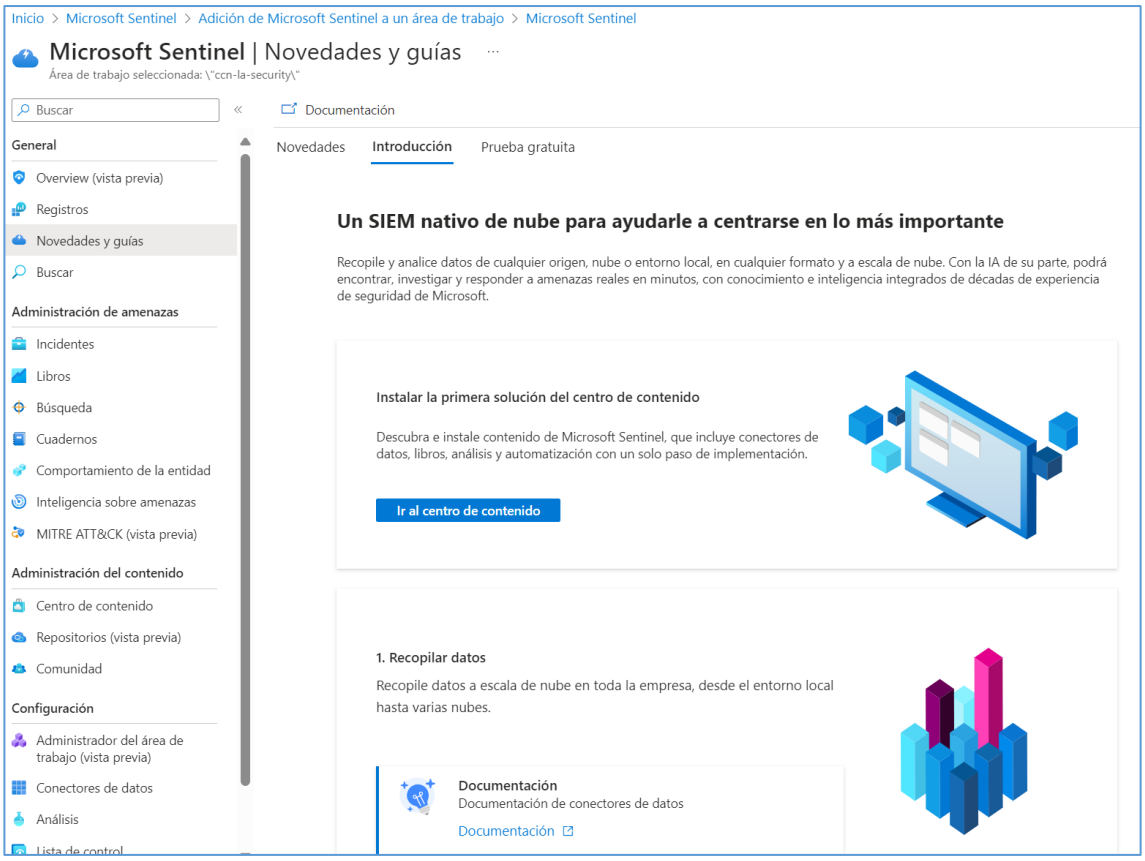
5. Por último, faltaría seleccionar el espacio de trabajo de log analytics que se ha creado para poder conectar Microsoft Sentinel. Se agrega Microsoft Sentinel al área de trabajo pulsando *Agregar*.



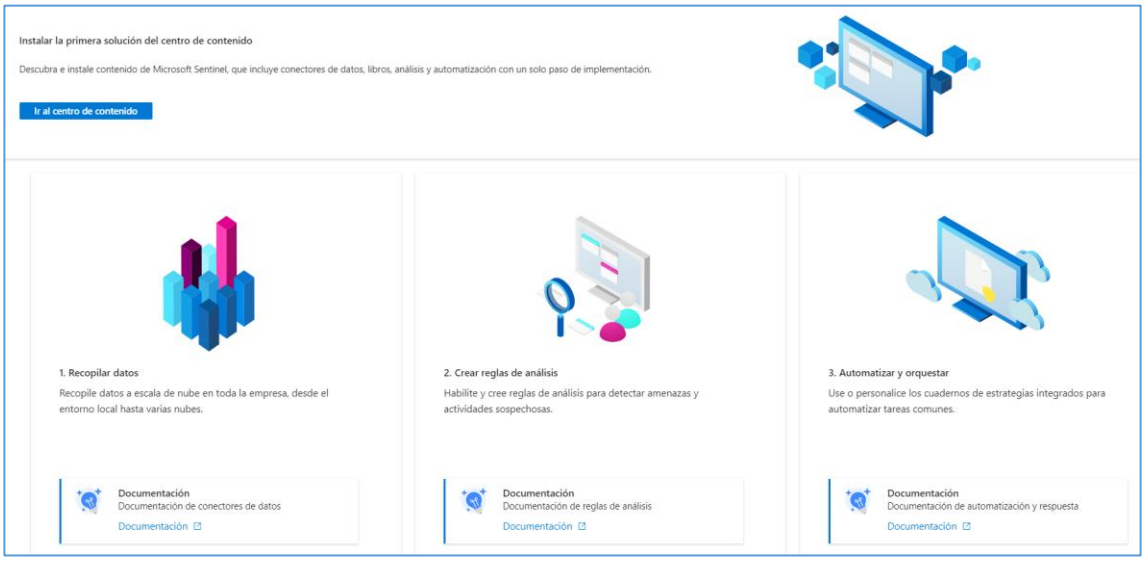
6. Se comprueba que el proceso finaliza correctamente.



7. Una vez habilitado Microsoft Sentinel, se puede acceder a las novedades del servicio y a la introducción.



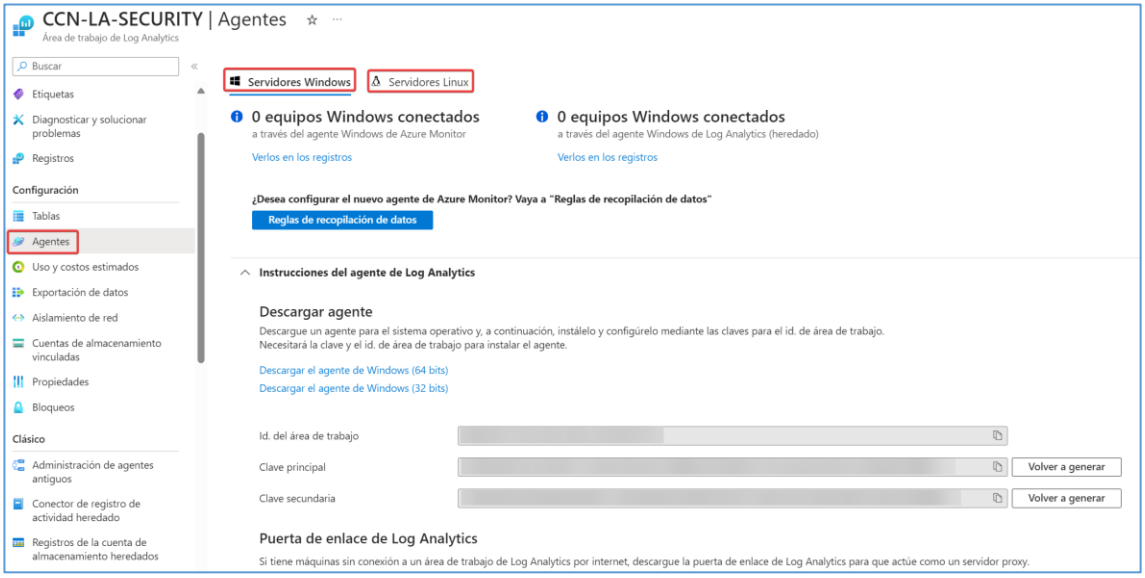
8. Los siguientes pasos serían: Instalar la primera solución del centro de contenido, Recopilar datos, crear reglas de análisis y Automatizar y orquestar las tareas comunes y las respuestas frente a amenazas.



Microsoft Sentinel ingiere datos de servicios y aplicaciones mediante la conexión y el reenvío de los eventos y registros a Microsoft Sentinel. Tanto en las máquinas físicas

como en las virtuales, se puede instalar el agente de Log Analytics que recopila los registros y los reenvía a Microsoft Sentinel. En el caso de los firewalls y servidores proxy, Microsoft Sentinel instala el agente de Log Analytics en un servidor de Syslog de Linux, desde el cual, el agente recopila los archivos de registro y los reenvía a Microsoft Sentinel.

Para la descarga e instalación de estos agentes, es necesario desplazarse al área de Logs Analytics y en el apartado de configuración se descarga el agente para su instalación, según el sistema operativo.



2.2.1 CONECTAR LOS ORÍGENES DE DATOS

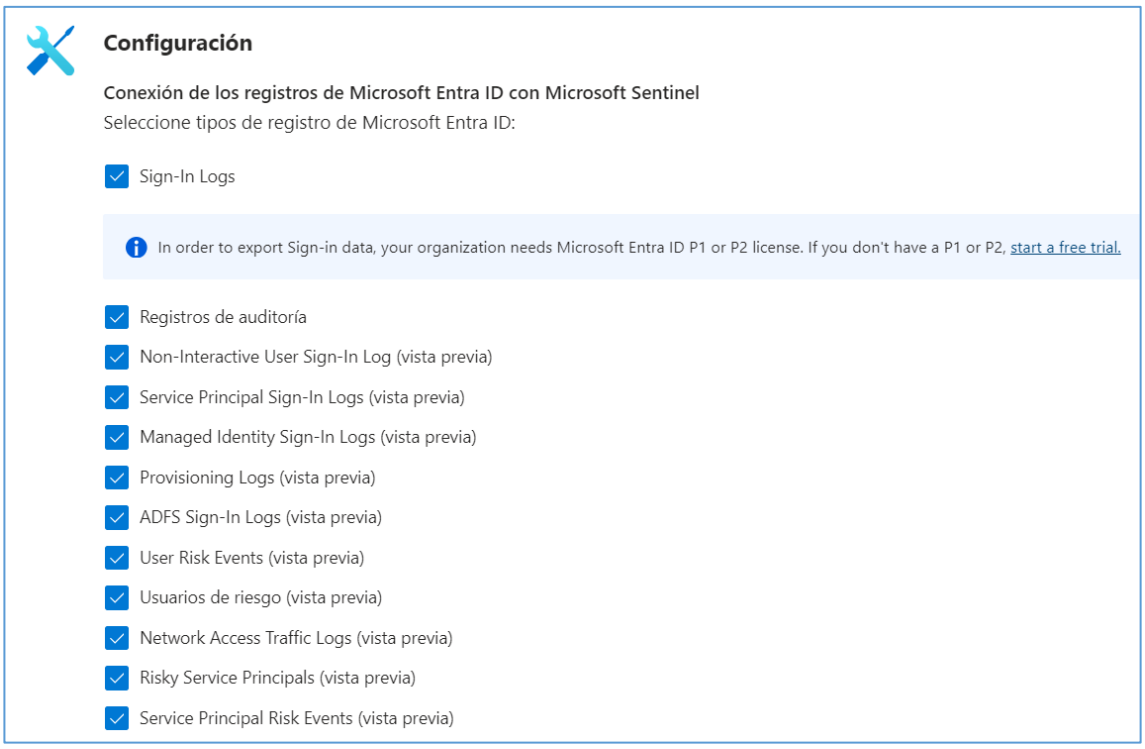
Uno de los principales objetivos de una solución SIEM es centralizar el almacenamiento y análisis de los eventos de seguridad a través de los distintos productos que proporcionan protección en una organización. Sentinel se encarga de recopilar todos los eventos relacionados con la seguridad de los distintos sistemas que disparan dichos eventos. Además, y gracias a su inteligencia frente a amenazas es capaz de cruzar estos datos y correlacionarlos para poder detectar amenazas y definir reglas que permitan su remediación. Los conectores se categorizan según su tipo de ingesta de datos, existen los siguientes tipos:

- Conectores de datos proporcionados con soluciones
- Formato de evento común (CEF)
- Data Collector API de Microsoft Sentinel
- Azure Functions y la API REST
- Syslog
- Registros personalizados
- Integración entre servicios para conectores de datos

Para cumplir con el ENS como mínimo se utilizarán los conectores con un tipo de ingesta de integración entre servicios de Azure y se deben integrar al menos los siguientes conectores: Microsoft Entra ID, Azure Activity y Microsoft Defender XDR. También se mostrará como conectar servidores que utilicen un agente para recopilar los eventos de seguridad de Windows y el conector de AWS para transmitir los eventos de administración de AWS CloudTrail a Microsoft Sentinel. De esta forma queda detallado el despliegue de los principales conectores que encontramos en Microsoft Sentinel.

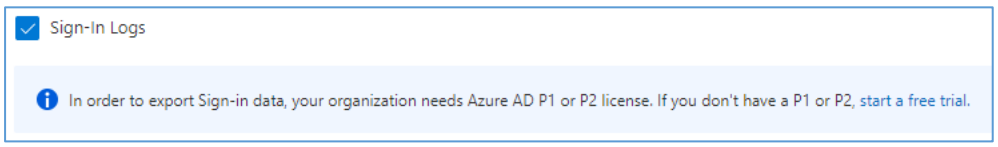
2.2.1.1 AGREGAR CONECTOR MICROSOFT ENTRA ID

Los registros de auditoria generados por Microsoft Entra ID se ingestarán en Microsoft Sentinel utilizando el conector de datos Microsoft Entra ID. El conector permite enviar los siguientes tipos de registro:



Requisitos previos

- Se necesita una licencia de Microsoft Entra ID P1 o P2 para ingerir registros de inicio de sesión en Microsoft Sentinel. Cualquier licencia de Microsoft Entra ID (gratuita/O365/P1/P2) es suficiente para ingerir los otros tipos de registro. Se pueden aplicar cargos adicionales por gigabyte para Azure Monitor (Log Analytics) y Microsoft Sentinel.

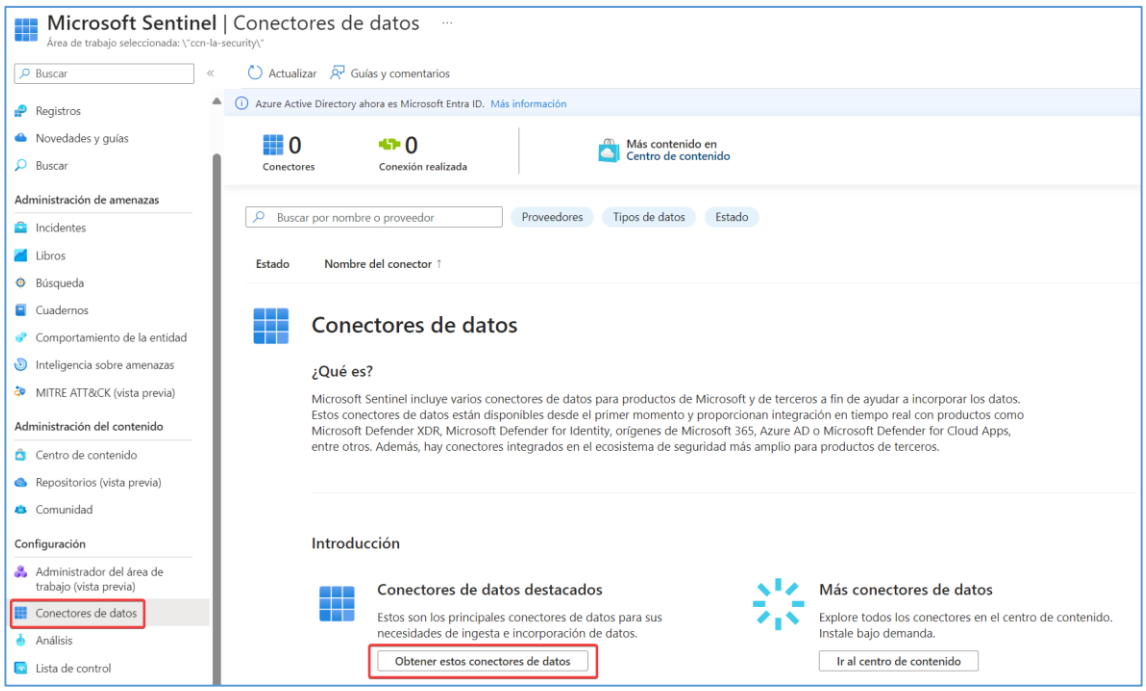


- El usuario debe tener asignado el rol Colaborador de Microsoft Sentinel en el área de trabajo.
- El usuario debe tener asignados los roles Administrador global o Administrador de seguridad en el inquilino desde el que se quiere transmitir los registros.
- El usuario debe tener permisos de lectura y escritura en la configuración de diagnóstico de Microsoft Entra ID para poder ver el estado de la conexión.

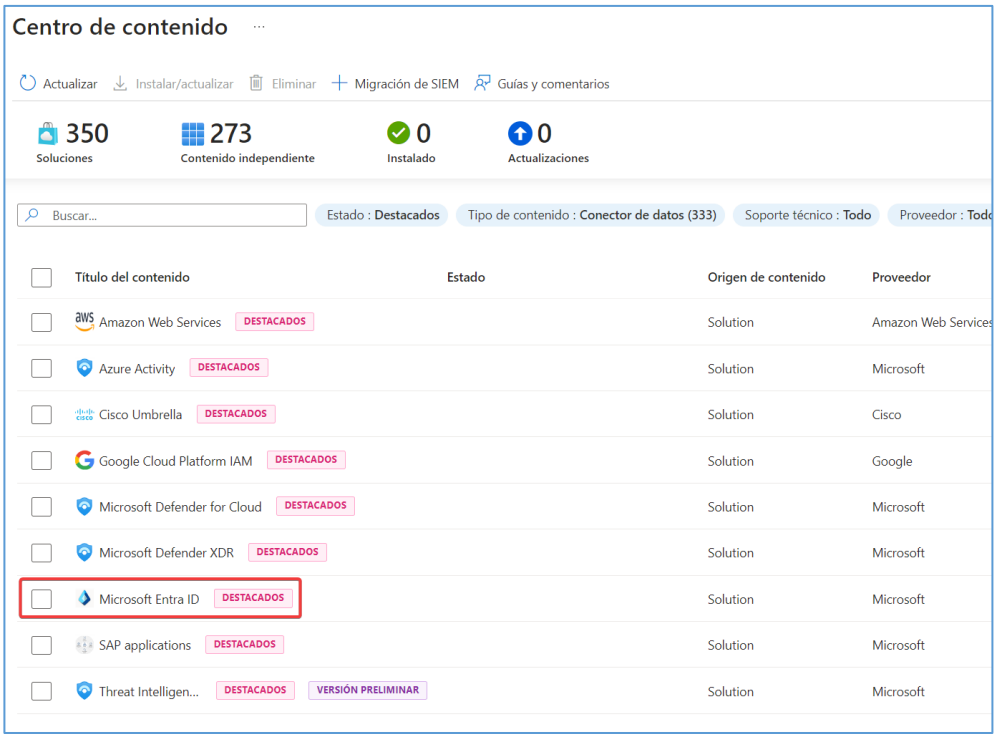
Conectarse a Microsoft Entra ID

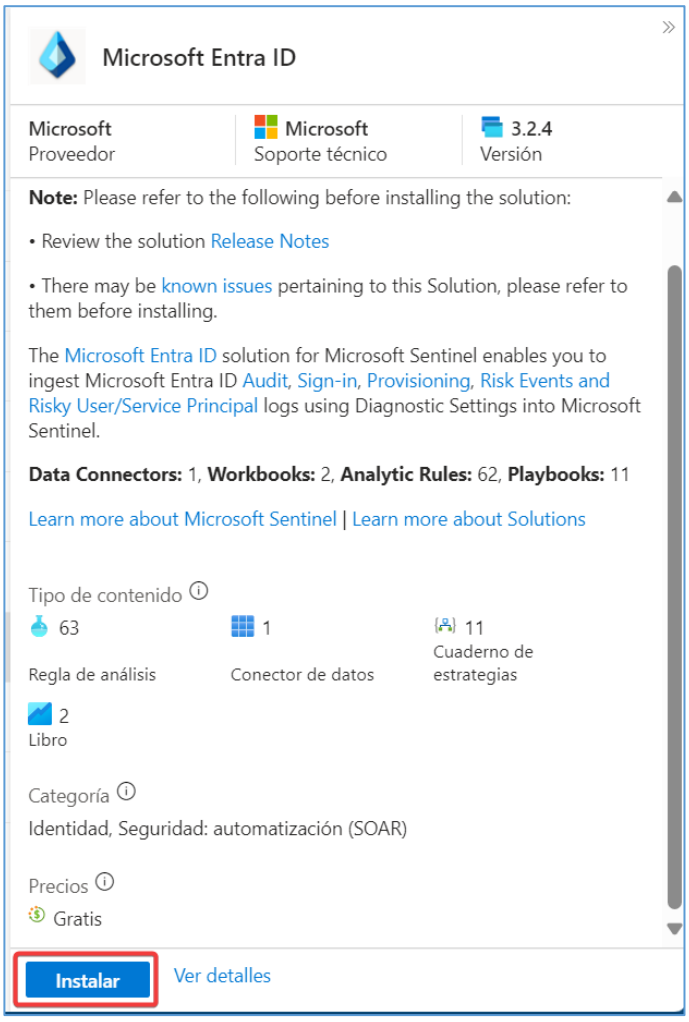
Para activar el conector de Microsoft Entra ID se realizarán los siguientes pasos:

1. En el menú de navegación de Microsoft Sentinel, seleccionar *Conectores de datos*.

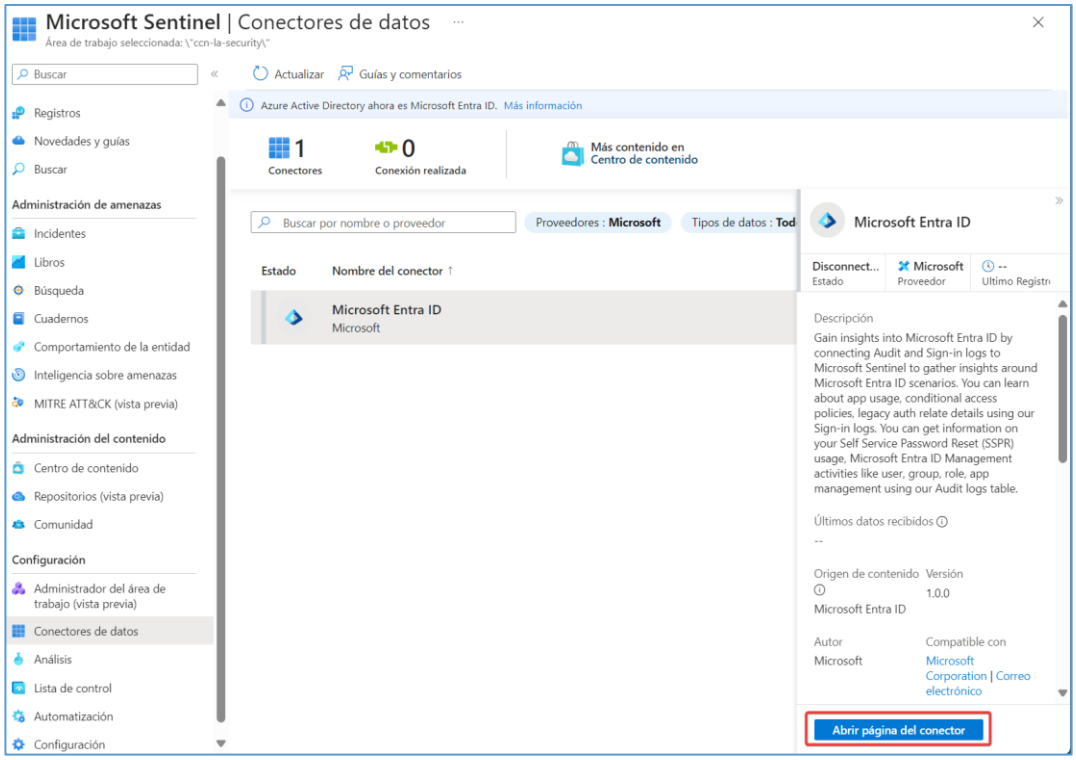


2. En la galería de conectores de datos, seleccionar Obtener estos conectores de datos. Esto abrirá el centro de contenido, donde se encuentran las soluciones, que a su vez, contienen los conectores de datos, Reglas de análisis, cuaderno de estrategias, etc.

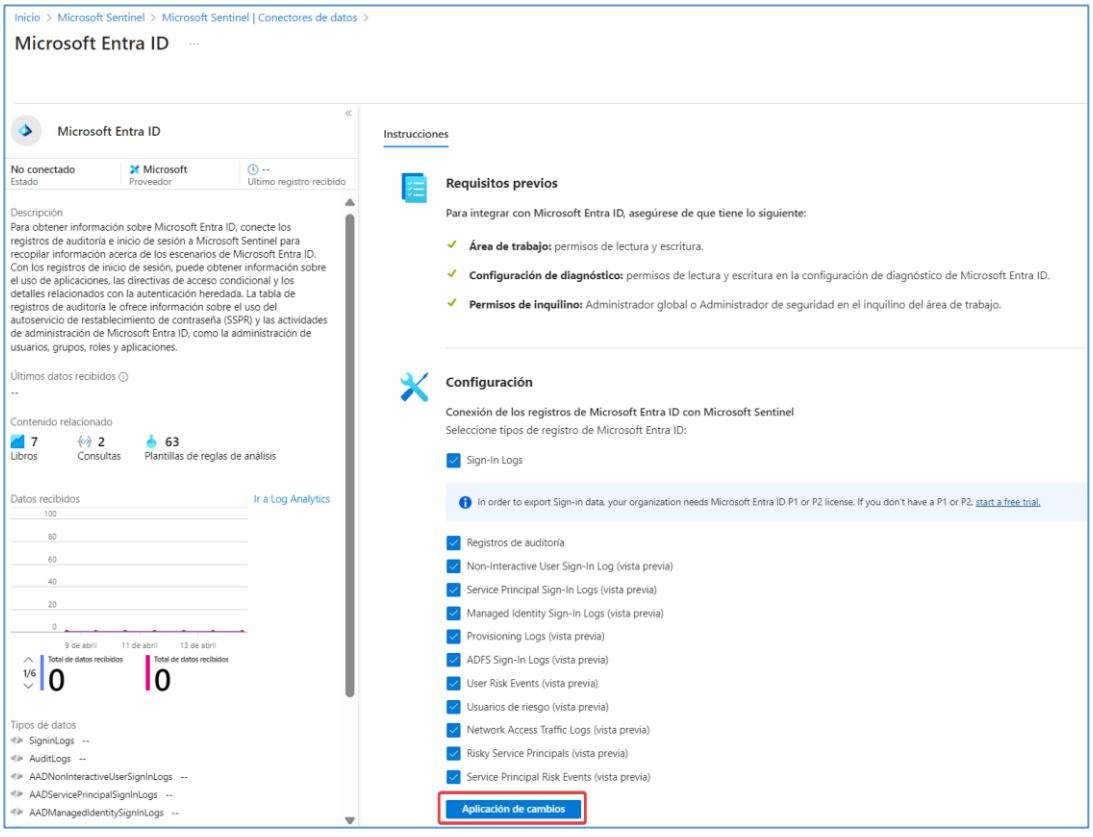

Centro de contenido
Actualizar
Instalar/actualizar
Eliminar
Migración de SIEM
Guías y comentarios
350
Soluciones
273
Contenido independiente
0
Instalado
0
Actualizaciones
Buscar...
Estado : Destacados
Tipo de contenido : Conector de datos (333)
Soporte técnico : Todo
Proveedor : Tod
Título del contenido
Estado
Origen de contenido
Proveedor
Amazon Web Services DESTACADOS Solution Amazon Web Services
Azure Activity DESTACADOS Solution Microsoft
Cisco Umbrella DESTACADOS Solution Cisco
Google Cloud Platform IAM DESTACADOS Solution Google
Microsoft Defender for Cloud DESTACADOS Solution Microsoft
Microsoft Defender XDR DESTACADOS Solution Microsoft
Microsoft Entra ID DESTACADOS Solution Microsoft
SAP applications DESTACADOS Solution Microsoft
Threat Intelligen... DESTACADOS VERSIÓN PRELIMINAR Solution Microsoft


Microsoft Entra ID
Microsoft
Proveedor
Microsoft
Soporte técnico
3.2.4
Versión
Note: Please refer to the following before installing the solution:
• Review the solution Release Notes
• There may be known issues pertaining to this Solution, please refer to them before installing.
The Microsoft Entra ID solution for Microsoft Sentinel enables you to ingest Microsoft Entra ID Audit, Sign-in, Provisioning, Risk Events and Risky User/Service Principal logs using Diagnostic Settings into Microsoft Sentinel.
Data Connectors: 1, Workbooks: 2, Analytic Rules: 62, Playbooks: 11
Learn more about Microsoft Sentinel | Learn more about Solutions
Tipo de contenido
63
Regla de análisis
1
Conector de datos
11
Cuaderno de estrategias
2
Libro
Categoría
Identidad, Seguridad: automatización (SOAR)
Precios
Gratis
Instalar
Ver detalles

3. Una vez instalado se configura el conector:



4. Activar las casillas que se encuentran junto a los tipos de registros que se quieren transmitir a Microsoft Sentinel (ver anteriormente).



