Guía de Seguridad de las TIC
CCN-STIC 884F

Guía de configuración segura para Microsoft Intune

MAYO 2024

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

Edita:

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2024.05.30 12:17:39 +02'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-24-183-0
Fecha de Edición: mayo de 2024

ÍNDICE

1. MICROSOFT INTUNE

1.1 DESCRIPCIÓN DEL USO DE ESTA GUÍA

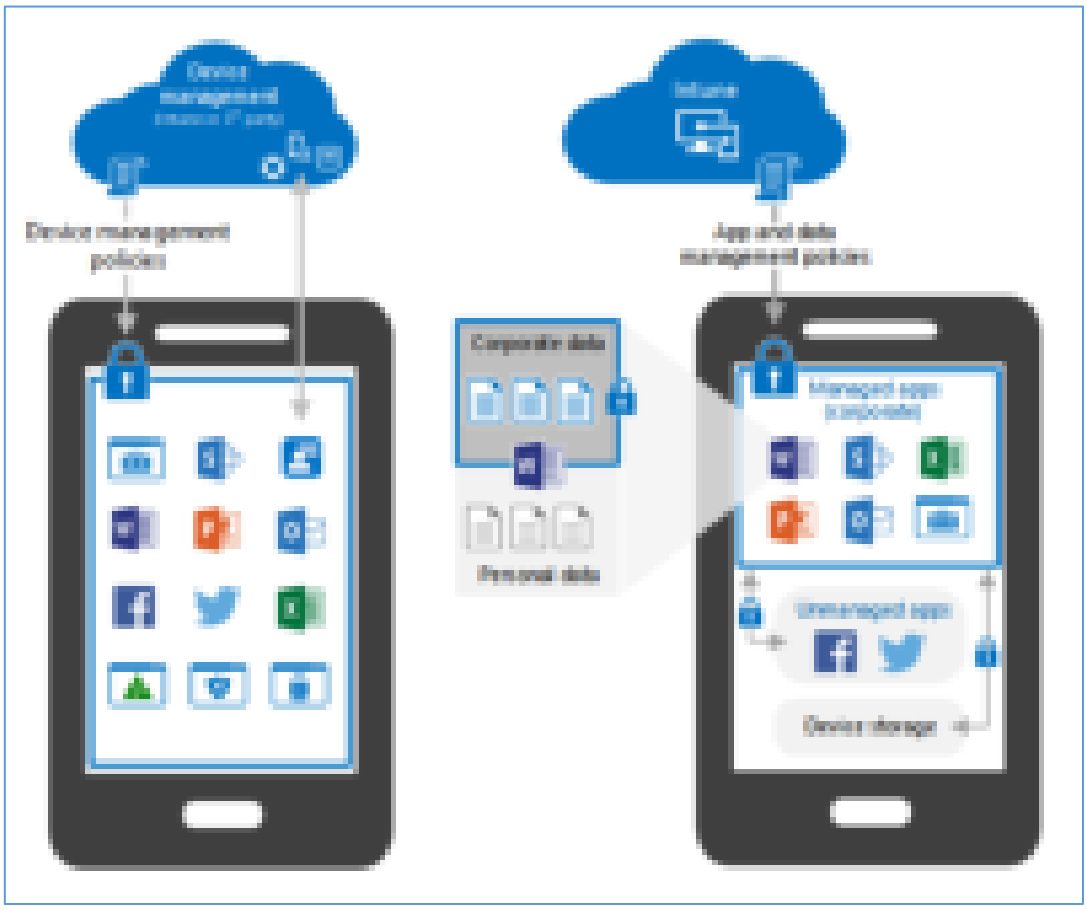
El objetivo de la presente guía es indicar los pasos a seguir para la configuración de Guía de configuración segura para Microsoft Intune cumpliendo con los requisitos *Esquema Nacional de Seguridad*.

1.2 DEFINICIÓN DE LA SOLUCIÓN

Microsoft Intune es una solución de administración de dispositivos basada en la nube. Administra el acceso de los usuarios a los recursos de la organización y simplifica la administración de aplicaciones y dispositivos, incluidos dispositivos móviles, equipos de escritorio y puntos de conexión virtuales.

Se puede proteger el acceso y los datos en dispositivos propiedad de la organización y en personales de usuarios. Además, Intune tiene características de cumplimiento e informes que respaldan el modelo de seguridad de Confianza cero.

Microsoft Intune es un componente de Enterprise Mobility + Security (EMS) que gestiona dispositivos móviles y aplicaciones. Está integrado estrechamente con otros componentes EMS como Entra ID para control de acceso e identidad.



- Habilidad de restringir el acceso a SharePoint Online, Exchange On-premises y Exchange Online Email basado en la inscripción de dispositivo y directivas de cumplimiento.
- Gestión de aplicaciones móviles (Word, Excel, PowerPoint) para dispositivos móviles, incluido restringir acciones tales como copiar, cortar y pegar fuera del ecosistema gestionado por la herramienta.
- Gestión de la aplicación buscador y Edge de Microsoft para dispositivos Android\iOS pudiendo controlar las acciones que realizan los usuarios, incluido permitir o denegar el acceso a páginas web específicas.
- Despliegue de certificados, Wi-Fi, VPN y perfiles de correo automáticamente a un dispositivo inscrito, habilitando así el acceso a los usuarios para acceder a los recursos de la organización con las configuraciones de seguridad apropiadas.
- Proporcionar con la aplicación Portal de Empresa, un autoservicio para que los usuarios se inscriban en sus propios dispositivos e instalar aplicaciones corporativas.
- Gestión moderna de Windows 10.
- Publicación y despliegue de aplicaciones en dispositivos gestionados.
- Informes y mediciones del cumplimiento de las normas corporativas por parte de los dispositivos.
- Retiro de dispositivos y borrado de datos corporativos de dispositivos gestionados.
- Borrado de datos corporativos para dispositivos en modo BYOD.

Microsoft Intune combina capacidades en la nube y entornos On-Premises. De esta forma, las organizaciones pueden facilitar a sus empleados el acceso a aplicaciones corporativas, datos y recursos desde prácticamente cualquier lugar y en casi cualquier dispositivo, mientras ayudamos a mantener segura la información corporativa.

Si en la infraestructura se tiene todavía dependencia de la parte On-Premises, se puede configurar **Co-Management** con Configuration Manager, el cual permite gestionar dispositivos Windows con Microsoft Intune y SCCM al mismo tiempo.

Co-Management permite gestionar simultáneamente los dispositivos de Windows utilizando tanto SCCM como Microsoft Intune, así el dispositivo se registra en Entra ID y Microsoft Intune, al mismo tiempo que se une al dominio local y se gestiona por SCCM.

Además, también es posible configurar **Tenant-attach**, que permite gestionar los dispositivos de SCCM desde el centro de administración de Intune.

1.3 PRERREQUISITOS MICROSOFT INTUNE

Para poder utilizar la solución de Microsoft Intune, es necesario cumplir unos requisitos mínimos.

Licenciamiento

Microsoft Intune está disponible como un servicio de Azure independiente, como parte de Enterprise Mobility + Security (EMS) y, además, está incluido en Microsoft 365.

- Microsoft Intune Plan 1 se incluye en las siguientes licencias:
  - Microsoft 365 E5
  - Microsoft 365 E3
  - Enterprise Mobility + Security E5
  - Enterprise Mobility + Security E3
  - Microsoft 365 Empresa Premium
  - Microsoft 365 F1
  - Microsoft 365 F3
  - Microsoft 365 Administración Pública G5
  - Microsoft 365 Administración Pública G3
  - Intune para educación
- Intune Plan 1 para educación se incluye en las siguientes:
  - Microsoft 365 Education A5
  - Microsoft 365 Education A3
- Intune Plan 2, que es un complemento de Intune Plan 1 que ofrece funcionalidades avanzadas en la administración de los dispositivos. Este Plan 2 se incluye en Microsoft Intune Suite.

Un administrador debe tener una licencia asignada para administrar Microsoft Intune (a menos que permita a los administradores usar Microsoft Intune sin licencia).

Se puede conceder a los administradores acceso a Microsoft Intune sin necesidad de una licencia de Microsoft Intune. Esto aplica a cualquier administrador, incluidos los administradores de Microsoft Intune, los administradores globales, los administradores de Entra ID, etc.

Se puede activar esta característica en el centro de administración de Microsoft Intune.

1. **Administración de inquilinos > Roles > Licencias de administrador**.
2. Se habilita la opción **Permitir el acceso a administrador sin licencia**.

Esta opción no se puede deshacer después de habilitarla.

A partir de ahora cualquier usuario que inicie sesión en la consola de administración de Microsoft Intune no requerirá de una licencia para su administración, ámbito de acceso solo se definirá mediante los roles que tenga asignados.

1.4 GUÍA DE IMPLEMENTACIÓN O MIGRACIÓN A MICROSOFT INTUNE

Una vez se haya elaborado el plan para migrar a Microsoft Intune, el siguiente paso es determinar el método de migración más adecuado para la organización. Hay varios escenarios de los cuales se puede partir:

- Actualmente, no se utiliza ninguna herramienta para la gestión de dispositivos.
- Si se utiliza un proveedor MDM de terceros.
- Si se utiliza Configuration Manager.
- Se están utilizando directivas de grupo locales.
- Si se usa Microsoft 365 Básico Movilidad y seguridad.

A continuación, se puede ver en detalle las opciones que se permiten en cada escenario.

1.4.1 SIN USO ACTUAL DE HERRAMIENTAS DE GESTIÓN

Existen las siguientes opciones si actualmente no se usa ningún proveedor de administración de aplicaciones móviles MAM o MDM:

- **Microsoft Intune**. Microsoft Intune es una solución directamente en la nube. Al optar por esta herramienta se obtienen las características de cumplimiento, configuración de las características del dispositivo, implementación de aplicaciones y las políticas de actualización del sistema & aplicación.
- **Configuration Manager**. Si se está considerando el uso de las características de Configuration Manager con la combinación de gestión en la nube, se tiene la opción de usar una asociación de inquilinos o administración conjunta, comúnmente llamada Co-management. Si se utiliza Configuration Manager:
    - Se pueden gestionar dispositivos locales, como Windows Server.
    - Gestión de actualizaciones de software de asociados o terceros.
    - Creación de secuencias de tareas personalizadas al implementar sistemas operativos.
    - Despliegue e implementación de aplicaciones.

1.4.2 USO ACTUAL DE HERRAMIENTA MDM DE TERCEROS

Es aconsejable que los dispositivos solo estén gestionados por un proveedor de MDM, ya que podría haber conflictos. Si, por ejemplo, se está usando actualmente otro MDM como Workspace ONE o MobileIron, se puede migrar a Microsoft Intune.

Desde Microsoft se recomienda lo siguiente si la empresa se encuentra en este escenario:

- Método por fases, es decir, empezar por un pequeño grupo de usuarios piloto y, una vez que funcione, ir agregando más grupos hasta completar la implementación.
- Es una buena práctica anotar las tareas que realiza el MDM/MAM actual e implementarlas en Microsoft Intune. Este método da una idea de cómo empezar a configurar la herramienta de Microsoft Intune.
- Es recomendable que exista un departamento de soporte técnico que supervise el éxito de inscripción en cada fase, se deben evaluar los criterios de éxito de cada grupo y fase antes de comenzar con la siguiente.
- Una implementación de Microsoft Intune piloto debe validar las siguientes tareas:
    - Comprobar que el porcentaje de éxito y error en la inscripción sea el esperado.
    - Se debe comprobar el funcionamiento de los recursos corporativos configurados, como VPN, Wi-Fi, correo electrónico y certificados, además del acceso a las aplicaciones implementadas.
    - Se deben revisar los informes de cumplimiento para comprobar si existen problemas para su posterior resolución.
    - Que se han aplicado protección a las aplicaciones móviles.
- Una vez se completa la primera fase de las migraciones y se está satisfecho con los resultados, se repite el proceso de migración en la siguiente fase.
    - Este ciclo de migraciones por fases se repetirá sucesivamente hasta que todos los usuarios hayan sido migrados satisfactoriamente a Intune.
    - Es fundamental asegurarse de que el departamento de soporte técnico esté completamente preparado para brindar asistencia a los usuarios finales durante todo el proceso de migración. Se llevará a cabo una migración voluntaria inicial para evaluar la carga de trabajo del soporte técnico.
    - No se establecerán fechas límite para la inscripción hasta que el departamento de soporte técnico esté en condiciones de controlar la totalidad de usuarios restantes de manera efectiva.

1.4.3 USO ACTUAL DE CONFIGURATION MANAGER

El Configuration Manager permite dispositivos Windows, MacOS y Windows Server. Si actualmente se usa esta herramienta en la empresa y se quiere usar también Microsoft Intune, se disponen de los siguientes métodos:

- Método 1: Asociación de Inquilinos

Con el método de asociación de inquilinos, se permite cargar los dispositivos existentes en el entorno de Configuration Manager en la infraestructura de Microsoft Intune.

Una vez estén asociados los dispositivos en Microsoft Intune, se podrán realizar acciones a los mismos desde la consola de Microsoft Intune.

Esta asociación está incluida con la licencia de administración conjunta de Configuration Manager (Preguntas más frecuentes sobre productos y licencias - Configuration Manager | Microsoft Learn)

Para más información sobre el proceso de habilitar la asociación entre inquilinos:

Habilitación de Microsoft Intune asociación de inquilinos - Configuration Manager | Microsoft Learn

- Método 2: Administración conjunta

  Con la administración conjunta, se usa Configuration Manager para unas tareas y Microsoft Intune para otras. Para habilitar la administración conjunta se puede ver información más en detalle en el siguiente enlace.

  Habilitar la administración conjunta: - Configuration Manager | Microsoft Learn

  Una vez se tiene habilitada la administración conjunta, simplemente hay que implementar Microsoft Intune y establecer la autoridad MDM en Microsoft Intune.

  Al trabajar en administración conjunta, las cargas de trabajo se reparten entre Configuration Manager y Microsoft Intune consiguiendo un equilibrio y asegurándose de que no existan conflictos.

- Método 3: Migración de Configuration Manager a Microsoft Intune

  La mayoría de los clientes que ya utilizan Configuration Manager desean seguir haciéndolo, ya que ofrece servicios beneficiosos para los dispositivos locales.

  Sin embargo, para aquellos usuarios que buscan una solución completamente en la nube, se ofrece una opción adicional. Con esta opción, pueden:

  1. Registrar los dispositivos cliente de Windows existentes en el Active Directory local como dispositivos en Microsoft Intune.
  2. Migrar las cargas de trabajo locales existentes de Configuration Manager a Intune.

- Método 4: Empezar de cero con Microsoft 365 e Intune

  Para administrar los dispositivos cliente de Windows:

  1. Implementar Microsoft 365, lo que implica la creación de usuarios y grupos. Evitar el uso o la configuración de Microsoft 365 Básico Mobility and Security.

     Información general de Microsoft 365 para empresas - Microsoft 365 Enterprise | Microsoft Learn

2. Configuración de Intune, incluida la configuración de la entidad de MDM en Intune.
3. En los dispositivos existentes, se debe proceder a desinstalar el cliente de Configuration Manager (Administrar clientes - Configuration Manager | Microsoft Learn).

Una vez realizado esto, los dispositivos estarán listos para ser inscritos en Intune y recibir las políticas y directivas correspondientes.

2. DESPLIEGUE DE MICROSOFT INTUNE

Los siguientes apartados ayudarán a montar la infraestructura necesaria para habilitar la administración de dispositivos (MDM) mediante Microsoft Intune.

Antes de conceder acceso a los recursos de la empresa, los dispositivos deben administrarse mediante Microsoft Intune.

Algunas configuraciones, como la suscripción a Microsoft Intune y de la identidad de MDM, son necesarios en casi todos los escenarios. Otras configuraciones como la de crear un dominio personalizado o agregar aplicaciones, son opcionales.

2.1 CONFIGURACIÓN

Las siguientes configuraciones ayudaran a habilitar la administración de dispositivos móviles mediante Intune.

Hay algunas configuraciones como la configuración de una suscripción a Intune o la configuración de la entidad MDM que son prácticamente obligatorias para la utilización de esta herramienta.

Por otro lado, configuraciones como el despliegue de aplicaciones o la configuración de un dominio personalizado son opcionales.

2.1.1 CONFIGURACIONES ADMITIDAS

A continuación, se exponen los diferentes sistemas operativos y navegadores web compatibles con la plataforma de Microsoft Intune.

2.1.1.1 SISTEMAS OPERATIVOS Y EXPLORADORES COMPATIBLES CON INTUNE

Antes de empezar a configurar Microsoft Intune, es prioritario saber que sistemas operativos y exploradores Web son compatibles con la herramienta:

Sistemas operativos admitidos por Microsoft Intune

Los siguientes sistemas operativos pueden ser administrador por Microsoft Intune:

Apple:

- Apple iOS 15.0 y versiones posteriores.
- Apple iPadOS 15.0 y versiones posteriores.
- MacOS X 12.0 y versiones posteriores.

Android:

- Android 8.0 y versiones posteriores (incluido Samsung KNOX Standard 3.0 y versiones posteriores).
- Android Enterprise.
- Dispositivo de proyecto de Android código abierto.

Linux:

- Ubuntu Desktop 22.04 LTS con entorno gráfico de escritorio GNOME.
- Ubuntu Desktop 20.04 LTS con entorno gráfico de escritorio GNOME.

Microsoft:

- Surface Hub.
- Windows 10/11 (versiones Home, S, Pro, Education, Enterprise e IoT Enterprise).
- Equipos en la nube Windows 10/11 en Windows 365.
- Windows 10 LTSC 2019/2021 (versiones Enterprise e IoT Enterprise).
- Windows 10 1709 (RS3) y versiones posteriores, Windows 8.1 RT, equipos que ejecutan Windows 8.1 (modo de mantenimiento).
- Windows Holographic for Business.
- Windows 10 Teams (Surface Hub).

Actualmente, Microsoft Intune no admite la administración de dispositivos habilitados para el filtro de escritura unificado (UWF) (Característica de filtro de escritura unificada (UWF) (unified-write-filter) | Microsoft Learn).

Exploradores Web compatibles con Microsoft Intune

Las diferentes tareas administrativas requieren que se use uno de los siguientes sitios web de administración.

- https://intune.microsoft.com
- https://portal.azure.com

Estos portales son compatibles con los siguientes exploradores:

- Microsoft Edge (versiones más recientes).
- Safari (versión más reciente, solo Mac).
- Chrome (versión más reciente).
- Firefox (versión más reciente).

2.1.2 ANCHO DE BANDA Y REQUISITOS DE CONFIGURACIONES DE RED

Para asegurarse de que los dispositivos reciban actualizaciones y contenido de Microsoft Intune, se deben conectar a Internet de forma periódica. El tiempo que se requiere para recibir actualizaciones o contenido puede variar, pero los dispositivos deben permanecer conectados de forma continua a Internet como mínimo una hora al día.

En la siguiente tabla se expone el tráfico de red medio que muestra el tamaño aproximado y la frecuencia de contenido común que pasa a través de la red de cada cliente.

Tipo de contenido	Tamaño aproximado	Frecuencia y detalles
Instalación cliente de Intune	125 MB	Una vez
Paquete de inscripción de cliente	15 MB	Una vez
Agente de Endpoint Protection	65 MB	Una vez
Agente de Operations Manager	11 MB	Una vez
Agente de directivas	3 MB	Una vez
Asistencia remota a través de agente Microsoft Easy Assist	6 MB	Una vez
Operaciones diarias de cliente Service Pack	6 MB	A diario
Actualizaciones de definiciones de malware de Endpoint Protection	Varía De 40 KB a 2 MB	Hasta 3 veces al día.
Actualización del motor de Endpoint Protection	5 MB	Mensualmente
Actualizaciones de software	Varía El tamaño depende de las actualizaciones que implementa	Mensualmente
Service Pack	Varía El tamaño varía para cada Service Pack implementado	Depende de cuándo se implementan los Service Pack
Distribución de software	Varía El tamaño depende del software implementado	Depende de cuándo se implementa el software

Se puede usar uno de los siguientes métodos para reducir el uso de ancho de banda de red de los clientes de Microsoft Intune.

Utilizar un servidor proxy para almacenar en caché solicitudes de contenido

Un servidor proxy tiene la capacidad de almacenar en caché contenido con el fin de reducir la duplicación de descargas y minimizar el uso del ancho de banda de red para acceder al contenido de Internet.

Cuando un servidor proxy de almacenamiento en caché recibe solicitudes de contenido de los clientes, puede recuperar ese contenido y guardar tanto las respuestas web como las descargas en su memoria caché. Posteriormente, cuando se reciben solicitudes similares, el servidor puede responder utilizando los datos almacenados en caché en lugar de solicitar nuevamente el contenido desde Internet.

Si utilizas un servidor proxy para almacenar en caché las solicitudes de contenido, la comunicación se cifra solamente entre el cliente y el proxy, así como desde el proxy a Microsoft Intune. Sin embargo, la conexión directa desde el cliente a Microsoft Intune no estará cifrada de extremo a extremo.

Optimización de entrega

La optimización de entrega mediante Microsoft Intune te permite disminuir el uso del ancho de banda cuando los dispositivos Windows 10 descargan aplicaciones y actualizaciones. Esta función utiliza una memoria caché distribuida de manera automática, lo que significa que las descargas pueden obtenerse de servidores

tradicionales y de fuentes alternativas, evitando así la saturación de los servidores principales y reduciendo la carga de la red.

Windows 10 configuración de optimización de distribución para Intune - Microsoft Intune | Microsoft Learn

Servicio de transferencia inteligente en segundo plano (BITS) y BranchCache en los equipos

Durante los horarios que se hayan establecido, se puede emplear el servicio de BITS en un dispositivo con Windows para reducir el consumo de ancho de banda de la red. Se puede también ajustar la configuración de la política para BITS en la sección de Ancho de banda de red dentro de la política del agente de Intune.

Los clientes de Intune pueden utilizar BranchCache para reducir el tráfico de la red de área extensa (WAN). Los sistemas operativos compatibles incluyen Windows 7, Windows 8.0, Windows 8.1 y Windows 10. Para utilizar BranchCache, los equipos clientes deben tenerlo habilitado y configurado en modo de caché distribuida.

Cuando se instala el cliente de Intune en los equipos, BranchCache y el modo de caché distribuida se activan automáticamente. Sin embargo, si una directiva de grupo ha deshabilitado BranchCache, Intune no modificará esta configuración y BranchCache permanecerá deshabilitado.

Si se decide utilizar BranchCache, es importante coordinar con otros administradores de la organización para gestionar las políticas de grupo y las políticas de firewall de Intune. Se debe evitar la implementación de políticas que desactiven las excepciones de BranchCache o del firewall.

2.1.3 USO DE MÁQUINAS VIRTUALES WINDOWS 10

Intune admite el uso de máquinas virtuales que ejecuten Windows 10 Enterprise.

A continuación, se muestran las limitaciones y/o configuraciones para este tipo de máquinas.

2.1.3.1 INSCRIPCIÓN

Limitaciones a la hora de inscribir un dispositivo:

- No es aconsejable administrar máquinas virtuales de Host de sesión a petición con Intune, se debe inscribir cada máquina virtual creada.
- La implementación automática por Windows Autopilot no se admite porque requiere un módulo de plataforma segura (TPM) físico.
- Las máquinas virtuales a las que solo se pueden acceder a ellas a través de RDP, no admiten la inscripción de experiencia rápida (OOBE). Por lo tanto, no admiten:
    - Windows Autopilot.
    - Página de estado de Inscripción.

2.1.3.2 CONFIGURACIÓN

Al ser máquinas virtuales que no tienen un módulo de plataforma segura (TPM) físico, Intune no admite las siguientes configuraciones:

- Configuración de BitLocker.
- Configuración de la interfaz de configuración de firmware del dispositivo (BIOS).

Intune detecta automáticamente las máquinas virtuales y las notifica como "Máquina virtual" en el apartado **Dispositivos** > **Todos los dispositivos** > elegir un dispositivo > **Información general** > **Modelo**.

2.1.4 USO DE WINDOWS VIRTUAL DESKTOP CON MICROSOFT INTUNE

Azure Virtual Desktop es un servicio que ofrece virtualización de escritorio y aplicaciones. Esto posibilita que los usuarios finales se conecten de manera segura a un escritorio completo desde cualquier dispositivo. Mediante Intune, es posible proteger y administrar las máquinas de Azure Virtual Desktop a gran escala, aplicando políticas y distribuyendo aplicaciones una vez que han sido inscritas.

2.1.4.1 PRERREQUISITOS

En la actualidad, Microsoft Intune es compatible con las máquinas virtuales de Azure Virtual Desktop que cumplen con los siguientes requisitos:

- Ejecuten Windows 10 Enterprise, versión 1809 o posterior.
- Microsoft Entra joined y enroladas habilitando Inscribir la máquina virtual con Intune en el portal de Azure.
- Sean establecidas como escritorios remotos personales en Azure.
- Microsoft Entra hybrid joined y estén inscritas en Intune mediante uno de los siguientes métodos:
    - Configuración de una directiva de grupo en Active Directory para inscribir automáticamente dispositivos con el estado Microsoft Entra hybrid joined.
    - Configuración de Co-management con Configuration Manager.
    - Uso de auto-inscripción a través de Microsoft Entra joined.
- En el mismo inquilino que Intune.

Microsoft Intune trata las máquinas virtuales personales de Azure Virtual Desktop como escritorios físicos de Windows 10 Enterprise, lo que permite aprovechar algunas de las configuraciones existentes y aplicar políticas de cumplimiento y acceso condicional para asegurar las máquinas virtuales.

2.1.4.2 LIMITACIONES

Existen algunas limitaciones cuando gestionamos escritorios remotos con Windows 10 Enterprise.

En temas de configuración los siguientes perfiles no son compatibles:

- Wi-Fi.
- Unión a dominio.

En cuanto a las acciones remotas dirigidas por Intune a máquinas de Azure Virtual Desktop, no están soportadas las siguientes:

- Autopilot Reset
- Rotación de clave de BitLocker
- Comienzo de cero
- Bloqueo remoto
- Reestablecer contraseña
- Borrado

Cuando se eliminan máquinas virtuales de Azure, hay que tener en cuenta que las máquinas virtuales de Azure dejan registros de dispositivos huérfanos en la consola de Intune. Estos registros son eliminados automáticamente siguiendo las reglas de limpieza configuradas para el inquilino.

2.1.5 CONFIGURACIÓN DE PROXY/FW EN IMPLEMENTACIONES CON INTUNE

En un entorno donde se gestionan los dispositivos que se encuentren detrás de Firewalls o servidores Proxy, se debe habilitar la comunicación para Intune.

- Los puntos de conexión mencionados facilitan el acceso a los puertos detallados en las tablas que se presentan a continuación.
- Para realizar ciertas tareas, Intune necesita acceso al servidor proxy sin autenticación para **manage.microsoft.com**, ***.azureedge.net** y **graph.microsoft.com**.

Se puede modificar la configuración de los servidores proxy en cada equipo cliente o a través de directivas de grupo para cambiar la configuración de varios equipos a la vez.

2.1.5.1 SCRIPT DE POWERSHELL

Para simplificar la configuración de servicios a través de firewalls, se ha integrado el servicio de punto de conexión de Office 365. En este momento, se accede a la información del punto de conexión de Intune a través de un script de PowerShell. Hay otros servicios dependientes para Intune, que ya están cubiertos como parte del servicio de Microsoft 365 y están marcados como "obligatorios". Los servicios ya cubiertos por Microsoft 365 no se incluyen en el script para evitar la duplicación.

Con el siguiente script de PowerShell, se puede recuperar la lista de direcciones IP del servicio Intune.

```
(invoke-restmethod -Uri
("https://endpoints.office.com/endpoints/WorldWide?ServiceAreas=MEM`&`clientrequestid=" +
([GUID]::NewGuid()).Guid)) | ?{$_.ServiceArea -eq "MEM" -and $_.ips} | select -unique -
ExpandProperty ips
```

Además, este script permite obtener la lista de FQDN utilizados por Intune y los servicios dependientes. Al ejecutar el script, las direcciones URL de salida pueden diferir de las que se muestran en las tablas siguientes.

```
(invoke-restmethod -Uri
("https://endpoints.office.com/endpoints/WorldWide?ServiceAreas=MEM`&`clientrequestid=" +
([GUID]::NewGuid()).Guid)) | ?{$_.ServiceArea -eq "MEM" -and $_.urls} | select -unique -
ExpandProperty urls
```

Este script ofrece un método práctico para enumerar y revisar todos los servicios necesarios para Intune y Autopilot en un solo lugar. Además, el servicio de punto de conexión puede devolver propiedades adicionales, como la propiedad "category", que indica si el FQDN o la dirección IP deben configurarse como Permitir, Optimizar o Predeterminado.

2.1.5.2 PUNTOS DE CONEXIÓN

En la siguiente tabla se muestran los puertos y los servicios a los que el cliente Microsoft Intune necesita acceder:

Descripción	Direcciones
Intune servicio principal	
Cliente y servicio host de Intune	*.manage.microsoft.com manage.microsoft.com EnterpriseEnrollment.manage.microsoft.com 104.46.162.96/27, 13.67.13.176/28, 13.67.15.128/27, 13.69.231.128/28, 13.69.67.224/28, 13.70.78.128/28, 13.70.79.128/27, 13.71.199.64/28, 13.73.244.48/28, 13.74.111.192/27, 13.77.53.176/28, 13.86.221.176/28,13.89.174.240/28, 13.89.175.192/28, 20.189.229.0/25, 20.191.167.0/25, 20.37.153.0/24, 20.37.192.128/25, 20.38.81.0/24, 20.41.1.0/24, 20.42.1.0/24, 20.42.130.0/24, 20.42.224.128/25, 20.43.129.0/24, 20.44.19.224/27, 20.49.93.160/27, 40.119.8.128/25, 40.67.121.224/27, 40.70.151.32/28, 40.71.14.96/28, 40.74.25.0/24, 40.78.245.240/28, 40.78.247.128/27, 40.79.197.64/27, 40.79.197.96/28, 40.80.180.208/28, 40.80.180.224/27, 40.80.184.128/25, 40.82.248.224/28, 40.82.249.128/25, 52.150.137.0/25, 52.162.111.96/28, 52.168.116.128/27, 52.182.141.192/27, 52.236.189.96/27, 52.240.244.160/27, 20.204.193.12/30, 20.204.193.10/31, 20.192.174.216/29, 20.192.159.40/29
Optimización de entrega de MDM	*.do.dsp.mp.microsoft.com *.dl.delivery.mp.microsoft.com *.emdl.ws.microsoft.com kv801.prod.do.dsp.mp.microsoft.com geo.prod.do.dsp.mp.microsoft.com emdl.ws.microsoft.com 2.dl.delivery.mp.microsoft.com bg.v4.emdl.ws.microsoft.com

MEM: PS y Win32Apps	swda01-mscdn.azureedge.net swda02-mscdn.azureedge.net swdb01-mscdn.azureedge.net swdb02-mscdn.azureedge.net swdc01-mscdn.azureedge.net swdc02-mscdn.azureedge.net swdd01-mscdn.azureedge.net swdd02-mscdn.azureedge.net swdin01-mscdn.azureedge.net swdin02-mscdn.azureedge.net
Outlook.com de consumidor y OneDrive	account.live.com login.live.com
Dependencias de Autopilot	
Autopilot: Windows Update	*.download.windowsupdate.com *.windowsupdate.com *.dl.delivery.mp.microsoft.com *.prod.do.dsp.mp.microsoft.com emdl.ws.microsoft.com *.delivery.mp.microsoft.com *.update.microsoft.com tsfe.trafficshaping.dsp.mp.microsoft.com au.download.windowsupdate.com 2.dl.delivery.mp.microsoft.com download.windowsupdate.com dl.delivery.mp.microsoft.com geo.prod.do.dsp.mp.microsoft.com catalog.update.microsoft.com
Autopilot: sincronización NTP	time.windows.com www.msftncsi.com www.msftconnecttest.com
Autopilot: dependencias de WNS	clientconfig.passport.net windowsphone.com *.s-microsoft.com www.msftncsi.com c.s-microsoft.com
Autopilot: dependencias de implementación de terceros	ekop.intel.com ekcert.spserv.microsoft.com ftpm.amd.com
Autopilot: carga de diagnóstico	lgmsapeweu.blob.core.windows.net
Ayuda remota	
MEM: característica de Ayuda remota	*.support.services.microsoft.com remoteassistance.support.services.microsoft.com rdprelayv3eastusprod- 0.support.services.microsoft.com *.trouter.skype.com remoteassistanceprodacs.communication.azure.com edge.skype.com aadcdn.msftauth.net aadcdn.msauth.net alcdn.msauth.net wcpstatic.microsoft.com *.aria.microsoft.com browser.pipe.aria.microsoft.com *.events.data.microsoft.com v10.events.data.microsoft.com *.monitor.azure.com js.monitor.azure.com edge.microsoft.com

	*.trouter.communication.microsoft.com go.trouter.communication.microsoft.com *.trouter.teams.microsoft.com trouter2-usce-1-a.trouter.teams.microsoft.com api.flightproxy.skype.com ecs.communication.microsoft.com remotehelp.microsoft.com trouter-azsc-usea-0-a.trouter.skype.com
Dependencia: Ayuda remota web pubsub	*.webpubsub.azure.com AMSUA0101-RemoteAssistService-pubsub.webpubsub.azure.com
Dependencia de Ayuda remota para clientes GCC	remoteassistanceweb-gcc.usgov.communication.azure.us gcc.remotehelp.microsoft.com gcc.relay.remotehelp.microsoft.com *.gov.teams.microsoft.us

Existe también un requerimiento si en el despliegue de Microsoft Intune se implementan en los dispositivos Scripts de Powershell o aplicaciones Win32, se debe conceder acceso a los puntos de conexión donde reside actualmente el inquilino.

Se puede ver donde reside el inquilino en **Administración de inquilinos > Detalles del inquilino**:

Como se ve en la imagen, la ubicación aparece en **Ubicación de inquilino**, algo como Europa 0502.

En la siguiente tabla, se puede buscar el número de inquilino, en esa fila se indicará a que nombre de almacenamiento y puntos de conexión de CDN se debe conceder acceso.

Unidad de escalado de Azure (ASU)	Nombre de almacenamiento	CDN
AMSUA0601 **AMSUA0602** **AMSUA0101** **AMSUA0102** **AMSUA0201**	naprodimedatapri naprodimedatasec naprodimedatahotfix	naprodimedatapri.azureedge.net naprodimedatasec.azureedge.net naprodimedatahotfix.azureedge.net

AMSUA0202 **AMSUA0401** **AMSUA0402** **AMSUA0501** **AMSUA0502** **AMSUA0601** **AMSUA0701** **AMSUA0702** **AMSUA0801** **AMSUA0901**		
AMSUB0101 **AMSUB0102** **AMSUB0201** **AMSUB0202** **AMSUB0301** **AMSUB0302** **AMSUB0501** **AMSUB0502** **AMSUB0601** **AMSUB0701** **AMB0601**	euprodimedatapri euprodimedatasec euprodimedatahotfix	euprodimedatapri.azureedge.net euprodimedatasec.azureedge.net euprodimedatahotfix.azureedge.net
AMSUC0101 **AMSUC0201** **AMSUC0301** **AMSUC0501** **AMSUC0601** **AMSUD0101**	approdimedatapri approdimedatasec approdimedatahotifx	approdimedatapri.azureedge.net approdimedatasec.azureedge.net approdimedatahotfix.azureedge.net

2.1.6 REGISTRO E INICIO DE SESIÓN EN MICROSOFT INTUNE

Antes de iniciar sesión en Microsoft Intune se debe determinar si ya se tiene una cuenta de Microsoft de servicios Online, de contrato Enterprise o de contrato de licencias por volumen.

Se puede registrar en Microsoft Intune a través del enlace Microsoft - Sign up.

En esta página, se puede iniciar sesión o registrarse para administrar una nueva suscripción de Microsoft Intune. Y, una vez exista una cuenta se puede iniciar sesión a través de este enlace:

https://intune.microsoft.com

De manera predeterminada, la cuenta debe tener uno de los siguientes permisos en Entra ID:

- Administrador Global.
- Administrador de Microsoft Intune.

2.1.7 CONFIGURAR NOMBRE DE DOMINIO

Cuando se registra un servicio en la nube como Microsoft Intune, se asigna un nombre de dominio inicial en Entra ID tal como "**XXX.onmicrosoft.com". "XXX"** es el nombre de dominio que se eligió al suscribirse y ".**onmicrosoft.com"** es el fijo asignado a las cuentas que se agreguen a la suscripción.

Como recomendación, antes de crear nuevas cuentas de usuario o sincronizar con Active Directory, se debe decidir si se van a utilizar nombres de dominio personalizados o va a utilizar el nombre dominio "**.onmicrosoft.com"**. Se utilizan nombres de dominio personalizados para simplificar a los usuarios finales el inicio de sesión con las credenciales que usan para obtener acceso a los recursos del dominio.

El nombre de dominio inicial "**XXX.onmicrosoft.com"** no se puede cambiar, ni eliminar.

2.1.7.1 CREACIÓN Y COMPROBACIÓN DE UN DOMINIO PERSONALIZADO

Para agregar y comprobar un dominio personalizado se puede hacer de dos formas diferentes, a través del Centro de administración de Microsoft 365 o desde el portal de Entra. A continuación, se expone como se configuraría desde el portal de administración de Entra.

Como se ha comentado previamente, cada inquilino de Entra ID nuevo incluye un nombre dominio inicial "**nombrededominio.onmicrosoft.com".** Este nombre de dominio no se puede cambiar ni eliminar, pero se pueden agregar nombres de dominio personalizados que nos ayudan a crear nombres de usuario que facilitan el uso a los usuarios finales.

Para empezar el proceso es necesario tener el nombre de dominio que queremos utilizar registrado en un registrador de dominios, para más información sobre registradores de dominio acreditados: List of Accredited Registrars (icann.org)

2.1.7.2 CREACIÓN DEL DIRECTORIO EN ENTRA ID

Si aún no se dispone de un inquilino en Entra ID se debe crear uno para poder crear dominios personalizados. Si ya se dispone de un inquilino en Entra ID se puede saltar este paso.

Iniciar sesión en el portal de Azure con una cuenta que tenga el rol de propietario de la suscripción.

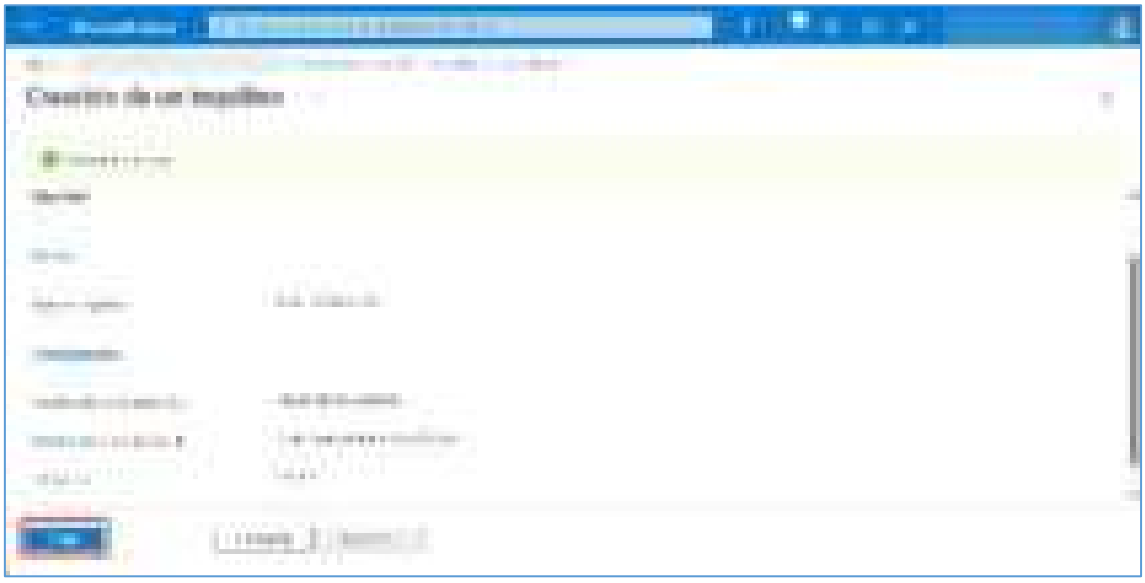
Para crear un inquilino de Entra ID:

1. Iniciar sesión en el portal de Azure.
2. En el menú principal del portal de Azure, seleccionar **Microsoft Entra ID**.
3. En el menú de **Microsoft Entra ID**, seleccionar "**Administrar inquilinos**".

4. Seleccionar Crear.

5. En la pestaña principal, seleccionar el tipo de inquilino que se desee crear, **Microsoft Entra ID** o **Azure Active Directory (B2C)**.
6. Seleccionar **siguiente** para pasar a la pestaña de configuración.
7. En esta pestaña se configurará el nombre de la organización si se desea, el nombre de dominio inicial y el País o región donde se desea crear el inquilino.

