centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 885E

Guía de configuración segura para Microsoft Defender for Endpoint

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 13:07:45 +02'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-24-249-4
Fecha de Edición: junio de 2024

ÍNDICE

1. MICROSOFT DEFENDER FOR ENDPOINT

1.1 DESCRIPCIÓN DEL USO DE ESTA GUÍA

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

1.2 DEFINICIÓN DE LA SOLUCIÓN

Microsoft Defender for Endpoint forma parte de la suite de seguridad integrada Microsoft Defender XDR (anteriormente Microsoft 365 Defender).

Microsoft Defender for Endpoint es una plataforma de seguridad de extremo de empresa diseñada para ayudar a las redes empresariales a prevenir, detectar, investigar y responder a amenazas avanzadas.

Defender for Endpoint utiliza una combinación de tecnología integrada en Windows 10 y el servicio en la nube de Microsoft:

- **Sensores de comportamiento de extremo:** incrustados en Windows 10, estos sensores recopilan y procesan señales de comportamiento del sistema operativo y envían estos datos del sensor a la instancia privada en la nube de Microsoft Defender for Endpoint.
- **Análisis de seguridad en la nube:** Al aprovechar los macrodatos (big-data), el aprendizaje de dispositivos y la óptica exclusiva de Microsoft en todo el ecosistema de Windows, los productos empresariales en la nube (como Office 365) y los activos en línea, las señales de comportamiento se traducen en conocimientos, detecciones y respuestas recomendadas a amenazas avanzadas.
- **Inteligencia de amenazas:** generada por los hunters de Microsoft (equipo de buscadores expertos en amenazas cibernéticas de Microsoft), equipos de seguridad y enriquecida por la inteligencia de amenazas proporcionada por otros partners, la inteligencia de amenazas permite a Defender for Endpoint identificar herramientas, técnicas y procedimientos de atacantes y generar alertas cuando se observan en datos de sensor recopilados.

Nota: Microsoft Defender XDR se conocía antes como Microsoft Threat Protection o MTP.

Microsoft Defender for Endpoint se conocía antes como Protección contra amenazas avanzada de Microsoft Defender o MDATP.

Es posible ver los nombres antiguos en la documentación de Microsoft que todavía estarán en uso durante un tiempo.

1.3 PROTECCIÓN DEL PUESTO DE TRABAJO

Microsoft Defender XDR, (anteriormente conocido como Microsoft 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.

Con la solución Microsoft Defender XDR integrada, 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; 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 auto sanar los buzones, cargas de trabajo, puntos de conexión e identidades de usuario afectados.

El conjunto de aplicaciones de Microsoft Defender XDR protege:

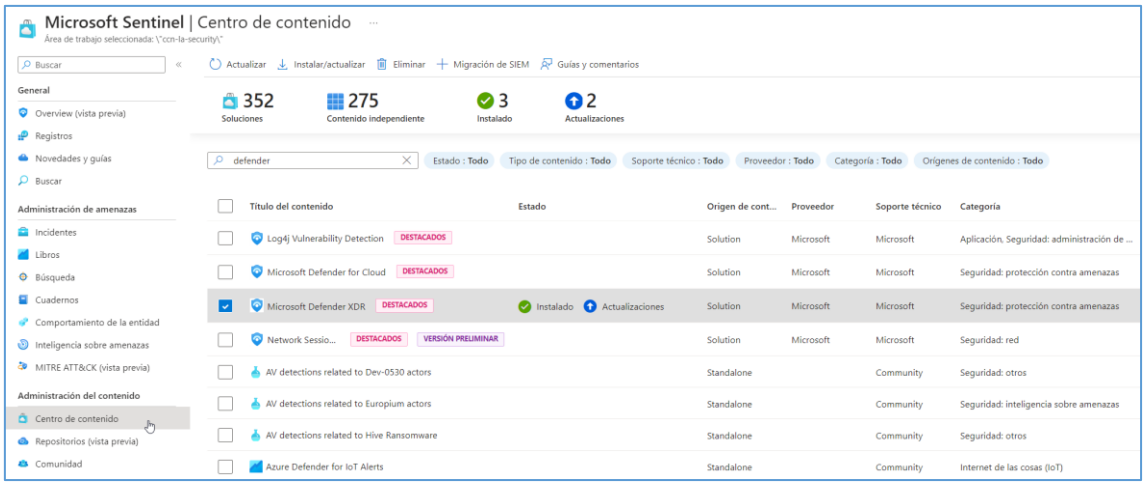
- **Puntos de Conexión** con *Microsoft Defender for Endpoint*: Microsoft Defender for Endpoint es una plataforma de extremo unificada para la protección preventiva, la detección posterior a la infracción, la investigación automatizada y la respuesta.

- **Correo electrónico y colaboración** con *Microsoft Defender XDR 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, para identificar, detectar e investigar amenazas avanzadas, identidades en peligro y acciones internas malintencionadas dirigidas a su organización. Protección de Microsoft Entra ID ayuda a las organizaciones 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 seguridad de *Microsoft Cloud App*: la seguridad de Microsoft Cloud App 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.
- **Administración de vulnerabilidades** ofrece visibilidad continua de los recursos, evaluaciones inteligentes basadas en riesgos y herramientas de corrección integradas para ayudar a los equipos de TI y seguridad a priorizar y abordar vulnerabilidades críticas y configuraciones incorrectas en toda la organización.

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.

1.3.1 INTEGRACIÓN CON MICROSOFT SENTINEL

A través del centro de contenido (Content hub), **Microsoft Sentinel** genera la integración con **Microsoft Defender XDR** (M365XDR) permitiendo transmitir todos los incidentes y alertas de M365XDR a Microsoft Sentinel y manteniendo todos los incidentes sincronizados entre ambos portales. Los incidentes de M365XDR incluyen todas sus alertas, entidades y otra información relevante de todos los servicios que lo componen.



Nota: Más información en la guía [CCN-STIC-884E - Guía de configuración segura para Microsoft Sentinel].

1.3.2 INTEGRACIÓN CON MICROSOFT INTUNE

Con Microsoft Defender XDR para punto de conexión, se pueden usar directivas de seguridad de punto de conexión desde Microsoft Intune para configurar la seguridad de Defender en los dispositivos que se han incorporado a Defender sin inscribirlos con Intune.

Esta integración brinda las siguientes funcionalidades:

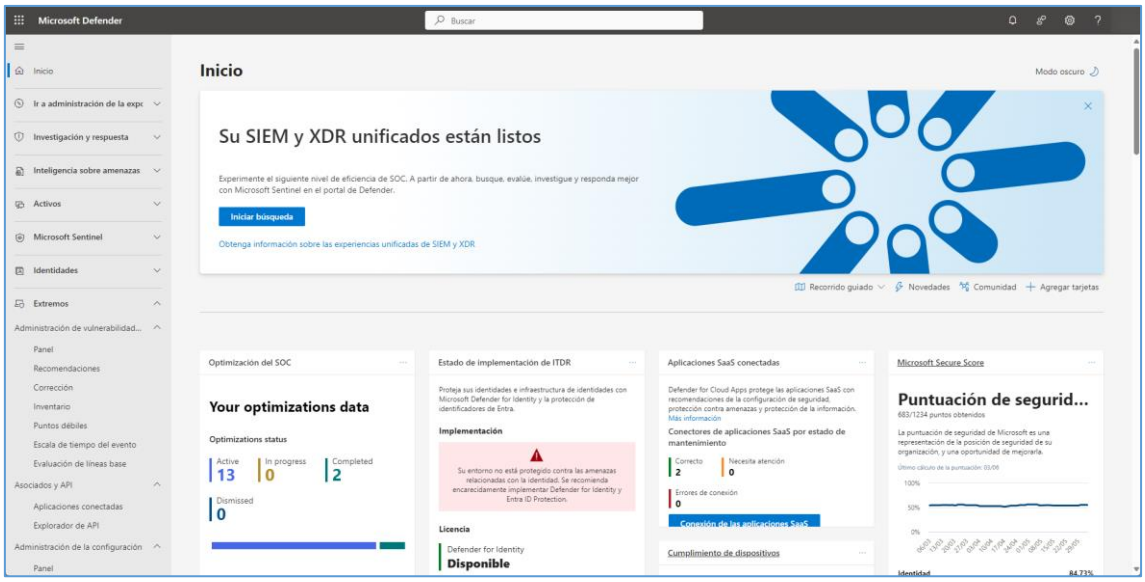
- Con el Centro de administración de Intune o el portal de Defender 365, se pueden crear y asignar directivas de seguridad para Defender para punto de conexión con grupos de Entra ID.
- Los dispositivos reciben las directivas configuradas según su identificador de objeto de dispositivo Entra.
- Los objetos de dispositivo Entra ID determinan las directivas asignadas a los dispositivos.

Para más información sobre como integrar las herramientas revisar el punto [4.1.5.1 Administracion de configuración de la seguridad.]

Nota: Para más información sobre como integrar las herramientas desde la parte de Microsoft Intune, en la guía [CCN-STIC-884F - Guía de configuración segura para Microsoft Intune].

1.4 FUNCIONALIDADES DEL PORTAL

El acceso a las funcionalidades de Microsoft Defender XDR for Office 365 se realiza desde el portal mejorado de seguridad de Microsoft Defender XDR, accediendo a la siguiente URL: https://security.microsoft.com/

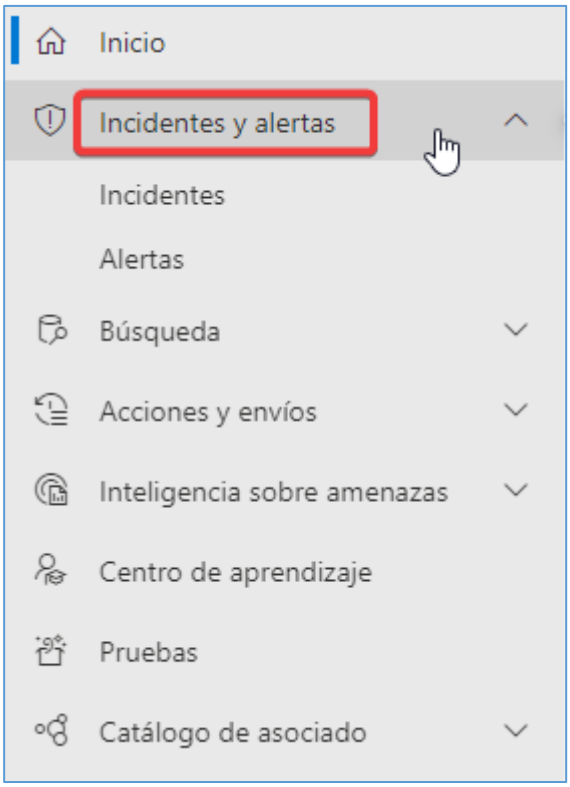


El nuevo portal de *Microsoft Defender XDR*, reúne las funcionalidades que solían estar en portales independientes en un solo lugar, de modo que pueda protegerse de una manera más sencilla y centralizada de cualquier tipo de amenaza.

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, cargas de trabajo y aplicaciones) e integrase con Microsoft Sentinel.

1.4.1 INVESTIGAR INCIDENTES Y RESPONDER A AMENAZAS

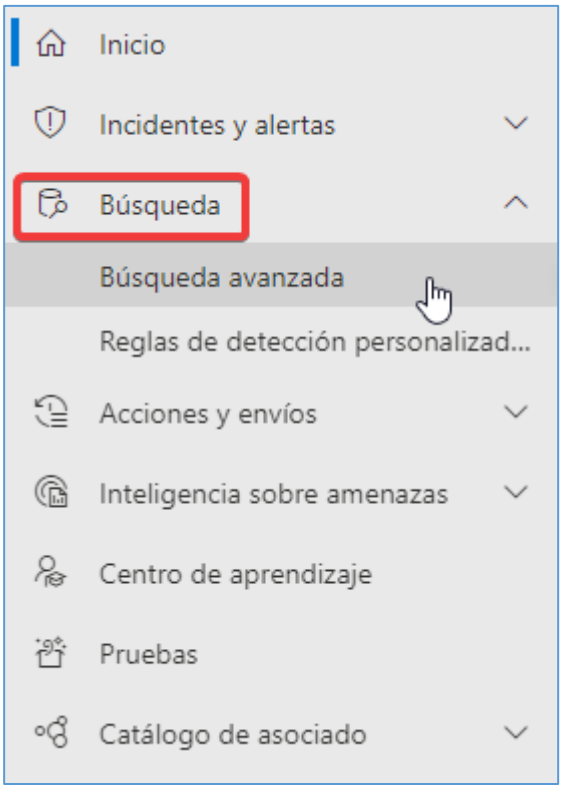
Las alertas están categorizadas, combinadas y correlacionadas en incidentes completos.



- **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. Puedes ver la fuente de la alerta, la descripción y tomar acciones como la investigación adicional o la resolución.

1.4.2 BUSCAR AMENAZAS DE MANERA PROACTIVA

Mediante la creación de consultas avanzadas se permite buscar amenazas en correos electrónicos y elementos de colaboración.



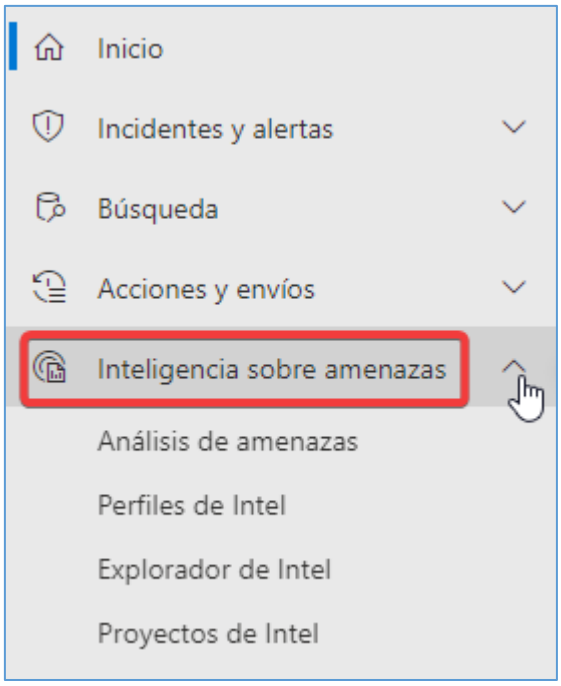
- **Búsqueda avanzada:** Herramienta que permite crear consultas personalizadas utilizando un lenguaje de consulta avanzado para buscar indicadores de compromiso (IOC) y actividades sospechosas en los datos recopilados por la plataforma.

1.4.3 REALIZAR UN SEGUIMIENTO Y RESPONDER A LAS AMENAZAS EMERGENTES

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.

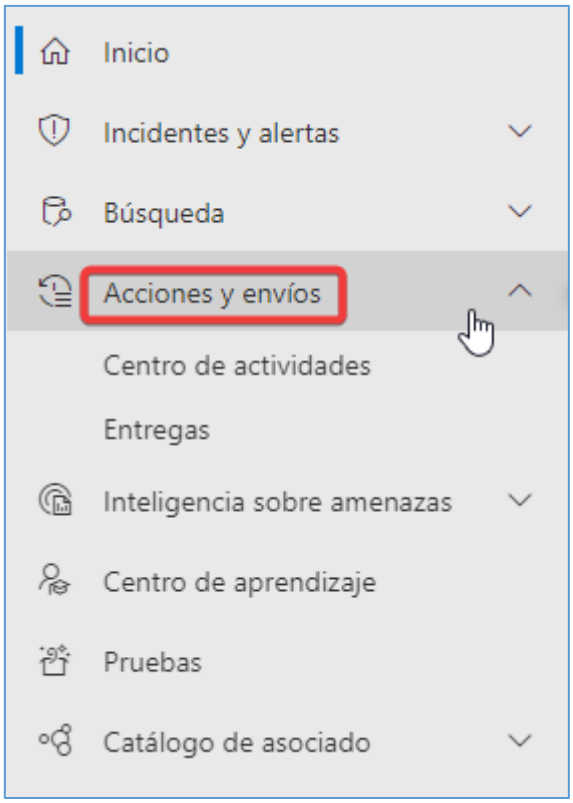


En el menú de Inteligencia de amenazas se encuentra el menú para la función **Análisis de amenazas** que está diseñado para ayudar a los equipos de seguridad a ser más eficientes y dos nuevas incorporaciones:

- **Perfiles Intel:** una nueva característica que introduce contenido curado organizado por actores de amenazas, sus herramientas y vulnerabilidades conocidas.
- **Explorador de Intel**: la experiencia existente de búsqueda e investigación de contenidos de TI de Defender.

1.4.4 SUPERVISAR LAS ACCIONES Y EL ESTADO DE 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:



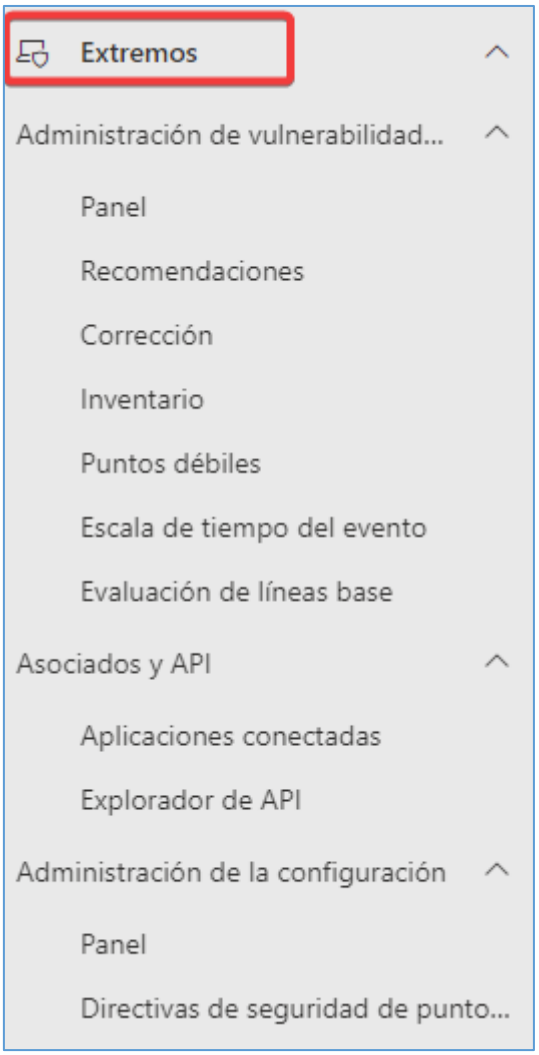
- **Acciones:** Esta sección se encarga de gestionar las acciones recomendadas y las tareas de respuesta a incidentes de seguridad. Incluye:
  - **Acciones Pendientes:** Muestra una lista de todas las acciones de seguridad recomendadas que aún no se han completado. Estas acciones pueden incluir tareas 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.
  - **Acciones Completadas:** 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.

- **Envíos:** La sección de envíos 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.
  - **Envío de Archivos:** Permite a los usuarios enviar 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.

- **Envío de URLs:** 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.
- **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

1.4.5 PROTECCIÓN DEFENDER FOR ENDPOINT

A continuación, se muestran las funcionalidades de Microsoft Defender para puntos de conexión existentes en el portal de Microsoft Defender.



- **Administración de vulnerabilidades:** Sección para consultar la puntuación segura de Microsoft para dispositivos, la puntuación de exposición, los dispositivos expuestos, el software vulnerable y tomar medidas sobre las recomendaciones de seguridad más destacadas.
  - **Panel:** Este es el panel de control de seguridad. Muestra información general sobre el número de alertas activas, los dispositivos y los

usuarios que están en riesgo y la gravedad de las alertas, dispositivos y usuarios. También se puede ver si algún dispositivo tiene problemas con el sensor, el estado general del servicio y cómo se clasificaron alertas pendientes.

- **Recomendaciones:** Contiene una lista de recomendaciones de seguridad para las amenazas y vulnerabilidades que se encuentran en la organización.
- **Corrección:** Cuando se envía una solicitud de corrección desde la página de Recomendaciones de seguridad, se inicia una actividad de corrección. Esto crea una tarea de seguridad que se puede monitorear en la página de Corrección y también genera un vale de corrección en Microsoft Intune.
  En esta sección, seleccionar la actividad de corrección deseada para seguir los pasos, monitorear el progreso, ver la recomendación relacionada, exportar a CSV o marcar como completada.
- **Inventario:** Muestra la lista de dispositivos que están incorporados a Defender for Endpoint, información sobre ellos y sus niveles de exposición y riesgo.
- **Puntos débiles:** Muestra una lista de las vulnerabilidades CVE que afectan a los dispositivos. Aquí se puede consultar la gravedad, la clasificación del sistema de puntuación CVSS, y la información relevante sobre violaciones y amenazas, entre otros detalles.
- **Escala de tiempo del evento:** Se puede consultar toda la información relevante relacionada con un evento.
- **Evaluación de líneas base:** Evaluaciones continuas y en tiempo real en comparación con los estándares del sector, como CIS y STIG. Permite crear y gestionar perfiles, generar informes sobre dispositivos no conformes, utilizar la búsqueda avanzada de amenazas para consultar diferentes hallazgos, o emplear las nuevas funciones de exportación de API para crear informes personalizados.

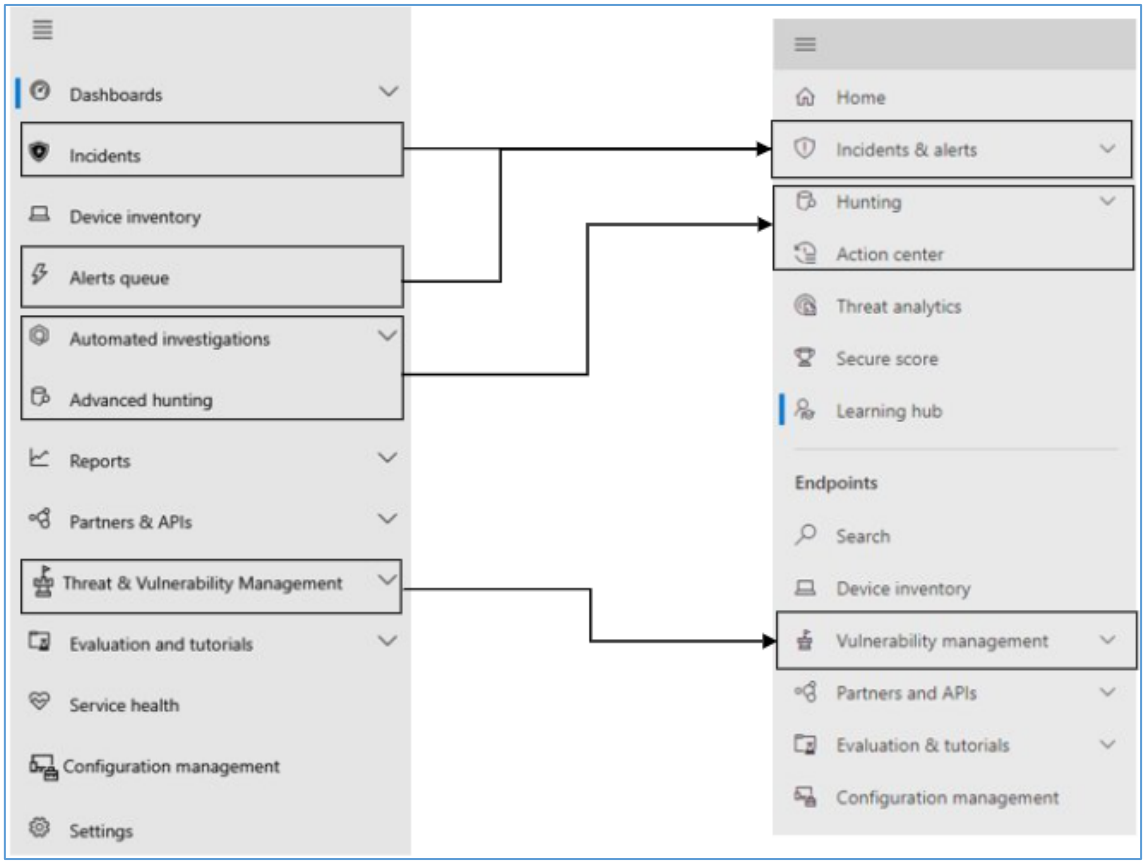
- **Asociados y API:** Se pueden ver las conexiones de partners compatibles, que mejoran las capacidades de detección, investigación e inteligencia de amenazas de la plataforma. También se pueden observar las aplicaciones conectadas, el explorador de API, la información general sobre el uso de la API y la configuración de exportación de datos.
  - **Aplicaciones conectadas**: Ayuda a rastrear las diversas aplicaciones de Entra ID que se integran con la plataforma de Microsoft Defender ATP en su organización.
  - **Explorador de API:** Es una herramienta que permite explorar de manera interactiva las diversas APIs de Microsoft Defender ATP. Con el Explorador de API, se puede:
    - Ejecutar solicitudes para cualquier método y ver las respuestas en tiempo real.
    - Navegar rápidamente por los ejemplos de API y aprender qué parámetros admiten.

        - Realizar llamadas a la API fácilmente sin necesidad de autenticación adicional más allá del inicio de sesión en el portal de administración.
- **Administración de configuración:** Muestra los dispositivos abordo, la línea base de seguridad de la organización, el análisis predictivo, la cobertura de protección web y permite realizar la administración de superficies de ataques en los dispositivos.
    - **Panel:** Este es el panel de configuración de dispositivos. Muestra información general sobre la configuración aplicada a los dispositivos por MDE, controlar la administración de configuración de seguridad, dispositivos incorporados, administración de superficie expuesta a ataques de dispositivos, etc.
    - **Directivas de seguridad de puntos de conexión:** Se pueden ver todas las políticas de seguridad de Intune directamente. Además, se puede filtrar la lista y buscar políticas específicas utilizando las funciones integradas de "filtro" y "búsqueda".

1.5 COMPARATIVA DE PORTALES

La imagen y la tabla siguiente enumeran los cambios en la navegación entre el Centro de seguridad de Microsoft Defender y Microsoft Defender XDR.

Centro de seguridad de Microsoft Defender	Microsoft Defender XDR
Paneles • **Operaciones de seguridad** • **Análisis de amenazas**	Inicio • Análisis de amenazas
Incidentes	Alertas de & incidentes
Inventario de dispositivos	Inventario de dispositivos
Cola de alertas	Alertas de & incidentes
Investigaciones automatizadas	Centro de actividades
Búsqueda avanzada de amenazas	Búsqueda
Informes	Informes
Partners & API	Partners & API
Administración & vulnerabilidades de amenazas	Administración de amenazas y vulnerabilidades
Evaluación y tutoriales	Tutoriales & evaluación
Administración de la configuración	Administración de la configuración
Configuración	Configuración



1.6 POSIBILIDAD DEL USO DEL PORTAL ANTERIOR AL ACTUAL

Para volver a la Centro de seguridad de Microsoft Defender anterior:

Iniciar sesión en el portal de Microsoft Defender como administrador global o con una cuenta y con permisos de administrador de seguridad en Microsoft Entra ID.

a) Ir al redireccionamiento del Portal general de puntos de conexión de configuración.
b) Cambiar la configuración de redireccionamiento automático a Desactivado.
c) Seleccionar *Deshabilitar & compartir* comentarios cuando se le solicite.

Esta configuración se puede habilitar de nuevo en cualquier momento.

Una vez deshabilitadas, las cuentas no se enrutan a security.microsoft.com y tendrá acceso al portal anterior: securitycenter.windows.com o securitycenter.microsoft.com.

1.7 PRERREQUISITOS MICROSOFT DEFENDER FOR ENDPOINT

Para poder utilizar la solución e incorporar dispositivos a la misma, es necesario cumplir unos requisitos mínimos.

1.7.1 REQUERIMIENTO DE LICENCIAS

Microsoft Defender for Endpoint requiere una de las siguientes ofertas de licencias por volumen de Microsoft:

- **Microsoft Defender for Endpoint Plan 1 o Plan2**.

  Microsoft Defender para Endpoint P1 está disponible como una licencia de suscripción de usuario independiente y como parte de Microsoft 365 E3/A3/G3.

  Microsoft Defender para Endpoint P2 está disponible como licencia independiente y como parte de los siguientes planes:

  - Windows 11 Empresa E5/A5
  - Windows 10 Empresa E5/A5
  - Microsoft 365 E5/A5/G5 (que incluye Windows 10 o Windows 11 Enterprise E5)
  - Seguridad de Microsoft 365 E5/A5/G5/F5
  - Seguridad y cumplimiento de Microsoft 365 F5

  En Defender para punto de conexión, un escenario de licencias mixtas se refiere a cuando una organización combina licencias de Defender para punto de punto 1 y Plan 2.

  En la siguiente tabla se muestran algunos ejemplos de escenarios de licencias mixtas:

Escenario	Descripción
Inquilino mixto	Uso de diferentes conjuntos de funcionalidades para grupos de usuarios y sus dispositivos. Algunos ejemplos son: - Plan 1 de Defender para punto de conexión y Defender para punto de conexión 2 - Microsoft 365 E3 y Microsoft 365 E5
Prueba mixta	Test de una suscripción de nivel Premium para algunos usuarios. Algunos ejemplos son: - Plan 1 de Defender para punto de conexión (todos los usuarios) y Plan 2 de Defender para punto de conexión (se ha iniciado una suscripción de prueba para algunos usuarios) - Microsoft 365 E3 (todos los usuarios) y Microsoft 365 E5 (se ha iniciado una suscripción de prueba para algunos usuarios)
Actualizaciones por fases	Actualización de las licencias de usuario en fases. Algunos ejemplos son: - Traslado de grupos de usuarios del plan 1 de Defender para punto de conexión al plan 2 - Traslado de grupos de usuarios de Microsoft 365 E3 a E5

El reporte de uso de licencias se basa en las actividades de inicio de sesión en el dispositivo. Las licencias del plan 2 de Defender para punto de conexión son por usuario y cada usuario puede tener hasta cinco dispositivos incorporados al mismo tiempo.

- ***Microsoft Defender for Endpoint* para servidores**

Microsoft Defender para servidor está diseñado para proteger las cargas de trabajo de los servidores tradicionales locales, y también funciona con servidores Windows y Linux. Cada entorno de sistema operativo (OSE), ya sea un servidor o una máquina virtual, necesita una licencia distinta.

Para la incorporación de servidores se requieren licencia de servidor, a elegir entre:

  - Opción de Microsoft Defender para servidores Plan 1 o Plan 2 (incluidos en Defender for Cloud).
  - Microsoft Defender para EndPoint para servidores.
  - Servidores Microsoft Defender for Business (solo para pequeñas y medianas empresas).

1.7.2 REQUISITOS DE LOS EXPLORADORES

El acceso a Microsoft Defender for Endpoint se realiza a través de:

- Microsoft Edge
- Google Chrome

1.7.3 REQUISITOS DE HARDWARE Y SOFTWARE

1.7.3.1 REQUISITOS SOFTWARE

Versiones Windows compatibles:

- Windows 7 SP1 Enterprise (Requiere actualizaciones de seguridad extendidas, ESU)
- Windows 7 SP1 Pro (Requiere actualizaciones de seguridad extendidas, ESU)
- Windows 8.1 Enterprise
- Windows 8.1 Pro
- Windows 10 Enterprise
- Windows 10 Enterprise LTSC 2016 (o posterior)
- Windows 10 Education
- Windows 10 Pro
- Windows 10 Pro Education
- Windows 11 Enterprise
- Windows 11 Education
- Windows 11 Pro
- Windows 11 Pro Education
- Windows servidor
  - Windows Server 2012 R2

  - Windows Server 2016
  - Windows Servidor, versión 1803 o posterior
  - Windows Server 2019
  - Windows Server 2022
- Azure Virtual Desktop
- Windows 365, bajo uno de los sistemas operativos anteriores.

Otros sistemas operativos compatibles con *Defender for Endpoint* son:

- Android
- iOS
- Linux
- Subsistema de Windows para Linux (WSL)
- macOS

En **máquinas virtuales** con Windows 10 Enterprise 2016 LTSB pueden aparecer problemas de rendimiento si se ejecutan en plataformas de virtualización que no son de Microsoft.

Para entornos virtuales, se recomienda usar Windows 10 Enterprise LTSC 2019 o posterior.

1.7.3.2 REQUISITOS HARDWARE

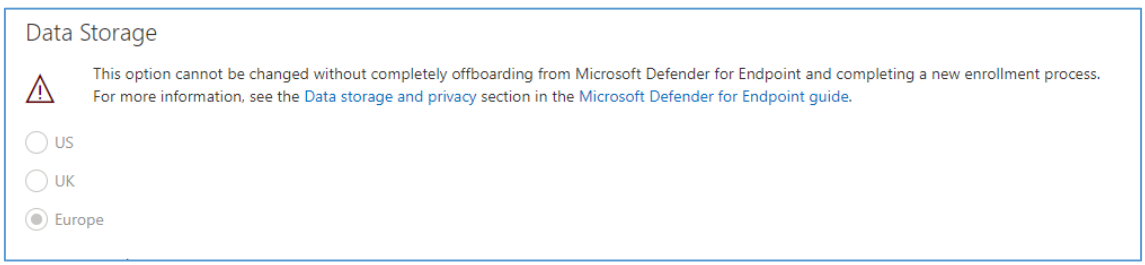
Defender para Endpoint en dispositivos Windows no tiene requisitos de hardware más allá de los que ya tiene el sistema operativo (es decir, son iguales a los requisitos del sistema operativo).

- Cores: 2 como mínimo, 4 como mejor opción
- Memoria: 1 GB como mínimo, 4 como mejor opción

1.7.4 REQUISITOS DE CONFIGURACIÓN Y ALMACENAMIENTO DE DATOS Y RED

Al ejecutar el asistente de incorporación por primera vez, se debe elegir el *datacenter* (Centro de datos) dónde se almacena la información relacionada con Microsoft Defender for Endpoint: Unión Europea, Reino Unido o Estados Unidos.

Nota: No se puede cambiar la ubicación de almacenamiento de datos después de la configuración por primera vez.