2.2.1.2 AGREGAR CONECTOR DE AZURE ACTIVITY

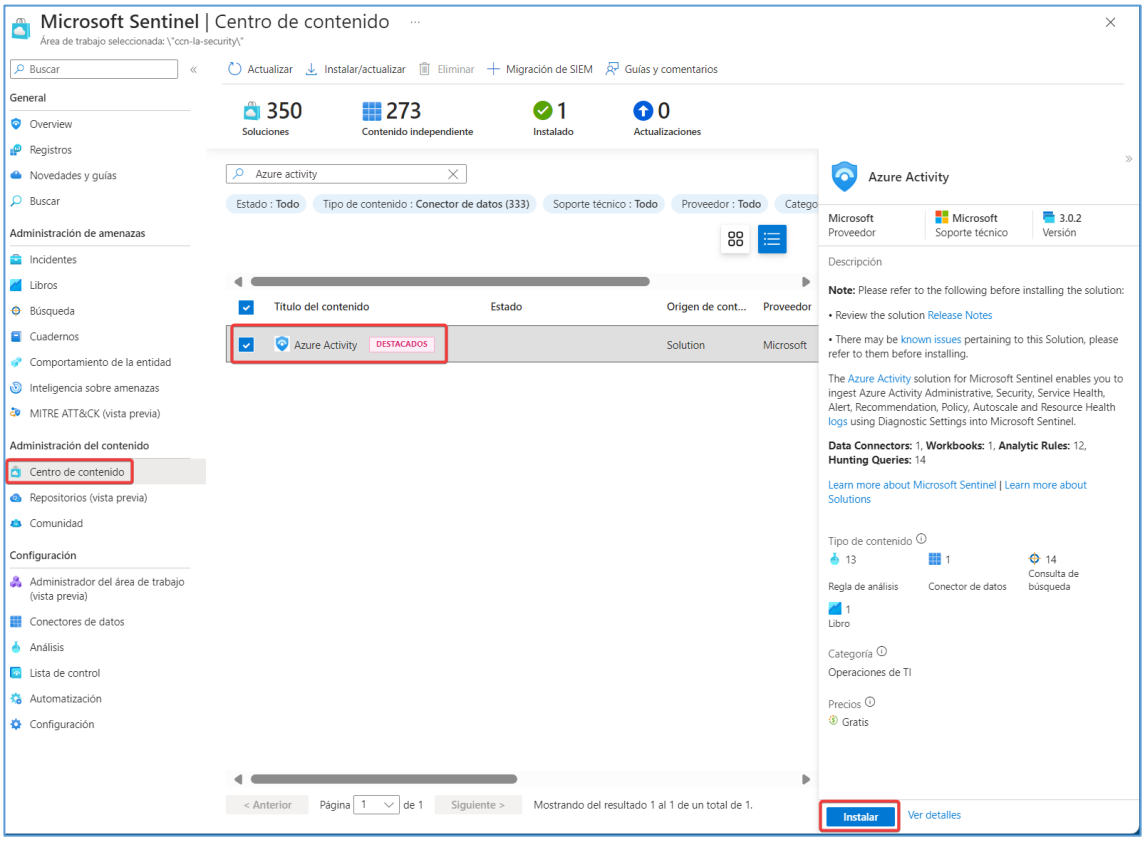
El registro de actividad es un registro de las suscripciones que graba y muestra los eventos de nivel de suscripción en Azure, desde los datos operativos de Azure Resource Manager hasta las actualizaciones de eventos de Service Health. Con el registro de actividades, se pueden determinar los interrogantes "qué, quién y cuándo" de las operaciones de escritura (PUT, POST, DELETE) que se realizan en los recursos de la suscripción.

Requisitos previos

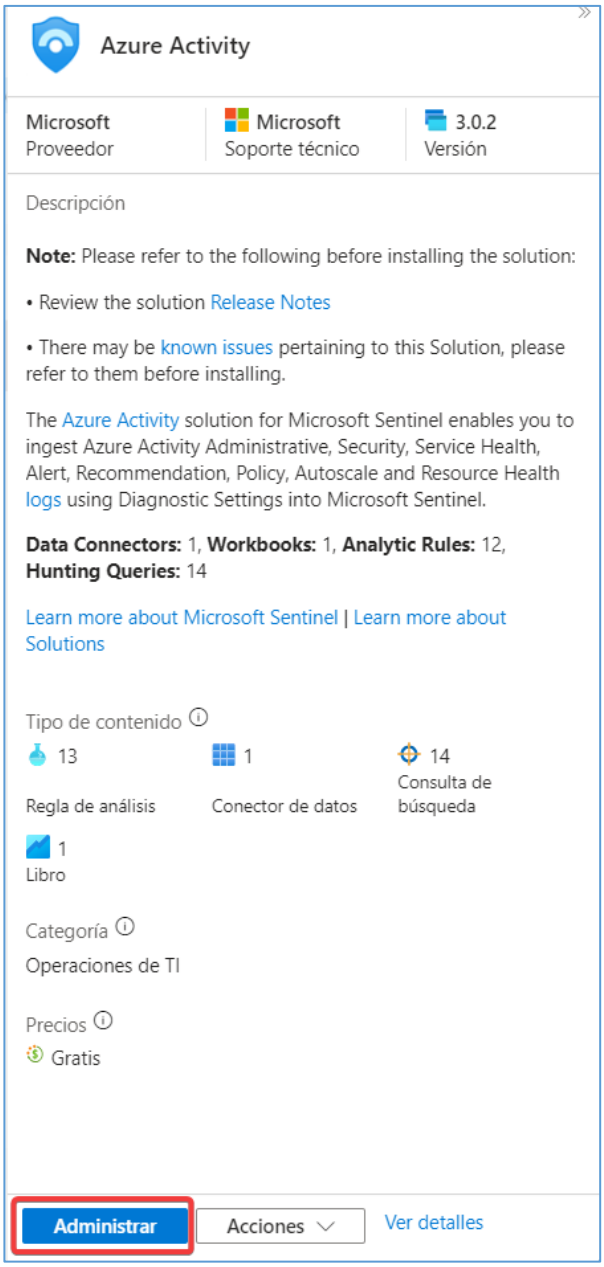
- El usuario debe tener permisos de colaborador en el área de trabajo de Log Analytics.
- El usuario debe tener permisos de lector en cualquiera de las suscripciones cuyos registros se quieren transmitir a Microsoft Sentinel.

Configuración del conector de actividad de Azure

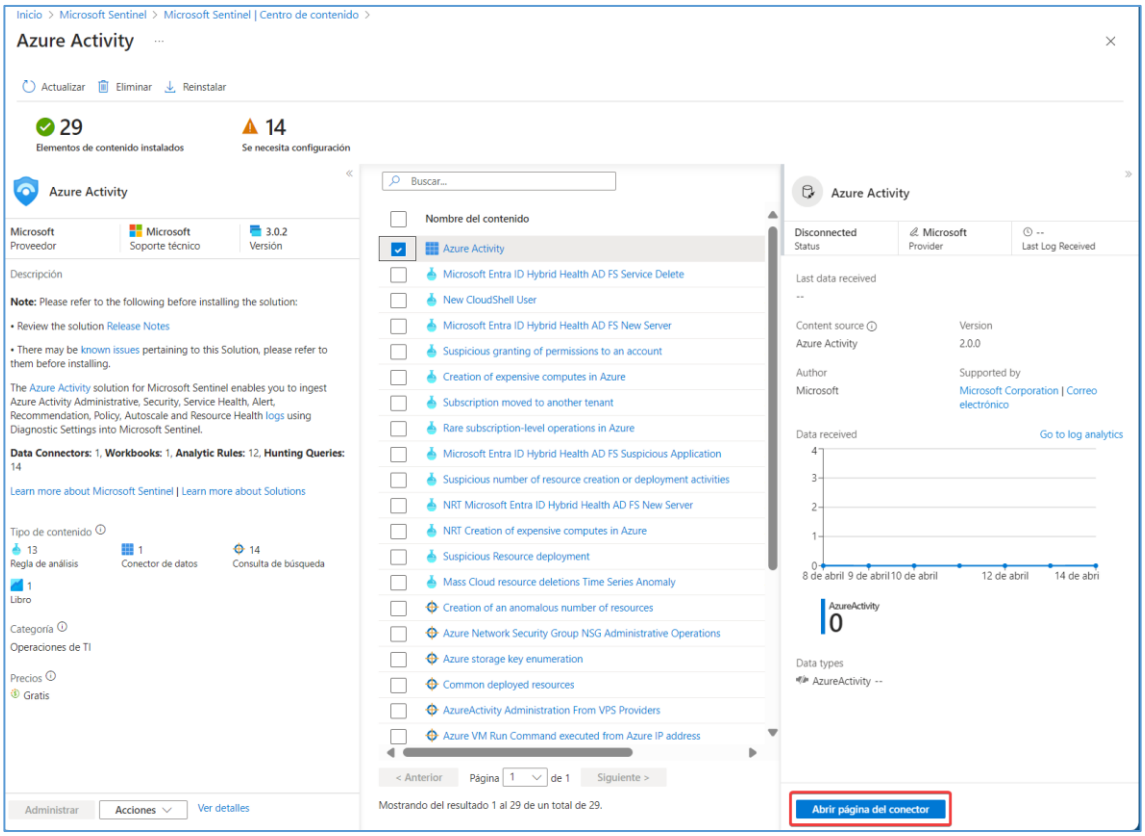
1. En el menú de navegación de Microsoft Sentinel, seleccionar *Centro de contenido*. En la lista de soluciones, hacer clic en Actividad de Azure y, a continuación, en el botón Instalar, en la parte inferior derecha.



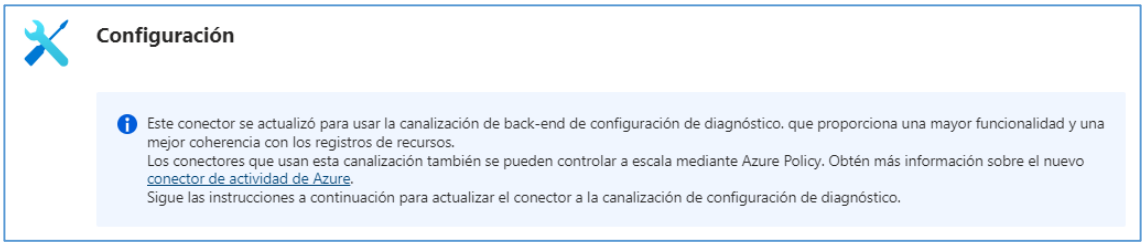
2. Una vez instalada la solución, se realizará la configuración del conector:



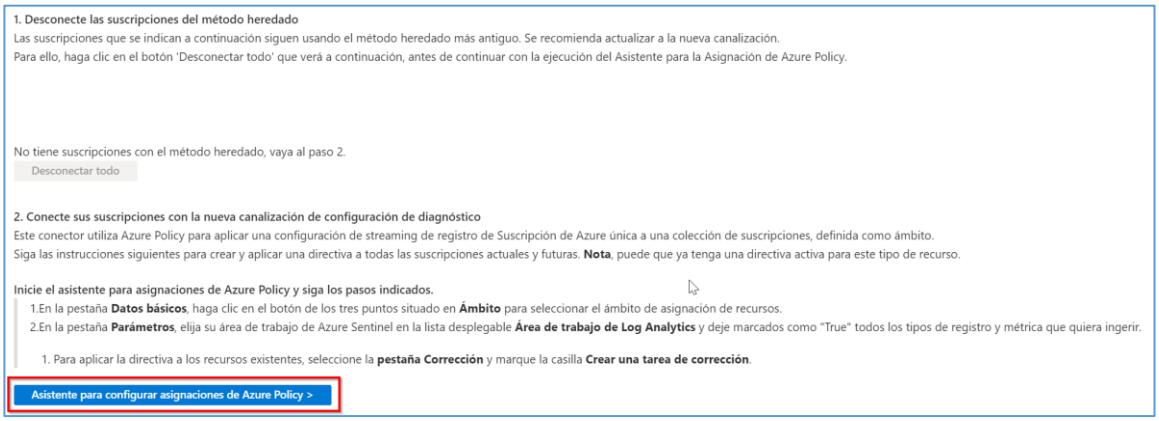
3. Seleccionar el conector y pulsar el botón Abrir página del conector:



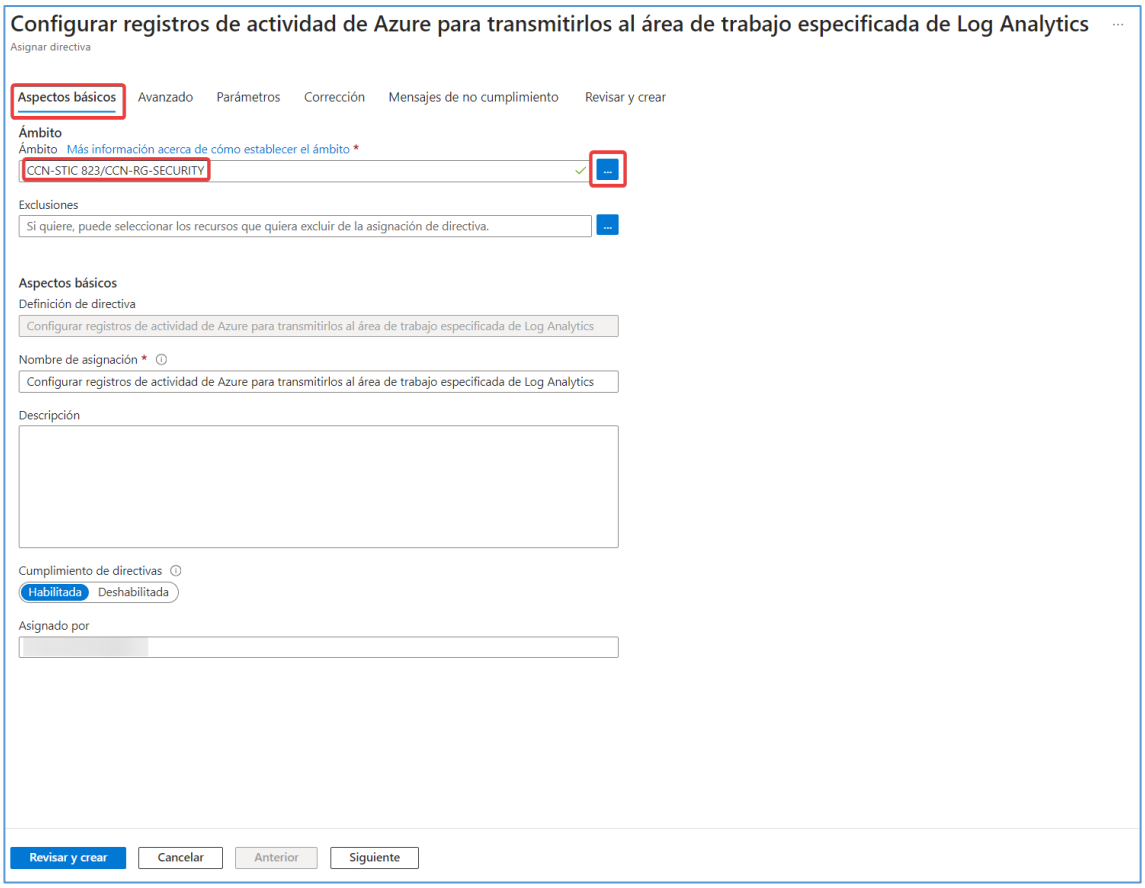
4. En la pestaña Instrucciones, aparece un mensaje que indica que el conector se ha actualizado para cambiar el mecanismo interno de recolección de eventos:



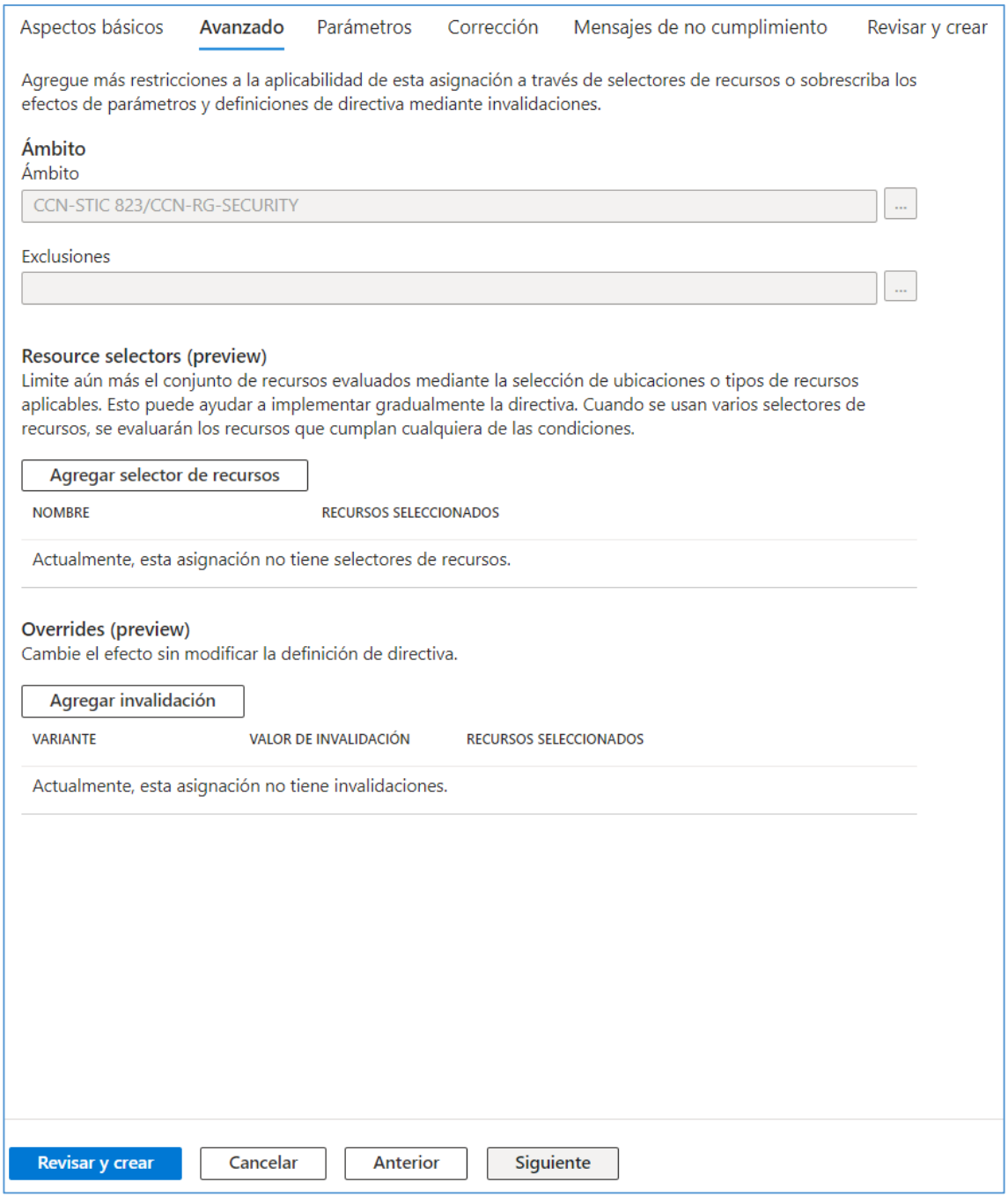
5. Para configurar este conector se necesitará habilitar una Azure Policy donde se establecerá la suscripción de la que se va a recoger los eventos:



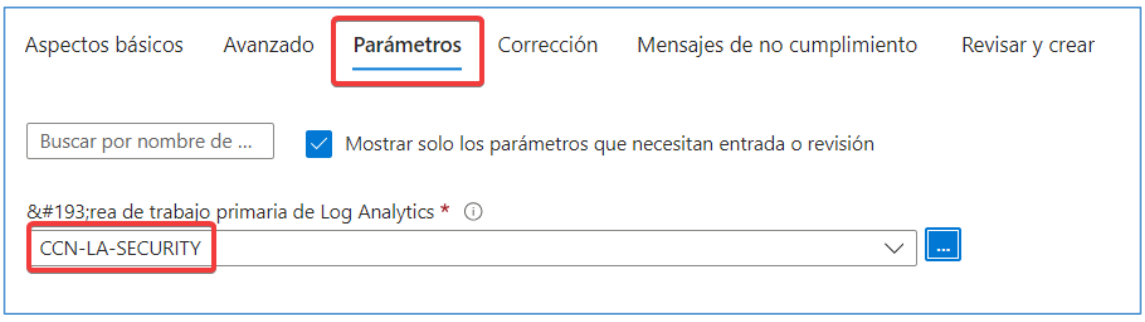
6. Una vez lanzado el asistente para la creación de Azure Policy, en la pestaña **Aspectos Básicos** → seleccionar el ámbito.



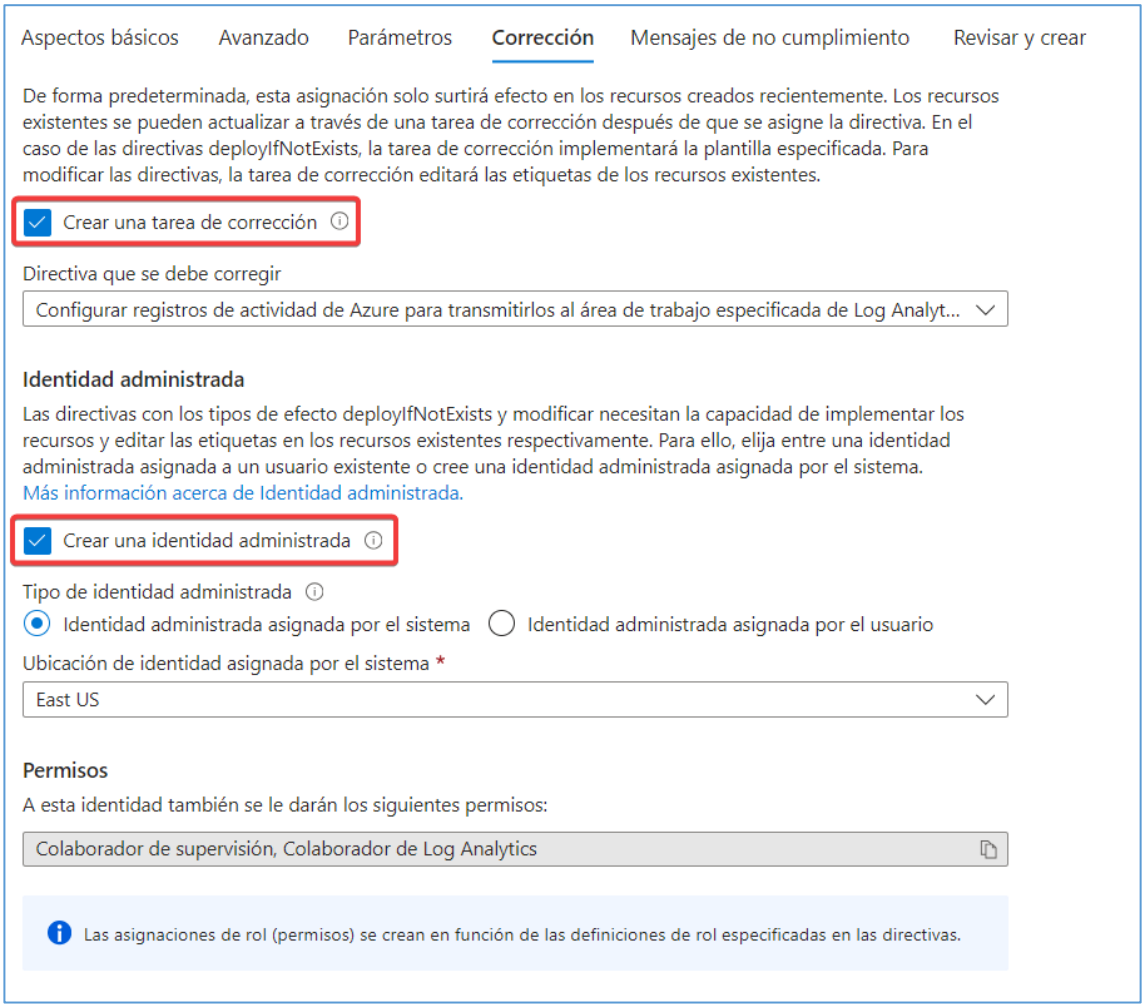
7. En la pestaña de Avanzado se puede afinar más aún el ámbito de aplicación de la política:



8. En la pestaña de Parámetros seleccionar el área de trabajo de Sentinel.



9. En la pestaña Corrección, es necesario habilitar **Crear una tarea de corrección**, de esta manera la directiva no solo aplicará a los recursos que se creen, también aplicará a los recursos ya existentes. Además, también se puede crear una entidad administrada:



10. Seleccionar **Revisar y crear** para crear la asignación de directiva.

2.2.1.3 AGREGAR EL CONECTOR MICROSOFT DEFENDER XDR

El conector Microsoft Defender XDR de Microsoft Sentinel permite incorporar alertas/incidentes de seguridad y registros sin procesar de los productos de la suite Microsoft Defender XDR y mantiene los incidentes sincronizados entre ambos portales. Los incidentes de Defender incluyen todas sus alertas, entidades y otra información relevante, completando y agrupando las alertas del resto de los servicios integrados en Microsoft Defender XDR: **Microsoft Defender for Endpoint, Microsoft Defender for Identity, Microsoft Defender for Office 365, Microsoft Defender for Cloud Apps**.

El conector permite enviar eventos de **búsqueda de amenazas** desde Microsoft Defender for Endpoint a Microsoft Sentinel. Copiando consultas de búsqueda avanzada de Defender for Endpoint en Microsoft Sentinel, enriqueciendo las alertas de Sentinel con datos de eventos sin formato de Defender for Endpoint para proporcionar

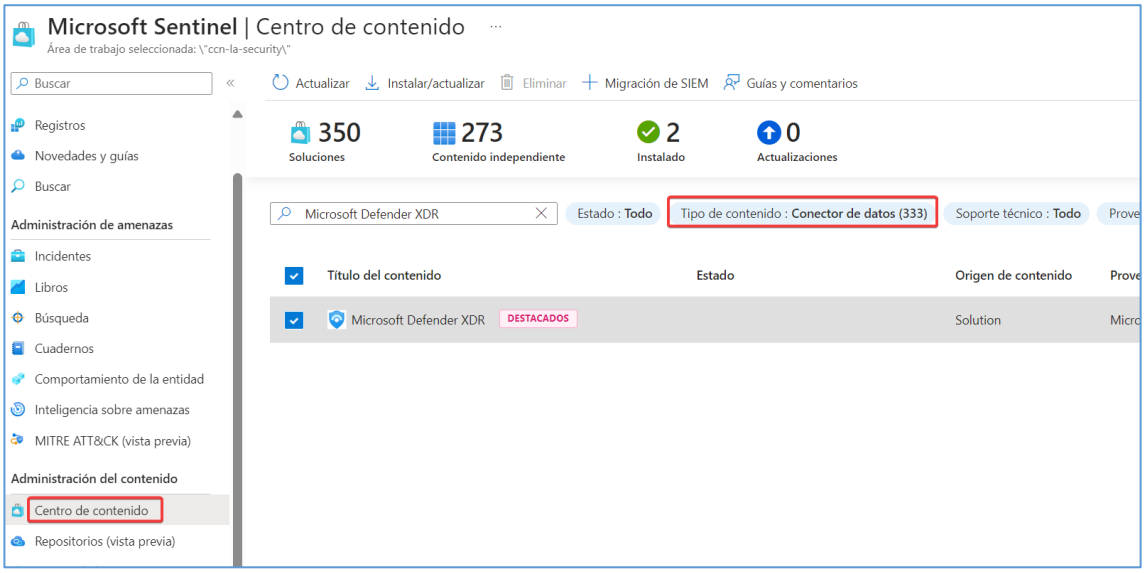
información adicional y almacenar los registros con un mayor periodo de retención en Log Analytics. También se incluye la prevención de pérdida de datos de Microsoft Purview y Azure AD Identity Protection.

Requisitos previos

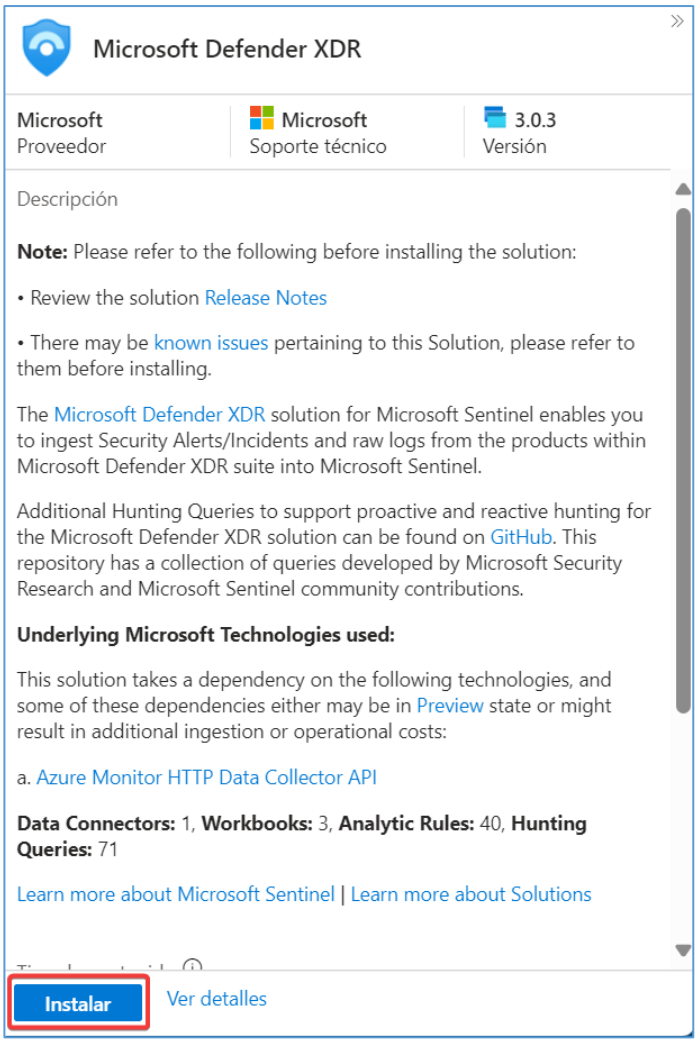
- Se debe tener una licencia válida de Microsoft Defender XDR, como se describe en Requisitos previos de Microsoft Defender XDR.
- El usuario debe ser **administrador global** o un **administrador de seguridad** en Microsoft Entra ID.