8. Seleccionar **siguiente**, se deberá revisar la información y si es correcta, seleccionar **Crear.**

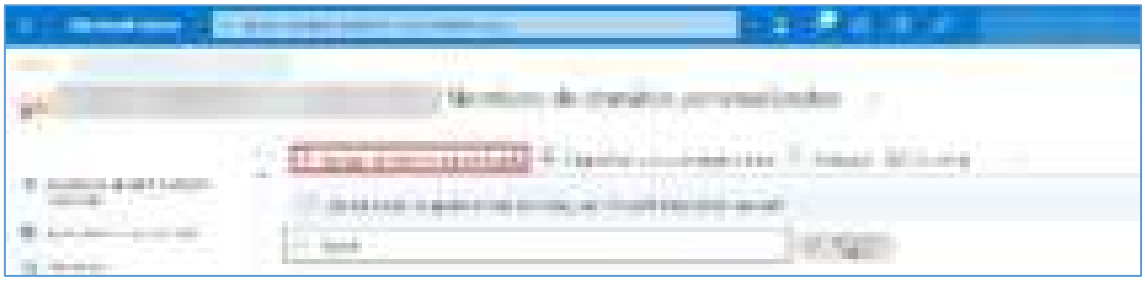


2.1.7.3 CREACIÓN DEL NOMBRE PERSONALIZADO EN ENTRA ID

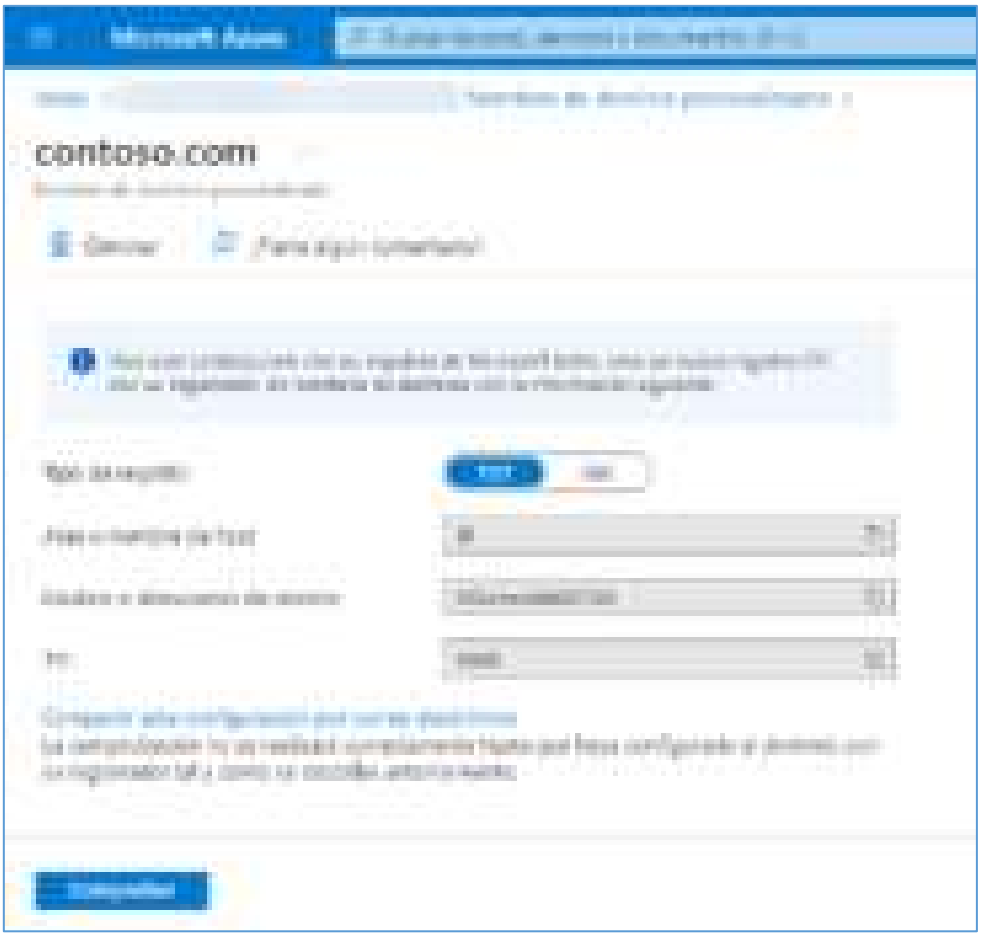
Una vez creado el directorio, se pueden agregar nombres de dominio personalizados.

1. Iniciar sesión en el portal de Entra ID con una cuenta de Administrador de nombres de dominio.
2. Seleccionar **Identidad** > **Configuración** > **Nombres de dominio** > **Agregar dominio personalizado.**

3. En **Nombre de dominio personalizado**, introducir el dominio de la organización y seleccionar **Agregar dominio**.



4. El dominio personalizado se agrega sin comprobar, aparece una pantalla con la información del dominio personalizado la cual contiene la información que necesitará más adelante para configurar registros TXT y configurar el DNS.



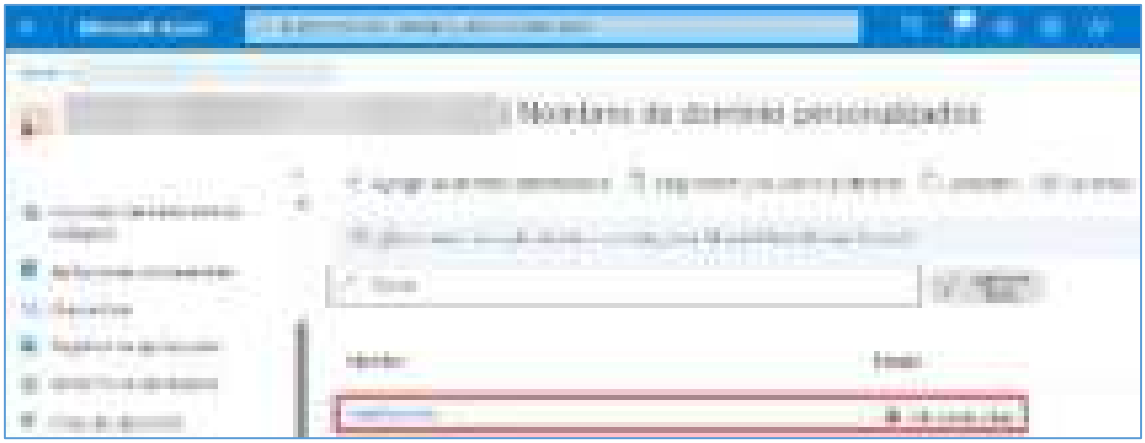
Una vez se ha creado el nombre de dominio personalizado, se debe agregar la información de DNS de Entra ID al registrador de dominios. En el registrador de dominios, crear un nuevo registro TXT para el dominio y copiar la información del nombre de dominio personalizado creado en Entra ID.

Se pueden registrar los nombres personalizados de dominio que se desee, cada uno de ellos tendrá su propio registro TXT de Entra ID. Hay que tener en cuenta que si escribe mal algún registro debe esperar a que expire el TTL antes de volver a intentarlo.

Una vez creado y añadido el nombre de dominio personalizado en el registrador de dominios, se puede comprobar si es válido en Entra ID, hay que tener en cuenta que la propagación desde los registradores de dominios puede ser inmediata o puede tardar unos días.

Se deben seguir estos pasos para la comprobación del nombre de dominio personalizado.

1. Iniciar sesión en el Centro de administración de Entra como Administrador de nombres de dominio.
2. Seleccionar **Identidad** > **Configuración** > **Nombres de dominio.**
3. En **Nombres de dominio personalizado**, seleccionar el nombre de dominio personalizado.



4. Dentro de la página del nombre personalizado de dominio, seleccionar **Comprobar**.

2.1.8 USUARIOS Y GRUPOS

La administración de usuarios y grupos se describe en la sección [3.1.1.1 Identificación].

DEFINICIÓN DE LA SOLUCIÓN

2.1.9 CONCESIÓN DE PERMISOS ADMINISTRATIVOS A LOS USUARIOS

La concesión de permisos administrativos a usuarios o grupos de Microsoft Intune se describe en la sección [3.1.1.3 Segregación de funciones y tareas].

2.1.10 ASIGNACIÓN DE LICENCIA DE MICROSOFT INTUNE A USUARIOS

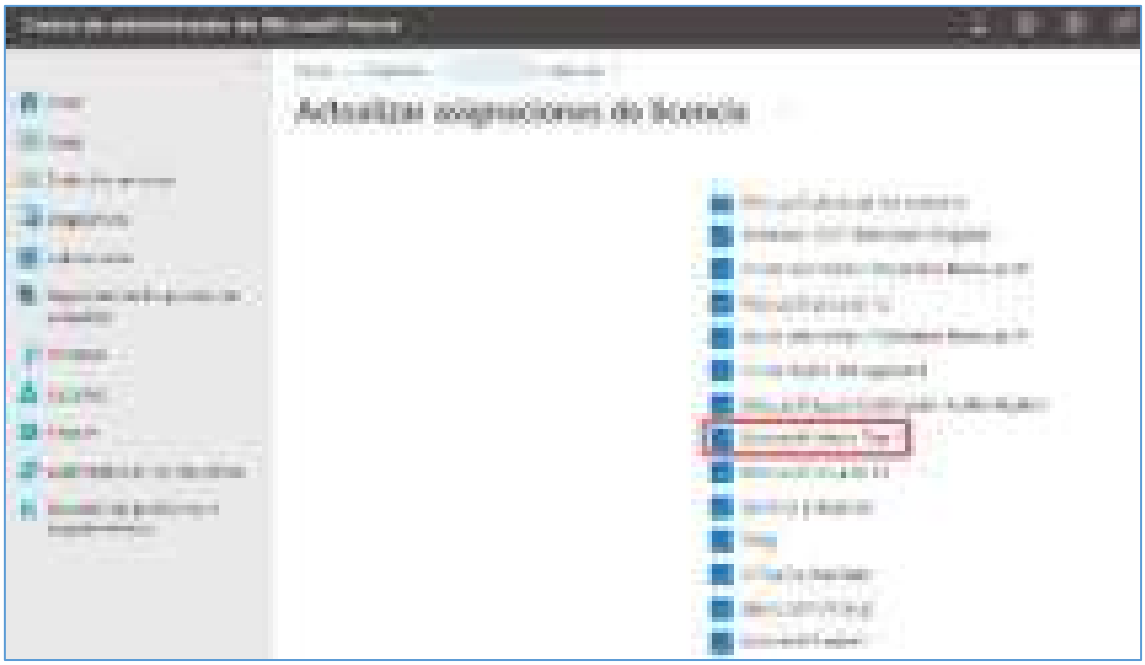
Para que los usuarios puedan recibir directivas de Microsoft Intune o puedan inscribir dispositivos, necesitan tener una licencia de Microsoft Intune asignada.

Para comprobar las licencias que incluyen Microsoft Intune, consultar la sección [1.3 Prerrequisitos Microsoft Intune].

Para asignar una licencia de Microsoft Intune desde el propio portal:

1. En la consola de Intune, seleccionar **Usuarios > Todos los usuarios > Seleccionar un usuario > Licencias > Tareas**

2. En la siguiente pantalla se podrá asignar una licencia de las que ya posea a un usuario.



3. Una vez el usuario tenga asignada la licencia de Microsoft Intune, tendrá los permisos para usar el servicio de Microsoft Intune e inscribir dispositivos.

   Se pueden comprar licencias para dispositivos por separado, cada dispositivo que acceda y utilice los servicios y el software relacionado con Microsoft Intune debe tener una licencia de dispositivo.

2.1.11 AUTORIDAD MDM

La configuración de la entidad de administración de dispositivos móviles (MDM) define las reglas de gestión de dispositivos. Como administrador de TI, es necesario establecer una entidad MDM antes de permitir que los usuarios inscriban dispositivos para su gestión. Además, se requiere una licencia de Intune para configurar la entidad MDM.

Existen varias configuraciones posibles, a continuación, se exponen las siguientes:

- **Intune independiente**: esta configuración es puramente en nube, con lo que se administra a través de Azure. Incluye todas las configuraciones que ofrece Microsoft Intune.
- **Administración conjunta de Intune**: integración de Microsoft Intune con Configuration Manager para dispositivos Windows. Intune pasaría a configurarse a través de la consola de Configuration Manager.
- **Movilidad y seguridad básicas para Microsoft 365**: si se tiene esta configuración activada, la entidad de MDM se establecer como “Office 365”.
- **Movilidad y seguridad básicas para Microsoft 365 con Microsoft Intune**: pueden coexistir ambas configuraciones si en la asignación de licencias a usuarios, unos tienen licencia de Microsoft Intune y otros licencia básica o estándar de Office 365. Dependiendo de la licencia que se tenga se administrará

con una configuración u otra, sabiendo que, si a un usuario que administre su dispositivo a través de office 365 se le asigna una licencia de Microsoft Intune, automáticamente se administrará su dispositivo con Intune.

2.1.12 CONFIGURACIÓN DE MDM EN INTUNE

Si el inquilino de Azure usa la versión 1911 o posterior, la entidad MDM se establece automáticamente en Microsoft Intune. En cambio, si el inquilino de Azure usa una versión más antigua, se debe establecer manualmente la entidad MDM.

Para hacerlo manualmente:

1. En el portal de Intune, seleccionar el banner naranja para abrir la configuración **Entidad de administración de dispositivos móviles.** Este banner solo aparece si no se ha establecido la entidad MDM.
2. Como entidad MDM se puede elegir entre las siguientes opciones:
    - Autoridad MDM de Microsoft Intune.
    - Autoridad MDM Configuration Manager.
    - Ninguno.

Una vez que la entidad MDM es cambiada, puede haber un tiempo de hasta 8 horas antes de que el dispositivo se compruebe y se sincronice con el servicio. Por lo tanto, los dispositivos deben conectarse al servicio después del cambio para que puedan actualizarse al nuevo MDM y recibir las nuevas configuraciones.

Si previamente existen perfiles del anterior MDM en un dispositivo, permanecerán en el durante 7 días o hasta que el dispositivo se conecte al servicio por primera vez.

Para escenarios como la inscripción masiva o el programa de inscripción de iOS/iPad, no se migra el MDM automáticamente, esta acción debe realizarla el soporte técnico de Microsoft.

2.1.13 COEXISTENCIA ENTRE MOVILIDAD BÁSICA O365 Y MICROSOFT INTUNE

Con este método se puede usar Microsoft Intune en nuevos usuarios y a la vez, seguir usando la movilidad básica de Office 365 en los usuarios que ya existían.

Para habilitar esta coexistencia es recomendable seguir una serie de pasos:

1. Preparación del entorno:
    - Se debe asegurar que los usuarios dispongan de suficientes licencias de Microsoft Intune. Es recomendable no asignar ninguna licencia de Intune hasta que esté habilitada la coexistencia.
    - Si previamente existen directivas configuradas en movilidad y seguridad básicas, es necesario crear e implementar directivas nuevas en Microsoft Intune para reemplazar las directivas de seguridad de dispositivos que se implementaron originalmente mediante el portal de seguridad y

cumplimiento de Office 365. Si los usuarios no tienen ninguna directiva de Intune asignada, habilitar la coexistencia podría resultar en la pérdida de configuraciones básicas de movilidad y seguridad. Incluso al reemplazar las directivas de seguridad de dispositivos con las directivas de Intune, es posible que se les solicite a los usuarios que vuelvan a autenticar sus perfiles de correo electrónico una vez que el dispositivo se traslade a la gestión de Intune.

- Después de configurarlas, no es posible desaprovisionar la movilidad y seguridad básicas. No obstante, existen pasos que se pueden seguir para desactivar las directivas.

2. Adición de la entidad de MDM de Intune:

   Para agregar Intune como entidad MDM:

   1. Iniciar sesión en el portal de Intune con un usuario con permisos de administrador global o administrador de Microsoft Intune.
   2. Ir a **Dispositivos.**
   3. En esta pestaña, si no se tiene Intune como MDM activado, se mostrará un banner para cambiar la entidad de MDM de Office 365 a Intune. Aquí se marcará la Entidad de Intune MDM y se dará al botón **Añadir.**

Una vez que la autoridad de MDM de Intune está configurada, se puede empezar a administrar usuarios y dispositivos a través de Microsoft Intune. Si los usuarios o dispositivos existentes poseen una licencia de Microsoft Intune, en la siguiente sincronización de MDM cambiarán a Microsoft Intune y si se aplicaba alguna configuración de movilidad y seguridad básica dejará de hacerlo.

2.1.14 CONFIGURACIÓN DE RESTRICCIONES DE INSCRIPCIÓN DE DISPOSITIVOS

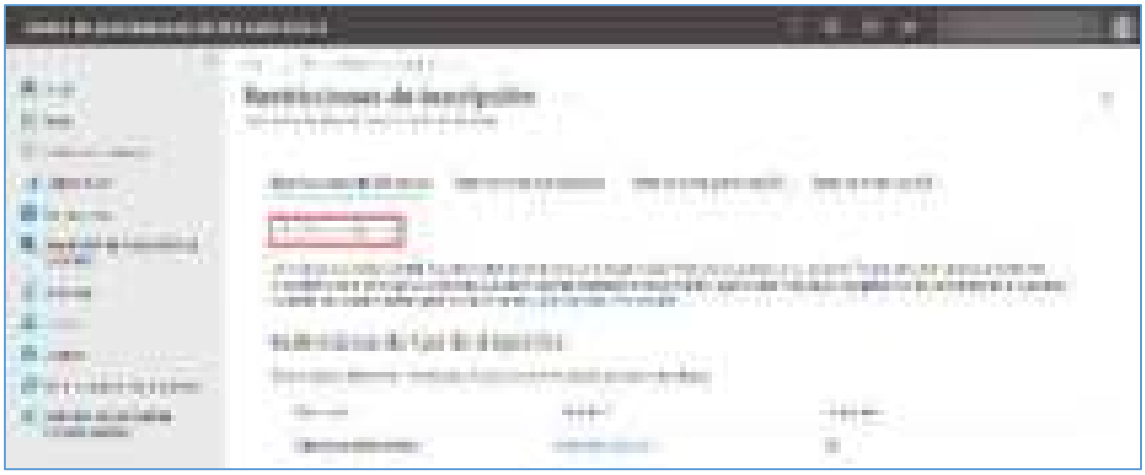
Restricciones de plataforma de dispositivos

En Intune se pueden crear y gestionar restricciones de inscripción que definen el número y tipos de dispositivos que se pueden inscribir con Microsoft Intune. Se pueden crear múltiples restricciones y aplicarlas luego a diferentes grupos de usuarios.

Para crear una restricción de inscripción seguir los siguientes pasos:

1. Iniciar sesión en el portal de Microsoft Intune y seleccionar **Dispositivos > Inscripción > Windows/Apple/Android > Restricción de plataforma de dispositivos > Crear restricción**. Si no se crease una nueva restricción y se modifica la de por defecto, se aplicará a todos los usuarios. Se podrá crear la restricción por tipo de dispositivo o por limite o dispositivo.

   Se pueden tener hasta 25 directivas de restricción de plataforma de dispositivos.



2. En la siguiente pantalla, se debe poner Nombre a la restricción y una descripción opcional.
3. A continuación, se puede configurar restricciones para cualquier tipo de dispositivos, permitiendo o no también una versión mínima o máxima.

4. Por último, se pueden añadir etiquetas de ámbito que son opcionales, y para que aplique la restricción se debe asignar a grupos.

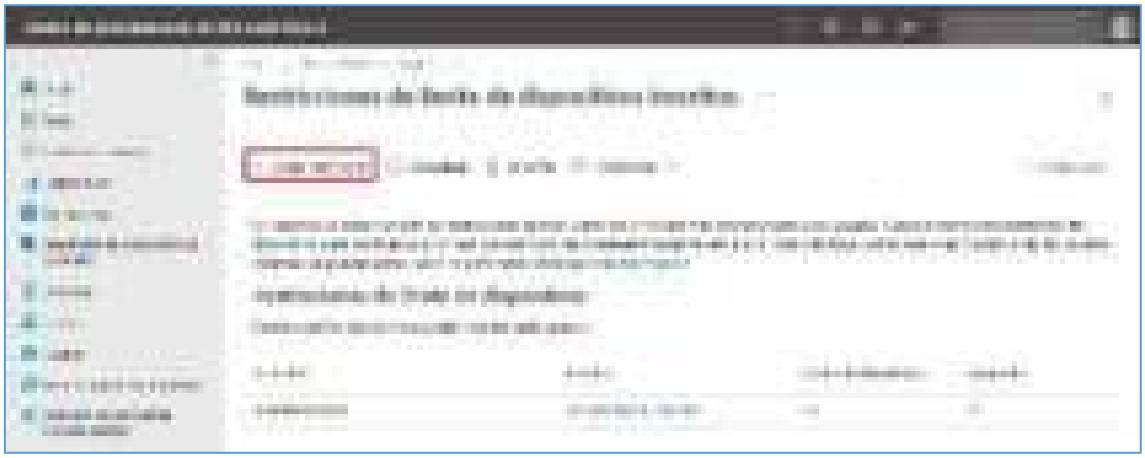
Restricciones de límite de dispositivos

La directiva de restricción de inscripción de límite de dispositivos limita el número de dispositivos que un usuario puede inscribir. Esta directiva se aplica a dispositivos que cumplen con los siguientes criterios:

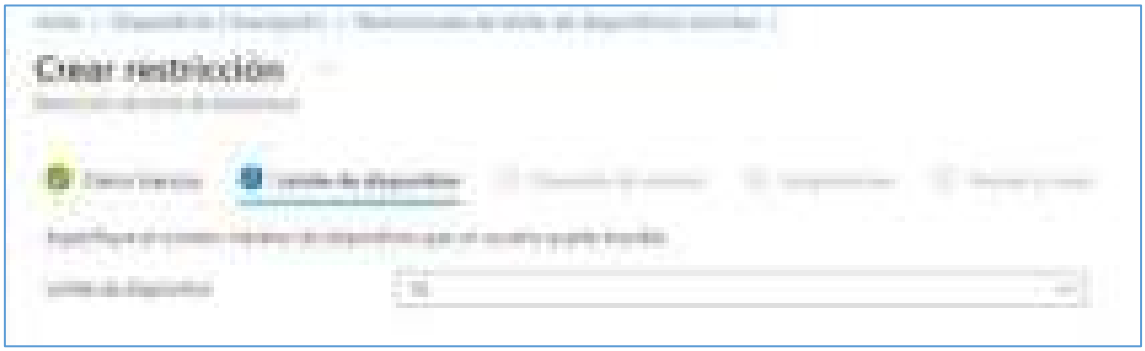
- Administrados por Microsoft Intune.
- Han tenido contacto con Intune en los últimos 90 días.
- No están en un estado pendiente de registro durante más de 24 horas.
- No han experimentado errores durante la inscripción de Apple.
- No han sido eliminados de Microsoft Intune.
- El tipo de inscripción no está en modo compartido.

Para crear una restricción de inscripción seguir los siguientes pasos:

1. Iniciar sesión en el portal de Microsoft Intune y seleccionar **Dispositivos > Inscripción > Windows/Apple/Android > Restricción de límite de dispositivos > Crear restricción**. Si no se crease una nueva restricción y se modifica la de por defecto, se aplicará a todos los usuarios y dispositivos.



2. En **Límite de dispositivo**, seleccione el número máximo de dispositivos que un usuario puede inscribir.



3. Por último, se pueden añadir etiquetas de ámbito que son opcionales, y para que aplique la restricción se debe asignar a grupos.

2.1.15 IDENTIFICAR DISPOSITIVOS COMO TOTALMENTE CORPORATIVOS

En Microsoft Intune se pueden identificar dispositivos como totalmente corporativos para definir la gestión y administración. Puede realizar tareas de gestión adicionales y recoger información, como el número de teléfono o un inventario de aplicaciones desde dispositivos totalmente corporativos.

También se pueden crear restricciones para bloquear los dispositivos que no sean totalmente corporativos.

A la hora de inscribir un dispositivo, Intune automáticamente asigna el estado de totalmente corporativo a los dispositivos que son:

1. Inscritos por un administrador de inscripción de dispositivos (todas las plataformas).
2. Inscritos con el programa de inscripción de dispositivos de Apple, Apple School Manager o Apple Configurator (solo iOS/iPadOS).
3. Identificados como totalmente corporativos antes de su inscripción con la existencia de número de serie o IMEI.
4. Dispositivos unidos a Microsoft Entra con credenciales profesionales o educativas.
5. Configurados como corporativos en las propiedades del dispositivo una vez unido ya a Intune. Después de la inscripción, esta opción se puede cambiar de Personal a Corporativo.
6. Inscritos mediante Google Zero Touch.
7. Inscritos con Knox Mobile Enrollment.
8. Inscritos como dispositivos Android Enterprise de propiedad corporativa con perfil de trabajo.
9. Inscritos como dispositivos Android Enterprise totalmente administrados.
10. Inscritos como dispositivos dedicados de Android Enterprise.
11. Dispositivos asociados a usuarios de propiedad corporativa de Android Open Source Project (AOSP).
12. Dispositivos corporativos sin usuario inscritos como proyectos de código abierto de Android (AOSP).

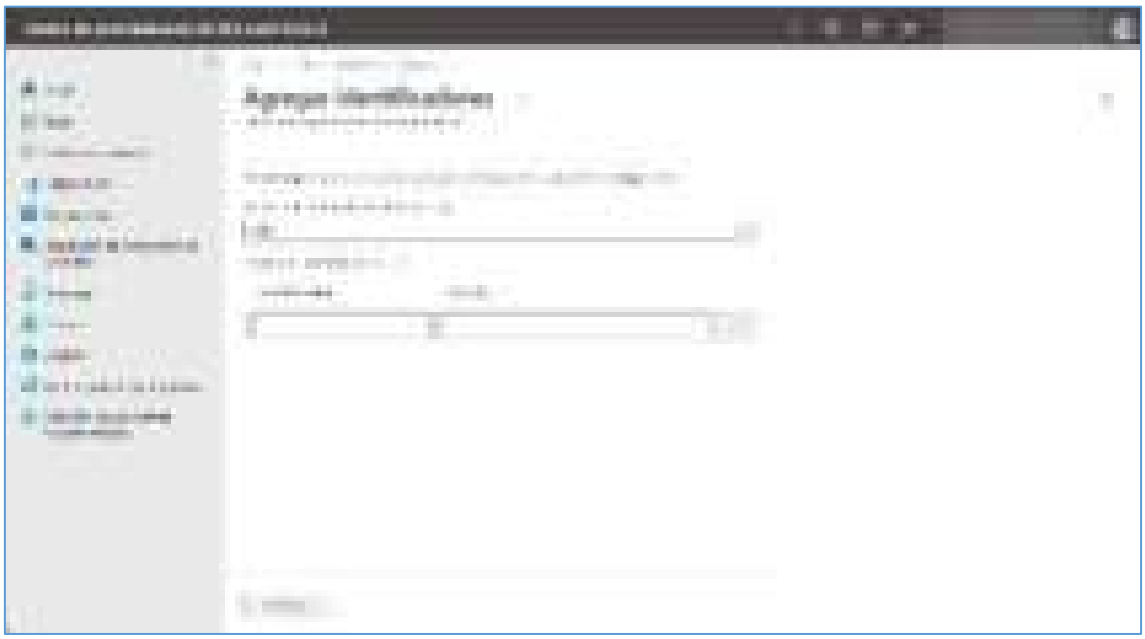
Identificar dispositivos como corporativos como IMEI o número de serie

Como administrador de Intune, se pueden crear e importar ficheros de valores separados por comas (.CSV) que listen números IMEI o números de serie. Intune usa estos números para identificar la propiedad de un dispositivo en específico como corporativo. Para cargar un IMEI o número de serie, o un archivo .CSV con varios IMEI o números de serie seguir los siguientes pasos:

1. Iniciar sesión en el portal de Microsoft Intune seleccionar **Dispositivos > Inscripción > Identificadores de dispositivo corporativos > Agregar**.

2. Se pueden añadir IMEI o números de serie manualmente uno a uno, o subir un archivo .CSV con varios IMEI o números de serie.

   En este caso, será de manera manual. Seleccionar el tipo de identificador y escribir los datos necesarios.



De esta manera los dispositivos que tengan su número corporativo en la plataforma de Microsoft Intune se tratarán como corporativos.

Añadir identificadores corporativos usando un fichero .CSV

Para crear la lista, primero crear dos columnas separadas por comas sin un encabezado. Añadir el numero identificativo a la izquierda y la descripción a la derecha. El fichero .CSV solo puede tener un tipo de identificador, no se pueden mezclar números de serie con IMEI.

La descripción tiene un límite de 128 caracteres y es solo para uso administrativo. El límite actual son 5000 filas o 5 Mb por archivo CSV. Aquí un ejemplo de archivo CSV:

Es posible que algunos dispositivos Android tengan dos identificadores IMEI. Intune solo lee un IMEI por dispositivo inscrito, por lo tanto, se tendrán que subir los dos IMEI para que el dispositivo se trate como dispositivo corporativo.

Una vez se tenga el fichero CSV preparado, se puede subir a Intune y así meter todos los identificadores de una vez. Para ello seguir los siguientes pasos:

1. Iniciar sesión en el portal de Microsoft Intune seleccionar **Dispositivos > Inscripción > Identificadores de dispositivo corporativos > Agregar**.
2. Cargar el archivo .CSV y, si no hay ningún error en el fichero, Microsoft Intune reconocerá cuantos identificadores hay en el archivo.

2.1.16 INSCRIPCIÓN MÓVILES

2.1.16.1 PREPARACIÓN MDM PARA GESTIONAR DISPOSITIVOS ANDROID

Tal y como funciona en Apple, en Android también se necesita disponer de una cuenta de Google para gestionar los dispositivos Android y su tienda. Una vez se tenga la cuenta, hacer lo siguiente:

1. Iniciar sesión en el portal de Microsoft Intune y seleccionar **Dispositivos** > **Android** > **Inscripción de Android > Google Play Administrado.**

2. Aceptar los términos e iniciar sesión en Google para la configuración.

3. Seguir los pasos y una vez configurada, se puede ver el estado como activado.

Después de vincular la cuenta a Google Play, estas aplicaciones comunes para Android Enterprise se añaden al centro de administración:

- **Microsoft Intune**: Utilizado para configuraciones de perfil de trabajo, incluyendo propietario corporativo, dedicado y completamente administrado de Android Enterprise.
- **Microsoft Authenticator**: Ayuda en el inicio de sesión con autenticación de dos factores y también es utilizado para dispositivos dedicados de Android Enterprise que están inscritos con el Modo de dispositivo compartido de Microsoft Entra.

- **Portal de empresa de Intune**: Utilizado en escenarios de perfil de trabajo de Android Enterprise en dispositivos personales, y para aplicar políticas de protección de aplicaciones de Intune (APP).
- **Managed Home Screen**: Empleado en el modo de pantalla completa de múltiples aplicaciones en dispositivos dedicados de Android Enterprise.

2.1.16.2 PREPARACIÓN MDM PARA GESTIONAR DISPOSITIVOS iOS Y MAC

Se requiere un certificado push MDM de Apple para administrar dispositivos iOS/iPadOS y macOS en Microsoft Intune. Este permite la inscripción de dispositivos a través de la aplicación Portal de empresa de Intune, así como mediante métodos de inscripción masiva de Apple, como el Programa de inscripción de dispositivos, Apple School Manager y Apple Configurator.

Para obtener y configurar el certificado, es necesario disponer de un ID de Apple. Una vez se tenga la cuenta de Apple, hacer lo siguiente:

1. Iniciar sesión en el portal de Microsoft Intune, seleccionar **Dispositivos > iOS/iPad > Inscripción de iOS/IpadOS**.

2. Pulsar sobre **Certificado Push MDM de Apple** y seguir las instrucciones que están reflejadas en esta pantalla.

3. Una vez configurado aparecerá como activo:

Con esta configuración ya se podrá acceder a las opciones de configuración tanto de Mac como de iOS, y gestionar la tienda de Apple para las aplicaciones móviles.

2.1.16.3 INSCRIPCIÓN DE DISPOSITIVOS ANDROID

Los dispositivos personales y los que son propiedad de la organización se pueden inscribir en Intune. Una vez inscritos, reciben las directivas y los perfiles que se crean. Al inscribir dispositivos Android en Intune, se tienen las siguientes opciones:

- **Dispositivos Android Enterprise de propiedad personal con un perfil de trabajo (BYOD).** Estos dispositivos son dispositivos Android personales o BYOD (Bring

Your Own Device), lo que significa que son propiedad de los usuarios y tienen acceso al correo electrónico, aplicaciones y otros datos de la organización.

- **Dispositivos Android Enterprise dedicados de propiedad corporativa (COSU).** Anteriormente conocidos como COSU (Corporate-Owned Single-Use), estos dispositivos son propiedad de la organización y compatibles con Zero Touch de Google. Su función principal es actuar como dispositivos de pantalla completa, sin estar asociados a ningún usuario único o específico.
- **Dispositivos Android Enterprise de propiedad corporativa totalmente administrados (COBO).** Anteriormente conocidos como COBO (Corporate-Owned Business-Only), estos dispositivos son propiedad de la organización y están asignados a un usuario específico.
- **Perfil de trabajo de propiedad corporativa de Android Enterprise (COPE).** Anteriormente conocidos como COPE (Corporate-Owned, Personally Enabled), estos dispositivos son propiedad de la organización y están asignados a un usuario específico.
- **Proyecto de código abierto de Android (AOSP).** También conocidos como AOSP (Android Open Source Project), estos dispositivos son propiedad de la organización y no utilizan Google Mobile Services (GMS). Pueden ser dispositivos de estilo pantalla completa que no están asociados a un usuario único o específico, o bien pueden tener un usuario.
- **Administrador de dispositivos Android (DA).** Estos dispositivos Android pueden ser corporativos o personales/BYOD, lo que significa que pueden ser propiedad de la organización o del usuario. Tienen acceso al correo electrónico, las aplicaciones y otros datos de la organización.

Una vez configurados los dispositivos dedicados, ya se podrán inscribir. La inscripción en Intune para los dispositivos dedicados, totalmente administrados o con perfil de trabajo corporativo de Android Enterprise comienza con un restablecimiento de fábrica. Los diferentes métodos de inscripción son los siguientes:

- Código QR
- Zero-touch
- Knox Mobile Enrollment
- Transmisión de datos en proximidad (NFC)
- Token

Esta guía se centra en explicar uno de los métodos de inscripción, mediante Zero Touch. Para más información, consultar:

Inscripción de dispositivos dedicados, totalmente administrados o corporativos de perfil de trabajo de Android Enterprise en Intune - Microsoft Intune | Microsoft Learn

CREACIÓN DE UNA CONFIGURACIÓN ZERO-TOUCH

Este método emplea la inscripción sin contacto y el portal de inscripción sin contacto de Google para aprovisionar e inscribir dispositivos propiedad de la empresa. El proceso de aprovisionamiento se inicia automáticamente cuando los usuarios encienden sus dispositivos.

Antes de poder realizar la configuración para Zero Touch, es necesario habilitar el iframe de contacto cero, que brinda acceso al portal de inscripción sin contacto y a las configuraciones de Zero Touch en el centro de administración de Microsoft Intune.

Para activar el iframe, primero se debe agregar el permiso de sincronización de la aplicación de actualización y habilitar la inscripción para dispositivos corporativos totalmente administrados. Seguir los siguientes pasos para activar el iframe.

Paso 1: Agregar permiso necesario

Para agregar el permiso de *sincronización de la aplicación de actualización*, seguir estos pasos:

1. Iniciar sesión en el portal de Microsoft Intune y seleccionar **Administrador de inquilinos > Roles.**
2. Seleccionar el rol en la lista **> Propiedades > Permisos** y **Editar**.
3. Seleccionar **Android for Work**.
4. Junto a **Actualizar sincronización de aplicaciones**, seleccionar **Sí**.

5. Seleccionar **Revisar y guardar** para revisar los cambios.
6. Seleccionar **Guardar**.

Paso 2: Habilitar la inscripción para dispositivos corporativos

Verificar que la inscripción esté habilitada para dispositivos corporativos totalmente administrados. Esta verificación es crucial para garantizar que los dispositivos puedan

inscribirse correctamente y recibir las configuraciones y políticas necesarias desde Intune.

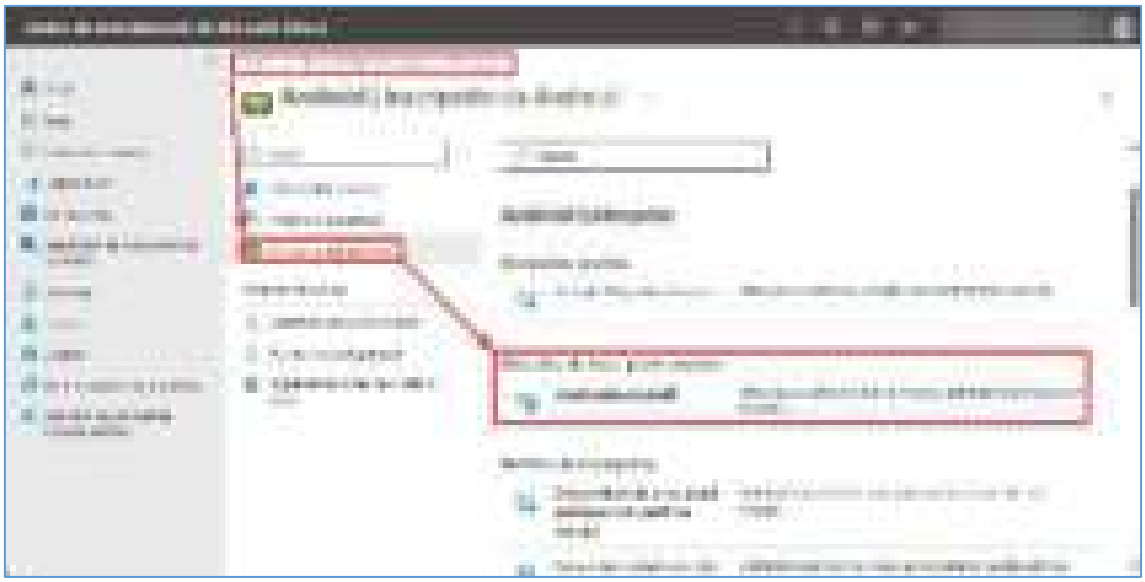
1. Iniciar sesión en el portal de Microsoft Intune y seleccionar **Dispositivos > Android > Inscripción de Android.**
2. En **Perfiles de inscripción**, elegir **Dispositivos de usuario totalmente administrados de propiedad corporativa**.

3. Y comprobar que la opción **Permitir que los usuarios inscriban dispositivos de usuario de propiedad corporativa** esté en **Sí**.

Paso 3: Vinculación de una cuenta de contacto cero a Intune

Conectar una cuenta de contacto cero con la cuenta de Microsoft Intune. Esto permitirá acceder y gestionar las configuraciones y políticas de inscripción sin contacto directamente desde Intune.

1. Iniciar sesión en el portal de Microsoft Intune y seleccionar **Dispositivos > Android > Inscripción de Android.**
2. En **Métodos de inscripción masiva**, elegir **Inscripción táctil cero.**



3. Se abre el iframe. Seleccionar Siguiente para comenzar la instalación.
4. Iniciar sesión con la cuenta de Google que se proporcionó al revendedor. Seleccionar la cuenta que se quiera vincular y seleccionar Vincular.
5. Se crea una configuración predeterminada e Intune la aplicará automáticamente a cualquier dispositivo habilitado para Zero Touch que no tenga una configuración existente. Esto garantiza que todos los dispositivos reciban una configuración básica para comenzar su aprovisionamiento sin contacto de manera efectiva.
6. Seleccionar **Siguiente** y **Guardar**.

INSCRIPCIÓN ZERO-TOUCH

1. Iniciar sesión en el portal de inscripción sin contacto con la cuenta de Google.
2. Seleccionar la opción para agregar nueva configuración y rellenar la información.
3. Seleccionar Microsoft Intune como aplicación EMM DPC.
4. Copiar el siguiente texto JSON en el campo DPC. Reemplazar **YourEnrollmentToken** el token de inscripción que se creó como parte del perfil de inscripción.

```
{

"android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME":
"com.google.android.apps.work.clouddpc/.receivers.CloudDeviceAdminReceiver",

"android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM":
"I5YvS0O5hXY46mb01BlRjq4oJJGs2kuUcHvVkAPEXlg",

"android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION":
"https://play.google.com/managed/downloadManagingApp?identifier=setup",

"android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": {

"com.google.android.apps.work.clouddpc.EXTRA_ENROLLMENT_TOKEN": "YourEnrollmentToken"

}

}
```

5. Escribir el nombre de la organización y la información de soporte, que se mostrará en pantalla mientras los usuarios configuran sus dispositivos.

2.1.16.4 INSCRIPCIÓN DE DISPOSITIVOS iOS/iPadOS CON APPLE CONFIGURATOR

Microsoft Intune permite la inscripción de dispositivos iOS/iPadOS mediante la aplicación Apple Configurator en un dispositivo Mac. La aplicación requiere que cada dispositivo que se quiera inscribir con este método esté conectado al dispositivo Mac a través de USB. Se pueden inscribir dispositivos en Intune con Apple Configurator de dos maneras:

- **Asistente de configuración:** Borra los dispositivos y los prepara para la inscripción durante el asistente.
- **Inscripción directa**: No borra el dispositivo y lo inscribe a través de la configuración de iOS. Este método solo está disponible **sin afinidad de usuario**.

