E.T.S. de Ingeniería Industrial,
Informática y de Telecomunicación

Gestión de dispositivos Microsoft Windows e iOS/iPadOS

Grado en Ingeniería
en Tecnologías de Telecomunicación

Trabajo Fin de Grado

Alumna: María Herrero Arbizu

Directores: Rosa Ana Pérez Herrera

Bernardo Ciriza Mendívil

Pamplona, 7 de junio 2023

upna
Universidad Pública de Navarra
Nafarroako Unibertsitate Publikoa

Agradecimientos

A todo el profesorado que ha estado implicado en mi formación y por todos los conocimientos que he adquirido durante estos 4 años, en especial a los que, sin dejar de exigir lo que una carrera de este tipo pide, disfrutan de su trabajo y han intentado ayudarnos y motivarnos en todo momento.

A CYC, y más concretamente al equipo de sistemas, por toda la acogida y nuevas experiencias que me han dado, ayudándome a terminar la carrera con muy buen sabor de boca.

A Natalia y Saioa, las personas con las que he compartido agobios, desahogos y, sobre todo, muchas risas. Sin ninguna duda, la carrera sin ellas no habría sido lo mismo.

Y por supuesto, a mi familia, por todo el apoyo que me da, por aguantarme en los momentos más duros y por alegrarse y sentirse orgullosos de todo lo que poco a poco voy consiguiendo.

Resumen

Hoy en día el mundo digital se ha visto forzado a crecer exponencialmente y con ello, los servicios en la nube y el uso simultáneo de recursos que se encuentran en ella. De la misma forma, la movilidad empresarial y el teletrabajo se han convertido en una actividad cada vez más recurrente, en parte debido a la pandemia que se ha vivido en los últimos años y que ha obligado a las personas a realizar su actividad laboral desde espacios no controlados por las empresas, haciendo vulnerables datos de estas. Es por esto por lo que ha aparecido una gran necesidad de ofrecer una solución para mantener los datos corporativos seguros fuera de la organización.

Se ha realizado un análisis del mercado y por diferentes motivos como la seguridad, la compatibilidad y los costes, se ha optado por utilizar los servicios basados en la nube proporcionados por Microsoft, como son Azure AD y Microsoft Intune admin center.

Todas las funcionalidades que proporcionan los servicios de Microsoft han servido para llevar a cabo este proyecto, en el que con dispositivos de la empresa consultora se han realizado diferentes pruebas.

Además, se han podido comprobar también las funcionalidades de gestión y administración de dispositivos y aplicaciones (MDM y MAM) de los sistemas operativos Windows e iOS/iPadOS, aunque este último en menor profundidad.

Palabras clave

- Mobile Application Management (MAM)
- Mobile Device Management (MDM)
- Microsoft Intune
- Microsoft Intune admin center
- Microsoft Azure
- Active Directory (AD)
- Hybrid Azure AD-joined
- Windows AutoPilot

Abstract

Nowadays the digital world has been forced to grow exponentially and with it, cloud services and the simultaneous use of resources found in it. In the same way, business mobility and teleworking have become an increasingly recurrent activity, partly due to the pandemic that has been experienced in recent years and that has forced people to carry out their work activity from spaces not controlled by companies, making their data vulnerable. This is why a great need has appeared to offer a solution to keep corporate data safe outside the organization.

An analysis of the market has been carried out and for different reasons such as security, compatibility, and costs, it has been chosen to use the cloud-based services provided by Microsoft such as Azure AD and Microsoft Intune admin center.

All the functionalities provided by Microsoft services have served to carry out this project, in which different tests have been carried out with devices from the consulting company.

In addition, it has also been possible to verify the management and administration functionalities of devices and applications (MDM and MAM) of the Windows and iOS / iPadOS operating systems, although the latter in less depth.

Key Words

- Mobile Application Management (MAM)
- Mobile Device Management (MDM)
- Microsoft Intune
- Microsoft Intune admin center
- Microsoft Azure
- Active Directory (AD)
- Hybrid Azure AD-joined
- Windows AutoPilot

Índice

Índice de figuras

Índice de abreviaturas

Abreviatura	Significado	Traducción
AAD	Azure Active Directory	Directorio activo Azure
AD	Active Directory	Directorio activo
AD FS	Active Directory Federation Services	Servicio de federación de directorio activo
DC	Domain Controller	Controlador de dominio
DMZ	Demilitarized Zone	Zona desmilitarizada
DNS	Domain Name System	Sistema de nombre de dominio
EMM	Enterprise Mobility Management	Gestión de movilidad empresarial
GPO	Group Policy Object	Directivas de grupo
HTTP	HyperText Transfer Protocol	Protocolo de transferencia de hipertexto
HTTPS	HyperText Transfer Protocol Secure	Protocolo seguro de transferencia de hipertexto
MAM	Mobile Application Management	Administración de aplicaciones móviles
MDM	Mobile Device Management	Administración de dispositivos móviles
OU	Organizational Unit	Unidad organizativa
SID	Security Identifier	Identidad de seguridad
UEM	Unified Endpoint Management	Administración unificada de punto final

1. Introducción

Cada vez son más las empresas que han implementado el teletrabajo y la movilidad empresarial, generando una transición en el método tradicional de trabajo. Esto ha hecho que aparezca la necesidad de buscar una solución para mantener seguros los datos corporativos fuera de la organización.

Tras un análisis del mercado y de los recursos existentes, se ha optado por la solución que proporcionan los servicios de Microsoft Intune para gestionar y administrar los dispositivos de empresa.

El centro de administración de Microsoft Intune es la combinación de servicios basados en la nube, y gracias a la unión de todos ellos y a las herramientas de Microsoft 365, como Microsoft Intune y Azure Active Directory, es posible administrar tanto dispositivos como aplicaciones de diversas plataformas.

En este Trabajo de Fin de Grado se ha tratado de gestionar y administrar los ordenadores con sistema operativo Microsoft Windows de la empresa, con el objetivo de implementar el software de gestión y administración de dispositivos móviles y aplicaciones (MDM y MAM).

1.1. Justificación/Motivación

Hoy en día el mundo digital se ha visto forzado a crecer exponencialmente y con ello, los servicios en la nube y el uso simultáneo de recursos que se encuentran en ella. De la misma forma, la movilidad empresarial y el teletrabajo se han convertido en una actividad cada vez más recurrente, en parte debido a la pandemia que se ha vivido en los últimos años y que ha obligado a las personas a realizar su actividad laboral desde espacios no controlados por las empresas, haciendo vulnerables datos de estas. Además, el hecho de que cada vez sean más las organizaciones que ponen a disposición de su plantilla el teletrabajo, ha generado una transición en el método tradicional de trabajo, provocando inseguridades en los sistemas corporativos.

Para que estas nuevas metodologías de trabajo se puedan llevar a cabo de manera segura, los métodos de autenticación y la migración de los recursos locales a la nube adquieren una gran importancia.

La empresa consultora CYC ha hecho una propuesta de TFG que consiste en la gestión de dispositivos Microsoft Windows con el objetivo de poder administrar y gestionar dispositivos de una forma más sencilla, teniendo en cuenta, en la práctica, las propuestas de los diferentes clientes de esta.

1.2. Ámbito

El ámbito en el que se lleva a cabo este proyecto es únicamente empresarial, sabiendo que es una necesidad cada vez más recurrente y que se está extendiendo a distintos ámbitos, como puede ser el escolar. La metodología llevada a cabo, basada en implementar el software MDM y MAM, consigue configurar, controlar y gestionar los dispositivos de forma segura. Esta metodología se puede aplicar en otros ámbitos de una forma similar a la que se ha llevado a cabo en la empresa consultora.

1.3. Objetivo

El objetivo principal de este Trabajo de Fin de Grado no es otro que el de gestionar y administrar los ordenadores con sistema operativo Microsoft Windows de la empresa, con el objetivo de implementar el software de gestión y administración de dispositivos móviles y aplicaciones (MDM y MAM) en un escenario híbrido con personas y equipamiento que se conectan desde la oficina, donde se dispone de conexión con el directorio activo local; y otras personas que se conectan con su equipamiento desde "fuera" haciendo uso del directorio activo de Azure.

Se requiere una formación inicial en Microsoft Intune y Azure AD, asegurando así que los dispositivos y aplicaciones configuradas además de los datos corporativos de la empresa cumplen con los requisitos de seguridad.

2. Estado del arte

Desde hace unos años ha habido una serie de acontecimientos y circunstancias que han provocado un crecimiento exponencial de la tecnología. La pandemia que se ha vivido en los últimos años ha sido uno de los principales motivos que ha hecho que muchas empresas se hayan visto forzadas a teletrabajar o a realizar su actividad laboral desde espacios no controlados por la compañía, generando vulnerabilidades en los datos sensibles de esta.

De la misma forma, el aumento del uso, en distintos ámbitos, de dispositivos conectados a Internet y el auge que la digitalización está viviendo en todo el mundo, han provocado un aumento en el volumen de datos con los que se trabaja. Es por esto por lo que ha nacido una necesidad de almacenar los datos en la nube, permitiendo así que los usuarios puedan acceder a ellos desde cualquier punto de conexión. Los servicios en la nube eliminan la necesidad de que las organizaciones almacenen las aplicaciones y los datos en sus propios servidores locales.

El teletrabajo y la movilidad empresarial son cada vez más recurrentes y es por esto por lo que cada vez son más las empresas y multinacionales que deciden apostar por los softwares de gestión y administración de dispositivos (MDM) y/o aplicaciones (MAM), habiendo así mucha demanda en el mercado.

2.1. Análisis del mercado

El mercado de servicios en la nube se ha convertido en uno de los sectores más dinámicos y con mayor crecimiento de la industria tecnológica en los últimos años. Este crecimiento de los servicios en la nube está siendo impulsado por la aceleración de la transformación digital en todo el mundo y por la adopción generalizada de la tecnología de la nube por parte de empresas de todos los tamaños y sectores. De la misma forma, ha aparecido la necesidad de mantener protegidos los datos corporativos fuera de la organización.

Las multinacionales tecnológicas, se han visto obligadas a actualizarse para mantenerse competitivas y para mejorar su eficiencia y escalabilidad, ya que compiten en un sector que está en constante evolución y crecimiento y que, además, se espera que siga siendo así en los próximos años. Es por esto por lo que hoy en día existe una gran rivalidad en el mercado.

Tras un primer análisis, se ha comprobado que algunas de las compañías "líderes" que ofrecen servicios en la nube actualmente son Microsoft con Microsoft Intune, IBM con IBM MaaS360 y Oracle con Oracle Cloud, con unas cuotas de mercado, a día de hoy, del 20%, 7% y 6%, respectivamente. Hay que tener en cuenta que se trata de un mercado que está en constante evolución y que estas cuotas van cambiando con el tiempo.

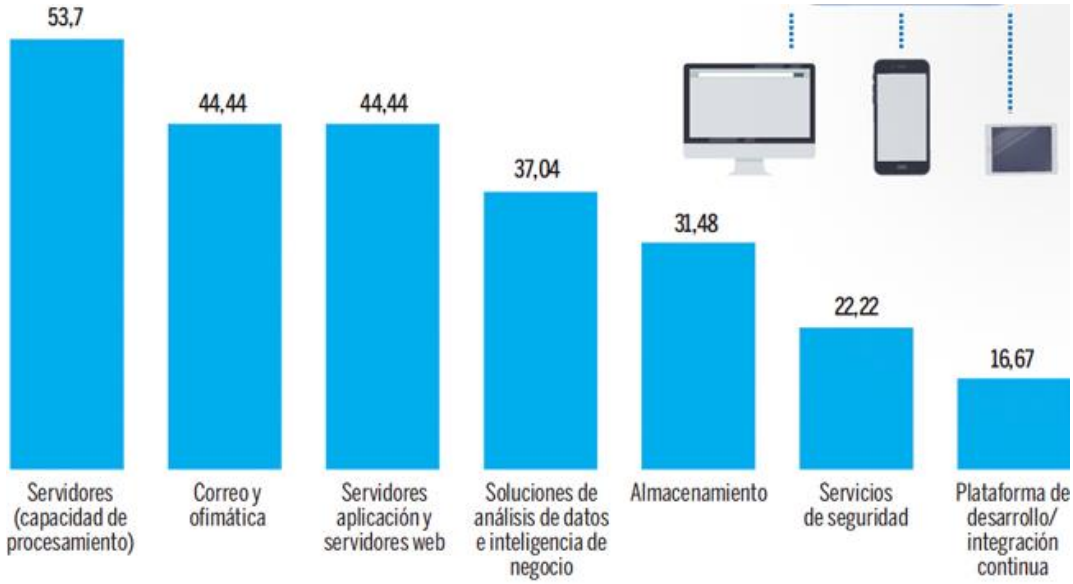


Figura 1. *Funciones y servicios más relevantes en el ámbito de la nube. [1]*

2.1.1. Microsoft Intune

Microsoft es una multinacional tecnológica de origen estadounidense que desarrolla y comercializa una amplia gama de software, hardware y servicios de IT, tanto para empresas como para consumidores privados. Actualmente, se encuentra en las posiciones más altas del mercado.

Microsoft Intune está integrado con otros productos y servicios de Microsoft, como Enterprise Mobility + Security (EMS), que es un servicio basado en la nube que proporciona Microsoft Azure y el Centro de administración de Intune, herramientas que se detallarán más adelante. Es así como se puede controlar el acceso de los usuarios. Además, Intune proporciona la infraestructura en la nube, la administración de dispositivos móviles (MDM), la administración de aplicaciones (MAM) y la administración de equipos basada en la nube para su organización. También ayuda a asegurarse de que los dispositivos, aplicaciones y datos empresariales cumplan los requisitos de seguridad de la empresa, teniendo el control de establecer qué requisitos deben comprobar y qué sucede cuando no se cumplen. En el centro de administración de Microsoft Intune es donde se encuentra el servicio de Intune y las configuraciones relacionadas con la administración de dispositivos. [2]

Como se puede ver en la Figura 2, hay diferentes licencias que proporcionan el acceso al centro de administración de Intune, siendo las enfocadas a empresas las E3, E5, las Enterprise y la Empresa Premium.

Figura 2. *Paquetes de licencias de Microsoft en los que se incluye Intune. [3]*

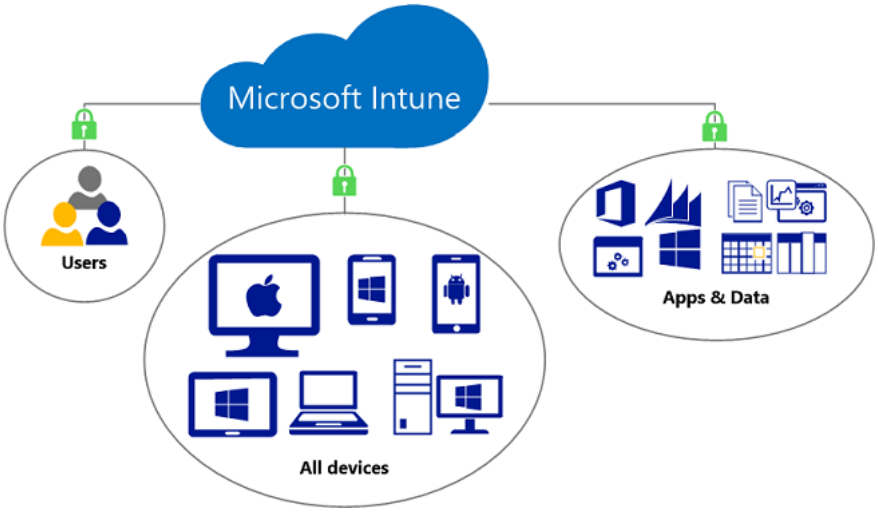


Figura 3. *Esquema resumen Microsoft Intune. [4]*

2.1.2. IBM MaaS360

International Business Machines (IBM) es una multinacional estadounidense de tecnología y consultoría que fabrica y comercializa hardware y software, además de ofrecer servicios de infraestructura, alojamiento de Internet y consultoría en el ámbito informático. [5]

Ofrece servicios como MaaS360 Mobile Device Management (Saas), que es una plataforma de gestión de movilidad empresarial (EMM) que proporciona visibilidad y control de teléfonos y tabletas de empresa. El software de MaaS360 se integra con IBM Security Verify, que es una solución de gestión de acceso e identidades basada en la nube que garantiza que solo los dispositivos y aplicaciones de confianza puedan acceder a los recursos corporativos.

La consola de administración que proporciona la plataforma permite al departamento IT de la empresa controlar en tiempo real todos los dispositivos registrados y las aplicaciones de interés, facilitando la resolución y diagnóstico de problemas por medio de herramientas de monitorización. La plataforma también permite a las empresas proteger sus datos y dispositivos móviles mediante la configuración de políticas de seguridad de la industria, además de proporcionar informes detallados y analíticas para

ayudar a las organizaciones a tomar decisiones informadas sobre su estrategia de gestión de dispositivos móviles. [6]

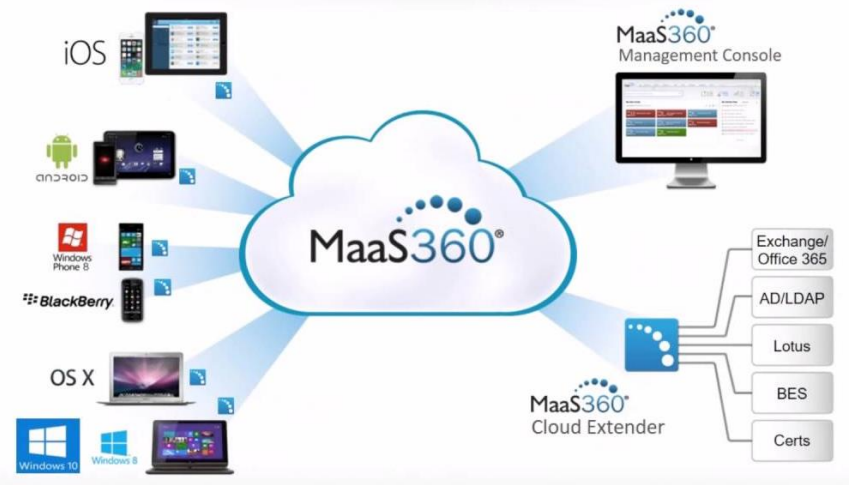


Figura 4. *Esquema sistemas operativos compatibles con IBM MaaS360. [6]*

2.1.3. Oracle Cloud

Oracle es una empresa tecnológica estadounidense que se especializa en la creación y venta de software empresarial, hardware y servicios en la nube. Inicialmente la empresa se centró en la creación de sistemas de gestión de bases de datos y ha sido uno de los principales proveedores de software de bases de datos durante décadas. Sin embargo, con el tiempo, Oracle se ha ido diversificando y ha expandido su gama de productos y servicios, incluyendo soluciones como la de servicios en la nube.

Oracle Cloud es la plataforma de nube pública que ofrece Oracle. Proporciona una amplia gama de servicios en la nube, incluyendo servicios de infraestructura (IaaS), servicios de plataforma (PaaS) y servicios de software como servicio (SaaS). Oracle Cloud está diseñada para satisfacer las necesidades de los clientes empresariales que requieren escalabilidad, rendimiento y seguridad en su infraestructura en la nube. Además, ofrece herramientas y servicios de automatización que ayudan a los clientes a gestionar y optimizar sus entornos de nube. [7]

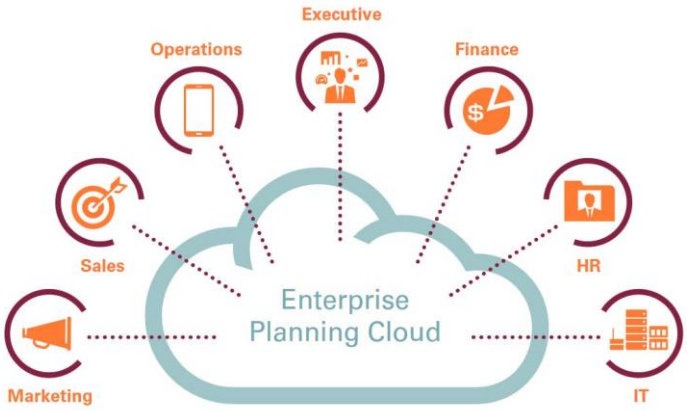


Figura 5. *Servicios en la nube de planificación empresarial de Oracle. [8]*

2.2. Elección del servicio

A la hora de elegir un servicio en la nube hay que tener en cuenta aspectos como el económico, la seguridad, el rendimiento, la capacidad, la compatibilidad y la fiabilidad. [9]

La elección de cualquiera de los proveedores de servicios en la nube mencionados anteriormente podría ser una buena elección. Son una forma útil de acceder a servicios informáticos que, de otro modo, las empresas tendrían que proporcionarse por su cuenta. Algunos de estos servicios serían:

- ***Infraestructura*.-** Es la base de todo entorno informático y puede incluir redes, servidores, virtualización y/o bases, gestión y almacenamiento de datos.
- ***Software*.-** Un ejemplo de software son las aplicaciones estándar y/o personalizadas que se ofrecen ya listas para usar.
- ***Plataformas*.-** Son las herramientas necesarias para gestionar dispositivos y para gestionar, crear y desplegar aplicaciones.

Actualmente a nivel nacional, la mayoría de las empresas trabajan con dispositivos del sistema operativo Windows. Este hecho hace que los empleados de la organización necesiten un usuario propio, además de una licencia para tener acceso a las herramientas y servicios de Microsoft. Es por esto por lo que, tras analizar los servicios descritos anteriormente, la opción más económica sería la de elegir Microsoft Intune, al ser la de mayor compatibilidad con el sistema operativo Windows por el hecho de que ambas pertenecen a Microsoft, evitando así un coste adicional.

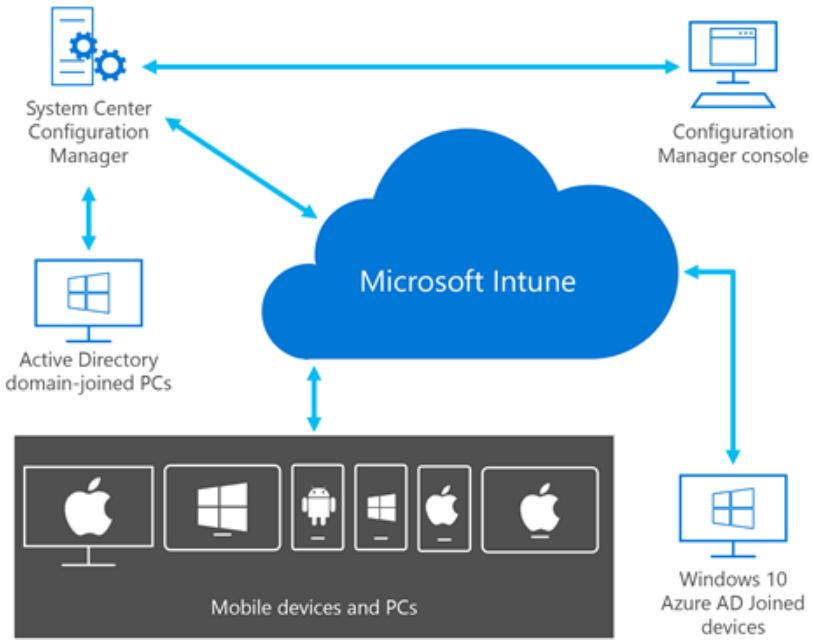


Figura 6. *Servicios Microsoft Intune. [2]*

3. Marco teórico

En este apartado se van a explicar el contexto y las bases conceptual y teórica sobre las que se ha desarrollado el proyecto, así como la definición de los conceptos más relevantes.

3.1. Fundamentos tecnológicos

3.1.1. Qué es la nube

La nube (Cloud) hace referencia a los servidores a los que se accede a través de Internet y al software y bases de datos que se ejecutan en esos servidores, es decir, es un conjunto de servidores físicos que se encuentran en uno o varios centros de datos y que pueden estar ubicados por todo el mundo. Gracias a la informática en la nube, los usuarios y las empresas no necesitan gestionar los servidores físicos ni ejecutar aplicaciones de software en sus propios ordenadores, pudiendo acceder a los mismos archivos y aplicaciones casi desde cualquier dispositivo. Esto es posible porque los procesos informáticos y de almacenamiento tienen lugar en servidores en un centro de datos, y no de forma local en el dispositivo del usuario. [10]

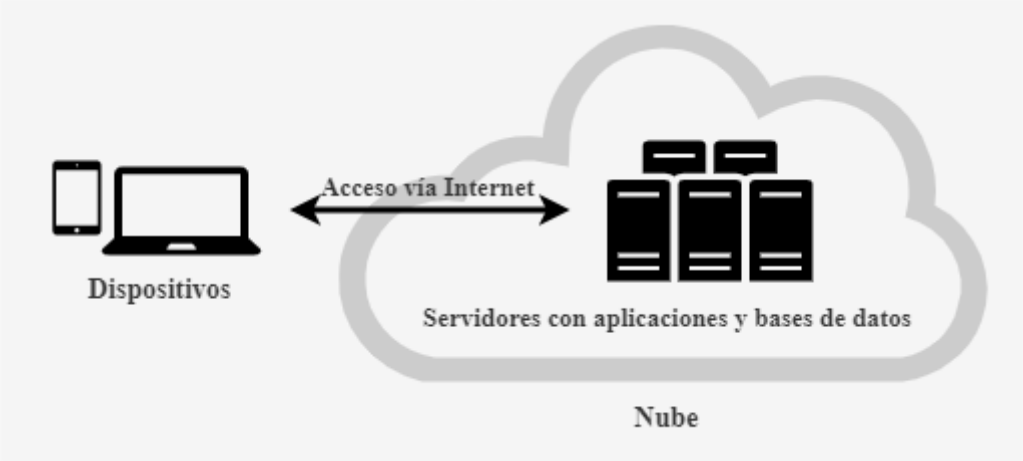


Figura 7. *Servicios en la nube*

Otro de los beneficios que aporta a las empresas la informática en la nube es que supone menos gastos generales y de IT, al no tener que mantener y actualizar sus propios servidores.

3.1.2. Servicios Microsoft Azure

Microsoft Azure es un servicio de computación en la nube desarrollado por Microsoft y que está compuesto por más de 200 productos y servicios que facilita la gestión y administración de dispositivos y aplicaciones a través de un gran centro de datos mundial. Entre los productos y servicios que ofrece, incluye las funcionalidades de plataforma como servicio (PaaS), infraestructura como servicio (IaaS) y servicio de base de datos administrado. Al igual que otras plataformas en la nube, se basa en una tecnología conocida como *virtualización*. Esta tecnología permite crear servicios de IT que tradicionalmente están limitados al hardware, es decir, permite la creación de ordenadores virtuales, simulados y digitales que se comportan como si fuesen ordenadores físicos con su propio hardware. Ese "ordenador virtual" recibe el nombre

técnico de *máquina virtual* y hacen un uso más eficiente del hardware en el que están alojadas.