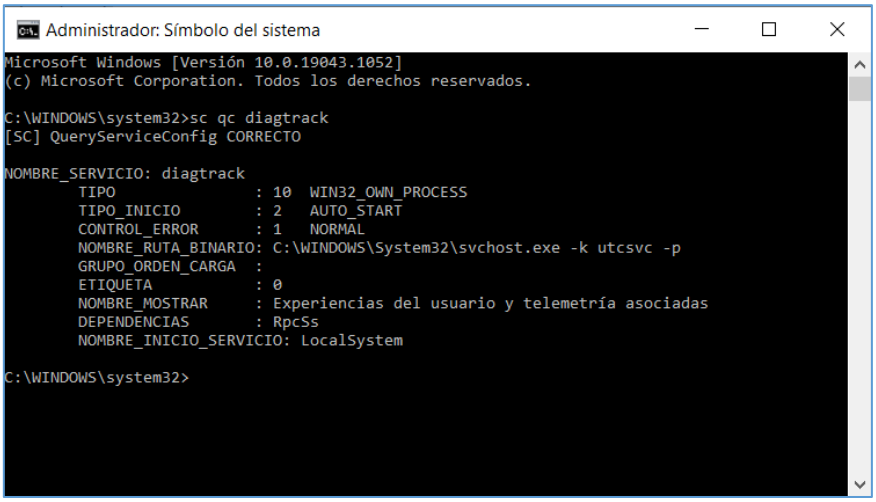
1.7.5 CONFIGURACIÓN DE DATOS DE DIAGNÓSTICO

Antes de comenzar con la configuración, es conveniente asegurarse que el servicio de datos de diagnóstico está habilitado en todos los dispositivos de la organización. Este servicio suele estar habilitado de forma predeterminada. Es una buena práctica comprobarlo para asegurar que los datos del sensor se obtienen de ellos.

Para ello simplemente abrir un símbolo de sistema con privilegios elevados y ejecutar el siguiente comando:

```
sc qc diagtrack
```

Si el servicio está habilitado, el resultado debería ser parecido a la siguiente captura de pantalla:

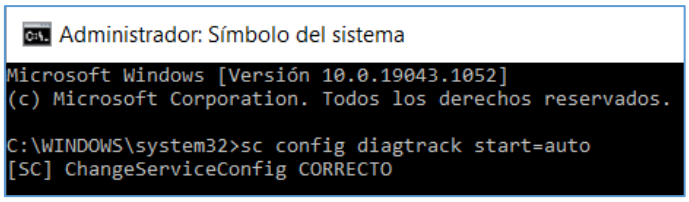


Se establecerá el servicio para que se inicie de forma automática si el START_TYPE no está establecido en AUTO_START.

Para ello, sobre un símbolo de sistema con privilegios elevados, escribir el siguiente comando:

```
sc config diagtrack start=auto
```

Se muestra el siguiente mensaje de éxito:



Finalmente, para comprobar dicho cambio, escribir el siguiente comando:

```
sc qc diagtrack
```

1.7.6 CONECTIVIDAD A INTERNET

La conectividad a Internet en dispositivos es necesaria directamente o a través del proxy.

El sensor Defender for Endpoint puede usar un ancho de banda promedio diario de 5 MB para comunicarse con el servicio en la nube de Defender for Endpoint e informar de los datos. Las actividades únicas, como las cargas de archivos y la colección de paquetes de investigación, no se incluyen en este ancho de banda promedio diario.

Como se ve en el punto anterior, antes de incorporar dispositivos, el servicio de datos de diagnóstico debe estar habilitado. El servicio está habilitado de forma predeterminada en Windows 10/11.

1.7.7 REQUERIMIENTO DE CONFIGURACIÓN DEL MICROSOFT DEFENDER

El agente de Defender for Endpoint depende de la capacidad de Antivirus de Microsoft Defender para examinar archivos y proporcionar información sobre estos.

Se deben configurar las actualizaciones de seguridad, independientemente de si Microsoft Defender Antivirus es o no el antimalware activo dentro de la compañía. Cuando el Antivirus de Microsoft Defender no es el antimalware activo de la compañía y se utiliza el servicio de Defender for Endpoint, el Antivirus de Microsoft Defender entra en modo pasivo.

En caso de haber desactivado el Antivirus de Microsoft Defender mediante GPO o cualquier otro método, los dispositivos que se vayan incorporando deberán excluirse de la GPO.

Nota: Durante el proceso de aplicación de las medidas de seguridad establecidas por el ENS en sistemas operativos Windows, se deshabilita el antivirus mediante directivas de grupo (GPO) y en caso de requerir el uso de Windows Defender se deberán modificar las directivas correspondientes.

Por otro lado, si se está ejecutando el Antivirus de Microsoft Defender como el producto antimalware principal en los dispositivos, el agente de Defender for Endpoint se incorporará correctamente.

1.8 PRERREQUISITOS ACTUACIONES MEDIANTE POWERSHELL

Para ejecutar mediante código Powershell algunos de los comandos descritos en la presente guía es necesario disponer de un entorno con el **módulo de Azure PowerShell**.

Para obtener información de la instalación de dicho módulo, consultar la guía [CCN-STIC-884A - Guía de configuración segura para Azure].

2. DESPLIEGUE DE MICROSOFT DEFENDER FOR ENDPOINT

Se recomienda realizar una planificación de la implementación de *Microsoft Defender for Endpoint* de forma que se puedan aprovechar todas las capacidades de seguridad dentro del conjunto de aplicaciones y así protegerse mejor de las amenazas.

La solución proporciona instrucciones sobre cómo configurar Microsoft Defender para puntos de conexión, asignar funciones y permisos, identificar la arquitectura del entorno, seleccionar el tipo de herramienta de implementación que mejor se adapte a

las necesidades e instrucciones sobre cómo configurar las capacidades. En la siguiente imagen se pueden observar los pasos principales de cara a poder realizar la planificación.

Configuración y requisitos	Asignación de funciones y permisos
Preparación del entorno para el despliegue	**Identificación y asignación funciones y permisos**
• Validación de licencia • Configuración de inquilino • Configuración de la red	• Control de Acceso basado en roles.

Identificar arquitectura y método de implementación	Incorporación de dispositivos	Configurar las funcionalidades
Identificar qué arquitectura representa mejor la organización y método de implementación	**Uso del método preferido para el despliegue**	**Configurar las siguientes funcionalidades:**
• Nativo en la nube • Administración conjunta • Arquitectura On-premises • Script y Evaluación • Microsoft Intune • SCCM • Política de grupo • Script local	• Script local (hasta 10 dispositivos) • Política de grupo • Microsoft Intune/ Mobile Device Manager • Microsoft Endpoint Configuration Manager • Script	• Detección y respuesta • Administración de vulnerabilidades • Protección de próxima generación • Reducción de la superficie de ataque • Capacidades de investigación y remediación automática (AIR)

2.1 CONFIGURACIÓN Y REQUISITOS

Para empezar a usar Microsoft Defender para Endpoint, hay que preparar el entorno de Defender para Endpoint.

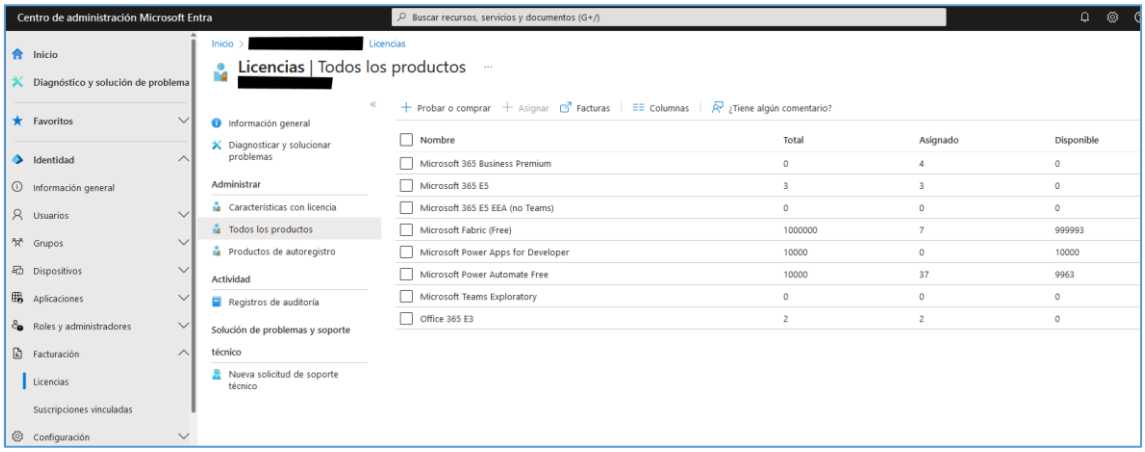
Para la preparación del entorno es necesario revisar los siguientes puntos:

- Validación de licencia
- Configuración de inquilino
- Configuración de la red

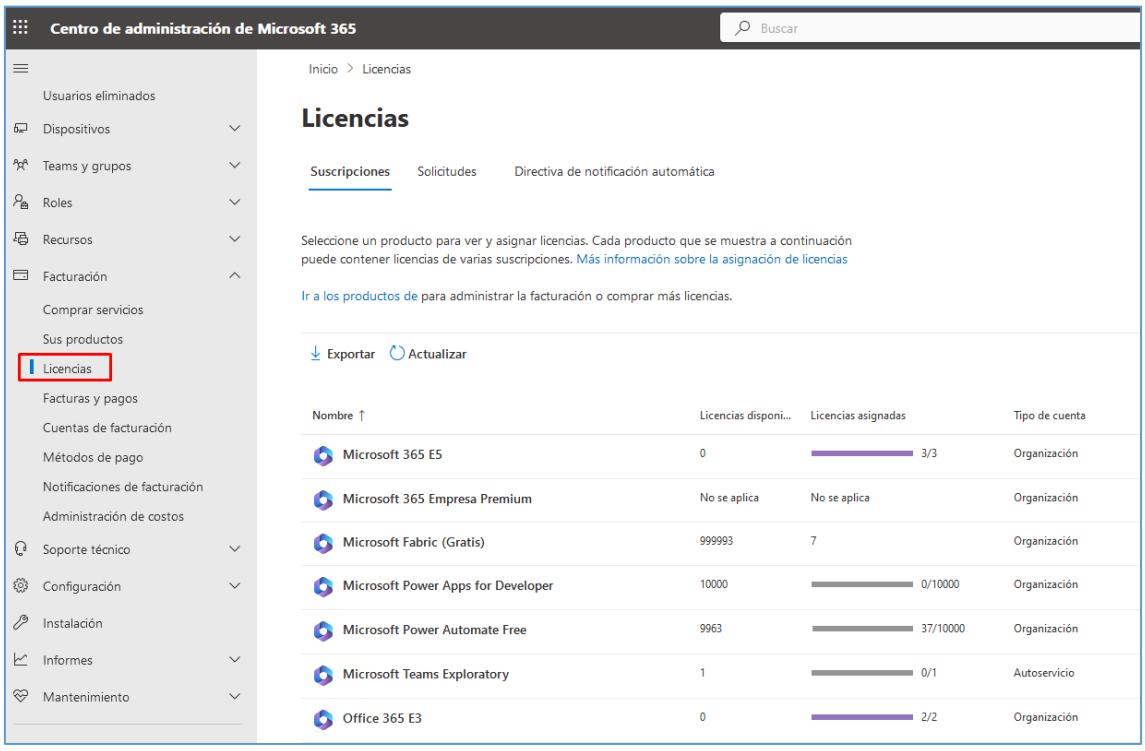
2.1.1 VALIDACIÓN DE LICENCIA

Comprobar el estado de la licencia y si se aprovisionó correctamente, se puede realizar a través del Centro de administración o a través del portal Microsoft Azure.

Para acceder a las licencias, entrar al portal de Entra, Facturación y a continuación seleccionar “licencias”.



Como alternativa, se puede acceder desde el *Centro de Administración de Microsoft 365*:



Mas información en el punto de 1.7.1 Requerimientos de licencias.

2.1.2 CONFIGURACIÓN DE INQUILINO

Para comenzar el proceso de incorporación, elegir cualquier opción en la sección Puntos finales del menú de navegación o cualquier función de Microsoft Defender XDR, como Incidentes, Búsqueda, Centro de actividades o Análisis de amenazas.

2.1.3 UBICACIÓN DEL CENTRO DE DATOS

Al usar Microsoft Defender para Endpoint, los datos se guardarán y procesarán en la misma ubicación que Microsoft Defender XDR. Si no se ha activado Microsoft Defender XDR, al incorporarse a Microsoft Defender para Endpoint también se activará Microsoft Defender XDR y se elegirá una ubicación nueva del centro de datos basada en la ubicación de los servicios de seguridad activos de Microsoft 365.

2.1.4 CONFIGURACIÓN DE RED

Si la organización no requiere que los puntos de conexión usen un proxy para tener acceso a Internet, omitir esta sección. En caso contrario, obtener información completa en la documentación de Microsoft:

Configuración de Microsoft Defender para punto de conexión implementación - Microsoft Defender for Endpoint | Microsoft Learn

2.2 ASIGNACIONES DE FUNCIONES Y ROLES

2.2.1 CONTROL DE ACCESO BASADO EN ROLES (RBAC)

Microsoft Defender for Endpoint admite dos formas de administrar permisos:

- **Configuración de permisos básicos:** asignación de permisos de acceso completo o solo lectura. Los usuarios que tienen el rol de Administrador global o Administrador de seguridad en Microsoft Entra ID tienen acceso completo. El rol de lector de seguridad tiene acceso solo lectura y no permite ver el inventario de máquinas/dispositivos.
- **Control de acceso basado en roles (RBAC):** defina permisos detallados creando roles, asociando grupos de usuarios de Microsoft Entra a los roles y dando a los grupos de usuarios acceso a los grupos de dispositivos.

Para más información en la documentación de Microsoft.

Uso del control de acceso basado en rol para conceder acceso específico a Microsoft Defender portal - Microsoft Defender for Endpoint | Microsoft Learn

2.3 IDENTIFICAR LA ARQUITECTURA Y MÉTODO DE IMPLEMENTACIÓN

2.3.1 IDENTIFICACIÓN DE LA ARQUITECTURA

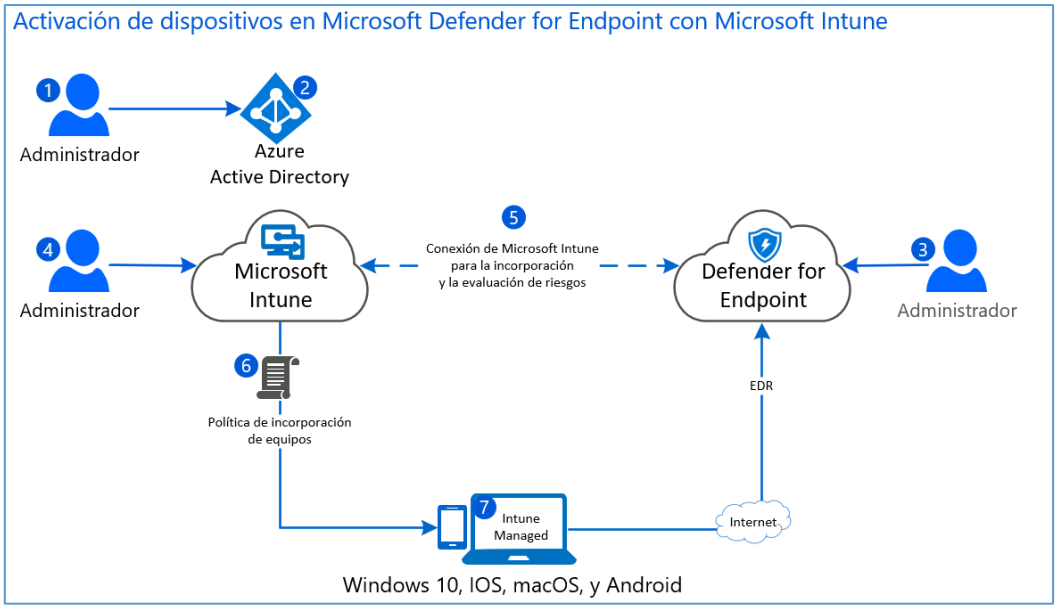
Cada entorno de empresa es único, por lo que se proporcionan varias opciones para dar la flexibilidad necesaria para elegir cómo implementar el servicio. Ciertas herramientas serán más o menos adecuadas para determinadas arquitecturas dependiendo del entorno. La implementación se puede realizar basándose en las siguientes arquitecturas:

- Nativo en la nube
- Administración conjunta

- Arquitectura On-premises
- Script y Evaluación

2.3.1.1 NATIVO EN LA NUBE

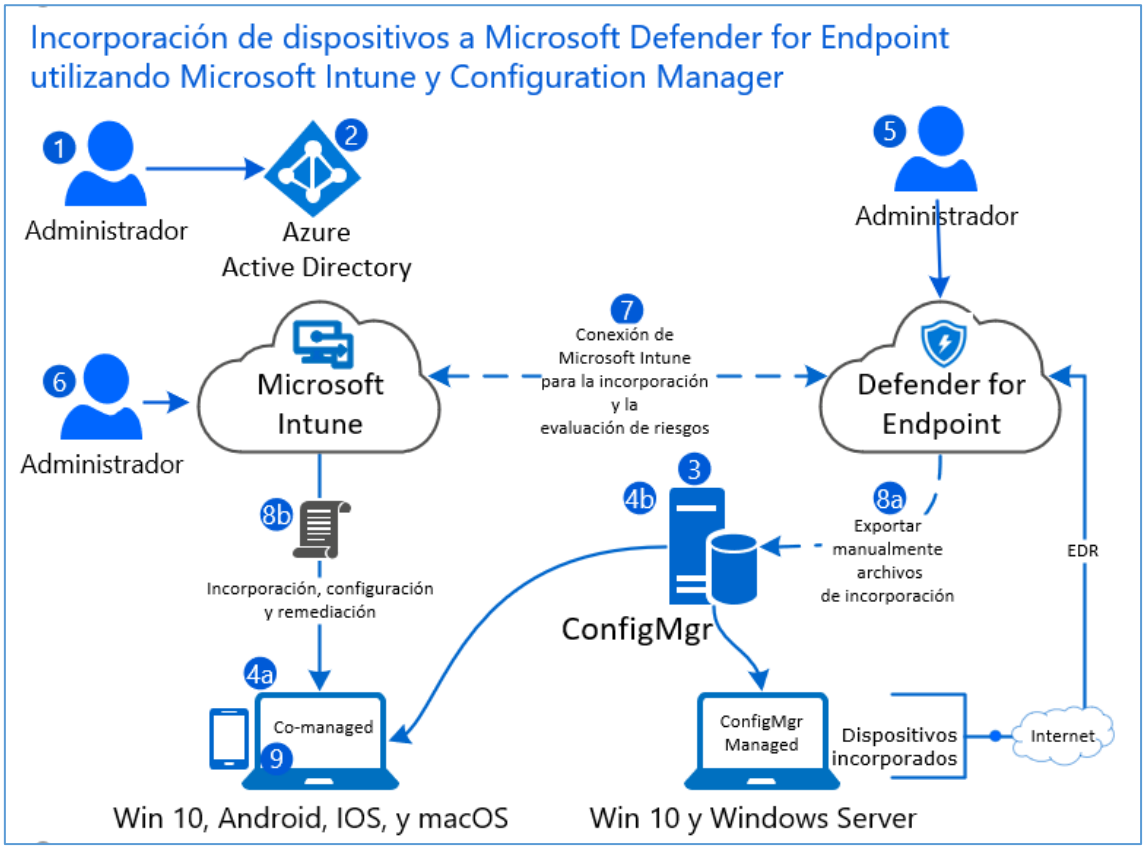
El despliegue se realiza mediante Microsoft Intune tal y como se refleja en la siguiente imagen.



1. Iniciar sesión en el portal de Azure y configurar la inscripción automática para Intune configurando el ámbito de usuario de MDM en Entra ID.
2. Asignar licencias de Intune a los usuarios en Entra ID y comprobar que los dispositivos estén inscritos.
3. Iniciar sesión en el **Centro de seguridad de Microsoft Defender** y completar el asistente de configuración inicial.
4. Iniciar sesión en el centro de administración de Microsoft Intune y navegar hasta **Abrir el Centro de seguridad de Microsoft Defender** para conectarse al servicio *Microsoft Defender for Endpoint*.
5. En el Centro de seguridad de Microsoft Defender, activar la configuración de conexión de Microsoft Intune.
6. En el centro de administración de Microsoft Intune, crear una política de configuración de dispositivos utilizando el tipo de perfil de *Microsoft Defender for Endpoint* (escritorio de Windows 10/11). Los dispositivos que no son de Windows requieren un paquete de instalación que debe descargarse del Centro de seguridad de Microsoft Defender.
7. Para verificar que los dispositivos están correctamente integrados y generando informes, ejecutar una prueba de detección en los dispositivos recién incorporados. Estos comandos se encuentran en la configuración del Centro de seguridad de Microsoft Defender en la sección **Onboarding**.

2.3.1.2 ADMINISTRACIÓN CONJUNTA

El siguiente método de despliegue se realiza mediante Microsoft Intune o Configuration Manager a través del denominado Co-management tal y como se refleja en la siguiente imagen.

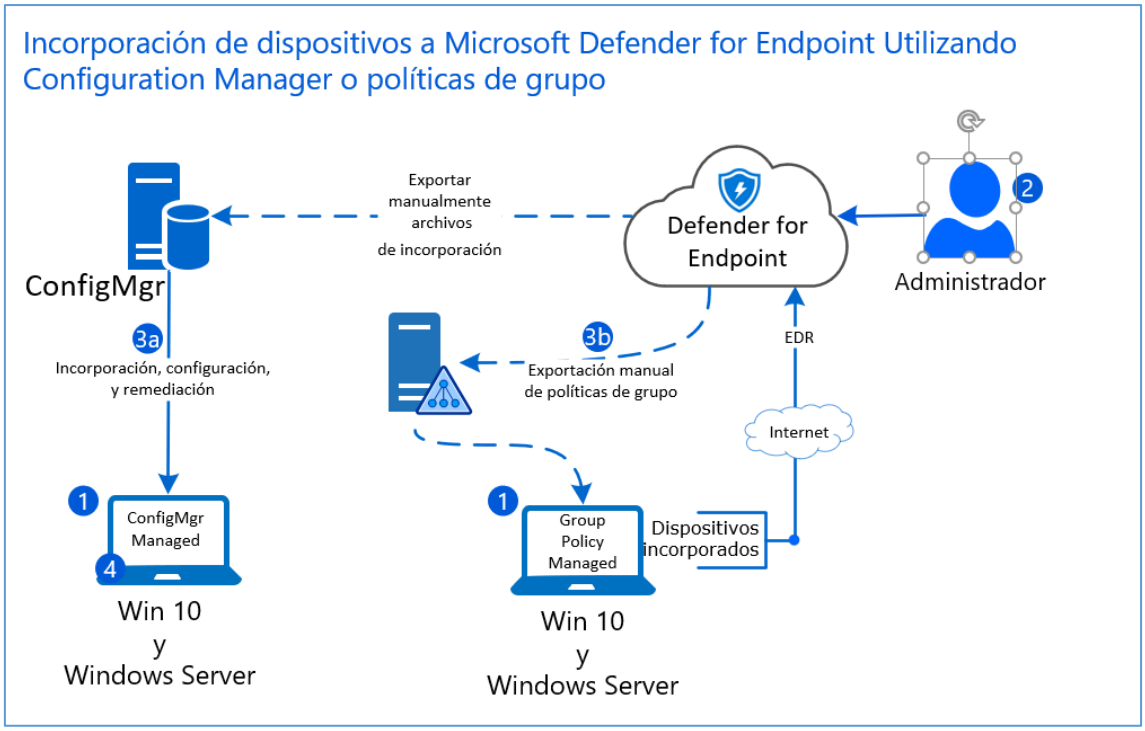


1. Iniciar sesión en el portal de Azure y configurar la inscripción automática para Intune configurando el ámbito de usuario de MDM en Entra ID.
2. Asignar licencias de Intune a los usuarios en Entra ID y comprobar que los dispositivos estén inscritos.
3. Elegir qué cargas de trabajo queremos que Microsoft Intune administre y realizamos el cambio en el nodo de administración conjunta de Configuration Manager.
4. Instalar el agente de Configuration Manager en dispositivos nuevos que se inscriban automáticamente en Azure AD (Comprobar que Azure AD Connect esté configurado en modo Azure AD híbrido) o configurar los dispositivos de Windows 10 que ya son clientes de Configuration Manager para unirlos a Azure AD híbrido e inscribirlos en Intune.
5. Iniciar sesión en el Centro de seguridad de Microsoft Defender y completar el asistente de configuración inicial.
6. Iniciar sesión en el centro de administración de Microsoft Intune y navegar hasta **Abrir el Centro de seguridad de Microsoft Defender** para conectarse al servicio *Microsoft Defender for Endpoint*.
7. En el Centro de seguridad de Microsoft Defender, activar la configuración de conexión de Microsoft Intune.

8. En el Centro de seguridad de Microsoft Defender, ir a **Onboarding** en la configuración, descargar un paquete de System Center Configuration Manager e importarlo en el entorno de Configuration Manager. O En el centro de administración de Microsoft Intune, crear una política de configuración de dispositivos utilizando el tipo de perfil de *Microsoft Defender for Endpoint* (escritorio de Windows 10). Los dispositivos que no son de Windows requieren un paquete de instalación que debe descargarse del Centro de seguridad de Microsoft Defender.
9. Para verificar que los dispositivos están correctamente integrados y generando informes, ejecutar una prueba de detección en los dispositivos recién incorporados. Estos comandos se encuentran en la configuración del Centro de seguridad de Microsoft Defender en la sección **Onboarding**.

2.3.1.3 ARQUITECTURA ON-PREMISES

El siguiente método de despliegue se realiza mediante Configuration Manager u objetos de directiva de grupo (GPO).



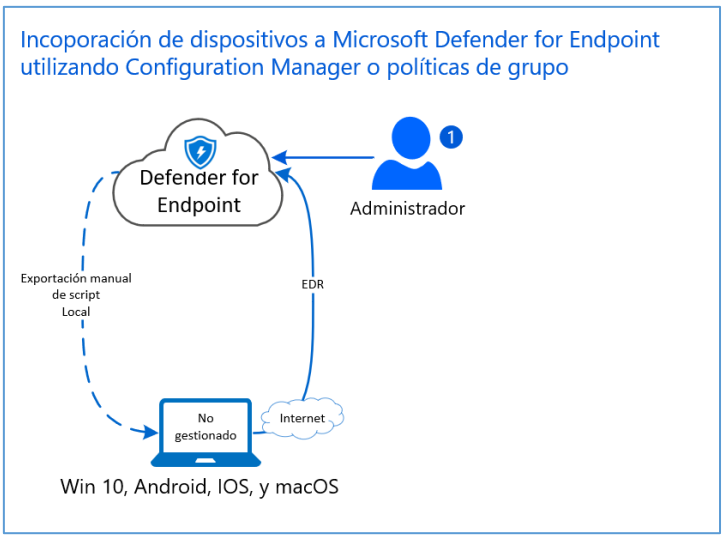
1. Comprobar que los dispositivos que se incorporarán se estén comunicando con el servicio de Configuration Manager o bien extraigan la política de un controlador de dominio.
2. Iniciar sesión en el Centro de seguridad de Microsoft Defender y completar el asistente de configuración inicial.
3. Para realizar la incorporación usando Configuration Manager, ir a la pestaña Onboarding de Microsoft Defender Security Center en la configuración, descargar un paquete de System Center Configuration Manager y desplegarlo en una colección predefinida.

a. Para hacer el onboard o incorporación mediante política de grupo, ir a la pestaña Onboard del Centro de seguridad de Microsoft Defender en la configuración, descargar un paquete de políticas de grupo, crear un programa en la Consola de administración de políticas de grupo e indicar que ejecute una tarea para ejecutar el script de incorporación como un programa.

4. Para verificar que los dispositivos están correctamente integrados y generando informes, ejecutaremos una prueba de detección en los dispositivos recién incorporados. Estos comandos se encuentran en la configuración del Centro de seguridad de Microsoft Defender en la sección **Onboarding**.

2.3.1.4 SCRIPT Y EVALUACIÓN

El siguiente método de despliegue se realiza mediante script local.



1. Iniciar sesión en el Centro de seguridad de Microsoft Defender y completar el asistente de configuración inicial.
2. Ir a la pestaña **Onboarding** del Centro de seguridad de Microsoft Defender en la configuración, seleccionamos el sistema operativo apropiado y descargar un script local.
3. Copiar el script en los dispositivos que queremos incorporar y lo ejecutamos localmente.
4. Para verificar que los dispositivos están correctamente integrados y generando informes, ejecutaremos una prueba de detección en los dispositivos recién incorporados. Estos comandos se encuentran en la configuración del Centro de seguridad de Microsoft Defender en la sección **Onboarding**.

2.3.2 SELECCIONAR MÉTODO DE IMPLEMENTACIÓN

Defender for Endpoint admite una variedad de puntos de conexión que se pueden incorporar al servicio.

En la tabla siguiente se enumeran los puntos de conexión admitidos y la herramienta de implementación correspondiente:

Extremo	Herramienta de implementación
Windows	Script local (hasta 10 dispositivos) Directiva de grupo Microsoft Intune/ Administrador de dispositivos móviles Microsoft Endpoint Configuration Manager Scripts VDI
macOS	Script local Microsoft Intune Jamf Pro Administración de dispositivos móviles
Servidores Windows **Servidores Linux**	Integración con Microsoft Defender para la nube
Servidor Linux	Script local Puppet Ansible
iOS	Basado en aplicaciones
Android	Microsoft Intune

Para más información sobre los métodos de implementación, revisar el siguiente enlace:

Identificación de la arquitectura y el método de implementación de Defender para punto de conexión - Microsoft Defender for Endpoint | Microsoft Learn

2.4 INCORPORACIÓN DE DISPOSITIVOS EN MICROSOFT DEFENDER FOR ENDPOINT

Este punto de la configuración puede cambiar dependiendo del método elegido en el punto anterior para la implementación.

La recomendación a la hora de afrontar una incorporación de dispositivos en Microsoft Defender para Endpoint es realizar la implementación utilizando un enfoque basado en anillos.

Un método basado en anillos es una forma de seleccionar un grupo de puntos finales para integrar y comprobar que se satisfacen ciertas condiciones antes de continuar con el despliegue del servicio en un número mayor de dispositivos.

2.5 CONFIGURAR LAS FUNCIONALIDADES

Después de incorporar puntos de conexión, se recomienda configurar las funcionalidades de seguridad en *Defender for Endpoint* para maximizar la protección de seguridad en el conjunto de servidores. Las funcionalidades incluyen:

- EDR (Endpoint Detection and Response)
- Defender Vulnerability Management
- Protección de última generación
- Reducción de la superficie expuesta a ataques
- Capacidades de investigación y remediación automática (AIR)
- Microsoft Experts

2.5.1 EDR (ENDPOINT DETECTION AND REPONSE)

Defender for Endpoint ofrece funciones de detección y respuesta de endpoints que alertan de forma rápida y útil sobre los ataques avanzados. Los analistas de seguridad pueden ordenar las alertas según su importancia, ver el alcance total de una intrusión y tomar medidas de respuesta para eliminar las amenazas.

Para más información sobre este apartado, revisar el siguiente enlace:

Introducción a las funcionalidades de detección y respuesta de puntos de conexión - Microsoft Defender for Endpoint | Microsoft Learn

2.5.2 DEFENDER VULNERABILITY MANAGEMENT

Defender Vulnerability Management permite ver los activos, realizar evaluaciones inteligentes y usar herramientas de corrección integradas para Windows, macOS, Linux, Android, iOS y dispositivos de red. Con la información de las amenazas de Microsoft, las predicciones de las posibilidades de brechas, los contextos comerciales y las evaluaciones de los dispositivos, Defender Vulnerability Management ordena rápidamente y de forma continua las vulnerabilidades más graves en sus activos más importantes y ofrece recomendaciones de seguridad para reducir el riesgo.

Las herramientas avanzadas que ayudan a comprender y evaluar los riesgos son las siguientes:

- Evaluación de líneas de base de seguridad: diseño de perfiles de línea de base a medida para evaluar el cumplimiento de riesgos según criterios definidos.
- Conocimiento del software y de sus riesgos: acceso a una visión del inventario de software de la organización y de las modificaciones del software, como instalaciones, desinstalaciones y actualizaciones.
- Análisis de recursos compartidos de red: análisis de la configuración de redes internas que tengan recursos compartidos expuestos a riesgos y posibilidad de sugerencias de seguridad aplicables.
- Análisis autenticado para Windows: escaneo de forma periódica los dispositivos Windows no administrados para detectar vulnerabilidades de software.
- Evaluación de vulnerabilidades y ordenamiento de eventos: uso de ordenamientos de eventos y análisis de vulnerabilidades a nivel de entidad para identificar y jerarquizar las vulnerabilidades.
- Revisión de las extensiones del navegador: consultas sobre listas de las extensiones del navegador que se usan en los distintos navegadores de la organización.
- Revisión de certificados digitales: consultas sobre los certificados que están instalados en la organización en una página centralizada de inventario de certificados.
- Revisión de hardware y firmware: consultas sobre la lista de hardware y firmware conocidos en la organización clasificados por modelos de sistema, procesadores y BIOS.

2.5.3 PROTECCIÓN DE ÚLTIMA GENERACIÓN

La protección de última generación se basa en Microsoft Defender Antivirus, que es una solución antimalware integrada que proporciona protección de última generación para computadoras de escritorio, laptops y servidores.

Esta herramienta incluye:

- Un sistema de protección basado en la nube que detecta y bloquea rápidamente las amenazas nuevas y emergentes.
- Análisis constante mediante seguimiento avanzado del comportamiento de procesos y archivos y otras técnicas (también llamado "protección en tiempo real").
- Protección especializada basada en aprendizaje automático, análisis de datos masivos con intervención humana y automática e investigación avanzada de resiliencia frente a amenazas.

2.5.4 REDUCCIÓN DE LA SUPERFICIE EXPUESTA A ATAQUES

Las superficies de ataque son los puntos débiles de la organización donde puede ser atacada por ciberamenazas. Defender for Endpoint ofrece varias funcionalidades para ayudar a disminuir las superficies de ataque.

Entre las más importantes se encuentran:

- Las reglas de reducción de superficie de ataques
- Protección contra exploits
- Protección de red
- Acceso controlado a carpetas
- Control del dispositivo.

2.5.4.1 REGLAS DE SUPERFICIE DE ATAQUE

Las reglas de reducción de la superficie de ataque se centran en algunos aspectos del comportamiento del software.

El software a veces muestra estos comportamientos en aplicaciones que son legítimas. Sin embargo, estos comportamientos a menudo se consideran de riesgo porque los atacantes suelen abusar de ellos mediante malware. Las reglas de reducción de la superficie de ataque pueden limitar los comportamientos de riesgo basados en el software y ayudar a mantener segura la organización.