Los prerrequisitos para usar Apple Configurator son los siguientes:

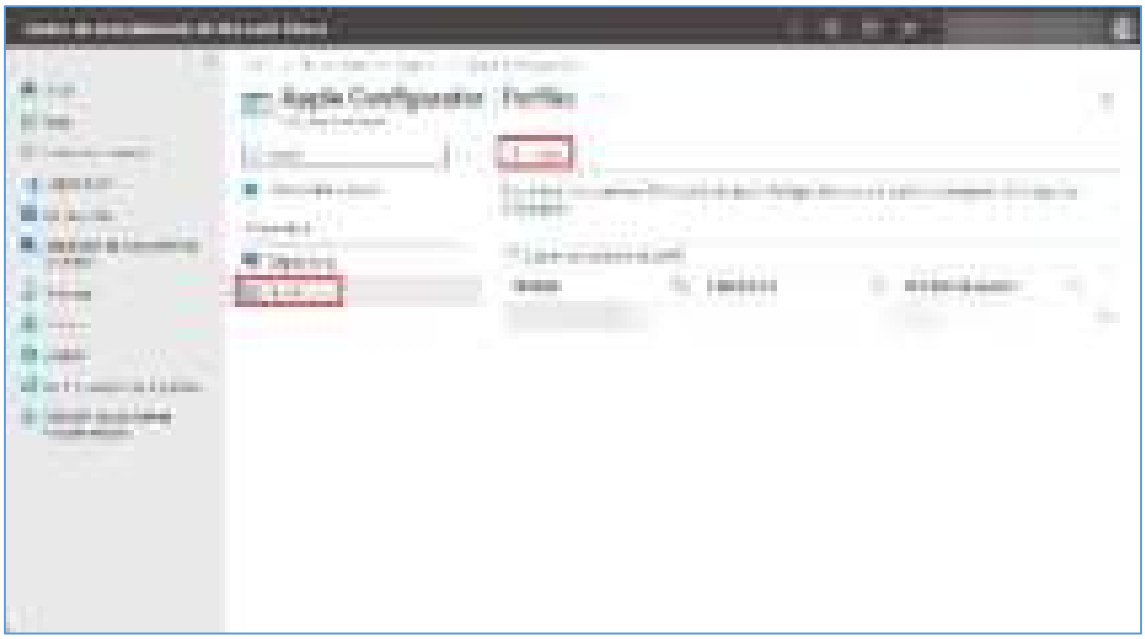
- Configurar la autoridad MDM.
- Acceso físico a los dispositivos iOS/iPadOS.
- Activado el certificado Push de Apple.
- Números de serie de los dispositivos (solo en el modo asistente).
- Cable de conexión USB.
- Equipo macOS con Apple Configurator.

CREACIÓN DE UN PERFIL APPLE CONFIGURATION PARA LOS DISPOSITIVOS

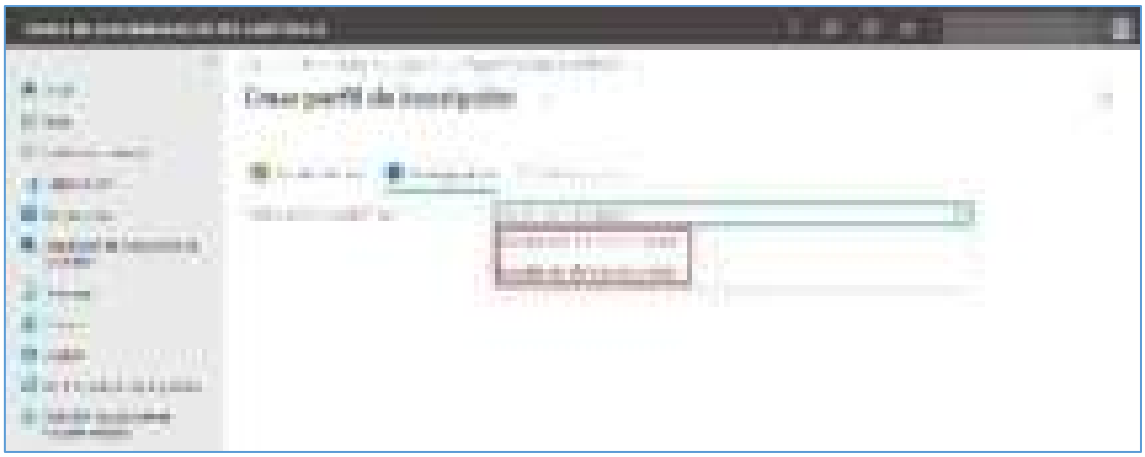
Un perfil de inscripción de dispositivos define que configuraciones se aplicarán durante la inscripción. Seguir los siguientes pasos para crear un perfil:

1. Iniciar sesión en el portal de Microsoft Intune y seleccionar **Dispositivos > Inscripción > Apple > Configurador de Apple.**

2. Una vez dentro, seleccionar **Perfiles > Crear.**



3. Configurar en los datos básicos un nombre para el perfil y pasar a la siguiente pantalla.



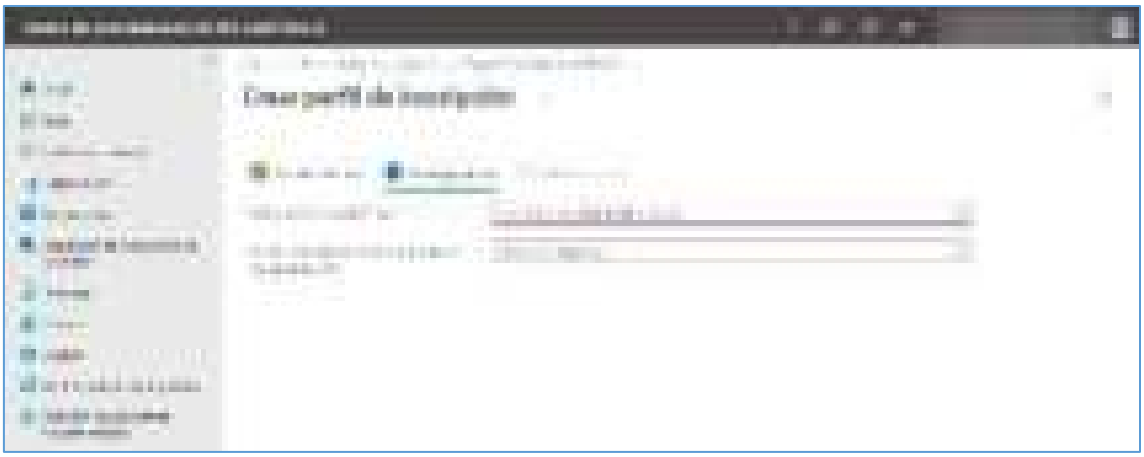
4. Como se ve en la imagen se pueden elegir dos tipos de perfiles:

   - **Inscribir con afinidad de usuario:** Elegir esta opción si los dispositivos pertenecen a los usuarios finales y ellos quieren usarlos en la compañía. El proceso implica primero afiliar el dispositivo a un usuario utilizando el Asistente de Configuración. Luego, una vez afiliado, se le otorga acceso a los datos y al correo electrónico de la empresa.

     Es importante destacar que únicamente se permite la inscripción utilizando el Asistente de Configuración.

   - **Inscribir sin afinidad de usuario**: Elegir esta opción para dispositivos que no están asociados a un solo usuario. Usar esta opción para dispositivos en los que realicen tareas sin acceso a los datos locales del usuario. Las aplicaciones que necesiten tener asociado un usuario no funcionarán, entre ellas el portal de empresa, por lo tanto, esta opción es requerida la **Inscripción directa.**

   Si se ha elegido **Con afinidad de usuario,** aparece la opción de que los usuarios puedan identificarse con el portal de empresa, en lugar de identificarse con el asistente de Apple. Las ventajas de identificarse con el portal de empresa son que se puede usar autenticación multifactor, por ejemplo.



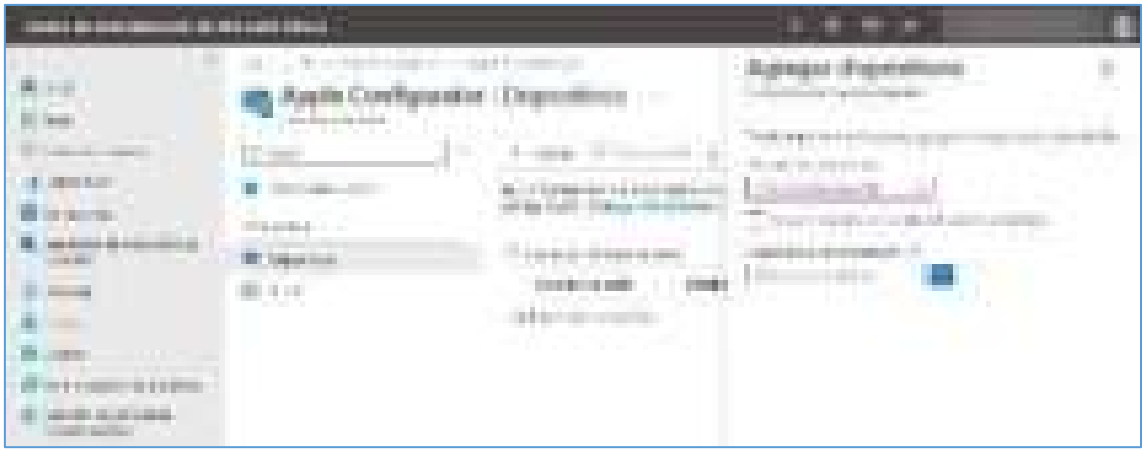
5. Seleccionar **Crear** para guardar el perfil.

INSCRIPCIÓN CON ASISTENTE DE CONFIGURACIÓN

Paso 1: Añadir números de serie a Apple Configurator

1. Crear el archivo CSV con los números de serie de los dispositivos, tal y como se hizo anteriormente.
2. Iniciar sesión en el portal de Microsoft Intune y seleccionar **Dispositivos > Inscripción > Apple > Configurador de Apple > Dispositivos.**

   Aquí se puede agregar un archivo CSV que contendrá los dispositivos a asociar al perfil creado.



Paso 2: Reasignar el perfil a los números de serie de los dispositivos

Se puede asignar un perfil de inscripción al importar los números de serie de iOS/iPadOS para la inscripción mediante Apple Configurator. Además, existe la opción de asignar perfiles desde dos ubicaciones en el portal de Azure:

- Dispositivos de Apple Configurator

  1. Iniciar sesión en el portal de Microsoft Intune y seleccionar **Dispositivos > Inscripción > Apple > Configurador de Apple > Dispositivos** y seleccionar un número de serie.

2. **Asignar perfil**, seleccionar el nuevo perfil a asignar y **Asignar**.

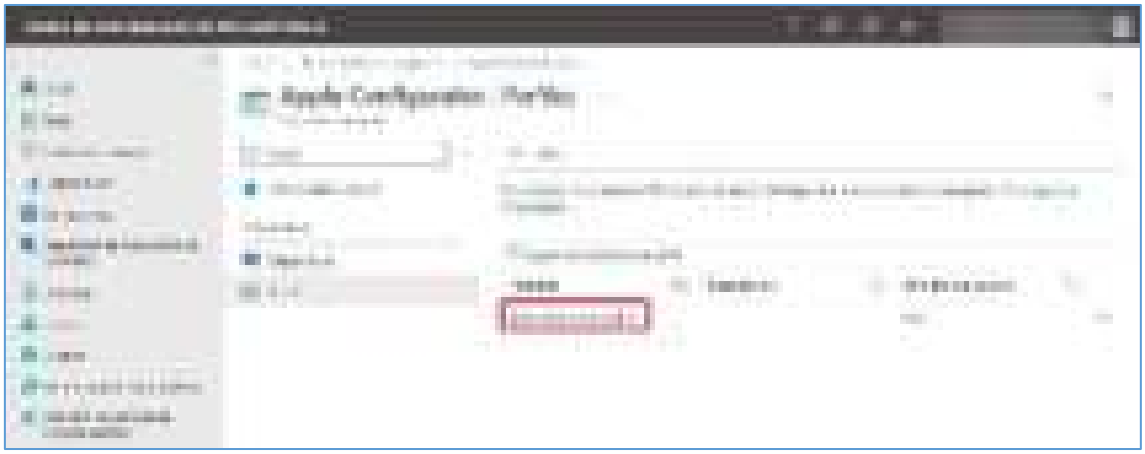
- Perfiles de AC

1. Iniciar sesión en el portal de Microsoft Intune y seleccionar **Dispositivos > Inscripción > Apple > Configurador de Apple > Perfiles** y seleccionar un perfil.
2. En el perfil, seleccionar **Dispositivos asignados** y **Asignar**.
3. Filtrar para buscar los números de serie de dispositivo que asignar al perfil, seleccionar y **Asignar**.

Paso 3: Exportar el perfil

Después de crear el perfil y asignar los números de serie, se debe exportar el perfil desde Intune como una URL. Luego se deberá importar el perfil a la aplicación Apple Configurator en un Mac para el despliegue de los dispositivos.

1. Iniciar sesión en el portal de Microsoft Intune y seleccionar **Dispositivos > Inscripción > Apple > Configurador de Apple > Perfiles** y elegir el perfil a exportar.



2. En el perfil seleccionar **Exportar perfil,** y copiar la URL.

3. Lo siguiente será importar el perfil a la aplicación Apple Configurator.

Paso 4: Inscribir dispositivos con el asistente de configuración

1. En un dispositivo Mac, abrir la aplicación Apple Configurator. En la barra de herramientas seleccionar **Apple Configurator > Preferencias**.
2. En el panel preferencias, seleccionar **Servidores** y elegir el símbolo (+) para lanzar el asistente de MDM.
3. Introducir la URL exportada de Microsoft Intune en el paso 2, elegir **siguiente**.
4. Conectar los dispositivos móviles iOS/iPadOS al ordenador MAC con un adaptador USB.
5. Seleccionar los dispositivos iOS/iPadOS que se quieran gestionar y elegir **Preparar**. En el menú **Preparar** elegir la configuración manual y seleccionar siguiente.
6. En el panel de **Servidor de MDM,** seleccionar el nombre del servidor creado y luego seleccionar **siguiente** e iniciar sesión con el Apple ID.
7. En el panel de **Dispositivos supervisados,** seleccionar el nivel de supervisión y seleccionar **siguiente**.
8. En el panel de **Crear una organización**, elegir una **Organización** o crear una nueva.
9. En el panel del **Asistente de configuración IOS,** elegir los pasos que serán mostrados al usuario en la configuración del dispositivo. También se tendrá que conectar a un perfil de red para completar ciertas configuraciones.
10. Cuando el dispositivo IOS finalice la preparación, desconectar el cable USB.

Paso 4: Distribución de dispositivos

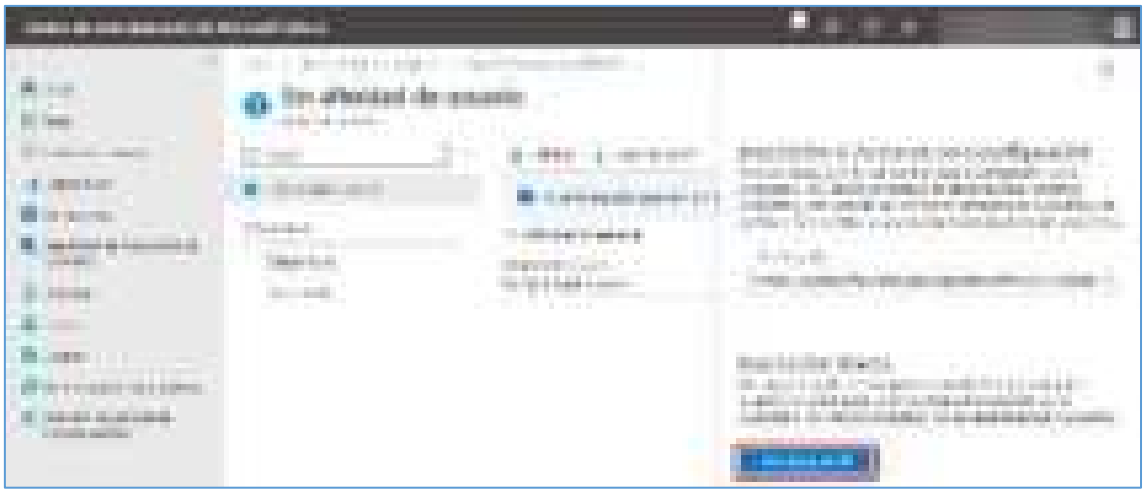
Después de los pasos anteriores, los dispositivos ya están preparados para la inscripción corporativa. Apagar los dispositivos y distribuir a los usuarios. Cuando los usuarios enciendan los dispositivos, el asistente de configuración se iniciará.

Los usuarios deben completar el asistente de configuración. Los dispositivos con **Afinidad de usuario**, y pueden instalar y ejecutar la aplicación Portal de Empresa para descargar aplicaciones y gestionar sus dispositivos.

INSCRIPCIÓN DIRECTA

Cuando se inscriben dispositivos iOS/iPadOS directamente con Apple Configurator, existe la capacidad de inscribir un dispositivo sin necesidad de adquirir su número de serie. Además, se puede asignar un nombre al dispositivo con el fin de identificarlo antes de que Intune capture su nombre durante el proceso de inscripción. Es importante tener en cuenta que no se admite el uso de la aplicación Portal de Empresa para dispositivos inscritos de esta manera. Además, este método no implica el borrado del dispositivo.

Para ello, crear un perfil sin afinidad de usuario y asociar los dispositivos que inscribir a dicho perfil. Posteriormente descargar este perfil.



Para inscribir un dispositivo directamente:

1. Abrir la aplicación Apple Configurator en un Mac, y conectar el dispositivo iOS/iPadOS que se quiera inscribir a Intune, cerrando todas las aplicaciones.
2. Seleccionar **Añadir > Perfiles.**
3. Seleccionar el perfil que se exportó desde Intune, y el siguiente paso será instalar este perfil en el dispositivo conectado.
4. Una vez instalado el perfil, el dispositivo ya estará inscrito en Intune y listo para su distribución.

2.1.17 EXPERIENCIAS DEL USUARIO FINAL

2.1.17.1 PERSONALIZACIÓN

Con la personalización de la experiencia al usuario final, se podrá configurar un entorno conocido y útil para el usuario final.

Para configurar este aspecto seguir los siguientes pasos:

1. Iniciar sesión en el portal de Microsoft Intune y seleccionar **Administración de Inquilinos > Personalización.**

2. Aquí se podrá configurar el nombre de la organización, color, logo y la información del soporte técnico de la empresa entre otras cosas.

Esta información será accesible para los usuarios en la aplicación Portal de Empresa.

2.1.17.2 CONFIGURACIÓN DE TÉRMINOS Y CONDICIONES DE LA COMPAÑÍA

Como administradores de Intune, se puede requerir a los usuarios que lean y acepten los términos y condiciones previamente configurados para usar la aplicación Portal de Empresa.

Se pueden crear varios conjuntos de términos y condiciones asignados a diferentes grupos. Para creación de los términos y condiciones:

1. Iniciar sesión en el portal de Microsoft Intune y seleccionar **Administración de inquilinos > Términos y condiciones > Crear.**

2. En los datos básicos, el nombre y la descripción son de uso interno en Microsoft Intune, mientras que el **Titulo, y las propiedades de términos y condiciones** es lo que les aparecerá a los usuarios.

3. Por último, asignar a los grupos que se desee para que se apliquen y aparezcan en los dispositivos.

2.2 PROTECCIÓN DE DISPOSITIVOS

Microsoft Intune ayuda a garantizar la seguridad y actualización de dispositivos administrados, al mismo tiempo que protege los datos de la organización contra posibles amenazas. Esto implica controlar cómo los usuarios interactúan con los datos en dispositivos tanto administrados como no administrados. Además, se asegura de bloquear el acceso a los datos desde dispositivos que puedan representar un riesgo para la seguridad.

Para garantizar la protección y cumplir con los requisitos de seguridad de la organización, se recomienda la implementación de los perfiles que se detallan a continuación.

2.2.1 DIRECTIVAS DE SEGURIDAD DE PUNTO DE CONEXIÓN

Microsoft Intune facilita la herramienta **Seguridad de los puntos de conexión** para configurar la seguridad de los dispositivos y administrar las tareas de seguridad de los dispositivos ante posibles incidentes.

Esta sección de Información general ofrece una visión rápida de las configuraciones disponibles en este apartado de Seguridad de los puntos de conexión.

En el apartado **Todos los dispositivos,** se puede ver un listado de todos los dispositivos de Microsoft Entra ID, incluidos los dispositivos administrados por **Microsoft Intune**, **Configuration Manager** o la **administración conjunta** de Microsoft Intune y Configuration Manager.

La vista inicial **Todos los dispositivos** muestra los dispositivos e incluye información clave sobre cada uno:

- Cómo se administra el dispositivo
- Estado de cumplimiento
- Detalles del sistema operativo
- Cuando el dispositivo se probó por última vez

El siguiente apartado es **Líneas base de Seguridad,** donde estarán disponibles líneas de base de seguridad para dispositivos Windows, Microsoft Defender para puntos de conexión, Microsoft Edge, Windows 365 y para las aplicaciones de M365 para empresas. Las líneas de base de seguridad son grupos preconfigurados de configuraciones de Windows que ayudan a aplicar la configuración recomendada por los equipos de seguridad de Microsoft.

Las líneas base de seguridad se aplican a grupos de usuarios o dispositivos en Microsoft Intune y la configuración se aplica a dispositivos que ejecutan Windows 10 o posterior.

El objetivo de las líneas base de seguridad es poder ayudar a tener un flujo de trabajo seguro de un extremo a otro cuando se trabaja con herramientas de Microsoft.

Estas líneas base ofrecen las siguientes ventajas:

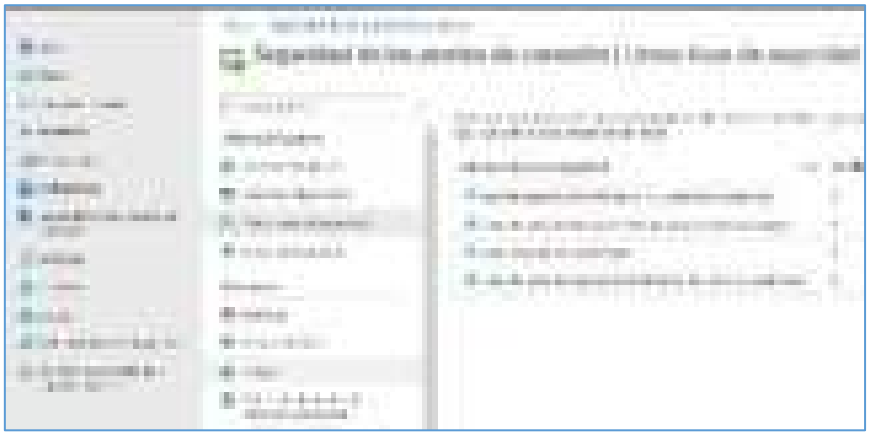
- Incluyen los procedimientos recomendados y las recomendaciones sobre la configuración que afectan a la seguridad. Microsoft Intune se asocia con el mismo equipo de seguridad de Windows que crea las líneas de base de seguridad de directiva de grupo. Estas recomendaciones se basan en la orientación y en una amplia experiencia.
- Si actualmente se tienen directivas de grupo, migrar a Microsoft Intune para la administración es mucho más fácil con estas líneas de base de seguridad. Estas líneas base de seguridad están integradas de forma nativa en Microsoft Intune e incluyen una experiencia de administración moderna.
- Si es la primera vez utilizando Microsoft Intune y no se sabe por dónde empezar, las líneas de base de seguridad ofrecen una ventaja. Se puede crear e implementar rápidamente un perfil seguro, sabiendo que ayuda a proteger los recursos y datos de la organización.

Para crear una línea base de seguridad y asignarla a un grupo hay que tener en cuenta unos requisitos básicos:

- Para administrar líneas base en Microsoft Intune, la cuenta debe tener el rol **Administrador de directiva** y de **perfil integrado**.
- El uso de algunas líneas de base podría exigir tener una suscripción activa a servicios adicionales, como Microsoft Defender para punto de conexión.
- El uso de Intune para implementar líneas base de seguridad requiere una suscripción Microsoft Intune Plan 1.

Una vez se tengan los requisitos claros para crear una línea de base de seguridad:

1. Iniciar sesión en la consola de Microsoft Intune, seleccionar **Seguridad de los puntos de conexión > Líneas de base de seguridad.**
2. Seleccionar la línea de base de seguridad que se quiera desplegar entre las disponibles y presionar **crear perfil**.



3. En los **Aspectos básicos**, escriba nombre y descripción.

   En la pestaña **Opciones de configuración**, consulte los grupos de configuración que están disponibles en la línea de base de seguridad que se eligió. Se puede expandir un grupo para ver su configuración, además de los valores predeterminados de dicha configuración de la línea de base de seguridad.

4. Cada uno de los valores de una línea base cuenta con una configuración predeterminada para esa versión de línea de base, es decir, con lo que Microsoft

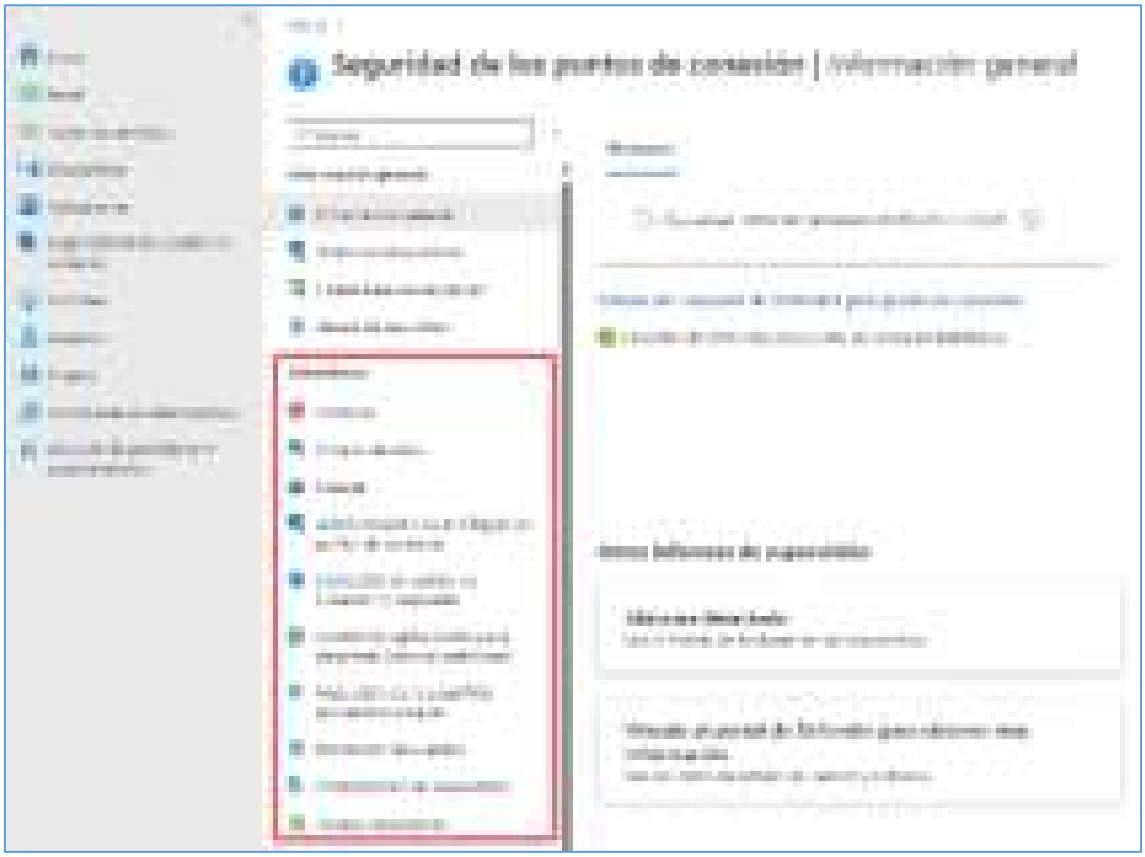
cree que es una base segura. Todo esto es configurable, pero se saldría de la base de lo que Microsoft tiene definido.

5. En la pestaña Etiquetas de ámbito, pulsar **Seleccionar etiquetas de ámbito** para abrir el panel **Seleccionar etiquetas** para asignar etiquetas de ámbito al perfil si se tuvieran.
6. En la pestaña Asignaciones, pulsar **Seleccionar grupos para incluir** y, a continuación, asignar la línea de base a uno o varios grupos. Usar **Seleccionar grupos para excluir** para ajustar la asignación.

Una vez revisados los puntos de información general en **Seguridad de los puntos de conexión,** se encuentra el apartado **Administrar.**

En este apartado, se pueden usar las directivas de seguridad para configurar la seguridad del dispositivo. Al usar estas directivas centradas en la seguridad, evitas la sobrecarga de navegar a través de un mayor número de configuraciones diversas que se encuentran en los perfiles de configuración de dispositivos y las líneas base de seguridad.

Estas directivas se encuentran en **Administrar** en el apartado Seguridad de los puntos de conexión.



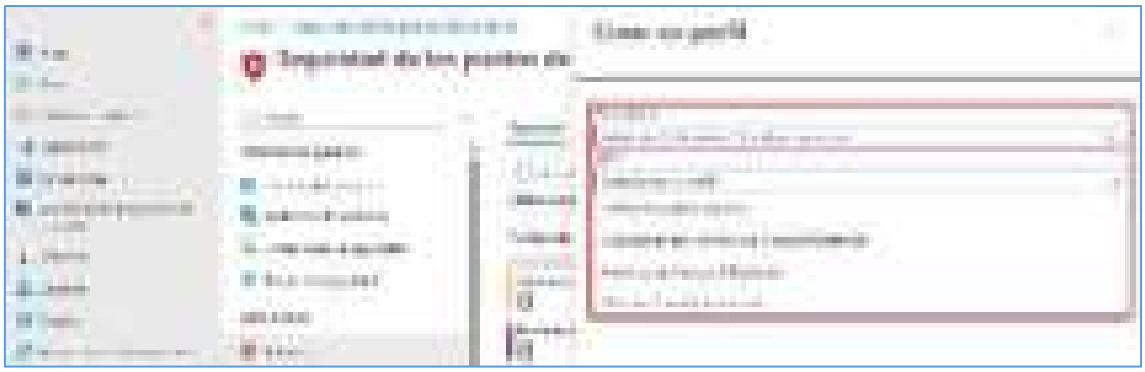
- **Antivirus**: las directivas de antivirus ayudan a los administradores de seguridad a administrar el grupo de configuraciones de antivirus para dispositivos administrados.

- **Cifrado de disco**: los perfiles de cifrado de disco de seguridad de extremo se centran solo en la configuración que es relevante para un método de cifrado integrado de dispositivos, como FileVault o BitLocker. Este enfoque facilita a los administradores de seguridad administrar la configuración de cifrado de disco sin tener que navegar por una gran cantidad de configuraciones no relacionadas.
- **Firewall**: usar la directiva firewall de seguridad de puntos de conexión en Microsoft Intune para configurar un firewall integrado para dispositivos que ejecuten macOS y Windows 10/11.
- **Detección y respuesta**: cuando se integra Microsoft Defender for Endpoint con Microsoft Intune, se pueden utilizar las directivas de seguridad de puntos de conexión para detección y respuesta (EDR) para administrar la configuración de EDR e incorporar los dispositivos a Microsoft Defender for Endpoint.
- **Reducción de superficie de ataque**: cuando el antivirus de Defender esté en uso en los dispositivos Windows 10/11, usar directivas de seguridad de puntos de conexión de Microsoft Intune para la reducción de superficie de ataque para administrar esa configuración en los dispositivos.
- **Protección de cuentas**: las directivas de protección de cuentas ayudan a proteger la identidad y las cuentas de los usuarios. La directiva de protección de cuentas se centra en la configuración de Windows Hello y Credential Guard, que forma parte de la administración Windows identity y acceso.
- **Control de aplicaciones para empresas (versión preliminar)**: administrar aplicaciones aprobadas para dispositivos Windows es posible mediante estas directivas. Las directivas de Control de aplicaciones para empresas son una adaptación del Control de aplicaciones de Windows Defender (WDAC).

Para crear una directiva:

1. Iniciar sesión en la consola de Microsoft Intune, seleccionar **Seguridad de los puntos de conexión** y, a continuación, seleccionar el tipo de directiva que se desea configurar y seleccionar **Crear directiva**. Elegir entre los siguientes tipos de directiva:
    - Antivirus
    - Cifrado de disco
    - Firewall
    - Detección y respuesta de puntos de conexión
    - Control de aplicaciones para empresas
    - Protección de cuentas
    - Reducción de la superficie expuesta a ataques
    - Protección de cuentas

2. Seleccionar la directiva deseada y elegir las propiedades de plataforma y perfil deseados:



Seleccionar **Crear**, y en la página de conceptos básicos, escribir nombre y descripción.

7. En la página Configuración, expandir cada grupo de opciones y configurar las opciones que se desee administrar con este perfil. Cuando haya terminado de configurar la configuración, seleccionar **Siguiente**.
8. En la pestaña Etiquetas de ámbito, pulsar **Seleccionar etiquetas de ámbito** para abrir el panel **Seleccionar etiquetas** para asignar etiquetas de ámbito al perfil si se tuvieran.
9. En la pestaña **Asignaciones**, pulsar **Seleccionar grupos para incluir** y, a continuación, asignar a uno o varios grupos. Usar **Seleccionar grupos para excluir** para ajustar la asignación.
10. Por último, revisar y pulsar **Crear.**

2.2.2 PERFILES DE CONFIGURACIÓN

Las políticas de configuración de dispositivos en Intune ayudan a proteger los dispositivos y configurarlos controlando una gran cantidad de configuraciones y características.

Microsoft recomienda la implementación de perfiles de configuración para Endpoint Protection, aprovisionar certificados para la autenticación, establecer comportamientos de actualización de software, etc.

2.2.2.1 POLÍTICAS DE RESTRICCIÓN DE DISPOSITIVOS

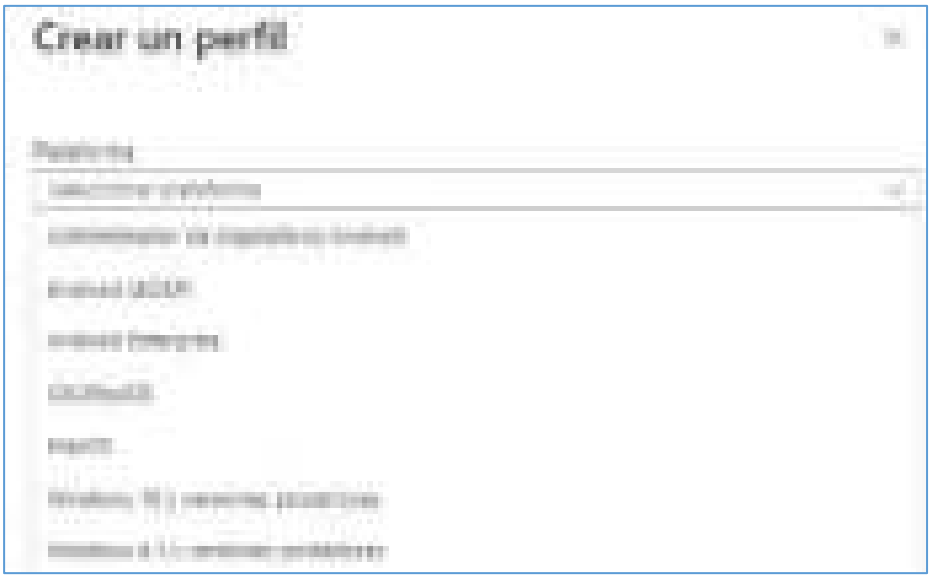
Las políticas de restricción de dispositivos permiten controlar un amplio rango de configuraciones y características a gestionar a través de una serie de categorías tales como:

- Seguridad
- Búsqueda
- Hardware

- Uso compartido de datos
- Otras opciones de configuración de los dispositivos

Para crear y desplegar una política de restricción de dispositivos, se pueden seguir los siguientes pasos:

1. Iniciar sesión en el portal de Microsoft Intune y seleccionar **Dispositivos > Configuración > Directivas**. Seleccionar la plataforma en la que quiere crear esta política.



2. Una vez elegida la plataforma, por ejemplo, Windows 10 y versiones posteriores, elegir el tipo de perfil que será **Plantillas**. Seleccionar **Restricciones de dispositivos.**


Crear un perfil

3. Dentro de este perfil hay bastantes configuraciones que se pueden personalizar, tales como la contraseña, la personalización de escritorio etc.

4. Lo siguiente será asignar esta política a un grupo de usuarios o dispositivos.
5. A continuación, se puede configurar una **Regla de aplicabilidad**, se asignará o no el perfil si se cumple una condición como la versión del sistema operativo o su edición.

2.2.2.2 PERFILES CUSTOMIZADOS

Microsoft Intune incluye muchas configuraciones para controlar diferentes características en un dispositivo. Se pueden crear perfiles personalizados para configurar características que no están integradas en Microsoft Intune. Estos perfiles incluyen características y configuraciones para controlar los dispositivos en la organización.

Para crear y desplegar una política de restricción de dispositivos, se deben seguir los siguientes pasos:

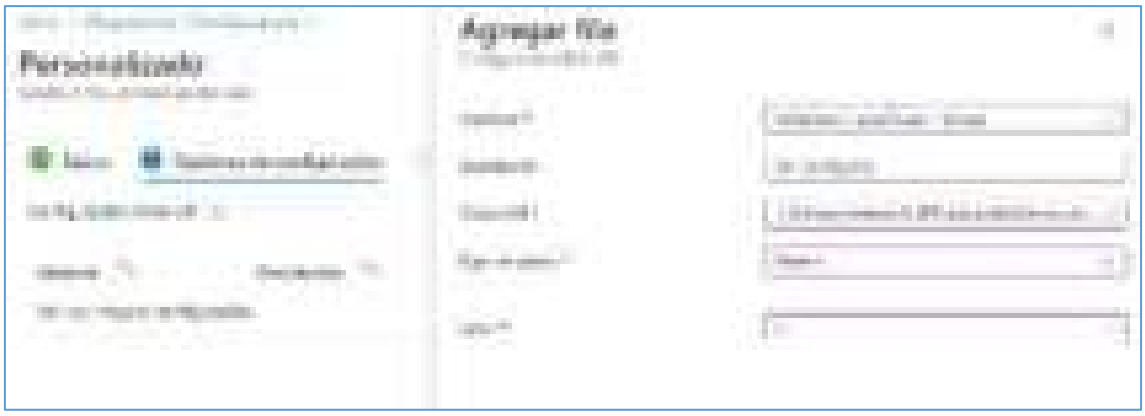
1. Iniciar sesión en el portal de Microsoft Intune y seleccionar **Dispositivos > Configuración > Crear**. Seleccionar la plataforma en la que quiere crear esta política.
2. Una vez elegida la plataforma, por ejemplo, Windows 10 y versiones posteriores, elegir el tipo de perfil que será **Plantillas**. Seleccionar **Personalizado.**

3. En las opciones básicas, introducir un nombre y descripción.
4. En las opciones de configuración seleccionar **Añadir**. Aquí se puede configurar una configuración de OMA-URI personalizada. Se debe dar un **nombre** y **descripción**.

   En el apartado **OMA-URI**, se debe introducir el OMA-URI que se quiera usar como configuración, por ejemplo:

   "./Device/Vendor/MSFT/Accounts/Users/LocalUser/LocalUserGroup".

En el **tipo de datos** elegir el tipo que quiera usar para esta configuración, en este caso ENTERO. Y en el **Valor,** introducir los datos que se quiera asociar con la configuración OMA-URI, en este caso dos.



Este OMA-URI es un ejemplo, pero actualmente en Intune ya es posible modificar los miembros del grupo de Administrares locales de cada equipo mediante una directiva de seguridad de Protección de cuentas.

Otra opción para añadir configuraciones personalizadas que no se encuentren de forma nativa en Intune para dispositivos Windows, es importar plantillas ADMX y ADML personalizadas y de terceros. Una vez importadas, se crea una directiva de configuración de dispositivo mediante esta configuración y se asigna a los dispositivos administrados. Para ello:

1. Iniciar sesión en el portal de Microsoft Intune y seleccionar **Dispositivos > Configuración > Importar ADMX > Importar**.
2. Cargar los archivos:
    - **Archivo ADMX**: seleccionar el ADMX que se quiere cargar.
    - **Archivo ADML**: elegir el archivo ADML para el idioma predeterminado que se quiere cargar. Solo un archivo de idioma por cada archivo ADMX que se cargue.
3. Seleccionar **Siguiente** y **Crear**.

2.2.3 DIRECTIVAS DE CUMPLIMIENTO

Las políticas de cumplimiento definen las reglas y configuraciones que un dispositivo debe cumplir para ser compatibles con lo que la empresa considera. Se pueden usar estas políticas en combinación con políticas de acceso condicional para securizar el acceso en base al cumplimiento de dichas políticas.

Estas reglas incluyen, entre otras cosas:

- Configuración de números PIN y contraseñas.
- Cifrado del dispositivo.
- Si el dispositivo está comprometido o rooteado.

- Si el correo electrónico está gestionado por Microsoft Intune o no.