Algunos de los servicios que ofrece y que tienen una gran labor en la realización de este proyecto son Microsoft Intune, Microsoft Configuration Manager, Microsoft Intune admin center, Windows AutoPilot, Azure Active Directory (AAD). [11]

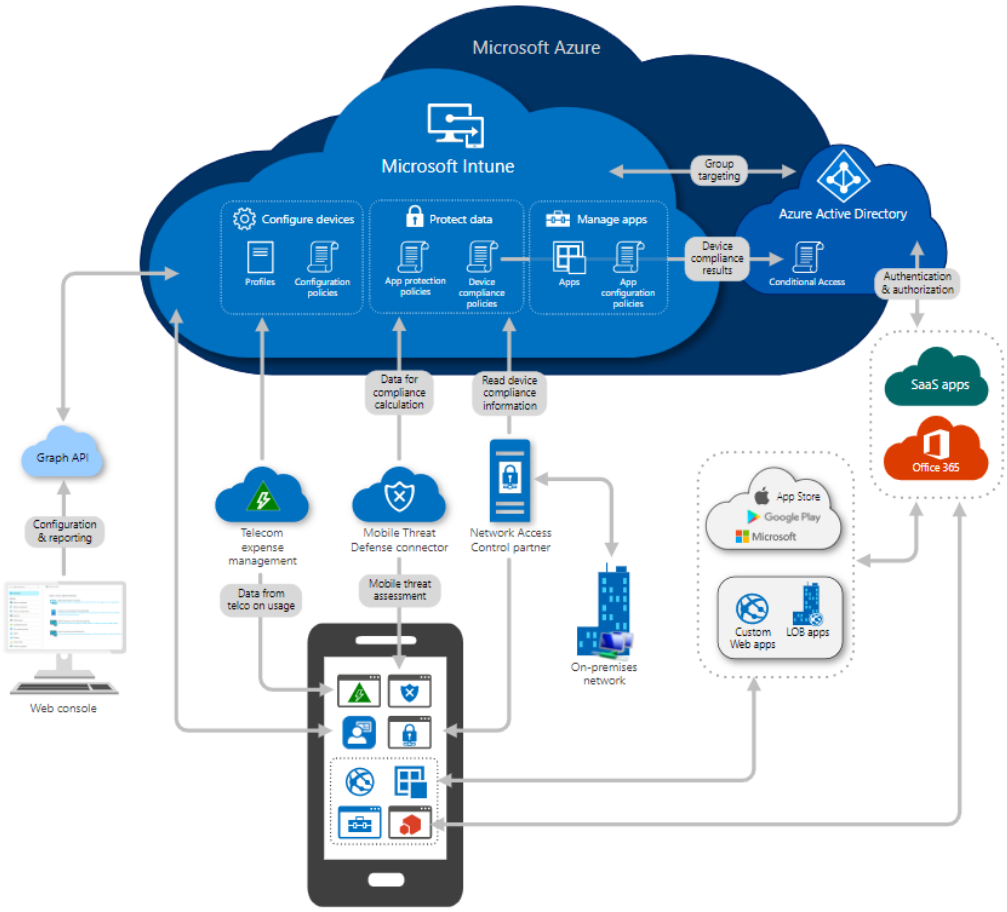


Figura 8. *Integración de los servicios de Microsoft. [11]*

3.1.2.1. Servicios utilizados

Para poder gestionar las herramientas descritas a continuación, es necesaria una cuenta con roles de administrador o global o de Intune y una licencia de Microsoft.

- ***Microsoft Intune.-*** Es una plataforma de administración unificada de dispositivos móviles (MDM) y aplicaciones móviles (MAM) basada en la nube. Administra el acceso de los usuarios y, mediante configuraciones de perfiles y directivas, administra también dispositivos móviles (MDM) y aplicaciones (MAM). Además, Intune se integra con otras herramientas de seguridad y administración de Microsoft, como Microsoft Endpoint Manager y Microsoft Defender ATP, ofreciendo así una solución completa de administración y seguridad de dispositivos. [12]

- ***Microsoft Intune admin center.-*** Es un servicio que integra Microsoft Configuration Manager y Microsoft Intune. Proporciona un interfaz web que permite a los administradores IT realizar todas las tareas de gestión y administración de dispositivos y aplicaciones móviles desde una ubicación centralizada y con una gestión simplificada. [13]

- ***Intune connector.-*** El conector de Intune es el que establece la conexión entre el directorio activo del dominio local y la parte en la nube del directorio activo de Azure. Microsoft recomienda, por seguridad, instalar el conector en un equipo distinto al controlador de dominio (DC). Además, los requisitos para poder llevar a cabo la instalación y puesta en marcha de este son un usuario con rol de Administrador o global o de Intune, que la cuenta desde la que se realiza este sincronizada en el Active Directory global, una licencia de Microsoft y que el equipo en el que se instala tenga permisos para crear objetos informáticos dentro del dominio, por lo que habrá que delegarle esos controles desde el DC. Es una herramienta clave para permitir la administración y protección de dispositivos móviles en entornos empresariales. En el *Anexo* se pueden ver los pasos a seguir para llevar a cabo su instalación de forma correcta. [14]

- ***Windows AutoPilot.-*** Es un conjunto de tecnologías que se utilizan para configurar y preconfigurar dispositivos Windows, preparándolos para un uso productivo. En lugar de tener que configurar manualmente cada dispositivo, Windows AutoPilot permite que los dispositivos se configuren y se entreguen automáticamente a los usuarios finales, lo que reduce el tiempo y los costes de administración de dispositivos. Los dispositivos, al ser desempaquetados y encendidos por los usuarios, se van a configurar automáticamente con todas las políticas y aplicaciones empresariales relevantes. Para tener operativo este servicio, es necesario que el conector de Intune este instalado y enrolado. De esta forma se consigue que los equipos inscritos por AutoPilot, se vean reflejados en el dominio local del directorio activo. [15]

- ***Azure Active Directory (AAD).-*** Se trata de un servicio de directorio de identidad y acceso basado en la nube de Microsoft que proporciona gestión de identidades y autenticación para aplicaciones y servicios en la nube. Ayuda a los empleados a acceder a recursos externos, como Microsoft 365 y a recursos internos de la red corporativa de una forma simplificada. También permite a las organizaciones controlar y administrar el acceso a los recursos empresariales, aplicar políticas de seguridad, gestionar el acceso a las aplicaciones y servicios, y automatizar la gestión de identidades. [16]

El “denominador común” que tienen todos estos servicios es el de gestionar y administrar los dispositivos (MDM) y/o aplicaciones (MAM).

3.1.3. Entorno Windows

Al ser el principal entorno en el que se lleva a cabo el proyecto, es necesario definir los siguientes términos, ayudando así a comprender las arquitecturas de las que más adelante se va a hablar.

- ***Domain controller (DC).-*** Un controlador de dominio es un servidor de red que, de manera centralizada, gestiona un dominio Windows. Proporciona el almacenamiento físico para la base de datos de Servicios de dominio de Active Directory (AD DS), además de proporcionar los servicios y los datos que permiten a las empresas administrar de manera eficaz sus servidores, usuarios y aplicaciones. Es una parte fundamental de la infraestructura de red de las organizaciones. [17]

- ***Unidad organizativa (OU) de un directorio activo.-*** Es la herramienta que permite agrupar lógicamente objetos como cuentas de usuario, de servicio o de equipo. Cada unidad organizativa tiene su propia estructura jerárquica, ayudando a mejorar la coordinación y colaboración entre los diferentes grupos de empleados. Además, se pueden asignar administradores a unidades organizativas específicas y también se pueden delegar controles a otros servidores para que puedan crear objetos. [18]

- ***Directorio Activo (AD) de Windows.-*** Es el término que usa Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadoras. Es una herramienta de gestión de identidades que permite a los administradores de IT organizar y gestionar todos los elementos de una red informática (ordenadores, grupos, usuarios, dominios, políticas de seguridad, y cualquier tipo de objetos definidos para el usuario). Proporciona facilidades como la de poder gestionar y administrar los elementos mediante políticas de grupo (GPOs), verificar las autenticaciones de los usuarios y controlar los equipos registrados en el dominio.
  En esencia, el Directorio Activo es una base de datos que almacena información sobre los objetos de la red. Esta información se utiliza para controlar el acceso a los recursos y para aplicar políticas de seguridad en la red. [19][20]

- ***Azure AD Connect.-*** Se trata de una aplicación local de Microsoft diseñada para empresas híbridas que hace el papel de conectar la parte local con la parte en la nube. Es decir, es una herramienta que ayuda a las organizaciones a extender su Directorio Activo local a la nube de Azure. Está configurado en un solo sentido, es decir, los objetos que se crean en local se sincronizan con la nube, pero no del revés. Los usuarios que son creados en el *Directorio Activo* (local) se sincronizan a través del AD Connect y de esta forma pasan a formar parte de la nube. Sin embargo, si se crea un usuario en la nube, no hay configurado ningún conector que sincronice esa información con el *Directorio Activo*, por lo que esos usuarios no van a poder iniciar sesión en los equipos gestionados por la empresa.

El tipo de inicio de sesión de los usuarios se configura en el AD Connect y puede ser de autenticación en la nube, sincronización de hash de contraseña o autenticación local con federación con AD FS. [21]

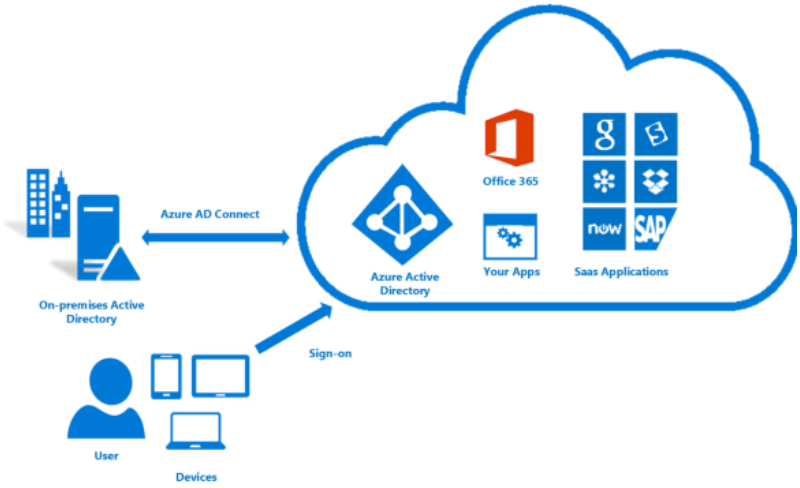


Figura 9. *Conexión de los servicios de Microsoft. [21]*

Siguiendo las recomendaciones de seguridad de Microsoft, el conector debe estar en un servidor distinto al controlador de dominio y que, como mínimo, este sea Windows Server 2012. Además, es necesaria una licencia de Microsoft para poder usar esta herramienta.

- ***Servicio de Federación de Directorio Activo (AD FS).-*** Es un servicio que se encarga de la gestión federada de identidad y de la administración del acceso. Permite que los usuarios puedan iniciar sesión en los servicios de la nube de Microsoft con las credenciales que usan en la red local. Además, con la gestión de la identidad federada, no hace falta que los usuarios autentiquen su identidad en cada aplicación.
  Cuando se inicia sesión en uno de los servicios, el usuario es redirigido a su instancia local de AD FS y la autenticación la verifican los controladores de dominio, es decir, se genera un inicio de sesión que es validado localmente. Además, se puede establecer el AD FS Proxy de forma complementaria, añadiendo así capas de seguridad adicionales a la implementación del AD FS y permitiendo que los usuarios puedan iniciar sesión desde una red externa. Lo que hace es redirigir la petición de autenticación que ha tenido lugar en una red externa al AD FS local, atravesando el firewall (si es que lo hay) y después hace el mismo proceso descrito antes. [22]

3.2. Funcionalidades

A continuación, se van a detallar más en profundidad las funcionalidades implementadas durante el desarrollo de este proyecto.

3.2.1. MDM y MAM

Los softwares Mobile Device Management (MDM) y Mobile Application Management (MAM) son la base fundamental para el desarrollo de la gestión y administración de dispositivos y aplicaciones, siendo por eso fundamentales para llevar a cabo el proyecto. Ambos se utilizan para administrar y proteger dispositivos móviles, pero difieren en su enfoque y funcionalidades. [23]

El software MDM se encarga de proteger, monitorizar y administrar dispositivos, independientemente del proveedor, personalizando así el dispositivo para un entorno empresarial. Es especialmente útil para empresas que necesitan gestionar y administrar muchos dispositivos, ya que permite a los administradores de IT realizar cambios en múltiples dispositivos de forma remota. [24]

Por otro lado, el software MAM es el que se encarga de controlar y asegurar las aplicaciones, estando por eso más enfocado para dispositivos personales. Permite a los administradores de IT controlar qué aplicaciones están disponibles en los dispositivos de los usuarios y el cifrado de datos. Este software es útil para empresas que permiten a sus usuarios utilizar dispositivos personales para acceder a aplicaciones y datos de la empresa, ya que permite gestionar las aplicaciones empresariales de forma separada de las personales.

La arquitectura que hace que funcione el servicio de MDM en los dispositivos gestionados se basa en instalar un agente en cada uno de ellos (esto ocurre de forma automática al inscribir el dispositivo en Intune) y en configurar una base de datos en Intune en la que se va a almacenar toda la información recogida, quedando así guardada en la nube (pertenece a Microsoft).

Figura 10. *Arquitectura MDM básica de Microsoft Intune*

El servidor de Intune es el encargado de establecer las directivas y configuraciones requeridas por el administrador y el agente se autentica con este para recibir las actualizaciones y las nuevas configuraciones. Para que se pueda dar la conexión, el dispositivo debe tener conexión a la red.

Resumiendo, los softwares MDM y MAM permiten, de forma remota, administrar dispositivos de la empresa y/o aplicaciones, así como aplicar políticas o forzar ciertas opciones de seguridad, siendo por esto una herramienta crucial para las empresas que buscan gestionar de manera eficiente todos sus dispositivos móviles.

3.2.2. Autenticación

El registro de dispositivos en Azure AD es un requisito previo para llevar a cabo la autenticación basada en la nube. Normalmente, se realiza una unión de los dispositivos a Azure AD o a Azure AD híbrido para completar su registro.

La autenticación de un dispositivo es el proceso de seguridad que se lleva a cabo para verificar la identidad de un dispositivo en una red, garantizando que está autorizado para acceder a los recursos de esta.

La autenticación a través del AD FS permite un inicio de sesión gestionado localmente por la empresa y Microsoft lo que hace es redirigir las peticiones al AD FS local o al AD FS Proxy, por lo que hay que hacer una distinción entre inicio de sesión desde una red interna y desde una red externa. [25]

3.2.2.1. Interna

Esta autenticación se da cuando un dispositivo intenta iniciar sesión y está dentro de la red local de la empresa. La petición de inicio de sesión llega al AD FS y este pregunta al controlador de dominio (DC) si las credenciales introducidas corresponden a algún usuario ya registrado. En caso de ser así, se va a verificar su identidad y el AD FS autentica al usuario que ha intentado iniciar sesión.

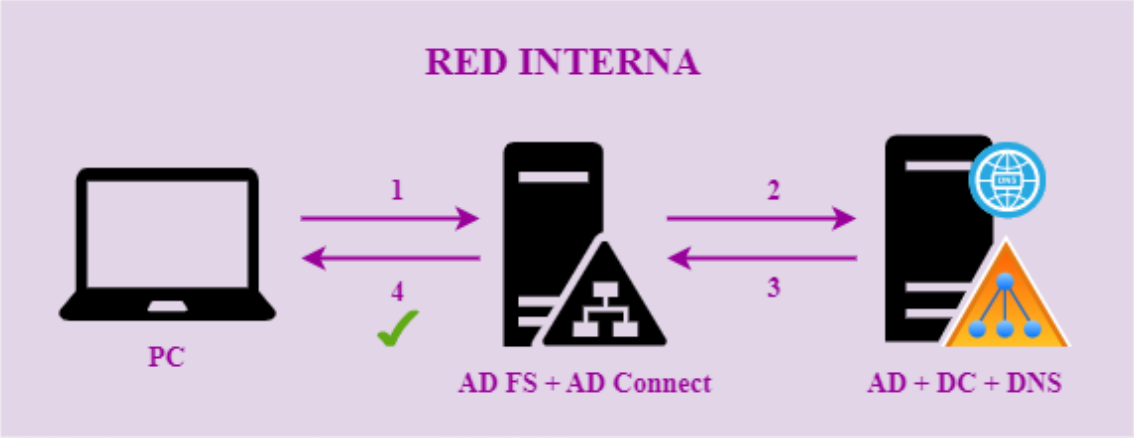


Figura 11. *Autenticación desde red interna*

3.2.2.2. Externa

A diferencia del caso anterior, esta se da cuando un dispositivo intenta iniciar sesión desde una red externa. Un claro ejemplo sería el de un PC intentando iniciar sesión en el portal de Office365 encontrándose en una red externa. Cuando el PC intenta el inicio de sesión, el portal Office detecta que la cuenta introducida forma parte del dominio de una empresa, redirigiéndolo así al AD FS Proxy y pasando antes por el Firewall de la organización (si es que tiene). El AD FS Proxy comprueba si las credenciales introducidas son correctas, y en caso de ser así, redirige esa petición de inicio de sesión al AD FS local, pasando otra vez por el firewall y llegando hasta el controlador de dominio. Una vez llegado a este punto, se repite el proceso de autenticación interna explicado antes. Es decir, el inicio de sesión se autentica de manera local y, en este caso, se usa a Microsoft como "intermediario".

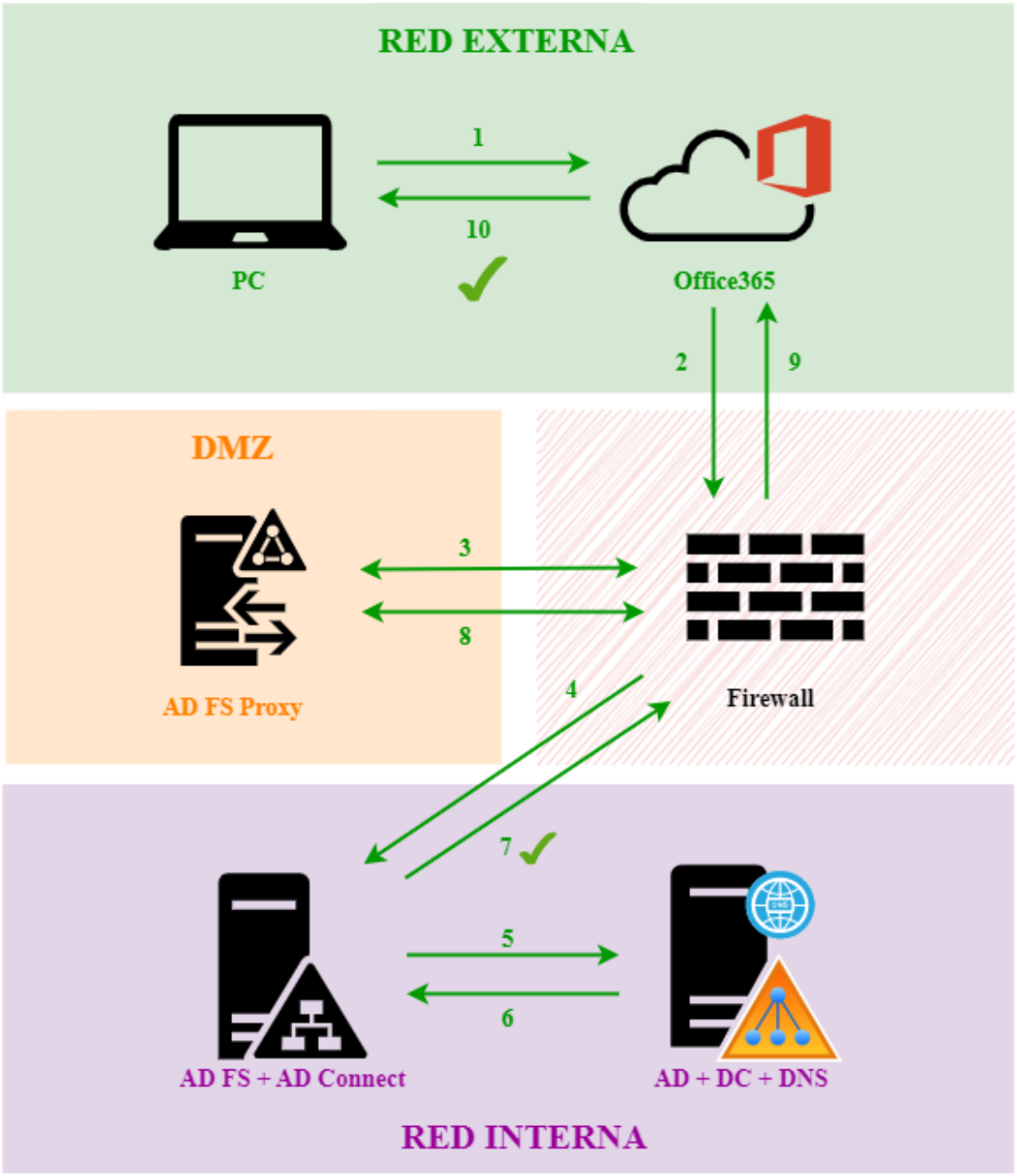


Figura 12. *Autenticación desde red externa*

3.2.3. Inscripción de dispositivos

La inscripción de dispositivos es el proceso de registrar y conectar un dispositivo a un sistema o plataforma específica, como por ejemplo a un servidor.

Es un proceso que establece una relación entre el usuario, el dispositivo y el servicio Microsoft Intune. Inscribir un dispositivo le permite a este acceder a los recursos internos de la empresa, siendo por esto muy utilizado en entornos empresariales que buscan asegurar que los dispositivos utilizados por los empleados son seguros y que cumplen con los requisitos de la organización. [26]

Microsoft Intune, junto con Azure AD, proporcionan un proceso seguro y simplificado para registrar e inscribir los dispositivos que desean acceder a los recursos internos.

Durante la inscripción, Intune instala un certificado MDM en el dispositivo de inscripción. Este certificado se comunica con el servicio Intune y le permite así empezar a aplicar las directivas de la organización (directivas de inscripción y cumplimiento y perfiles de configuración).

Hay varios métodos para inscribir los dispositivos. Cada método depende de la propiedad del dispositivo (personal o corporativo) y del tipo de dispositivo (Windows, iOS o Android). Esto se detallará más adelante. Además, hay que distinguir entre inscripción en entornos híbridos y en entornos en la nube. [27]

3.2.3.1. Entornos híbridos

Un entorno híbrido es aquel que cuenta tanto con AD local como con Azure AD. La inscripción se puede dar de dos formas distintas, una en la que el dispositivo se inscriba desde una red externa y otra en la que el dispositivo se inscriba desde una red interna.

- **Dispositivo en red externa.**

Cuando un dispositivo se encuentra en una red externa, como es el caso del PCA en la Figura 13, y se inscribe mediante Intune, se produce una sincronización y se crea el objeto en el Azure AD y en Intune. Además, al ser un entorno híbrido, la petición pasa por el firewall y va hacia el servidor (que como mínimo tiene que ser Windows Server 2012) en el que se encuentra el conector de Intune. Este es el que tiene los controles, delegados por el DC, y crea el objeto de tipo equipo en la unidad organizativa permitida, en el Directorio Activo local. De esta forma, se tiene el dispositivo tanto en la nube como en local.

- **Dispositivo en red interna.**

En este tipo de inscripción, el papel que realiza el Azure AD Connect es muy importante. El proceso que se da es el siguiente. Al registrar un dispositivo en el Directorio Activo local (como el PCB en la Figura 13) en el controlador de dominio, este crea un objeto de tipo equipo. Esa información, además, le llega al AD Connect y la sincroniza con el Azure AD (nube), pasando por el firewall de la empresa. Sin embargo, los equipos no se van a ver reflejados en el centro de administración de Microsoft Intune hasta que no se realice el enrolado.

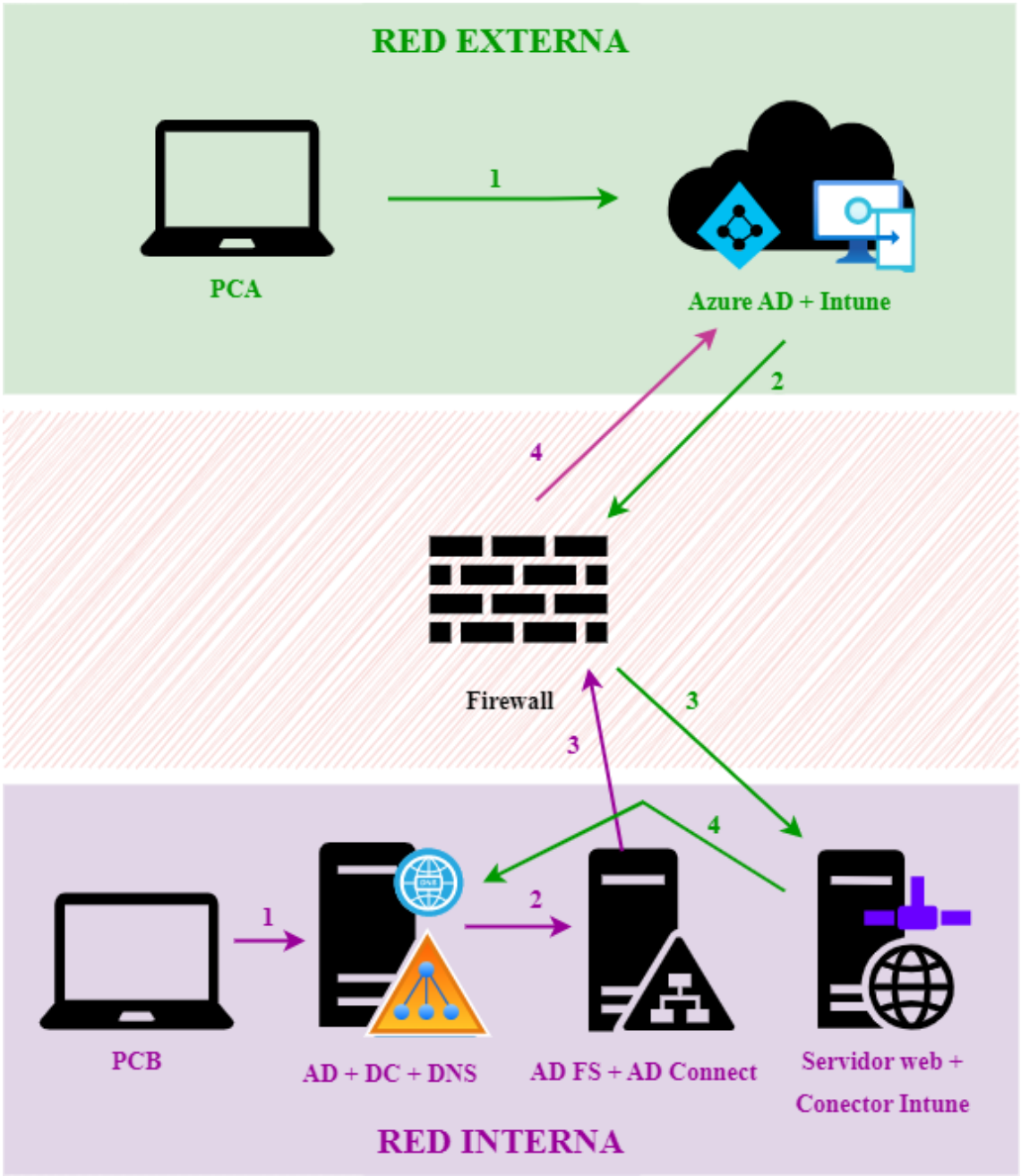


Figura 13. *Inscripción dispositivos en entorno híbrido*

3.2.3.2. Entornos en la nube

Este proceso se da en los dispositivos que son inscritos directamente en la nube, desde una red externa y que sólo tienen presencia en el directorio activo de Azure AD y en el Microsoft Intune admin center. Es por esto por lo que todas las configuraciones y políticas se deben implementar desde ahí, al no tener presencia en el dominio local.