2.2.1.4 Conexión a Microsoft Defender XDR

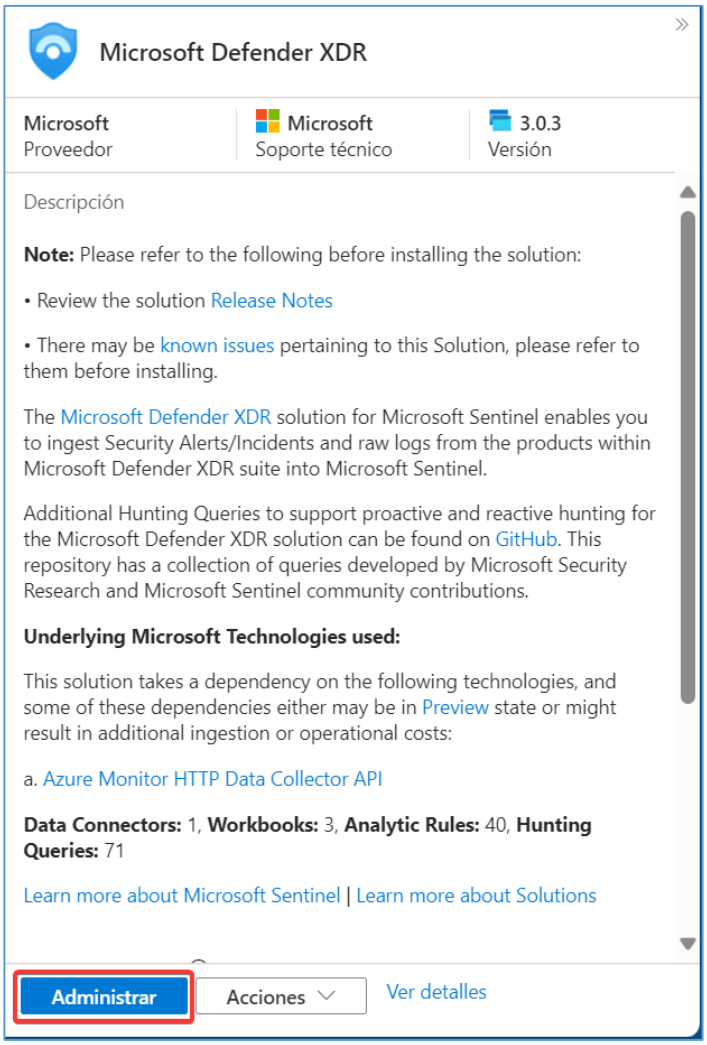
1. En Microsoft Sentinel, seleccionar Centro de contenido, filtrar por Tipo de contenido y elegir la solución: Microsoft Defender XDR.



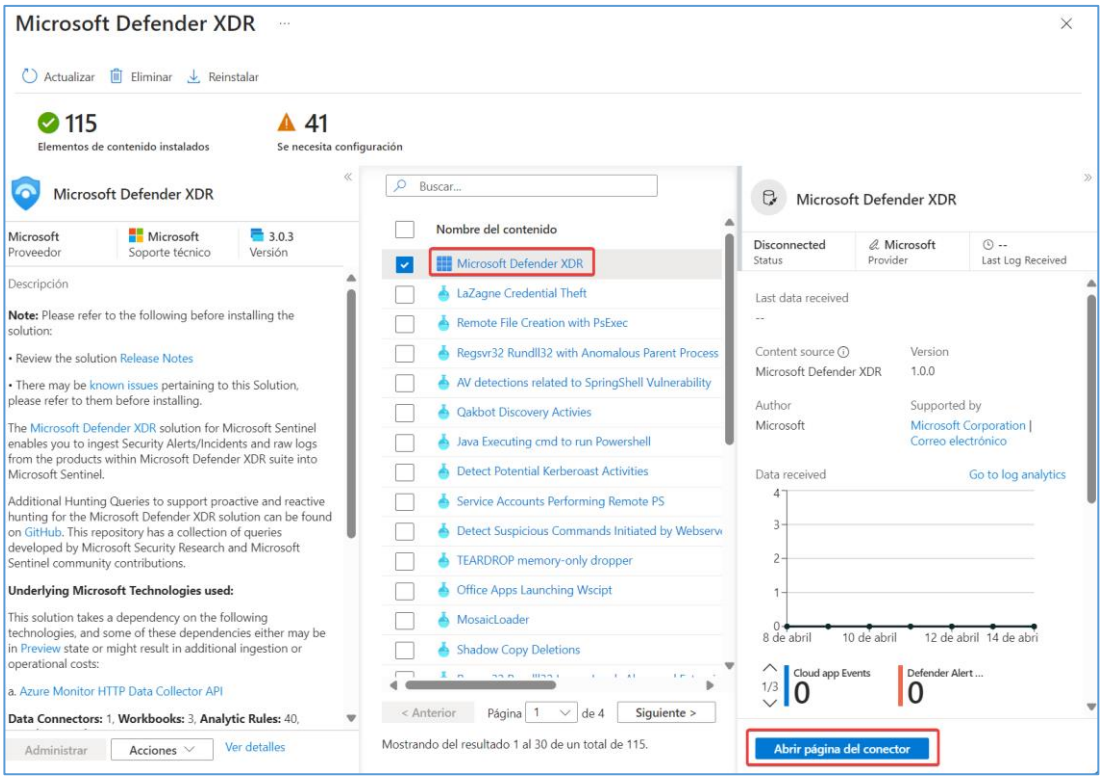
2. Seleccionar Microsoft Defender XDR y, a continuación, hacer clic en el botón Instalar, en la parte inferior derecha:



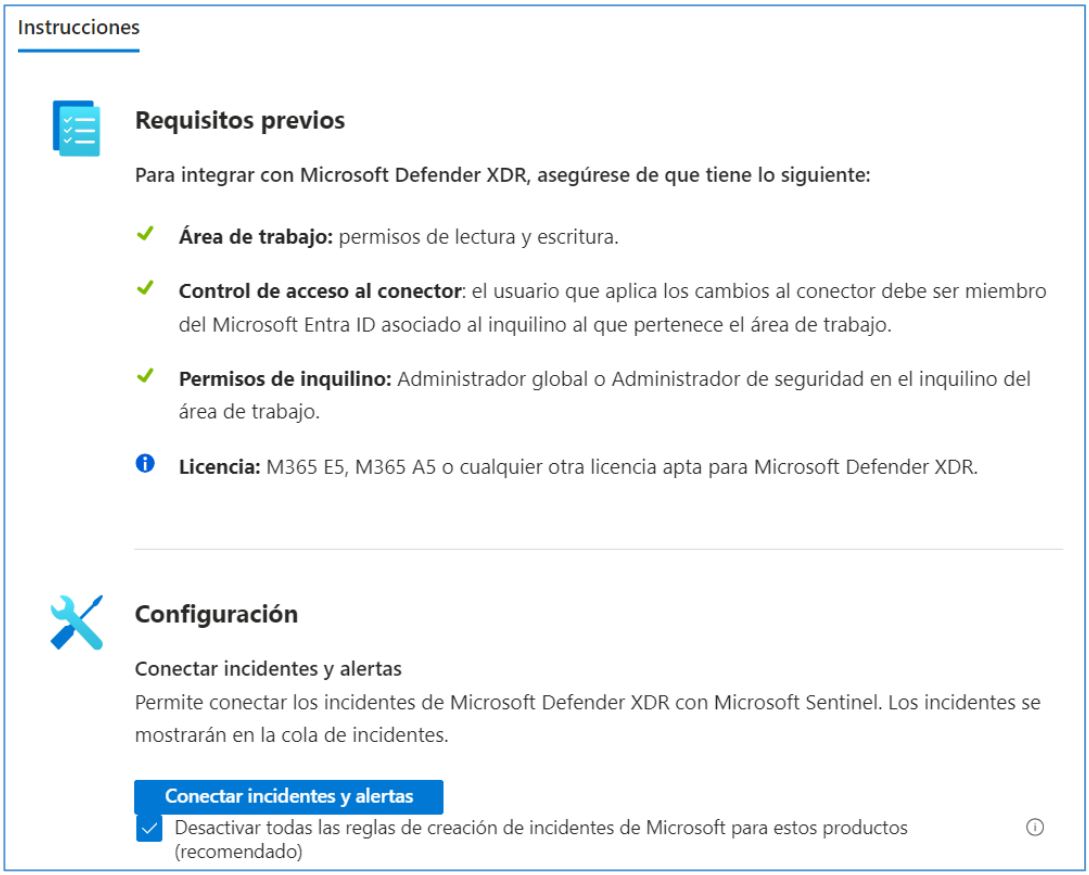
3. Una vez instalada la solución, se realizará la configuración del conector:



4. Seleccionar el conector y pulsar el botón Abrir página del conector:



5. En la página del conector aparecen las instrucciones para configurar el conector, así como otras instrucciones adicionales que se puedan necesitar.



6. Después de conectar los orígenes de datos, se podrán utilizar los *workbooks* creados por expertos en seguridad que exponen información basada en los datos. Estos workbooks también se pueden personalizar fácilmente en función de las necesidades. Además de los workbooks, y dependiendo de la solución instalada, fse incluyen: consultas, Plantillas de reglas de análisis, Consulta de búsqueda, etc.

2.2.1.5 Agregar conector Microsoft Defender for Endpoint

El conector de Microsoft Defender for Endpoint permite enviar alertas de Microsoft Defender for Endpoint a Microsoft Sentinel. Esto permitirá analizar de manera más exhaustiva los eventos de seguridad en la organización y crear playbooks para obtener una respuesta efectiva e inmediata.

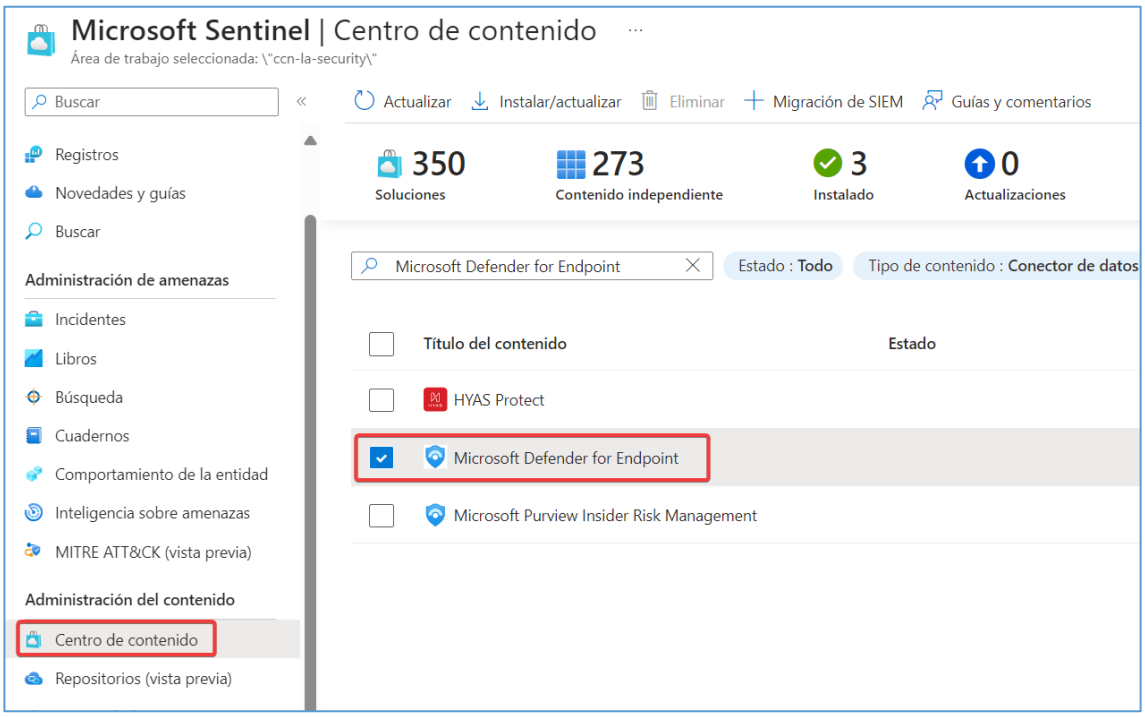
Requisitos previos

- El usuario debe tener una licencia válida de Microsoft Defender para Endpoint, tal como se describe en Configuración de la implementación de Microsoft Defender para Endpoint.
- El usuario debe ser administrador global o de seguridad en el inquilino de Microsoft Sentinel.

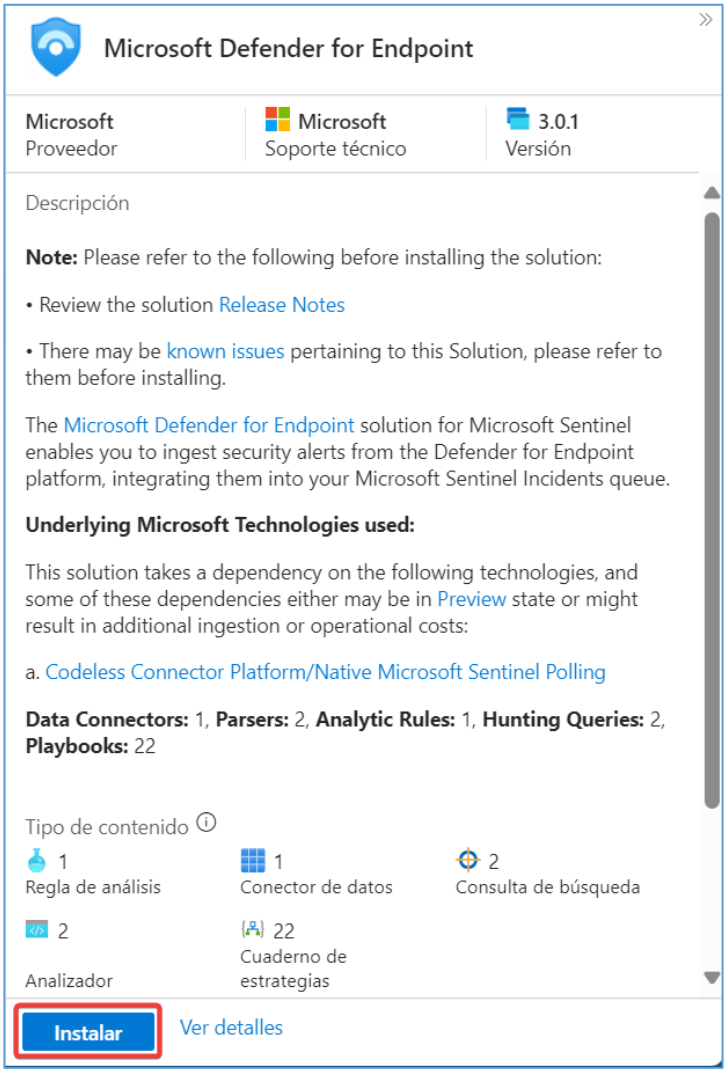
Conexión a Microsoft Defender para Endpoint

Si Microsoft Defender para Endpoint ya está implementado e ingiriendo datos, las alertas se pueden transmitir a Microsoft Sentinel muy fácilmente.

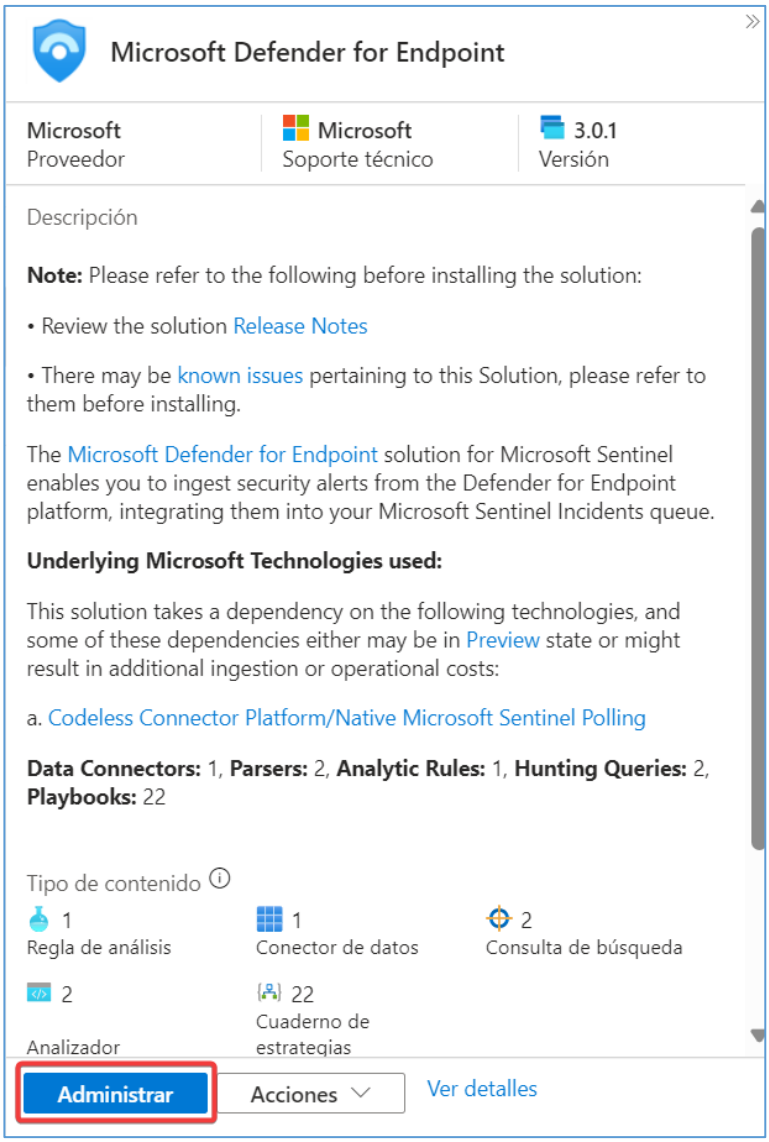
- En el menú principal, se seleccionará *Centro de contenido*. Seleccionar Microsoft Defender for Endpoint:



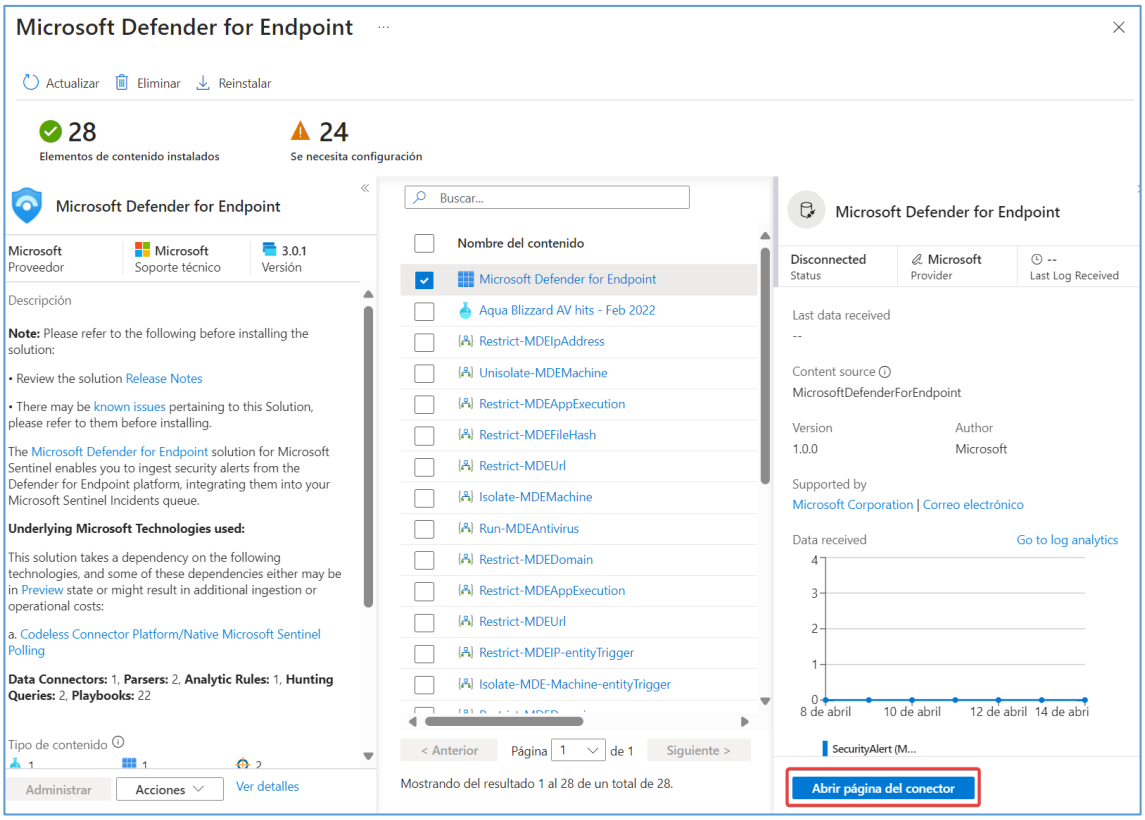
- Seleccionar Microsoft Defender XDR y, a continuación, hacer clic en el botón Instalar, en la parte inferior derecha



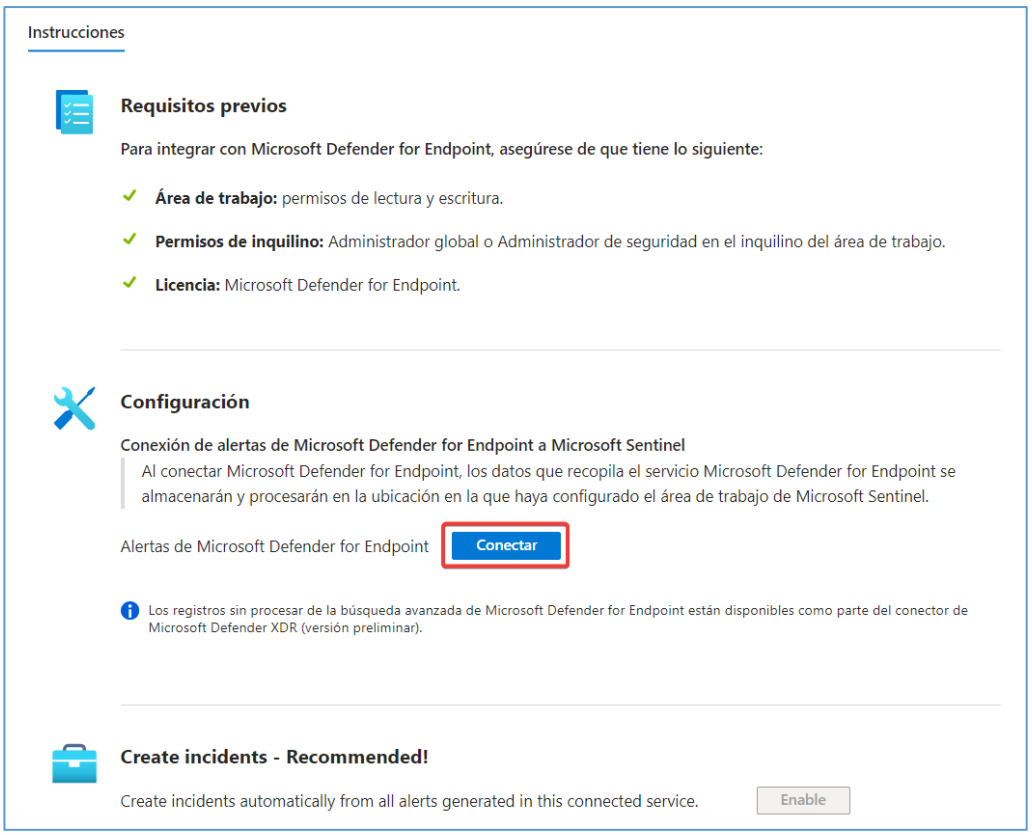
- Una vez instalada la solución, se realizará la configuración del conector:



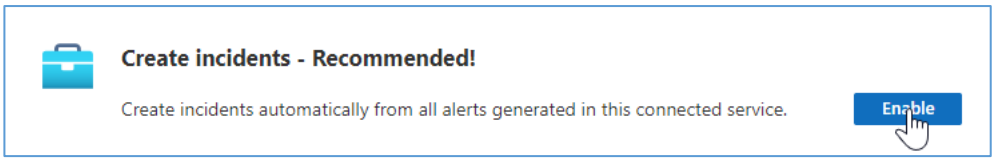
- Seleccionar el conector y pulsar el botón Abrir página del conector



- En la página del conector aparecen las instrucciones para configurar el conector, así como otras instrucciones adicionales que se puedan necesitar.



Se recomienda crear incidentes automáticamente desde las alertas generadas por el servicio conectado:



2.2.1.6 AGREGAR EL CONECTOR PARA RECOLECTAR DATOS DE AWS CLOUDTRAIL

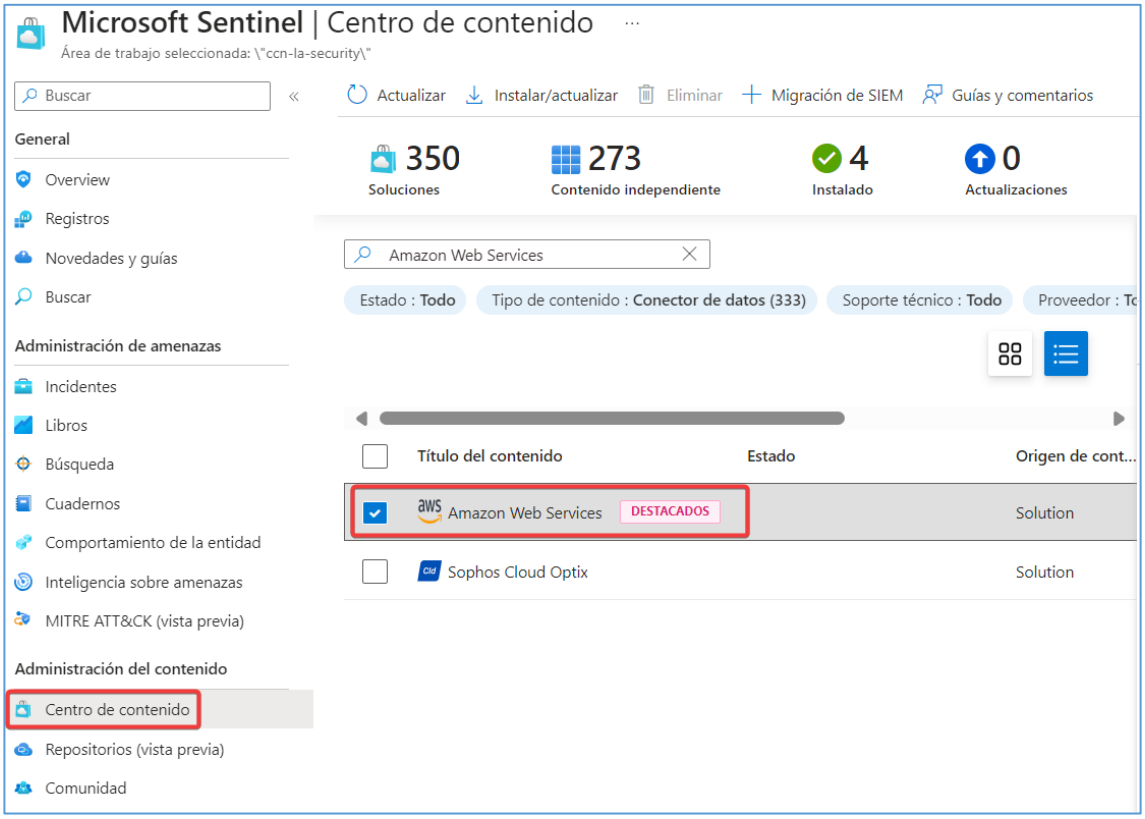
En un escenario multinube, en el que haya recursos en la nube de Amazon, conocida como Amazon Web Services, es interesante conectar el servicio AWS CloudTrail. Este servicio monitoriza y registra la actividad de la cuenta en toda la infraestructura de AWS, lo que permite controlar las acciones de almacenamiento, análisis y reparación.

Requisitos previos

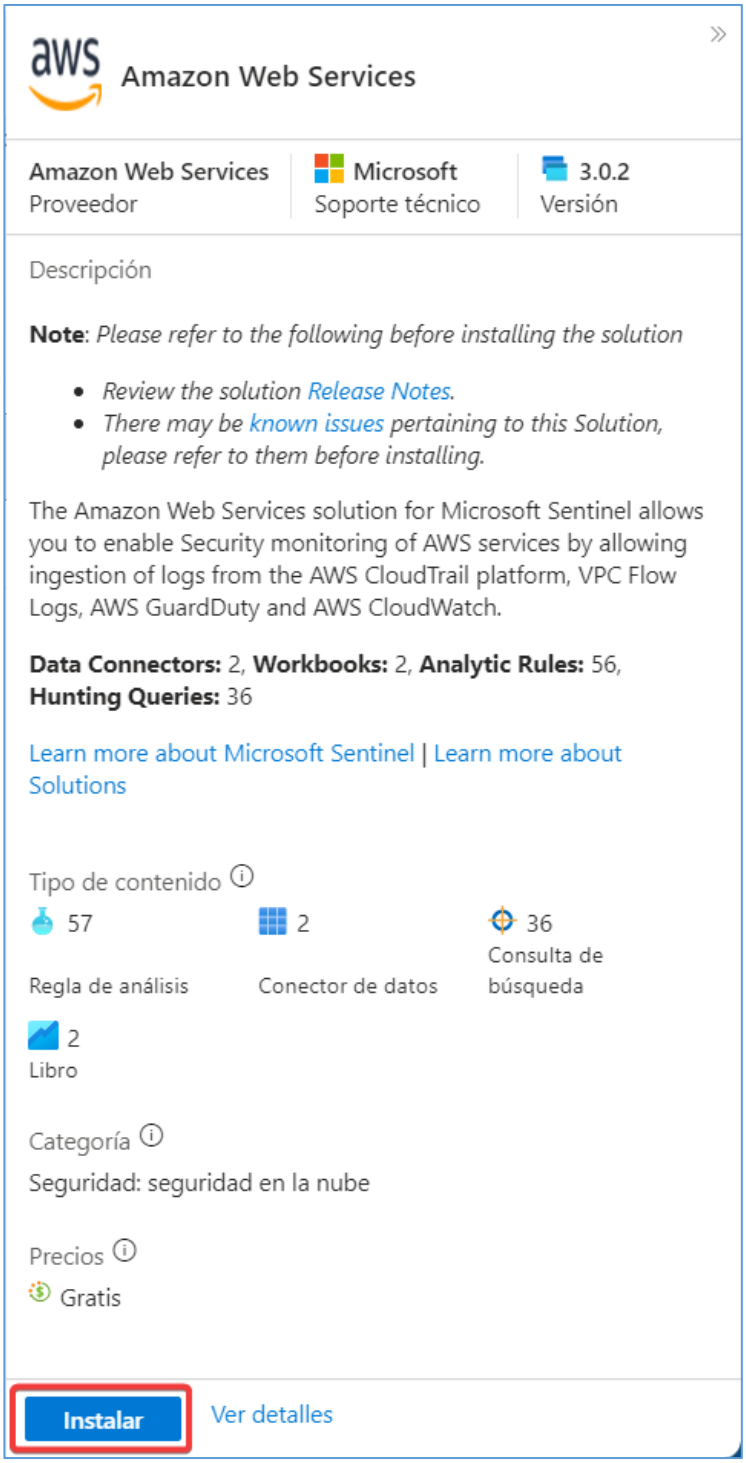
- El usuario debe tener permiso de escritura en el área de trabajo de Microsoft Sentinel.