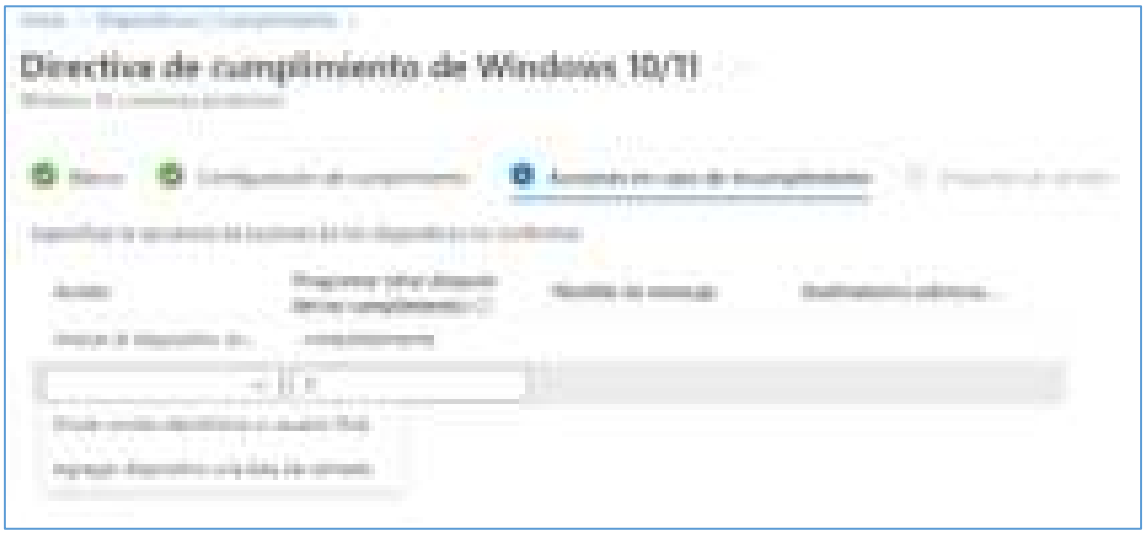
Para crear una política de cumplimiento, seguir los siguientes pasos:

1. Iniciar sesión en el portal de Microsoft Intune y seleccionar **Dispositivos > Cumplimiento > Directivas > Crear directiva**.
2. Seleccionar la plataforma en la que se quiere crear la directiva.

3. Elegir los parámetros a configurar, entre los siguientes.

4. Una vez elegidos los parámetros, en el siguiente paso se pueden realizar acciones para los dispositivos que no cumplan con los parámetros configurados. Por defecto, cuando un dispositivo no cumple con lo establecido Microsoft Intune lo marca automáticamente como "**No conforme",** pero se pueden añadir acciones

adicionales como el envío de un correo electrónico al usuario final para que sepa que el dispositivo no cumple con los requerimientos de la empresa y tiene que cambiar cierta configuración para entrar en ese cumplimiento. También se puede configurar que se retire el dispositivo de Microsoft Intune si no cumple con lo requerido.



5. Por último, asignar la directiva a grupos de usuarios o dispositivos y seleccionar **Crear.**

2.2.4 POLÍTICAS DE ACCESO CONDICIONAL

Microsoft Intune usa las políticas de acceso condicional para controlar los dispositivos y aplicaciones que puedan conectarse a recursos dentro del entorno empresarial. Esta función es una funcionalidad de Microsoft Entra ID que se incluye con una licencia de Microsoft Entra Premium. Al estar integrado en Intune, esta funcionalidad se mejora ya que se puede agregar el cumplimiento de dispositivos y la administración de aplicaciones.

El acceso condicional en Microsoft Intune funciona con configuraciones de dispositivo, directivas de cumplimiento y directivas de protección de aplicaciones. Hay dos formas de usar el acceso condicional en Microsoft Intune:

Acceso condicional basado en dispositivos

Microsoft Intune y Microsoft Entra ID trabajan juntos para asegurarse de que solo determinados dispositivos compatibles puedan acceder al correo electrónico, los servicios de Microsoft 365, las aplicaciones de software como servicio (SaaS) y las aplicaciones locales.

Acceso condicional basado en la aplicación

Microsoft Intune y Microsoft Entra ID funcionan conjuntamente para asegurarse de que solo las aplicaciones administradas puedan acceder al correo electrónico corporativo u otros servicios de Microsoft 365.

Para más información sobre el acceso condicional consulte la guía [CCN-STIC-884A - Guía de configuración segura para Azure].

2.3 APLICACIONES

2.3.1 DESPLIEGUE APLICACIONES

Microsoft Intune ofrece la capacidad de desplegar aplicaciones a los dispositivos que las requieran. Desde la consola de Microsoft Intune, se pueden configurar, así como realizar su asignación, protección y supervisión.

Es importante anotar que el **despliegue de manera disponible para dispositivos inscritos** solo funciona para grupos de usuarios y no para grupo de dispositivos.

Hay varios tipos de aplicaciones admitidas en Microsoft Intune:

Tipos de Aplicación	Instalación	Actualizaciones
Aplicaciones de la tienda	Microsoft Intune instala la aplicación en el dispositivo.	Automáticas.
Aplicaciones personalizadas (línea de negocio)	Carga de archivo en Microsoft Intune para su instalación en el dispositivo.	Se debe actualizar la aplicación.
Aplicaciones integradas	Microsoft Intune instala la aplicación en el dispositivo.	Automáticas.
Aplicaciones vía Web	Intune crea un acceso directo a la aplicación web en el dispositivo.	Automáticas.
Aplicaciones de otros servicios de Microsoft	Intune crea un acceso directo a la aplicación en el Portal de empresa.	Automáticas.

También existen aplicaciones específicas que se pueden agregar en Intune. Estas aplicaciones funcionan en diferentes tipos de dispositivos y son las siguientes:

Tipo Aplicación	Tipo	Procedimiento configuración
Aplicaciones Google Play Store	Aplicaciones de tienda	SO Android, escriba la URL de la tienda.
Aplicaciones de Android Enterprise	Aplicaciones de tienda	SO Android, escriba la URL de la tienda o seleccionar la aplicación desde la misma.
Aplicaciones de la Tienda iOS/iPad	Aplicaciones de tienda	SO iOS, buscar la aplicación y selecciónela en Microsoft Intune.
Aplicaciones de Microsoft Store	Aplicaciones de tienda	SO Windows, escriba la URL de la tienda o seleccionar la aplicación desde la misma.
Aplicaciones administradas por Google Play	Aplicaciones de tienda	Tipo Google Play administrado, buscar y seleccionar la aplicación en Microsoft Intune.
Aplicaciones Microsoft 365 para Windows 10 y posteriores	Aplicaciones de tienda	SO Windows 10, seleccionar tipo Aplicaciones de Microsoft 365 y seleccionar la aplicación que se desee instalar.
Aplicaciones Microsoft 365 para MacOS	Aplicaciones de tienda	SO MacOS, seleccionar tipo Aplicaciones de Microsoft 365 y

		seleccionar la aplicación que se desee instalar.
Aplicación Microsoft Edge versión 77 y posteriores para Windows 10 / MacOS	Aplicaciones de tienda	Seleccionar Windows 10 y posteriores o MacOS en Microsoft Edge, como el tipo de aplicación.
Aplicación de línea de negocio de Android	Aplicación de Línea de negocio (LOB)	Seleccionar línea de negocio, subir un archivo ".APK" para la instalación a través de Microsoft Intune.
Aplicación de línea de negocio de iOS/iPadOS	Aplicación LOB	Seleccionar línea de negocio, subir un archivo ".ipa" para la instalación a través de Microsoft Intune.
Aplicaciones LOB de Windows	Aplicación LOB	Seleccionar línea de negocio, subir un archivo ".msi", ".appx", "appxbundle", ".msix" o ".msixbundle" para la instalación a través de Microsoft Intune.
Aplicación iOS/iPadOS integrada	Aplicación integrada	Seleccionar Aplicación integrada y la aplicación en la lista proporcionada.
Aplicación de Android integrada	Aplicación integrada	Seleccionar Aplicación integrada y la aplicación en la lista proporcionada.
Aplicaciones web	Aplicación web	Seleccionar Vínculo web y escribir una dirección URL válida que apunte a la aplicación web.
Clip web iOS/iPadOS	Aplicación web	Seleccionar clip web iOS/iPadOS, escribir una dirección URL válida que apunte a la aplicación web.
Clip web macOS	Aplicación web	Seleccionar clip web macOS, escribir una dirección URL válida que apunte a la aplicación web.
Vínculo web de Windows	Aplicación web	Seleccionar Vínculo web de Windows y escribir una dirección URL que apunte a la aplicación web.
Aplicaciones web multiplataforma	Aplicación web	Seleccionar Vínculo web y escribir una dirección URL que apunte a la aplicación web.
Aplicaciones del sistema Android enterprise	Aplicación de la tienda	Seleccionar Aplicación del sistema Android Enterprise y escribir el nombre de la aplicación, publicador y el archivo.
Aplicaciones Win32 (Windows)	Aplicación LOB	Seleccionar tipo **Aplicación Windows (Win32),** y seleccionar un archivo ".intunewin" previamente creado
Aplicación Catálogo de aplicaciones empresariales	Aplicación LOB	Seleccionar Aplicación de catálogo de aplicaciones empresariales, también la aplicación y establecer la información de la aplicación (comandos instalación, etc.)
Aplicaciones LOB de macOS	Aplicación LOB	Seleccionar Aplicación de línea de negocio, seleccionar el archivo paquete de la aplicación y el propio archivo ".pkg".
Aplicaciones macOS (DMG)	Aplicación LOB	Seleccionar aplicación macOS (DMG), seleccionar el archivo paquete de la aplicación y el propio archivo ".dmg".

Aplicaciones macOS (PKG)	Aplicación LOB	Seleccionar aplicación macOS (PKG), seleccionar el archivo paquete de la aplicación y el propio archivo ".pkg".
Microsoft Defender para punto de conexión (macOS)	Aplicación de la tienda	Seleccionar macOS en Microsoft Defender para punto de conexión y configurar la aplicación.

2.3.1.1 STORE

Android

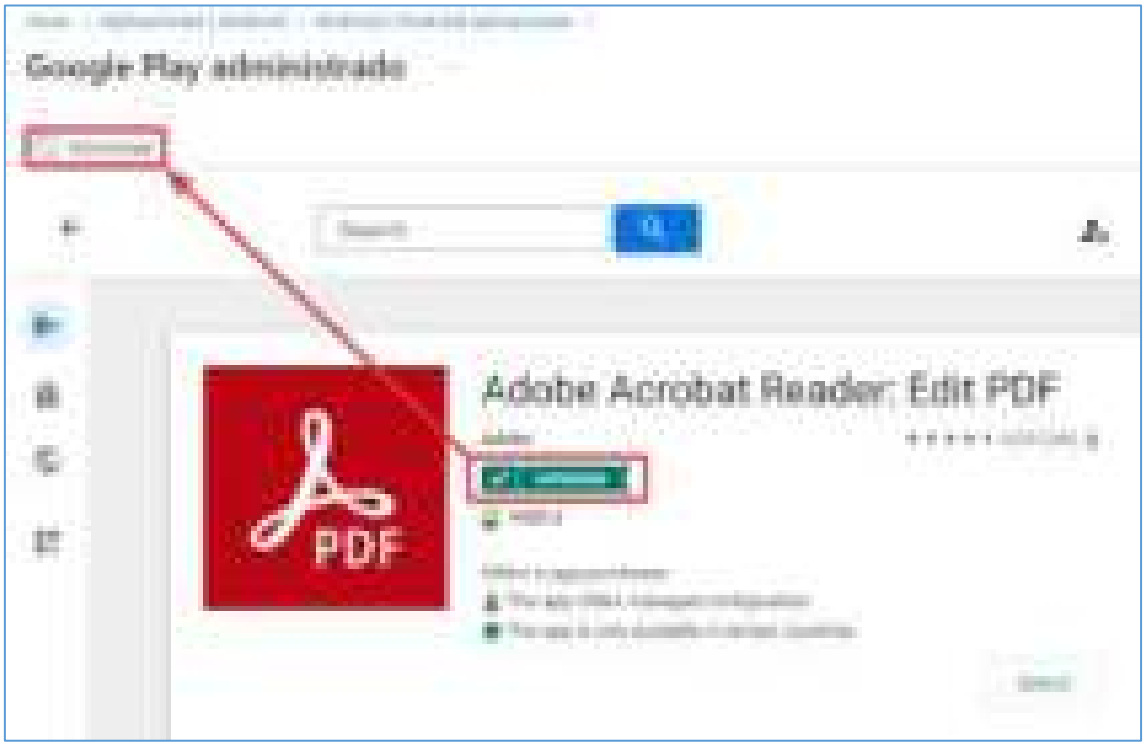
Antes de realizar este paso, debe estar habilitada la tienda de Android.

Para agregar aplicaciones desde la tienda:

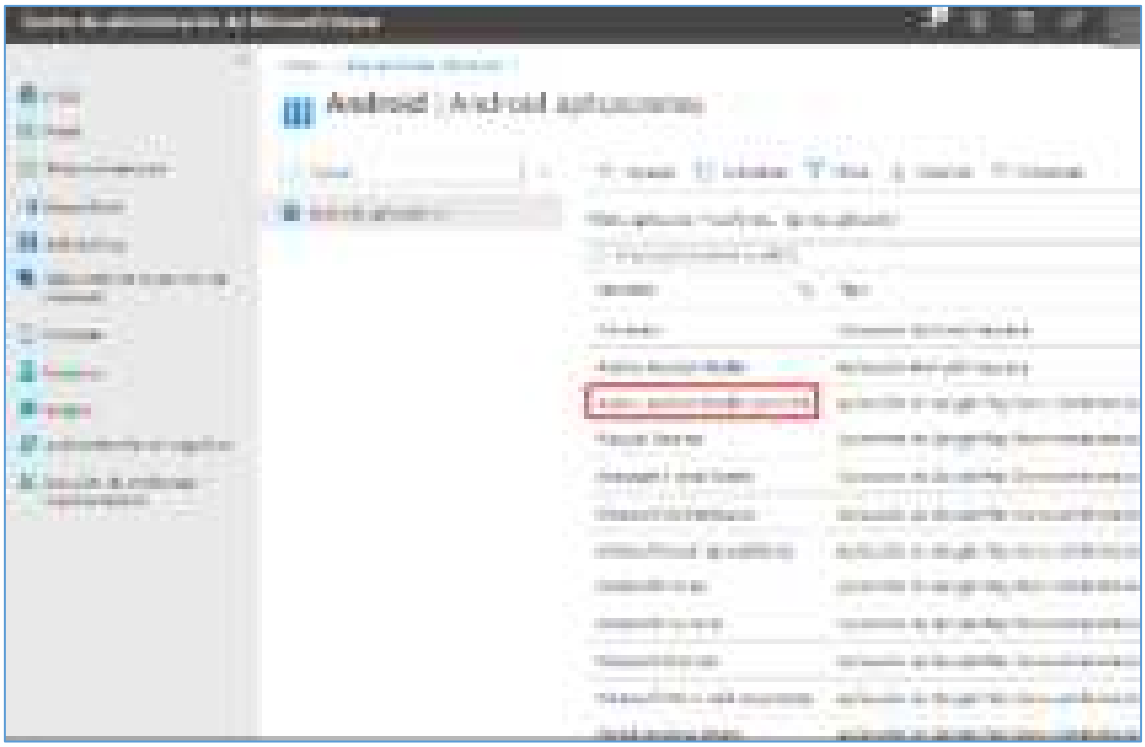
1. Iniciar sesión en el portal de Intune, seleccionar **Aplicaciones > Android > Agregar > Aplicación de Google Play Administrado**.

2. En la siguiente pantalla se debe buscar la aplicación que se desee y hacer clic en **Seleccionar.**

3. Por último, para que la aplicación salga disponible en el menú aplicaciones de Intune, se debe pulsar sobre el botón **Sincronizar,** esto hará que aparezca la aplicación para ser asignada.



4. En el menú aplicaciones de Android se puede ver como aparece la aplicación disponible para ser asignada.

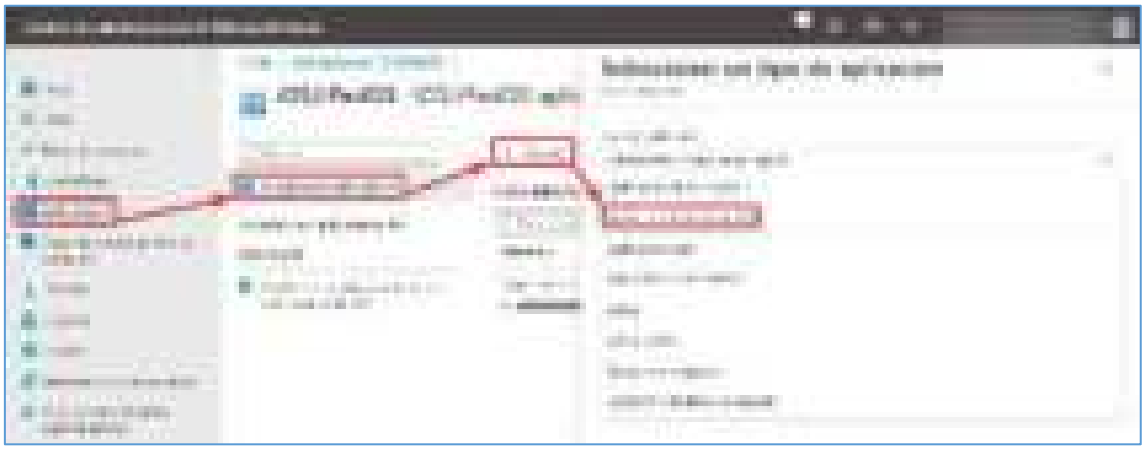


iOS

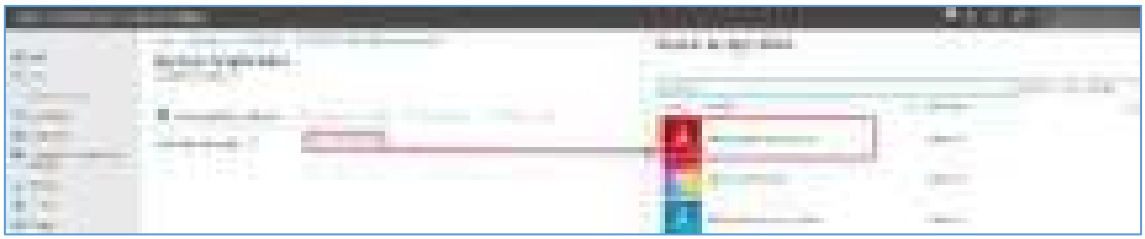
Al igual que en Android, para realizar este paso debe estar habilitada la tienda de iOS.

Para agregar aplicaciones desde la tienda:

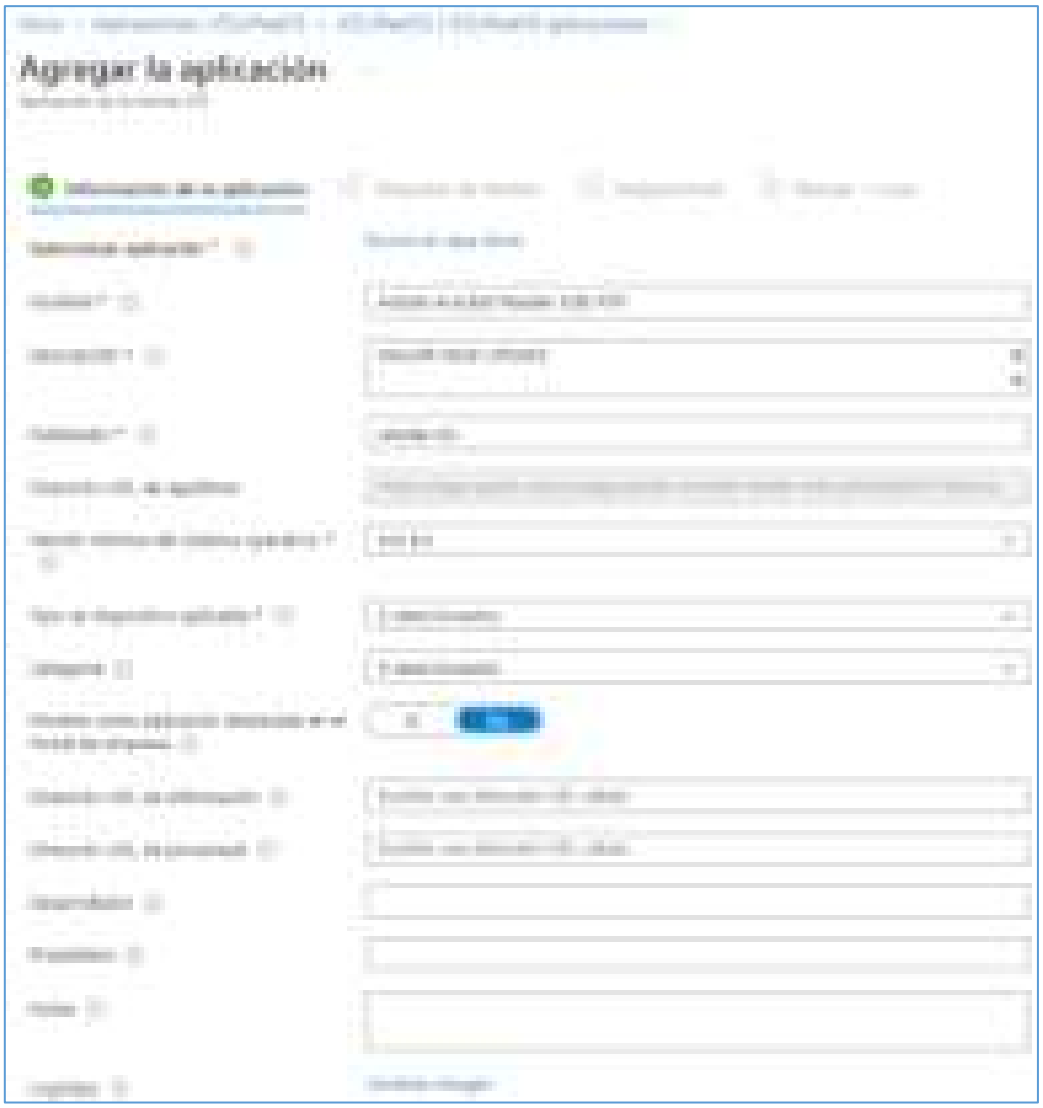
1. Iniciar sesión en el portal de Intune, seleccionar **Aplicaciones > iOS/iPadOS aplicaciones > Agregar > Aplicación de la tienda iOS.**



2. En la siguiente pantalla buscar la aplicación que se desea y pulsar **Seleccionar.**



3. En la siguiente pantalla podrá configurar varios aspectos de la aplicación como nombre y descripción.



Windows

Un administrador con privilegios de Administrador global o de Intune puede seguir estos pasos para agregar e implementar una aplicación para dispositivos Windows desde la Store:

1. Iniciar sesión en el portal de Intune, seleccionar **Aplicaciones > Windows aplicaciones > Agregar > Aplicación Microsoft Store.**
2. En la siguiente pantalla buscar la aplicación que se desea y **Seleccionar.**

3. Por último, de igual forma que para iOS, se podrán configurar varios aspectos de la aplicación como nombre, descripción, categoría, logotipo, etc.

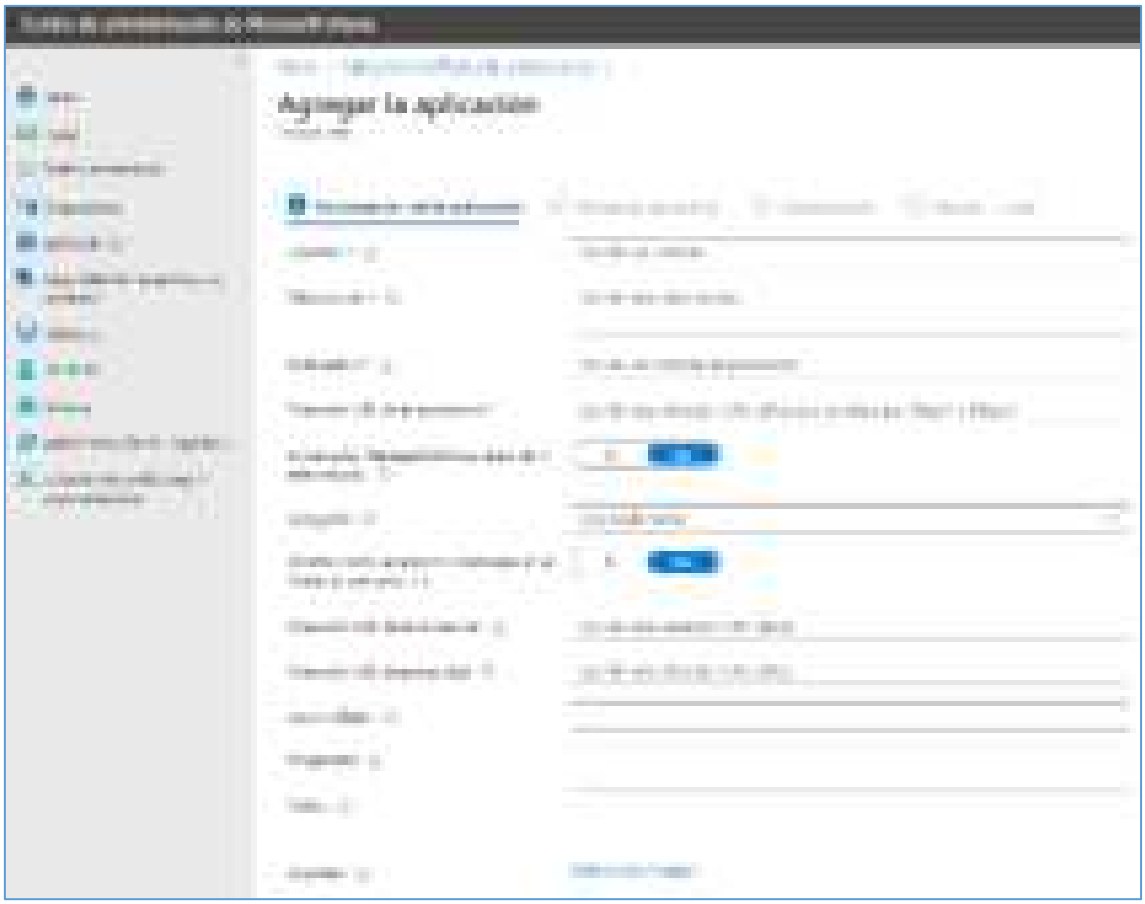
2.3.1.2 APLICACIONES WEB

Windows, iOS y macOS

Para añadir una aplicación a Microsoft Intune como un acceso directo de una página Web, hacer lo siguiente:

1. Iniciar sesión en el portal de Microsoft Intune y seleccionar **Aplicaciones > Todas las aplicaciones > Agregar > Vínculo web.**

2. En la siguiente pantalla, se podrá elegir un nombre para el vínculo web, una descripción, logo etc.



3. Por último, habrá que asignarlo a un grupo para su instalación.

Android

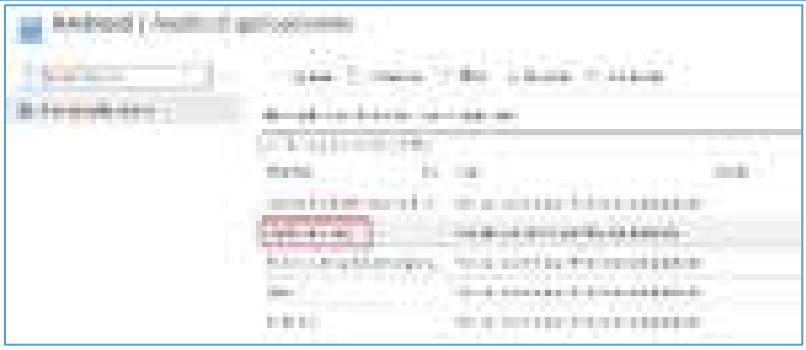
En la plataforma Android hay dos métodos, el primero es igual que el expuesto, y el segundo es más practico porque el resultado final queda como si de una aplicación de Android se tratase. Para ver este método seguir los siguientes pasos:

1. Iniciar sesión en Microsoft Intune, seleccionar **Aplicaciones > Android > Aplicación de Google Play Administrado**.

2. Dentro de esta pantalla que es donde se seleccionan aplicaciones Android desde la tienda, se elegirá el símbolo de aplicaciones Web y para añadir una aplicación, pulsar sobre el botón **"+"** de la esquina inferior derecha.

3. Aquí se podrá dar un nombre a la aplicación, se deberá introducir la dirección URL de la página Web y se podrá subir un icono.

4. Una vez creada es importante pulsar sobre el botón **Sincronizar,** para que la aplicación salga disponible para asignar.



2.3.1.3 APLICACIONES LOB

Windows, iOS, Android y macOS

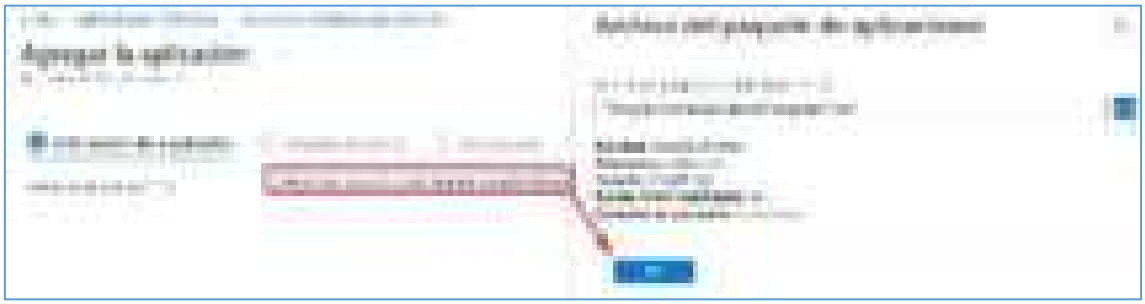
Las aplicaciones que se crean internamente o como una aplicación personalizada son aplicaciones de línea de negocio (LOB). La funcionalidad de este tipo de aplicación se ha creado para las plataformas compatibles con Microsoft Intune, por ejemplo, Windows, iOS/iPad, macOS o Android.

- La plataforma Windows trabaja con archivos *".msi", ".appx", ".appxbundle", ".msix" y ".msixbundle"*.
- La plataforma Android trabaja con archivos *".apk".*
- La plataforma macOS trabaja con archivos *".pkg".*
- La plataforma iOS/iPad trabaja con archivos *".ipa".*

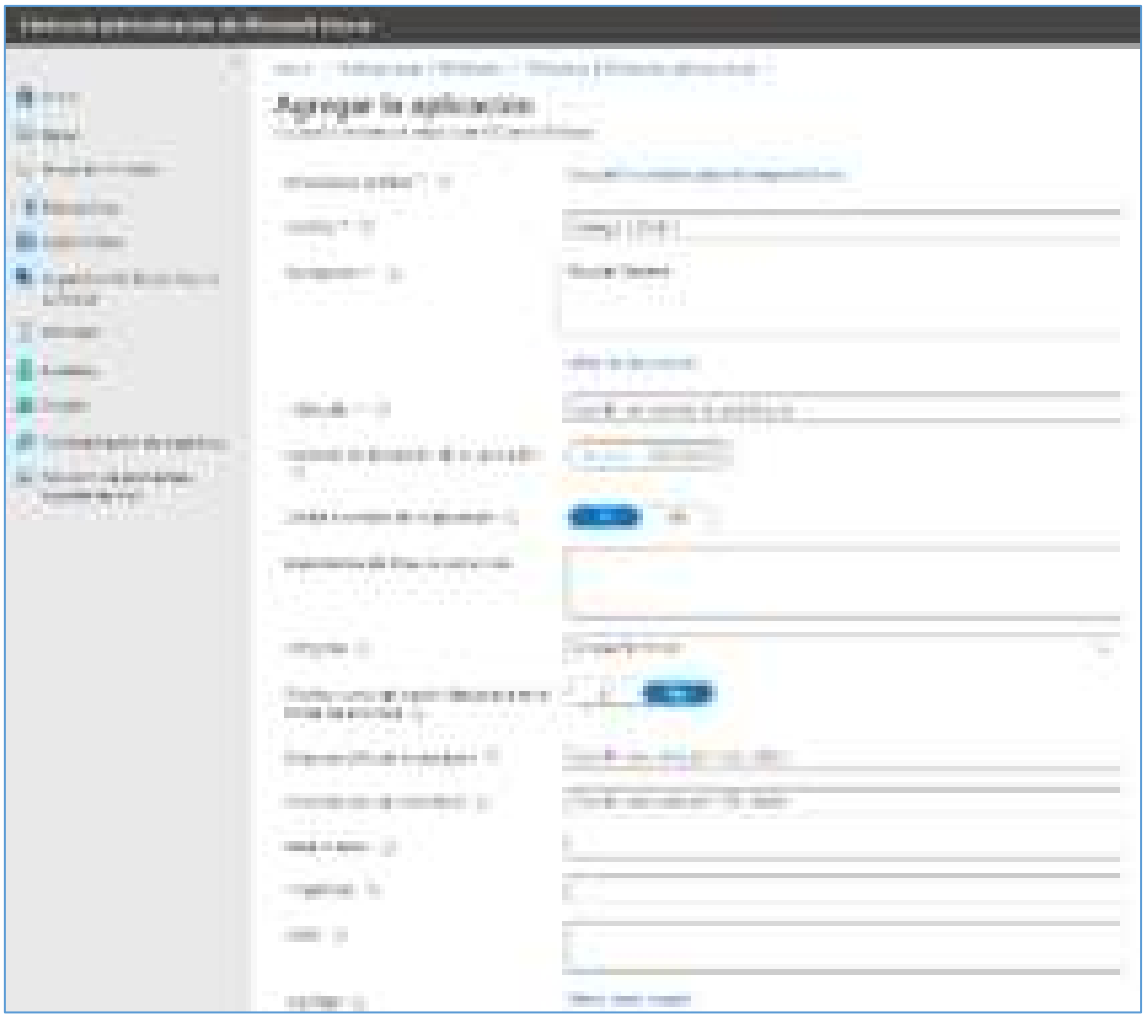
Para agregar una aplicación de este tipo hay que tener preparado el archivo que se quiera subir a Microsoft Intune y elegir su plataforma, el método es el mismo para las cuatro plataformas:

1. Iniciar sesión en la consola de Microsoft Intune, seleccionar **Aplicaciones > Windows/Android/iOS/iPad/MAC > Aplicación de línea de negocio**.

2. En la siguiente pantalla se debe subir el archivo a la consola.



3. En la pantalla de información, se podrá dar un nombre a la aplicación y diferentes configuraciones.



2.3.1.4 APLICACIONES WIN32

Con Microsoft Intune se puede administrar aplicaciones Win32, es decir, aplicaciones, por ejemplo, en las que no se dispone de un archivo *".msi"* y habría que transformar el paquete en *".intunewin".*

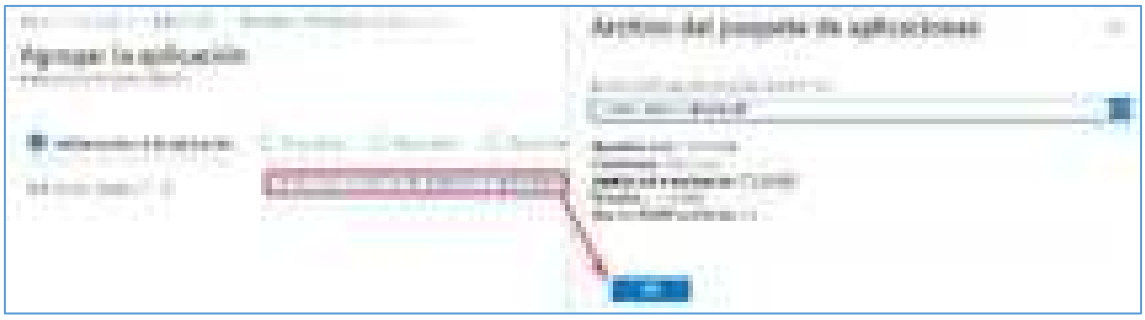
En el siguiente enlace se podrá descargar el software necesario para convertir los archivos de instalación en formato *".intunewin".*

GitHub - microsoft/Microsoft-Win32-Content-Prep-Tool: A tool to wrap Win32 App and then it can be uploaded to Intune

Desde este enlace se descargará un archivo .zip, el cual contiene la herramienta de preparación.

Una vez se haya preparado la aplicación Win32 para cargarla en Intune siguiendo el flujo anterior, se deben seguir los siguientes pasos:

1. Iniciar sesión en el portal de Microsoft Intune y seleccionar **Aplicaciones > Todas las aplicaciones > Agregar > Aplicación de Windows (Win32).**
2. Seleccionar un archivo *".intunewin"* para subir a Microsoft Intune y configurar el nombre, descripción entre otras opciones.



3. Es necesario añadir los comandos de instalación y desinstalación necesarios para cada aplicación que añada de esta manera.

4. En la siguiente pantalla se debe configurar los requisitos que debe tener el dispositivo para que la aplicación se instale.

5. A continuación, se deben configurar las reglas para detectar la presencia de la aplicación.

6. En las siguientes pantallas se podrá configurar dependencias, que son aplicaciones que deben instalarse antes de instalar la aplicación que se está agregando y sustituciones, que son las aplicaciones que se sustituirán o borrarán al instalarse la aplicación que se está agregando.

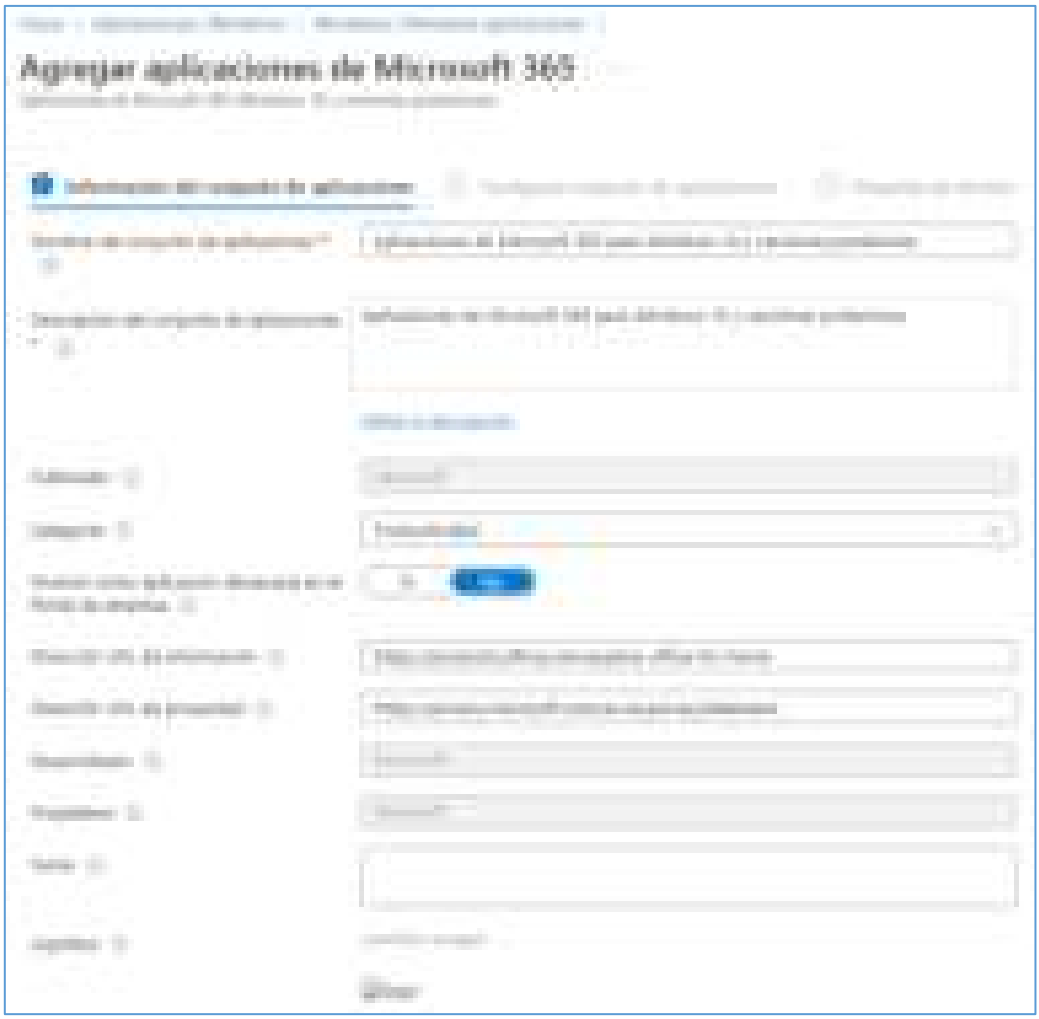
2.3.1.5 PAQUETE APLICACIONES M365

En el siguiente proceso, se verá como desplegar y asignar aplicaciones de M365 tanto en dispositivos Windows como en macOS.

Para desplegar la aplicación en dispositivos Windows o macOS:

1. Iniciar sesión en la consola de Intune y seleccionar **Aplicaciones.**
2. Seleccionar **Aplicaciones de Windows o macOS > Agregar** y seleccionar **Aplicaciones de Microsoft 365 para Windows 10 o macOS** si está en la parte de MacOS, el proceso es el mismo.

3. En la siguiente pantalla se podrá configurar un Nombre, descripción o categoría de la aplicación, una vez configurado pasar a la siguiente pantalla.



4. Aquí se podrá configurar el conjunto de aplicaciones de M365 que se quiere desplegar, eligiendo su arquitectura, el canal de actualización o sus propiedades.

5. El último paso de la adición de una aplicación es asignar la misma a un grupo de dispositivos o usuarios, una vez se haya configurado todo lo previamente descrito. Aquí existen tres opciones:

   - **Modo requerido**: Seleccionar los grupos en los que se quiere que la aplicación sea obligatoria. Las aplicaciones obligatorias se instalan automáticamente en los dispositivos inscritos.
   - **Disponible para dispositivos inscritos**: Seleccionar los grupos en los que se quiere que la aplicación esté disponible. Las aplicaciones disponibles se muestran en la aplicación portal de empresa en cada dispositivo para que los usuarios puedan instalarla opcionalmente.
   - **Disponible con o sin inscripción**: Asignar esta aplicación a grupos de usuarios que tengan dispositivos no inscritos en Intune. Además, es importante recordar que los usuarios necesitarán tener una licencia de Intune asignada.

- **Desinstalar**: Seleccionar los grupos que quiere desinstalar la aplicación. Las aplicaciones con esta asignación se desinstalan de los dispositivos seleccionados que tengan la aplicación instalada.