Cuando se inicia sesión con una cuenta de empresa en un equipo con los valores de fábrica, este pasa a estar en el Directorio Activo de Azure y si la organización además dispone de Microsoft Intune, este podrá verse también reflejado en el centro de administración de Intune.

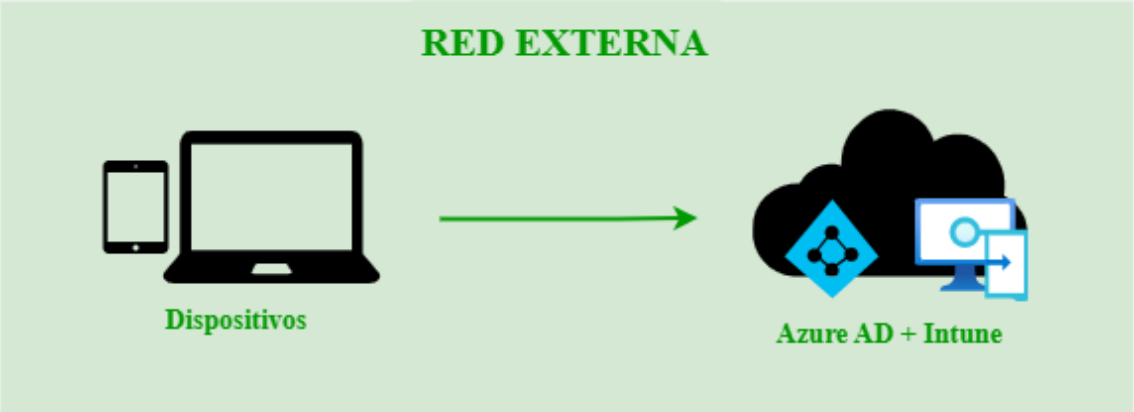


Figura 14. *Inscripción dispositivos en la nube*

3.3. Conceptos

3.3.1. Dispositivos registrados en Azure AD

El objetivo de los dispositivos registrados en Azure AD es el de permitir a los usuarios acceder a los recursos de la organización con un dispositivo personal (BYOD). Los dispositivos BYOD (Bring Your Own Device) son dispositivos personales de los empleados que además usan para realizar tareas laborales.

Es decir, los dispositivos registrados en Azure AD son dispositivos que han sido registrados en Azure AD sin necesitar una cuenta de la organización para iniciar sesión en el dispositivo. [28]

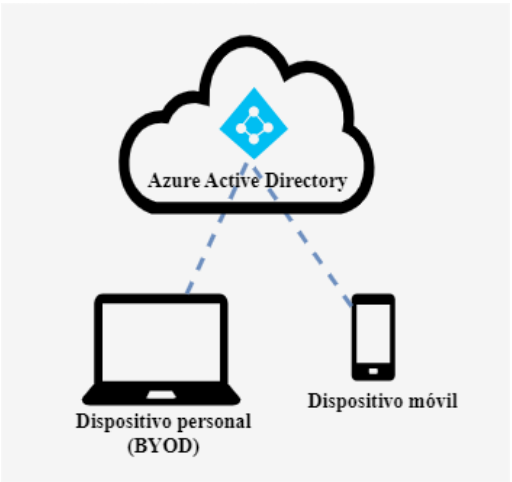


Figura 15. *Escenario de dispositivos registrados en Azure AD*

3.3.2. Dispositivos unidos a Azure AD

Son dispositivos propiedad de la organización unidos solo a Azure AD que necesitan una cuenta de la organización para poder iniciar sesión en el dispositivo. El acceso a los recursos de estos dispositivos se puede controlar en función de la cuenta de Azure AD y de las directivas de acceso condicional aplicadas al dispositivo. Aun así, pueden autenticarse en los servidores locales como archivo, impresión y otras aplicaciones.

Con un dispositivo unido a Azure AD, los usuarios cuentan con inicio de sesión único para las aplicaciones de la nube en el entorno, esto es posible gracias al token de actualización principal, el cual se va a detallar más adelante. [29]

Figura 16. *Escenario de dispositivos unidos a Azure AD*

3.3.3. Dispositivos híbridos unidos a Azure AD

Son dispositivos propiedad de la organización unidos tanto al AD local como a Azure AD que requieren una cuenta de la organización para iniciar sesión en el dispositivo. [30]. El aprovisionamiento de estos dispositivos (preparar el equipo con sus configuraciones, programas…) puede ser por:

- Unión a un dominio por IT y unión automática (a través de Azure AD Connect o del AD FS)
- Unión a un dominio por Windows AutoPilot y unión automática (a través de Azure AD Connect o del AD FS)

Figura 17. *Escenario de dispositivos híbridos unidos a Azure AD*

3.3.4. Tokens de actualización principales

Un token de actualización principal (PRT) es un tipo de token de autenticación utilizado en Microsoft Intune. Es un elemento clave de autenticación de Azure AD en dispositivos Windows 10 o versiones posteriores, iOS y Android. Se trata de un token JSON Web (JWT) emitido especialmente con el fin de habilitar el inicio de sesión único (SSO) en las aplicaciones usadas en los dispositivos.

Un PRT se emite durante la autenticación del usuario en un dispositivo. Si el dispositivo está unido a Azure AD o a Azure AD híbrido, cuando un usuario inicia sesión con sus credenciales de la organización, se emite un PRT durante el inicio de sesión. En cambio, en un dispositivo registrado de Azure AD, se emite un PRT cuando un usuario agrega una cuenta de trabajo secundaria a su dispositivo. Una vez emitido, un PRT es válido durante 14 días y se renueva continuamente siempre y cuando el usuario use activamente el dispositivo.

Sin embargo, el PRT solo se emite y se renueva durante la autenticación de aplicaciones nativas, no lo hace durante una sesión del explorador. Además, este token puede ser revocado en cualquier momento si se sospecha de actividades maliciosas. [31]

4. Despliegue

En este apartado del trabajo se describen los procedimientos llevados a cabo para desplegar los servicios de Microsoft Intune admin center en los dispositivos con los sistemas operativos Microsoft Windows e iOS/iPadOS.

4.1. Escenario práctico

El proyecto, como ya se ha mencionado antes, ha tenido lugar en dispositivos de la empresa consultora CYC, con objetivo de, en un futuro, poder implantar estos servicios en sus clientes. Es por esto por lo que el escenario práctico en el que se ha llevado a cabo es en el entorno híbrido de la empresa (cuenta con red interna, DMZ, Firewall y red externa). Este se puede ver en la Figura 18.

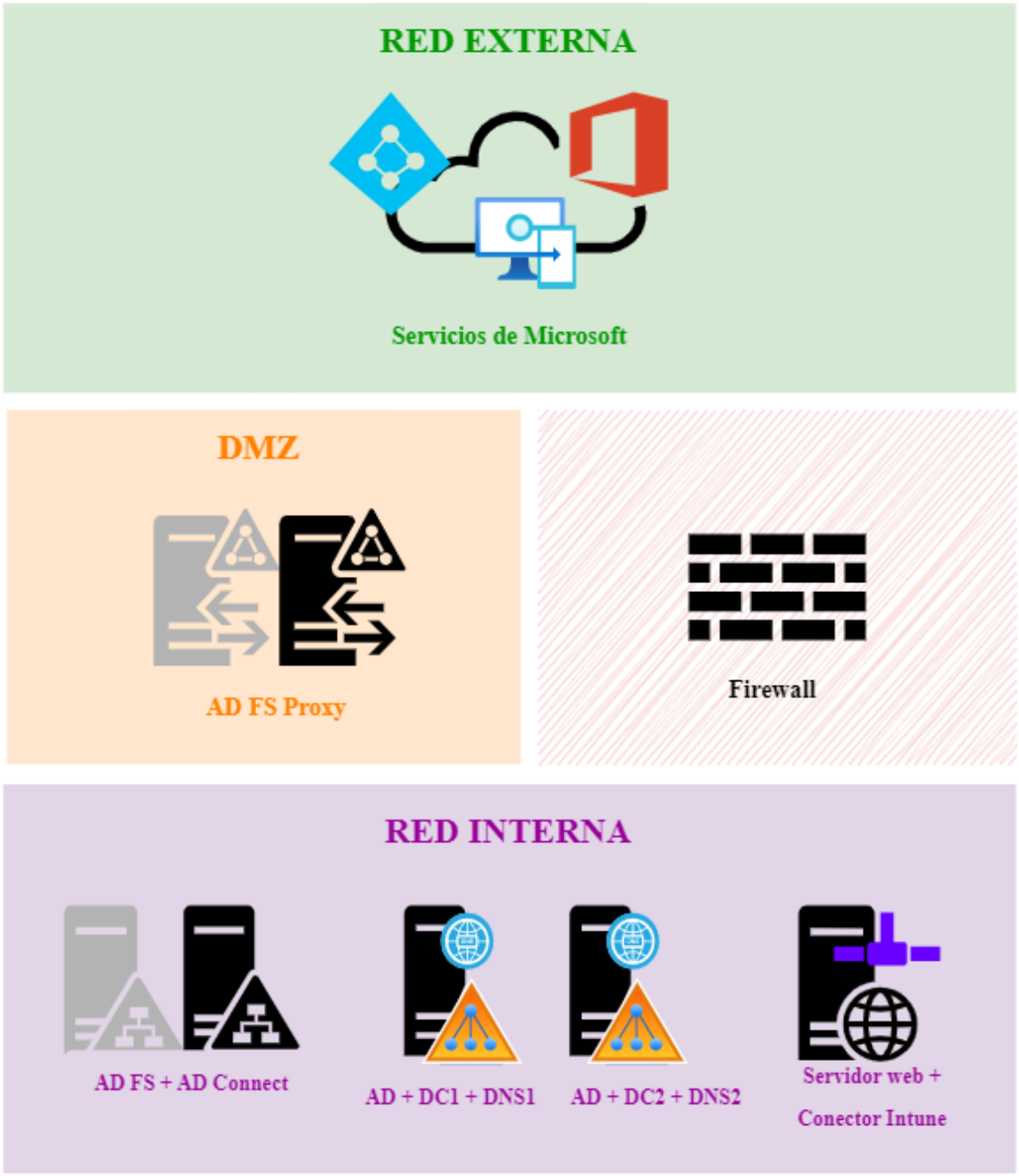


Figura 18. *Escenario práctico. Entorno híbrido de la empresa*

4.1.1. Red interna

En la red interna, como se puede ver en la Figura 18, se tienen dos controladores de dominio con sus respectivos DNS, para poder hacer consultas en el directorio activo. En ellos, por recomendaciones de seguridad de Microsoft, no puede haber otros servicios implementados. Además, el hecho de que haya dos controladores de dominio es debido a que de esta forma se consigue tener un sistema más robusto y seguro.

Se tienen también dos servidores para el AD Connect y el AD FS local y otro en el que está instalado el conector de Intune, que es el encargado de sincronizar los datos creados en la nube con la parte local. Este último servidor, tiene que ser, como mínimo, Windows Server 2012 y, además, se le tienen que haber delegado los controles necesarios

para poder crear y administrar objetos de tipo equipo en local. Este proceso está detallado en el apartado *Anexos* del proyecto. Excepto uno de los controladores de dominio, el resto de los servidores mencionados son máquinas virtuales.

Uno de los dos servidores que se usan para el AD Connect y el AD FS trabaja en *staging mode* (modo provisional). Con este modo se consigue alta disponibilidad, permite probar e implementar nuevos cambios de configuración y la posibilidad de introducir un nuevo servidor para dar de baja el antiguo. Un servidor en modo provisional está activado para la importación y sincronización, pero no realiza ninguna exportación. Cuando se deshabilita este modo del servidor es cuando se iniciará la exportación. [32]

4.1.2. DMZ

La zona desmilitarizada (DMZ) es una red que se encuentra entre la red interna y la externa de la organización que se utiliza para proporcionar una capa adicional de seguridad. Sirve como una zona intermedia que separa los servidores públicos accesibles desde Internet de los recursos privados de la red interna. Su objetivo principal es proteger la red interna de posibles ataques, limitando los accesos que provienen desde la red externa y, a su vez, facilitar el acceso de la red interna a la externa. [33]

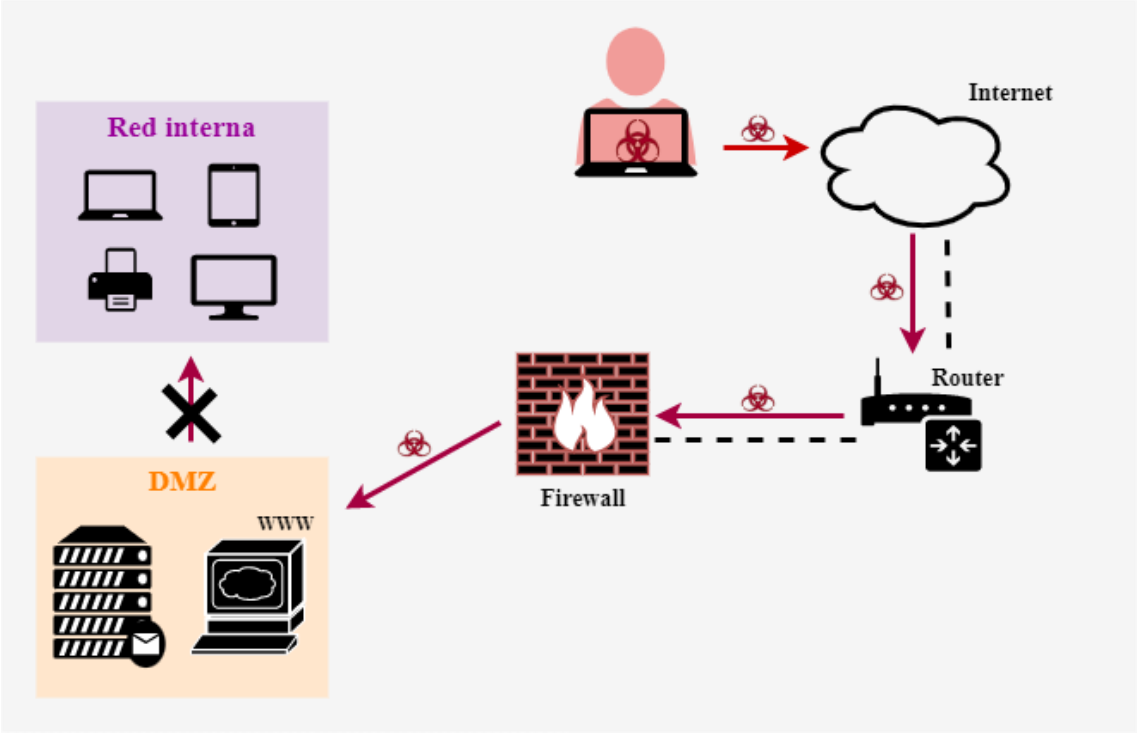


Figura 19. *Ejemplo de ataque evitado por la DMZ*

4.1.3. Firewall

El firewall es un elemento de seguridad de la red que se encarga de monitorizar el tráfico entrante y saliente y es el encargado de decidir si permitir o bloquear un tráfico específico, en función de las restricciones de seguridad que tenga configuradas. Es decir, realiza un proceso de filtrado del tráfico de red no deseado. La empresa cuenta con un entorno híbrido, por lo que por él pasa todo el flujo de datos y peticiones, como pueden ser los inicios de sesión, la inscripción de usuarios… siendo por esto muy importante el papel que realiza. [34]

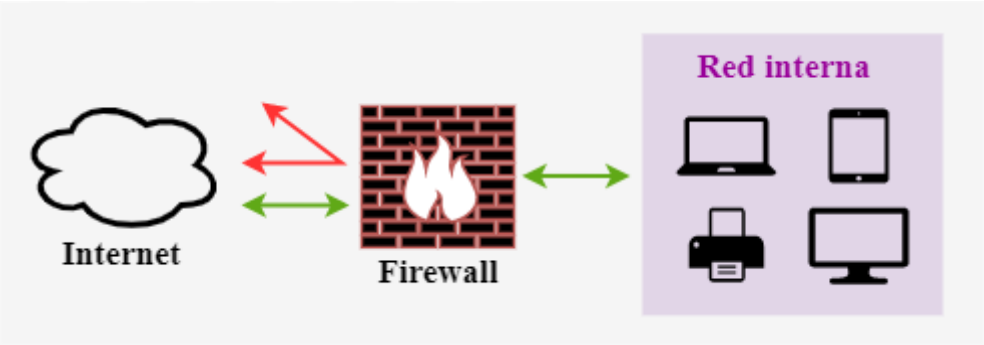


Figura 20. *Labor del Firewall*

4.1.4. Red externa

En la red externa es donde se encuentra Internet, así como los servicios que proporciona Microsoft.

4.2. Terminología

En este apartado se van a definir las terminologías necesarias para entender el despliegue del proyecto.

4.2.1. Directiva de cumplimiento

Una directiva de cumplimiento es una solución que ofrece el software MDM para proteger los datos de la organización, exigiendo a los usuarios y dispositivos que cumplan ciertos requisitos. Define las reglas y configuración que los usuarios y los dispositivos administrados deben cumplir para estar conformes e incluyen las acciones que se le aplicarán cuando esto no sea así. La configuración de las directivas se hace directamente desde el Centro de administración de Microsoft Intune. [35]

Microsoft recomienda una serie de directivas de cumplimiento en función del nivel de seguridad deseado y del sistema operativo. [36]

- ***Nivel 1.-*** Nivel de cumplimiento mínimo del dispositivo.
- ***Nivel 2.-*** Configuración de cumplimiento de dispositivos mejorada.
- ***Nivel 3.-*** Configuraciones avanzadas de cumplimiento de dispositivos.

Un dispositivo que no cumple una directiva se verá como dispositivo *no conforme* en el Centro de administración de Intune y se le aplicarán las acciones que hayan sido programadas cuando se dé ese caso, como por ejemplo bloquear o borrar los datos corporativos.

Se pueden combinar con el acceso condicional (en el siguiente punto se detallará), ya que la conformidad de un dispositivo depende de forma directa con el cumplimiento de las directivas y, por tanto, el acceso condicional va a estar completamente ligado.

Además, se puede configurar el momento en el que el dispositivo queda como *no conforme*, influyendo por tanto en el acceso condicional ya que cuando un dispositivo está marcado como *no conforme* se le puede bloquear el acceso hasta que vuelva a estarlo.

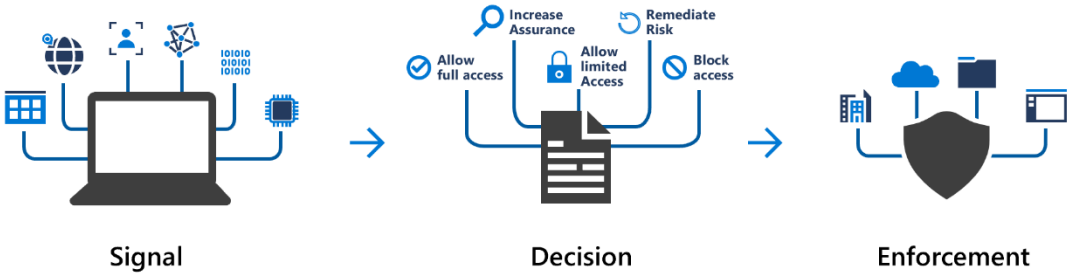


Figura 21. *Decisiones tomadas en función de las señales reunidas por el acceso condicional para aplicar las directivas de cumplimiento. [36]*

4.2.2. Acceso condicional

El acceso condicional es una funcionalidad de Azure AD que se incluye con una licencia de Azure AD Premium. Su propósito es ayudar a controlar el acceso a datos de la empresa identificando señales concretas como son el estado del dispositivo, la ubicación de la IP, el usuario… que llevarían a tomar una decisión u otra. En otras palabras, permite, bloquea el acceso y/o establece criterios adicionales de control, como puede ser la doble autenticación.

Con Intune se pueden usar dos tipos de directivas de Acceso Condicional: el Acceso Condicional basado en dispositivos y el Acceso Condicional basado en aplicaciones. El Acceso Condicional basado en dispositivos determina si un dispositivo cumple los requisitos de configuración y seguridad esperados, mientras que el Acceso Condicional basado en aplicaciones se encarga de asegurar que solo las aplicaciones administradas puedan acceder al correo electrónico corporativo u otros servicios de Microsoft 365.

Sin embargo, no es una funcionalidad pensada para usar como primera línea de defensa, su enfoque está más centrado en hacer de pasarela de acceso a los recursos corporativos, mejorando la seguridad de estos. Además, su uso proporciona respuestas automatizadas en función de las señales del entorno recibidas. Esas respuestas se pueden aplicar a usuarios, dispositivos y/o grupos de ellos, por lo que puede ser muy útil para programar distintas opciones como consecuencia de una señal. [37]

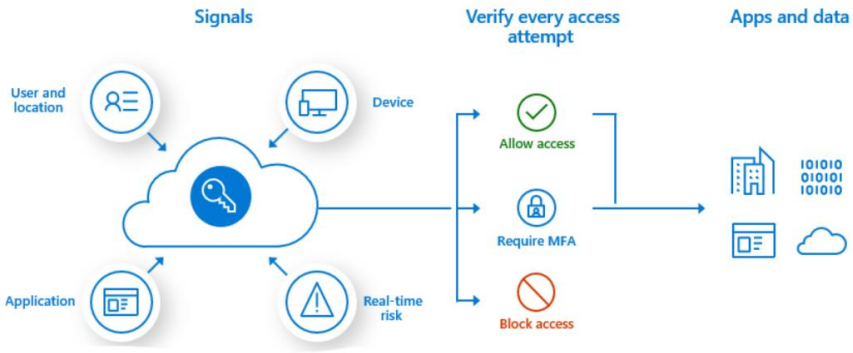


Figura 22. *Funcionamiento del Acceso Condicional. [37]*

4.2.3. Perfil de configuración

Un perfil de configuración permite agregar y ajustar configuraciones para luego insertarlas en dispositivos de la organización. En un perfil se pueden "personalizar" las configuraciones en función de las características deseadas, ya sea a través de plantillas administrativas, líneas base (en dispositivos Windows) o catálogo de configuración. Los perfiles de configuración se pueden asignar a usuarios, dispositivos y/o grupos de ellos.

Las plantillas contienen grupos de valores, organizados por funcionalidad y el catálogo de configuración permite empezar de cero una configuración siguiendo la biblioteca de valores disponibles. Una línea base es un grupo de opciones de configuración ya preconfigurado que ayuda a implementar una configuración de Windows recomendada por Microsoft. Al crear un perfil de líneas base de seguridad en Intune, realmente lo que se está creando es una plantilla que consta de varios perfiles de configuración de dispositivos. [38]

4.2.4. Análisis de directivas de grupo (GPOs)

El *Análisis de directiva de grupo* es una herramienta de Microsoft Intune que permite analizar los objetos de directiva de grupo (GPO) locales y determinar el nivel de compatibilidad con la administración moderna. La autenticación moderna es una combinación de métodos de autenticación, autorización y algunas medidas de seguridad que dependen de las directivas de acceso. Además, a través de esta herramienta se pueden importar las políticas de grupo usadas en local a la nube, por lo que puede llegar a ser muy interesante para las organizaciones con entornos híbridos que busquen pasar a un entorno completamente en la nube.

Figura 23. *Ejemplo de preparación para la migración de la directiva de grupo*

Para poder importar las políticas de grupo, aplicadas en el AD local, al centro de administración de Microsoft Intune, se deben exportar en formato *.xml*. Como se puede ver en la Figura 23, la herramienta proporciona el porcentaje de nivel de compatibilidad, pudiendo ver así qué partes se pueden migrar a la nube. Además, al migrar las GPOs, se generan informes del estado de las asignaciones. En esos informes se detalla cómo las GPO afectan en la experiencia del usuario, su compatibilidad con Intune y, además,

incluyen recomendaciones para resolver los conflictos de configuración para asegurar que las GPO se integran correctamente con Intune. [39]

4.3. Gestión de dispositivos

A la hora de gestionar un dispositivo hay que seguir una serie de procesos que, además, requieren una planificación previa en función de qué necesite o qué se busque con el dispositivo.

Se empieza eligiendo el tipo de inscripción a realizar. En el caso de los dispositivos Windows, al contrario que en dispositivos Android o iOS/iPadOS, el tipo de inscripción no influye en la propiedad de estos ya que todas las inscripciones están dirigidas para equipos de propiedad empresarial. El tipo de inscripción, en este caso, se refiere a la metodología empleada para registrar el dispositivo. Después, se crearán y se le aplicarán las directivas de configuración deseadas para mantener el dispositivo conforme, incluyendo la seguridad requerida en cada caso. Y, por último, se le aplicará un perfil de configuración en función de las configuraciones y características que se le quieran dar al dispositivo, aplicando una configuración segura en él.

Figura 24. *Procesos para gestionar un dispositivo*

4.3.1. Dispositivos Microsoft Windows

En este apartado se describen los pasos y algunos ejemplos prácticos llevados a cabo para gestionar y administrar dispositivos Windows.

- **Tipos de inscripción.**

Como ya se ha mencionado antes, en dispositivos Windows, el tipo de inscripción no influye en la propiedad del dispositivo, por lo que solo se refiere al método empleado para inscribirlo. Los dos tipos de inscripción más comunes son la inscripción automática y la inscripción AutoPilot.

- **Inscripción automática**

Esta opción de inscripción une el dispositivo con Azure Active Directory (Azure AD) y permite que los usuarios inicien sesión en Windows con sus credenciales de Azure AD. Además, con la inscripción automática habilitada, el dispositivo se va a inscribir automáticamente en Intune. La ventaja de esta inscripción es que es que, para el usuario, es un proceso de un solo paso. El dispositivo inscrito queda marcado en Intune como un dispositivo de propiedad corporativa.