Una guía paso a paso sobre cómo gestionar las reglas de reducción de la superficie de ataque se puede consultar en los enlaces de cada punto:

- Descripción general de la implementación de reglas de reducción de la superficie de ataque.

  Microsoft Defender para punto de conexión introducción a la implementación de reglas de reducción de superficie expuesta a ataques - Microsoft Defender for Endpoint | Microsoft Learn

- Planificar la implementación de reglas de reducción de la superficie de ataque.

  Planeación de la implementación de reglas de reducción de superficie expuesta a ataques - Microsoft Defender for Endpoint | Microsoft Learn

- Pruebas sobre las reglas de reducción de la superficie de ataque.

  Reglas de reducción de superficie expuesta a ataques de prueba - Microsoft Defender for Endpoint | Microsoft Learn

- Habilitar reglas de reducción de la superficie de ataque.

  Implementar las reglas de reducción de la superficie expuesta a ataques - Microsoft Defender for Endpoint | Microsoft Learn

- Poner en práctica las reglas de reducción de la superficie de ataque.

  Operacionalización de las reglas de reducción de superficie expuesta a ataques - Microsoft Defender for Endpoint | Microsoft Learn

2.5.5 CAPACIDADES DE INVESTIGACIÓN Y REMEDIACIÓN AUTOMÁTICA (AIR)

Al usar esta característica se puede ahorra mucho tiempo ya que, esta herramienta imita la estrategia ideal que seguiría un analista de seguridad para investigar y remediar amenazas.

Se puede ajustar el nivel de automatización de la herramienta para que, al detectar una amenaza, la entidad se pueda corregir de forma automática o solo con el visto bueno del equipo de seguridad.

Para más información sobre la herramienta, consulte:

Configuración de funcionalidades automatizadas de investigación y corrección - Microsoft Defender for Endpoint | Microsoft Learn

2.5.6 MICROSOFT DEFENDER EXPERTS FOR HUNTING

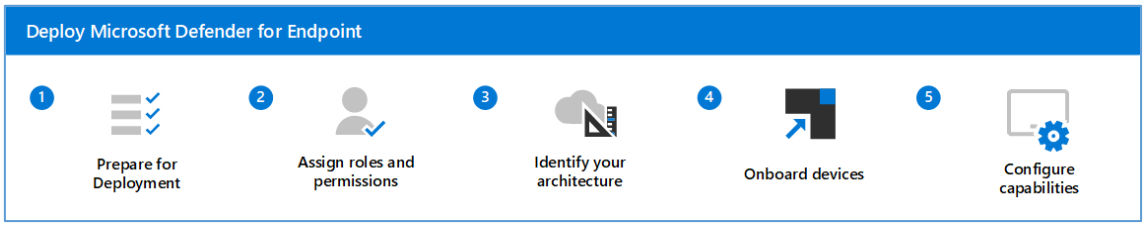
Es un servicio administrado que está pensado para organizaciones que cuentan con un centro de operaciones de seguridad robusto pero que quieren que Microsoft les apoye en la detección proactiva de amenazas usando datos de Microsoft Defender.

Para más información, acceder a la documentación oficial de Microsoft.

¿Qué es Expertos de detección de Microsoft Defender oferta? - Microsoft Defender XDR | Microsoft Learn

2.6 FASES DE IMPLEMENTACIÓN

Como hemos visto en el punto anterior el despliegue de *Microsoft Defender for Endpoint* comprende cinco fases principales que son preparación para el despliegue, asignación de roles y permisos, identificación de la infraestructura, incorporación de dispositivos y configuración de funcionalidades, tal y como se puede ver en la siguiente imagen.



Para la correcta implementación de la herramienta se han resumido estas cinco fases en tres, haciendo así la implementación más simple y segura.

2.6.1 PREPARACIÓN

La preparación es clave para realizar una implementación correcta. Aquí se exponen los puntos que se deben tener en cuenta para preparar una implementación de Defender for Endpoint.

Partes interesadas y aprobación

En primer lugar, habrá que identificar a todas las partes interesadas que participan en el proyecto y necesitan aprobar, revisar o mantenerse informados. Para ello se recomienda confeccionar la siguiente tabla en donde quedará reflejado.

La siguiente sección sirve para identificar a todas las partes interesadas que participan en el proyecto y necesitan aprobar, revisar o mantenerse informados.

En la tabla siguiente, se añadirá al personal interesado, según corresponda a nuestra compañía. Según la acción a desempeñar, hay tres roles bien diferenciados que son:

- SO = Aprobar proyecto
- R = Revisar este proyecto y proporcionar entrada
- I = Informado de este proyecto

Nombre	Función	Acción
Nombre y correo electrónico	**Director de seguridad de la información (CISO)** Representante ejecutivo que actúa como patrocinador dentro de la organización para la nueva implementación de tecnología.	SO
Nombre y correo electrónico	**Jefe del Centro de operaciones de Ciberdefensa (CDOC)** Representante del equipo CDOC encargado de definir cómo se alinea este cambio con los procesos del equipo de operaciones de seguridad de clientes.	SO
Nombre y correo electrónico	**Arquitecto de Seguridad** Representante del equipo de seguridad encargado de definir cómo se alinea este cambio con la arquitectura de seguridad principal de la organización.	R
Nombre y correo electrónico	**Workplace Architect** Representante del equipo de IT encargado de definir cómo se alinea este cambio con la arquitectura básica del lugar de trabajo de la organización.	R
Nombre y correo electrónico	Se pueden ver las alertas generadas desde dispositivos de las organizaciones.	I

Entorno

Garantiza que las partes interesadas entienden el entorno, lo que ayuda a identificar posibles dependencias o cambios necesarios en tecnologías o procesos.

Qué	Descripción
Recuento de extremos	Recuento total de puntos de conexión por sistema operativo.

Recuento de servidores	Recuento total de servidores por versión del sistema operativo.
Motor de administración	Nombre y versión del motor de administración (por ejemplo, System Center Configuration Manager rama actual 1902).
Distribución de CDOC	Estructura CDOC de alto nivel (por ejemplo, nivel 1 subcontratado a la empresa X, nivel 2 y nivel 3 internamente distribuidos en Europa y Asia).
Información de seguridad y evento (SIEM)	Tecnología SIEM en uso.

Control de acceso basado en roles

Se recomienda usar el concepto de privilegios mínimos. *Defender for Endpoint* aprovecha los roles integrados dentro de Microsoft Entra y se recomienda revisar los diferentes roles disponibles y elegir el adecuado para resolver las necesidades para cada persona de la aplicación.

Más información en la sección [3.1.2 Control de acceso] de la presente guía.

Orden de adopción

En muchos casos, suele haber implementadas soluciones de seguridad endpoint o al menos una solución de antivirus como mínimo, pero en otros, también podría haber implementada ya una solución EDR.

Normalmente, sustituir cualquier solución de seguridad solía ser un proceso complejo, tedioso y alargado en el tiempo debido a los nulos vínculos entre la capa de infraestructura y la capa de aplicaciones. Sin embargo, puesto que Defender for endpoint está integrado en el sistema operativo, es mucho más sencillo reemplazar soluciones de terceros.

En este caso, se podrá elegir el componente de Defender for endpoint que se va a utilizar y quitar los que no se apliquen. En la tabla siguiente se indica el orden que recomendado que se debe seguir para habilitar la solución de *Microsoft Defender for Endpoint*.

Componente	Descripción	Clasificación de orden de adopción
Detección de Endpoint & Respuesta (EDR)	Las capacidades de defender para detección y respuesta de puntos de conexión endpoint proporcionan detecciones avanzadas de ataques que son casi en tiempo real y procesables. Los analistas de seguridad pueden asignar prioridades a las alertas de forma eficaz, obtener visibilidad para todo el ámbito de la vulneración	1

	y llevar a cabo acciones de respuesta para corregir las amenazas.	
Amenazas & Administración de vulnerabilidades (TVM)	Threat & Vulnerability Management es un componente de Microsoft Defender for endpoint y proporciona a los administradores de seguridad y a los equipos de operaciones de seguridad un valor único, incluyendo: - Información en tiempo detección y respuesta de puntos de conexión (EDR) correlacionada con vulnerabilidades de punto de conexión - Contexto de vulnerabilidad de dispositivo incalculable durante investigaciones de incidentes - Procesos de corrección integrados mediante Microsoft Intune y Microsoft System Center Configuration Manager	2
Protección de última generación (NGP)	Antivirus de Microsoft Defender es una solución antimalware integrada que proporciona protección de última generación para escritorios, equipos portátiles y servidores. El Antivirus de Microsoft Defender incluye: - Protección entregada en nube para la detección casi instantánea y bloqueo de amenazas nuevas y emergentes. Junto con Intelligent Security Graph y el aprendizaje automático, la protección en la nube forma parte de las tecnologías de última generación utilizadas por el Antivirus de Microsoft Defender. - Análisis continuo mediante la supervisión avanzada del comportamiento de procesos y archivos y otras heurísticas (también conocida como "protección en tiempo real"). - Actualizaciones de protección dedicadas basadas en machine learning, análisis de big data automatizado e investigación detallada de resistencia a amenazas.	3
Reducción de superficie de ataque (ASR)	Las capacidades de reducción de ataque de superficie en Microsoft Defender for endpoint ayudan a proteger los dispositivos y aplicaciones de la compañía frente a amenazas nuevas y emergentes.	No aplicable
Auto Investigation & Remediation (AIR)	Microsoft Defender for endpoint usa investigaciones automatizadas para reducir significativamente el volumen de alertas que deben investigarse individualmente. La característica de investigación automatizada aprovecha varios algoritmos de inspección y procesos usados por analistas, como playbooks, para examinar alertas y tomar medidas de corrección inmediatas para resolver infracciones. Esto reduce considerablemente el volumen de alertas, lo que facilita que los expertos de operaciones de seguridad	No aplicable

	puedan centrarse en amenazas más complejas y otras iniciativas de alto valor.	
Expertos en amenazas de Microsoft (MTE)	Expertos en amenazas de Microsoft es un servicio de búsqueda administrado que proporciona a los Centros de operaciones de seguridad (SOC) supervisión y análisis de nivel de experto para ayudarles a garantizar que las amenazas críticas en sus entornos únicos no se pierden.	No aplicable

2.6.2 CONFIGURACIÓN

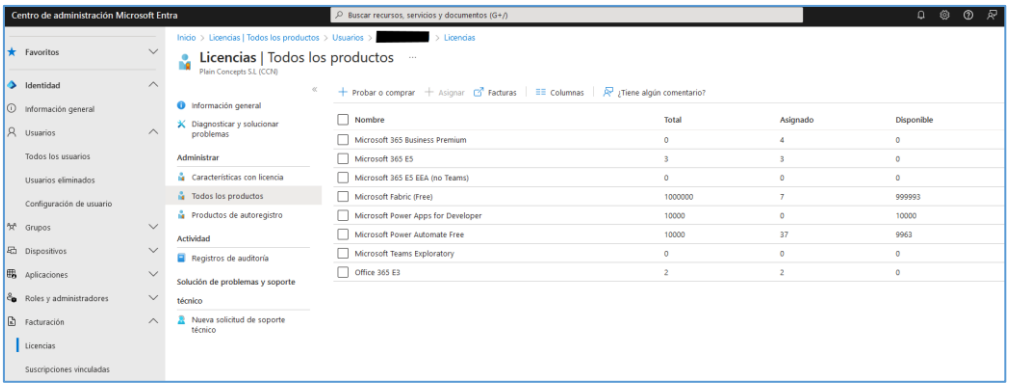
Pasos iniciales para tener acceso al portal, como validar licencias, completar el asistente de instalación y configuración de red.

Nota: Con el fin de mostrar una implementación típica, este escenario solo abarcará el uso de Script local. Defender for Endpoint admite el uso de otras herramientas de incorporación, pero no cubrirá esos escenarios en la guía de implementación.

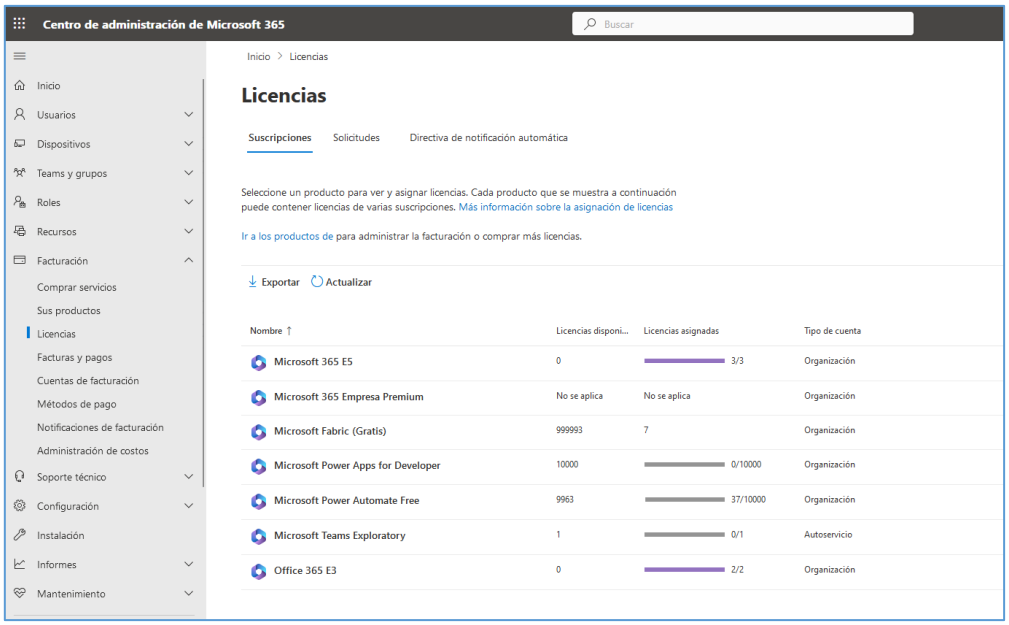
Comprobar el estado de la licencia

Comprobar el estado de la licencia y si se aprovisionó correctamente, se puede realizar a través del Centro de administración o a través del portal Microsoft Entra.

Para acceder a las licencias, entrar al portal de Azure, Entra y a continuación seleccionar **Facturación > licencias**.



Como alternativa, se puede acceder desde el *Centro de Administración de Microsoft 365*:



Configuración del espacio empresarial

Desde un explorador web, acceder al Centro Microsoft 365 seguridad.

https://security.microsoft.com/

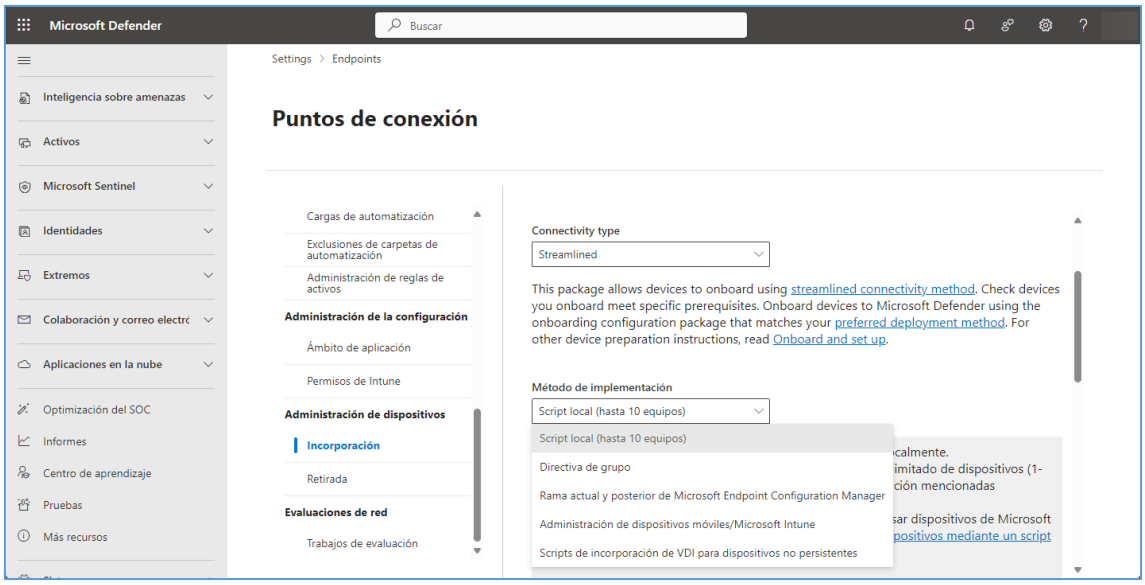
Configuración de red

Si la organización no requiere que los puntos de conexión usen un proxy para tener acceso a Internet, omitir esta sección. En caso contrario, obtener información completa en la documentación de Microsoft:

Configuración de Microsoft Defender para punto de conexión implementación - Microsoft Defender for Endpoint | Microsoft Learn

2.6.3 INCORPORACIÓN (ONBOARD)

Después de identificar la arquitectura, hay que decidir qué método de implementación usar. La herramienta de implementación que se elija influye en la forma en que se incorporan puntos de conexión al servicio.



Nota: Consultar los distintos métodos de implementación en la sección [2.3.2 Seleccionar método de implementación].

2.7 DESPLIEGUE PASO A PASO CON SCRIPTING LOCAL

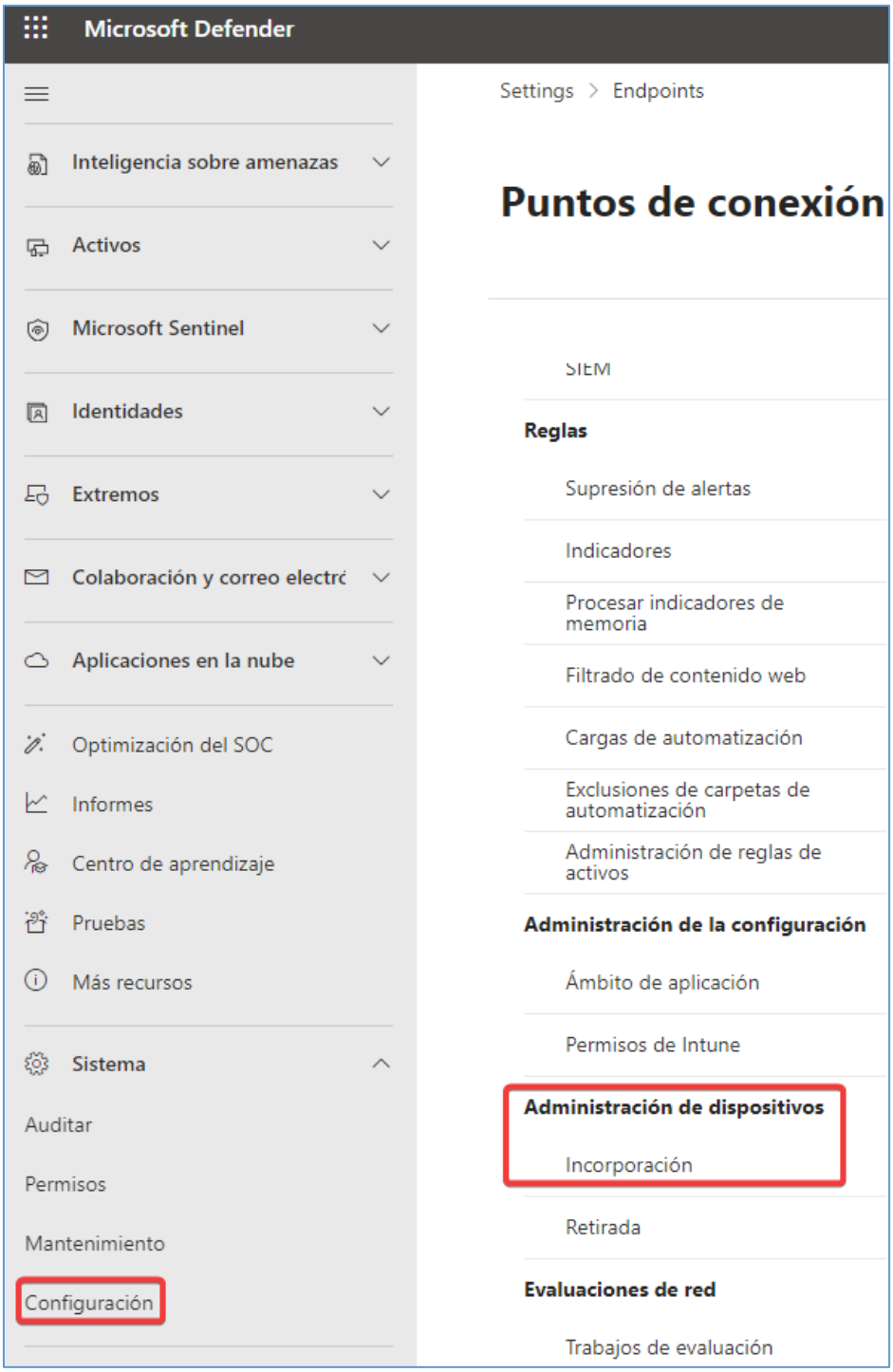
A continuación, se explica, a modo de ejemplo, un despliegue paso a paso con el método de implementación de "Script local".

Existen otros métodos de despliegue, como se detalla en la sección [2.3.2 Seleccionar método de implementación].

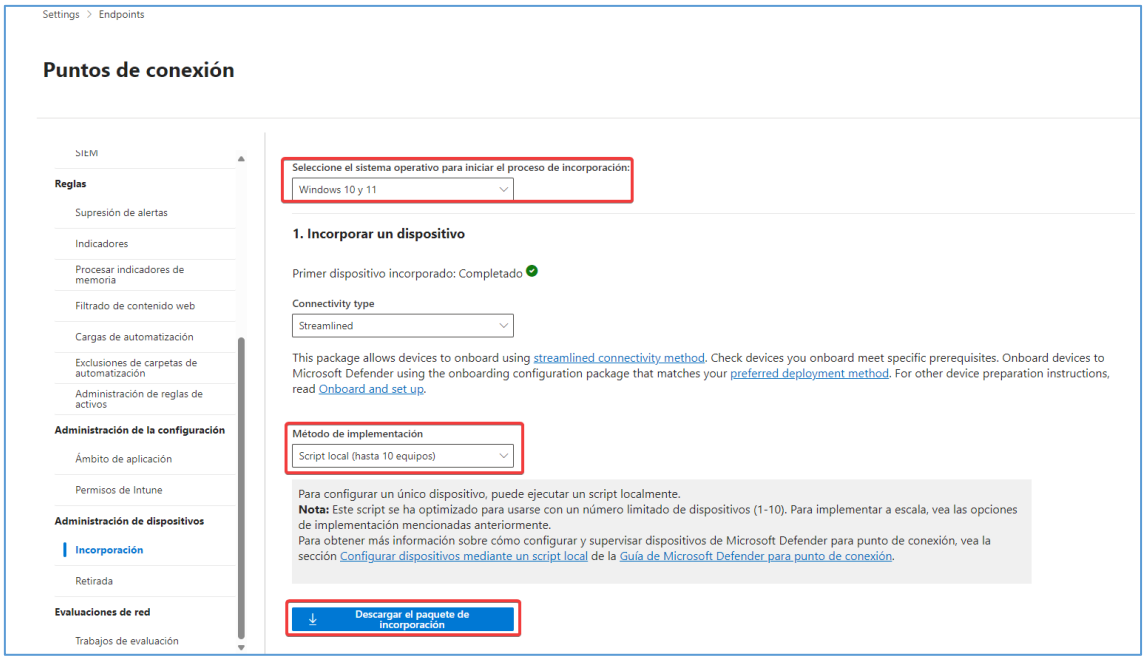
2.7.1 SCRIPT LOCAL PARA WINDOWS 10/11

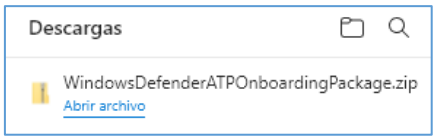
Cuando se ejecuta el script de incorporación en un dispositivo, se establece una confianza con Microsoft Entra ID (si no existe previamente), se registra el dispositivo en Microsoft Intune (si no está registrado todavía) y, luego, se incorpora el dispositivo a Defender for Business.

1. Acceder al Centro de Seguridad con las credenciales de acceso.
2. En el panel de navegación, elegir **Configuracion > Endpoints**, y, a continuación, elegir **Incorporación**.



3. Seleccionar Windows 10 y 11 y, a continuación, en la sección **Método de implementación**, elegir **Script local**.
4. Seleccionar Descargar el paquete de incorporación. Se recomienda guardar el paquete de incorporación en una unidad extraíble.





2.7.1.1 ONBOARDING DE DISPOSITIVOS

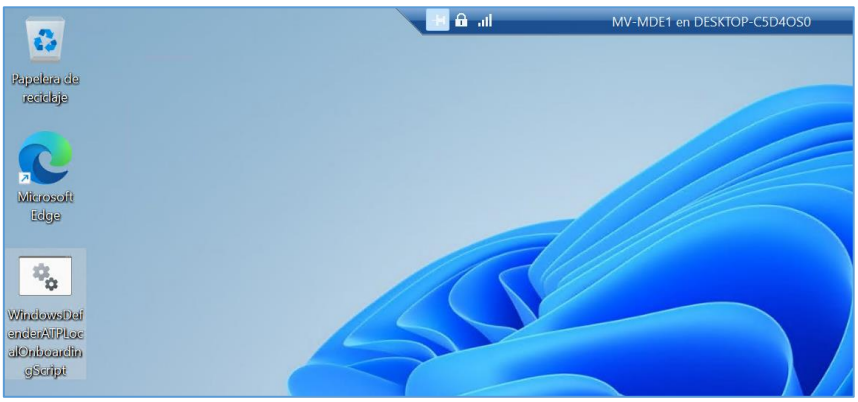
Siguiendo el orden de configuración anterior:

5. Acceder al dispositivo a incorporar y ejecutar el sw. descargado.

En este paso se ejecutará el script para incorporar un dispositivo. Deberá ejecutarse en tantos dispositivos como sea necesario. Para el escenario que se está presentando, se ejecutará en una máquina con Windows 11.

Nota: Para este escenario se utilizará una máquina virtual de HyperV, con sistema operativo Windows 11 Pro.

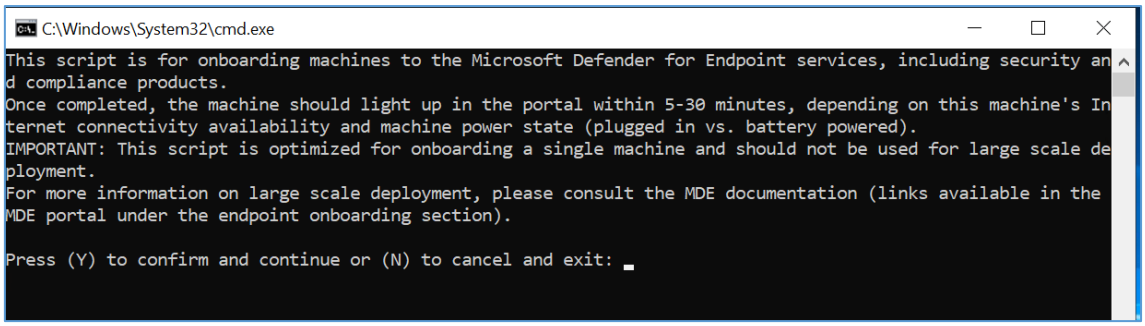
Para saber los dispositivos compatibles y resto de requerimientos consultar la sección [1. 7 Prerrequisitos Microsoft Defender for Endpoint].



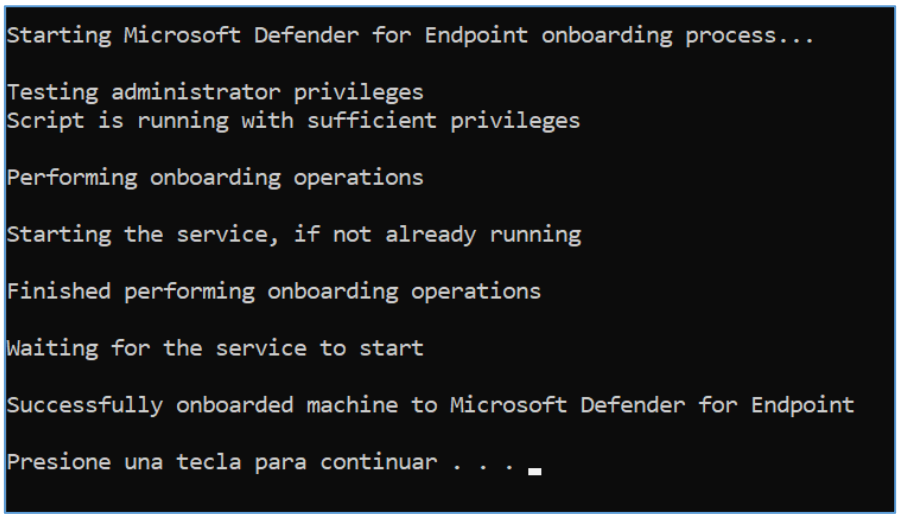
Ejecutar el archivo con privilegios de administración:

WindowsDefenderATPLocalOnboardingScript.cmd

A continuación, pulsar "Y":



Comienza el proceso de Onboarding de Microsoft Defender for Endpoint:



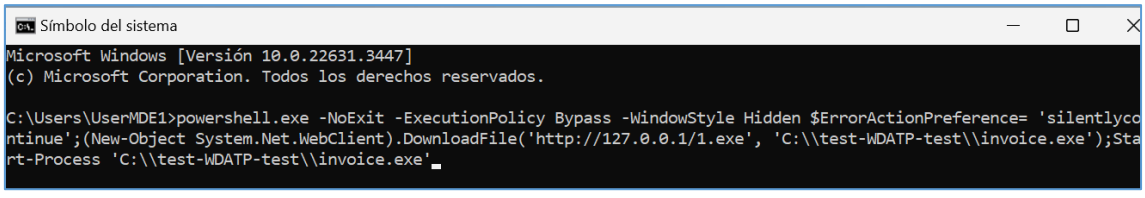
Pulsar cualquier tecla para finalizar.

La máquina aparecerá en el portal entre 5-30 minutos después.

6. Comprobar que el dispositivo ha sido agregado adecuadamente:

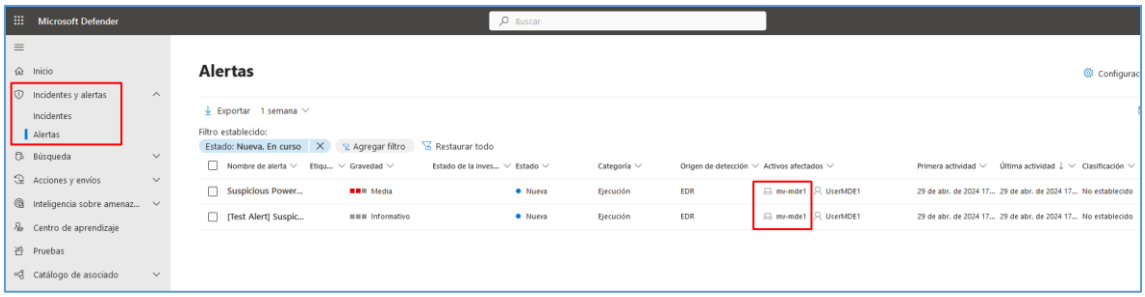
   Ejecutar el siguiente comando en el dispositivo incorporado en el paso anterior, en una ventana CMD:

```
powershell.exe -NoExit -ExecutionPolicy Bypass -WindowStyle Hidden $ErrorActionPreference=
    'silentlycontinue';(New-Object System.Net.WebClient).DownloadFile('http://127.0.0.1/1.exe',
    'C:\\test-WDATP-test\\invoice.exe');Start-Process 'C:\\test-WDATP-test\\invoice.exe'
```



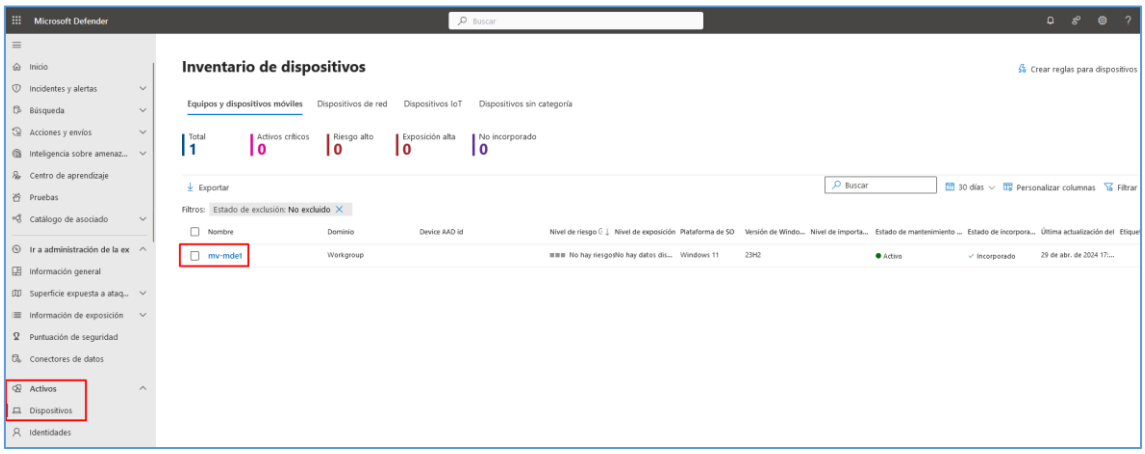
La ventana se cerrará automáticamente.

Si se realizó correctamente, la prueba de detección se marcará como completada y en unos minutos se mostrará una nueva alerta en el portal de Microsoft Defender.



2.7.2 INVENTARIO DE DISPOSITIVOS AGREGADOS

Así, por ejemplo, en "Dispositivos" aparecerá la lista de dispositivos inventariados para Microsoft Defender:



3. CONFIGURACIÓN SEGURA PARA MICROSOFT DEFENDER FOR ENDPOINT

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.

3.1.1.1 IDENTIFICACIÓN

La gestión de identidades de Microsoft Entra ID es común para el acceso a todas las funcionalidades de todo Microsoft 365, lo que también incluye Microsoft Defender para O365 y se describe en la guía [CCN-STIC-885A - Guía de configuración segura para Office 365].

3.1.1.2 REQUISITOS DE ACCESO

Según el ENS, los recursos del sistema se protegerán con algún mecanismo que impida su utilización, salvo a las entidades que disfruten de derechos de acceso suficientes. Además, todos los usuarios autorizados deben tener un conjunto de atributos de seguridad (privilegios) que puedan ser mantenidos individualmente.