Al igual que este paquete de M365, también es posible agregar aplicaciones específicas ya disponibles directamente en Microsoft Intune como Microsoft Edge para Windows y macOS, y Microsoft Defender para punto de conexión para macOS.

2.3.2 PROTECCIÓN DE APLICACIONES

Se puede usar Microsoft Intune para gestionar las aplicaciones cliente que usan los empleados de la compañía. Una de las prioridades de un administrador es asegurar a los usuarios finales el acceso a las aplicaciones que ellos necesitan para trabajar. Este objetivo puede ser un reto debido a:

- Gran variedad de tipos de dispositivos y tipos de aplicaciones.
- Es posible que se necesite gestionar aplicaciones en dispositivos corporativos y dispositivos personales.
- Asegurarse mantener los datos seguros en la red.

Las directivas de protección de aplicaciones (APP) son reglas que se encargan de mantener los datos de la organización seguros dentro de las aplicaciones administradas. Estas directivas dan el control sobre cómo las aplicaciones en dispositivos móviles pueden acceder y compartir datos, asegurando así que la información confidencial permanezca protegida. Por ejemplo, se pueden restringir las operaciones de cortar, copiar y pegar o configurar un navegador gestionado para que abra todos los enlaces Web.

Las opciones disponibles en las directivas APP permiten que las organizaciones personalicen la protección según sus necesidades específicas. Para ayudar a las organizaciones a priorizar la protección del punto de conexión del cliente móvil, Microsoft ha introducido una taxonomía en su marco de protección de datos de APP para la administración de aplicaciones móviles en iOS y Android. Este marco de protección se divide en tres niveles de configuración, cada uno construido sobre el nivel anterior:

- **Protección de datos empresariales básica (nivel 1):** Se asegura de que las aplicaciones estén protegidas con un PIN y cifradas, y permite el borrado selectivo. En dispositivos Android, este nivel también verifica la certificación del dispositivo.
- **Protección de datos empresariales mejorada (nivel 2):** Incluye medidas para prevenir la pérdida de datos de APP y establece requisitos mínimos para el sistema operativo. Esta configuración es adecuada para la mayoría de los usuarios móviles que acceden a datos profesionales o educativos.
- **Protección de datos empresariales alta (nivel 3):** Incorpora mecanismos avanzados para la protección de datos, un PIN mejorado y defensas contra

amenazas móviles de APP. Esta configuración es ideal para usuarios que acceden a datos de alto riesgo.

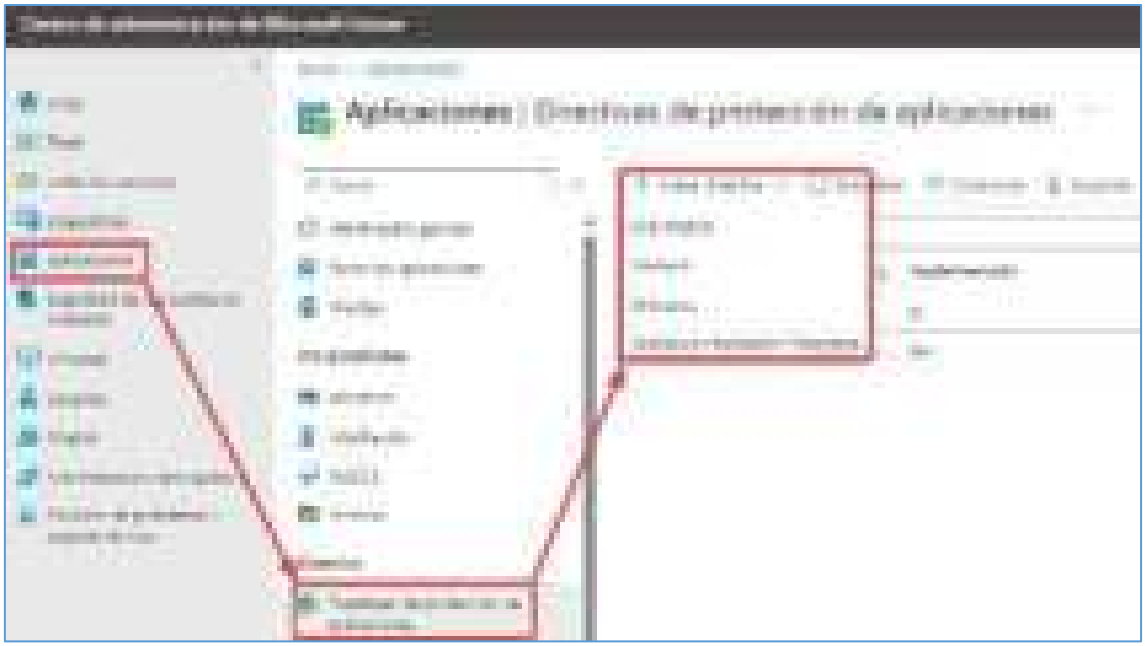
2.3.2.1 DISPOSITIVOS MÓVILES

En este apartado se verá como configurar una directiva de protección de aplicaciones para dispositivos iOS/iPadOS y Android para evitar las acciones de "cortar y pegar" desde una aplicación gestionada, como "Outlook" o "Teams", a aplicaciones no gestionadas, como "Facebook" o "WhatsApp". También se puede configurar que los archivos solo se puedan guardar en OneDrive y SharePoint Online, o establecer un PIN de acceso o la huella dactilar para acceder a estas aplicaciones gestionadas dotándolas así de una capa adicional de seguridad.

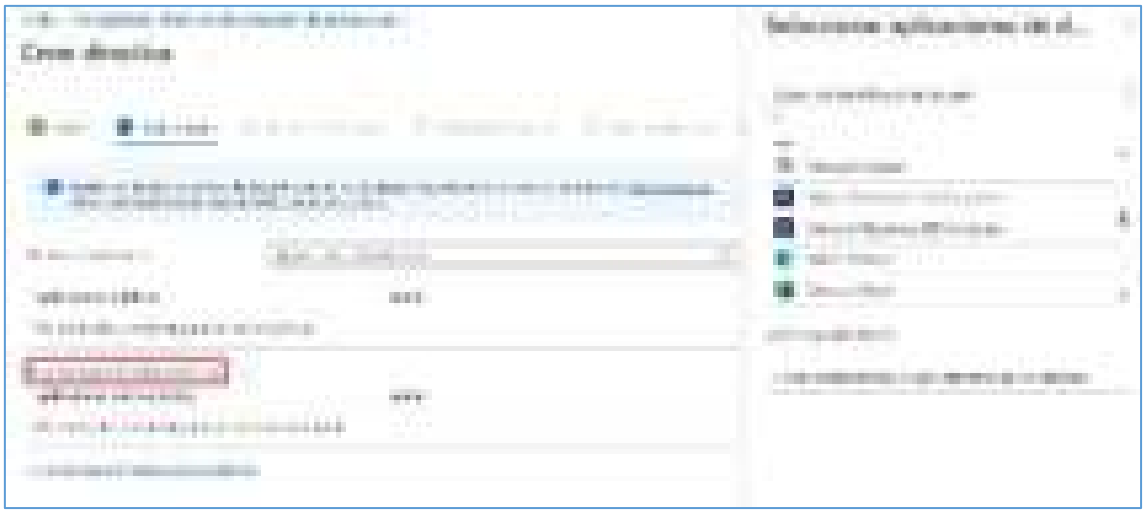
Nota: El Portal de empresa de Intune es necesario en el dispositivo Android para poder recibir las directivas de protección de aplicaciones.

Para crear una política de protección de aplicaciones:

1. Iniciar sesión en la consola de Intune y seleccionar **Aplicaciones > Directivas de protección de aplicaciones > Crear una directiva** y seleccionar la plataforma deseada**.**



2. Se deberá poner un nombre y descripción a la política y se seleccionarán las aplicaciones que se quieran proteger, estas aplicaciones son aplicaciones nativas de Microsoft.



3. En la siguiente pantalla se podrá restringir, por ejemplo, las copias de seguridad a otras aplicaciones, el envío de datos a otras aplicaciones, teclados de terceros, y la opción deseada **Restringir copiar y pegar entre otras aplicaciones.**

4. En la siguiente pestaña, se pueden configurar los requisitos de acceso, es decir, se puede configurar un método de acceso de PIN y credenciales que los usuarios deben cumplir para acceder a las aplicaciones en un contexto de trabajo.

5. La última configuración es el **Inicio condicional**, aquí se establecen los requisitos de seguridad de inicio de sesión para la directiva de protección de acceso. Se pueden realizar acciones como restablecer el PIN o bloquear el acceso si el usuario no inicia la aplicación en un periodo establecido de días.

También se pueden configurar acciones sobre la condición del dispositivo, por ejemplo, si el dispositivo tiene Jailbreak o esta rooteado bloquearle el acceso.

2.3.2.2 WINDOWS

Las directivas de protección de aplicaciones en la plataforma Windows no funcionan igual que en los dispositivos móviles. En Windows se pueden usar directivas de Windows Information Protection (WIP) con aplicaciones de Windows 10/11 para proteger las aplicaciones. Se podrían proteger aun no estando el equipo gestionado por Microsoft Intune.

Nota: Microsoft ha dejado de realizar inversiones en la administración e implementación de WIP, ya que se encuentra fuera de soporte. Recomienda el uso de protección de la información con Microsoft Purview y DLP [CCN-STIC-885E - Guía de configuración segura para Microsoft Defender for Endpoint].

Directivas de protección de aplicaciones

El acceso protegido a los datos de la organización a través de Microsoft Edge en dispositivos Windows personales se puede habilitar mediante la funcionalidad conocida como MAM de Windows. Esta función se realiza mediante las directivas de configuración de aplicaciones (ACP) de Intune, las directivas de protección de

aplicaciones de Intune (APP), la seguridad del cliente de Windows Defender Threat Protection y el acceso condicional de la protección de aplicaciones.

Hay dos categorías de configuración de directivas de protección de aplicaciones para Windows:

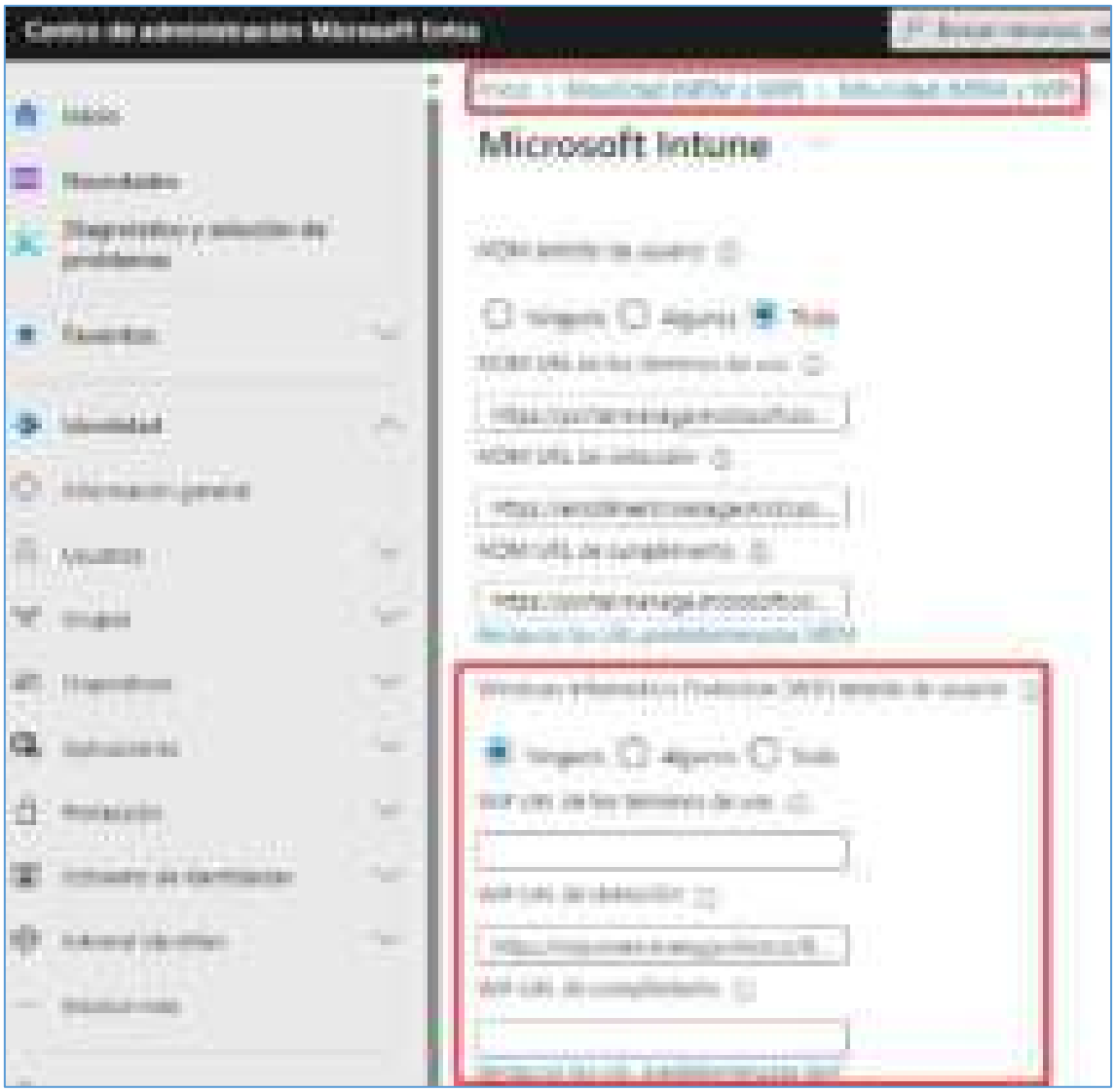
- **Protección de datos**. Como administrador, se puede supervisar el flujo de datos dentro y fuera del ámbito de protección de la organización. Este ámbito se define mediante documentos, servicios y sitios a los que accede la cuenta de la organización especificada. Estas configuraciones ayudan a controlar los datos que ingresan al contexto de la organización desde el exterior, así como los datos de la organización que se envían fuera de su ámbito.

- **Comprobaciones de estado**. Para establecer las condiciones de comprobación de estado de la directiva de protección de aplicaciones, seleccionar una configuración y definir el valor que deben cumplir los usuarios para acceder a los datos de la organización. Luego, elegir la acción a realizar si los usuarios no cumplen los requisitos condicionales. En algunos casos, se pueden configurar varias acciones para un único valor.

WIP

Para poder crear una directiva WIP, se debe configurar antes el proveedor MAM. Para ello:

1. Iniciar sesión en la consola de Intune y seleccionar **Todos los servicios > Microsoft Entra ID > Movilidad (MDM y WIP) > Microsoft Intune.**
2. Se deben de configurar los valores del grupo **Restaurar las URL predeterminadas WIP**.



- **Dirección URL de los términos de uso de WIP:** La URL de los términos de uso de WIP no es compatible con Microsoft Intune. Este campo debe dejarse en blanco para que las políticas de protección se apliquen correctamente.
- **Dirección URL de detección de WIP:** Esta es la dirección URL del punto de conexión de inscripción del servicio WIP. Se utiliza para inscribir dispositivos en la administración con el servicio WIP.
- **Dirección URL de cumplimiento de WIP:** La URL de cumplimiento de WIP no es compatible con Microsoft Intune. Este campo debe dejarse en blanco para asegurar que las políticas de protección se apliquen según lo previsto.

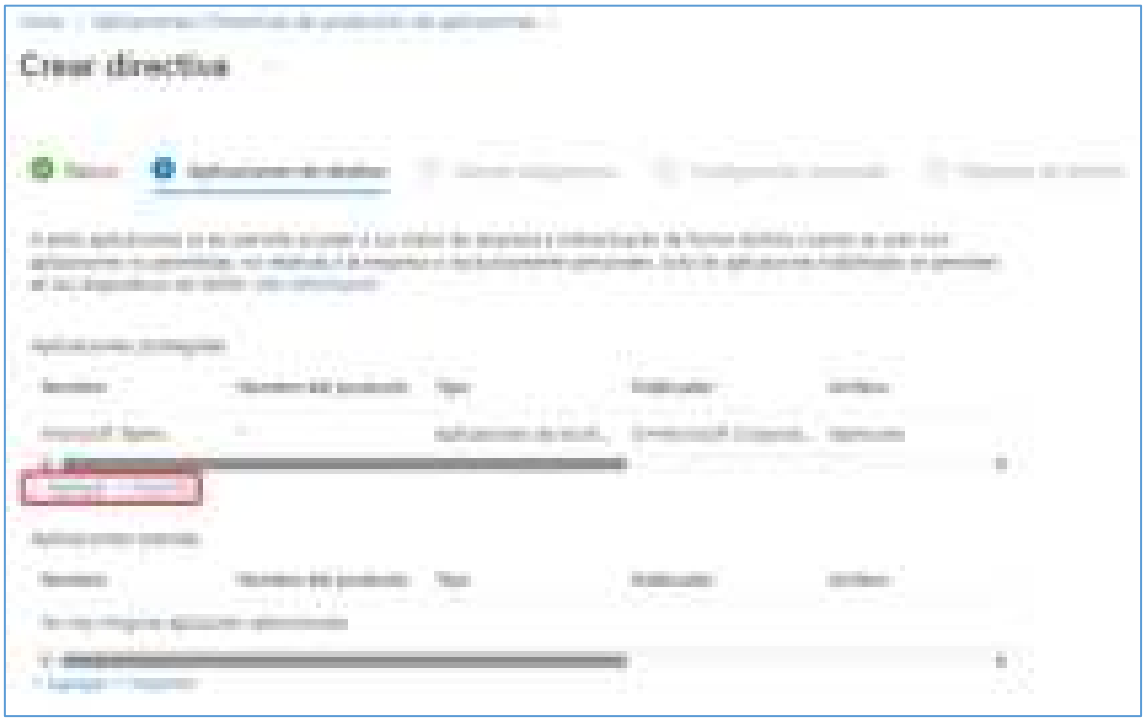
Para el ámbito de usuario WIP se dispone de las siguientes opciones:

- **Ninguno**: Seleccionar si no se puede inscribir ningún usuario en WIP.
- **Alguno**: Seleccionar grupos de Microsoft Entra que contengan usuarios que se inscribirán en WIP.
- **Todos**: Seleccionar si todos los usuarios se pueden inscribir en WIP.

Nota: Ya no se admite la creación de WIP sin directivas de inscripción (WIP-ME).

Después de haber configurado el proveedor MAM, ya se puede crear una directiva específica de WIP. Para ello:

1. Iniciar sesión en la consola de Intune y seleccionar **Aplicaciones > Directiva de protección de aplicaciones > Crear directiva,** seleccionar la plataforma Windows 10/11**.**
2. Se deberá poner un nombre y descripción a la política, y se seleccionarán las aplicaciones que se quieran proteger. Estas aplicaciones son aplicaciones nativas de Microsoft, en este caso Microsoft Teams.



3. En la siguiente pantalla se deberá elegir el modo de protección de WIP entre estos cuatro:
   - **Bloquear**: WIP detecta prácticas de intercambio de datos no autorizadas y previene que el usuario las lleve a cabo. Estas acciones bloqueadas pueden abarcar desde compartir información entre aplicaciones no autorizadas por la empresa hasta compartir datos corporativos con personas o dispositivos externos a la organización.
   - **Permitir validaciones**: WIP detecta el intercambio inapropiado de datos y notifica a los usuarios cuando realizan acciones que se consideran potencialmente no seguras. Sin embargo, este modo permite que los usuarios anulen la política y compartan los datos, registrando esta acción en el registro de auditoría.
   - **Silencio**: WIP opera en silencio, registrando el intercambio inadecuado de datos sin bloquear las interacciones solicitadas por los empleados mientras está en modo de Permitir Invalidación. Sin embargo, las acciones no

autorizadas, como las aplicaciones que intentan acceder de manera inapropiada a recursos de red o datos protegidos por WIP, aún serán detenidas.

- **Desactivado (no recomendado)**: Después de desactivar WIP, se intenta descifrar los archivos marcados con WIP en las unidades conectadas localmente. Es importante tener en cuenta que la información de descifrado y las políticas anteriores no se aplicarán automáticamente si se decide volver a activar la protección de WIP.

Además de estas opciones, se debe introducir el dominio principal, en el cual se confía.

4. En la siguiente pantalla de configuración avanzada, se podrá imponer un perímetro de red donde las aplicaciones protegidas podrán acceder a los recursos de la empresa. Se puede especificar una lista de extensiones de archivo para que esos archivos se cifren cuando se copian desde un recurso compartido de bloque de mensajes del servidor (SMB) dentro de los límites corporativos, tal y como se define en la lista de ubicaciones de red, o imponer Windows Hello para entrar a la aplicación.

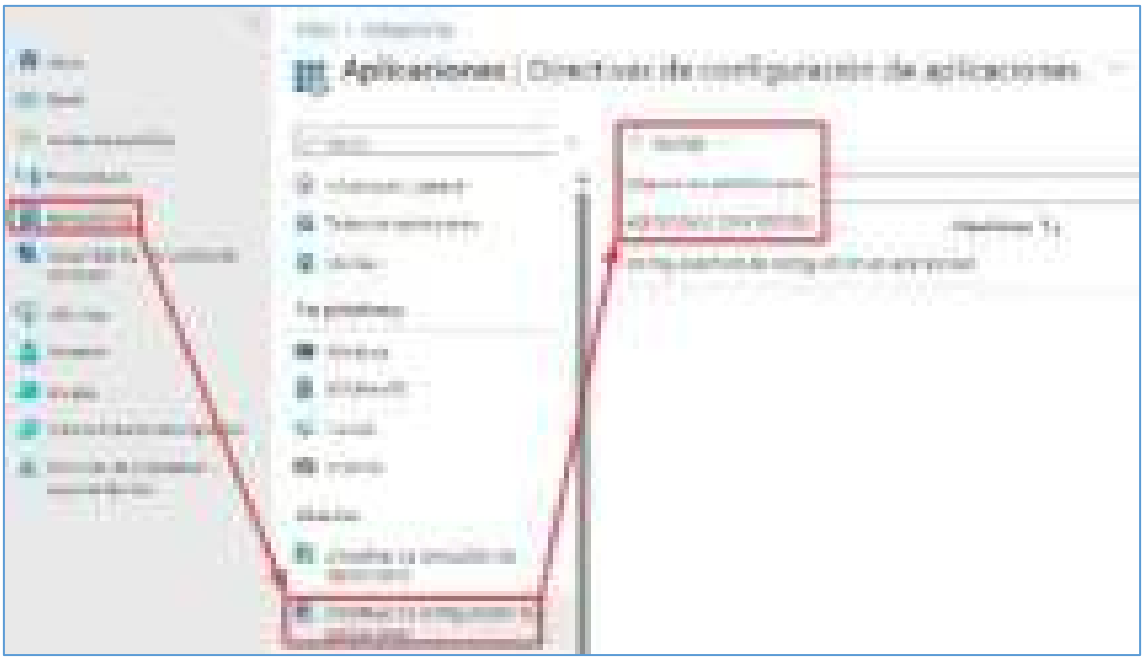
2.3.3 DIRECTIVAS DE CONFIGURACIÓN DE APLICACIONES

Las directivas de configuración de aplicaciones pueden ayudar a resolver problemas de configuración al asignar opciones de configuración antes de que los usuarios ejecuten la aplicación. Si los usuarios tuvieran que configurarla por sí mismos, podrían cometer errores, lo que podría comprometer la seguridad y la funcionalidad. Por eso, contar con una configuración predeterminada mediante directivas asegura un entorno seguro y correctamente configurado.

Este tipo de directivas solo se aplican a dispositivos móviles Android e iOS/iPadOS.

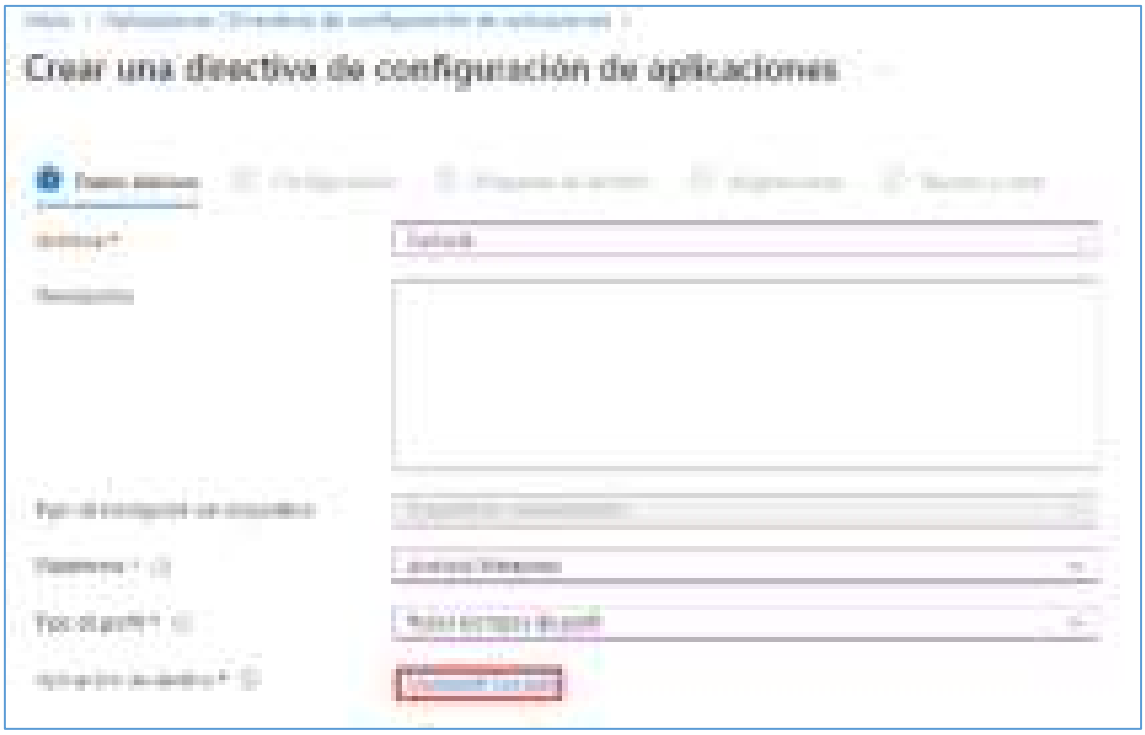
Para crear una directiva de configuración de aplicación:

1. Iniciar sesión en la consola de Intune y seleccionar **Aplicaciones > Directivas de configuración de aplicaciones > Agregar,** seleccionar el canal de directiva de configuración deseado**.**

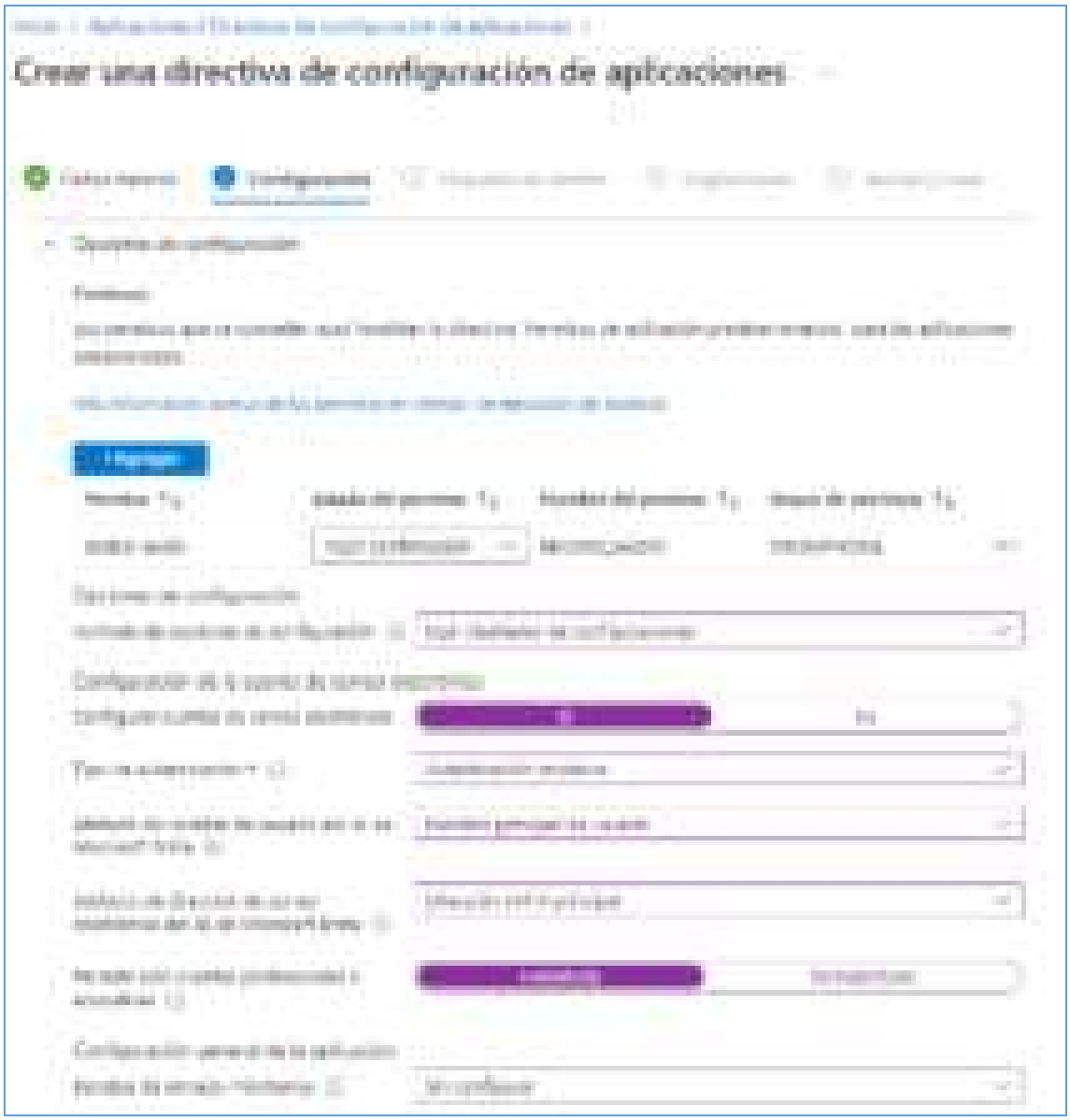


- **Dispositivos administrados**: Intune administra el dispositivo como un único proveedor de MDM. La aplicación debe estar vinculada al perfil de administración en iOS/iPadOS o ser implementada a través de Google Play administrado en dispositivos Android. Además, la aplicación es compatible con la configuración de la aplicación deseada.
- **Aplicaciones administradas**: Son aplicaciones que han integrado el SDK de aplicaciones de Intune o han sido encapsuladas mediante la herramienta de ajuste de Intune y admiten directivas APP. En esta configuración, el estado de inscripción del dispositivo y cómo se entrega la aplicación no importan. La aplicación también es compatible con la configuración de la aplicación deseada.

2. Se deberá poner un nombre y descripción a la política, y se seleccionarán las aplicaciones que se quieran proteger, estas aplicaciones son aplicaciones que están desplegadas en Microsoft Intune, en este caso Outlook.



3. Se podrán configurar los permisos que se conceden a la aplicación, configurar automáticamente la cuenta de correo electrónico, permitir solo cuentas corporativas, etc.



Esta directiva es de configuración, pero brinda seguridad añadida al poder tocar sobre los permisos que tiene la aplicación y sobre la configuración de esta, por ello es recomendable usar estas directivas.

3. CONFIGURACIÓN SEGURA PARA MICROSOFT INTUNE

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:

BOE-A-2022-7191 Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Las medidas que se presentan a continuación son importantes para proteger el entorno creado en el servicio de Microsoft Intune.

3.1 MARCO OPERACIONAL

3.1.1 CONTROL DE ACCESO

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

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

Nota: Para cumplir con los requisitos exigidos dentro del ámbito del ENS, se recomienda consultar la guía [CCN-STIC-884A Guía de Configuración segura para Azure].

3.1.1.1 IDENTIFICACIÓN

Usuarios y grupos en Microsoft Intune

El servicio de Microsoft Intune utiliza grupos de Microsoft Entra ID para administrar usuarios y/o dispositivos.

El proveedor de identidades es el responsable de comprobar la identidad de los usuarios que existen en el directorio de una organización y de emitir tokens de seguridad tras la autenticación correcta de dichos usuarios. Para ello, se deben crear cuentas en Microsoft Intune o Microsoft Entra ID. En esta guía se trata el método de creación de usuarios desde la consola de Intune, pero se haría de la misma manera en Entra ID.

A continuación, se describe cómo se realiza la gestión de cuentas de usuario y grupos de usuarios.

La configuración de estos grupos es totalmente configurable, pudiendo organizar los usuarios o dispositivos por ubicación geográfica, departamento, etc. El servicio de Microsoft Intune utiliza estos grupos para aplicar tareas a escala, tales como instalación de aplicaciones o establecer directivas.

El servicio de Microsoft Intune puede utilizar los siguientes tipos de grupo:

- Grupos asignados.
- Grupos dinámicos (Requiere Entra ID Premium).

Para agregar un nuevo grupo:

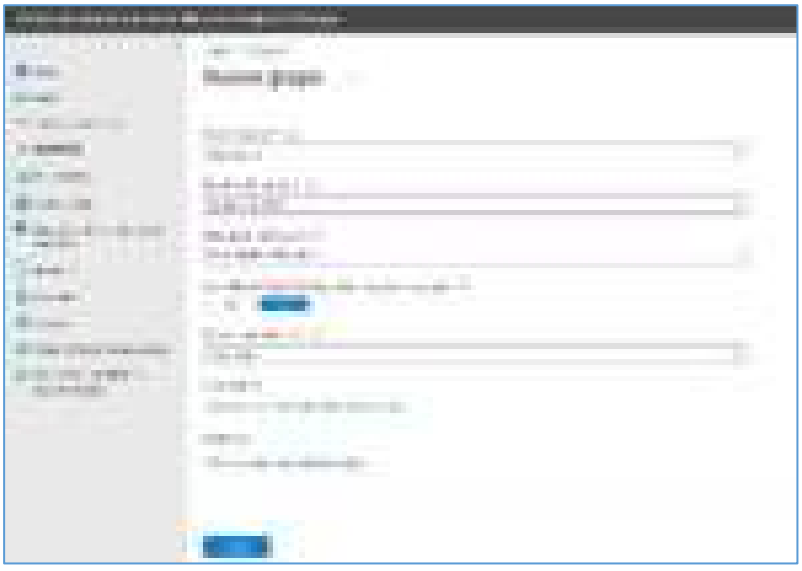
1. Iniciar sesión en el Centro de Administración de Intune. Seleccionar **Grupos** > **Nuevo grupo**.

2. En la pantalla de creación de grupo, debemos elegir el tipo de grupo, de seguridad o de tipo Microsoft 365.

   Para el uso de Microsoft Intune se recomienda utilizar grupos de seguridad.

   También se deben escribir los valores de **Nombre de grupo, descripción del grupo** y, por último, elegir el **Tipo de pertenencia** entre las siguientes opciones:

   - **Asignados**: Manualmente se asignan usuarios o dispositivos al grupo.
   - **Usuario dinámico**: se crean reglas de pertenencia para agregar y quitar usuarios automáticamente.
   - **Dispositivo mecánico**: se crean reglas de pertenencia para agregar y quitar dispositivos automáticamente.



Con estos grupos se puede controlar el acceso a los recursos a través de Microsoft Intune.

Adición de usuarios

En Azure, un usuario administrador puede agregar usuarios directamente o sincronizarlos desde una infraestructura de Active Directory Local. Los usuarios creados o sincronizados ya existentes en Azure podrán o no inscribir dispositivos y obtener acceso a los recursos de la empresa.

A estos usuarios también se les pueden dar permisos adicionales, tales como Administrador Global y Administrador de Microsoft Intune.

Según el ENS cuando un usuario disponga de diferentes roles frente al sistema, debe recibir identificadores singulares para cada uno de los casos, de forma que siempre queden delimitados los privilegios y los registros de actividad. Estos roles, se pueden configurar garantizando los mínimos privilegios posibles mediante RBAC y PIM [3.1.1.2 Requisitos de acceso].

Adición de usuarios a Microsoft Intune

Un administrador puede agregar usuarios manualmente a Microsoft Intune desde la consola de M365, desde el portal de Azure o desde la consola de Intune.

Una vez agregados los usuarios, un administrador puede editarlos y asignarle las licencias necesarias para el funcionamiento de Microsoft Intune. Para agregar un usuario a través de la consola de Intune, seguir los siguientes pasos:

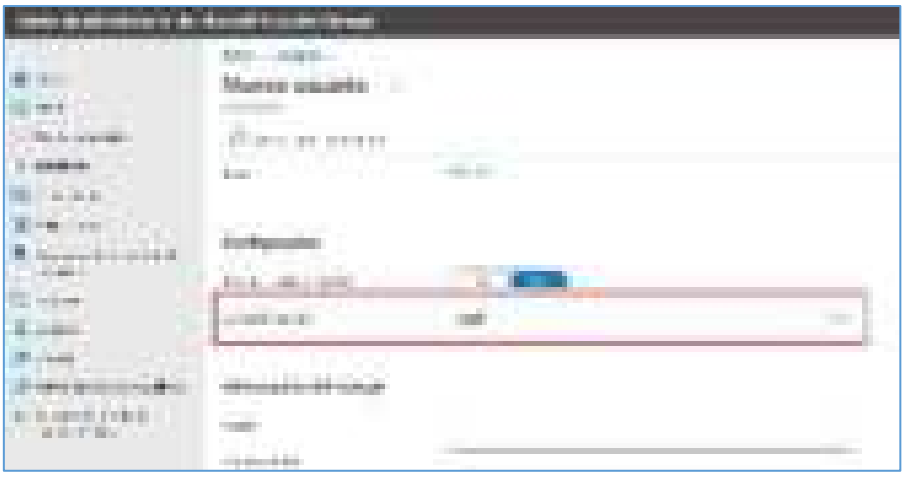
1. En la consola de Intune, seleccionar **Usuarios > Todos los usuarios > Nuevo usuario > Crear usuario.**

2. Se deben especificar los detalles del usuario tales como **Nombre de usuario** y **nombre de pila**. También, elegir si se desea crear una contraseña para el nuevo usuario o hacer que se genere automáticamente.
3. Se puede agregar o no al usuario en un grupo, esta tarea es opcional.

   Se le pueden agregar roles, de manera predeterminada tiene el rol de Usuario.

   Además, se puede impedir que el usuario final inicie sesión, seleccionando en Sí el **Bloqueo de inicio de sesión**.

4. Para agregar al usuario una licencia de Microsoft Intune, es imprescindible que se elija una **Ubicación de uso** para el usuario.



Se puede agregar también información como el **Departamento, Puesto, Nombre de compañía y Administrador.**

Cada cuenta de usuario está asociada a un identificador propio en Azure AD.

Cuando un usuario abandona la compañía, es importante que a esa cuenta de usuario se le revoquen los accesos o sea eliminada. De igual forma, se haría con el dispositivo asociado a ese usuario, teniendo así un determinado ciclo de vida de los dispositivos en la organización [3.2.3.2 Protección de la navegación web].

Para dar de baja un usuario:

1. En la consola de Intune, seleccionar **Usuarios > Todos los usuarios.**
2. Seleccionar el usuario que se quiera dar de baja y pulsar sobre el botón **Eliminar.**

Hay que tener en cuenta que las cuentas de los usuarios y dispositivos se retendrán durante un determinado periodo de retención necesario para atender a las necesidades de trazabilidad de los registros de actividad asociados a las mismas.

Para cumplir con los requisitos exigidos dentro del ámbito del ENS, consultar la guía [CCN-STIC-885A - Guía de configuración segura para Office 365].

3.1.1.2 REQUISITOS DE ACCESO

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

Así mismo, si se dispone de una licencia de Microsoft Entra ID P2, se recomienda activar el acceso condicional [2.2.4 Políticas de acceso condicional] y configurar Microsoft Entra ID Identity Protection.

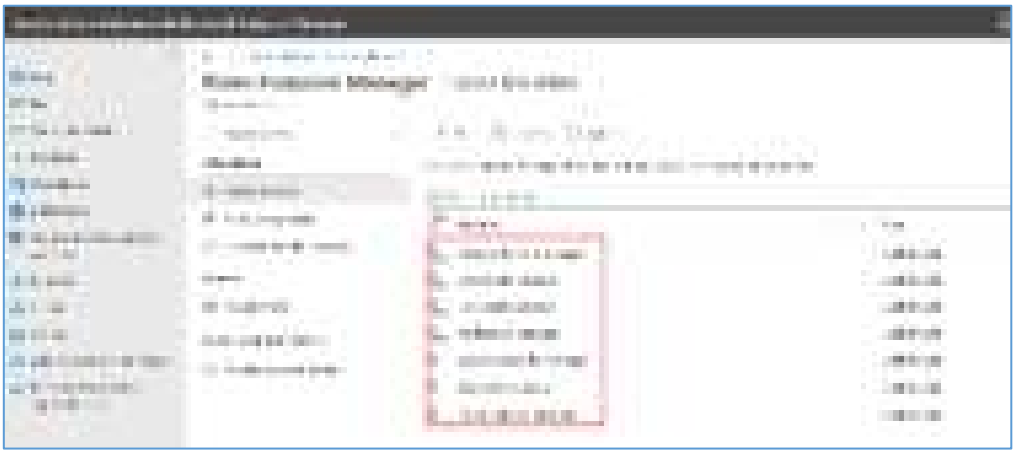
Existen roles específicos del servicio ya creados en Azure, como, por ejemplo, el específico de Microsoft Intune: "**Administrador de Microsoft Intune**". Este rol y los que pueden ser necesarios para la administración de los dispositivos, se detallan en el punto siguiente [3.1.1.3 Segregación de funciones y tareas].