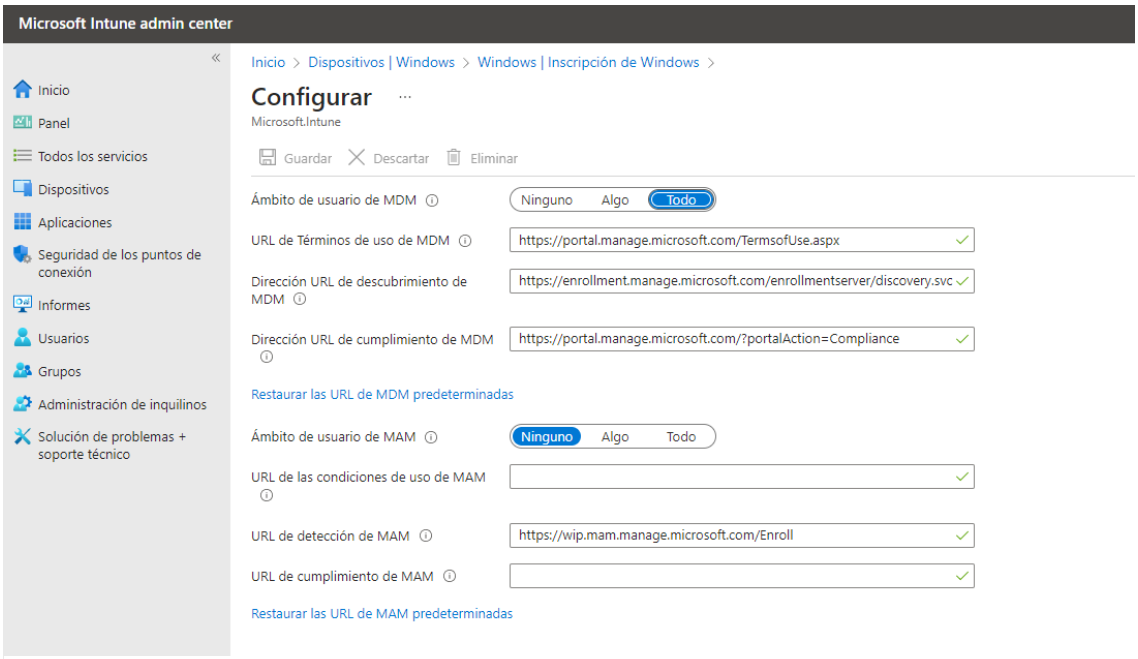


Figura 25. *Configuración predeterminada para realizar la inscripción automatizada*

En la Figura 25 se puede ver la configuración predeterminada por Intune para habilitar la inscripción automática en el inquilino. Se puede limitar esta inscripción a los usuarios deseados asignando esta configuración solo al grupo concreto de ellos.

Sin embargo, este tipo de inscripción cuenta con dos problemas, uno de ellos por estar ante un entorno híbrido. Como se ha explicado antes, el escenario práctico en el que se ha llevado a cabo el proyecto cuenta tanto con parte local como con parte en la nube por lo que los dispositivos inscritos de esta forma únicamente se van a ver reflejados en la nube. Esto es así porque el conector Azure AD está configurado solo en sentido "ascendente". Es decir, los objetos creados en local se sincronizan con la nube, pero no se sincronizan en local si se crean en la nube.

El otro problema que existe es que, por defecto, el primer usuario que inicia sesión en el dispositivo se convierte automáticamente en administrador de este. Sin embargo, esto se puede evitar creando un grupo de usuarios al que se le asigna el rol de administradores locales. Y, añadiendo ese grupo a un perfil de configuración de tipo personalizado, en el que habrá que introducir el parámetro SID (Security Identifier) del grupo creado, se consigue que solo los usuarios deseados por la organización sean administradores locales. [40]

- **Inscripción AutoPilot**

La inscripción AutoPilot automatiza la unión a Azure AD e inscribe nuevos dispositivos corporativos en Intune. A diferencia de la inscripción automática, ofrece la opción de configurar el rol (administrador o usuario) del usuario que inicia sesión, por lo que desaparece el problema de que el primer usuario que inicie sesión en el dispositivo se convierta en administrador de este. [41]

Para poder llevar a cabo este tipo de inscripción, se necesita tener el dispositivo ya registrado en el centro de administración de Intune como dispositivo AutoPilot.

El registro de un dispositivo con Windows AutoPilot lo realiza o el Fabricante de Equipo Original (OEM) o el revendedor o el distribuidor al que se le compra el dispositivo, ya que la idea de este tipo de inscripción es para configurar y preconfigurar dispositivos nuevos. Sin embargo, es posible registrar el dispositivo de forma manual para los casos en los que el dispositivo es una máquina virtual, es un dispositivo ya existente o en los que el dispositivo se obtuvo de un fabricante o revendedor no participantes.

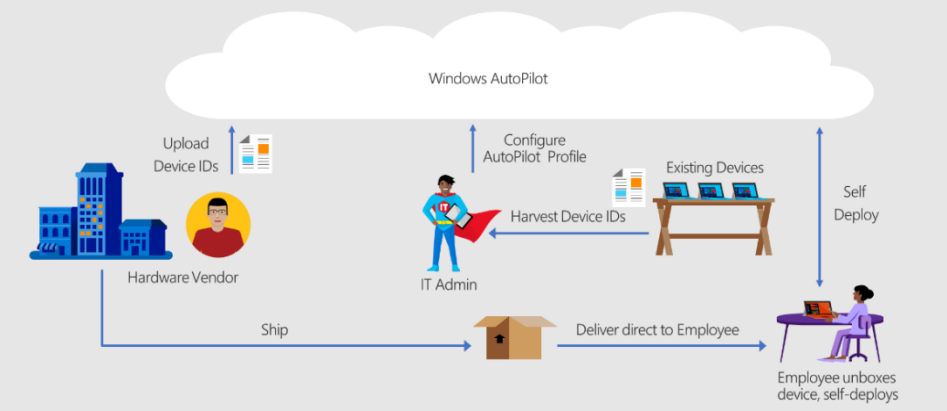


Figura 26. *Diagrama registro dispositivos Windows AutoPilot nuevos y existentes. [41]*

El registro manual se realiza importando el hash de hardware del dispositivo en formato *.csv*. El hash se puede obtener poniéndose en contacto con el proveedor o a través de Windows PowerShell, aunque esta última opción está más pensada para escenarios de prueba y evaluación, al ser necesario arrancar el dispositivo para llevarla a cabo. A continuación, se muestran los comandos PowerShell para obtener el hash. [42]

```
PowerShell

New-Item -Type Directory -Path "C:\HWID"
Set-Location -Path "C:\HWID"
$env:Path += ";C:\Program Files\WindowsPowerShell\Scripts"
Set-ExecutionPolicy -Scope Process -ExecutionPolicy RemoteSigned
Install-Script -Name Get-WindowsAutopilotInfo
Get-WindowsAutopilotInfo -OutputFile AutopilotHWID.csv
```

Figura 27. *Comandos desde un símbolo del sistema de Windows PowerShell con privilegios elevados para obtener el hash del ordenador*

Una vez se tiene el hash importado, solo hay que iniciar sesión en el dispositivo y seguir los pasos que este indique, quedando así inscrito en Microsoft Intune. En caso de querer eliminar o dar de baja un dispositivo, además de formatearlo habrá que borrar el hash de Intune, ya que, si no se elimina, el dispositivo seguirá formando parte de la organización por tener registrado el hash.

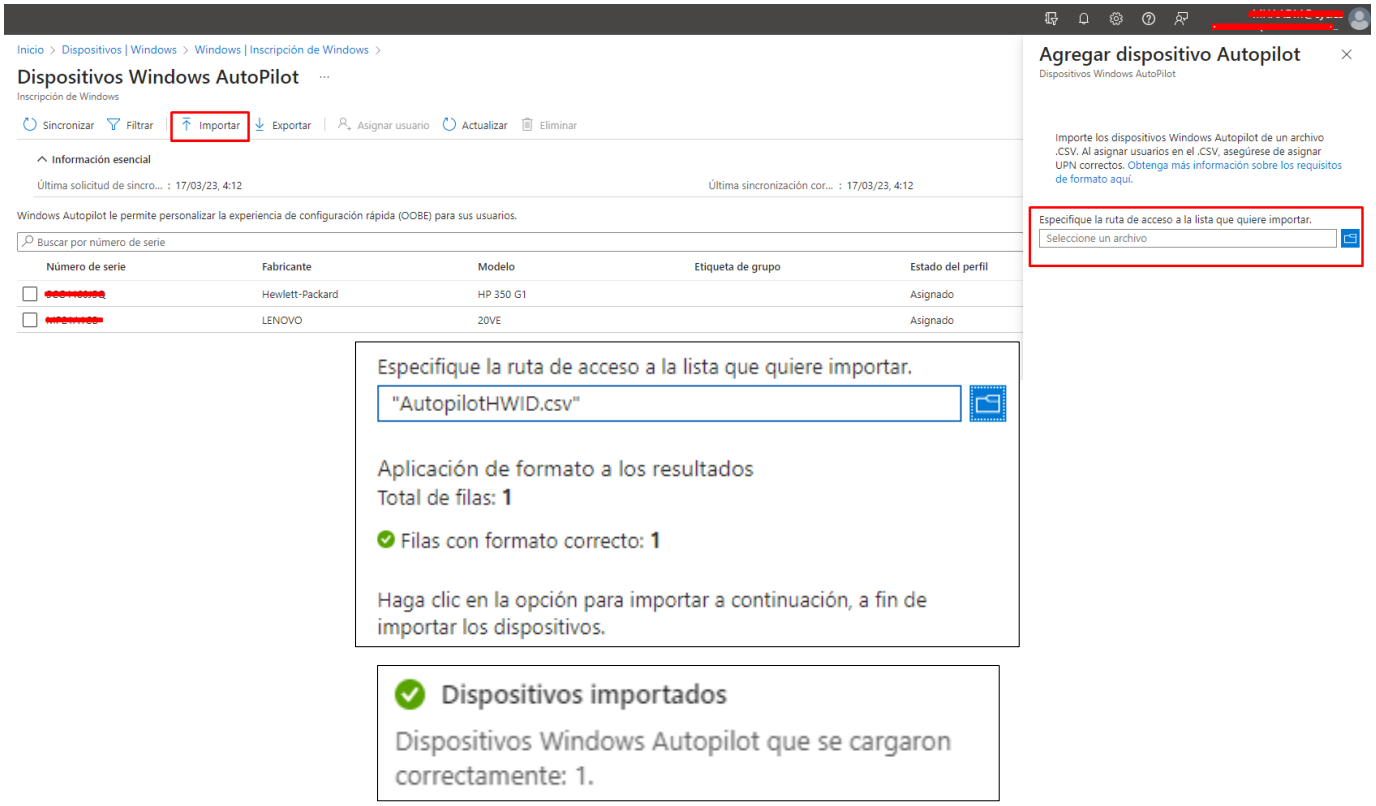


Figura 28. *Ejemplo agregar dispositivo AutoPilot por su hash*

En escenarios híbridos, se necesita tener instalado el conector de Intune y con los controles delegados para crear objetos de tipo equipo en la unidad organizativa (OU), para que el dispositivo se vea reflejado también en el directorio activo local (se especificará más adelante, pero además es necesario aplicarle al dispositivo un perfil de implementación del tipo unión a un dominio).

- **Directivas de cumplimiento.**

Como se ha explicado antes, las directivas de cumplimiento ayudan a proteger los datos de la organización exigiendo a los usuarios y dispositivos que cumplan algunos requisitos.

Las reglas que definen las características que deben cumplir los dispositivos y las acciones que se llevaran a cabo en caso de que no sea así se definen en la configuración de las directivas. Requerimientos de contraseñas, de fondos de pantalla, de sistema operativo, cifrado del disco duro y Microsoft Defender son algunos ejemplos de directivas que se pueden aplicar en dispositivos con sistema operativo Microsoft Windows.

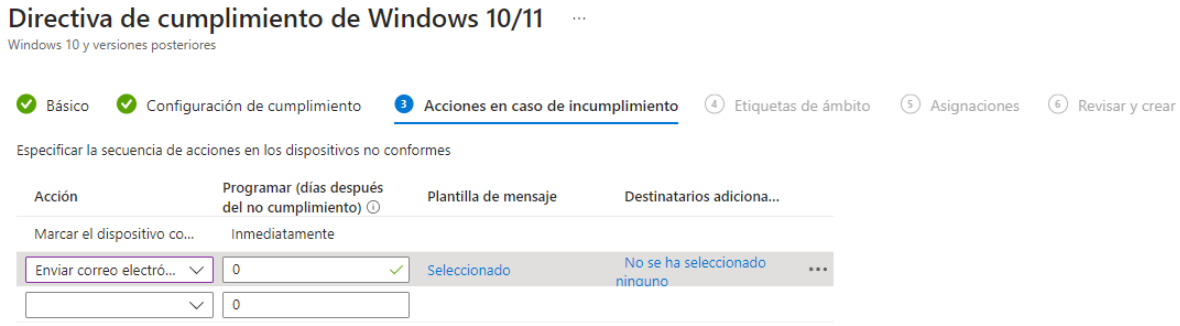


Figura 29. *Ejemplo creación directiva de cumplimiento*

Las directivas de cumplimiento se implementan en grupos de dispositivos o usuarios. Cuando se implementa en los usuarios, cualquier dispositivo en el que el usuario inicie sesión debe cumplir los requisitos de las directivas.

Algunas de las acciones por incumplimiento que se pueden llevar a cabo son el bloqueo remoto del dispositivo y el envío de un correo electrónico o notificaciones al dispositivo o usuario sobre el problema de cumplimiento, para que un usuario del dispositivo pueda volver a ponerlo en cumplimiento.

Como se puede ver en la Figura 29, cuando se elige como acción el envío de un correo electrónico, se puede añadir un destinatario adicional al usuario, como por ejemplo el administrador IT. El texto del correo se configura a través de una plantilla de mensaje, la cual se puede configurar desde el centro de administración de Intune, siguiendo la ruta especificada en la Figura 30.

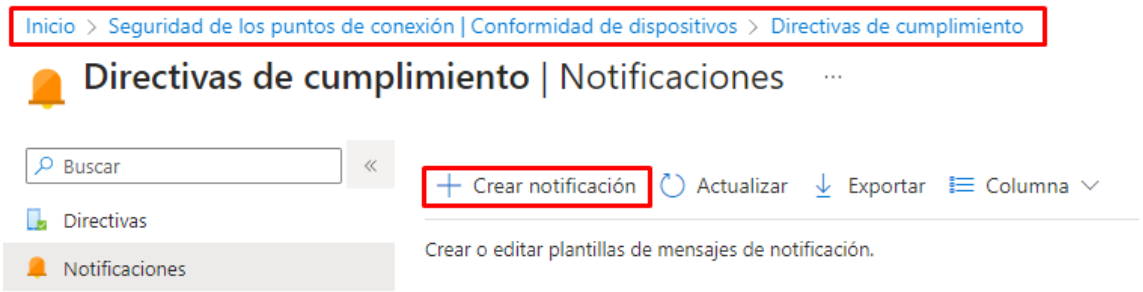


Figura 30. *Ejemplo creación plantilla de mensaje*

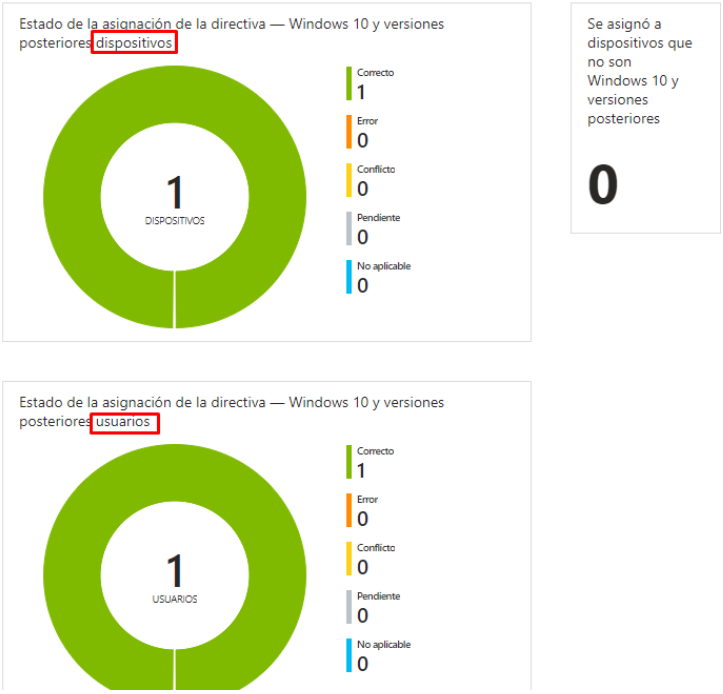


Figura 31. *Estado de la asignación de la directiva creada como prueba, diferenciando entre dispositivo y usuario*

Dispositivo	Nombre principal del usuario	Estado de cumplimiento	Última actualización de estado
TEST-INTUNE1	Cuenta del sistema	Conforme	21/03/2023 2:57
NA-PORT103	MHA@cyc.es	Conforme	21/03/2023 8:29

Figura 32. *Información estado del dispositivo*

Los usuarios pueden hacer un seguimiento de los requisitos establecidos por la organización a través de la aplicación *Portal de Empresa* y en caso de no cumplir con la directiva asignada, pueden seguir los pasos que se indican en ella para corregirlo.

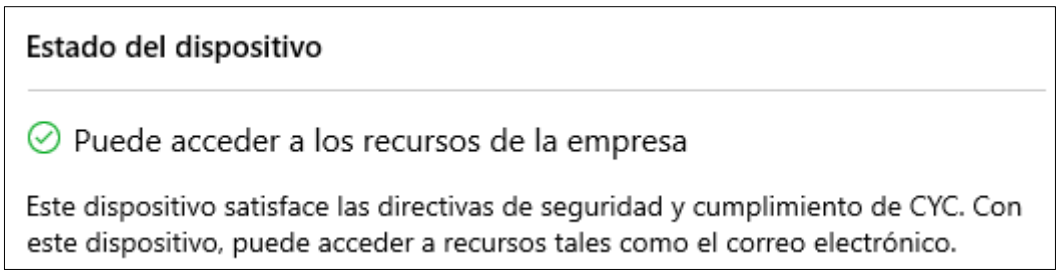


Figura 33. *Información sobre el estado del dispositivo proporcionada por la aplicación Portal de Empresa a un dispositivo conforme*

A modo de ejemplo práctico, se creó una nueva directiva de cumplimiento que exigía a los dispositivos Windows a los que fue asignada la versión 11 del sistema operativo y como acción en caso de incumplimiento se eligió el envío de un correo electrónico. Se aplicó esta directiva en uno de los dispositivos de prueba con sistema operativo Windows 10 y, como era de esperar, el dispositivo quedó como no conforme.

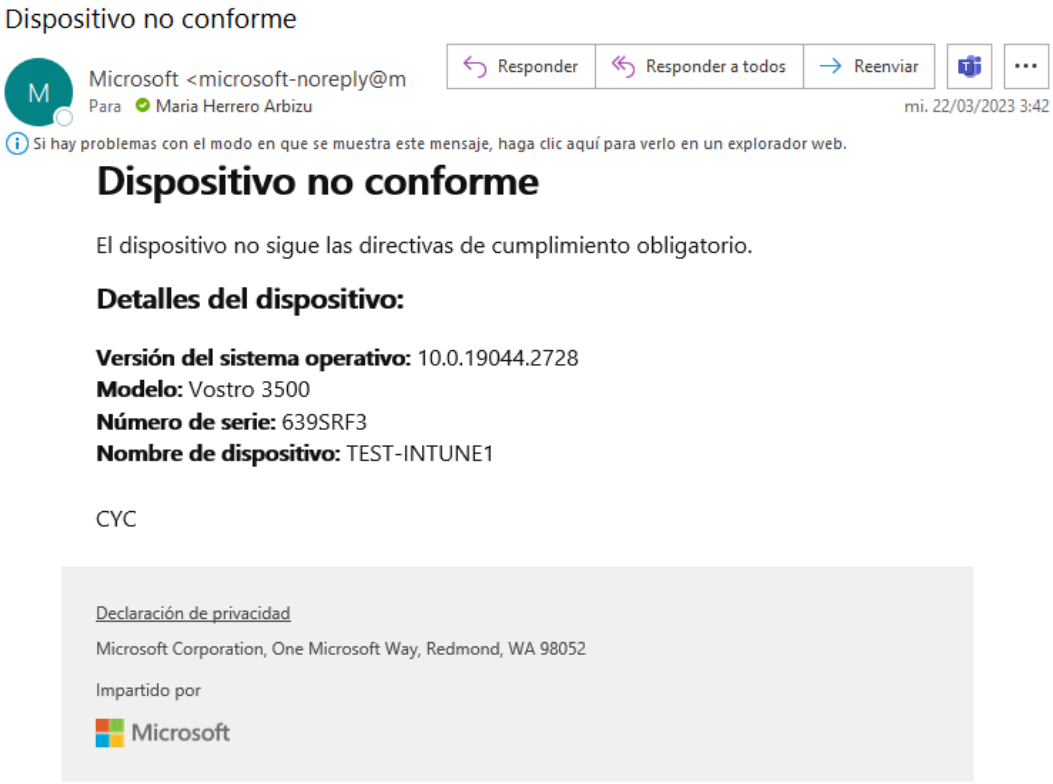


Figura 34. *Correo recibido como acción por incumplimiento de la directiva de versión mínima del sistema operativo*

Nombre del dispositivo	Administrado por	Propiedad	Cumplimiento	SO	Versión del SO
TEST-INTUNE1	Intune	Organización	No conforme	Windows	10.0.19044.2728

Figura 35. *Estado de un dispositivo en Intune que no cumple una directiva de cumplimiento*

Además, como se ha mencionado antes, desde la aplicación *Portal de Empresa*, se puede hacer un seguimiento de los requisitos establecidos por la organización y, en caso de no cumplir una directiva, seguir los pasos que se indican en ella para remediarlo.

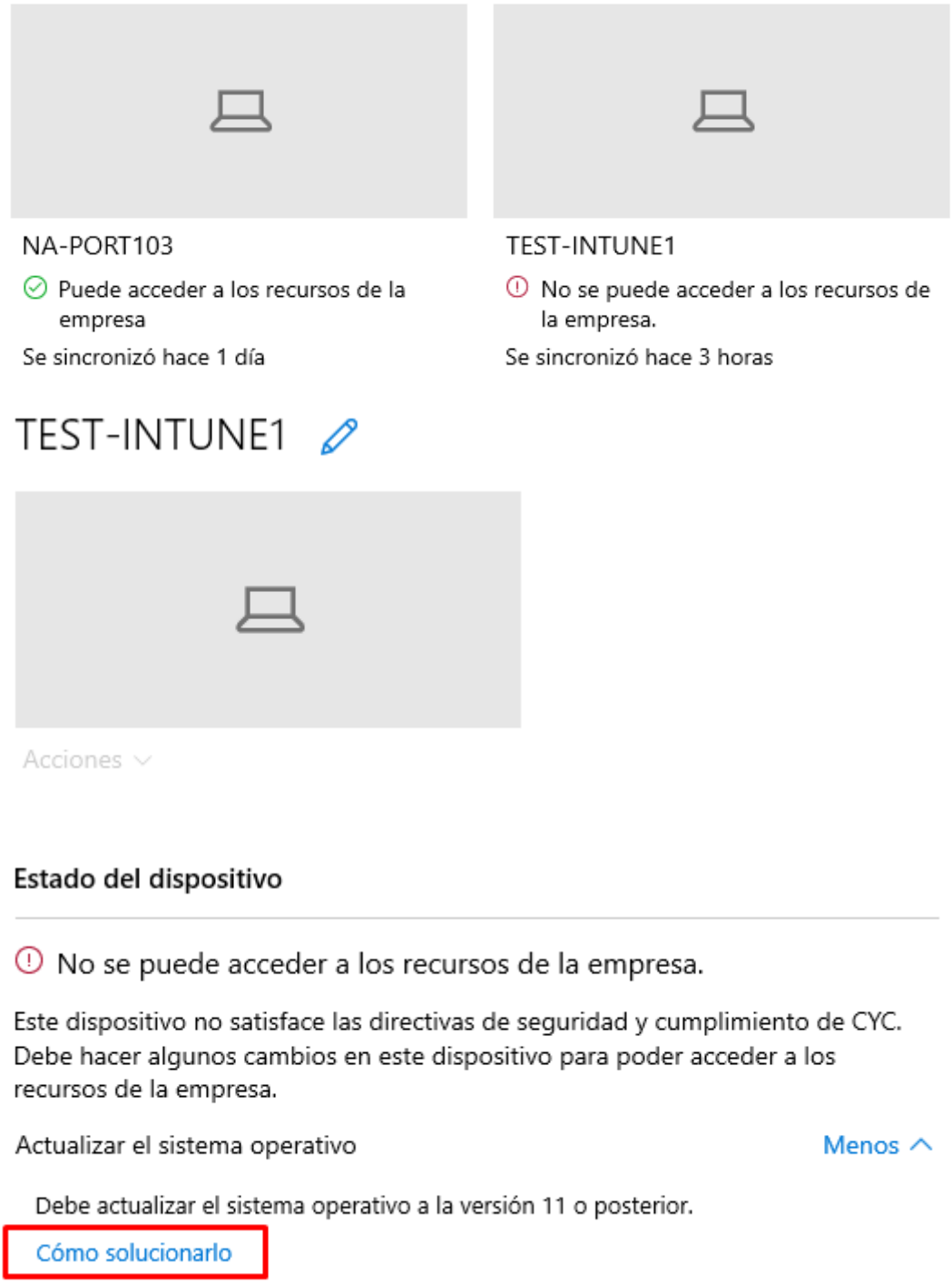


Figura 36. *Captura de pantalla de la aplicación Portal de Empresa sobre el ejemplo práctico de conformidad de dispositivos*

- **Perfiles de configuración.**

Como se ha explicado antes, un perfil de configuración permite agregar y ajustar configuraciones para poder insertarlas en los dispositivos de una organización. En dispositivos Windows, además de las plantillas administrativas y el catálogo de configuración, disponibles también los demás sistemas operativos, se dispone de las líneas base. Estas ayudan a tener un flujo de trabajo seguro de un extremo a otro cuando se trabaja con Microsoft 365. Algunas de ellas son líneas base de seguridad (para Windows 10 y versiones posteriores), líneas base de Microsoft Defender para punto de conexión, líneas de base de Microsoft Edge y líneas base de seguridad de Windows 365. [43]

A continuación, se van a detallar algunos de los ejemplos prácticos llevados a cabo aplicando perfiles de configuración desde Intune en los dispositivos de prueba.

- **Fondos de pantalla**

Con el fin de aplicar el mismo fondo de escritorio y bloqueo a todos los dispositivos de una organización de forma única y rápida, se probó a realizar esta opción de configuración.

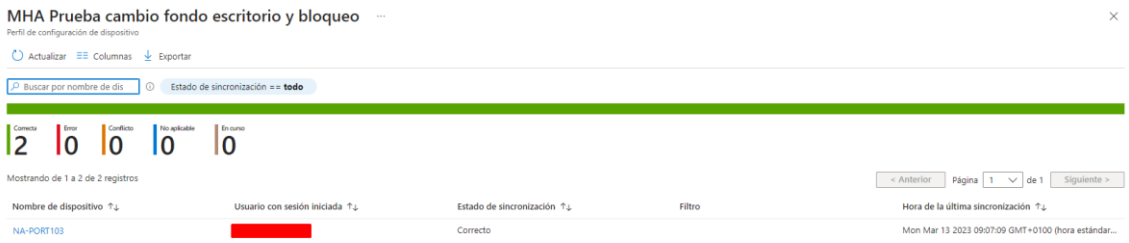


Figura 37. *Estado de protección del usuario y del dispositivo*

En la imagen anterior se puede ver el estado de protección del usuario y del dispositivo que se genera cuando se les aplica un perfil de configuración. En él se puede ver el nombre del dispositivo, el usuario que ha iniciado sesión, el estado y la hora de la última sincronización.