Para dar cumplimiento a estos requerimientos, *Defender for Endpoint* dispone de un sistema completo de permisos, administrados de dos formas distintas:

- **Administración de Permisos Básicos:** se establecen permisos de acceso completo o solo lectura. En el caso de la gestión de permisos de usuarios como *Administrador global o Administrador de seguridad* de Azure Active Directory, tendrán acceso completo, mientras que el rol *Lector de seguridad* tiene acceso de solo lectura.
- **Control de acceso basado en roles (RBAC):** Se establecen permisos granulares definiendo roles, asignando grupos de usuarios de Azure AD a los roles y concediendo a los grupos de usuarios acceso a grupos de dispositivos.

Nota: Para obtener información completa sobre la creación de roles RBAC consultar la guía [CCN-STIC-884A - Guía de configuración segura para Azure].

Consideraciones

Si ya se ha asignado permisos básicos, se puede cambiar a RBAC en cualquier momento. Tenga en cuenta lo siguiente antes de realizar el cambio:

- A los usuarios con acceso completo (usuarios a los que se les asigna el rol de directorio Administrador global o Administrador de seguridad en Azure AD), se les asigna automáticamente el rol de administrador de Defender for Endpoint predeterminado, que también tiene acceso completo. Después de cambiar a RBAC, se pueden asignar grupos de usuarios de Azure AD adicionales al rol de administrador Defender for Endpoint. Solo los usuarios asignados al rol de administrador Defender for Endpoint pueden administrar permisos mediante RBAC.
- Los usuarios con acceso de solo lectura (lectores de seguridad) perderán el acceso al portal hasta que se les asigne un rol. Tenga en cuenta que solo se puede asignar un rol a los grupos de usuarios de Azure AD en RBAC.
- Después de cambiar a RBAC, no se podrá volver a usar la administración de permisos básicos.

Es posible que algunos roles deban aplicarse temporalmente y quitarse una vez completada la implementación. Conviene llevar un control con los roles relacionados en la organización, las funciones que realiza, si necesita algún rol adicional de Azure, y las personas físicas a las cuales se les ha asignado:

Rol	Funciones	Rol de Azure AD (si fuese necesario)	Asignar a
Administrador de seguridad			
Analista de seguridad			
Administrador de extremos			
Administrador de infraestructura			
Propietario/stakeholder de la empresa			

Es recomendable utilizar el denominado Privileged Identity Management (PIM) para proporcionar auditoría, control y revisión de acceso adicionales para los usuarios con permisos de directorio.

Se recomienda aprovechar RBAC para asegurarnos de que solo los usuarios que tienen justificación pueden acceder a Defender for Endpoint. La persona responsable del recurso deberá encargarse de administrar los derechos de acceso a los mismos, tal y como se indica en el ENS.

En la siguiente tabla se puede ver un ejemplo de los roles que se podrían asignar a un departamento de seguridad. De esta forma se podría definir una estructura RBAC acorde al entorno.

Nivel	Descripción	Permiso necesario
Nivel 1	**Equipo de operaciones de seguridad local / equipo de TI** Este equipo normalmente realiza una clasificación e investiga las alertas contenidas en la geolocalización y escala al nivel 2 en los casos en los que se requiere una corrección activa.	N/A
Nivel 2	**Equipo de operaciones de seguridad regional** Este equipo puede ver todos los dispositivos de la región y realizar acciones de corrección.	Ver datos
Nivel 3	**Equipo de operaciones de seguridad global** Este equipo está formado por expertos en seguridad y está autorizado a ver y realizar todas las acciones desde el portal.	Ver datos Investigación de alertas Acciones de corrección activas Investigación de alertas Acciones de corrección activas Administrar la configuración del sistema del portal Administrar la configuración de seguridad

3.1.1.3 SEGREGACIÓN DE FUNCIONES Y TAREAS

Según el ENS, el sistema de control de acceso se organizará de forma que se exija la concurrencia de dos o más personas para realizar tareas críticas, anulando la posibilidad de que un solo individuo autorizado, pueda abusar de sus derechos para cometer alguna acción ilícita.

Como se ha comentado en la sección de requisitos de acceso, una forma simplificada de establecer el acceso a la aplicación es mediante la asignación de una serie de permisos básicos englobados en dos roles:

- **Acceso completo**

  Los usuarios con acceso completo pueden iniciar sesión, ver toda la información del sistema y resolver alertas, enviar archivos para un análisis profundo y descargar el paquete de incorporación. La asignación de derechos de acceso completo requiere agregar los usuarios a los roles integrados "Administrador de seguridad" o "Administrador global" de AAD.

- **Acceso de solo lectura**

  Los usuarios con acceso de solo lectura pueden iniciar sesión, ver todas las alertas e información relacionada. No podrán cambiar los estados de alerta, enviar archivos para un análisis profundo o realizar operaciones de cambio de

estado. La asignación de derechos de acceso de solo lectura requiere agregar los usuarios al rol integrado de Azure AD "Lector de seguridad".

También pueden establecerse nuevos roles aún más segregados para tareas específicas, como “acciones de corrección activas” e “investigación de alertas”.

Consultar el apartado [4.1.2 Permisos].

A continuación, se detallan las distintas opciones de permisos:

- **Ver datos**
  - *Operaciones de seguridad*: ver todos los datos de operaciones de seguridad en el portal.
  - *Administración de vulnerabilidades y amenazas*: Ver amenazas y datos de administración de vulnerabilidades en el portal.
- **Acciones de corrección activas**
  - *Operaciones de seguridad*: realizar acciones de respuesta, aprobar o descartar acciones de corrección pendientes, administrar listas permitidas o bloqueadas para automatización.
  - *Amenazas y administración de vulnerabilidades - Control de excepciones:* crear nuevas excepciones y administrar excepciones activas.
  - *Amenazas y administración de vulnerabilidades - Control de remediación:* enviar nuevas solicitudes de corrección, crear *tickets* y administrar las actividades de remediación existentes.
- **Investigación de alertas:** administrar alertas, iniciar investigaciones automatizadas, ejecutar exámenes, recopilar paquetes de investigación, administrar etiquetas de dispositivo y descargar solo archivos portables ejecutables (PE).
- **Administrar la configuración de** sistema del portal: configurar las opciones de almacenamiento, SIEM y la API Intel de amenazas (se aplica globalmente), la configuración avanzada, las cargas automatizadas de archivos, los roles y los grupos de dispositivos
  - Esta configuración solo está disponible en el rol Administrador de *Microsoft Defender for Endpoint* (predeterminado).
- **Administrar la configuración de seguridad en el Centro de seguridad:** configure la configuración de supresión de alertas, administre las exclusiones de carpetas para la automatización, los dispositivos integrados y externos, y administre las notificaciones de correo electrónico, administre el laboratorio de evaluación
- **Capacidades de respuesta en directo:**
  - *Comandos básicos*:
    - Iniciar una sesión de respuesta en directo
    - Realizar comandos de solo lectura de respuesta en directo en dispositivo remoto (excepto copia y ejecución de archivos)
    - Descargar un archivo desde el dispositivo remoto a través de una respuesta en directo
  - *Comandos avanzados*:

- Descargar archivos PE y que no son PE de la página de archivos
- Cargar un archivo al dispositivo remoto
- Ver un script desde la biblioteca de archivos
- Ejecutar un script en el dispositivo remoto desde la biblioteca de archivos

Para la asignación de roles, pueden usarse cualquiera de las siguientes soluciones: *Azure PowerShell* o el *Portal de Azure*.

Establecer roles mediante PowerShell

Seguir estos pasos para asignar roles de seguridad:

- Para obtener acceso de lectura y escritura, se asignan usuarios al rol de administrador de seguridad mediante el siguiente comando:

```
Add-MsolRoleMember -RoleName "Security Administrator" -RoleMemberEmailAddress "secadmin@Contoso.onmicrosoft.com"
```

- Para el acceso de solo lectura, se asignan usuarios al rol de lector de seguridad mediante el siguiente comando:

```
Add-MsolRoleMember -RoleName "Security Reader" -RoleMemberEmailAddress reader@Contoso.onmicrosoft.com
```

Establecer roles mediante el Portal Entra

Comúnmente, se asignan roles de Entra ID a los usuarios desde la página Roles asignados de un usuario. Se puede igualmente configurar que se eleve la idoneidad del usuario cuando sea necesario a un rol mediante Privileged Identity Management (PIM).

Nota: Para obtener información completa consultar la guía [CCN-STIC-884A - Guía de configuración segura para Azure].

3.1.1.4 PROCESO DE GESTIÓN DE DERECHOS DE ACCESO

Según el ENS los derechos de acceso de cada entidad, usuario o proceso deben limitarse.

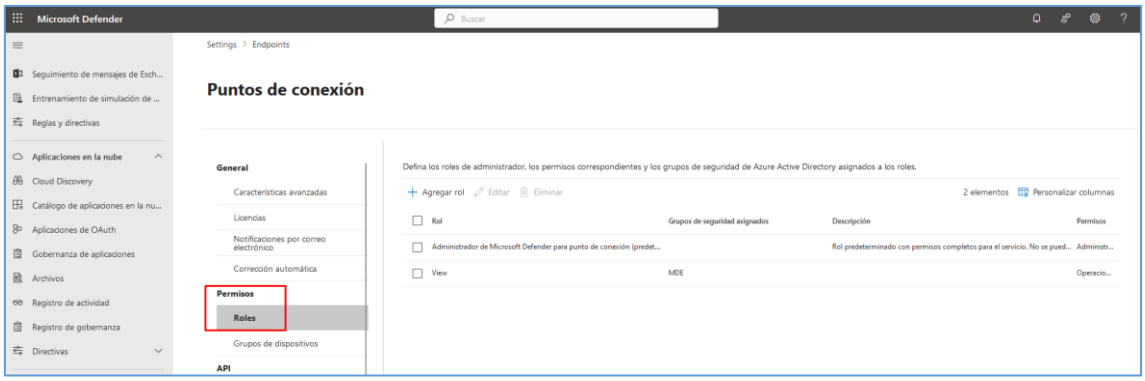
Mediante el acceso condicional de Microsoft Entra, se podrá prohibir el acceso a los servicios de Defender for Endpoint, salvo autorización expresa.

Nota: Para obtener información completa consultar la guía [CCN-STIC-884A - Guía de configuración segura para Azure].

Para lograr el mínimo privilegio posible para el cumplimiento de obligaciones y funciones de los usuarios, entidades o procesos, se hace uso de RBAC, asignando así el rol necesario con el mínimo privilegio posible.

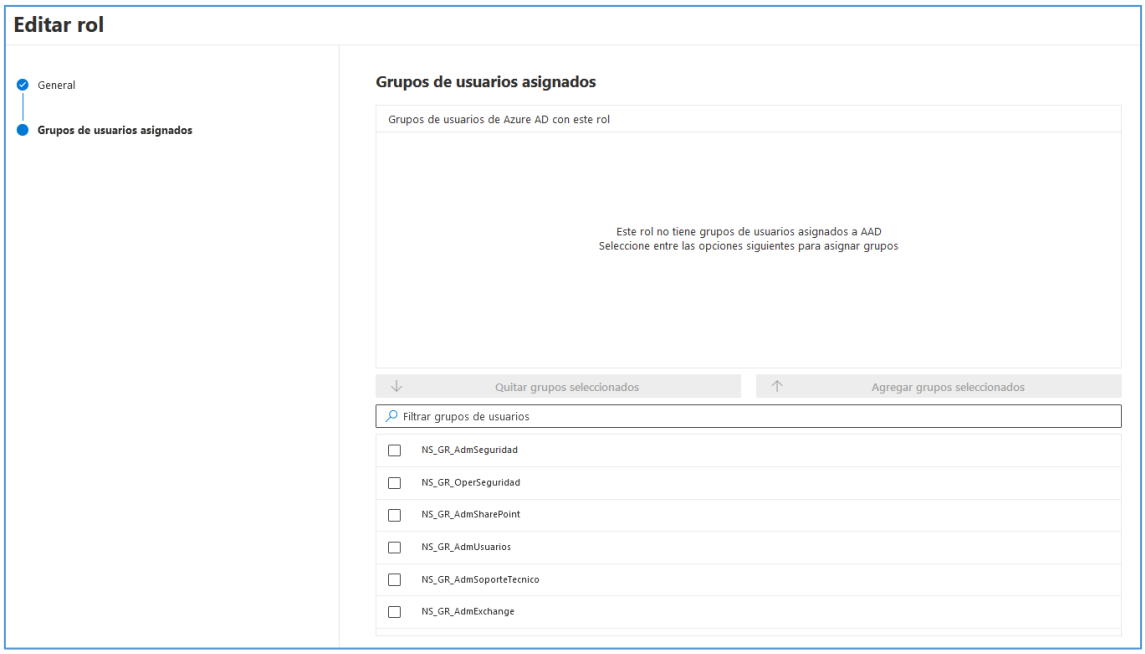
Establecer roles mediante la configuración de Microsoft Defender

En el apartado de **Configuración** del portal de Microsoft Defender, dirigirse a **Puntos de conexión** para definir roles de administrador, permisos y grupos definidos a los roles en el apartado **Permisos -> Roles**.



Una vez en esta pantalla se puede crear el rol que se necesite en cada momento.

Para asignarlo después al grupo de usuarios que se quiera que tengan los roles creados.



Establecer roles mediante PowerShell

Seguir estos pasos para asignar roles de seguridad:

- Para obtener acceso de lectura y escritura, se asignan usuarios al rol de administrador de seguridad mediante el siguiente comando:

```
Add-MsolRoleMember -RoleName "Security Administrator" -RoleMemberEmailAddress "secadmin@Contoso.onmicrosoft.com"
```

- Para el acceso de solo lectura, se asignan usuarios al rol de lector de seguridad mediante el siguiente comando:

```
Add-MsolRoleMember -RoleName "Security Reader" -RoleMemberEmailAddress reader@Contoso.onmicrosoft.com
```

Establecer roles mediante el Portal de Entra ID

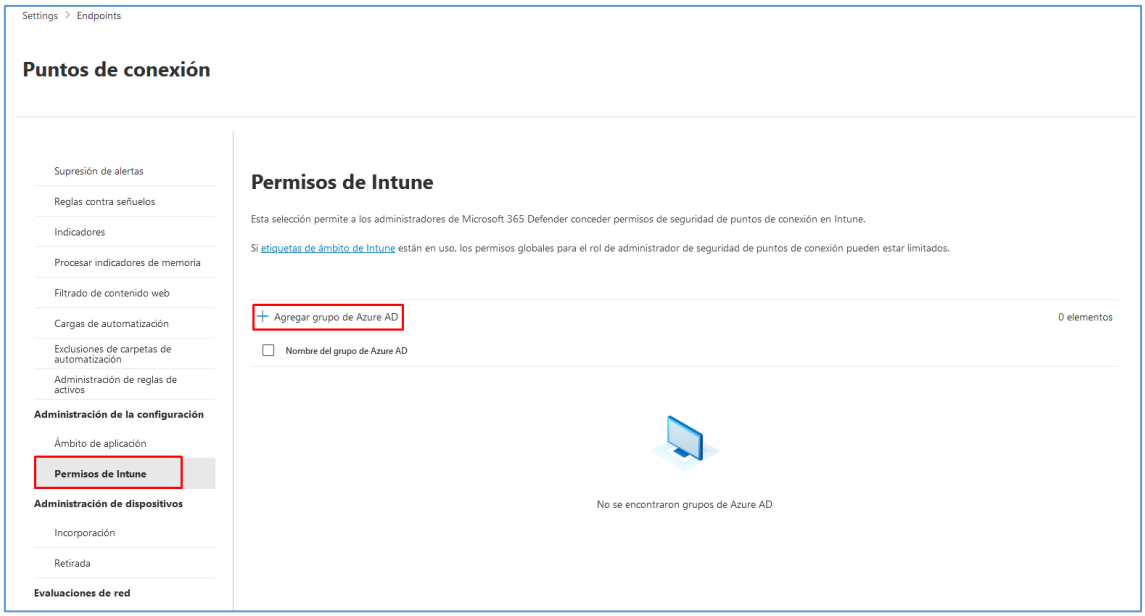
Comúnmente, se asignan roles de Entra ID a los usuarios desde la página Roles asignados de un usuario. Se puede igualmente configurar que se eleve la idoneidad del usuario cuando sea necesario a un rol mediante Privileged Identity Management (PIM).

Para obtener información completa sobre la creación de roles RBAC consultar la guía [CCN-STIC-884A - Guía de configuración segura para Azure].

En el siguiente apartado se puede permitir a los administradores de Microsoft Defender conceder permisos de seguridad de puntos de conexión en Microsoft Intune.

Para ello, se debe acceder al apartado de **Configuración** del portal de Microsoft Defender, dirigirse a **Puntos de conexión**, **Administración de la configuración** y **Permisos de Intune**.

Aquí se podrá agregar un grupo de Entra ID, ese grupo tendrá permisos para la configuración de directivas de punto de conexión en el portal de Microsoft Intune.



3.1.1.5 MECANISMOS DE AUTENTICACIÓN (USUARIOS EXTERNOS)

El acceso remoto se entiende como el acceso remoto al realizado desde fuera de las propias instalaciones de la organización, a través de redes de terceros. Se recomienda reforzar la seguridad:

- Equipos administrados.

  Al tener el acceso solo a los equipos administrados se evitan accesos desde equipos que no pertenecen a la organización.

- Autenticación de doble factor.

  Este proceso securizará el acceso remoto, protegiendo así los inicios de sesión en todo momento.

- Conformidad de dispositivos.

  Al asegurar que los dispositivos cumplan con las directivas de cumplimiento asignadas, se asegura que el acceso remoto desde esos equipos será seguro.

- Ubicaciones de confianza.

  Con las ubicaciones seguras de las políticas de acceso condicional, se asegura que solo desde una localización confiable se conectarán los usuarios.

- Evitar accesos de usuarios sin licenciamiento.

  Al evitar el acceso a usuarios sin licencia, se evitará de manera indirecta a todos los usuarios que no pertenezcan a la organización.

- Información derechos usuario.

  El sistema informará al usuario de sus derechos u obligaciones inmediatamente después de obtener el acceso.

- Credenciales.

Las credenciales se cambiarán con una periodicidad marcada por la política de seguridad de la organización.

- Otras medidas a través de acceso condicional.

  El número de intentos permitidos será limitado, bloqueando la oportunidad de acceso una vez superado tal número, y requiriendo una intervención específica para reactivar la cuenta, que se describirá en la documentación.

La configuración de las medidas de seguridad mencionadas en los puntos anteriores se puede consultar en la guía [CCN-STIC-884A - Guía de configuración segura para Azure].

3.1.1.6 MECANISMOS DE AUTENTICACIÓN (USUARIOS DE LA ORGANIZACIÓN)

Se entiende como *acceso local* al acceso al servicio desde la red corporativa o sedes autorizadas, aunque el servicio se encuentra alojado en las instalaciones del fabricante (nube).

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, como se describe en la guía [CCN-STIC-884A - Guía de configuración segura para Azure].

El acceso remoto se entiende como acceso desde Internet (cualquier IP). Se recomienda reforzar la seguridad cuando se accede desde Internet (*solo equipos administrados*, *MFA*, *conformidad de dispositivos*, etc.).

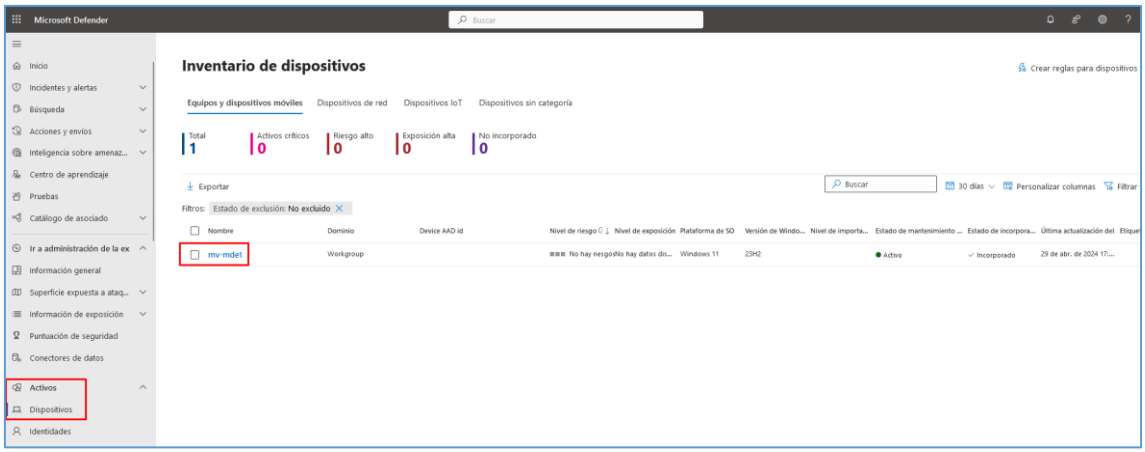
Más información en la guía [CCN-STIC-884A - Guía de configuración segura para Azure].

3.1.2 EXPLOTACIÓN

En esta sección se detallan aspectos relevantes de Microsoft Defender for Endpoint en cuanto a la Explotación de los recursos. Para acceder a información detallada de todas las 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 dispositivos endpoints agregados a la plataforma de seguridad, accediendo al portal unificado Microsoft Defender XDR [Extremos|Inventario de dispositivos]:



Detección de dispositivos

Proteger el entorno requiere realizar un inventario de los dispositivos que están en la red. Sin embargo, la asignación de dispositivos en una red a menudo puede ser costosa, desafiante y consume mucho tiempo.

Microsoft Defender for Endpoint proporciona una funcionalidad de detección de dispositivos que ayuda a encontrar dispositivos no administrados conectados a la red corporativa sin necesidad de dispositivos adicionales o cambios engorrosos en el proceso.

La funcionalidad de detección de dispositivos permite:

- ***Detectar puntos de conexión empresariales conectados a la red corporativa***

  Con las opciones de detección básicas o estándar, puede detectar estaciones de trabajo, servidores y puntos de conexión móviles que aún no están incorporados a Microsoft Defender para endpoint.

- ***Extremos detectados incorporados***

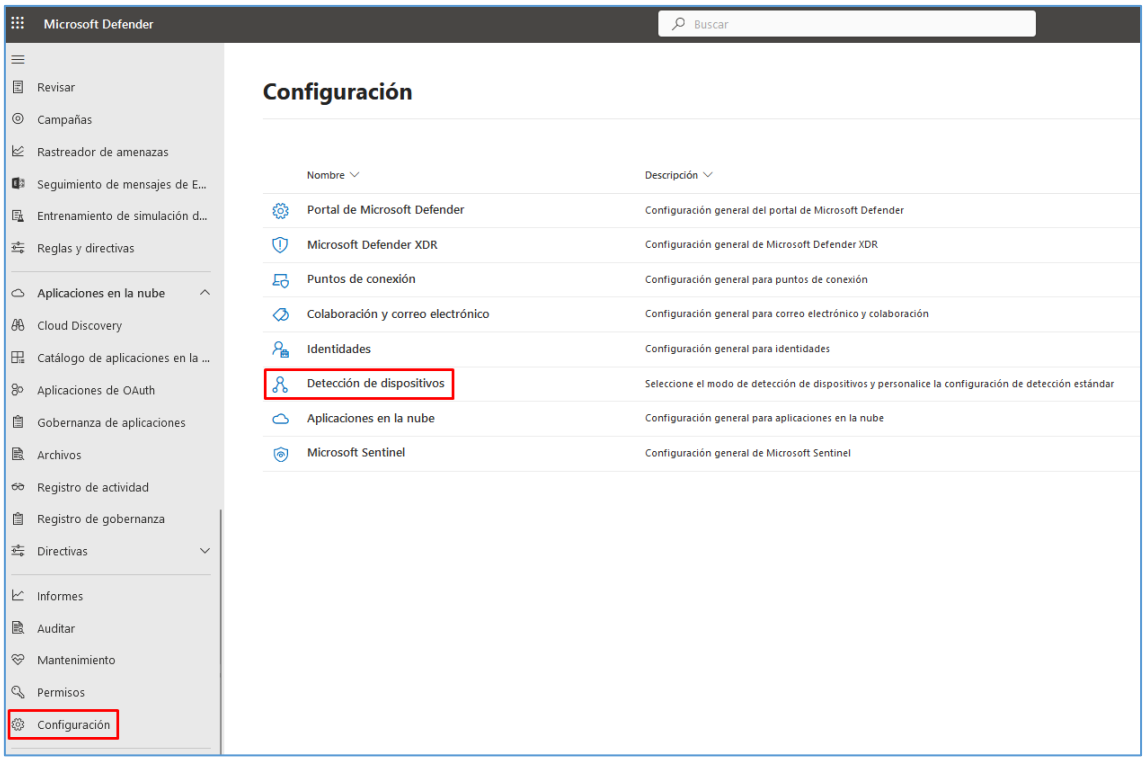
  Los puntos de conexión no administrados de la red pueden introducir vulnerabilidades y riesgos en la red. Incorporarlos al servicio puede aumentar la visibilidad de seguridad en ellos.

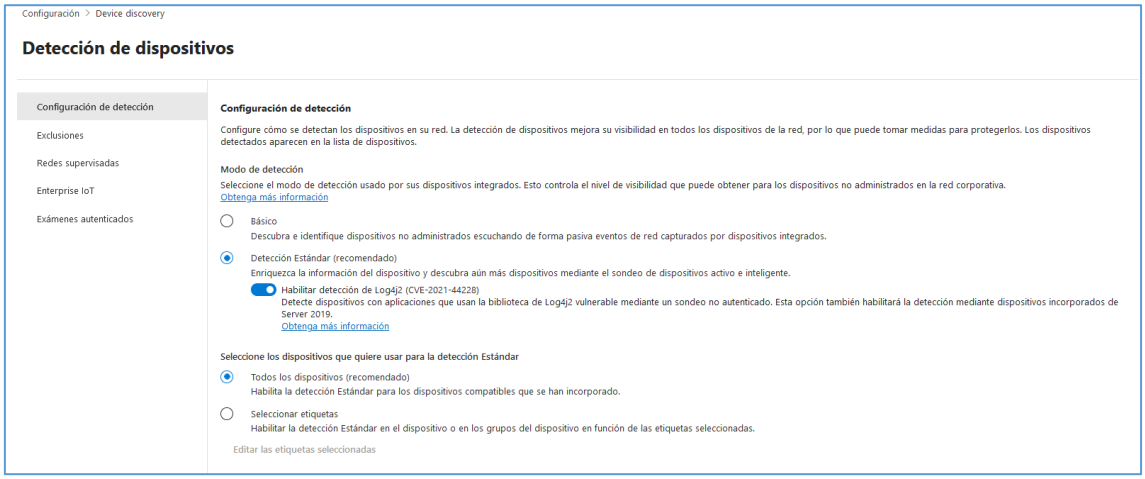
Métodos de detección

Hay dos modos de detección:

- Detección básica
- Detección estándar (recomendado)

Se puede cambiar y personalizar la configuración de detección, para obtener más información, consultar [Configuración | Detección de dispositivos]:

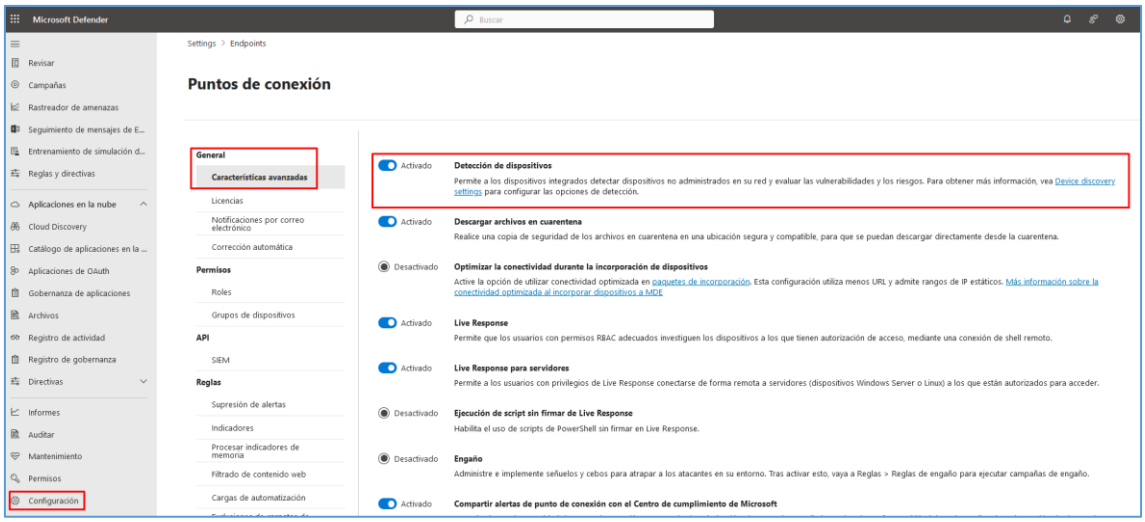




Detección de dispositivos no administrados

Esta opción permite a los dispositivos integrados detectar dispositivos no administrados en su red y evaluar las vulnerabilidades y los riesgos.

Para habilitarla, en el apartado **Configuración** del portal de Microsoft Defender, **Puntos de conexión > General > Características avanzadas**, habilitar la opción **Detección de dispositivos**.



3.1.2.2 CONFIGURACIÓN DE SEGURIDAD

Según el ENS, se configurarán los equipos previamente a su entrada en operación, de forma que:

- Se retiren cuentas y contraseñas estándar.
- Se aplicará la regla de mínima funcionalidad.
- Se aplicará la regla de «seguridad por defecto», es decir:

A través de perfiles configuración y líneas base de seguridad configuradas en Microsoft Intune es posible lograr los puntos anteriormente descritos.

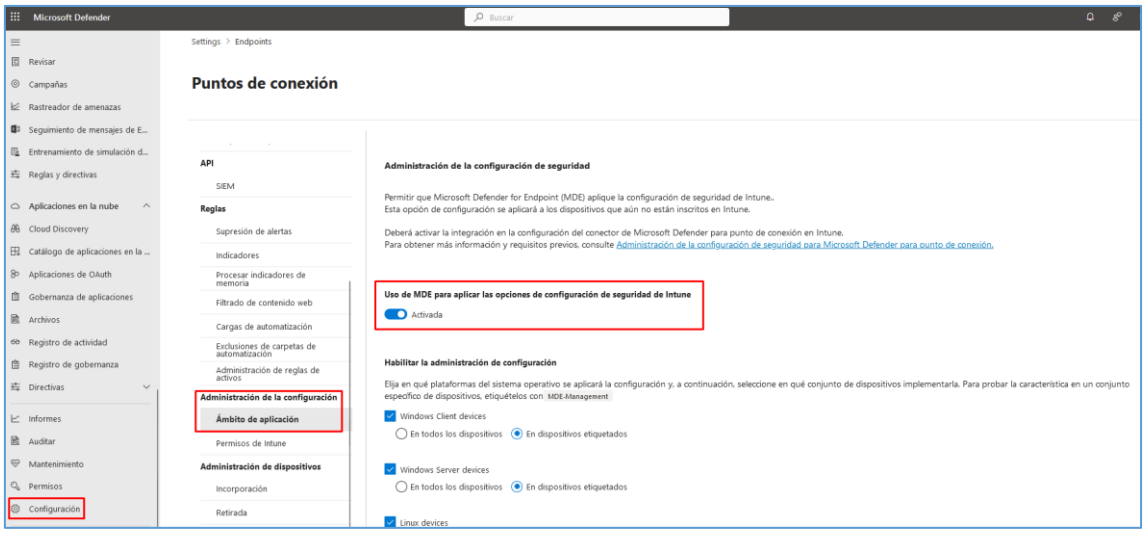
Más información en la guía [CCN-STIC-884F - Guía de configuración segura para Microsoft Intune].

Para que los dispositivos que no estén inscritos a Microsoft Intune, pero si incorporados a Microsoft Defender for EndPoint, es posible permitir que MDE aplique la configuración de seguridad de Microsoft Intune para estos dispositivos.

Para ello es necesario que la integración de MDE con Microsoft Intune está habilitada, como se ve en el punto [4.1.5.1 Administración de la configuración de seguridad]

Para habilitar el uso de MDE para aplicar las opciones de configuración de seguridad de Intune:

En el apartado **Configuración** del portal de Microsoft Defender, **Puntos de conexión > General > Características avanzadas**, habilitar la opción **Uso de MDE para aplicar las opciones de configuración de seguridad de Intune.**



3.1.2.3 GESTIÓN DE LA CONFIGURACIÓN DE SEGURIDAD

A través de las funcionalidades de detección y respuesta de puntos de conexión, los analistas de seguridad pueden asignar prioridades a las alertas, obteniendo así visibilidad para todo el ámbito de la vulneración y llevar a cabo acciones de respuesta para corregir las amenazas.

3.1.2.4 MANTENIMIENTO Y ACTUALIZACIONES DE SEGURIDAD

En esta sección se detallan aspectos relevantes en cuanto al mantenimiento y actualización de los activos en la organización.

Para acceder a información detallada de todas las medidas de mantenimiento y actualizaciones de seguridad consultar la guía [CCN-STIC-884F – Guía de configuración segura para Microsoft Intune].