Control de acceso basado en roles (RBAC)

Es importante proteger el acceso a los recursos del sistema mediante RBAC. Así lo dictan las buenas prácticas de Microsoft, siguiendo el principio de Seguridad de la información de privilegios mínimos.

Una entidad que no proteja sus recursos de accesos no autorizados está expuesta a accesos a datos sin autorización o a la realización de operaciones no permitidas. Por ello, se utiliza el RBAC para controlar quien puede realizar varias tareas dentro de la organización. Se pueden usar Roles de Azure que cubren algunos escenarios comunes en Microsoft Intune, o crear roles propios.

Se pueden ver los roles integrados de Microsoft Intune en **Administración de inquilinos > Roles > Todos los Roles**.



En un rol integrado no se puede editar el nombre, la descripción o los permisos que están configurados. A continuación, se puede ver un breve resumen de lo que permite cada uno de ellos:

- **Administrador de aplicaciones**: permite administrar las aplicaciones móviles y administradas, leer la información del dispositivo y ver los perfiles de configuración del dispositivo.

- **Administrador de privilegios de punto de conexión**: controla las políticas de administración de privilegios de conexión desde la consola de Intune.
- **Lector de privilegios de punto de conexión**: los usuarios con permisos de lectura de privilegios de conexión pueden visualizar las políticas de administración de privilegios de conexión en la consola de Intune.
- **Administrador de puntos de conexión**: administra las características de seguridad y cumplimiento, como las líneas de base de seguridad, el cumplimiento de dispositivos, el acceso condicional y Microsoft Defender para punto de conexión.
- **Operador del departamento de soporte técnico**: realiza tareas remotas relacionadas con usuarios y dispositivos y puede asignar aplicaciones o directivas a usuarios o dispositivos.
- **Administrador de roles de Microsoft Intune**: permite administrar los roles de Microsoft Intune personalizados y agregar las asignaciones de roles de Microsoft Intune integrados. Esta es la única función de Microsoft Intune que permite asignar permisos a los administradores.
- **Administrador de directivas y perfiles**: administra la directiva de cumplimiento, los perfiles de configuración, la inscripción de Apple, los identificadores de dispositivos corporativos y las líneas base de seguridad.
- **Administrador de mensajes de la organización**: administra los mensajes de la organización en Intune consola.
- **Operador de solo lectura**: ve información sobre usuarios, dispositivos, inscripciones, configuraciones y aplicaciones. No puede realizar cambios en Microsoft Intune.
- **Administrador de la escuela**: administra dispositivos Windows en Microsoft Intune for Education.
- **Administrador de P en la nube**: un administrador de PC en la nube tiene acceso de lectura y escritura a todas las características de PC en la nube ubicadas dentro del área de PC en la nube.
- **Lector de PC en la nube**: un lector de PC en la nube tiene permisos de solo lectura para todas las características ubicadas dentro del ámbito de PC en la nube.

Si ninguno de estos roles coincide con los permisos que se quieren asignar, se pueden crear roles personalizados en Microsoft Intune, un rol está definido por:

- Definición de rol: El nombre del rol, los recursos que gestiona y los permisos que le da a cada recurso.
- Miembros: Grupo de usuarios a los cuales se les dan permisos.
- Ámbito: El usuario o grupos de usuarios o dispositivos que se van a gestionar.
- Asignación: Cuando la definición, los miembros y el ámbito ha sido configurado el rol está asignado.

Para crear un rol personalizado:

1. Iniciar sesión en la consola de Microsoft Intune y seleccionar **Administración de inquilinos > Roles > Todos los Roles > Crear rol.**

Definir nombre y descripción.

2. En la siguiente página se configurarán los permisos que se quieran usar con este rol.

3. En la página **Ámbito (etiquetas),** seleccionar las etiquetas para este rol. Cuando este rol se asigna a un usuario, el usuario puede acceder a los recursos que también tienen estas etiquetas.

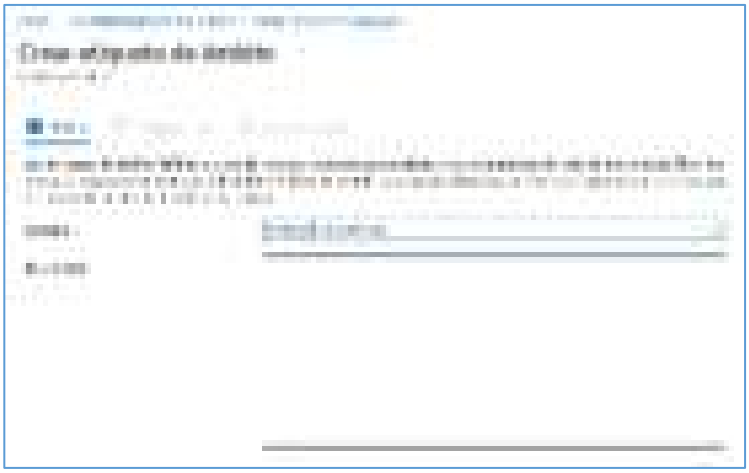
Etiquetas de ámbito

El control de acceso basado en roles y las etiquetas de ámbito se utilizan para garantizar que los administradores adecuados tengan el acceso y la visibilidad correctos a los objetos de Microsoft Intune correspondientes. Los roles definen qué acceso tienen los administradores a qué objetos, mientras que las etiquetas de ámbito determinan qué objetos pueden ver los administradores.

Para crear una etiqueta de ámbito:

1. Iniciar sesión en la consola de Microsoft Intune y seleccionar **Administración de inquilinos > Roles > Ámbito (etiquetas) > Crear.**

Definir nombre y descripción.



2. En **Asignaciones**, se asignarán los grupos de dispositivos que se desea que tengan esta etiqueta aplicada.

Una vez creada la etiqueta de ámbito, se puede asignar a un rol, de esta manera un usuario con un rol solo podrá gestionar los dispositivos que tengan esta etiqueta. Para asignar la etiqueta de ámbito a un rol:

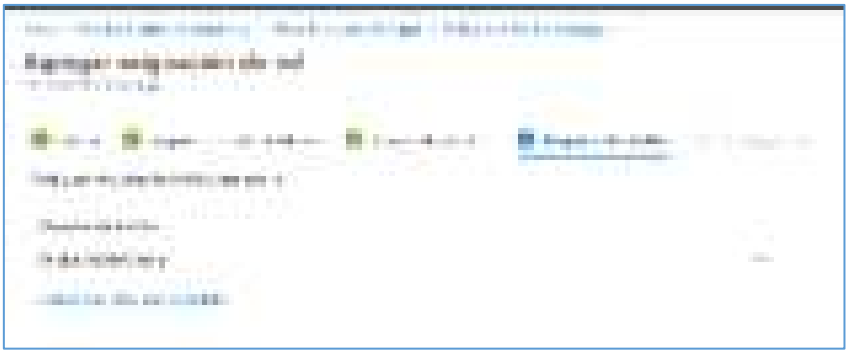
1. Iniciar sesión en la consola de Microsoft Intune y seleccionar **Administración de inquilinos > Roles > Todos los Roles** y seleccionar el rol que se desee asignar.

   Definir nombre y descripción.

2. En la página **Grupos de administración**, elegir **Seleccionar grupos para incluir** y seleccionar los grupos que quiera que formen parte de esta asignación. Los usuarios de este grupo tendrán permisos para administrar los usuarios o dispositivos de Ámbito (grupos).

3. En la página **Grupos de ámbito,** seleccionar los grupos a los que se quiere administrar.

4. En la página **Ámbito (etiquetas)**, seleccionar las etiquetas que quiera agregar a este rol. Los usuarios de los grupos de administración tendrán acceso a los objetos de Microsoft Intune que también tengan la misma etiqueta de ámbito. Se puede asignar un máximo de 100 etiquetas de ámbito a un rol.



Con las etiquetas de ámbito se deben recordar ciertos detalles:

- Cuando un administrador crea un objeto en Microsoft Intune, todas las etiquetas de ámbito asignadas a ese administrador se asignan automáticamente al nuevo objeto.
- El RBAC de Microsoft Intune no se aplica a los roles de Entra ID. Por lo tanto, los roles Administradores de servicios de Microsoft Intune y Administradores globales tienen acceso de administrador completo a Microsoft Intune independientemente de las etiquetas de ámbito que tengan.
- Si una asignación de roles no tiene etiqueta de ámbito, el administrador de TI puede ver todos los objetos en función de los permisos de los administradores de TI. Los administradores que no tienen etiquetas de ámbito esencialmente tienen todas las etiquetas de ámbito.
- Se pueden asignar etiquetas de ámbito a ciertos tipos de objetos de Intune cuando el inquilino puede tener múltiples versiones de esos objetos, como asignaciones de roles o aplicaciones. Sin embargo, hay algunas excepciones a esta regla, ya que ciertos objetos de Intune actualmente no admiten etiquetas de ámbito. Estas excepciones incluyen:
    - Identificadores de dispositivo corporativo

- Dispositivos Autopilot
- Ubicaciones de cumplimiento de dispositivos
- Dispositivos Jamf

- Las aplicaciones del Programa de compras por volumen (VPP) y los libros electrónicos asociados al token de VPP heredan las etiquetas de ámbito asignadas al token de VPP asociado.
- Solo se puede asignar una etiqueta de ámbito que esté presente en las asignaciones de roles y solo puede dirigirse a grupos que aparezcan en el ámbito de la asignación de roles.
- Si se tiene una etiqueta de ámbito asignada a un rol, no podrá eliminar todas las etiquetas de ámbito de un objeto de Intune, ya que se requiere al menos una etiqueta de ámbito.

3.1.1.3 SEGREGACIÓN DE FUNCIONES Y TAREAS

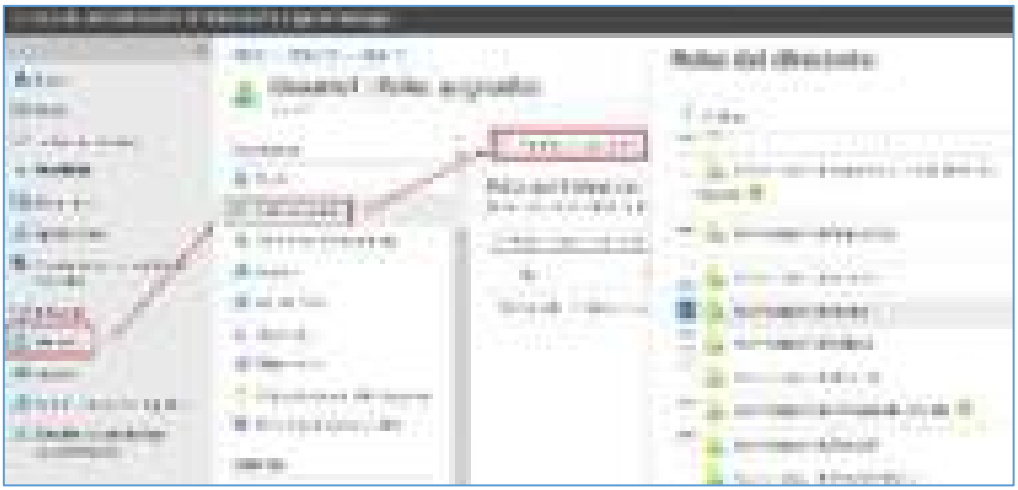
Es importante la segregación de funciones y tareas, el sistema de control de acceso se organizará de forma que se exija la concurrencia de dos o más personas para realizar tareas críticas, anulando la posibilidad de que un solo individuo autorizado pueda abusar de sus derechos para cometer alguna acción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

Concesión de permisos administrativos a los usuarios

Una vez creado el usuario, se le pueden dar permisos de administración. Es recomendable dar solo a usuarios seleccionados los permisos de administración.

A través de los siguientes pasos, se pueden conceder permisos administrativos a los usuarios:

1. Iniciar sesión en la consola de Intune con una cuenta de Administrador Global. Seleccionar **Usuarios** y seleccionar el usuario al que se quieran conceder los permisos.
2. Seleccionar **Roles asignados > Agregar asignaciones.**
3. En el panel emergente, se seleccionarán los roles que desea asignar al usuario, una vez seleccionados para terminar seleccionar **Agregar.**



En cuanto a los permisos administrativos, estos definen las tareas que pueden realizar los usuarios a los que se les ha brindado dicho rol. En esta guía nos enfocaremos en los permisos de administrador de Microsoft Intune, los cuales incluyen las siguientes opciones:

- **Administrador global**: Este rol tiene acceso a todas las características de Azure, entre ellas el servicio de Microsoft Intune. Los usuarios con este rol serán los únicos que pueden asignar roles de administrador a otros usuarios.
- **Administrador de soporte técnico de servicio**: Este rol es usado para abrir solicitudes de soporte técnico con Microsoft y con él el usuario puede ver el panel de servicio y el centro de mensajes.
- **Administrador de contraseñas**: Rol para reestablecer contraseñas, administrar solicitudes de restablecimiento de contraseñas y supervisar el mantenimiento de dicho servicio.
- **Administrador de facturación**: Rol usado para realizar compras, administrar suscripciones y supervisar el mantenimiento del servicio de facturación.
- **Administrador de usuarios**: Con este rol el usuario podrá reestablecer contraseñas, supervisar el mantenimiento del servicio, crear y eliminar cuentas de usuario y administrar solicitudes.
- **Administrador de Microsoft Intune**: Puede administrar todos los aspectos del producto Microsoft Intune.

3.1.1.4 MECANISMOS DE AUTENTICACIÓN (USUARIOS EXTERNOS)

Azure Multi-Factor Authentication (MFA) protege el acceso a los datos y aplicaciones, y al mismo tiempo mantiene la simplicidad para los usuarios. Proporciona más seguridad, ya que requiere una segunda forma de autenticación y ofrece autenticación segura a través de una variedad de métodos de autenticación.

La autenticación multifactor de Microsoft Entra requiere uno o más métodos de autenticación, incluyendo:

- Algo que el usuario conoce, típicamente una contraseña.

- Algo que el usuario posee, como un dispositivo de confianza que no es fácil de duplicar, como un teléfono móvil o una clave de hardware.
- Algo que es inherente al usuario, como datos biométricos, por ejemplo, huella dactilar o reconocimiento facial.

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 deben cambiar 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.

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].

3.1.1.5 MECANISMOS DE AUTENTICACIÓN (USUARIOS DE LA ORGANIZACIÓN)

Se entiende como *acceso local* al realizado desde puestos de trabajo dentro de las propias instalaciones de la organización, 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].

3.1.2 EXPLOTACIÓN

3.1.2.1 INVENTARIO DE ACTIVOS

Con Microsoft Intune se dispone de un centro integrado de control del inventario de la organización, pudiendo gestionar dicha información de forma sencilla y organizada desde un mismo panel.

El inventario de equipos, además de poder realizar un inventario de hardware y software de la organización, ofrece una amplia información y actualización sobre riesgos en cada equipo, incluyendo dispositivos móviles.

Es de vital importancia tener un control exhaustivo del inventario actualizado de la compañía, siendo así, se tendrá una visión sobre los elementos que existen en la organización, consiguiendo de esta manera una mayor productividad y control.

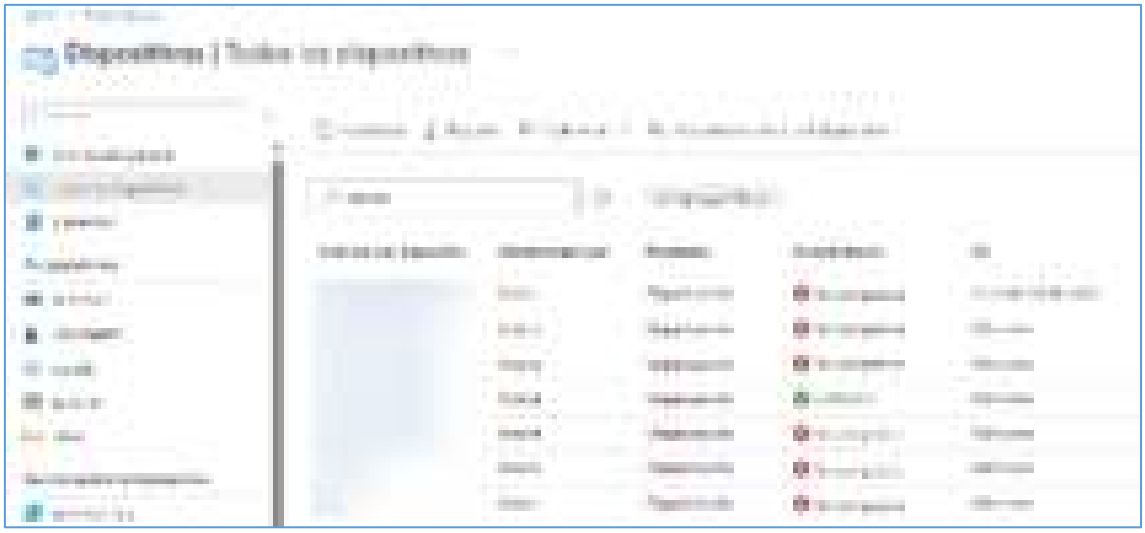
El apartado **Dispositivos** en la consola de Microsoft Intune ofrece información detallada sobre los dispositivos que administra y permite realizar tareas remotas sobre los mismos. Para ver los dispositivos disponibles en la organización:

1. Iniciar sesión en la consola de Intune, seleccionar **Dispositivos.**

Como se puede apreciar en la imagen, en el apartado **Dispositivos** existen varias opciones:

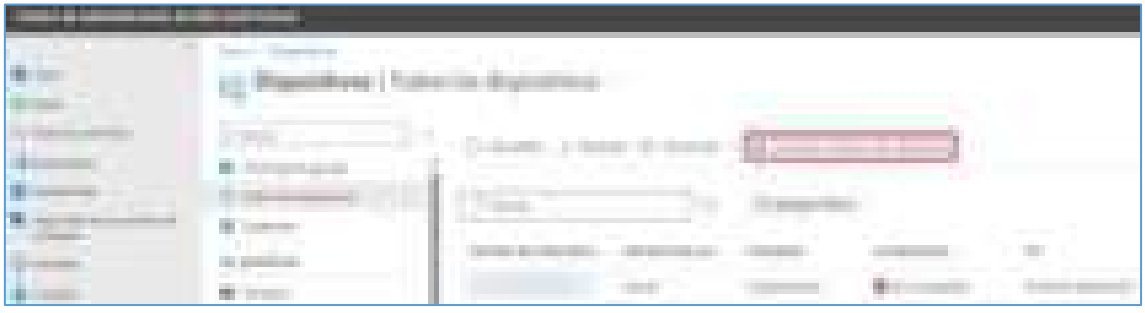
- **Información general**: se muestra una instantánea vial de los dispositivos inscritos, cuántos dispositivos usan las diferentes plataformas y mucho más.
- **Todos los dispositivos:** se muestra una lista de los dispositivos inscritos. Es posible exportar una lista con todos los dispositivos existentes en Microsoft Intune.
- **Por plataforma**: se puede ver el inventario de dispositivos por plataforma.
- Existen otras opciones relacionadas al inventario de dispositivos tales como la **regla de limpieza de dispositivos** que permite quitar automáticamente los dispositivos inactivos de Microsoft Intune y la **categoría de dispositivos**, opción que permite crear categorías de dispositivos.

Para ver un inventario completo de todos los dispositivos, seleccionar **Dispositivos > Todos los dispositivos.**



Se pueden realizar acciones masivas sobre un gran grupo de dispositivos, estas acciones varias dependiendo de la plataforma, son acciones como Sincronizar, Reiniciar o borrar.

2. Para ejecutar acciones masivas del dispositivo en varios dispositivos a la vez, seleccionar **Dispositivos > Todos los dispositivos > Acciones masivas del dispositivo**.



También se pueden realizar muchas más acciones sobre un solo dispositivo. Para ello, seleccionar un dispositivo en **Todos los dispositivos** o elegir por tipo de plataforma.

Las acciones que se pueden realizar a un solo dispositivo son más que las que se pueden hacer de forma masiva. A continuación, se exponen las acciones que se pueden realizar sobre un dispositivo:

- Restablecimiento de Autopilot (solo Windows)
- Rotación de claves de BitLocker (solo Windows)
- Recopilación de diagnósticos (solo Windows 10)
- Eliminar
- Deshabilitar bloqueo de activación (solo para iOS y macOS)
- Comienzo de cero (solo para Windows)
- Examen completo (solo Windows)
- Buscar dispositivo (solo para iOS/iPadOS, Android y Windows)
- Modo perdido (solo para iOS/iPadOS)
- Pausar actualización de configuración (solo Windows 11)
- Examen rápido (solo Windows)
- Control remoto Team Viewer (solo Android, iOS/iPadOS, macOS y Windows)
- Bloqueo remoto (solo Android, iOS/iPadOS, macOS)
- Cambio de nombre de un dispositivo (solo Android, iOS/iPadOS, macOS y Windows)
- Restablecer el código de acceso (solo Android, iOS/iPadOS)

- Reiniciar (Android, iOS/iPadOS, macOS y Windows)
- Retirar (Android, iOS/iPadOS, macOS y Windows)
- Rotación de la contraseña de administrador local (solo Windows)
- Actualizar la inteligencia de seguridad de Windows Defender (solo Windows)
- Restablecimiento del PIN de Windows 10 (solo Windows 10 Mobile)
- Eliminación de datos (Android, iOS/iPadOS, macOS y Windows)
- Envío de notificaciones personalizadas (Android y iOS/iPadOS)
- Sincronización del dispositivo (Android, iOS/iPadOS, macOS y Windows)
- Actualización del plan de datos móviles (iOS/iPadOS)

También, Intune tiene un listado de aplicaciones identificadas de los dispositivos inscritos, sirviendo como un inventario de software. Normalmente, el informe se actualiza cada siete días desde la inscripción del dispositivo, salvo por la información recopilada a través de la extensión de administración de Intune para aplicaciones Win32, que se actualiza cada 24 horas.

3.1.2.2 CONFIGURACIÓN DE SEGURIDAD

Microsoft Intune ofrece una variedad de configuraciones de seguridad a través de políticas de seguridad, configuración y cumplimiento de dispositivos. Estas políticas permiten configurar los dispositivos para cumplir con los objetivos de seguridad de su organización.

- Mediante las **políticas de seguridad de punto de conexión**, se pueden implementar medidas de seguridad enfocadas en identificar y mitigar riesgos en los dispositivos. Las tareas disponibles permiten identificar y corregir dispositivos en riesgo, asegurándose de que estén en un estado compatible o más seguro.
- Las **políticas de configuración de dispositivos** permiten administrar perfiles que definen la configuración y características de los dispositivos en la organización. Se puede configurar la protección del punto final, implementar certificados para autenticación, evitar que los usuarios sean administradores de sus dispositivos, entre otros ajustes.
- Con las **políticas de cumplimiento de dispositivos**, se crean perfiles para diferentes plataformas que establecen requisitos para los dispositivos. Estos requisitos pueden incluir credenciales robustas, cifrado de disco obligatorio o mantener niveles de amenaza específicos según lo definido por el software de gestión de amenazas.

Para más detalle de todas estas configuraciones, en esta guía se hace hincapié en el punto de protección de los dispositivos, que se puede consultar: [2.2 Protección de dispositivos].

En cuanto a las máquinas virtuales, la configuración de seguridad será como si tratara de un dispositivo físico teniendo en cuenta las limitaciones que estas tienen dentro de Microsoft Intune.

- Se desaconseja utilizar Intune para administrar máquinas virtuales de host de sesión bajo demanda, también conocidas como infraestructura de escritorio virtual (VDI) no persistente.
- Los tipos de implementación de aprovisionamiento previo y de implementación automática de Windows Autopilot no son compatibles, ya que requieren un Módulo de plataforma segura (TPM) físico.
- La inscripción en la experiencia rápida (OOBE) no se admite en máquinas virtuales que solo se pueden acceder mediante RDP, como las máquinas virtuales alojadas en Azure. Esto implica que Windows Autopilot y la OOBE comercial no son compatibles, y la página de Estado de la inscripción tampoco se admite.

3.1.2.3 GESTIÓN DE LA CONFIGURACIÓN DE SEGURIDAD

Para cumplir con los requisitos exigidos dentro del ámbito del ENS, se recomienda consultar la guía [CCN-STIC-885E- Guía de configuración segura para Microsoft Defender for Endpoint].

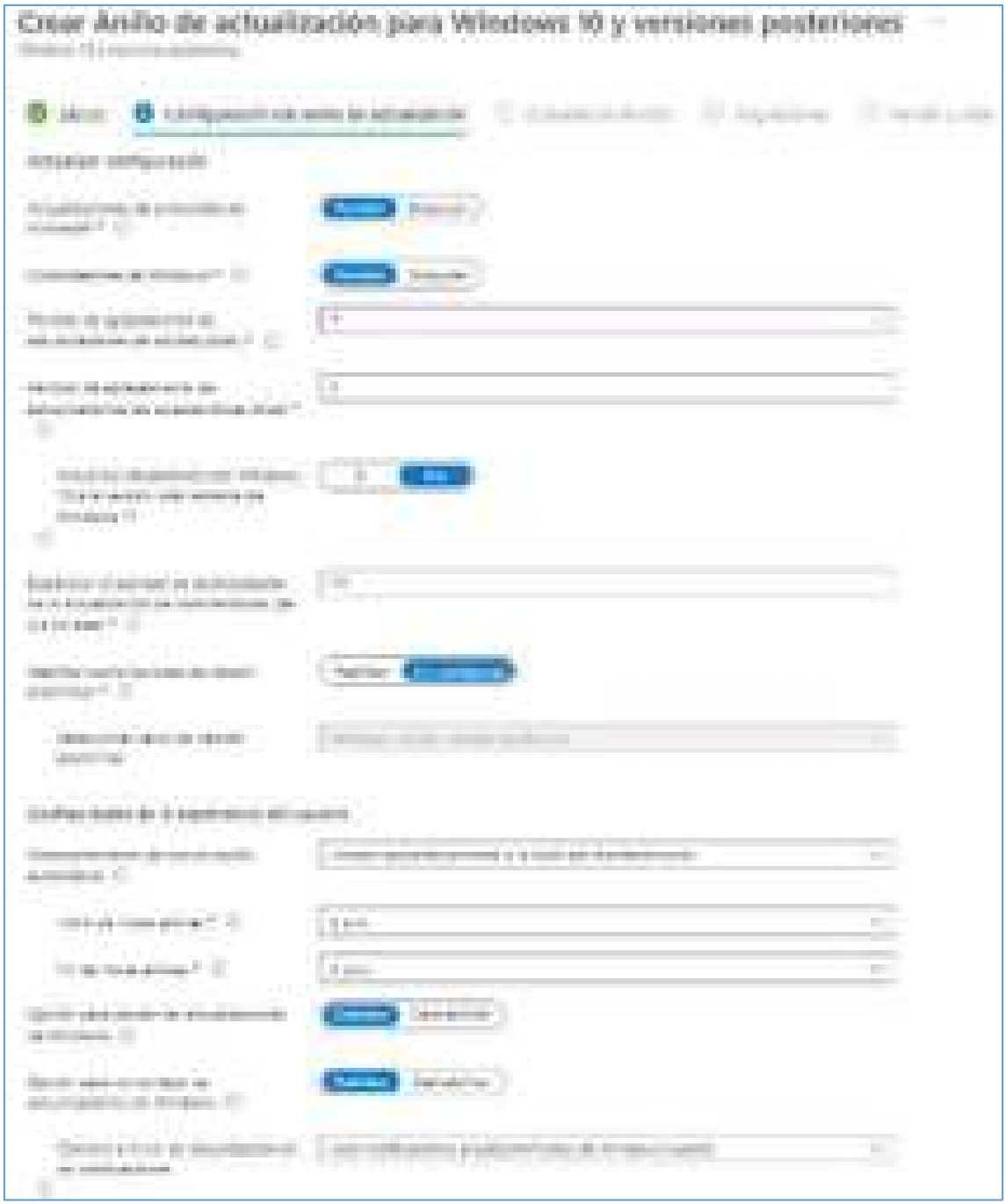
3.1.2.4 MANTENIMIENTO Y ACTUALIZACIONES DE SEGURIDAD

Al utilizar Intune para administrar la instalación de actualizaciones de software, se puede simplificar la administración de actualizaciones, configurar opciones de actualización y establecer un aplazamiento de instalación. También permite controlar las características de las nuevas versiones para mantener la estabilidad de los dispositivos y garantizar la calidad y seguridad de las actualizaciones.

WINDOWS

Los anillos de actualización de Windows son una estrategia para implementar actualizaciones en diferentes grupos de dispositivos en un período de tiempo escalonado, lo que ayuda a reducir el riesgo de problemas derivados de las actualizaciones de características. Se crean perfiles de anillos de actualización, donde cada anillo representa un grupo de dispositivos con diferentes plazos para recibir las actualizaciones. Por ejemplo, un anillo puede recibir las últimas actualizaciones primero, mientras que otro puede retrasarlas hasta que se compruebe la estabilidad de las actualizaciones en el primer anillo.

1. Iniciar sesión en el portal de Microsoft Intune y seleccionar **Dispositivos > Windows > Anillos de actualización para Windows 10 y versiones posteriores > Crear perfil**.



Los anillos de actualización de Windows son compatibles con las etiquetas de ámbito (detalle en el punto[3.1.1.2 Requisitos de acceso] de este documento). Por tanto, es posible configurarlo de forma que únicamente los administradores de determinados grupos puedan realizar esta gestión.

También se pueden implementar actualizaciones de características para nuestros dispositivos gestionados por Intune. Por ejemplo, si existe un grupo de dispositivo en la versión 1809 y se quiere actualizar a la versión 20H2, se puede lanzar la actualización desde aquí para un grupo en concreto.

Otro método disponible en Intune para gestionar las actualizaciones es Windows Autopatch. Windows Autopatch simplifica la gestión de actualizaciones para Windows, Microsoft 365, Microsoft Edge y Teams al minimizar la necesidad de intervención de los recursos de TI en la planificación y ejecución de estas actualizaciones. Utiliza secuencias de lanzamiento cuidadosamente diseñadas, informando durante el proceso y permitiendo que los administradores de TI se enfoquen en otras tareas importantes.

Nota: Para más información sobre Windows Autopatch consultar la documentación oficial de Microsoft: Guía de implementación de Windows Autopatch - Windows Deployment | Microsoft Learn.

iOS/macOS

Con Microsoft Intune, se pueden usar perfiles de configuración para gestionar las actualizaciones de software en dispositivos iOS/iPad que estén inscritos como dispositivos supervisados.

1. Iniciar sesión en el portal de Microsoft Intune y seleccionar **Dispositivos > iOS/iPadOS > Directivas de actualización para iOS/iPadOS > Crear perfil**.

2. Elegir una versión para instalar, con las siguientes opciones:
    - **Actualización más reciente**: Implementa la última actualización publicada para iOS/iPadOS.
    - **Cualquier versión anterior disponible**: Si se elige una versión anterior, también se debe configurar una directiva de configuración de dispositivo para retrasar la visibilidad de las actualizaciones de software.

    Seleccionar el tipo de programación:

    - **Actualizar en la próxima sincronización:** La actualización se instala en el dispositivo la próxima vez que se sincronice con Intune. Esta opción no requiere configuraciones adicionales y es la más sencilla.
    - **Actualizar durante el tiempo programado**: Configura una o varias ventanas de tiempo durante las cuales la actualización se instalará al realizar el registro.
    - **Actualizar fuera del tiempo programado**: Configura una o varias ventanas de tiempo durante las cuales las actualizaciones no se instalarán al realizar el registro.

    Establecer también los períodos de tiempo para limitar la instalación de actualizaciones. El impacto de estas opciones varía según el tipo de

programación elegido. Al definir un día de inicio y un día de finalización, se pueden aplicar bloqueos durante la noche.

De forma muy similar se configurarían las actualizaciones en dispositivos macOS.

1. Iniciar sesión en el portal de Microsoft Intune y seleccionar **Dispositivos > macOS > Directivas de actualización para macOS > Crear perfil**.

2. Para las actualizaciones críticas, de firmware, archivos de configuración y otras actualizaciones, se pueden establecer las siguientes acciones de instalación:
    - **Descargar e instalar**: Descarga o instala la actualización, según el estado actual del dispositivo.
    - **Descargar solo**: Descarga la actualización de software sin instalarla.
    - **Instalar inmediatamente:** Descarga la actualización y desencadena la notificación de cuenta regresiva para reiniciar el dispositivo. Recomendado para dispositivos sin usuario.

- **Notificar solo**: Descarga la actualización y notifica al usuario a través de Configuración del sistema.
- **Instalar más tarde**: Descarga la actualización y la instala en un momento posterior. Esta opción no está disponible para las actualizaciones principales del sistema operativo.

Además, al configurar "Instalar más tarde" para las "Todas las demás actualizaciones", también están disponibles las siguientes opciones:

- **Aplazamientos máximos de usuarios**: Permite especificar el número máximo de veces que un usuario puede posponer una actualización secundaria del sistema operativo antes de instalarla. El sistema solicita al usuario una vez al día.
- **Prioridad**: Especifique valores bajos o altos para la prioridad de programación para descargar y preparar actualizaciones secundarias del sistema operativo.
- **No configurado**: No se ha realizado ninguna acción en la actualización de software.

Y configurar la programación de la política de la misma forma que para los dispositivos macOS.

Por otro lado, para la actualización de las aplicaciones de la organización, es recomendable utilizar Intune para implementar las aplicaciones, ya que la mayoría se actualizan automáticamente cuando hay una nueva versión disponible. Esto asegura que las aplicaciones estén siempre actualizadas con correcciones de errores, mejoras de características y actualizaciones de seguridad.

Además, Windows Autopatch puede utilizarse para aplicar automáticamente parches de Aplicaciones Microsoft 365 para empresas, Microsoft Edge y Microsoft Teams.

Si los usuarios instalan sus propias aplicaciones, estas deben actualizarse manualmente, incluso si provienen de una tienda de aplicaciones pública. En este caso, las directivas de protección de aplicaciones pueden ser útiles para garantizar que se aplique una versión mínima de la aplicación y para borrar los datos de la organización en dispositivos que no cumplan con los estándares de seguridad establecidos.

3.1.2.5 PROTECCIÓN FRENTE A CÓDIGO DAÑINO

La función de protección contra alteraciones de Microsoft Intune (**Tamper protection**) está diseñada para salvaguardar determinadas configuraciones de seguridad, como la protección antivirus, de ser deshabilitadas o modificadas sin autorización. Con Intune, tiene la capacidad de:

- Activar o desactivar la protección contra alteraciones en algunos o todos los dispositivos.

- Proteger las exclusiones del antivirus de Microsoft Defender contra cambios no autorizados.

Si se tiene una política de cumplimiento de dispositivos en Intune que etiqueta los dispositivos con riesgo medio o alto como no conformes, cualquier dispositivo en riesgo será etiquetado de esa manera. Esta etiqueta desencadenará la aplicación de la política de acceso condicional, lo que resultará en el bloqueo del acceso a los recursos corporativos desde ese dispositivo.

Para dispositivos Android, Intune también ofrece la capacidad de ajustar la configuración de Microsoft Defender para puntos de conexión a través de políticas específicas.

Configuración de Defender para endpoint Web Protection en dispositivos Android en Intune: Azure | Microsoft Learn

Integración de Microsoft Defender para punto de conexión con Intune

Además, para una protección adicional, se puede vincular Microsoft Intune con Microsoft Defender para puntos de conexión para establecerlo como una solución de defensa móvil contra amenazas. Esta integración es una medida efectiva para prevenir violaciones de seguridad y reducir su impacto en la organización.

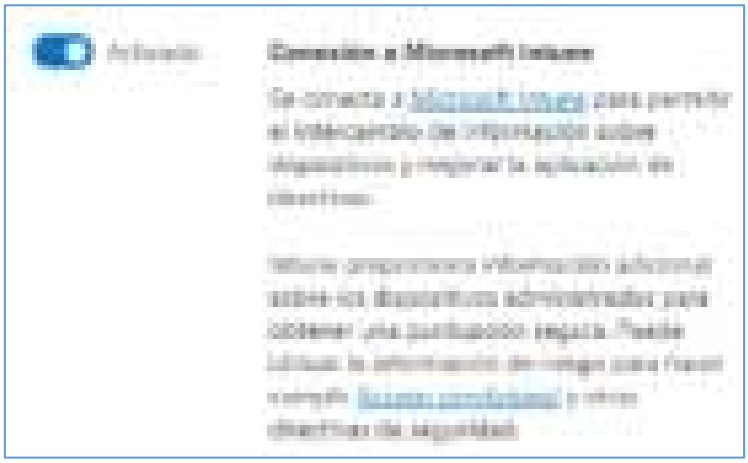
La configuración implica los siguientes pasos generales:

- **Establecer una conexión de servicio a servicio entre Intune y Microsoft Defender para punto de conexión**. Esto permite que Microsoft Defender recopile datos de riesgo de los dispositivos administrados por Intune.
- **Usar directivas de Intune para vincular dispositivos con Microsoft Defender**. Esta acción configura la comunicación entre los dispositivos y Microsoft Defender, proporcionando datos para evaluar el riesgo.
- **Utilizar directivas de cumplimiento de dispositivos para establecer el nivel de riesgo permitido.** Microsoft Defender notifica el nivel de riesgo de los dispositivos, identificando aquellos que superan el límite como no conformes.
- **Implementar una directiva de acceso condicional** para bloquear el acceso a recursos corporativos desde dispositivos no conformes.
- **Emplear directivas de protección de aplicaciones** para Android e iOS/iPadOS para definir los niveles de riesgo del dispositivo. Estas directivas funcionan tanto en dispositivos inscritos como no inscritos.

Para habilitar Microsoft Defender para puntos de conexión:

1. Iniciar sesión en el portal de Microsoft Intune y seleccionar **Seguridad de puntos de conexión > Microsoft Defender para punto de conexión > Abrir la consola de administración de Microsoft Defender for Endpoint**.

2. En el portal de Microsoft Defender, seleccionar **Configuración > Puntos de conexión > Características avanzadas** y activar **conexión Microsoft Intune**.



3. Volver al portal de Intune a la parte de Microsoft Defender para punto de conexión:

    a. Para utilizar Defender para punto de conexión con **directivas de cumplimiento,** seguir estos pasos en la Evaluación de directivas de cumplimiento para las plataformas compatibles:

        - Establecer **Conectar dispositivos Android** a Microsoft Defender para punto de conexión en **Activado**.
        - Establecer **Conectar dispositivos iOS/iPadOS** en Microsoft Defender para punto de conexión en **Activado**.
        - Establecer **Conectar dispositivos Windows** a Microsoft Defender para punto de conexión en **Activado**.

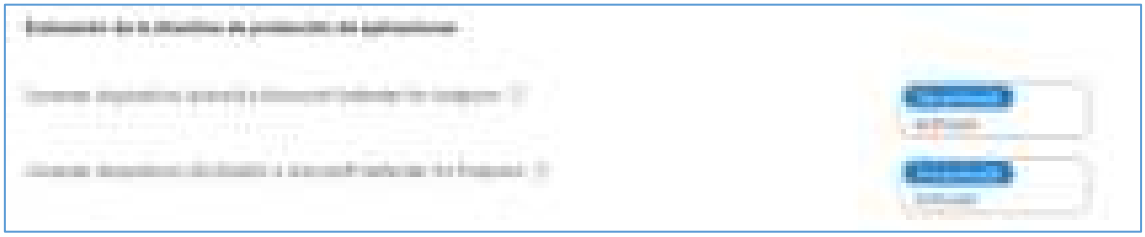
        Para dispositivos iOS, Defender para punto de conexión ofrece configuraciones adicionales que facilitan la evaluación de

vulnerabilidades de las aplicaciones en Microsoft Defender para punto de conexión para iOS:

- **Habilitar sincronización de aplicaciones para dispositivos iOS:** Activar esta opción para permitir que Defender para punto de conexión solicite metadatos de las aplicaciones iOS de Intune. Es necesario que el dispositivo iOS esté inscrito en MDM y proporcione datos actualizados de la aplicación durante la protección del dispositivo.
- **Enviar datos de inventario de aplicaciones completos en dispositivos iOS/iPadOS de propiedad personal**: Esta configuración controla los datos de inventario de aplicaciones que Intune comparte con Defender para punto de conexión. Se refiere a cuando Defender for Endpoint sincroniza los datos de la aplicación y solicita la lista de inventario de aplicaciones.

b. Para usar Defender para punto de conexión con **directivas de protección de aplicaciones** para Android e iOS/iPadOS, configurar lo siguiente en la evaluación de directivas de protección de aplicaciones para las plataformas que se utilicen:

- Establecer **Conectar dispositivos Android a Microsoft Defender** para punto de conexión en **Activado**.
- Establecer **Conectar dispositivos iOS/iPadOS para Microsoft Defender** para punto de conexión en **Activado**.



Para cumplir con los requisitos exigidos dentro del ámbito del ENS, consultar la guía [CCN-STIC-885E- Guía de configuración segura para Microsoft Defender for Endpoint].

3.1.2.6 GESTIÓN DE INCIDENTES

En Microsoft Intune se puede llevar un registro de las actividades que generan un cambio. Las acciones de creación, actualización (edición), eliminación, asignación y remotas crean eventos de auditoría que los administradores pueden revisar para la mayoría de las cargas de trabajo de Microsoft Intune.

La auditoría está habilitada de forma predeterminada para todos los clientes. No se puede deshabilitar.