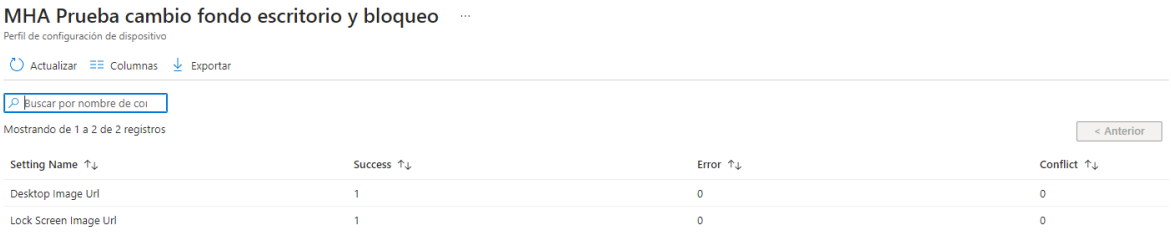


Figura 38. *Estado por ajuste de protección del usuario y del dispositivo*

Además, como se puede ver en la Figura 37, el resultado de la prueba fue exitoso entre los dispositivos de la prueba, siendo posible ver el estado de configuración de cada ajuste en todos los dispositivos y usuarios para la directiva creada.

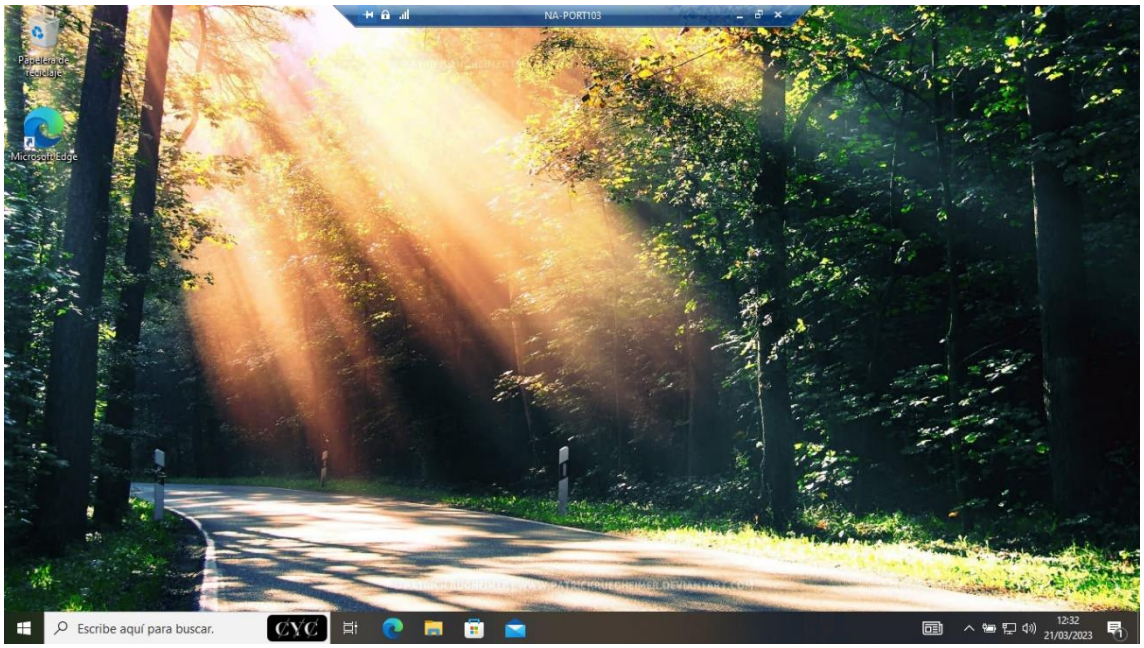


Figura 39. *Resultado práctico tras establecer el fondo de pantalla deseado desde Intune*

- **Modo quiosco**

Los dispositivos Windows 10/11 se pueden configurar para que se ejecuten en modo pantalla completa, ya sea de una o varias aplicaciones. Es decir, es posible configurar y gestionar el *modo quiosco* en un dispositivo Windows desde Intune. [44]

Intune distingue entre perfiles en modo pantalla completa de una sola aplicación, como un explorador web o una aplicación de la Tienda, y en perfiles en modo pantalla completa de varias aplicaciones, en los que se van a ejecutan varias aplicaciones en el dispositivo. Estas aplicaciones son las únicas aplicaciones que el usuario va a poder abrir por lo que, si una aplicación tiene una dependencia en otra aplicación, hay que añadir ambas aplicaciones a la lista de aplicaciones permitidas.

Esta prueba se llevó a cabo con el fin de poder ofrecer este servicio en unos meses a uno de los clientes de la empresa consulta. El objetivo de este quiosco era permitir el acceso únicamente a las aplicaciones Microsoft Edge (navegador), Microsoft Teams, Microsoft Word y Microsoft PowerPoint. Además de no permitir cambiar de usuario ni apagar el dispositivo. Es decir, se quería configurar un equipo de sala al que cualquiera pudiese acceder, pero con ciertas restricciones configuradas previamente.

Se empezó creando un grupo de tipo asignado al que se añadieron los dispositivos Windows de prueba (previamente inscritos y enrolados en Intune) a los que se quería incorporar esta configuración. Además, para poder ejecutar dichas aplicaciones en el dispositivo, es necesario que estén instaladas previamente en este. A modo de anécdota, las primeras veces que se intentó realizar esta prueba, el equipo estaba recién formateado, por lo que no tenía ninguna aplicación instalada. Entonces, al aplicarle la configuración de quiosco, las aplicaciones aparecían como cuadrados vacíos y, además, no ocurría nada cuando se pinchaba sobre ellas, por lo que se vio que era necesario instalar las

aplicaciones en el dispositivo previamente. La gestión de aplicaciones desde Intune está explicada en el apartado 4.4 de este proyecto.

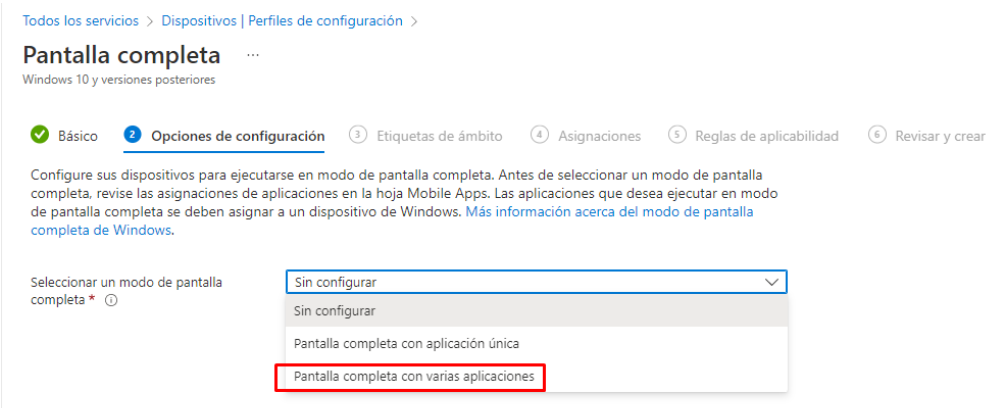


Figura 40. *Selección modo quiosco con varias aplicaciones*

Para crear el perfil de configuración de quiosco y poder ejecutar aplicaciones Win32 (método en el que por defecto se programan todas las aplicaciones) se necesita especificar en el perfil la ruta de acceso directo local del archivo ejecutable (.exe) de la aplicación y el modelo del usuario de la aplicación (AUMID) para la aplicación.

El AUMID se puede obtener a través de la aplicación Windows PowerShell (como administrador) ejecutando el comando *get-startapps*.

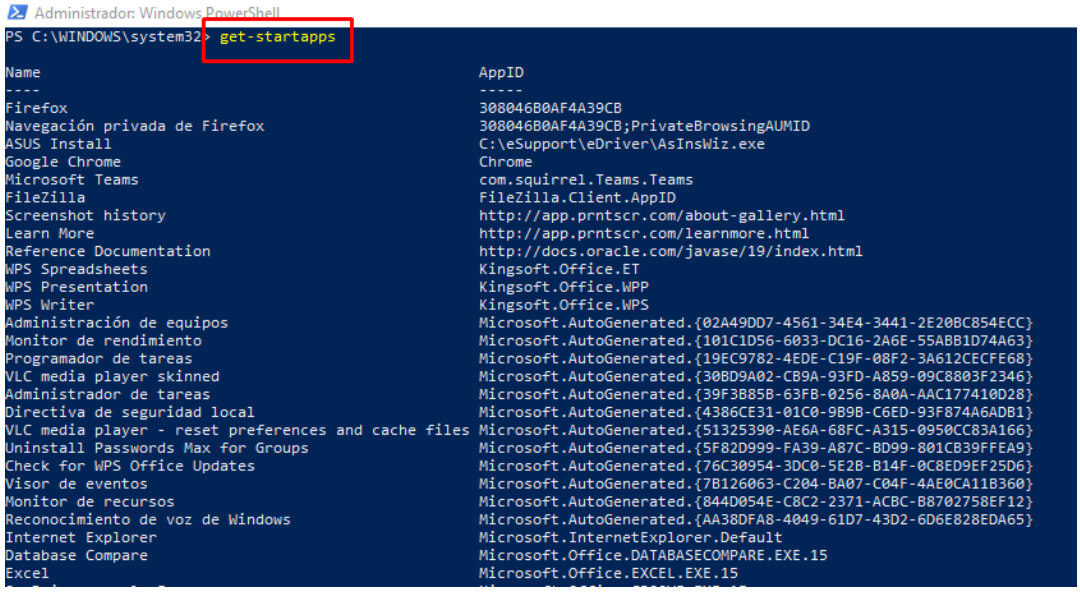


Figura 41. *Ejemplo ejecución del comando PowerShell para obtener el AUMID de las aplicaciones*

Además, se creó y asignó al mismo grupo otro *perfil de configuración* a través del cual se bloquean las opciones de cambio de usuario y apagado del dispositivo.

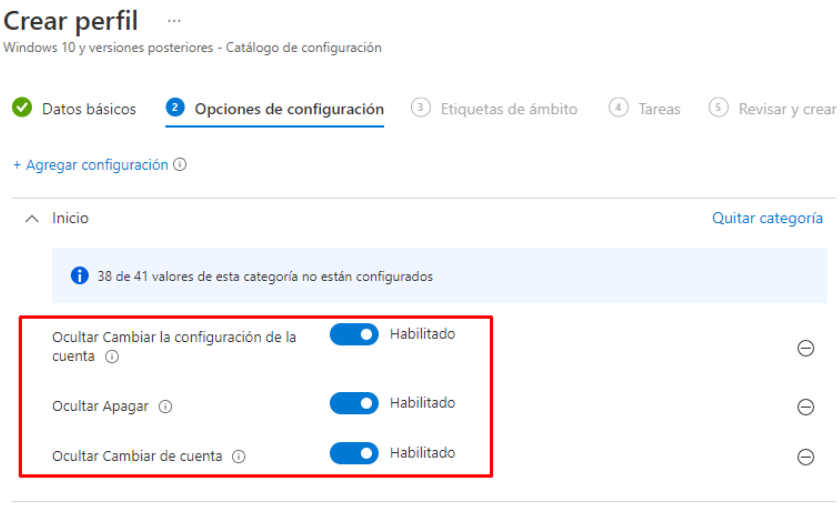


Figura 42. *Configuraciones cambio de usuario y apagado del equipo*

Como se puede apreciar en la Figura 43, en la Figura 44 y en la Figura 45, se obtuvo un resultado exitoso en el grupo asignado de prueba, por lo que fue posible ofrecer al cliente de la empresa esta solución para dispositivos de salas comunes.

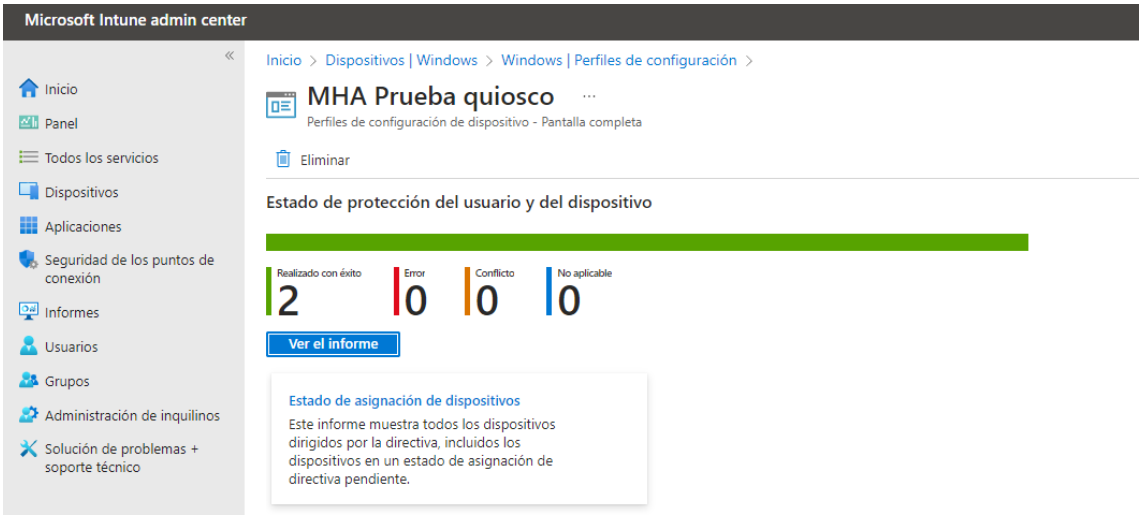


Figura 43. *Resultado asignación del perfil de configuración para modo quiosco en los dispositivos asignados*

Figura 44. *Resultado práctico final del quiosco multimedia en el dispositivo Windows de prueba configurado a través de Intune*

Figura 45. *Resultado práctico tras aplicar la configuración de bloquear la opción de apagado*

- **Aviso legal**

El objetivo de esta prueba era la de configurar el dispositivo de forma que, al desbloquearlo, aparezca automáticamente un aviso legal, con el objetivo de que así todos los usuarios estén al tanto de las políticas de uso y de seguridad de su organización, así como poder mostrarles mensajes personalizados.

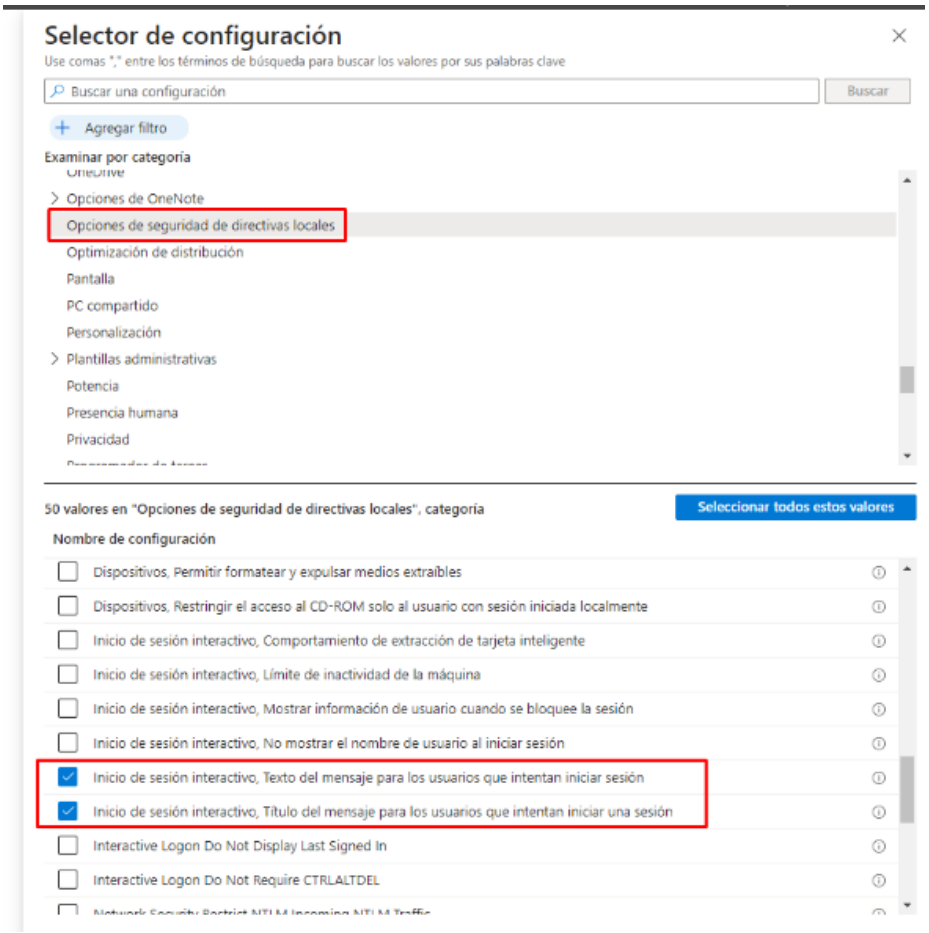


Figura 47. *Selector de configuración para crear establecer aviso legal en dispositivos*

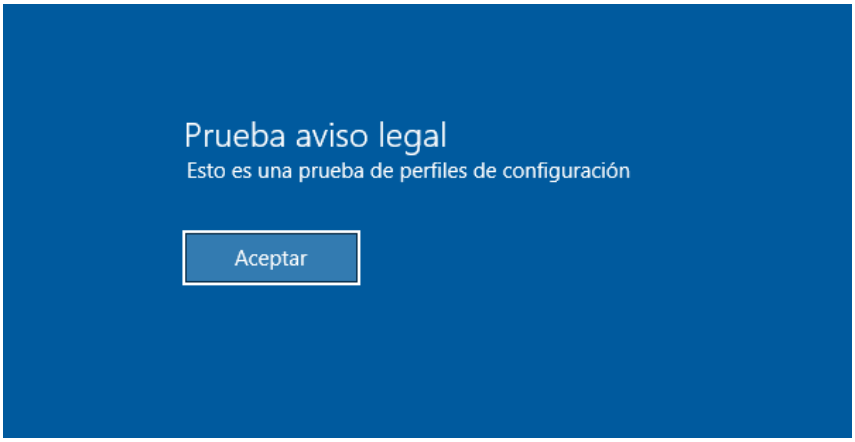


Figura 46. *Ejemplo práctico de aviso legal establecido en los dispositivos de prueba*

- **Programa Windows AutoPilot Deployment.**

Windows AutoPilot además de la inscripción de dispositivos, ofrece más servicios como son la configuración del conector de Intune, la creación de perfiles de implementación y la administración de los dispositivos Windows AutoPilot.

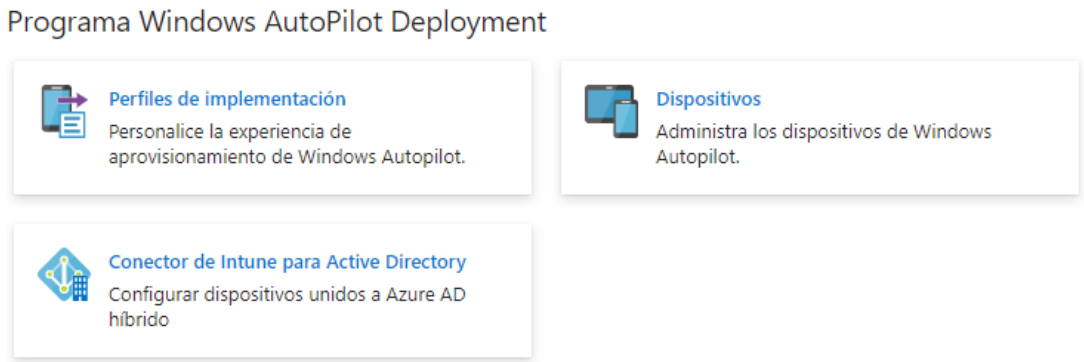


Figura 48. *Servicios ofrecidos por el programa Windows AutoPilot Deployment*

Todos los dispositivos Windows AutoPilot contienen en su id "[ZTDId]". Sabiendo esto, la administración y seguimiento de los dispositivos AutoPilot se facilita mucho. Aprovechando esa característica, se puede crear un grupo dinámico de dispositivos AutoPilot val que se unan de forma automática todos ellos una vez sean inscritos, consiguiendo así que se configuren todos de la misma forma.

Para ello habrá que crear un grupo de tipo dinámico, asignándole la regla de pertenencia que se puede ver en la Figura 50. [45]

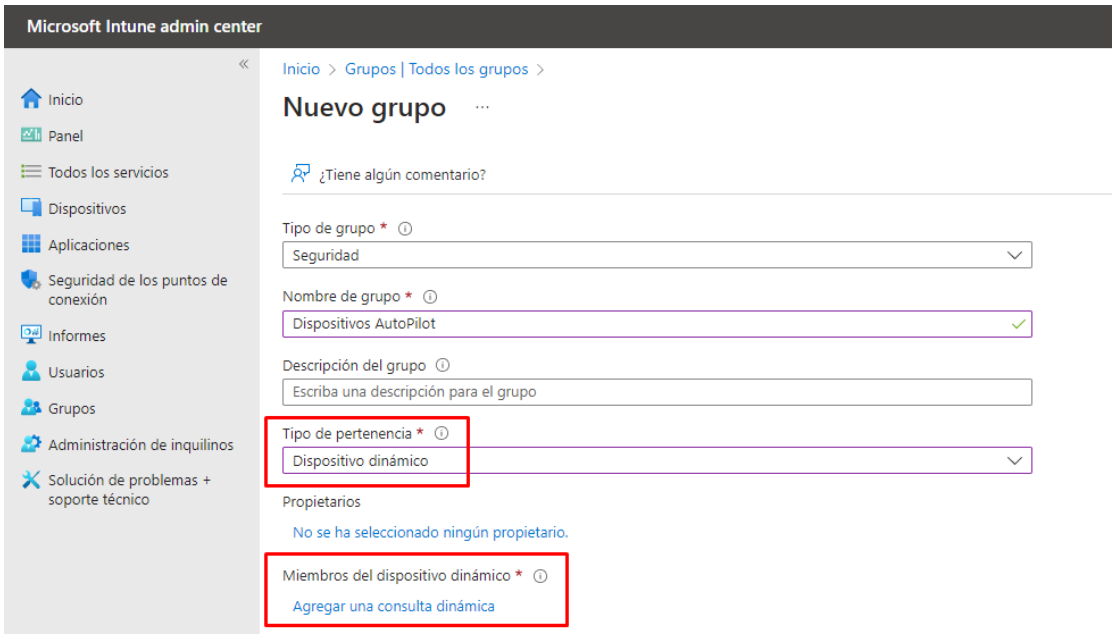


Figura 49. *Ejemplo creación grupo dinámico para la unión automática de dispositivos AutoPilot*

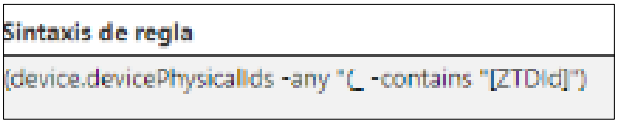


Figura 50. *Sintaxis de la regla de pertenencia para el grupo dinámico de dispositivos AutoPilot*

La propiedad *devicePhysicalIDs* es la que selecciona los dispositivos que contienen en su id "[ZTDId]".

- **Perfiles de implementación**

Los perfiles de implementación tienen como principal objetivo configurar los dispositivos inscritos mediante AutoPilot. En estos perfiles es donde se especifica el tipo de usuario que inicia sesión, ya sea como usuario administrador local de la máquina o como un usuario normal. Además, hay que especificar si se va a unir a Azure AD de forma híbrida o no.

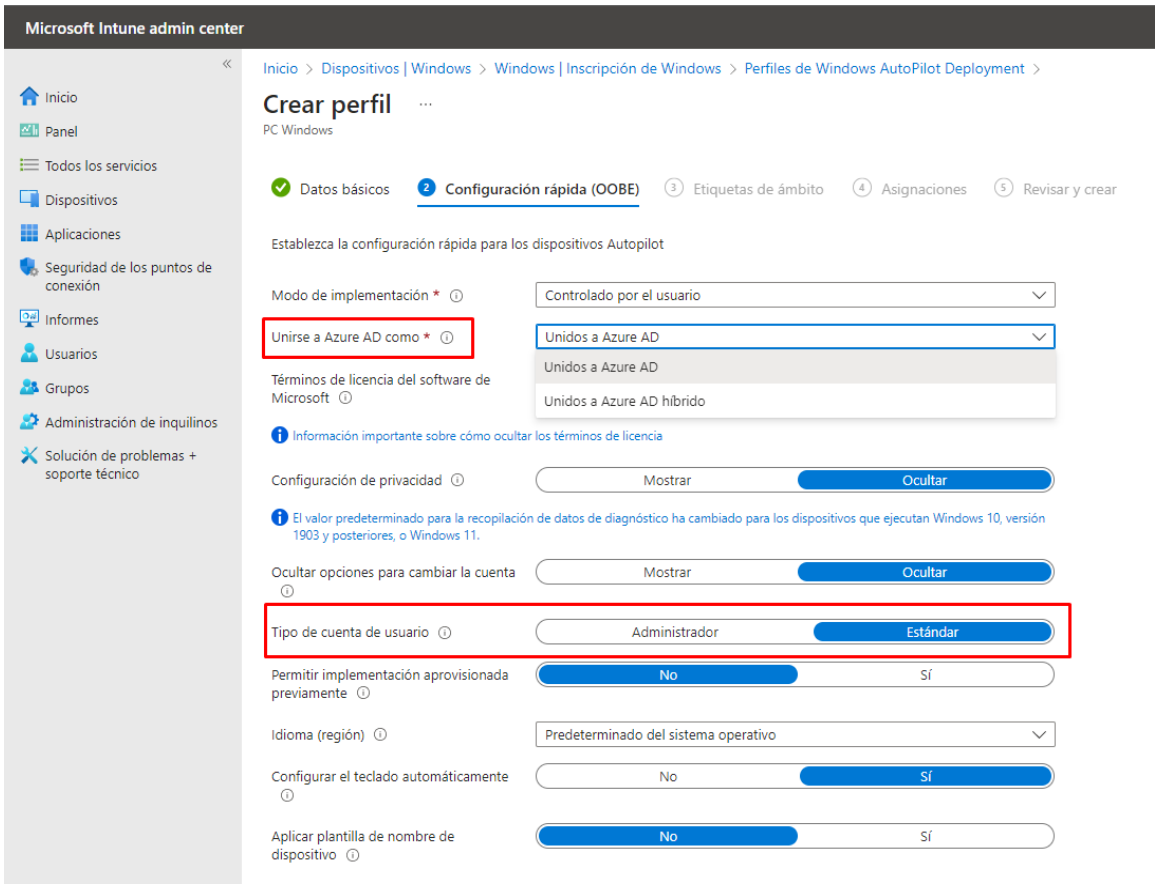


Figura 51. *Ejemplo de creación de un perfil de implementación*

- **Perfil de configuración de unión a un dominio**

Al estar ante un entorno híbrido, como se ha mencionado antes, para hacer de forma correcta la inscripción de un dispositivo AutoPilot, es necesario crear un perfil de configuración de tipo *unión a un dominio*.