3.1.2.5 PROTECCIÓN FRENTE A CÓDIGO DAÑINO

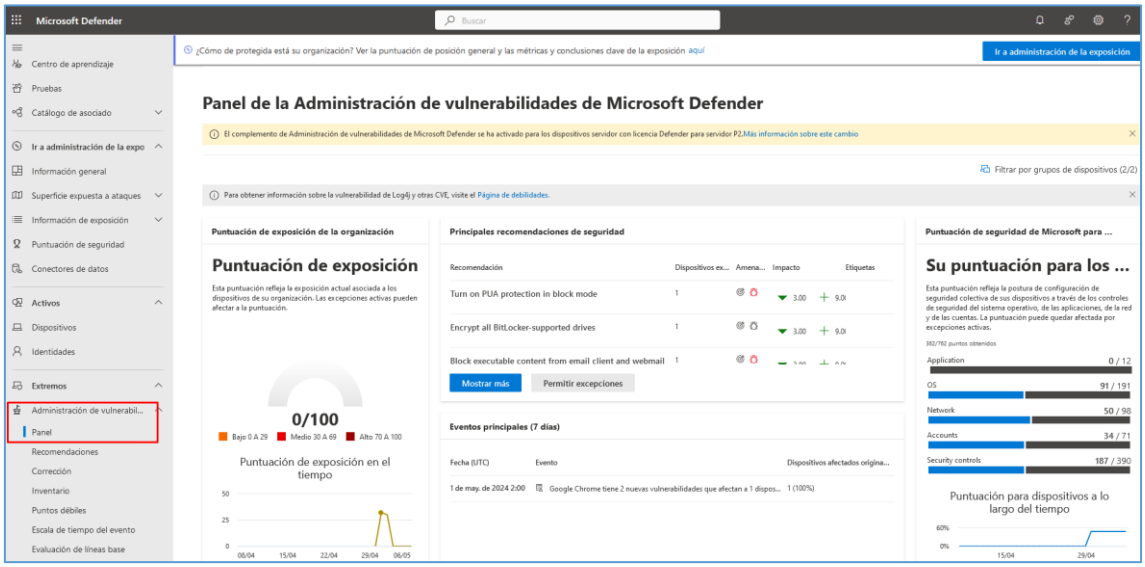
Defender for Endpoint utiliza una combinación de tecnología integrada en Windows 10/11 y el servicio en la nube de Microsoft:

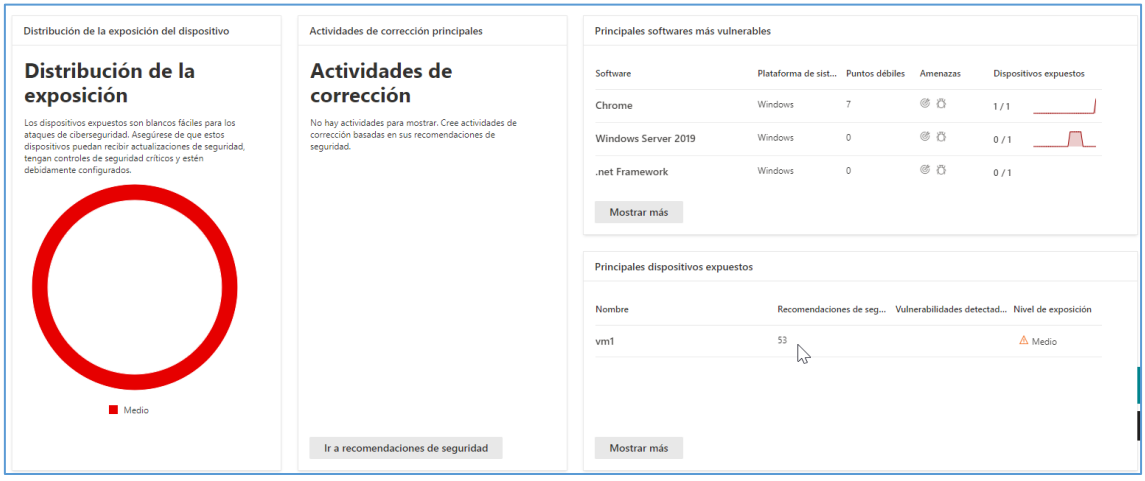
- **Sensores de comportamiento de extremo:** incrustados en Windows 10/11, estos sensores recopilan y procesan señales de comportamiento del sistema operativo y envían estos datos de sensor a la instancia privada, aislada y en la nube de *Microsoft Defender for Endpoint*.

- **Análisis de seguridad en la nube:** aprovechar los datos grandes, el aprendizaje de dispositivos y la óptica única de Microsoft en todo el ecosistema de Windows, los productos en la nube empresarial (como Office 365) y los activos en línea, las señales de comportamiento se traducen en información, detecciones y respuestas recomendadas a amenazas avanzadas.

- **Inteligencia de amenazas**: generada por los *hunters* de Microsoft (equipo de buscadores expertos en amenazas cibernéticas de Microsoft), equipos de seguridad y enriquecida por la inteligencia de amenazas proporcionada por otros partners, la *inteligencia de amenazas* permite a *Defender for Endpoint* identificar herramientas, técnicas y procedimientos de atacantes y generar alertas cuando se observan en datos de sensor recopilados.

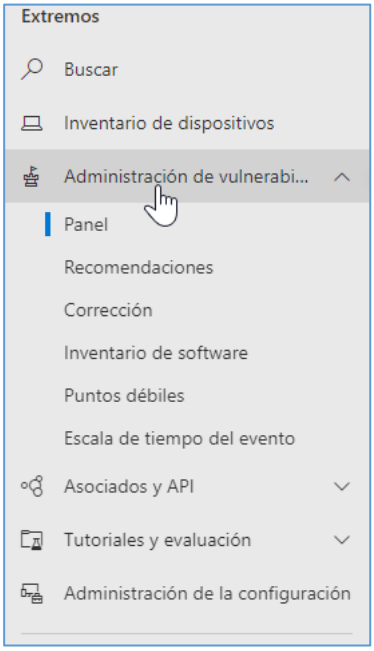
Para consultar la puntuación segura de Microsoft para dispositivos, la puntuación de exposición, los dispositivos expuestos, el software vulnerable y tomar medidas sobre las recomendaciones de seguridad más destacadas, acceder al portal de Microsoft Defender [Extremos|Administración de vulnerabilidades]:



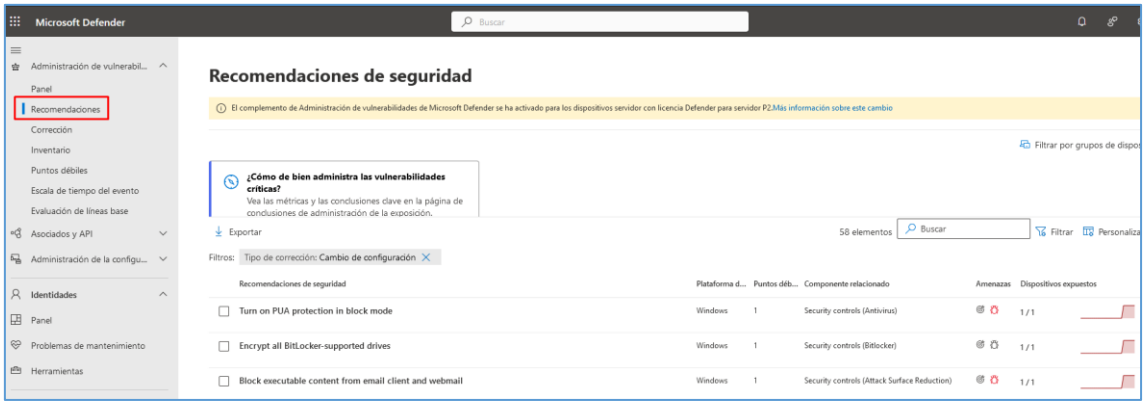


Panel de navegación

Área	Descripción
Panel	Vista de alto nivel de la puntuación de exposición de la organización, puntuación segura de Microsoft para dispositivos, distribución de exposición de dispositivos, recomendaciones de seguridad principales, software vulnerable superior, actividades de corrección superior y datos de dispositivos expuestos superiores.
Recomendaciones de seguridad	Lista de recomendaciones de seguridad e información de amenazas relacionada. Al seleccionar un elemento de la lista, se abre un panel desplegable con detalles de vulnerabilidad, un vínculo para abrir la página de software y opciones de corrección y excepción.
Corrección	Ver las actividades de corrección que han creado y las excepciones de recomendación.
Inventario de software	Consulta la lista de software vulnerable de la organización, junto con información de debilidad y amenazas.
Debilidades	Consultar la lista de vulnerabilidades y exposiciones comunes (CVE) en la organización.
Línea de tiempo de eventos	Ver eventos que pueden afectar el riesgo de la organización.



Recomendaciones de seguridad

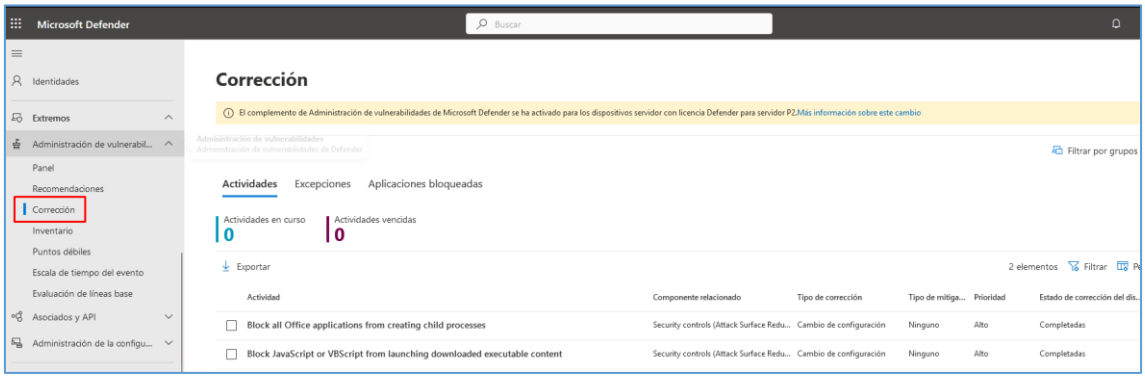


Al seleccionar un elemento de la lista, se abre un panel desplegable con detalles de vulnerabilidad, un vínculo para abrir la página de software y opciones de corrección y excepción.

Corrección

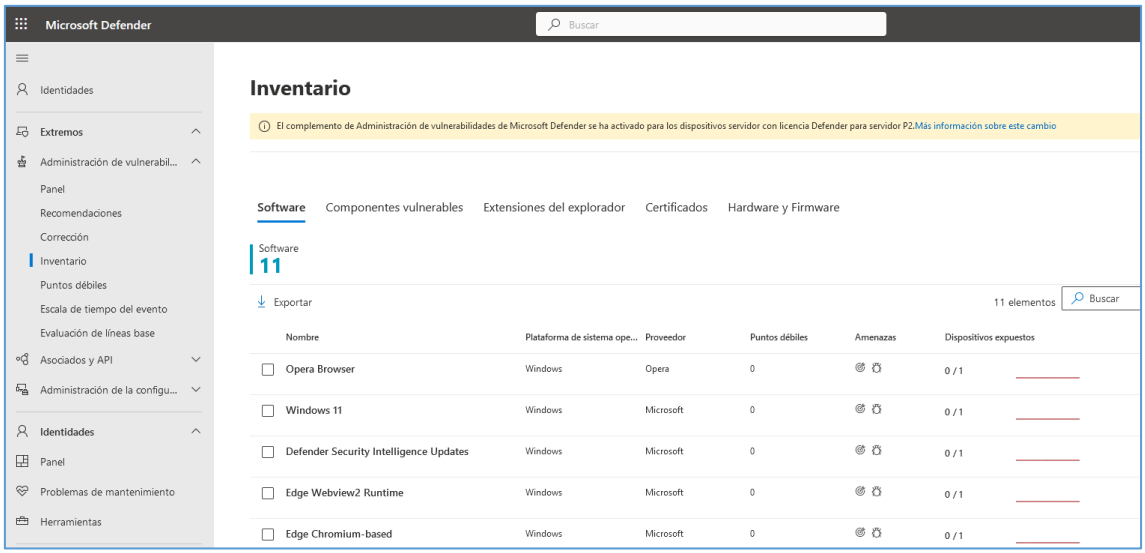
Las amenazas y administración de vulnerabilidades permiten a los administradores de seguridad y a los administradores de TI colaborar sin problemas para solucionar problemas.

- **Solicitudes de corrección enviadas a IT**: crear una tarea de corrección en Microsoft Intune desde una recomendación de seguridad específica.
- **Mitigaciones alternativas**: obtener información sobre mitigaciones adicionales, como cambios de configuración que pueden reducir el riesgo asociado con vulnerabilidades de software.
- **Estado de corrección en tiempo real:** supervisión en tiempo real del estado y el progreso de las actividades de corrección en toda la organización.



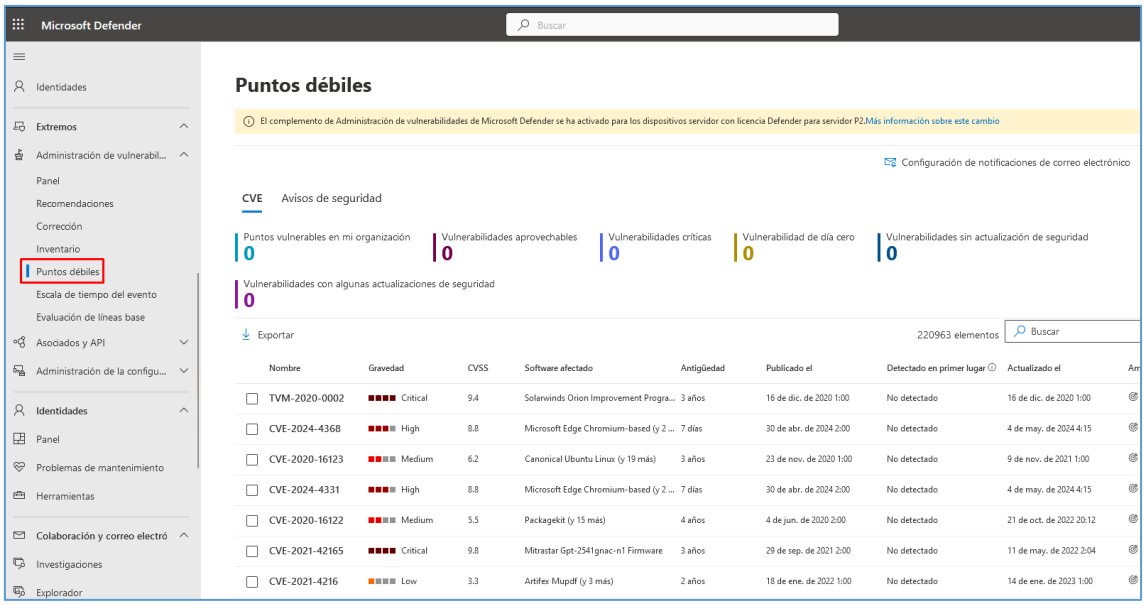
Inventario de Software

Lista de software vulnerable de la organización, junto con información de debilidad y amenazas.



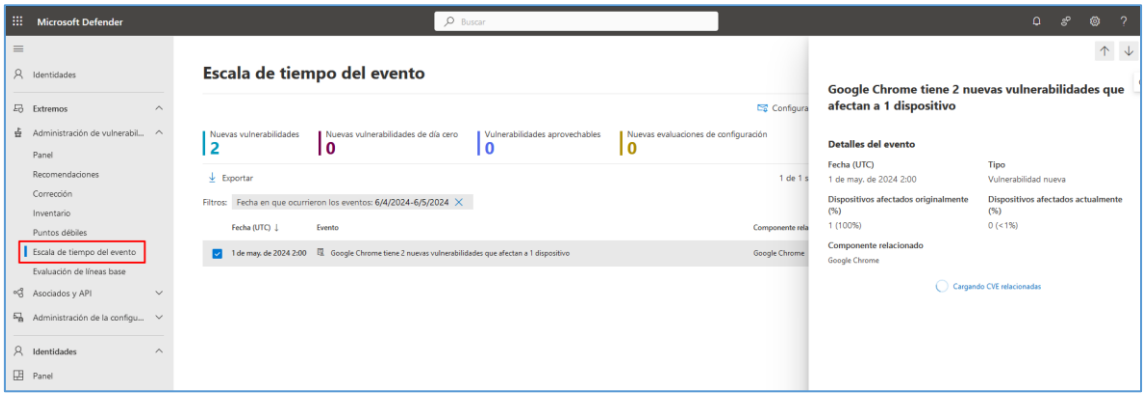
Debilidades

Lista de vulnerabilidades y exposiciones comunes (CVE) en la organización:



Línea de tiempo de eventos

Eventos que pueden afectar el riesgo de la organización:

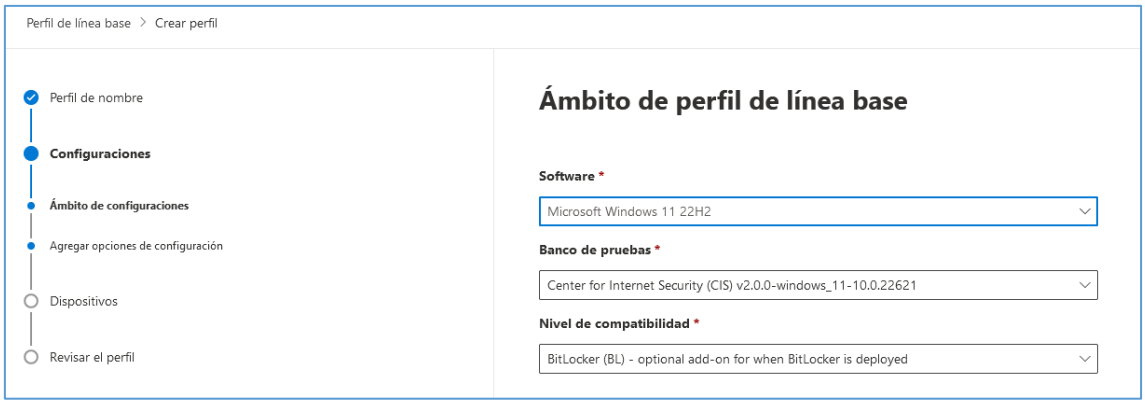


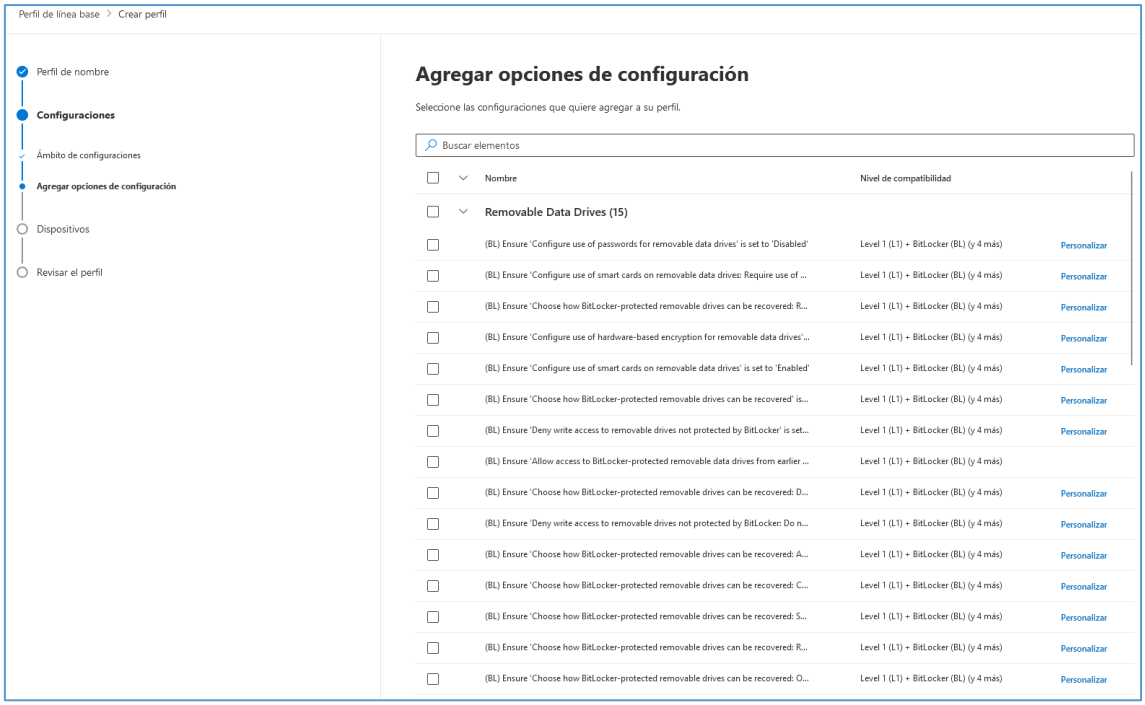
Evaluación de líneas base de seguridad

La evaluación de líneas base de seguridad permiten monitorear de forma continua y fácil el cumplimiento de las líneas base de seguridad de la organización e identificar los cambios al instante, sin hacer exámenes de cumplimiento constantes.

Para configurar evaluaciones de seguridad:

1. Ir a ***Evaluación de líneas base*** en administración de vulnerabilidades en el portal de Microsoft Defender.
2. Seleccionar la pestaña ***Perfiles*** en la parte superior y, a continuación, seleccionar el botón ***Crear perfil***.
3. En la página **Ámbito del perfil de línea base**, establezca la configuración del perfil como software, base benchmark (CIS o STIG) y el nivel de cumplimiento y seleccione Siguiente.
4. Seleccione las configuraciones que desea incluir en el perfil.



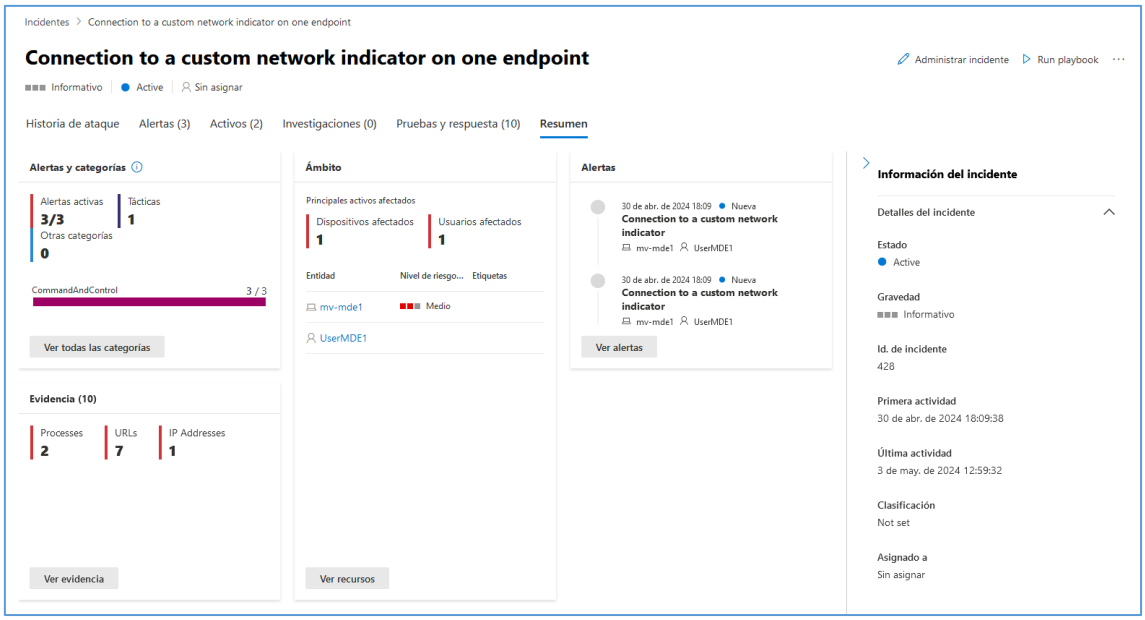


3.1.2.6 GESTIÓN DE INCIDENTES

En el portal de **Microsoft Defender**, seleccionar la opción **Incidentes**:

Aparecerá una lista con todos los incidentes y elementos sospechosos relacionados con los dispositivos que se han agregado a Microsoft Defender for Endpoint.

Para obtener información detallada pulsar sobre el nombre del incidente:



La cola Incidentes muestra una colección de incidentes marcados desde dispositivos de la red. Ayuda a ordenar los incidentes para asignar prioridades y crear una decisión de respuesta de ciberseguridad fundamentada.

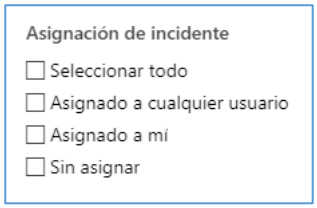
Ordenar y filtrar la cola de incidentes

Se puede aplicar los siguientes filtros para limitar la lista de incidentes y obtener una vista más centrada.

Gravedad

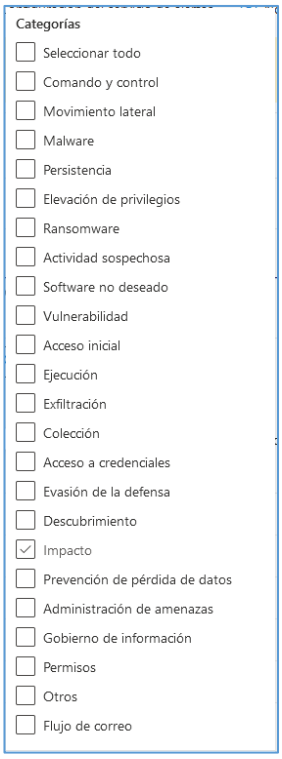
Gravedad del incidente	Descripción
Alto	Amenazas asociadas a menudo con amenazas persistentes avanzadas (APT). Estos incidentes indican un alto riesgo debido a la gravedad de los daños que pueden causar en los dispositivos.
Medio	Las amenazas rara vez se observan en la organización, como cambios anómalos en el Registro, ejecución de archivos sospechosos y comportamientos observados típicos de fases de ataque.
Bajo	Amenazas asociadas con malware y herramientas de piratería que no indican necesariamente una amenaza avanzada dirigida a la organización.
Informativo	Es posible que los incidentes informativos no se consideren perjudiciales para la red, pero podrían ser buenos para realizar un seguimiento.

Asignado a



Se puede filtrar la lista seleccionando los incidentes asignados a cualquiera o solo los asignados a su usuario.

Categoría



Los incidentes se clasifican en función de la descripción de la fase en la que se encuentra la cadena de eliminación de ciberseguridad. Esta vista ayuda al analista de amenazas a determinar la prioridad, la urgencia y la estrategia de respuesta correspondiente para implementar en función del contexto.

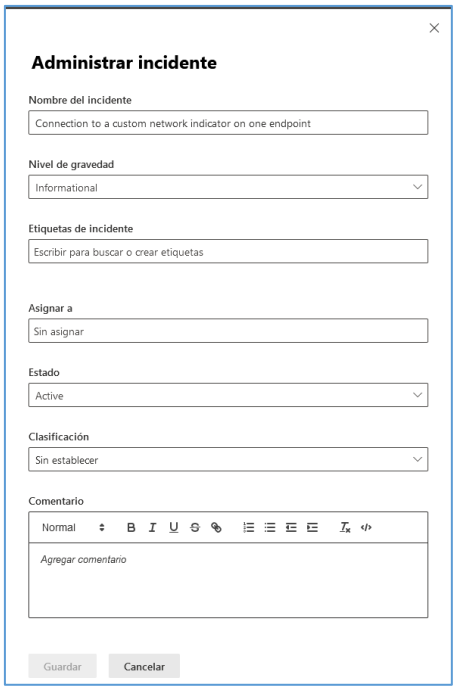
Estado

Limitar la lista de incidentes que se muestra en función de su estado para ver cuáles están activos o resueltos.

Confidencialidad de datos

Mostrar incidentes que contienen etiquetas de confidencialidad.

Dentro del incidente se puede administrar con las siguientes opciones:

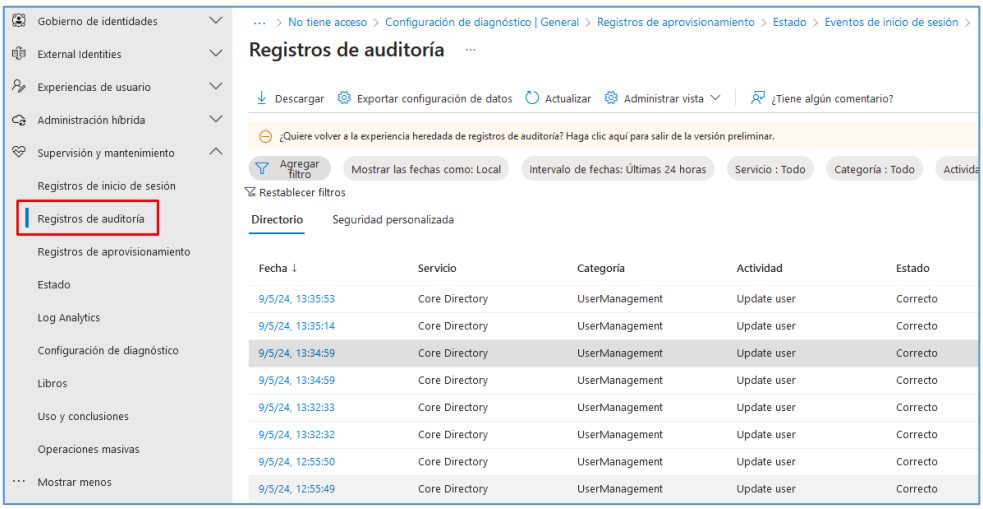


Lo recomendable es categorizar los incidentes en base a su severidad, y asignarlos a las personas con el rol correspondiente para que los atiendan.

3.1.2.7 REGISTRO DE ACTIVIDAD

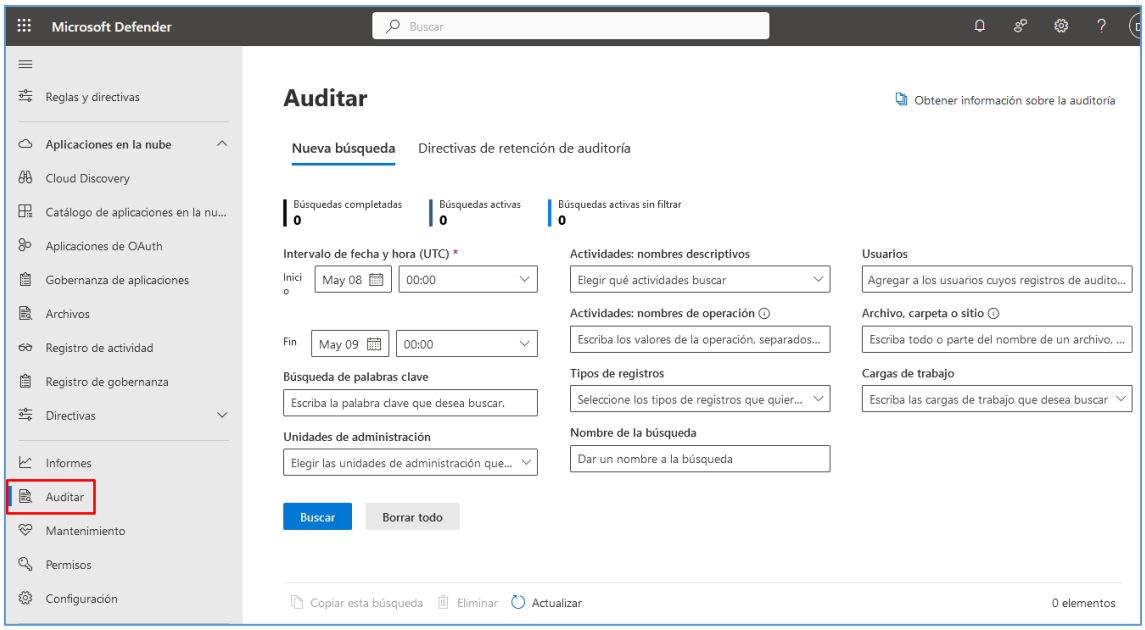
Se mantiene y se guarda un registro tanto de los inicios de sesión como de los registros de auditoría.

El primero de ellos se puede llegar a través del portal de Entra ID, **supervisión** y **mantenimiento > Registros de auditoría**.



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

En cuanto al registro de auditoría, se puede acceder desde el portal de Defender a través del botón ***Auditar***.



3.1.2.8 REGISTRO DE LA GESTIÓN DE INCIDENTES

Como se ve en el punto anterior, el registro de la gestión de incidentes se puede revisar en el punto de Auditar accesible desde el punto del portal de Defender.

La auditoría (estándar) está activada de forma predeterminada cuando se hacen uso de licencias de pago en el inquilino.

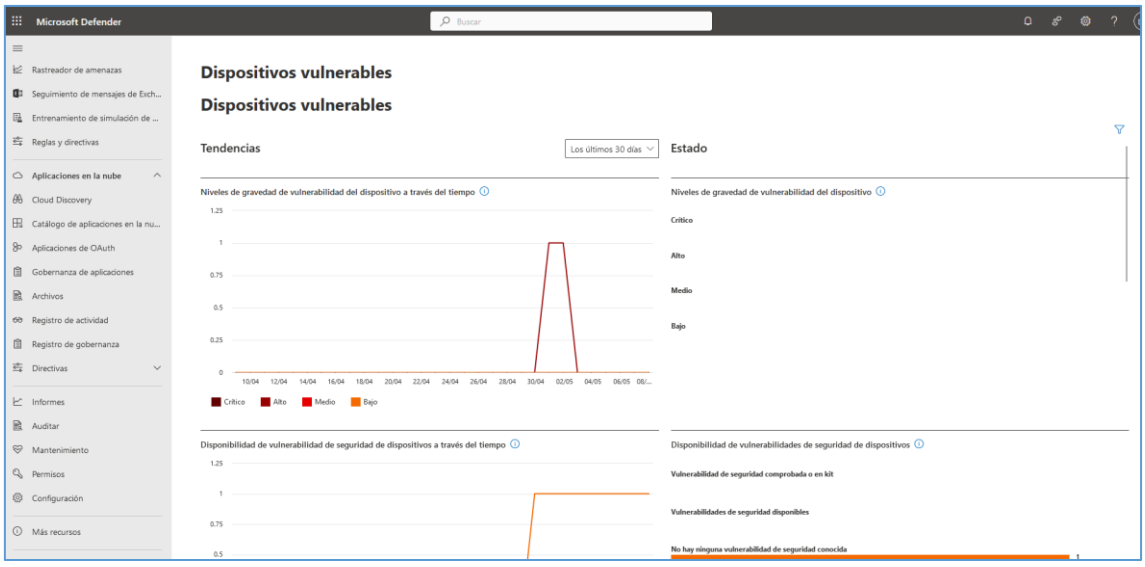
3.1.3 MONITORIZACIÓN DEL SISTEMA

Se recomienda la integración de *Microsoft Defender for Endpoint* con *Microsoft Sentinel*. Mediante el conector específico se permite transmitir eventos de búsqueda avanzada desde Microsoft Defender for Endpoint a Microsoft Sentinel, lo que permite copiar consultas de búsqueda avanzada de *Defender for Endpoint* en Microsoft Sentinel, enriquecer las alertas de Sentinel con datos de eventos sin formato de *Defender for Endpoint* para proporcionar información adicional y almacenar los registros con una mayor retención en Log Analytics.

Nota: Para más información de la integración con Microsoft Sentinel consultar la guía [CCN-STIC-884E - Guía de configuración segura para Microsoft Sentinel].

3.1.3.1 DETECCIÓN DE INTRUSIÓN

Defender dispone de informes los cuales se pueden ver la detección de vulnerabilidades e intrusiones de malware si existiesen.



