CCN
centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 885F

Guía de configuración segura para Microsoft Defender for Identity

JUNIO 2024

MINISTERIO DE DEFENSA

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

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

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
2024.07.23 13:09:33 +02'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-24-251-2
Fecha de Edición: junio de 2024

ÍNDICE

1. MICROSOFT DEFENDER FOR IDENTITY

1.1 DESCRIPCIÓN DEL USO DE ESTA GUÍA

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

1.2 DEFINICIÓN DE LA SOLUCIÓN

Microsoft Defender for Identity forma parte de la suite de seguridad integrada Microsoft Defender *XDR*.

Microsoft Defender for Identity (antes Azure Advanced Threat Protection, conocido también como Azure ATP) es una solución de seguridad en la nube que ayuda a proteger las identidades que se usan en las organizaciones.

Defender for Identity está completamente integrado con Microsoft Defender XDR y usa las señales de Active Directory local e identidades en la nube para ayudar a identificar, detectar e investigar amenazas dirigidos a la organización.

Defender for Identity permite a los analistas de operaciones de seguridad y a los profesionales de la seguridad, que pueden tener problemas para detectar ataques avanzados en entornos híbridos, realizar las siguientes acciones:

- Evitar infracciones, mediante evaluaciones proactivas de la posición de seguridad de identidad.
- Detectar amenazas, utilizando análisis en tiempo real e inteligencia de datos.
- Investigación de actividades sospechosas en toda la cadena del ciberataque.
- Responder a ataques mediante respuesta automática a identidades en peligro.

Evaluación proactiva de la posición de Identidad

Defender for Identity ofrece una visión clara de la posición de seguridad de identidad, ayudando a identificar y resolver problemas antes de un atacante pueda explotarlos. Proporciona información útil sobre las configuraciones de identidad y los procedimientos de seguridad sugeridos. Mediante análisis de perfiles de usuario, reduce la superficie de ataque de la organización. Supervisa y analiza las actividades de los usuarios y la información de la red, creando una línea de base de comportamiento para cada usuario. Identifica anomalías y revela amenazas avanzadas y usuarios en peligro. Los sensores de *Defender for Identity* supervisan los controladores de dominio de la organización, proporcionando una vista completa de todas las actividades de los usuarios. Las evaluaciones de seguridad de *Defender for Identity* proporcionan información adicional para mejorar la posición y las directivas de seguridad de la organización.

Detección de amenazas en entornos de identidad modernos

Los entornos de identidad modernos, que suelen abarcar tanto en el entorno local como en la nube, dependen en gran medida de los Servicios de federación de Active Directory (AD FS) para la autenticación en entornos híbridos. Defender for Identity utiliza datos de todo el entorno, incluidos los controladores de dominio, AD FS y los servicios de certificados de Active Directory (AD CS), para proporcionar una vista completa del entorno de identidad.

Defender for Identity protege AD FS mediante la detección de ataques locales en AD FS y mostrando los eventos de autenticación generados por AD FS. Los sensores de Defender for Identity supervisan el tráfico del controlador de dominio de forma predeterminada. Para una supervisión completa de la identidad, es crucial instalar el tipo de sensor pertinente en los servidores de AD FS/AD CS.

Esta solución de seguridad ayuda a proteger la supervisión de identidades en toda la organización, proporcionando valiosas perspectivas sobre las configuraciones de identidad y las mejores prácticas de seguridad sugeridas. A través de informes de seguridad y análisis de perfiles de usuario, Defender for Identity ayuda a reducir drásticamente la superficie de ataque de la organización, dificultando el compromiso de las credenciales de usuario y el avance de un ataque.

Identificación de actividades sospechosas a través de la cadena de ataque

Normalmente, los ataques se inician contra cualquier entidad accesible, como un usuario con pocos privilegios, y después se mueven lateralmente hasta que el atacante accede a recursos valiosos, como cuentas confidenciales, administradores de dominio y datos altamente sensibles. *Defender for Identity* identifica estas amenazas avanzadas a través de toda la cadena de ataques (*cyber-attack kill-chain*):

- *Reconocimiento*

Identificar los intentos de usuarios malintencionados y atacantes de obtener información. Los atacantes buscan información sobre nombres de usuario, pertenencia a grupos, direcciones IP asignadas a dispositivos, etc.

- *Credenciales en peligro*

Identificar los intentos de comprometer las credenciales de usuario mediante ataques de fuerza bruta, autenticaciones erróneas, cambios en la pertenencia a un grupo de usuarios y otros métodos.

- *Movimientos laterales*

Detectar intentos de desplazamiento lateralmente dentro de la organización para obtener control de usuarios confidenciales mediante ataques como *pass-the-hash, pass-the-ticket, overpass-the-hash*, etc.

- *Dominación de dominio*

Investigar el comportamiento del atacante si se logra la "dominación del dominio" mediante la ejecución remota de código en el controlador de dominio, o métodos tales como *DC Shadow*, actividades de *golden ticket*, etc.

Investigar alertas y actividades de usuario

Defender for Identity está diseñado para reducir el ruido general de las alertas, y proporcionar solo las pertinentes e importantes en una "escala de tiempo de ataque" organizada, simple y en tiempo real.

La integración de Defender for Identity con Microsoft Defender XDR proporciona otra capa de seguridad mejorada mediante la correlación de datos de otros dominios, para una mayor visibilidad y precisión entre usuarios, dispositivos y recursos de red.

Por otro lado, conviene recalcar que Microsoft Defender for Identity proporciona valor de seguridad para todas las cuentas de Active Directory (AD DS), incluidas las que no se sincronizan con el identificador de Microsoft Entra. Las cuentas de usuario que se sincronizan con Entra ID también se beneficiarán del valor de seguridad proporcionado por Entra ID (basado en el nivel de licencia) y de la puntuación de prioridad de investigación.

1.3 PROTECCIÓN DEL PUESTO DE TRABAJO

1.3.1 MICROSOFT DEFENDER XDR

Microsoft Defender XDR, (anteriormente conocido como Microsoft 365 Defender), es un conjunto de defensa empresarial unificado previo y posterior a la vulneración. Este sistema coordina de forma nativa la detección, prevención, investigación y respuesta entre puntos de conexión, identidades, correo electrónico y aplicaciones para proporcionar protección integrada contra ataques sofisticados. Los profesionales de seguridad pueden unir las señales de amenaza que cada uno de estos productos

recibe y determinar el alcance completo y el impacto de la amenaza. 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, proporcionando así una solución integral para la seguridad del puesto de trabajo.

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

- **Puntos de Conexión (endpoints)** con *Microsoft Defender for Endpoint*: Defender para punto de conexión es una plataforma de punto de conexión integrada que ofrece prevención, detección después de la vulneración, investigación automatizada y respuesta.
- **Correo electrónico y colaboración** con *Microsoft Defender for Office 365*: Defender for Office 365 protege la organización contra las amenazas malintencionadas que suponen los mensajes de correo electrónico, los vínculos (URL) y las herramientas de colaboración.
- **Identidades con Defender for Identity y Protección de Microsoft Entra ID**: Microsoft Defender for Identity es una solución de seguridad basada en la nube que aprovecha las señales del Active Directory local (AD DS) para identificar, detectar e investigar amenazas avanzadas, identidades en peligro y acciones internas malintencionadas dirigidas a la organización. Protección de Microsoft Entra ID ayuda a detectar, investigar y corregir los riesgos relacionados con las identidades, que pueden ser utilizados posteriormente en herramientas como 'Acceso condicional' para tomar decisiones de acceso o alimentar una herramienta de administración de eventos e información de seguridad (SIEM) para realizar una investigación más detallada.
- **Aplicaciones** con *Microsoft Defender for Cloud Apps*: la seguridad de Microsoft Defender for Cloud Apps es una solución completa entre SaaS que ofrece una visibilidad profunda, controles de datos sólidos y una protección contra amenazas mejorada para las aplicaciones en la nube.

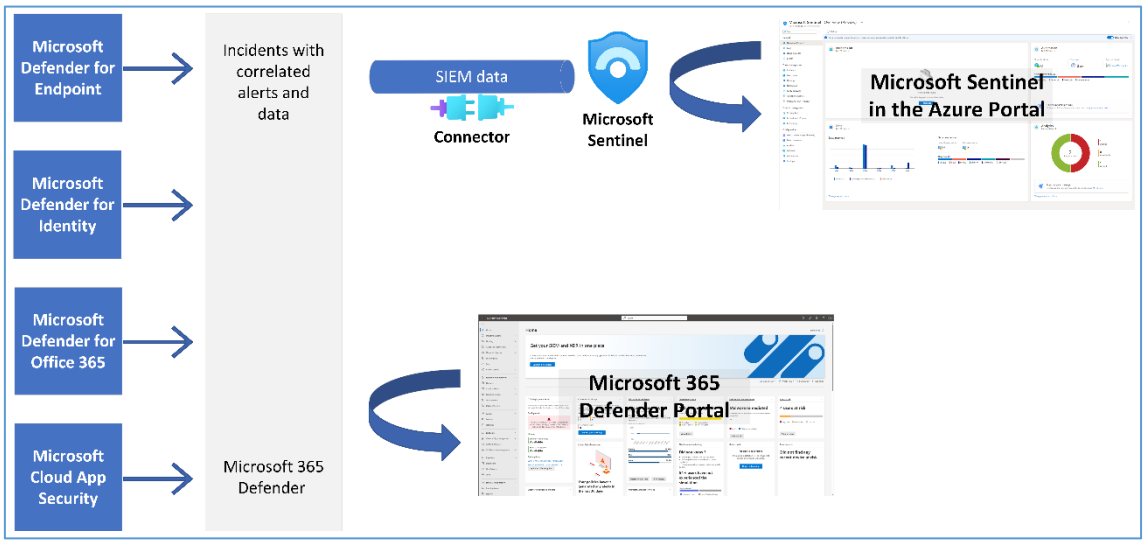
Microsoft Sentinel como SIEM/SOAR, es una plataforma de administración de eventos e información de seguridad (SIEM) nativa de la nube que utiliza IA integrada

para ayudar a analizar grandes volúmenes de datos en toda una empresa, rápidamente. Microsoft Sentinel agrega datos de todas las fuentes, incluidos usuarios, aplicaciones, servidores y dispositivos que se ejecutan en la infraestructura local o en cualquier nube, lo que te permite razonar sobre millones de registros en unos segundos, permitiendo crear construir *playbooks* para dar una respuesta efectiva e inmediata.

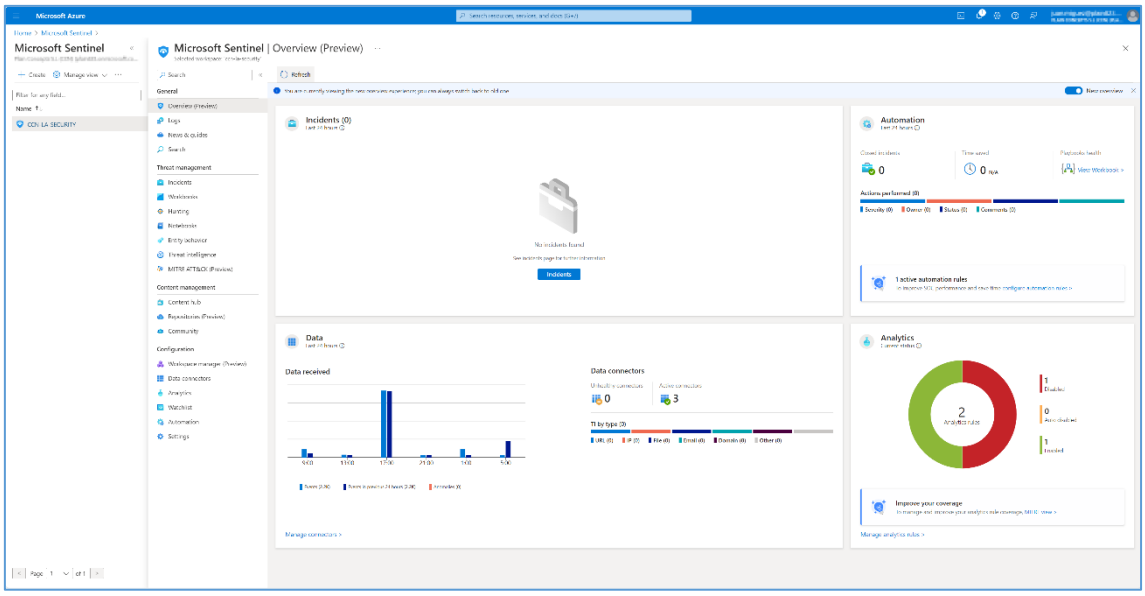
1.3.2 INTEGRACIÓN CON MICROSOFT SENTINEL

El conector de Microsoft Defender XDR para Microsoft Sentinel permite enviar y sincronizar toda la información de alertas e incidentes de Microsoft Defender XDR con Microsoft Sentinel.

Con este conector, se pueden transmitir a Microsoft Sentinel como datos SIEM los incidentes de Microsoft Defender XDR, que contienen todas las alertas relacionadas, entidades e información relevante que proviene de Microsoft Defender para punto de conexión, Microsoft Defender for Identity, Microsoft Defender para Office 365 y Microsoft Defender for Cloud Apps. Esto le ayuda a tener contexto para priorizar y responder a los incidentes con Microsoft Sentinel.



El conector también permite enviar los eventos de búsqueda avanzada de todos los componentes de Defender mencionados anteriormente a Microsoft Sentinel, de modo que se pueden replicar las consultas de búsqueda avanzada de esos componentes de Defender en Microsoft Sentinel, ampliar las alertas de Sentinel con los datos de eventos en bruto de los componentes de Defender para obtener información adicional y conservar los registros con una mayor duración en Log Analytics.



Consultar: [CCN-STIC- 884E- Guía de configuración segura para Microsoft Sentinel].

1.3.3 INTEGRACIÓN CON MICROSOFT DEFENDER FOR ENDPOINT

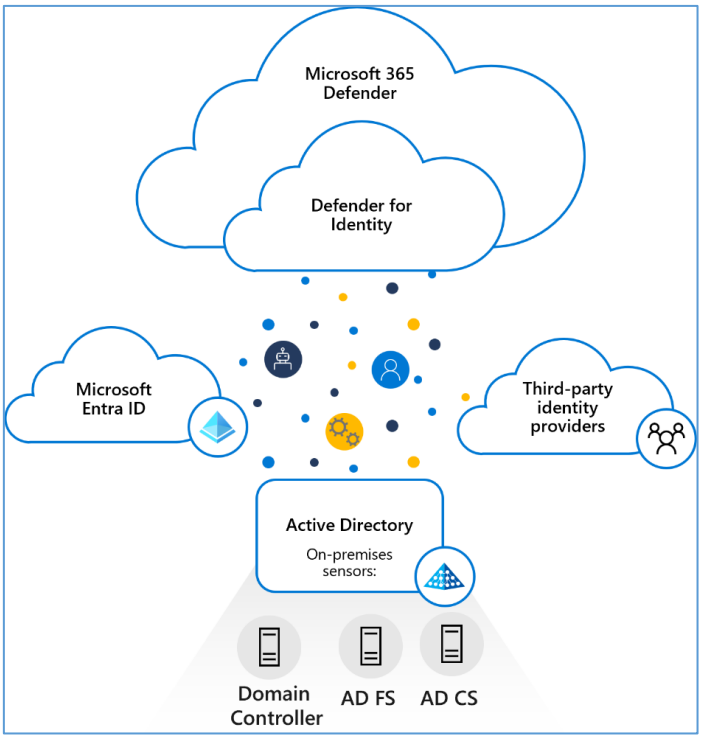
Desde la actualización de Defender for Identity de noviembre de 2022 (release 2.194) la integración manual con Defender for Endpoint no está soportada. Desde este momento se recomienda el uso del portal https://security.microsoft.com/ donde ya se encuentran todos los servicios de Defender integrados.