Figura 52. *Opciones de configuración a introducir en un perfil de configuración de tipo unión a un dominio*

En las opciones de configuración hay que especificar el nombre del dominio, la unidad organizativa (OU) creada para los dispositivos AutoPilot y un prefijo que se le asignará al nombre del equipo inscrito. De esta forma se consigue que los equipos que hayan sido registrados en la nube se vean reflejados en la OU del directorio activo local y con el prefijo del nombre especificado.

Para que este tipo de perfil de configuración funcione hay que tener instalado y activo el conector de Intune. Los pasos para seguir para la instalación de este conector están detallados en el Anexo, al final de este documento.

4.3.2. Dispositivos iOS/iPadOS

Al igual que con los dispositivos Windows, Intune admite la administración de dispositivos móviles (MDM) de iPads y iPhones para conceder acceso seguro a los usuarios al correo electrónico, los datos y las aplicaciones profesionales. Sin embargo, a diferencia de los dispositivos Windows, al tratarse de dispositivos móviles, van a funcionar en entornos únicamente en la nube.

- **Tipos de inscripción.**

Principalmente existen tres tipos de inscripción en soluciones de gestión de dispositivos móviles (MDM). Cuando se inscriben dispositivos Apple en una solución MDM, esos dispositivo pueden estar supervisados. La supervisión, en términos generales, indica que el dispositivo es propiedad de la organización, lo cual proporciona un control adicional sobre su configuración y sus restricciones. [46][47]

Tipo de inscripción	¿Pasa a supervisado al inscribirse en MDM?
Inscripción de usuario (no es posible con tvOS)	No
Inscripción de dispositivo	No (iOS, iPadOS y tvOS) Sí (macOS)
Inscripción automatizada de dispositivo	Sí

Figura 53. *Tipos de inscripción y si el dispositivo pasa a supervisado o no. [46]*

Dependiendo de las necesidades de la organización y de la forma en que se desee gestionar los dispositivos ser realizará la inscripción de una forma u otra, ya que cada una tiene sus propias ventajas y es adecuada para diferentes situaciones empresariales. A continuación, se van a detallar los tipos vistos en la Figura 53.

- **Inscripción de usuario**

Con este método, los usuarios pueden inscribir sus propios dispositivos en Intune a través de la aplicación *Portal de Empresa*. Está diseñada para implementaciones BYOD, en las que el propietario del dispositivo es el usuario, no la organización y a través de ellos acceden a los recursos corporativos.

Una vez se ha inscrito el dispositivo, se convierte en administrado. Es decir, la organización puede asignar directivas y aplicaciones al dispositivo mediante Intune. Sin embargo, tras este tipo de inscripción, el dispositivo no pasa a supervisado. Además, si el dispositivo se ha inscrito con inscripción de usuario, no se podrá cambiar a inscripción de dispositivos.

Existen dos formas principales en las que los usuarios pueden inscribir un dispositivo personal en la inscripción de usuario. Estas son la inscripción de usuario basada en la cuenta y la inscripción de usuario basada en perfil.

La inscripción de usuario crea una partición de trabajo en los dispositivos. Las características y la seguridad configuradas en el perfil de inscripción de usuario existen solamente en la partición de trabajo, no en la de usuario. Los usuarios no van a poder restablecer la partición de trabajo a los valores de fábrica, pero sí los administradores. Sin embargo, los administradores no podrán restablecer la partición personal a los valores de fábrica, pero los usuarios sí.

Una vez completada la inscripción de usuario, se crean automáticamente claves de encriptación en el dispositivo, protegiendo los datos y evitando que se roben, cambien o se vulneren. Si se anula la inscripción el dispositivo de forma remota con Intune o lo hace el usuario directamente, esas claves de encriptación se destruyen de forma segura.

MDM puede	MDM no puede
Configurar cuentas	Ver información personal, datos de uso o registros
Inventario personal de apps gestionadas	Inventario personal de apps personales
Eliminar solo datos gestionados	Eliminar datos personales
Instalar y configurar apps	Tomar el control de la gestión de una app personal
Solicitar un código	Requerir un código o una contraseña que sean complejos
Aplicar determinadas restricciones	Acceder a la ubicación del dispositivo
Configurar VPN por app	Acceder a los identificadores únicos de los dispositivos
	Borrar todo el dispositivo de forma remota
	Gestionar el bloqueo de activación
	Acceder al estado de la itinerancia
	Activar el modo Perdido

Figura 54. *Acciones que pueden realizar los administradores del sistema en dispositivos iOS/iPadOS inscritos por inscripción de usuario. [46]*

- **Inscripción por Apple Configurator**

Este método utiliza la herramienta Apple Configurator para preparar los dispositivos, propiedad de la organización, antes de inscribirlos en Intune. Es muy útil para empresas que tienen una gran cantidad de dispositivos que necesitan ser inscritos en Intune.

La inscripción con Apple Configurator requiere que conecte mediante USB cada dispositivo iOS/iPadOS a un equipo Mac para configurar la inscripción corporativa. Se pueden inscribir dispositivos en Intune con Apple Configurator de dos maneras. Estas son la inscripción con el Asistente de configuración, el cual borra el dispositivo y lo prepara para la inscripción y la inscripción directa, la cual no borra el dispositivo y lo inscribe mediante la configuración de iOS/iPadOS. Este método de inscripción solo admite dispositivos sin afinidad de usuario.

- **Inscripción automatizada**

La inscripción automatizada de dispositivo está diseñada para los dispositivos de propiedad de la organización, permitiendo a las organizaciones configurar y gestionar dispositivos desde el momento en que se sacan de su embalaje.

Este método permite que los usuarios se inscriban automáticamente en Intune al encenderlos por primera vez y conectarlos a Internet. Está pensado para organizaciones que busquen configurar rápidamente muchos dispositivos.

MDM puede	MDM no puede
Ver y establecer el nombre del dispositivo	Ver el correo electrónico, el calendario y los contactos personales
Solicitar el número de teléfono	Ver los mensajes SMS o de iMessage
Solicitar el número de serie	Ver el historial de navegación de Safari
Solicitar el nombre y número del modelo	Ver los registros de llamadas telefónicas o de FaceTime
Ver la capacidad y el espacio disponible	Ver las notas y los recordatorios personales
Solicitar el número de versión del sistema operativo	Recopilar la frecuencia de uso de apps
Instalar apps gestionadas	
Configurar todas las restricciones	
Configurar el proxy HTTP global	
Borrar todos los contenidos y ajustes del dispositivo de forma remota	
Gestionar el bloqueo de activación	
Acceder al estado de la itinerancia	
Activar el modo Perdido	

Figura 55. *Acciones que pueden realizar los administradores del sistema en dispositivos iOS/iPadOS inscritos por inscripción de usuario. [46]*

- **Directivas de cumplimiento.**

Las soluciones de administración de dispositivos móviles (MDM) como Intune ayudan a proteger datos de la organización exigiendo a los usuarios y dispositivos que cumplan algunos requisitos. [48]

Un ejemplo práctico llevado a cabo consistió en exigir una versión mínima del sistema operativo iOS. Esta era la 16.

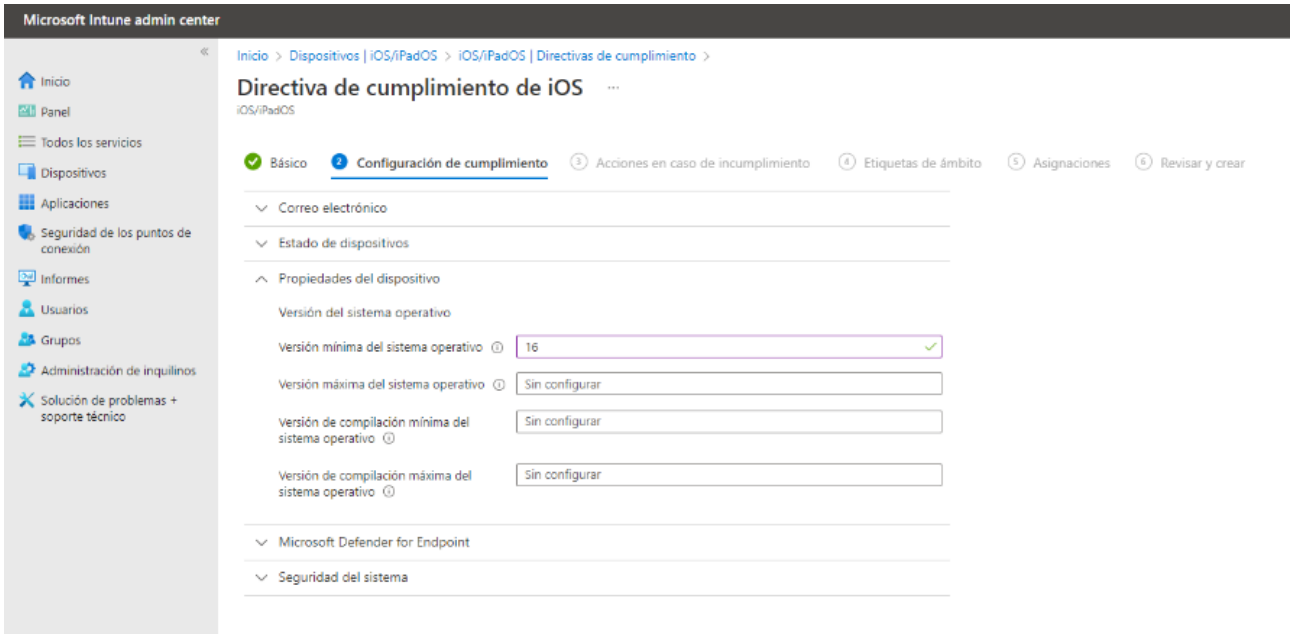


Figura 56. *Configuración de una directiva de cumplimiento para dispositivos iOS/iPadOS*

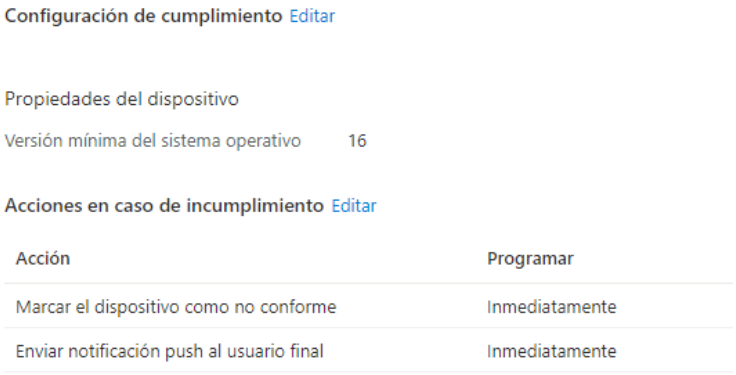
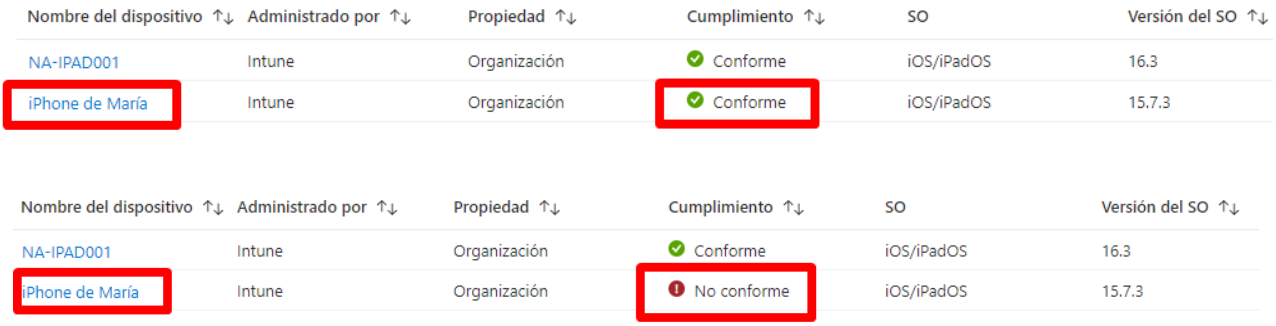


Figura 57. *Configuración final de la directiva y acciones en caso de incumplimiento*

Esta directiva se aplicó a un dispositivo con versión del sistema operativo 15.7.3, por lo que tras aplicarle la directiva iba a quedar como no conforme, llevándose a cabo sobre él las acciones pertinentes.



Nombre del dispositivo	Administrado por	Propiedad	Cumplimiento	SO	Versión del SO
NA-IPAD001	Intune	Organización	Conforme	iOS/iPadOS	16.3
iPhone de María	Intune	Organización	Conforme	iOS/iPadOS	15.7.3

Nombre del dispositivo	Administrado por	Propiedad	Cumplimiento	SO	Versión del SO
NA-IPAD001	Intune	Organización	Conforme	iOS/iPadOS	16.3
iPhone de María	Intune	Organización	No conforme	iOS/iPadOS	15.7.3

Figura 58. *Estado de cumplimiento del dispositivo antes y después de aplicar la directiva de configuración*

- **Perfiles de configuración.**

Al igual que con los dispositivos Windows, a través de los perfiles de configuración es posible aplicar muchas características y configuraciones que ayudan a los administradores IT a controlar dispositivos iOS y iPadOS, en función de las necesidades de la organización. [49]

La prueba llevada a cabo consistió en aplicarle al dispositivo una serie de configuraciones para probar qué ocurre al aplicar a un dispositivo que no está en modo supervisado una serie de configuraciones. Este modo se detalla dos apartados más adelante.

Se eligió hacer la prueba con un dispositivo BYOD, inscrito en Intune mediante inscripción de usuario, para que de esta forma no estuviese supervisado.

Figura 59. *Estado de configuración del dispositivo tras aplicarle configuraciones*

Se comprobó que, al no estar en modo supervisado, hay configuraciones que no se le pueden aplicar, por lo que se tiene menor control sobre el dispositivo.

- **Directivas de actualización para iOS/iPadOS.**

Las directivas para las actualizaciones de software permiten implementar la actualización de software más reciente que esté disponible o una actualización anterior, en función del número de versión de la actualización. [50]

Al implementar una actualización anterior, hay que implementar también un perfil de restricciones de dispositivo para restringir la visibilidad de las actualizaciones de software, ya que los perfiles de actualización no impiden que los usuarios actualicen el sistema operativo manualmente. Sin embargo, sí que se puede impedir que los usuarios actualicen el sistema operativo de forma manual a través de una directiva de configuración de dispositivos que restrinja la visibilidad de las actualizaciones de software.

Además, las directivas de actualización permiten también especificar una programación que determine cuándo se va a instalar la actualización. Se puede programar para que se instalen la siguiente vez que se registre el dispositivo, o si no se pueden crear intervalos de fecha y hora durante los que se puedan instalar las actualizaciones o bloquear su instalación.

Si no se configura nada, de forma predeterminada, los dispositivos se registran con Intune aproximadamente cada 8 horas. Si hay una actualización disponible a través de una directiva de actualización, el dispositivo descarga la actualización. Después, el dispositivo instala la actualización la próxima vez que se registre dentro de la configuración de programación.

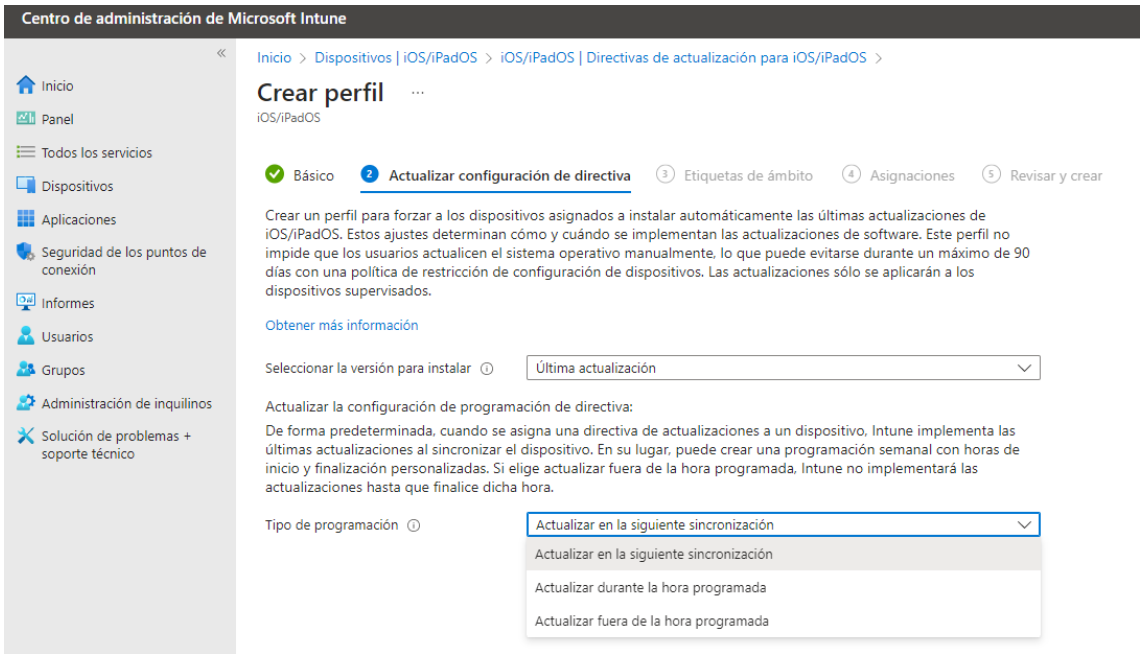


Figura 60. *Ejemplo configuración directiva de actualización para iOS/iPadOS*

- **Modo supervisado de iOS/iPadOS.**

El modo supervisado de Apple iOS/iPadOS ofrece a los administradores IT más opciones a la hora de administrar dispositivos Apple, lo que resulta útil para dispositivos corporativos implementados a escala. Es decir, los dispositivos supervisados ofrecen más opciones de administración. [51]

El modo supervisado de iOS/iPadOS en Intune es una característica que permite tener un control completo sobre los dispositivos. Cuando se activa este modo, se establece una relación de confianza entre el dispositivo e Intune, permitiendo una administración más profunda y granular.

Algunas de las características del modo supervisado de iOS/iPadOS incluyen la capacidad de configurar restricciones y permisos específicos, como el bloqueo de ajustes y aplicaciones, la restricción de funciones de la cámara y la limitación de la capacidad de instalar aplicaciones no autorizadas. También permite la implementación de perfiles de configuración y la administración remota de los dispositivos, lo que hace que mejore la seguridad y la eficiencia en el uso de los dispositivos móviles de la organización.

Para comprobar si el dispositivo está supervisado, se puede hacer desde la pantalla de bloqueo en la que se indica “Este iPhone está administrado por “Nombre de la compañía” o en la página Acerca de del dispositivo, en la que se indica “Este iPhone está supervisado. La empresa puede supervisar el tráfico de Internet y localizar este dispositivo”.

En términos generales, la supervisión indica que el dispositivo es propiedad de la organización, lo cual proporciona un control adicional sobre su configuración y sus restricciones.

4.4. Gestión de aplicaciones

La gestión de aplicaciones móviles de Intune hace referencia al conjunto de funciones de administración que permite publicar, insertar, configurar, proteger, supervisar y actualizar aplicaciones móviles. Se lleva a cabo en función del tipo de aplicación y de su compatibilidad dependiendo del tipo de plataforma. Por ejemplo, las de tipo Tienda son compatibles con todas ya que cada sistema operativo tiene una Tienda de Aplicaciones, sin embargo, el paquete de aplicaciones de Microsoft 365 y Microsoft Edge están más enfocados para equipos con sistema operativo Windows o macOS. [52]

Tipos de aplicación	Instalación	Actualizaciones
Aplicaciones de la tienda	Intune instala la aplicación en el dispositivo.	Las actualizaciones de aplicaciones son automáticas.
Aplicaciones escritas internamente o como una aplicación personalizada (línea de negocio)	Intune instala la aplicación en el dispositivo (el usuario proporciona el archivo de instalación).	Debe actualizar la aplicación.
Aplicaciones integradas	Intune instala la aplicación en el dispositivo.	Las actualizaciones de aplicaciones son automáticas.
Aplicaciones en la web (vínculo web)	Intune crea un acceso directo a la aplicación web en la pantalla de inicio del dispositivo.	Las actualizaciones de aplicaciones son automáticas.
Aplicaciones de otros servicios de Microsoft	Intune crea un acceso directo a la aplicación en el Portal de empresa.	Las actualizaciones de aplicaciones son automáticas.

Figura 61. *Tipos de aplicaciones en Microsoft Intune. [52]*

Funcionalidad de administración de aplicaciones	Android o Android Enterprise	iOS/iPadOS	macOS	Windows 10/11
Agregar y asignar aplicaciones a dispositivos y usuarios	Sí	Sí	Sí	Sí
Asignar aplicaciones a dispositivos no inscritos en Intune	Sí	Sí	No	No
Usar directivas de configuración de aplicaciones para controlar el comportamiento de inicio de las aplicaciones	Sí	Sí	No	No
Usar directivas de aprovisionamiento de aplicaciones móviles para renovar aplicaciones caducadas	No	Sí	No	No
Proteger los datos de empresa en las aplicaciones con directivas de protección de aplicaciones	Sí	Sí	No	No [1]
Quitar solo los datos corporativos de una aplicación instalada (borrado selectivo de aplicaciones)	Sí	Sí	No	Sí
Supervisar las asignaciones de aplicaciones	Sí	Sí	Sí	Sí
Asignar y realizar el seguimiento de aplicaciones compradas por volumen desde una tienda de aplicaciones	No	Sí	No	Sí
Instalación obligatoria de aplicaciones en dispositivos (obligatorio) [2]	Sí	Sí	Sí	Sí
Instalación opcional en dispositivos desde el Portal de empresa (instalación disponible)	Sí [3]	Sí	Sí	Sí
Instalar acceso directo a una aplicación en la web (enlace web)	Sí [4]	Sí	Sí	Sí
Aplicaciones internas (línea de negocio)	Sí [5]	Sí	Sí	Sí
Aplicaciones de una tienda	Sí	Sí	No	Sí
Actualizar aplicaciones	Sí	Sí	No	Sí

Figura 62. *Resumen de las capacidades de administración de aplicaciones en función de la plataforma. [52]*

En los siguientes apartados se ha tratado de explicar con más en detalle la gestión de aplicaciones con Intune, centrando los sistemas operativos Windows e iOS/iPadOS.

4.4.1. Tipos de aplicaciones

Como se puede ver en la Figura 61, tanto la instalación como las actualizaciones dependen del tipo de aplicación.

Uno de los ejemplos prácticos llevados a cabo, al estar ante un entorno empresarial, fue la instalación del paquete de aplicaciones de Microsoft Office 356 (de la Microsoft Store), el cual incluye Excel, OneNote, Outlook, PowerPoint, Teams y Word en dispositivos de prueba recién iniciados e inscritos en Intune.

Figura 63. *Estado instalación Aplicaciones de Microsoft 365*

Las aplicaciones que se implementan tanto de la Microsoft Store como de la tienda iOS se pueden mantener actualizadas automáticamente, ya que Intune las actualiza cuando una nueva versión está disponible. Para esto es importante no habilitar la *opción Desactivar la descarga automática y la instalación de actualizaciones*, además de que el dispositivo tiene que estar inscrito con Intune.

A la hora de configurar una aplicación desde Intune, hay que asignarlas a grupos de dispositivos y/o usuarios. Hay distintas opciones a elegir.

- **Requerido.** Asignación para los grupos en los que quiere que esta aplicación sea obligatoria. Las aplicaciones obligatorias se instalan automáticamente en los dispositivos inscritos. Esta opción de asignación es válida tanto para grupos de dispositivos como de usuarios, pero el dispositivo debe estar inscrito con Intune.
- **Disponible para dispositivos inscritos.** Asignación para los grupos en los que se quiere que esta aplicación esté disponible y es válida tanto para dispositivos inscritos como no inscritos con Intune. Las aplicaciones disponibles para los dispositivos inscritos se muestran en la aplicación Portal de empresa y en el sitio web para que los usuarios puedan instalarlas opcionalmente. Esta opción de asignación solo es válida para los grupos de usuarios, no para los grupos de dispositivos

y, además, para que el usuario final pueda instalar aplicaciones desde el portal de empresa, el dispositivo tiene que estar inscrito con Intune. Sin embargo, desde el portal de empresa web esto no es necesario.

- **Desinstalar**. Las aplicaciones con esta asignación se desinstalan de los dispositivos administrados en los grupos seleccionados si Intune ha instalado la aplicación en el dispositivo previamente mediante la asignación "Disponible para dispositivos inscritos" o "Requerido" en la misma implementación.

4.4.2. Directivas de protección

Una directiva puede ser una regla que se aplica cuando el usuario intenta acceder y/o mover datos corporativos o un conjunto de acciones que se prohíben/supervisan cuando el usuario está dentro de una aplicación. Están enfocadas para ser implementadas en dispositivos móviles con sistemas operativos Android o iOS/iPadOS. El uso de MDM con directivas de protección de aplicaciones permite proteger los datos de la empresa a nivel de aplicación, garantizando que los dispositivos móviles estén protegidos. Las directivas de protección de aplicaciones son reglas que garantizan que los datos de la organización siguen siendo seguros o se encuentran en una aplicación administrada.

Los requisitos de línea base para usar directivas de protección de aplicaciones en una aplicación administrada por Intune son que el usuario final tenga una cuenta de Azure AD, una licencia de Microsoft Azure asignada a esa cuenta y, además, que el usuario final debe pertenecer a un grupo de seguridad al que se aplique una directiva de protección de aplicaciones. [53]

La protección de datos de aplicación se organiza en tres niveles de configuración distintos, cada uno de ellos basado en el anterior:

- ***Nivel 1*.- Protección de datos empresariales básica.** Este nivel garantiza que las aplicaciones estén protegidas con un PIN y cifradas y, además, realiza operaciones de borrado selectivo. Microsoft recomienda este nivel como configuración de datos mínima.
- ***Nivel 2*.- Protección de datos empresariales mejorada.** Este nivel incorpora mecanismos para la prevención de la pérdida de datos de APP y los requisitos mínimos para el sistema operativo, de forma que si no se cumplen no se podrá acceder a los recursos.
- ***Nivel 3*.- Protección de datos empresariales alta.** Este nivel incorpora mecanismos avanzados para la protección de datos, configuración de PIN mejorada y defensa contra amenazas móviles de APP. Este nivel va más dirigido a usuarios que tienen acceso a los recursos más delicados de la organización.

El problema de usar aplicaciones sin directivas de protección de aplicaciones es que se pueden entremezclar los datos empresariales con los personales.