El informe presenta gráficos y diagramas de barras con tendencias de dispositivos vulnerables y estadísticas recientes. El propósito es entender la dimensión y el impacto de la exposición del dispositivo.

3.1.3.2 SISTEMA DE MÉTRICAS

Como se cometaba en el punto anterior recomendamos la integración de *Microsoft Defender for Endpoint* con *Microosft Sentinel*. Mediante el conector específico se permite transmitir eventos de búsqueda avanzada desde Microsoft Defender for Endpoint a Microsoft Sentinel, lo que permite copiar consultas de búsqueda avanzada de *Defender for Endpoint* en Microsoft Sentinel, enriquecer las alertas de Sentinel con datos de eventos sin formato de *Defender for Endpoint* para proporcionar información adicional y almacenar los registros con una mayor retención en Log Analytics.

De esta manera se lograrán buenas métricas para visualizar el estado.

Nota: Para más información de la integración con Microsoft Sentinel consultar la guía [CCN-STIC-884E - Guía de configuración segura para Microsoft Sentinel].

3.1.3.3 VIGILANCIA

En esta categoría de *vigilancia* del ENS, se contemplan sistemas para detección de amenazas avanzadas y comportamiento anómalos.

Las capacidades de defender para detección y respuesta de puntos de conexión endpoint (**EDR**) proporcionan detecciones avanzadas de ataques que son casi en tiempo real y respuestas inmediatas. Los analistas de seguridad pueden asignar prioridades a las alertas de forma eficaz, obtener visibilidad para todo el ámbito de la vulneración y llevar a cabo acciones de respuesta para corregir las amenazas.

Cuando se detecta una amenaza, se crean **alertas** en el sistema para que un analista la investigue. Las alertas con las mismas técnicas de ataque o atribuidas al mismo atacante se agregan a una entidad denominada ***incidente***. Agregar alertas de esta manera permite a los analistas investigar y responder de forma colectiva a las amenazas con facilidad.

Inspirada en la mentalidad de "asumir vulneración", Defender for Endpoint recopila continuamente la telemetría cibernética de comportamiento. Esto incluye la información de procesos, las actividades de red, ópticas profundas en el kernel y el administrador de memoria, las actividades de inicio de sesión de usuario, los cambios en el registro y el sistema de archivos, entre otros. La información se almacena durante seis meses, lo que permite que un analista se desplace hacia el tiempo de inicio de un ataque. El analista puede dinamizar varias vistas y enfocar una investigación a través de varios vectores.

Las capacidades de respuesta le ofrecen la posibilidad de solucionar rápidamente las amenazas al actuar en las entidades afectadas.

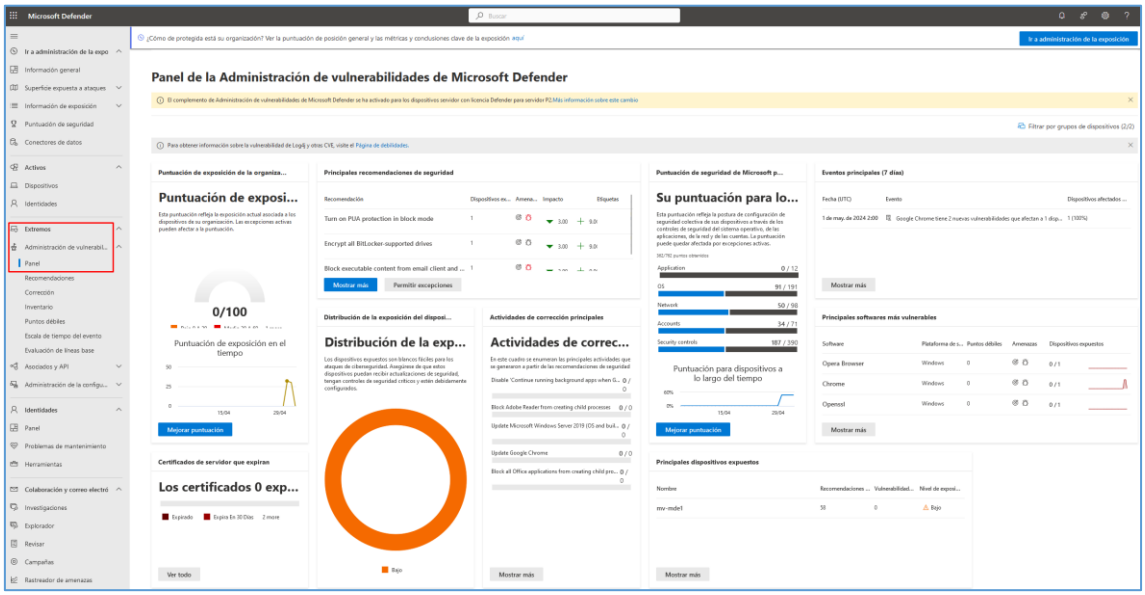
Panel de Administración de vulnerabilidades de Microsoft Defender

Proporciona una introducción de alto nivel de dónde se han visto las detecciones y resalta dónde se necesitan acciones de respuesta.

El panel se puede usar para:

- Obtener la puntuación de exposición y la Puntuación de seguridad de Microsoft para dispositivos, así como las principales sugerencias de seguridad, las vulnerabilidades de software, las acciones de corrección y los dispositivos vulnerables.
- Relación entre la información de EDR y las vulnerabilidades de punto de conexión y su tratamiento
- Selección de alternativas de corrección para valorar y monitorear las actividades de corrección
- Elegir opciones de excepción y monitorear las excepciones vigentes

Desde el portal de Microsoft Defender [Extremos | Administración de vulnerabilidades | Panel]:



3.2 MEDIDAS DE PROTECCIÓN

3.2.1 PROTECCIÓN DE LOS EQUIPOS

Para la correcta protección de equipos en Defender para puntos de conexión es necesaria la incorporación de estos en la plataforma de Defender para puntos de conexión, tal y como se refleja en el punto [2.6.3 Incorporación (Onboard)].

Por otro lado, es muy importante recalcar la integración con Microsoft Intune con Defender para puntos de conexión, parte esencial en la protección de los dispositivos.

Para acceder a información detallada de todas las medidas de configuración y seguridad consultar la guía [CCN-STIC-884F – Guía de configuración segura para Microsoft Intune].

3.2.2 PROTECCIÓN DE LOS SOPORTES DE INFORMACIÓN

3.2.2.1 CRIPTOGRAFÍA

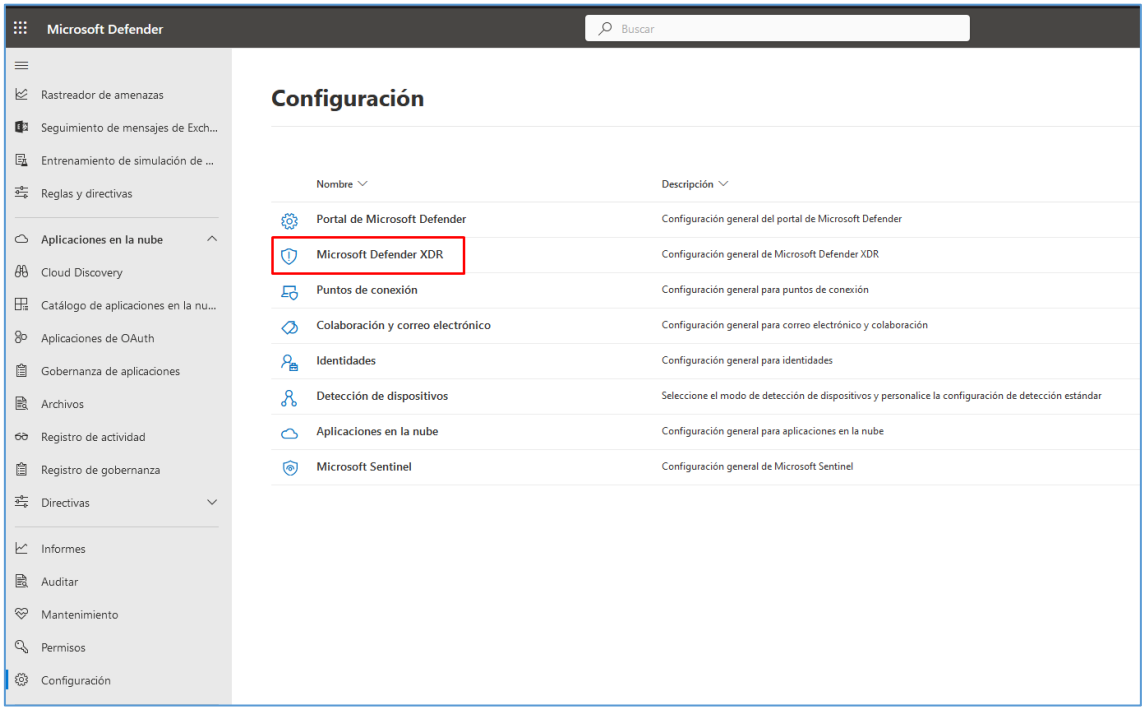
Se puede hacer uso de BitLocker para cifrar los discos en dispositivos a través de directivas de BitLocker para dispositivos Windows gestionados con Microsoft Intune.

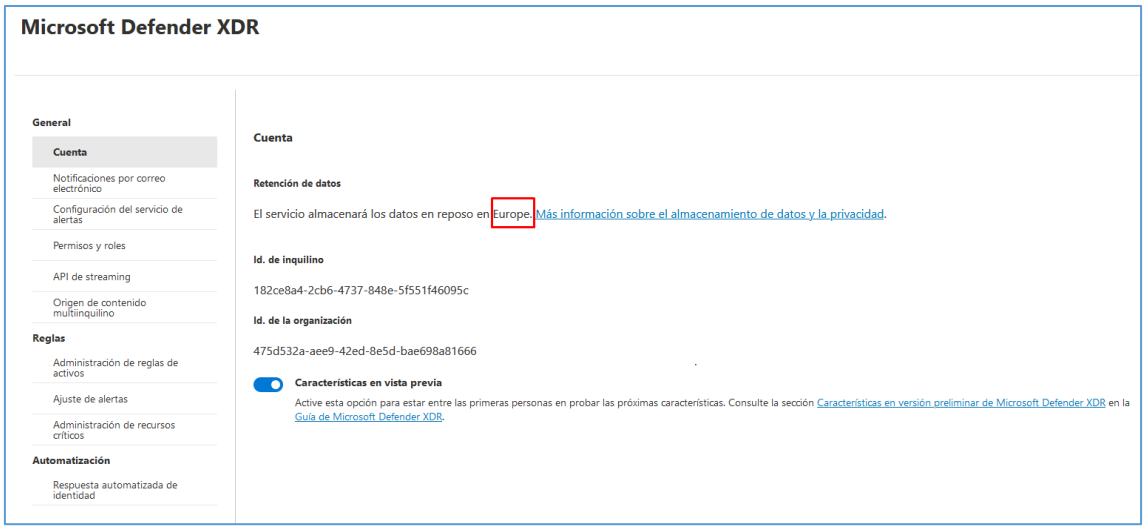
A través del método de directivas de cifrado de disco de seguridad de punto final para BitLocker se puede proteger toda la información de los dispositivos.

Al igual que el apartado anterior, para más información consultar la guía [CCN-STIC-884F – Guía de configuración segura para Microsoft Intune].

3.2.3 PROTECCIÓN DE LA INFORMACIÓN

Microsoft Defender XDR opera en Microsoft Azure centros de datos de la Unión Europea, el Reino Unido y los Estados Unidos. Los datos de cliente recopilados por el servicio se almacenan en reposo en (a) la ubicación geográfica del inquilino identificada durante el aprovisionamiento o, (b) si Microsoft Defender XDR usa otro servicio en línea de Microsoft para procesar dichos datos, la geolocalización definida por las reglas de almacenamiento de datos de ese otro servicio en línea.





La información almacenada cumple las siguientes características:

- Una vez configurado, **no se puede cambiar la ubicación** donde se almacenan los datos. Esto proporciona una forma cómoda de minimizar el riesgo de

cumplimiento seleccionando activamente las ubicaciones geográficas donde residirán los datos.

- De forma predeterminada, los datos **se conservan durante 180 días**; sin embargo, se puede especificar la directiva de retención de datos para los datos. Esto determina el tiempo que Windows Defender for Endpoint almacenará los datos.
- **Microsoft aísla los datos** mediante la autenticación de acceso y la segregación lógica basada en el identificador del cliente. Cada cliente solo puede acceder a los datos recopilados de su propia organización y a los datos genéricos que Proporciona Microsoft.
- Los desarrolladores y administradores de Microsoft tienen, por diseño, privilegios suficientes para llevar a cabo sus tareas asignadas para operar y desarrollar el servicio. Microsoft implementa combinaciones de controles preventivos, de detective y reactivos. Además, Microsoft lleva a cabo comprobaciones en segundo plano de cierto personal de operaciones y limita el acceso a aplicaciones, sistemas e infraestructura de red en proporción al nivel de verificación en segundo plano. El personal de operaciones sigue un proceso formal cuando se les exige tener acceso a la cuenta de un cliente o a la información relacionada en el rendimiento de sus funciones.

En cuanto a la protección de la información del dato en si en Microsoft 365, se hace uso de Microsoft Purview.

Para más información sobre la protección de la información de Microsoft Purview [CCN-STIC 885A - Guía de configuración segura para Office 365].

3.2.4 PROTECCIÓN DE LOS SERVICIOS

3.2.4.1 PROTECCIÓN DE LA NAVEGACIÓN WEB

Indicadores

Al crear indicadores para direcciones IP y direcciones URL o dominios, se puede autorizar o rechazar direcciones IP, direcciones URL o dominios según su propia inteligencia sobre amenazas.

Defender para punto de conexión puede usar lo siguiente para bloquear direcciones IP o direcciones URL que Microsoft considere maliciosas:

- Windows Defender SmartScreen para exploradores de Microsoft
- Protección de red para exploradores que no son de Microsoft o llamadas realizadas fuera de un explorador.

Requisitos

Para la creación de indicadores de IPs, direcciones IP o dominios se deben cumplir los siguientes requisitos:

Permitir y bloquear direcciones URL/IP requiere que el componente de Microsoft Defender para punto de conexión Protección de red esté habilitado en modo de bloqueo.

Para más información sobre este requisito, acceder a la siguiente URL:

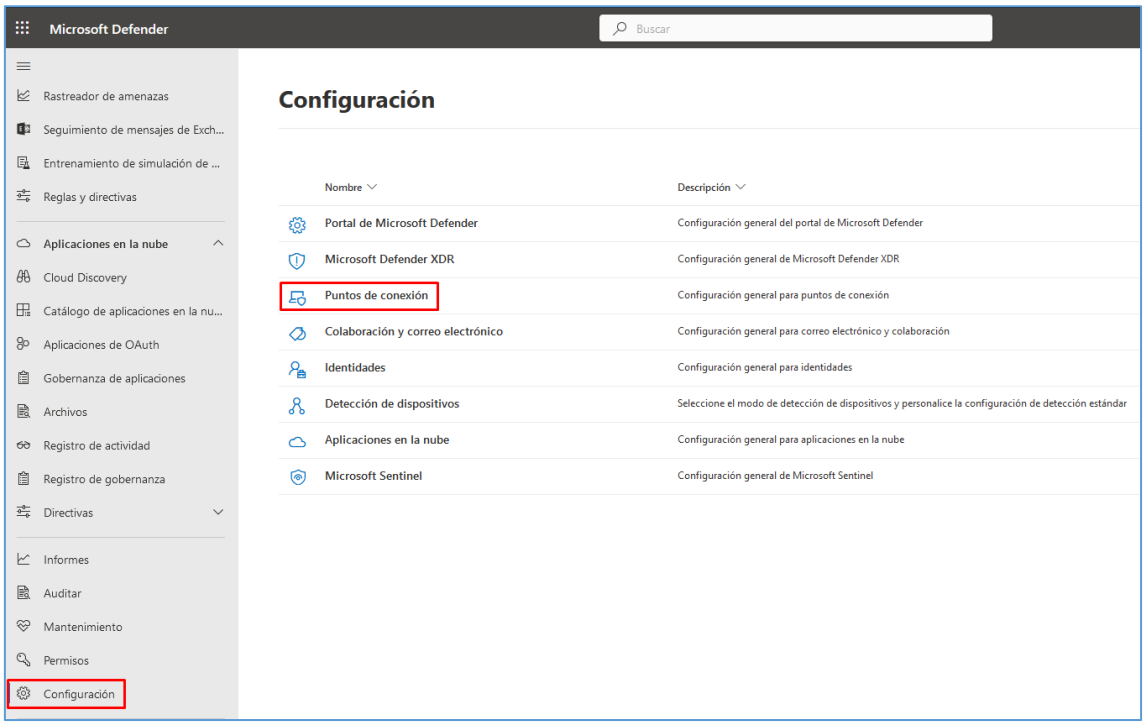
Habilitar protección de red - Microsoft Defender for Endpoint | Microsoft Learn

Se admiten los siguientes sistemas operativos:

- Windows 10, versión 1709 o posterior
- Windows 11
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2019
- Windows Server 2022
- macOS
- Linux
- iOS
- Android

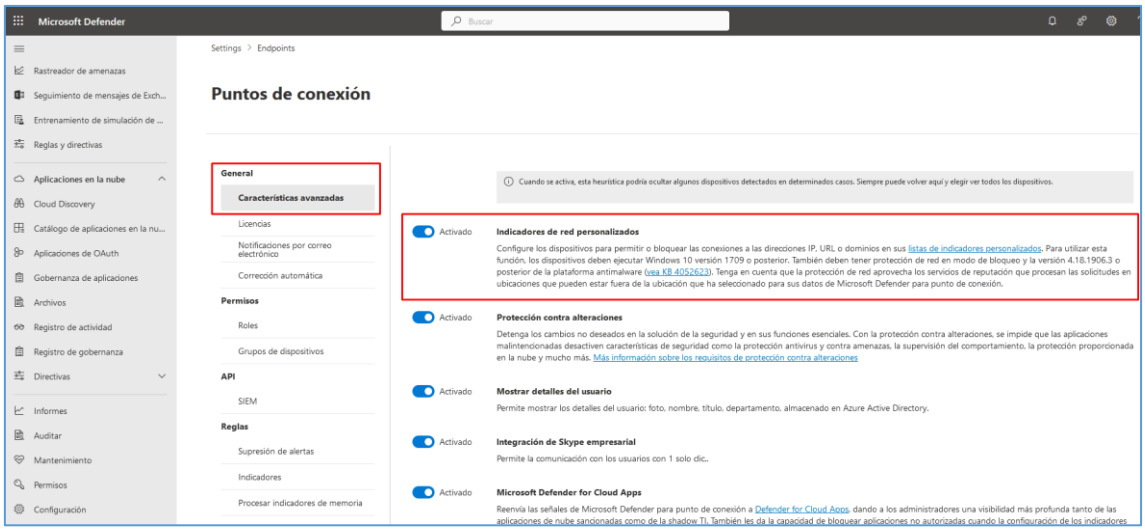
Otro requisito obligatorio es que los indicadores de red estén habilitados en las características avanzadas de Microsoft Defender.

Para hablitarlo, acceda al portal de Microsoft Defender -> Configuración -> Puntos de conexión.



Una vez allí, **General -> Características avanzadas**.

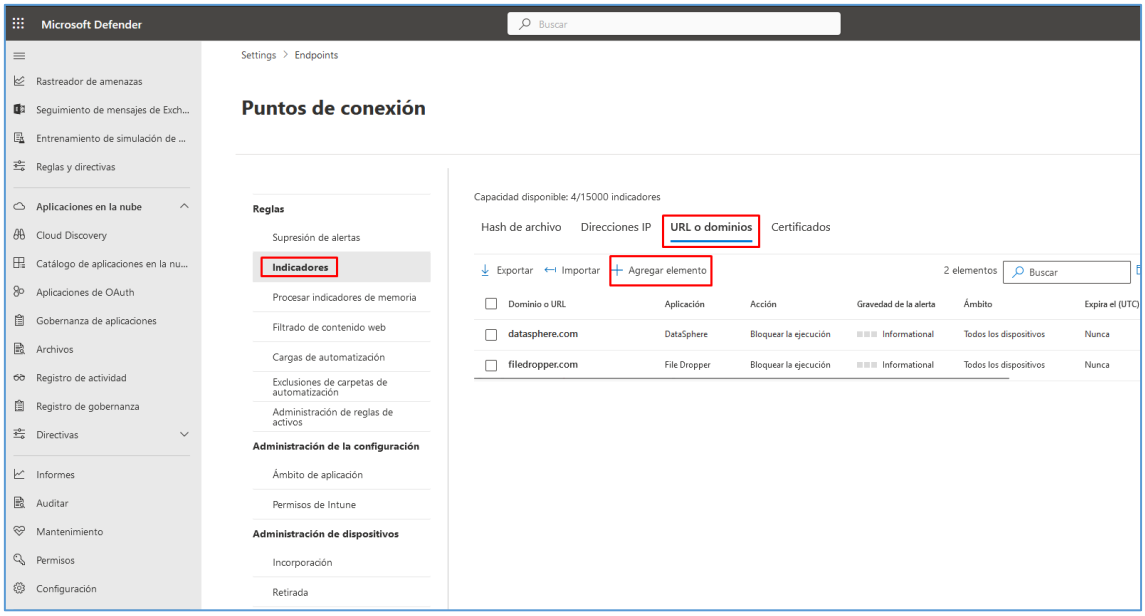
Aquí habilitar los Indicadores de red personalizados.

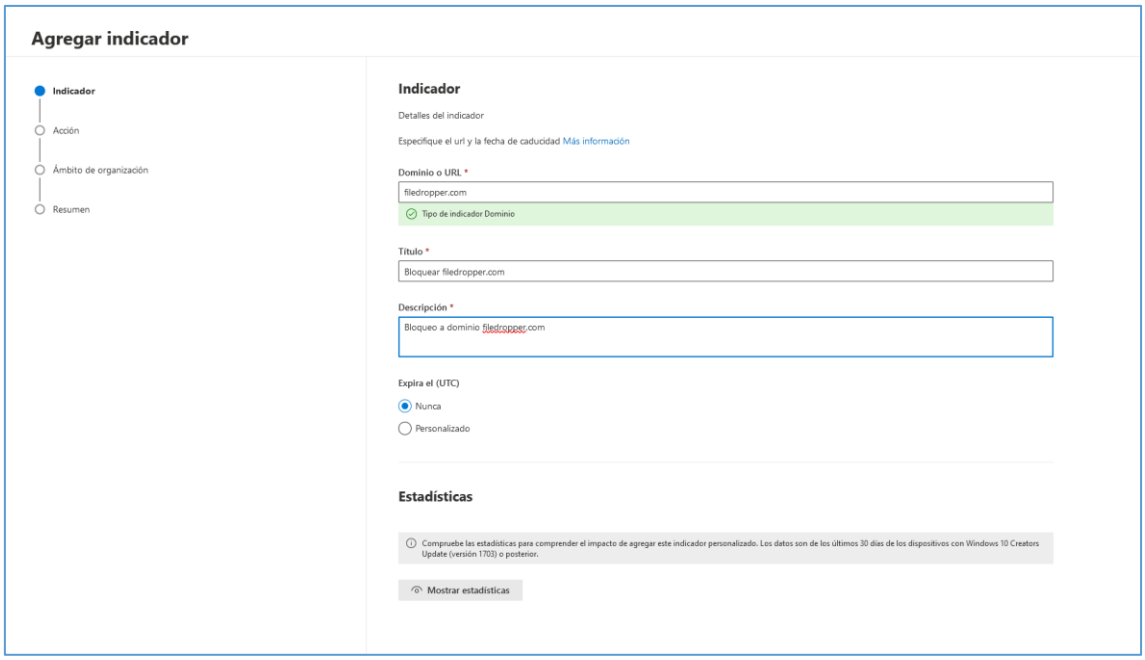


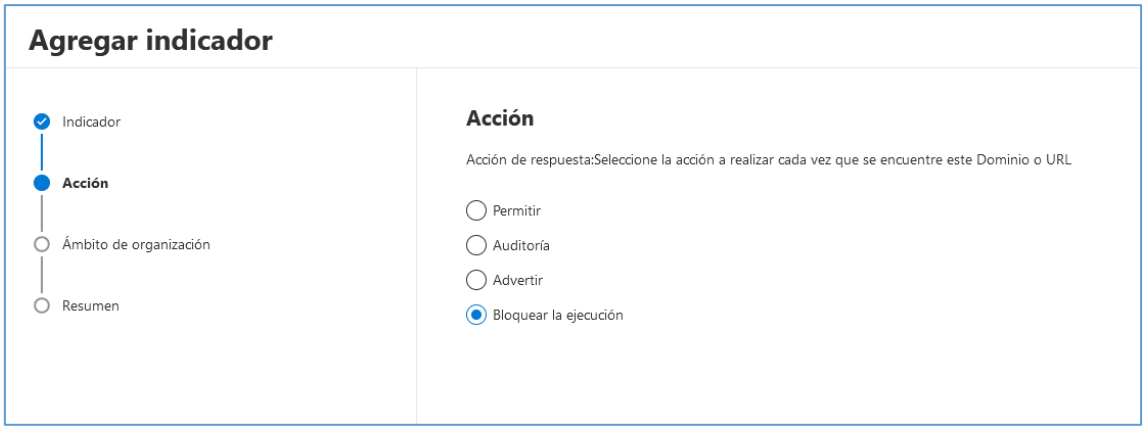
Para crear el indicador.

- En el panel de navegación, **Configuración -> Indicadores de puntos de conexión**.
- Seleccione la pestaña **Direcciones IP, direcciones URL o dominios**.
- Seleccione **Agregar elemento**.
- Especificar los detalles siguientes:
    - **Indicador**: especifique los detalles de la entidad y defina la expiración del indicador.
    - **Acción**: especifique la acción que se va a realizar y proporcione una descripción.
    - **Ámbito**: defina el ámbito del grupo de máquinas.

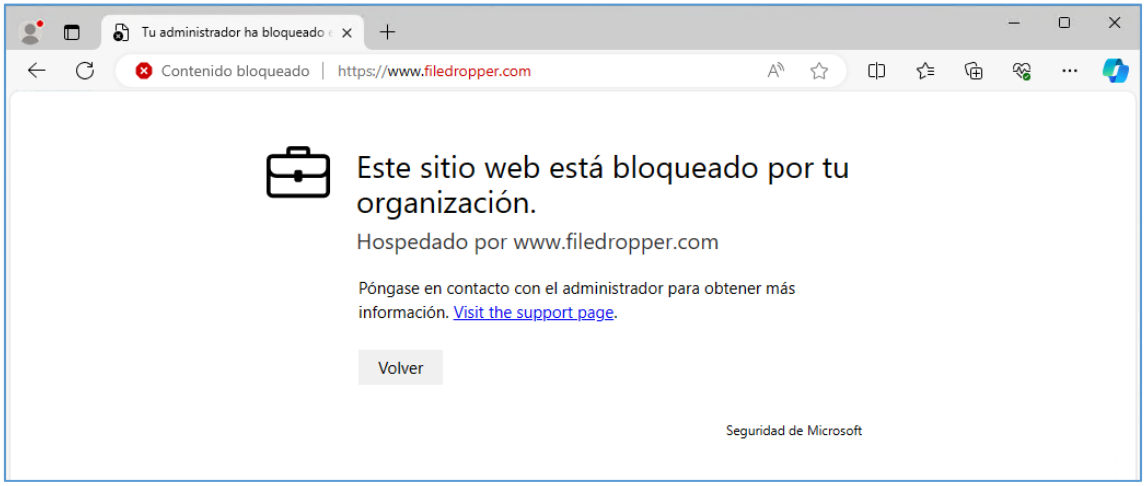
Revise los detalles de la pestaña **Resumen** y, a continuación, seleccione **Guardar**.







En la siguiente imagen, se puede ver en un dispositivo bajo el amparo de Defender para puntos de conexión, como se aplica el bloqueo al dominio previamente configurado.



Filtrado de contenido Web

Otra manera de securizar la navegación web en los equipos de la organización con Defender para puntos de conexión, es el filtrado de contenido web.

Para que esta característica de protección web funcione correctamente, se tienen que cumplir los siguientes requisitos:

- Licenciamiento:
  - Windows 10/11 Enterprise E5
  - M365 E5/E3/A5,
  - MDefender Plan ½.

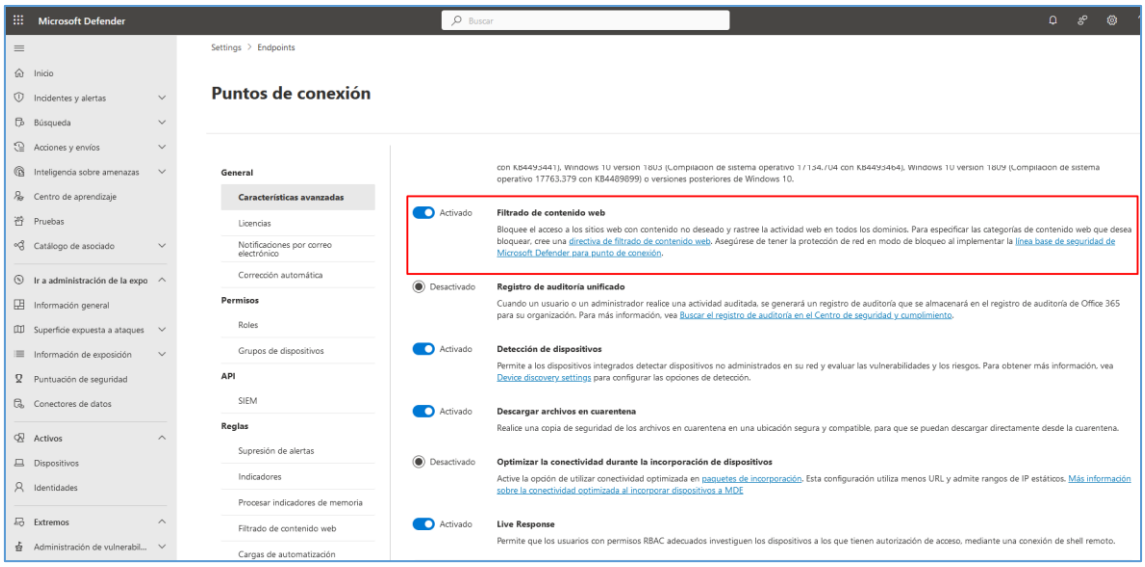
- Cualquiera de estos exploradores:
  - Microsoft Edge
  - Google Chrome
  - Mozilla FireFox
  - Ópera
- Y las características de Windows Defender SmartScreen y la protección de red habilitadas en los dispositivos de la organización.

  Para más información sobre estas características, se añaden los siguientes enlaces:

  Introducción a SmartScreen de Microsoft Defender - Windows Security | Microsoft Learn

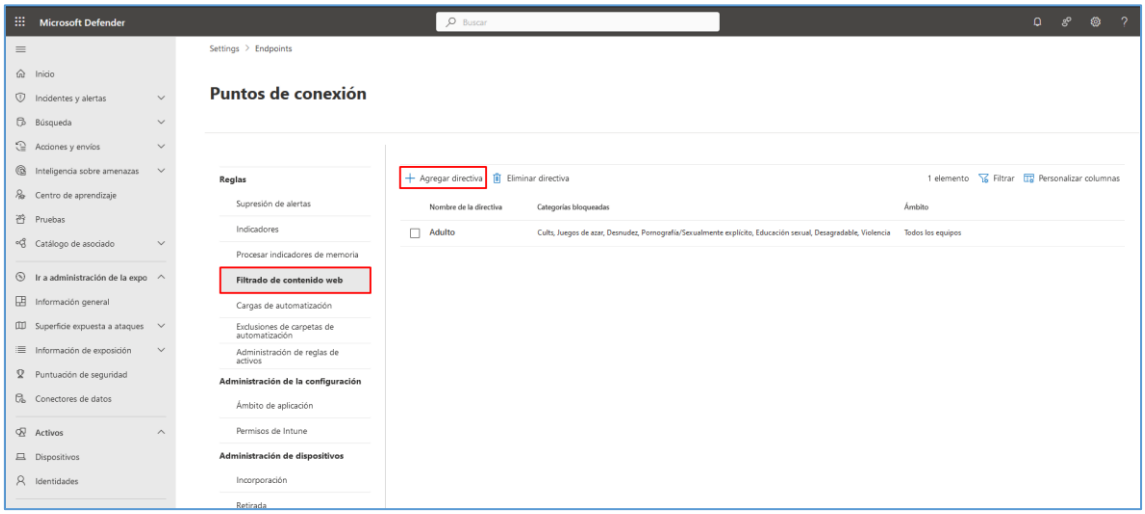
  Uso de la protección de red para evitar conexiones a sitios incorrectos - Microsoft Defender for Endpoint | Microsoft Learn

- Debe estar activo el filtrado de contenido web, para habilitarlo:
  - Ir al portal de Microsoft Defender e iniciar sesión.
  - En el panel de navegación, seleccionar **Configuración > Puntos de conexión > Características avanzadas**.
  - Activar el filtrado de contenido web.