Conexión de AWS

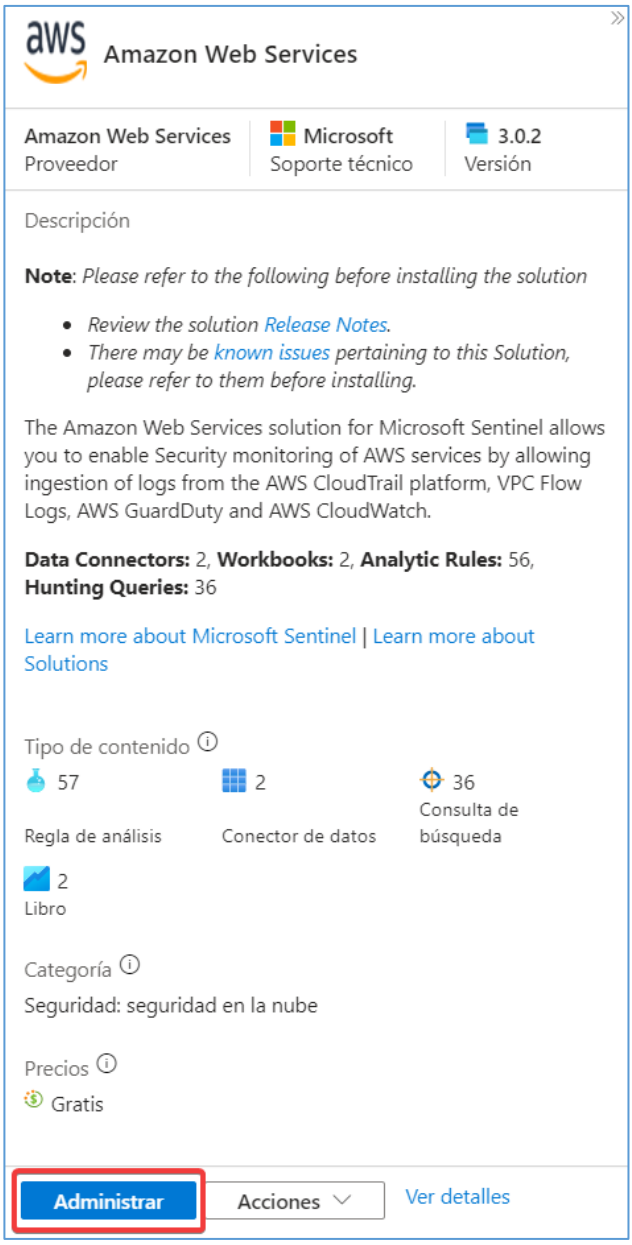
1. En Microsoft Sentinel, seleccionar Centro de contenido y, a continuación, Amazon Web Services.



2. Después, en el panel de AWS situado a la derecha, seleccionar Instalar.

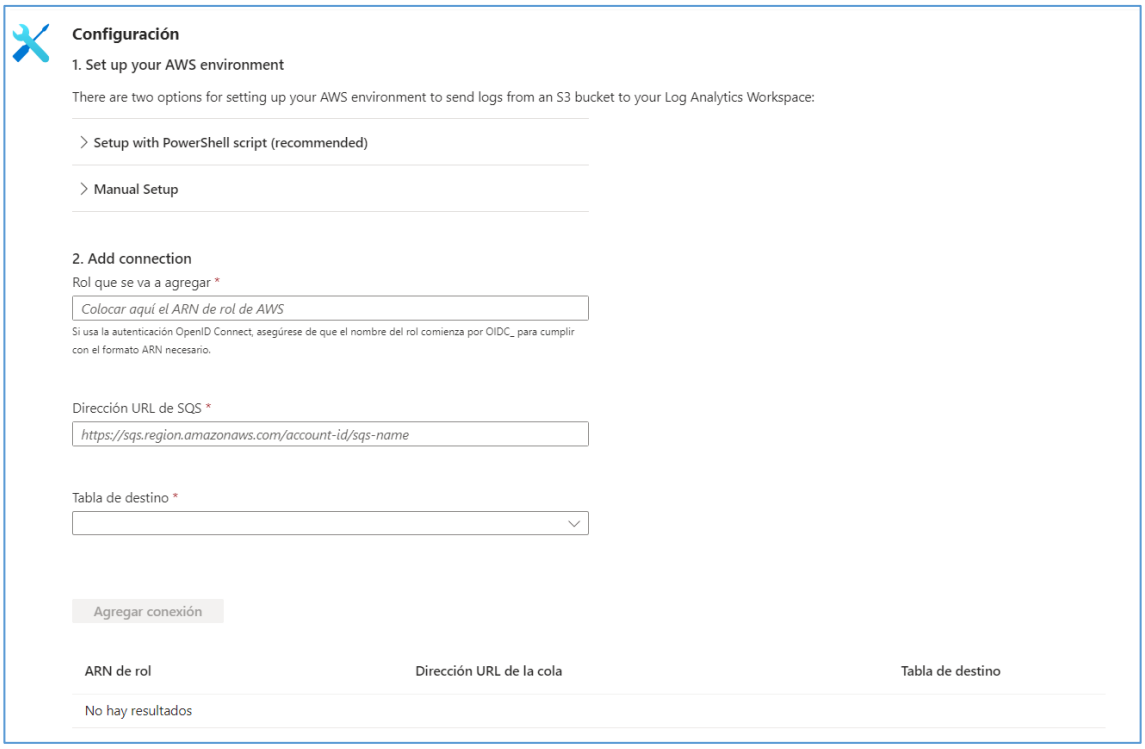


3. Una vez instalada la solución, se realizará la configuración del conector



4. Seleccionar el conector y pulsar el botón Abrir página del conector

5. Seguir las instrucciones que aparecen en Configuración mediante los pasos siguientes.



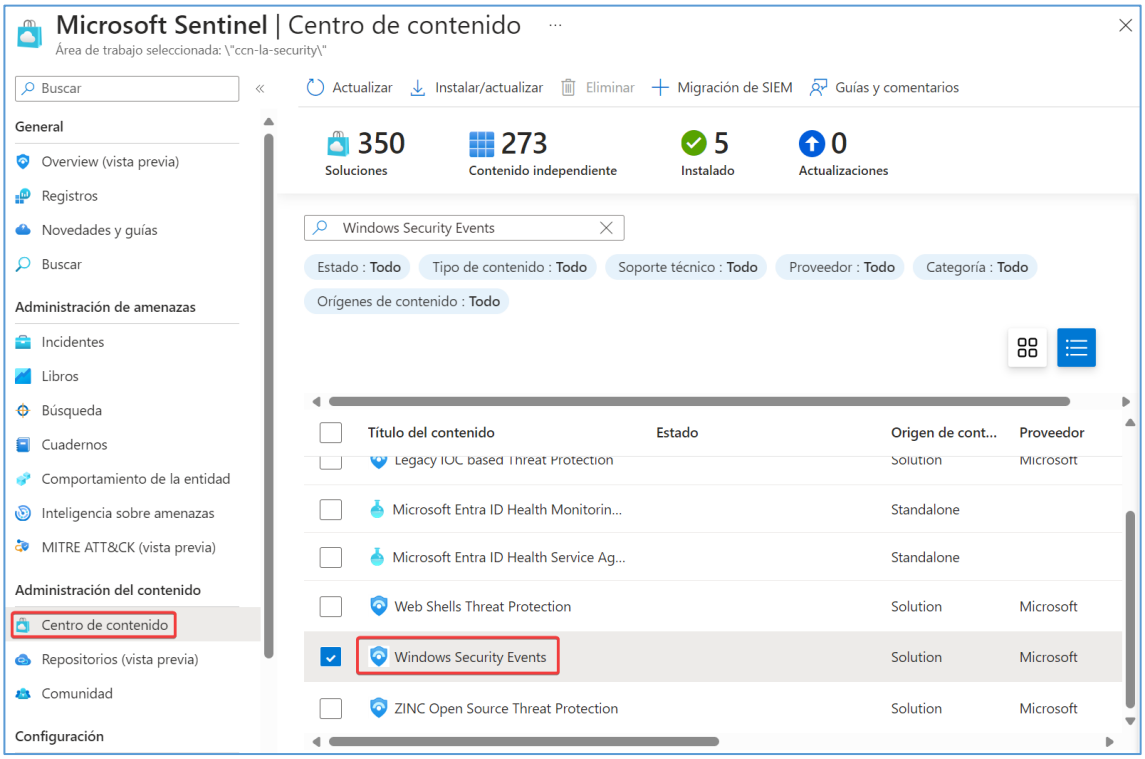
6. Para simplificar el proceso de incorporación, existe un script de PowerShell para automatizar la configuración de la parte de AWS del conector: los recursos, las credenciales y los permisos de AWS necesarios. El script realiza las siguientes acciones:
    a. Crea un proveedor de identidad web OIDC, para autenticar a los usuarios de Microsoft Entra ID en AWS.
    b. Crea un rol IAM con los permisos mínimos necesarios, para otorgar a los usuarios autenticados por OIDC acceso a sus registros en un determinado bucket S3 y cola SQS.
    c. Habilita los servicios de AWS especificados para enviar logs a ese bucket de S3 y mensajes de notificación a esa cola de SQS.
    d. Si es necesario, crea ese bucket de S3 y esa cola de SQS para este fin.
    e. Configura las políticas de permisos de IAM necesarias y las aplica al rol de IAM creado anteriormente.
    f. Para las nubes Azure Government, un script especializado crea un proveedor de identidad web OIDC diferente, al que asigna el rol IAM.
7. Una vez finalizado el script se mostrará por consola los datos necesarios para configurar el conector. Es necesario copiar el ARN de rol y la dirección URL de SQS de la salida del script, para posteriormente pegarlos en sus respectivos campos en la configuración del conector que se ha mostrado anteriormente:

```
Updating the SQS policy to allow S3 notifications, and ARN to read/delete/change visibility of SQS messages and get queue url
  Changes S3: SQS SendMessage permission to 'vpc-sentinel-demo' s3 bucket
  Changes Role ARN: SQS ChangeMessageVisibility, DeleteMessage, ReceiveMessage and GetQueueUrl permissions to 'SentinelDemo' rule

Attaching S3 read policy to Sentinel role.

Changes Role arn: S3 Get and List permissions to 'SentinelDemo' rule


Updating the S3 policy to allow Sentinel to read the data.
Changes: S3 Get and List permissions to 'SentinelDemo' rule



Enabling S3 event notifications (for *.gz file)

Please enter the event notifications name: demo
  Using event notification name: demo
Event notificaion prefix definition, to Limit the notifications to objects with key starting with specified characters.

The default prefix is 'AWSLogs/123412341234/vpcflowlogs/'.
  Do you want to override the event notification prefix? [y/n]: n


Use the values below to configure the Amazon Web Service S3 data connector in the Azure Sentinel portal.

Role Arn: arn:aws:iam::123412341234:role/SentinelDemo
Sqs Url: https://sqs.us-east-1.amazonaws.com/123412341234/vpc-sentinel-demo
Destination Table: AWSVPCFlow
```

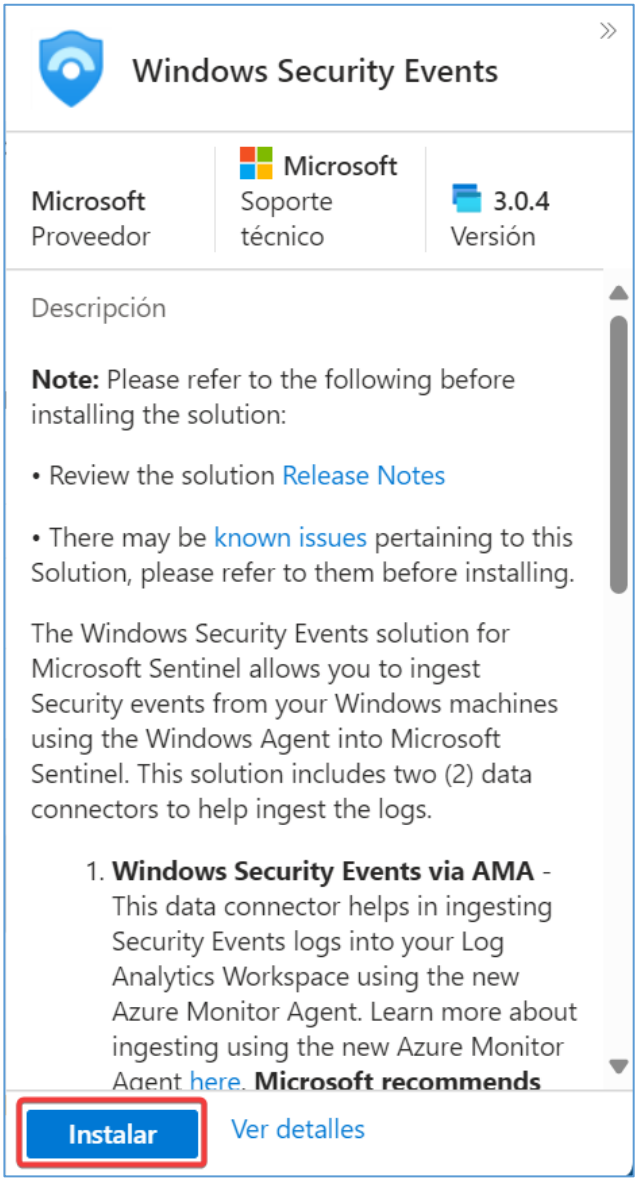
2.2.1.7 CONFIGURACIÓN DEL CONECTOR DE EVENTOS DE SEGURIDAD DE WINDOWS

La solución de eventos de seguridad de Windows incluye dos tipos de conectores que permiten transmitir eventos de seguridad desde cualquier servidor de Windows (físico o virtual, local o en cualquier nube) conectado al área de trabajo de Microsoft Sentinel. Estos eventos se pueden usar en la creación de alertas personalizadas y basarse en ellos para mejorar las investigaciones, lo que proporcionará más información sobre la red de la organización y amplía las funciones de las operaciones de seguridad.

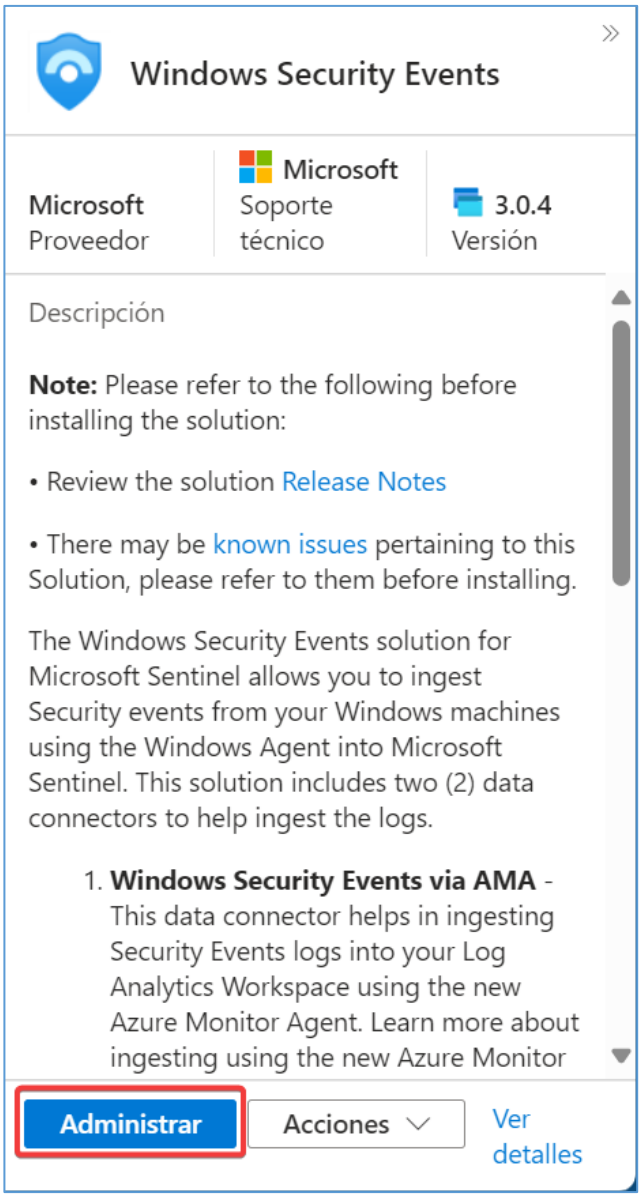
- En el menú principal, se seleccionará *Centro de contenido*. Seleccionar Windows Security Events:



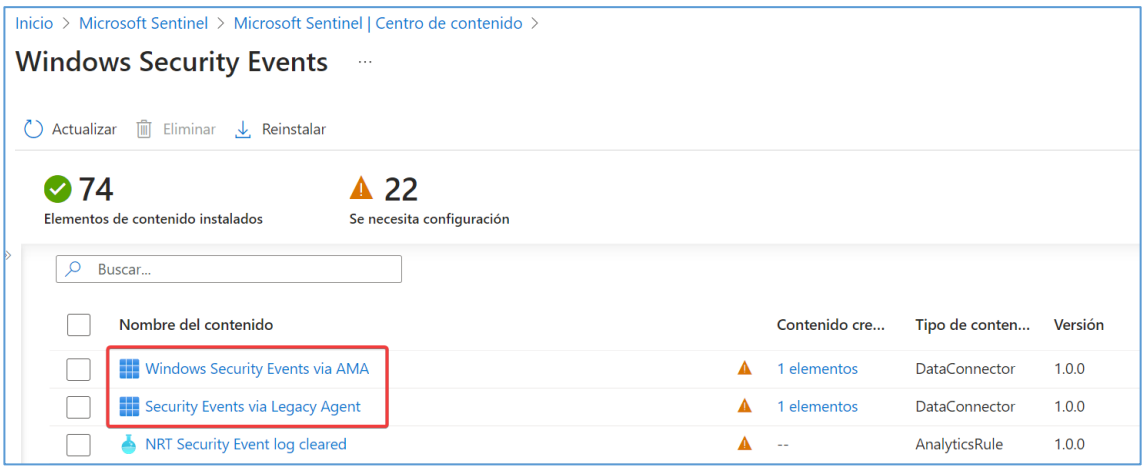
- Seleccionar Windows Security Events y, a continuación, hacer clic en el botón Instalar, en la parte inferior derecha



- Una vez instalada la solución, se realizará la configuración de los conectores:



- Se muestran los dos conectores disponibles:

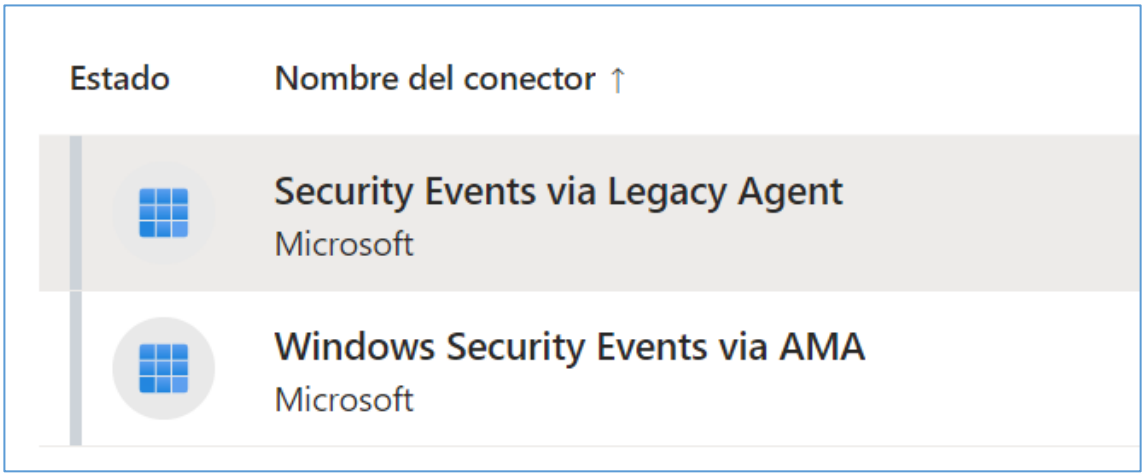


Tipo de agente instalado

La solución eventos de seguridad de Windows admite dos tipos de conectores en base al agente utilizado:

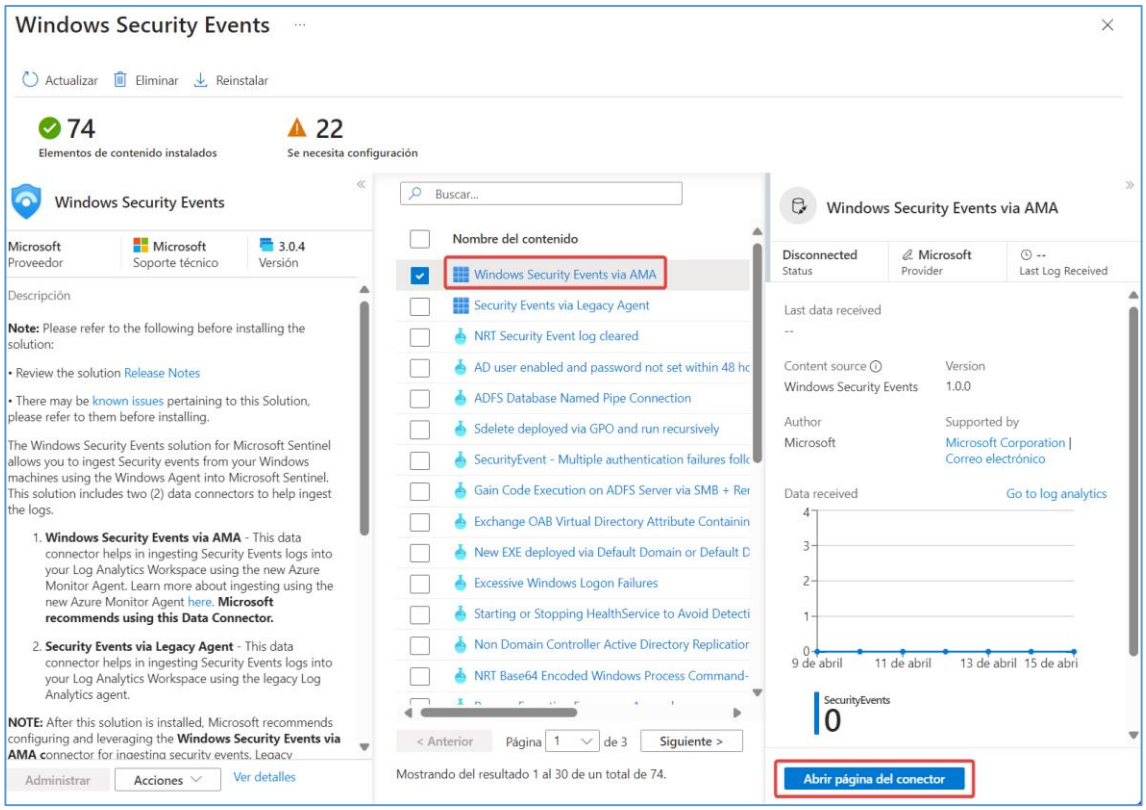
- **Eventos de seguridad de Windows**: Versión heredada, basada en el agente de Log Analytics y a veces conocida como Microsoft Monitoring Agent (MMA) o el agente OMS. El agente de Log Analytics se retirará el 31 de agosto de 2024 y por este motivo se va a omitir su configuración en esta guía. Se recomienda migrar a la versión reciente del agente de Azure Monitor (AMA).
- **Eventos de seguridad de Windows via AMA**: Versión más reciente, actualmente en versión preliminar, basada en el agente de Azure Monitor (AMA). Admite características adicionales, como el filtrado de registros previos a la ingesta y las reglas de recopilación de datos individuales para determinados grupos de máquinas. Se recomienda el uso de este conector.

Para cada versión de agente existe un conector:

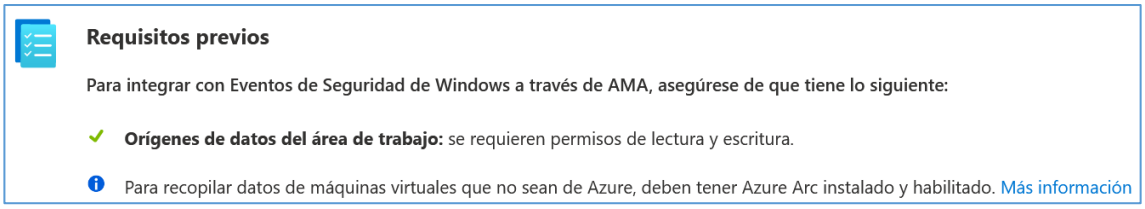


Configuración del conector de eventos de seguridad de Windows a través de AMA

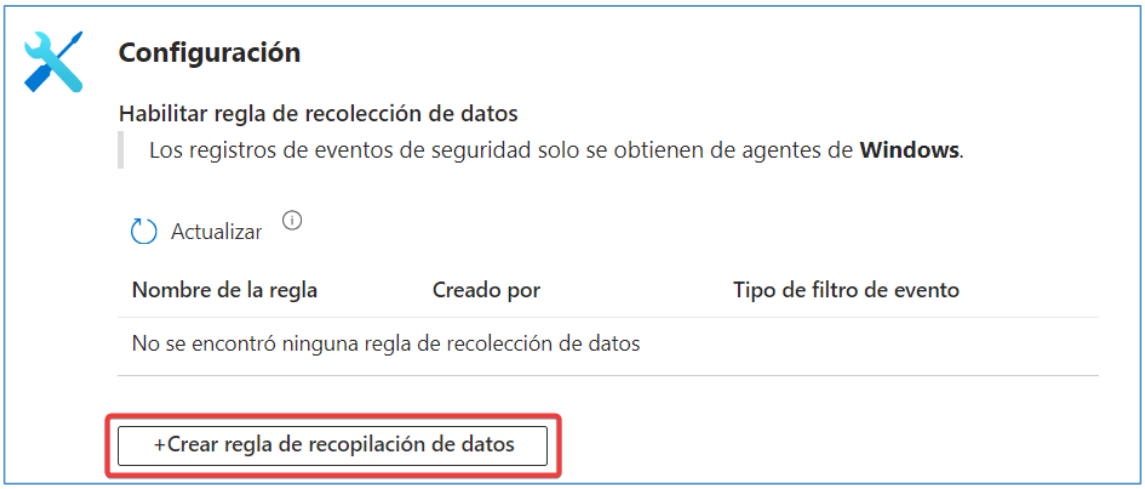
1. En el centro de contenido, seleccionar Windows Security Events → administrar, a continuación, seleccionar el conector **Windows Security Events via AMA** y, a continuación, pulsar en el botón **Abrir página del conector** en la parte inferior derecha.



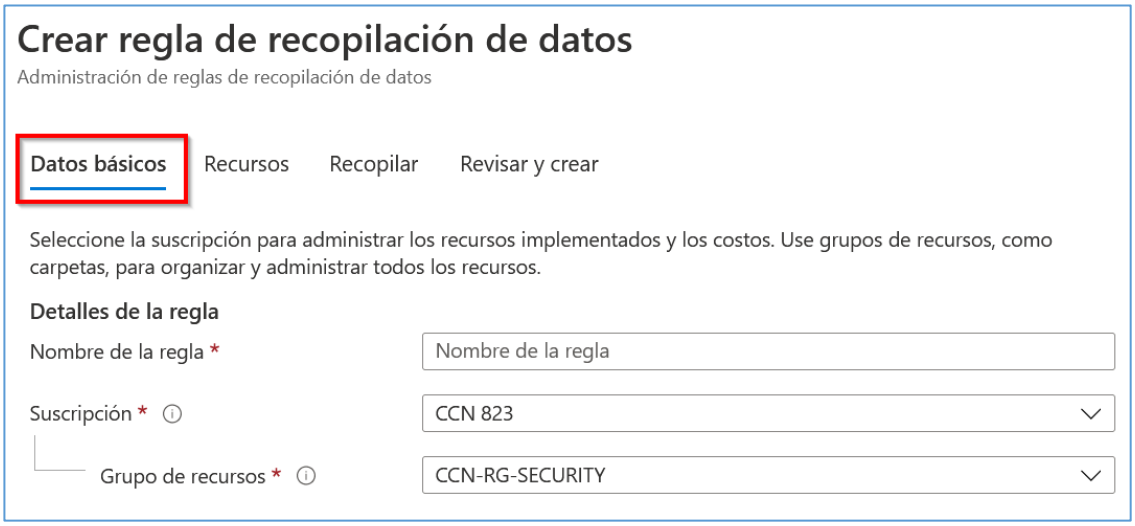
2. A continuación, siga las instrucciones en pantalla debajo de la pestaña **Instrucciones**.
3. Comprobar los permisos adecuados, tal como se describe en la sección **Requisitos previos** de la página del conector.
    1. Es necesario permisos de lectura y escritura en el área de trabajo y en todos los orígenes de datos desde los que va a ingerir eventos de seguridad de Windows.
    2. Para recopilar eventos de máquinas Windows que no sean máquinas virtuales de Azure, las máquinas (físicas o virtuales) deben tener Azure Arc instalado y habilitado.