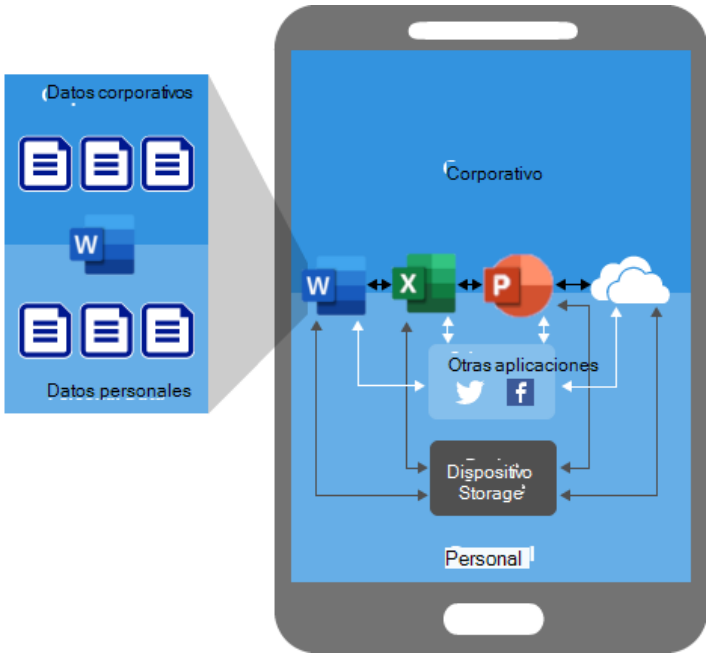


Figura 64. *Aplicaciones sin directivas de protección de aplicaciones. [54]*

Las flechas del diagrama de la Figura 64, muestran el movimiento sin restricciones de los datos entre aplicaciones personales y corporativas y hacia ubicaciones de almacenamiento.

Al usar directivas de protección de aplicaciones se consigue evitar que los datos de empresa se guarden en el almacenamiento local del dispositivo, de la misma forma que restringe el movimiento de datos a otras aplicaciones que no estén protegidas por las directivas de protección de aplicaciones.

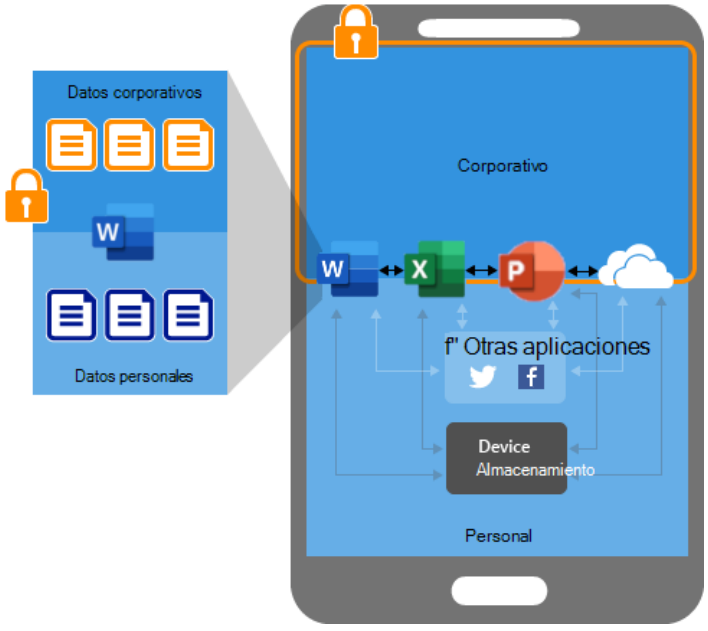


Figura 65. *Aplicaciones con directivas de protección de aplicaciones en dispositivos. [54]*

En Figura 65 se puede ver que, a diferencia de en la Figura 64, al tener aplicadas directivas de protección, el movimiento de los datos entre aplicaciones y su almacenamiento sí está restringido.

4.4.3. Directivas de configuración

Las directivas de configuración de aplicaciones permiten asignar valores de configuración a una directiva que se asigna a los usuarios finales antes de que ejecuten la aplicación, permitiendo configurar y personalizar las aplicaciones de forma masiva y remota. Como es lógico, hoy en día esto es algo cada vez más buscado por las empresas, al facilitar la experiencia tanto de los usuarios/clientes como del administrador IT en dispositivos móviles (iOS/iPadOS y Android Enterprise).

Intune distingue entre dispositivos y aplicaciones administrados a la hora de aplicar directivas de configuración de aplicaciones.

- **Dispositivos administrados**

Elegir *Dispositivos administrados* como tipo de inscripción de dispositivos, se refiere a las aplicaciones implementadas por Intune en el dispositivo inscrito, por lo que se administran mediante Intune como proveedor de inscripción.

En dispositivos iOS para poder usar este tipo de directiva, la aplicación tiene que estar anclada al perfil de administración. Además, para configurar una aplicación hay que elegir entre usar el diseñador de configuración y especificar datos XML. [55]

El diseñador de configuración permite configurar claves de configuración y valores específicos y estos son los siguientes:

- **Clave de configuración**: identifica de forma única la configuración de configuración específica.
- **Tipo de valor**: indica el tipo de datos del valor de configuración (Integer, Real, String o Boolean).
- **Valor de configuración**.

Por ejemplo, para controlar qué cuentas profesionales se agregan a las aplicaciones de Microsoft en dispositivos administrados iOS/iPadOS, se puede usar la clave *IntuneMAMAllowedAccountOnly*. De esta forma, si el valor es *habilitado*, la única cuenta permitida es la cuenta de usuario administrada definida por la clave IntuneMAMUPN, y si el valor es *deshabilitado* se permite cualquier cuenta. Esto se puede ver en la Figura 66, en la que se puede ver una configuración de directiva de configuración aplicada a la plataforma iOS/iPadOS y asociada a la aplicación Portal de Empresa.

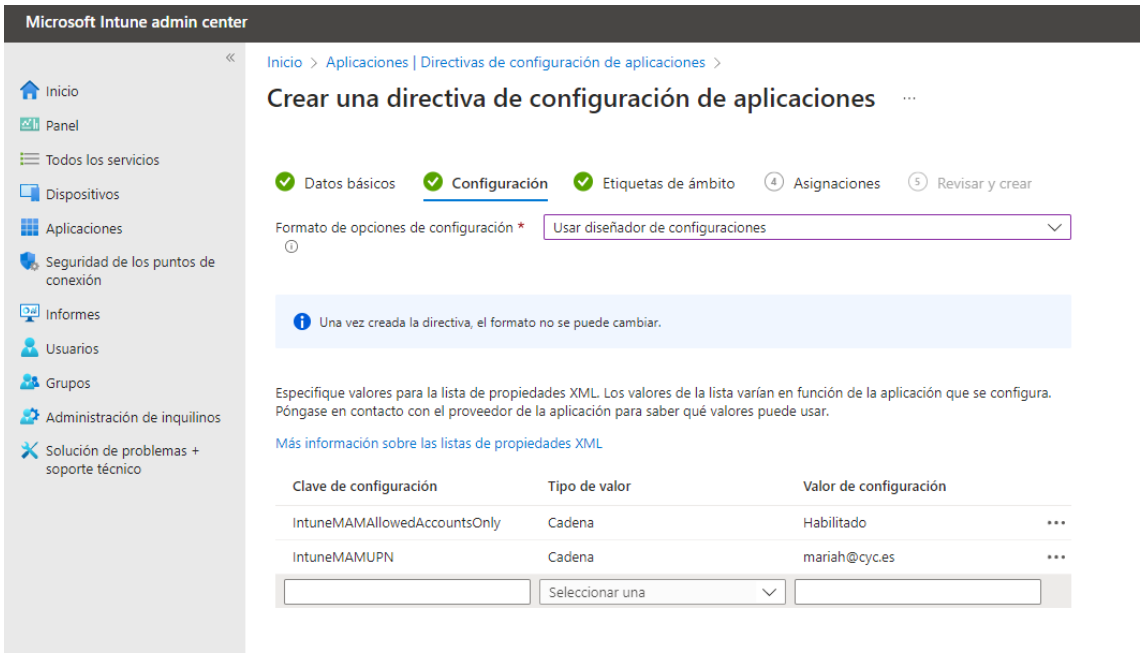


Figura 66. *Ejemplo creación directiva de configuración de aplicaciones por diseñador de configuración*

Además del Portal de Empresa, otra aplicación muy usada en dispositivos de empresa es el Outlook (aplicación de correo electrónico de Microsoft), para la que es de gran interés la configuración automática del correo electrónico. De esta forma cuando el usuario inicia sesión por primera vez, se va a configurar automáticamente el correo en la aplicación.

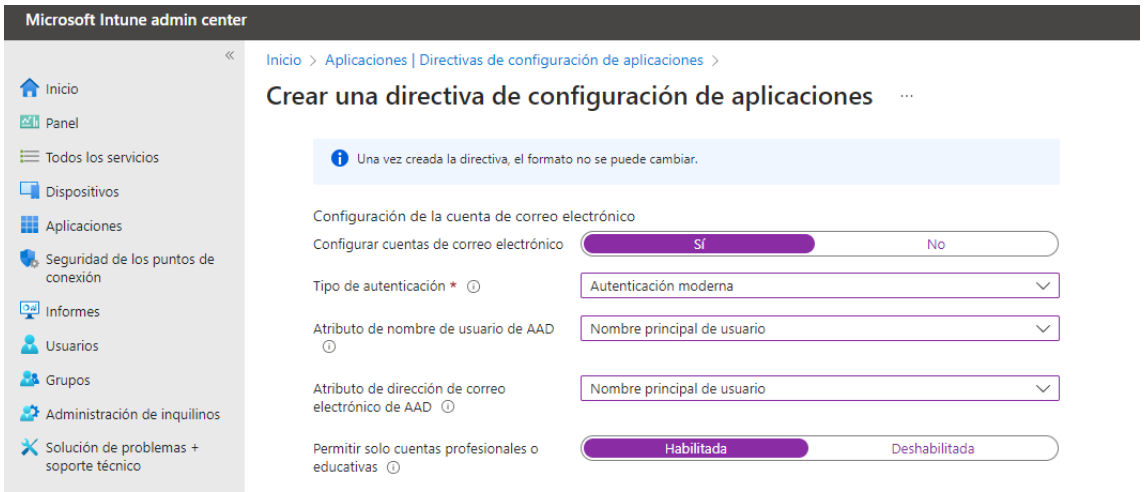


Figura 67. *Parámetros de interés para la directiva de configuración de Outlook*

En la Figura 67, se muestran los parámetros relacionados con la configuración automática de la cuenta profesional. Los atributos de nombre de usuario y de dirección de correo electrónico de Azure AD, en el caso de la empresa en la que se está llevando a cabo el proyecto, son en ambos casos el nombre principal del usuario. En cuanto al tipo de autenticación, es más conveniente elegir la autenticación moderna al ofrecer mayor seguridad en autenticación y autorización de usuarios que la básica. La autenticación moderna, como se ha mencionado antes, es una combinación de métodos de autenticación, autorización y algunas medidas de seguridad que dependen de las directivas de acceso.

- **Aplicaciones administradas**

Elegir *Aplicaciones administradas* como tipo de inscripción de dispositivos, se refiere a las aplicaciones configuradas con una directiva de protección de aplicaciones de Intune en los dispositivos, independientemente del estado de inscripción. Esto es así porque mediante el canal MAM las aplicaciones pueden recibir directivas de configuración de aplicaciones independientemente del estado de inscripción del dispositivo. Esta directiva permite gestionar paquetes de aplicaciones, como por ejemplo del de Microsoft.

Para admitir la configuración de las aplicaciones a través del canal de MAM, la aplicación debe integrarse con el SDK (Software Development Kit o Kit de Desarrollo de Software) de aplicaciones de Intune. El SDK de Intune es un grupo de herramientas que permiten la programación de aplicaciones móviles y es el que permite que la aplicación admita directivas de protección de aplicaciones Intune, esforzándose por minimizar la cantidad de cambios de código necesarios para el desarrollador de la aplicación. [56]

4.4.4. Perfiles de aprovisionamiento de aplicaciones de iOS

Las aplicaciones de línea de negocio de iOS/iPadOS de Apple que se asignan a iPhone y iPad se crean con un perfil de aprovisionamiento incluido y con código firmado con un certificado. Entonces cuando se ejecuta la aplicación, iOS/iPadOS confirma la integridad de esta y aplica las directivas definidas por el perfil de aprovisionamiento, produciéndose dos validaciones. Una de ellas es la *integridad del archivo de instalación*, en la que se comparan los detalles de la aplicación con la clave pública del certificado de firma empresarial, los cuales tienen que coincidir para poder ejecutar la aplicación. La segunda validación consiste en un *cumplimiento de funcionalidades* en la que se intentan aplicar las funcionalidades de la aplicación desde el perfil de aprovisionamiento empresarial (no los perfiles de aprovisionamiento de desarrolladores individuales) que se encuentran en el archivo de instalación de aplicaciones (.ipa). [57]

5. Conclusiones

En este Trabajo de Fin de Grado se han tratado de analizar las principales características y ventajas que ofrece Microsoft Intune, como es la capacidad de administrar dispositivos desde una única plataforma, pudiendo aplicar perfiles y directivas de configuración a través de una consola centralizada. La atención se ha centrado principalmente en la gestión de dispositivos Microsoft Windows.

A lo largo del proyecto se han llevado a cabo diversas pruebas y ejemplos prácticos que han permitido comprobar la eficacia que ofrece Intune para la gestión de dispositivos Windows. Sin embargo, el análisis ha estado más limitado en el caso de los dispositivos iOS/iPadOS, ya que, por falta de tiempo, no se ha podido indagar tanto.

La elección de Microsoft Intune como servicio para la gestión de dispositivos ha sido acertada, ya que, junto con toda la información recabada y la amplia gama de herramientas y funcionalidades avanzadas que ofrece, se han podido realizar y documentar distintas pruebas que, en un futuro, podrán ser aplicadas a clientes de la empresa.

Es importante destacar que todas las pruebas realizadas se han llevado a cabo en un entorno híbrido, que cuenta tanto con directorio activo local como con directorio activo de Azure. En él se han podido simular ejemplos de uso, además de poder evaluar el funcionamiento de esta solución en este tipo de entornos empresariales.

En conclusión, en este trabajo se ha llevado a cabo un análisis de la solución de gestión de dispositivos móviles que ofrece Microsoft Intune, comprobando su eficacia y capacidad de forma más profunda en dispositivos Windows y más superficial en dispositivos iOS/iPadOS. Sin duda, ha sido una experiencia valiosa que ha permitido adquirir conocimientos y experiencia en un sector que está en constante evolución y crecimiento.

5.1. Futuras líneas de investigación

Al tratarse de un sector en constante evolución y crecimiento, es un tema que permite expandirse en distintas líneas de investigación. Es más, cabe destacar que este mismo proyecto es una línea de investigación que se ha desarrollado a partir de un proyecto anterior centrado en la gestión de dispositivos Android en entornos empresariales.

En este caso, se han quedado abiertas varias líneas de investigación, quedando pendiente profundizar más en la gestión de dispositivos iOS/iPadOS e incluir además tanto la gestión de dispositivos macOS como la gestión de dispositivos Linux.

Como ya se ha mencionado antes, el proyecto se ha desarrollado en un entorno híbrido, por lo que sería interesante profundizar en entornos únicamente en la nube que no cuenten con directorio activo local, ya que, al tratarse de un sector con gran demanda en el mercado, podría ser interesante para aportar nuevos conocimientos y perspectivas sobre la gestión de dispositivos en distintos tipos de entornos empresariales.

6. Referencias bibliográficas

[1]. «El “cloud” en España, a punto del gran salto», Expansión.com, 19 de noviembre de 2018. https://www.expansion.com/economia-digital/companias/2018/11/19/5bedaa6346163f9a438b4620.html (accedido 21 de abril de 2023).

[2]. luisclausin, «¿Qué es Microsoft Intune? ¿Para qué sirve?», *NTS SEIDOR*, 8 de junio de 2020. https://www.nts-solutions.com/blog/microsoft-intune-que-es.html (accedido 7 de febrero de 2023).

[3]. Erikre, «Licencias disponibles para Microsoft Intune», 25 de marzo de 2023. https://learn.microsoft.com/es-es/mem/intune/fundamentals/licenses (accedido 21 de abril de 2023).

[4]. «Protect Your Business with Our Trusted Intune-Based MDM Solutions», Communication Square LLC. https://www.communicationsquare.com/mobile-device-management/ (accedido 21 de abril de 2023).

[5]. Dynamic, «IBM | Consultoría con base tecnológica», *DYNAMIC*, 25 de noviembre de 2019. https://www.dynamicgc.es/principales-consultoras-estrategicas-en-espana/ibm-consultoria-con-base-tecnologica/ (accedido 13 de marzo de 2023).

[6]. «IBM Documentation», 18 de enero de 2023. https://www.ibm.com/docs/es/security-verify?topic=integrations-maas360 (accedido 13 de abril de 2023).

[7]. «Descubre la plataforma en la nube de próxima generación». https://www.oracle.com/es/cloud/ (accedido 13 de abril de 2023).

[8]. «Servicios en la nube de planificación empresarial de Oracle | MindStream Analytics», Servicios en la nube de planificación empresarial de Oracle | MindStream Analytics. https://www.mindstreamanalytics.com/esp/servicio-en-la-nube-de-planificacion-empresarial-de-oracle.html (accedido 21 de abril de 2023).

[9]. «¿Cuáles son los Proveedores de Servicios en la Nube?» https://www.accessq.com.mx/cuales-son-los-proveedores-servicios-nube/ (accedido 13 de abril de 2023).

[10]. «¿Qué es la nube? | Conceptos esenciales», *Cloudflare*. https://www.cloudflare.com/es-es/learning/cloud/what-is-the-cloud/ (accedido 13 de abril de 2023).

[11]. M. Gualda, «¿Qué es Microsoft Azure? ¿Cómo funciona?», Tecon, 7 de enero de 2020. https://www.tecon.es/que-es-microsoft-azure-como-funciona/ (accedido 7 de febrero de 2023).

[12]. MandiOhlinger, «¿Qué es Microsoft Intune?», 23 de noviembre de 2022. https://learn.microsoft.com/es-es/mem/intune/fundamentals/what-is-intune (accedido 7 de febrero de 2023).

[13]. Erikre, «Tutorial: Tutorial del centro de administración de Microsoft Intune - Microsoft Intune», 4 de abril de 2023. https://learn.microsoft.com/es-es/mem/intune/fundamentals/tutorial-walkthrough-endpoint-manager (accedido 13 de abril de 2023).

[14]. frankroj, «Inscripción para dispositivos híbridos unidos a Azure AD - Windows Autopilot», 18 de enero de 2023. https://learn.microsoft.com/es-es/mem/autopilot/windows-autopilot-hybrid (accedido 8 de febrero de 2023).

[15]. frankroj, «Introducción a Windows Autopilot». https://learn.microsoft.com/es-es/mem/autopilot/windows-autopilot (accedido 8 de febrero de 2023).

[16]. barclayn, «¿Qué es Azure Active Directory? - Microsoft Entra»,https://learn.microsoft.com/es-es/azure/active

[17]. Mercadeo, «¿Qué son los controladores de dominio?», MSI Networks, 16 de marzo de 2020. https://msinetworks.com.do/en/blog/que-son-los-controladores-de-dominio/ (accedido 8 de febrero de 2023).

[18]. Justinha, «Creación de una unidad organizativa (OU) en Azure AD Domain Services», 29 de noviembre de 2022. https://learn.microsoft.com/es-es/azure/active-directory-domain-services/create-ou (accedido 13 de abril de 2023).

[19]. «Directorio Activo de Microsoft - ¿qué es y qué ventajas tiene?» https://www.tecnozero.com/blog/directorio-activo-de-microsoft-que-es-que-ventajas-tiene-para-la-empresa/ (accedido 13 de abril de 2023).

[20]. iainfoulds, «Introducción a Active Directory Domain Services», 9 de marzo de 2023. https://learn.microsoft.com/es-es/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview (accedido 13 de abril de 2023).

[21]. billmath, «¿Qué es Azure AD Connect y Connect Health? - Microsoft Entra», 17 de marzo de 2023. https://learn.microsoft.com/es-es/azure/active-directory/hybrid/whatis-azure-ad-connect (accedido 13 de abril de 2023).

[22]. billmath, «Servicios de federación de Active Directory», 9 de marzo de 2023. https://learn.microsoft.com/es-es/windows-server/identity/active-directory-federation-services (accedido 13 de abril de 2023).

[23]. I. Arteaga, «Gestión de dispositivos móviles: MDM y MAM», ICM, 4 de noviembre de 2021. https://www.icm.es/2021/11/04/mdm-vs-mam-gestion-dispositivos-moviles/ (accedido 9 de febrero de 2023).

[24]. «¿Qué es MDM?» https://www.jamf.com/es/blog/que-es-un-mdm/ (accedido 9 de febrero de 2023).

[25]. billmath, «Configuración de AD FS para autenticar a los usuarios almacenados en directorios LDAP», 9 de marzo de 2023. https://learn.microsoft.com/es-es/windows-server/identity/ad-fs/operations/configure-ad-fs-to-authenticate-users-stored-in-ldap-directories (accedido 13 de abril de 2023).

[26]. BrendaCarter, «Step 2. Enroll devices into management with Intune», 17 de febrero de 2023. https://learn.microsoft.com/en-us/microsoft-365/solutions/manage-devices-with-intune-enroll (accedido 13 de abril de 2023).

[27]. dougeby, «Inscripción en Microsoft Intune». https://learn.microsoft.com/es-es/mem/intune/enrollment/ (accedido 13 de abril de 2023).

[28]. MicrosoftGuyJFlo, «¿Qué son los dispositivos registrados en Azure AD? - Microsoft Entra», 21 de marzo de 2023. https://learn.microsoft.com/es-es/azure/active-directory/devices/concept-azure-ad-register (accedido 13 de abril de 2023).

[29]. MicrosoftGuyJFlo, «¿Qué es un dispositivo unido a Azure AD? - Microsoft Entra», 21 de marzo de 2023. https://learn.microsoft.com/es-es/azure/active-directory/devices/concept-azure-ad-join (accedido 13 de abril de 2023).

[30]. MicrosoftGuyJFlo, «¿Qué es un dispositivo híbrido unido a Azure AD? - Microsoft Entra», 21 de marzo de 2023. https://learn.microsoft.com/es-es/azure/active-directory/devices/concept-azure-ad-join-hybrid (accedido 13 de abril de 2023).

[31]. MicrosoftGuyJFlo, «Token de actualización principal (PRT) y Azure Active Directory - Microsoft Entra», 21 de marzo de 2023. https://learn.microsoft.com/es-es/azure/active-directory/devices/concept-primary-refresh-token (accedido 13 de abril de 2023).

[32]. billmath, «Sincronización de Azure AD Connect: tareas y consideraciones operativas - Microsoft Entra», 17 de marzo de 2023. https://learn.microsoft.com/es-es/azure/active-directory/hybrid/how-to-connect-sync-staging-server (accedido 13 de abril de 2023).

[33]. «¿Qué es una DMZ y por qué la usaría?», Fortinet. https://www.fortinet.com/lat/resources/cyberglossary/what-is-dmz.html (accedido 8 de febrero de 2023).

[34]. «¿Qué es un firewall?», Cisco. https://www.cisco.com/c/es_es/products/security/firewalls/what-is-a-firewall.html (accedido 13 de abril de 2023).

[35]. «Directivas de cumplimiento de dispositivos en Microsoft Intune | Microsoft Learn». https://learn.microsoft.com/es-es/mem/intune/protect/device-compliance-get-started (accedido 13 de abril de 2023).

[36]. Brenduns, «Configurar directivas de cumplimiento - Microsoft Intune», 8 de marzo de 2023. https://learn.microsoft.com/es-es/mem/intune/fundamentals/deployment-plan-compliance-policies (accedido 13 de abril de 2023).

[37]. Gargi-Sinha, «Planeamiento de la implementación del acceso condicional de Azure Active Directory - Microsoft Entra», 5 de diciembre de 2022. https://learn.microsoft.com/es-es/azure/active-directory/conditional-access/plan-conditional-access (accedido 9 de febrero de 2023).

[38]. MandiOhlinger, «Creación de perfiles de dispositivo en Microsoft Intune», 4 de abril de 2023. https://learn.microsoft.com/es-es/mem/intune/configuration/device-profile-create (accedido 13 de abril de 2023).

[39]. MandiOhlinger, «Usar el análisis de directiva de grupo para importar y analizar GPO en Microsoft Intune», 4 de abril de 2023. https://learn.microsoft.com/es-es/mem/intune/configuration/group-policy-analytics (accedido 13 de abril de 2023).

[40]. MicrosoftGuyJFlo, «Administración de los administradores locales en dispositivos unidos a Azure AD - Microsoft Entra», 5 de diciembre de 2022. https://learn.microsoft.com/es-es/azure/active-directory/devices/assign-local-admin (accedido 13 de abril de 2023).

[41]. paolomatarazzo, «Inscripción en Intune con Windows Autopilot - Windows Education», 18 de marzo de 2023. https://learn.microsoft.com/es-es/education/windows/tutorial-school-deployment/enroll-autopilot (accedido 13 de abril de 2023).

[42]. frankroj, «Registro manual de dispositivos para Windows Autopilot», 24 de marzo de 2023. https://learn.microsoft.com/es-es/mem/autopilot/manual-registration (accedido 13 de abril de 2023).

[43]. Brenduns, «Obtenga información sobre las líneas base de seguridad de Windows que puede implementar con Microsoft Intune», 16 de marzo de 2023. https://learn.microsoft.com/es-es/mem/intune/protect/security-baselines (accedido 13 de abril de 2023).

[44]. MandiOhlinger, «Configuración de pantalla completa para Windows 10/11 en Microsoft Intune», 4 de abril de 2023. https://learn.microsoft.com/es-es/mem/intune/configuration/kiosk-settings-windows (accedido 13 de abril de 2023).

[45]. frankroj, «Creación de grupos de dispositivos para Windows Autopilot», 14 de marzo de 2023. https://learn.microsoft.com/es-es/mem/autopilot/enrollment-autopilot (accedido 13 de abril de 2023).

[46]. «Introducción a los tipos de inscripción de dispositivos Apple», Apple Support. https://support.apple.com/es-es/guide/deployment/dep08f54fcf6/web (accedido 14 de abril de 2023).

[47]. lenewsad, «Inscripción de dispositivos iOS/iPadOS en Microsoft Intune - Microsoft Intune», 23 de noviembre de 2022. https://learn.microsoft.com/es-es/mem/intune/enrollment/ios-enroll (accedido 9 de febrero de 2023).

[48]. Brenduns, «Configuración de cumplimiento de dispositivos iOS/iPadOS en Microsoft Intune», 16 de marzo de 2023. https://learn.microsoft.com/es-es/mem/intune/protect/compliance-policy-create-ios (accedido 13 de abril de 2023).

[49]. MandiOhlinger, «Creación de perfiles de dispositivos iOS/iPadOS o macOS con Microsoft Intune», 4 de abril de 2023. https://learn.microsoft.com/es-es/mem/intune/configuration/device-features-configure (accedido 13 de abril de 2023).