What's new archive - Microsoft Defender for Identity | Microsoft Learn

1.4 ARQUITECTURA DE MICROSOFT DEFENDER FOR IDENTITY

Microsoft Defender for Identity supervisa los controladores de dominio mediante la captura y el análisis del tráfico de red, aprovechando los eventos de Windows directamente desde los controladores de dominio. Analiza datos de amenazas y ataques.

La siguiente imagen muestra cómo Defender para la Identidad se superpone a Microsoft Defender XDR y funciona junto con otros proveedores de identidad de servicios de Microsoft y terceros para supervisar el tráfico proveniente de controladores de dominio y servidores de Active Directory (AD DS).



Instalado directamente en los controlador de dominio, en los servidores de Active Directory Federation Services (AD FS) o Active Directory Certificate Services (AD CS), el sensor de Defender for Identity accede a los registros de eventos directamente desde los servidores. Después de que el sensor analiza los registros y el tráfico de red, Defender for Identity envía únicamente la información analizada al servicio en la nube de Defender for Identity.

1.5 COMPONENTES DE DEFENDER FOR IDENTITY

Defender for Identity consta de los siguientes componentes principales:

a. **Portal** de Microsoft Defender

El portal de Microsoft Defender crea una instancia de Defender for Identity, muestra los datos recibidos de los sensores de Defender for Identity y permite supervisar, administrar e investigar las amenazas en el entorno de red.

b. **Sensor** de *Defender for Identity*

Los sensores de *Defender for Identity* se pueden instalar directamente en los siguientes servidores:

- Controladores de dominio: El sensor supervisa directamente el tráfico del controlador de dominio, sin que sea necesario usar un servidor dedicado ni la configuración de una creación de reflejo del puerto.
- AD FS / AD CS: El sensor supervisa directamente los eventos de autenticación y el tráfico de red.

c. **Servicio en la nube de *Defender for Identity***

El servicio en la nube de *Defender for Identity* se ejecuta en la infraestructura de Azure y actualmente está implementado en Estados Unidos, Europa y Asia. El servicio en la nube de *Defender for Identity* está conectado a Microsoft Intelligent Security Graph. Microsoft Intelligent Security Graph es un repositorio único y una API de seguridad de "punto final" con acceso a información en tiempo real de miles de millones de datos. Muchos partners de la industria, cada uno con su propia especialidad, informan sobre datos de telemetría y señales de seguridad a Intelligent Security Graph.

1.5.1 PORTAL DE DEFENDER FOR IDENTITY

Desde el portal de *Defender for Identity*, https://security.microsoft.com/, pueden realizarse las siguientes tareas:

a) Crear la instancia de *Defender for Identity*.
b) Integrar con otros servicios de seguridad de Microsoft.
c) Administrar la configuración del sensor de *Defender for Identity*.
d) Visualizar los datos recibidos de los sensores de *Defender for Identity*.
e) Supervisar las actividades sospechosas detectadas y los ataques sospechosos basados en el modelo de cadena de interrupción de ataque.
f) Opcional: el portal también puede configurarse para que envíe correos electrónicos y eventos cuando se detecten problemas de mantenimiento o alertas de seguridad.

Nota: Si no hay ningún sensor instalado en la instancia de Defender for Identity al cabo de 60 días, se podría eliminar y habría que volver a crearla.

1.5.2 SENSOR DE DEFENDER FOR IDENTITY

La funcionalidades principales del sensor de *Defender for Identity* son:

a) Capturar e inspeccionar el tráfico de red del controlador de dominio (tráfico local del controlador de dominio).
b) Recibir eventos de Windows directamente desde los controladores de dominio.
c) Recibir información de cuentas de Radius del proveedor de VPN.
d) Recuperar datos sobre usuarios y equipos del dominio de Active Directory.
e) Llevar a cabo tareas de resolución de entidades de red (usuarios, grupos y equipos).
f) Transferir datos de interés al servicio en la nube de *Defender for Identity*.

Características de los sensores de Defender for Identity

El sensor de *Defender for Identity* lee los eventos localmente, sin necesidad de adquirir y mantener ningún hardware o configuración adicional. También admite *Seguimiento*

de eventos para Windows (ETW), que proporciona información de registro de varias detecciones. Las detecciones basadas en ETW incluyen las sospechas de ataques *DC Shadow* que se hayan intentado realizar mediante solicitudes de replicación del controlador de dominio y la promoción de este.

- *Proceso del sincronizador de dominio*

El proceso del sincronizador de dominio es responsable de sincronizar todas las entidades de un dominio de Active Directory específico de forma proactiva (similar al mecanismo que usan los propios controladores de dominio para la replicación). Un sensor se selecciona de forma automática de entre todos los sensores aptos para que actúe como sincronizador de dominio.

Si el sincronizador del dominio está sin conexión durante más de 30 minutos, se seleccionará otro automáticamente.

- *Limitaciones de recursos*

El sensor de *Defender for Identity* incluye un componente de supervisión que evalúa la capacidad de proceso y memoria disponibles en el controlador de dominio en el que se está ejecutando. El proceso de supervisión se ejecuta cada 10 segundos y actualiza dinámicamente la cuota de uso de CPU y memoria en él. El proceso de supervisión se asegura de que el controlador de dominio siempre tiene al menos el 15% de recursos de proceso y memoria disponibles.

Independientemente de lo que ocurra en el controlador de dominio, el proceso de supervisión libera continuamente recursos para asegurarse de que la función principal del controlador de dominio no se vea nunca afectada.

Si el proceso de supervisión hace que el sensor de *Defender for Identity* se quede sin recursos, se supervisa únicamente el tráfico parcial y, en la página de estado del portal de *Defender for Identity*, aparecerá una alerta de estado para indicar esta circunstancia.

- *Eventos de Windows*

Para mejorar la cobertura de detección de *Defender for Identity* relativa a las autenticaciones NTLM, las modificaciones de grupos confidenciales y la creación de servicios sospechosos, *Defender for Identity* necesita analizar los registros de ciertos eventos de Windows.

Para obtener más información sobre los registros de eventos y la configuración de la directiva de auditoría correcta, consultar el siguiente enlace:

https://learn.microsoft.com/es-es/defender-for-identity/deploy/configure-windows-event-collection#relevant-windows-events

1.6 ANALISIS DE CAPACIDAD MICROSOFT DEFENDER FOR IDENTITY

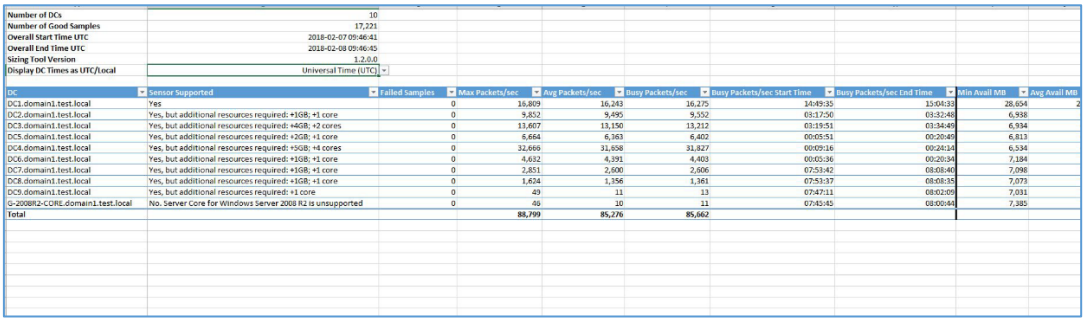
La manera recomendada y más sencilla de determinar la capacidad del despliegue de *Defender for Identity* es usar la herramienta de *Defender for Identity Sizing Tool*. Otra opción sería recopilar la información de tráfico manualmente.

La herramienta puede descargarse del siguiente enlace: https://aka.ms/aatpsizingtool

A continuación se describe el proceso de utilización de la herramienta:

1. Ejecutar la herramienta de tamaño, **TriSizingTool.exe**, desde el archivo ZIP descargado.

2. Al finalizar la ejecución abrir los resultados del archivo de Excel.
3. En el archivo de Excel, buscar y seleccionar la **hoja Resumen de Azure ATP.**



Number of DCs	10
Number of Good Samples	17,221
Overall Start Time UTC	2018-02-07 09:46:41
Overall End Time UTC	2018-02-08 09:46:43
Sizing Tool Version	1.2.0.0
Display DC Times as UTC/Local	Universal Time (UTC)

DC	Sensor Supported	Failed Samples	Max Packets/sec	Avg Packets/sec	Busy Packets/sec	Busy Packets/sec Start Time	Busy Packets/sec End Time	Min Avail MB	Avg Avail MB
DC1.domain1.test.local	Yes	0	16,809	16,243	16,275	14:49:32	15:04:31	28,694	2
DC2.domain1.test.local	Yes, but additional resources required: +1GB; +1 core	0	9,852	9,495	9,552	03:17:50	03:32:48	6,938	
DC3.domain1.test.local	Yes, but additional resources required: +4GB; +2 cores	0	13,607	13,150	13,212	03:19:51	03:34:49	6,934	
DC5.domain1.test.local	Yes, but additional resources required: +2GB; +1 core	0	6,664	6,363	6,402	00:05:51	00:20:49	6,813	
DC4.domain1.test.local	Yes, but additional resources required: +5GB; +4 cores	0	32,666	31,658	31,827	00:09:16	00:24:14	6,534	
DC6.domain1.test.local	Yes, but additional resources required: +1GB; +1 core	0	4,632	4,391	4,403	00:05:36	00:20:34	7,184	
DC7.domain1.test.local	Yes, but additional resources required: +1GB; +1 core	0	2,851	2,600	2,606	07:53:42	08:08:40	7,098	
DC8.domain1.test.local	Yes, but additional resources required: +1GB; +1 core	0	1,624	1,356	1,361	07:53:37	08:08:35	7,073	
DC9.domain1.test.local	Yes, but additional resources required: +1 core	0	49	11	13	07:47:11	08:02:09	7,031	
G-2008R2-CORE.domain1.test.local	No. Server Core for Windows Server 2008 R2 is unsupported	0	49	10	11	07:45:45	08:00:44	7,385	
Total			88,799	85,276	85,662				

4. Buscar el campo **Busy Packets/sec** (Paquetes ocupados por segundo) en la tabla de sensores de Azure ATP en el archivo de resultados de Excel y anotarlo.
5. Hacer coincidir **el campo Busy Packets/sec** (Paquetes ocupados/s) con **el campo *packets per second* (paquetes por segundo)** de la tabla de sensores. Usar los campos para determinar la memoria y la CPU que usará el sensor.

Paquetes por segundo	CPU (núcleos)*	Memoria** (GB)
0-1k	0,25	2,50
1k-5k	0,75	6,00
5k-10k	1,00	6,50
10k-20k	2,00	9,00
20k-50k	3,50	9,50
50k-75k	3,50	9,50
75k-100k	3,50	9,50

* Esto incluye los núcleos físicos, no los núcleos con Hyper-Threading.

* Memoria de acceso aleatorio (RAM)

Más información en la página de Microsoft:

https://learn.microsoft.com/es-es/defender-for-identity/deploy/capacity-planning

1.7 PRERREQUISITOS MICROSOFT DEFENDER FOR IDENTITY

Para crear la instancia de *Defender for Identity*, se necesita un ***Tenant*** **de Microsoft Entra ID** con al menos un administrador global o de seguridad.

Cada instancia de *Defender for Identity* admite un límite de bosque de Active Directory múltiple y un nivel funcional de bosque (FFL) de Windows 2003 y versiones posteriores.

A continuación se dividirán los prerrequisitos en secciones para facilitar su identificación.

1.7.1 LICENCIAS, CUENTAS Y ENTIDADES DE RED

En esta sección se muestra la información que debe reunirse, así como las cuentas y la información de las entidades de red que deben existir antes de comenzar el despliegue de Defender for Identity.

Licenciamiento

La implementación de Defender for Identity requiere una de las siguientes licencias de Microsoft 365:

- Enterprise Mobility + Security E5 (EMS E5/A5)
- Microsoft 365 E5 (Microsoft E5/A5/G5)
- Seguridad de Microsoft 365 E5/A5/G5/F5*
- Seguridad y cumplimiento de Microsoft 365 F5*
- Licencias de Defender for Identity independientes

* Ambas licencias de F5 requieren Microsoft 365 F1/F3 u Office 365 F3 y Enterprise Mobility + Security E3.

Mas información sobre licencias se puede encontrar en este enlace: https://learn.microsoft.com/es-es/defender-for-identity/technical-faq#licencia-y-privacidad

Permisos:

Para crear el área de trabajo de Defender for Identity se necesita una cuenta empresarial de Microsoft Entra ID con al menos un administrador de seguridad.

Se necesita al menos acceso de Administrador de seguridad en su cuenta empresarial para acceder a la sección Identidad del área de Configuraciones de Microsoft Defender XDR y crear el área de trabajo.

Para más información, consulte el siguiente enlace:
https://learn.microsoft.com/es-es/defender-for-identity/role-groups

Se recomienda utilizar al menos una cuenta de Servicio de directorio con acceso de lectura a todos los objetos de los dominios supervisados. Para obtener más información:
https://learn.microsoft.com/es-es/defender-for-identity/deploy/directory-service-accounts

Conectividad de red:

El sensor de Defender for Identity debe poder comunicarse con el servicio en la nube de Defender for Identity mediante uno de los métodos siguientes:

- **Configurar un proxy**: Si se dispone de un proxy de reenvío, se puede aprovechar el proxy para proporcionar conectividad al servicio en la nube MDI.
- **ExpressRoute**: ExpressRoute se puede configurar para reenviar el tráfico del sensor MDI a través de la ruta rápida del cliente.
- **Servidor de seguridad, mediante las direcciones IP de Azure de Defender for Identity: Si no se dispone de** un proxy o ExpressRoute, una opción es configurar **el** firewall con las direcciones IP que el servicio en la nube MDI tiene asignadas. Esto implica que **se** debe estar atento a la lista de direcciones IP de Azure para detectar posibles cambios en las direcciones IP que el servicio en la nube MDI utiliza.