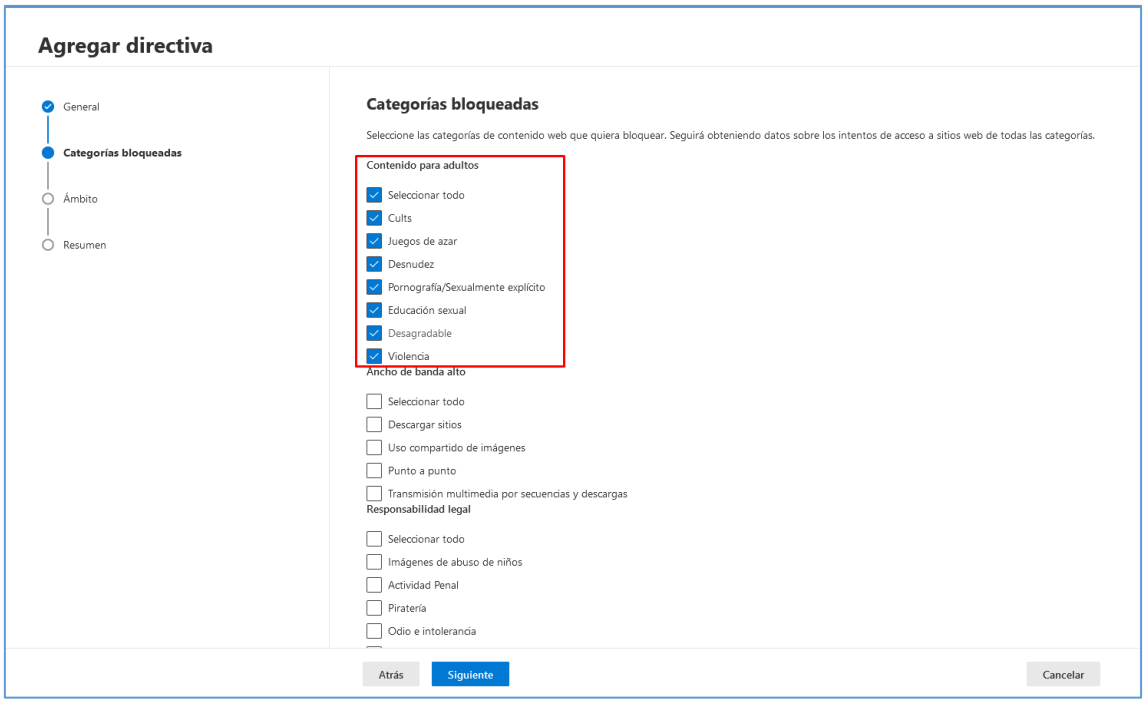


Una vez cumplidos los requisitos, para crear una directiva de filtrado web:

En el portal de Microsoft Defender, elegir **Configuración > Puntos de conexión > Reglas Filtrado de contenido web > Agregar directiva**.



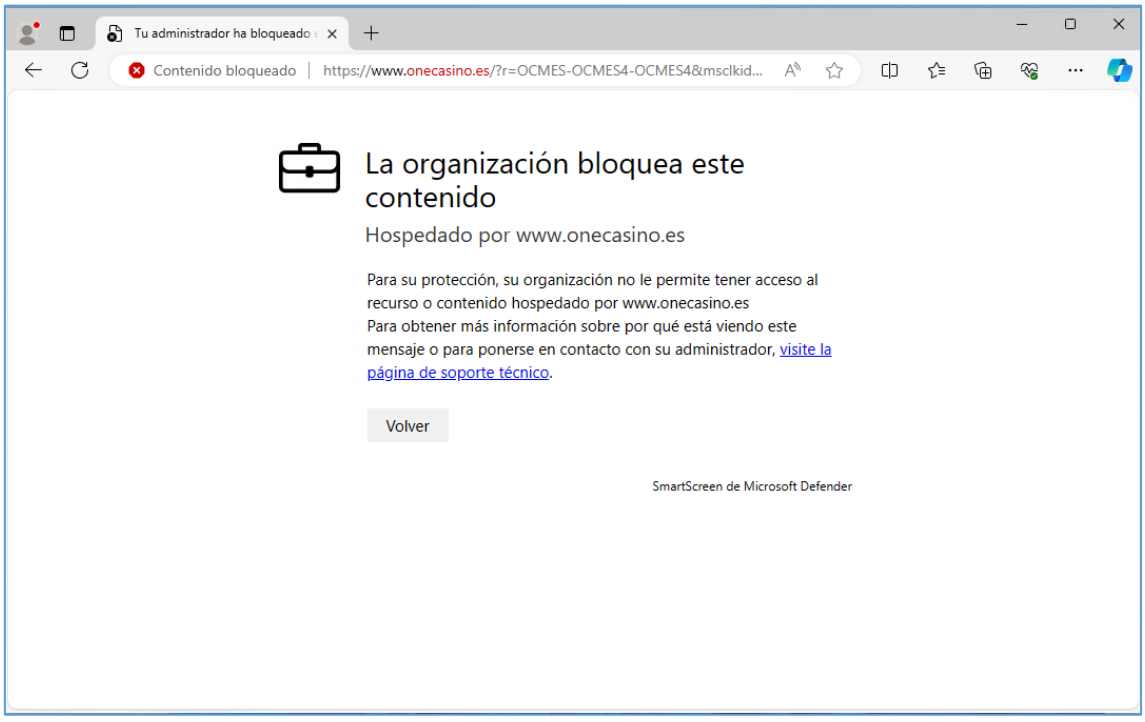
Se asigna el nombre, y a continuación se elige el contenido que se quiere filtrar en la organización, en este caso se ha elegido contenido para adultos.



Por último, especificar el ámbito de la directiva. Solo se impedirá que los dispositivos de los grupos de dispositivos seleccionados accedan a sitios web de las categorías seleccionadas.

Una vez configurado, la experiencia del usuario final es la siguiente.

Al intentar acceder a una página de apuestas desde un dispositivo inscrito a Defender para puntos de conexión, se bloqueará el acceso.



3.2.4.2 PROTECCIÓN FRENTE A LA DENEGACIÓN DE SERVICIO

Office 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.

El sistema de defensa DDoS de Azure está diseñado no solo para resistir ataques desde el exterior, sino también desde otros *tenants* de Azure. Los mecanismos de limitación de peticiones de Exchange Online y SharePoint Online forman parte de un enfoque de varias capas para defenderse contra ataques DoS.

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. OTRAS CONSIDERACIONES DE SEGURIDAD

4.1 CONFIGURACIÓN DE PARÁMETROS EN EL CENTRO DE SEGURIDAD DE MICROSOFT DEFENDER

En el menú Configuración (Settings) es posible modificar la configuración general, las características avanzadas propias de los puntos de conexión, habilitar la detección de dispositivos, identidades, aplicaciones en la nube etc.

En esta guía se abarcarán diferentes aspectos que pueden influir en el uso de Defender para puntos de conexión.

Tema	Descripción
General	Modificar la configuración general que se definió como parte del proceso de incorporación.
Permisos	Administrar el acceso al portal mediante RBAC, así como grupos de dispositivos.
API	Habilitar la integración con el SIEM y la inteligencia de amenazas.
Reglas	Configurar reglas de supresión y opciones de automatización.
Administración de dispositivos	Dispositivos integrados y no integrados.
Evaluaciones de red	Elegir los dispositivos que se examinarán periódicamente y se agregarán al inventario de dispositivos.

4.1.1 CONFIGURACIÓN GENERAL

Para la configuración de los siguientes parámetros se usa como referencia el portal Defender: security.microsoft.com, como se describe en el apartado [1.4 Funcionalidades del portal].

4.1.1.1 ALMACENAMIENTO DE DATOS Y PRIVACIDAD

Defender for Endpoint funciona en los centros de datos de Microsoft Azure en la Unión Europea, el Reino Unido, Estados Unidos o Australia. Los datos del cliente que el servicio recoge pueden guardarse en: la zona geográfica del arrendatario que se determina durante la configuración o, la zona geográfica que establecen las normas de almacenamiento de datos de un servicio online si Defender for Endpoint usa este servicio online para procesar esos datos.

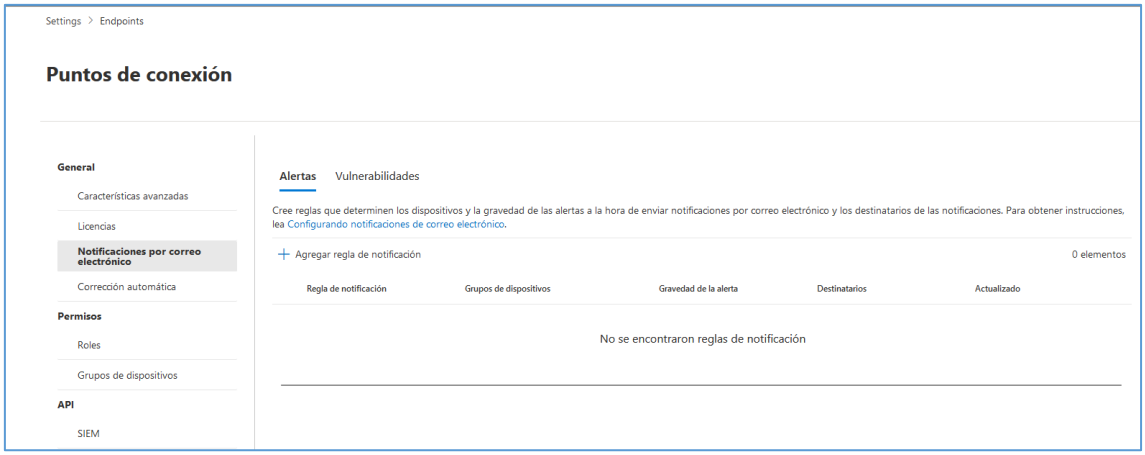
Microsoft Defender for Endpoint guarda información de los dispositivos que se han configurado y la mantiene en un espacio independiente y exclusivo para cada cliente del servicio, para poder gestionarla, supervisarla e informar sobre ella.

Los datos de Microsoft Defender para punto de conexión se conservan durante 180 días, visibles en el portal. Sin embargo, en la experiencia de investigación de búsqueda avanzada, es accesible a través de una consulta durante 30 días.

4.1.1.2 CONFIGURAR NOTIFICACIONES DE ALERTAS Y VULNERABILIDADES

Se accede desde [Settings|General|Notificaciones por correo electronico]:

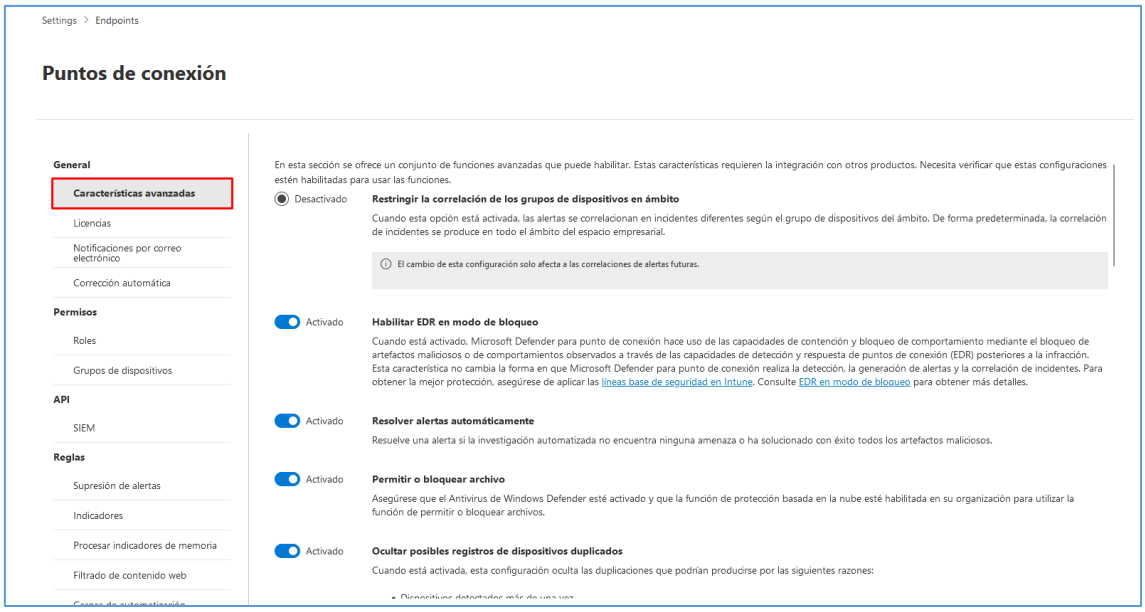
Se puede configurar Defender for Endpoint para enviar notificaciones por correo electrónico a destinatarios específicos para nuevas alertas. Esta característica posibilita identificar un grupo de personas que se informarán inmediatamente y podrán actuar en función de la gravedad de alerta.



4.1.1.3 CARACTERÍSTICAS AVANZADAS

En esta sección se proporciona un conjunto de funciones avanzadas que puede habilitarse. Estas características requieren integración con otros productos. Se debe verificar que esta configuración esté habilitada para usar las características.

Se accede desde [Configuración|Puntos de conexión | General|Caracerísticas avanzadas]:



Restringir la correlación de los grupos de dispositivos en ámbito

Esta opción permite agrupar las alertas en incidentes distintos según el grupo de dispositivos del ámbito. Por defecto, los incidentes se correlacionan para todo el ámbito del espacio empresarial.

Habilitar EDR en modo bloqueo

Cuando está activado, *Microsoft Defender for Endpoint* aprovecha las capacidades de contención bloqueando los comportamientos o artefactos maliciosos observados a través de las capacidades de detección y respuesta de puntos de conexión (EDR) posteriores a la infracción.

Resolver alertas automáticamente

Resuelve una alerta si la investigación automatizada no encuentra amenazas o ha solucionado con éxito todos los artefactos maliciosos.

Permitir o bloquear archivo

Comprobar que el Antivirus de Windows Defender esté activado y la función de protección basada en la nube esté habilitada en su organización para usar la función de permitir o bloquear archivos.

Ocultar posibles registros de dispositivos duplicados

Cuando está activada, esta configuración oculta las duplicaciones que podrían producirse al detectarse dispositivos más de una vez o no detectados accidentalmente.

Indicadores de red personalizados

Configurar dispositivos para permitir o bloquear conexiones a direcciones IP, dominios o URL en las listas de indicadores personalizados.

Protección contra alteraciones

La protección contra alteraciones evita que las aplicaciones maliciosas deshabiliten funciones de seguridad como la protección antivirus y contra amenazas, el análisis del comportamiento, la protección en la nube y otras más.

Mostrar detalles de usuario

Permite mostrar los detalles del usuario: imagen, nombre, cargo, departamento, almacenados en Entra ID.

Integración de Skype para empresas

Permite la comunicación con los usuarios con un solo clic.

Microsoft Defender for Cloud Apps

Reenvía las señales de Microsoft Defender para punto de conexión a Defender for Cloud Apps, dando a los administradores una visibilidad más profunda tanto de las aplicaciones de nube sancionadas como de la shadow TI. También les da la capacidad de bloquear aplicaciones no autorizadas cuando la configuración de los indicadores de red personalizados está activada.

Filtrado de contenido web

Esta opción permite bloquear el acceso a los sitios web con contenido no deseado y rastrear la actividad web en todos los dominios.

Registro de auditoría unificado

Si una actividad auditada es realizada por un usuario o un administrador, se creará un registro de auditoría que se guardará en el registro de auditoría de Office 365 de su organización.

Detección de dispositivos

Permite a los dispositivos integrados detectar dispositivos no administrados en su red y evaluar las vulnerabilidades y los riesgos.

Descargar archivos en cuarentena

Realiza una copia de seguridad de los archivos en cuarentena en una ubicación segura y compatible, para que se puedan descargar directamente desde la cuarentena.

Optimizar la conectividad durante la incorporación de dispositivos

Activa la opción de utilizar conectividad optimizada en paquetes de incorporación. Esta configuración utiliza menos URL y admite rangos de IP estáticos.

Respuesta en vivo

Permite a los usuarios con los permisos adecuados de RBAC investigar los dispositivos a los que están autorizados a acceder mediante una conexión de *shell* remota.

Respuesta en vivo para servidores

Permite a los usuarios con privilegios de *respuesta en vivo* conectarse de forma remota a servidores (dispositivos Windows Server o Linux) a los que están autorizados para acceder.

Ejecución de script sin firmar de Live Response

Habilita el uso de scripts sin firmar en Live Response.

Señuelos

Administre e implemente señuelos y cebos para atrapar a los atacantes en su entorno. Tras activar esto, vaya a Reglas > Reglas contra señuelos para ejecutar campañas de engaño.

Conexión de Microsoft Intune

Conectarse a Microsoft Intune para permitir compartir la información del dispositivo y mejorar la aplicación de políticas.

Intune proporciona información adicional sobre dispositivos administrados para una puntuación segura. Se puede utilizar información de riesgo para hacer cumplir el acceso condicional y otras políticas de seguridad.

Telemetría autenticada

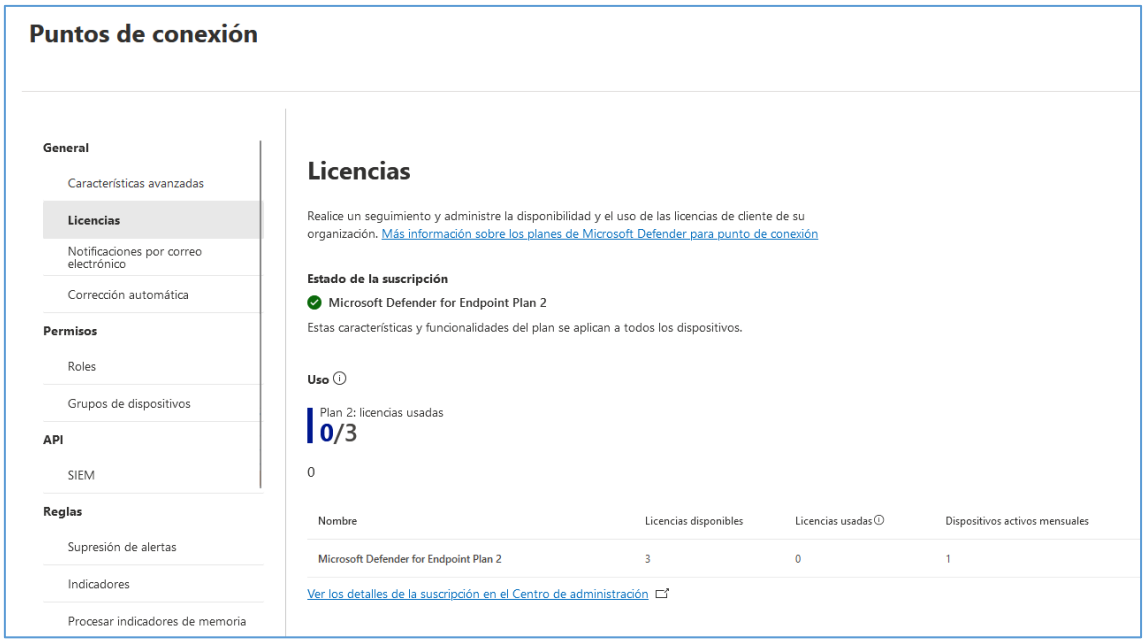
Mantén activada la telemetría autenticada para evitar la suplantación de identidad en el panel.

Funciones de vista previa

Permita el acceso a las funciones de vista previa. Active el acceso para estar entre los primeros en probar las próximas características.

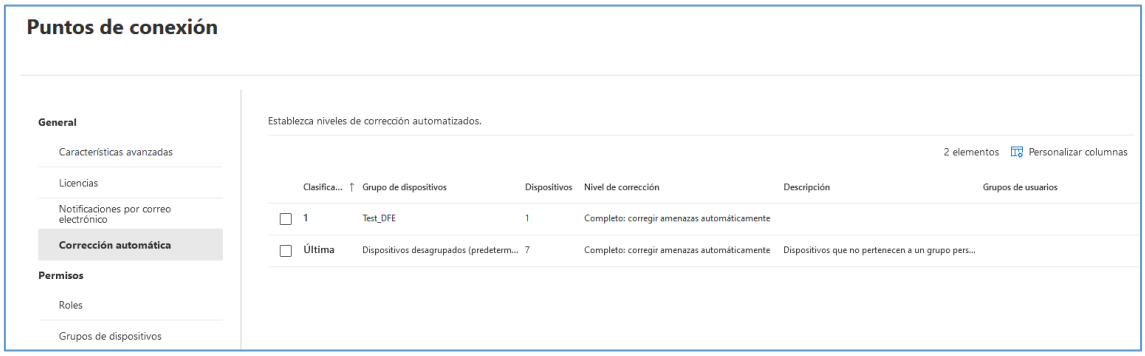
4.1.1.4 LICENCIAS

En esta sección se puede hacer un seguimiento sobre la disponibilidad y el uso de las licencias actualmente en la organización.



4.1.1.5 CORRECCIÓN AUTOMÁTICA

Se puede especificar un nivel de automatización para que cuando se detecte una amenaza en un dispositivo, la entidad se pueda corregir automáticamente o solo tras la aprobación del equipo de seguridad. Se puede configurar la investigación y la corrección automatizadas con grupos de dispositivos.

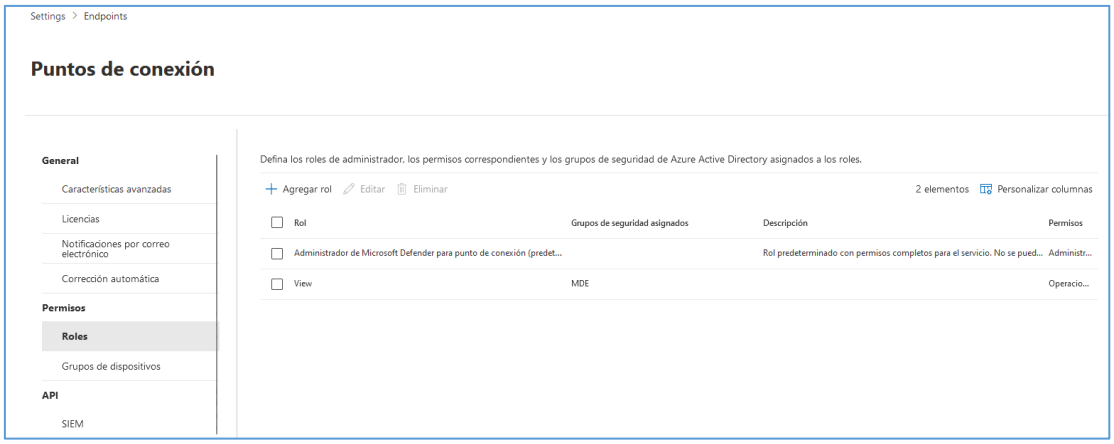


Estos grupos de dispositivos se pueden crear en [Configuración|Puntos de conexión | Permisos|Grupos de dispositivos].

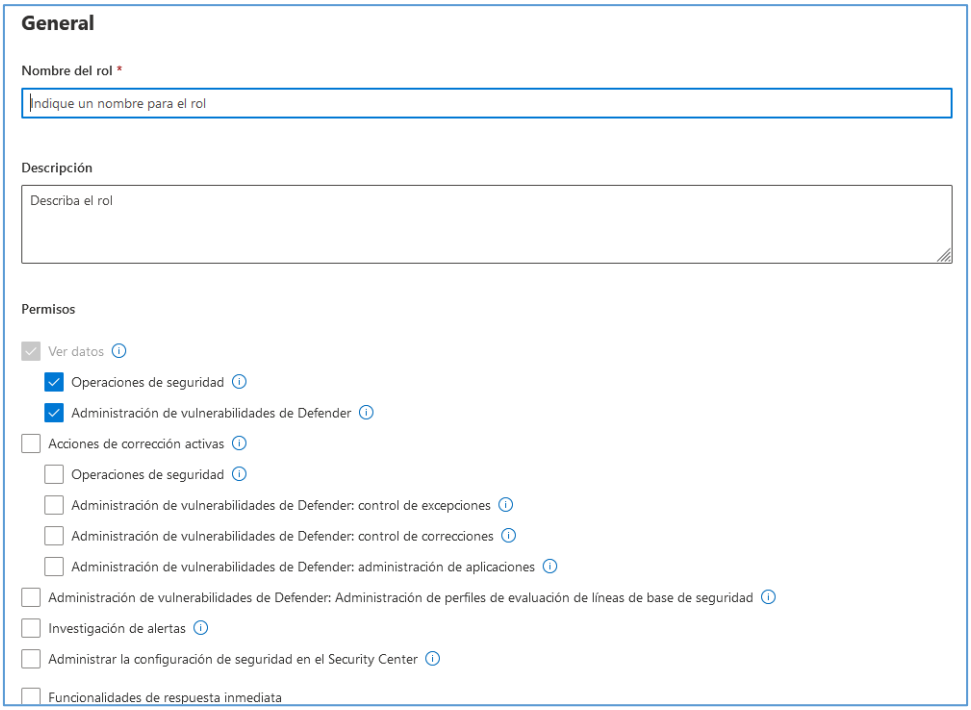
4.1.2 PERMISOS

Con esta sección de configuración, accesible desde [Configuración|Puntos de conexión | Permisos] se permite:

- Definir los **roles** de administrador, los permisos correspondientes y los grupos de seguridad de Azure Active Directory asignados a los roles.
- Organizar los **dispositivos en grupos**, establecer niveles de corrección automatizados y asignar administradores.



A continuación, se detallan las distintas opciones de permisos al añadir un rol:

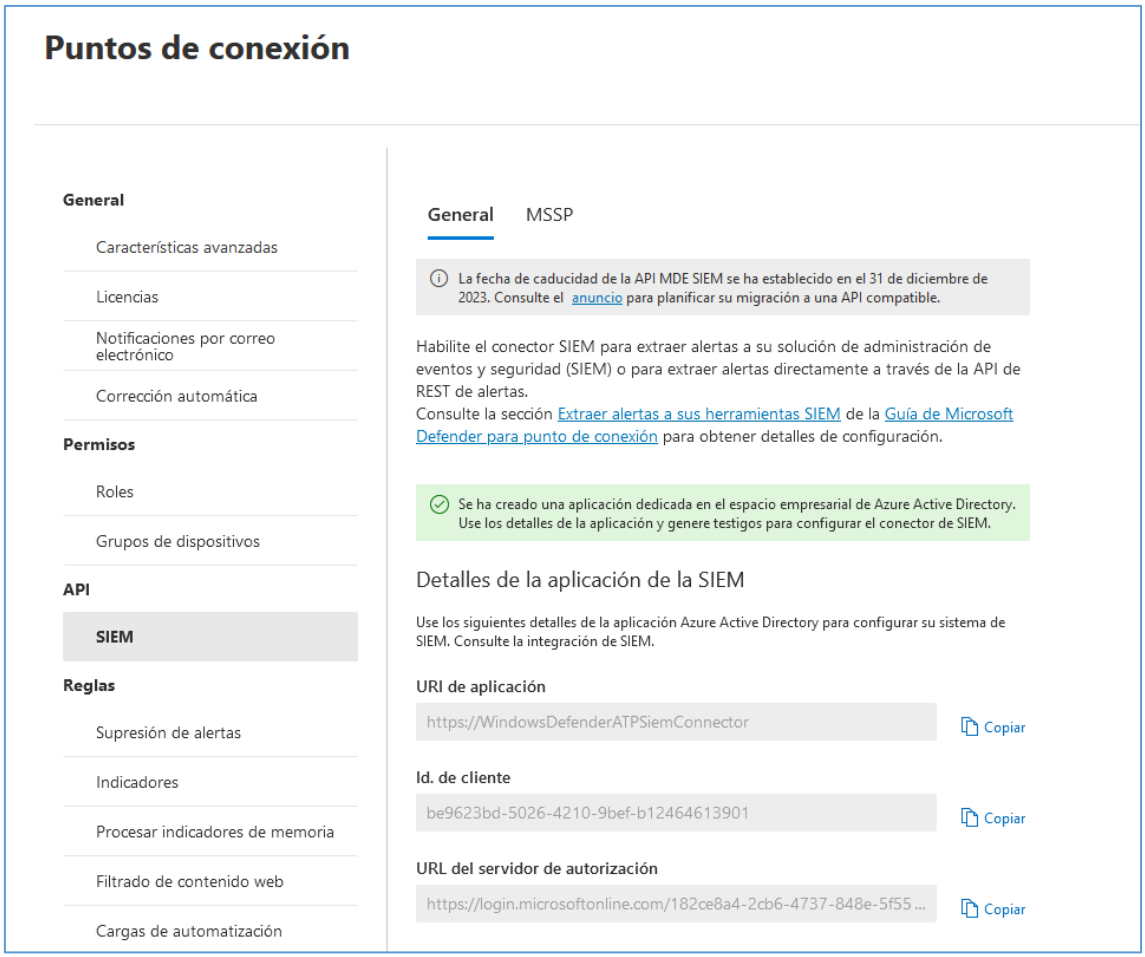


La explicación de cada uno de ellos en la sección [3.1.2.2 Segregación de funciones y tareas].

4.1.3 API

Se accede desde [Configuración|Puntos de conexión | APIs]

Desde esta sección se puede habilitar el conector SIEM para enviar alertas a la solución de gestión de eventos y seguridad (SIEM) o para generar alertas directamente a través de la API REST de alertas.

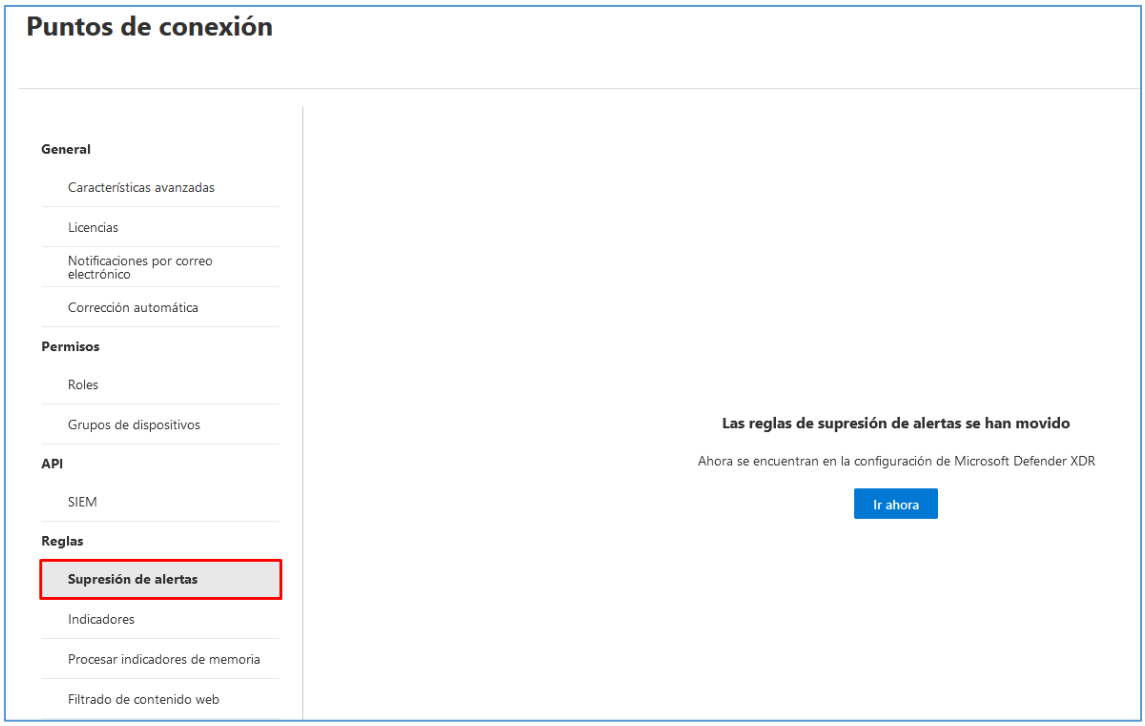


4.1.4 REGLAS

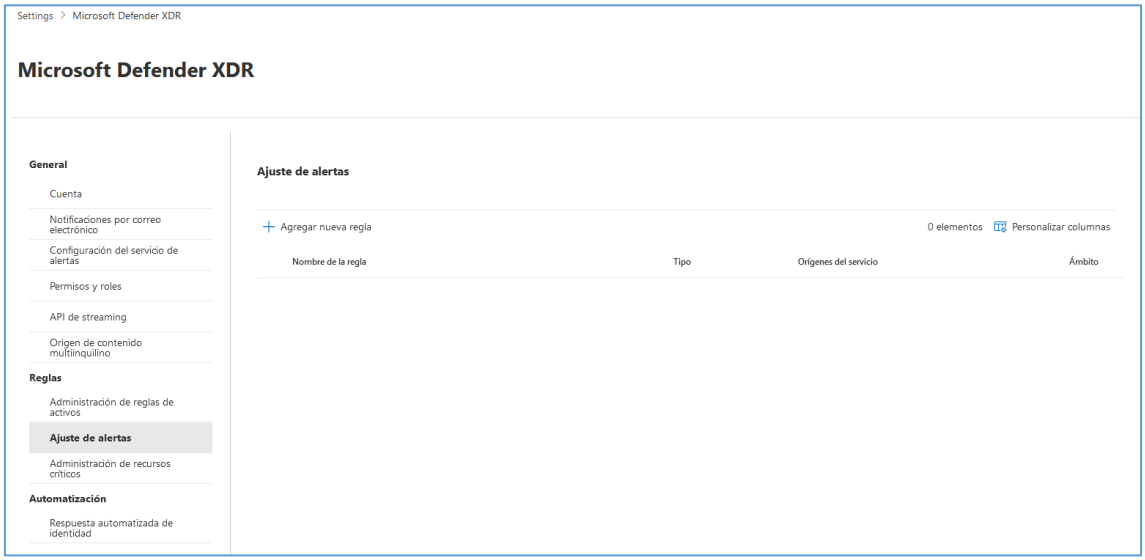
4.1.4.1 SUPRESIÓN DE ALERTAS

En algunos escenarios es deseable suprimir alertas para que no aparezcan en el portal. Pueden crearse reglas de supresión para alertas específicas que se sabe que son inocuas, como herramientas o procesos conocidos de la organización.

A través de [Configuración|Puntos de conexión | Reglas | Supresión de alertas] se puede llegar a la configuración de Microsoft Defender XDR, donde se ha movido esta opción.



Una vez en la nueva ubicación se obtiene una lista de todas las reglas de supresión, pudiéndose activar o desactivar cada regla de supresión de alertas.

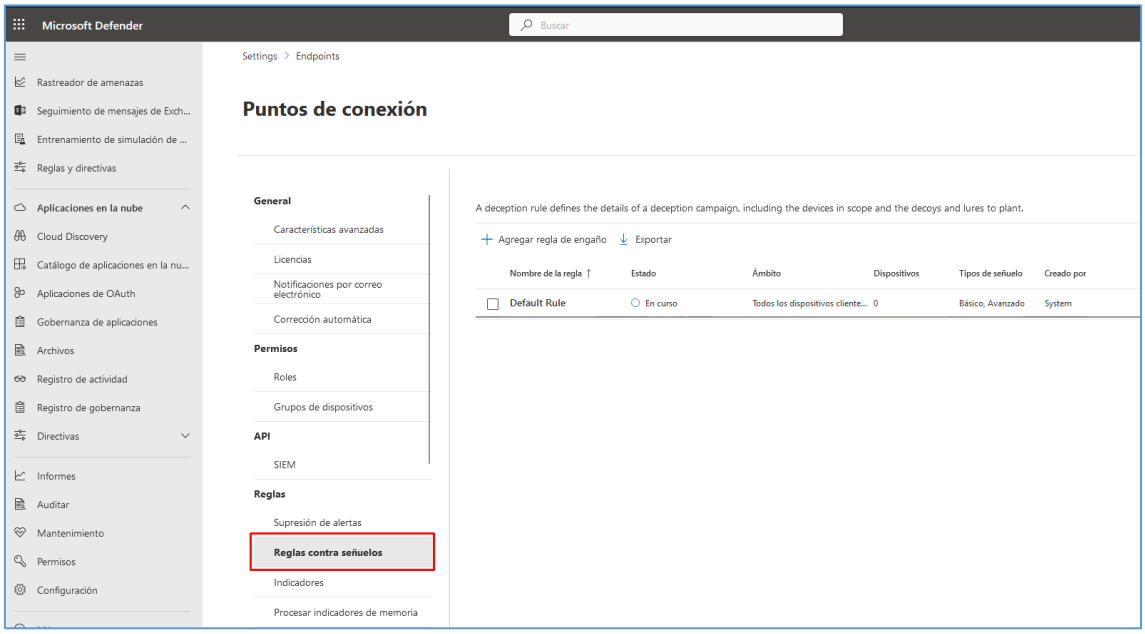


4.1.4.2 REGLAS CONTRA SEÑUELOS

La característica de señuelo del portal de Microsoft Defender usa reglas para generar señuelos que se ajustan al entorno. La característica utiliza el aprendizaje automático para proponer señuelos personalizados para la red. También se puede usar la característica de engaño para crear los señuelos manualmente. Estos señuelos se despliegan automáticamente en la red y se insertan en los dispositivos que elija mediante PowerShell.