[50]. Brenduns, «Uso de directivas de Microsoft Intune para administrar las actualizaciones de software de iOS/iPadOS», 16 de marzo de 2023. https://learn.microsoft.com/es-es/mem/intune/protect/software-updates-ios (accedido 13 de abril de 2023).

[51]. Smritib17, «Activación del modo supervisado de iOS/iPadOS con Microsoft Intune», 4 de abril de 2023. https://learn.microsoft.com/es-

es/mem/intune/remote-actions/device-supervised-mode (accedido 13 de abril de 2023).

[52]. Erikre, «¿Qué es la administración de aplicaciones de Microsoft Intune?», 3 de abril de 2023. https://learn.microsoft.com/es-es/mem/intune/apps/app-management (accedido 13 de abril de 2023).

[53]. MandiOhlinger, «Plataformas y tipos de directivas compatibles con los filtros en Microsoft Intune», 4 de abril de 2023. https://learn.microsoft.com/es-es/mem/intune/fundamentals/filters-supported-workloads (accedido 13 de abril de 2023).

[54]. Erikre, «Información general de las directivas de protección de aplicaciones - Microsoft Intune», 4 de abril de 2023. https://learn.microsoft.com/es-es/mem/intune/apps/app-protection-policy (accedido 13 de abril de 2023).

[55]. Erikre, «Agregar directivas de configuración de aplicaciones para dispositivos iOS/iPadOS administrados - Microsoft Intune», 3 de abril de 2023. https://learn.microsoft.com/es-es/mem/intune/apps/app-configuration-policies-use-ios (accedido 13 de abril de 2023).

[56]. Erikre, «Introducción al SDK de Microsoft Intune App», 4 de abril de 2023. https://learn.microsoft.com/es-es/mem/intune/developer/app-sdk-get-started (accedido 13 de abril de 2023).

[57]. Erikre, «Perfiles de aprovisionamiento de aplicaciones de iOS/iPadOS en Microsoft Intune», 3 de abril de 2023. https://learn.microsoft.com/es-es/mem/intune/apps/app-provisioning-profile-ios (accedido 13 de abril de 2023).

[58]. MandiOhlinger, «Guía de inscripción de dispositivos para Microsoft Intune», 23 de noviembre de 2022. https://learn.microsoft.com/es-es/mem/intune/fundamentals/deployment-guide-enrollment (accedido 8 de febrero de 2023).

Anexos

- Instalación del conector de Intune en un servidor

Los requisitos para instalar el conector en un *equipo distinto al controlador de dominio* (recomendación de seguridad de Microsoft) son un *usuario con rol de administrador global o administrador de Intune*, que la *cuenta de servicio esté sincronizada con el AD local*, una *licencia de Microsoft Intune* y que el *equipo tenga permisos para crear objetos informáticos* dentro del dominio (para esto, el AD está obligado a delegarle esos controles).

Se empieza creando el usuario administrador. Para ello, hay que acceder a la unidad organizativa donde se encuentran los demás usuarios y se crea un objeto nuevo de tipo usuario (con nombre, por ejemplo, admadm). Después, se fuerza la sincronización del usuario en Azure con el comando *Start-ADSyncSyncCycle -PolicyType Delta* en la aplicación Windows PowerShell desde el servidor en el que esté alojado el Azure AC Connect. Una vez se ven reflejados los cambios en Azure AD, se continua con la instalación del conector de Intune.

El siguiente paso es crear una unidad organizativa en la que se vayan a ubicar todos los dispositivos AutoPilot y, en otro servidor que no sea el DC, se instala el conector de Intune. El enlace del .exe lo proporciona Intune, como se puede ver en la siguiente Figura.

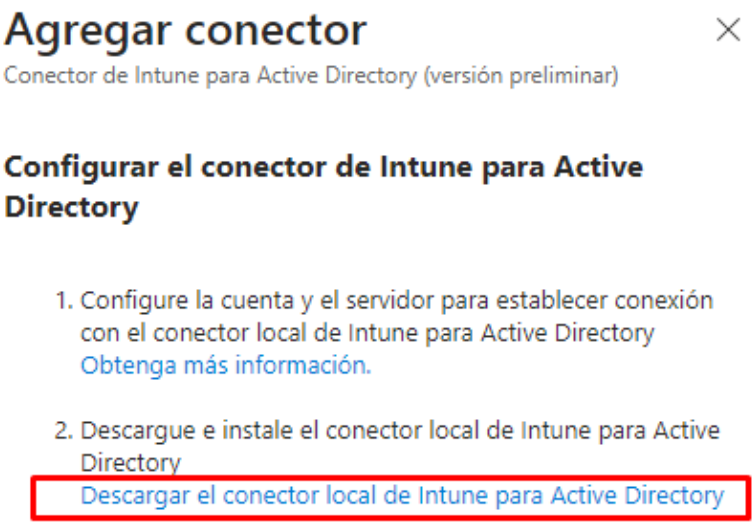


Figura 68. *Enlace proporcionado por Intune para instalar el conector*

Ahora, en el servidor elegido (que no sea el DC), se instala el enlace descargado. Una vez terminada la instalación, desde el DC hay que delegarle a ese servidor los controles sobre la unidad organizativa creada. Se customizan las tareas que se quieran delegar, concretamente las relacionadas a los objetos de tipo computadoras. Se le asignará control total de todo lo que tenga que ver con ese tipo de objeto y una vez hecho eso, ya estará la unidad organizativa configurada y se podrán inscribir dispositivos AutoPilot híbridos.

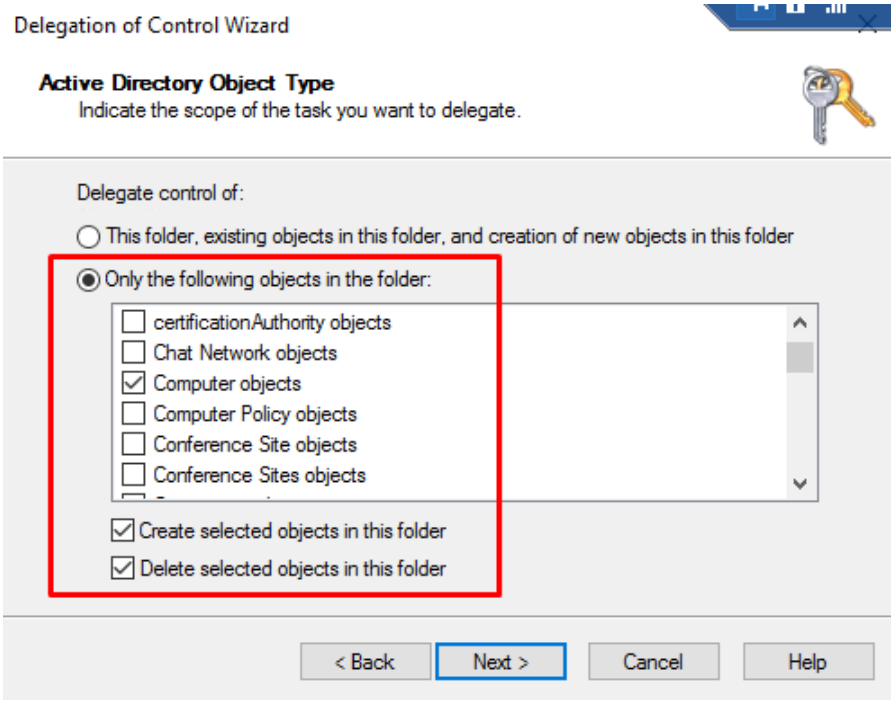


Figura 69. *Ajustes delegación de controles para la creación de objetos de tipo computadoras*

Por último, desde el centro de administración Microsoft Intune comprobar que el conector está activo y, por tanto, haber realizado con éxito la instalación de este.

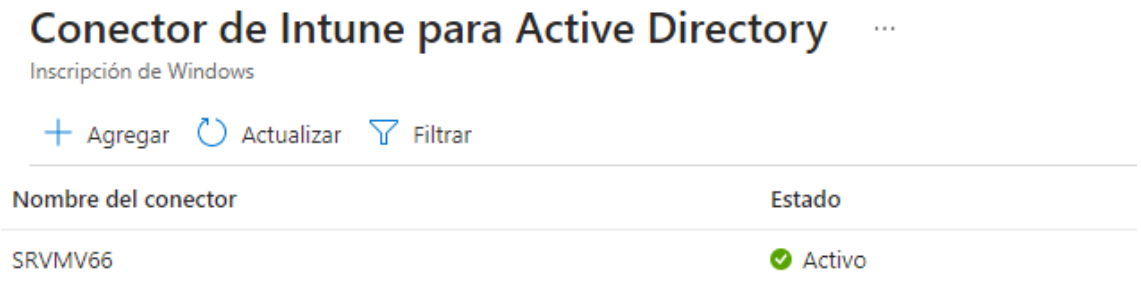


Figura 70. *Conector de Intune*

- Desinstalación del conector de Intune de un servidor

Para desinstalar el Conector de Intune para Active Directory, lo único que hay que hacer es ejecutar el mismo archivo .exe en el servidor del que se quiere eliminar. Cuando se ejecuta en un servidor en el que ya está instalado, la única opción disponible es quitar la instalación del conector actual.

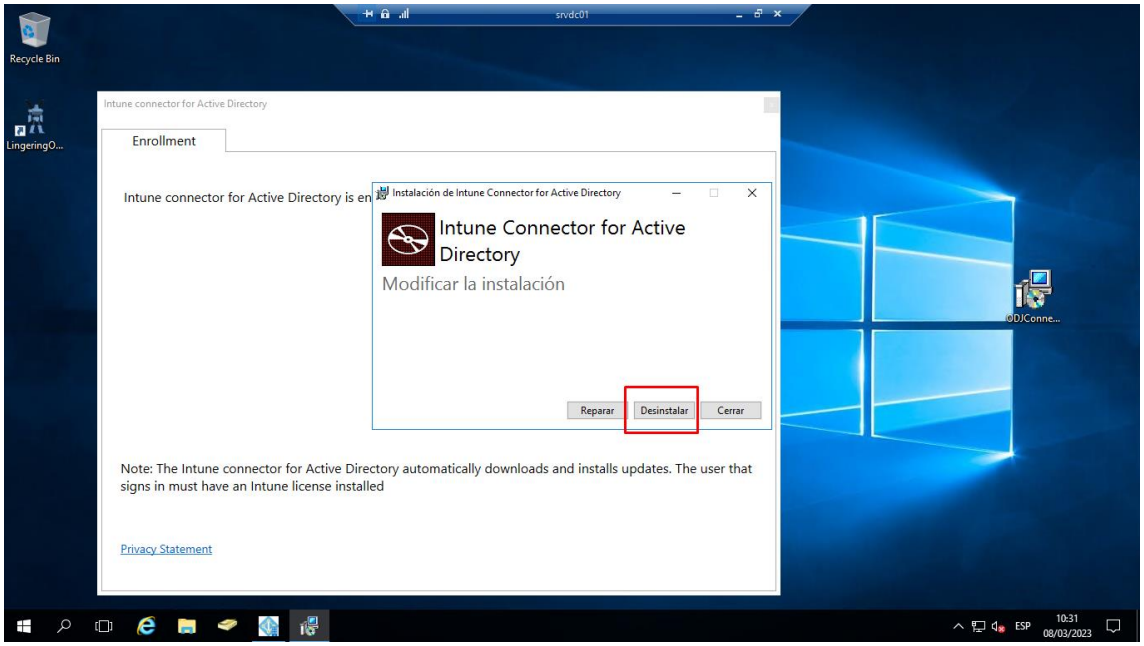


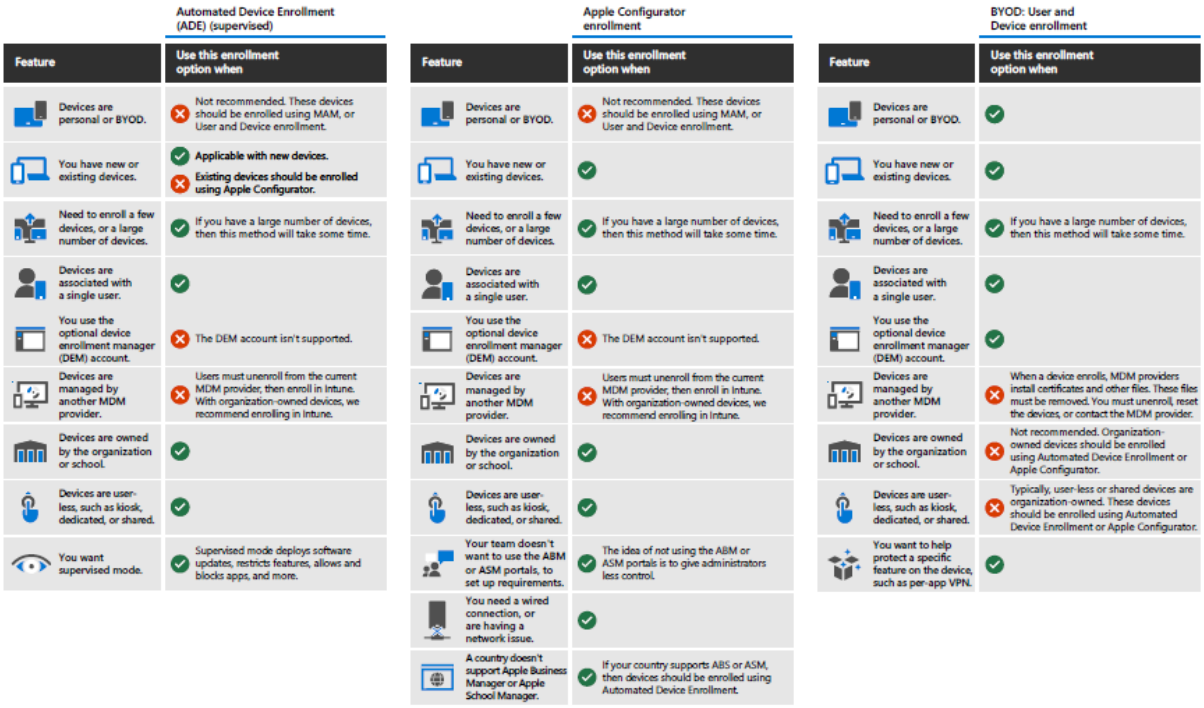
Figura 71. *Desinstalación del conector de Intune de un servidor.*

- Formas de enrolado de dispositivos Windows en Microsoft Intune

	Windows Automatic enrollment	Windows Autopilot	BYOD: User enrollment	Co-management with Configuration Manager
Feature	**Use this enrollment option when**	**Use this enrollment option when**	**Use this enrollment option when**	**Use this enrollment option when**
You have Azure AD Premium.	✓	✓ Windows Autopilot uses Automatic enrollment. Automatic enrollment requires Azure AD Premium.	✗ Azure AD Premium isn't required. ✓ If the devices join Azure AD, then they can use Azure AD Premium features.	✓ Depending on your co-management configuration, Azure AD Premium may be required.
You'll use Conditional Access on devices enrolled via bulk enrollment.	✓ Available on Windows 11 and Windows 10 1803+.	Not applicable	Not applicable	✓
You purchase devices from an OEM that supports the Windows Autopilot service.	✗ If your OEM supports Windows Autopilot, then use Windows Autopilot enrollment.	✓	Not applicable	✓
Devices are hybrid Azure AD joined.	✗ Automatic enrollment is available for full Azure AD joined devices (cloud-native endpoints).	✓ Hybrid Azure AD joined devices are joined to your on-premises AD, and registered with your Azure AD. Devices registered in Azure AD are available to Intune.	✓ Users should know that their personal devices might be managed by the organization IT.	✓ Hybrid Azure AD joined devices are joined to your on-premises AD, and registered with your Azure AD. Devices registered in Azure AD are available to Intune.
You have remote workers.	✓	✓ With Windows Autopilot, the OEM can ship devices directly to users.	✓ Users should know that their personal devices might be managed by the organization IT.	✓
Devices are personal or BYOD.	✓	✗ For BYOD or personal devices, use Windows automatic enrollment or a User enrollment option.	✓	✓
You have new or existing devices.	✓	✓ You can update desktops running older Windows versions, e.g. Windows 7 to 10. This option also uses Microsoft Endpoint Configuration Manager.	✓	✓ For devices that aren't running Windows 10/11, such as Windows 7, you'll need to upgrade.
Need to enroll a few devices, or a large number of devices.	✓ Bulk enrollment is available for organization-owned devices, not personal/BYOD.	✓	✓	✓
Devices are associated with a single user.	✓	✓	✓	✓
You use the optional device enrollment manager (DEM) account.	✓	✓	✗ DEM accounts don't apply to User enrollment.	✗ DEM accounts don't apply to co-management.
Devices are managed by another MDM provider.	✗ To be fully managed by Intune, users need to unenroll from the current MDM provider, and then enroll in Intune.	✗ To be fully managed by Intune, users need to unenroll from the current MDM provider, and then enroll in Intune.	✓ A device managed by another MDM provider can register in Azure AD. ✗ For Intune, users need to unenroll from the current provider, and then enroll in Intune.	✗ To be co-managed, users need to unenroll from the current MDM provider. They shouldn't be enrolled using the Intune classic agents.
Devices are owned by the organization or school.	✓	✓	✓ You can use User enrollment, but it's recommended to use Windows Autopilot, or Windows Automatic enrollment.	✓
Devices are user-less, such as kiosk, dedicated, or shared.	✓ Requires users to sign in with their organization account and automatically enroll. Then create a kiosk profile, and assign it to this device.	✓ Requires users to sign in with their organization account and automatically enroll. Then create a kiosk profile, and assign it to this device.	✗ Requires a user to sign in with an organization account, and use the Settings app, which isn't common on shared devices.	✓ Requires users to sign in with their organization account and automatically enroll. Then create a kiosk profile, and assign it to this device.
Devices are enrolled in Intune.	Not applicable	Not applicable	Not applicable	✓ You have devices you want to bring to co-management. Devices may have been enrolled using Windows Autopilot, or directly from your hardware OEM.

Figura 72. *Enrolado dispositivos Windows en Intune. [58]*

- Formas de enrolado de dispositivos iOS/iPadOS en Microsoft Intune



Feature	Automated Device Enrollment (ADE) (supervised) — Use this enrollment option when
Devices are personal or BYOD.	Not recommended. These devices should be enrolled using MAM, or User and Device enrollment.
You have new or existing devices.	Applicable with new devices. Existing devices should be enrolled using Apple Configurator.
Need to enroll a few devices, or a large number of devices.	If you have a large number of devices, then this method will take some time.
Devices are associated with a single user.	✓
You use the optional device enrollment manager (DEM) account.	The DEM account isn't supported.
Devices are managed by another MDM provider.	Users must unenroll from the current MDM provider, then enroll in Intune. With organization-owned devices, we recommend enrolling in Intune.
Devices are owned by the organization or school.	✓
Devices are user-less, such as kiosk, dedicated, or shared.	✓
You want supervised mode.	Supervised mode deploys software updates, restricts features, allows and blocks apps, and more.

Feature	Apple Configurator enrollment — Use this enrollment option when
Devices are personal or BYOD.	Not recommended. These devices should be enrolled using MAM, or User and Device enrollment.
You have new or existing devices.	✓
Need to enroll a few devices, or a large number of devices.	If you have a large number of devices, then this method will take some time.
Devices are associated with a single user.	✓
You use the optional device enrollment manager (DEM) account.	The DEM account isn't supported.
Devices are managed by another MDM provider.	Users must unenroll from the current MDM provider, then enroll in Intune. With organization-owned devices, we recommend enrolling in Intune.
Devices are owned by the organization or school.	✓
Devices are user-less, such as kiosk, dedicated, or shared.	✓
Your team doesn't want to use the ABM or ASM portals, to set up requirements.	The idea of not using the ABM or ASM portals is to give administrators less control.
You need a wired connection, or are having a network issue.	✓
A country doesn't support Apple Business Manager or Apple School Manager.	If your country supports ABS or ASM, then devices should be enrolled using Automated Device Enrollment.

Feature	BYOD: User and Device enrollment — Use this enrollment option when
Devices are personal or BYOD.	✓
You have new or existing devices.	✓
Need to enroll a few devices, or a large number of devices.	If you have a large number of devices, then this method will take some time.
Devices are associated with a single user.	✓
You use the optional device enrollment manager (DEM) account.	✓
Devices are managed by another MDM provider.	When a device enrolls, MDM providers install certificates and other files. These files must be removed. You must unenroll, reset the devices, or contact the MDM provider.
Devices are owned by the organization or school.	Not recommended. Organization-owned devices should be enrolled using Automated Device Enrollment or Apple Configurator.
Devices are user-less, such as kiosk, dedicated, or shared.	Typically, user-less or shared devices are organization-owned. These devices should be enrolled using Automated Device Enrollment or Apple Configurator.
You want to help protect a specific feature on the device, such as per-app VPN.	✓

Figura 73. *Enrolado dispositivos OS/iPadOS en Intune. [58]*

- Retirar, borrar, reiniciar, eliminar y empezar de cero un dispositivo

Cada una de estas acciones tiene un propósito específico y es importante entender las implicaciones desde cada una de ellas antes de llevarlas a cabo. Como medida de precaución, es recomendable hacer copias de seguridad de los datos importantes antes de llevar a cabo cualquiera de estas acciones.

- Retirar

Cuando se retira un dispositivo en Intune, se elimina el control de Intune sobre él. Es decir, el dispositivo deja de estar administrado por Intune y, por tanto, todas las políticas, configuraciones y aplicaciones que se le hayan asignado dejarán de estar vigentes en él.

Si el dispositivo está encendido y conectado, la acción *Retirar* se propaga por todos los tipos de dispositivos en menos de 15 minutos.

- Borrar

Borrar un dispositivo desde Intune significa que se borran todos los datos del dispositivo, incluyendo aplicaciones, configuraciones, políticas, archivos y cualquier otra información almacenada en el dispositivo. Es decir, se va a restaurar el dispositivo a su configuración de fábrica. Esta acción es irreparable y no se puede deshacer, por lo que es importante tener precaución antes de llevarla a cabo. Si no se quieren quitar los datos de usuario, es posible conservarlos si se activa la casilla *Conservar el estado de inscripción y la cuenta de usuario*.

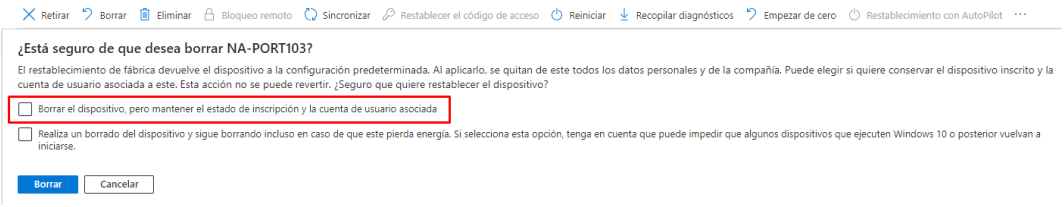


Figura 74. *Opción conservar el estado de inscripción y la cuenta del usuario tras la acción de Borrar el dispositivo*

Un borrado es útil para restablecer un dispositivo antes de dárselo a otro usuario o en el caso de que el dispositivo se haya perdido o lo hayan robado. Hay que tener cuidado al seleccionar *Borrar*, ya que los datos del dispositivo no se pueden recuperar. En dispositivos Windows, esta opción solo está disponible para Windows 10 versión 1709 o posteriores.

- Reiniciar

Esta acción lo que hace es simplemente permitir reiniciar el dispositivo desde Intune, algo que puede ser muy útil para aplicar cambios de configuración o solucionar problemas técnicos. Al aplicar esta acción, no se borran datos ni configuraciones del dispositivo.

Al usuario del dispositivo, por defecto, no se le notifica del reinicio, por lo que es importante que el administrador avise antes, evitando así que puedan perder el trabajo que estén haciendo en ese momento. Aunque es posible habilitar la opción de mostrar al usuario un mensaje con el texto: “El administrador de dispositivo ha programado un reinicio”. Cuando el mensaje se muestra, se inicia un contador de reinicio de 5 minutos.

En dispositivos Windows, esta acción es compatible con Windows 8.1 y versiones posteriores y en dispositivos iOS/iPadOS solo está disponible para dispositivos supervisados.

- Eliminar

Cuando se elimina un dispositivo de Intune, se van a borrar todas las asociaciones de Intune con ese dispositivo y no va a poder obtener acceso a los recursos corporativos de la empresa. Esto significa que ya no se van a poder administrar ni proteger los datos del dispositivo desde Intune. Sin embargo, los datos y las configuraciones en el dispositivo seguirán siendo los mismos, siendo posible que se borren de él los datos de la empresa en caso de que este intente sincronizarse tras su eliminación.

- Empezar de cero

Esta acción implica restablecer el dispositivo a su configuración de fábrica, lo que significa que se van a borrar todos los datos y configuraciones del dispositivo. Esto es útil cuando se quiere eliminar toda la información personal o cualquier configuración dañada en el dispositivo y empezar desde cero con una configuración “limpia”.

Con esta acción está dirigida sólo a dispositivos Windows. Se van a quitar las aplicaciones ya instaladas en un equipo que ejecuta Windows 10 versión 1709 o posterior. Además, ayuda a eliminar las aplicaciones preinstaladas (OEM) que normalmente se instalan con un nuevo equipo.

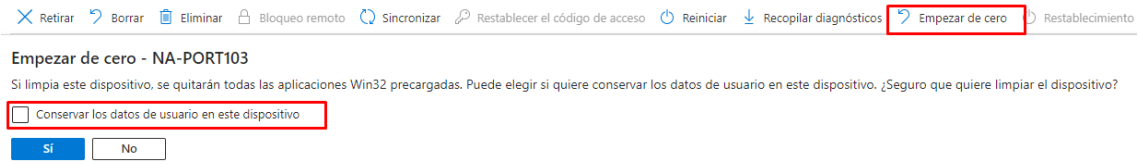


Figura 75. *Opción conservar los datos de usuario en un dispositivo tras la acción Empezar de cero el dispositivo*

Si se selecciona la opción *Conservar los datos de usuario en este dispositivo*, se mantiene el dispositivo unido a Azure AD, el dispositivo vuelve a estar inscrito en la administración de dispositivos móviles cuando un usuario habilitado de Azure Active Directory inicia sesión en el dispositivo y se mantiene el contenido de la carpeta Inicio del usuario del dispositivo, las aplicaciones y la configuración.

- Bloqueo remoto de dispositivos iOS/iPadOS con Intune

El bloqueo remoto de dispositivos iOS/iPadOS con Intune es una función interesante ya que ayuda a garantizar la seguridad y privacidad de los datos empresariales. Cuando un dispositivo iOS/iPadOS se pierde o se roba, es importante bloquearlo inmediatamente para evitar el acceso no autorizado a los datos de la empresa. Para bloquearlo, el administrador de IT lo único que tiene que hacer es seleccionar desde el centro de administración de Intune el dispositivo de la lista de dispositivos administrados en Intune y seleccionar la opción *Bloqueo remoto*. Además, el bloqueo remoto permite también al administrador borrar todos los datos del dispositivo en caso de que sea imposible recuperarlo.