1.7.2 ACCESO DEL PORTAL DE DEFENDER FOR IDENTITY

El acceso al portal de *Defender for Identity* se efectúa a través de un explorador Web. Se admiten los siguientes exploradores y configuraciones:

- Un explorador que admita TLS 1.2, como:
  - Microsoft Edge
  - Google Chrome 30.0 y versiones posteriores

- Firewall/proxy abierto: para comunicarse con el servicio en la nube de *Defender for Identity*, el puerto 443 (SSL) debe estar abierto en el firewall o proxy.

1.7.3 RESOLUCIÓN DE NOMBRES DE RED (NNR) DE DEFENDER FOR IDENTITY

La resolución de nombres de red (NNR) es una funcionalidad clave de Microsoft Defender for Identity que permite correlacionar actividades sin procesar (que

contienen direcciones IP) con los equipos relevantes involucrados en cada actividad. Esta correlación ayuda a generar alertas de seguridad para actividades sospechosas.

Para resolver las direcciones IP a nombres de equipo, Defender for Identity utiliza varios métodos, principalmente NTLM a través de RPC, NetBIOS y RDP, consultando de forma secundaria al servidor DNS. Se recomienda usar al menos uno de los métodos principales para obtener mejores resultados. La búsqueda inversa de DNS se realiza solo cuando no hay respuesta de los métodos principales o hay un conflicto en las respuestas recibidas.

Mas información en el siguiente enlace: https://learn.microsoft.com/es-es/defender-for-identity/nnr-policy

1.7.4 SENSORES DE DEFENDER FOR IDENTITY

En esta sección se enumeran los requisitos del sensor de *Defender for Identity*. El sensor de *Defender for Identity* permite su instalación en controladores de dominio, en servidores de *Servicios de Federación de Active Directory* (AD FS) y en *Servicios de Certificados de Active Directory* (AD CS) , tal como se muestra en la tabla siguiente:

Versión del sistema operativo	Servidor con experiencia de escritorio	Server Core	Nano Server	Instalaciones compatibles
Windows Server 2016	✔	✔	✘	Controlador de dominio, AD FS y AD CS
Windows Server 2019*	✔	✔	✘	Controlador de dominio, AD FS y AD CS
Windows Server 2022	✔	✔	✘	Controlador de dominio, AD FS y AD CS

* Requiere KB4487044 o una actualización acumulativa más reciente.

Para disfrutar del mejor rendimiento posible, establecer la opción de energía de la máquina en la que se ejecuta el sensor de Defender for Identity en Alto rendimiento.

Se recomienda programar una ventana de mantenimiento para los controladores de dominio, ya que es posible que se requiera un reinicio si la instalación se ejecuta y ya hay un reinicio pendiente, o si es necesario instalar .NET Framework.

Si la versión 4.7 o posterior de .NET Framework aún no se encuentra en el sistema, se instala .NET Framework versión 4.7 y puede ser necesario reiniciar los equipos.

Se requiere un mínimo de **6 GB de espacio en disco**, pero se recomienda disponer de 10 GB, teniendo en cuenta el espacio para los archivos binarios y registros de Defender for Identity.

1.7.5 ESPECIFICACIONES DEL SERVIDOR

El sensor de *Defender for Identity* necesita tener instalados **2 núcleos y 6 GB de RAM y 6 GB de espacio en disco** (la recomendación es 10 GB) como mínimo en el controlador de dominio. Para disfrutar del mejor rendimiento posible, establecer la opción de energía de la máquina en la que se ejecuta el sensor de *Defender for Identity* en Alto rendimiento.

Cuando se ejecuta como una máquina virtual, es necesario asignar toda la memoria a la VM en todo momento.

Mas información disponible en https://learn.microsoft.com/es-es/defender-for-identity/deploy/capacity-planning

1.7.6 SINCRONIZACIÓN DE HORA

Los servidores y controladores de dominio en los que está instalado el sensor deben estar sincronizados a intervalos de cinco minutos entre sí.

1.7.7 PUERTOS

En la tabla siguiente se enumeran los puertos necesarios para el funcionamiento del sensor de *Defender for Identity*:

Protocolo	Transporte	Puerto	Desde	Hacia
Puertos de Internet				
SSL (*.atp.azure.com) Como alternativa configurar el acceso a través de un proxy.	TCP	443	Sensor de Defender for Identity	Servicio en la nube de Defender For Identity
Puertos internos				
DNS	TCP y UDP	53	Sensor de Defender for Identity	Servidores DNS
Netlogon (SMB, CIFS, SAM-R)	TCP/UDP	445	Sensor de Defender for Identity	Todos los dispositivos en la red

Protocolo	Transporte	Puerto	Desde	Hacia
RADIUS	UDP	1813	RADIUS	Sensor de Defender for Identity
Puertos localhost: necesario para el actualizador del servicio de sensor. De manera predeterminada, se permite el tráfico de localhost a localhost a menos que una directiva de servidor de seguridad lo bloquee.				
SSL	TCP	444	Servicio de sensores	Servicio del actualizador de sensores
Puertos de resolución de nombres de red (NNR) Para resolver las direcciones IP en los nombres de equipo, se recomienda abrir todos los puertos enumerados. Sin embargo, solo se requiere un puerto.				
NTLM sobre RPC	TCP	Puerto 135	Sensor de Defender for Identity	Todos los dispositivos en la red
NetBIOS	UDP	137	Sensor de Defender for Identity	Todos los dispositivos en la red
RDP Solo el primer paquete de bienvenida al Cliente consulta el servidor DNS mediante la búsqueda inversa de DNS de la dirección IP (UDP 53)	TCP	3389	Sensor de Defender for Identity	Todos los dispositivos en la red

Si se dispone de varios bosques, deberán asegurarse de abrir los siguientes puertos en cualquier máquina en la que se instale un sensor de Defender for Identity.

Protocolo	Transporte	Puerto	Desde/hacia	Dirección
Puertos de Internet				
SSL (*.atp.azure.com)	TCP	443	Servicio en la nube de Defender for Identity	Salida
Puertos internos				
LDAP	TCP y UDP	389	Controladores de dominios	Salida
LDAP Seguro (LDAPS)	TCP/UDP	636	Controladores de dominios	Salida
LDAP al Catálogo global	UDP	3268	Controladores de dominios	Salida
LDAPS al Catálogo global		3269	Controladores de dominios	Salida

1.7.8 REQUISITOS DE MEMORIA DINÁMICA

La memoria que necesita el servidor para el sensor de Defender for Identity depende del tipo de virtualización que use. En la tabla siguiente se muestran los requisitos de memoria según el tipo de virtualización

VM en ejecución en	Descripción
Hyper-V	Asegurar que no esté habilitada la función **Habilitar memoria dinámica** para la máquina virtual.
VMware	Asegurar que la cantidad de memoria configurada y la memoria reservada sean iguales o seleccionar la opción Reservar toda la memoria invitada (Todas bloqueadas) en la configuración de la máquina virtual.
Otros host de virtualización	Consultar la documentación proporcionada por el proveedor sobre cómo asegurarse de que la memoria está totalmente asignada a la máquina virtual en todo momento.

1.8 PORTAL UNIFICADO DE SEGURIDAD MICROSOFT DEFENDER XDR

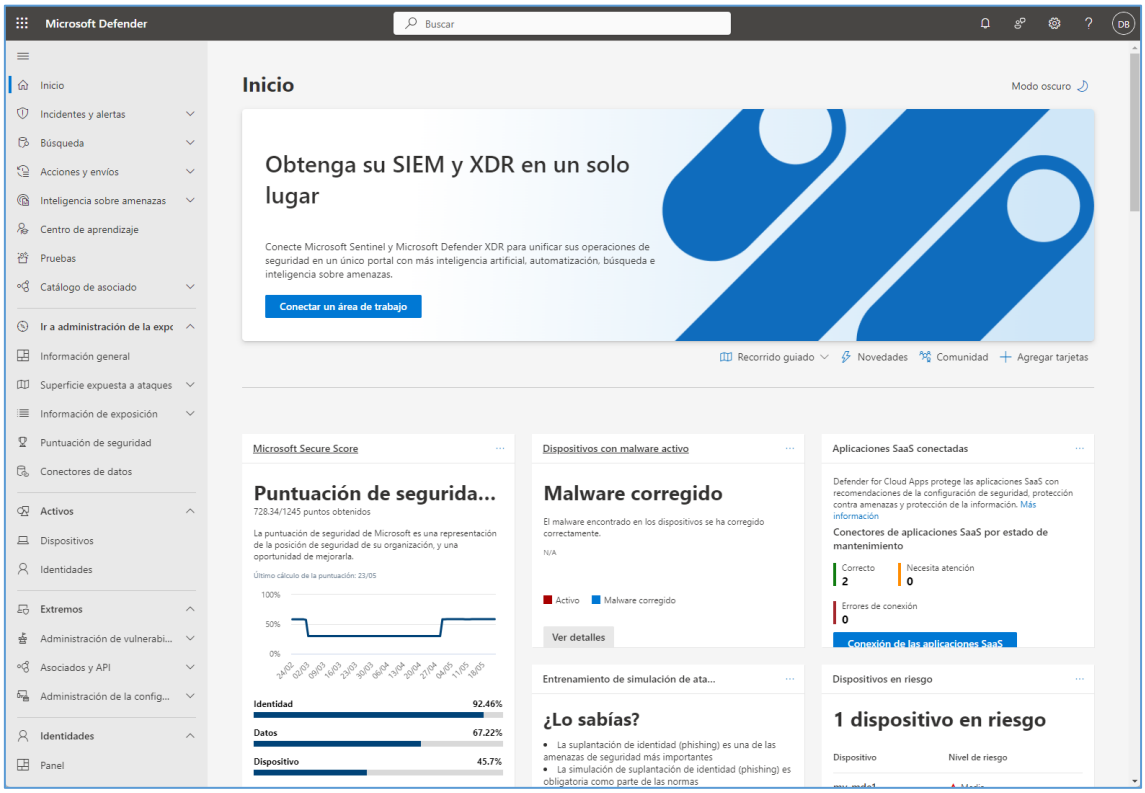
1.8.1 ACCESO AL PORTAL

Microsoft Defender for Identity es ahora parte del portal de Microsoft Defender, la plataforma para gestionar y monitorizar la seguridad en las identidades, los datos, los dispositivos, las aplicaciones y la infraestructura de Microsoft. El portal de Microsoft Defender facilita las tareas de seguridad a los administradores al ofrecerles una

ubicación única, lo que agiliza los flujos de trabajo e integra las funciones de otros servicios de Microsoft Defender XDR.

Microsoft Defender for Identity ofrece información enfocada en la identidad en los incidentes y alertas que muestra el portal de Microsoft Defender. Esta información es fundamental para dar contexto y relacionar alertas de los otros productos dentro de Microsoft Defender XDR.

El acceso al portal se realiza desde la siguiente URL: https://security.microsoft.com



1.8.2 FUNCNIOANLIDADES DEL PORTAL

El portal https://security.microsoft.com de Microsoft Defender XDR combina protección, detección, investigación y respuesta a amenazas en toda la organización y todos sus componentes, en un lugar central. El portal hace hincapié en el acceso rápido a la información, diseños más sencillos y reunir información relacionada para facilitar su uso. Incluye:

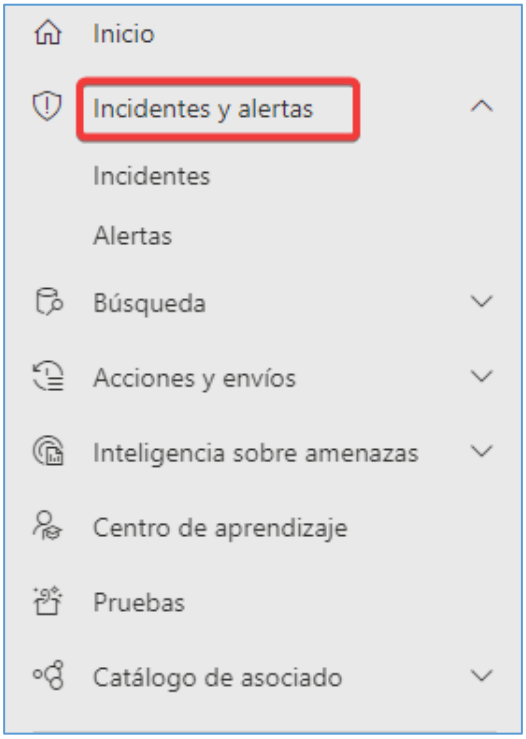
- Microsoft Defender para Office 365.
- Microsoft Defender para punto de conexión.
- Microsoft Defender for Identity.
- Microsoft Defender for Cloud Apps.
- Microsoft Sentinel.

El nuevo portal de *Microsoft Defender XDR*, reúne las funcionalidades que solían estar en portales independientes en un solo lugar, de modo que pueda protegerse de una manera más sencilla y centralizada de cualquier tipo de amenaza.

Desde un punto de vista genérico, en este portal puede realizarse distintas acciones relacionadas con la defensa empresarial (detección, prevención, investigación y respuesta entre *endpoints*, identidades, correo electrónico, workloads y aplicaciones) e integrase con Microsoft Sentinel.

1.8.2.1 INVESTIGAR INCIDENTES Y RESPONDER A AMENANZAS

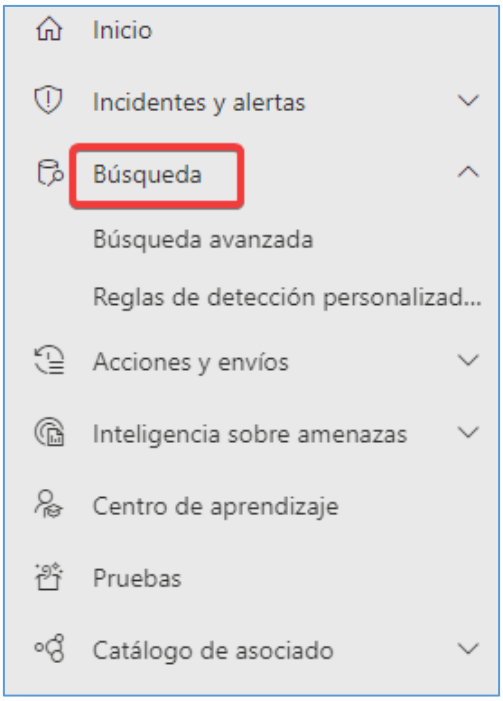
Las alertas están categorizadas, combinadas y correlacionadas en incidentes completos.



- **Incidentes:** Muestra una lista de incidentes de seguridad, con opciones para investigar, clasificar y resolver cada incidente.
- **Alertas**: Proporciona una lista detallada de alertas individuales. Se visualiza la fuente de la alerta, la descripción y tomar acciones como la investigación adicional o la resolución.

1.8.2.2 BUSCAR AMENAZAS DE MANERA PROACTIVA

Las alertas están categorizadas, combinadas y correlacionadas en incidentes completos.