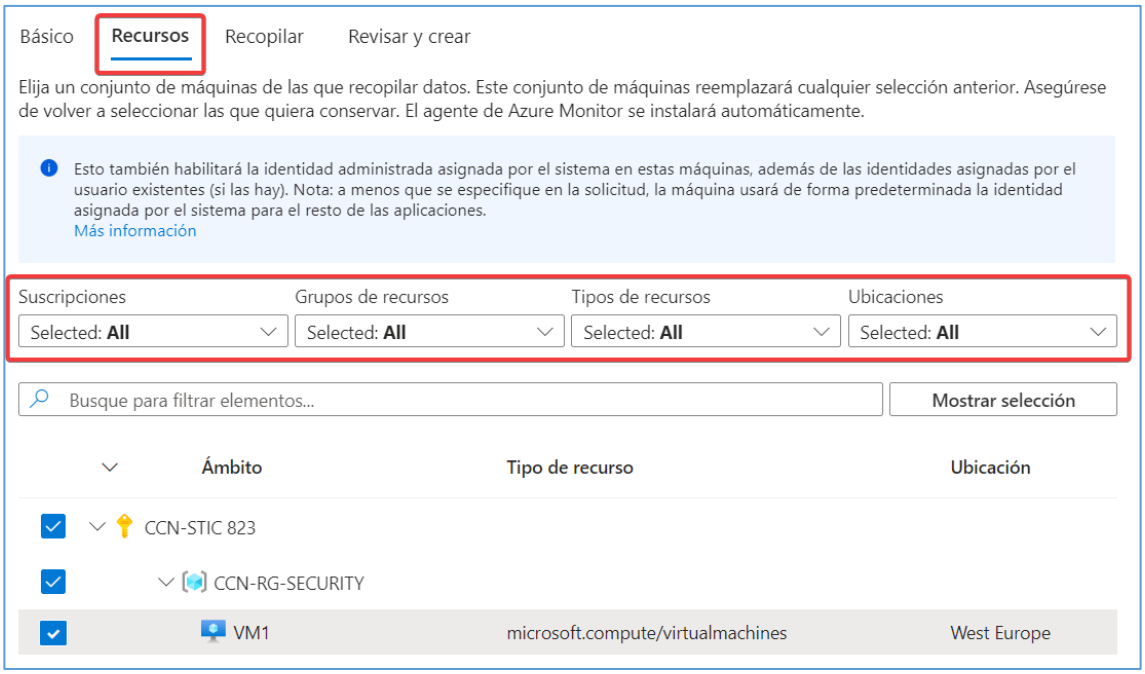
4. En **Configuración,** seleccionar **+Crear regla de recopilación de datos**. El **Asistente para crear reglas de recopilación de datos** se abrirá a la derecha.



5. En **Datos básicos,** escribir una **regla de nombre** y especificar una **suscripción** y un **grupo de recursos** donde se creará la regla de recopilación de datos (DCR). *No* tiene que ser el mismo grupo de recursos o suscripción en el que se encuentran las máquinas supervisadas y sus asociaciones, siempre y cuando estén en el mismo inquilino.

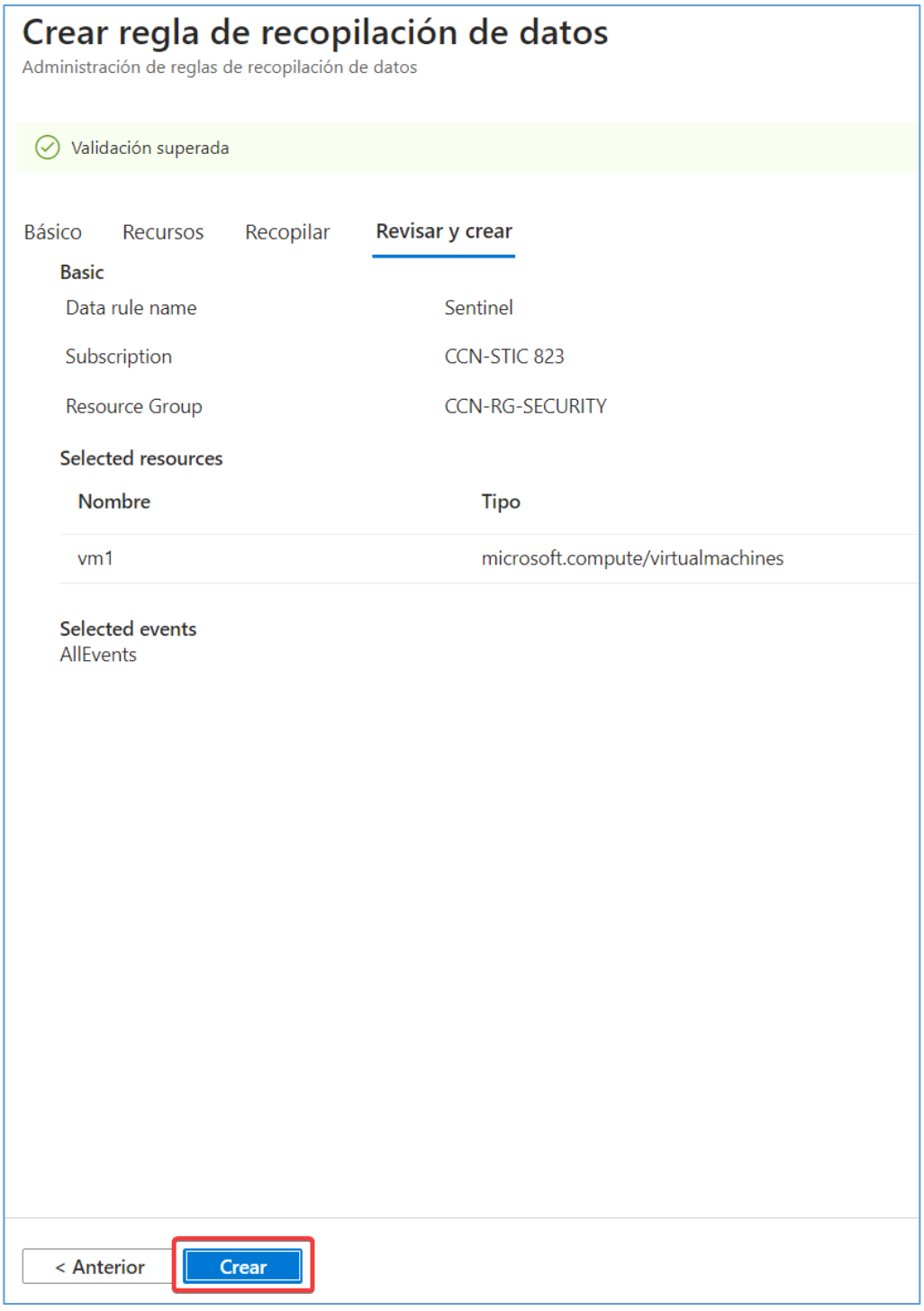


6. En la pestaña **Recursos,** seleccionar las máquinas a las que se aplicará la regla de recopilación de datos. Al final de este proceso, el agente de Azure Monitor se instalará en las máquinas seleccionadas que aún no lo tengan instalado.

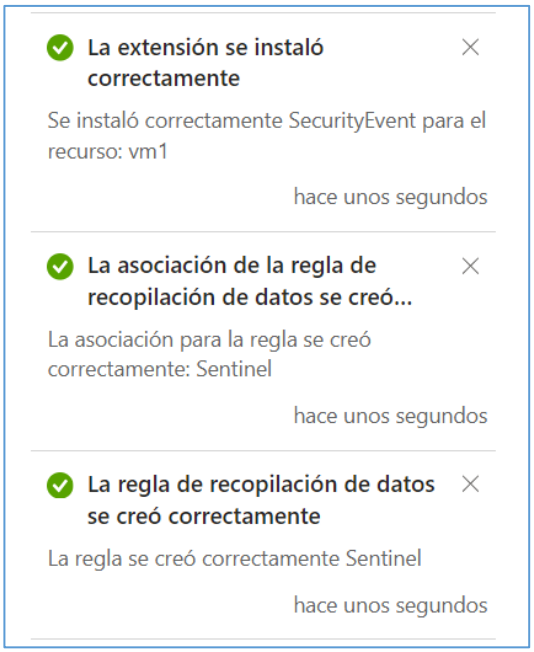


7. En la pestaña **Recopilar**. Seleccionar los eventos que se quieren recopilar o seleccionar **Personalizado** para especificar otros registros o filtrar eventos mediante consultas XPath.

8. Cuando se hayan agregado todas las expresiones de filtro que se quiera, seleccionar **Siguiente: Revisar y crear**.
9. Cuando aparezca el mensaje "Validación superada", seleccionar **Crear**.



10. Se comprueba que la creación ha finalizado con éxito:


La extensión se instaló correctamente
Se instaló correctamente SecurityEvent para el recurso: vm1
hace unos segundos
La asociación de la regla de recopilación de datos se creó...
La asociación para la regla se creó correctamente: Sentinel
hace unos segundos
La regla de recopilación de datos se creó correctamente
La regla se creó correctamente Sentinel
hace unos segundos

3. CONFIGURACIÓN SEGURA PARA MICROSOFT SENTINEL

Dentro de este apartado se definen una serie de medidas de obligado cumplimiento para la normativa del Esquema Nacional de Seguridad (ENS) establecidas en el BOE-A-2022-7191 Real Decreto 311/2022, de 3 de mayo:

https://www.boe.es/diario_boe/txt.php?id=BOE-A-2022-7191

3.1 MARCO OPERACIONAL

3.1.1 CONTROL DE ACCESO

El control de acceso comprende el conjunto de actividades preparatorias y ejecutivas tendentes a permitir o denegar a una entidad, usuario o proceso, el acceso a un recurso del sistema para la realización de una acción concreta.

Microsoft Entra ID es la herramienta principal para la gestión de accesos y privilegios sobre los recursos de Azure dentro de una organización. Al ser **Microsoft Sentinel** un recurso de Azure, el proveedor de identidad será **Microsoft Entra ID**.

Nota: Si bien esta guía trata únicamente la gestión de cuentas de usuarios en nube Microsoft Entra ID, también permite configuraciones hibridas.
Se puede consultar la documentación de identidades hibridas en el enlace:
https://docs.microsoft.com/es-es/azure/active-directory/hybrid/index
Para cumplir con los requisitos exigidos dentro del ámbito del ENS, se recomienda consultar la guía [CCN-STIC-884A Guía de Configuración segura para Azure].

3.1.1.1 IDENTIFICACIÓN

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

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

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

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

Se hace referencia a estos enlaces de Microsoft:

- *https://docs.microsoft.com/es-es/azure/active-directory/hybrid/whatis-hybrid-identity*
- *https://docs.microsoft.com/es-es/azure/active-directory/devices/hybrid-azuread-join-managed-domains*

3.1.1.2 REQUISITOS DE ACCESO

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

Así mismo, si se dispone de una licencia de Microsoft Entra ID P2, se recomienda activar el acceso condicional y configurar Microsoft Entra ID Identity Protection.

Existen roles específicos del servicio ya creados en Azure, como, por ejemplo, los específicos de Microsoft Sentinel: "**Colaborador de automatización de Microsoft Sentinel**", "**Colaborador de Microsoft Sentinel**", "**Lector de Microsoft Sentinel**", "**Microsoft Sentinel Business Applications Agent Operator**", "**Microsoft Sentinel Playbook Operator**" y "**Respondedor de Microsoft Sentinel**". Estos roles se detallan en el punto [3.1.1.3 Segregación de funciones y tareas].

Control de Acceso Basado en Roles (RBAC)

Microsoft Sentinel usa el control de acceso basado en rol (RBAC) para proporcionar roles integrados que se pueden asignar a usuarios, grupos y servicios en Azure.

Utilice RBAC de Azure para crear y asignar roles dentro del equipo de operaciones de seguridad para conceder el acceso adecuado a Microsoft Sentinel. Los diferentes roles proporcionan un control exhaustivo sobre lo que los usuarios de Microsoft Sentinel pueden ver y hacer. Los roles de Azure se pueden asignar directamente en el área de trabajo de Microsoft Sentinel, o bien en una suscripción o un grupo de recursos al que pertenece el área de trabajo, y que Microsoft Sentinel heredará.

En la tabla siguiente se resaltan los escenarios en los que el RBAC de contexto de recursos es más útil. Tenga en cuenta las diferencias en los requisitos de acceso entre los equipos del **Centro de Operaciones de Seguridad** (SOC Security Operations Center) y los equipos que no son de SOC.

Tipo de requisito	Equipo de SOC	Equipo que no es de SOC
Permisos	Toda el área de trabajo	Solo recursos específicos
Acceso a datos	Todos los datos del área de trabajo	Solo los datos de los recursos a los que el equipo está autorizado a acceder

Experiencia	La experiencia completa de Microsoft Sentinel, posiblemente limitada por los permisos funcionales asignados al usuario.	Solo consultas de registro y libros

Funcionamiento de RBAC

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

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

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

- **Propietario:** Tiene 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 se puede conceder acceso a otros.
- **Lector:** Tiene permisos para ver los recursos existentes de Azure.
- **Administrador de control de acceso basado en roles:** Tiene permisos para administrar el acceso a los recursos de Azure asignando roles mediante RBAC de Azure. Este rol no permite administrar el acceso de otras formas, como Azure Policy
- **Administrador de acceso de usuario:** Tiene permisos para administrar el acceso de los usuarios a los recursos de Azure.

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

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

https://docs.microsoft.com/es-es/azure/sentinel/roles

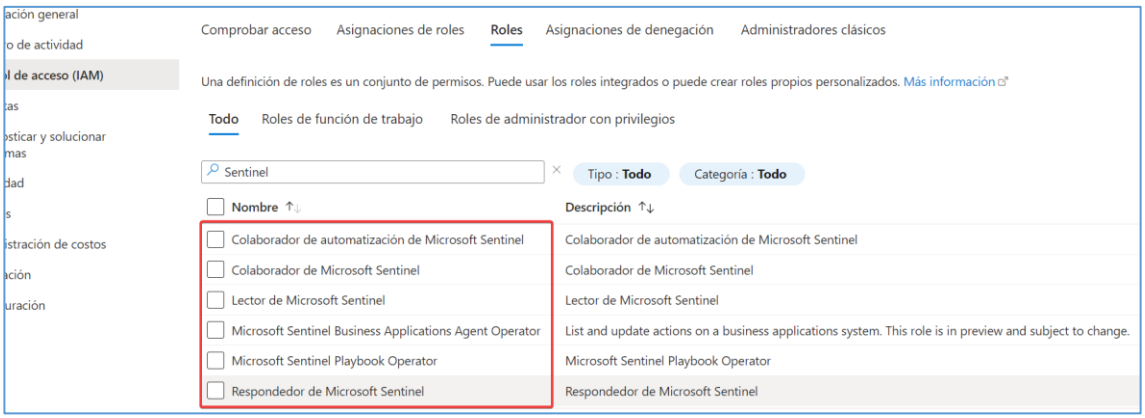
Roles personalizados RBAC

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

3.1.1.3 SEGREGACIÓN DE FUNCIONES Y TAREAS

Para la correcta administración de Microsoft Sentinel se utilizarán los permisos RBAC. Todos los roles integrados de Microsoft Sentinel conceden acceso de lectura a los datos en el área de trabajo de Microsoft Sentinel. Los roles son los siguientes:

- El rol **Lector de Microsoft Sentinel** puede ver datos, incidentes, libros y otros recursos de Microsoft Sentinel.
- **El respondedor de Microsoft Sentinel** puede, además de los permisos para el anterior rol, administrar incidentes como asignar, descartar y cambiar incidentes.
- **El colaborador de Microsoft Sentinel** puede, además de los permisos para el rol anterior, instalar y actualizar soluciones desde el centro de contenido, y crear y editar recursos de Microsoft Sentinel, como libros, reglas de análisis, etc.
- El rol **Operador de cuaderno de estrategias de Microsoft Sentinel** puede enumerar, ver y ejecutar manualmente cuadernos de estrategias (playbooks).
- **Colaborador de automatización de Microsoft Sentinel** permite que Microsoft Sentinel agregue cuadernos de estrategias a las reglas de automatización. No está diseñado para las cuentas de usuario.



El rol de **Microsoft Sentinel Business Applications Agent Operator** no se comenta en esta guía por estar en preview en el momento de elaboración de esta.

Roles y permisos adicionales

Es posible que sea necesario asignar roles adicionales o permisos específicos a los usuarios con requisitos de trabajo concretos para que puedan realizar sus tareas.

Instalar y administrar contenido de fábrica (Content Hub)

Existen soluciones empaquetadas para productos integrales o contenido independiente del **centro de contenido** en Microsoft Sentinel. Para instalar y administrar contenido desde el centro de contenido, asigne el rol Colaborador de Microsoft Sentinel en el nivel de grupo de recursos.

Automatizar respuestas a amenazas con cuadernos de estrategias

Microsoft Sentinel usa cuadernos de estrategias para una respuesta automatizada ante amenazas. Los cuadernos de estrategias se basan en Azure Logic Apps y son recursos independientes de Azure. Es posible que se desee asignar a miembros específicos del equipo de operaciones de seguridad la posibilidad de usar Logic Apps para las operaciones de orquestación, automatización y respuesta de seguridad (SOAR). Se puede usar el rol Operador de cuaderno de estrategias de Microsoft Sentinel para asignar permisos explícitos y limitados para ejecutar cuadernos de estrategias y el rol Colaborador de aplicaciones lógicas para crear y editar cuadernos de estrategias.

Conceder permisos a Sentinel para ejecutar cuadernos de estrategias

Microsoft Sentinel usa una cuenta de servicio especial para ejecutar cuadernos de estrategias de desencadenador de incidentes manualmente o para llamarlos desde reglas de automatización. El uso de esta cuenta (en lugar de su cuenta de usuario) aumenta el nivel de seguridad del servicio.

Para que una regla de automatización ejecute un cuaderno de estrategias, se deben conceder a esta cuenta permisos explícitos para acceder al grupo de recursos en el que se encuentra el cuaderno. En ese momento, cualquier regla de automatización puede ejecutar cualquier cuaderno de estrategias de ese grupo de recursos. Para conceder estos permisos a esta cuenta de servicio, la cuenta debe tener permisos de propietario en los grupos de recursos que contienen los cuadernos de estrategias.

Conectar orígenes de datos a Microsoft Sentinel

Para que un usuario pueda agregar conectores de datos, debe asignar permisos de escritura a ese usuario en el área de trabajo de Microsoft Sentinel. Tenga en cuenta los permisos adicionales necesarios para cada conector, tal como se muestra en la página del conector correspondiente.

Permitir que los usuarios invitados asignen incidentes

Si es necesario que un usuario invitado pueda asignar incidentes, se deberá asignarle el rol Lector de directorios, además del rol Respondedor de Microsoft Sentinel. El rol Lector de directorios no es un rol de Azure, sino un rol de Microsoft Entra y los usuarios normales (no invitados) tienen asignado este rol de forma predeterminada.

Crear y eliminar libros

Para crear y eliminar un libro de Microsoft Sentinel, el usuario requiere el rol Colaborador de Microsoft Sentinel o un rol menor de Microsoft Sentinel, junto con el rol Colaborador de libros de Azure Monitor. Este rol no es necesario para usar los libros, solo para crearlos y eliminarlos.

Otros roles que podría ver asignados

En la asignación de roles de Azure específicos de Microsoft Sentinel, se pueden encontrar otros roles de Azure y Log Analytics que se pueden haber asignado a los usuarios para otros fines. Se debe tener en cuenta que estos roles conceden un conjunto más amplio de permisos que incluye el acceso al área de trabajo de Microsoft Sentinel y a otros recursos:

- **Roles de Azure**: Propietario, colaborador y lector. Los roles de Azure conceden acceso a todos los recursos de Azure, incluidas las áreas de trabajo de Log Analytics y los recursos de Microsoft Sentinel.
- **Roles de Log Analytics**: Colaborador de Log Analytics y Lector de Log Analytics. Los roles de Log Analytics conceden acceso a las áreas de trabajo de Log Analytics.
    - **Colaborador de aplicaciones lógicas**: permite administrar aplicaciones lógicas y ejecutar cuadernos de estrategias, pero no puede cambiar el acceso a ellos (para ello se necesita el rol Propietario).
    - **Operador de aplicaciones lógicas**: permite leer, habilitar y deshabilitar aplicaciones lógicas, pero no puede editarlas ni actualizarlas.

Por ejemplo, un usuario al que se haya asignado el rol de Lector de Microsoft Sentinel, pero no el rol de Colaborador de Microsoft Sentinel, todavía podrá editar elementos en Microsoft Sentinel si se le asigna el rol de Colaborador de nivel de Azure. Por tanto, si desea conceder permisos solo para un usuario en Microsoft Sentinel, elimine con cuidado los permisos anteriores de este usuario, y asegúrese de que no interrumpe ningún acceso necesario para otro recurso.

3.1.1.4 PROCESO DE GESTIÓN DE DERECHOS DE ACCESO

3.1.1.5 MECANISMOS DE AUTENTICACIÓN (USUARIOS EXTERNOS)

En el entorno empresarial actual, la identidad es el nuevo perímetro de seguridad. Si cada dispositivo, usuario, servidor, proceso y dispositivo IoT tiene una identidad única, estas identidades se convierten en el nuevo “perímetro”, evitando el acceso no autorizado a los datos y sistemas.

La **autenticación** es **crucial** en este contexto de la identidad como nuevo perímetro de seguridad. Aquí hay algunas razones por las que la autenticación es de suma importancia:

- **Verificación de Identidad**: La autenticación garantiza que la persona o el dispositivo que intenta acceder a los recursos de la organización sea realmente quien dice ser. Esto ayuda a prevenir el acceso no autorizado y protege contra amenazas internas y externas.
- **Control de Acceso**: La autenticación permite a las organizaciones establecer políticas de acceso basadas en roles.

- **Prevención de Ataques de Fuerza Bruta**: La autenticación sólida dificulta que los atacantes adivinen o descifren las credenciales de acceso. La ausencia de contraseñas (passwordless), la autenticación multifactor (MFA) y otros métodos ayudan a prevenir ataques de fuerza bruta.
- **Protección contra Amenazas Emergentes**: A medida que las amenazas evolucionan, la autenticación también debe adaptarse. Las soluciones modernas, como la autenticación biométrica (huellas dactilares, reconocimiento facial), ayudan a mitigar riesgos emergentes.

En resumen, la autenticación es fundamental para garantizar que solo las personas y dispositivos autorizados tengan acceso a los recursos de la organización, especialmente en un mundo donde la identidad es el nuevo perímetro de seguridad.

Microsoft Entra multifactor authentication (MFA) 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.

Se requiere establecer un "doble factor de autenticación" (MFA) y tener una política adecuada de gestión de credenciales. Así mismo, se requiere un registro de intentos de accesos con éxito y fallidos al sistema. Adicionalmente se puede controlar el acceso al servicio mediante directivas de acceso condicional o reglas en ADFS.

El acceso a los portales de administración se puede realizar de forma descentralizada. Se recomienda reforzar la seguridad:

- Equipos administrados.
- Autenticación de doble factor.
- Conformidad de dispositivos.
- Ubicaciones de confianza.
- Evitar accesos de usuarios sin licenciamiento.
- Otras medidas a través de acceso condicional

Una configuración detallada puede consultarse en la guía [CCN-STIC-884A - Guía de configuración segura para Azure].

3.1.1.6 MECANISMOS DE AUTENTICACIÓN (USUARIOS DE LA ORGANIZACIÓN)

Los mecanismos de autenticación que se utilizarán para proteger a los usuarios de la organización serán los mismos que los indicados en el punto anterior para los usuarios externos. Como se ha comentado, ahora el acceso a los recursos está descentralizado, siendo la identidad el nuevo perímetro de seguridad, y, por lo tanto, no se debería diferenciar entre tipos de usuarios en cuanto a las medidas de protección de acceso.

3.1.2 EXPLOTACIÓN

3.1.2.1 PROTECCIÓN FRENTE A CÓDIGO DAÑINO

Microsoft Sentinel tiene eficaces herramientas de búsqueda y consulta que permiten buscar amenazas de seguridad en los orígenes de datos de cualquier organización. Para ayudar a los analistas de seguridad a buscar proactivamente nuevas anomalías que ni las aplicaciones de seguridad ni las reglas de análisis programadas han sido capaces de identificar, las consultas de búsqueda de amenazas integradas de Microsoft Sentinel servirán de guía para formular las preguntas adecuadas para detectar problemas en los datos que ya hay en la red. Aquí es donde el Threat Hunting puede resultar muy útil.

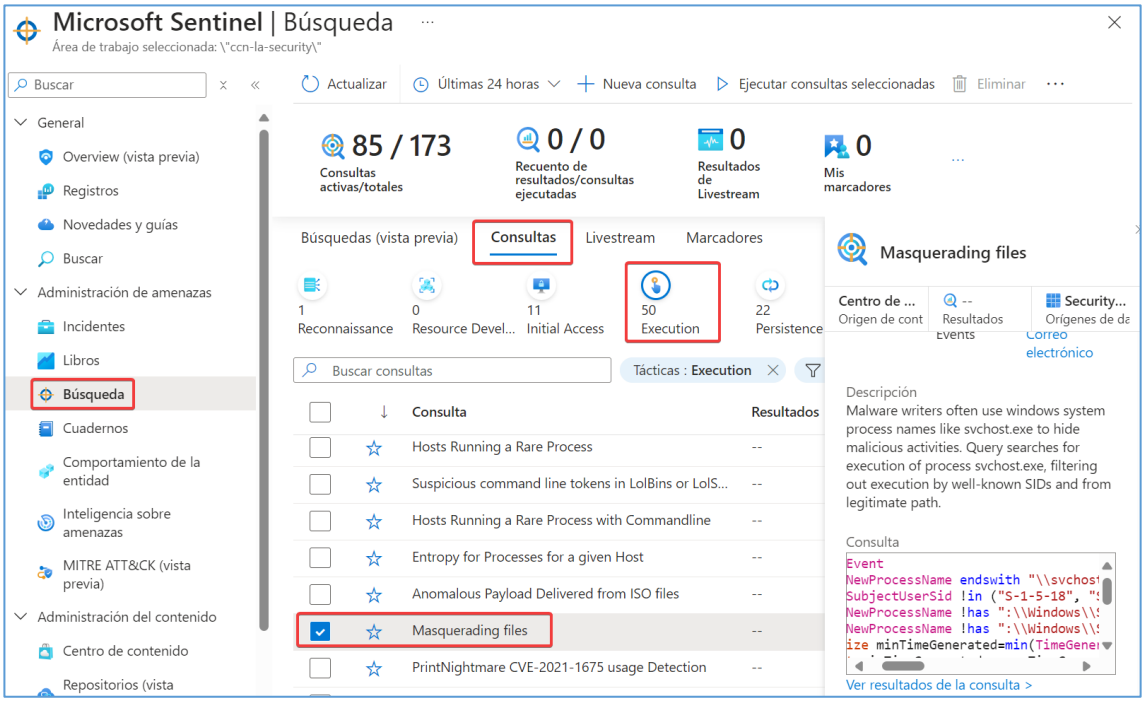
Microsoft Sentinel usa el framework MITRE ATT&CK para clasificar y ordenar las consultas por técnicas y tácticas. ATT&CK es una basede datos de conocimiento de tácticas y técnicas usadas y observadas en el panorama de amenazas global. Se puede usar MITRE ATT&CK para desarrollar modelos y métodos de búsqueda de amenazas en Microsoft Sentinel y para entrenarlos. Al buscar amenazas en Microsoft Sentinel, se puede usar el framework ATT&CK para clasificar y ejecutar consultas mediante la escala de tiempo de tácticas de MITRE ATT&CK.

Al seleccionar cualquier táctica se filtran las consultas disponibles por la táctica seleccionada. Las tácticas incluyen:

- **Reconocimiento**: Conjunto de técnicas con las cuales los atacantes recopilan información sobre sus objetivos. Esto puede incluir la búsqueda de direcciones IP, nombres de dominio, detalles de empleados, relaciones comerciales y cualquier otra información relevante. El objetivo es preparar futuros ataques y comprender la infraestructura de la organización objetivo.
- **Desarrollo de Recursos**: Los atacantes crean o adquieren los recursos necesarios para facilitar otras tácticas. Esto podría incluir la creación de herramientas personalizadas, la adquisición de exploits o la obtención de credenciales.
- **Acceso inicial:** Tácticas que usa el adversario para obtener acceso a una red aprovechando vulnerabilidades o debilidades de configuración de los sistemas de cara al público. Un ejemplo de esto son los ataques de phishing de objetivo definido.
- **Ejecución**: Tácticas que dan lugar a que un adversario ejecute su código en un sistema de destino. Por ejemplo, un hacker malintencionado puede ejecutar un script de PowerShell para descargar más herramientas de ataque o examinar otros sistemas.
- **Persistencia:** Tácticas que permiten a un adversario conservar el acceso a un sistema de destino, incluso después de reinicios y cambios de credenciales. Un ejemplo de una técnica de persistencia es un atacante que crea una tarea programada que ejecuta su código a una hora concreta o al reiniciar.
- **Elevación de privilegios:** Tácticas que usa un adversario para obtener privilegios de nivel superior en un sistema, como de administrador local o raíz.

- **Evasión defensiva:** Tácticas que usan los atacantes para evitar la detección. Las tácticas de evasión incluyen la ocultación de código malintencionado en procesos y carpetas de confianza, el cifrado u ofuscación de código enemigo o la inhabilitación de software de seguridad.
- **Acceso con credenciales:** Tácticas implementadas en sistemas y redes para robar nombres de usuario y credenciales para su reutilización.
- **Detección:** Tácticas que usan los adversarios para obtener información sobre los sistemas y las redes que quieren aprovechar o usar para su ventaja táctica.
- **Movimiento lateral:** Tácticas que permiten a un atacante pasar de un sistema a otro dentro de una red. Las técnicas comunes incluyen métodos Pass-the-Hash para autenticar a los usuarios y el uso del Protocolo de escritorio remoto.
- **Recopilación:** Tácticas que usa un adversario para recopilar y consolidar la información que quiere como parte de sus objetivos.
- **Comando y control:** Tácticas que usa un atacante para comunicarse con un sistema bajo su control. Un ejemplo es un atacante que se comunica con un sistema mediante un puerto infrecuente o con un número alto para eludir la detección por parte de los dispositivos de seguridad o los servidores proxy.
- **Filtración:** Tácticas que se usan para trasladar los datos de la red en peligro a un sistema o red que está totalmente bajo el control del atacante.
- **Impacto:** Tácticas que usa un atacante para afectar a la disponibilidad de los sistemas, las redes y los datos. Los métodos de esta categoría incluyen ataques por denegación de servicio y software de eliminación de datos o discos.