Para poder ver estos registros de auditoria los usuarios deben tener el rol de:

- Administrador global
- Administrador del servicio de Intune
- Administradores asignados a un rol de Intune con los permisos de Lectura de Datos de auditoría

Se pueden revisar los registros de auditoría de las cargas de trabajo de Microsoft Intune de la siguiente manera:

1. Iniciar sesión en la consola de Intune con una cuenta que tenga los permisos necesarios para poder ver los informes. Seleccionar **Administración de inquilinos > Registros de auditoría.**

2. Para una búsqueda más exhaustiva, se pueden aplicar filtros que ayuden a encontrar algo en concreto. A continuación, se exponen diferentes opciones para aplicar en los filtros:
   - **Categoría**: como, por ejemplo, Cumplimiento, Dispositivo y Rol.
   - **Actividad**: las opciones que se muestran aquí están restringidas por la opción elegida en Categoría.

- **Intervalo de fechas**: se pueden elegir registros para el mes, semana o día anteriores.

3. Una vez aplicados los filtros, seleccionar **aplicar** y seleccionar un elemento de la lista para ver los detalles de la actividad.

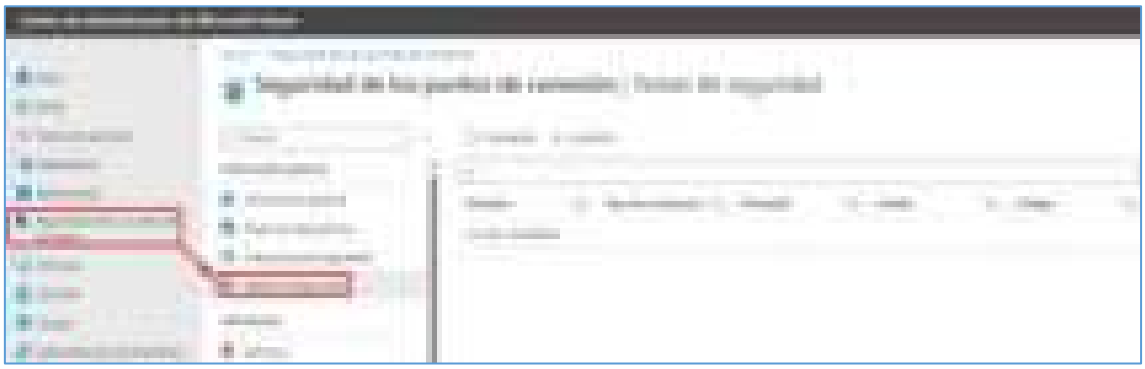
Otro de los puntos dentro de seguridad de puntos de conexión que nos puede ayudar a la gestión de incidentes es el de Tareas de seguridad. Este punto va de la mano con Microsoft Defender for Endpoint, ya que al integrar Microsoft Intune con Microsoft Defender for Endpoint, se pueden aprovechar las ventajas de administración de amenazas y vulnerabilidades de Defender for Endpoint y usar Microsoft Intune para corregir las debilidades de los puntos de conexión que se han identificado con la funcionalidad de administración de vulnerabilidades de Defender.

Después de conectar Microsoft Intune a Microsoft Defender for Endpoint, este recibe detalles de amenazas y vulnerabilidades de los dispositivos administrados.

En la consola del Centro de seguridad de Microsoft Defender, los administradores de seguridad de Defender para punto de conexión revisan los datos sobre las

vulnerabilidades del punto de conexión. Es allí donde se crean estas Tareas de seguridad, que pasarán de inmediato a la consola de Microsoft Intune.

Estas tareas identifican el tipo de vulnerabilidad, la prioridad, el estado y los pasos que hay que tomar para corregirla. El administrador de Microsoft Intune elige aceptar o rechazar la tarea.



Por lo tanto, es requisito que se tenga una suscripción para Microsoft Defender for Endpoint.

Para más información sobre Microsoft Defender for Endpoint, referencia a la guía [CCN-STIC-885E- Guía de configuración segura para Microsoft Defender for Endpoint]

3.1.3 MONITORIZACIÓN DEL SISTEMA

3.1.3.1 DETECCIÓN DE INTRUSIÓN

En Microsoft Intune la monitorización se realiza a través de informes que permiten supervisar el estado y la actividad de los activos de toda la organización, además de proporcionar otros datos de informes.

La consola tiene organizado los informes por áreas:

- **Operativo**: proporciona datos que ayudan a centrar la atención y tomar medidas.
- **Organizativo**: proporciona un remen más amplio comparándolo con una vista general. Los administradores encontrarán estos informes particularmente útiles.
- **Histórico**: proporciona patrones y tendencias a lo largo de un período de tiempo.
- **Especialista**: le permite usar datos sin procesar para crear sus propios informes personalizados.

Para que un usuario pueda ver estos informes necesitara uno de los siguientes roles:

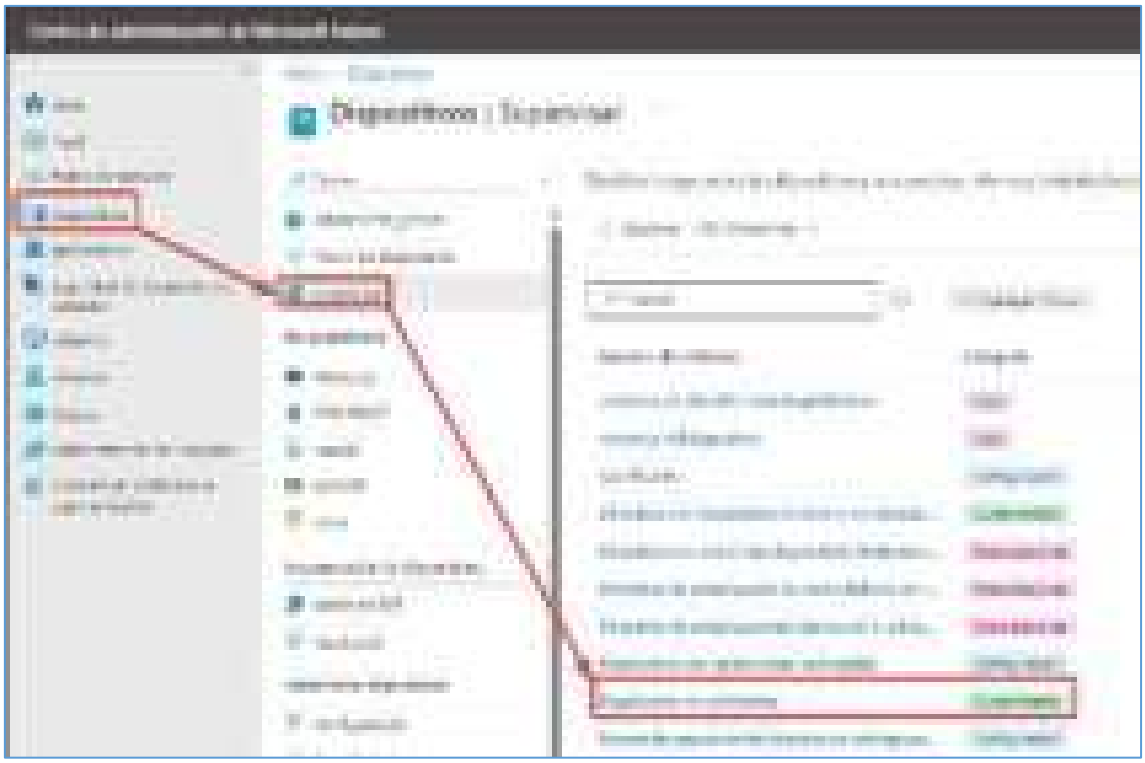
- Administrador global
- Administrador del servicio de Intune
- Administradores asignados a un rol de Intune con los permisos de **Lectura**

Informes operativos dentro de Microsoft Intune

- Informe de dispositivos no conformes

  Para llegar a este informe:

  1. Iniciar sesión en la consola de Microsoft Intune.
  2. Seleccionar **Dispositivos > Monitor > Dispositivos no conformes.**

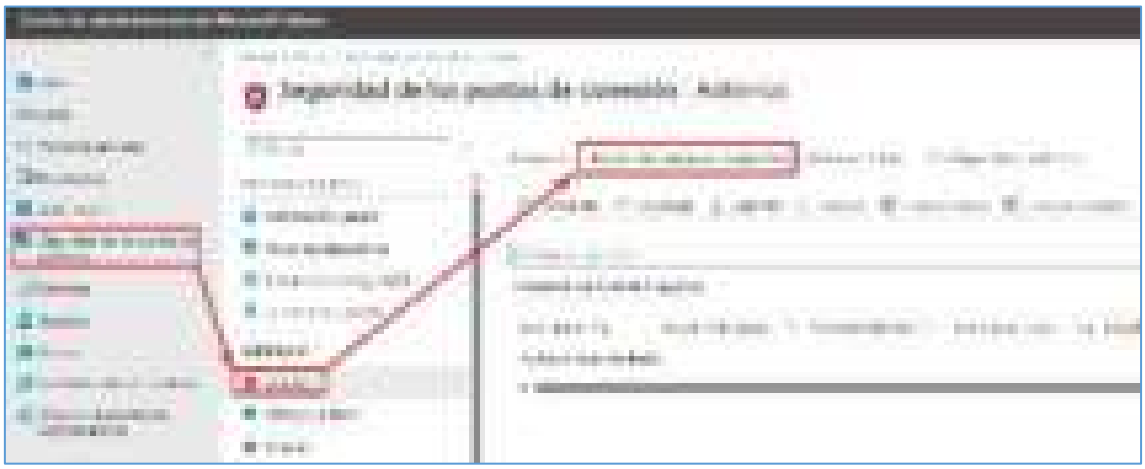


Este informe proporciona los datos que suele usar el administrador para identificar problemas de cumplimiento en los dispositivos y proporciona una ayuda para poder resolverlos.

- Informe Puntos de conexión incorrectos

  Para llegar a estos informes:

  1. Iniciar sesión en la consola de Microsoft Intune.
  2. Seleccionar **Seguridad de los puntos de conexión > Antivirus > Puntos de conexión incorrectos.**



Estos informes brindan datos para identificar problemas y su gravedad con todo lo relacionado a Antivirus y Malware en los dispositivos de la organización.

- Informe Estado de instalación de la aplicación

Para llegar a este informe:

1. Iniciar sesión en la consola de Microsoft Intune.
2. Seleccionar **Aplicaciones > Monitor > Estado de instalación de la aplicación.**

El informe **Estado de instalación de la aplicación** proporciona una lista de aplicaciones con versiones y detalles de instalación.

- Informe Estado de instalación del dispositivo para aplicaciones

  Para llegar a este informe:

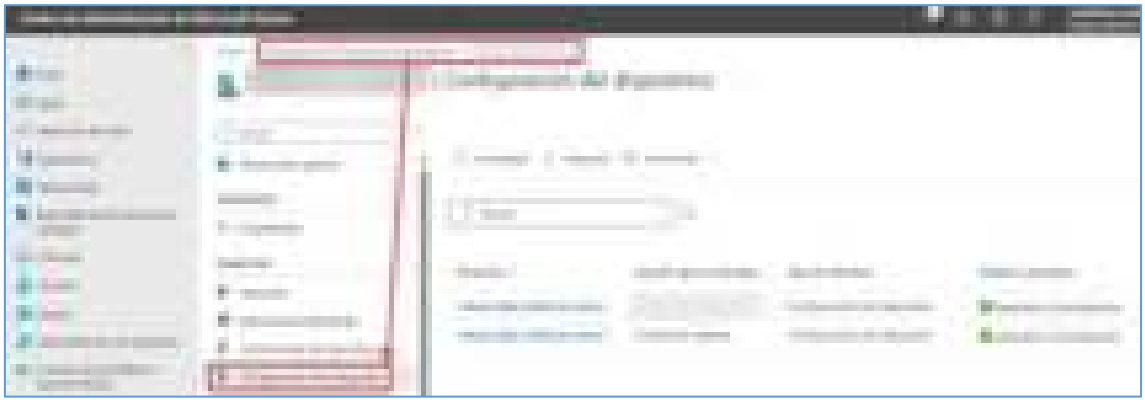
  1. Iniciar sesión en la consola de Microsoft Intune.
  2. Seleccionar **Aplicaciones > Todas las aplicaciones >** Seleccionar una aplicación > **Estado de instalación del dispositivo**.

En función la aplicación seleccionada, el informe proporciona una lista de dispositivos e información de estado.

- Informe de configuración de dispositivos

  Para llegar a este informe:

1. Iniciar sesión en la consola de Microsoft Intune.
2. Seleccionar **Dispositivos > Todos los dispositivos > seleccionar el dispositivo > Configuración del dispositivo.**



Se pueden ver todas las directivas aplicadas al dispositivo. Al seleccionar una directiva se proporcionarán detalles adicionales sobre la configuración aplicada al dispositivo y el estado del dispositivo.

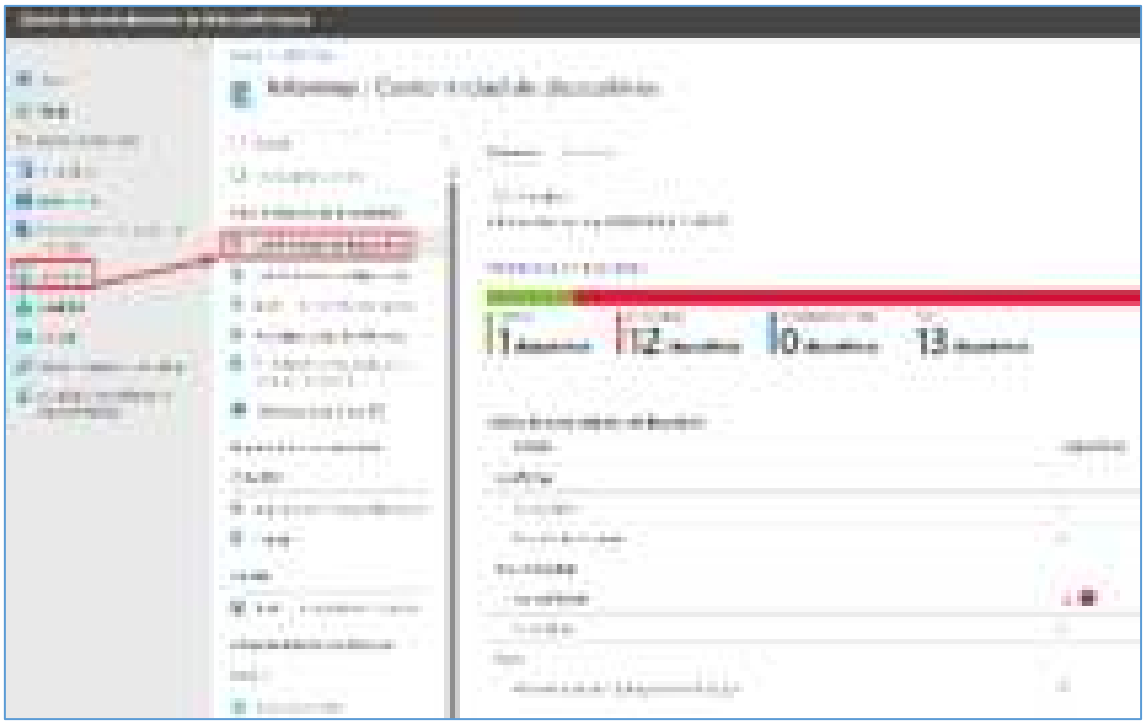
Informes organizativos dentro de Microsoft Intune

- Informe de cumplimiento de dispositivos

  Los informes de cumplimiento de dispositivos proporcionan una vista de los datos para identificar las métricas agregadas. Este informe está diseñado para trabajar con grandes conjuntos de datos a fin de obtener una imagen completa del cumplimiento de los dispositivos. Para generarlo, se le pueden aplicar filtros y seleccionar el botón "Generar informe".

  Para ver un informe generado del estado de un dispositivo:

  1. Iniciar sesión en la consola de Microsoft Intune.
  2. Seleccionar la pestaña **Informes > Conformidad de dispositivos > Informes > Cumplimiento de dispositivos**.



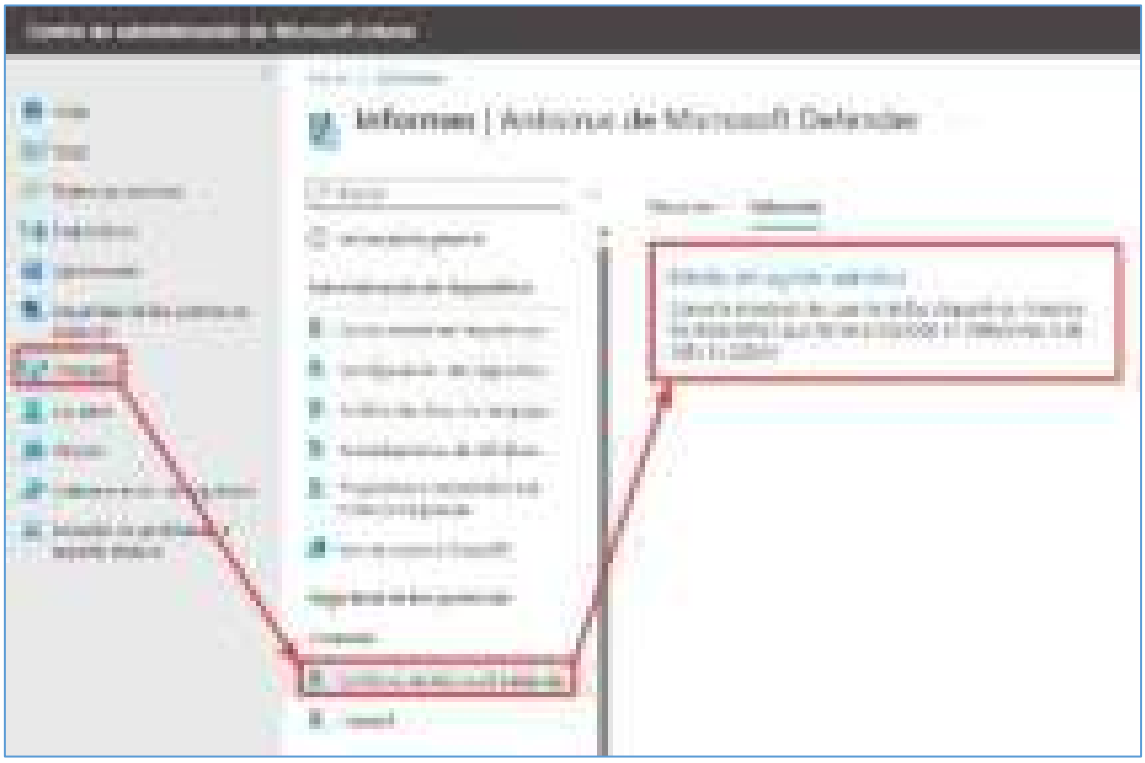
3. Seleccionar los filtros **Estado de cumplimiento, OS y Propiedad** para refinar el informe.
4. Hacer clic en **Generar informe** (o Generar de nuevo) para recuperar los datos actuales.

- Informe Estado del agente de antivirus
  El informe **Estado del agente de antivirus** proporciona el estado del agente de los dispositivos de la organización. Los datos de este informe son puntuales y muestran los detalles siguientes:
  - Si un dispositivo tiene protección en tiempo real o de red, así como el estado.
  - El estado de Windows Defender.

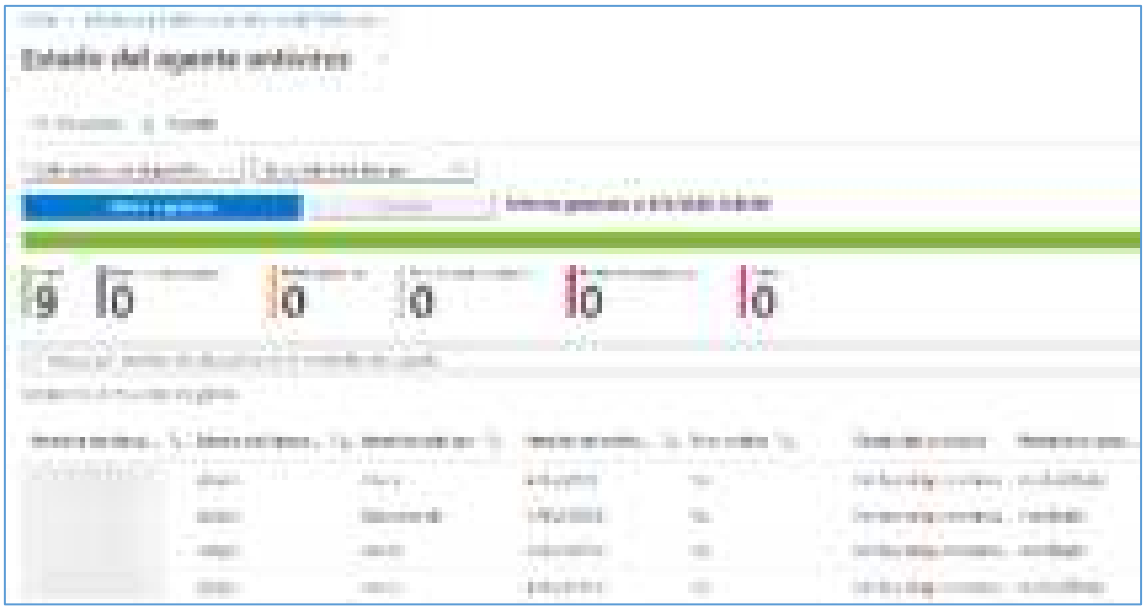
- Si está habilitada la protección contra alteraciones.
- Si el dispositivo es una máquina virtual o un dispositivo físico.
- Indica el dispositivo “Unhealthy”, el nombre de usuario y la gravedad.

Se puede ver el informe Estado del agente de antivirus:

1. Iniciar sesión en la consola de Microsoft Intune.
2. Seleccionar **Informes > Antivirus de Microsoft Defender > Informes > Estado del agente de antivirus.**



3. Hacer clic en **Generar informe** (o Generar de nuevo) para recuperar los datos actuales.



- Informe de malware detectado

  El informe **Malware detectado** proporciona el estado de malware de los dispositivos de la organización, muestra el número de dispositivos con malware detectado, así como detalles de malware.

  Se puede ver el informe Malware detectado mediante los pasos siguientes:

  1. Iniciar sesión en la consola de Microsoft Intune.
  2. Seleccionar **Informes > Antivirus de Microsoft Defender > Informes > Malware detectado**.

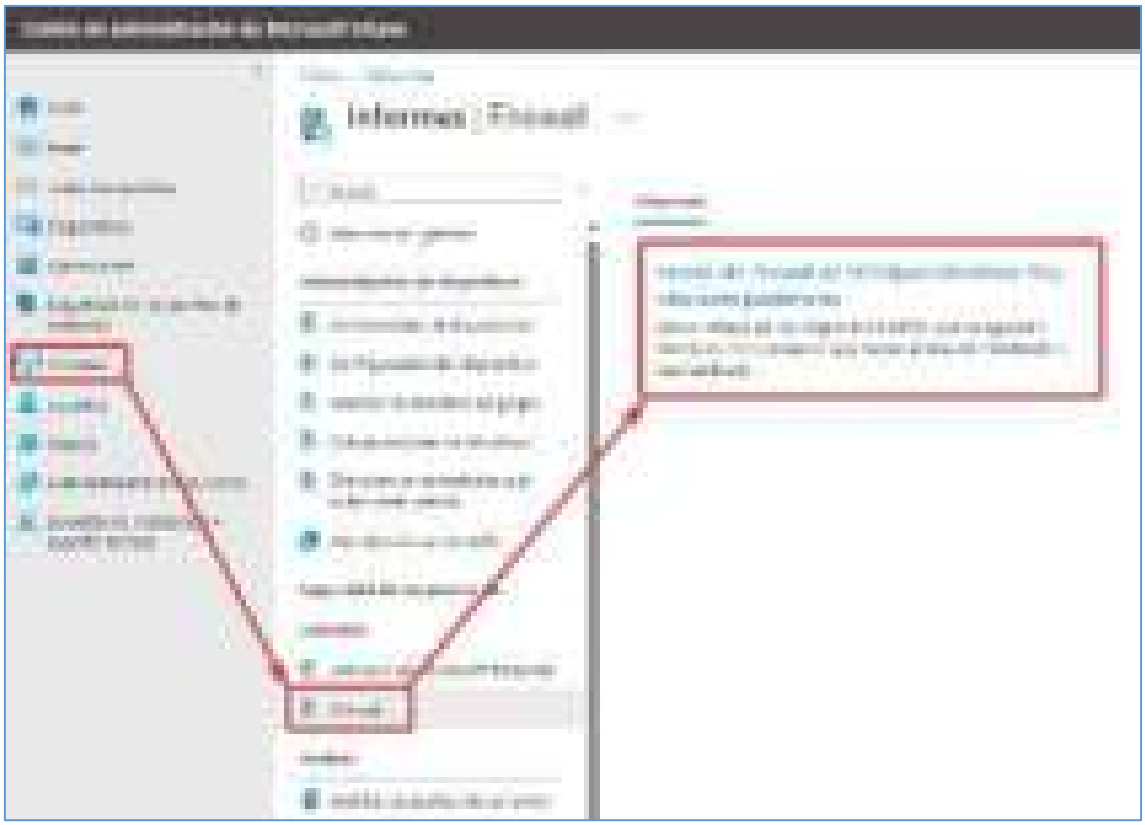
3. Hacer clic en **Generar informe** (o Generar de nuevo) para recuperar los datos actuales.

- Estado del firewall de los dispositivos MDM

  El informe Estado del firewall de los dispositivos MDM para Windows 10 y versiones posteriores proporciona una vista de alto nivel del estado de firewall de los dispositivos administrados.

  Para ver este informe:

  1. Iniciar sesión en la consola de Microsoft Intune.
  2. Seleccionar **Informes > Firewall > Informes > Estado de firewall de MDM** para Windows 10 y versiones posteriores.



3. Hacer clic en **Generar informe** (o **Generar de nuevo**) para recuperar los datos actuales.

Informes históricos dentro de Microsoft Intune

- Informe de tendencias de cumplimiento de dispositivos

  Los informes de tendencias de cumplimiento de dispositivos se utilizan para identificar las tendencias a largo plazo en el cumplimiento de los dispositivos. Los datos se muestran durante un período de tiempo y resultan útiles para tomar

decisiones, mejorar los procesos o promover la investigación de posibles anomalías.

Para ver el informe de **Tendencias de cumplimiento de dispositivos**, seguir estos pasos:

1. Iniciar sesión en la consola de Microsoft Intune.
2. Seleccionar la pestaña **Informes > Conformidad de dispositivos > Informes > Tendencias de cumplimiento de dispositivos.**

3.2 MEDIDAS DE PROTECCIÓN

Las siguientes medidas de protección ayudaran a la organización a mantener un mantenimiento correcto de la plataforma, monitoreando y protegiendo en todo momento los activos de la empresa.

3.2.1 PROTECCIÓN DE LOS EQUIPOS

Para más detalle de todas estas configuraciones, en esta guía se hace hincapié en el punto de protección de los dispositivos, que se puede consultar en [2.2 Protección de dispositivos]

3.2.1.1 BLOQUEO DE PUESTO DE TRABAJO

Con el perfil de restricciones de dispositivo es posible configurar el "Máximo de minutos de inactividad hasta que se bloquea la pantalla", de forma que, por ejemplo, se establezca 5 para bloquear los dispositivos después de 5 minutos de inactividad. Para ello:

1. Iniciar sesión en la consola de Microsoft Intune, seleccionar **Dispositivos > Configuración > Directivas > Crear > Nueva directiva.**
2. Escoger la plataforma **Windows 10 y versiones posteriores**, el tipo de perfil **Plantillas** y el tipo de plantilla **Restricciones de dispositivos.**

3. En la página Opciones de configuración, expandir **Contraseña**, y configurar los valores que se deseen para la organización.

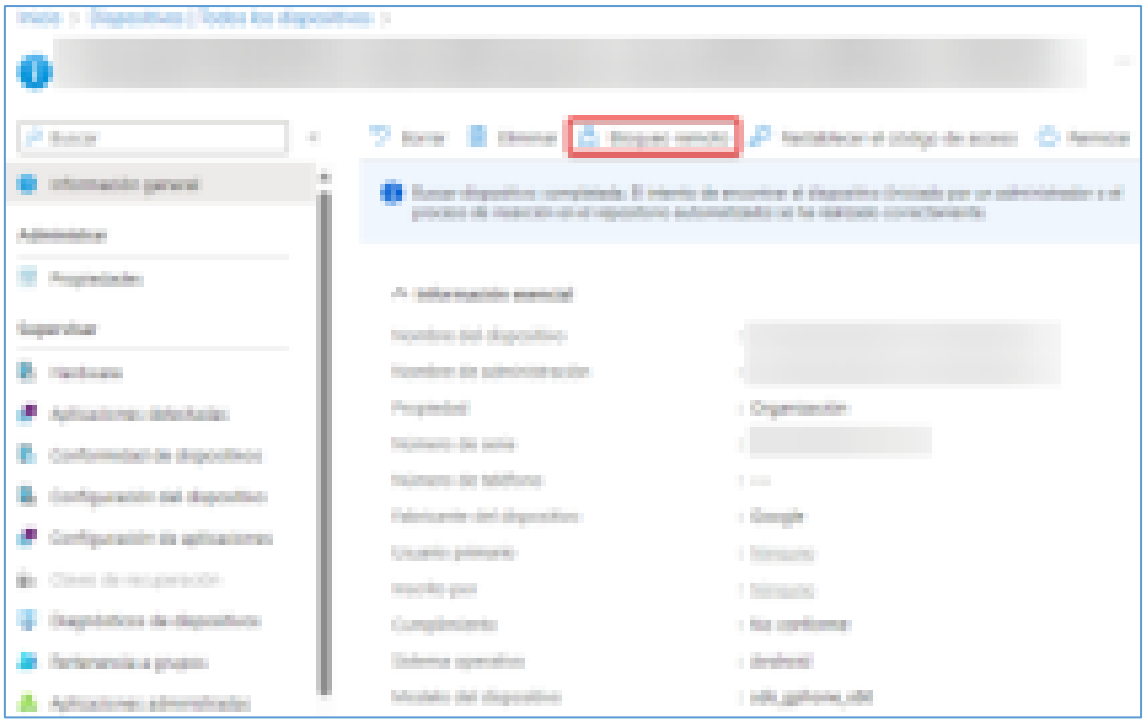
4. Seleccionar **Siguiente** y en la pestaña **Asignaciones**, pulsar **Seleccionar grupos para incluir** y, a continuación, asignar a uno o varios grupos. Usar **Seleccionar grupos para excluir** para ajustar la asignación.
5. Por último, revisar y pulsar **Crear.**

Para el resto de los dispositivos, Android, iOS y macOS, Intune dispone de la acción de dispositivo de **Bloqueo remoto**, mediante la cual se detiene el acceso al dispositivo, requiriendo que el propietario ingrese el código de acceso para desbloquearlo. Esta opción puede ser aplicada a dispositivos que tengan un PIN o contraseña configurados.

Cuando se aplica el **Bloqueo remoto** en dispositivos sin PIN o contraseña, la pantalla se desactiva, pero el dispositivo no se bloquea.

Para bloquear un dispositivo móvil de forma remota:

1. Iniciar sesión en la consola de Microsoft Intune, seleccionar **Dispositivos > Todos los dispositivos.**
2. Seleccionar un dispositivo y la opción **Bloqueo remoto**.



3.2.1.2 PROTECCIÓN DE DISPOSITIVOS PORTÁTILES

Los dispositivos móviles que pueden salir de las instalaciones de la organización y están expuestos al riesgo de pérdida o robo, con Intune se pueden proteger adecuadamente siguiendo los requisitos de la organización.

Entre las medidas que se pueden aplicar a los dispositivos cuando se conecten remotamente, están las reglas de acceso condicional basadas en la ubicación física. Las organizaciones pueden emplear esta función para realizar acciones habituales como:

1. Requerir autenticación MFA a usuarios que acceden a servicios desde fuera de la red corporativa.
2. Restringir el acceso a usuarios que intentan acceder desde países o regiones donde la organización no opera.

Además de estas acciones, mediante las CAs también se puede configurar para que se restrinja el acceso a determinadas aplicaciones/servicios a los dispositivos que accedan desde determinadas ubicaciones.

Para información adicional sobre las reglas de acceso condicional, revisar el punto [2.2.4 Políticas de acceso condicional].

Si los dispositivos de la organización se pierden o roban, desde Intune es posible buscar el dispositivo mediante las tareas remotas que se pueden lanzar remotamente y, además, también es recomendable lanzar un **Wipe** en este caso para garantizar el borrado completo de todos los datos del dispositivo y que no se accedan a los datos de la organización.

En el caso de las plataformas de dispositivos compatibles (Android, iOS/iPadOS), se puede activar remotamente una alerta de sonido para ayudar al usuario a encontrar el dispositivo perdido. El sonido continuará hasta que el usuario lo desactive en el dispositivo o hasta que se quite del modo perdido.

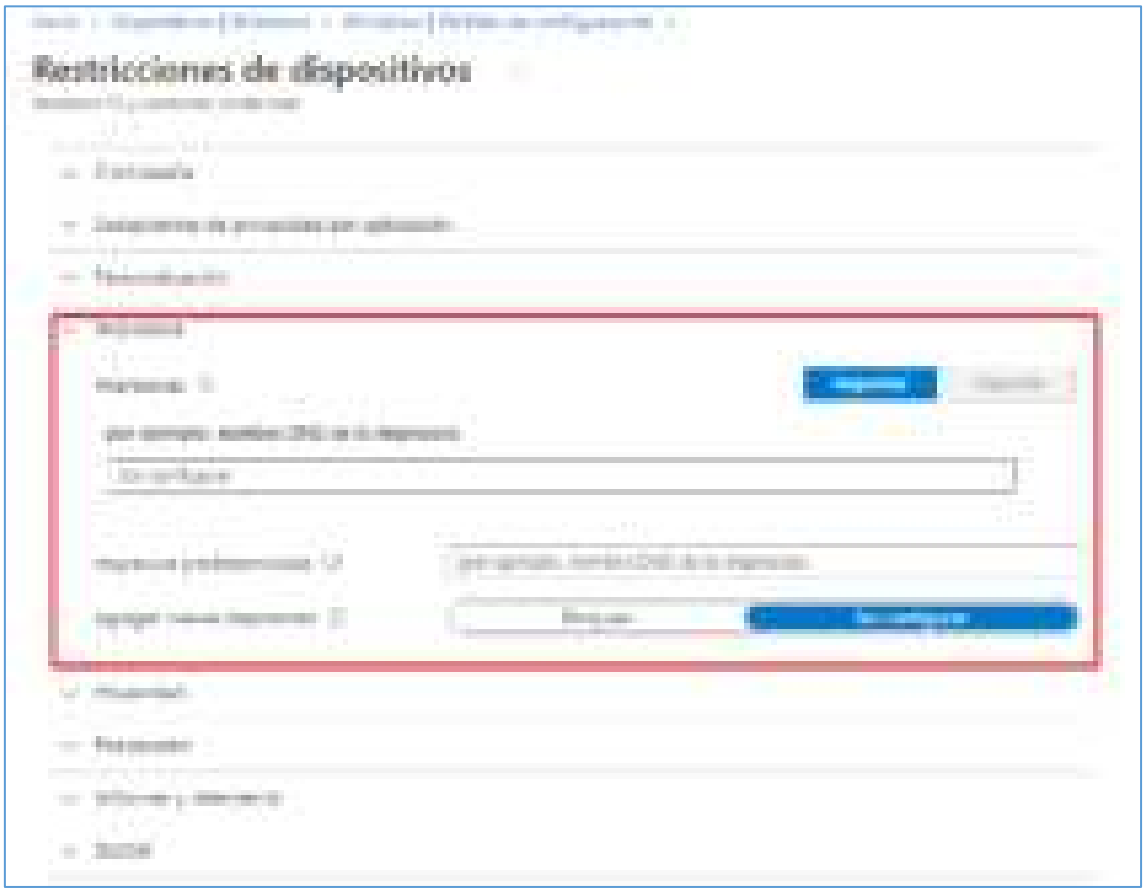
Para más información sobre la supervisión de dispositivos perdidos o robados, consultar la documentación de Microsoft:

Supervisión de dispositivos perdidos con Microsoft Intune | Microsoft Learn

3.2.1.3 OTROS DISPOSITIVOS CONECTADOS A LA RED

En cuanto a la protección de otros dispositivos conectados a la red, tales como impresoras, escáneres, proyectores, etc., estos deben estar configurados con medidas de seguridad apropiadas para controlar el flujo de entrada y salida de información según se defina en la organización.

En Microsoft Intune, existen varias secciones dentro del perfil de restricciones de dispositivo mediante las cuales se pueden realizar configuraciones de las impresoras, así como impedir que los usuarios agreguen nuevas impresoras. También se recomienda revisar las configuraciones relativas al *Acceso a redes* para cerciorarse, por ejemplo, de que se bloquean los recursos compartidos accesibles anónimamente, que se pueden configurar desde el perfil de **Catálogo de configuración**.



Por otro lado, muchas organizaciones permiten que los dispositivos de propiedad personal accedan a los recursos corporativos, como el correo electrónico y las reuniones. Las opciones disponibles varían según la rigurosidad de la organización.

Una opción es requerir que los dispositivos personales se inscriban en Intune. Esto permite a los administradores implementar directivas, establecer reglas y configurar características del dispositivo. Otra opción es utilizar directivas de protección de aplicaciones que se enfoquen en salvaguardar los datos de aplicaciones específicas, como Outlook, Teams y SharePoint. También es posible emplear una combinación de directivas de inscripción de dispositivos y protección de aplicaciones para garantizar un nivel adecuado de seguridad y control.

Además de todo lo mencionado anteriormente, se puede configurar la directiva de seguridad de punto de conexión de Firewall con el fin de bloquear o permitir únicamente el acceso desde determinadas direcciones IP/puertos.

Para cumplir con los requisitos exigidos dentro del ámbito del ENS, consultar la guía [CCN-STIC-884A - Guía de Configuracion segura para Azure].

3.2.2 PROTECCIÓN DE LOS SOPORTES DE INFORMACIÓN

En cuanto a la protección de la información, en esta guía se hace hincapié en la protección de aplicaciones, la cual se puede consultar en el siguiente enlace:

[2.4 Protección de aplicaciones].

3.2.2.1 CRIPTOGRAFÍA

Cuando se habla de cifrado en Microsoft Intune se refiere a todo lo relacionado con Bitlocker para Windows, FileVault para dispositivos macOS y el cifrado para los dispositivos Android e iOS.

Bitlocker Windows

BitLocker está disponible en dispositivos que ejecutan Windows 10 o versiones posteriores. Algunos valores de configuración de BitLocker requieren que el dispositivo tenga un TPM compatible.

El cifrado de los dispositivos Windows con BitLocker se puede realizar con los siguientes tipos de directivas:

- Directiva de cifrado de discos de seguridad de punto de conexión para BitLocker en Windows. El perfil de BitLocker en Seguridad de los puntos de conexión es un grupo prioritario de opciones dedicado a la configuración de BitLocker.

  Para la creación de este tipo de directiva:

  1. Iniciar sesión en la consola de Microsoft Intune, seleccionar **Seguridad de los puntos de conexión > Cifrado de disco > Crear perfil.** Establecer las opciones de Windows 10 y BitLocker.

2. En la página Opciones de configuración, configurar los valores de BitLocker que se deseen.
3. En la pestaña **Etiquetas de ámbito**, pulsar **Seleccionar etiquetas de ámbito** para abrir el panel **Seleccionar etiquetas** para asignar etiquetas de ámbito al perfil si se tuvieran.
4. En la pestaña **Asignaciones**, pulsar **Seleccionar grupos para incluir** y, a continuación, asignar a uno o varios grupos. Usar **Seleccionar grupos para excluir** para ajustar la asignación.

El siguiente método para utilizar BitLocker con Microsoft Intune es el siguiente:

- **Perfil de configuración de dispositivo** para BitLocker de Windows 10. La configuración de BitLocker es una de las categorías de configuración disponibles para la protección de dispositivos Windows 10.

  Para la creación de este tipo de perfil:

  1. Iniciar sesión en la consola de Microsoft Intune, seleccionar **Dispositivos > Configuración > Directivas > Crear > Nueva directiva.**
  2. Escoger la plataforma **Windows 10 y versiones posteriores**, el tipo de perfil **Plantillas** y el tipo de plantilla **Endpoint Protection.**

3. En la página Opciones de configuración, expandir **Cifrado de Windows**, y configurar los valores que se deseen para la organización.

4. Seleccionar **Siguiente** y en la pestaña **Asignaciones**, pulsar **Seleccionar grupos para incluir** y, a continuación, asignar a uno o varios grupos. Usar **Seleccionar grupos para excluir** para ajustar la asignación.
5. Por último, revisar y pulsar **Crear.**

FileVault MAC

Microsoft Intune es compatible con el cifrado de discos FileVault de macOS. FileVault es un programa de cifrado de disco completo que se incluye con macOS. Se puede usar Microsoft Intune para configurar FileVault en dispositivos que ejecuten macOS 10.13 o versiones posteriores.

El cifrado de los dispositivos Mac con File Vault se puede realizar con los siguientes tipos de directivas dentro de Microsoft Intune:

- **Directiva de seguridad de puntos de conexión para FileVault de macOS**: El perfil de FileVault de Seguridad de los puntos de conexión es un grupo prioritario de opciones dedicado a la configuración de FileVault.

Para la creación de este tipo de directiva:

1. Iniciar sesión en la consola de Microsoft Intune, seleccionar **Seguridad de los puntos de conexión > Cifrado de disco > Crear directiva.**
2. Establecer las opciones de Mac y File Vault.