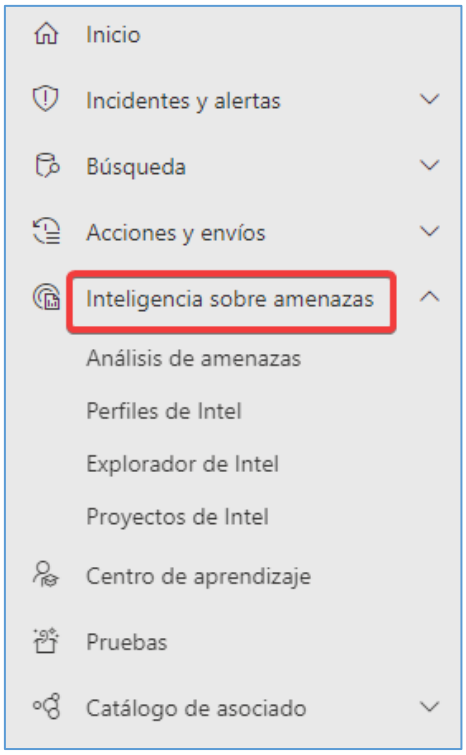
- **Búsqueda avanzada:** herramienta que permite crear consultas personalizadas utilizando un lenguaje de consulta avanzado para buscar indicadores de compromiso (IOC) y actividades sospechosas en los datos recopilados por la plataforma.

1.8.2.3 REALIZAR SEGUIMIENTO Y RESPONDER A LAS AMENAZAR EMERGENTE

Microsoft Defender Threat Intelligence (Defender TI) permite acceder a la información sobre amenazas desde el portal de Microsoft Defender.

Microsoft Defender TI ayuda a agilizar el triaje de los analistas de seguridad, la respuesta a incidentes, la caza de amenazas y los flujos de trabajo de gestión de vulnerabilidades. Defender TI agrega y enriquece la información crítica sobre amenazas en una interfaz fácil de usar.

Este cambio introduce un nuevo menú de navegación dentro del portal de Microsoft Defender denominado Inteligencia de amenazas.

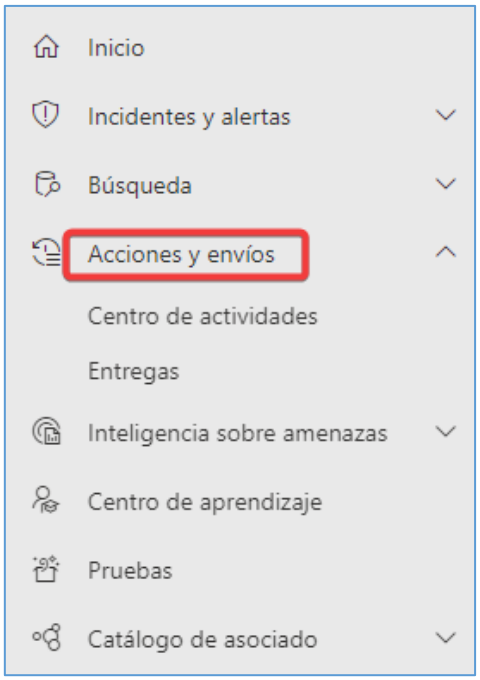


En el menú de Inteligencia de amenazas existe la función **Análisis de amenazas** que está diseñado para ayudar a los equipos de seguridad a ser más eficientes y dos nuevas funcionalidades:

- **Perfiles de Intel:** una nueva característica que facilita información sobre contenido de actores de amenazas, sus herramientas y vulnerabilidades conocidas.
- **Explorador de Intel**: proporciona la experiencia existente de búsqueda e investigación de contenidos de TI de Defender.

1.8.2.4 SUPERVISAR LAS ACCIONES Y EL ESTADO DE LA INVESTIGACIÓN

Está enfocado en la gestión de acciones de seguridad y la administración de archivos o elementos sospechosos que han sido enviados para su análisis. Aquí se describen las principales funciones y submenús que típicamente se encuentran en esta sección:



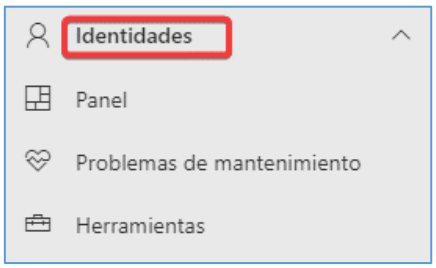
- **Acciones:** esta sección se encarga de gestionar las acciones recomendadas y las tareas de respuesta a incidentes de seguridad. Incluye:
  - **Pendiente:** muestra una lista de todas las acciones de seguridad recomendadas que aún no se han completado. Estas acciones pueden incluir tareas como aislar un dispositivo, ejecutar un análisis completo, aplicar parches de seguridad, o eliminar software malicioso. Cada acción pendiente suele incluir detalles como el tipo de amenaza, el dispositivo afectado, y la urgencia de la acción recomendada.
  - **Historial**: registra todas las acciones que han sido llevadas a cabo en respuesta a alertas o recomendaciones. Esto permite a los administradores de seguridad revisar qué medidas se han tomado y verificar que las respuestas adecuadas se han implementado correctamente.

- **Entregas:** permite a los usuarios enviar archivos sospechosos o URLs para un análisis más profundo por parte de Microsoft. Esta función es crucial para gestionar posibles falsos positivos y obtener una comprensión más clara de las amenazas detectadas.
  - **File (Envío de Archivos):** los usuarios envían archivos sospechosos directamente a Microsoft para su análisis detallado. Esto puede ser útil cuando hay dudas sobre si un archivo es realmente malicioso o no. Microsoft proporciona un análisis detallado y una respuesta sobre la naturaleza del archivo enviado.
  - **Direcciones URL:** similar a los envíos de archivos, esta función permite enviar URLs sospechosas para su análisis. Esto ayuda a identificar si una URL conduce a un sitio web malicioso o a un posible ataque de phishing.

- **Submission History (Historial de Envíos):** proporciona un registro de todos los archivos y URLs que se han enviado para análisis, junto con el estado y los resultados de esos análisis. Esto ayuda a los equipos de seguridad a mantener un seguimiento de lo que se ha revisado y las conclusiones obtenidas.

1.8.2.5 DEFENDER FOR IDENTITY

Ofrece herramientas y recursos para gestionar las identidades y seguridad de estas. Es la sección principal del menú y agrupa las siguientes opciones relacionadas con la gestión de identidades y seguridad.



- **Panel**: vista general o dashboard donde se presenta un resumen del estado actual de las identidades monitoreadas, incluidas métricas clave, alertas recientes y otra información relevante. Se muestran los datos para ayudar a analizar mejor la posición de seguridad de nuestra organización, comprender el nivel de protección, identificar las vulnerabilidades y realizar acciones recomendadas. Ofrece la posibilidad de ver información crítica y datos en tiempo real sobre la detección y respuesta de amenazas de identidad (ITDR). Se pueden ver gráficos y widgets que muestran información importante relacionada con accesos no autorizados, riesgo de cuentas, amenazas internas y actividades anómalas. También permite, supervisar y administrar de forma los posibles riesgos de seguridad relacionados con la identidad.
- **Problemas de mantenimiento**: se enumeran los problemas de mantenimiento existentes en dos secciones diferenciadas: en la implementación global de Defender for Identity, y en los sensores de Defender for Identity. El propósito de esta sección es informar de los problemas que puedan surgir en la implementación de Defender for Identity.
- **Herramientas**: Recursos adicionales para ayudar a administrar la seguridad y el cumplimiento en toda la organización de Microsoft Defender for Identity.

2. DESPLIEGUE DE MICROSOFT DEFENDER FOR IDENTITY

El procedimiento de despliegue de *Microsoft Defender for Identity* incluye los siguientes pasos:

- **Preparar el dominio** local para Microsoft Defender para la operación de identidad.
- **Instalar sensores** para controladores de dominio.
- **Configurar** Microsoft *Defender for Identity*.
- **Solucionar** problemas y probar.

2.1 PLANIFICACIÓN

Se recomienda implementar *Defender for Identity* en dos fases:

- **Configuración y prueba de la conectividad con Defender for Identity**
  - Configuración y de opciones
  - Prueba de la configuración
- **Configuración de sensor de Defender for Identity**
  - Descarga
  - Instalación
  - Configuración

2.2 DESPLIEGUE PASO A PASO

Una vez comprobados todos los requerimientos descritos en la sección [1.7 Prerrequisitos Microsoft Defender for Identity], el paso fundamental es configurar y verificar que nuestra conectividad con el servicio de Defender for Identity

En los siguientes subapartados se describe el despliegue paso a paso.

2.2.1 CREACIÓN DE LA INSTANCIA DE DEFENDER FOR IDENTITY

1. Acceder al portal de Microsoft Defender a través de la siguiente URL https://security.microsoft.com e introducir las credenciales de usuario con privilegios.
2. En el menú de navegación, seleccionar cualquier elemento, como **Incidentes y alertas, Búsqueda, Centro de actividades o Análisis de amenazas** para iniciar el proceso de incorporación.

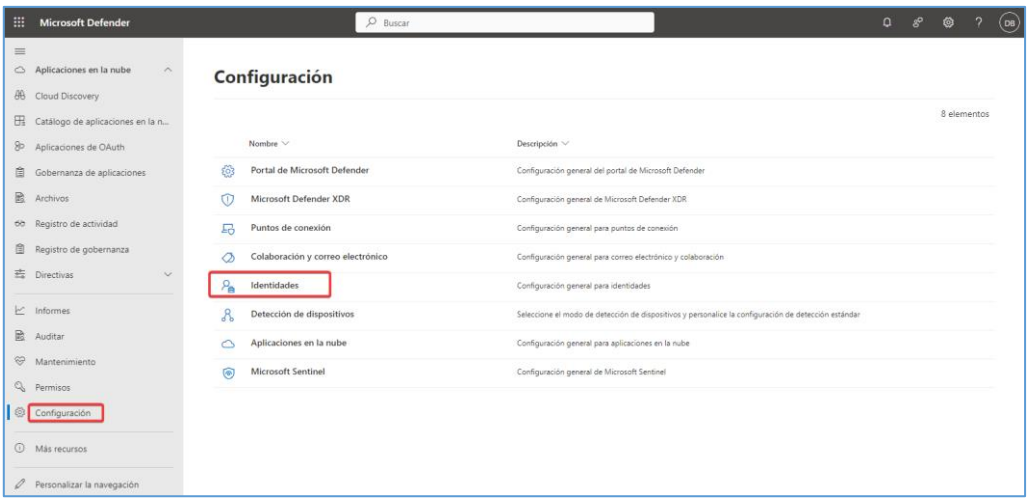
A continuación, se dará la opción de implementar los servicios admitidos, incluido Microsoft Defender for Identity. Los componentes en la nube necesarios para Defender for Identity se agregan automáticamente al abrir la página de configuración de Defender for Identity.

2.2.2 CONEXIÓN A ACTIVE DIRECTORY

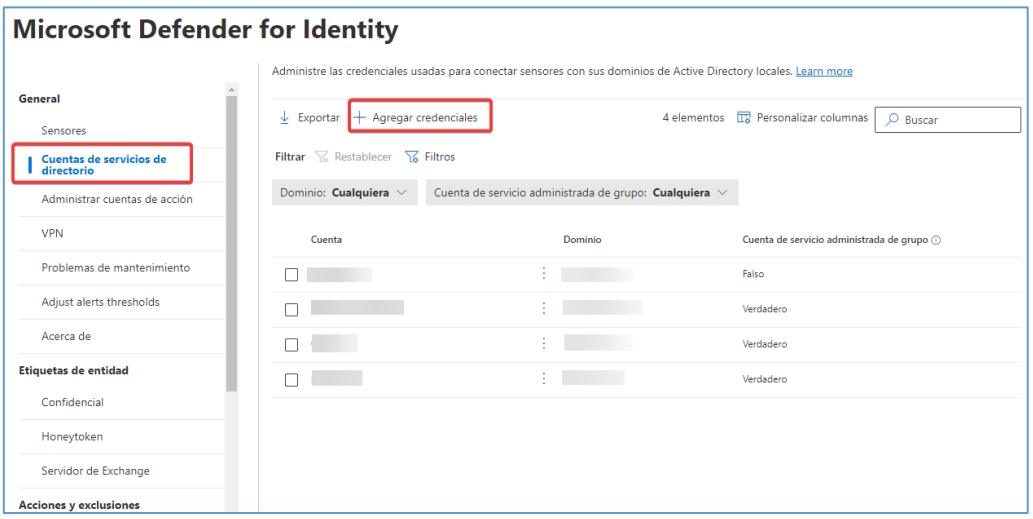
Se conectará *Microsoft Defender for Identity* a Active Directory (AD) para recuperar datos sobre usuarios y equipos.

Lo primero que debe hacerse es proporcionar un nombre de usuario y una contraseña para conectarse al bosque de Active Directory.

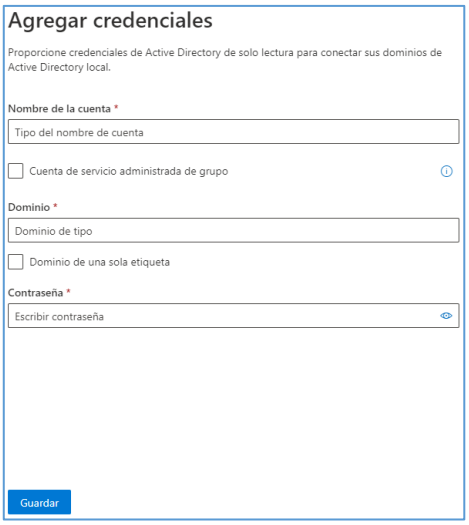
1. Pulsar sobre “Configuración” en el menú lateral y pulsar “Identidades”.



2. Seleccionar “Cuentas de servicios de directorio” y pulsar sobre el botón “+ Agregar credenciales”:



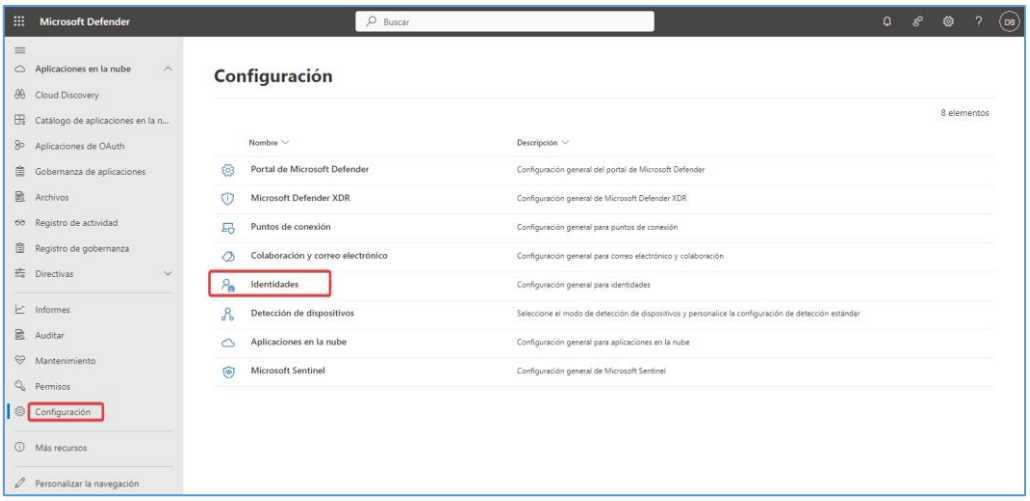
3. Escribir la información siguiente y hacer pulsar sobre el botón “Guardar”:



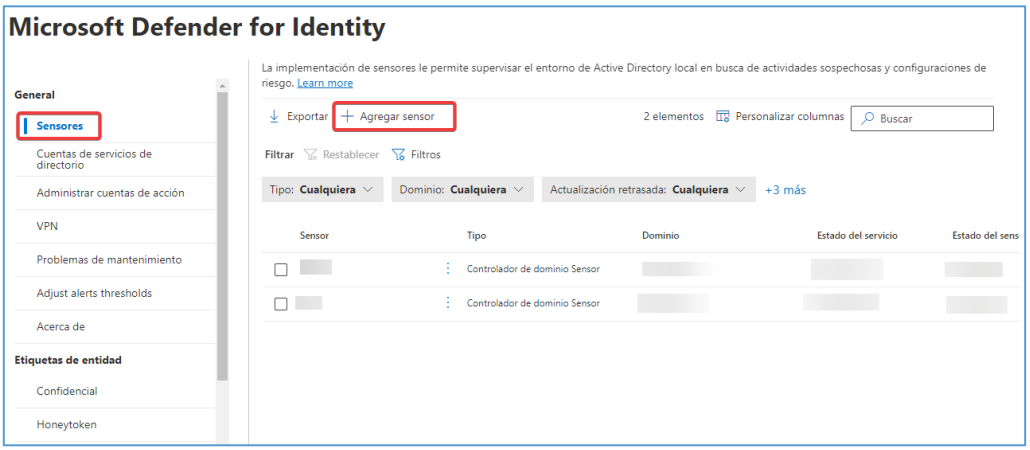
Campo	Comentarios
Nombre de la cuenta (obligatorio)	Escribir el nombre de usuario de AD de solo lectura. Por ejemplo: ***DefenderForIdentityUser***. Se debe usar una cuenta de usuario **estándar** de AD o gMSA. **No** usar el formato UPN para el nombre de usuario. **NOTA:** Se recomienda evitar el uso de cuentas asignadas a usuarios específicos.
Cuenta de servicio administrada de grupo (obligatorio para la cuenta de gMSA)	Solo para la cuenta de gMSA, seleccionar la **cuenta de servicio administrada de grupo**.
Dominio (obligatorio)	Escribir el dominio del usuario de solo lectura. Por ejemplo: **contoso.com**. Es importante escribir el FQDN completo del dominio donde se encuentra el usuario. Por ejemplo, si la cuenta de usuario está en el dominio corp.contoso.com, escribir corp.contoso.com, no contoso.com.
Contraseña (necesaria para la cuenta de usuario de AD estándar)	Solo para la cuenta de usuario de AD, escribir la contraseña del usuario de solo lectura.

2.2.3 DESCARGAR SOFTWARE DEL SENSOR

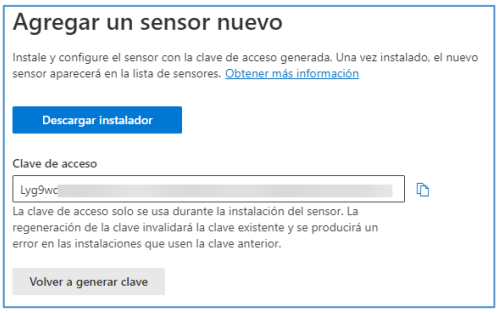
1. Pulsar sobre “Configuración” en el menú lateral y pulsar “Identidades”.



2. Seleccionar “Sensores” y pulsar sobre el botón “+ Agregar sensor”:



3. Pulsar sobre el botón “Descargar instalador” y copiar la clave de acceso necesaria en el proceso de instalación del sensor en el Controlador de Dominio.

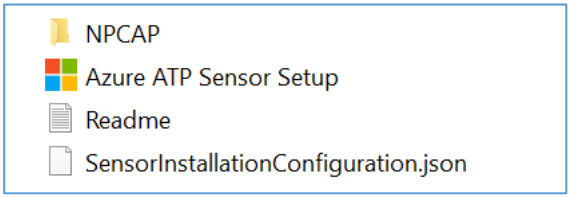


Nota: Solo es necesario descargar el instalador una vez, ya que se puede usar para todos los Controladores de Dominio.

2.2.4 INSTALAR SOFTWARE DEL SENSOR

Para la instalación del software del sensor, seguir los pasos siguientes en el controlador de dominio o en el servidor de AD FS / AD CS.

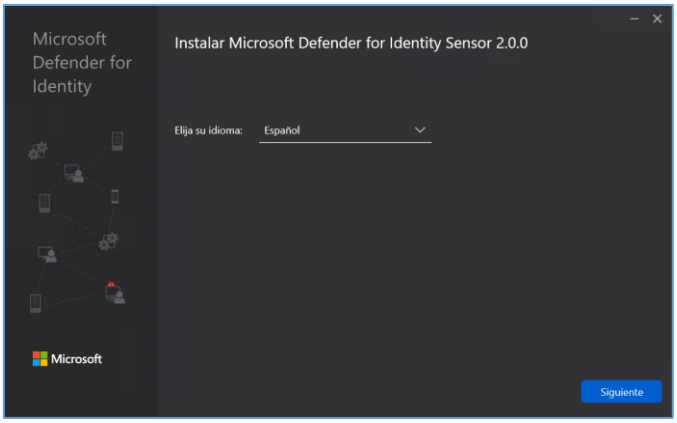
1. Extraer los archivos de instalación del archivo ZIP.



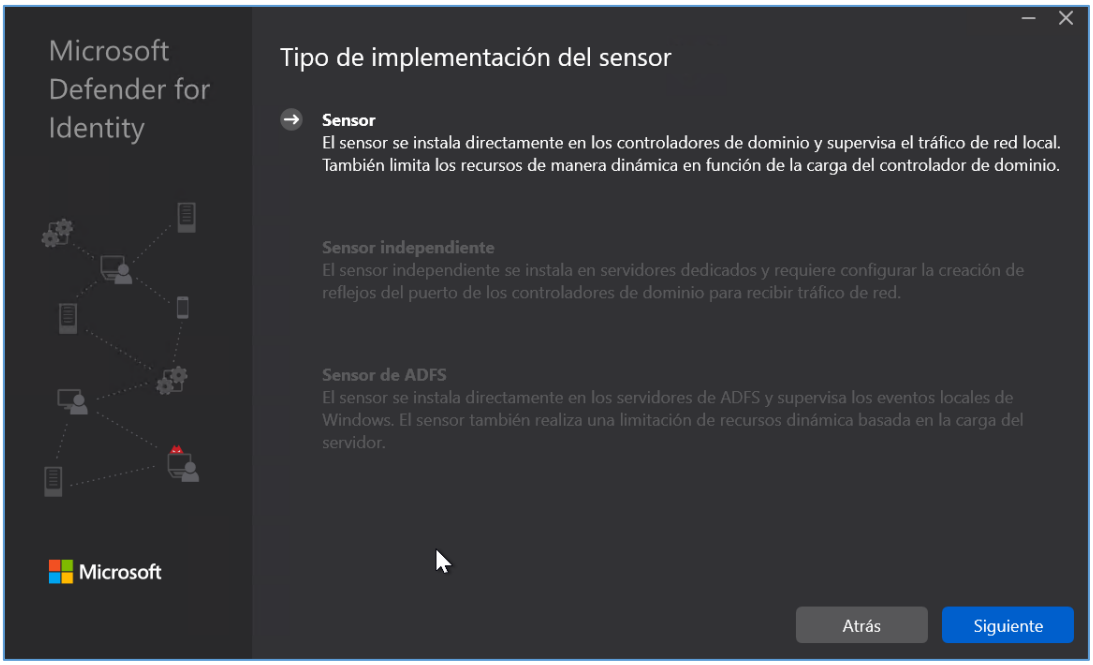
Nota: Se producirá un error si se intenta instalar directamente desde el archivo zip.

2. Ejecutar *Azure ATP sensor setup.exe* con privilegios elevados (como administrador) y seguir el Asistente para la instalación.

3. Seleccionar idioma y pulsar *Siguiente*:

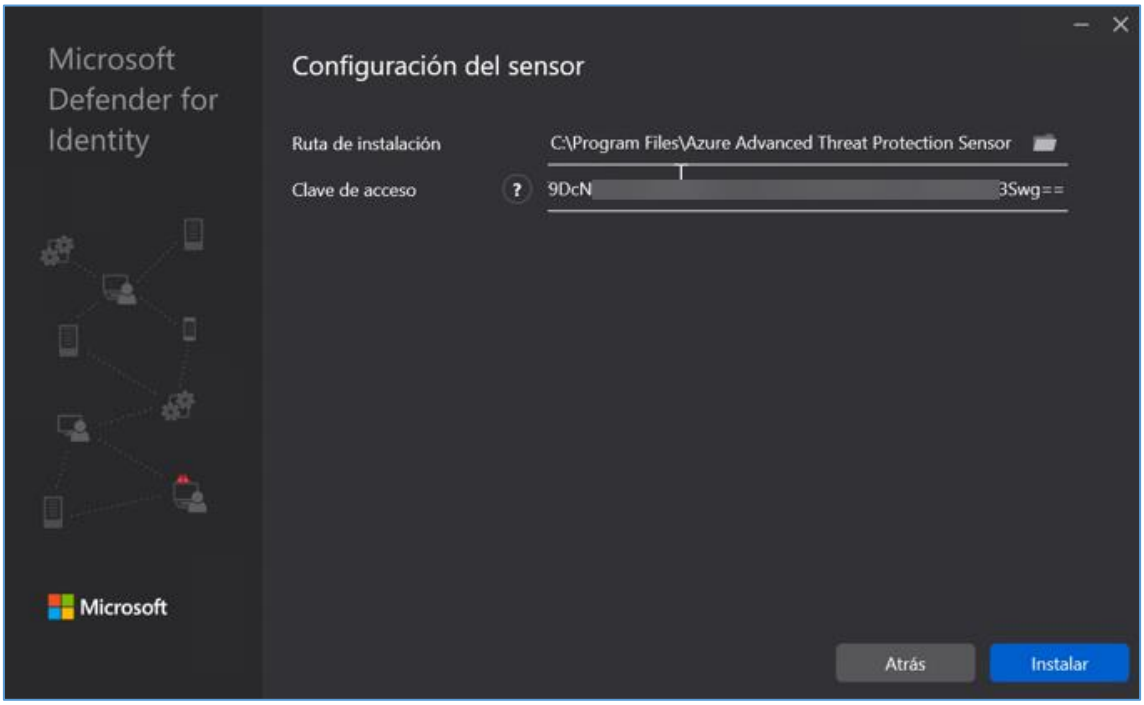


4. El Asistente para la instalación comprobará automáticamente si el servidor es un controlador de dominio / servidor AD FS o un servidor dedicado. Si es un controlador de dominio / servidor AD FS, se instala el *sensor de Defender for Identity*. Si es un servidor dedicado, se instala el *sensor independiente de Defender for Identity*.



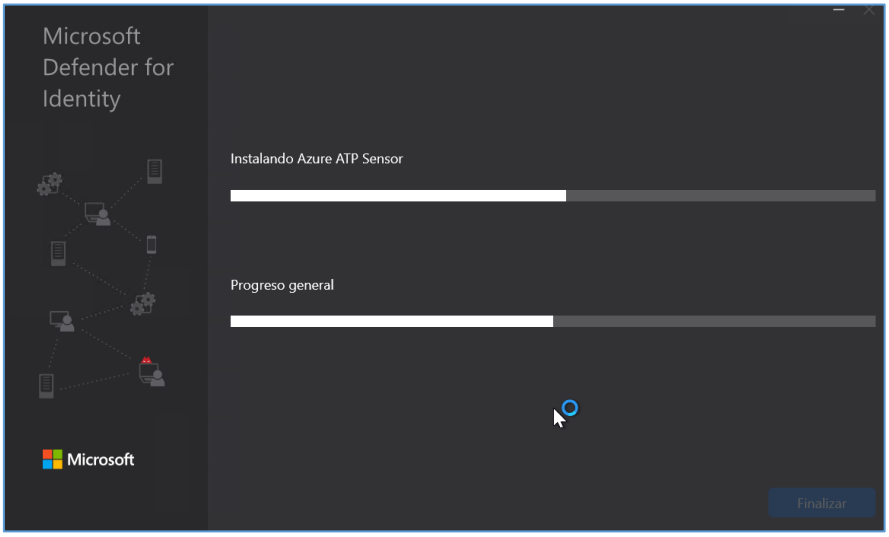
Nota: Si el controlador de dominio / servidor AD FS o un servidor dedicado no cumple los requisitos mínimos de hardware para la instalación, se generará una advertencia.

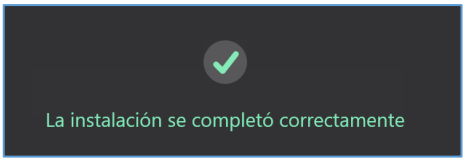
5. En Configuración del sensor, escribir la ruta de instalación y la clave de acceso que se copió en el proceso de descarga del sensor desde el portal:



- Ruta de instalación: ubicación donde se instala el sensor de *Defender for Identity*. La ruta predeterminada es *%programfiles%\Azure Advanced Threat Protection Sensor*. Dejar el valor predeterminado.
- Clave de acceso: recuperada del portal de *Defender for Identity* en el paso anterior.

6. Seleccionar ***Instalar***.





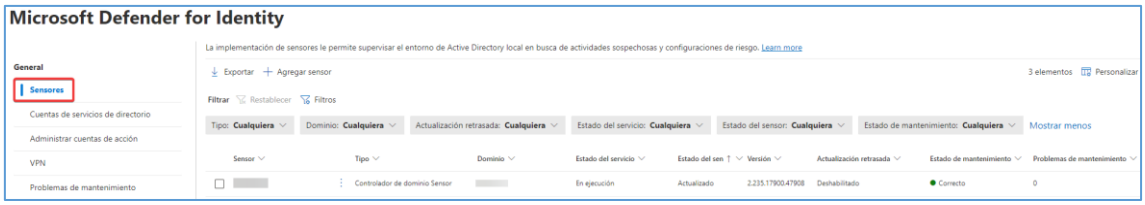
Y a continuación **Finalizar**.

Durante la instalación del sensor de *Defender for Identity* se instalan y configuran los siguientes componentes:

- El servicio del sensor de *Defender for Identity* y el servicio de actualización del sensor de *Defender for Identity*.
- Npcap OEM versión 1.0.

2.2.5 COMPROBACIONES

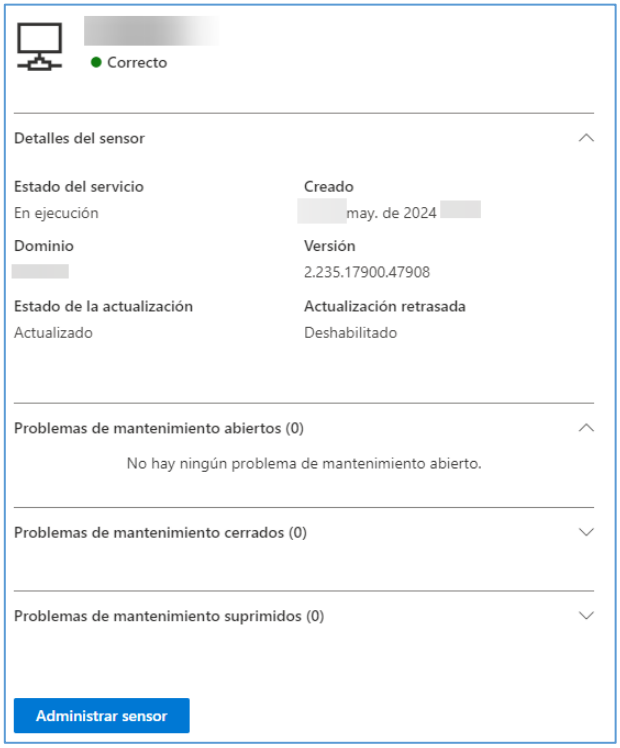
Volviendo al portal de Microsoft Defender, acceder al menú dispuesto en [Configuración\Identidades\Sensores]. Puede comprobarse que aparece el sensor recién incorporado:



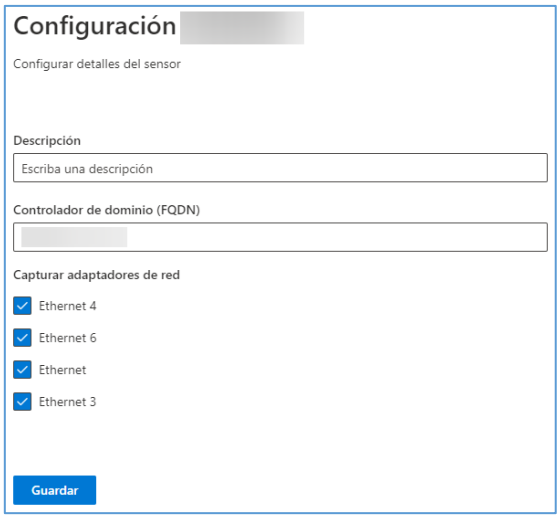
También se muestran todos los sensores de Defender for Identity y se enumeran los detalles siguientes por sensor:

- Sensor name (Nombre del sensor)
- Pertenencia al dominio del sensor
- Número de versión del sensor
- Si se deben retrasar las actualizaciones
- Estado de servicio del sensor
- Estado del sensor
- Estado de mantenimiento del sensor
- Número de problemas de mantenimiento
- Cuando se creó el registro

Seleccionando un sensor, se mostrará un panel de detalles con más información relativa al sensor y su estado de mantenimiento:



Pulsando sobre el botón “Administrar sensor” podremos introducir una descripción al mismo y habilitar o deshabilitar la captura en ciertos adaptadores de red que no sean de interés:


Configuración
Configurar detalles del sensor
Descripción
Escriba una descripción
Controlador de dominio (FQDN)
Capturar adaptadores de red
Ethernet 4
Ethernet 6
Ethernet
Ethernet 3
Guardar

3. CONFIGURACIÓN SEGURA PARA MICROSOFT DEFENDER FOR IDENTITY

A continuación, se abordará la configuración del servicio Microsoft Defender for Identity centrándose en el cumplimiento de los requisitos del Esquema Nacional de Seguridad (ENS) establecidas en el BOE-A-2022-7191 Real Decreto 311/2022, de 3 de mayo que aplican exclusivamente a este servicio:

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 Defender for Identity un recurso de Azure, el proveedor de identidad será **Microsoft Entra ID**.

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://learn.microsoft.com/es-es/entra/identity/hybrid/

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

3.1.1.2 REQUISITOS DE ACCESO

La gestión de identidades de Microsoft Defender es común a todas las aplicaciones de la solución Microsoft 365 y se describe en la guía [CCN-STIC-885A - Guía de configuración segura para Office 365].

Los usuarios que tienen el rol e de *administrador global* o *administrador de seguridad* en Microsoft Entra ID también son automáticamente administradores de Defender for Indetity. Los administradores globales y de seguridad de Microsoft Entra no necesitan permisos adicionales para obtener acceso a Defender for Identity.

Para otros usuarios, se puede habilitar y usar el control de acceso basado en roles (RBAC) de Microsoft 365 para crear roles personalizados y para admitir más roles de Entra ID, como operador de seguridad o lector de seguridad de forma predeterminada, para administrar el acceso a Defender for Identity.

Para acceder a la experiencia de *Defender for Identity* en *Microsoft Defender XDR*, se necesitan los siguientes **permisos**:

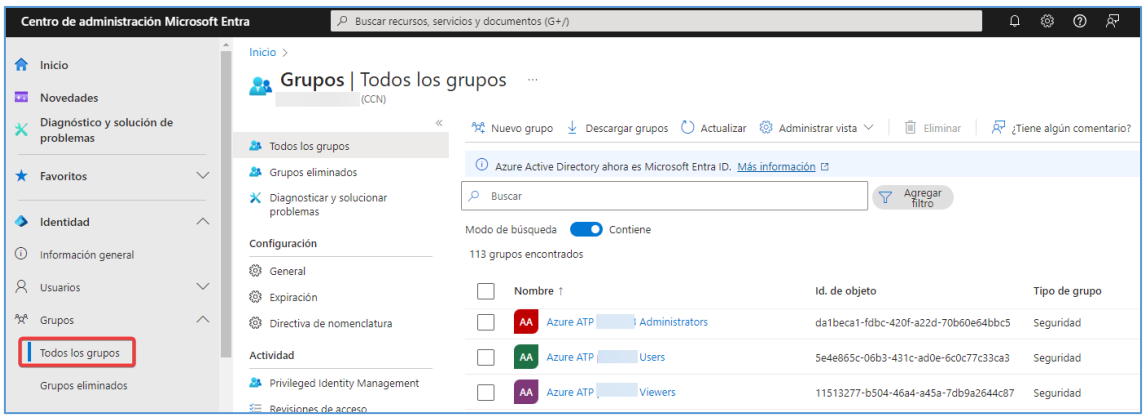
- En el caso de las *alertas, actividades y evaluaciones de seguridad* en Microsoft Defender XDR, asegurarse de tener los roles suficientes de *Microsoft Entra ID* o roles internos de *Microsoft Cloud App Security*. Para obtener más información, consultar *Microsoft Defender for Identity* requisitos previos de integración.
  * Los roles de administrador Cloud App Security admitidos actualmente son Administrador global, Lector de seguridad y Administrador de cumplimiento.

- Para la configuración de *Defender for Identity* en *Microsoft Defender XDR*, asegurarse de tener los roles de Microsoft Entra ID suficientes o ser miembro de los **grupos** de administradores de Azure ATP o usuarios de Azure ATP (de la instancia correspondiente).

Agregar y quitar usuarios a los grupos de seguridad

Defender for Identity usa Microsoft Entra ID de seguridad como base para los grupos de roles. Solo los usuarios de Entra ID se pueden agregar a los grupos de seguridad o quitar de estos. Los grupos de roles se pueden administrar desde la página de administración Grupos.

https://entra.microsoft.com/#view/Microsoft_AAD_IAM/GroupsManagementMenuBlade/~/AllGroups/menuId/AllGroups



Tipos de grupos de seguridad de Defender for Identity

Defender for Identity proporciona tres tipos de grupos de seguridad: *Administradores de Azure ATP* (nombre de instancia), *Usuarios de Azure ATP* (nombre de instancia) y *Visores de Azure ATP* (nombre de instancia). En la tabla siguiente se describe el tipo de acceso en el portal de *Defender for Identity* disponible para cada rol. Según el rol que se asigne, varias pantallas y opciones de menú del portal estarán o no disponibles para esos usuarios, como se muestra a continuación:

Actividad	**Administradores de Azure ATP *(nombre de instancia)***	**Usuarios de Azure ATP *(nombre de instancia)***	**Visores de Azure ATP *(nombre de instancia)***
Cambiar el estado de problema de mantenimiento	Disponible	No disponible	No disponible
Cambiar el estado de alertas de seguridad (volver a abrir, cerrar, excluir, suprimir)	Disponible	Disponible	No disponible
Eliminar el área de trabajo	Disponible	No disponible	No disponible
Descargar un informe	Disponible	Disponible	Disponible
Iniciar sesión	Disponible	Disponible	Disponible
Compartir o exportar las alertas de seguridad (por correo electrónico, obtener vínculo, descargar detalles)	Disponible	Disponible	Disponible
Actualizar configuración de Defender for Identity (actualizaciones)	Disponible	No disponible	No disponible
Actualizar configuración de Defender for Identity (etiquetas de entidad, incluidas confidenciales y honeytoken)	Disponible	Disponible	No disponible
Actualizar configuración de Defender for Identity (exclusiones)	Disponible	Disponible	No disponible
Actualizar configuración de Defender for Identity (idioma)	Disponible	Disponible	No disponible
Actualizar configuración de Defender for Identity (notificaciones, incluidos el correo electrónico y syslog)	Disponible	Disponible	No disponible
Actualizar configuración de Defender for Identity (detecciones de versión preliminar)	Disponible	Disponible	No disponible
Actualizar configuración de Defender for Identity (informes programados)	Disponible	Disponible	No disponible

Actualizar configuración de Defender for Identity (orígenes de datos, incluidos los servicios de directorio, SIEM, VPN, Defender para el punto de conexión)	Disponible	No disponible	No disponible
Actualizar configuración de Defender for Identity (sensores, incluida la descargar, regenerar clave, configuración, eliminación)	Disponible	No disponible	No disponible
Visualización de perfiles de entidad y alertas de seguridad	Disponible	Disponible	Disponible

3.1.1.3 SEGREGACIÓN DE FUNCIONES Y TAREAS

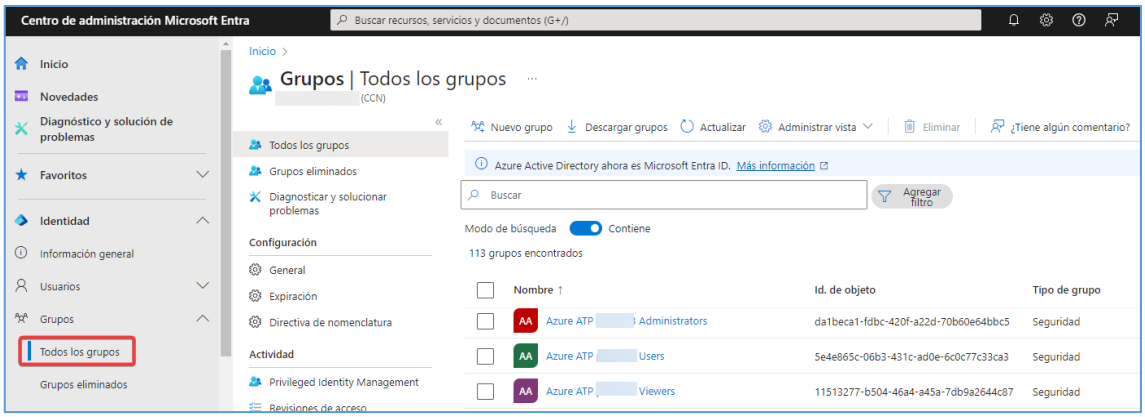
Microsoft *Defender for Identity* ofrece seguridad basada en roles para proteger los datos según las necesidades específicas de seguridad y cumplimiento de una organización. *Defender for Identity* admite tres roles independientes:

- Administradores
- Usuarios
- Visores

Los grupos de roles habilitan la administración de acceso para *Defender for Identity*. Con los grupos de roles, es posible separar las tareas dentro del equipo de seguridad y conceder los derechos de acceso que los usuarios necesitan para realizar su trabajo.

Nota: Cualquier administrador global o administrador de seguridad del tenant Azure Active Directory automáticamente es un administrador de Defender for Identity.

Defender for Identity usa los grupos de seguridad de Entra ID como base para los grupos de roles. Los grupos de roles se pueden administrar desde la página de administración Grupos del portal de Entra:



Solo los usuarios de Microsoft Entra ID se pueden agregar a los grupos de seguridad o quitar de estos.

Nota: Para más información sobre asignación de roles consultar guía [CCN-STIC-884A - Guía de Configuración segura para Azure].

3.1.1.4 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].

3.1.1.5 MECANISMOS DE AUTENTICACIÓN (USUARIOS DE LA ORGANIZACIÓN)

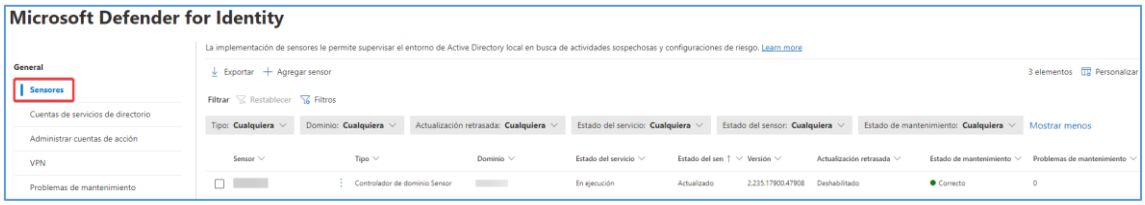
Los mecanismos de autenticación que se utilizarán para proteger a los usuarios de la organización serán los mismos que los indicados en el punto anterior para los usuarios externos. Como se ha comentado, ahora el acceso a los recursos está descentralizado, siendo la identidad el nuevo perímetro de seguridad, 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

En esta sección se detallan aspectos relevantes de *Microsoft Defender for Identity* en cuanto a la Explotación de los recursos. Para acceder a información detallada de todas la medidas de seguridad y mecanismos de protección y acceso consultar la guía [CCN-STIC-884A - Guía de configuración segura para Azure].

3.1.2.1 INVENTARIO DE ACTIVOS

Se puede obtener un inventario actualizado de todos los controladores de dominio que tienen instalado sensores MDI, desde el portal de Microsoft Defender XDR. Para ello, acceder al menú [Configuración\Identidades\Sensores]:



3.1.2.2 PROTECCIÓN FRENTE A CÓDIGO DAÑINO

En el portal de Microsoft *Defender* y más concretamente en [Identidades\Panel] se proporciona una vista rápida de todas las actividades sospechosas. Permite profundizar en los detalles de cualquier actividad y realizar acciones basadas en esas actividades. También se muestran alertas y notificaciones para resaltar los problemas detectados *por Defender for Identity* o las actividades nuevas que se consideren sospechosas.

3.1.2.3 GESTION DE INCIDENTES

El portal de Security Microsoft Defender XDR es la nueva experiencia de seguridad donde se irán aglutinando todas las funcionalidades relacionadas con este ámbito. https://security.microsoft.com

Las alertas de Defender for Identity se integran de forma nativa en Microsoft Defender XDR con un formato de alerta de identidad dedicado. Esta ofrece un enriquecimiento superior de señales entre diferentes dominios y nuevas capacidades de respuesta automatizada en materia de identidad. Asegura su protección y contribuye a optimizar la eficiencia de las operaciones de seguridad.

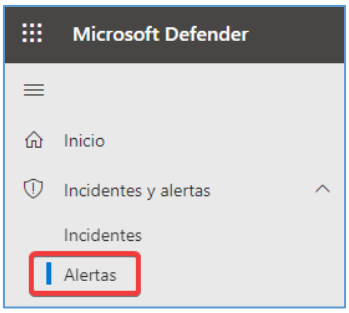
Una de las ventajas de investigar alertas con Microsoft Defender XDR es que las alertas de Microsoft Defender for Identity se integran de manera más profunda con la información de otros productos del mismo conjunto de aplicaciones. Estas alertas mejoradas son consistentes con los otros formatos de alerta de Microsoft Defender XDR, provenientes de Microsoft Defender para Office 365 y Microsoft Defender para Endpoints. La nueva página elimina la necesidad de cambiar a otro portal de productos para investigar las alertas relacionadas con la identidad.

Las alertas generadas por Defender for Identity pueden activar funciones automatizadas de investigación y respuesta (AIR) de Microsoft Defender XDR, incluyendo la corrección automática de alertas y la neutralización de herramientas y procesos que podrían estar relacionados con actividades sospechosas.

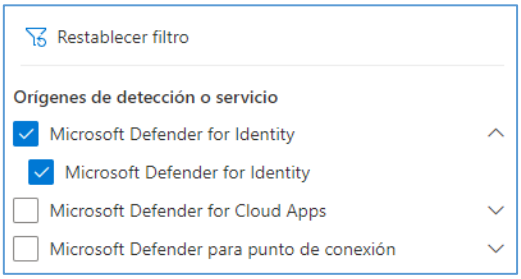
ALERTAS DE SEGURIDAD EN EL PORTAL

Se puede acceder a las alertas desde varias ubicaciones, incluida la página Alertas, la página Incidentes, las páginas de dispositivos individuales y la página Búsqueda avanzada. En este caso, revisaremos la página Alertas.

En el portal de Microsoft Defender XDR, seleccionaremos [Incidentes y alertas\Alertas].



Para ver las alertas de Defender for Identity se puede aplicar filtro en "Orígenes de detección o servicio"



Cada alerta de seguridad tiene la información siguiente:

- *Activos afectados* (usuarios, equipos, servidores, controladores de dominio y recursos).
- *Horas y período de tiempo* de las actividades sospechosas que han desencadenado la alerta de seguridad.
- *Gravedad* de la alerta: alta, media, baja o informativo.
- *Clasificación:* verdadero positivo (TP), verdadero positivo benigno (B-TP) o Falso positivo (FP).
- *Estado*: nueva, resuelta y en curso.
- Posibilidad de hacer lo siguiente:
    - Compartir la alerta de seguridad por correo electrónico con otras personas de la organización.
    - Descargar la alerta de seguridad en formato Excel.
    - Asignarla a equipos de soporte o escalado.

Las alertas de seguridad de *Defender for Identity* se clasifican en las siguientes categorías o fases, que se corresponden con las fases que conforman una cadena de eliminación de ciberataques estándar.

- Alertas de reconocimiento
- Alertas de credenciales en peligro
- Alertas de desplazamiento lateral
- Alertas de dominación de dominio
- Alertas de exfiltración

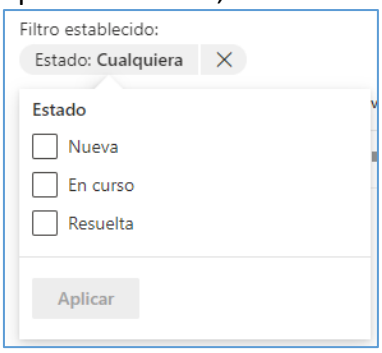
FILTRAR LA LSITA DE ALERTAS DE SEGURIDAD

Las alertas de seguridad se clasifican en:

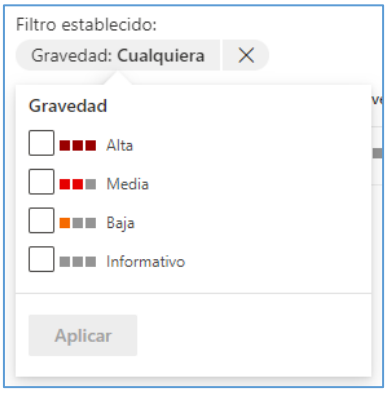
- **Baja**: Indica actividades que pueden desembocar en ataques diseñados para que un usuario o software malintencionado tenga acceso a los datos de la organización.
- **Media**: Indica actividades que pueden poner a determinadas identidades en riesgo de sufrir ataques más graves que culminen en un robo de identidad o en un escalado de privilegios.
- **Alta**: Indica actividades que pueden derivar en un robo de identidad, un escalado de privilegios u otros ataques de gran impacto.

Para filtrar la lista de alertas de seguridad:

1. En el panel de la izquierda de la pantalla, seleccionar una de las siguientes opciones: Nueva, en curso o resuelta.



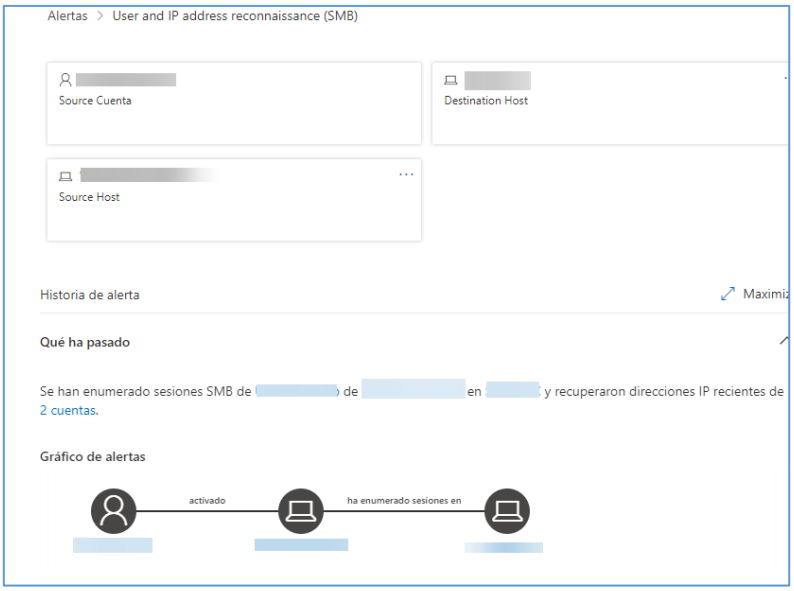
2. Para filtrar la lista aún más, seleccionar: Alta, Media o Baja.



ADMINISTRACIÓN DE ALERTAS DE SEGURIDAD

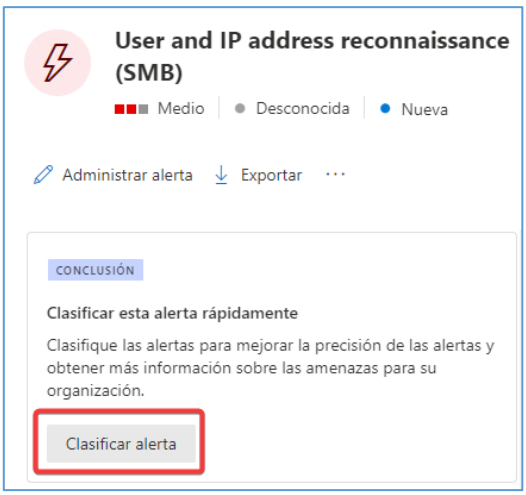
Seleccionando el nombre de la alerta de una de las alertas del panel, abrirá página con detalles sobre la alerta.

1. En el lado izquierdo se mostrará un resumen de “Qué ha pasado”:

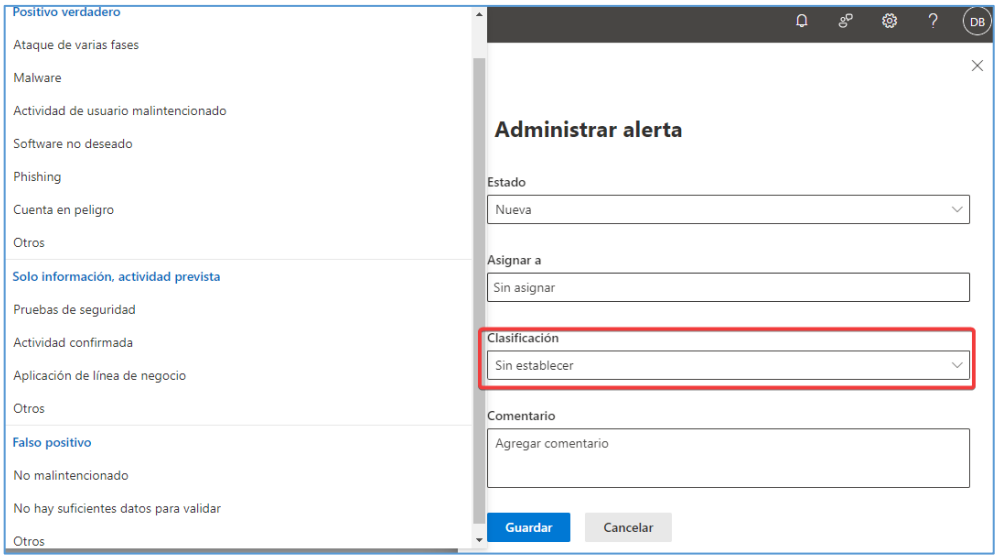


Encima del cuadro "Qué ha pasado" aparecen los botones Cuentas, Host de destino y Host de origen de la alerta. Para otras alertas, es posible que se muestren botones para obtener más información sobre hosts, cuentas, direcciones IP, dominios y grupos de seguridad adicionales. Seleccionando cualquiera de ellos se podrá obtener más detalles sobre las entidades implicadas.

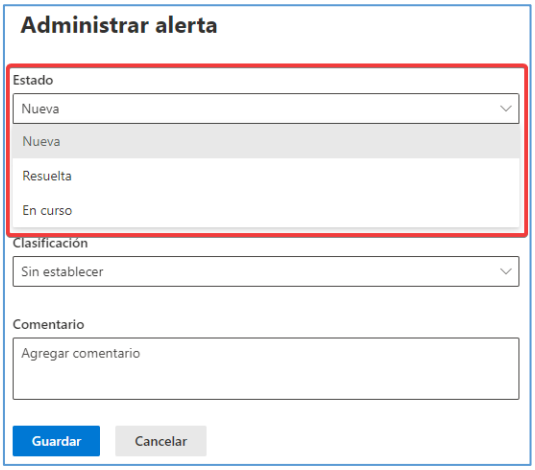
2. En el panel derecho, se mostrarán los detalles de la alerta. Aquí se pueden ver más detalles y realizar varias tareas:
   a) Clasificar la alerta: aquí se puede designar esta alerta como una alerta verdadera o una alerta falsa. Pulsar sobre el botón "Clasificar alerta:



Y en la ventana que muestra pulsar sobe "Clasificación".

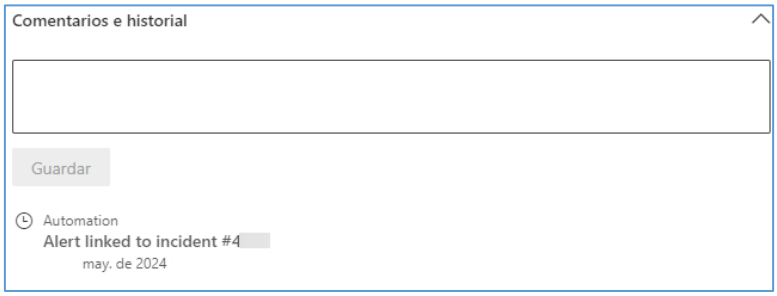


b) Estado de la alerta: podremos establecer como nueva, resuelta o en curso.



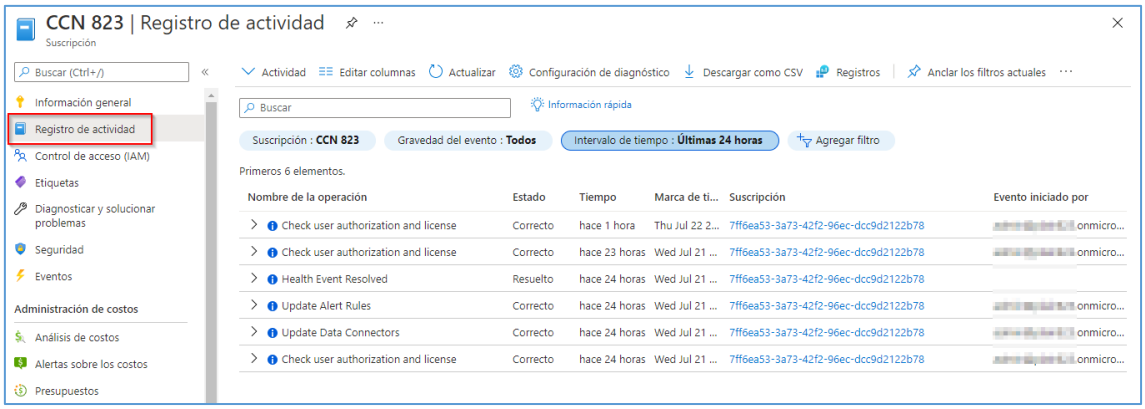
c) Detalles de la alerta: se puede encontrar más información sobre la alerta específica, seguir un vínculo a la documentación sobre el tipo de alerta, ver qué incidente está asociado a la alerta, revisar las investigaciones automatizadas vinculadas a este tipo de alerta y ver los dispositivos y usuarios afectados.

d) Comentarios e historial: se puede agregar comentarios a la alerta y ver el historial de todas las acciones asociadas a la alerta.



3.1.2.4 REGISTRO DE LA ACTIVIDAD

El Registro de actividad es un registro de plataforma de Azure que proporciona información de los eventos de nivel de suscripción. Esto incluye información como cuándo se modificó un recurso o cuándo se inició una máquina virtual. Puede ver el registro de actividad en Azure Portal o recuperar entradas con PowerShell y la CLI.



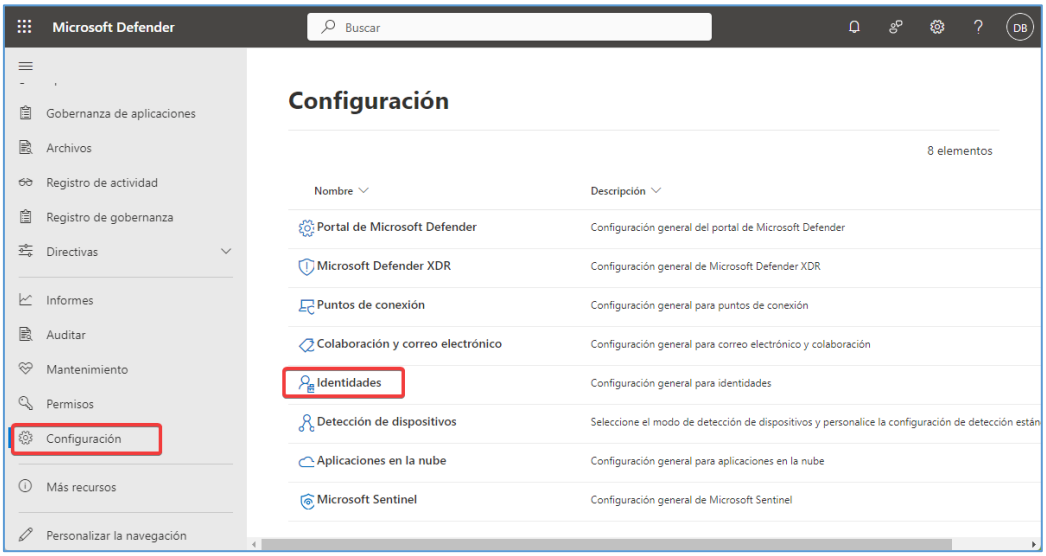
Más información en la guía [CCN-STIC-884A - Guía de configuración segura para Azure].

3.1.3 MONITORIZACIÓN DEL SISTEMA

Se puede configurar *Microsoft Defender for Identity* para avisar por correo electrónico cuando detecte una actividad sospechosa y emitir una alerta de seguridad o estado.

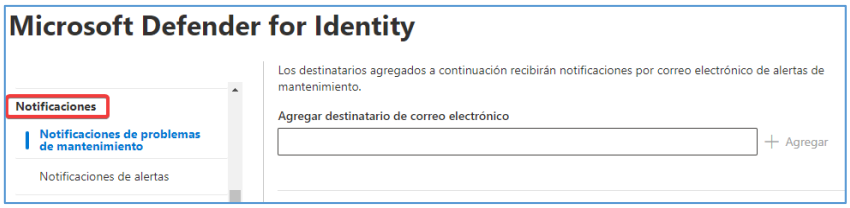
Para recibir notificaciones a una dirección de correo electrónico específica, establecer los parámetros siguientes:

1. En el portal de Microsoft *Defender*, en el menú izquierdo seleccionar la opción [Configuración\Identidades].



2. Aquí se podrán establecer notificaciones a nivel de:
   a) Notificaciones de Problemas de mantenimiento.
   b) Notificaciones de alertas.

   Agregar direcciones de correo electrónico para las notificaciones que se quieran recibir, según corresponda.



3.2 MEDIDAS DE PROTECCIÓN

3.2.1 PROTECCIÓN DE LA INFORMACIÓN

3.2.1.1 CALIFICACIÓN DE LA INFORMACIÓN

En esta sección se explica cómo aplicar etiquetas de entidad a cuentas confidenciales. Esto es importante porque algunas detecciones, como la detección de modificaciones de grupos confidenciales y la ruta de desplazamiento lateral, dependen del estado de confidencialidad de una entidad.

Defender for Identity también habilita la configuración de cuentas de *honeytoken*, que se usan como capturas para actores malintencionados: cualquier autenticación asociada a estas cuentas de *honeytoken* (normalmente inactivas), desencadena una alerta.

ENTIDADES CONFIDENCIALES

Los grupos de la siguiente lista se consideran confidenciales en *Defender for Identity*. Cualquier entidad que sea miembro de uno de estos grupos de Active Directory (incluidos los grupos anidados y sus miembros) se considera automáticamente confidencial:

- Administradores
- Usuarios avanzados
- Operadores de cuentas
- Operadores de servidores
- Operadores de impresión
- Operadores de copia de seguridad
- Replicadores
- Operadores de configuración de red
- Creadores de confianza de bosque de entrada
- Admins. del dominio
- Controladores de dominio
- Propietarios del creador de directivas de grupo
- Controladores de dominio de solo lectura
- Controladores de dominio empresariales de solo lectura
- Administradores de esquema
- Administradores de empresas

- Servidores de Microsoft Exchange

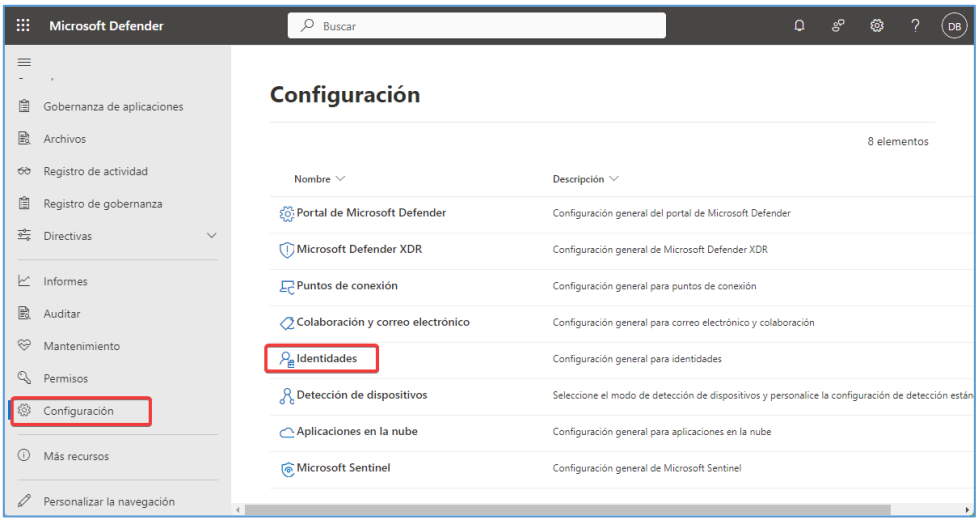
Además de estos grupos, *Defender for Identity* identifica los siguientes servidores de recursos de alto valor y los etiqueta automáticamente con el distintivo de *Confidencial*:

- Servidor de entidad de certificación.
- Servidor DHCP.
- Servidor DNS.
- Servidor de Microsoft Exchange.

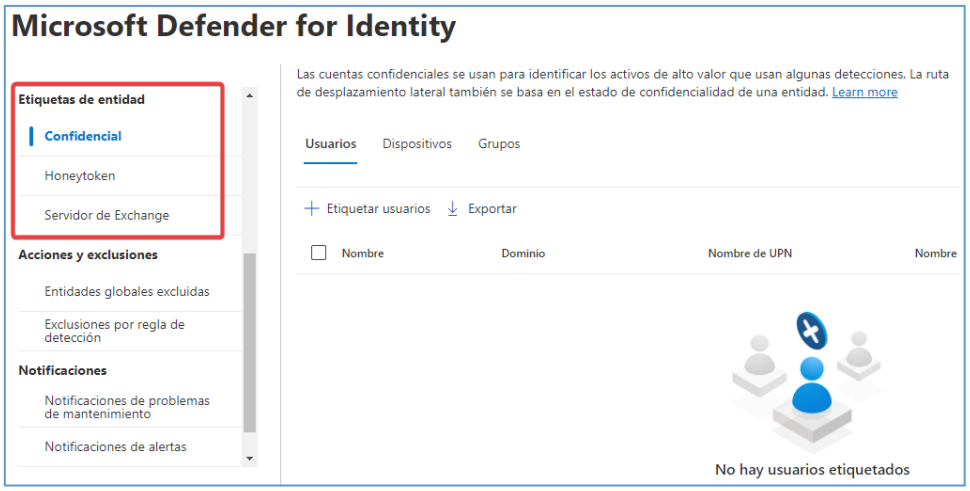
ETIQUETADO MANUAL DE ENTIDADES

También es posible etiquetar manualmente entidades como cuentas confidenciales o de *honeytoken*. Si se etiquetan manualmente usuarios o grupos adicionales (como miembros del consejo, ejecutivos de empresa y directores de ventas) los considerará *Defender for Identity* como confidenciales.

1. En el portal de Microsoft Defender XDR, seleccionar [Configuración\Identidades].



2. Seleccionar el tipo de etiqueta que se desea aplicar: Confidencial, Honeytoken o Servidor Exchange.



La etiqueta Confidencial admite usuarios, dispositivos y grupos.
La etiqueta Honeytoken admite usuarios y dispositivos.
La etiqueta Servidor de Exchange solo admite dispositivos.

3.2.2 PROTECCIÓN DE LOS SERVICIOS

3.2.2.1 PROTECCIÓN FRENTE A LA DENEGACIÓN DE SERVICIO

Microsoft 365 ofrece un sistema avanzado de **detección de amenazas** y **sistemas de mitigación** para proteger la infraestructura subyacente de los ataques de *denegación de servicio* (DoS) y prevenir la interrupción de servicio a los clientes.

Consultar la guía [CCN-STIC-884A - Guía de configuración segura para Azure] para obtener más información sobre el *sistema de defensa DDoS de Azure*, así como la guía [CCN-STIC-884E - Guía de configuración segura para Microsoft Sentinel].

4. GLOSARIO Y ABREVIATURAS

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

Término	Definición
AAD	*Azure Active Directory* (Directorio Activo de Azure).
AD DS	*Active Directory Domain Services* (Servicios de dominio de Directorio Activo).
Azure AD	*Azure Active Directory*.
Centro de Administración de Microsoft 365	Portal de Administración de Office 365. Accesible desde la url: admin.microsoft.com.
DC Shadow	*DC Shadow* es una técnica de ataque donde los atacantes registran un controlador de dominio de Active Directory falso y lo utilizan para inyectar objetos malicioso (por ejemplo, credenciales) a otros controladores de dominio que forman parte de la misma infraestructura de Active Directory.
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.*
ETW	Seguimiento de eventos para Windows
gMSA	Cuenta de servicio administrada de grupo.
honeytoken	Cuentas confidenciales.
M365D	*Microsoft 365 Defender*
MFA	*Multifactor Authentication* (Autenticación Multifactor). Sistema de seguridad que requiere más de una forma de autenticarse, por ejemplo a través de una *app*, *sms*, etc.
Microsoft Intelligent Security Graph	*Microsoft Intelligent Security Graph* es un repositorio único y una API de seguridad de "punto final" con acceso a información en tiempo real de miles de millones de datos. Muchos Partners de la industria, cada uno con su propia especialidad, informan sobre datos de telemetría y señales de seguridad a Intelligent Security Graph.
O365	*Office 365.*
PowerShell	PowerShell (originalmente llamada Windows PowerShell) es una interfaz de consola (*CLI*) con posibilidad de escritura y unión de comandos por medio de instrucciones (*scripts*).
SaaS	*Software as a Service* (Software como Servicio). Modelo de distribución de software donde el soporte lógico y los datos que maneja se alojan en servidores de una compañía de TIC, y se accede vía internet.

Término	Definición
Tenant	Un *tenant* de Office 365 es un espacio reservado en la nube de Microsoft desde el que tendremos acceso a los recursos y servicios que Microsoft ofrece.
TLS	TLS (Seguridad de la capa de transporte) y SSL (antecesor de TLS) son protocolos criptográficos que protegen la comunicación por red con certificados de seguridad que cifran una conexión entre equipos.

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 podrá valorar qué medidas de las propuestas se cumplen.

Control ENS	Configuracion	Estado	
op	**Marco Operacional**		
op.acc	**Control de Acceso**		
Op.acc.1	**Identificación**		
	Se ha configurado el uso de cuentas y la asignación de licencias a usuarios. Siguiendo las recomendaciones de Office 365 basada en la guía [CCN-STIC-885A - Guía de configuración segura para Office 365].	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
Op.acc.2	**Requisitos de acceso**		
	Se han comprobado los niveles de permisos para los recursos de la organización: administradores, usuarios y visores.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**

Control ENS	Configuracion	Estado	
Op.acc.3	**Segregación de funciones y tareas**		
	Se ha asignado adecuadamente los roles de administración y la asignación de los usuarios a los grupos de seguridad (en función de los accesos que se quieran permitir).	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
Op.acc.5	**Mecanismo de autenticación (usuarios externos)**		
	Se encuentra habilitado el “doble factor de autenticación” y se dispone de una adecuada política de gestión de credenciales.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
op.acc.6	**Mecanismo de autenticación (usuarios de la organización)**		
	Ídem que el control anterior [op.aac.5]	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**

Control ENS	Configuracion	Estado	
op.exp	**Explotación**		
Op.exp.1	**Inventario de activos**		
	Se comprobará que todos los sensores instalados están presentes en el portal de Defender for Identity.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
op.exp.6	**Protección frente a código dañino**		
	Se consultan periódicamente todas las actividades sospechosas abiertas que se muestran de forma predeterminada en el Panel. Se apican filtros para mostrar todas las actividades sospechosas o solo las que estén abiertas, descartadas o suprimidas.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**

Control ENS	Configuracion	Estado	
op.exp.7	**Gestión de incidentes**		
	Se realiza un seguimiento de las alertas mediante la configuración del estado de las mismas.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
Op.exp.8	**Registro de la actividad**		
	Se revisarán informalmente, de forma periódica, los registros de actividad, buscando patrones anormales.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
Op.mon	**Monitorización del sistema**		
	Se ha configurado Microsoft *Defender for Identity* para avisar por correo electrónico cuando detecte una actividad sospechosa y emitir una alerta de seguridad o estado.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**

Control ENS	Configuracion	Estado	
mp	**Medidas de protección**		
mp.info	**Protección de la información**		
mp.info.2	**Calificación de la información**		
	Se han etiquetado manualmente entidades como cuentas confidenciales o de honeytoken (como miembros del consejo, ejecutivos de empresa y directores de ventas, etc.).	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
mp.s	**Protección de los servicios**		
mp.s.4	**Protección frente a denegación de servicio**		
	Consultar la guía [CCN-STIC-884A - Guía de configuración segura para Azure] para obtener más información sobre el sistema de defensa DDoS de Azure, así como la guía [CCN-STIC-884E - Guía de configuración segura para Microsoft Sentinel].	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
Otras	**Protección del puesto de trabajo**		
	Se ha habilitado la integración con el SIEM Microsoft Sentinel (si procede).	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No

Control ENS	Configuracion	Estado	
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
Otras	**Protección del puesto de trabajo**		
	Se ha establecido la integración con el servicio de *Defender for Endpoint* para una securización más completa del puesto de trabajo, y se ha comprobado que está funcionando correctamente.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
Otras	**Capacidad de Microsoft Defender for Identity**		
	Se ha analizado la capacidad de despliegue de Microsoft *Defender for Identity*, por ejemplo mediante el uso de la herramienta *TriSizingTool* u otros mecanismos similares.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**

PUBLICACIONES DE DEFENSA

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