Para detectar la ejecución de código malicioso podríamos buscar en la táctica de **ejecución**, la técnica **Enmascarar archivos**:

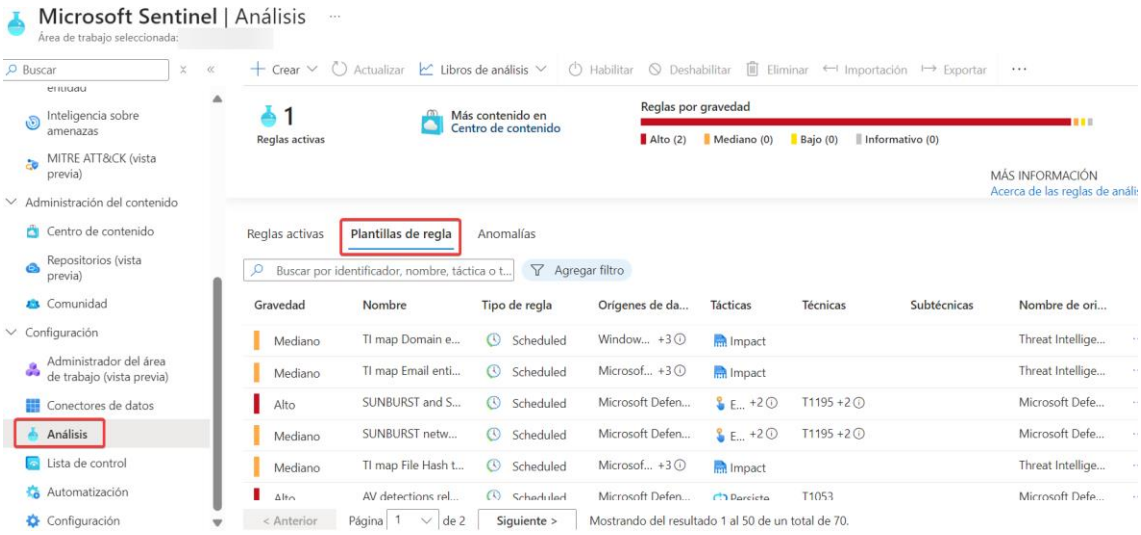


En el ejemplo mostrado se analizarán los procesos svchost.exe de un sistema filtrando los identificadores de seguridad conocidos que son legítimos para ejecutar el proceso svchost.exe y también se filtran las ubicaciones legítimas desde donde se ejecuta este proceso.

Plantillas integradas para detección de amenazas

Después de conectar los orígenes de datos a Microsoft Sentinel, se puede recibir una notificación cuando suceda algo sospechoso. Por este motivo, Microsoft Sentinel proporciona plantillas integradas predefinidas para ayudarle a crear reglas de detección de amenazas. Estas plantillas fueron diseñadas por un equipo de expertos y analistas en seguridad de Microsoft basándose en amenazas conocidas, vectores de ataque habituales y cadenas de escalado de actividades sospechosas. Las reglas creadas a partir de estas plantillas buscarán automáticamente en el entorno las actividades que parezcan sospechosas.

Para ver todas las detecciones estándar, acceder a [Análisis] y, después, a [Plantillas de regla]. Esta pestaña contiene todas las reglas integradas de Microsoft Sentinel.



Los diferentes tipos de plantillas son:

Seguridad de Microsoft

Las plantillas de seguridad de Microsoft crean automáticamente incidentes de Microsoft Sentinel a partir de las alertas generadas en otras soluciones de seguridad de Microsoft, en tiempo real.

Fusión

Basada en la tecnología de fusión, la detección avanzada de ataques de varias fases de Microsoft Sentinel emplea algoritmos de aprendizaje automático escalables que pueden correlacionar muchas alertas y eventos de baja fidelidad de varios productos con incidentes útiles y de alta fidelidad.

Análisis de comportamiento de aprendizaje automático

Las plantillas de análisis de comportamiento de aprendizaje automático se basan en algoritmos de aprendizaje automático de Microsoft, por lo que no puede ver la lógica interna de cómo funcionan ni cuándo se ejecutan.

Dado que la lógica está oculta y, por lo tanto, no se puede personalizar, solo puede crear una regla con cada plantilla de este tipo.

Inteligencia sobre amenazas

Se puede aprovechar la inteligencia sobre amenazas producida por Microsoft para generar alertas e incidentes de alta fidelidad con la regla de Análisis de Inteligencia sobre amenazas de Microsoft. Esta regla única no es personalizable, pero cuando está habilitada, coincide automáticamente con los registros del formato de evento común (CEF), los datos de Syslog o los eventos DNS de Windows con indicadores de amenazas de dominio, IP y dirección URL de la inteligencia sobre amenazas de Microsoft. Algunos indicadores contienen información de contexto adicional mediante MDTI (Inteligencia contra amenazas de Microsoft Defender).

Anomalía

Las plantillas de reglas de anomalías usan el aprendizaje automático para detectar tipos específicos de comportamiento anómalo. Cada regla tiene sus propios parámetros y umbrales únicos, adecuados para el comportamiento que se está analizando.

Aunque las configuraciones de las reglas predeterminadas no se pueden cambiar ni ajustar, se puede duplicar una regla y, a continuación, cambiar y ajustar el duplicado. En tales casos, se ejecuta el duplicado en modo Distribución de paquetes piloto y el original de manera simultánea en modo Producción. Luego se compara los resultados y se cambia el duplicado a Producción siempre que se ajuste a lo que espera.

Programadas

Las reglas de análisis programado se basan en consultas escritas por expertos de seguridad de Microsoft. Puede ver la lógica de consulta y realizar cambios en ella. Puede usar la plantilla de reglas programadas y personalizar la lógica de consulta y la configuración de programación para crear otras reglas.

Varias plantillas de reglas de análisis programadas nuevas generan alertas correlacionadas por el motor de Fusion con alertas de otros sistemas para generar incidentes de alta fidelidad.

Casi en tiempo real (NRT)

Las reglas NRT son un conjunto limitado de reglas programadas, diseñadas para ejecutarse una vez al minuto, con el fin de proporcionar información lo más actualizada posible.

Funcionan principalmente como reglas programadas y se configuran de forma similar, con algunas limitaciones.

3.1.2.2 REGISTRO DE LA ACTIVIDAD

Uno de los conectores principales que se utilizará con Microsoft Sentinel será "*Microsoft Entra ID*", este conector almacenará los registros de auditoría y de inicios de sesión de Microsoft Entra ID en Azure Monitor, en un espacio de trabajo de Log Analytics. Para poder hacer uso de este conector se instalará la solución para **Microsoft Entra ID** desde **Centro de contenido**. El conector permite enviar los siguientes tipos de registro:

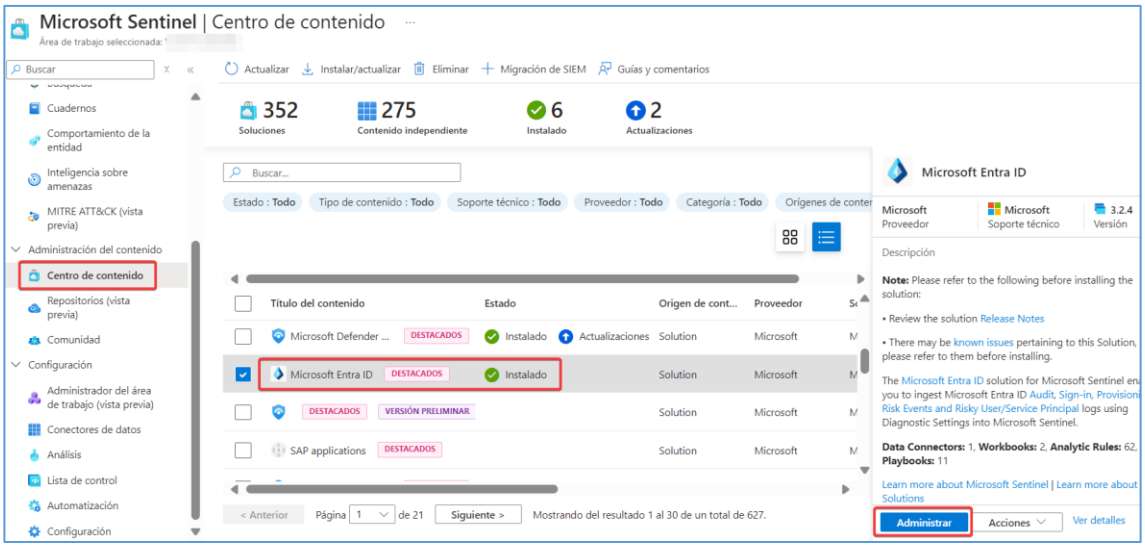
- **Registros de inicio de sesión**, que contienen información sobre inicios de sesión de usuario interactivos, donde un usuario proporciona un factor de autenticación.

  Ahora, el conector de Microsoft Entra ID incluye las tres categorías adicionales de registros de inicio de sesión:

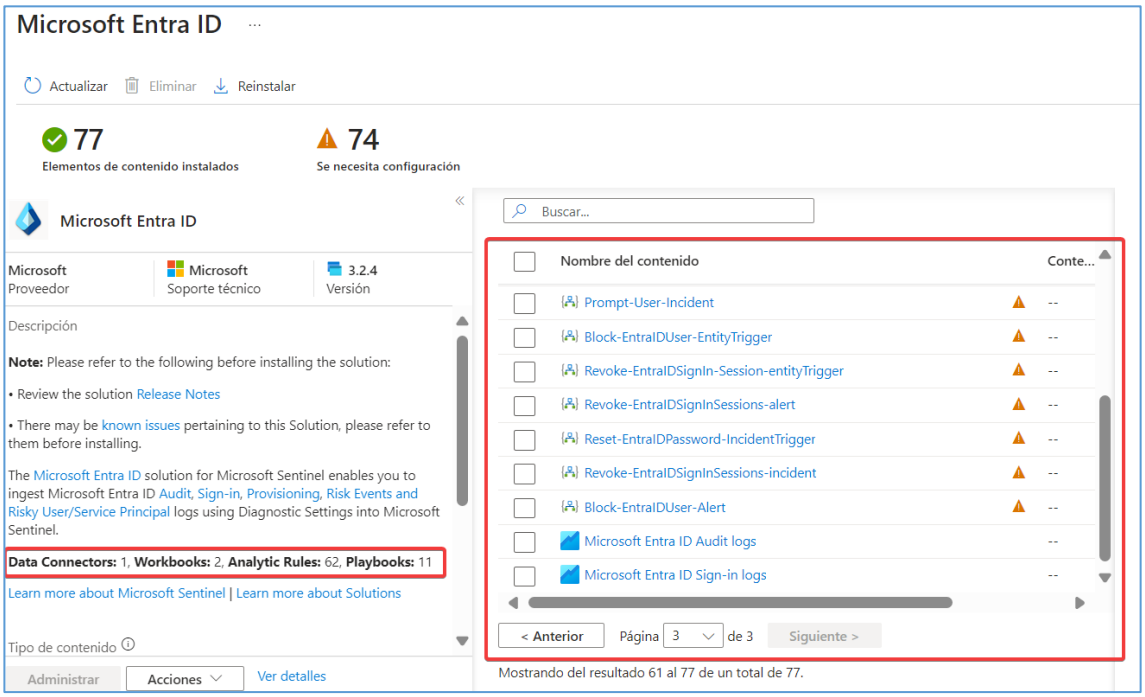
  - **Registros de inicios de sesión de usuario no interactivos**, que contienen información sobre los inicios de sesión realizados por un cliente en nombre de un usuario sin ninguna interacción ni factor de autenticación de parte del usuario.
  - **Registros de inicios de sesión de entidad de servicio**, que contienen información sobre inicios de sesión realizados por aplicaciones y entidades de servicio que no involucran a ningún usuario. En estos inicios de sesión, la aplicación o el servicio proporcionan una credencial en su propio nombre para autenticarse o acceder a los recursos.
  - **Registros de inicios de sesión de identidades administradas**, que contienen información sobre inicios de sesión realizados por recursos de Azure que tienen secretos administrados por Azure.
- **Registros de auditoría**, que contienen información sobre la actividad del sistema relativa a la administración de usuarios y grupos, aplicaciones administradas y actividades de directorio.
- **Registros de aprovisionamiento**, que contienen información sobre la actividad del sistema relativa a usuarios, grupos y roles aprovisionados por el servicio de aprovisionamiento de Microsoft Entra ID.

A continuación, se muestra cómo visualizar estos registros:

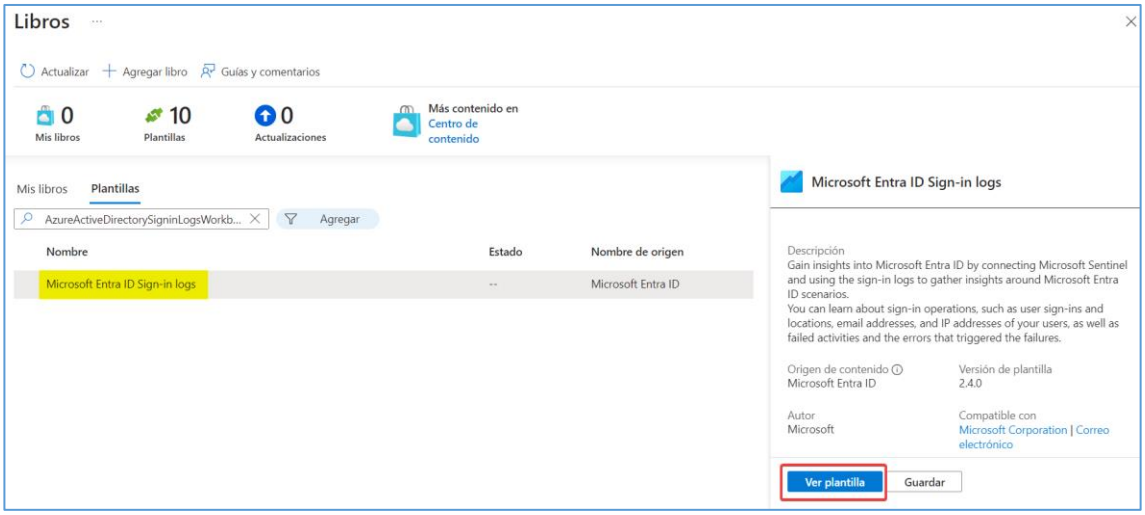
1. Acceder a *Centro de contenido*, y seleccionar la solución instalada: *Microsoft Entra ID*:



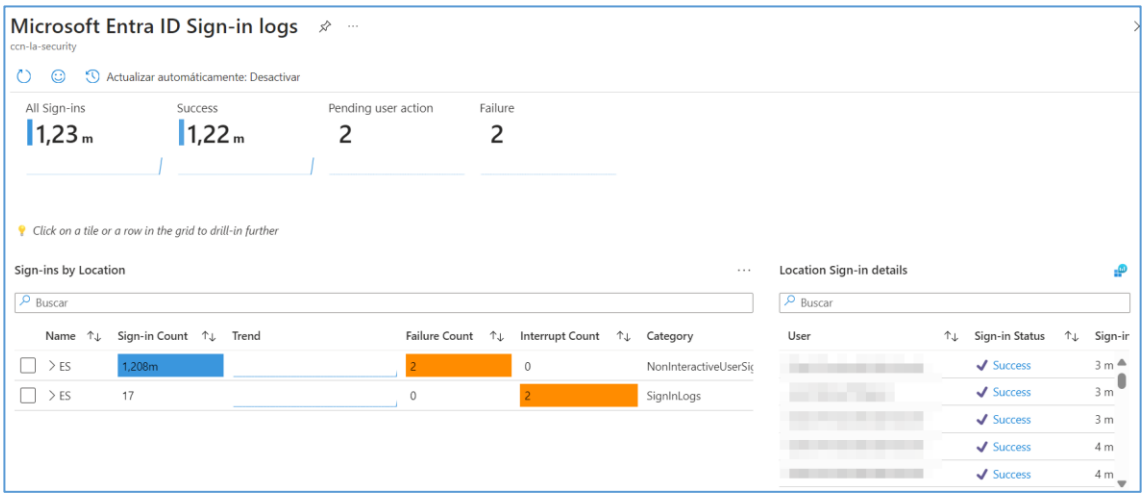
2. Cuando se selecciona Administrar, en la sección central se muestran los libros recomendados para este conector, los ejemplos de consultas y las plantillas de análisis:



3. Seleccionar el libro Microsoft Entra ID Sign-in logs:



4. Seleccionar Ver plantilla, se mostrarán los eventos relacionados con los inicios de sesión en Microsoft Entra ID. Estos informes son interactivos y se podrán aplicar filtros para afinar la búsqueda.



Otro conector habitual para alimentar datos en Microsoft Sentinel será: "*Azure Activity*". Este conector es el encargado de recolectar el registro de actividad de Azure y proporciona información de los eventos de nivel de suscripción que se han producido en Azure. Esta incluye una serie de datos, desde datos operativos de Azure Resource Manager hasta actualizaciones en eventos de Estado del servicio. En este tipo de conector se encontrarán incluidos todos los registros sobre las acciones que se realizan sobre el propio servicio de Sentinel.

A través del uso de roles de usuarios se puede bastionar quién puede consultar la información del registro de actividad. Los roles definidos para tal fin:

- Microsoft Sentinel Reader.
- Microsoft Sentinel Responder.

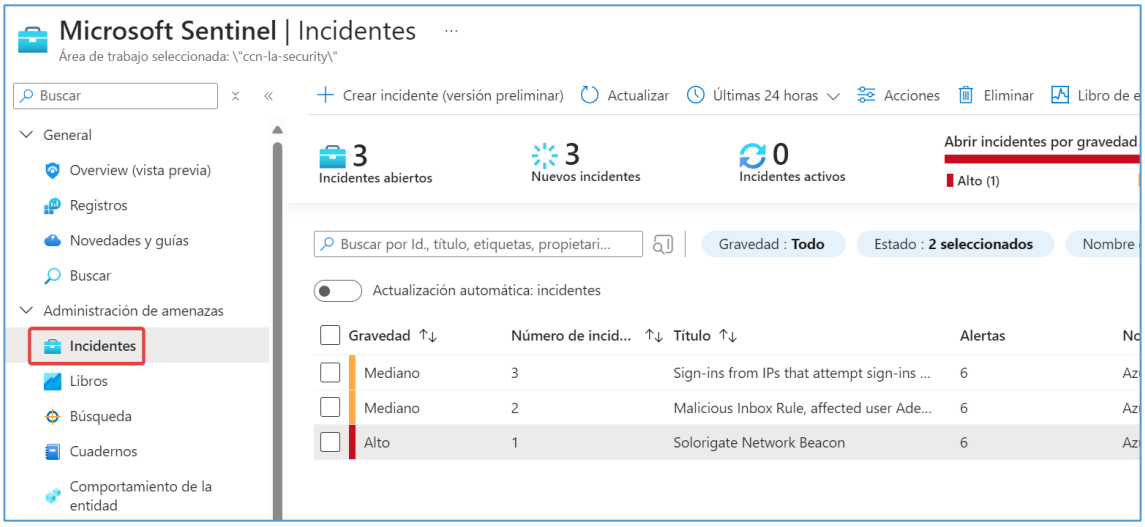
- Microsoft Sentinel Contributor.
- Microsoft Sentinel Playbook Operator.
- Microsoft Sentinel Automation Contributor.

* Estos roles se explican en el punto [3.1.1.3 Segregación de funciones y tareas] de la presente guía.

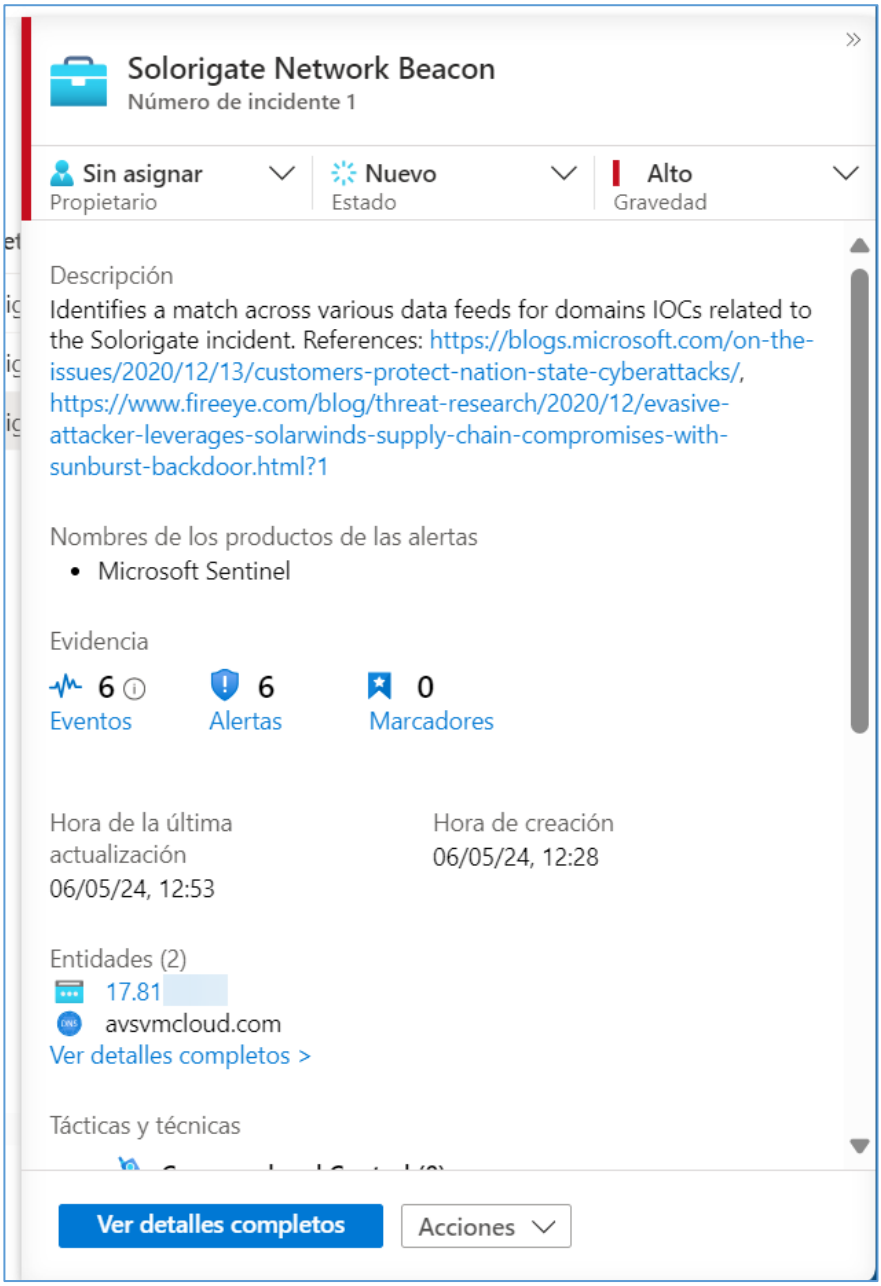
3.1.2.3 REGISTRO DE LA GESTIÓN DE INCIDENTES

Cómo se ha visto en los anteriores apartados, Microsoft Sentinel se alimentará con diferentes orígenes de datos. Una vez que se dispone de esos datos, se podrá recibir una notificación cuando suceda algo sospechoso. Para ello, Microsoft Sentinel permite crear reglas de alerta avanzadas, que generan incidentes que se pueden asignar e investigar.

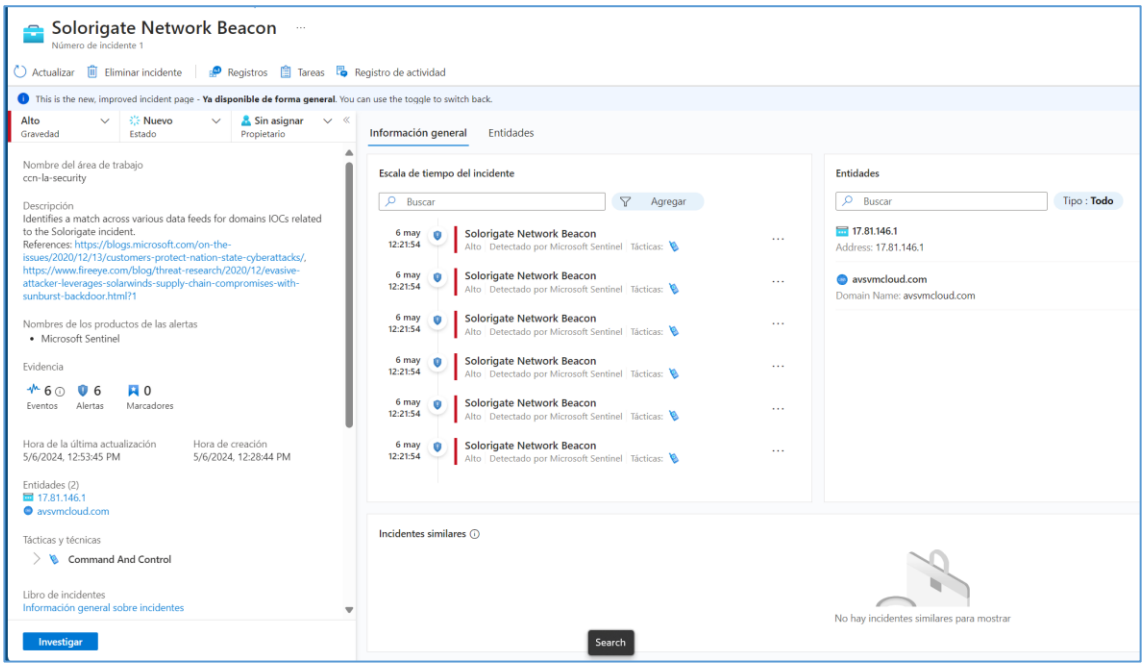
La página **Incidentes** permite saber cuántos incidentes hay, cuántos están **abiertos**, cuántos están establecidos en "**En curso"** y cuántos se han cerrado. De cada incidente se puede ver la hora a la que tuvo lugar y su estado. Una tira de color indica la severidad del incidente: rojo para alta, naranja para media, amarilla para baja y gris para informativa.



Para iniciar una investigación, seleccionar un incidente específico. A la derecha, puede ver información detallada del incidente, como la gravedad o un resumen del número de entidades implicadas, los eventos sin procesar que desencadenaron este incidente y el identificador único del mismo. A continuación, se muestra un ejemplo:



Para ver más detalles sobre las alertas y las entidades del incidente, seleccionar **Ver detalles completos** en la página del incidente y revisar las pestañas correspondientes donde se resume la información del incidente.



Por ejemplo:

- En la sección **Escala de tiempo del incidente**, revisar la escala de tiempo de las alertas y los marcadores del incidente, para poder reconstruir la escala de tiempo de la actividad del atacante.
- En **Alertas**, se puede revisar la alerta en sí. Se puede ver toda la información relevante sobre la alerta: la consulta que la ha desencadenado, el número de resultados devueltos por consulta y la capacidad de ejecutar cuadernos de estrategias en las alertas. Para explorar el incidente más en profundidad, se puede abrir la consulta que ha generado los resultados y los eventos que han desencadenado la alerta en Log Analytics.
- En el widget **Entidades**, se puede ver todas las entidades que se han asignado como parte de la definición de regla de alerta.

Si se está investigando un incidente de manera activa, una buena práctica consiste en establecer el estado del incidente a "**En curso"**, de esta manera queda identificado el incidente para el resto del equipo de seguridad lo sepa mientras se consigue solucionar.

Los incidentes se pueden asignar a un usuario específico. Para asignar un propietario a un incidente, hay que establecer el campo **Propietario**. Todos los incidentes se inician sin tener un propietario asignado. También se puede agregar

comentarios para que otros analistas puedan comprender lo que se ha investigado y las preocupaciones o hallazgos en torno al incidente.

3.1.3 MONITORIZACIÓN DEL SISTEMA

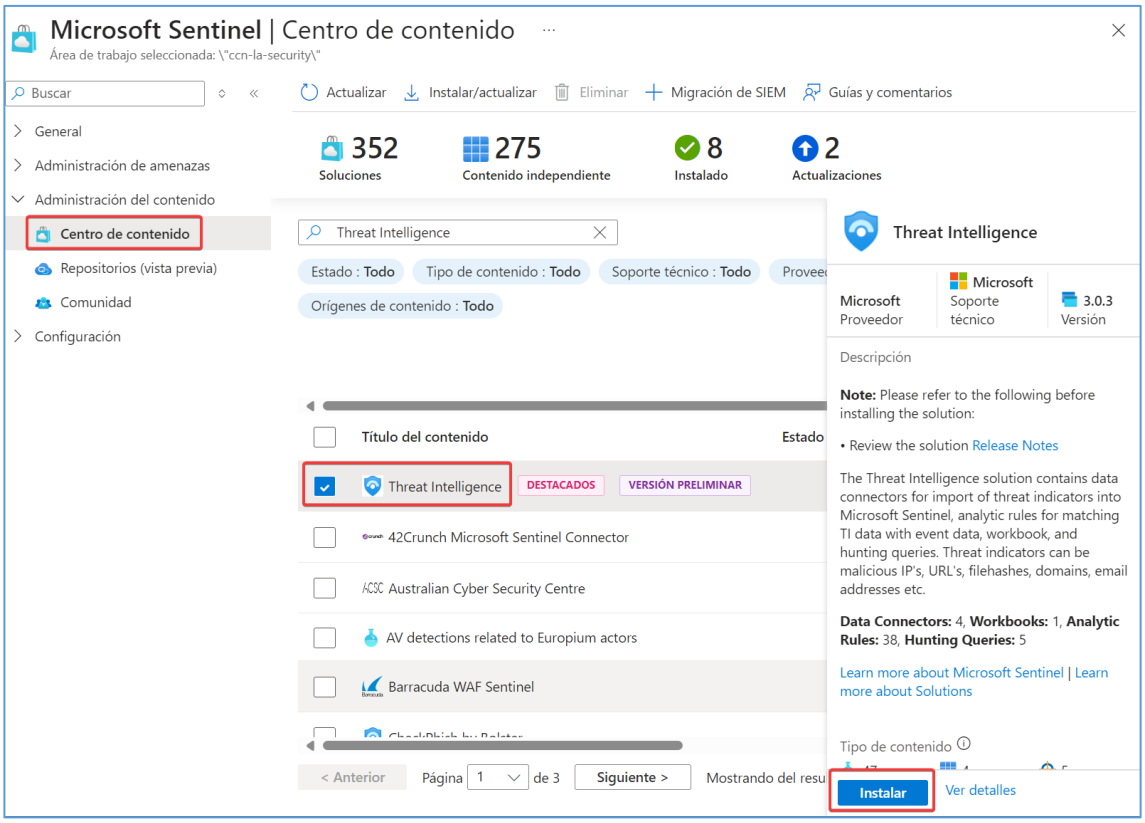
3.1.3.1 DETECCIÓN DE INTRUSIÓN

Microsoft Sentinel cuenta con una amplia colección de consultas, que como se ha visto anteriormente se pueden clasificar en técnicas y tácticas usadas por los atacantes, para detectar amenazas.