3. En la página Opciones de configuración, establezca **Habilitar FileVault** en **Sí**.
4. En **Tipo de clave de recuperación** solo se admite **Clave de recuperación personal**.
5. Configurar las demás opciones como se deseen.
6. Cuando haya finalizado la configuración, seleccionar **Siguiente**.
7. En la pestaña Etiquetas de ámbito, pulsar **Seleccionar etiquetas de ámbito** para abrir el panel **Seleccionar etiquetas** para asignar etiquetas de ámbito al perfil si se tuvieran.
8. En la pestaña **Asignaciones**, pulsar **Seleccionar grupos para incluir** y, a continuación, asignar a uno o varios grupos. Usar **Seleccionar grupos para excluir** para ajustar la asignación.
9. Por último, revisar y pulsar **Crear.**

El método para utilizar el cifrado en dispositivos Mac con Microsoft Intune es el siguiente:

- Perfil de configuración de dispositivos para la protección de puntos de conexión para FileVault de macOS: La configuración de FileVault es una de las categorías de configuración disponibles para la protección de punto de conexión de macOS.

Para la creación de este tipo de perfil:

1. Iniciar sesión en la consola de Microsoft Intune, seleccionar **Dispositivos > Configuración > Directivas > Nueva directiva.**
2. Escoja la plataforma **MacOS**, el tipo de perfil Plantillas y el tipo de plantilla **Endpoint Protection.**

3. En la página Opciones de configuración, seleccionar **FileVault** para expandir las opciones disponibles:

4. Configurar la opción **Habilitar FileVault** en **Sí,** y configurar el resto de los valores de FileVault que se deseen, luego, seleccionar **Siguiente**.
5. En la pestaña **Asignaciones**, pulsar **Seleccionar grupos para incluir** y, a continuación, asignar a uno o varios grupos. Usar **Seleccionar grupos para excluir** para ajustar la asignación.
6. Por último, revisar y pulsar **Crear.**

Cifrado de dispositivos Android

Es importante que los dispositivos Android estén cifrados ya que de esta manera quedan protegidos sus archivos y carpetas del acceso no autorizado frente a perdidas o robos del dispositivo.

Desde Microsoft Intune, se puede exigir al usuario que el dispositivo este cifrado a través de una directiva de cumplimiento:

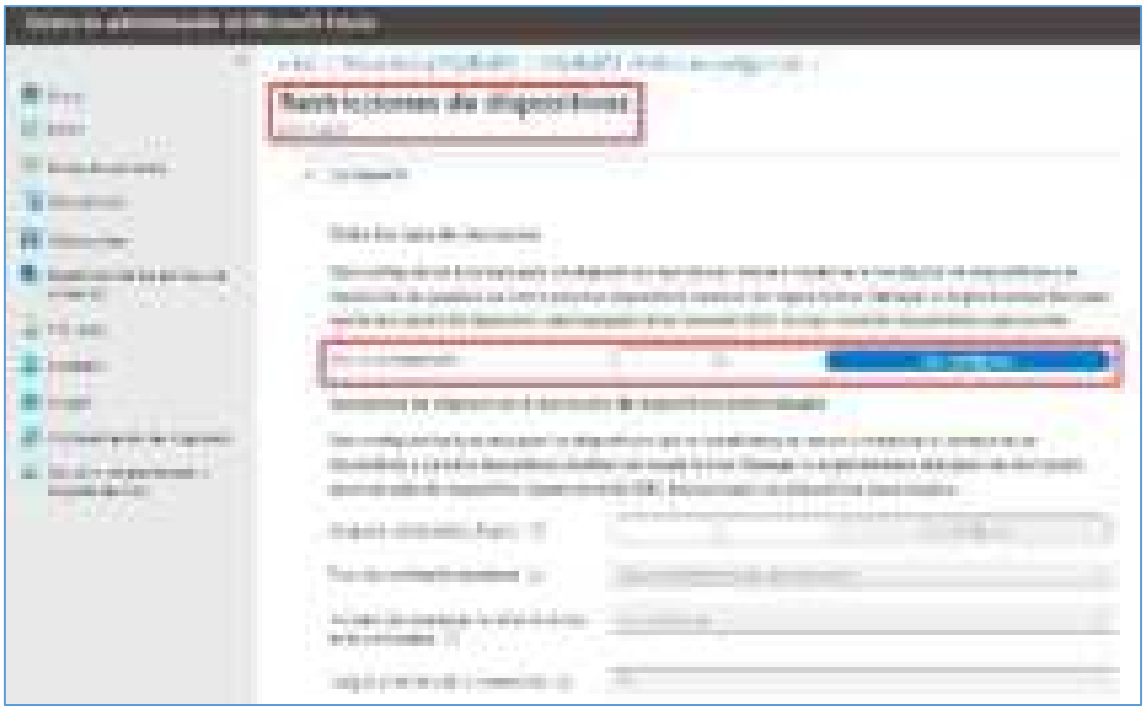
En caso de no estar cifrado el dispositivo, si tiene esta directiva de cumplimiento asignada, obligará al usuario a cifrar su dispositivo.

En caso de que el usuario quiera cifrar manualmente el dispositivo, buscar **cifrar** o **seguridad** en el dispositivo y pulsar sobre **cifrar el dispositivo** y seguir las instrucciones. Este método puede variar según el modelo de dispositivo.

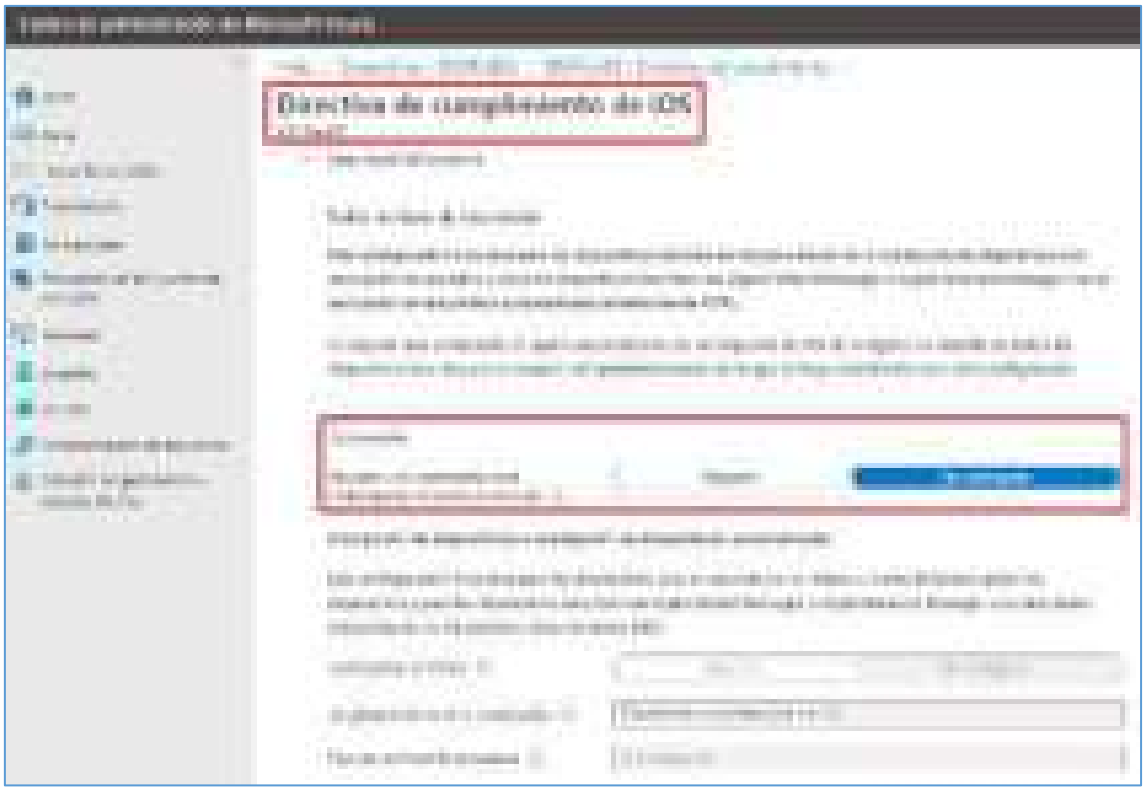
Cifrado en dispositivos iOS/iPadOS

Para cifrar obligatoriamente un dispositivo iOS o iPad, simplemente habría que aplicar una directiva de cumplimiento o configuración al dispositivo iOS o iPad. Esto hará que se le pida al usuario que establezca un código de acceso cada 15 minutos hasta que lo complete. Cuando se ha completado el proceso de establecer el código por parte del usuario, automáticamente se inicia el proceso de cifrado del dispositivo. El dispositivo quedará cifrado hasta que se deshabilite el código de acceso.

Este código de acceso se puede configurar a través de un perfil de configuración de dispositivos iOS/iPadOS de tipo restricciones de dispositivo.



Y se puede exigir a través de una directiva de cumplimiento de iOS/iPadOS:



3.2.2.2 BORRADO Y DESTRUCCIÓN

Todos los dispositivos que se administran tienen un ciclo de vida. Intune está diseñado para ayudar a gestionar este ciclo de principio a fin: desde la inscripción inicial, pasando por la configuración y la protección, hasta la retirada del dispositivo cuando ya no sea necesario.

Cuando surge la necesidad de retirar o borrar un dispositivo, ya sea porque se ha perdido, ha sido robado, necesita ser reemplazado, o el usuario cambia de posición en la empresa, existen varias opciones disponibles. Esto incluye procedimientos como restablecer el dispositivo a su configuración original, quitarlo del sistema de administración, o borrar específicamente los datos corporativos que almacena.

Restablecimiento del dispositivo

La opción **Borrar** dispositivo o **Wipe** restaura el dispositivo a su estado original de fábrica. Si se marca la opción **Conservar el estado de inscripción y la cuenta de usuario**, los datos del usuario se mantendrán. De lo contrario, se eliminarán todos los datos, aplicaciones y configuraciones.

- **No conservar el estado de inscripción y la cuenta de usuario**. Elimina todas las cuentas de usuario, datos, directivas de MDM y configuraciones. Restaura el sistema operativo a su configuración y estado predeterminados.
- **Conservar el estado de inscripción y la cuenta de usuario.** Conserva los datos y cuentas de usuario, pero restablece la configuración del usuario a los valores predeterminados. Además, restablece el sistema operativo a su configuración y estado predeterminados.

Esta opción no quita el dispositivo de la administración de Intune.

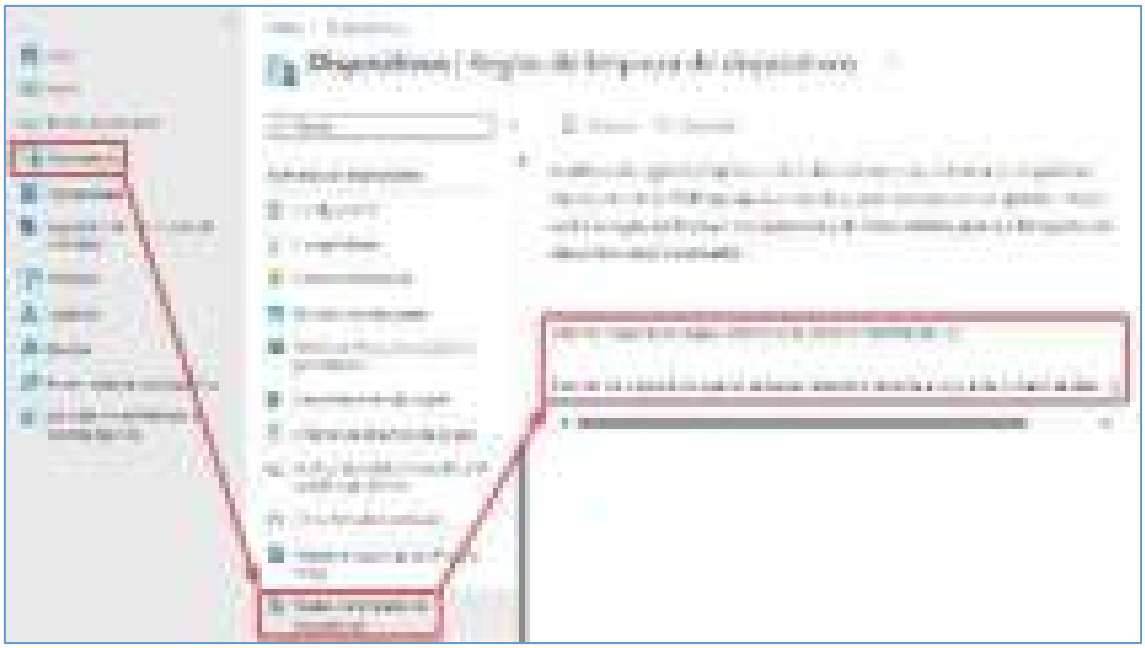
Quitar del sistema de administración

Una de las formas en Intune para eliminar los dispositivos del MDM es establecer una configuración para que automáticamente retire dispositivos que parezcan estar inactivos, obsoletos o que no respondan. Estas reglas de limpieza están diseñadas para monitorear constantemente el inventario de dispositivos, asegurando que los registros de dispositivos estén siempre actualizados. Los dispositivos eliminados de esta manera son retirados de la administración de Intune.

Cuando se activa una regla de limpieza de dispositivos, este se elimina de Intune. En consecuencia, el dispositivo debe someterse a un proceso de reinscripción para volver a aparecer en la consola.

Para su configuración, seguir los siguientes pasos:

1. Iniciar sesión en la consola de Microsoft Intune, seleccionar **Dispositivos > Reglas de limpieza de dispositivos > Sí.**
2. En **Eliminar los dispositivos que no se hayan registrado durante el siguiente número de días**, escribir un número entre 30 y 270**.**



3. Seleccionar **Guardar**.

Nota: Las reglas de limpieza de dispositivos no están disponibles para dispositivos administrados por Jamf.

Si se necesita directamente remover dispositivos del centro de administración de Intune manualmente, se puede hacer eliminándolos desde el panel de dispositivos. Intune ejecuta una acción de **Retirar** o **Borrar** dependiendo del tipo de sistema operativo o método de inscripción. Es importante tener en cuenta que no todos los tipos de inscripción admiten la acción **Retirar**.

Para ver cómo hacerlo o tener más información sobre el resto de las tareas remotas que se pueden realizar, en esta guía se hace hincapié en el punto [3.1.2.1 Inventario de activos].

Borrado de datos corporativos

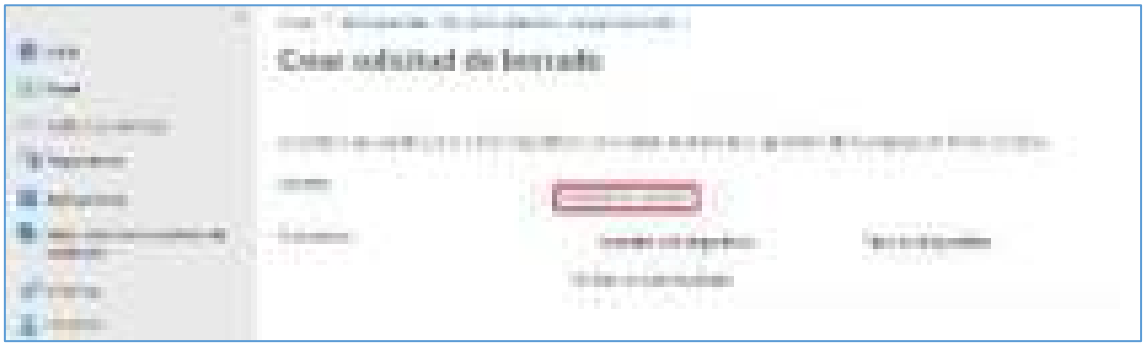
Cuando un dispositivo se extravía, es robado o un empleado deja la empresa, es importante eliminar los datos de las aplicaciones corporativas del dispositivo. Sin embargo, es posible que se quieran mantener los datos personales en el dispositivo, especialmente si es propiedad del empleado.

En Intune, gracias a las directivas de protección de aplicaciones, que se pueden ver más en detalle en el punto [2.3.2 Protección de aplicaciones], es posible eliminar selectivamente los datos de las aplicaciones corporativas. Para ello, hay dos formas de hacerlo en función de si es basada en el dispositivo o en el propio usuario:

Creación de solicitud de borrado basada en dispositivos

1. Iniciar sesión en la consola de Microsoft Intune, seleccionar **Aplicaciones > Borrado selectivo de aplicaciones > Solicitudes de borrado > Crear solicitud de borrado.**

2. Seleccionar el usuario cuyos datos de aplicación se quieren borrar y hacer clic en **Seleccionar**.



3. Hacer clic en **Seleccionar el dispositivo**, elegir el dispositivo y **Seleccionar**.
4. **Crear** para realizar la solicitud de borrado.

El servicio genera y supervisa una solicitud de borrado individual para cada aplicación protegida en el dispositivo, junto con el usuario vinculado a dicha solicitud de borrado.

Creación de solicitud de borrado basada en usuarios

1. Iniciar sesión en la consola de Microsoft Intune, seleccionar **Aplicaciones > Borrado selectivo de aplicaciones > Borrado en el nivel de usuario > Crear solicitud de borrado.**
2. Hacer clic en **Seleccionar el usuario**, elegir el usuario cuyos datos de aplicación se quieren borrar y **Seleccionar**.

   Automáticamente aparecerá el dispositivo asociado a ese usuario.
3. **Crear** para realizar la solicitud de borrado.

Una vez se completa la solicitud, la próxima vez que se ejecute la aplicación en el dispositivo, los datos corporativos serán eliminados de la misma. Además, se puede

configurar un borrado selectivo de datos corporativos como una acción adicional cuando las condiciones de las políticas de protección de aplicaciones no se cumplan. Esta función garantiza la protección y eliminación automática de datos corporativos confidenciales de las aplicaciones.

3.2.3 PROTECCIÓN DE LOS SERVICIOS

3.2.3.1 PROTECCIÓN DEL CORREO ELECTRÓNICO

Es posible utilizar certificados con Intune para autenticar a los usuarios en aplicaciones y recursos corporativos mediante VPN, Wi-Fi o perfiles de correo electrónico. Esta autenticación mediante certificados elimina la necesidad de que los usuarios tengan que introducir nombres de usuario y contraseñas, lo que mejora la experiencia de acceso. Además, los certificados se utilizan para firmar y cifrar el correo electrónico mediante S/MIME.

Los certificados de correo electrónico ofrecen una capa adicional de seguridad a las comunicaciones por correo electrónico mediante el cifrado y descifrado. Intune puede utilizar estos certificados para firmar y cifrar el correo electrónico en dispositivos móviles que ejecuten en Android, iOS/iPadOS, macOS y Windows.

Intune puede generar automáticamente certificados de cifrado S/MIME para todas las plataformas. Estos certificados se asignan automáticamente a los perfiles de correo que utilizan el cliente de correo nativo en iOS y a Outlook en dispositivos iOS y Android. Sin embargo, para plataformas como Windows y macOS, así como para otros clientes de correo en iOS y Android, Intune distribuye los certificados, pero los usuarios deben activar manualmente S/MIME en su aplicación de correo y seleccionar los certificados S/MIME.

Certificados de firma

Los certificados de firma en Intune utilizan certificados PKCS. El proceso para implementar y utilizar estos certificados en el entorno de Intune es el siguiente:

1. Instalar y configurar **Certificate Connector** para Microsoft Intune para admitir solicitudes de certificados PKCS. El conector tiene los mismos requisitos de red que los dispositivos administrados.
2. Crear un perfil de certificado raíz de confianza para los dispositivos. Este paso implica el uso de certificados raíz de confianza e intermedios para la entidad de certificación, y luego la implementación del perfil en los dispositivos.
3. Crear un perfil de certificado PKCS utilizando la plantilla de certificado previamente creada. Este perfil emite certificados de firma para los dispositivos e implementa el perfil de certificado PKCS en los dispositivos.

También es posible importar un certificado de firma para un usuario específico en Intune. Este certificado se implementa en todos los dispositivos inscritos por ese usuario. Para implementarlo:

1. Descargar, instalar y configurar **Certificate Connector** para Microsoft Intune. Este conector proporciona certificados PKCS importados a los dispositivos.
2. Importar los certificados de firma de correo electrónico S/MIME a Intune.
3. Crear un perfil de certificado PKCS importado. Este perfil suministra los certificados PKCS importados a los dispositivos del usuario adecuado.

Certificado de cifrado

Los certificados utilizados para el cifrado aseguran que un correo electrónico cifrado solo pueda ser descifrado por el destinatario previsto. El cifrado S/MIME añade una capa adicional de seguridad que puede ser utilizada en las comunicaciones por correo electrónico.

Para implementar un certificado PKCS importado en Intune que se utilizará para el cifrado de correo electrónico, se haría de forma similar a los pasos indicados en el apartado anterior para el usuario específico.

Nota: Es recomendable no crear los certificados de cifrado de correo electrónico en Intune. Aunque Intune puede emitir certificados PKCS que admiten el cifrado, genera un certificado único por dispositivo. Esto no es ideal para un escenario de cifrado S/MIME, donde el certificado de cifrado debe ser compartido entre todos los dispositivos del usuario.

Para más información sobre el uso de los certificados para firmar y cifrar el correo electrónico en Intune, consultar: S/MIME para la firma y el cifrado de mensajes | Microsoft Learn.

Microsoft Intune incluye también un perfil de configuración de correo electrónico. Con este perfil, se puede configurar la aplicación de correo electrónico integrada en los dispositivos o implementar otras aplicaciones de correo electrónico que se conecten al sistema de correo electrónico, como Microsoft Exchange. Luego, los usuarios finales pueden conectarse, autenticarse y sincronizar sus cuentas de correo electrónico de la organización en sus dispositivos.

Aquí se va a poder elegir cómo se autentican los usuarios, utilizando S/MIME para el cifrado, etc.

Para más información consultar la guía de Exchange [CCN-STIC 885C - Guía de configuración segura para Exchange Online].

3.2.3.2 PROTECCIÓN DE LA NAVEGACIÓN WEB

La protección web de Microsoft Defender bloquea el acceso a sitios de phishing, vectores de malware, páginas con vulnerabilidades de seguridad, sitios no confiables o de reputación dudosa, y aquellos identificados en listas de indicadores personalizados. Al integrarse con Microsoft Edge y exploradores de terceros populares como Chrome y Firefox, la protección contra amenazas web detiene las amenazas web sin un proxy web y puede proteger los dispositivos mientras están fuera o en el entorno local.

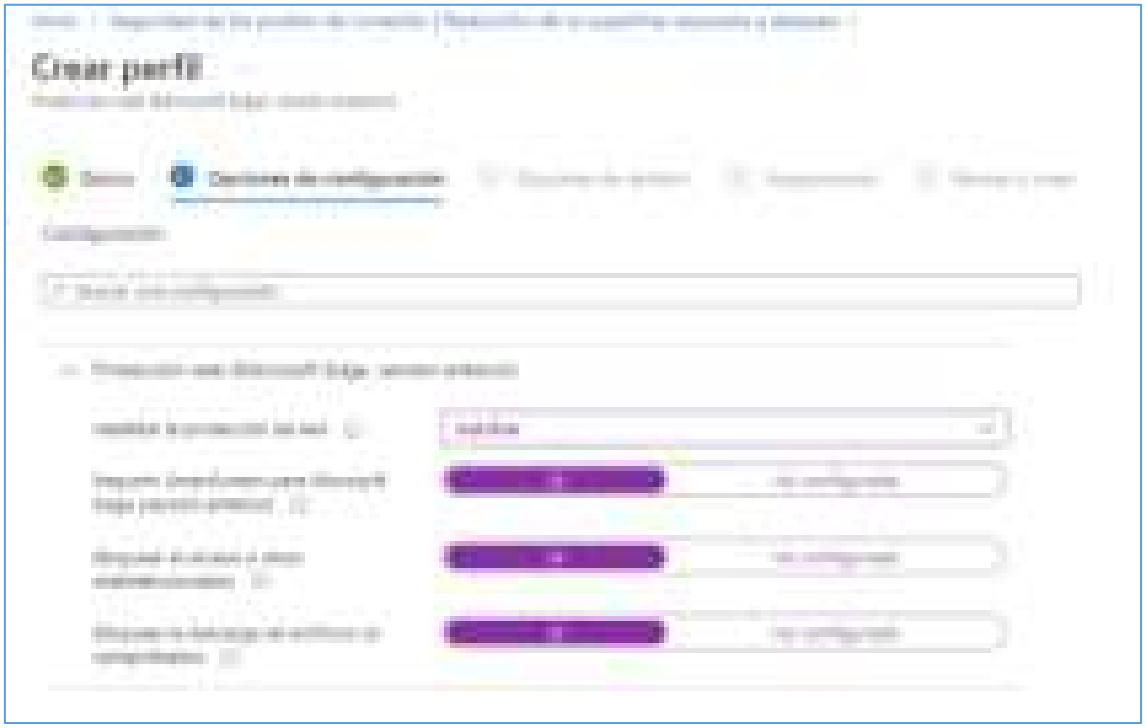
Actualmente, esta función está disponible en plataformas como Windows, iOS y Android.

Para configurar la protección contra amenazas web mediante el portal de Intune:

1. Iniciar sesión en la consola de Microsoft Intune, seleccionar **Seguridad de puntos de conexión > Reducción de la superficie expuesta a ataques > Crear directiva.**

2. Seleccionar plataforma, como **Windows 10 y versiones posteriores**, el perfil **Protección web** y **Crear**.
3. En la pestaña de aspectos básicos, especificar nombre y descripción.
4. En **Opciones de configuración**, especificar la configuración, según lo siguiente:
   - Habilitar la opción **Habilitar protección de red** para activar la protección web. Como alternativa, se puede establecer en modo auditoría para realizar un seguimiento de las detecciones sin bloquear el acceso a los sitios.
   - Para proteger a los usuarios contra phishing y malware, activar **Requerir SmartScreen** para Microsoft Edge.
   - Evitar que los usuarios ignoren advertencias sobre sitios maliciosos configurando **Bloquear el acceso a sitios malintencionados**.

- Para evitar que los usuarios descarguen archivos no comprobados, establecer **Bloquear descarga de archivos no comprobados** en **Sí**.



Microsoft Defender SmartScreen

Microsoft Defender SmartScreen protege contra malware en sitios web y aplicaciones que intentan suplantar identidades, así como descargas de archivos potencialmente peligrosos.

Para determinar la amenaza de un sitio web:

- Microsoft Defender SmartScreen analiza el comportamiento de las páginas visitadas en busca de signos de actividad sospechosa. Si se detecta una página como maliciosa, se muestra una advertencia al usuario.
- SmartScreen verifica los sitios visitados utilizando una lista en constante actualización de sitios denunciados por phishing y software malicioso. Si se encuentra una coincidencia, se muestra una advertencia para alertar al usuario sobre la posible amenaza del sitio.

Una de las formas de configurar SmartScreen desde Intune, es siguiendo los siguientes pasos. También es posible desde el perfil de Endpoint Protection, Catálogo de configuraciones, Plantillas administrativas, etc.

1. Iniciar sesión en la consola de Microsoft Intune, seleccionar **Seguridad de puntos de conexión > Líneas base de seguridad > Línea base de Microsoft Defender para punto de conexión > Crear perfil.**

2. En las opciones básicas, introducir un nombre y descripción.
3. Buscar la sección de **SmartScreen** y configurar todo lo necesario según la organización.

Para mejorar la protección de la organización, se recomienda activar y utilizar las siguientes configuraciones específicas de Microsoft Defender SmartScreen mediante Intune.

Configuración de MDM	Recomendación
Explorador/AllowSmartScreen	**1.** Activa Microsoft Defender SmartScreen.
Explorador/PreventSmartScreenPromptOverride	**1.** Impide que los empleados ignoren los mensajes de advertencia y continúen en un sitio web potencialmente malintencionado.
Explorador/PreventSmartScreenPromptOverrideForFiles	**1.** Impide que los empleados ignoren los mensajes de advertencia y sigan descargando archivos potencialmente malintencionados.
SmartScreen/EnableSmartScreenInShell	**1.** Activa Microsoft Defender SmartScreen en Windows.
SmartScreen/PreventOverrideForFilesInShell	**1.** Impide que los empleados ignoren los mensajes de advertencia sobre archivos malintencionados descargados de Internet.

Además, los administradores pueden ajustar la interacción entre Microsoft Edge y Microsoft Defender SmartScreen para proteger a los usuarios contra direcciones URL relacionadas con Aplicaciones Potencialmente No Deseadas (PUA). Existen varias opciones de configuración específicas para SmartScreen, incluida una para bloquear PUA.

Para más información sobre la configuración para bloquear PUA, consultar:

Documentación de directiva de explorador Microsoft Edge | Microsoft Learn

Microsoft Edge

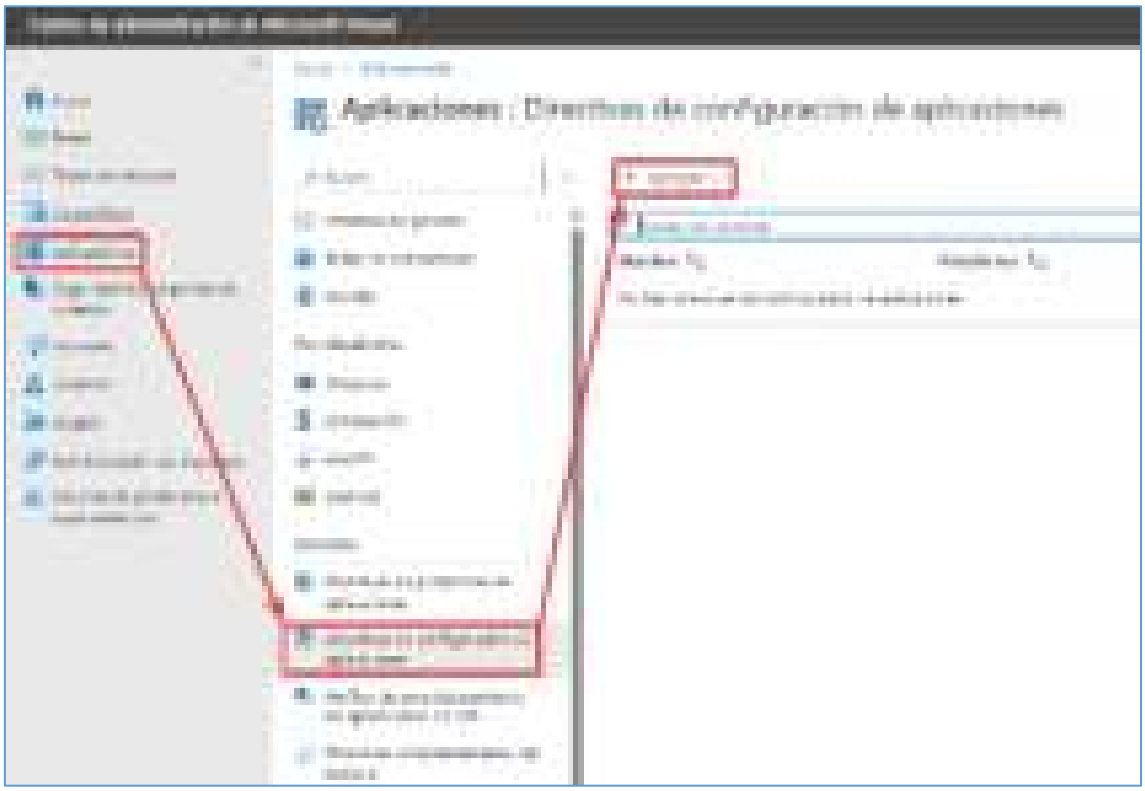
Desde los perfiles de configuración de aplicaciones, se puede definir una política de configuración de Microsoft Edge, donde se establezcan los sitios web a los que los usuarios finales pueden o no acceder utilizando este navegador administrado. Si se usa una lista de permitidos, los usuarios solo tendrán acceso a los sitios web que se hayan especificado. Por otro lado, con una lista de bloqueados, los usuarios podrán acceder a todos los sitios web excepto aquellos que se hayan bloqueado específicamente. Solo debe imponer una lista de permitidos o bloqueados, no ambas.

Las organizaciones también establecen las acciones que ocurren cuando un usuario intenta acceder a un sitio web restringido. Si la organización lo permite, los sitios web

restringidos pueden abrirse en el contexto de la cuenta personal, en el contexto de una sesión InPrivate de Microsoft Entra, o simplemente se bloquean por completo.

Por ejemplo:

1. Iniciar sesión en la consola de Microsoft Intune, seleccionar **Aplicaciones > Directivas de configuración de aplicaciones > Agregar.**



2. Seleccionar si la configuración es para **Dispositivos administrados** o **Aplicaciones administradas**.
3. Seleccionar la aplicación a configurar.

4. Luego, también es posible realizar la configuración necesaria para el navegador mediante los settings del **Cátalogo de configuración**.

5. Una vez se haya configurado todo lo necesario desde el **Catálogo**, ya se pueden determinar los sitios web a los que se permite/bloquea el acceso.

Nota: Esta configuración está disponible para dispositivos iOS y Android.

Además, también se puede ajustar la configuración para permitir o bloquear las cookies para todos los sitios y establecer excepciones para sitios específicos. Todas las cookies están permitidas por defecto en todos los navegadores web.

Algunas cookies pueden poner en peligro la privacidad al rastrear los sitios que se visitan. Las cookies de terceros permiten a los anunciantes rastrear el historial de navegación de una persona a través de la web en cualquier sitio que contenga sus anuncios.

El filtrado de contenido web forma parte de la protección web en Microsoft Defender for Endpoint. Para más información sobre la protección adicional que se proporciona desde Defender for Endpoint, consultar la guía [CCN-STIC-885E- Guía de configuración segura para Microsoft Defender for Endpoint].

3.2.3.3 PROTECCIÓN FRENTE A LA DENEGACIÓN DE SERVICIO

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

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

Para cumplir con los requisitos exigidos dentro del ámbito del ENS, consultar la guía [CCN-STIC-884A - Guía de configuración segura para Azure].

4. GLOSARIO Y ABREVIATURAS

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

Término	Definición
AD DS	Active Directory Domain Services (Servicios de dominio de Directorio Activo).
AES	AES, también conocido como “Advanced Encryption Standard“, es un sistema usado por el gobierno de Estados Unidos para la encriptación de sus archivos.
Entra ID	Directorio Activo de Entra.
Azure RMS	Azure Rights Management (Azure RMS).
BranchCache	BranchCache es una tecnología de Microsoft que trata de reducir los flujos de la red WAN (Wide Area Network), permitiendo la puesta en caché de aquellos archivos que se utilizan con mayor frecuencia.
Centro de Administración de Microsoft 365	Portal de Administración de Office 365. Accesible desde la url: admin.microsoft.com.
CDN	CDN o red de distribución de contenido es un grupo de servidores repartidos en distintas zonas geográficas que aceleran la entrega del contenido web.
Código dañino	El código malicioso es un tipo de código informático o script web dañino diseñado para crear vulnerabilidades en el sistema que permiten la generación de puertas traseras, brechas de seguridad, robo de información y datos, así como otros perjuicios potenciales en archivos y sistemas informáticos.
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.
EMS	Microsoft Enterprise Mobility + Security (EMS) es una plataforma inteligente de seguridad y administración de la movilidad. Ayuda a proteger tu organización y permite a tus empleados trabajar de formas nuevas y flexibles.

ENS	Esquema Nacional de Seguridad.
FileVault	FileVault un sistema de encriptación que usa como método de encriptación AES.
Jailbreak	Se trata de procedimientos mediante los cuales se pueden eliminar las limitaciones que los smartphones y tablets tienen de fábrica.
Malware	Malware o "software malicioso" es un término amplio que describe cualquier programa o código malicioso que es dañino para los sistemas.
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. Microsoft 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.
Mobile Iron	MobileIron es una plataforma creada para asegurar y administrar datos corporativos en un mundo en el que los usuarios acceden a estas informaciones mediante dispositivos móviles y puntos de conexión modernos desde cualquier lugar y en cualquier momento.
M365	Microsoft 365.
OOBE	Windows Out of Box Experience (OOBE) permite a los administradores inscribir de forma automática dispositivos de 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.
Tenant	Un tenant de Office 365 es un espacio reservado en la nube de Microsoft desde el que tendremos acceso a los recursos y servicios que Microsoft ofrece.
TLS	TLS (Seguridad de la capa de transporte) y SSL (antecesor de TLS) son protocolos criptográficos que protegen la comunicación por red con certificados de seguridad que cifran una conexión entre equipos.
Token	Un Token es un string aleatorio que identifica a un usuario y puede ser utilizado por la aplicación para realizar llamadas API.
TPM	TPM o “Trusted Platform Module” es un estándar internacional para un criptoprocesador seguro, un microcontrolador dedicado diseñado para proteger el hardware a través de claves criptográficas integradas.
TTL	TTL o Tiempo de vida (Time to live) es un mecanismo que se usa para limitar la duración de la información que circula por la red.

5. CUADRO RESUMEN DE MEDIDAS DE SEGURIDAD

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

<table>
<tr><th>Control ENS</th><th colspan="2">Configuracion</th><th>Estado</th></tr>
<tr><td>op</td><td colspan="3">Marco Operacional</td></tr>
<tr><td>op.acc</td><td colspan="3">Control de Acceso</td></tr>
<tr><td>op.acc.1</td><td colspan="3">Identificación</td></tr>
<tr><td rowspan="2"></td><td rowspan="2">Se ha realizado la asignación de licencias de Microsoft Intune a usuarios para la inscripción de los dispositivos.
Es necesaria la licencia de Microsoft Intune para la inscripción de los dispositivos en la consola de Microsoft Intune.</td><td>Aplica:
☐ Si ☐ No</td><td>Cumple:
☐ Si ☐ No</td></tr>
<tr><td>Evidencias Recogidas:
☐ Si ☐ No</td><td>Observaciones:</td></tr>
</table>

op.acc.1	**Identificación**		
	Siguiendo las medidas de seguridad sobre la gestión de usuario por el ENS, se ha evaluado la eliminación de los usuarios que abandonen la compañía.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
op.acc.2	**Requisitos de acceso**		
	Se han combinado las etiquetas de ámbito y el control de acceso basado en roles para así separar de alguna manera la tarea de los administradores.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
op.acc.3	**Segregación de funciones y tareas**		
	Se ha asignado adecuadamente los roles de administración.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
op.acc.5	**Mecanismos de autenticación (usuarios externos)**		

	Se ha habilitado Multi-Factor Authentication (MFA) para los usuarios externos.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
op.acc.6	**Mecanismos de autenticación (usuarios de la organización)**		
	Se ha habilitado Multi-Factor Authentication (MFA) para los usuarios de la organización que se conecten desde redes que no estén en la organización.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
op.acc.6	**Mecanismos de autenticación (usuarios de la organización)**		
	Se han configurado directivas de acceso condicional para que los usuarios y dispositivos que se conectan desde las redes de la organización dispongan de un acceso menos restrictivo que aquellos que se conectan desde Internet, identificando correctamente las direcciones IPs y redes de origen.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
op.exp	**Explotación**		
op.exp.1	**Configuración de seguridad**		

	Se ha asignado una Línea base de seguridad con las recomendaciones de seguridad configuradas por Microsoft en los dispositivos Windows.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
op.exp.4	**Mantenimiento y actualizaciones de seguridad**		
	Se han configurado directivas de actualizaciones de software y controladores de los dispositivos para así tener el control de las actualizaciones y mantenerlos protegidos.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
op.exp.7	**Gestión de incidentes**		
	Se consulta el registro de las actividades que generan un cambio en Microsoft Intune.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
op.mon	**Monitorización del sistema**		
op.mon.1	**Detección de intrusión**		

	Se revisan paulatinamente los informes en Microsoft Intune para subsanar o anteponerse a incidencias.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
mp	**Medidas de protección**		
mp.eq	**Protección de los equipos**		
mp.eq.2	**Bloqueo de puesto de trabajo**		
	Se ha establecido un tiempo para el bloqueo de los dispositivos, requiriendo una nueva autenticación del usuario para reanudar la actividad.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
mp.eq.3	**Protección de dispositivos portátiles**		
	Se han configurado directivas de acceso condicional basadas en la ubicación para proteger adecuadamente los datos de la organización y a los dispositivos móviles que pueden salir de las instalaciones de la organización y están expuestos al riesgo de pérdida o robo.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**

mp.si	**Protección de los soportes de información**		
mp.si.2	**Criptografía**		
	Se ha asignado una directiva de BitLocker para cifrar los equipos Windows.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
mp.si.2	**Criptografía**		
	Se ha asignado una directiva de FileVault para cifrar los equipos macOS.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
mp.si.2	**Criptografía**		
	Se ha exigido al usuario a través de una directiva de cumplimiento que su dispositivo Android o iOS este cifrado.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas:	**Observaciones:**
		Si No	

		☐ ☐	
mp.si.5	**Borrado y destrucción**		
	Se han asignado directivas de protección de aplicaciones para poder hacer un borrado selectivo de los datos corporativos de las aplicaciones si un dispositivo se extravía, es robado o un empleado deja la empresa.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
mp.s	**Protección de los servicios**		
mp.s.3	**Protección de la navegación web**		
	Se ha configurado la protección web y SmartScreen de Microsoft Defender para bloquear el acceso a sitios de phishing, descargas de archivos potencialmente peligrosos, sitios no confiables, etc.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
otros	**Configuración de reestricción de dispositivo**		
	Se ha configurado una restricción para que un tipo de dispositivo en concreto no pueda inscribirse en Intune.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas:	**Observaciones:**

		☐ Si ☐ No