Cuando un atacante usa un señuelo en cualquier cliente incorporado de Defender for Endpoint, la funcionalidad de engaño desencadena una alerta que indica la posible actividad del atacante, independientemente de si el engaño se implementó en el cliente o no.

Para la creación de reglas de señuelo se accede desde [Configuración|Puntos de conexión | Reglas | Reglas de señuelo]



Para más información sobre la creación de reglas de este tipo, acceder al enlace:

Configuración de la funcionalidad de engaño en Microsoft Defender XDR - Microsoft Defender XDR | Microsoft Learn

4.1.4.3 INDICADORES

Se accede desde [Configuración|Puntos de conexión | Reglas |Indicadores].

El indicador de coincidencia de puntos de conexión (IoCs) es una característica esencial en cada solución de protección de puntos de conexión. Esta funcionalidad ofrece al equipo de operaciones de seguridad (SecOps) la capacidad de establecer una lista de indicadores para la detección y para el bloqueo (prevención y respuesta).

Se pueden crear indicadores que definan la detección, prevención y exclusión de entidades, además de definir la acción que se va a realizar, así como la duración de la misma y el ámbito del grupo de dispositivos al que aplicarla.

Los orígenes compatibles actualmente son el motor de detección en la nube de Defender for Endpoint, el motor automatizado de investigación y corrección y el motor de prevención de puntos de conexión (Antivirus de Microsoft Defender).

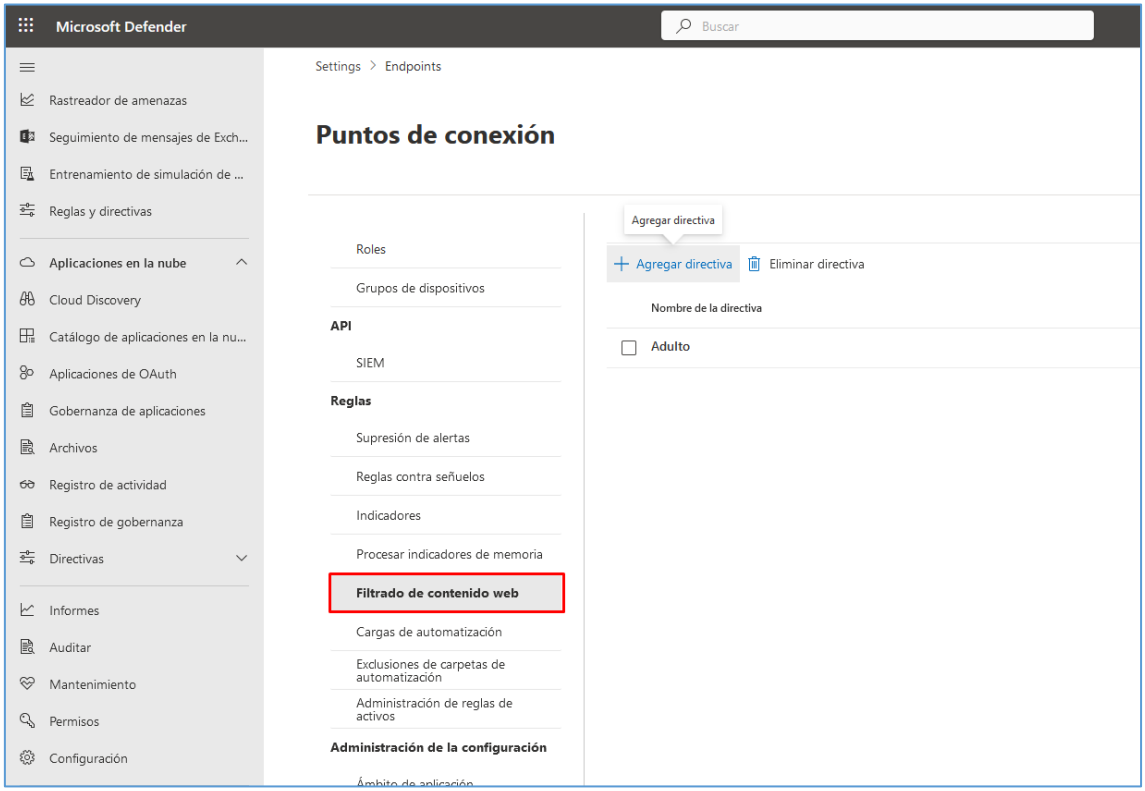
Más información en la página oficial de Microsoft:

Crear indicadores - Microsoft Defender for Endpoint | Microsoft Learn

4.1.4.4 FILTRADO DE CONTENIDO WEB

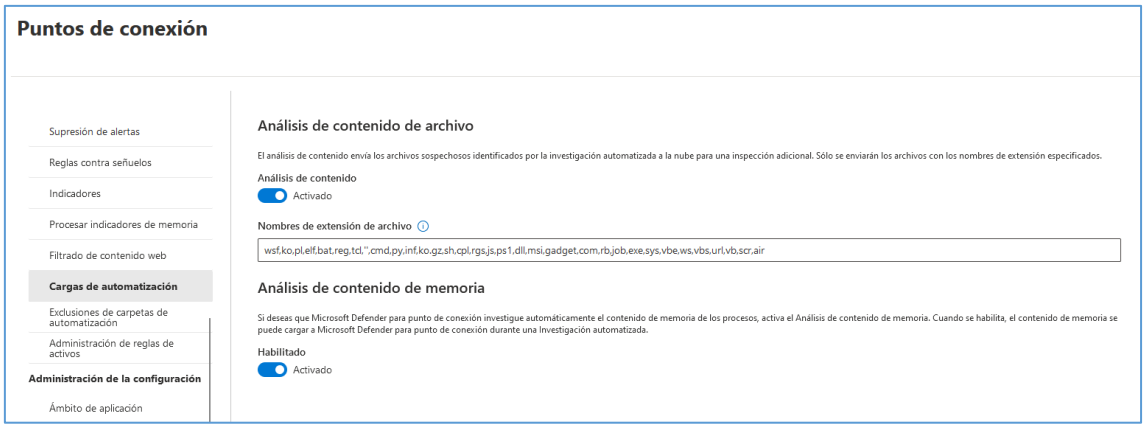
El filtrado de contenido web permite a la organización controlar y limitar el acceso a sitios web según tipos de contenido. Muchos de estos sitios web (aunque no tengan malas intenciones) pueden causar problemas por las normas de cumplimiento, el consumo del ancho de banda u otras cuestiones.

Los navegadores web más populares ofrecen filtros de contenido web, que bloquean sitios peligrosos con Windows Defender SmartScreen (Microsoft Edge) y protección de red (Chrome, Firefox, Brave y Opera).



4.1.4.5 ADMINISTRAR AUTOMATIZACIÓN DE CARGAS DE ARCHIVOS

Se accede desde [Configuración|Puntos de conexión | Reglas | Cargas de automatización].



Se recomienda habilitar la funcionalidad de análisis de contenido para que determinados archivos y datos adjuntos de correo electrónico se puedan cargar automáticamente en la nube para una inspección adicional en la investigación automatizada.

Identificar los archivos y los datos adjuntos de correo electrónico especificando los nombres de extensión de archivo y los nombres de extensión de datos adjuntos de correo electrónico.

Por ejemplo, si se agrega exe y bat como nombres de extensión de archivo o datos adjuntos, todos los archivos o datos adjuntos con esas extensiones se enviarán automáticamente a la nube para una inspección adicional durante la investigación automatizada.

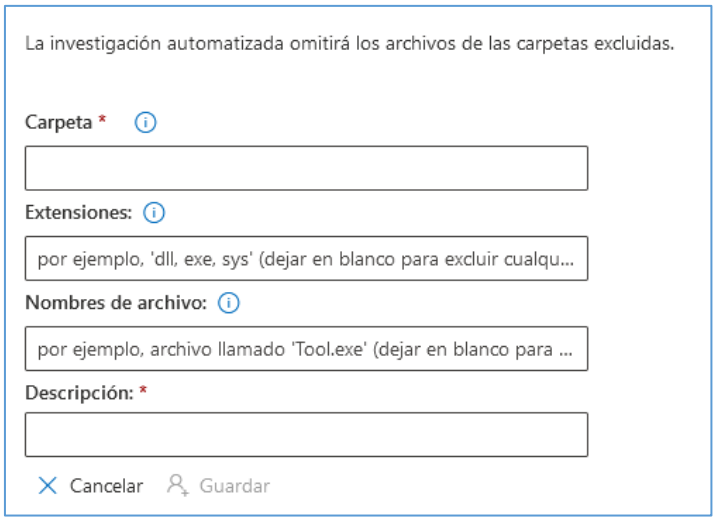
4.1.4.6 ADMINISTRAR LAS EXCLUSIONES DE CARPETAS DE AUTOMATIZACIÓN

Se accede desde [Configuración|Puntos de conexión | Reglas | Exclusión de carpetas de Automatización].

Las exclusiones de carpetas de automatización permiten especificar carpetas que omitirá la investigación automatizada.

Se pueden controlar los siguientes atributos acerca de la carpeta que desea omitir:

- Carpetas: para especificar una carpeta y las subcarpetas que se omitirán.
- Extensiones de los archivos: especificar las extensiones que se excluirán en un directorio específico. Las extensiones son una forma de impedir que un atacante use una carpeta excluida para ocultar una vulnerabilidad. Las extensiones definen explícitamente los archivos que se deben omitir.
- Nombres de archivo: se puede especificar los nombres de archivo que desea excluir en un directorio específico. Los nombres son una forma de impedir que un atacante use una carpeta excluida para ocultar una vulnerabilidad. Los nombres definen explícitamente los archivos que se deben omitir.



4.1.5 ADMINISTRACIÓN DE LA CONFIGURACIÓN

Microsoft Defender para punto de conexión permite aplicar directivas de seguridad de punto de conexión desde Microsoft Intune para gestionar la configuración de seguridad de Defender en los dispositivos que se han conectado a Defender sin registrar esos dispositivos con Intune. Esta funcionalidad se llama administración de la configuración de seguridad de Defender para punto de conexión.

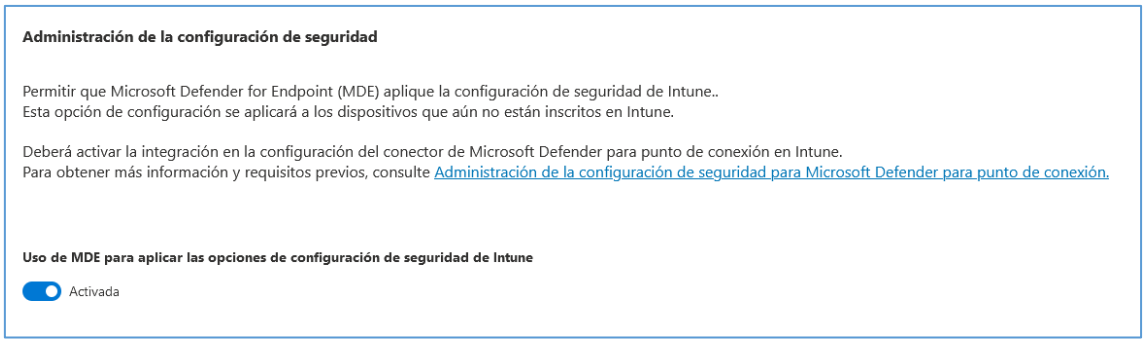
4.1.5.1 ADMINISTRACIÓN DE LA CONFIGURACIÓN DE SEGURIDAD

Al administrar dispositivos mediante la administración de la configuración de seguridad:

Se puede usar Microsoft Intune o el portal de Microsoft Defender XDR para configurar directivas de seguridad de puntos de conexión y asignar esas directivas a grupos de Microsoft Entra ID. El portal de Defender contiene la interfaz de usuario para ver dispositivos, administrar directivas e informes para gestionar la configuración de seguridad.

Para admitir la administración de la configuración de seguridad a través del centro de administración de Microsoft Intune, se debe habilitar la comunicación entre ellos desde cada consola.

Se accede desde [Configuración|Puntos de conexión | Administración de la configuración | Ámbito de aplicación].



Para la habilitación de la característica de Microsoft Intune, consultar la guía [CCN-STIC-884F – Guía de configuración segura para Microsoft Intune].

Para más información revisar la documentación oficial de Microsoft:

Use Intune para administrar la configuración de seguridad de Microsoft Defender en dispositivos que no están inscritos con Microsoft Intune | Microsoft Learn

4.1.6 ADMINISTRACIÓN DE DISPOSITIVOS

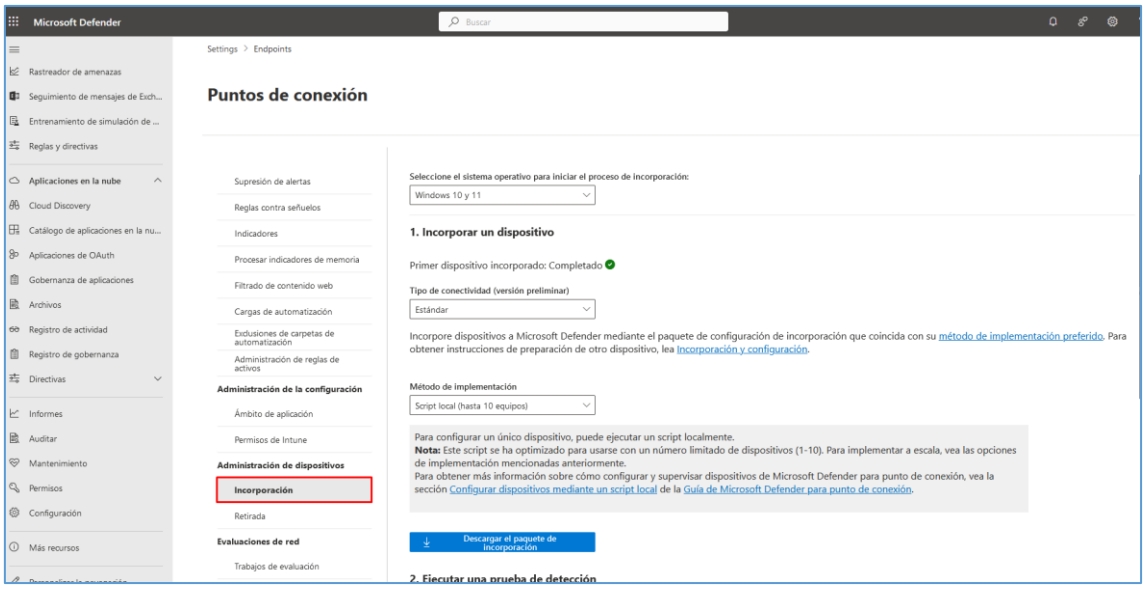
4.1.6.1 INCORPORACIÓN

Se accede desde [Configuración|Puntos de conexión | Administración de dispositivos|Incorporación].

Desde esta sección se puede incorporar cualquiera de los dispositivos compatibles, como se ha explicado previamente en la sección [2.6.3 Incorporación (Onboard)]. Según el dispositivo, se guiará con los pasos adecuados y se ofrecerán opciones de herramientas de administración e implementación adecuadas para el dispositivo.

En general, para incorporar dispositivos al servicio:

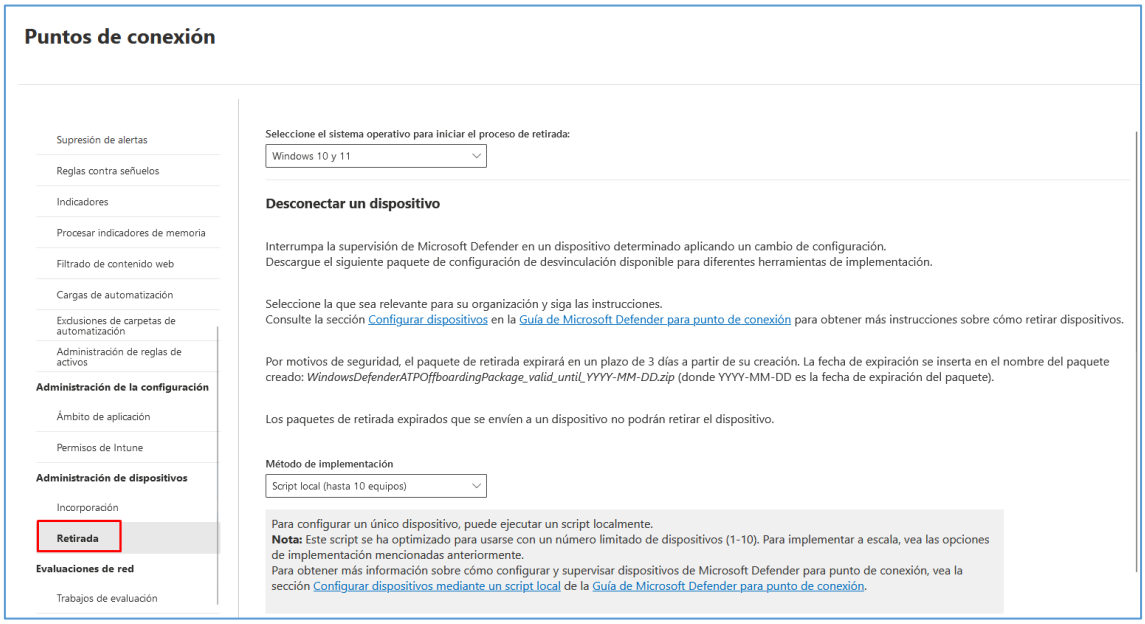
- Comprobar que el dispositivo cumple los requisitos mínimos.
- Según el dispositivo, seguir los pasos de configuración proporcionados.
- Usar la herramienta de administración y el método de implementación adecuados para los dispositivos.
- Ejecutar una prueba de detección para comprobar que los dispositivos están correctamente incorporados e informando al servicio



4.1.6.2 RETIRADA

Se accede desde [Configuración|Puntos de conexión | Administración de dispositivos|Retirada].

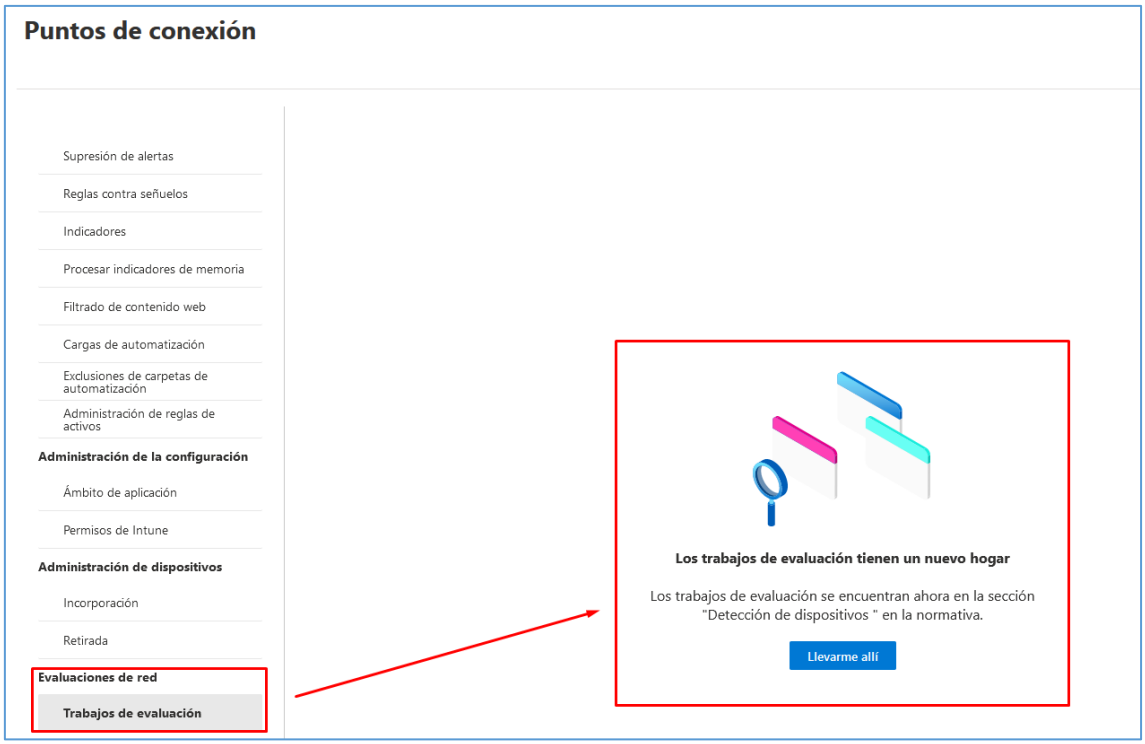
Para dejar de supervisar un dispositivo específico con Microsoft Defender, cambia una configuración.



4.1.7 EVALUACIONES DE RED

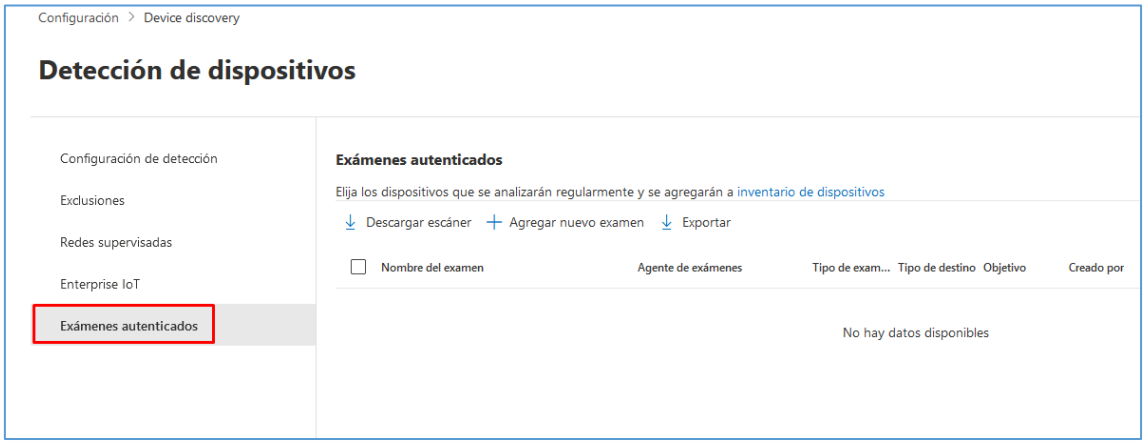
Se accede desde [Configuración|Puntos de conexión | Evaluaciones de red | Trabajos de evaluación].

Los trabajos de evaluación de red se han movido a la configuración general de Microsoft Defender, en la sección de Detección de dispositivos.



Renombrados como *Exámenes autenticados,* proporcionan la capacidad de ejecutar exámenes en dispositivos Windows no administrados.

Una vez configurados, los dispositivos no administrados de destino se examinarán periódicamente en busca de vulnerabilidades de software.



5. GLOSARIO Y ABREVIATURAS

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

Término	Definición
AAD	*Azure Active Directory* (Directorio Activo de Azure).
AD DS	*Active Directory Domain Services* (Servicios de dominio de Directorio Activo).
AIP	*Azure Information Protection.*
Azure AD	*Azure Active Directory*.
Azure RMS	*Azure Rights Management* (Azure RMS).
Centro de Administración de Microsoft 365	Portal de Administración de Office 365. Accesible desde la url: admin.microsoft.com.
Entra ID	*Microsoft Entra ID*
CSC	Centro de Seguridad y Cumplimiento de Office 365.
CSP	*Cloud Service Provider*
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.
EDR	*Endpoint Detection and Response.* Es una herramienta que proporciona monitorización y análisis continuo del endpoint y la red.
ENS	*Esquema Nacional de Seguridad.*
IoCs	Indicador de coincidencia de puntos de conexión
Hunting	Búsqueda avanzada de amenazas cibernéticas
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 Intune	Microsoft Intune es un servicio de administración de movilidad empresarial (EMM) basado en nube que ayuda a los empleados a ser productivos mientras mantiene protegidos los datos corporativos. Al igual que otros servicios de Azure, Microsoft Intune está disponible en el portal de Azure. **Intune** permite: - Administrar los dispositivos móviles y los equipos que los empleados usan para tener acceso a datos de la empresa. - Administrar las aplicaciones móviles que usa la plantilla. - Proteger la información de la empresa al ayudar a controlar la manera en que los empleados tienen acceso a ella y la comparten. - Garantizar que los dispositivos y las aplicaciones sean compatibles con los requisitos de seguridad de la empresa
O365	*Office 365.*
Onboarding	Proceso de incorporación de dispositivos
PE	El formato Portable Executable (PE) es un formato de archivo para archivos ejecutables, de código objeto, bibliotecas de enlace dinámico (DLL), y otros usados en versiones de 32 bit y 64 bit del sistema operativo Microsoft Windows.
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*).
PS	*PowerShell*.
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.
Sensitivity label	*Etiqueta de sensibilidad.* Permiten clasificar, cifrar, agregar marcadores y controlar accesos en documentos y correos electrónicos en Office 365.
Spectre y Meltdown	Tanto Spectre como Meltdown son dos vulnerabilidades descubiertas en las CPU.
SOC	SOC (*Security Operations Center*) o Centro de Operaciones de Seguridad

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.
XDR	Solución que unifica múltiples productos de seguridad en una sola plataforma para mejorar la detección, investigación y respuesta a amenazas
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.

6. CUADRO RESUMEN DE MEDIDAS DE SEGURIDAD

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

<table>
<tr><th>Control ENS</th><th colspan="3">Configuracion</th><th>Estado</th></tr>
<tr><td>op</td><td colspan="4">Marco Operacional</td></tr>
<tr><td>op.acc</td><td colspan="4">Control de Acceso</td></tr>
<tr><td rowspan="3">op.acc.1</td><td colspan="4">Identificación</td></tr>
<tr><td colspan="2" rowspan="2">Se ha realizado adecuadamente la gestión de identidades.</td><td>Aplica:
☐ Sí ☐ No</td><td>Cumple:
☐ Sí ☐ No</td></tr>
<tr><td>Evidencias Recogidas:
☐ Sí ☐ No</td><td>Observaciones:</td></tr>
<tr><td>op.acc.3</td><td colspan="4">Segregación de funciones y tareas</td></tr>
</table>

	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 y se dispone de una adecuada política de gestión de credenciales.	**Aplica:** ☐ Sí ☐ No	**Cumple:** ☐ Sí ☐ No

		Evidencias Recogidas: ☐ Sí ☐ No	**Observaciones:**
op.acc.6	**Mecanismo de autenticación (usuarios de la organización)**		
	Se ha activado la *Ubicación de red* para permitir el acceso solo desde determinadas direcciones IP. Y la limitación de acceso a los administradores.	**Aplica:** ☐ Sí ☐ No	**Cumple:** ☐ Sí ☐ No
		Evidencias Recogidas: ☐ Sí ☐ No	**Observaciones:**
op.mon	**Monitorización del sistema**		
	Se ha activado el registro de auditoría para ver los datos en los informes de protección contra amenazas y poder explotar la herramienta Explorador.	**Aplica:** ☐ Sí ☐ No	**Cumple:** ☐ Sí ☐ No
		Evidencias Recogidas: ☐ Sí ☐ No	**Observaciones:**
op.vig	**Vigilancia**		

	Se ha revisado la configuración actual, con los planes estrictos o estandar que nos ofrece Microsoft para seguir sus buenas prácticas.	**Aplica:** ☐ Sí ☐ No	**Cumple:** ☐ Sí ☐ No
		Evidencias Recogidas: ☐ Sí ☐ No	**Observaciones:**
Otras	**Configurar notificaciones de alertas y vulnerabilidades**		
	Se ha configurado *Defender for Endpoint* para enviar notificaciones por correo electrónico a destinatarios específicos para nuevas alertas. * Esta característica posibilita identificar un grupo de personas que se informarán inmediatamente y podrán actuar en función de la gravedad de alerta.	**Aplica:** ☐ Sí ☐ No	**Cumple:** ☐ Sí ☐ No
		Evidencias Recogidas: ☐ Sí ☐ No	**Observaciones:**
Otras	**Periodo de retención**		
	Se ha establecido una retención adecuada de los datos en la instancia Cloud.	**Aplica:** ☐ Sí ☐ No	**Cumple:** ☐ Sí ☐ No
		Evidencias Recogidas: ☐ Sí ☐ No	**Observaciones:**

Otras	**Investigación automatizada**		
	Se han habilitado las capacidades de automatización para investigación y respuesta.	**Aplica:** ☐ Sí ☐ No	**Cumple:** ☐ Sí ☐ No
		Evidencias Recogidas: ☐ Sí ☐ No	**Observaciones:**
Otras	**Habilitar EDR en modo bloqueo**		
	Se ha activado para aprovechar las capacidades de contención bloqueando los comportamientos o artefactos maliciosos observados a través de las capacidades de detección y respuesta de puntos de conexión (EDR) posteriores a la infracción.	**Aplica:** ☐ Sí ☐ No	**Cumple:** ☐ Sí ☐ No
		Evidencias Recogidas: ☐ Sí ☐ No	**Observaciones:**
Otras	**Resolver alertas automáticamente**		
		Aplica: ☐ Sí No	**Cumple:** ☐ Sí ☐ No

	Se ha activado la resolución automática de alertas. Es recomendable resolver una alerta si la investigación automatizada no encuentra amenazas o ha solucionado con éxito todos los artefactos maliciosos.	☐	
		Evidencias Recogidas: ☐ Sí ☐ No	**Observaciones:**
Otras	**Mostrar detalles de usuario**		
	Se ha habilitado el mostrar los detalles del usuario: imagen, nombre, cargo, departamento, almacenados en Entra ID.	**Aplica:** ☐ Sí ☐ No	**Cumple:** ☐ Sí ☐ No
		Evidencias Recogidas: ☐ Sí ☐ No	**Observaciones:**
Otras	**Integración con Microsoft Defender for Identity**		
	Se ha activado la integración con Microsoft Defender for Identity.	**Aplica:** ☐ Sí ☐ No	**Cumple:** ☐ Sí ☐ No
		Evidencias Recogidas: ☐ Sí ☐ No	**Observaciones:**

Otras	**Conexión de Microsoft Threat Intelligence (Inteligencia de amenzas)**		
	Se ha habilitado la conexíon de Microsoft Threat Intelligence (Inteligencia de amenzas).	**Aplica:** ☐ Sí ☐ No	**Cumple:** ☐ Sí ☐ No
		Evidencias Recogidas: ☐ Sí ☐ No	**Observaciones:**
Otras	**Integración Cloud App**		
	Se ha habilitado la integración Cloud App.	**Aplica:** ☐ Sí ☐ No	**Cumple:** ☐ Sí ☐ No
		Evidencias Recogidas: ☐ Sí ☐ No	**Observaciones:**
Otras	**Conexión de Microsoft Intune**		
	Se ha habilitado la conexión a Microsoft Intune para permitir compartir la información del dispositivo y mejorar la aplicación de políticas.	**Aplica:** ☐ Sí ☐ No	**Cumple:** ☐ Sí ☐ No

		Evidencias Recogidas: ☐ Sí ☐ No	**Observaciones:**
Otras	**Descubrimiento de dispositivos (Device Discovery)**		
	Se ha activado para permitir que los dispositivos incorporados descubran dispositivos no administrados en la red y evalúen vulnerabilidades y riesgos.	**Aplica:** ☐ Sí ☐ No	**Cumple:** ☐ Sí ☐ No
		Evidencias Recogidas: ☐ Sí ☐ No	**Observaciones:**
Otras	**Indicador de coincidencia de puntos de conexión (IoCs)**		
	Se han creado indicadores de coincidencia de puntos de conexión (IoCs).	**Aplica:** ☐ Sí ☐ No	**Cumple:** ☐ Sí ☐ No
		Evidencias Recogidas: ☐ Sí ☐ No	**Observaciones:**
Otras	**Administrar automatización de cargas de archivos**		

	Se ha habilitado la funcionalidad de análisis de contenido para que determinados archivos y datos adjuntos de correo electrónico se puedan cargar automáticamente en la nube para una inspección adicional en la investigación automatizada.	**Aplica:** ☐ Sí ☐ No	**Cumple:** ☐ Sí ☐ No
		Evidencias Recogidas: ☐ Sí ☐ No	**Observaciones:**
Otras	**Administrar las exclusiones de carpeta de automatización**		
	Se han especificado exclusiones de carpetas de automatización para permitir especificar carpetas que omitirá la investigación automatizada.	**Aplica:** ☐ Sí ☐ No	**Cumple:** ☐ Sí ☐ No
		Evidencias Recogidas: ☐ Sí ☐ No	**Observaciones:**
Otras	**Administración de dispositivos**		
	Se ha realizado una prueba de detección para comprobar que los dispositivos están correctamente incorporados e informando al servicio.	**Aplica:** ☐ Sí ☐ No	**Cumple:** ☐ Sí ☐ No
		Evidencias Recogidas: ☐ Sí ☐ No	**Observaciones:**

Otras	**Configurar zona horaria**		
	Se ha establecido una correcta configuración de la zona horaria	**Aplica:** ☐ Sí ☐ No	**Cumple:** ☐ Sí ☐ No
		Evidencias Recogidas: ☐ Sí ☐ No	**Observaciones:**
Otras	**Trabajo de evaluación de la red**		
	Se han añadido un trabajo de evaluación de la red para ejecutar análisis en dispositivos de red no administrados.	**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