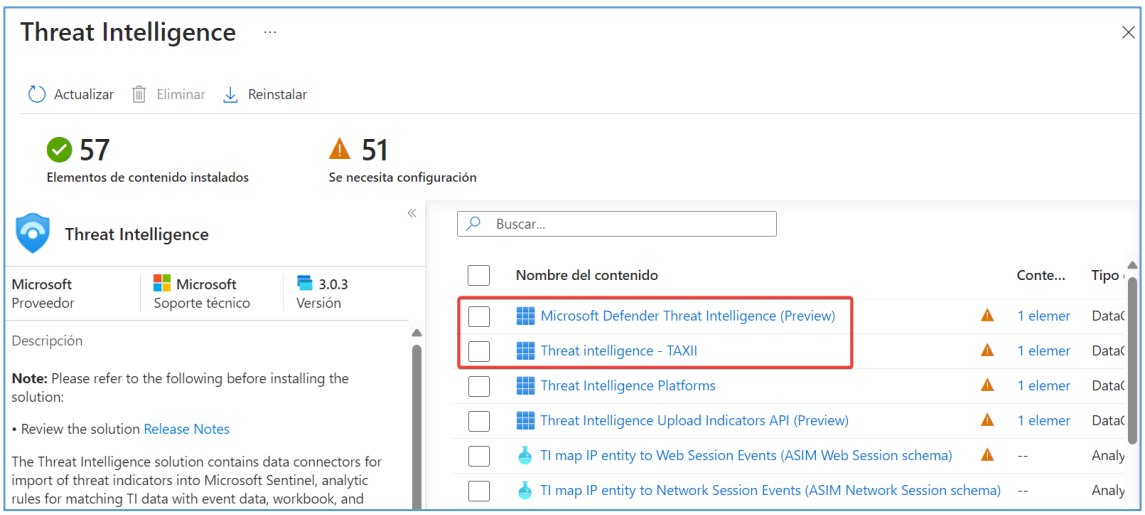
En este caso se recomienda implementar sistemas de detección de intrusión (Intrusion Detection System [IDS]), o sistemas de prevención de intrusos (intrusión Prevention system [IPS]). Por ejemplo, se puede usar Azure Firewall con inteligencia frente a amenazas (Threat intelligence [TI]). El filtrado basado en TI de Azure Firewall puede alertar y denegar el tráfico hacia y desde dominios y direcciones IP maliciosas conocidas. Las direcciones IP y los dominios se obtienen de la fuente de Microsoft Threat Intelligence. En la solución Azure Firewall, existe un conector nativo para Azure Firewall que permite que se envíen los registros de diagnóstico a Microsoft Sentinel.

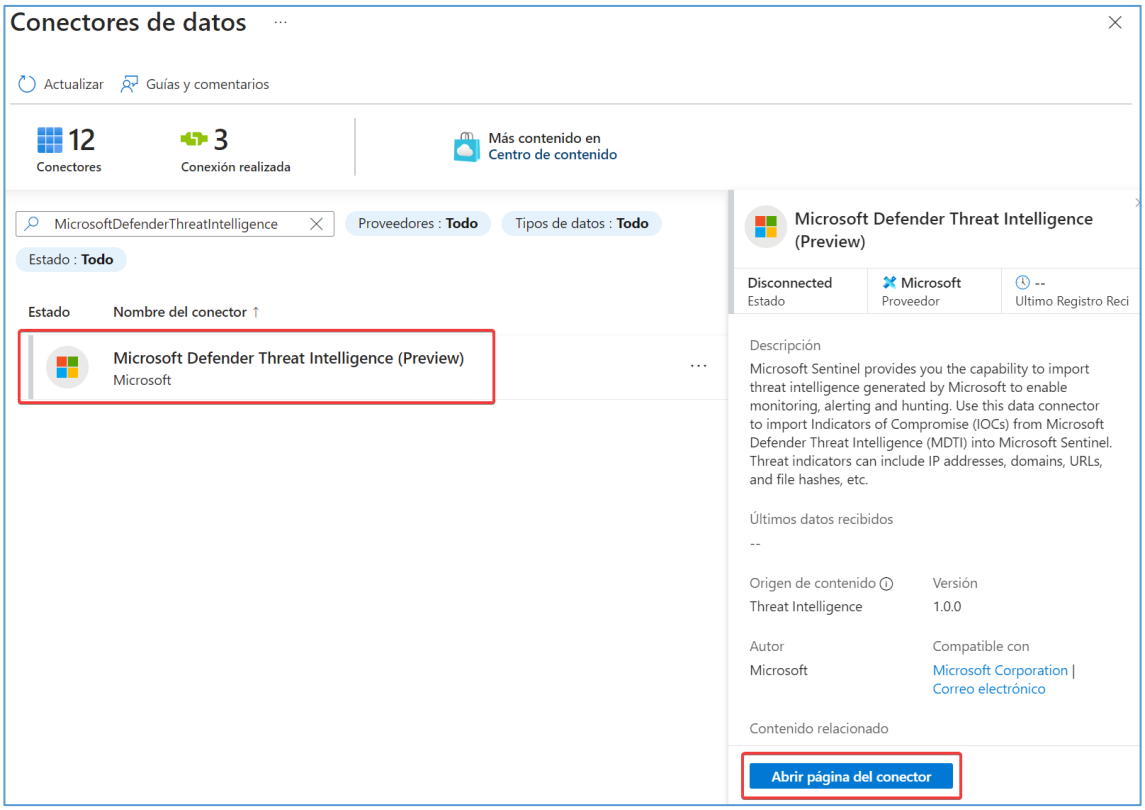
Microsoft Sentinel proporciona varias maneras diferentes de usar fuentes de inteligencia sobre amenazas para mejorar la capacidad de los analistas de seguridad para detectar y priorizar las amenazas conocidas. **Se recomienda que las fuentes de TI sean lo más heterogéneas posibles**, como ejemplo, se mostrará la configuración necesaria para integrar una fuente de TI de **Microsoft Defender Threat Intelligence** y también la conocida comunidad de inteligencia de amenazas abierta **AlienVault - Open Threat Exchange (OTX)**.

Como se ha visto anteriormente, lo primero será instalar la solución Threat Intelligence, que contiene los conectores de datos necesarios para configurar las fuentes de TI:

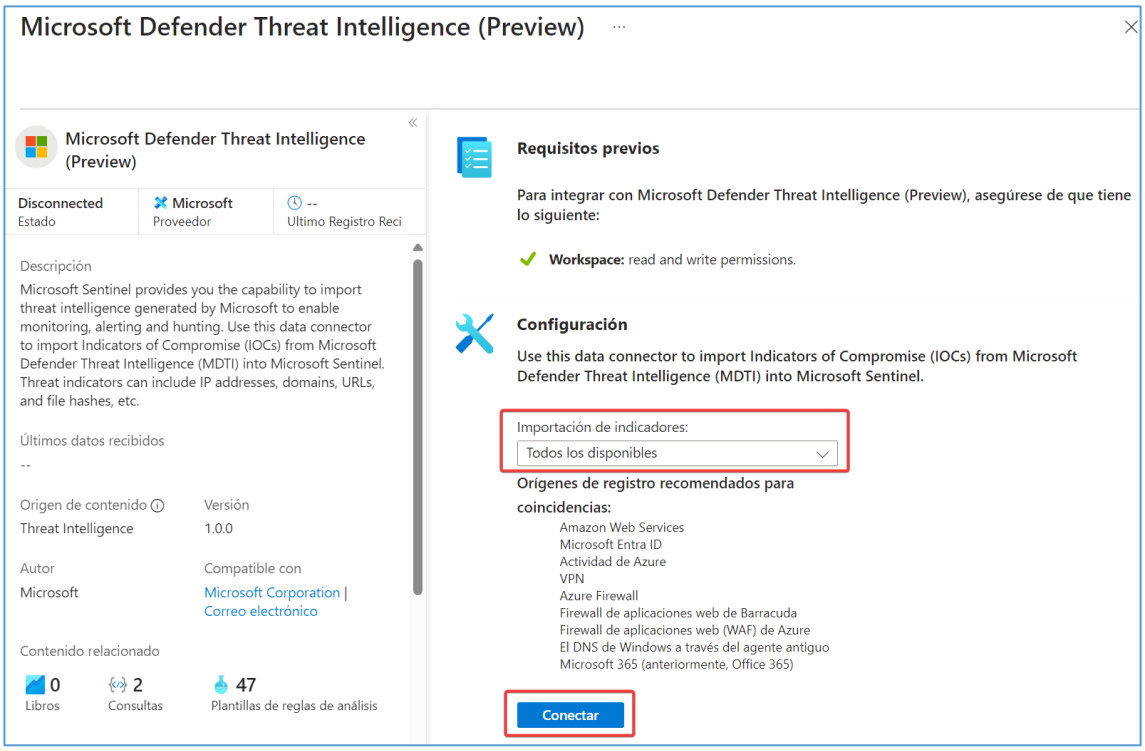


Una vez instalada la solución se procederá a configurar los dos conectores que se van a utilizar en este ejemplo:

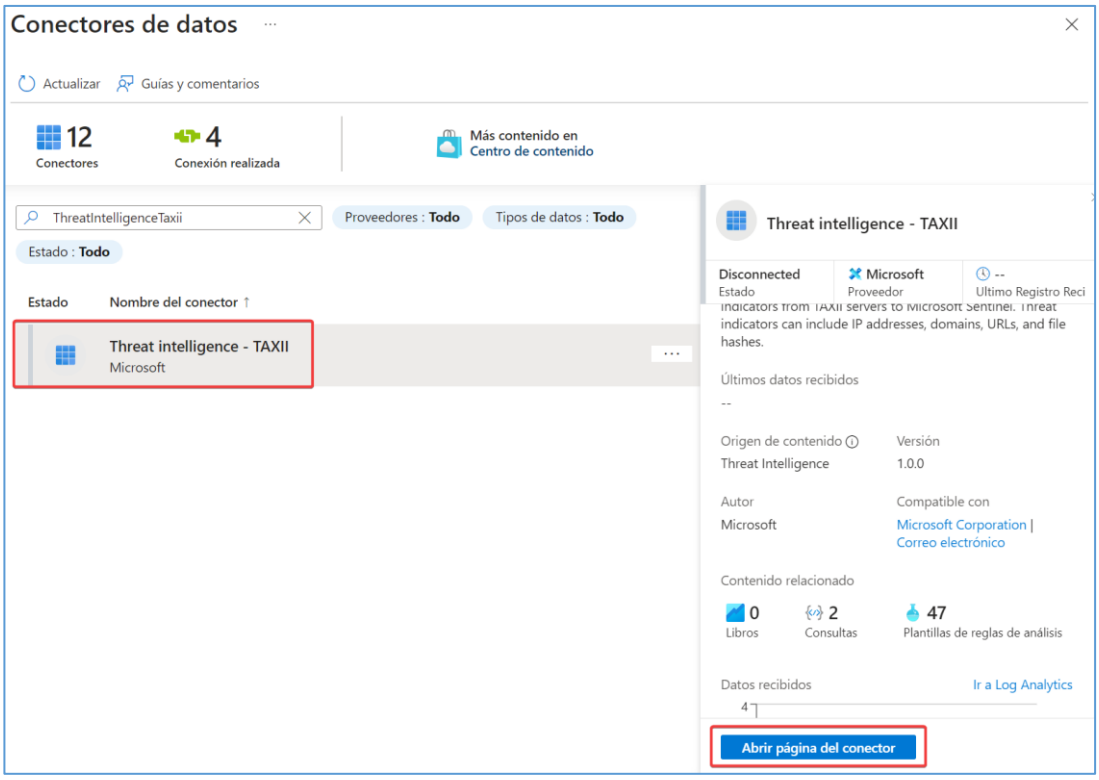




Para el conector Microsoft Defender Threat Intelligence, únicamente se seleccionarán los indicadores y se conectará:

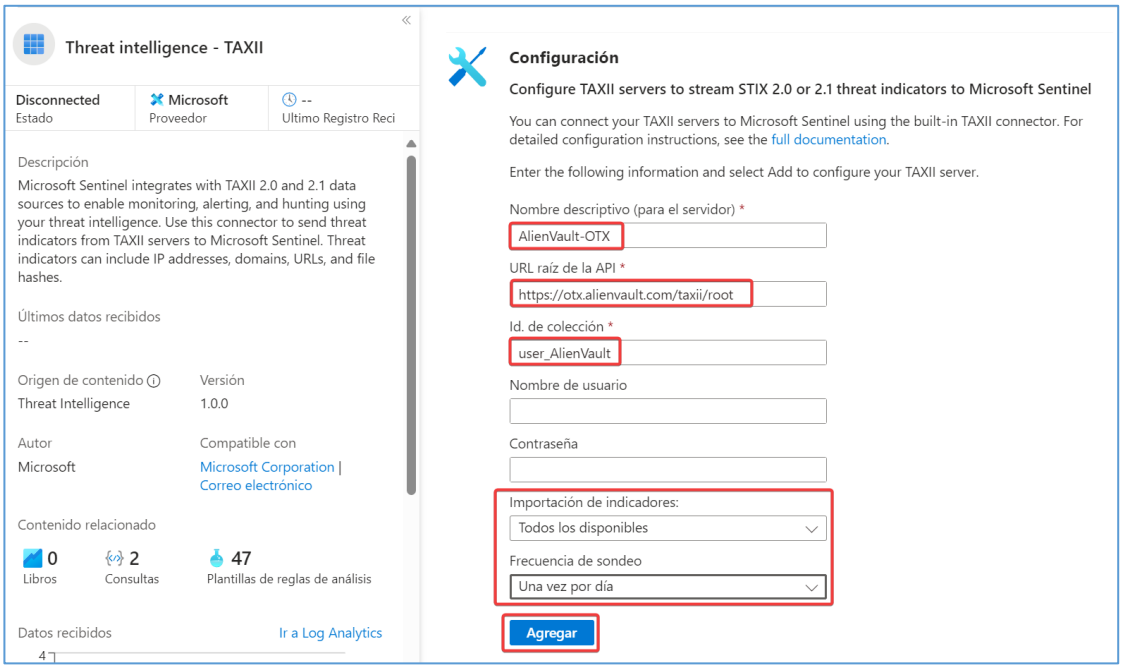


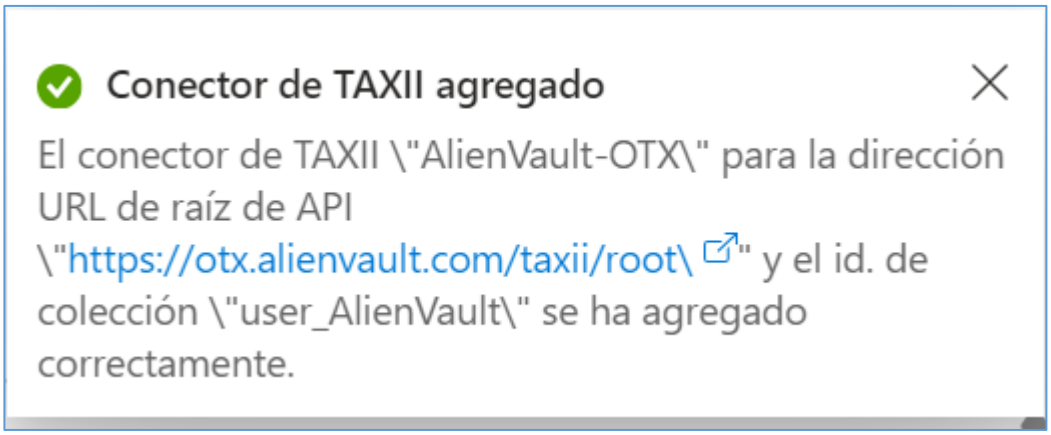
A continuación, se configurará el conector Threat intelligence – TAXII:



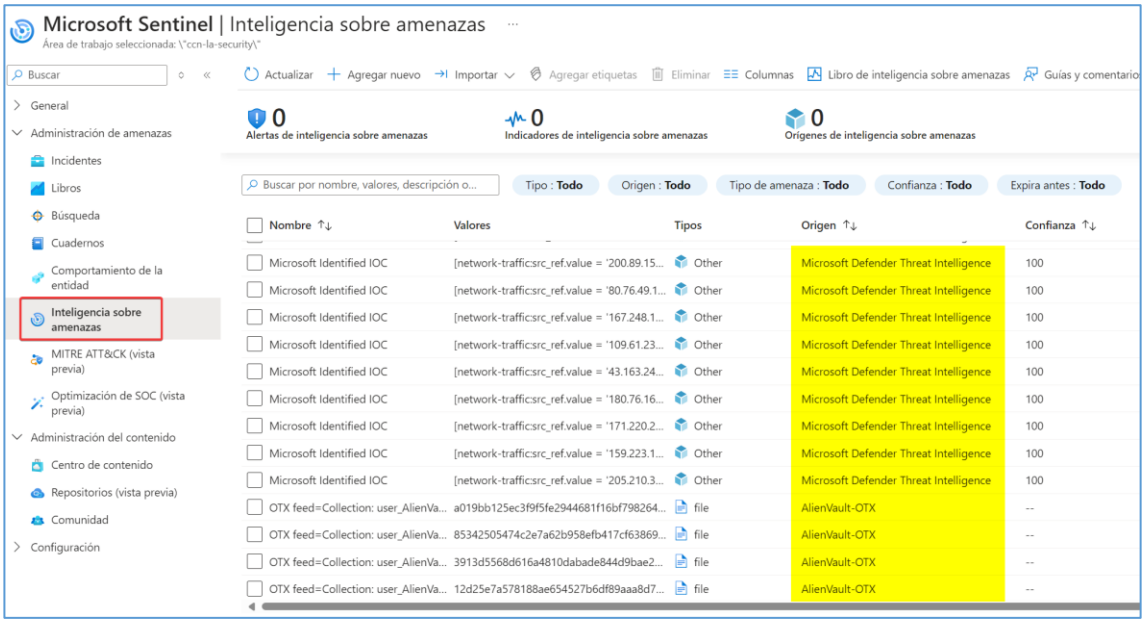
En la parte de configuración, se configura el servidor TAXII con los siguientes parámetros:

- Nombre descriptivo (para el servidor): Este nombre aparecerá como origen de la inteligencia sobre amenazas
- URL raíz de la API: https://otx.alienvault.com/taxii/root
- Id. de colección: user_AlienVault





Para comprobar que se han configurado correctamente los conectores y que las fuentes ya están disponibles seleccionaremos *Inteligencia sobre amenazas*:



A partir de este momento se dispondrá de nuevas alertas enriquecidas que ayudarán en la búsqueda de amenazas y completarán la funcionalidad que ofrece Microsoft Sentinel. Para obtener más información se puede consultar el siguiente enlace: https://docs.microsoft.com/es-es/azure/sentinel/threat-intelligence-integration

3.1.3.2 VIGILANCIA

Azure Monitor

Microsoft Sentinel trabaja con los datos almacenados en Log Analytics, y Log Analytics forma parte de Azure Monitor que es la solución que permite recopilar, analizar y administrar datos telemétricos tanto en la nube como en los entornos locales. Permite identificar de manera proactiva los problemas que les afectan y los recursos de los que dependen.

Todos los datos recopilados por Azure Monitor se pueden clasificar como uno de los dos tipos fundamentales: métricas y registros. Las métricas son valores numéricos que describen algún aspecto de un sistema en un momento dado.

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

Azure Monitor recopila y enruta los datos de supervisión mediante algunos mecanismos diferentes, en función de los datos que se enrutan y del destino:

- **Instrumentación de aplicaciones (Application Insights)**: se habilita mediante la instrumentación automática (agente) o la incorporación del SDK de Application Insights al código de la aplicación. Además, Application Insights está en proceso de implementación de Open Telemetry.
- **Agentes**: Los agentes pueden recopilar datos de supervisión del sistema operativo invitado de Azure y las máquinas virtuales híbridas.
- **Reglas de recopilación de datos**: Se usan reglas de recopilación de datos para especificar qué datos deben recopilarse, cómo transformarlos y dónde enviarlos.
- **Zero Config**: Los datos se envían automáticamente a un destino sin configuración de usuario. Las métricas de plataforma son el ejemplo más común.
- **Configuración de diagnóstico**: Se usa la configuración de diagnóstico para determinar dónde enviar datos de registro de actividad y recursos en la plataforma de datos.
- **API de REST de Azure Monitor**: La API de ingesta de registros en Azure Monitor le permite enviar datos a un área de trabajo de Log Analytics en los registros de Azure Monitor. También puede enviar métricas al almacén de métricas de Azure Monitor mediante la API de métricas personalizadas.

Visualizar y supervisar los datos con Microsoft Sentinel

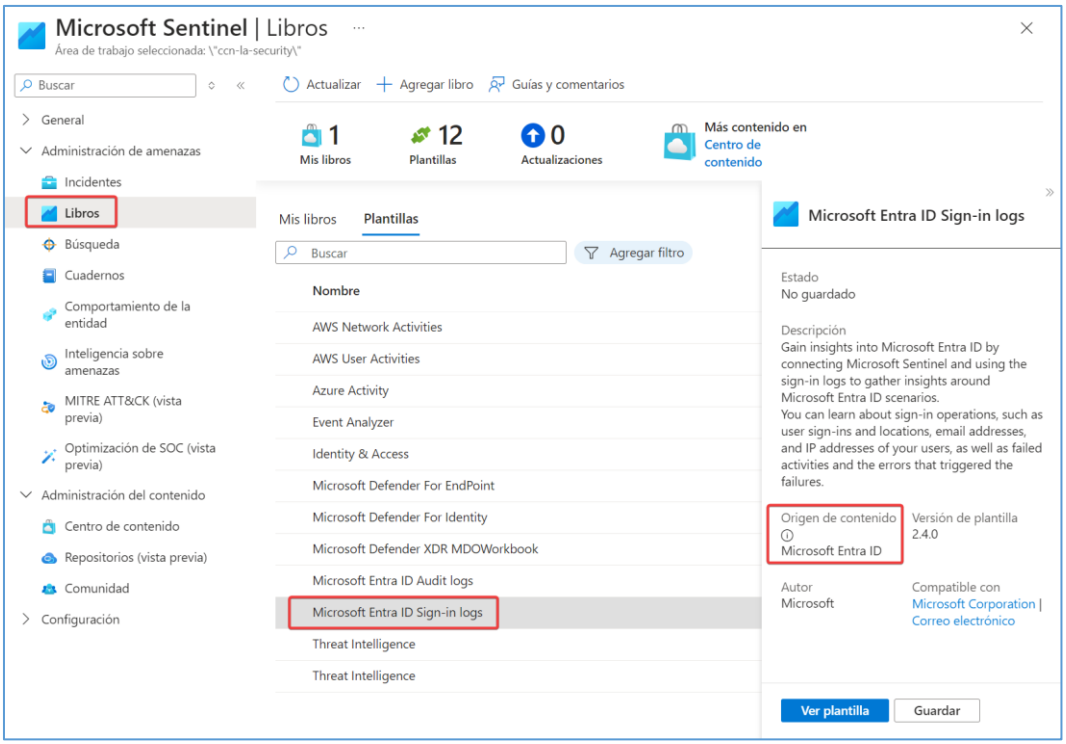
Después de conectar los orígenes de datos a Microsoft Sentinel, se puede visualizar y supervisar los datos mediante la adopción de Microsoft Sentinel Workbooks basados en Azure Monitor, lo que proporciona versatilidad para crear paneles personalizados.

Microsoft Sentinel permite crear libros personalizados en los datos o usar plantillas de libro existentes disponibles con soluciones empaquetadas o como contenido independiente del centro de contenido.

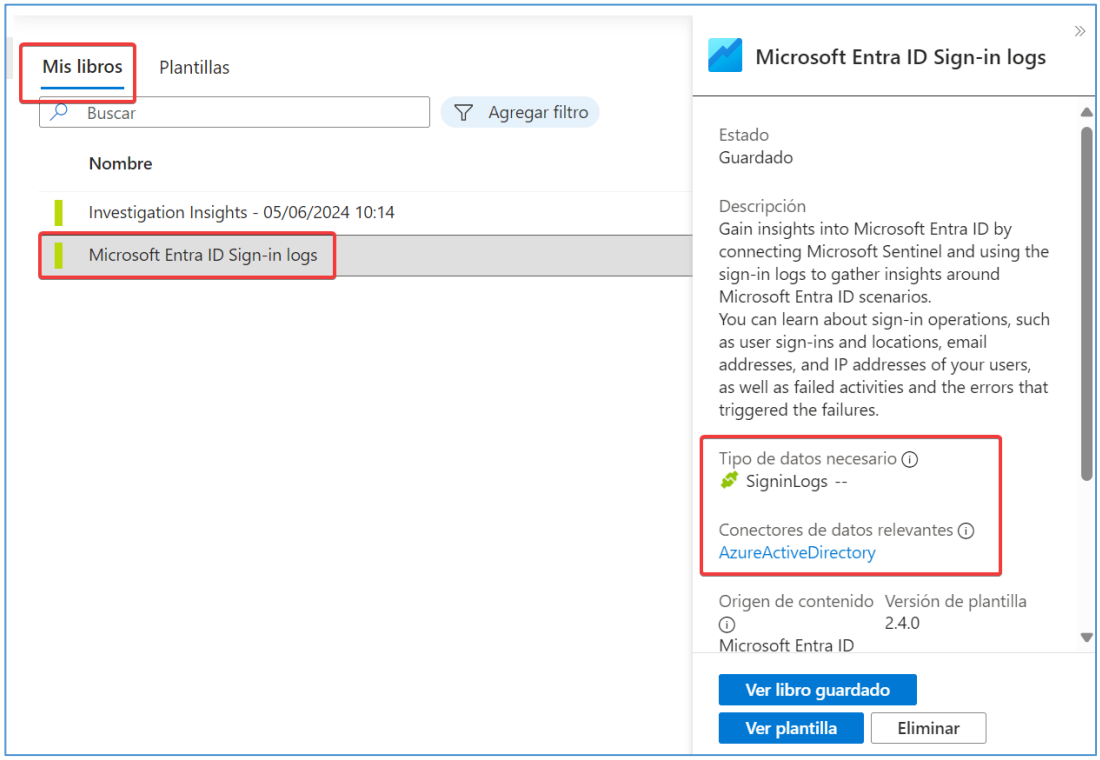
Para usar una plantilla de libro, instale la solución que contiene el libro o instale el libro como un elemento independiente desde el Centro de contenido. Para crear un libro a partir de una plantilla se seguirán los siguientes pasos:

1. Seleccionar **Administración de amenazas** y luego **Libros**, a continuación, seleccionar **Plantillas** para ver la lista de plantillas de libro instaladas.

   Para ver cuáles son pertinentes para los tipos de datos que se han conectado, el campo Origen de contenido de cada libro mostrará la fuente de datos de la que se alimentará ese libro.



2. Seleccionar **Ver plantilla** para visualizar los datos ofrecidos por la plantilla elegida.
3. Para editar el libro, seleccionar Guardar y, a continuación, la ubicación de azure en la que se quiere guardar el archivo JSON de la plantilla. Se pueden ver seleccionando **Mis libros**. Una vez guardado también se puede ver el tipo de dato necesario para ese libro y los conectores de datos relevantes:



Una vez guardado, se puede ver la plantilla desde la que ha sido creado, ver los datos que muestra el libro y editarlo para mostrar otro tipo de gráficos o eliminar el libro.

También se pueden crear los libros desde cero.

3.2 MEDIDAS DE PROTECCIÓN

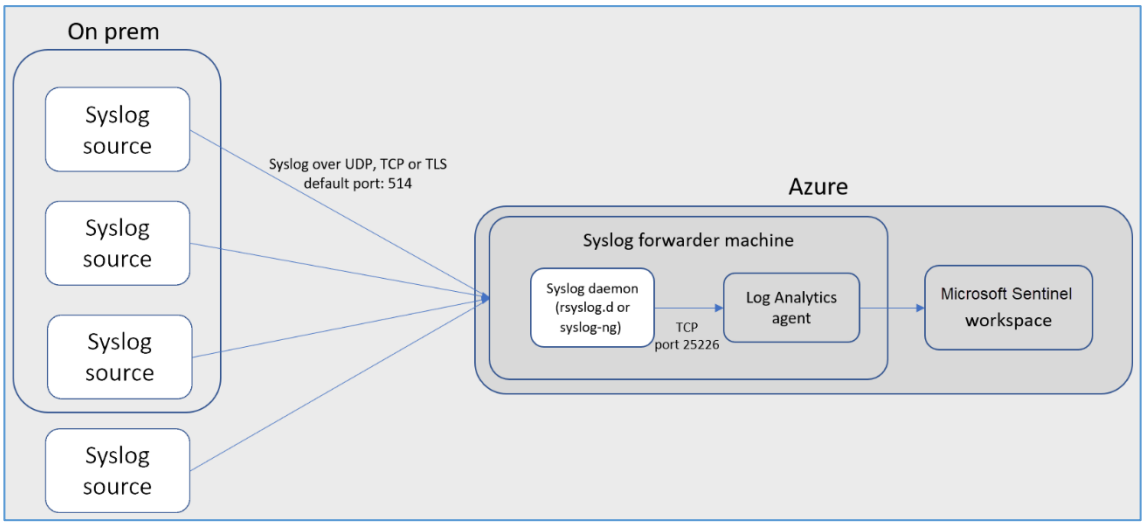
3.2.1 PROTECCIÓN DE LAS COMUNICACIONES

En cuanto a la protección de las comunicaciones, Microsoft Sentinel necesita conectar los orígenes de datos. Microsoft Sentinel incluye varios conectores para soluciones de Microsoft, que están disponibles inmediatamente y proporcionan integración en tiempo real, entre las que se incluyen las soluciones de Microsoft Defender XDR, Microsoft Defender Threat Intelligence, Microsoft Defender for Office 365, Microsoft Entra ID, Microsoft Defender for Identity, Microsoft Defender for Endpoint y Microsoft Defender for Cloud Apps, entre otros. Además, hay conectores integrados al amplio ecosistema de seguridad para soluciones que no son de Microsoft. También puede usar el formato de evento común (CEF), Syslog o la API REST para conectar los orígenes de datos con Microsoft Sentinel.

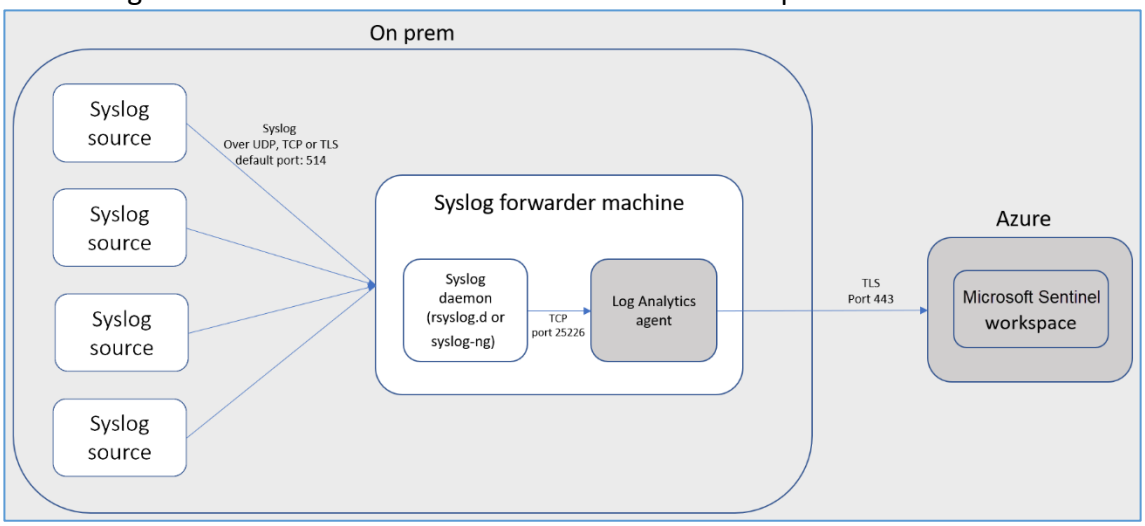
Los siguientes métodos de conexión de datos son compatibles con Microsoft Sentinel:

- **Conexiones de datos basadas en configuración de diagnóstico:** Este grupo de conectores de datos usan conexiones basadas en la configuración de diagnóstico administradas por Azure Policy. Algunos de estos tipos de conectores se administran mediante Azure Policy. Algunos ejemplos de este tipo de conector son: Actividad de Azure, Azure DDoS Protection o Cuenta de Azure Storage.
- **Conexiones de datos basadas en API**: Algunos orígenes de datos se conectan mediante las API proporcionadas por el origen de datos conectado. Normalmente, la mayoría de las tecnologías de seguridad proporcionan un conjunto de API a través del cual se pueden recuperar registros de eventos. Las API se conectan a Microsoft Sentinel y recopilan y envían tipos de datos específicos a Azure Log Analytics. Algunos ejemplos de este tipo de conector son: Protección de Microsoft Entra ID, Microsoft Defender for cloud apps, Microsoft Office 365, etc.
- **Conexiones basadas en agentes de Windows**: Algunos conectores basados en el agente de Azure Monitor (AMA) se encuentran actualmente en VERSIÓN PRELIMINAR. Además de utilizar el agente directamente, también se puede usar los conectores Syslog a través de AMA y formato de evento común (CEF) a través de AMA para filtrar e ingerir rápidamente mensajes de Syslog, incluidos los de formato de evento común (CEF), desde máquinas Linux y desde dispositivos de seguridad y red.

Se muestra la arquitectura para trabajar con registros con formato CEF para conectar los orígenes de datos. Configuración en el caso de una máquina virtual Linux en Azure:



Configuración si usa una VM en otra nube o en una máquina del entorno local:

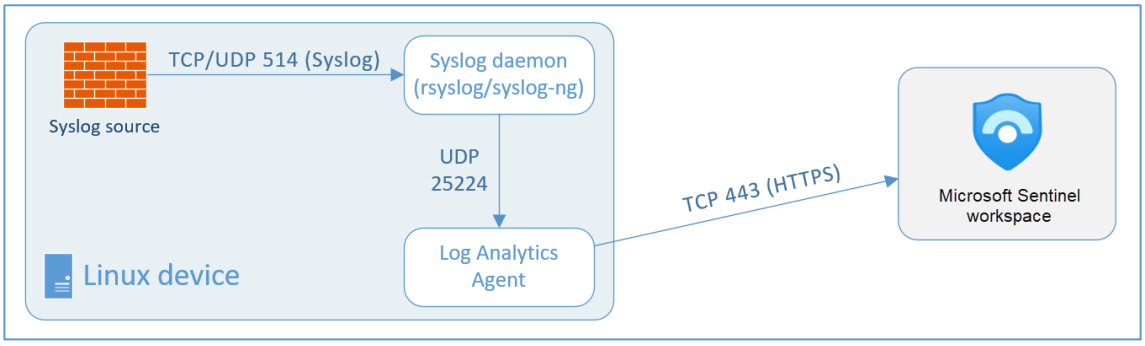


El agente de Microsoft Sentinel, que en realidad es el agente de Log Analytics, convierte los registros con formato CEF a un formato que Log Analytics puede ingerir. Dependiendo del tipo de dispositivo, el agente se instala directamente en el dispositivo o en un reenviador de registros Linux dedicado. El agente para Linux recibe eventos del demonio de Syslog a través de UDP; sin embargo, si se espera que una máquina Linux recopile un gran volumen de eventos Syslog, se envían a través de TCP desde el demonio de Syslog al agente y desde allí a Log Analytics.

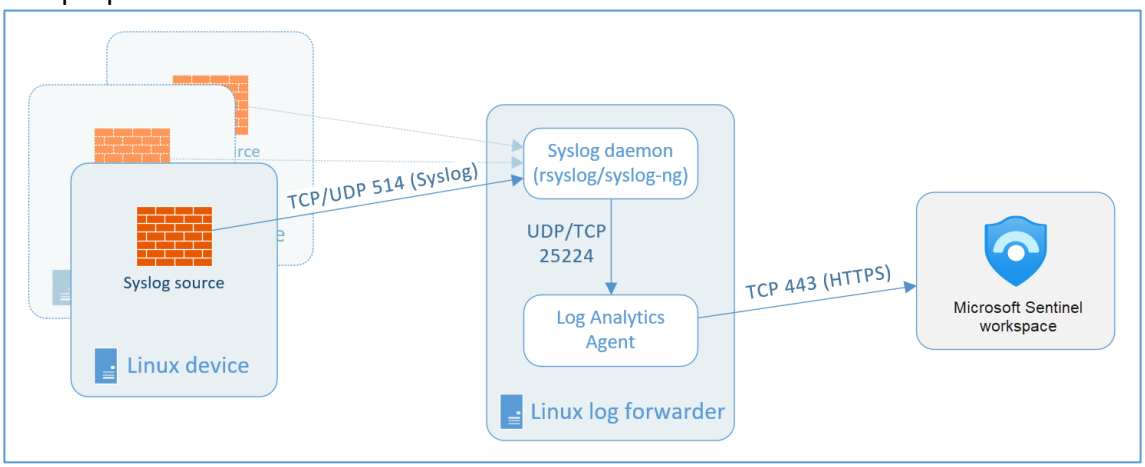
Para garantizar la seguridad de los datos en tránsito hacia los registros de Azure Monitor, se recomienda encarecidamente configurar el agente para que use al menos Seguridad de la capa de transporte (TLS) 1.2. Las versiones anteriores de TLS/Capa de sockets seguros (SSL) han demostrado ser vulnerables y, si bien todavía funcionan para permitir la compatibilidad con versiones anteriores, no se recomiendan. Para información adicional, revise

Sending data securely using TLS 1.2 (Envío de datos de forma segura mediante TLS 1.2).

El agente para Linux y Windows se comunica con el servicio Azure Monitor a través del puerto TCP 443. Ejemplo de arquitectura para la recopilación de datos de orígenes basados en Linux mediante Syslog:

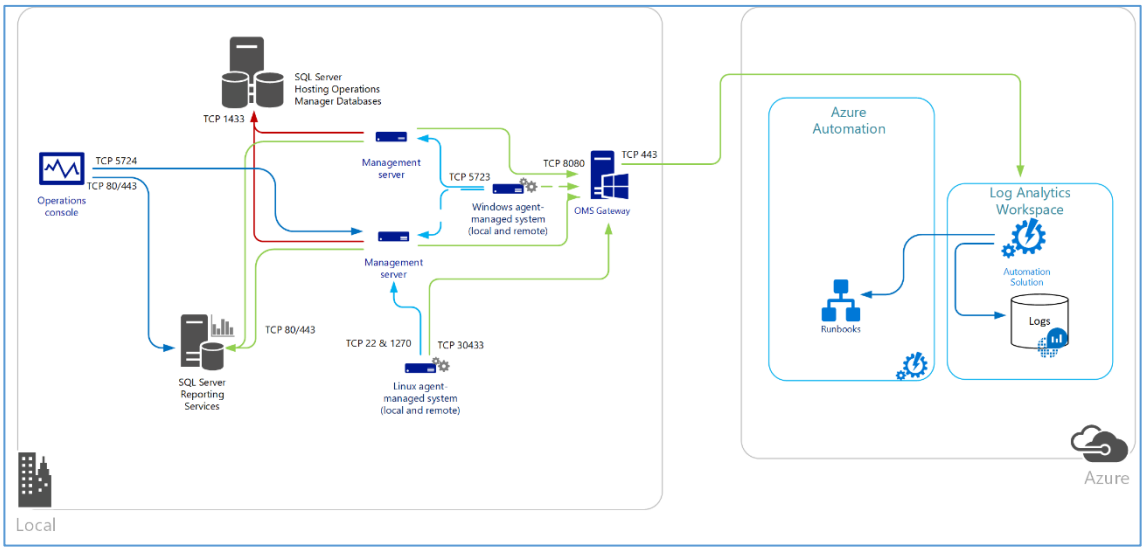


En el caso de contar con un reenviador, el ejemplo de arquitectura propuesto sería:



Como se puede ver en ambas arquitecturas la conexión se establece por el canal seguro HTTPS.

Si la máquina se conecta mediante un servidor proxy o firewall para comunicarse a través de Internet, es necesario consultar los requisitos siguientes para comprender qué configuración de red es necesaria. Si las directivas de seguridad de TI no permiten que los equipos de la red se conecten a Internet, se puede configurar una puerta de enlace de Log Analytics y, luego, configurar el agente para conectarse a Azure Monitor a través de la puerta de enlace. Después, el agente puede recibir información de configuración y enviar los datos recopilados.



3.2.2 PROTECCIÓN DE LA INFORMACIÓN

3.2.2.1 CALIFICACIÓN DE LA INFORMACIÓN

Los datos recopilados en Microsoft Sentinel se clasifican en **entidades**. Algunos ejemplos comunes de entidades son: usuarios, hosts, archivos, procesos, direcciones IP y direcciones URL.

Microsoft Sentinel admite una gran variedad de tipos de entidad. Cada tipo contiene atributos únicos, incluyendo algunos que pueden usarse para identificar una entidad determinada. Estos atributos se representan como campos en la entidad y se denominan **identificadores**.

Estos **identificadores** pueden hacer referencia a **identificadores seguros** si identifican una única entidad sin ambigüedad, o pueden hacer referencia a **identificadores no seguros** si identifican una entidad en algunas circunstancias, pero no identifican de forma única a una entidad en todos los casos. Por lo tanto, en una gran cantidad de ocasiones podemos combinar una selección de identificadores no seguros para generar un identificador seguro.

Por ejemplo, las cuentas de usuario se pueden identificar como entidades de **cuenta** de más de una manera. A través de un único **identificador seguro** como el identificador numérico de una cuenta de Microsoft Entra ID (el campo **GUID**) o a través de su valor de **Nombre principal de usuario (UPN)**. También es posible identificarlos con una combinación de **identificadores no seguros** como sus campos **Nombre** y **NTDomain**. Con estos orígenes de datos se identificará al mismo usuario de diferentes maneras. Si Microsoft Sentinel encuentra dos entidades que puede reconocer como la misma entidad en función de sus identificadores, las combinará para mantener un control más coherente.

Sin embargo, si uno de los proveedores de recursos crea una alerta en la que una entidad no está suficientemente identificada (por ejemplo, con un solo **identificador**

no seguro como un nombre de usuario sin el contexto de nombre de dominio), la entidad de usuario no se puede combinar. Generando instancias que se identificarán como entidades independientes en lugar de unificarse.

Para reducir el riesgo de que esto suceda, es necesario comprobar que todos los proveedores de alertas identifican correctamente las entidades en las alertas que producen. Además, la sincronización de entidades de cuenta de usuario con Microsoft Entra ID puede crear un directorio unificador para combinar entidades de cuenta de usuario.

Microsoft Sentinel almacena los datos en tablas en el área de trabajo de Log Analytics. Estas tablas se consultan a intervalos programados por las reglas de análisis que se han definido y habilitado. Una de las muchas acciones que realizan estas reglas de análisis es la asignación de campos de datos de las tablas a las entidades reconocidas por Microsoft Sentinel. Con estas asignaciones, Microsoft Sentinel tomará los campos de los resultados devueltos por la consulta, reconocerá los identificadores específicos de cada tipo de entidad y les aplicará el tipo de entidad identificado por esos identificadores.

Cuando Microsoft Sentinel es capaz de identificar entidades en alertas de diferentes tipos de orígenes de datos y, especialmente, si puede hacerlo con identificadores seguros comunes a cada origen de datos o a un tercer esquema, puede establecer fácilmente la correlación entre todos estos orígenes de datos y alertas. Permitiendo crear un almacén de información completo ayudando a generar una base sólida para las operaciones de seguridad.

3.2.2.2 COPIAS DE SEGURIDAD (BACKUP)

Microsoft utiliza un modelo de responsabilidad compartida donde especifica qué es responsabilidad de Microsoft y qué responsabilidad tiene el cliente en materia de *copias de seguridad*.

En concreto para Microsoft Sentinel se podría exportar la configuración y los datos a Azure Blobs (cuentas de almacenamiento) utilizando Logic App, en Azure Storage se podría configurar Azure backup.

La solución de backup integrada para los datos de Azure Storage se almacenan localmente en la propia cuenta de Azure Storage para la que se realiza la copia de seguridad, permitiendo recuperar los datos a un momento determinado en el tiempo cuando sea necesario.

Su funcionamiento se basa en una solución de copia de seguridad local, por tanto, no se transfieren los datos al almacén de Azure Backup. La copia de seguridad operativa se encarga de habilitar la restauración a un momento dado, así como las funcionalidades subyacentes, para que los datos se conserven durante el tiempo especificado.

La protección de los datos se establece a través de una directiva de copia de seguridad para administrar la duración de la retención de los datos de la copia de seguridad. Teniendo una retención máxima de 360 días en el caso de utilizar una copia de seguridad operativa de blobs.

La administración de las copias de seguridad permite realizar las operaciones de copia de seguridad de una cuenta de almacenamiento, como iniciar restauraciones, supervisar, detener la protección, etc., al integrarse en el Centro de copia de seguridad para ayudar a administrar de forma centralizada la protección de todas las cuentas de almacenamiento, además de todas las otras cargas de trabajo compatibles con copias de seguridad.

El Centro de copia de seguridad es un panel único para todos los requisitos de copia de seguridad: supervisar los trabajos y el estado de las copias de seguridad y restauraciones, garantizar el cumplimiento y la gobernanza, analizar el uso de las copias de seguridad y ejecución de operaciones relacionadas con la copia de seguridad y restauración de los datos.

Mediante la restauración, se pueden recuperar los datos de cualquier punto en el tiempo para el cual exista un punto de recuperación. Los puntos de recuperación se crean cuando una cuenta de almacenamiento se encuentra en estado protegido, y se pueden usar para restaurar datos siempre que se encuentren dentro del período de retención definido.

Consultar el siguiente enlace para ampliar la información sobre Azure backup: https://docs.microsoft.com/es-es/azure/backup/blob-backup-overview.

3.2.3 PROTECCIÓN DE LOS SERVICIOS

3.2.3.1.1 PROTECCIÓN FRENTE A LA DENEGACIÓN DE SERVICIO

Azure proporciona protección continua contra los ataques de denegación de servicio. Esta protección se integra en la plataforma Azure mediante Azure DDoS Protection

DDoS Protection aprovecha la escalabilidad y la elasticidad de la red global de Microsoft para aportar una funcionalidad de mitigación de DDoS masiva en todas las regiones de Azure. El servicio DDoS Protection de Microsoft limpia el tráfico en la red perimetral de Azure antes de que pueda afectar a la disponibilidad del servicio, a fin de proteger las aplicaciones de Azure.

Hay dos niveles de DDoS Protection:

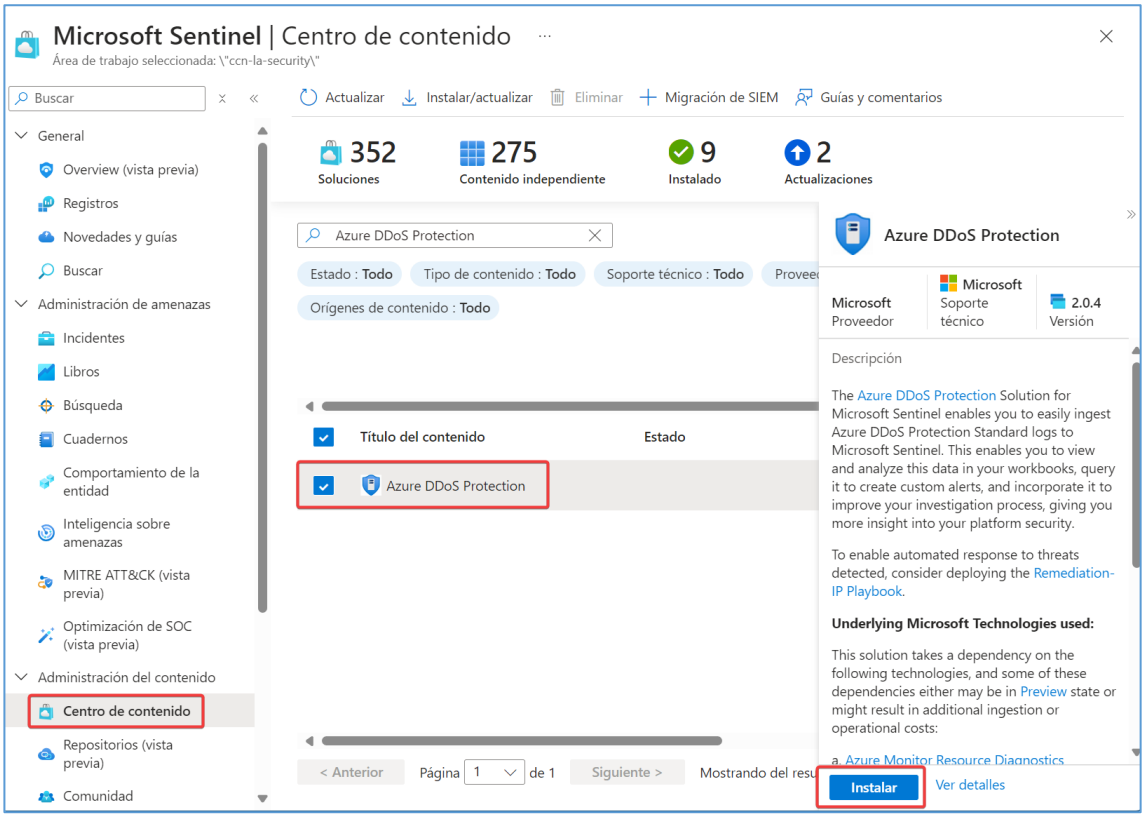
a) Protección de red contra DDoS (Azure DDoS Network Protection): Junto con los procedimientos recomendados de diseño de aplicaciones, proporciona características mejoradas de mitigación DDoS para protegerse de los ataques DDoS. Se ajusta automáticamente para proteger los recursos específicos de Azure de una red virtual.

b) Protección de IP de Azure contra DDoS: Es un modelo de IP de pago por protección. Protección de IP de Azure contra DDoS contiene las mismas características de ingeniería principales que Protección de red contra DDoS, pero variará en los siguientes servicios de valor añadido: compatibilidad con respuesta rápida de DDoS, protección de costos y descuentos en WAF.

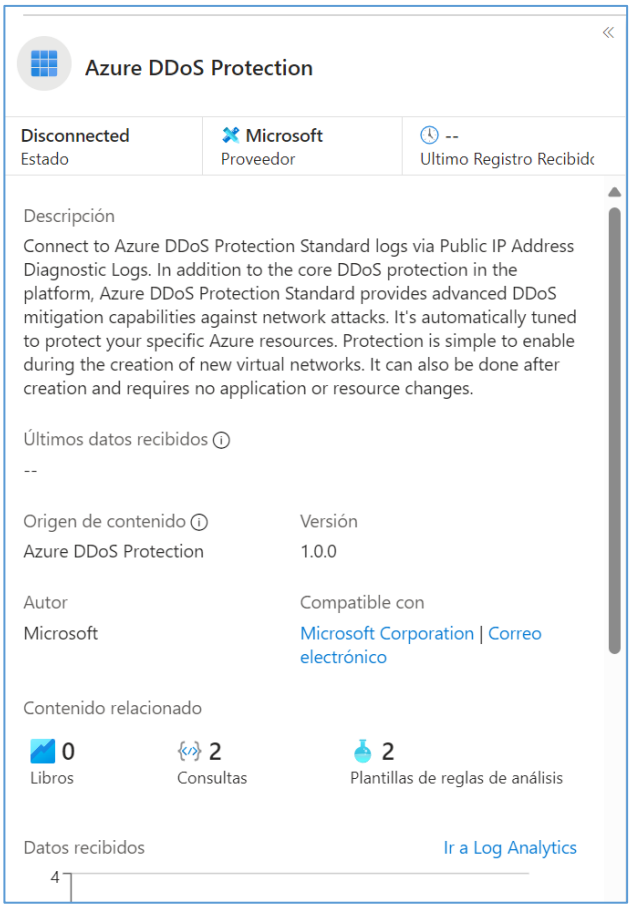
Durante el proceso de creación de una red virtual se ofrece la posibilidad de asociar la VNET con un Plan de protección contra DDoS.

Durante el proceso de creación de una IP pública se ofrece la posibilidad de especificar el tipo de protección DDoS: protección de red (hereda la protección contra DDoS de la red virtual), dirección IP (específico de la IP) o deshabilitar. Se puede ampliar información consultando la guía: CCN-STIC-884A Guía de Configuración segura para Azure.

Si se desea integrar en Microsoft Sentinel, es necesario habilitar el servicio DDoS Protection en una red virtual (VNET), este proceso se explica en la guía: CCN-STIC-884ª Guía de Configuración segura para Azure. Una vez hecho esto se podrá utilizar el conector disponible en la solución Azure DDoS Protection para ingestar estos datos con Microsoft Sentinel:



A continuación, se muestran los detalles del conector:


Azure DDoS Protection
Disconnected
Estado
Microsoft
Proveedor
--
Ultimo Registro Recibid
Descripción
Connect to Azure DDoS Protection Standard logs via Public IP Address Diagnostic Logs. In addition to the core DDoS protection in the platform, Azure DDoS Protection Standard provides advanced DDoS mitigation capabilities against network attacks. It's automatically tuned to protect your specific Azure resources. Protection is simple to enable during the creation of new virtual networks. It can also be done after creation and requires no application or resource changes.
Últimos datos recibidos
--
Origen de contenido
Azure DDoS Protection
Versión
1.0.0
Autor
Microsoft
Compatible con
Microsoft Corporation | Correo electrónico
Contenido relacionado
0
Libros
2
Consultas
2
Plantillas de reglas de análisis
Datos recibidos
Ir a Log Analytics
4

4. GLOSARIO Y ABREVIATURAS

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

Término	Definición
AMA	*Azure Monitor Agent (Agente de Azure Monitor).*
AWS	*Amazon Web Services.*
Microsoft Entra ID	*Servicio de administración de identidades y acceso.*
Azure PowerShell	*Una interfaz de la línea de comandos para administrar los servicios de Azure a través de una línea de comandos*
CEF	*Common Event Format. Es un formato estándar de la industria para los mensajes de Syslog, utilizado por muchos proveedores de seguridad para permitir la interoperabilidad de eventos entre diferentes plataformas.*
CLI	*Una interfaz de la línea de comandos que se puede utilizar para administrar los servicios de Azure desde Windows, OSX y Linux.*
DDoS	*Distributed Denial of Service (Ataque de Denegación de Servicio Distribuido), el cual se lleva a cabo generando un gran flujo de información desde varios puntos de conexión hacia un mismo punto de destino.*
ENS	*Esquema Nacional de Seguridad.*
GUID	*Globally Unique Identifier (Identificador único global).*
JSON	*Acrónimo de JavaScript Object Notation, «notación de objeto de JavaScript») es un formato de texto sencillo para el intercambio de datos.*
IDS	*Intrusion Detection System (Sistema de detección de intrusos)*
IPS	*Intrusion Prevention System (Sistema de prevención de intrusos)*
Log Analytics	*Es una herramienta de Azure Portal que se usa para editar y ejecutar consultas de registro en los datos del almacén de registros de Azure Monitor.*

Logic Apps	*Es una plataforma basada en la nube para crear y ejecutar flujos de trabajo automatizados que integren las aplicaciones, datos, servicios y sistemas.*
MFA	*Multifactor Authentication (Autenticación Multifactor). Sistema de seguridad que requiere más de una forma de autenticarse, por ejemplo, a través de una aplicación, señal Biométrica, etc.*
PIM	*Privileged Identity Management (Administración de identidades privilegiadas)*
Playbook	*Es una colección de acciones correctivas que se pueden ejecutar desde Microsoft Sentinel en respuesta a una alerta o un incidente.*
RBAC	*RBAC es un sistema de autorización basado en Azure Resource Manager que proporciona administración de acceso específico a los recursos de Azure.*
SaaS	*Software as a Service*
SIEM	*Security Information and Event Management. (Seguridad de la Información y Administración de Eventos)*
SOAR	*Security Orchestration, Automation and Response. (Orquestación de la Seguridad y Respuestas Automatizadas)*
SOC	*Security Operations Center (Centro de Operaciones de Seguridad)*
TI	*Threat Intelligence (Inteligencia frente a amenazas)*
UPN	*Universal Principal Name (Nombre Universal Principal).*
VNET	*Virtual Network (Red virtual).*
Workbook	*Un workbook permite visualizar y supervisar los datos proporcionando versatilidad al crear paneles personalizados.*

5. CUADRO RESUMEN DE MEDIDAS DE SEGURIDAD

Se facilita a continuación un cuadro resumen de configuraciones a aplicar para la protección del servicio, donde la organización puede valorar qué medidas de las propuestas se cumplen.

Control ENS	Configuracion	Estado	
op	**Marco Operacional**		
op.acc	**Control de Acceso**		
op.acc.1	**Identificación**		
	Se ha realizado adecuadamente la gestión de identidades.	**Aplica:** ☐ Sí ☐ No	**Cumple:** ☐ Sí ☐ No
		Evidencias Recogidas: ☐ Sí ☐ No	**Observaciones:**
Op.acc.3	**Segregación de funciones y tareas**		
	Se ha asignado adecuadamente los roles de administración.	**Aplica:** ☐ Sí ☐ No	**Cumple:** ☐ Sí ☐ No

		Evidencias Recogidas: ☐ Sí ☐ No	**Observaciones:**
Op.acc.5	**Mecanismo de autenticación (usuarios externos)**		
	Se ha habilitado Multi-Factor Authentication (MFA) para los usuarios externos. Se han configurado directivas de acceso condicional para el control de acceso.	**Aplica:** ☐ Sí ☐ No	**Cumple:** ☐ Sí ☐ No
		Evidencias Recogidas: ☐ Sí ☐ No	**Observaciones:**
Op.acc.6	**Mecanismo de autenticación (usuarios de la organización)**		
	Se ha habilitado Multi-Factor Authentication (MFA) para los usuarios externos. Se han configurado directivas de acceso condicional para el control de acceso.	**Aplica:** ☐ Sí ☐ No	**Cumple:** ☐ Sí ☐ No
		Evidencias Recogidas: ☐ Sí ☐ No	**Observaciones:**
op.exp.6	**Protección frente a código dañino**		
	Se han habilitado las plantillas de detección de amenazas con el tipo de regla de Microsoft Security	**Aplica:** ☐ Sí ☐ No	**Cumple:** ☐ Sí ☐ No

		Evidencias Recogidas: ☐ Sí ☐ No	**Observaciones:**
Op.mon.1	**Detección de intrusión**		
	Se han incorporado nuevas fuentes de TI a Microsoft Sentinel para mejorar el análisis.	**Aplica:** ☐ Sí ☐ No	**Cumple:** ☐ Sí ☐ No
		Evidencias Recogidas: ☐ Sí ☐ No	**Observaciones:**
mp.com	**Protección de las comunicaciones**		
	Se ha configurado el agente de Log Analytics para que use al menos Seguridad de la capa de transporte (TLS) 1.2.	**Aplica:** ☐ Sí ☐ No	**Cumple:** ☐ Sí ☐ No
		Evidencias Recogidas: ☐ Sí ☐ No	**Observaciones:**
Otras	**Log Analytics**		

	Se ha configurado adecuadamente la retención y el control de acceso en el servicio de Log Analytics sobre el cuál se habilitará la instancia de Microsoft Sentinel.	**Aplica:** ☐ Sí ☐ No	**Cumple:** ☐ Sí ☐ No
		Evidencias Recogidas: ☐ Sí ☐ No	**Observaciones:**

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL