Gestión moderna del puesto de trabajo

Edgar Mera Couto
Grado de Ingeniería Informática
Administración de Redes y Sistemas Operativos

Mario Prieto Vega
Montse Serra Vicern / David Bañeres Besora

Fecha Entrega 15/01/2023

Esta obra está sujeta a una licencia de Reconocimiento-NoComercial-SinObraDerivada 3.0 España de Creative Commons

Agradecimientos y dedicatoria:

Han pasado 3044 días desde aquel 15 de septiembre de 2014 en el que comencé mi aventura, animado y respaldado por mi pareja y mis padres. 3044 duros y largos días, con pocas horas de sueño, muchas de dedicación sentado delante de un ordenador, y muchos planes postpuestos.

Quiero agradecer, en mi primer lugar, el apoyo a Elena, mi futura esposa. Sin ti, el camino habría sido todavía más duro. Gracias por el apoyo constante y la comprensión, a pesar de perdernos tantos planes juntos durante estos más de 8 años. Prometo hacer todo lo posible por recuperar el tiempo perdido a partir de ahora y retomar esos viajes aparcados, vuelta al mundo incluida (algún día).

A mis padres, José y María, por el respaldo ofrecido no solo durante este tiempo, procurando no interrumpir mis horas de estudio ni si quiera con llamadas, si no durante toda mi vida, siempre apoyando mis decisiones.

También a Manolo y Conchita, mis suegros. Nunca nadie me ha preguntado tantas veces: ¿qué tal la carrera? Muchas gracias por vuestra constante preocupación e interés.

Por último, no quiero terminar estas líneas sin dedicar este trabajo a mi hija Blanca. Llevo invertido en él casi media vida tuya, pero a partir de ahora todo mi tiempo va a ser para ti. Estoy seguro de que el esfuerzo habrá valido la pena para los dos y confío en poder enseñarte parte de las cosas aprendidas.

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Gestión moderna del puesto de trabajo*
Nombre del autor:	*Edgar Mera Couto*
Nombre del consultor/a:	*Mario Prieto Vega*
Nombre del PRA:	*Montse Serra Vizern / David Bañeres Besora*
Fecha de entrega (mm/aaaa):	01/2023
Titulación:	*Grado de Ingeniería Informática*
Área del Trabajo Final:	*Administración de Redes y Sistemas Operativos*
Idioma del trabajo:	*Castellano*
Palabras clave	*Workplace, MDM, Intune*

Resumen del Trabajo (máximo 250 palabras): *Con la finalidad, contexto de aplicación, metodología, resultados y conclusiones del trabajo.*

El trabajo tiene como objetivo analizar la situación actual de las organizaciones en lo que al puesto de trabajo del usuario se refiere. Se plasma la evolución experimentada en las dos últimas décadas y se identifican las nuevas necesidades surgidas debido, principalmente, a la gran adopción de Internet, la transformación digital y la movilidad.

Así, trata de poner de manifiesto la importancia que tiene la gestión del puesto de trabajo en los entornos corporativos y reflejar los motivos que conducen a las compañías a invertir esfuerzos en ello. Se muestran algunas de las herramientas tradicionales en las que se apoyan las organizaciones para gestionar y administrar su parque de dispositivos y se evidencia como dichas herramientas no son capaces de cubrir las necesidades de los nuevos escenarios.

Por ello, se realiza un estudio de los beneficios que aportan las nuevas soluciones cloud de MDM respecto a las tradicionales y se comparan las tres principales soluciones de mercado con el fin de decantarse por la que mejor se adapte, de forma general, a la mayor parte de los entornos empresariales. A continuación, se detalla el proceso de configuración e implantación de la solución MDM cloud elegida, primero de forma aislada como herramienta única y, por último, integrada con la herramienta de gestión tradicional.

Como conclusión, se extrae que las nuevas soluciones MDM cloud pueden encajar en determinados entornos modernos, pero habitualmente siguen siendo necesarias algunas funcionalidades únicamente presentes en las herramientas tradicionales, por lo que tienden a coexistir ambas.

Abstract (in English, 250 words or less):

The main aim of this final degree project is to analyze the workplace current situation on enterprise environments. It shows the evolution experienced in the last two decades and identifies the new needs that have arisen mainly due to the widespread adoption of the Internet, digital transformation and mobility.

Thus, it tries to highlight the importance of workplace management in corporate environments and reflect the reasons that lead companies to invest efforts in it. It shows some of the traditional tools on which organizations rely to manage and administer their fleet of devices and it is also shown how these tools are not able to meet the needs of the new scenarios.

Therefore, a study of the benefits of the new MDM cloud solutions compared to the traditional is carried out and the three main market solutions are compared in order to opt for the one that best suits, in general terms, the majority of business environments. The process of configuration and implementation of the chosen MDM cloud solution is then detailed, first in full cloud mode as a single tool, and finally integrated with the traditional management tool.

The conclusion is that the new MDM cloud solutions can fit in certain modern environments, but some functionalities that are only present in traditional tools are still usually necessary, so both tend to coexist.

Índice

1. Introducción ... 1
1.1 Motivación del proyecto ... 1
1.2 Breve descripción del proyecto ... 1
1.3 Objetivos del proyecto ... 2
1.4 Requerimientos o funcionalidades ... 2
1.5 Viabilidad tecnológica del proyecto ... 2
1.6 Planificación general ... 3
1.7 Dificultad del proyecto ... 5
2. La gestión del puesto de trabajo ... 6
2.1 Definición ... 6
2.2 La importancia de la gestión del puesto de trabajo ... 7
2.3 Cómo elegir la solución adecuada ... 8
2.4 Soluciones tradicionales ... 11
2.5 Análisis de la situación actual ... 13
2.6 Beneficios que aporta el cloud ... 14
2.7 Comparativa de las principales soluciones de mercado ... 17
3. Solución MDM completamente cloud ... 21
3.1 Definición de requisitos ... 22
3.2 Diseño y arquitectura ... 23
3.3 Configuración de la solución MDM Intune ... 24
3.3.1 Licenciamiento ... 25
3.3.2 Configuración de requisitos previos ... 27
3.3.3 Creación de grupos de seguridad ... 32
3.3.4 Perfiles de inscripción e implementación ... 34
3.3.5 Directivas de cumplimiento ... 37
3.3.6 Perfiles de configuración ... 49
3.3.7 Acceso condicional ... 57
3.3.8 Gestión de actualizaciones ... 59
3.3.9 Gestión de aplicaciones ... 63
3.3.10 Personalización de la experiencia de usuario ... 68
3.3.11 Alta de usuarios y asignación de licencia ... 69
4. Pruebas de gestión de dispositivos ... 69
4.1 Preparación de dispositivos ... 70
4.2 Inscripción en Microsoft Intune ... 70
4.3 Comprobación de estado y monitorización ... 79
4.4 Acciones desde el portal de administración ... 81
5. Proceso de migración para transición al cloud ... 83
5.1 Integración de Intune con MECM ... 83
6. Conclusiones ... 87
7. Glosario ... 89
8. Bibliografía ... 92
9. Anexos ... 96
Anexo 1. Creación de certificado push MDM de Apple ... 96
Anexo 2. Creación de una cuenta empresarial de Google ... 99
Anexo 3. Creación de grupos de seguridad en Intune ... 105
Anexo 4. Creación de perfil de implementación Windows AutoPilot ... 109

Anexo 5. Creación de directivas de cumplimiento 112
Anexo 6. Creación de perfiles de configuración 137
Anexo 7. Creación de directiva de acceso condicional 156
Anexo 8. Creación de perfiles de actualización 159
Anexo 9. Despliegue de aplicaciones por plataforma 167
Anexo 10. Creación de directiva de personalización 183
Anexo 11. Creación de usuarios y asignación de licencias 187
Anexo 12. Creación de máquina virtual Ubuntu 194
Anexo 13. Proceso de inscripción de dispositivos en Intune 205
Anexo 14. Proceso de integración de Intune con MECM 240

Lista de figuras

Figura 1 - Diagrama de Gantt del proyecto 3
Figura 2 - Diagrama de Gantt Hito 1 4
Figura 3 - Diagrama de Gantt Hito 2 4
Figura 4 - Diagrama de Gantt Hito 3 4
Figura 5 - Diagrama de Gantt Hito 4 5
Figura 6 - Cuota de mercado global de sistemas operativos cliente 9
Figura 7 - Arquitectura MDT + WDS 12
Figura 8 - Ejemplo de arquitectura de SCCM 13
Figura 9 - Gartner Magic Quadrant for Unified Endpoint Management Tools 18
Figura 10 - Arquitectura MEM – MECM + Intune 19
Figura 11 - Arquitectura cloud Workspace ONE 20
Figura 12 - Arquitectura cloud Ivanti Neurons for Unified Endpoint Protection 21
Figura 13 - Cuota de mercado de las principales herramientas de productividad a febrero de 2022 23
Figura 14 - Arquitectura de Microsoft Intune 24
Figura 15 - Suscripciones y licencias del entorno de laboratorio 1 de 2 25
Figura 16 - Suscripciones y licencias del entorno de laboratorio 2 de 2 25
Figura 17 - Licencias de Intune en el entorno de laboratorio 27
Figura 18 - Configuración del nombre del tenant de Azure Active Directory 27
Figura 19 - Estado inicial de Microsoft Intune 28
Figura 20 - Inscripción automática de dispositivos Windows en Intune 29
Figura 21 - Acceso a obtención del certificado push MDM de Apple en Intune 30
Figura 22 - Configuración de certificado push MDM de Apple en Intune 31
Figura 23 - Configuración de Google Play administrado en Intune 32
Figura 24 - Creación de grupo de seguridad en Intune 33
Figura 25 - Resumen de perfil de implementación de Windows AutoPilot 34
Figura 26 - Perfil de inscripción de dispositivos Android (BYOD) 35
Figura 27 - Token de inscripción de dispositivos Android corporativos 36
Figura 28 - Frecuencias de sincronización por plataforma en Intune 38
Figura 29 - Configuración global de directivas de cumplimiento de Intune 38
Figura 30 - Directiva de cumplimiento para dispositivos Windows 40
Figura 31 - Directiva de cumplimiento para dispositivos Android corporativos 42
Figura 32 - Directiva de cumplimiento para dispositivos Android BYOD 43
Figura 33 - Directiva de cumplimiento para dispositivos Apple macOS 45
Figura 34 - Directiva de cumplimiento para dispositivos Apple iOS/iPadOS 47
Figura 35 - Directiva de cumplimiento para dispositivos Linux 48
Figura 36 - Perfil de configuración de dispositivos Windows en Intune 51
Figura 37 - Perfil de configuración de dispositivos Android BYOD 52
Figura 38 - Perfil de configuración de dispositivos Android Corporativos 54
Figura 39 - Perfil de configuración de dispositivos Apple macOS 55
Figura 40 - Perfil de configuración de dispositivos Apple iOS/iPadOS 57
Figura 41 - Directiva de acceso condicional a Office 365 58
Figura 42 - Perfil de actualización de dispositivos Windows corporativos 60
Figura 43 - Perfil de actualización de dispositivos Apple macOS 62
Figura 44 - Perfil de actualización de dispositivos Apple iOS/iPadOS 63
Figura 45 - Funcionalidades de administración de aplicaciones de Intune 64

Figura 46 - Despliegue de aplicación en dispositivos Windows 65
Figura 47 - Despliegue de aplicación en dispositivos Android 66
Figura 48 - Despliegue de aplicación en dispositivos macOS 67
Figura 49 - Despliegue de aplicación en dispositivos iOS/iPadOS 68
Figura 50 - Licencias de usuario para la prueba de concepto 69
Figura 51 - Dispositivo Windows 11 inscrito en Intune vía AutoPilot 72
Figura 52 - Dispositivo Windows 10 inscrito en Intune vía Configuración 73
Figura 53 - Dispositivo Windows 10 BYOD registrado en Azure AD 74
Figura 54 - Dispositivo Android BYOD inscrito en Intune 75
Figura 55 - Error de acceso condicional por incumplimiento de directivas 76
Figura 56 - Dispositivo macOS inscrito en Intune 77
Figura 57 - Dispositivo iOS inscrito en Intune 78
Figura 58 - Dispositivo Linux inscrito en Intune 79
Figura 59 - Paneles de estado predefinidos de Intune 80
Figura 60 - Dispositivos inscritos en Intune 81
Figura 61 - Acciones de dispositivo disponibles en Intune 81
Figura 62 - Dispositivos unidos de forma híbrida a Azure AD 84
Figura 63 - Traspaso de cargas de trabajo de MECM a Intune 85
Figura 64 - Dispositivos con administración conjunta Intune-MECM 86

1. Introducción

1.1 Motivación del proyecto

De un tiempo a esta parte, las soluciones cloud se han ido imponiendo a las tradicionales on-premises y les han ido ganando terreno en el ámbito empresarial. Esto es debido, principalmente, al ahorro de costes que supone el uso de este tipo de tecnologías (basadas en el pago por uso) y a los beneficios que aportan, tanto a nivel técnico (simplicidad) como de gestión (centralización). Además, el gasto en servicios en la nube repercute de una manera más positiva a las compañías que el uso de soluciones on-premises (que conllevan adquirir infraestructura y licencias), pues se refleja en su balance de cuentas como OPEX en vez de como CAPEX.

Por otro lado, el uso de dispositivos electrónicos (ordenadores, tablets, smartphones) en el entorno laboral ha ido cobrando cada vez más peso, dejando de lado el papel en pro de la digitalización gracias a la transformación digital. Así, a medida que las empresas crecen también aumenta el número de dispositivos corporativos, por lo que se torna necesario establecer mecanismos para poder gestionarlos.

La gestión del puesto de trabajo del usuario, en lo que a sus dispositivos corporativos se refiere, consiste en administrar por completo dichos dispositivos y requiere de una infraestructura y una serie de herramientas para tal fin. Por ello, es otro de los pilares del área de sistemas de las compañías susceptible a ser migrado al cloud. Esto, conocido como gestión moderna del puesto de trabajo, será el objeto de este trabajo de fin de grado.

1.2 Breve descripción del proyecto

El proyecto consiste en exponer de qué trata la gestión del puesto de trabajo y su importancia para las compañías, analizando los beneficios que aporta el cloud y comparando las soluciones de mercado más reconocidas.

A continuación, y tras elegir la solución que mejor se adapte a la mayoría de los entornos empresariales, se definirá, de principio a fin, cómo realizar la gestión de los dispositivos del puesto de trabajo del usuario de cualquier organización mediante una solución cloud. Esto será puesto en práctica en la plataforma escogida y servirá como guía para cualquier administrador de sistemas que desee iniciarse en la gestión cloud del puesto de trabajo.
El alcance incluye la gestión de todo tipo de dispositivos corporativos estándar de usuario final (ordenadores, smartphones, tablets) independientemente del fabricante de estos.

1.3 Objetivos del proyecto

El proyecto tiene como propósito lograr los siguientes objetivos:

- Poner de manifiesto la importancia de la gestión del puesto de trabajo en las organizaciones.
- Identificar los beneficios de un MDM cloud respecto de los tradicionales on-premises.
- Evaluar las principales soluciones MDM cloud del mercado actuales.
- Definir la arquitectura estándar de la solución MDM escogida para la gestión del puesto de trabajo.
- Ofrecer una guía práctica de implementación en la solución MDM elegida.
- Proponer el proceso de migración a seguir para la transición al modelo cloud.

1.4 Requerimientos o funcionalidades

La solución MDM elegida debe permitir gestionar de manera completa todos los dispositivos estándar existentes en cualquier compañía independientemente de su fabricante. Se entiende por gestión completa la capacidad de administración total sobre estos a la hora de establecer configuraciones, restricciones, instalación de aplicaciones, actualizaciones de seguridad e incluso el borrado parcial o completo de los datos que alberguen.

Los requerimientos técnicos se limitan a que los dispositivos tengan conexión a Internet para poder contactar con la solución MDM cloud, por lo que no deben suponer ningún reto adicional para ninguna compañía tipo. En definitiva, son los siguientes:

- Dispositivo con conexión a Internet.
- Suscripción a solución MDM.

1.5 Viabilidad tecnológica del proyecto

Las soluciones de gestión de puesto de trabajo cloud llevan más de una década en el mercado y disponen de un alto grado de madurez. Son muchas las organizaciones que ya han adoptado una de estas soluciones, aunque todavía queda una gran parte de ellas por realizar la transición. Habitualmente, estas últimas suelen ser compañías de sectores más tradicionales como el financiero (banca, seguros) o instituciones públicas, que aún muestran cierto recelo por las tecnologías en la nube en relación con la privacidad de la información.

En cuanto a los requisitos técnicos mencionados en el apartado anterior, tampoco deberían suponer un obstáculo para ninguna compañía tipo que disponga de un área de sistemas de tecnologías de la información.

Por todo ello, el proyecto tiene una alta viabilidad tecnológica y su aplicación es de ámbito general.

1.6 Planificación general

El proyecto, que se enmarca en el área de "Administración de Redes y Sistemas Operativos" del grado de Ingeniería Informática, está comprendido entre los meses de octubre de 2022 y enero de 2023, siendo el 15 de enero de 2023 la fecha límite de entrega. La realización de este será llevada a cabo de lunes a domingo durante el periodo indicado.

El trabajo se ha divido en cuatro entregables parciales (hitos), coincidiendo con las pruebas de evaluación continua (PECs) de la asignatura y siguiendo la metodología de proyecto en cascada. Dichos hitos están divididos, a su vez, en diferentes tareas. Los cuatro hitos principales del proyecto son:

1. Hito 1: Propuesta de plan de trabajo del TFG.
2. Hito 2: Entrega de entre el 40% y el 60% del proyecto.
3. Hito 3: Entrega de entre el 80% y el 90% del proyecto.
4. Hito 4: Entrega final del proyecto.

A continuación, se muestra el diagrama de Gantt de los cuatro hitos principales:

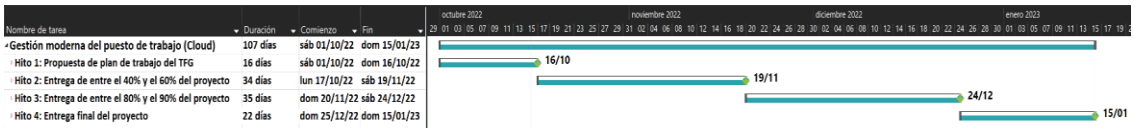


Figura 1 - Diagrama de Gantt del proyecto

Las tareas de cada hito, junto con su planificación en el diagrama de Gantt, son las siguientes:

- Hito 1: Propuesta de plan de trabajo del TFG.
  - Propuesta de título
  - Motivación del proyecto
  - Breve descripción del proyecto
  - Objetivos del proyecto
  - Requerimientos o funcionalidades
  - Viabilidad tecnológica
  - Planificación general
  - Dificultad del proyecto

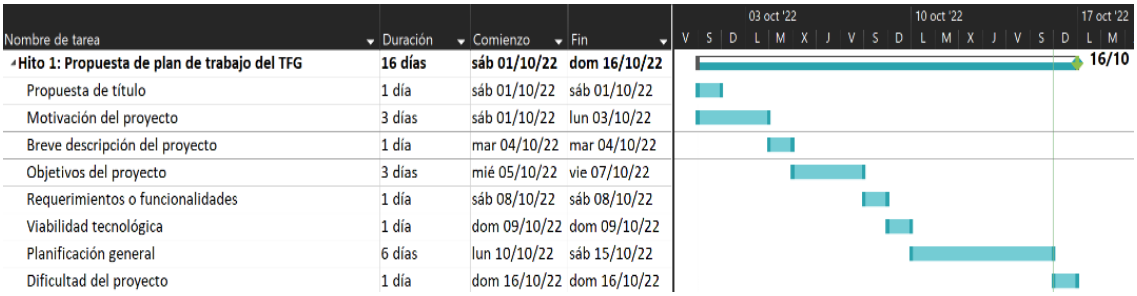


Figura 2 - Diagrama de Gantt Hito 1

- Hito 2: Entrega de entre el 40% y el 60% del proyecto.
  - Definición de la gestión del puesto de trabajo
  - La importancia de la gestión del puesto de trabajo
  - Cómo elegir la solución adecuada
  - Soluciones tradicionales
  - Análisis de la situación actual
  - Beneficios que aporta el cloud
  - Comparativa de las principales soluciones de mercado
  - Definición de requisitos
  - Diseño de la arquitectura de la solución escogida

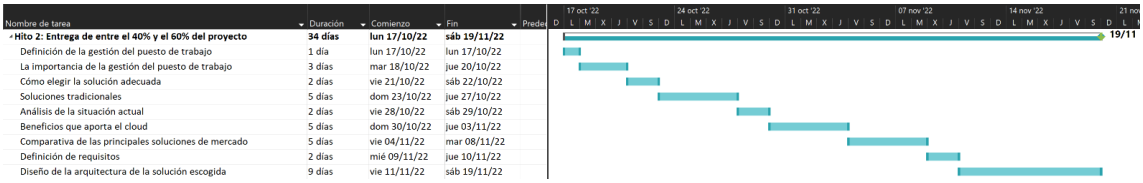


Figura 3 - Diagrama de Gantt Hito 2

- Hito 3: Entrega de entre el 80% y el 90% del proyecto.
  - Configuración de la solución de MDM
  - Preparación de dispositivos a utilizar
  - Inscripción de dispositivos en el MDM
  - Pruebas de gestión de dispositivos

Figura 4 - Diagrama de Gantt Hito 3

- Hito 4: Entrega final del proyecto.
  - Proceso de migración para transición al cloud
  - Conclusiones
  - Memoria final
  - Presentación

- Video de presentación
- Informe de autoevaluación
- Defensa del proyecto

Nombre de tarea	Duración	Comienzo	Fin	Predec
Hito 4: Entrega final del proyecto	**22 días**	**dom 25/12/22**	**dom 15/01/23**	
Proceso de migración para transición al cloud	2 días	dom 25/12/22	lun 26/12/22	
Conclusiones	2 días	mar 27/12/22	mié 28/12/22	
Memoria final	3 días	jue 29/12/22	sáb 31/12/22	
Presentación	5 días	dom 01/01/23	jue 05/01/23	
Video de presentación	5 días	vie 06/01/23	mar 10/01/23	
Informe de autoevaluación	3 días	mié 11/01/23	vie 13/01/23	
Defensa del proyecto	2 días	sáb 14/01/23	dom 15/01/23	

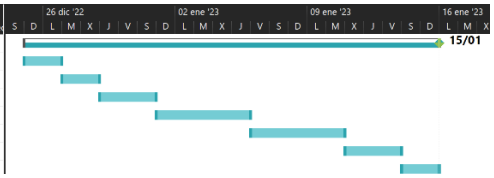


Figura 5 - Diagrama de Gantt Hito 4

1.7 Dificultad del proyecto

El proyecto tiene un grado de dificultad medio-alto. Aunque los requerimientos técnicos para realizar la implementación no son elevados, la gestión del puesto de trabajo precisa de conocimientos amplios y específicos en diversas áreas (*hardware*, *software,* sistemas operativos, redes, seguridad…), por lo que está enfocado a profesionales con cierta experiencia en ese ámbito.

Por otro lado, el alcance, en lo referente a diferentes tipos de dispositivos y escenarios, es muy ambicioso, tratando de perseguir el objetivo de representar el entorno real al que se enfrentan la mayoría de las organizaciones. Esto supondrá llevar a cabo un gran número de personalizaciones independientes para abarcar los máximos escenarios posibles.

No obstante, la elección de una solución cloud facilitará en gran medida la consecución de los objetivos propuestos al simplificar todos los requisitos de infraestructura necesarios que habría que cubrir en caso de optar por una solución de gestión on-premises.

2. La gestión del puesto de trabajo

2.1 Definición

En el ámbito de las Tecnologías de la Información y la Comunicación, se entiende por gestión del puesto de trabajo el área que engloba todas aquellas actividades relacionadas con la gestión integral de los dispositivos informáticos que utilizan los empleados de una organización. A grandes rasgos, las actividades comprendidas son las siguientes:

- Adquisición de los dispositivos y licencias: selección de proveedor/es y modelos para construir el catálogo corporativo, así como bajo qué tipo de régimen se obtendrán (compra, leasing, renting o pago por uso).

- Gestión del ciclo de vida: definición del tiempo de vida útil de cada dispositivo (3 o 4 años suele ser lo habitual), proceso de reemplazo, reciclaje y/o destrucción.

- Administración: definición y aplicación de los estándares de configuración de la organización para cada tipo de dispositivo, además de inventariado y supervisión.

- Protección: definición y aplicación de todo tipo de medidas de seguridad sobre los dispositivos para prevenir posibles incidentes (ataques, robo o pérdida de información, etc.).

- Mantenimiento: control del estado de los dispositivos, soporte y solución de problemas.

- Actualización: provisión de nuevas funcionalidades y corrección de las existentes.

- Parcheo de vulnerabilidades: remediación de vulnerabilidades para mantener protegidos los dispositivos a lo largo de su ciclo de vida.

La necesidad de gestionar los dispositivos de trabajo de los usuarios ha ido en aumento a medida que el uso de ordenadores se ha establecido en el entorno laboral, a partir de la década de los 80[1]. La llegada de las redes de área local e Internet[2], ofreciendo conexión y eliminando el entorno aislado previo en el que convivían esos dispositivos, ha afianzado todavía más, si cabe, dicha necesidad.

2.2 La importancia de la gestión del puesto de trabajo

La transformación digital en el mundo laboral ha supuesto, entre otros, la digitalización de la información de las organizaciones y de sus procesos de negocio. Esto significa que, en la mayoría de las empresas, independientemente de su tamaño, el uso del papel y las tecnologías analógicas (como la máquina de escribir) ha sido desbancado por la utilización de dispositivos electrónicos[3].

¿Cuán importante es la gestión del puesto de trabajo? Para responder a esta pregunta es necesario analizar qué supone para las compañías las actividades que engloba la gestión del puesto de trabajo.

En primer lugar, es imprescindible estudiar las necesidades de la organización, tanto a nivel funcional como económico, para poder seleccionar los dispositivos que se utilizarán y bajo qué sistema/s operativo/s. Del mismo modo, dichas necesidades marcarán la elección de un tipo de licenciamiento u otro. Probablemente haya diferentes requisitos dentro de una misma organización, no solo a nivel de hardware (usuarios estándar, dirección, alto rendimiento, por ejemplo) como también de software (*suite* ofimática, software dedicado para tareas concretas, etc.), por lo que es conveniente definir los tipos de perfiles y elegir lo que se adapte a todas las necesidades. Es decir, se trata de buscar la homogeneidad en cuanto a hardware y software, optando por el menor número de dispositivos y sistemas operativos/aplicaciones. Esto facilitará todas las gestiones posteriores.

A continuación, se debe definir el ciclo de vida de cada dispositivo/software adquirido, así como el proceso de renovación o reemplazo y su posible reciclaje. Es un factor clave que tener en cuenta, no solo antes de su adquisición (evaluar si se sigue fabricando o hasta cuándo tiene soporte, por ejemplo) como una vez adquirido. La obsolescencia programada es una característica casi inherente a los dispositivos electrónicos, por lo que suelen tener un tiempo de uso limitado[4]. Por ello, hay que establecer su ciclo de vida para la organización y estipular cómo y cuándo se realizará el reemplazo. Además, dado que suelen contener información de la compañía, es indispensable establecer los mecanismos oportunos de borrado. No llevar a cabo todas estas acciones puede suponer un malfuncionamiento de los dispositivos debido a su antigüedad, no disponer de soporte del fabricante ante incidencias (también en lo referente al software), quedarse sin stock al dejar de fabricarse un dispositivo y no haber decidido su sustituto, e incluso la pérdida o robo de información confidencial por no haberla destruido de los dispositivos que ya no se utilizan.

Otro de los grandes pilares es la configuración y el mantenimiento de dichos dispositivos y sistemas operativos/aplicaciones. Estos deben configurarse y optimizarse para adaptarse a las necesidades del negocio, facilitando y promoviendo la productividad, sin perder de vista las buenas prácticas recomendadas por los fabricantes. De igual forma, hay que administrarlos con el objetivo de controlar que esas configuraciones persistan en el tiempo e impedir que sean alteradas por quien no deba, así como ir modificándolas en

función de nuevas necesidades que puedan surgir. Esa administración también permitirá mantenerlos actualizados y proporcionarles nuevas funcionalidades. Asimismo, es necesario contar con un inventario de los activos y conocer en qué estado se encuentran (en uso, inactivos, retirados…), dando también solución a problemas técnicos que puedan surgir.

Por último, la seguridad ha ido cobrando más relevancia en los últimos años debido al aumento del número y tipología de ataques (*ransomware, spyware, virus, malware, keyloggers*…)[5]. La gran mayoría de los dispositivos de trabajo están conectados a Internet y eso implica una mayor exposición, lo que, a su vez, obliga a incrementar la protección del puesto de trabajo en todo su conjunto (dispositivo, sistema operativo, aplicaciones, red, etc.).

Tras entender un poco más en detalle en qué consiste la gestión del puesto de trabajo, queda patente que pasar por alto cualquiera de los puntos expuestos va a tener un impacto directo en la productividad de la compañía y en su situación financiera. Una mala gestión supondrá, tarde o temprano, incurrir en costes adicionales. Además, cualquier incidente de seguridad se puede traducir en un gran daño reputacional y deterioro de la imagen marca, aparte de en una sanción económica en caso de verse afectados datos personales.

En definitiva, la gestión del puesto de trabajo es necesaria independientemente del tamaño de la organización. Como es lógico, cuanto mayor sea esta y, por tanto, más dispositivos se utilicen, será necesario dedicar más recursos y esfuerzos a dicha gestión, llegando incluso a crear varios departamentos que se encarguen de las actividades mencionadas anteriormente. No obstante, es una tarea necesaria también en pequeños negocios, aunque a veces se realice de forma más superficial.

2.3 Cómo elegir la solución adecuada

Para llevar a cabo todas las acciones indicadas sobre el parque de dispositivos corporativos de una empresa existen una serie de herramientas de apoyo. Se debe evaluar cada escenario concreto para decidir cuál o cuáles usar, ya que las necesidades serán diferentes en cada caso. Algunos datos importantes que tener en cuenta son el número de dispositivos a gestionar, bajo qué sistema operativo trabajan, qué se necesita gestionar de estos y qué inversión se va a realizar, no solo para implementar las soluciones sino también para su futuro mantenimiento y operación.

No es objeto de este trabajo ofrecer una solución universal válida para todo tipo de escenarios, pues no sería viable. Sin embargo, a continuación se indican una serie de puntos clave a tener en cuenta a la hora de elegir soluciones de gestión de puesto de trabajo.

- **Sistema operativo cliente**

Conocer qué sistemas operativos se quieren gestionar es uno de los factores clave a la hora de buscar soluciones de apoyo para la gestión del puesto de trabajo. De las distintas soluciones de mercado disponibles, cada una dispone de diferentes capacidades y permite gestionar determinados sistemas operativos. Por ese motivo, es primordial concretar qué sistemas operativos hay en el parque de dispositivos y cuáles de ellos se quieren gestionar.

Según StatCounter GlobalStats, el sistema operativo para equipos cliente predominante a nivel mundial en el último año es Microsoft Windows, con una cuota de mercado superior al 75%[6].

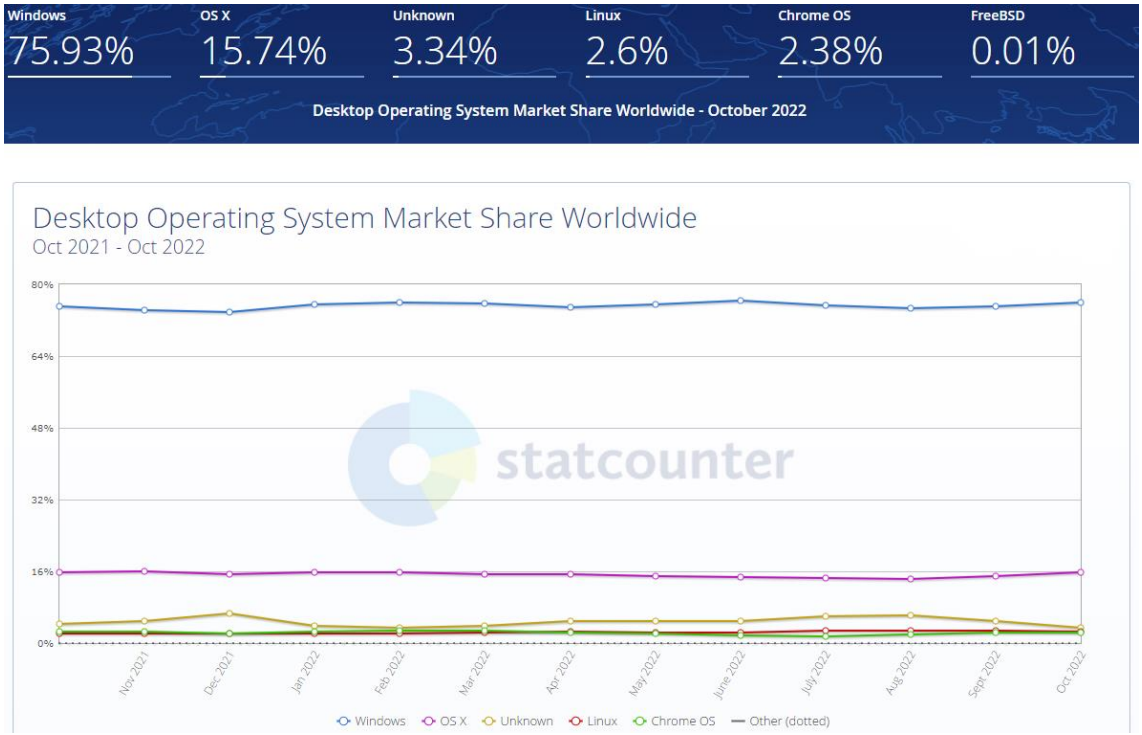


Figura 6 - Cuota de mercado global de sistemas operativos cliente

Fuente: https://gs.statcounter.com/os-market-share/desktop/worldwide

Aunque este dato tiene en cuenta tanto el mercado doméstico como el empresarial, sirve para tener una idea general de los actores principales. Según Statista, su estudio sobre "Los principales sistemas operativos usados por las empresas en España en 2019" revela que Microsoft Windows seguía liderando el mercado, estando presente en aproximadamente el 90% de las empresas del país[7].

- **Número de dispositivos a gestionar**

La cantidad de dispositivos que se necesita gestionar en la organización es un dato clave para decidir si es necesario utilizar herramientas con las que llevar a cabo su gestión o no. No hay un número concreto a partir del cual se precisen soluciones de apoyo, pero una buena aproximación sería cuando el coste de las herramientas (infraestructura y licenciamiento, en caso de ser de pago) y su mantenimiento sea inferior al de los recursos humanos necesarios para llevar a cabo las tareas de forma manual. Igualmente, se debe evaluar el valor que pueden aportar al negocio no solo las herramientas de gestión sino también las personas encargadas de esa gestión, pudiendo dedicar su tiempo a otras actividades gracias al apoyo de las herramientas. Un claro ejemplo de esto último es la automatización de tareas rutinarias como la instalación de software o la propia instalación y configuración de los sistemas operativos de los dispositivos.

- **Qué funciones o áreas se quieren gestionar**

Tener claro qué se quiere gestionar es otro de los factores clave que determinarán el uso y elección de las soluciones de gestión. Existen diversas herramientas en el mercado, cada una con diferentes funcionalidades. Si una empresa simplemente necesita disponer de un inventario de sus dispositivos, es probable que no requiera de ninguna herramienta extra de apoyo (podría obtener esa información de otras fuentes, como por ejemplo de un directorio activo si dispusiese de él, como es habitual). Sin embargo, lo más frecuente es que se quiera tener un mayor control sobre los dispositivos, como por ejemplo para restringir determinadas acciones, mantener las mismas versiones de sistemas operativos, distribuir aplicaciones de forma remota, etc. En ese caso, habrá que estudiar las soluciones con esas capacidades y elegir la que mejor se adapte a la compañía.

- **Coste**

El coste de las herramientas de gestión del puesto de trabajo también es un elemento relevante para las organizaciones, por lo que es otro de los componentes a considerar. El precio de una misma solución puede distar en función del cliente, en este caso las compañías. Por norma general, los proveedores de las soluciones tienen en cuenta una serie de variables (como el número de licencias a contratar, si ya se ha adquirido algún otro producto, etc.) a la hora de ofrecer un precio, lo que obliga a estudiar cada situación de forma independiente. Llevar a cabo la mejor decisión para la organización conlleva analizar en detalle la relación coste/funcionalidades que ofrece cada producto.

Dentro del coste de la solución (o soluciones), otro dato que tener en cuenta son los costes derivados de la propia solución, tales como los referentes a la infraestructura necesaria (servidores, bases de datos, energía…) y a la mano

de obra requerida para operarla y mantenerla. La suma de esos costes puede suponer que una solución más barata o incluso gratuita resulte finalmente más cara que una de pago, decantando la balanza hacia esta última.

Por otro lado, también se debe tasar cuánto supone no implementar herramientas dedicadas a la gestión e invertir en personal que realice las tareas manualmente. En situaciones donde hay muy poco personal dedicado a la gestión del puesto de trabajo, como en empresas pequeñas o incluso medianas, puede ser contraproducente adquirir soluciones de pago que no van a poder operarse ni mantenerse por falta de recursos y tiempo. Probablemente sea más rentable utilizar herramientas gratuitas, aunque con menos funcionalidades o más limitadas, y contratar personal adicional, antes que invertir miles de euros en herramientas bajo licencia destinadas a otro tipo de entornos.

2.4 Soluciones tradicionales

En la actualidad, la realidad es que la gran mayoría de organizaciones cuentan con herramientas de apoyo tradicionales (on-premises) para la gestión de su puesto de trabajo. Los productos que ofrece Microsoft son de los más utilizados debido, principalmente, a que la mayor parte de los dispositivos corporativos utilizan Windows como sistema operativo, tal y como se ha reflejado anteriormente. Las soluciones de Microsoft ayudan a mantener un ecosistema homogéneo, sobre todo en lo referente a la administración de las propias herramientas, y la integración con los dispositivos es muy alta, siendo prácticamente transparente para el usuario final.

Aunque existen múltiples soluciones tradicionales de otros proveedores, como BigFix de HCL Software[8] (anteriormente de IBM), Mobile Device Manager Plus de Manage Engine[9] o Ivanti Endpoint Manager[10], entre otras, a continuación se muestran, a modo de ejemplo de solución on-premises, las que ofrece Microsoft.

- **Microsoft Deployment Toolkit**[11] y **WDS**: es una solución gratuita que consta de una serie de herramientas para automatizar la instalación de imágenes de sistema operativo y aplicar configuraciones. También permite desplegar aplicaciones y drivers.

  Se trata de una herramienta muy básica, dadas sus limitadas funcionalidades, diseñada para pequeños entornos, sólo compatible con Windows y sin capacidades de gestión una vez instalados los equipos. Sin embargo, es de fácil uso e implementación. No se requiere una gran inversión en cuanto a infraestructura, pues simplemente necesita un servidor Windows compatible para instalarse (aunque también puede instalarse en un equipo cliente con Windows).

La siguiente imagen muestra la arquitectura típica de MDT junto con WDS, servicio en el que se apoya para realizar la instalación de sistemas operativos mediante la red:

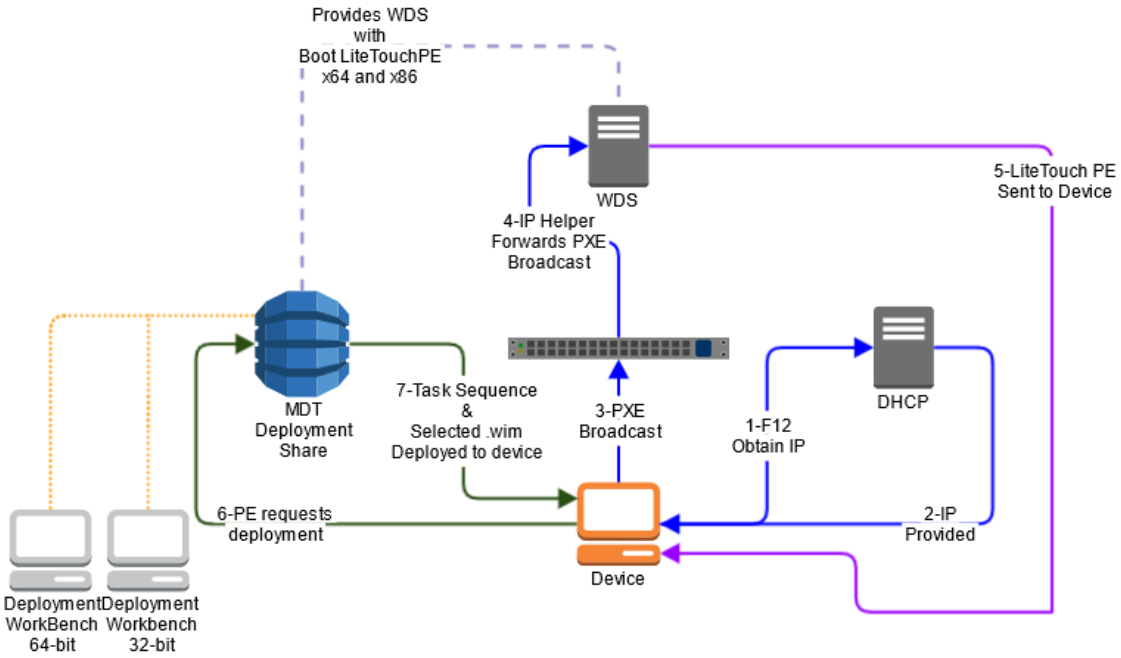


Figura 7 - Arquitectura MDT + WDS

Fuente: https://www.techthoughts.info/mdt-with-wds-integration-overview/

- **Microsoft Endpoint Configuration Manager**[12]: conocido anteriormente como SCCM, es la solución integral de gestión de dispositivos de Microsoft. A diferencia de MDT, cubre todas las necesidades de gestión pero requiere de licenciamiento, por lo que está pensado para entornos más grandes (a partir de 1000 dispositivos, aproximadamente).

  MECM mejora las funcionalidades de MDT, ofreciendo mayor personalización y configuración en el despliegue de sistemas operativos, permitiendo incluso la instalación totalmente desatendida, conocida como ZTI, y proporcionando gestión posterior de los dispositivos: inventario, instalación de aplicaciones, actualizaciones de seguridad, nuevas versiones de sistema operativo, configuraciones, realización de informes… El abanico de dispositivos cliente compatibles también es más grande, incluyendo equipos Mac, Linux e incluso sistemas operativos de servidor Windows y Linux. Por todo ello, los requisitos a nivel de infraestructura son más altos, necesitando incluso una base de datos SQ, como mínimo.

  A continuación, se muestra una posible arquitectura de SCCM formada por un servidor primario con distintos roles, un servidor SQL para la base

de datos y funciones de ejecución de informes, y varios puntos de distribución, desde donde los clientes descargarán el contenido:

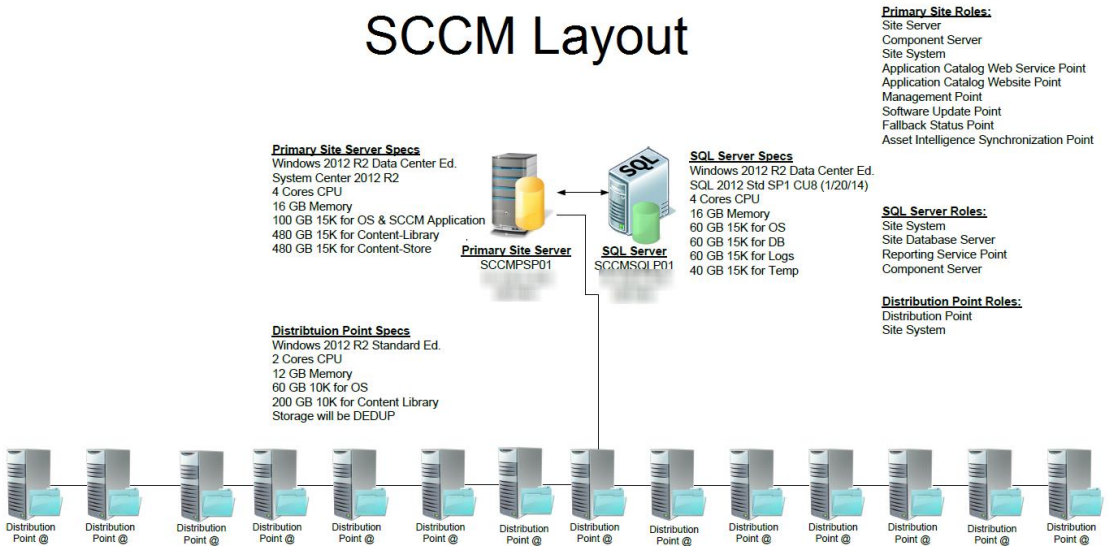


Figura 8 - Ejemplo de arquitectura de SCCM

Fuente: https://social.technet.microsoft.com/Forums/Azure/en-US/58ba35e5-d84e-4741-8089-624f5269a2ca/sccm-2012-design-consideration-advice?forum=configmanagergeneral

2.5 Análisis de la situación actual

En las dos últimas décadas, la tecnología ha avanzado a pasos agigantados y ha fomentado la aparición en el mercado de cada vez más dispositivos móviles[13]. Este tipo de dispositivos se han establecido también en el entorno profesional, ayudando a impulsar la transformación digital y favoreciendo situaciones de movilidad como el teletrabajo. Además, han llegado incluso, en determinadas situaciones, a reemplazar a los antiguos equipos fijos[14]. Entre ellos, se encuentran los siguientes: ordenadores portátiles, teléfonos inteligentes y tabletas.

El desembarco de dichos dispositivos móviles en los entornos corporativos ha supuesto varios retos para las organizaciones[15]. Por un lado, las compañías han tenido que reforzar la seguridad y el acceso a su información, imponiendo medios para evitar que sea robada o alterada. Esto se consigue requiriendo autenticación para poder acceder a ella y permitiendo el acceso sólo desde determinadas ubicaciones (redes o dispositivos de confianza, por ejemplo). Es decir, ha sido necesario invertir recursos para reforzar la información en origen.

Por otro lado, la gran proliferación y popularidad de este tipo de dispositivos se ha traducido en que todas las personas disponen de, al menos, uno de ellos. Por su propia naturaleza, son dispositivos que siempre (o casi siempre) se llevan encima, y además disponen de conexión permanente a Internet. Esto

implica que, aunque se trate de dispositivos personales, cada vez con mayor frecuencia se empleen para tareas laborales (como acceder al email corporativo o consultar documentos de trabajo). Así, las empresas se ven en la necesidad de gestionar esos dispositivos para proteger su información, bien sea realizando una gestión parcial o total de los mismos. Esto forma parte de la protección de la información en destino.

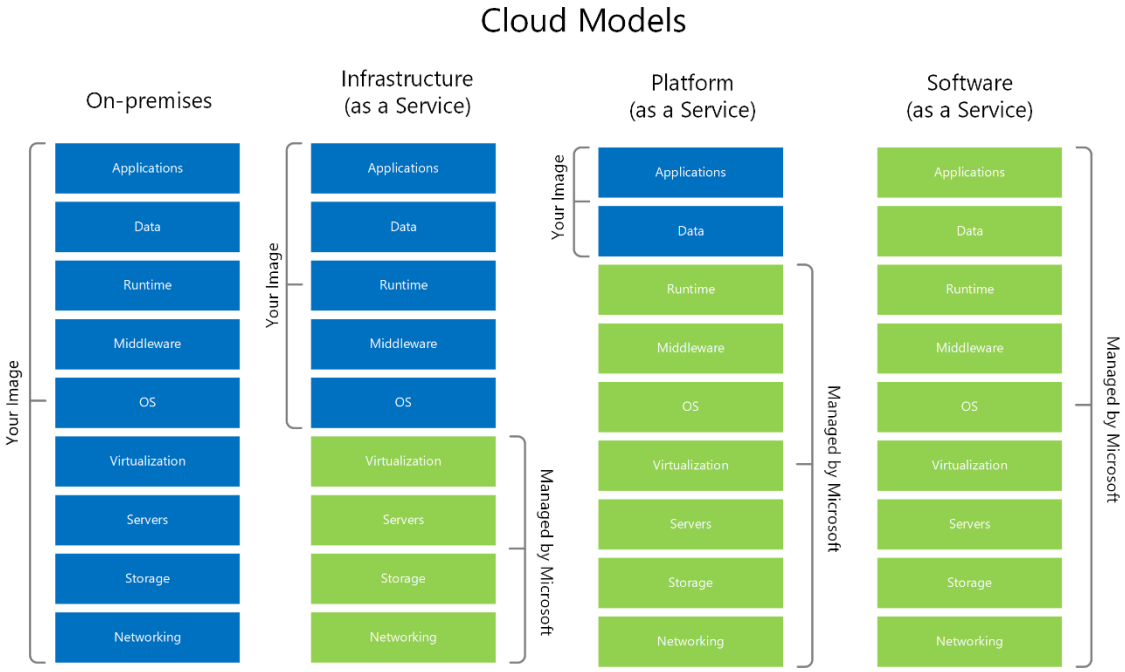
Este último punto ha representado una nueva necesidad para las organizaciones ante la cual no estaban preparadas. Las herramientas de gestión tradicionales, mencionadas en el apartado anterior, no se adaptan al nuevo paradigma dadas sus funcionalidades y limitaciones en cuanto a sistemas compatibles. El parque de dispositivos a gestionar se ha fragmentado y se ha vuelto mucho más heterogéneo, aumentando la diversidad de modelos y sistemas operativos, más aún si se permite el uso de dispositivos personales, sobre los que no se tiene poder de decisión sobre su adquisición. Además, el número de dispositivos a gestionar se ha incrementado considerablemente, llegando incluso a duplicarse, y las soluciones existentes no cuentan con una infraestructura dimensionada para asumir ese crecimiento.

Para adaptarse a estas nuevas necesidades, las compañías han tenido que estudiar alternativas a las soluciones de gestión de puesto de trabajo tradicionales. En algunos casos, la solución pasa por adquirir una herramienta específica totalmente independiente de la tradicional y que ambas coexistan, con el inconveniente de tener dos entornos diferentes. En otros casos, se busca alguna herramienta que se integre lo máximo posible con las que ya se dispone, o bien se elige una herramienta que cubra todo el espectro (dispositivos antiguos y nuevos) y se migran a ella los dispositivos tradicionales.

2.6 Beneficios que aporta el cloud

Las soluciones cloud de gestión de puesto de trabajo nacen para dar respuesta a las nuevas necesidades de las organizaciones. Se entiende por solución cloud al suministro de recursos informáticos bajo demanda mediante Internet, ofrecidos por un proveedor de servicios (CSP) y con un modelo de pago por uso[16]. Las soluciones cloud de MDM aportan todas las ventajas inherentes al cloud y ofrecen mayor versatilidad en cuanto a gestión de dispositivos que las soluciones tradicionales on-premises. Existen diferentes soluciones: IaaS, PaaS y SaaS; pero las relativas a la gestión del puesto de trabajo se enmarcan en SaaS.

La imagen siguiente muestra una breve comparativa entre servicios on-premises y cloud:



Las principales ventajas de las herramientas cloud frente a los recursos on-premises son las siguientes:

- **Flexibilidad**

La computación cloud ofrece mayor flexibilidad que la on-premises. Gracias a no requerir la adquisición de recursos locales como en on-premises (compra de hardware, instalación y configuración de servidores, etc.) y al pago por uso, se puede decidir en cada momento qué recursos se utilizan en función de las necesidades. Además, se reducen los tiempos de espera. A través de unos pocos clics se pueden añadir recursos (servidores, servicios, etc.) a nuestra infraestructura y optimizar su rendimiento, disponiendo única y exclusivamente de los necesarios. Esto se conoce como escalabilidad.

- **Eficiencia**

El pago por uso es uno de los pilares en los que se basan las soluciones cloud. Esto permite invertir de manera eficiente, pagando en cada momento por lo que se necesita sin necesidad de sobredimensionar las soluciones, como es habitual en on-premises, para adelantarse a los crecimientos futuros. De esta forma, el gasto se optimiza al máximo y siempre se conoce de antemano cuánto se va a pagar.

Por otra parte, todos los proveedores ofrecen unos acuerdos de nivel de servicio (SLA) mayor al 99%, muy por encima del de las soluciones on-premises. Es decir, una disponibilidad de los recursos contratados casi completa, sin cortes por reinicio de servidores o fallos. En el caso de Microsoft, por ejemplo, el SLA es del 99,9% o superior[17]. Esto es debido a que tanto la información como las soluciones están redundadas en diferentes ubicaciones geográficas, lo que aumenta en gran medida la tolerancia a fallos.

- **Impacto financiero**

Además de los beneficios que supone el ya mencionado pago por uso, los servicios cloud aportan varias ventajas financieras para las organizaciones. Por un lado, los gastos de capital (CapEx) relativos a las soluciones on-premises se transforman en gastos operativos (OpEx), lo que flexibiliza el balance de cuentas. Por otro, el gasto en cloud tiene un impacto en el EBITDA, pues no tiene en cuenta los costes reales (como el gasto en servidores y su depreciación), lo que obliga en determinadas ocasiones a identificar métricas financieras adicionales que se ajusten mejor a la realidad[18].

- **Mantenimiento**

Gran parte o la totalidad del mantenimiento de los servicios cloud, en función del tipo de servicio contratado (IaaS, PaaS o SaaS), lo realiza el proveedor de servicios, no el usuario de estos. Mientras que con las tecnologías on-premises es la propia compañía quien tiene que encargarse de su mantenimiento, en las soluciones cloud simplemente se preocupa de operarlas. Esto supone un gran ahorro de costes y tiempo para las organizaciones.

Otro punto importante relativo al mantenimiento es que los servicios cloud contratados siempre cuentan con las últimas actualizaciones, tanto a nivel de seguridad como de funcionalidades. Así, las compañías están en disposición de utilizar y aprovechar las nuevas características de las soluciones (sin inversión ni esfuerzo adicional), que además cuenta con las versiones de software más optimizadas.

Si se extrapolan las ventajas reflejadas de las tecnologías cloud al área de la gestión del puesto de trabajo, queda patente que estas pueden ayudar a cubrir las necesidades surgidas en los últimos años, así como propiciar la aparición de nuevas formas de trabajo en las organizaciones.

La primera necesidad que cubrir es la del aumento exponencial de dispositivos a gestionar debido a los dispositivos móviles. Gracias a las facilidades en cuanto a escalabilidad y al servicio basado en el pago por uso, las soluciones MDM cloud encajan perfectamente con ese escenario que se ha vuelto tan cambiante. Por norma general, los costes necesarios para redimensionar una solución on-premises son más altos que los de adquirir nuevas licencias para

poder gestionar dichos dispositivos, no siendo expresamente necesario en licenciamientos basados en usuario y no en dispositivo.

La segunda necesidad a la que dar respuesta es la de la heterogeneidad de dispositivos que gestionar. Cada vez más empresas quieren introducir iniciativas de BYOD o CYOD con las que flexibilizar el uso y elección de dispositivos a sus empleados, pero carecen de herramientas para gestionar esos nuevos dispositivos. Los proveedores de soluciones MDM cloud son conscientes de ello y por ende sus productos permiten gestionar en mayor o menor medida los tipos de dispositivos más comúnmente empleados. Además, gracias a la constante actualización y mejora de sus herramientas, son capaces de añadir nuevas funcionalidades y ampliar el soporte a los nuevos dispositivos que puedan surgir de manera totalmente transparente para las compañías, aportando así un valor añadido.

En definitiva, las soluciones MDM cloud son las herramientas que mejor se adaptan a las nuevas necesidades de las organizaciones. La llegada de los nuevos dispositivos y la movilidad les obligan a adoptar una de esas soluciones para avanzar en las formas de trabajo modernas. Continuar con herramientas de gestión tradicionales supone ir a contracorriente de lo que demanda no solo el mercado sino los propios trabajadores, dejando a un lado la movilidad y la experiencia digital.

2.7 Comparativa de las principales soluciones de mercado

De igual forma que existen numerosas herramientas tradicionales de gestión del puesto trabajo, la oferta de soluciones MDM cloud también es muy grande. El cuadrante mágico de Gartner de herramientas de gestión unificada de dispositivos finales sitúa como líderes a Ivanti, VMWare y Microsoft, estando este último por encima del resto.

Figura 9 - Gartner Magic Quadrant for Unified Endpoint Management Tools

Fuente: https://www.gartner.com/document/4017175?ref=hp-wylo

Según Gartner, la gestión unificada de dispositivos finales es parte de un mercado estable y el crecimiento de ingresos viene dado por la expansión orgánica que tiene lugar dentro de los clientes ya existentes, ampliando la gestión a nuevos sistemas operativos y dispositivos móviles. También percibe una creciente adopción en paralelo de soluciones UEM con la gestión de sistemas operativos modernos, recomendando a las organizaciones realizar una transición metódica desde las soluciones tradicionales. Además, advierte que no se debe esperar por una solución que ofrezca respuesta a todas las necesidades, porque probablemente no exista y la espera añada complejidad y aumento de gastos (TCO). La recomendación es elegir la solución que mejor se adapte a la mayoría de las necesidades y solventar la restantes con herramientas adicionales[19].

A continuación, se analizan con mayor detalle las soluciones líderes según Gartner:

- **Microsoft Endpoint Manager**

La propuesta de gestión unificada de Microsoft nace de la combinación de sus dos herramientas de gestión de dispositivos: Intune (solución MDM cloud) y Configuration Manager (solución on-premises). La solución ofrece compatibilidad completa con el resto de los productos de Microsoft, tanto on-premises (estaciones de trabajo Windows) como cloud (Azure AD, Microsoft 365 o Azure Virtual Desktop, entre otros). Microsoft, por su parte, está permanentemente mejorando la solución e invierte gran cantidad de esfuerzos en perfeccionar la experiencia tanto de la capa de administración como en cuanto al análisis y la automatización de los dispositivos finales.

De entre sus fortalezas destacan el tratarse de un producto nativo de Microsoft, por lo que la integración con todos sus productos y dispositivos es muy alta, ofreciendo para ellos más funcionalidades que la competencia. Asimismo, esto proporciona una estabilidad y rendimiento superiores a las soluciones de terceros. Ser la solución UEM con mayor cuota de mercado supone que las correcciones y nuevas funcionalidades se priorizan en función de la demanda de los clientes. Sin ir más lejos, a finales del pasado mes de octubre de 2022 se añadió el soporte para dispositivos Linux[20].

Por el contrario, sus debilidades están relacionadas con la complejidad a la hora de diseñar informes personalizados, siendo los predefinidos más limitados y básicos que los de sus competidores. De igual forma, las capacidades de aplicación de parches de terceros no son las mejores del mercado, siendo a veces necesario adquirir otra solución para tal fin.

El diagrama siguiente muestra la arquitectura de la plataforma unificada MEM.

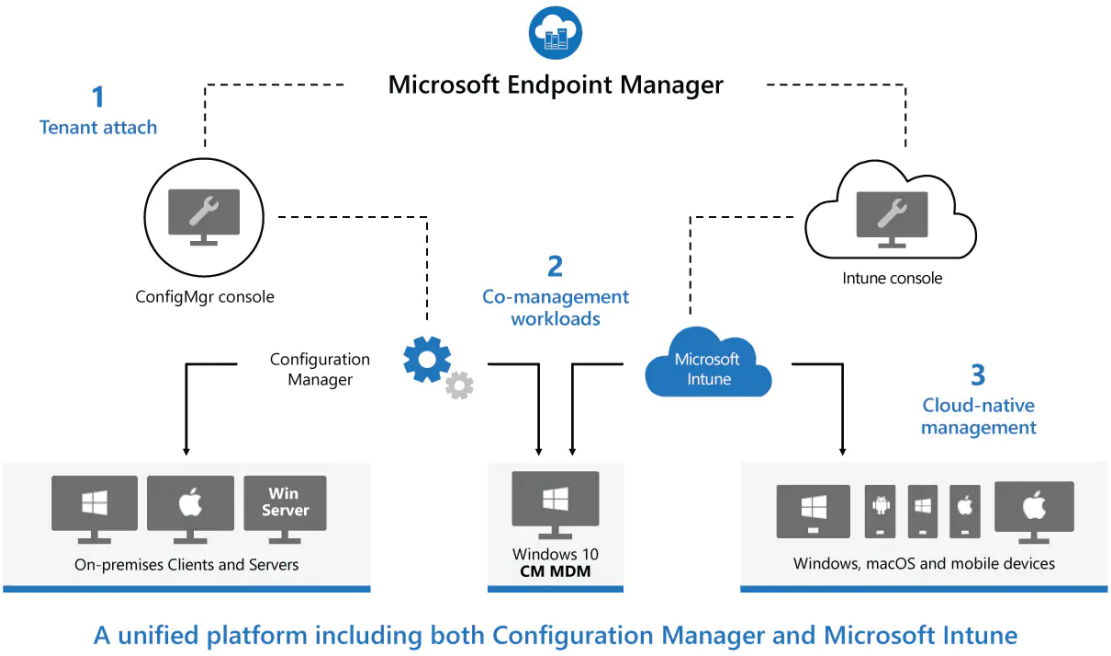


Figura 10 - Arquitectura MEM – MECM + Intune

Fuente: https://www.microsoft.com/es-es/security/business/microsoft-endpoint-manager

- **VMWare Workspace ONE**

El fabricante VMWare ofrece su solución de gestión de dispositivos unificada con la posibilidad de disponer de una arquitectura completamente cloud o instalarla en on-premises. En ambos casos, las funcionalidades son las mismas, siendo su punto fuerte la gestión de dispositivos VDI y aplicaciones virtualizadas en entornos VMWare.

Las grandes fortalezas de Workspace ONE son que ofrece un paquete completo que incluye administración de dispositivos, inicio de sesión único, soporte remoto, acceso remoto, seguridad de punto final, análisis, automatización y virtualización. Todo ello desde una plataforma con gran facilidad de uso y que proporciona plantillas, configuraciones de referencia y asistentes que ayudan a reducir los esfuerzos de los administradores. Además, dependiendo de la edición contratada, las capacidades de inteligencia y automatización permiten obtener informes y automatizar mediante reglas.

En cuanto a sus debilidades, las funcionalidades avanzadas sólo se obtienen a través de las licencias Advanced o Enterprise, cuyo precio se encuentra entre los más altos del mercado. Por otra parte, las compañías que ya disponen de Microsoft 365 disponen de las mismas funcionalidades ofrecidas por Microsoft pero sin sobrecoste, por lo que es difícil justificar la contratación de Workspace One.

El siguiente diagrama muestra la arquitectura de la solución Workspace ONE en su versión cloud:

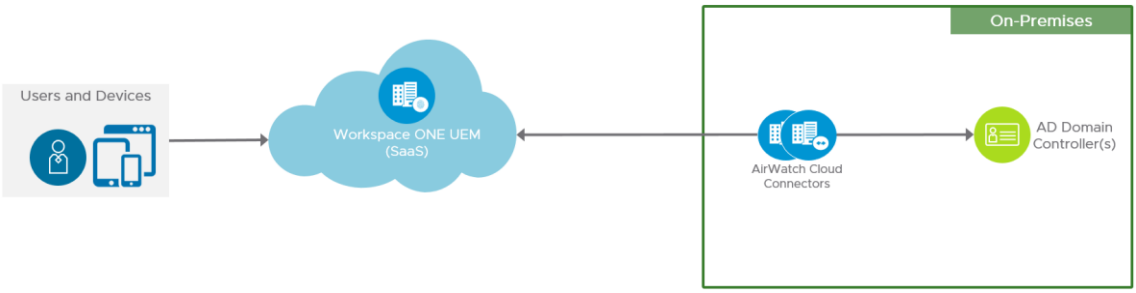


Figura 11 - Arquitectura cloud Workspace ONE

Fuente: https://techzone.vmware.com/resource/workspace-one-uem-architecture#introduction

- **Ivanti Neurons for Unified Endpoint Protection**

De igual modo que la solución de VMWare, Ivanti Neurons for Unified Endpoint Protection también se ofrece como producto con arquitectura únicamente cloud o con posibilidad de disponer de él on-premises. En este caso, sin embargo, las funciones distan entre ambos entornos, siendo superiores las ofrecidos en la solución SaaS. La solución brinda un amplio soporte a la mayor parte de los

dispositivos finales, permitiendo el descubrimiento, la automatización, reparación automática, aplicación de parches y seguridad de confianza cero.

De entre sus grandes fortalezas destaca la capacidad de proporcionar descubrimiento activo y pasivo de todos los dispositivos en la red para inventariar dispositivos no administrados. Además, aplica ML a los datos recopilados para producir información que pueda emplearse con el fin de automatizar la corrección de fallos. De igual forma, es una de las soluciones con mayor capacidad de administración de distribuciones Linux, incluyendo sistemas operativos de servidor, dispositivos OEMConfig y AOSP, y dispositivos portátiles. Por último, su capacidad de gestión de parches es superior a la de la competencia, tanto de sistemas operativos como de aplicaciones, y permite integrarse con herramientas de gestión de servicios y activos de TI (ITAM / ITSM).

Por otro lado, el sistema de licenciamiento es complejo y cuesta comprender qué capacidades específicas se incluyen con cada producto o si se requieren licencias adicionales. Además, la gestión de las diferentes funcionalidades se lleva a cabo desde distintas consolas de administración (aunque con diseño similar), lo que añade complejidad a la gestión. La desigualdad entre las funcionalidades de la solución en función de si es cloud u on-premise también es un aspecto negativo, más aún cuando las novedades se suelen introducir sólo en la versión cloud.

El siguiente diagrama muestra la arquitectura de la solución Ivanti Neurons for Unified Endpoint Protection en su versión cloud:

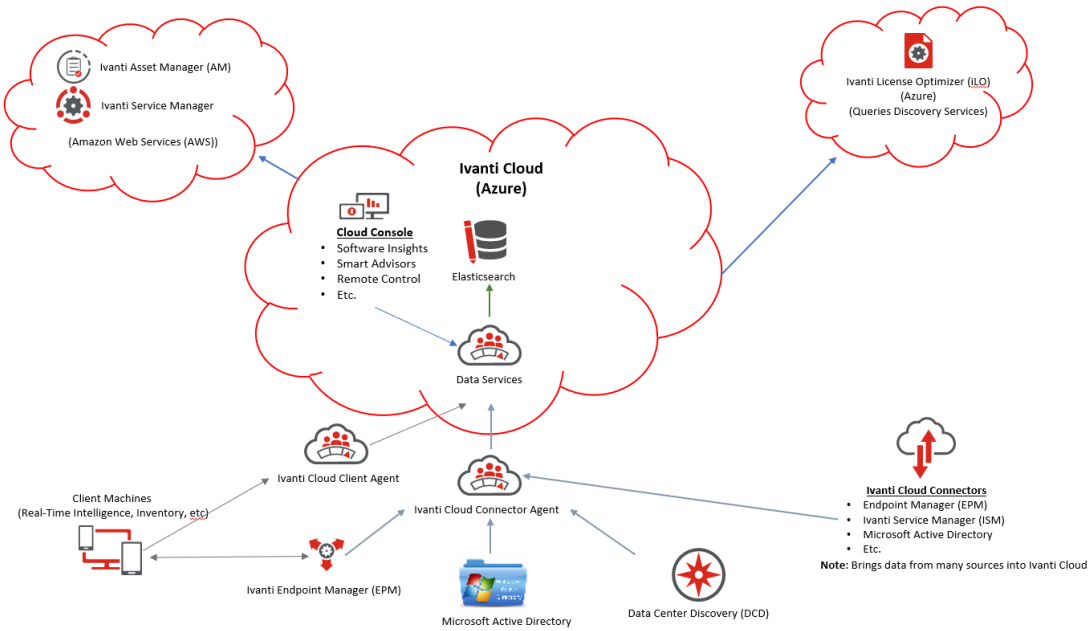


Figura 12 - Arquitectura cloud Ivanti Neurons for Unified Endpoint Protection

Fuente: https://forums.ivanti.com/s/article/Ivanti-Cloud-Diagram-An-Outer-Space-View-of-the-Ivanti-Cloud?language=en_US

3. Solución MDM completamente cloud

3.1 Definición de requisitos

La solución MDM cloud escogida tiene ser capaz de gestionar tanto dispositivos corporativos como BYOD de los siguientes tipos:

- PCs Windows.
- PCs Mac.
- PCs Linux.
- Dispositivos móviles Android (teléfonos inteligentes y tabletas)
- Dispositivos móviles iOS.

El único requisito es que los dispositivos dispongan de acceso a Internet.

La herramienta tiene que proporcionar las siguientes funcionalidades:

- Gestión centralizada (administración unificada).
- Inventario de dispositivos.
- Administración total (dispositivos corporativos) y parcial (BYOD).
- Aplicación de políticas de seguridad.
- Encriptación/cifrado de la información.
- Gestión de actualizaciones.
- Gestión de antivirus.
- Borrado remoto de dispositivos.
- Informe de estado de dispositivos.
- Distribución de aplicaciones.
- Tienda de aplicaciones corporativas.
- Acceso condicional.
- Bloqueo de dispositivos liberados (para teléfonos inteligentes y tabletas).
- Administración de aplicaciones móviles.
- Asistencia remota.

El escenario propuesto de tipos de dispositivos y funcionalidades necesarias es al que se enfrentan la gran mayoría de las organizaciones. Lo habitual, tal y como se ha indicado en el apartado 2.3, es que casi la totalidad de las estaciones de trabajo sean Windows y los dispositivos móviles Android e iOS.

No obstante, es frecuente encontrar algunos dispositivos con MacOS (para perfiles como diseñadores gráficos, usuarios de marketing, etc.) e incluso con Linux (en perfiles de desarrollador de software, por ejemplo), por lo que se han incluido dentro del alcance que debe cubrir la herramienta. En estos casos, sin embargo, es posible que no estén disponibles todas las funcionalidades exigidas, pues no existe ninguna herramienta capaz de ofrecer todo lo indicado para todas las plataformas y habría que implementar más de una. Según aconseja Gartner en el ya mencionado cuadrante mágico de herramientas de

gestión unificada de dispositivos, se debe optar por una solución que cubra la mayoría de las necesidades y afrontar el resto con herramientas adicionales[19].

3.2 Diseño y arquitectura

Tras analizar en detalle la principal oferta de soluciones MDM cloud y estudiar cuál se adapta mejor a las necesidades especificadas, la herramienta escogida es Microsoft Intune. En la decisión ha tenido mucho peso el hecho de que los equipos Windows representan la mayor parte del parque de dispositivos a gestionar y la solución se integra completamente con ellos, al ser del mismo fabricante. Además, la integración con otras herramientas y servicios de Microsoft, como Microsoft Office y Office 365 (ahora Microsoft 365), también es mejor que las de la competencia por el mismo motivo.

En el caso de Microsoft Office, el informe realizado por Statista en febrero de 2022 sobre las principales herramientas de productividad revela que su cuota de mercado es superior al 48%[21].

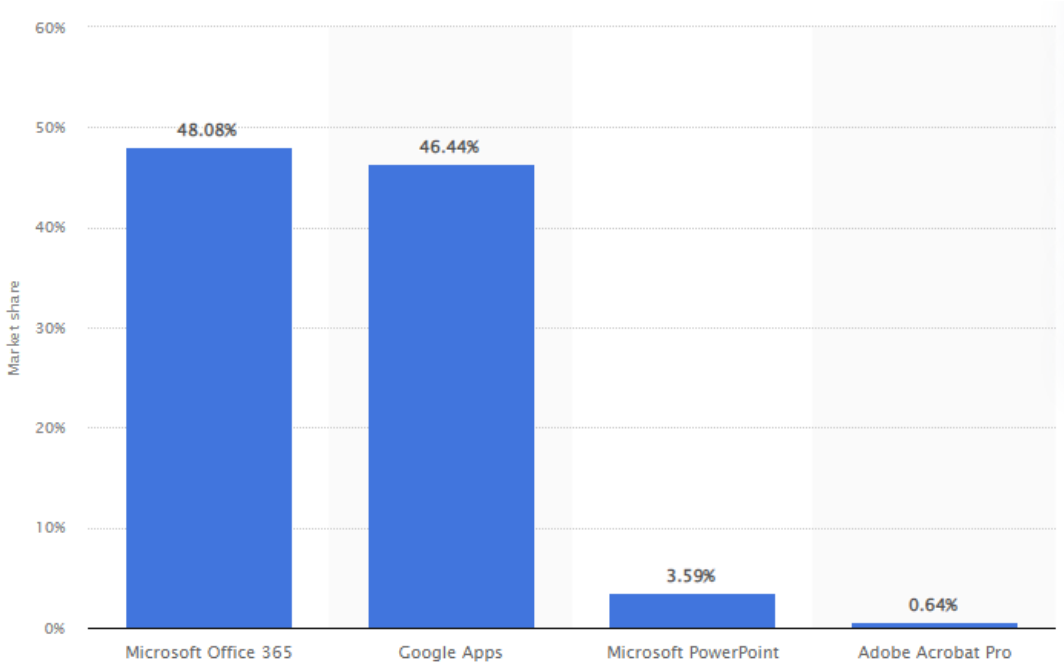


Figura 13 - Cuota de mercado de las principales herramientas de productividad a febrero de 2022

Fuente: https://www.statista.com/statistics/983299/worldwide-market-share-of-office-productivity-software/#:~:text=As%20of%20February%202022%2C%20Microsoft's,the%20lead%20to%20Office%20365.

En cuanto a Microsoft 365, un informe de Gartner de 2019 declara que Microsoft disponía de una cuota del 87.5% en el mercado del correo electrónico y la autoría[22].

Por todo lo indicado, queda patente que Microsoft Intune es la alternativa con más probabilidad de encajar en la mayoría de los escenarios corporativos, y por ello ha sido la elegida.

El objetivo de esta fase es realizar una prueba de concepto de una solución de gestión de puesto de trabajo completamente cloud, analizando sus capacidades de gestión para extrapolarlas a un entorno corporativo y estudiar su viabilidad. Así, la implementación inicial consistirá en implantar Intune como única herramienta de gestión para un grupo reducido de dispositivos que servirán de referencia al ser representativos del conjunto global, independientemente de que ya exista una herramienta tradicional en la organización.

El siguiente diagrama muestra la arquitectura de la solución SaaS Intune que se va a implementar:

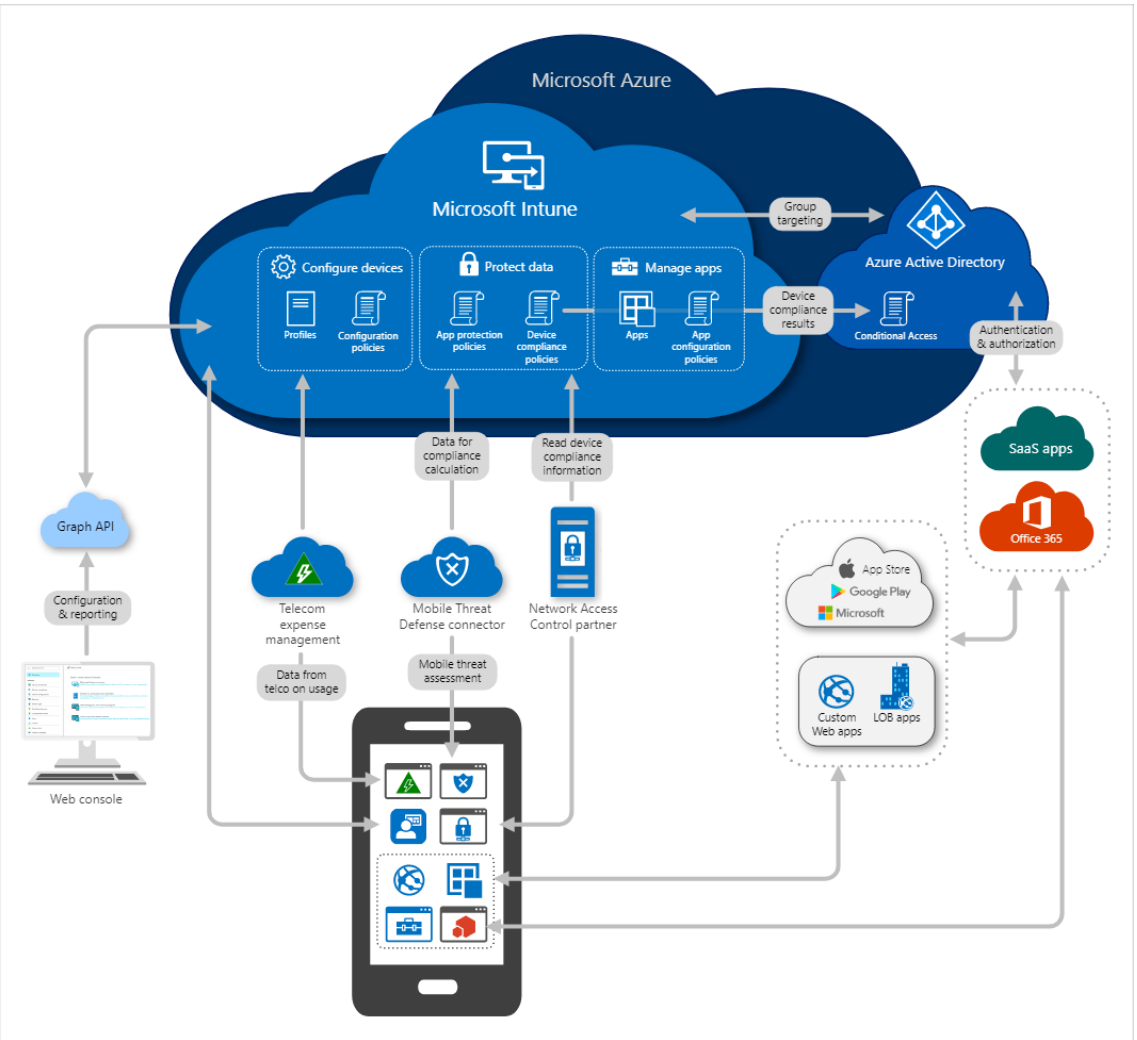


Figura 14 - Arquitectura de Microsoft Intune

Fuente: Propia. Imagen de Microsoft tras eliminar la infraestructura on-premises.

3.3 Configuración de la solución MDM Intune

3.3.1 Licenciamiento

Para llevar a cabo la prueba de concepto se ha utilizado un entorno de laboratorio de pruebas existente con licencia válida hasta el 22 de abril de 2023. El laboratorio no dispone de ningún tipo de configuración más allá de la propia creación del tenant de Azure, que se realiza de forma automática al inscribirse en cualquier servicio cloud de Azure, y cuenta con las licencias y suscripciones necesarias para utilizar el servicio de Microsoft Intune. En concreto, las suscripciones asignadas son:

- Windows 10/11 Enterprise E3.
- Enterprise Mobility + Security E5
- Office 365 E5

En la siguiente imagen se muestran las licencias incluidas en cada suscripción y se aprecia que Intune forma parte de Enterprise Mobility + Security E5 (también conocido como EMS E5):

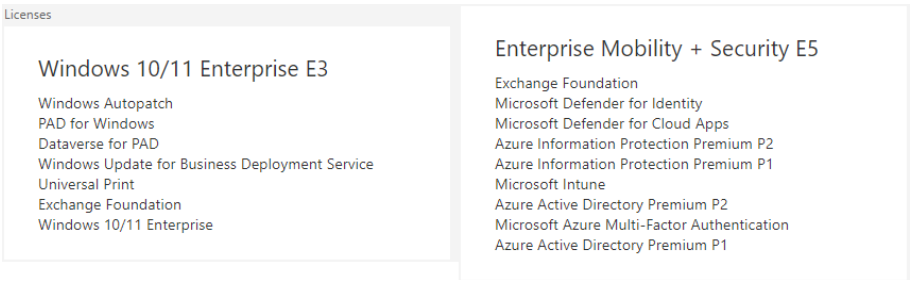


Figura 15 - Suscripciones y licencias del entorno de laboratorio 1 de 2

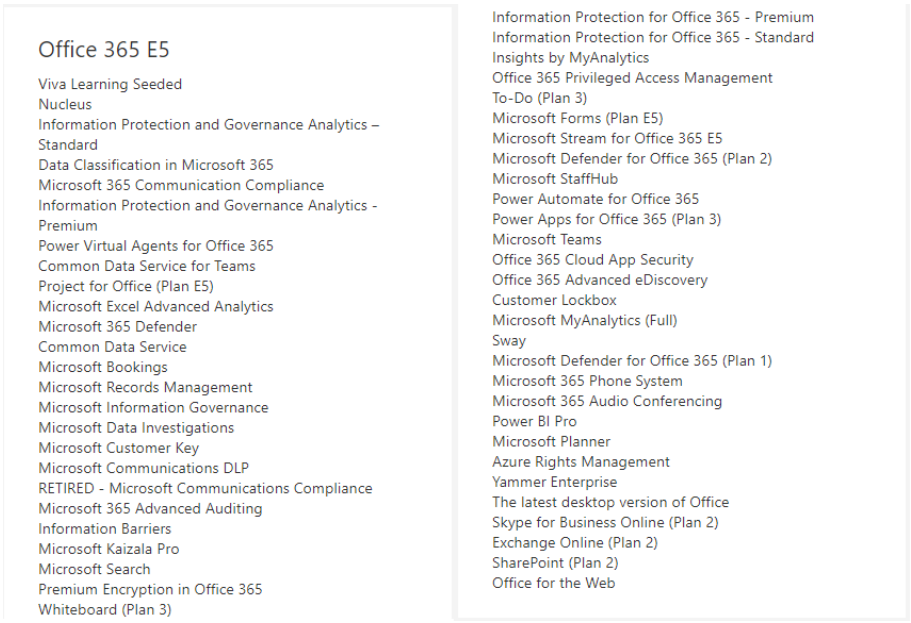


Figura 16 - Suscripciones y licencias del entorno de laboratorio 2 de 2

El entorno de laboratorio cuenta con más licencias de las necesarias para poder configurar y evaluar la solución MDM cloud Intune, ya que simplemente sería necesario disponer de una licencia de Azure Active Directory (P1 o P2) junto con la licencia de Intune (enmarcada en una suscripción Enterprise Mobility + Security E3 o E5). No obstante, según lo indicado en el apartado anterior, la cuota de mercado de Microsoft 365 es muy alta y es habitual que las organizaciones ya dispongan de él y/o de otros servicios cloud de Microsoft. Por tanto, disponer de licencias adicionales en el entorno de laboratorio permitirá mostrar el funcionamiento de restricciones adicionales como el acceso condicional basado en riesgos a determinados servicios como el correo (Exchange Online), necesidad frecuente en escenarios corporativos.

En cualquier caso, Microsoft pone a disposición de todos una prueba gratuita de Intune, válida durante 30 días, con los servicios imprescindibles anteriormente indicados para evaluar la solución. Transcurrido el periodo de prueba, se empieza a facturar por uso. Este es otro de los motivos por los que se ha optado por el laboratorio existente, pues tiene mayor validez. La prueba de 30 días la puede solicitar cualquier persona a través de la siguiente dirección: https://signup.microsoft.com/get-started/signup?products=40BE278A-DFD1-470a-9EF7-9F2596EA7FF9&ali=1

En la actualidad, Microsoft Intune se encuentra disponible dentro de diferentes suscripciones:

- Microsoft 365 E5
- Microsoft 365 E3
- Enterprise Mobility + Security E5
- Enterprise Mobility + Security E3
- Microsoft 365 Empresa Premium
- Microsoft 365 F1
- Microsoft 365 F3
- Microsoft 365 Administración Pública G5
- Microsoft 365 Administración Pública G3
- Microsoft 365 Educación A5
- Microsoft 365 Educación A3

El licenciamiento habitual de Intune es por usuario, es decir, se paga una cantidad (variable en función de la suscripción) por cada usuario que tenga asignada licencia de Intune. Como máximo, cada usuario puede enrolar hasta 15 dispositivos en Intune con una sola licencia, aunque esto es configurable por cualquier administrador para restringirlo a un número inferior.

Si bien es menos frecuente, Intune ofrece también licenciamiento por dispositivo, pensado para casos muy concretos como dispositivos con Android Enterprise dedicado, el modo de autoimplementación de Windows AutoPilot o la inscripción de dispositivos Apple sin afinidad de usuario. Este tipo de licenciamiento cuenta con limitaciones de funcionalidades, pues no se admiten el uso de directivas de protección de aplicaciones de Intune, el acceso condicional ni las características de administración basadas en usuario, como el correo electrónico y el calendario[23].

Las licencias de Intune disponibles en el entorno de laboratorio son 15, tal y como se muestra en la siguiente imagen, más que suficientes para la prueba de concepto de la solución MDM.

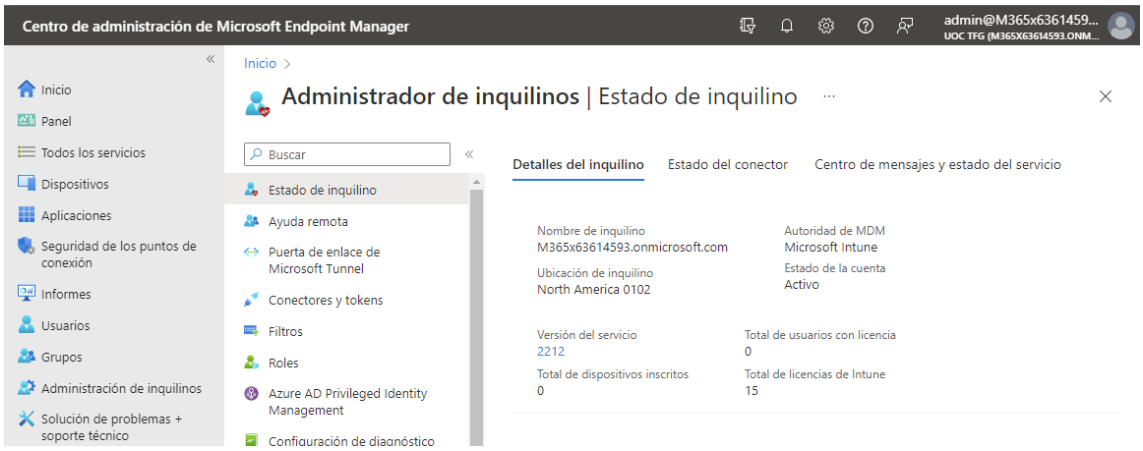


Figura 17 - Licencias de Intune en el entorno de laboratorio

3.3.2 Configuración de requisitos previos

El laboratorio no cuenta con ningún tipo de configuración más allá de algunos usuarios creados, por lo que la primera configuración a realizar es darle nombre al tenant. Esto se puede realizar accediendo con un usuario con rol de Administrador Global al portal de administración de Azure Active Directory, (https://portal.azure.com), editando las propiedades desde la información general del tenant.

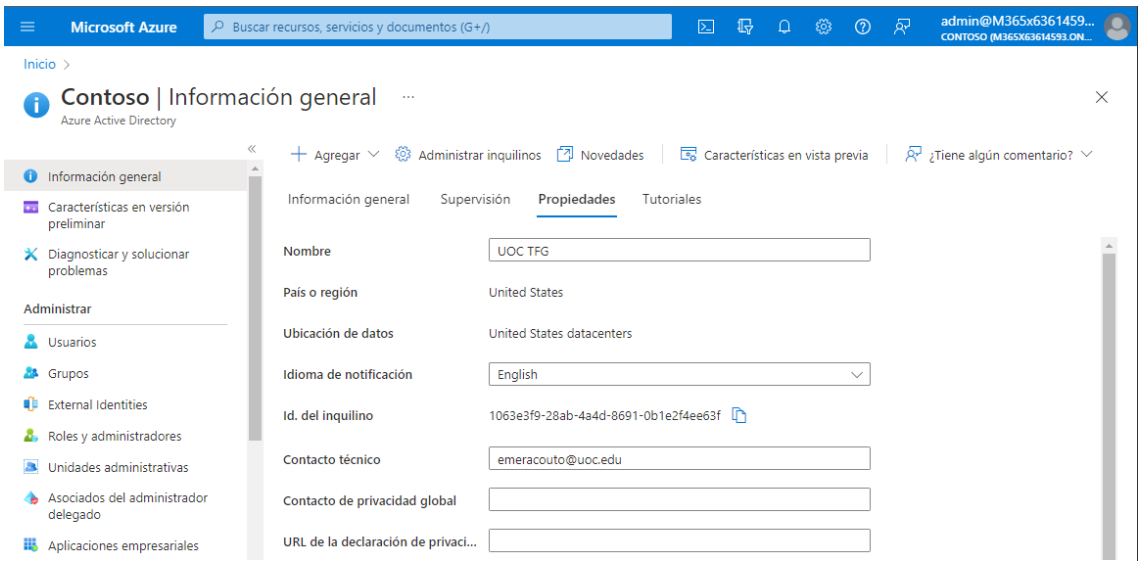


Figura 18 - Configuración del nombre del tenant de Azure Active Directory

Cuando se realiza la inscripción en cualquier servicio de Azure, Microsoft crea el tenant con la información proporcionada y asigna al usuario que ha solicitado la creación el rol de Administrador Global. Más adelante, el usuario con dicho rol puede crear nuevos usuarios y asignarle los roles y licencias que considere.

Una vez renombrado el tenant a “UOC TFG”, el siguiente paso es configurar cómo se realizará la inscripción de los dispositivos en la solución MDM. El acceso al portal de administración de Intune se realiza a través de la URL https://endpoint.microsoft.com/, y este es su estado inicial.

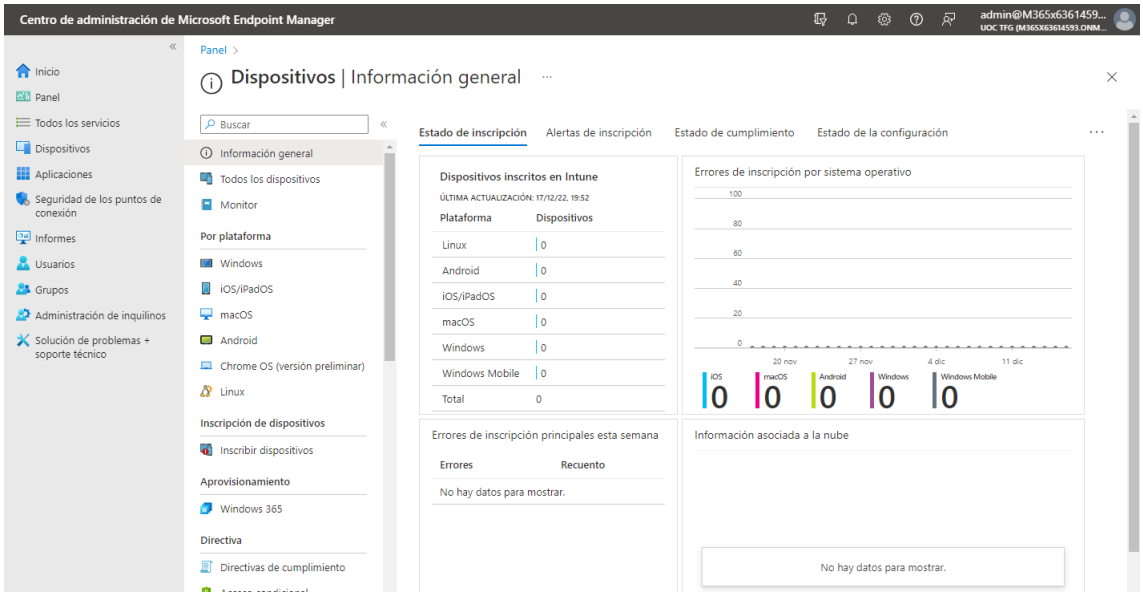


Figura 19 - Estado inicial de Microsoft Intune

En función de los requisitos establecidos en el apartado 3.1, los diferentes escenarios a cubrir son:

- Dispositivos corporativos nuevos.
- Dispositivos corporativos ya existentes.
- Dispositivos BYOD.

Así, las configuraciones a realizar son las siguientes:

- **Dispositivos Windows**

Para los dispositivos Windows, se debe habilitar la inscripción automática. Esto permitirá que los usuarios inscriban de manera automática los dispositivos al encenderlos por primera vez, simplemente introduciendo sus credenciales corporativas en la OOBE.

La inscripción automática en Intune se configura desde la opción “Inscribir dispositivos” del menú Dispositivos en el portal de administración. En este

caso, como se desea que todos los usuarios de la prueba de concepto inscriban sus dispositivos, se ha seleccionado “Todo” en el ámbito de usuario de MDM y MAM. En caso de querer restringir la inscripción de dispositivos a determinados usuarios, es posible seleccionar “Algo” y especificar el grupo o grupos a los que deberán pertenecer dichos usuarios. El ámbito de usuario MDM permitirá gestionar los dispositivos de los usuarios, mientras que el ámbito de usuario de MAM permitirá gestionar la cuenta de la organización en los dispositivos.

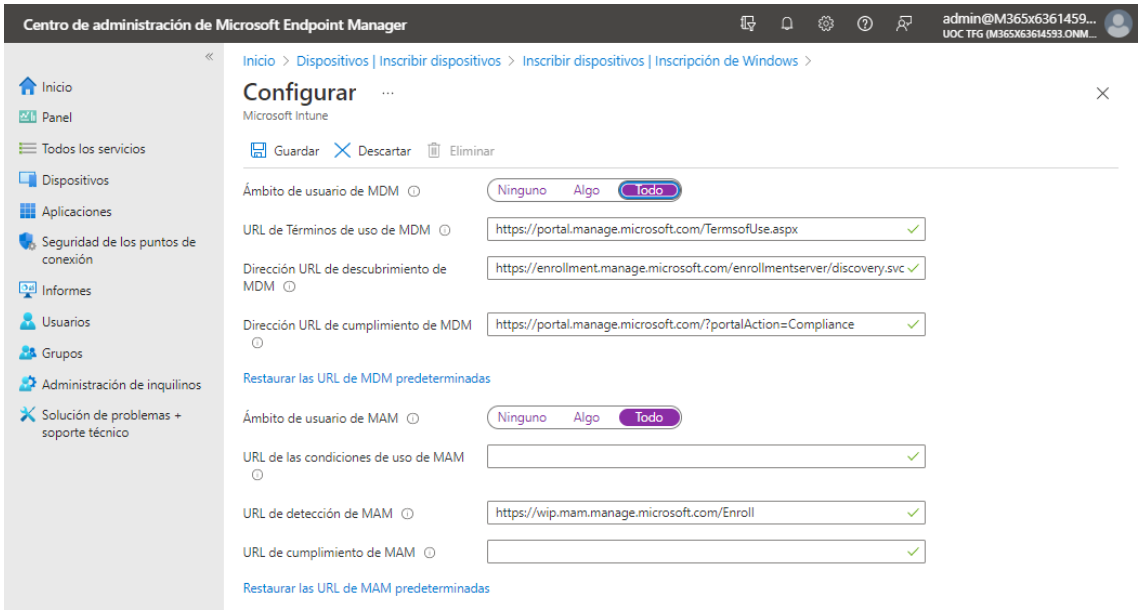


Figura 20 - Inscripción automática de dispositivos Windows en Intune

Los dispositivos Windows también se pueden inscribir en Intune mediante el servicio llamado AutoPilot. Para ello, es necesario preinscribir los dispositivos en el MDM mediante su identificador único de hardware, crear al menos un perfil de despliegue de Windows AutoPilot y asignarlo a esos dispositivos. La preinscripción se puede llevar a cabo de manera manual por un administrador de Intune o por el propio fabricante/revendedor del dispositivo, siempre que formen parte del programa *Cloud Solution Partners (CSP)* de Microsoft[24]. Esto último es lo más habitual, ya que es un servicio que se suele contratar junto con la adquisición del dispositivo y libera de carga a los administradores de la organización.

La configuración realizada en Intune permite inscribir tanto dispositivos corporativos Windows nuevos, como ya existentes y BYOD.

- **Dispositivos Apple**

Los dispositivos Apple (con sistema operativo macOS, iOS e iPadOS) se pueden inscribir en Intune de tres formas diferentes: de manera manual mediante el registro con la cuenta corporativa en la aplicación portal de empresa, de forma automática mediante la inscripción automatizada y de forma automática mediante la inscripción directa. Para la prueba de concepto se ha optado por la primera opción dado que la inscripción automatizada requiere una cuenta de Apple Bussines Manager (ABM) o Apple School Manager (ASM) y la inscripción directa está destinada a dispositivos sin usuario de tipo quiosco.

Para poder inscribir dispositivos Apple en Intune, con independencia del tipo de inscripción elegida de las indicadas, es necesario obtener el certificado push MDM de Apple. El proceso de obtención del certificado se inicia desde el portal de administración de Intune, en el apartado “Inscripción de Apple” del menú Dispositivos.

Figura 21 - Acceso a obtención del certificado push MDM de Apple en Intune

A continuación, se debe conceder permiso a Microsoft para enviar información del usuario y del dispositivo a Apple, descargar la solicitud de firma del certificado de Intune (CSR) y acceder al portal de solicitud de certificados push de Apple para generarlo. Por último, se debe indicar el identificador de Apple con el que se ha generado el certificado y subir el fichero con extensión .pem del certificado[25][26]. El proceso completo de creación de certificado push de Apple está detallado en el anexo 1.

La siguiente imagen muestra el proceso de configuración del certificado push MDM de Apple para poder gestionar dispositivos Apple en Intune.

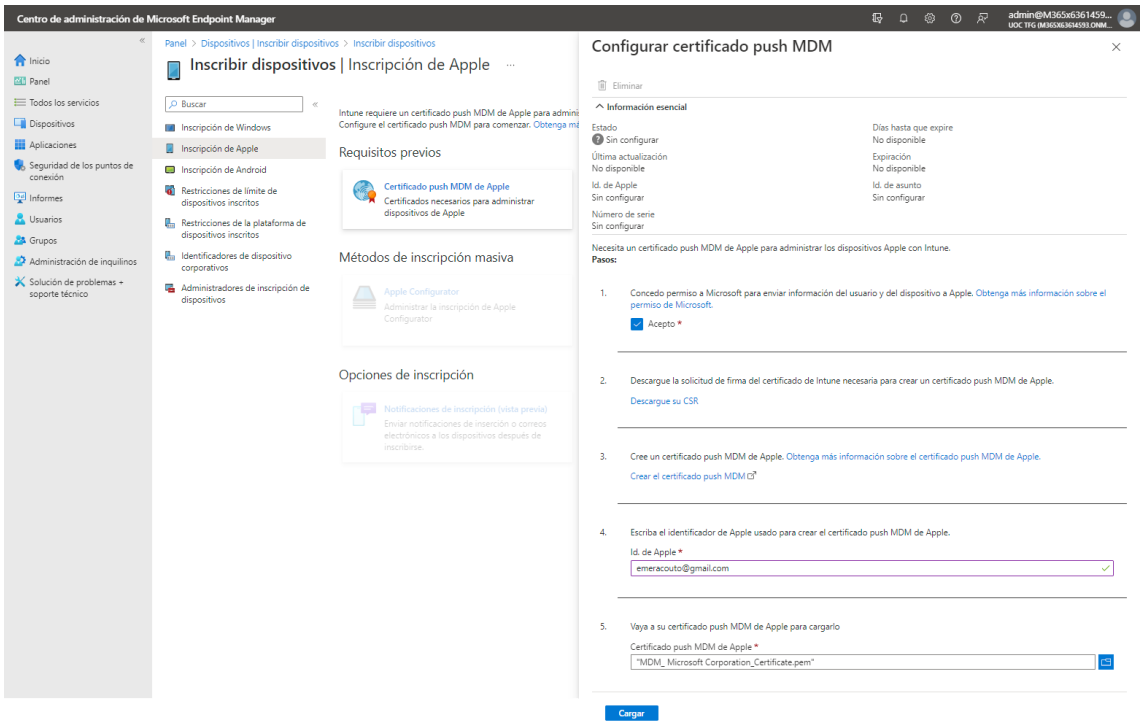


Figura 22 - Configuración de certificado push MDM de Apple en Intune

Tras la configuración del certificado push MDM de Apple en Intune, el entorno está listo para inscribir dispositivos Apple. Aunque la herramienta lo soporta, dado que no se dispone de acceso a ABM ni a ASM, la inscripción de dispositivos Apple se llevará a cabo de forma manual mediante la instalación del portal de empresa en ellos, por lo que se inscribirán equipos corporativos ya en uso y BYOD.

- **Dispositivos Android**

Los dispositivos Android también pueden inscribirse en Microsoft Intune de diferentes maneras, en función del tipo de dispositivo y de lo que se quiera gestionar de estos:

- Dispositivos Android Enterprise de propiedad personal con un perfil de trabajo (BYOD)
- Dispositivos Android Enterprise dedicados de propiedad corporativa (COSU)
- Dispositivos Android Enterprise de propiedad corporativa totalmente administrados (COBO)
- Perfil de trabajo de propiedad corporativa de Android Enterprise (COPE)
- Proyecto de código abierto de Android (AOSP)
- Administrador de dispositivos Android (DA)

Para todos los escenarios indicados, excepto el proyecto de código abierto Android, el único requisito común es la conexión de una cuenta empresarial de Google Play administrada a Microsoft Intune para disponer de Android

Enterprise, ya que el resto de las configuraciones se realizan mediante diferentes perfiles de inscripción[27]. El Administrador de dispositivos Android (DA) solo admite dispositivos Android con versión de sistema operativo inferior a la 10, publicada en septiembre de 2019, por lo que es una opción heredada y en desuso que ha sido reemplazada por Android Enterprise y no se tendrá en cuenta para la prueba de concepto.

La vinculación a Intune de la cuenta empresarial de Google Play administrado se realiza desde el apartado “Inscripción de Android” del menú dispositivos. De igual modo que para los dispositivos Apple, se debe conceder permiso a Microsoft para enviar información del usuario y del dispositivo a Google e indicar la cuenta administrativa de Google.

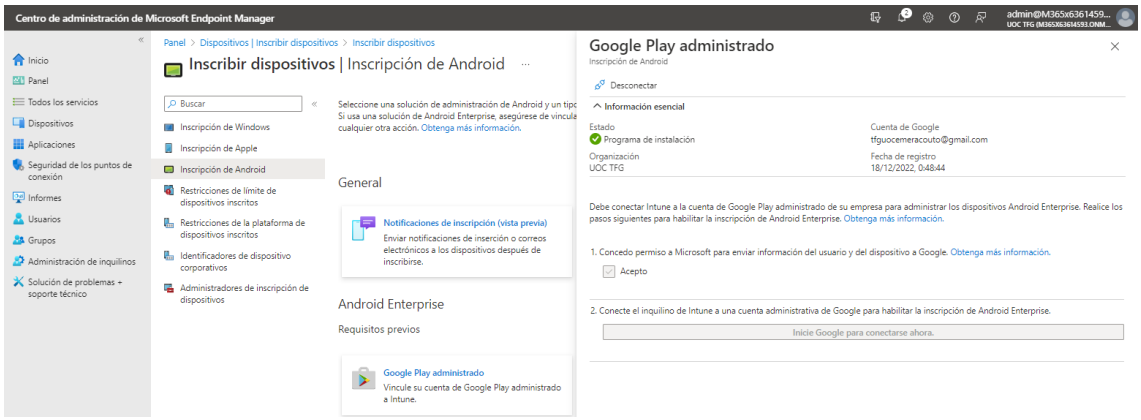


Figura 23 - Configuración de Google Play administrado en Intune

El proceso de creación de una cuenta empresarial gratuita de Android Enterprise y la vinculación con Intune está reflejado en el anexo 2.

- **Dispositivos Linux**

Los dispositivos Linux no requieren de ninguna configuración adicional de prerrequisitos a las ya realizadas para poder inscribirse en Intune. En versiones del servicio de Intune anteriores a 1911, es necesario establecer manualmente la entidad de MDM. Dado que la versión del servicio de Intune del entorno de laboratorio es la 2212, tal y como se aprecia en la figura 18, la autoridad de MDM se ha configurado de forma automática a Microsoft Intune[28].

3.3.3 Creación de grupos de seguridad

En Microsoft Intune, cualquier tipo de asignación se realiza mediante grupos de seguridad, como por ejemplo la asignación de directivas de cumplimiento, perfiles de configuración, perfiles de implementación de Windows Autopilot o

perfiles de inscripción de dispositivos Android. Así, es necesario crear una serie de grupos que se utilizarán más adelante.

Los grupos que se van a crear son:

- Dispositivos Windows Corporativos
- Dispositivos Windows BYOD
- Dispositivos Windows AutoPilot
- Dispositivos Android Enterprise
- Dispositivos Android Enterprise BYOD
- Dispositivos Android Enterprise COBO
- Dispositivos macOS
- Dispositivos iOS-iPadOS
- Dispositivos Linux
- Usuarios de Intune

La gestión de grupos (creación, modificación y eliminación) puede llevarse a cabo indistintamente desde el portal de administración de Azure Active Directoy o el portal de administración de Intune. En la siguiente imagen se muestra el proceso de creación de un grupo de seguridad desde Intune, accediendo al apartado “Grupos” y seleccionando “Nuevo grupo”.

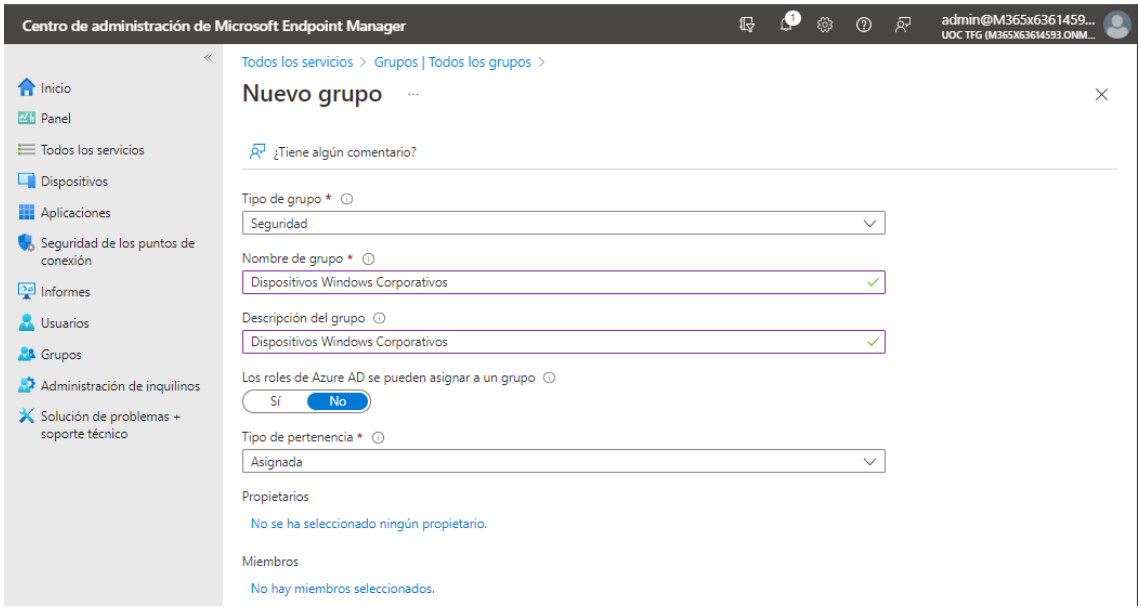


Figura 24 - Creación de grupo de seguridad en Intune

La creación del resto de grupos de seguridad está reflejada en el anexo 3. Los grupos se han creado vacíos, ya que no existen dispositivos en el entorno por el momento, y se irán añadiendo miembros a medida que se creen los dispositivos en Intune. Al tratarse de una prueba de concepto, los dispositivos se añadirán manualmente. En un entorno real, lo habitual es configurar la pertenencia a los grupos de forma dinámica mediante el uso de consultas.

3.3.4 Perfiles de inscripción e implementación

- **Perfil de implementación de Windows AutoPilot**

Una vez creados los grupos de seguridad, ya es posible generar todo tipo de perfiles y asignarlos a dichos grupos. Para los dispositivos Windows que se inscriban en Intune mediante AutoPilot, es necesario crear un perfil de implementación en el que personalizar la experiencia de aprovisionamiento. Este perfil se aplicará al grupo de seguridad Dispositivos Windows AutoPilot, al que pertenecerán los dispositivos que se deban inscribir en Intune de esa forma.

Para crear el perfil de implementación de Windows AutoPilot hay que acceder a "Perfiles de Implementación" dentro del apartado Inscripción de Windows en el menú Inscribir dispositivos de la sección Dispositivos de Intune. La siguiente imagen muestra el resumen con los detalles del perfil creado. El proceso completo se puede consultar en el anexo 4.

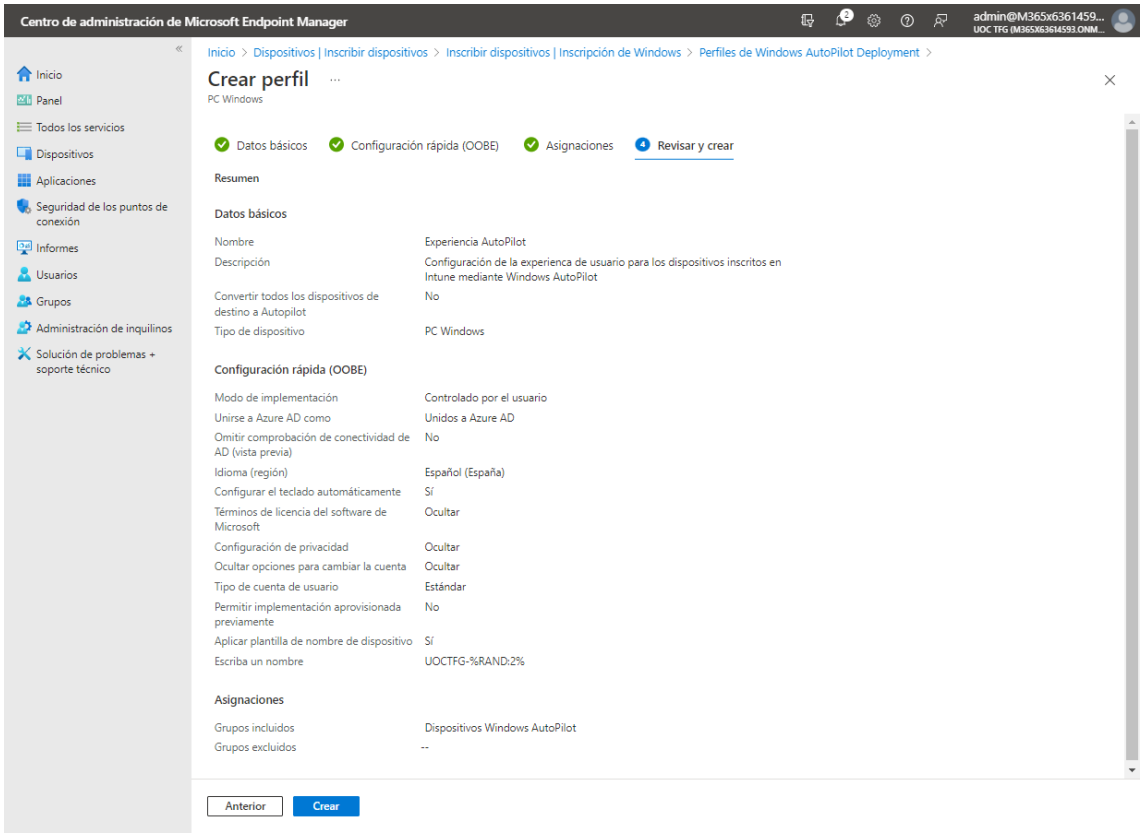


Figura 25 - Resumen de perfil de implementación de Windows AutoPilot

La inscripción en Intune mediante Windows AutoPilot se llevará a cabo en dispositivos corporativos nuevos o en aquellos en los que se haya restablecido

el sistema operativo, ya que es durante el proceso de OOBE cuando se introducen las credenciales corporativas y se realiza el proceso de inscripción.

- **Perfiles de inscripción de Android**

La inscripción de dispositivos Android también requiere de la creación de al menos un perfil de inscripción de Android. En base a los requisitos impuestos para la prueba de concepto, se deben crear dos perfiles de inscripción de Android, como mínimo, uno para los dispositivos corporativos y otro para los personales.

Tal y como se ha comentado en el apartado 3.3.2, existen diferentes tipos de escenarios para los dispositivos Android. En este caso, se ha optado por contemplar los dos siguientes:

- Dispositivos Android Enterprise de propiedad personal con un perfil de trabajo (BYOD)

Este escenario cubrirá aquellos dispositivos Android BYOD, es decir, personales, en los que la organización permite utilizar determinados servicios y recursos corporativos a cambio de gestionar cómo se utilizan.

La creación del perfil de inscripción de Android se lleva a cabo desde el apartado “Inscripción de Android” del menú Inscribir Dispositivos, al que se accede mediante Dispositivos. En el caso de los dispositivos de propiedad personal con perfil de trabajo (BYOD), el perfil está habilitado de forma predeterminada en Intune y no es necesario realizar ninguna configuración adicional, tal y como muestra la siguiente imagen.

Figura 26 - Perfil de inscripción de dispositivos Android (BYOD)

En caso necesario, se pueden configurar restricciones de plataforma para bloquear la inscripción de dispositivos según la versión de sistema operativo, el fabricante, o si han sido liberados.

- Dispositivos Android Enterprise de propiedad corporativa totalmente administrados (COBO)

Este escenario cubrirá los dispositivos Android corporativos, que serán gestionados por completo, a diferencia de los BYOD en los que sólo se gestionará el perfil de trabajo (y no la parte personal). Por ello, deben inscribirse cuando son nuevos o es necesario restablecerlos a los valores de fábrica. Es importante tener en cuenta que, en este escenario, los dispositivos serán utilizados única y exclusivamente para tareas laborales, sin contemplar el uso personal de estos.

El acceso a la creación del perfil se realiza según lo indicado en el punto anterior, pero en este caso se debe seleccionar “Dispositivos de usuario totalmente administrados de propiedad corporativa”. A continuación, se muestra el resumen con los detalles del perfil de inscripción creado, donde se refleja el token de inscripción para el perfil.

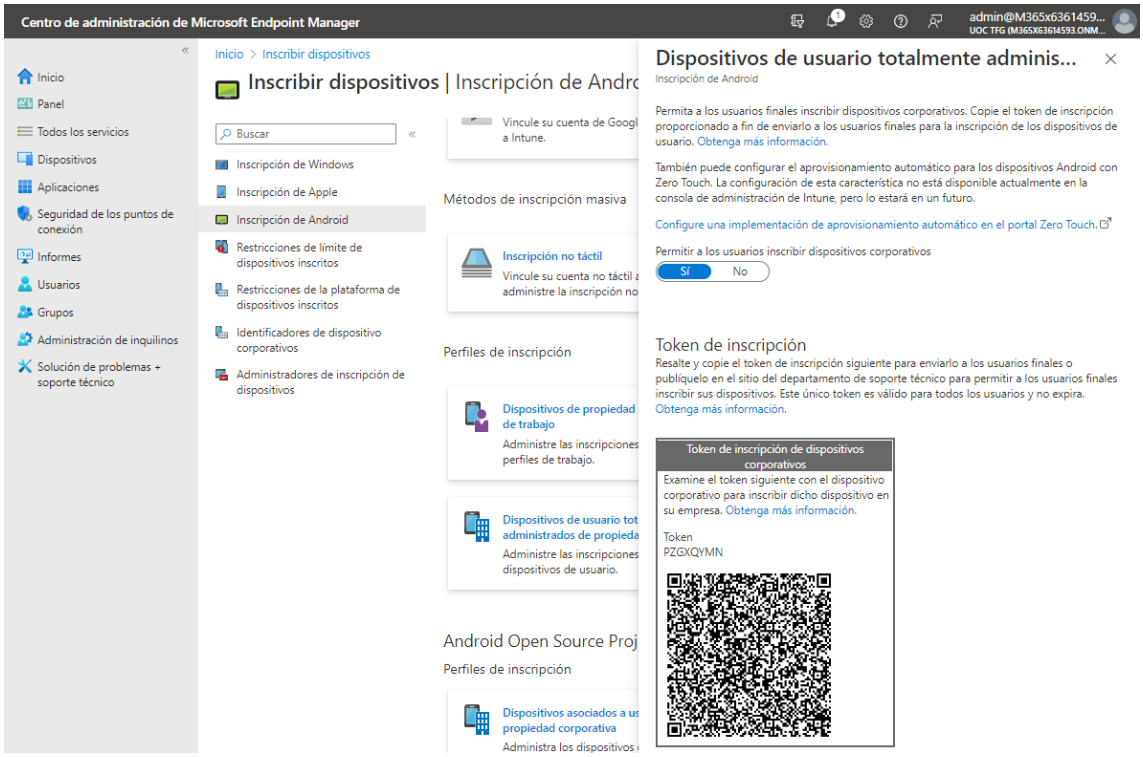


Figura 27 - Token de inscripción de dispositivos Android corporativos

- **Dispositivos Apple y Linux**

La inscripción de dispositivos Apple (macOS, iOS y iPadOS) y Linux no requiere de la creación expresa de ningún perfil de implementación o inscripción. Para los dispositivos Apple hay dos funcionalidades en versión preliminar (sin soporte hasta que se incluyan en una nueva versión de Intune), una que permite enviar notificaciones push o por correo electrónico a los dispositivos ya inscritos, y otra que permite crear perfiles de inscripción para definir el tipo de inscripción de los dispositivos (de usuario, de dispositivo, o a elección del usuario).

No obstante, dado que no es necesario crear ningún perfil de inscripción, se ha optado por no configurar las funcionalidades en versión preliminar.

3.3.5 Directivas de cumplimiento

Uno de los principales objetivos detrás de la gestión del puesto de trabajo es proteger la información corporativa. Para ello, los dispositivos con los que se accede a dicha información tienen que cumplir con unos requisitos de seguridad mínimos establecidos por la organización.

Las directivas de cumplimiento de Intune consisten en una serie de reglas que evalúan propiedades y configuraciones que los dispositivos deben cumplir para ser compatibles. En caso contrario, los dispositivos son marcados como no compatibles y los datos corporativos que albergan se protegen hasta que sean compatibles. Además, la evaluación de cumplimiento se puede combinar con el acceso condicional para bloquear el acceso a los usuarios y dispositivos que no cumplen las directivas a los recursos de la organización.

Las directivas de cumplimiento, de igual forma que los perfiles de configuración, se evalúan y aplican en los dispositivos cuando tiene lugar un ciclo de sincronización entre estos e Intune. Esto ocurre cada cierto tiempo de manera totalmente transparente para el usuario, aunque puede forzarse manualmente tanto desde el dispositivo como desde el portal de administración de Intune.

Los dispositivos inscritos en Intune tienen un ciclo de sincronización diferente en función de la plataforma. La siguiente imagen muestra las frecuencias aproximadas de los ciclos de sincronización de cada plataforma. Dado que la gestión de dispositivos Linux se ha integrado en Intune recientemente (a finales de octubre de 2022), todavía no se indica su frecuencia de sincronización en la tabla.

Frecuencias **estimadas**:

Plataforma	Ciclo de actualización
iOS/iPadOS	Aproximadamente cada 8 horas
macOS	Aproximadamente cada 8 horas
Android	Aproximadamente cada 8 horas
equipos Windows 10/11 inscritos como dispositivos	Aproximadamente cada 8 horas
Windows 8.1	Aproximadamente cada 8 horas

Si los dispositivos se han inscrito recientemente, la comprobación de cumplimiento, no cumplimiento y configuración se ejecuta con más frecuencia. Las protecciones se **estiman** en:

Plataforma	Frecuencia
iOS/iPadOS	Cada 15 minutos durante 1 hora y, luego, cada 8 horas
macOS	Cada 15 minutos durante 1 hora y, luego, cada 8 horas
Android	Cada 3 minutos durante 15 minutos, luego cada 15 minutos durante 2 horas y, luego, cada 8 horas
equipos Windows 10/11 inscritos como dispositivos	Cada 3 minutos durante 15 minutos, luego cada 15 minutos durante 2 horas y, luego, cada 8 horas
Windows 8.1	Cada 5 minutos durante 15 minutos, luego cada 15 minutos durante 2 horas y, luego, cada 8 horas

Figura 28 - Frecuencias de sincronización por plataforma en Intune

Fuente: https://learn.microsoft.com/es-es/mem/intune/configuration/device-profile-troubleshoot#how-long-does-it-take-for-devices-to-get-a-policy-profile-or-app-after-they-are-assigned

La configuración de directivas de cumplimiento en Intune se realiza por tipo de plataforma. Además, la solución permite definir qué hacer con los dispositivos que no tienen asignada una directiva de cumplimiento y se han inscrito, así como cada cuánto, como máximo, tienen que reportar como compatibles al MDM. Para definir estos parámetros se debe acceder a “Configuración de directivas de cumplimiento” dentro del apartado Directivas de cumplimiento del menú Dispositivos.

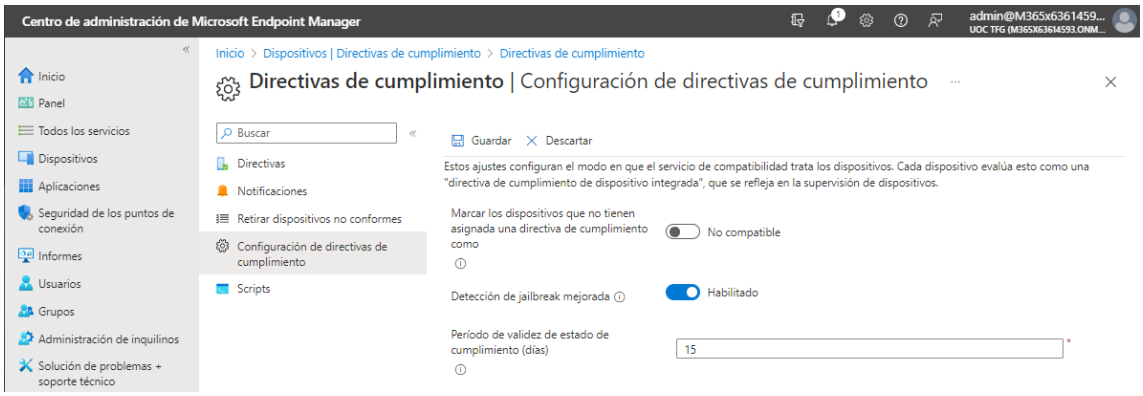


Figura 29 - Configuración global de directivas de cumplimiento de Intune

En este caso, se ha optado por marcar como no compatibles los dispositivos que no tengan asignada una directiva de cumplimiento (la opción por defecto era marcar como compatibles), habilitar la detección mejorada de jailbreak (deshabilitada por defecto) y configurar el periodo de validez del estado de cumplimiento a 15 días (30, por defecto).

Una vez definidas las opciones de configuración globales de directivas de cumplimiento de Intune, se debe crear una directiva de cumplimiento para cada una de las plataformas que se van a gestionar. A continuación, se muestra el resumen de cada directiva de cumplimiento creada. El proceso completo detallado se puede consultar en el anexo 5.

- **Dispositivos Windows**

Para los dispositivos Windows se ha optado por crear una directiva de cumplimiento con la siguiente configuración:

- Nombre: Dispositivos Windows
- Descripción: Directiva de cumplimiento para Dispositivos Windows 10 y versiones posteriores
- Plataforma: Windows 10 y versiones posteriores
- BitLocker: Requerir
- Arranque seguro: Requerir
- Integridad de código: Requerir
- Versión mínima del sistema operativo: 19042.2251 (Windows 10 20H2 con el parche acumulativo de noviembre 2022)
- Contraseña para desbloquear el dispositivo: Requerir
- Longitud mínima de la contraseña: 4
- Máximo de minutos de inactividad antes de solicitar la contraseña: 15 minutos
- Cifrado del almacenamiento de datos en el dispositivo: Requerir
- TPM: Requerir
- Antivirus: Requerir
- Antimalware de Microsoft Defender: Requerir
- Versión mínima de Antimalware de Microsoft Defender: 4.18.2109.6
- Protección en tiempo real: Requerir

La directiva de cumplimiento se aplicará a todos los dispositivos Windows inscritos en Intune, es decir, los corporativos, los BYOD y los de AutoPilot. En caso de que no cumplan cualquiera de las configuraciones exigidas se marcarán automáticamente como no conformes.

La siguiente imagen muestra los detalles de la directiva.

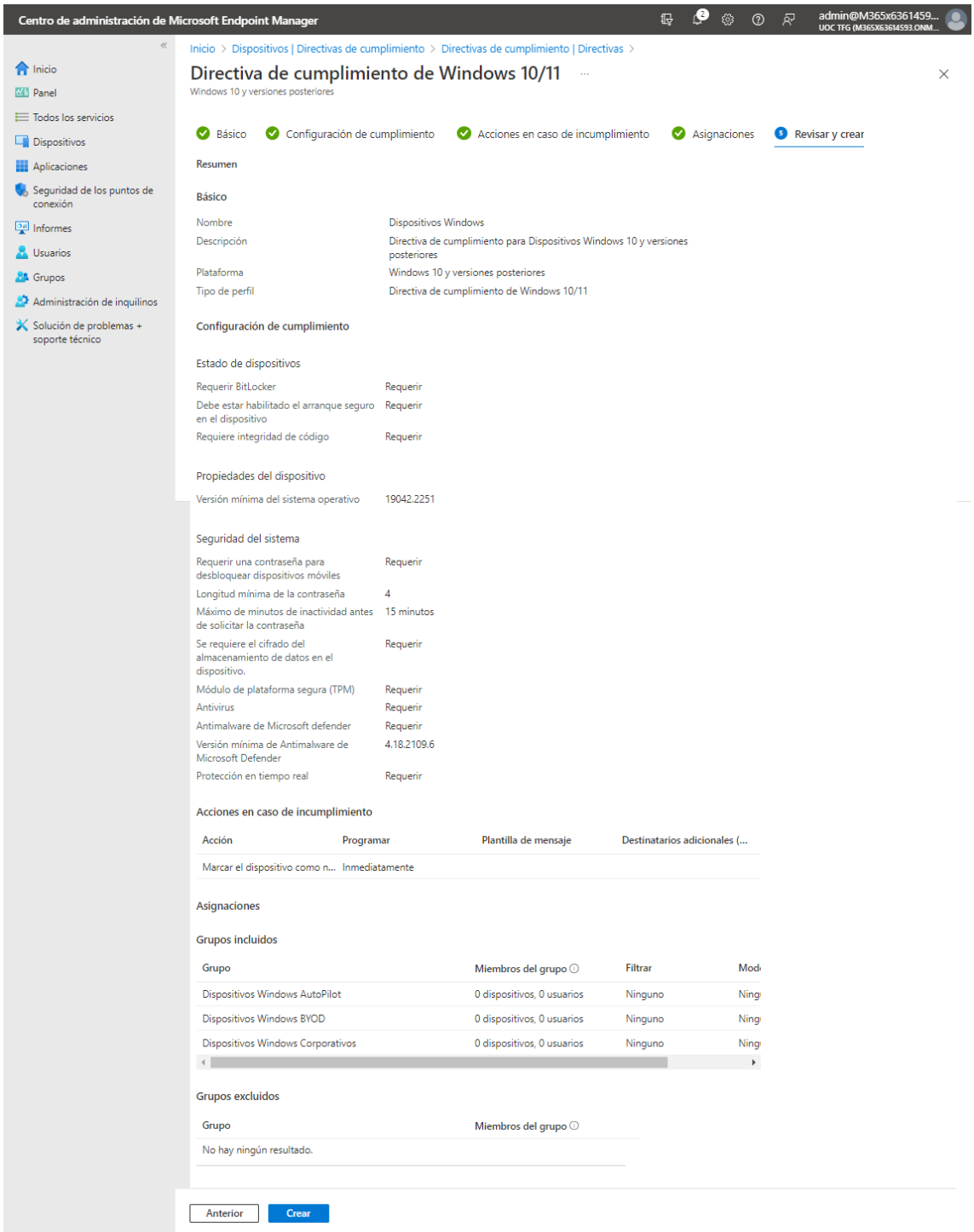


Figura 30 - Directiva de cumplimiento para dispositivos Windows

- **<u>Dispositivos Android</u>**

Para los dispositivos Android se debe diferenciar entre aquellos que serán propiedad de la organización y, por tanto, estarán completamente gestionados, y los que serán propiedad de los empleados y simplemente dispondrán de un perfil de trabajo.

Así, habrá dos directivas de cumplimiento diferentes, una más restrictiva para los dispositivos corporativos y otra más laxa para los dispositivos BYOD

En el caso de la directiva para los dispositivos corporativos, la configuración es la siguiente:

- Nombre: Dispositivos Android Corporativos
- Descripción: Directiva de cumplimiento para los dispositivos Android corporativos totalmente gestionados
- Plataforma: Android Enterprise
- Tipo de perfil: Perfil de trabajo de propiedad corporativa, dedicado y totalmente administrado
- Atestación de dispositivo SafetyNet: Comprobar integridad básica y dispositivos certificados
- Versión mínima del sistema operativo: 11.0
- Contraseña para desbloquear el dispositivo: Requerir
- Tipo de contraseña requerida: Biométrica deficiente
- Máximo de minutos de inactividad antes de solicitar la contraseña: 1
- Número de días hasta que expire la contraseña: 30
- Número de contraseñas requeridas antes de que el usuario pueda reusar una: 6
- Cifrado del almacenamiento de datos en el dispositivo: Requerir
- Integridad del entorno de ejecución de las aplicaciones de Intune: Requerir

La directiva se aplicará al grupo “Dispositivos Android Enterprise COBO”. Los dispositivos que no cumplan con los requisitos serán marcados inmediatamente como no conformes y el usuario recibirá una notificación push informa del estado. Además, si pasados 3 días no se ha remediado el estado y este sigue siendo no conforme, los dispositivos serán bloqueados automáticamente.

La directiva de los dispositivos corporativos es más restrictiva que la de los BYOD porque se trata de dispositivos sobre los que se tiene mayor control al ser propiedad de la organización y ser adquiridos por ella. Por tanto, se pueden exigir configuraciones más específicas, como una versión mínima de sistema operativo o que los dispositivos estén certificados, así como que la biometría esté habilitada (dado que la organización sabe que todos sus dispositivos cuentan con ella).

La siguiente imagen muestra los detalles de la directiva.

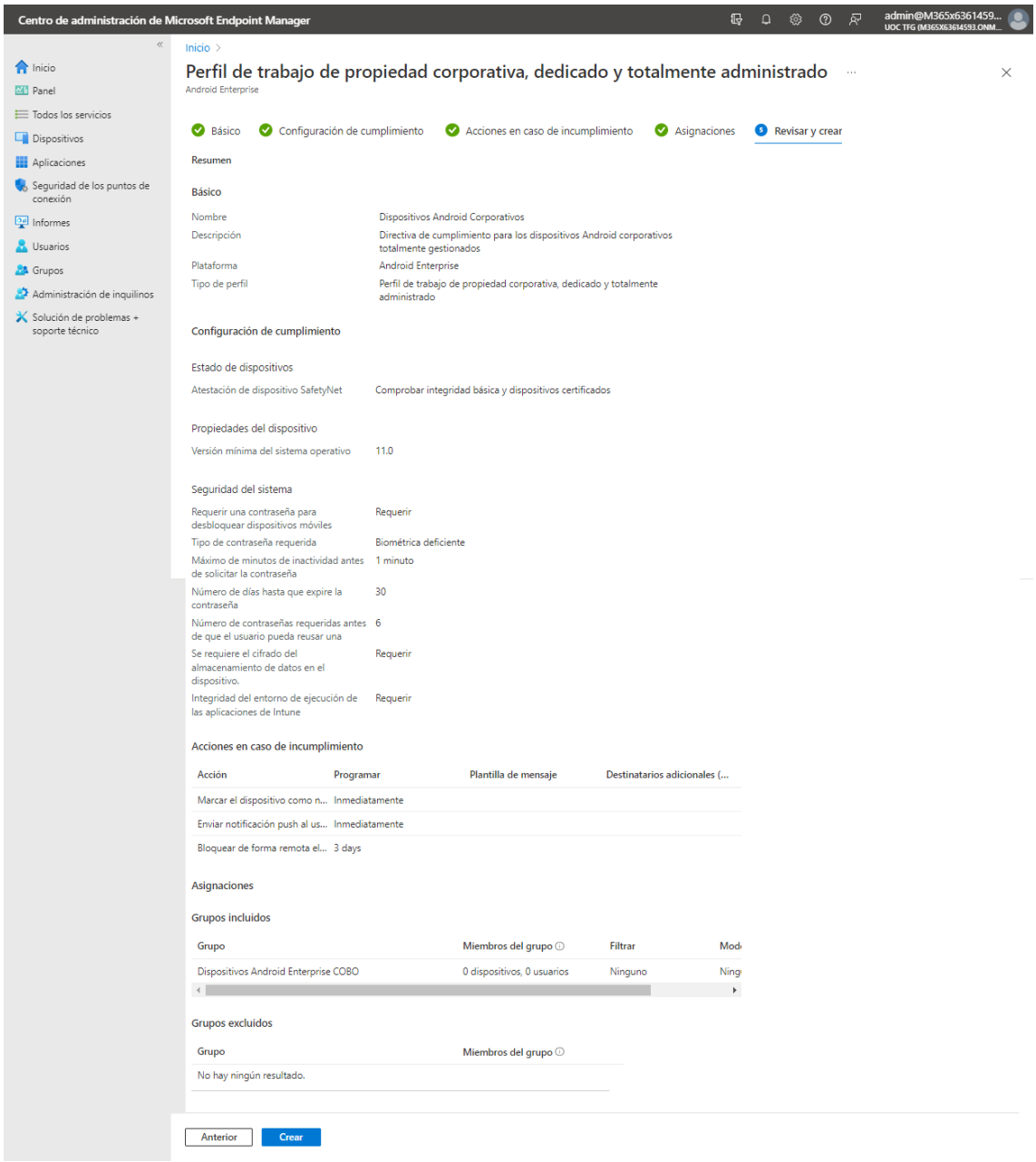


Figura 31 - Directiva de cumplimiento para dispositivos Android corporativos

En cuanto a los dispositivos Android BYOD, la configuración de la directiva de cumplimiento es:

- Nombre: Dispositivos Android BYOD
- Descripción: Directiva de cumplimiento para los dispositivos Android personales BYOD
- Plataforma: Android Enterprise
- Tipo de perfil: Perfil de trabajo de propiedad personal
- Dispositivos liberados (con acceso root): Bloquear
- Google Play Services configurado: Requerir
- Atestación de dispositivo SafetyNet: Comprobar integridad básica

- Integridad en tiempo de ejecución de la aplicación Portal de empresa: Requerir
- Contraseña para desbloquear el dispositivo: Requerir
- Tipo de contraseña requerida: Al menos numérica
- Complejidad de la contraseña: Baja
- Máximo de minutos de inactividad antes de solicitar la contraseña: 1
- Número de días hasta que expire la contraseña: 30
- Número de contraseñas requeridas antes de que el usuario pueda reusar una: 6

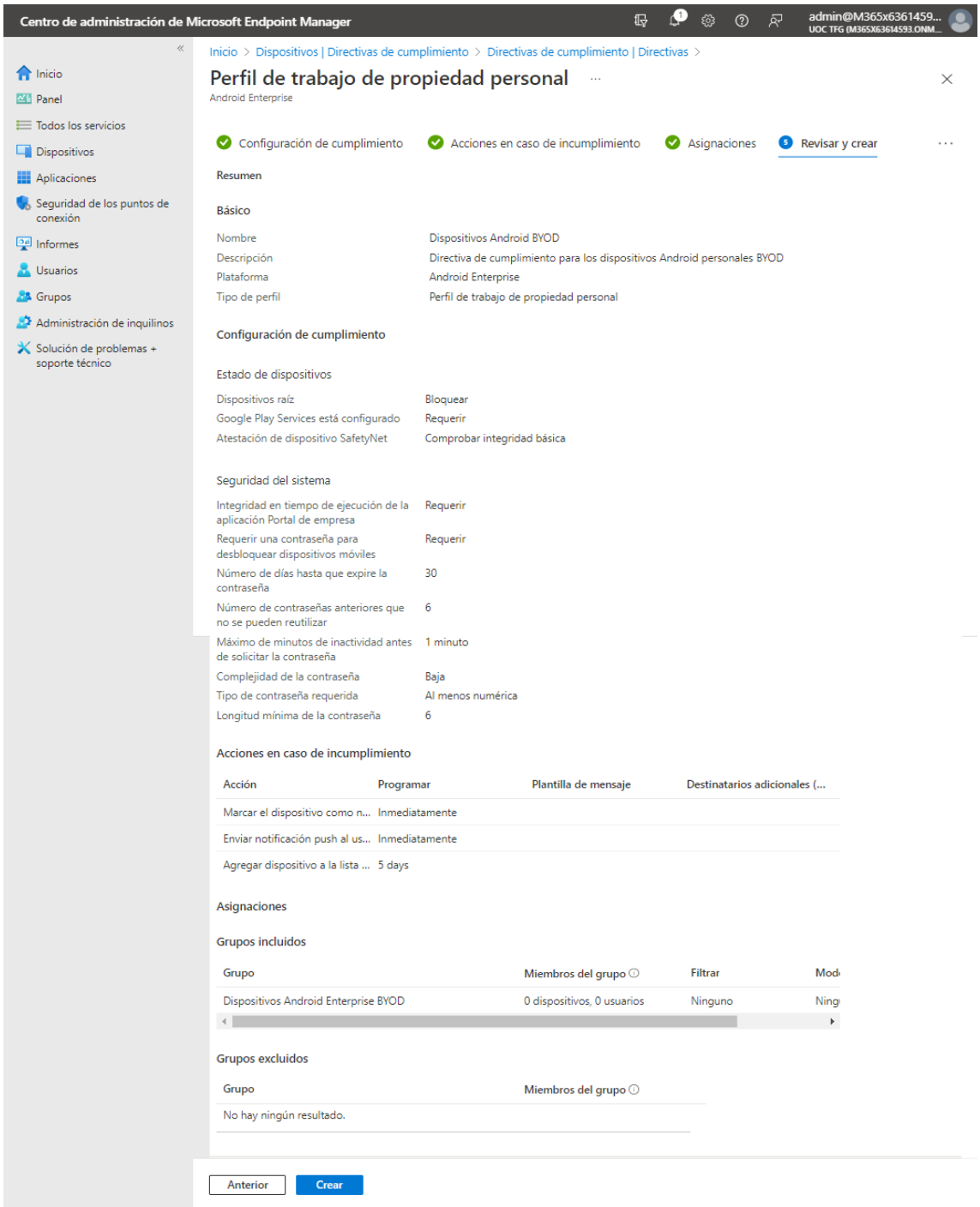


Figura 32 - Directiva de cumplimiento para dispositivos Android BYOD

La directiva se aplicará al grupo “Dispositivos Android Enterprise BYOD”, y los dispositivos que no cumplan los requisitos serán marcados inmediatamente como no conformes. Además, los usuarios recibirán una notificación push indicando que el dispositivo es no conforme y, si no se remedia para que sea conforme, será añadido a la lista de retirada pasados 5 días. Esto último implica que los datos de las aplicaciones administradas, la configuración y los perfiles de correo electrónico asignados con Intune serán eliminados del dispositivo. Los datos personales, sin embargo, permanecerán intactos.

- **Dispositivos macOS**

La directiva de cumplimiento para los dispositivos Apple con sistema operativo macOS incluye lo siguiente:

- Nombre: Dispositivos macOS
- Descripción: Directiva de cumplimiento para dispositivos Apple con sistema operativo macOS
- Plataforma: macOS
- Tipo de perfil: Directiva de cumplimiento de Mac
- Protección de integridad del sistema: Requerir
- Contraseña para desbloquear el dispositivo: Requerir
- Contraseñas sencillas: Bloquear
- Longitud mínima de la contraseña: 6
- Tipo de contraseña requerida: Alfanumérica
- Número de caracteres no alfanuméricos en la contraseña: 1
- Máximo de minutos de inactividad antes de solicitar la contraseña: 5
- Expiración de la contraseña (días): 30
- Complejidad de la contraseña: Baja
- Número de contraseñas requeridas antes de que el usuario pueda reusar una: 6
- Permitir aplicaciones descargadas desde: Mac App Store y desarrolladores identificados

La directiva se aplicará al grupo “Dispositivos macOS”. En caso de que los dispositivos sean no conformes, serán marcados inmediatamente como no conformes y si permanecen en dicho estado durante 5 días, serán añadidos a la lista de retirada de dispositivos. De igual forma que para los dispositivos Android BYOD, esto último implica que todos los datos corporativos serán eliminados del dispositivo.

Dado que no se puede discriminar a nivel de directiva entre dispositivos macOS corporativos o personales (sí se podría crear una directiva para cada caso), se ha optado por configurar una directiva de cumplimiento menos restrictiva de forma global para, más adelante, aplicar un perfil de configuración más restrictivo a los dispositivos macOS corporativos.

La siguiente imagen muestra los detalles de la directiva creada.

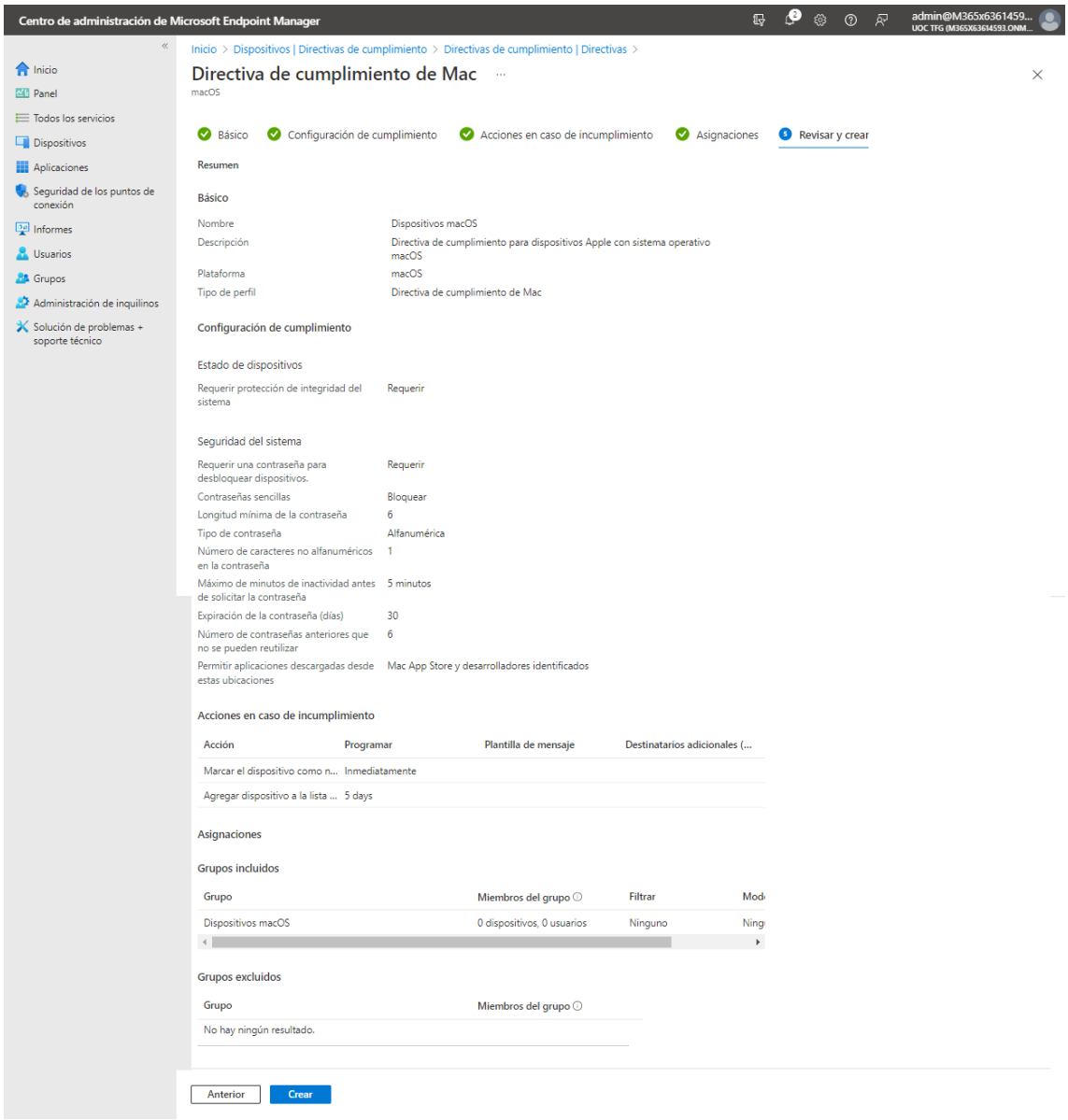


Figura 33 - Directiva de cumplimiento para dispositivos Apple macOS

- **<u>Dispositivos iOS e iPadOS</u>**

La directiva de cumplimiento para los dispositivos Apple con sistema operativo iOS e iPadOS se ha configurado según los siguientes parámetros:

- Nombre: Dispositivos macOS
- Descripción: Directiva de cumplimiento para dispositivos Apple con sistema operativo iOS e iPadOS
- Plataforma: iOS/iPadOS

- Tipo de perfil: Directiva de cumplimiento de iOS
- Dispositivos con jailbreak: Bloquear
- Versión mínima del sistema operativo: 15.0
- Contraseña para desbloquear el dispositivo: Requerir
- Contraseñas sencillas: Bloquear
- Longitud mínima de la contraseña: 6
- Tipo de contraseña requerida: Numérica
- Máximo de minutos de inactividad antes de solicitar la contraseña: 1
- Máximo de minutos de inactividad hasta que se bloquea la pantalla: 1
- Expiración de la contraseña (días): 30
- Número de contraseñas requeridas antes de que el usuario pueda reusar una: 6

De igual modo que para los dispositivos con sistema operativo macOS, se ha creado una directiva de cumplimiento global que se aplicará al grupo "Dispositivos iOS-iPadOS" en el que se encontrarán tanto dispositivos corporativos como BYOD. Por ello, se han rebajado los requisitos en ciertas áreas como la complejidad de la contraseña requerida, teniendo también en cuenta que se trata principalmente de dispositivos táctiles sin teclado físico y que introducir contraseñas alfanuméricas constantemente es bastante tedioso dada la propia interfaz del teclado.

Siguiendo en la línea del resto de directivas anteriores, no se permiten dispositivos liberados (*jailbreak*) por el gran riesgo de seguridad que ello supone. Además, gracias al gran soporte que ofrece Apple a sus dispositivos más antiguos en lo que a actualizaciones de sistema operativo se refiere, se ha configurado como versión mínima de iOS e iPadOS la 15.0, publicada a finales de 2021 y con la que son compatibles dispositivos iPhone lanzados a partir de finales de 2015 (iPhone 6S en adelante) e iPad a partir de 2014 (iPad Air 2 y posteriores)[29][30].

Los dispositivos iOS/iPadOS corporativos deberán disponer de configuraciones de seguridad adicionales, pero serán aplicadas más adelante mediante un perfil de configuración específico.

La siguiente imagen muestra los detalles de configuración de la directiva de cumplimiento creada.

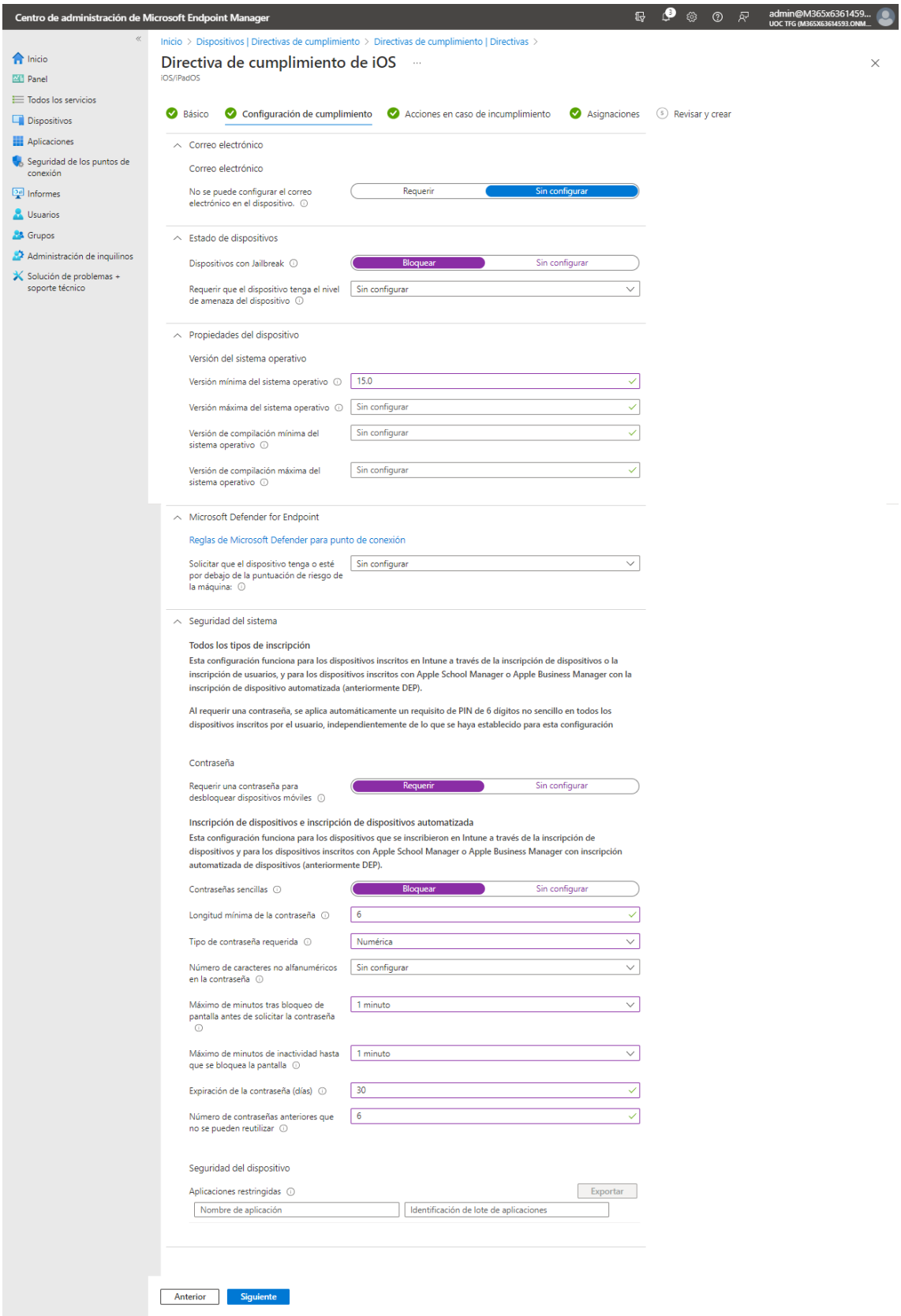


Figura 34 - Directiva de cumplimiento para dispositivos Apple iOS/iPadOS

- **Dispositivos Linux**

Tal y como se ha comentado anteriormente, el soporte de Dispositivos Linux en Microsoft Intune es muy reciente (finales de octubre de 2022) y por ello todavía no existen muchas funcionalidades disponibles a nivel de gestión de manera nativa (sí mediante scripts propios que se pueden subir a la herramienta, por ejemplo). Así, las configuraciones predefinidas que permiten controlar las directivas de cumplimiento de Linux son, por ahora, bastante limitadas.

Por lo indicado, la directiva de cumplimiento configurada simplemente contiene lo siguiente:

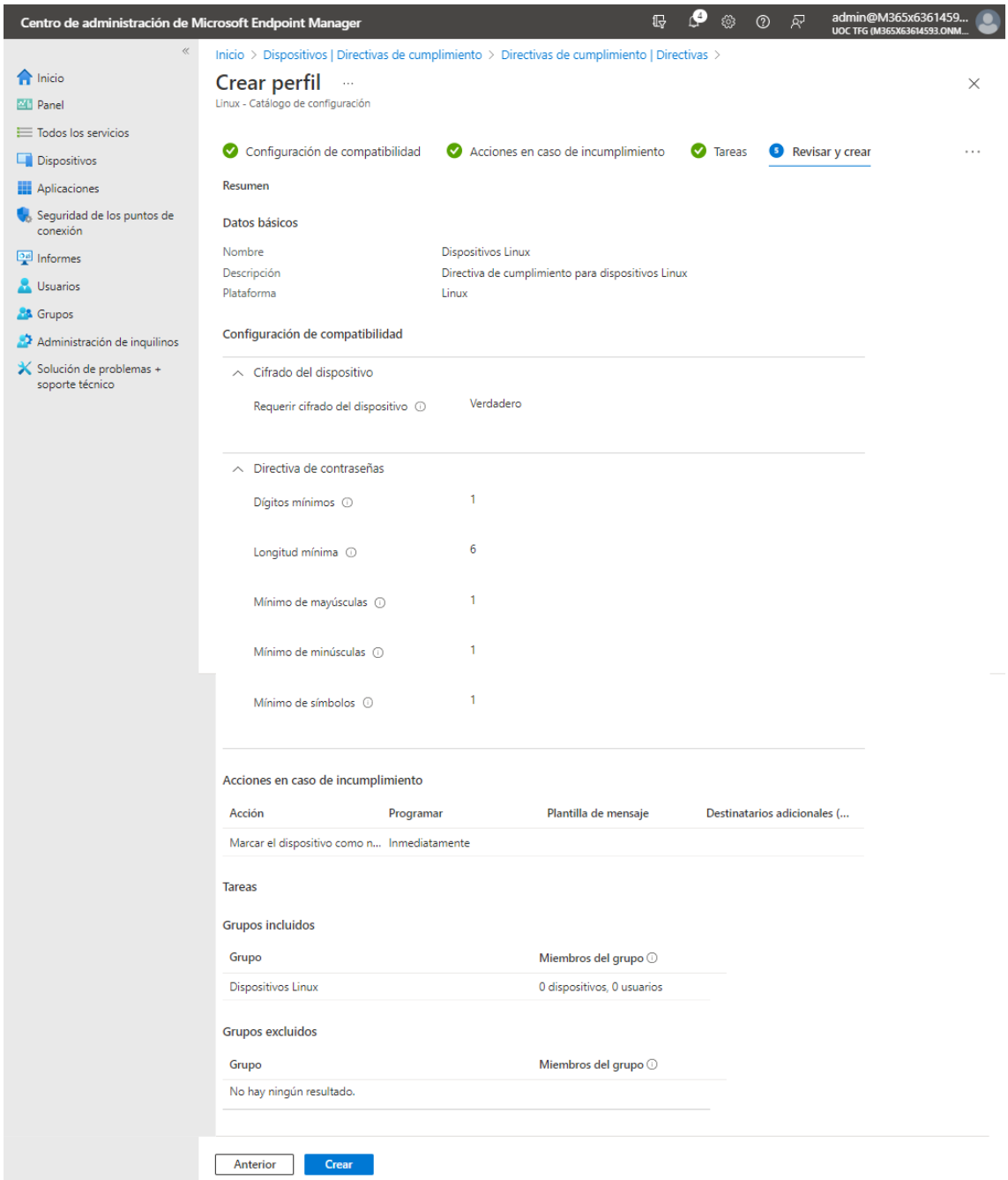


Figura 35 - Directiva de cumplimiento para dispositivos Linux

- Nombre: Dispositivos Linux
- Descripción: Directiva de cumplimiento para dispositivos Linux
- Plataforma: Linux
- Cifrado del dispositivo: Requerir
- Longitud mínima de contraseña: 6 caracteres
- Mínimo de dígitos: 1
- Mínimo de mayúsculas: 1
- Mínimo de minúsculas: 1
- Mínimo de símbolos: 1

La directiva se aplicará al grupo “Dispositivos Linux” y los dispositivos que no cumplan los requisitos serán marcados inmediatamente como no conformes.

3.3.6 Perfiles de configuración

Los perfiles de configuración se utilizan para aplicar las configuraciones deseadas a los dispositivos gestionados en Microsoft Intune. En muchas ocasiones, las diferencias entre las directivas de cumplimiento y los perfiles de configuración no se tienen del todo claras, ya que puede parecer que ambas comparten el mismo objetivo. Sin embargo, se trata de funcionalidades del MDM diferentes. Mientras que las directivas de cumplimiento sirven para evaluar si se cumplen una serie de configuraciones y/o propiedades, a modo de línea base, los perfiles de configuración se encargan de aplicar las configuraciones establecidas por los administradores. Es decir, las directivas de cumplimiento sólo evalúan (no fuerzan ningún cambio), y los perfiles de configuración aplican parámetros.

Por todo lo indicado, directivas de cumplimiento y perfiles de configuración deben trabajar en la misma dirección. Si se aplican configuraciones diferentes a las que se evalúan en las directivas de cumplimiento, los dispositivos se marcarán como no conformes, con lo que ello conlleva en cada caso.

De la misma manera que ha sido necesario crear distintas directivas de cumplimiento para cada plataforma, hay que hacer lo mismo con los perfiles de configuración, ya que cada plataforma tiene sus propias configuraciones. Por el momento, no es posible crear perfiles de configuración para dispositivos Linux en Intune, aunque visto el ritmo de actualización de la herramienta en cuanto a la incorporación de nuevas funcionalidades, es previsible que lo sea en un futuro no muy lejano.

A continuación se muestra, a modo de resumen, la configuración establecida en los perfiles de configuración de cada plataforma. El proceso completo detallado de la creación de cada perfil se puede consultar en el anexo 6, dada su gran extensión. Como se trata de un entorno de laboratorio para una prueba de concepto, se han realizado configuraciones mínimas con las que mostrar el funcionamiento de la solución y que permitan verificar su funcionamiento.

- **Dispositivos Windows**

Las opciones de configuración de los dispositivos Windows es, sin duda, una de las áreas en las que destaca Intune en cuanto a nivel de gestión y granularidad. La cantidad de posibles configuraciones a realizar de forma nativa (es decir, con opciones predefinidas en el portal web de administración) es infinitamente mayor que para el resto de las plataformas. Por si no fuera suficiente y alguna configuración no estuviese contemplada, la solución permite importar ficheros ADMX, que son plantillas administrativas de definición de directivas de grupo tradicionales on-premises, para complementar a las configuraciones predefinidas.

La configuración del perfil de configuración creado es:

- Nombre: Perfil Windows
- Descripción: Perfil de configuración para dispositivos Windows
- Plataforma: Windows 10 y versiones posteriores
- Impedir la escritura en dispositivos extraíbles: Habilitado
- Cifrado del dispositivo BitLocker: Requerir
- Contraseña del dispositivo: Habilitada
- Contraseña de dispositivo alfanumérica requerida: Se requiere una contraseña, un PIN numérico o un PIN alfanumérico
- Expiración de contraseña de dispositivo: 30
- Historial de contraseñas del dispositivo: 6
- Longitud mínima de la contraseña del dispositivo: 6
- Número máximo de errores de introducción de la contraseña del dispositivo: 5
- Número mínimo de caracteres complejos de la contraseña del dispositivo: Se requieren dígitos, letras minúsculas, letras mayúsculas y caracteres especiales. No se admite en el escritorio
- Deshabilitar el botón Quitar TPM: Habilitado
- No permitir la invalidación de Protección contra vulnerabilidades: Habilitado
- Comprobar las firmas de Defender antes de ejecutar el examen: Habilitado
- Acción correctiva para amenazas de gravedad alta: Limpiar. El servicio intenta recuperar archivos y desinfectar
- Permitir Cortana: Bloqueado
- Permitir servicio avanzado de juego: Bloqueado
- Dirección URL de imagen de escritorio: https://imagenes.20minutos.es/files/og_thumbnail/uploads/imagenes/2022/01/03/uoc-ransomware.png
- Integridad de código aplicada por Hipervisor: Habilitado sin bloqueo

El perfil se ha aplicado a “Dispositivos Windows AutoPilot” y “Dispositivos Windows Corporativos”. “Dispositivos Windows BYOD” se ha excluido.

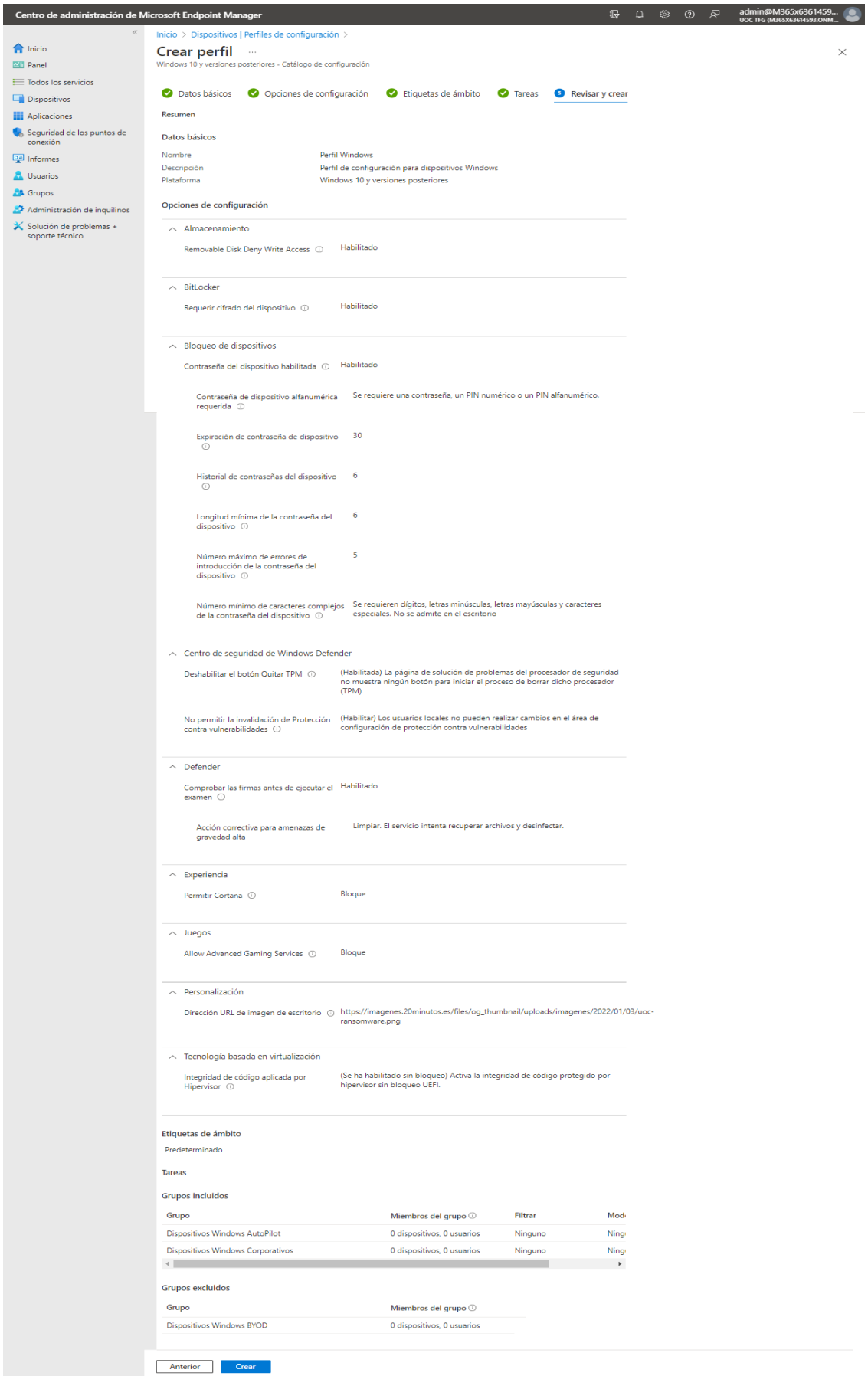


Figura 36 - Perfil de configuración de dispositivos Windows en Intune

- **Dispositivos Android BYOD**

Para los dispositivos Android BYOD se ha optado por crear un perfil que simplemente configure el correo, al tratarse de dispositivos personales.

- Nombre: Perfil Android BYOD
- Descripción: Perfil de configuración para dispositivos Android BYOD
- Plataforma: Android Enterprise
- Tipo de perfil: Correo electrónico
- Aplicación de correo electrónico: Nine Work
- Servidor de correo electrónico: outlook.office365.com
- Atributo de nombre de usuario de AAD: Nombre principal de usuario
- Atributo de dirección de correo electrónico de AAD: Nombre principal de usuario
- Método de autenticación: Nombre de usuario y contraseña
- SSL: Habilitar

El perfil se ha aplicado al grupo “Dispositivos Android BYOD”. En un escenario real, se podrían crear perfiles adicionales para aplicar restricciones tales como impedir la copia de información en el dispositivo entre el perfil personal y el de trabajo.

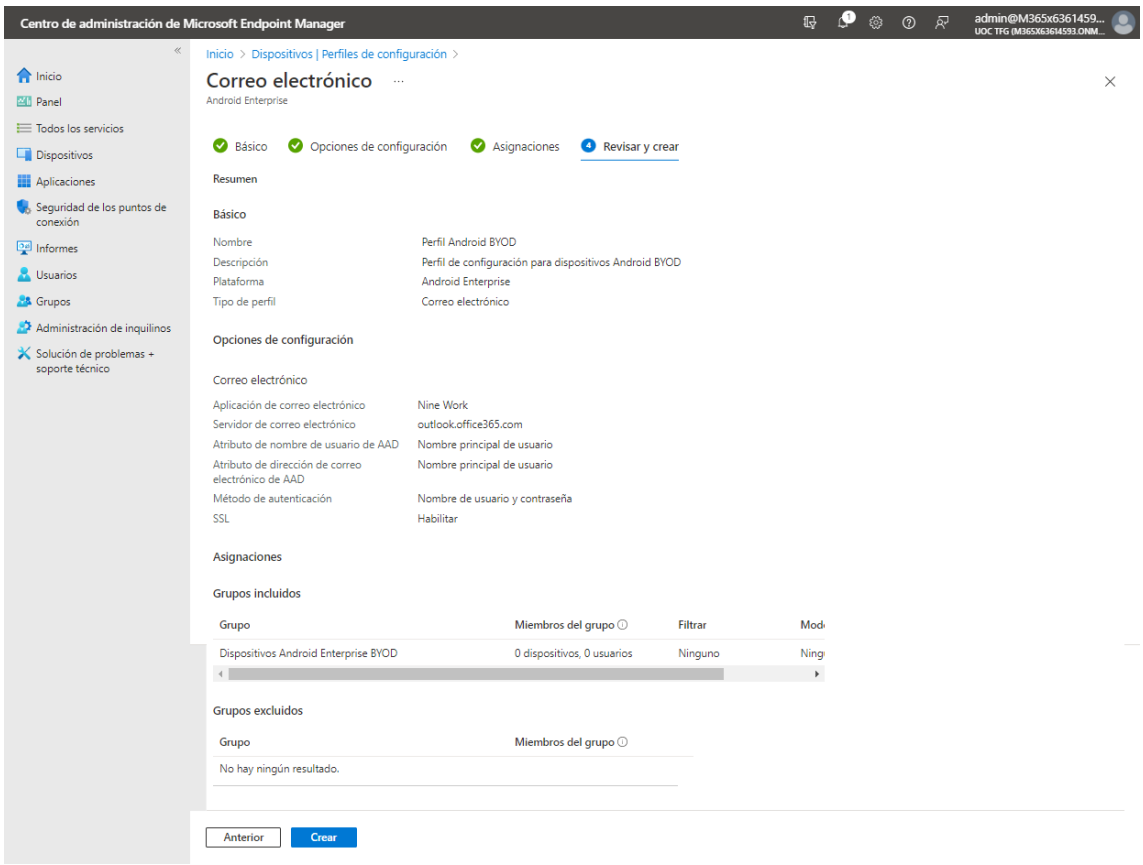


Figura 37 - Perfil de configuración de dispositivos Android BYOD

- **Dispositivos Android Corporativos**

En los dispositivos Android corporativos se aplicará un perfil con las siguientes restricciones y configuraciones:

- Nombre: Perfil Android Corporativo
- Descripción: Perfil de configuración para dispositivos Android Corporativos completamente gestionados
- Plataforma: Android Enterprise
- Tipo de perfil: Restricciones de dispositivos
- Captura de pantalla (nivel de perfil de trabajo): Bloquear
- Transferencia de archivos USB: Bloquear
- Medio de disco duro externo: Bloquear
- Correos electrónicos de protección frente al restablecimiento de fábrica: tfguocemeracouto@gmail.com
- Actualización del sistema: Automático
- Restablecimiento de fábrica: Bloquear
- Uso compartido de datos entre perfiles de trabajo y personales: Bloquear el uso compartido de un perfil de trabajo a otro personal
- Tipo de contraseña requerida: Biométrica deficiente
- Número de días hasta que expire la contraseña: 30
- Número de contraseñas requeridas antes de que el usuario pueda reusar una: 6
- Número de errores de inicio de sesión antes de borrar el dispositivo: 11
- Frecuencia de desbloqueo necesaria: 24 horas desde el último PIN, contraseña o desbloqueo de patrón
- Agregar usuarios nuevos: Bloquear
- Eliminación de usuario: Bloquear

El perfil de configuración se aplicará al grupo “Dispositivos Android Corporativos”. Como está dedicado a dispositivos Android Corporativos, se han restringido determinadas funcionalidades como restablecer el dispositivo de fábrica, el uso de medios extraíbles o el intercambio de información entre los perfiles personales y de trabajo.

En un entorno corporativo real sería necesaria la creación de perfiles adicionales para aplicar otro tipo de configuraciones, como por ejemplo la configuración automática de las redes Wifi corporativas o la instalación de algún certificado de empresa.

La siguiente imagen muestra los detalles de la configuración del perfil.

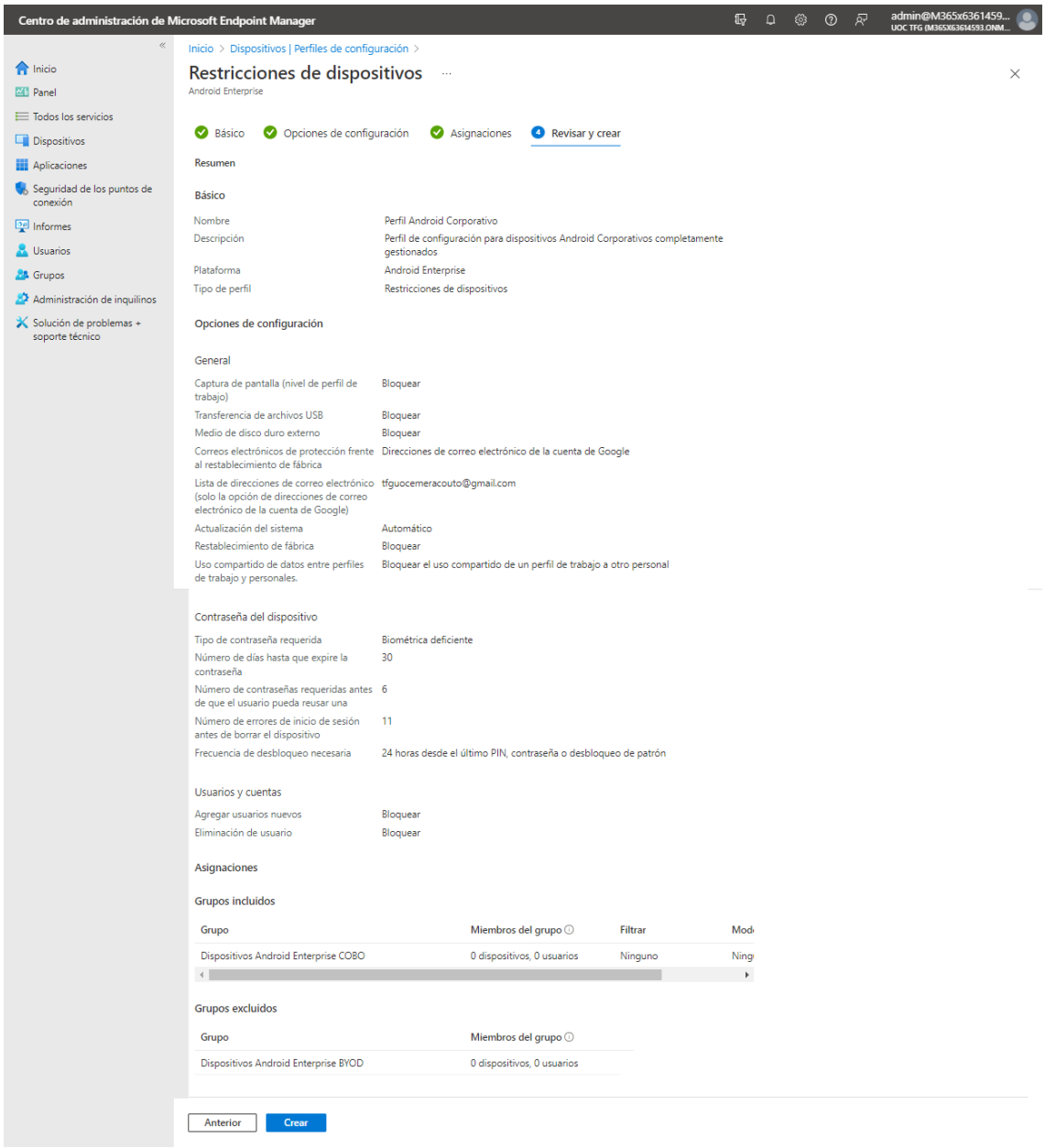


Figura 38 - Perfil de configuración de dispositivos Android Corporativos

- **<u>Dispositivos macOS</u>**

El perfil de configuración (se aplicará al grupo “Dispositivos macOS”) incluye:

- Nombre: Perfil macOS
- Descripción: Perfil de configuración para dispositivos Apple con sistema operativo macOS
- Plataforma: macOS
- Instalación de actualizaciones críticas: Verdadero
- Descarga automática: Verdadero
- Comprobación automática de actualizaciones habilitada: Verdadero

- Permitir relleno automático de contraseña: Falso
- Permitir juegos multijugador: Falso
- Permitir Game Center: Falso
- Permitir desbloqueo automático: Falso
- Permitir Air Drop: Verdadero
- Permitir agregar amigos de Game Center: Falso
- Longitud mínima del código de acceso: 6
- Inactividad máxima: 5
- Antigüedad máxima del PIN en días: 30
- Forzar PIN: Verdadero

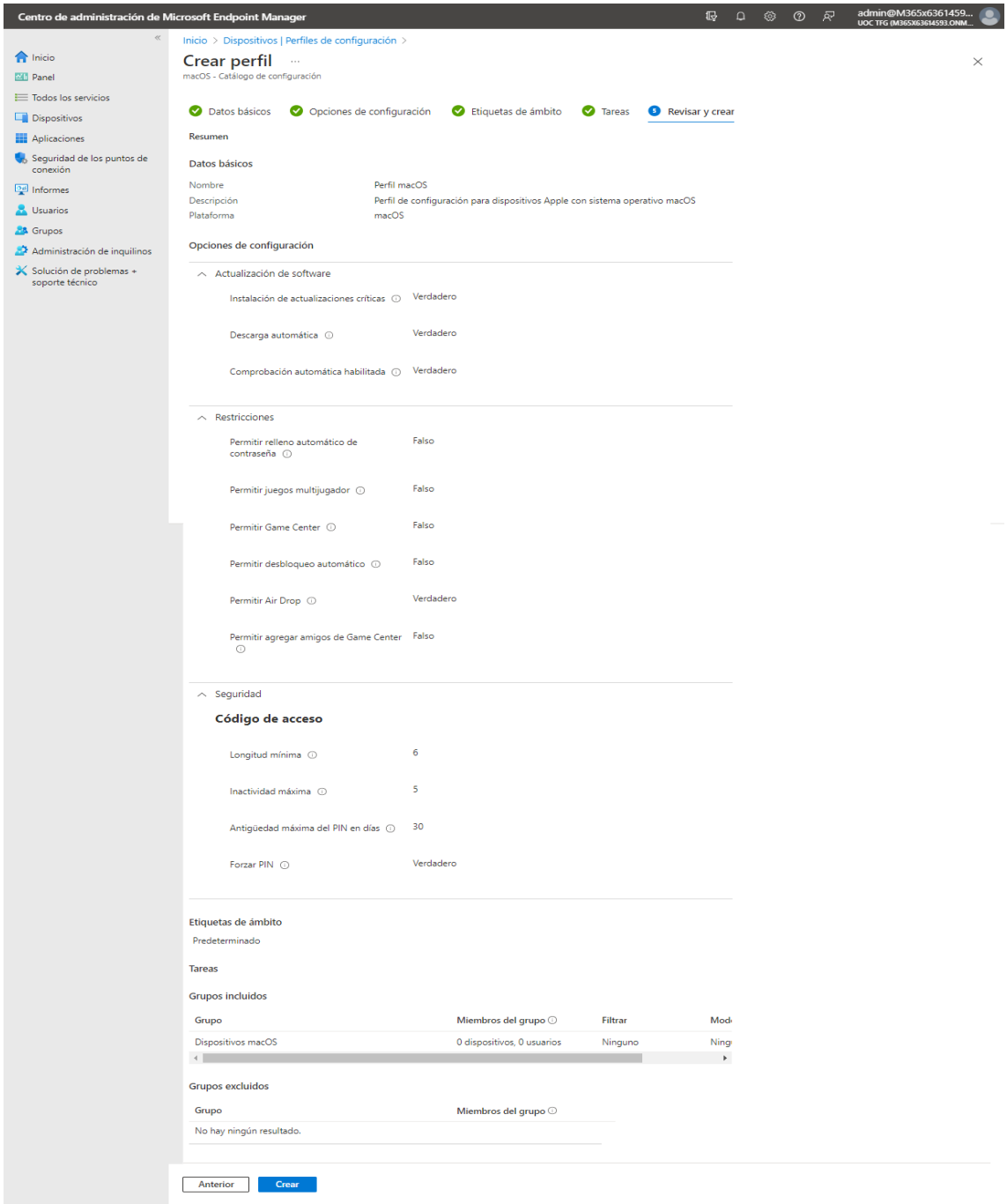


Figura 39 - Perfil de configuración de dispositivos Apple macOS

- **Dispositivos iOS e iPadOS**

El perfil de configuración para los dispositivos iOS e iPadOS se ha configurado de la siguiente forma:

- Nombre: Perfil iOS-iPadOS
- Descripción: Perfil de configuración para dispositivo Apple con sistema operativo iOS e iPadOS
- Plataforma: OS/iPadOS
- Permite configurar la confianza de las aplicaciones empresariales: Falso
- Forzar introducción de contraseña en iTunes Store: Verdadero
- Forzar fecha y hora automáticas: Verdadero
- Forzar copia de seguridad cifrada: Verdadero
- Núm. de intentos incorrectos del código de acceso: 11
- Longitud mínima del código de acceso: 6
- Antigüedad máxima del PIN en días: 30
- Forzar PIN: Verdadero
- Historial de PIN: 6
- Inactividad máxima: 1

El perfil se ha aplicado al grupo “Dispositivos iOS-iPadOS”. Se trata de un perfil de configuración básico que se aplicará a todos los dispositivos Apple con sistema operativo iOS e iPadOS que estén inscritos en el MDM, independientemente de si son dispositivos corporativos o BYOD.

La cantidad de configuraciones que Microsoft Intune permite aplicar a este tipo de dispositivos es muy amplia, igual que para los dispositivos macOS. Por tanto, la estrategia a seguir en entornos corporativos de producción es crear diferentes perfiles y dirigirlos de forma separada en función de si los dispositivos son personales o BYOD. Esto permitirá lograr un nivel de protección suficiente para los dispositivos personal y óptimo para los dispositivos corporativos.

En la siguiente imagen se muestran los detalles del perfil de configuración comentados anteriormente.

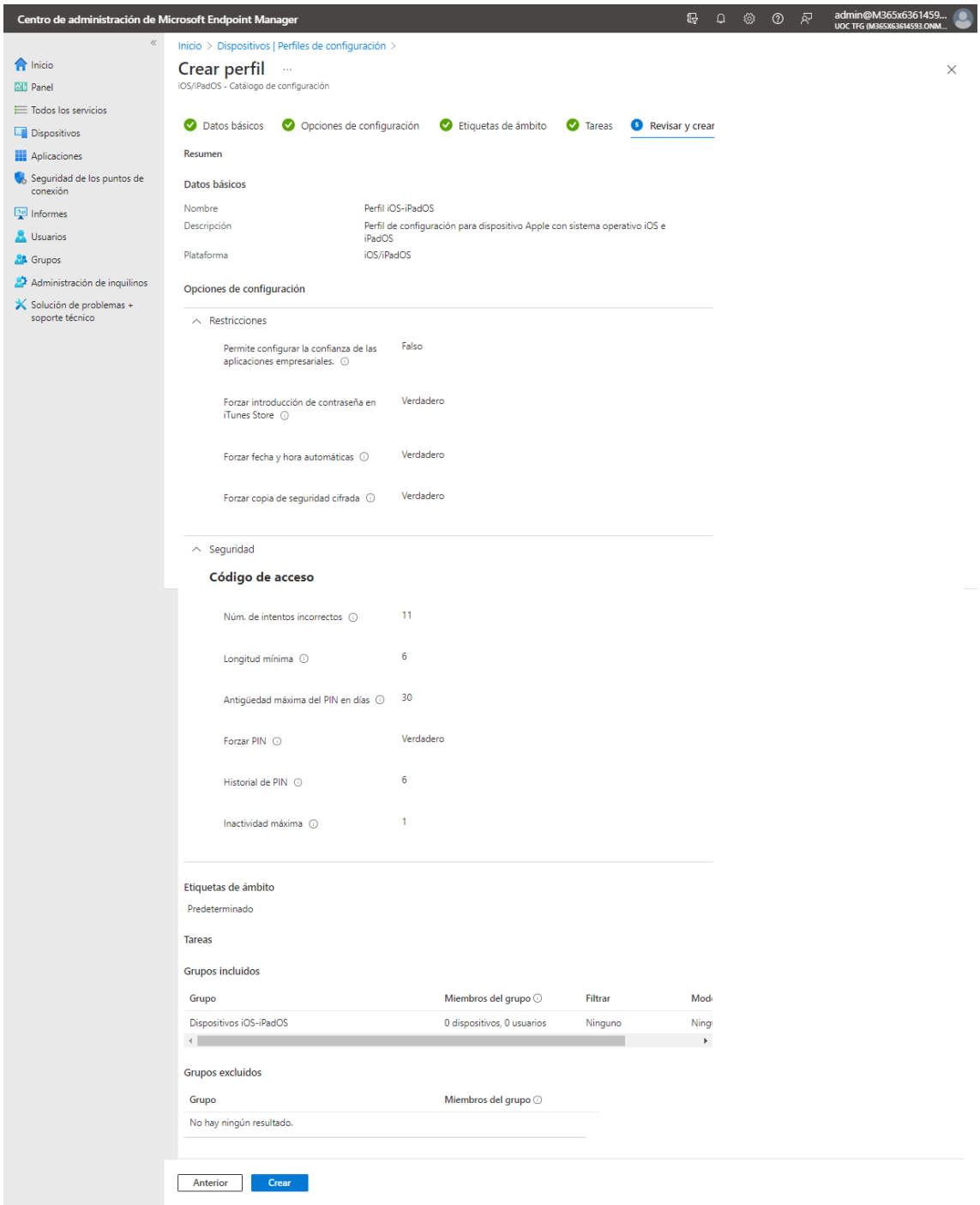


Figura 40 - Perfil de configuración de dispositivos Apple iOS/iPadOS

3.3.7 Acceso condicional

El acceso condicional es una funcionalidad de Microsoft Intune que permite controlar el acceso a determinados recursos en función de una serie de reglas impuestas. Esto ayuda a proteger la información corporativa, asegurando que

solo se pueda acceder a ella desde escenarios que se consideran de confianza para la organización.

Con el fin de evaluar la funcionalidad, se ha creado una directiva de acceso condicional que únicamente permitirá el acceso a las aplicaciones de Office 365 (Exchange Online, Yammer, SharePoint Online, Teams, Forms…) si el dispositivo desde el que se accede está marcado como conforme en base a las directivas de cumplimiento definidas en el apartado 3.3.5.

No obstante, las posibilidades de configuración de este tipo de directivas son muy amplias y contemplan una gran cantidad de variables[31]. El proceso completo de creación se puede consultar en el anexo 7.

La directiva de acceso condicional creada, como se muestra a continuación, se aplicará a los usuarios del grupo “Usuarios de Intune”, al que pertenecerán todos los usuarios con licencia de Intune, y afectará a todas las plataformas de dispositivos. En caso de querer monitorizar qué ocurriría si se habilitase, la directiva se puede configurar en modo “Solo informe”.

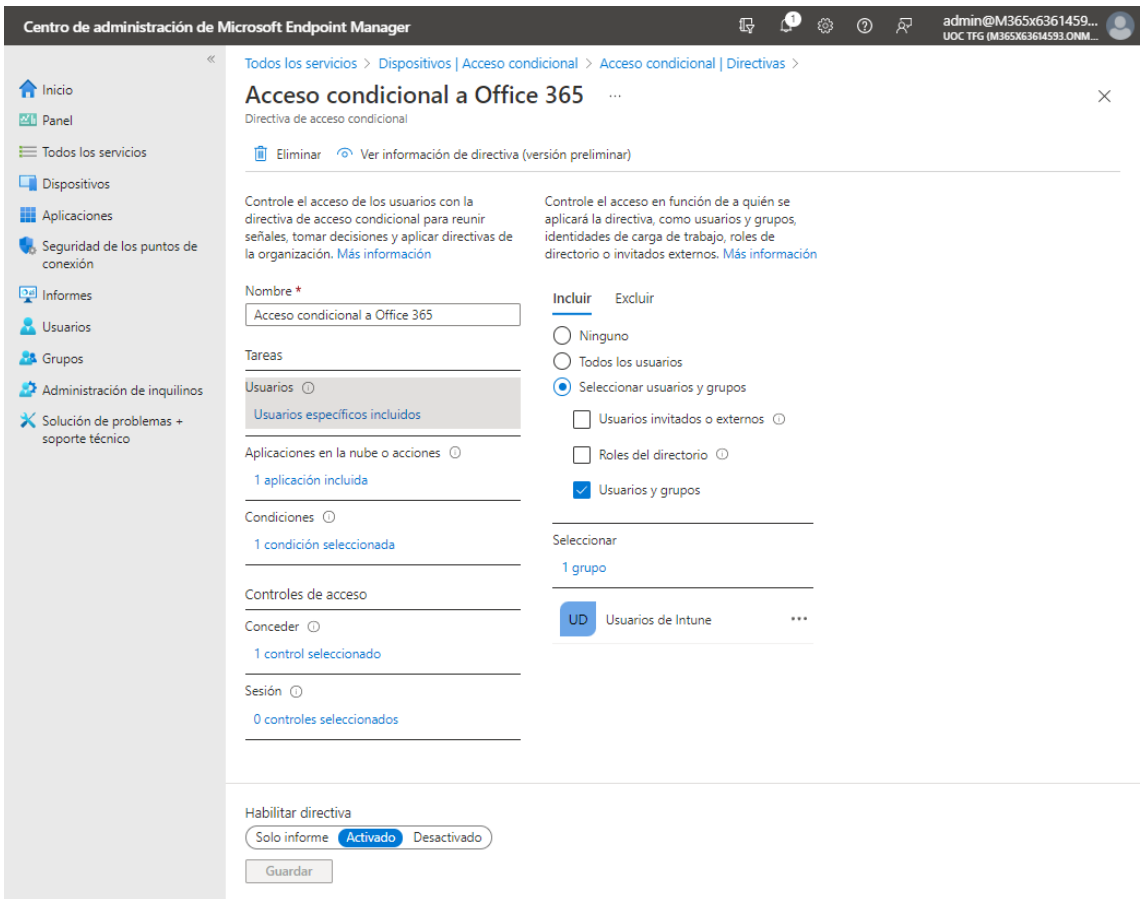


Figura 41 - Directiva de acceso condicional a Office 365

3.3.8 Gestión de actualizaciones

La gestión de actualizaciones de software es otra de las áreas que una buena solución de gestión de puesto de trabajo debe ofrecer, dado que las organizaciones necesitan mantener sus dispositivos actualizados para parchear vulnerabilidades y contar con de versiones de software en soporte. En el caso de Microsoft Intune, la herramienta dispone de dicha funcionalidad, aunque sus capacidades difieren en función del tipo de plataforma, como ya ha ocurrido con otras funcionalidades anteriormente utilizadas.

A continuación, se muestran las configuraciones de actualizaciones realizadas para cada plataforma. De nuevo, la plataforma Linux todavía no dispone de dicha funcionalidad en Microsoft Intune. El proceso de creación completo de cada perfil se puede consultar en el anexo 8.

- **Dispositivos Windows**

Como ya es habitual en la solución MDM, la capacidad de gestión de actualizaciones en dispositivos Windows es muy superior a las del resto de plataformas. En Windows, todas las configuraciones que se pueden aplicar de forma tradicional mediante directivas de grupo on-premises están disponibles a través del perfil de configuración. Entre ellas se encuentran, por ejemplo, qué día del mes se quieren instalar las actualizaciones, qué tipo de actualizaciones se deben instalar (seguridad, características o funcionalidad) o si se debe reiniciar el equipo automáticamente tras la instalación.

Microsoft Intune permite crear tres perfiles distintos dependiendo de lo que se quiera gestionar: anillos de actualización (donde se especifican el tipo de actualizaciones que se instalarán y la experiencia de usuario, entre otros), actualizaciones de funcionalidades (para determinar qué nuevas versiones de sistema operativo se instalarán) y actualizaciones de calidad.

Para la prueba de concepto, se ha optado por crear un perfil de anillos de actualización con los siguientes parámetros:

- Nombre: Configuración de actualización Windows
- Descripción: Configuración de actualizaciones para dispositivos Windows
- Actualizaciones de productos de Microsoft: Permitir
- Controladores de Windows: Permitir
- Período de aplazamiento de actualizaciones de calidad (días): 0
- Período de aplazamiento de actualizaciones de características (días): 0
- Actualizar dispositivos con Windows 10 a la versión más reciente de Windows 11: No
- Establecer el período de desinstalación de la actualización de características (de 2 a 60 días): 15
- Canal de servicio: Canal de disponibilidad general

- Comportamiento de actualización automática: Instalar automáticamente a la hora del mantenimiento
- Inicio de horas activas: 6 p.m.
- Fin de horas activas: 8 a.m.
- Comprobaciones de reinicio: Permitir
- Opción para pausar las actualizaciones de Windows: Deshabilitar
- Opción para comprobar las actualizaciones de Windows: Habilitar
- Cambiar el nivel de actualización de las notificaciones: Desactivar todas las notificaciones, excepto las advertencias de reinicio

El perfil de actualización se aplicará a todos los dispositivos Windows corporativos: “Dispositivos Windows AutoPilot” y “Dispositivos Windows Corporativos”.

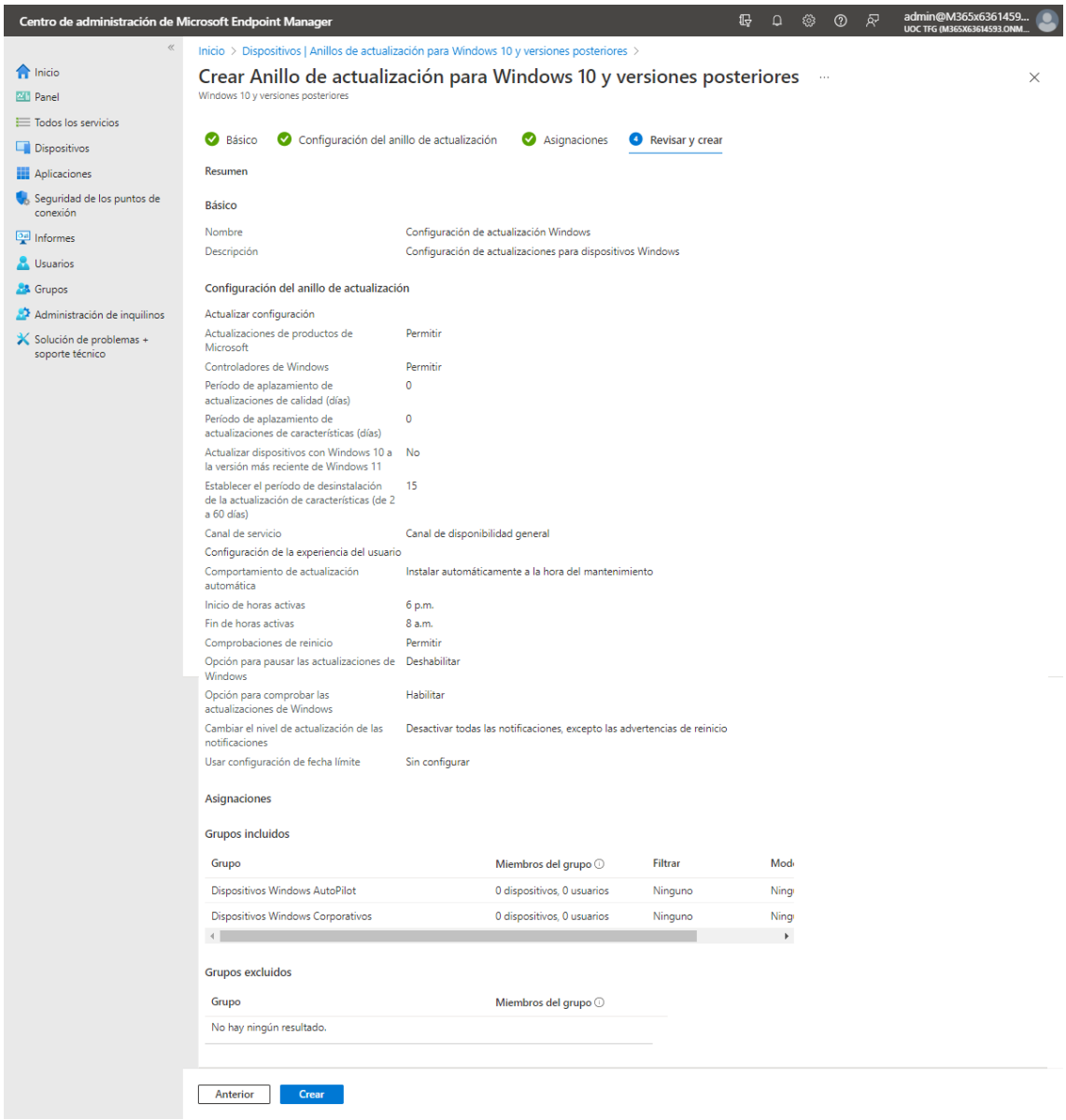


Figura 42 - Perfil de actualización de dispositivos Windows corporativos

- **Dispositivos Android**

A diferencia de para los dispositivos Windows, Microsoft Intune no dispone de ninguna opción predefinida para gestionar las actualizaciones de los dispositivos Android como tal, hasta la fecha. Esto es debido, principalmente, a dos motivos. El primero de ellos es que los dispositivos Android dependen del OEM para proporcionar una nueva plataforma o actualización del sistema, por lo que cada fabricante se encarga de las actualizaciones de sus dispositivos. El segundo, es que el proceso de actualización es distinto de un proveedor a otro.

Algunos fabricantes como Samsung brindan la posibilidad de gestionar las actualizaciones de sus dispositivos mediante plataformas propias como Knox E-FOTA que, además, se pueden integrar con Intune, pero requieren de licenciamiento[32].

Así, no hay funcionalidad explícita en Intune para tal fin. Sin embargo, es posible forzar de alguna forma a los usuarios a que mantengan sus dispositivos actualizados: mediante el uso de directivas de cumplimiento y de perfiles de configuración (para dispositivos corporativos). Con las directivas de cumplimiento, se puede exigir una versión mínima de Android para que sean conformes. Por otro lado, con los perfiles de configuración, se puede obligar a los dispositivos a que instalen automáticamente todas las actualizaciones disponibles. Estas dos configuraciones ya se han aplicado anteriormente en los apartados 3.3.5 y 3.3.6, respectivamente.

- **Dispositivos macOS**

La gestión de actualizaciones para dispositivos con sistema operativo macOS sí es posible en Microsoft Intune. Aunque la funcionalidad se encuentra en versión preliminar, por el momento, es completamente funcional y será añadida como funcionalidad plena del producto en una versión próxima.

El perfil de actualización, que se aplicará al grupo “Dispositivos macOS”, cuenta con las siguientes configuraciones:

- Nombre: Configuración de actualización macOS
- Descripción: Configuración de actualizaciones para dispositivos Apple con sistema operativo macOS
- Actualizaciones críticas: Instalar inmediatamente
- Actualizaciones de firmware: Instalar inmediatamente
- Actualizaciones del archivo de configuración: Solo notificación
- Actualizaciones restantes (sistema operativo, aplicaciones integradas): Solo notificación
- Tipo de programación: Actualizar durante la hora programada
- Zona horaria: UTC+1
- Período de tiempo: desde lunes (12 a.m.) hasta domingo (11 p.m)

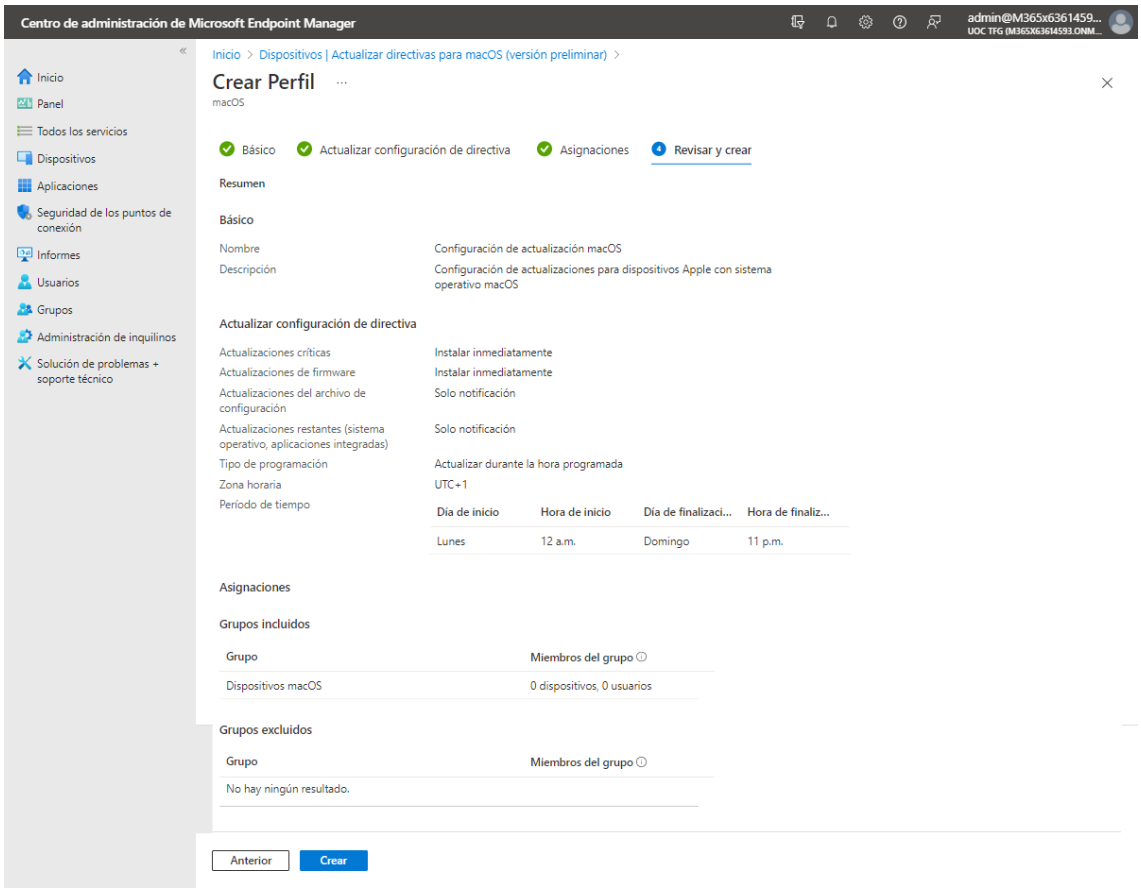


Figura 43 - Perfil de actualización de dispositivos Apple macOS

- **<u>Dispositivos iOS e iPadOS</u>**

La gestión de actualizaciones de dispositivos Apple con sistema operativo iOS e iPadOS también está disponible en Intune, de manera completa en este caso. Como los dispositivos dependen de un único proveedor, a diferencia de los Android, Microsoft puede integrar en su solución esta funcionalidad.

La configuración del perfil creado, que se aplicará al grupo “Dispositivos iOS-iPadOS”, es:

- Nombre: Configuración de actualización iOS-iPadOS
- Descripción: Configuración de actualizaciones para dispositivos Apple con sistema operativo iOS e iPadOS
- Actualización para instalar: Instalar iOS/iPadOS Última actualización
- Tipo de programación: Actualizar durante la hora programada
- Zona horaria: UTC+1
- Período de tiempo: desde lunes (10 p.m.) hasta martes (5 a.m.)

La siguiente imagen muestra los detalles del perfil de actualización.

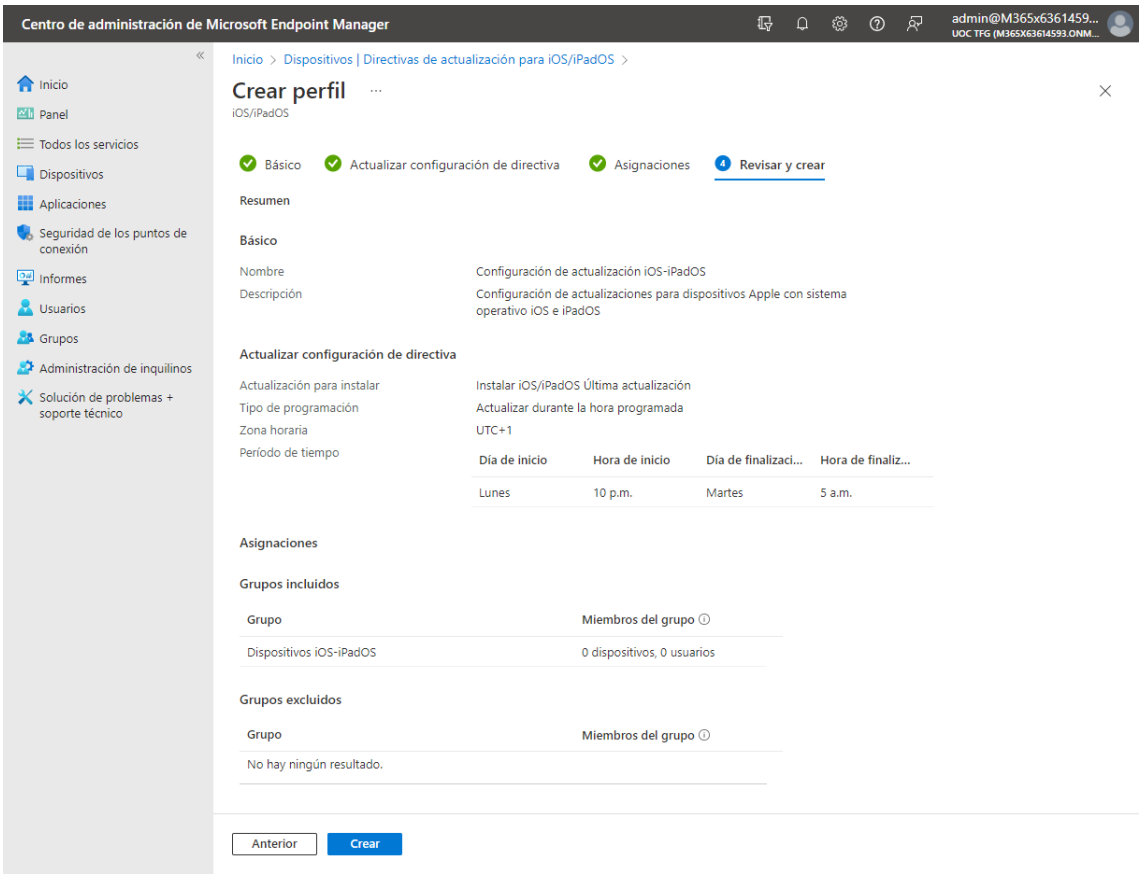


Figura 44 - Perfil de actualización de dispositivos Apple iOS/iPadOS

3.3.9 Gestión de aplicaciones

La gestión de aplicaciones es otra de las necesidades habituales a las que se enfrentan las organizaciones, pues todas las tareas de productividad se llevan a cabo, de un modo u otro, a través de ellas. La capacidad de gestión de Microsoft Intune en esta área es bastante amplia, permitiendo ofrecer un catálogo de aplicaciones e incluso aplicar en ellas configuraciones y restricciones.

Por un lado, Intune permite elegir qué aplicaciones se quieren publicar para las diferentes plataformas soportadas: Windows, Android, macOS e iOS/iPadOS. Ofrece un catálogo distinto en función de la plataforma, en base a sus correspondientes tiendas de aplicaciones, y también permite publicar aplicaciones propias de línea de negocio. Además, brinda la posibilidad de instalar las aplicaciones de forma requerida o dejarlas como disponibles en la tienda corporativa para que los usuarios instalen las que necesiten.

Por otro lado, la solución MDM permite crear directivas de protección y de configuración de aplicaciones, mediante las cuales se pueden definir restricciones en las aplicaciones (como, por ejemplo, que se cifren los datos corporativos) y establecer las configuraciones deseadas por la organización (como parámetros de Outlook o de Microsoft Edge).

La tabla siguiente muestra, de manera esquematizada, las funcionalidades ge gestión de aplicaciones existentes por plataforma.

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 45 - Funcionalidades de administración de aplicaciones de Intune

Fuente: https://learn.microsoft.com/es-es/mem/intune/apps/app-management

Con el fin de simplificar la prueba de concepto en un ámbito tan amplio como el de las aplicaciones, pero sin perder de vista los requisitos impuestos a la solución MDM, se ha optado por publicar una aplicación para cada plataforma disponible. Esto permitirá comprobar el funcionamiento de Intune en esta área.

A continuación, se muestra el resumen de las aplicaciones desplegadas para cada plataforma. Los detalles del proceso completo pueden consultarse en el anexo 9. De nuevo, todavía no es posible asignar aplicaciones a dispositivos Linux desde Microsoft Intune.

- **Dispositivos Windows**

La aplicación desplegada para los dispositivos Windows es la suite Microsoft 365. De entre las personalizaciones realizadas destacan la arquitectura de 64 bits y elección del canal actual, instalando siempre la versión más reciente. Los términos de licencia están aceptados (el usuario no tendrá que hacerlo) y el formato de documento elegido es XML abierto de Office. Además, se instalarán los idiomas español y catalán.

La aplicación se instalará de manera requerida en los dispositivos de los grupos "Dispositivos Windows AutoPilot" y "Dispositivos Windows Corporativos", y estará disponible para su instalación en los "Dispositivos Windows BYOD".

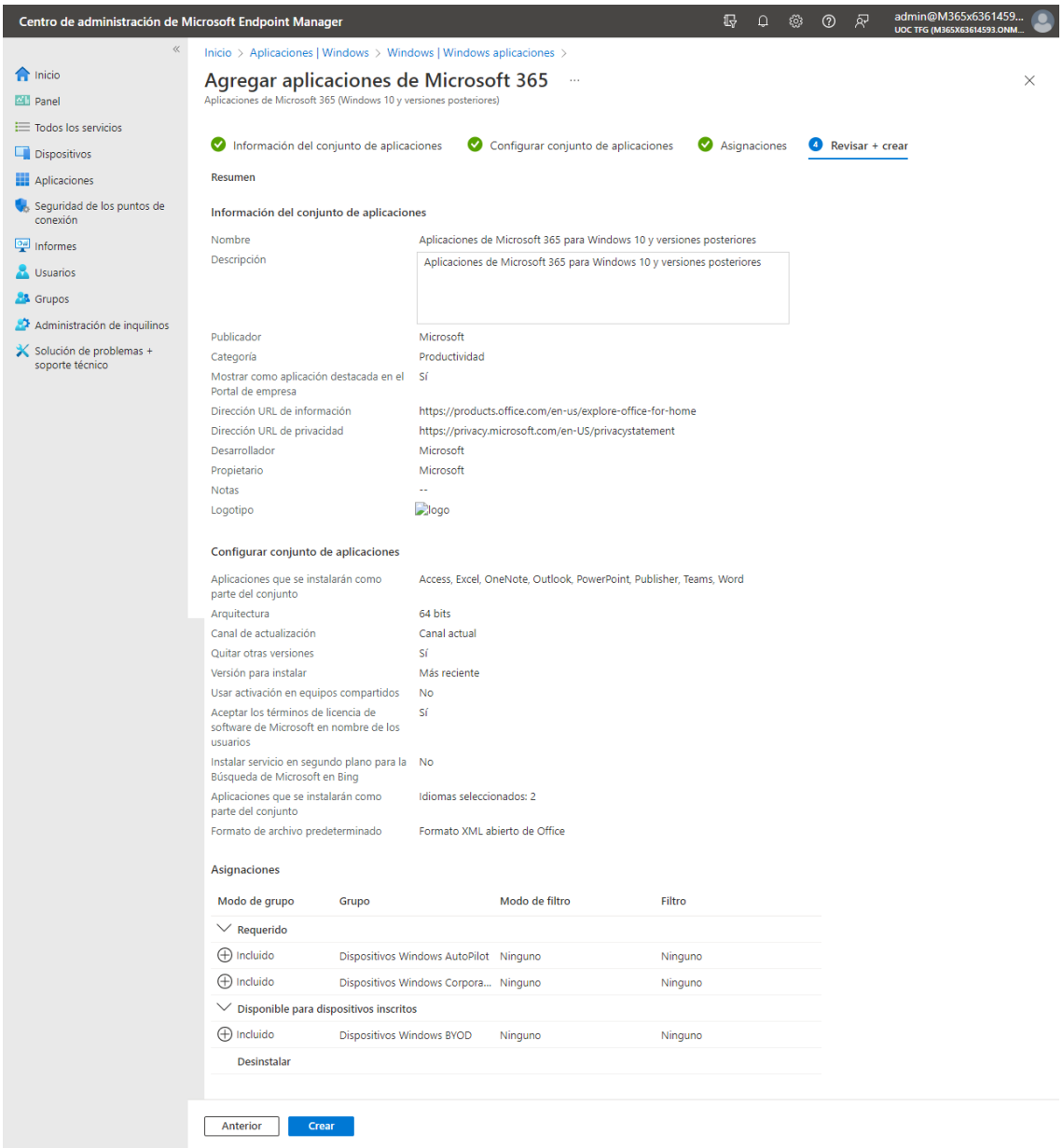


Figura 46 - Despliegue de aplicación en dispositivos Windows

- **Dispositivos Android**

En el caso de los dispositivos Android, la aplicación desplegada es Nine Work, que es el gestor de correo cuya configuración se ha realizado en el perfil de configuración para Android Enterprise BYOD. Se trata de una aplicación de Android Enterprise, por lo que debe ser aprobada primero en la tienda Google Play administrada para después poder ser asignada.

La aplicación se ha asignado como requerida al grupo “Dispositivos Android Enterprise BYOD”.

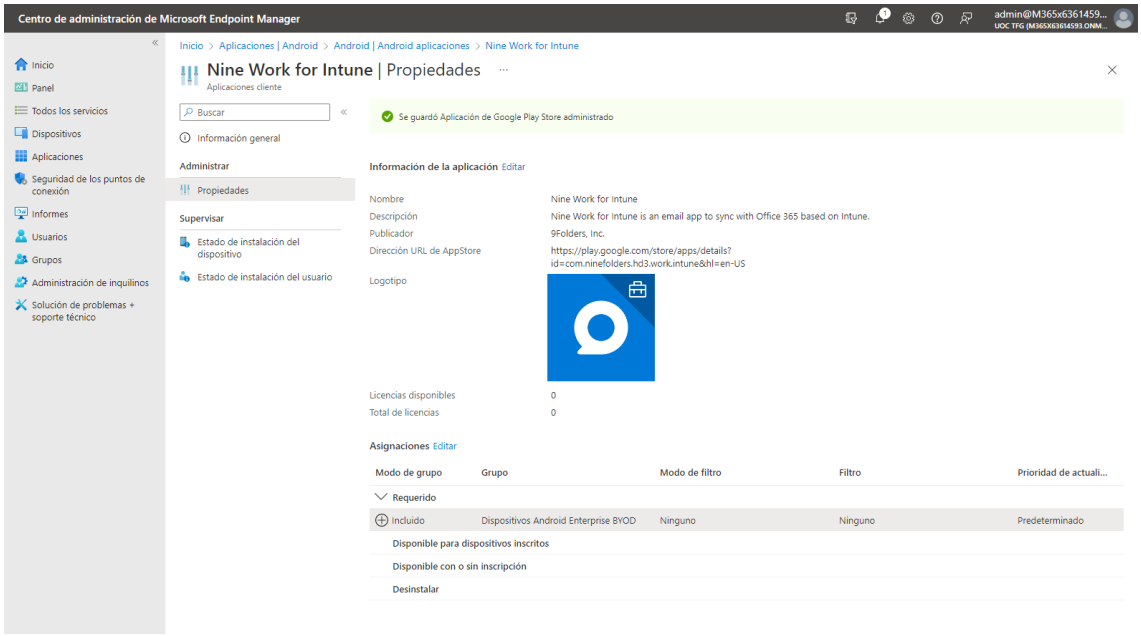


Figura 47 - Despliegue de aplicación en dispositivos Android

- **Dispositivos macOS**

Para los dispositivos macOS se ha decidido desplegar, de forma requerida, la aplicación Microsoft Edge Chromium. El canal elegido ha sido el estable, y el grupo de dispositivos al que se instalará es “Dispositivos macOS”.

Se trata de una aplicación sencilla en la que no es posible personalizar mucho más a nivel de despliegue. Sin embargo, se puede gestionar su comportamiento mediante perfiles de configuración, modificando los parámetros típicos de un navegador (página de inicio, proxy, opciones de seguridad…)

La siguiente imagen muestra el resumen del despliegue de la aplicación.

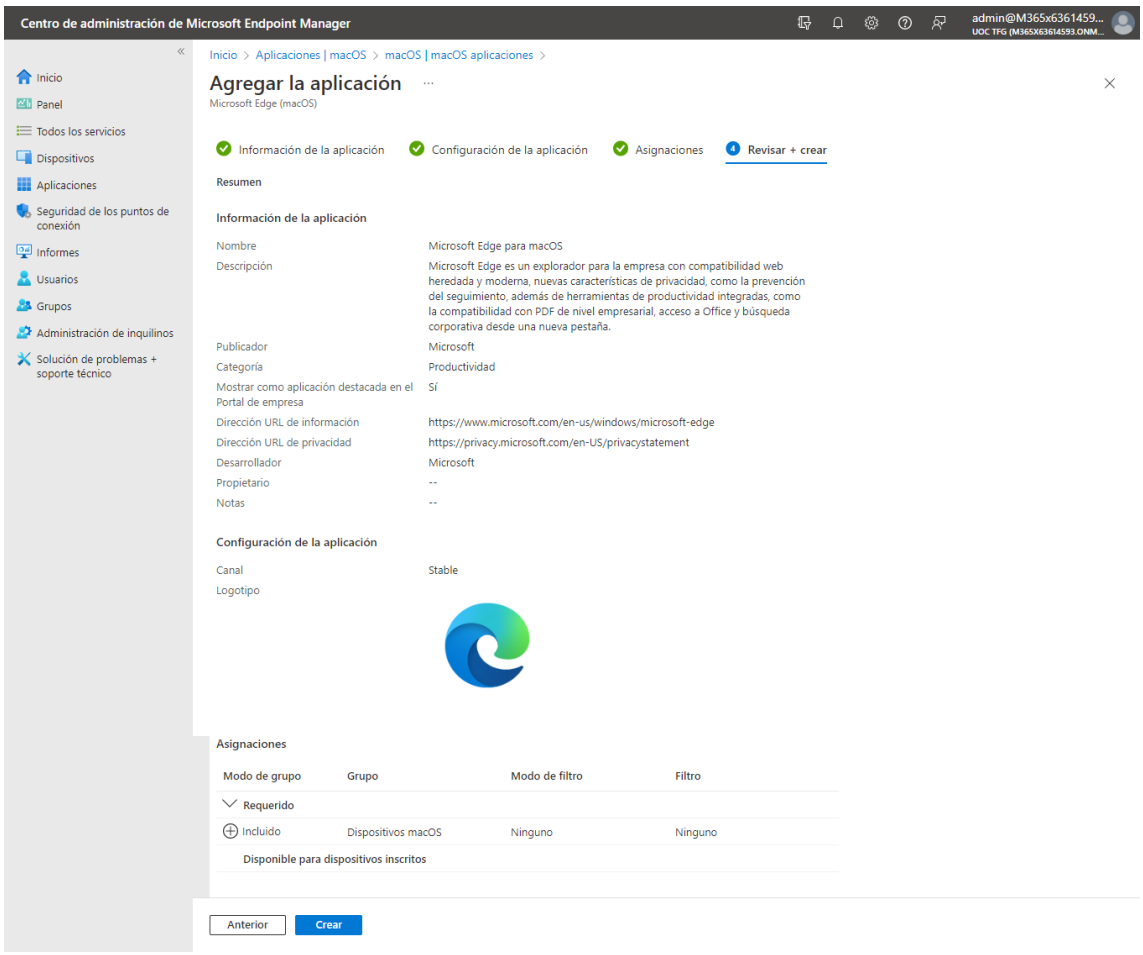


Figura 48 - Despliegue de aplicación en dispositivos macOS

- **Dispositivos iOS e iPadOS**

En cuanto a los dispositivos Apple con sistema operativo iOS e iPadOS, se ha optado por distribuir la aplicación Adobe Acrobat Reader, presente en la Apple Store para dispositivos iOS e iPadOS. La aplicación se ha asignado como disponible para los dispositivos inscritos que se encuentren dentro del grupo "Dispositivos iOS-iPadOS".

Todas las configuraciones de la aplicación se han dejado por defecto (nombre, descripción, publicador, etc.), a excepción de la versión mínima requerida de iOS para que se permita la instalación, que se ha establecido en la 14.0. Además, se ha marcado que aparezca como aplicación destacada en el portal de empresa de dichos dispositivos.

El resumen con los detalles del despliegue de la aplicación se puede consultar en la siguiente imagen.

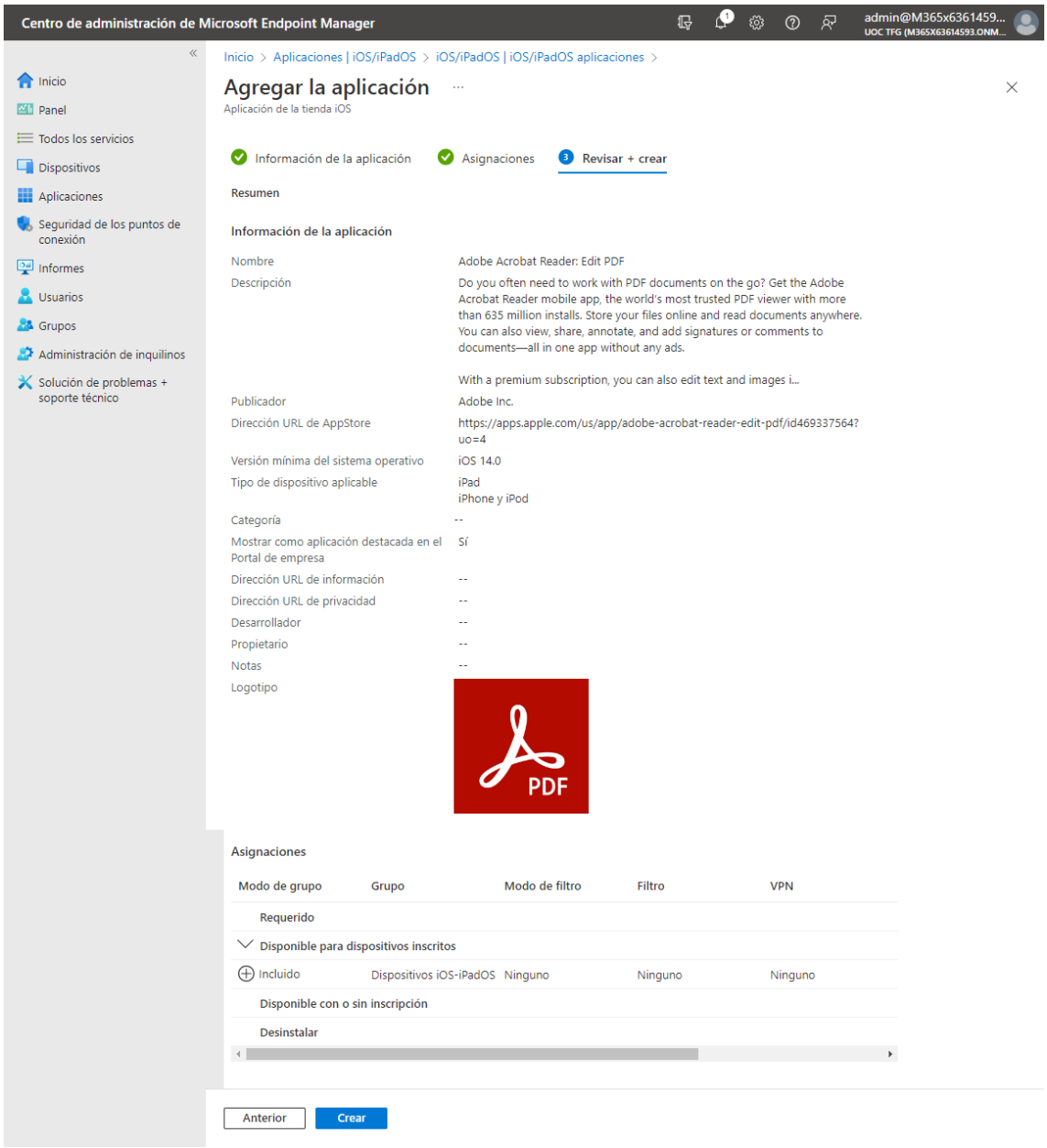


Figura 49 - Despliegue de aplicación en dispositivos iOS/iPadOS

3.3.10 Personalización de la experiencia de usuario

Microsoft Intune permite personalizar la experiencia de usuario mediante la personalización del portal de empresa. Para adecuar la interfaz a la organización de la prueba de concepto, en este caso la UOC, se ha creado una directiva de personalización específica que se aplicará a todos los dispositivos y usuarios del entorno.

La directiva incluye el nombre de la organización, el logo, la URL del sitio web, la persona de contacto y la declaración de privacidad. Los detalles completos de la creación de la directiva se pueden consultar en el anexo 10.

3.3.11 Alta de usuarios y asignación de licencia

Una vez configurada la solución MDM para que cumpla con los requisitos propuestos de la prueba de concepto, es el momento de dar de alta los usuarios y asignarles las licencias oportunas para que puedan inscribir sus dispositivos en Intune.

La creación de usuarios y asignación de licencias se puede realizar indistintamente desde el portal de administración de Azure AD o desde el portal de administración Intune. En este caso, se ha utilizado el segundo. Los usuarios creados en el entorno son los siguientes:

- Edgar Mera Couto: emeracouto@m365x63614593.onmicrosoft.com
- Elena Salgueiro: esalgueiro@m365x63614593.onmicrosoft.com
- Mario Prieto Vega: mprietovega@m365x63614593.onmicrosoft.com
- Montse Serra Vizern: mserravizern@m365x63614593.onmicrosoft.com
- David Bañeres Besora: dbaneresbesora@m365x63614593.onmicrosoft.com

A todos los usuarios se les ha asignado licencia de Intune, contemplada en EMS E5, de Office 365 E5 y de Windows 10/11 Enterprise E3. Aunque se ha optado por habilitar todos los servicios de cada producto, para poder inscribir dispositivos en el MDM sólo sería necesaria la licencia de Azure AD Premium y de Intune, como ya se ha indicado en el apartado 3.3.1. Además, se les ha permitido el inicio de sesión, se les ha añadido al grupo “Usuarios de Intune” y se les ha configurado la localización como España.

A continuación, se muestra el resumen de los detalles de las licencias de un usuario. El proceso completo de creación de todos los usuarios del entorno y la asignación de licencias correspondiente se puede consultar en el anexo 11, donde también se indica sus contraseñas.

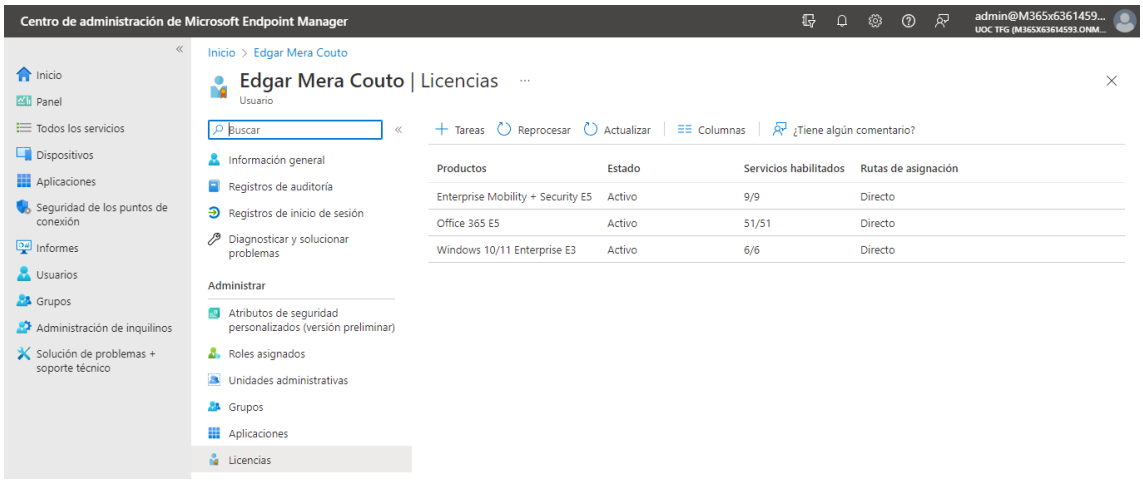


Figura 50 - Licencias de usuario para la prueba de concepto

4. Pruebas de gestión de dispositivos

4.1 Preparación de dispositivos

Para las pruebas de gestión de la solución MDM implantada, se han utilizado los siguientes dispositivos:

- Máquina virtual Windows 11 (AutoPilot)
- Máquina virtual Windows 10 (Corporativo)
- Máquina virtual Windows 10 (BYOD)
- Samsung Galaxy A71 con Android 13 (BYOD)
- Apple MacBook Pro Retina 2014 con macOS 11.6.5 (BYOD)
- iPhone 8 con iOS 15.3.1 (Corporativo)
- Máquina virtual Ubuntu (Corporativo)

Por falta de disponibilidad de más dispositivos, no ha sido posible evaluar la experiencia de usuario en dispositivos Android Corporativos. No obstante, el entorno está preparado para gestionarlos y simplemente habría que enrolarlos restablecidos con la configuración de fábrica para que evaluarán las directivas y aplicaran los perfiles creados.

Las máquinas virtuales de los dispositivos Windows ya existían en el entorno de laboratorio de la prueba de concepto, por lo que simplemente se ha restablecido el sistema operativo. El proceso detallado de la creación de la máquina virtual para el dispositivo Ubuntu puede consultarse en el anexo 12.

4.2 Inscripción en Microsoft Intune

El proceso de inscripción de los dispositivos es distinto en función de la plataforma y del escenario bajo el que se van a utilizar, si como dispositivo corporativo o como dispositivo BYOD.

A continuación, se exponen los diferentes procesos de inscripción llevados a cabo en los dispositivos. En el anexo 13 se puede consultar el detalle completo del proceso seguido en cada caso.

- **Dispositivos Windows**

Los dispositivos con sistema operativo Windows a partir de la versión 8.1 disponen de funcionalidades MDM integradas en el propio sistema operativo. Dichas funcionalidades MDM son proporcionadas mediante APIs debidamente documentadas que permiten controlar configuraciones y llevar a cabo tareas de administración. Las APIs son capaces de interactuar con protocolos de administración estándar, por lo que los servidores MDM pueden gestionar fácilmente configuraciones del dispositivo, realizar consultas, y otro tipo de factores que les permiten construir y asignar políticas[33].

Gracias a lo indicado, los dispositivos Windows actuales no requieren de la instalación de ningún software adicional en forma de cliente para poder ser inscritos y gestionados por Microsoft Intune. Es otro de los aspectos en el que la integración entre dispositivos y MDM de Microsoft es muy alta, siendo mayor que con otras plataformas.

El proceso de inscripción en Intune de los dispositivos Windows es distinto en los tres escenarios que se evalúan en la prueba de concepto. Por ello, se muestran de forma separada. El usuario elegido para todos los dispositivos Windows (tres escenarios de la prueba) es Edgar Mera Couto: emeracouto@m365x63614593.onmicrosoft.com

- Dispositivos Windows AutoPilot

Tal y como se ha comentado anteriormente en el apartado 3.3.4, AutoPilot es una tecnología de inscripción de dispositivos Windows (en las versiones 10 y 11) en Intune que se realiza de forma automática durante el proceso OOBE, que tiene lugar en el primer arranque del sistema operativo. Para que esto ocurra, los dispositivos tienen que estar previamente dados de alta en Intune como dispositivos Windows AutoPilot mediante su identificador único de hardware, tarea que puede realizar el proveedor del dispositivo en nombre de la organización o un administrador de Intune de la compañía.

Para la prueba de concepto, dado que el dispositivo de prueba es una máquina virtual, se ha obtenido el identificador de hardware mediante un script PowerShell y se ha importado manualmente en Intune.

El script PowerShell para obtener el identificador único de hardware del dispositivo es el siguiente:

```
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
```

Tras ejecutarlo, se genera un archivo con extensión .csv que se puede importar en Intune para aprovisionar el dispositivo[34].

Una vez el dispositivo ya consta como Dispositivo Windows AutoPilot en el MDM y se le ha asignado un perfil de implementación de Windows AutoPilot añadiéndolo al grupo “Dispositivos Windows AutoPilot”, está listo para la inscripción automática.

Cuando arranca el sistema operativo por primera vez, durante el proceso denominado OOBE, este solicita una conexión a Internet de cualquier tipo. Tras

disponer de conexión a Internet, contacta con los servidores de Microsoft y comprueba que está asignado a una organización (UOC TFG, en este caso). A continuación, solicita las credenciales del usuario de la compañía y, una vez Edgar se valida, el dispositivo se inscribe de forma automática en Intune en el tenant de UOC TFG y aplica la experiencia de usuario personalizada según el perfil de implementación asignado. Como se ha preconfigurado todo en el perfil de implementación de AutoPilot asignado al dispositivo, Edgar no debe realizar ninguna acción adicional. El dispositivo se configura automáticamente y el usuario puede empezar a trabajar con él.

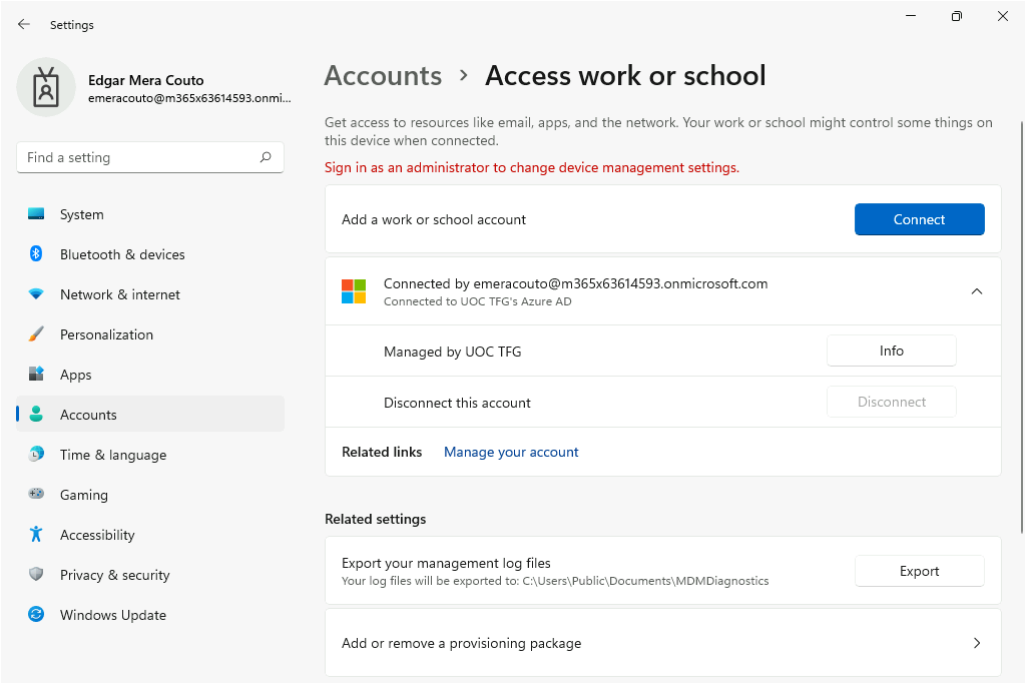


Figura 51 - Dispositivo Windows 11 inscrito en Intune vía AutoPilot

- Dispositivos Windows Corporativos

Los dispositivos Windows Corporativos pueden inscribirse en Microsoft Intune por dos vías diferentes: introduciendo la cuenta de la organización en el proceso OOBE del sistema operativo o haciéndolo mediante la opción “Unir este dispositivo a Azure Active Directory” del menú “Obtener acceso al trabajo o la escuela”, en el apartado Cuentas de la configuración del sistema. El resultado final es el mismo independientemente de la vía elegida.

Las principales diferencias entre este método de inscripción y AutoPilot son dos. La primera es que en los dispositivos inscritos en AutoPilot no es posible configurar el sistema operativo con una cuenta local. El dispositivo sabe que está inscrito mediante AutoPilot en una organización y sólo permite configurarse con una cuenta de dicha organización. Esto impide que ese dispositivo sea utilizado por alguien ajeno a la organización.

La segunda diferencia con AutoPilot es que el usuario debe elegir la configuración del equipo mediante el proceso OOBE (a diferencia de en AutoPilot, donde está preconfigurada en el perfil de inscripción asignado). Esto permite la configuración de cualquier tipo de cuenta en el dispositivo, incluyendo una cuenta personal, para más adelante inscribir el dispositivo a través de la opción “Unir este dispositivo a Azure Active Directory” en el menú “Obtener acceso al trabajo o la escuela” anteriormente mencionado.

La siguiente imagen muestra el estado del dispositivo inscrito.

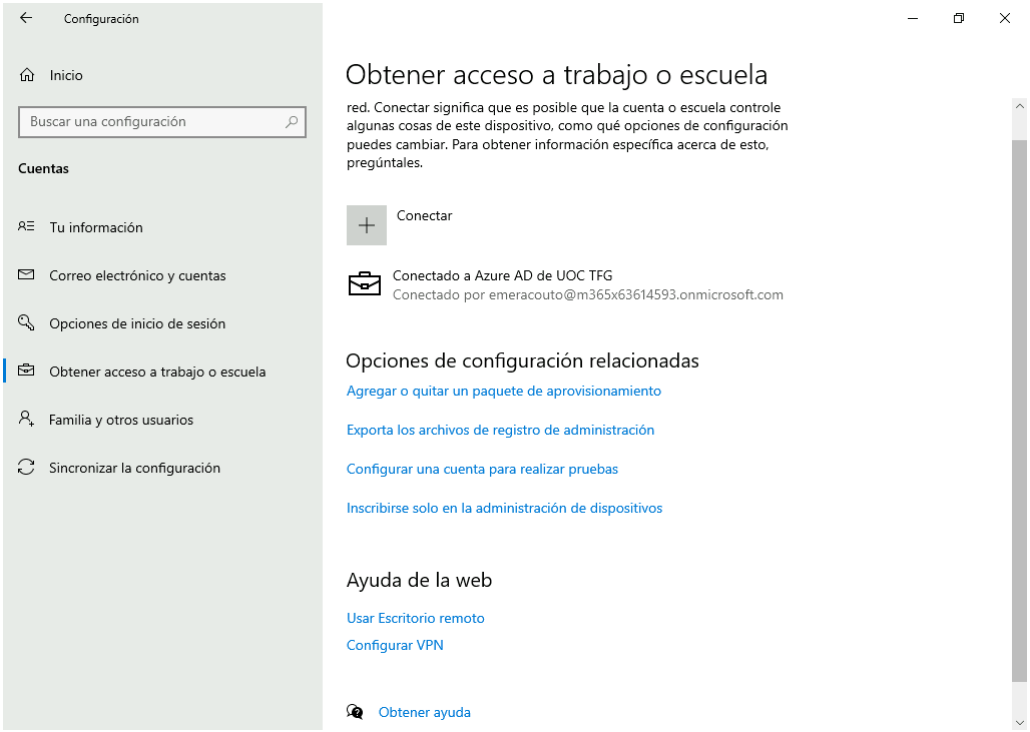


Figura 52 - Dispositivo Windows 10 inscrito en Intune vía Configuración

Tanto en este escenario como en el de AutoPilot, los dispositivos se inscriben automáticamente en Intune al unirse a Azure Active Directory gracias a la configuración de inscripción automática realizada en el apartado 3.3.2.

- Dispositivos Windows BYOD

En este escenario, el dispositivo Windows se inscribe en Intune pero, a diferencia de en los dos escenarios anteriores, no se une al dominio de Azure AD, tan solo se registra. Esto implica que el MDM es capaz de evaluar el estado del dispositivo mediante las directivas de cumplimiento, pero Intune no realiza ninguna administración de este a través del MDM.

En los dispositivos Windows BYOD, Intune realiza una gestión MAM. Esto significa que lo que se gestiona es la cuenta de la organización en dicho

dispositivo, así como las aplicaciones corporativas. El dispositivo es administrado por el propio usuario, y los datos corporativos que alberga por la organización. Aunque el dispositivo no se gestiona, es necesario que el usuario disponga de licencia de Intune asignada,

El registo en Azure AD se realiza de manera similar a los dispositivos corporativos, mediante el menú “Obtener acceso al trabajo o la escuela”. Una vez introducidas las credenciales de la organización, el dispositivo se registra y es evaluado para otorgar o no acceso a los datos y aplicaciones de la organización.

En la siguiente imagen se muestra el estado tras el registro en Azure AD.

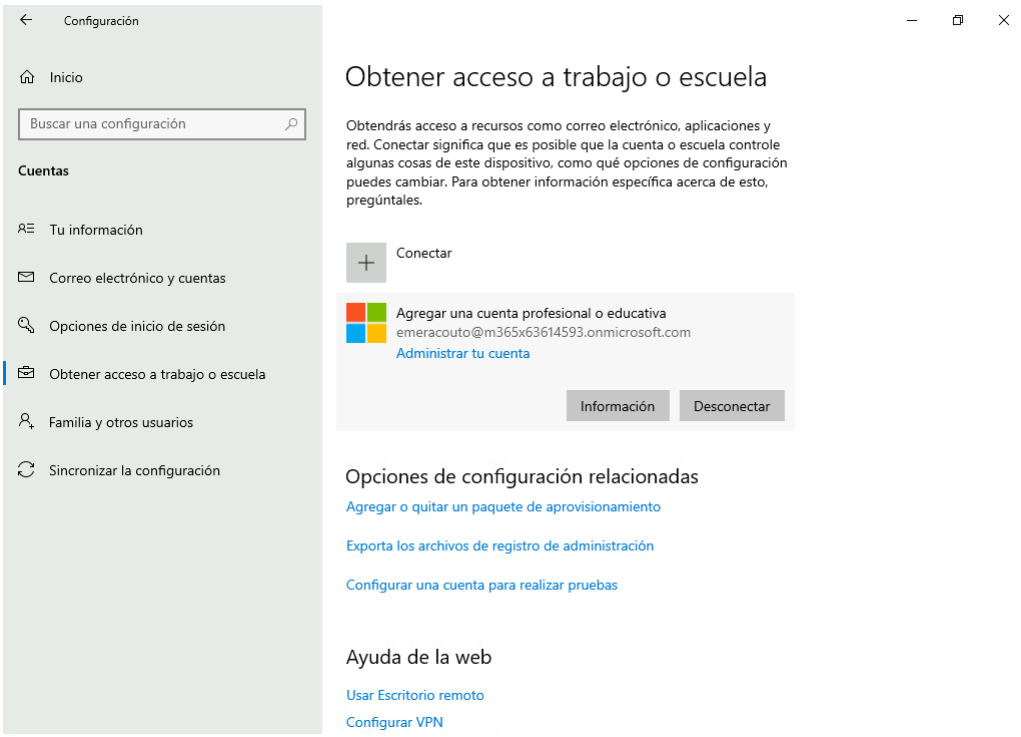


Figura 53 - Dispositivo Windows 10 BYOD registrado en Azure AD

- **Dispositivos Android**

La inscripción de dispositivos Android se puede llevar a cabo de diferentes maneras, en función del escenario que se quiera implementar de los indicados en el apartado 3.3.2. Por normal general, la inscripción de los dispositivos Android Enterprise se puede realizar mediante una etiqueta NFC, un código QR, Zero Touch (requiere estar afiliado a un proveedor que forme parte del servicio de inscripción sin contacto de Android), Knox Mobile Enrollment (para dispositivos Samsung y mediante suscripción adicional a Knox) o el portal de

empresa de Intune. Los dispositivos Android de código abierto únicamente pueden inscribirse con código QR.

Todos los métodos mencionados, excepto el de la instalación del portal de empresa de Intune, aplican solo para dispositivos nuevos o en los que se ha restablecido el sistema operativo, pues es durante la configuración inicial cuando tienen lugar.

Para la prueba de concepto, solamente se ha podido evaluar el método de inscripción mediante la instalación del portal de empresa de Intune en un dispositivo Android BYOD, por falta de dispositivos adicionales. El usuario elegido en este caso es David Bañeres Besora:
dbaneresbesora@m365x63614593.onmicrosoft.com

El proceso de inscripción es sencillo. Se debe descargar la aplicación Portal empresa Intune en Google Play Store e iniciar sesión con las credenciales corporativas. En este caso, el dispositivo solo se registra en Azure AD.

A continuación, se muestra una imagen con el estado del dispositivo inscrito:

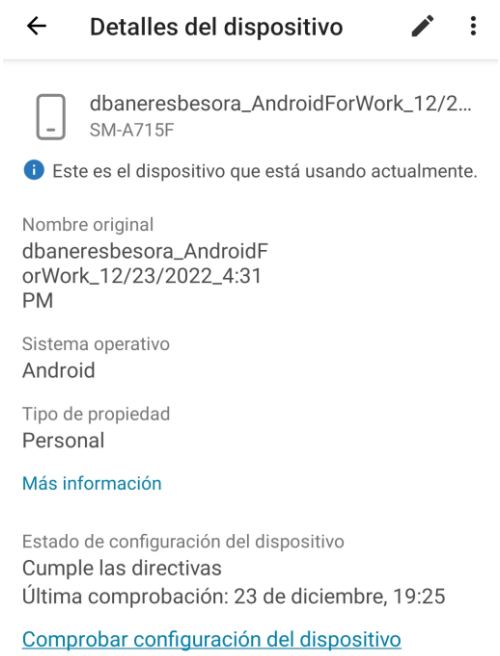


Figura 54 - Dispositivo Android BYOD inscrito en Intune

- **Dispositivos macOS**

El dispositivo Apple con sistema operativo macOS de usuario final disponible para la prueba de concepto solo se puede inscribir en Microsoft Intune mediante la instalación de la aplicación Portal de Empresa. Debido a la necesidad de tener que configurar el sistema operativo primero, cuando el

dispositivo es nuevo (o se ha restablecido), para después instalar manualmente el portal de empresa, este tipo de inscripción se suele emplear para dispositivos BYOD. Sin embargo, si se aplican las mismas directivas de cumplimiento y perfiles que a los dispositivos macOS corporativos, como se ha realizado en el entorno de laboratorio de la prueba de concepto, el comportamiento de ambos es exactamente el mismo.

Existen otras dos formas de inscripción de dispositivos macOS en Intune de forma automática y transparente, sin necesidad de instalar a mano el portal de empresa, pero no han podido evaluarse al no disponer de cuenta de ABM ni ASM, ni disponer de dispositivos adicionales para usar como pantalla completa (modo quiosco).

El usuario elegido para el dispositivo Apple MacBook Pro Retina es Elena Salgueiro: esalgueiro@m365x63614593.onmicrosoft.com. Antes de descargar la aplicación portal de empresa e inscribir su dispositivo, Elena intenta acceder al correo y recibe el siguiente mensaje de error (igual que ocurre en cualquier otro dispositivo no inscrito en Intune ni registrado en Azure AD).

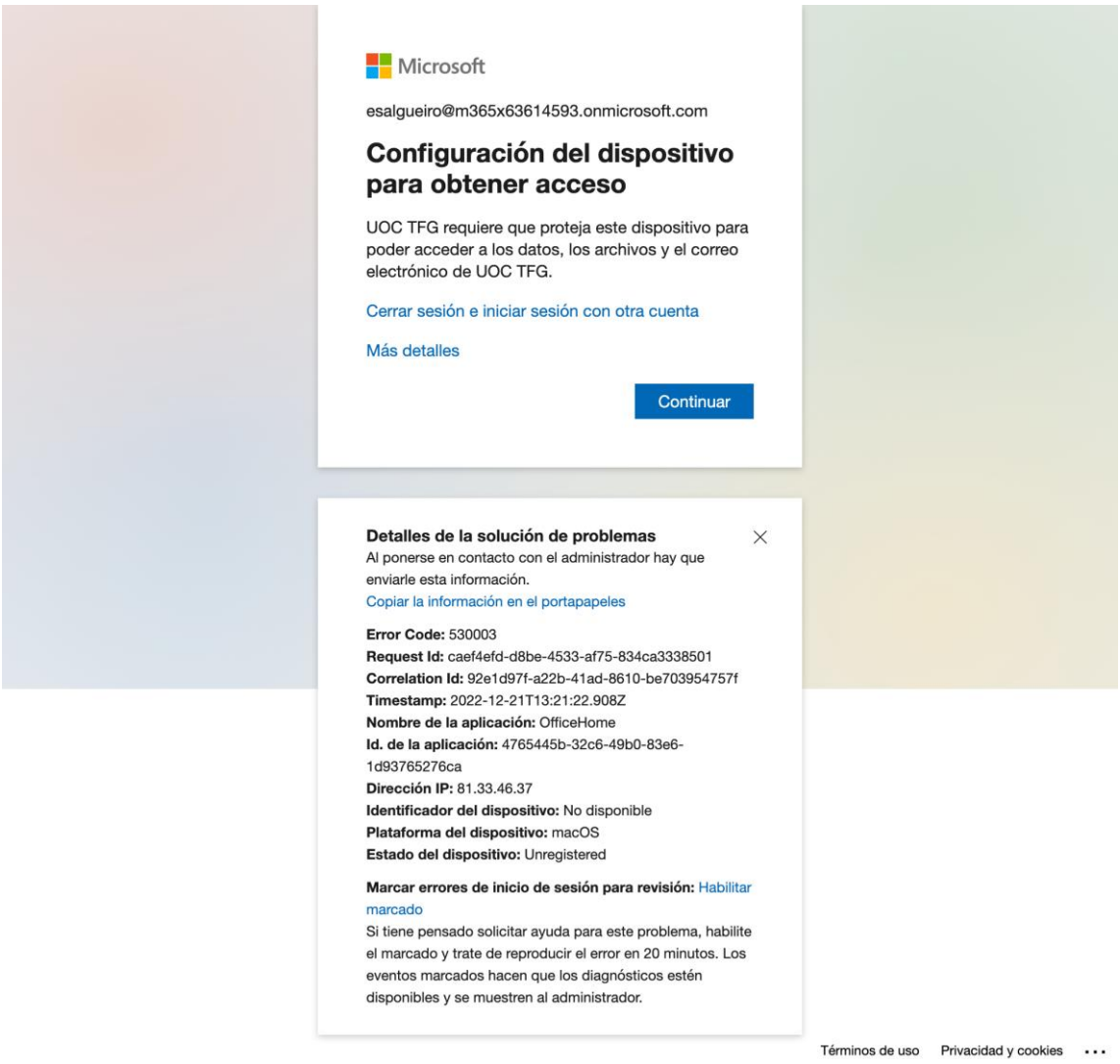


Figura 55 - Error de acceso condicional por incumplimiento de directivas

El mensaje de error indica que Elena no puede acceder al correo electrónico porque su equipo no está registrado en Intune y, por tanto, no se puede evaluar la directiva de cumplimiento pertinente. Así, Elena debe descargar la aplicación Portal de empresa para dispositivos macOS, instalarla y validarse con las credenciales corporativas. La aplicación está disponible en: https://go.microsoft.com/fwlink/?linkid=853070

Una vez descargada e instalada la aplicación, Elena se valida con sus credenciales y acepta la inscripción de su MacBook Pro en Intune, lo que permite a la solución MDM evaluar la directiva de cumplimiento y aplicar el perfil de configuración correspondiente. Además, las aplicaciones requeridas previamente configuradas se instalan (Microsoft Edge). Ahora, Elena ya puede acceder a los servicios de Office 365 como el correo desde su dispositivo. En este caso, el dispositivo solo se registra en Azure AD (no se une).

La siguiente imagen muestra el estado del dispositivo de Elena en la aplicación Portal de Empresa de Intune.

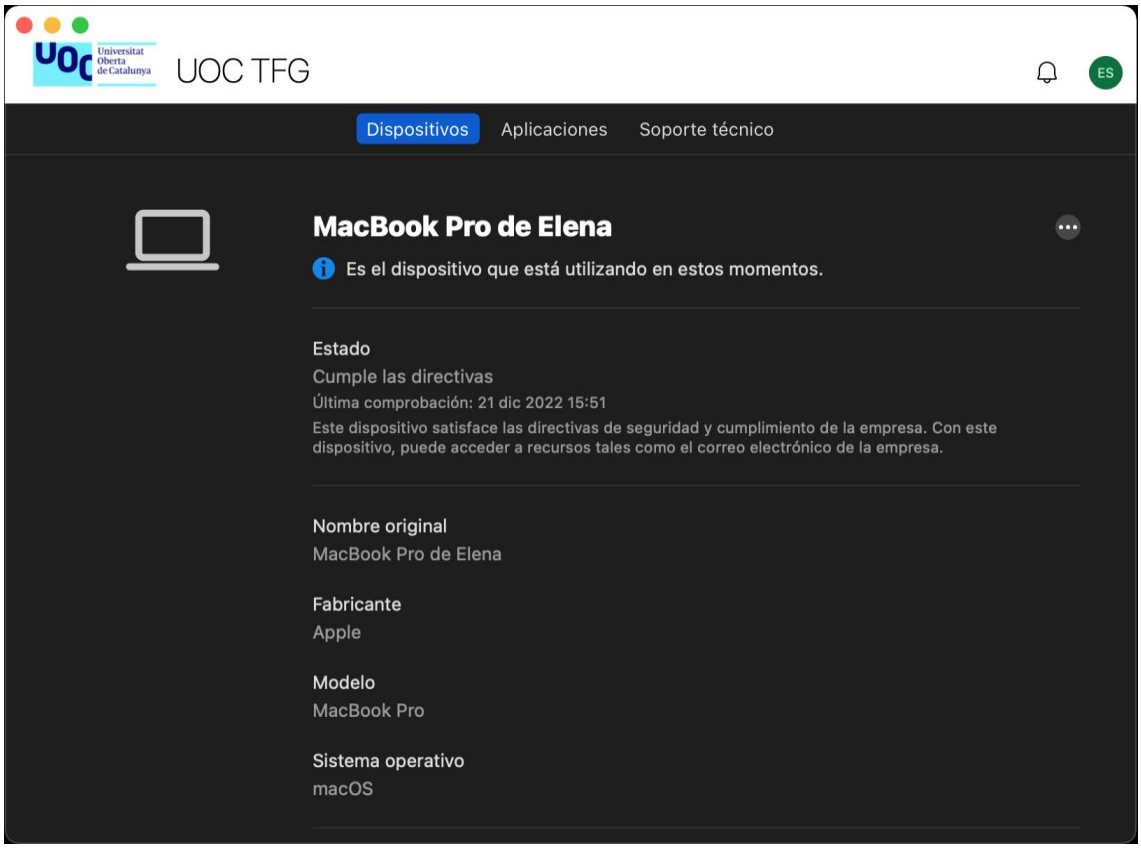


Figura 56 - Dispositivo macOS inscrito en Intune

- **Dispositivos iOS e iPadOS**

La inscripción en Intune de los dispositivos Apple con sistema operativo iOS e iPadOS se realiza de forma similar a la de los macOS, con la salvedad de que

en la Apple App Store de los dispositivos móviles si está presente la aplicación Portal de Empresa.

Para la prueba de este tipo de dispositivos, el usuario elegido es Mario Prieto Vega: mprietovega@m365x63614593.onmicrosoft.com

Tras descargar y validarse en el portal de empresa con las credenciales corporativas (y ser añadido al grupo correspondiente para que se le asigne una directiva de cumplimiento), el dispositivo evalúa la directiva de cumplimiento y es marcado como no conforme al no cumplir alguno de los requisitos de la directiva hasta que se remedie. En este caso, el dispositivo solo se registra en Azure AD.

La imagen siguiente muestra el estado del dispositivo de Mario en la aplicación Portal de Empresa de Intune.

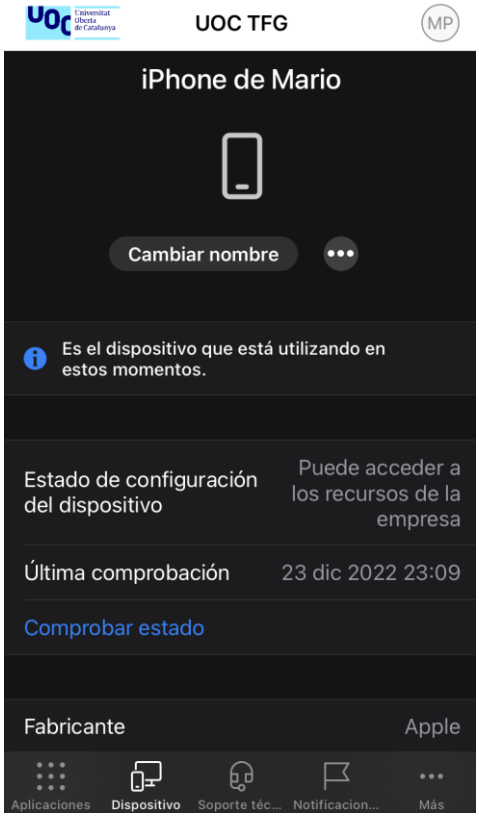


Figura 57 - Dispositivo iOS inscrito en Intune

- **Dispositivos Linux**

Los dispositivos Linux también deben inscribirse en Intune a través de una aplicación, en este caso llamada Microsoft Intune. Como se ha ido comentando a lo largo de todo el documento, la gestión de esta plataforma todavía es muy reducida, limitándose a la evaluación de las directivas de cumplimiento para

otorgar acceso a los recursos empresariales o no (en caso de estar configurado el acceso condicional, como en la prueba de concepto).

El usuario elegido para la prueba de inscripción del dispositivo Linux con sistema operativo Ubuntu 22.04 LTS es Montse Serra Vizern: mserravizern@m365x63614593.onmicrosoft.com

La aplicación Microsoft Intune está disponible para su descarga en la dirección https://packages.microsoft.com/. Una vez descargada e instalada, Montse se valida con sus credenciales y la inscripción en Intune se realiza, tal y como muestra el estado de cumplimiento del dispositivo en la imagen siguiente. De nuevo, el dispositivo solo se registra en Azure AD.

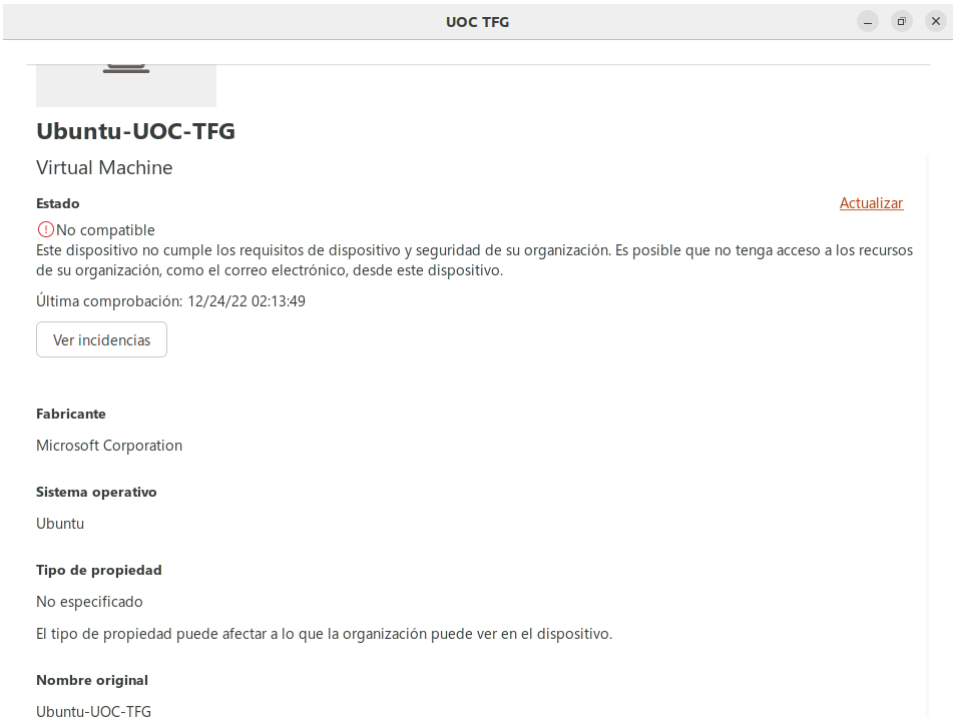


Figura 58 - Dispositivo Linux inscrito en Intune

4.3 Comprobación de estado y monitorización

La comprobación de estado de los equipos inscritos en Microsoft Intune se puede realizar tanto desde el propio dispositivo inscrito como desde el portal de administración de la solución. Cómo es lógico, el portal de administración muestra mucho más detalle de todos los componentes evaluados y del estado de cada configuración o aplicación que el dispositivo en sí mismo.

En los dispositivos de usuario inscritos en Microsoft Intune, el estado de la inscripción se consulta a través de la aplicación Portal de Empresa (o Microsoft Intune, para Linux). Para los dispositivos Windows, la aplicación está disponible

en la Microsoft Store. La interfaz es muy similar independientemente de la plataforma (como se aprecia en las imágenes del apartado anterior). En ella se puede consultar si el dispositivo es conforme o no con las directivas de cumplimiento que tiene asignadas y, por tanto, puede acceder a los recursos corporativos, las aplicaciones que tiene asignadas, los dispositivos inscritos en Intune del usuario y la información de soporte técnico de la organización. Además, en dispositivos BYOD ofrece la posibilidad de quitar el dispositivo, eliminando así la inscripción en Intune.

En cuanto al portal de administración, dispone de una gran cantidad de paneles predefinidos para cada área de gestión que facilitan la visualización de la situación actual del entorno con un simple vistazo. Además, son interactivos y permiten navegar a través de la información para profundizar en los detalles que se desee, como por ejemplo qué configuración en concreto no cumple un dispositivo marcado como no conforme o el estado de instalación de una aplicación asignada.

La siguiente imagen muestra varios paneles predefinidos.

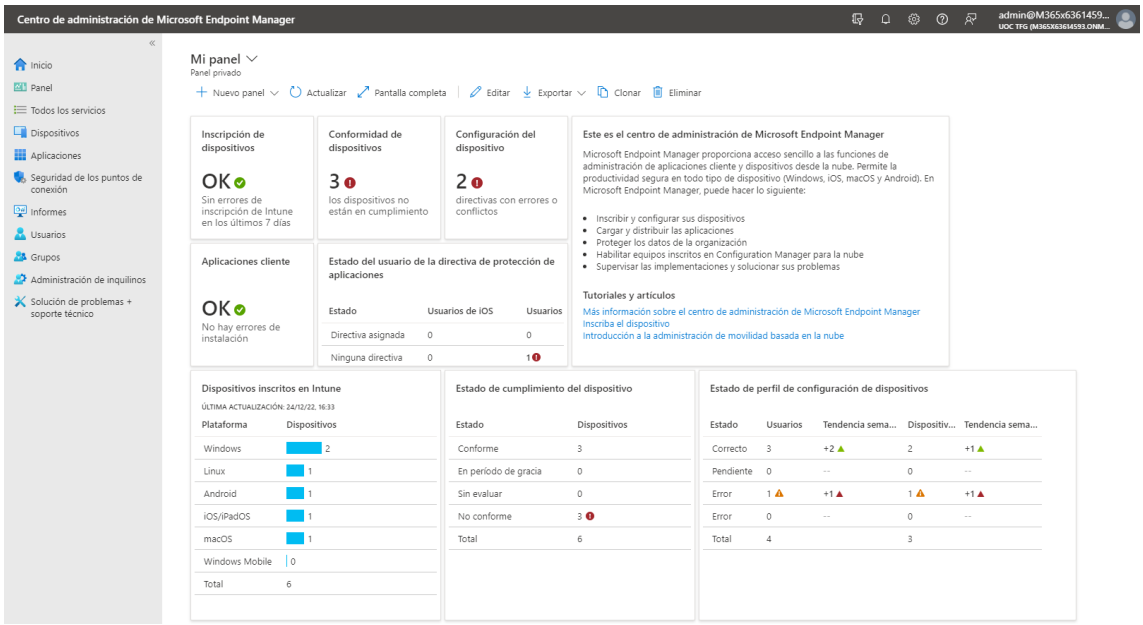


Figura 59 - Paneles de estado predefinidos de Intune

Según se aprecia en la imagen anterior, el panel es totalmente configurable.

Por otra parte, Intune ofrece una serie de informes predefinidos sobre el estado de conformidad de dispositivos, las configuraciones aplicadas, actualizaciones de Windows, registro de auditoría e incluso directivas de grupo (para equipos unidos a un dominio on-premises). Además, permite exportar los datos para construir informes desde otras herramientas e incluso dispone de un almacén de datos con datos históricos de Intune y datos actualizados en una cadencia diaria en un modelo de datos estándar OData.

4.4 Acciones desde el portal de administración

El portal de administración de Intune permite realizar diversas acciones sobre los dispositivos inscritos en el MDM. Estas acciones varían en función de la plataforma del dispositivo y de la propiedad (si son corporativos o personales). Para los dispositivos Linux, por el momento, únicamente es posible retirarlos de la inscripción para impedir que accedan a los recursos corporativos.

De entre las acciones comunes a todas las plataformas (excepto Linux) se puede destacar la de reiniciar o apagar el dispositivo, borrarlo (restableciéndolo de fábrica o eliminado solo la información personal), bloquearlo o enviar una notificación personalizada (para dispositivos móviles Android e iOS/iPadOS). En cada dispositivo, además, se puede consultar su información de hardware, aplicaciones instaladas, estado de conformidad y configuración de dispositivo/aplicaciones, la pertenencia a grupos y las aplicaciones administradas por la organización.

La siguiente imagen muestra los dispositivos inscritos en Intune para la prueba de concepto e información adicional sobre ellos, como de quién son propiedad, su estado de cumplimiento, sistema operativo y versión, entre otros.

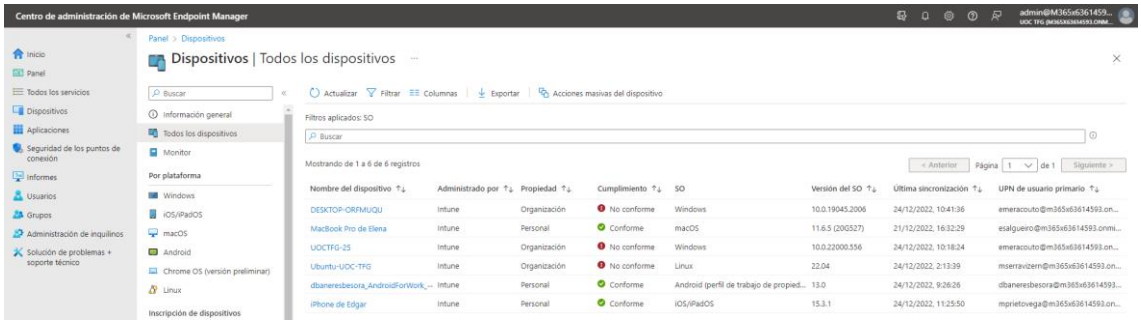


Figura 60 - Dispositivos inscritos en Intune

Si se hace click en el nombre del dispositivo, se accede a los detalles del mismo, con las acciones anteriormente mencionadas disponibles.

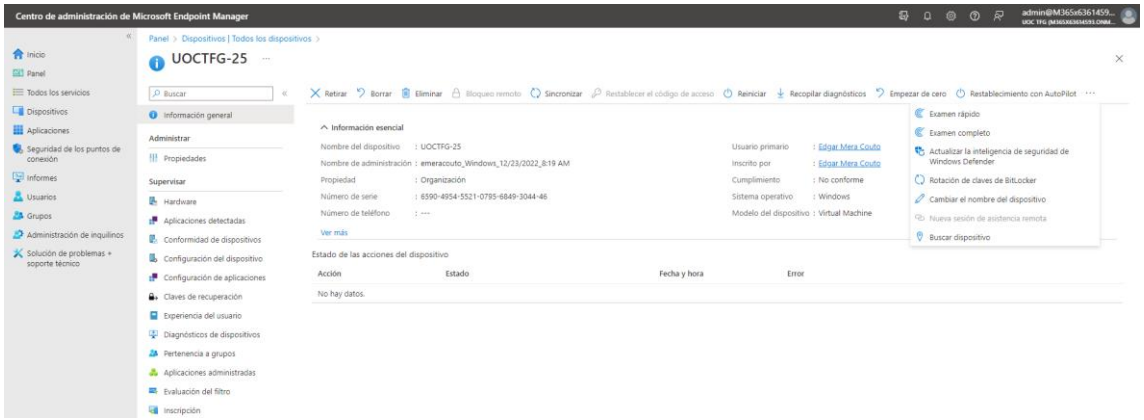


Figura 61 - Acciones de dispositivo disponibles en Intune

En cuanto a las opciones de asistencia remota a los dispositivos desde Intune, existen dos posibilidades, ambas bajo suscripción adicional: TeamViewer o Ayuda Remota de Intune.

TeamViewer es una aplicación de terceros que se puede integrar con Microsoft Intune. Para ello, es necesario disponer de la licencia correspondiente de TeamViewer y configurar el conector en Intune. Una vez realizado, la acción "Nueva sesión de asistencia remota" se habilita en los dispositivos soportados y se puede establecer la conexión con ellos, pudiendo tomar el control del dispositivo. Los dispositivos soportados son: Administrador de dispositivos Android (DA), Android Enterprise de propiedad personal con perfil de trabajo (BYOD), iOS/iPadOS, macOS y Windows. TeamViewer funciona con la aplicación Portal de empresa, vista en el apartado 4.2, no con la aplicación Microsoft Intune, por lo que no se admiten dispositivos Android Enterprise de propiedad corporativa[35].

Por otro lado, la Ayuda Remota de Intune es una funcionalidad incorporada recientemente a Intune (a mediados de diciembre de 2022) que permite la conexión remota a los dispositivos mediante una aplicación complementaria premium. De igual forma que con TeamViewer, es necesaria la adquisición de licencia, en este caso del complemento premium Ayuda Remota. Sin embargo, el número de plataformas soportadas por esta funcionalidad es menor, reduciéndose a dispositivos con sistema operativa Windows 10 y 11[36].

5. Proceso de migración para transición al cloud

Tal y como se ha expuesto a lo largo del apartado 2, el escenario actual de nuevos tipos de dispositivos y la creciente movilidad conduce a las empresas a adoptar soluciones cloud de gestión de puesto de trabajo que cubran las nuevas necesidades. Sin embargo, es habitual que las organizaciones ya dispongan de alguna solución tradicional, on-premises, con la que gestionan su parque de dispositivos. Esto puede causar rechazo a la hora de adoptar una herramienta cloud como Microsoft Intune, al tener que mantener y administrar ambas soluciones, con el aumento de costes que ello implica.

Para evitar que la adopción de la solución cloud suponga un problema adicional para las compañías, Microsoft Intune ofrece integración con herramientas on-premises de gestión de puesto de trabajo, en mayor o menor medida en función de cada herramienta. Cómo es lógico, la mejor integración posible se da con su solución homóloga on-premises, Microsoft Endpoint Configuration Manager (anteriormente conocida como SCCM), ampliamente utilizada.

La integración de Microsoft Intune con MECM permite realizar una transición al modelo de gestión cloud por fases, ofreciendo una administración compartida con la solución on-premises, donde cada herramienta gestiona diferentes áreas. Así, se puede ir traspasando la gestión de la herramienta tradicional a la moderna de manera escalonada y controlada, para finalmente gestionar todas las áreas desde Intune, si así se desea, y dar de baja toda la infraestructura de MECM. Además, la administración se lleva a cabo desde una consola de administración unificada.

Antes de decantarse por migrar la gestión a Microsoft Intune o cualquier otra solución cloud, es necesario analizar en detalle sus capacidades y funcionalidades con respecto a la solución tradicional existente, como por ejemplo MECM. Una de las principales diferencias entre ambas es que Intune no es capaz de realizar despliegue de sistemas operativos, mientras que MECM no puede aplicar políticas de acceso condicional. En cuanto a la gestión de dispositivos móviles (Android, iOS/iPadOS), MECM no permite aplicar perfiles configuración. Así, se deben valorar las funcionalidades necesarias para la organización y puede darse el caso en que ambas soluciones tengan que coexistir, al menos de manera temporal.

5.1 Integración de Intune con MECM

El resultado de la integración de Microsoft Intune con Microsoft Endpoint Configuration Manager es la solución conocida como Microsoft Endpoint Manager (MEM). La arquitectura de la solución es la mostrada en la figura 10 del apartado 2.7, donde se aprecia como ambas herramientas trabajan de manera conjunta en una administración compartida.

Para integrar las dos herramientas se ha utilizado un entorno de laboratorio existente con un dominio on-premises y MECM instalado, y el tenant de Azure AD con Intune configurado en el apartado 3 para la prueba de concepto de este proyecto. El proceso detallado se puede consultar en el anexo 14.

A grandes rasgos, el proceso de integración consiste, en primer lugar, en dar de alta los dispositivos on-premises en Azure AD para que Intune sea capaz de gestionarlos, pues Intune requiere que la identidad de los dispositivos exista en el directorio de la nube. Esto se conoce como unión híbrida a Azure AD y puede hacerse con una herramienta llamada Azure AD Connect.

El siguiente paso es inscribir los dispositivos en Intune. Debido a la configuración de inscripción automática realizada en el apartado 3.3.2, todos los dispositivos que se unen a Azure AD, bien de forma nativa o mediante una unión híbrida, serán inscritos en Intune, por lo que no es necesario realizar ninguna acción adicional.

Por último, se debe vincular el tenant de Azure AD en MECM con las credenciales de un administrador global de Azure. Así, la integración de ambas herramientas está finalizada y ya pueden trabajar de manera conjunta[37].

La siguiente imagen muestra los dispositivos on-premises unidos de forma híbrida a Azure AD (SEA-CL1 y SEA-CL2), donde aparece SCCM como MDM.

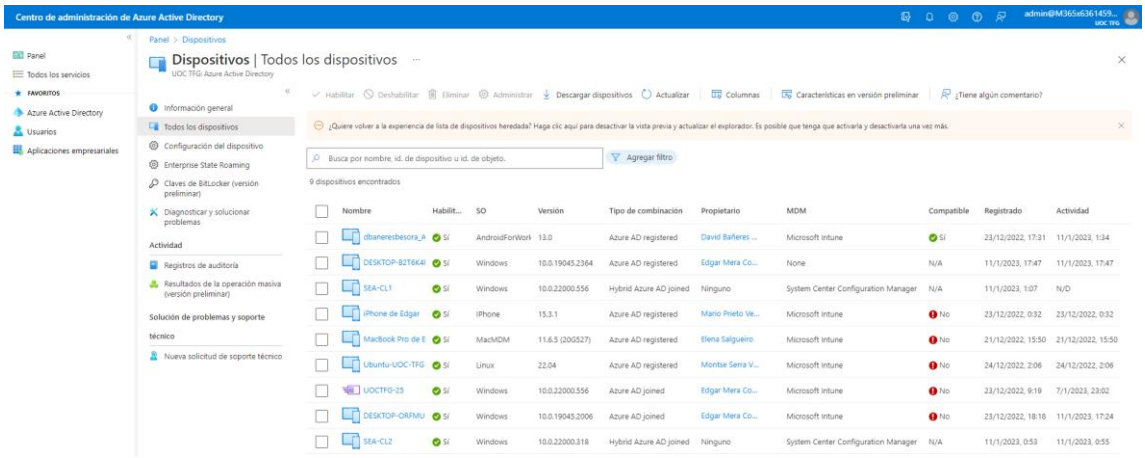


Figura 62 - Dispositivos unidos de forma híbrida a Azure AD

Una vez realizada la integración, se puede empezar a probar la gestión de los dispositivos, administrados hasta el momento únicamente por MECM, desde Intune. Para ello, lo recomendable es seleccionar un grupo pequeño de dispositivos y mover alguna de las cargas de trabajo disponibles (políticas de cumplimiento, configuración de dispositivo, aplicaciones cliente, aplicaciones de Office Click-to-Run o políticas de Windows Update) al pilotaje de Intune. Esto permite evaluar la capacidad de gestión de Intune de dicha área antes de traspasar la gestión por completo a la solución cloud. No obstante, esta

funcionalidad solo está disponible para dispositivos con sistema operativo Windows 10 o posterior, por lo que la gestión del resto de dispositivos gestionados por MECM (como los macOS) hasta la fecha deberá ser traspasada por completo a Intune.

Para pilotar las cargas de trabajo con Intune o traspasarlas por completo, se debe editar la política de MECM llamada “CoMgmtSettingsProd”, disponible tras realizar la integración en “Administration/Cloud Services/Cloud Attach”. En la pestaña Workloads, se puede seleccionar qué áreas traspasar al pilotaje (para lo cual se debe indicar la colección de pilotaje en la pestaña Staging) o a la gestión completa, tal y como refleja la siguiente imagen a modo de ejemplo.

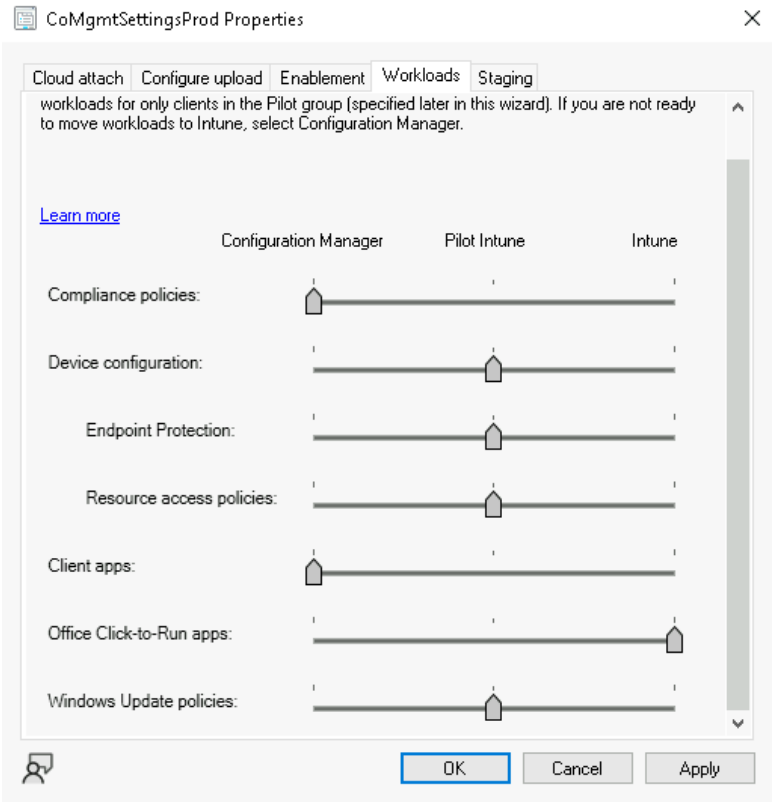


Figura 63 - Traspaso de cargas de trabajo de MECM a Intune

La administración de las cargas de trabajo traspasadas a Intune en los dispositivos administrados de forma conjunta por MECM e Intune se puede realizar desde el portal de administración de Intune. La solución cloud solo podrá gestionar aquellas áreas que se hayan traspasado, por lo que es importante traspasarlas todas si solo se quiere utilizar una única consola de administración. En caso contrario, será necesario realizar las acciones correspondientes a cada carga de trabajo en la consola de administración de la solución que la administra, lo que es poco práctico y ágil en términos de gestión.

A continuación, se muestra una imagen de los dispositivos inscritos en Intune, donde se aprecia como la pestaña cumplimiento de SEA-CL1 y SEA-CL2 indica que se debe comprobar la información en ConfigMgr (MECM). Esto es debido a que dicha carga de trabajo se ha mantenido en la solución on-premises, en vez de haberla traspasado a Intune.

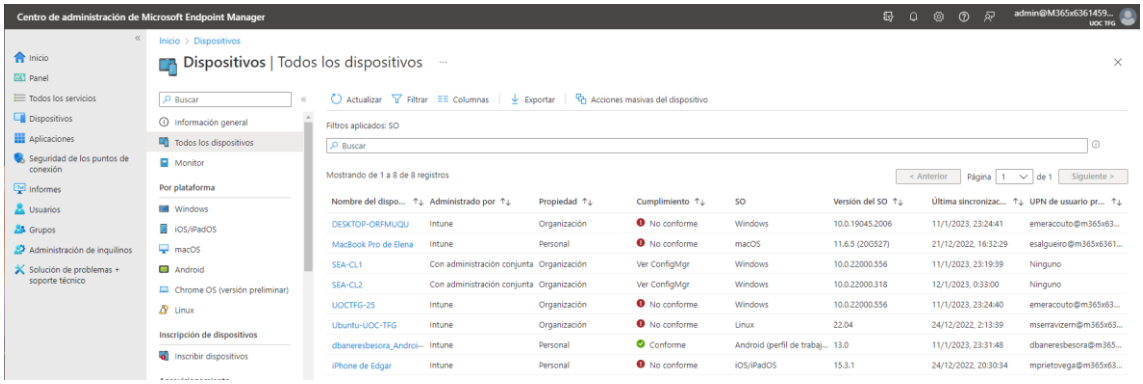


Figura 64 - Dispositivos con administración conjunta Intune-MECM

En caso de querer realizar cualquier acción sobre los dispositivos con administración conjunta, el funcionamiento es el mismo que con los administrados por Intune: se accede pulsando el nombre del dispositivo a los detalles del mismo, con toda la información recopilada y las acciones disponibles (en función de las áreas administradas por Intune).

6. Conclusiones

La gestión del puesto de trabajo se ha convertido en un deber para las organizaciones que quieren ofrecer dispositivos de productividad a sus empleados sin comprometer, bajo ningún concepto, la seguridad empresarial. La rápida evolución de la tecnología, sumado a la gran adopción del uso de Internet y a la implantación de estrategias de transformación digital, ha propiciado escenarios de movilidad y dispositivos que invitan a ello.

Las compañías llevan años invirtiendo esfuerzos en la gestión de su puesto trabajo, habitualmente apoyados por diferentes herramientas de mercado tradicionales desarrolladas específicamente para ello. Sin embargo, los nuevos tipos de dispositivos tales como teléfonos inteligentes, tabletas, e incluso ordenadores portátiles, junto con los escenarios de movilidad han generado nuevas necesidades que las soluciones tradicionales no son capaces de cubrir.

Las herramientas MDM cloud nacen para cubrir esas nuevas necesidades de las organizaciones en lo referente a la gestión del puesto de trabajo. Además de las funcionalidades propias de cada solución, traen consigo las ventajas inherentes a toda tecnología cloud (pago por uso, escalabilidad, flexibilidad y eficiencia, entre otras), por lo que la tendencia es que desbanquen a las soluciones tradicionales.

Sin embargo, dichas soluciones cloud carecen de algunas funcionalidades que pueden ser imprescindibles para determinadas organizaciones. Es previsible que, en entornos más tradicionales y aislados, donde todo el tráfico pasa por una red corporativa, las soluciones tradicionales se adapten en mayor medida a los requerimientos de la organización. Por el contrario, en empresas con escenarios más ágiles, en las que solo se requiere acceso a Internet para llevar a cabo el trabajo, las soluciones MDM cloud son el complemento perfecto para gestionar los dispositivos de usuario final.

Tras implementar una de las principales soluciones MDM cloud de mercado, Microsoft Intune, se ha podido comprobar cómo se trata de una herramienta que permite una implantación más rápida que una solución on-premises, en la que sería necesario invertir más tiempo y recursos. Intune ofrece la gran mayoría de funcionalidades que las empresas demandan para gestionar sus dispositivos. La integración con dispositivos con sistema operativo Windows 10 y posteriores y las capacidades de gestión sobre ellos son superiores a las de las soluciones de la competencia. La gestión de dispositivos Android y Apple (tanto macOS como iOS/iPadOS) es también bastante completa. Sin embargo, la capacidad de administración sobre dispositivos Linux es muy limitada, además de ser solo compatible con dos distribuciones de Ubuntu, por el momento. Asimismo, la inmediatez de las acciones realizadas sobre los dispositivos desde el portal de administración es inferior a la de la herramienta on-premises. Como punto positivo cabe destacar el gran esfuerzo realizado por Microsoft por incluir constantemente nuevas funcionalidades y ampliar el catálogo de sistemas soportados.

Debido a alguna de las carencias de Microsoft Intune, como el despliegue de imágenes de sistema operativo para construir equipos con maquetas corporativas, la solución permite integrarse con su homóloga on-premises, MECM. De esta forma, ambas herramientas realizan una administración conjunta, cada una encargándose de las áreas elegidas por la compañía, y se complementan ofreciendo una solución integral apta para la mayoría de los entornos. Además, poder traspasar la gestión de las áreas de una herramienta a otra facilita la adopción de la solución cloud a las organizaciones. Según Microsoft, este escenario de convivencia de las dos herramientas bajo una administración conjunta es, hoy en día, el más adoptado a nivel empresarial. Gartner, además, coincide en que debe elegirse la herramienta que mejor se adapte a las necesidades de la organización y complementar sus carencias con herramientas adicionales, pues no existe la herramienta que cubra todos los posibles escenarios.

Los proveedores de soluciones de gestión de puesto de trabajo están optando por el desarrollo de soluciones cloud, dejando cada vez más de lado sus soluciones tradicionales e incluyendo todas las nuevas funcionalidades solo en las cloud. Esto, unido a que los dispositivos tradicionales como los ordenadores de sobremesa tienden a desaparecer en un futuro no muy lejano, conduce a que las soluciones MDM cloud serán las más usadas en los próximos años.

Las conclusiones expuestas reflejan la consecución de los objetivos planteados al inicio del proyecto. La planificación y metodología definidas se ha respetado y las variaciones han sido mínimas, únicamente para añadir algún punto adicional a los planteados inicialmente con el objetivo de enriquecer el trabajo.

7. Glosario

On-premises Son aquellas soluciones o tecnologías que residen o están instaladas localmente en las instalaciones de la empresa.

OPEX Contracción del término inglés *Operational Expenditure*. Se refiere a los gastos operativos de una compañía.

CAPEX Contracción del término inglés *Capital Expenditure*. Se refiere a los gastos en capital de una compañía.

MDM Siglas del término inglés *Mobile Device Management*, es decir, gestión de dispositivos móviles.

WDS Siglas del término inglés *Windows Deployment Services*. Se trata de un servicio de Microsoft, que sucede a *Remote Installation Services*, que permite distribuir imágenes de instalación de sistema operativo a través de la red.

SCCM Siglas del término inglés *System Center Configuration Manager.* Es el nombre antiguo de *Microsoft Endpoint Configuration Manager (MECM).*

ZTI Siglas del término inglés *Zero Touch Installation.* Se refiere a las instalaciones que se realicen de forma totalmente automáticamente, sin requerir ningún tipo de intervención (por ejemplo, la instalación desatendida del sistema operativo de un dispositivo).

CSP Siglas del término inglés *Cloud Services Provider*, es decir, el proveedor de servicios en la nube.

IaaS Siglas del término inglés *Infrastructure as a Service*, es decir, infraestructura como servicio.

PaaS Siglas del término inglés *Platform as a Service*, es decir, plataforma como servicio.

SaaS Siglas del término inglés *Sofwtare as a Service*, es decir, software como servicio.

SLA Siglas del término inglés *Service Level Agreement*, es decir, acuerdo de nivel de servicio. Es un contrato entre cliente y proveedor en el que se estipula el nivel acordado para la calidad del servicio contratado.

EBITDA Siglas del término inglés *Earnings Before Interest, Taxes, Depreciation and Amortization*. Se trata de un indicador financiero del beneficio bruto de explotación calculado antes de la deducibilidad de los gastos financieros.

BYOD Siglas del término inglés *Bring Your Own Device*, es decir, trae tu propio dispositivo. Se trata de una iniciativa que están llevando a cabo determinadas compañías en la que permiten a los empleados utilizar sus dispositivos personales como dispositivos profesionales. En algunos casos, incluso se ofrecen incentivos o compensaciones económicas a los trabajadores.

CYOD Siglas del término inglés *Choose Your Own Device*, es decir, escoge tu propio dispositivo. Se trata de una iniciativa que están llevando a cabo determinadas compañías en la que permiten a los empleados elegir de entre una serie de dispositivos aprobados con cuál o cuáles quieren trabajar.

UEM Siglas del término inglés *Unified Endpoint Management*, es decir, gestión unificada de dispositivos finales. Son aquellas herramientas que permiten realizar la gestión de los dispositivos de forma centralizada desde una misma consola de administración.

TCO Siglas del término inglés *Total Costo of Ownership*. Es un método de cálculo diseñado para determinar los costes directos e indirectos, así como los beneficios, relacionados con un producto.

VDI Siglas del término inglés *Virtual Desktop Infrastructure*, es decir, infraestructura de escritorios virtuales.

AOSP Siglas del término inglés *Android Open Source Project*. Se trata del proyecto de código abierto de Android en el que se incluyen a las personas, procesos y código fuente que conforman Android.

ITAM Siglas del término inglés *IT Asset Management*. Son aquellas soluciones informáticas que sirven para realizar una gestión de los activos corporativos.

ITAM Siglas del término inglés *IT Service Management*. Son aquellas soluciones informáticas que permiten gestionar los servicios de tecnologías de la información mediante una disciplina basada en procesos.

Tenant Término inglés de inquilino. En Azure, se conoce como tenant a una instancia confiable e independiente de Azure AD (Active Directory) que representa a una organización y es independiente de otras instancias. Se crea en el momento en el que la organización se suscribe a un servicio en la nube de Azure.

MDM Siglas del término inglés *Mobile Application Management*, es decir, gestión de aplicaciones móviles.

OOBE Siglas del término inglés *Out of the Box Experience*. Se trata de una secuencia de pantallas que aparecen en Windows cuando el sistema operativo se ejecuta por primera vez, en las que el usuario tiene que realizar una serie de acciones como aceptar el contrato de licencia de usuario final, iniciar sesión con una cuenta personal o corporativa, conectarse a una red, elegir el idioma de la interfaz de usuario y la distribución del teclado, y configurar las preferencias de privacidad del dispositivo.

Jailbreak Término inglés cuya traducción literal en español es “fuga de la cárcel” que se utiliza para denominar el proceso de liberación de los dispositivos móviles Apple, mediante el cual se tiene acceso privilegiado al sistema. Su equivalente en dispositivos Android es root (del término raíz, en inglés).

OEM Siglas del término inglés *Original Equipment Manufacturer*, es decir, el fabricante del dispositivo.

API Siglas del término inglés *Application Programming Interfaces*. Se trata de un conjunto de subrutinas, funciones y procedimientos que ofrece una biblioteca para ser utilizada por otro software como una capa de abstracción.

8. Bibliografía

[1] Colaboradores de Wikipedia. (2022, 25 octubre). Historia de las computadoras personales. Wikipedia, la enciclopedia libre. Recuperado 17 de octubre de 2022, de https://es.wikipedia.org/wiki/Historia_de_las_computadoras_personales

[2] Historia de internet. (s. f.). Retroinformática. El pasado del futuro - FIB UPC. Recuperado 17 de octubre de 2022, de https://www.fib.upc.edu/retro-informatica/historia/internet.html

[3] Fuente, O. (2022, 6 mayo). ¿Qué es la Transformación Digital? IEBS School. Recuperado 18 de octubre de 2022, de https://www.iebschool.com/blog/que-es-transformacion-digital-business/

[4] Área Tecnológica. (s. f.). Obsolescencia Programada ¿Qué es? Ejemplos, Tipos, Ventajas, Desventajas.. Recuperado 19 de octubre de 2022, de https://www.areatecnologia.com/obsolescencia-programada.html

[5] Ramiro, R. (2022, 11 abril). 25 Tipos de ataques informáticos y cómo prevenirlos. CIBERSEGURIDAD.blog. Recuperado 19 de octubre de 2022, de https://ciberseguridad.blog/25-tipos-de-ataques-informaticos-y-como-prevenirlos/

[6] Desktop Operating System Market Share Worldwide | Statcounter Global Stats. (s. f.-b). StatCounter Global Stats. Recuperado 22 de octubre de 2022, de https://gs.statcounter.com/os-market-share/desktop/worldwide

[7] Statista. (2020, 7 octubre). Principales sistemas operativos de las empresas en España en 2019. Recuperado 22 de octubre de 2022, de https://es.statista.com/estadisticas/1064798/principales-sistemas-operativos-de-las-empresas-en-espana/

[8] HCLSoftware. (s. f.). HCL Software. Recuperado 23 de octubre de 2022, de https://www.hcltechsw.com/es/products/bigfix

[9] Gestión de dispositivos móviles | MDM Cloud |ManageEngine. (s. f.). ManageEngine. Recuperado 23 de octubre de 2022, de https://www.manageengine.com/es/mobile-device-management/

[10] Endpoint Management - Ivanti Endpoint Manager. (s. f.). Ivanti. Recuperado 23 de octubre de 2022, de https://www.ivanti.com/products/endpoint-manager

[11] Rojas, F. (2022, 4 noviembre). Introducción a Microsoft Deployment Toolkit (MDT) (Windows 10) - Windows Deployment. Microsoft Learn. Recuperado 25 de octubre de 2022, de https://learn.microsoft.com/es-es/windows/deployment/deploy-windows-mdt/get-started-with-the-microsoft-deployment-toolkit

[12] Kaur, B., Stewart, M., Czechowski, A., Arya, H., Coulter, D. & Eby, D. (2022, 5 octubre). What is Configuration Manager? - Configuration Manager. Microsoft Learn. Recuperado 27 de octubre de 2022, de https://learn.microsoft.com/en-us/mem/configmgr/core/understand/introduction

[13] Mesa central de redacción. (2020, 22 septiembre). Los últimos 20 años de tecnología. Los principales cambios que marcaron la diferencia entre 2000 y 2020. Confidencial Digital. Recuperado 28 de octubre de 2022, de https://www.elconfidencialdigital.com/articulo/tendencias/ultimos-20-anos-tecnologia-principales-cambios-marcaron-diferencia-2000-2020/20200922134031164470.html

[14] Cómo impacta la transformación digital móvil en la empresa. (2018, 31 enero). Bluumi, crea apps iOS y Android. Recuperado 28 de octubre de 2022, de https://bluumi.net/impacto-de-la-transformacion-digital-movil-en-la-empresa/

[15] Cómo debe ser la seguridad móvil corporativa. (s. f.). Leader Network. Recuperado 28 de octubre de 2022, de https://leader-network.com/ciberseguridad/como-debe-ser-la-seguridad-movil-corporativa/

[16] ¿Qué es cloud computing? (s. f.). España | IBM. Recuperado 31 de octubre de 2022, de https://www.ibm.com/es-es/cloud/learn/cloud-computing-gbl

[17] Microsoft. (s. f.). AZ-900T0XES-MICROSOFTAZUREFUNDAMENTALS. Microsoft Learning. Recuperado 3 de noviembre de 2022, de https://microsoftlearning.github.io/AZ-900T0xES-MicrosoftAzureFundamentals/Instructions/Walkthroughs/21-Calculate+Composite+SLAs.html

[18] Winter, J. (2020, 16 julio). Preparándonos para lo que viene: consideraciones financieras para la migración a la nube. Microsoft Azure. Recuperado 3 de noviembre de 2022, de https://azure.microsoft.com/es-es/blog/preparing-for-what-s-next-financial-considerations-for-cloud-migration/

[19] Cipolla, T., Wilson, D., Silva, C. & Fisler, C. (2022, 1 agosto). Magic Quadrant for Unified Endpoint Management Tools. Gartner. Recuperado 5 de noviembre de 2022, de https://www.gartner.com/document/4017175?ref=hp-wylo

[20] Newsad, L. (2022, 29 octubre). Enroll a Linux device in Intune. Microsoft Learn. Recuperado 5 de noviembre de 2022, de https://learn.microsoft.com/en-us/mem/intune/user-help/enroll-device-linux

[21] Statista. (2022, 23 febrero). Office productivity software market share worldwide 2022. Recuperado 13 de noviembre de 2022, de https://www.statista.com/statistics/983299/worldwide-market-share-of-office-productivity-software/

[22] Roth, C. & Gupta, N. (2020, 27 junio). Market Share Analysis: Enterprise Email and Authoring, Worldwide, 2019. Gartner. Recuperado 13 de noviembre de 2022, de https://www.gartner.com/document/code/717099?ref=ddisp&refval=717099

[23] Kjerland, E. (2022, 23 noviembre). Licencias disponibles para Microsoft Intune. Microsoft Learn. Recuperado 23 de noviembre de 2022, de https://learn.microsoft.com/es-es/mem/intune/fundamentals/licenses

[24] Rojas, F. (2022, 5 noviembre). Windows Autopilot registration overview. Microsoft Learn. Recuperado 25 de noviembre de 2022, de https://learn.microsoft.com/en-us/mem/autopilot/registration-overview

[25] Ohlinger, M. (2022, 13 octubre). Guía de inscripción de dispositivos macOS para Microsoft Intune. Microsoft Learn. Recuperado 25 de noviembre de 2022, de https://learn.microsoft.com/es-es/mem/intune/fundamentals/deployment-guide-enrollment-macos

[26] Ohlinger, M. (2022, noviembre 23). Guía de inscripción de dispositivos iOS/iPadOS para Microsoft Intune. Microsoft Learn. Recuperado 25 de noviembre de 2022, de https://learn.microsoft.com/es-es/mem/intune/fundamentals/deployment-guide-enrollment-ios-ipados

[27] Ohlinger, M. (2022b, noviembre 13). Guía de inscripción de dispositivos Android para Microsoft Intune. Microsoft Learn. Recuperado 25 de noviembre de 2022, de https://learn.microsoft.com/es-es/mem/intune/fundamentals/deployment-guide-enrollment-android

[28] Newsad, L. (2022, 23 noviembre). Guía de implementación para la administración de dispositivos Linux. Microsoft Learn. Recuperado 25 de noviembre de 2022, de https://learn.microsoft.com/es-es/mem/intune/fundamentals/deployment-guide-platform-linux

[29] Apple Support. (s. f.). Modelos de iPhone compatibles con iOS 15.5. Apple Support. Recuperado 27 de noviembre de 2022, de https://support.apple.com/es-es/guide/iphone/iphe3fa5df43/15.0/ios/15.0

[30] Apple Support. (s. f.). Modelos de iPad compatibles con iPadOS 15.5. Apple Support. Recuperado 27 de noviembre de 2022, de https://support.apple.com/es-es/guide/ipad/ipad213a25b2/15.0/ipados/15.0

[31] Dunsire, B. (2022, 22 noviembre). Escenarios para usar el Acceso Condicional con Microsoft Intune - Microsoft Intune. Microsoft Learn. Recuperado 27 de noviembre de 2022, de https://learn.microsoft.com/es-es/mem/intune/protect/conditional-access-intune-common-ways-use

[32] Krypton Solid. (2021, 28 diciembre). ▷▷▷ Administra las actualizaciones del sistema operativo móvil con Intune (Actualizado 2022). Recuperado 30 de noviembre de 2022, de https://kryptonsolid.com/administra-las-actualizaciones-del-sistema-operativo-movil-con-intune/

[33] Madden, J. (s. f.). White Paper: Windows 10 and mobile device management. Microsoft. Recuperado 30 de noviembre de 2022, de https://info.microsoft.com/rs/157-GQE-382/images/EN-CNTNT-Whitepaper-JMWindows10andmobiledevicemanagement.pdf

[34] Rojas, F. (2022, noviembre 18). Manually register devices with Windows Autopilot. Microsoft Learn. Recuperado 11 de diciembre de 2022, de https://learn.microsoft.com/en-us/mem/autopilot/add-devices

[35] Bhardwaj, S. (2022, 23 noviembre). Administración de dispositivos de forma remota en Microsoft Intune. Microsoft Learn. Recuperado 17 de diciembre de 2022, de https://learn.microsoft.com/es-es/mem/intune/remote-actions/teamviewer-support

[36] Bhardwaj, S. (2022, diciembre 16). Ayude de forma remota a los usuarios autenticados por la organización. Microsoft Learn. Recuperado 17 de diciembre de 2022, de https://learn.microsoft.com/es-es/mem/intune/remote-actions/remote-help

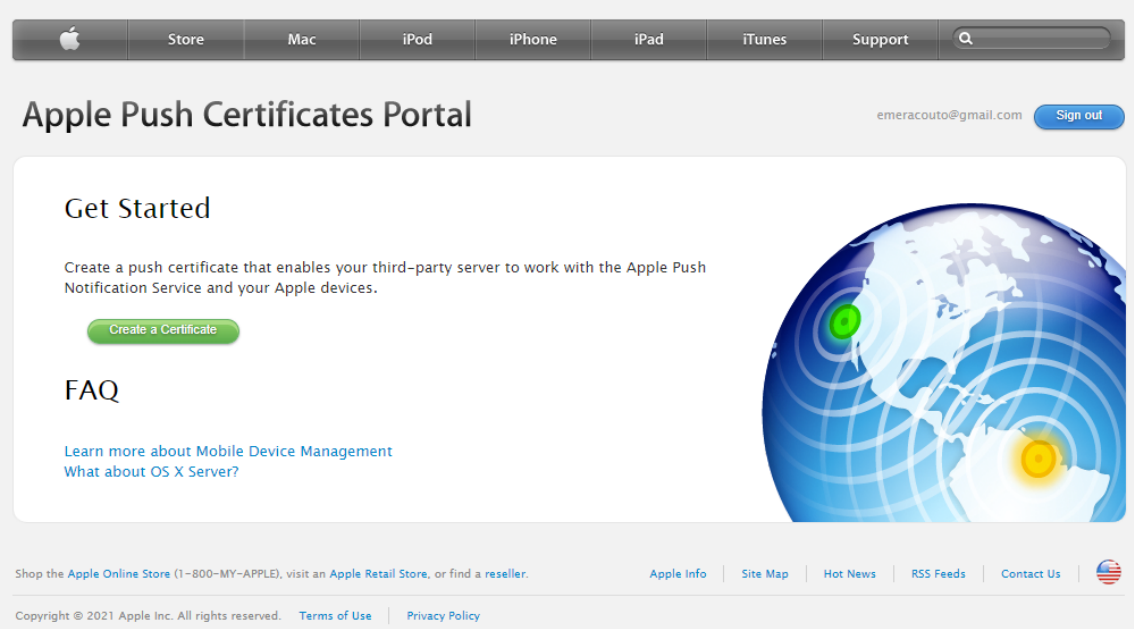
[37] Long, L. (2022, 29 diciembre). Habilita Asociación de inquilinos de Microsoft Endpoint Manager - Configuration Manager. Microsoft Learn. Recuperado 7 de enero de 2023, de https://learn.microsoft.com/es-es/mem/configmgr/tenant-attach/device-sync-actions

9. Anexos

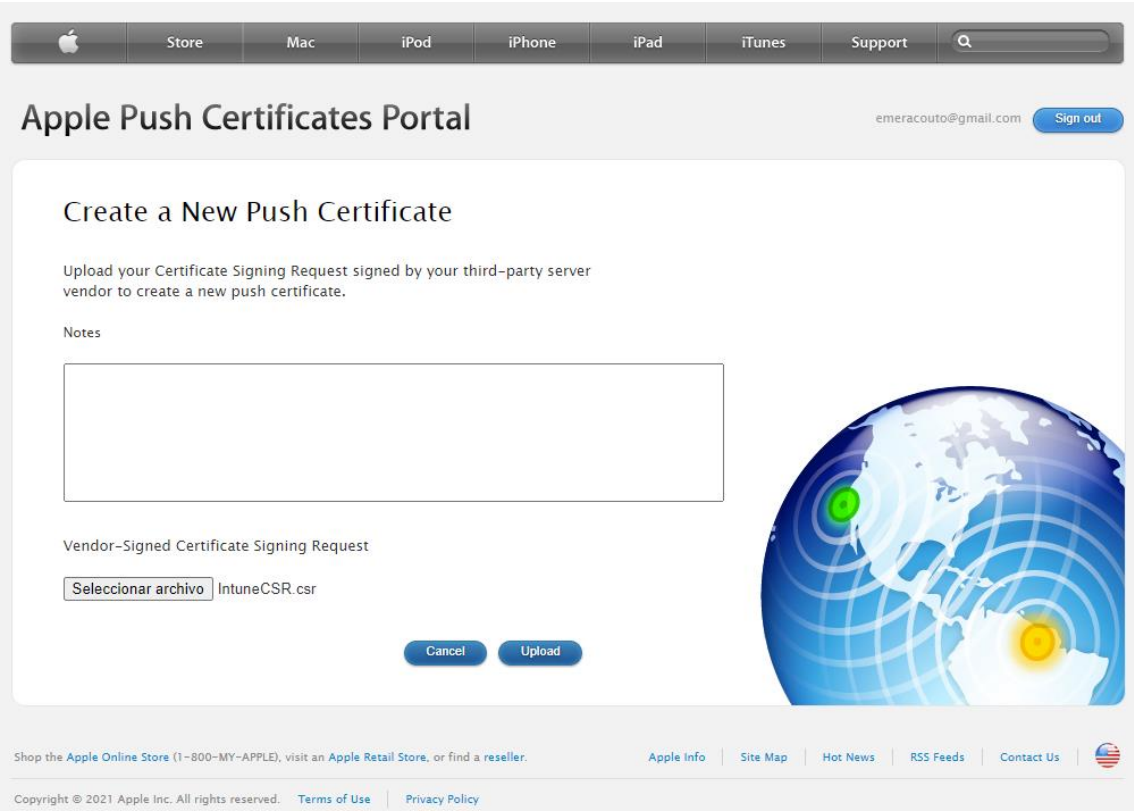
Anexo 1. Creación de certificado push MDM de Apple

Para crear un certificado push MDM de Apple se debe acceder a la dirección https://identity.apple.com/pushcert/ con una cuenta de Apple.

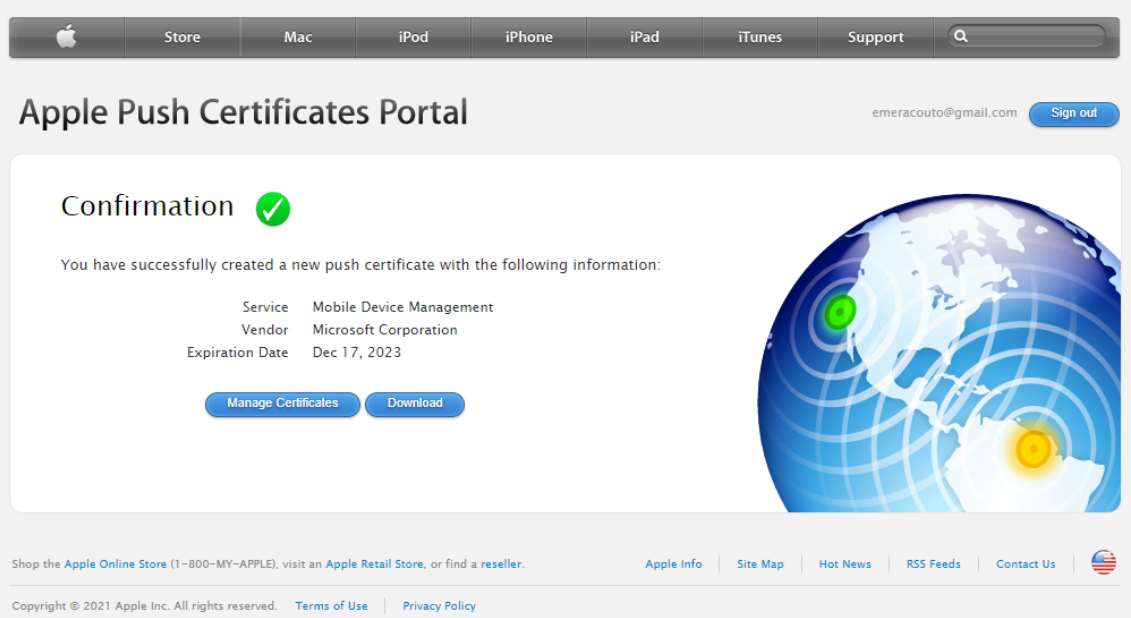
Tras validarse mediante doble factor de autenticación, se solicita la creación del certificado.



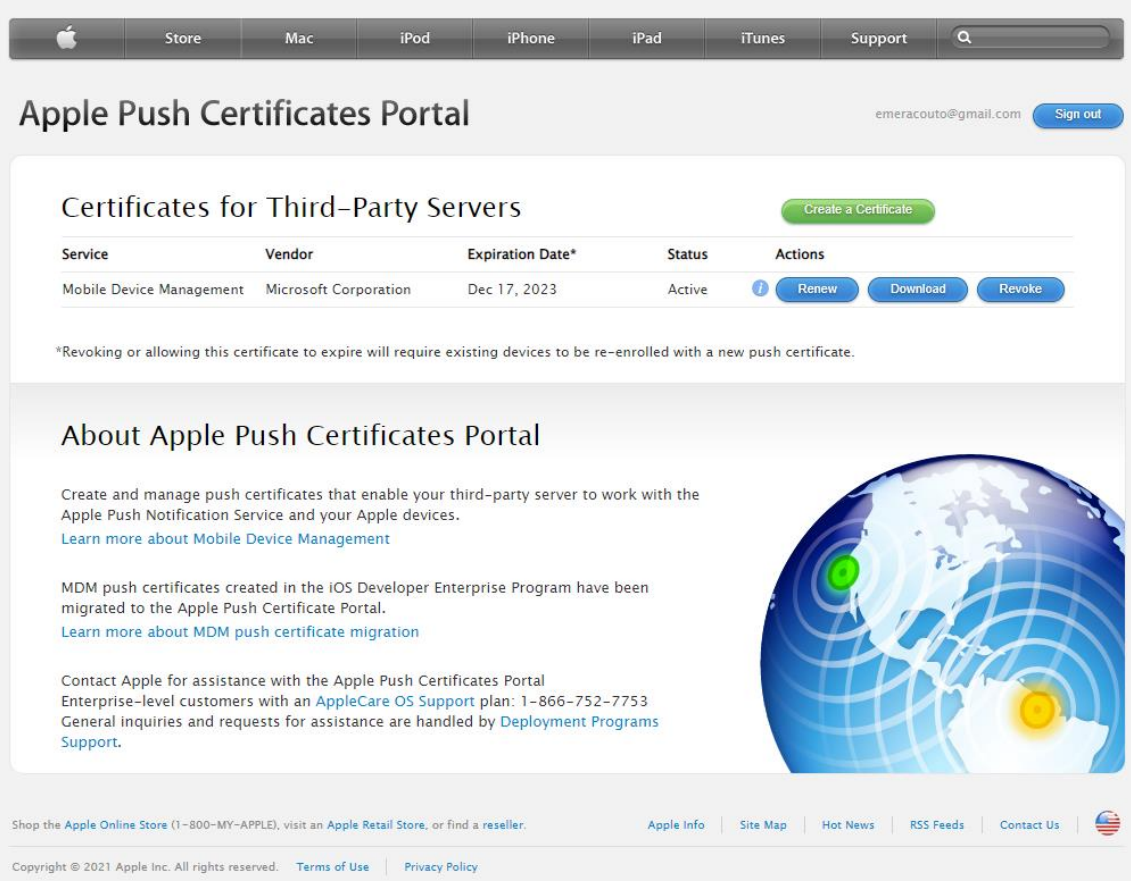
Se selecciona el archivo con extensión .csr generado en Microsoft Intune y se sube.



El portal muestra confirmación de la creación exitosa del certificado push y los detalles del mismo, así como la opción de descargarlo para importarlo en Microsoft Intune.

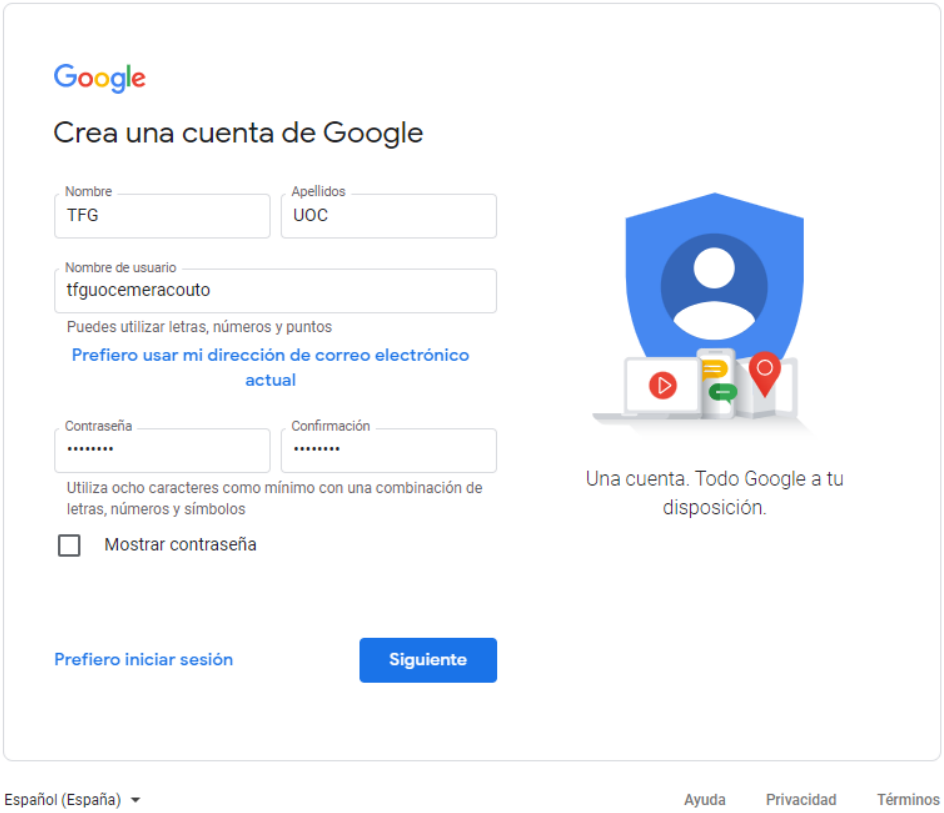


Si se accede a “Manage Certificates” se pueden visualizar los detalles del certificado, tales como su estado y fecha de caducidad. También se permite solicitar la renovación, revocación y descargarlo.



Anexo 2. Creación de una cuenta empresarial de Google

La creación de una cuenta de empresa de Google se realiza a través del siguiente enlace: https://accounts.google.com/signup/v2/webcreateaccount?gmb=exp&biz=true&flowName=GlifWebSignIn&flowEntry=SignUp



A continuación, se introduce la información solicitada y se eligen los ajustes de personalización. También se debe confirmar la configuración de la personalización y las cookies.

Google

Te damos la bienvenida a Google

tfguocemeracouto@gmail.com

Teléfono (opcional)

Google solo usará este número para mantener la seguridad de la cuenta. No lo mostrará a otros usuarios. Más tarde podrás elegir si quieres que se use con otros fines.

Dirección de correo electrónico de recuperación (o...
emeracouto@uoc.edu

La usaremos para mantener tu cuenta protegida

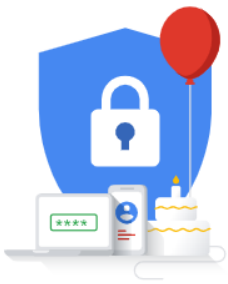
Día 24 | Mes Abril | Año 1989

Tu fecha de nacimiento

Género
Hombre

Por qué pedimos esta información

Atrás | Siguiente



Tu información personal es privada y está protegida

Español (España) | Ayuda | Privacidad | Términos

Google

Elige los ajustes de personalización

- (•) **Personalización rápida (1 paso)**
  Usa ajustes de personalización que ofrecen contenido y anuncios personalizados. Te recordaremos que revises tus ajustes en un par de semanas.
- ( ) **Personalización manual (5 pasos)**
  Configura los ajustes de personalización paso a paso. Tú decides qué ajustes quieres activar y cuáles no para tener la experiencia de contenido y anuncios que prefieras.

Puedes cambiar la configuración en cualquier momento en account.google.com

Siguiente

Tú controlas los datos que recogemos y el modo en que se utilizan

Español (España) | Ayuda | Privacidad | Términos

Google

Confirma la configuración de personalización y las cookies

Estos ajustes usan tus datos para ofrecerte una experiencia personalizada en todos los servicios y un mayor control de los anuncios que ves

Actividad en la Web y en Aplicaciones
Este ajuste se activará para ofrecer búsquedas más rápidas, resultados más relevantes y recomendaciones más útiles de aplicaciones y contenido, entre otras cosas.
Más información sobre Actividad en la Web y en Aplicaciones

Historial de YouTube
Este ajuste se activará para mostrar mejores recomendaciones de vídeos y ayudarte a recordar dónde te has quedado en un vídeo, entre otras cosas.
Más información sobre el historial de YouTube

Personalización de anuncios
Este ajuste se activará para que los anuncios que veas te sean más útiles.
Más información sobre Personalización de anuncios

Tú controlas los datos que recogemos y el modo en que se utilizan

Qué datos se usan

El ajuste Actividad en la Web y en Aplicaciones guarda tu actividad en sitios y aplicaciones de Google, como la Búsqueda y Maps, e incluye información relacionada (por ejemplo, la ubicación). También guarda el historial de Chrome sincronizado y la actividad en sitios, aplicaciones y dispositivos que utilizan los servicios de Google.

El historial de YouTube guarda los vídeos que ves y las búsquedas que haces en dicha plataforma.

El ajuste Personalización de anuncios utiliza información guardada en tu cuenta de Google (como tu actividad, intervalo de edad y sexo) y tus interacciones con anunciantes. También usaremos la actividad que realizas en otros sitios web y aplicaciones que utilizan nuestros servicios de publicidad.

Cómo usamos estos datos

Cuando inicies sesión con estos ajustes activados, tus datos personales se guardarán en tu cuenta y se usarán para personalizar tu experiencia en la Búsqueda, YouTube, Maps y otros servicios de Google para ofrecerte, por ejemplo:

- ayuda para recordar dónde te has quedado
- recomendaciones más personalizadas en los productos de Google, como artículos, aplicaciones y vídeos
- una página Inicio de YouTube adaptada a tus preferencias

También usamos tu información para mostrar anuncios. Los anuncios que se te muestran se personalizan en los servicios de Google y en sitios y aplicaciones que colaboran con Google para que puedas:

- Ver anuncios sobre temas que pueden interesarte.
- Bloquear temas y anunciantes concretos.

No vendemos tus datos personales a nadie.

Cómo puedes gestionar tus datos

Además de poder eliminar tu actividad manualmente cuando quieras, la Actividad en la Web y en Aplicaciones que tenga más de 18 meses de antigüedad y el historial de YouTube que tenga más de 36 meses de antigüedad se eliminarán automáticamente. Puedes ver tus datos, eliminarlos, cambiar la configuración y revocar tu consentimiento en account.google.com.

Información sobre las cookies y los ID

Utilizamos cookies e IDs de dispositivo para recordar tus ajustes y otras preferencias de los dispositivos en los que has iniciado sesión. También usamos cookies, IDs y datos para:

- proporcionar y mantener servicios, como hacer un seguimiento de las interrupciones y prevenir el spam, el fraude y los abusos
- medir la interacción de la audiencia y estadísticas de los sitios web para entender cómo se utilizan nuestros servicios

Si aceptas, también usaremos las cookies, los IDs y los datos para:

- mejorar la calidad de nuestros servicios y desarrollar otros nuevos
- mostrar anuncios y medir su eficacia
- mostrar contenido personalizado, en función de tus ajustes
- mostrar anuncios genéricos o personalizados, en función de tus ajustes, en Google y en la Web

Con respecto al contenido y los anuncios no personalizados, lo que veas puede estar influido por factores como lo que estés viendo en ese momento y tu ubicación (el servicio de anuncios se basa en la ubicación general). El contenido y los anuncios personalizados se pueden basar, además de en esos criterios, en tu actividad, como las búsquedas que hagas en Google y los vídeos que veas en YouTube. Los anuncios y el contenido personalizados incluyen, entre otras cosas, resultados y recomendaciones más relevantes, una página de inicio de YouTube personalizada y anuncios adaptados a tus intereses.

Puedes cambiar la configuración del navegador para rechazar algunas o todas las cookies.

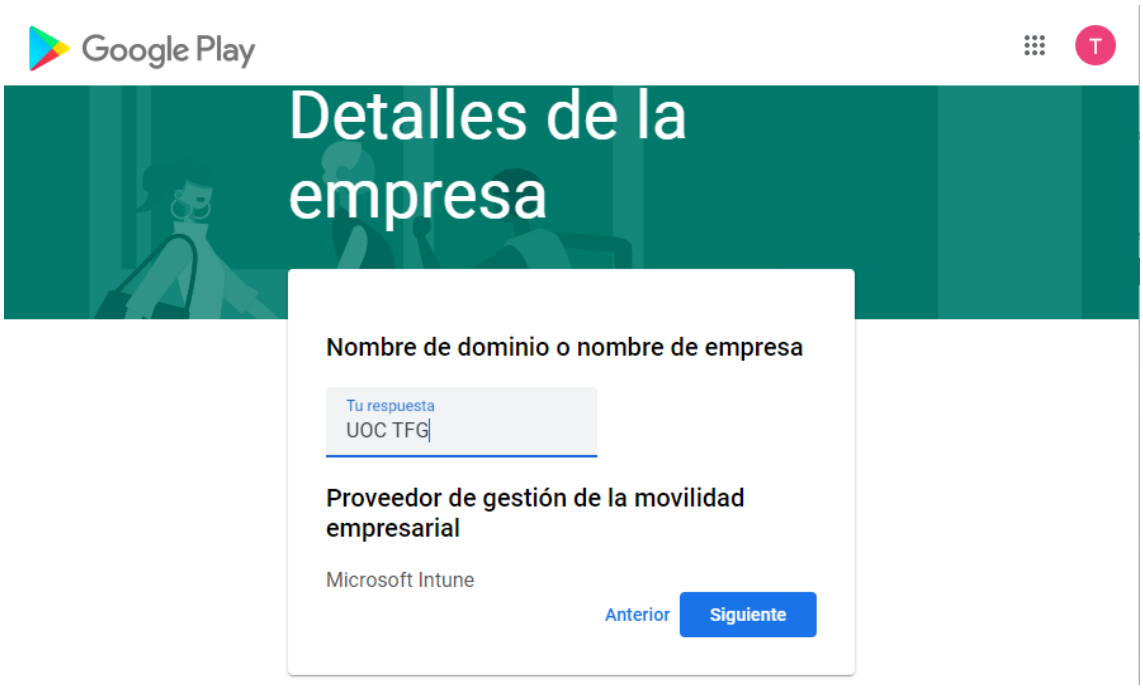
Recordatorio de privacidad
Te enviaremos un recordatorio en un par de semanas para que revises estos ajustes

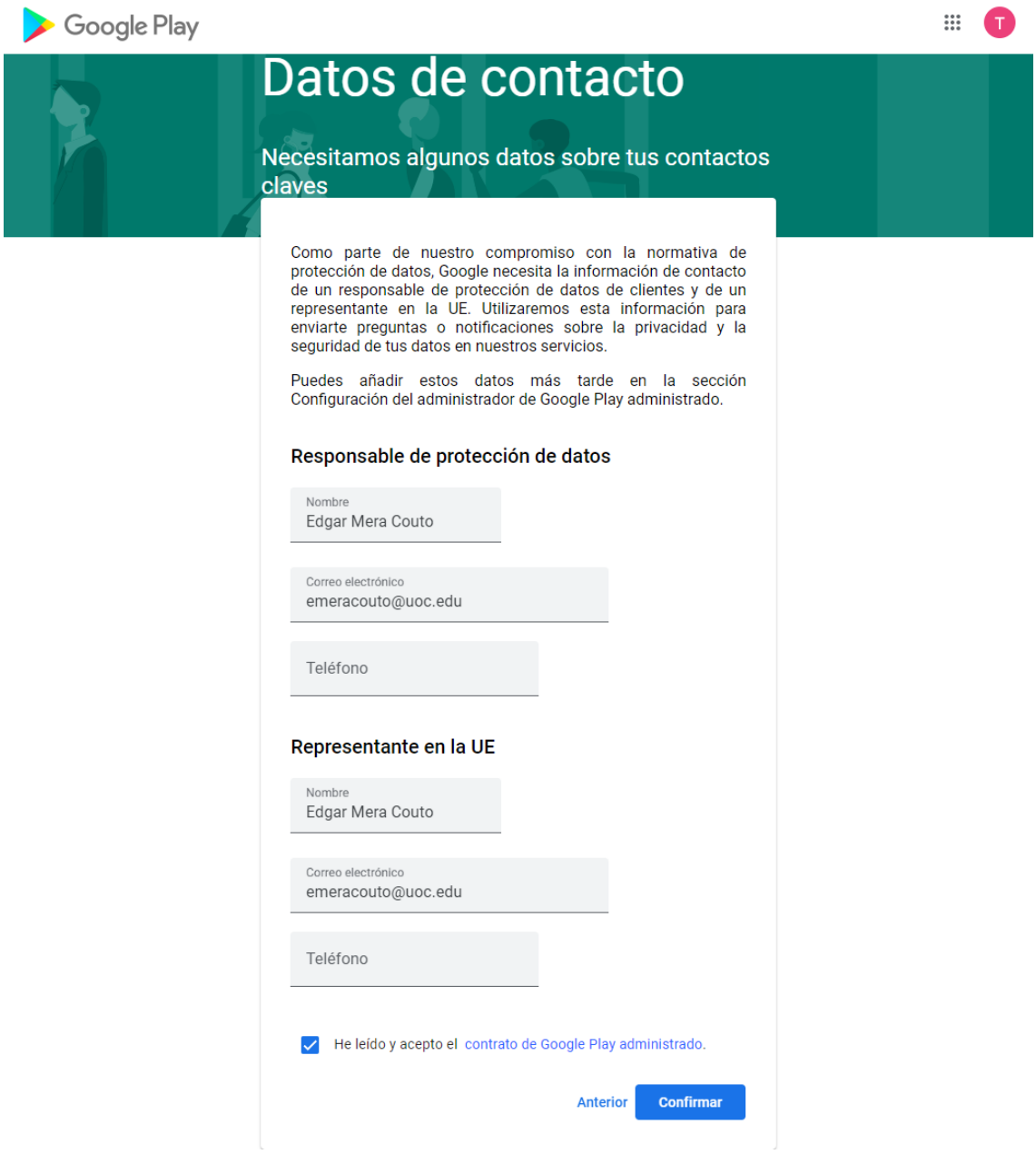
Atrás | Confirmar

Español (España) ▾ Ayuda Privacidad Términos

Una vez creada la cuenta, es posible añadir la información de la empresa a Google para tener visibilidad en la búsquedas.

El proceso de vinculación de la cuenta con Intune se muestra en la siguientes capturas.

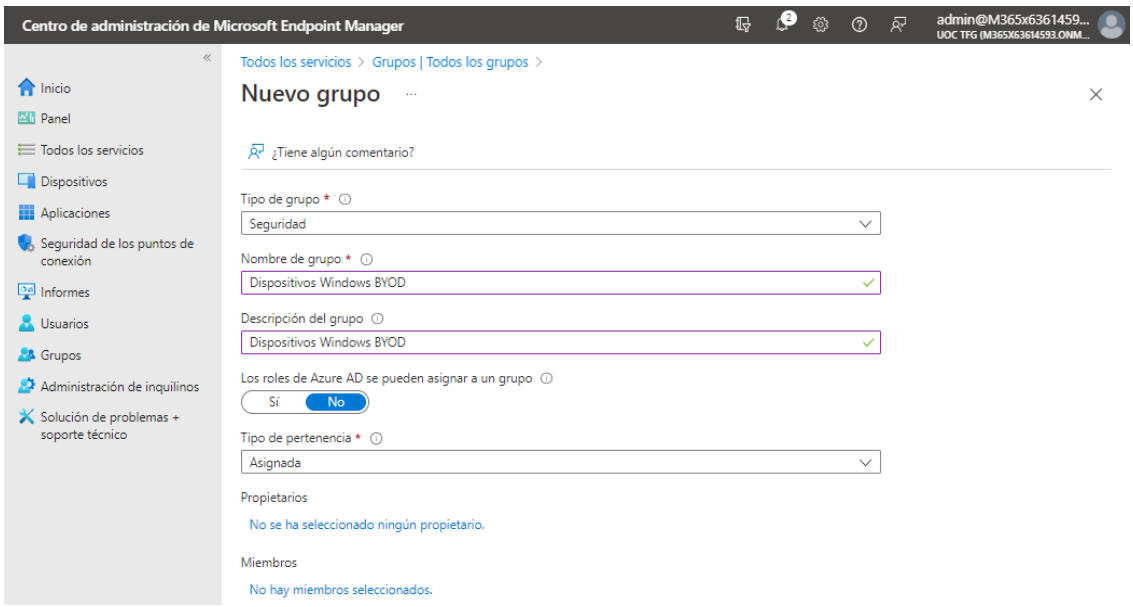


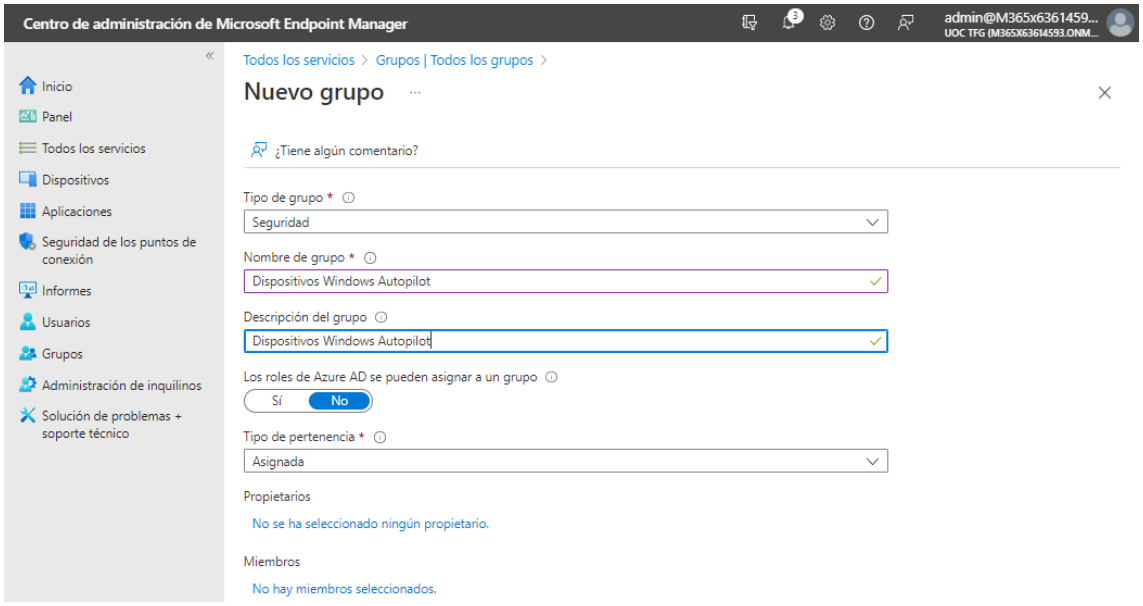

Google Play
T
Datos de contacto
Necesitamos algunos datos sobre tus contactos claves
Como parte de nuestro compromiso con la normativa de protección de datos, Google necesita la información de contacto de un responsable de protección de datos de clientes y de un representante en la UE. Utilizaremos esta información para enviarte preguntas o notificaciones sobre la privacidad y la seguridad de tus datos en nuestros servicios.
Puedes añadir estos datos más tarde en la sección Configuración del administrador de Google Play administrado.
Responsable de protección de datos
Nombre
Edgar Mera Couto
Correo electrónico
emeracouto@uoc.edu
Teléfono
Representante en la UE
Nombre
Edgar Mera Couto
Correo electrónico
emeracouto@uoc.edu
Teléfono
He leído y acepto el contrato de Google Play administrado.
Anterior
Confirmar

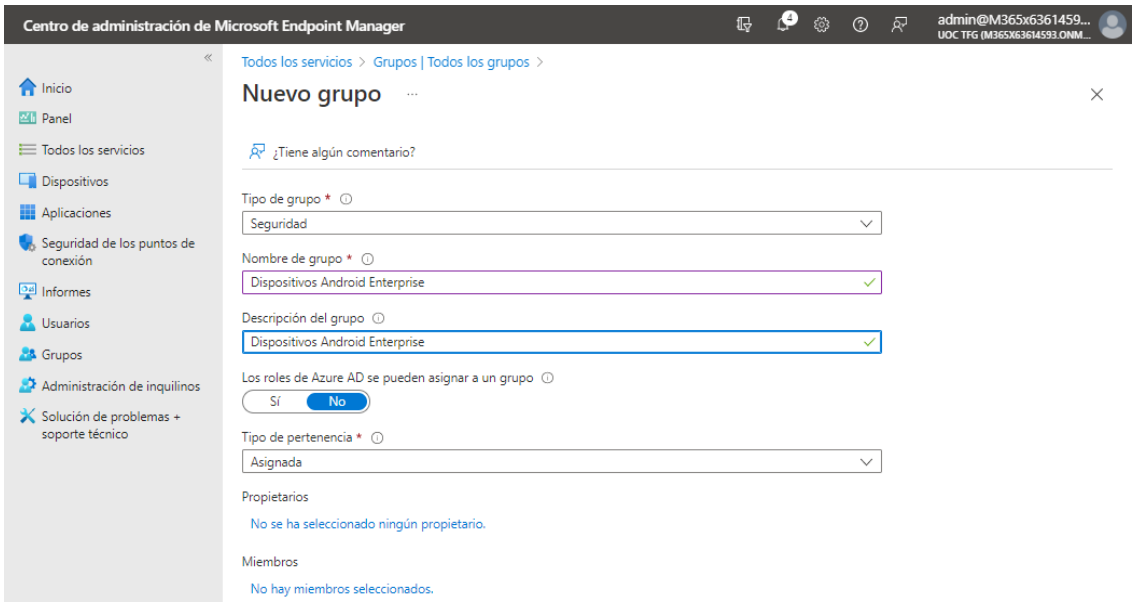
Google Play
T
Configuración completada
Completar registro

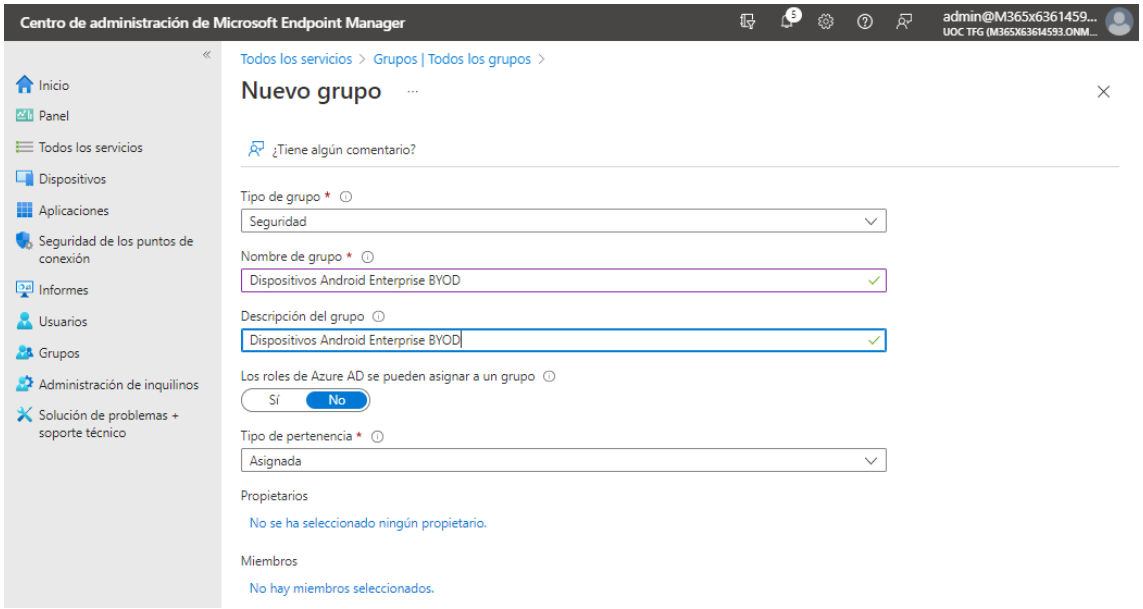
Anexo 3. Creación de grupos de seguridad en Intune

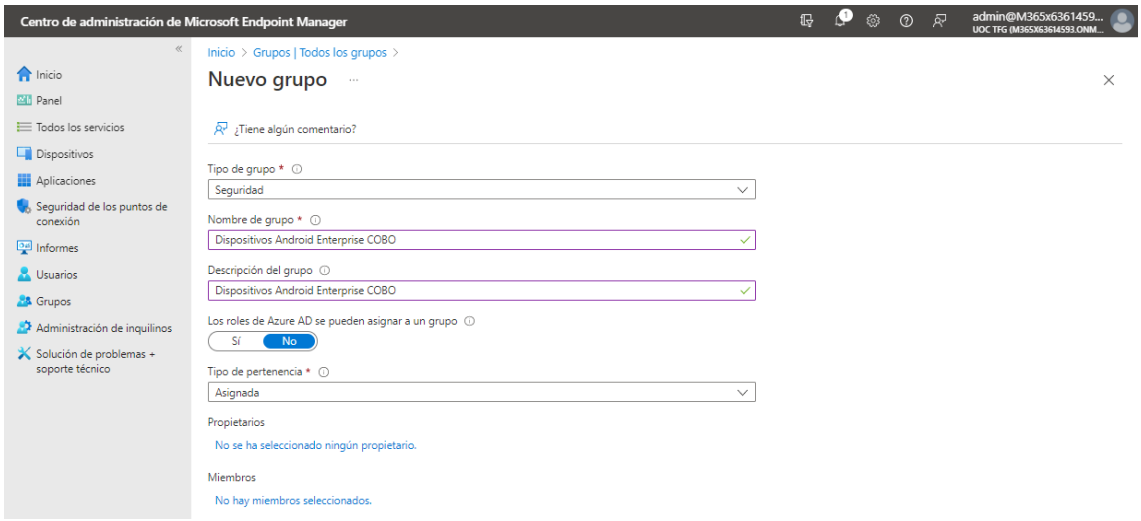
Las siguientes capturas muestran la creación de todos los grupos de dispositivos del entorno.

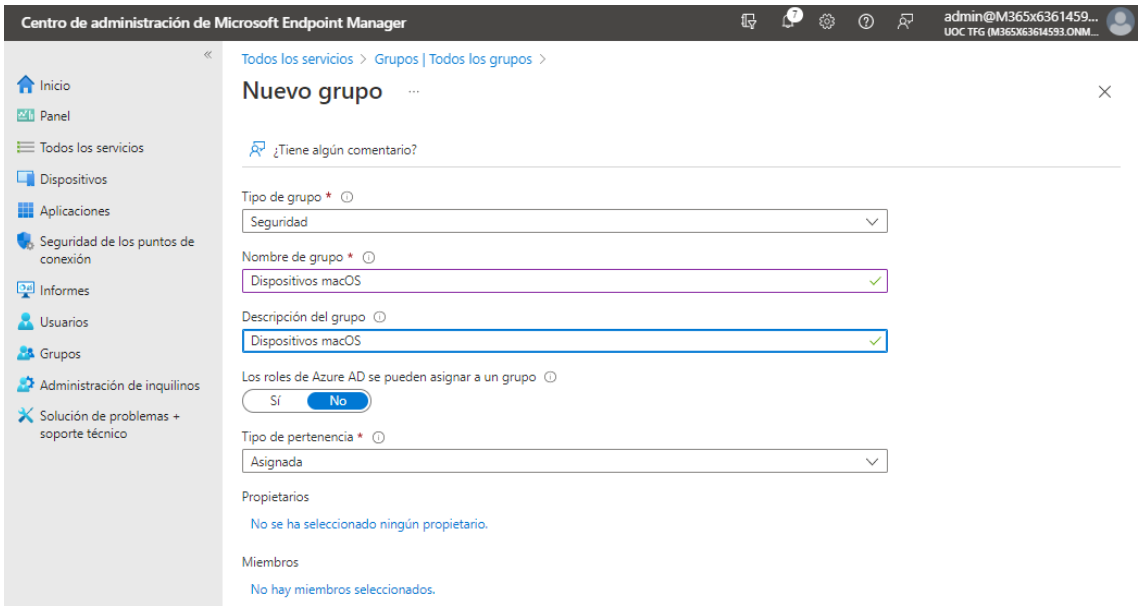


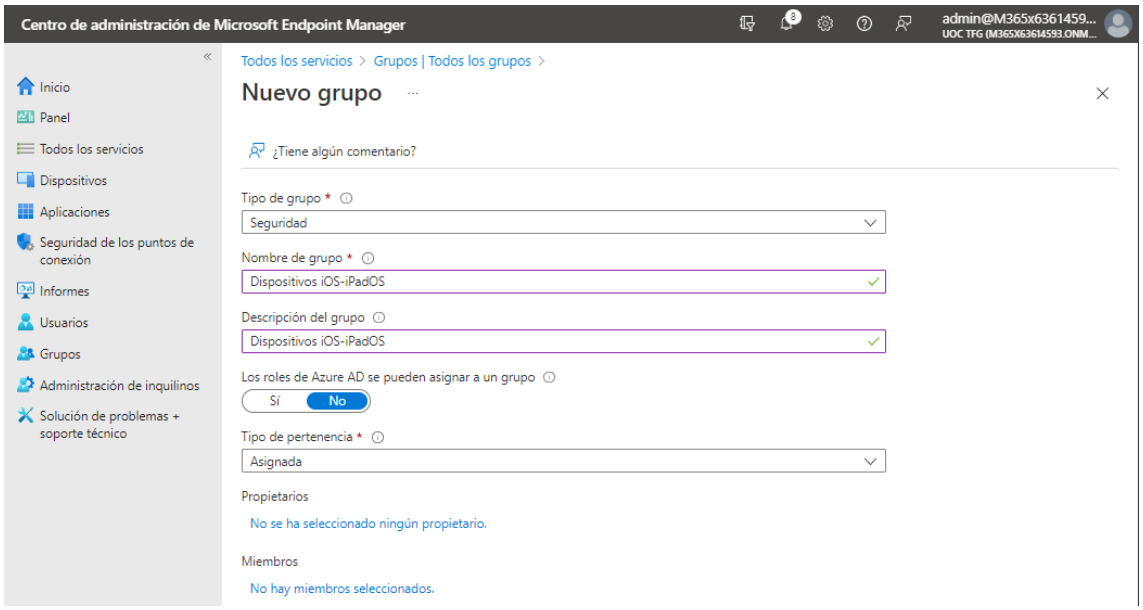


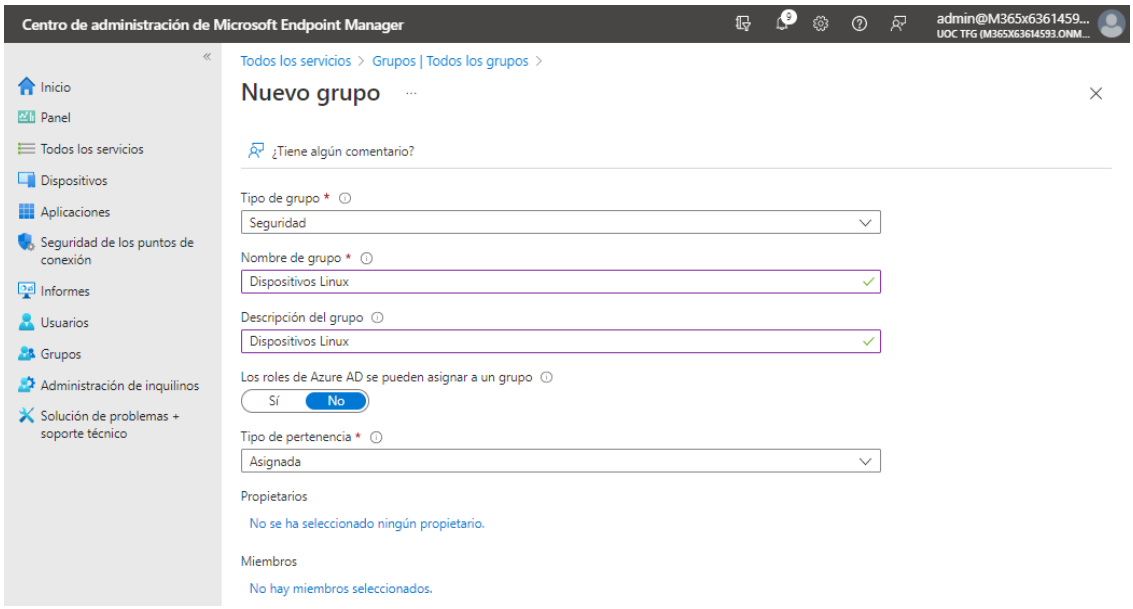

Centro de administración de Microsoft Endpoint Manager
admin@M365x6361459...
UOC TFG (M365X63614593.ONM...
Inicio
Panel
Todos los servicios
Dispositivos
Aplicaciones
Seguridad de los puntos de conexión
Informes
Usuarios
Grupos
Administración de inquilinos
Solución de problemas + soporte técnico
Todos los servicios > Grupos | Todos los grupos >
Nuevo grupo
¿Tiene algún comentario?
Tipo de grupo *
Seguridad
Nombre de grupo *
Dispositivos Android Enterprise
Descripción del grupo
Dispositivos Android Enterprise
Los roles de Azure AD se pueden asignar a un grupo
Sí
No
Tipo de pertenencia *
Asignada
Propietarios
No se ha seleccionado ningún propietario.
Miembros
No hay miembros seleccionados.

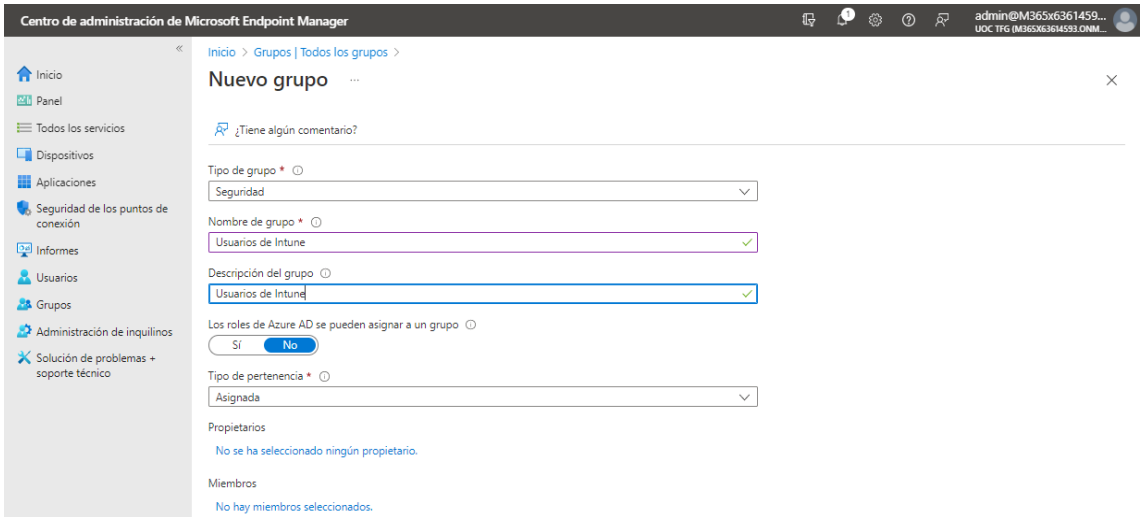

Centro de administración de Microsoft Endpoint Manager
admin@M365x6361459...
UOC TFG (M365X63614593.ONM...
Inicio
Panel
Todos los servicios
Dispositivos
Aplicaciones
Seguridad de los puntos de conexión
Informes
Usuarios
Grupos
Administración de inquilinos
Solución de problemas + soporte técnico
Todos los servicios > Grupos | Todos los grupos >
Nuevo grupo
¿Tiene algún comentario?
Tipo de grupo *
Seguridad
Nombre de grupo *
Dispositivos Android Enterprise BYOD
Descripción del grupo
Dispositivos Android Enterprise BYOD
Los roles de Azure AD se pueden asignar a un grupo
Sí
No
Tipo de pertenencia *
Asignada
Propietarios
No se ha seleccionado ningún propietario.
Miembros
No hay miembros seleccionados.


Centro de administración de Microsoft Endpoint Manager
admin@M365x6361459...
UOC TFG (M365X63614593.ONM...
Inicio
Panel
Todos los servicios
Dispositivos
Aplicaciones
Seguridad de los puntos de conexión
Informes
Usuarios
Grupos
Administración de inquilinos
Solución de problemas + soporte técnico
Inicio > Grupos | Todos los grupos >
Nuevo grupo
¿Tiene algún comentario?
Tipo de grupo *
Seguridad
Nombre de grupo *
Dispositivos Android Enterprise COBO
Descripción del grupo
Dispositivos Android Enterprise COBO
Los roles de Azure AD se pueden asignar a un grupo
Sí
No
Tipo de pertenencia *
Asignada
Propietarios
No se ha seleccionado ningún propietario.
Miembros
No hay miembros seleccionados.


Centro de administración de Microsoft Endpoint Manager
admin@M365x6361459...
UOC TFG (M365X63614593.ONM...
Inicio
Panel
Todos los servicios
Dispositivos
Aplicaciones
Seguridad de los puntos de conexión
Informes
Usuarios
Grupos
Administración de inquilinos
Solución de problemas + soporte técnico
Todos los servicios > Grupos | Todos los grupos >
Nuevo grupo
¿Tiene algún comentario?
Tipo de grupo *
Seguridad
Nombre de grupo *
Dispositivos macOS
Descripción del grupo
Dispositivos macOS
Los roles de Azure AD se pueden asignar a un grupo
Sí
No
Tipo de pertenencia *
Asignada
Propietarios
No se ha seleccionado ningún propietario.
Miembros
No hay miembros seleccionados.

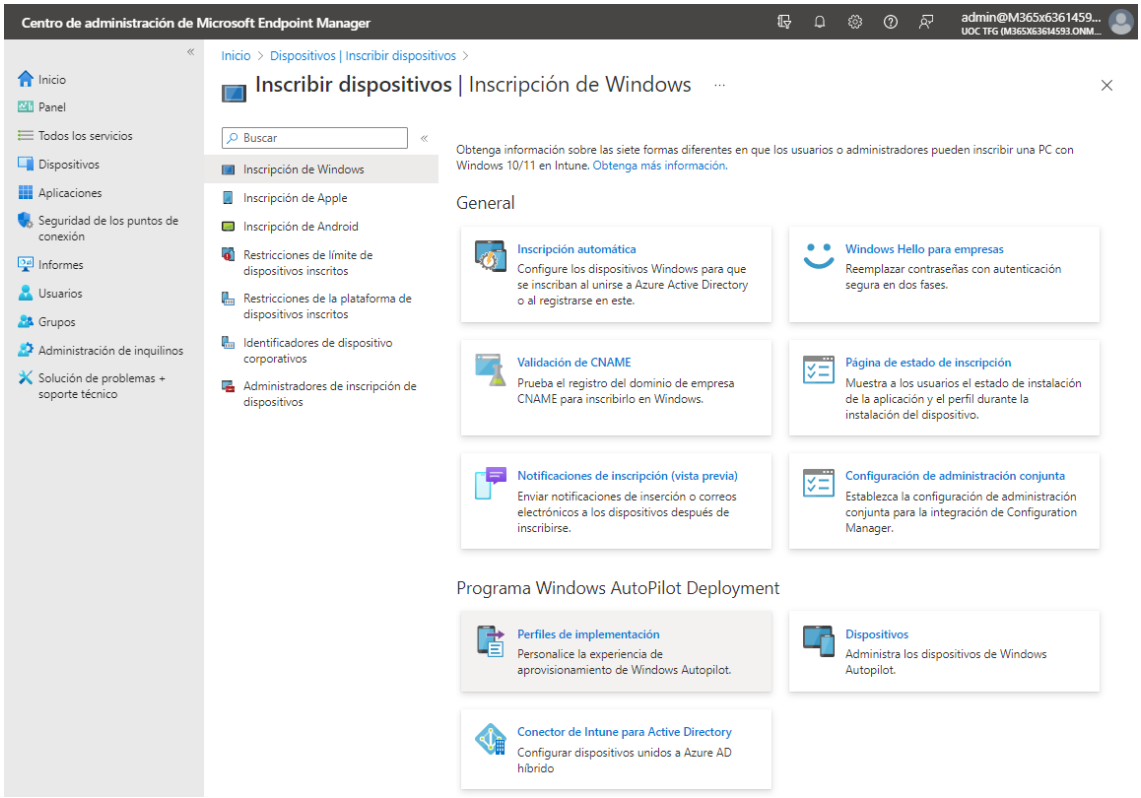

Centro de administración de Microsoft Endpoint Manager
admin@M365x6361459...
UOC TFG (M365X63614593.ONM...
Inicio
Panel
Todos los servicios
Dispositivos
Aplicaciones
Seguridad de los puntos de conexión
Informes
Usuarios
Grupos
Administración de inquilinos
Solución de problemas + soporte técnico
Todos los servicios > Grupos | Todos los grupos >
Nuevo grupo
¿Tiene algún comentario?
Tipo de grupo *
Seguridad
Nombre de grupo *
Dispositivos iOS-iPadOS
Descripción del grupo
Dispositivos iOS-iPadOS
Los roles de Azure AD se pueden asignar a un grupo
Sí
No
Tipo de pertenencia *
Asignada
Propietarios
No se ha seleccionado ningún propietario.
Miembros
No hay miembros seleccionados.


Centro de administración de Microsoft Endpoint Manager
admin@M365x6361459...
UOC TFG (M365X63614593.ONM...
Inicio
Panel
Todos los servicios
Dispositivos
Aplicaciones
Seguridad de los puntos de conexión
Informes
Usuarios
Grupos
Administración de inquilinos
Solución de problemas + soporte técnico
Todos los servicios > Grupos | Todos los grupos >
Nuevo grupo
¿Tiene algún comentario?
Tipo de grupo *
Seguridad
Nombre de grupo *
Dispositivos Linux
Descripción del grupo
Dispositivos Linux
Los roles de Azure AD se pueden asignar a un grupo
Sí
No
Tipo de pertenencia *
Asignada
Propietarios
No se ha seleccionado ningún propietario.
Miembros
No hay miembros seleccionados.

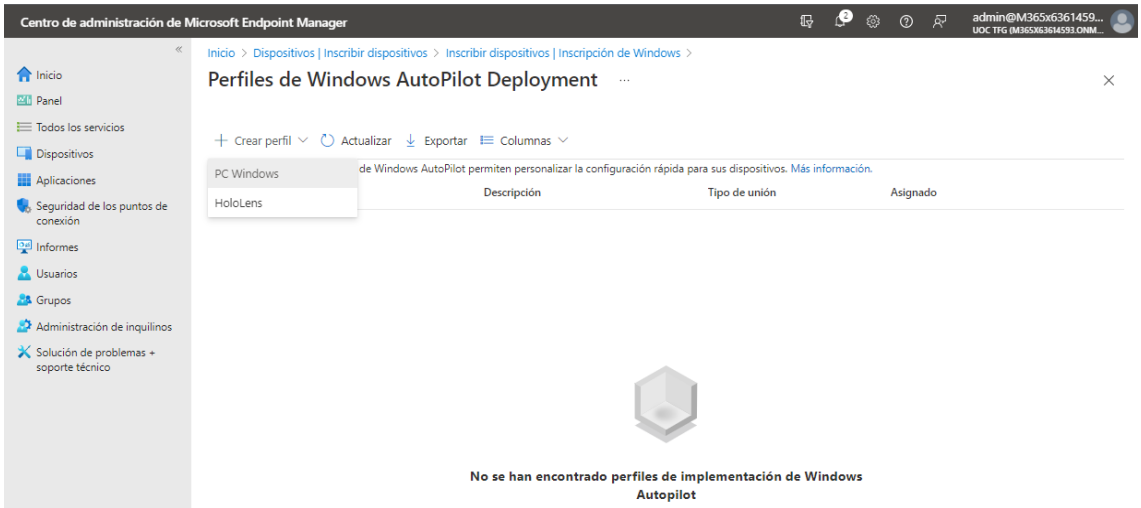

Centro de administración de Microsoft Endpoint Manager
admin@M365x6361459...
UOC TFG (M365X63614593.ONM...
Inicio
Panel
Todos los servicios
Dispositivos
Aplicaciones
Seguridad de los puntos de conexión
Informes
Usuarios
Grupos
Administración de inquilinos
Solución de problemas + soporte técnico
Inicio > Grupos | Todos los grupos >
Nuevo grupo
¿Tiene algún comentario?
Tipo de grupo *
Seguridad
Nombre de grupo *
Usuarios de Intune
Descripción del grupo
Usuarios de Intune
Los roles de Azure AD se pueden asignar a un grupo
Sí
No
Tipo de pertenencia *
Asignada
Propietarios
No se ha seleccionado ningún propietario.
Miembros
No hay miembros seleccionados.

Anexo 4. Creación de perfil de implementación Windows AutoPilot

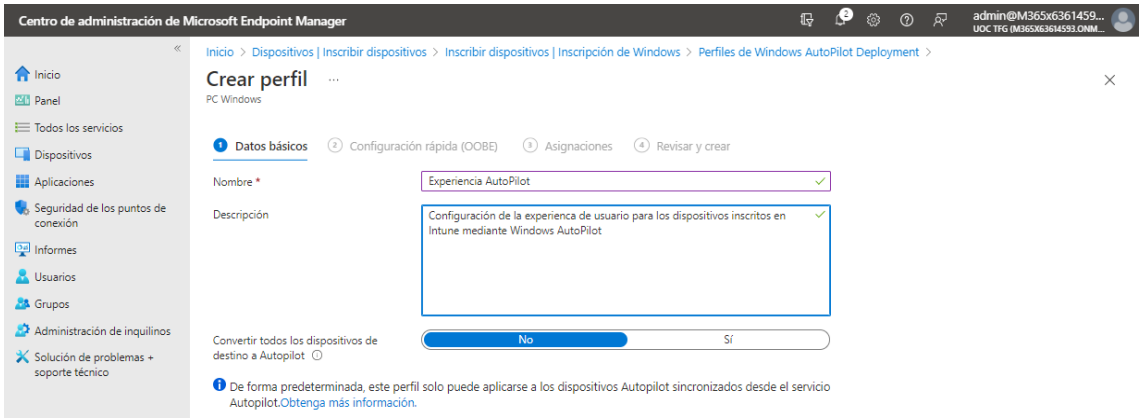
La creación de un perfil de implementación de Windows AutoPilot se realiza como se muestra a continuación. Para acceder a la creación del perfil, hay que navegar a través de Dispositivos/Inscribir Dispositivos/Inscripción de Windows y seleccionar “Perfiles de implementación” en el apartado Programa Windows AutoPilot Deployment.



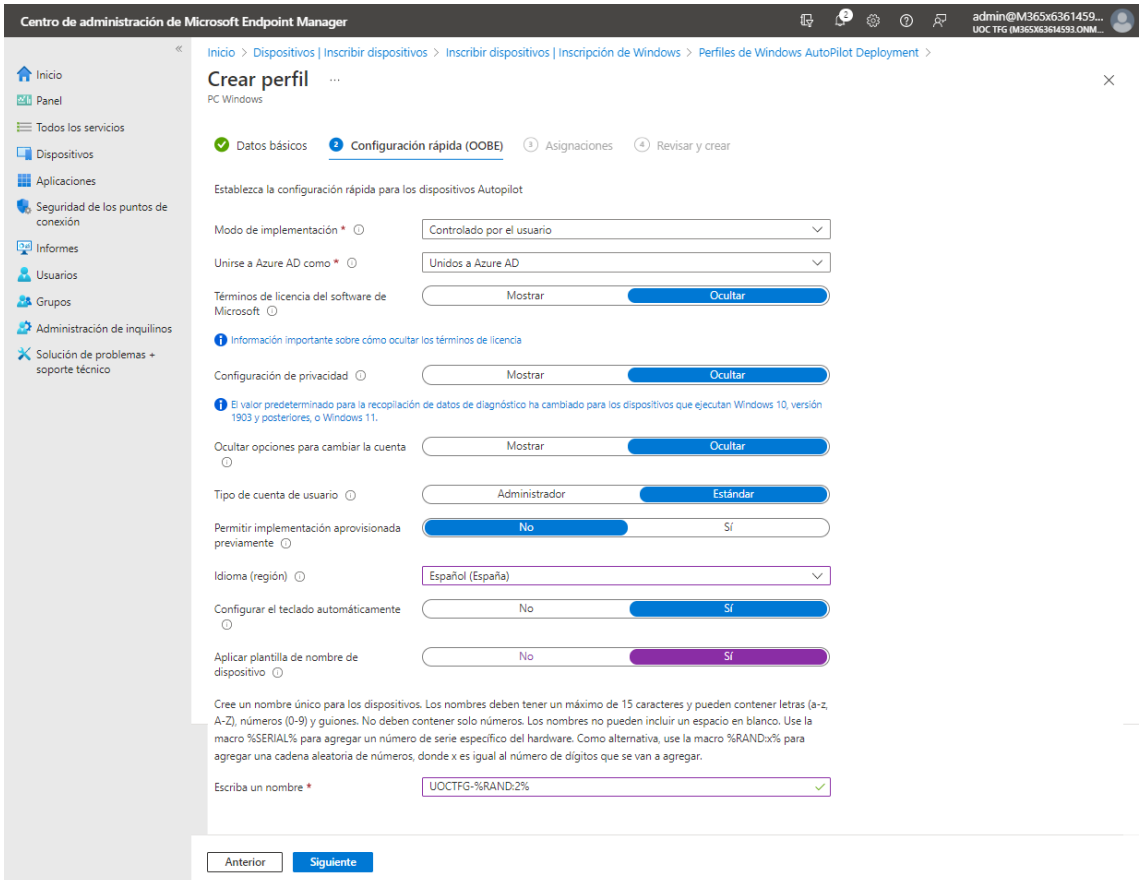
Una vez ventro de los perfiles de Windows AutoPilot Deployment, se selecciona “Crear perfil” y el tipo de dispositivo, PC Windows en este caso.



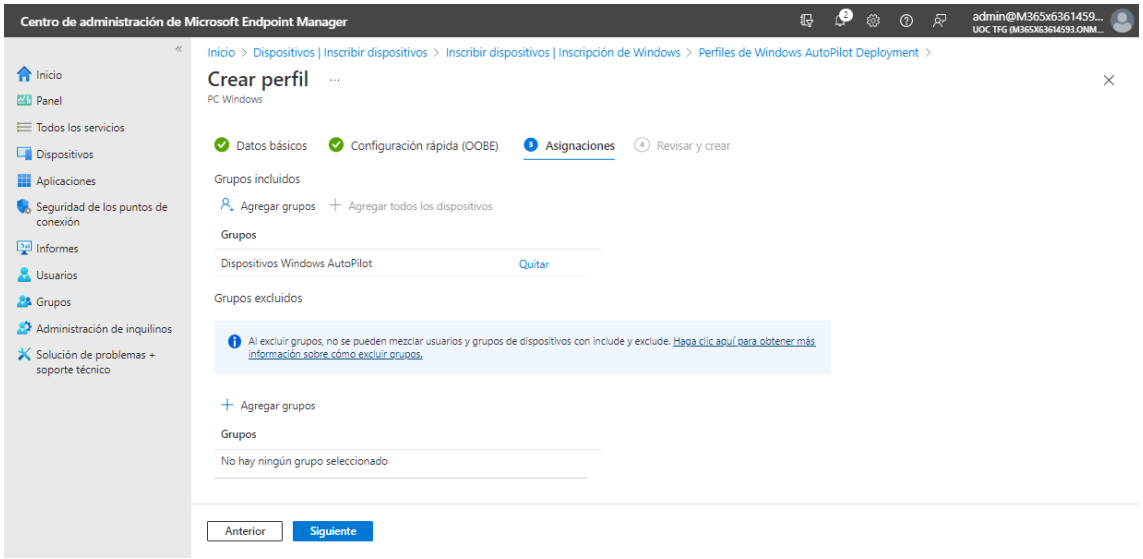
En el primer paso, se asigna un nombre y una descripción al perfil de implementación.



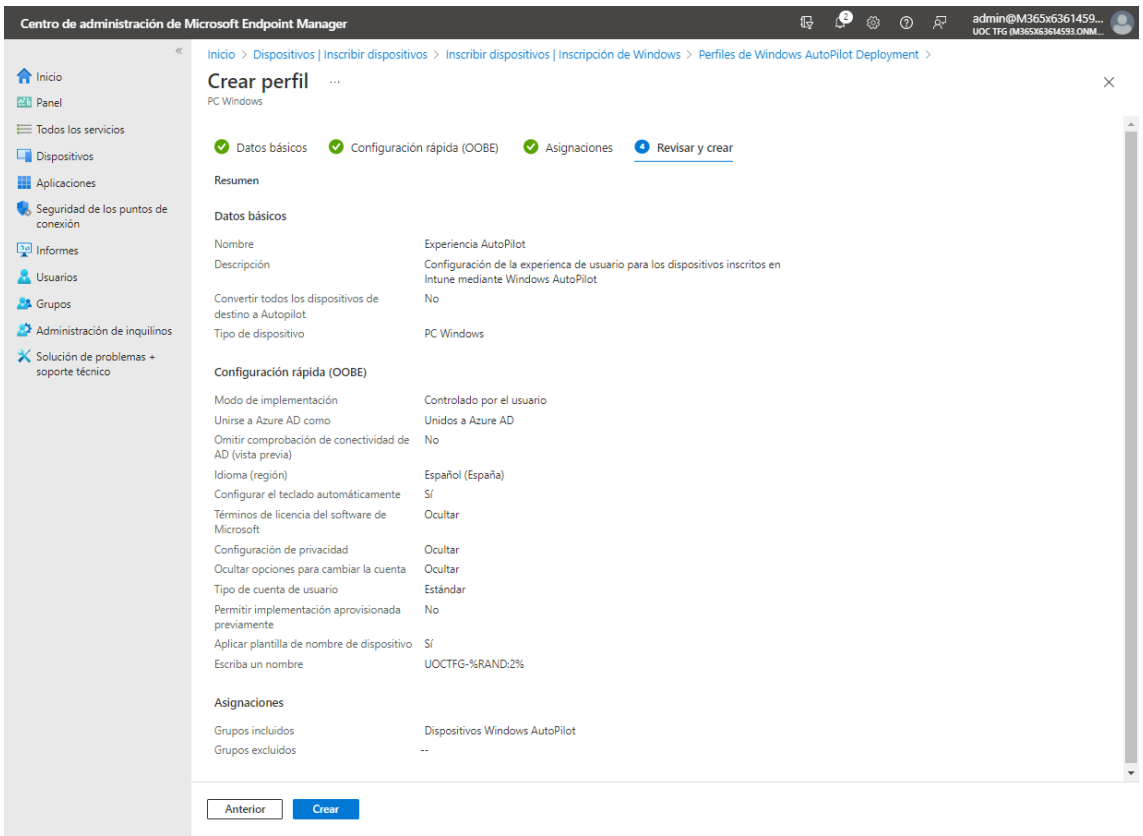
En el segundo paso, se configuran las opciones según lo deseado. El dispositivo se unirá a Azure AD, no se mostrarán los términos de licencia, el idioma y la región serán Español (España) y el nombre del dispositivo será UOCTFG-XX, donde XX serán 2 números aleatorios.



En el tercer paso se indican las asignaciones (inclusiones y exclusiones) a las que se aplicará el perfil de implementación.

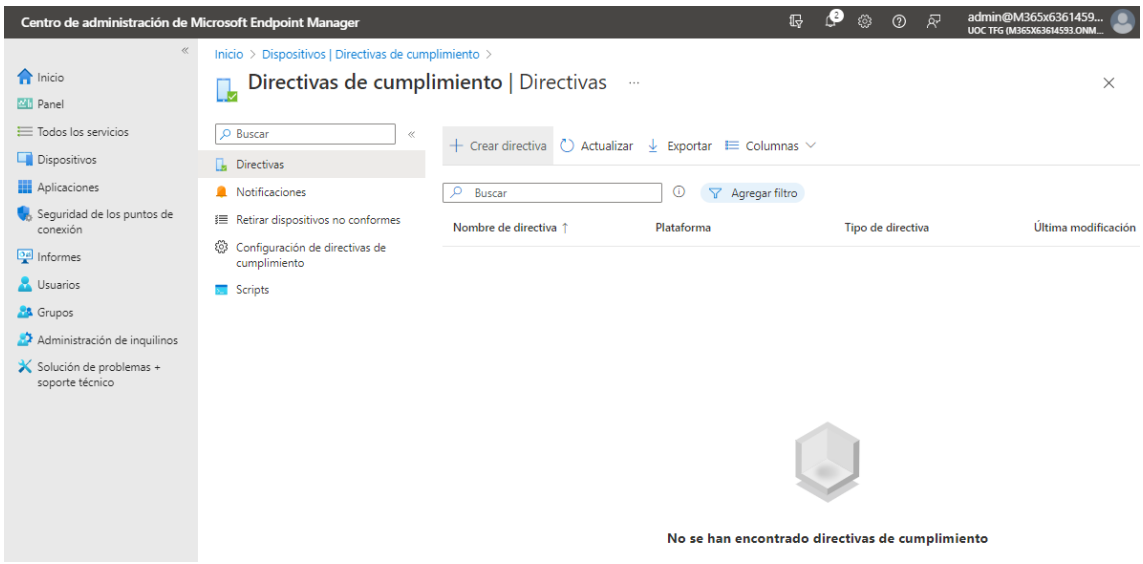


Por último, se revisan los detalles del perfil que se va a crear y se realiza la creación.



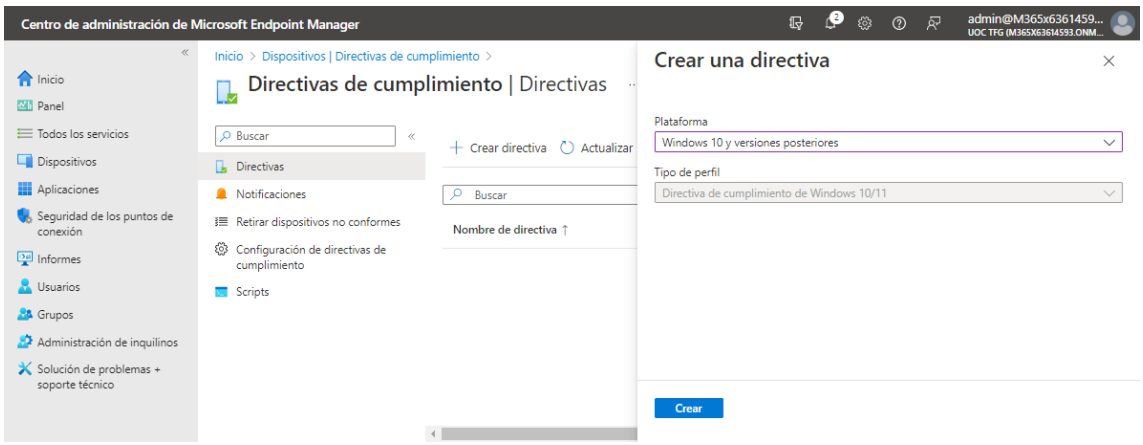
Anexo 5. Creación de directivas de cumplimiento

La creación de directivas de cumplimiento en Intune se lleva a cabo desde Dispositivos/Directivas de cumplimiento/Directivas.

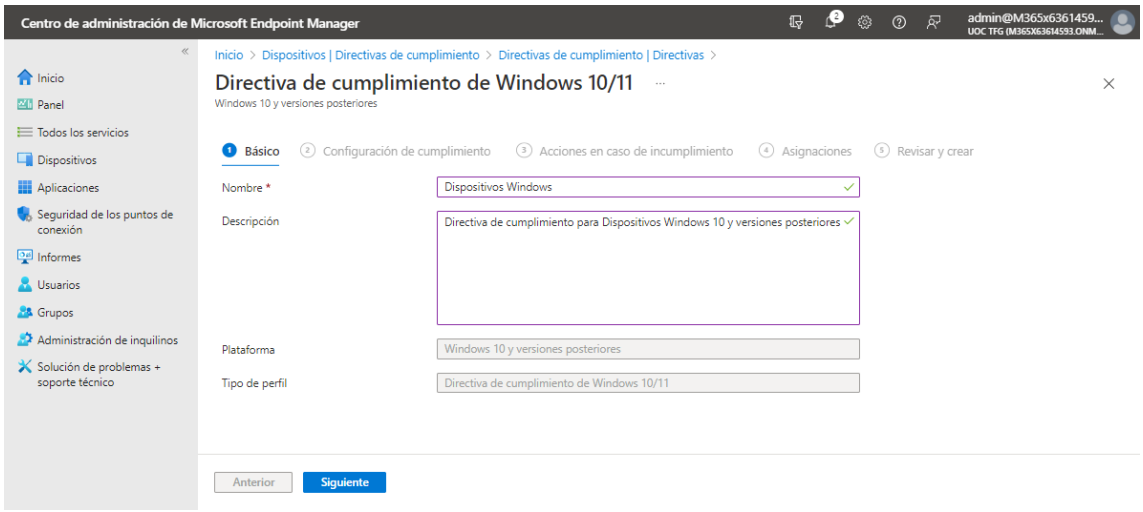


- **<u>Dispositivos Windows 10 y versiones posteriores</u>**

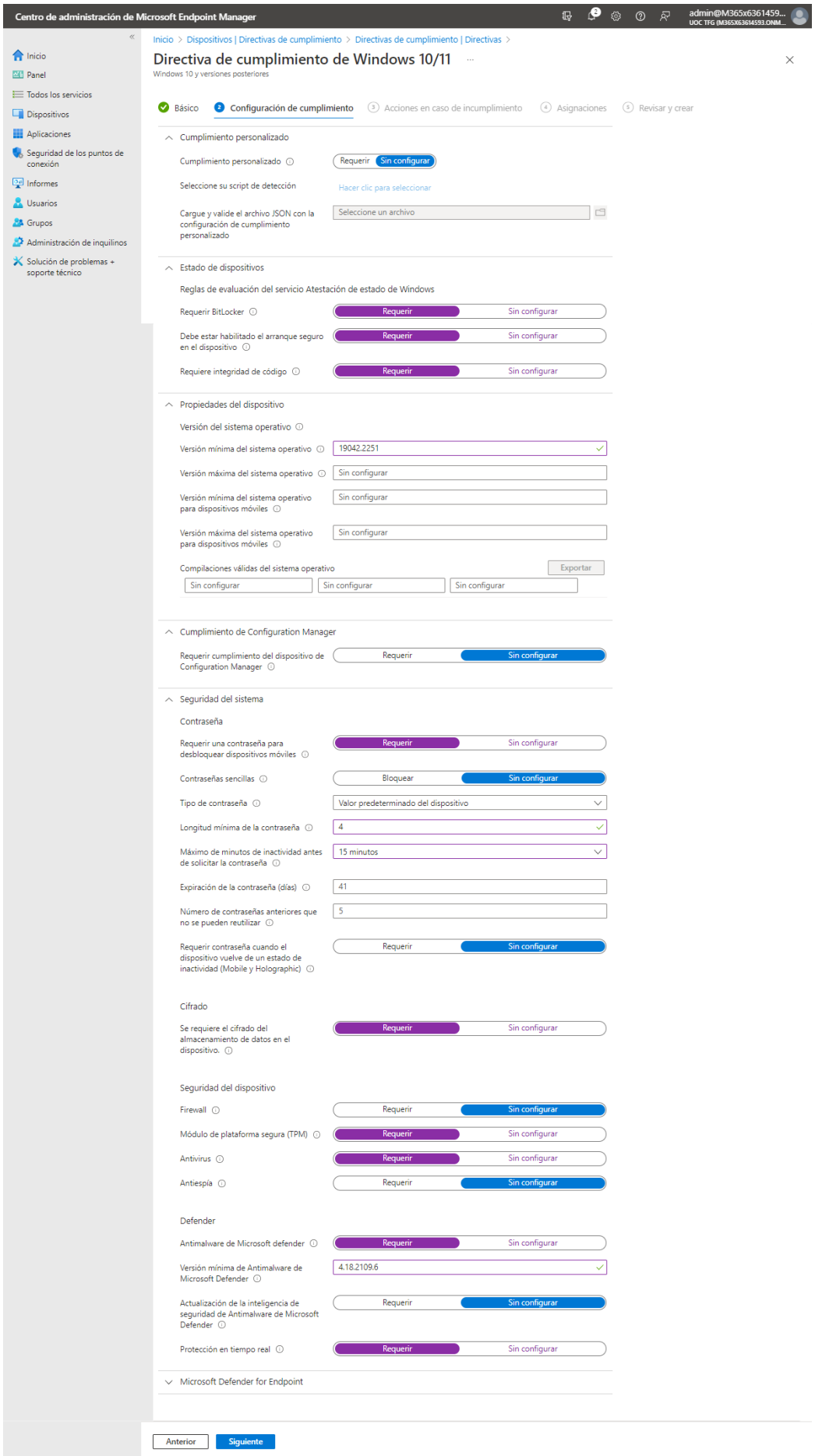
Al seleccionar “Crear Directiva”, se elige plataforma Windows 10 y versiones posteriores de las disponibles en el desplegable.



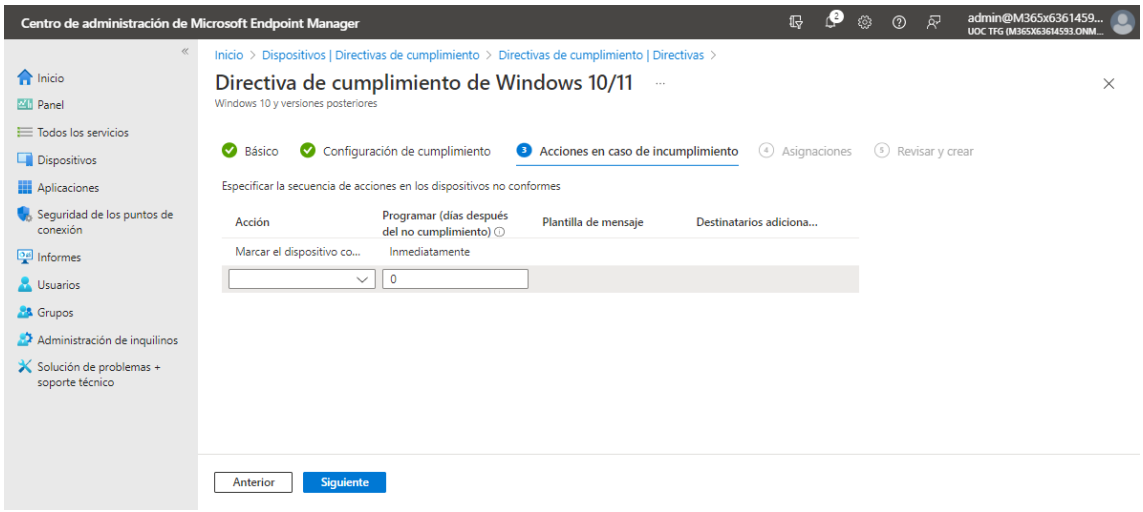
En el primer paso, se indica el nombre y la descripción de la directiva de cumplimiento.



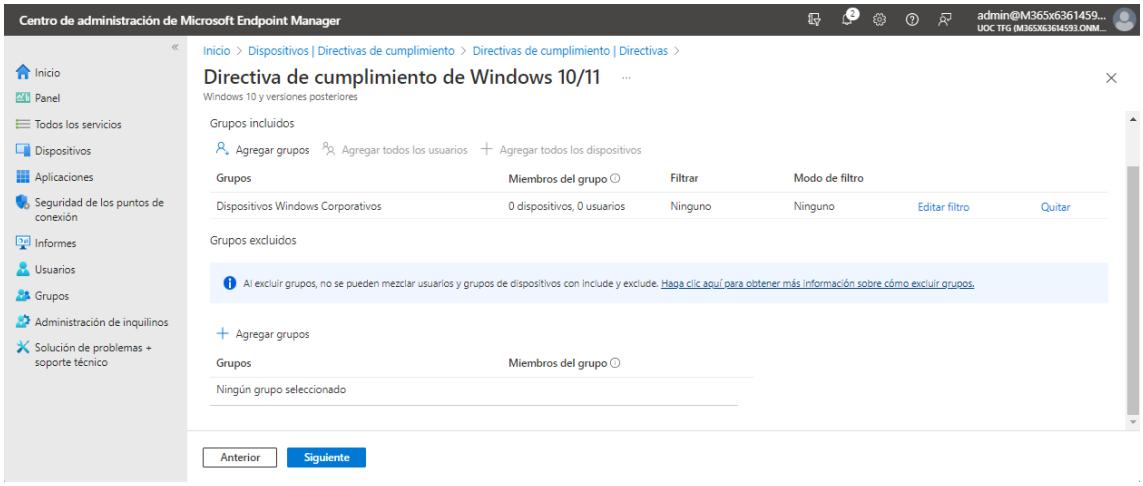
En el segundo paso, se configuran los parámetros deseados que deban cumplir los dispositivos para para ser marcados como compatibles. En este caso, se requiere que el dispositivo tenga los datos cifrados con BitLocker, el arranque seguro y la integridad de código estén habilitados, la versión mínima del sistema operativo sea Windows 10 20H2 con la actualización de noviembre de 2022 (compilación 19042.2251), el dispositivo disponga de contraseña con una determinada complejidad y el antimalware y la protección en tiempo real de Windows Defender estén habilitadas, entre otros.


Centro de administración de Microsoft Endpoint Manager
admin@M365x6361459...
UOC TFG (M365X6361459.ONM...
Inicio
Panel
Todos los servicios
Dispositivos
Aplicaciones
Seguridad de los puntos de conexión
Informes
Usuarios
Grupos
Administración de inquilinos
Solución de problemas + soporte técnico
Inicio > Dispositivos | Directivas de cumplimiento > Directivas de cumplimiento | Directivas >
Directiva de cumplimiento de Windows 10/11
Windows 10 y versiones posteriores
Básico
Configuración de cumplimiento
Acciones en caso de incumplimiento
Asignaciones
Revisar y crear
Cumplimiento personalizado
Cumplimiento personalizado
Requerir
Sin configurar
Seleccione su script de detección
Hacer clic para seleccionar
Cargue y valide el archivo JSON con la configuración de cumplimiento personalizado
Seleccione un archivo
Estado de dispositivos
Reglas de evaluación del servicio Atestación de estado de Windows
Requerir BitLocker
Requerir
Sin configurar
Debe estar habilitado el arranque seguro en el dispositivo
Requerir
Sin configurar
Requiere integridad de código
Requerir
Sin configurar
Propiedades del dispositivo
Versión del sistema operativo
Versión mínima del sistema operativo
19042.2251
Versión máxima del sistema operativo
Sin configurar
Versión mínima del sistema operativo para dispositivos móviles
Sin configurar
Versión máxima del sistema operativo para dispositivos móviles
Sin configurar
Compilaciones válidas del sistema operativo
Exportar
Sin configurar
Sin configurar
Sin configurar
Cumplimiento de Configuration Manager
Requerir cumplimiento del dispositivo de Configuration Manager
Requerir
Sin configurar
Seguridad del sistema
Contraseña
Requerir una contraseña para desbloquear dispositivos móviles
Requerir
Sin configurar
Contraseñas sencillas
Bloquear
Sin configurar
Tipo de contraseña
Valor predeterminado del dispositivo
Longitud mínima de la contraseña
4
Máximo de minutos de inactividad antes de solicitar la contraseña
15 minutos
Expiración de la contraseña (días)
41
Número de contraseñas anteriores que no se pueden reutilizar
5
Requerir contraseña cuando el dispositivo vuelve de un estado de inactividad (Mobile y Holographic)
Requerir
Sin configurar
Cifrado
Se requiere el cifrado del almacenamiento de datos en el dispositivo.
Requerir
Sin configurar
Seguridad del dispositivo
Firewall
Requerir
Sin configurar
Módulo de plataforma segura (TPM)
Requerir
Sin configurar
Antivirus
Requerir
Sin configurar
Antiespía
Requerir
Sin configurar
Defender
Antimalware de Microsoft defender
Requerir
Sin configurar
Versión mínima de Antimalware de Microsoft Defender
4.18.2109.6
Actualización de la inteligencia de seguridad de Antimalware de Microsoft Defender
Requerir
Sin configurar
Protección en tiempo real
Requerir
Sin configurar
Microsoft Defender for Endpoint
Anterior
Siguiente

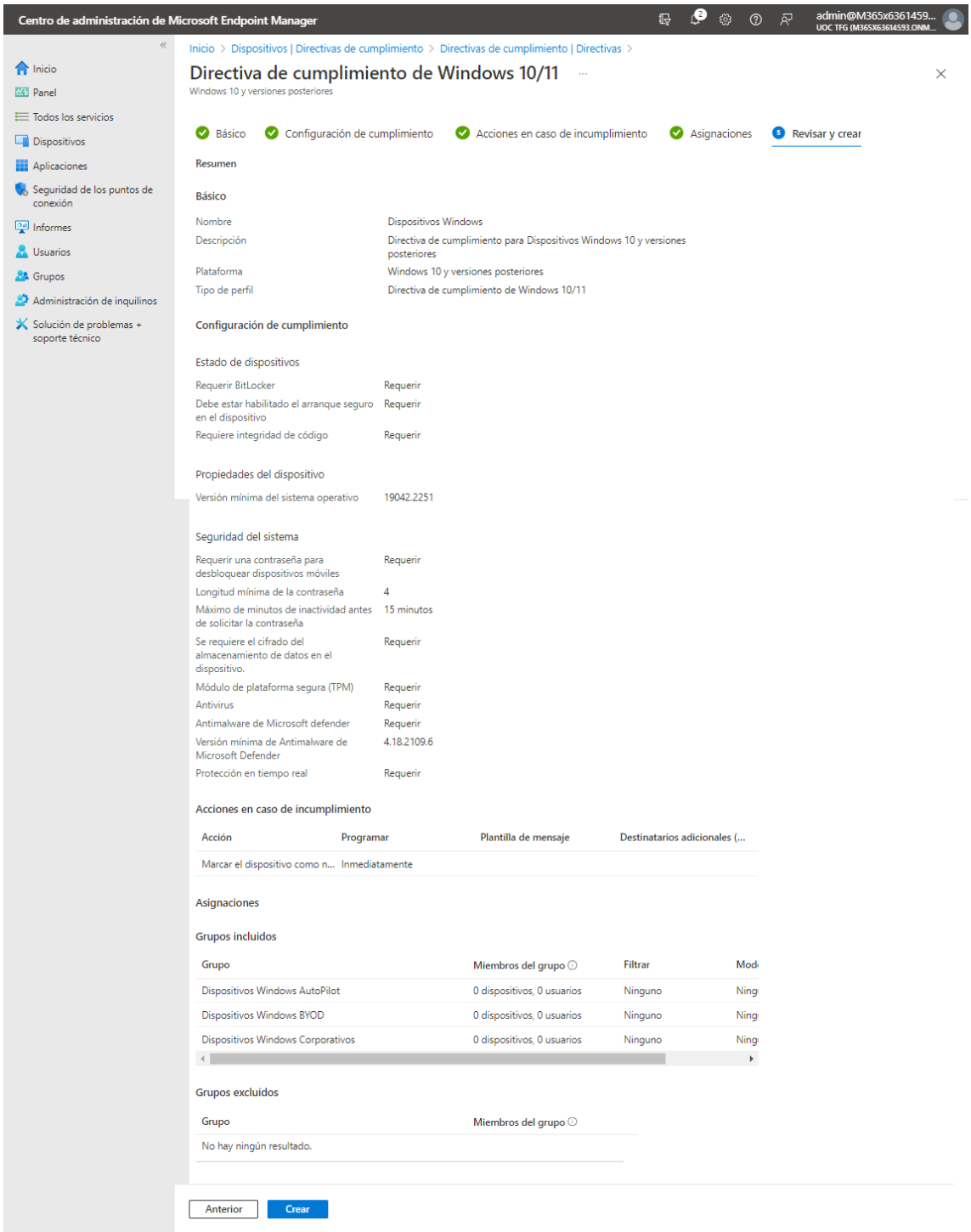
En el tercer paso se configuran las acciones a realizar en caso de incumplimiento, que son marcar el dispositivo como no conforme inmediatamente.



En el cuarto paso se asigna la directiva de cumplimiento a todos los grupos que incluirán dispositivos Windows, es decir, Dispositivos Windows AutoPilot, Dispositivos Windows BYOD y Dispositivos Windows Corporativos.

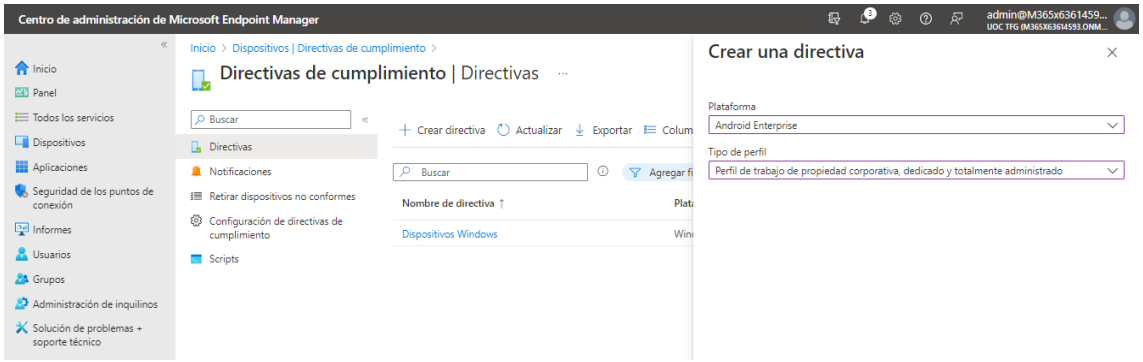


Finalmente, se revisan los detalles de configuración de la directiva de cumplimiento y se crea.

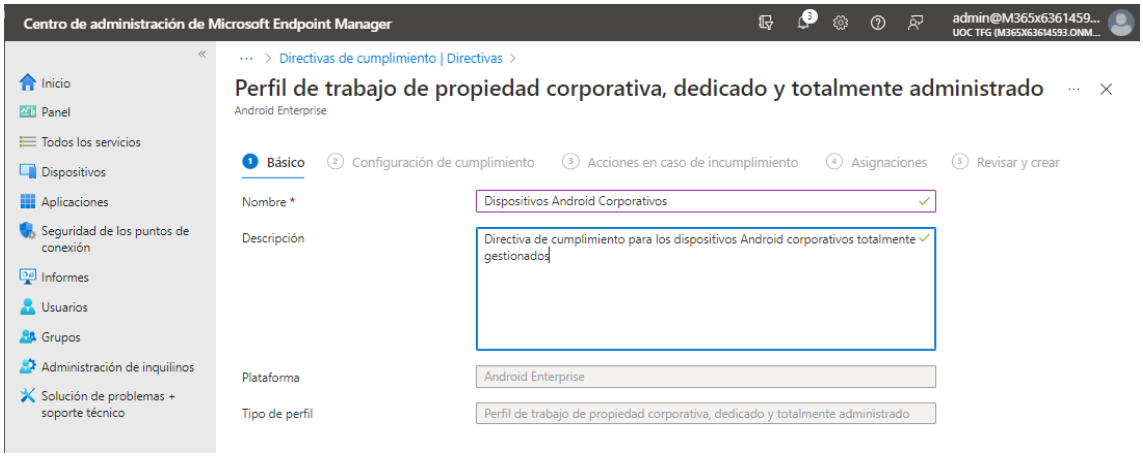

Centro de administración de Microsoft Endpoint Manager
admin@M365x6361459...
UOC TFG (M365X63614593.ONM...
Inicio
Panel
Todos los servicios
Dispositivos
Aplicaciones
Seguridad de los puntos de conexión
Informes
Usuarios
Grupos
Administración de inquilinos
Solución de problemas + soporte técnico
Inicio > Dispositivos | Directivas de cumplimiento > Directivas de cumplimiento | Directivas >
Directiva de cumplimiento de Windows 10/11
Windows 10 y versiones posteriores
Básico
Configuración de cumplimiento
Acciones en caso de incumplimiento
Asignaciones
Revisar y crear
Resumen
Básico
Nombre
Dispositivos Windows
Descripción
Directiva de cumplimiento para Dispositivos Windows 10 y versiones posteriores
Plataforma
Windows 10 y versiones posteriores
Tipo de perfil
Directiva de cumplimiento de Windows 10/11
Configuración de cumplimiento
Estado de dispositivos
Requerir BitLocker
Requerir
Debe estar habilitado el arranque seguro en el dispositivo
Requerir
Requiere integridad de código
Requerir
Propiedades del dispositivo
Versión mínima del sistema operativo
19042.2251
Seguridad del sistema
Requerir una contraseña para desbloquear dispositivos móviles
Requerir
Longitud mínima de la contraseña
4
Máximo de minutos de inactividad antes de solicitar la contraseña
15 minutos
Se requiere el cifrado del almacenamiento de datos en el dispositivo.
Requerir
Módulo de plataforma segura (TPM)
Requerir
Antivirus
Requerir
Antimalware de Microsoft defender
Requerir
Versión mínima de Antimalware de Microsoft Defender
4.18.2109.6
Protección en tiempo real
Requerir
Acciones en caso de incumplimiento
Acción
Programar
Plantilla de mensaje
Destinatarios adicionales (...
Marcar el dispositivo como n...
Inmediatamente
Asignaciones
Grupos incluidos
Grupo
Miembros del grupo
Filtrar
Dispositivos Windows AutoPilot
0 dispositivos, 0 usuarios
Ninguno
Dispositivos Windows BYOD
0 dispositivos, 0 usuarios
Ninguno
Dispositivos Windows Corporativos
0 dispositivos, 0 usuarios
Ninguno
Grupos excluidos
Grupo
Miembros del grupo
No hay ningún resultado.
Anterior
Crear

- **Dispositivos Android Enterprise corporativos**

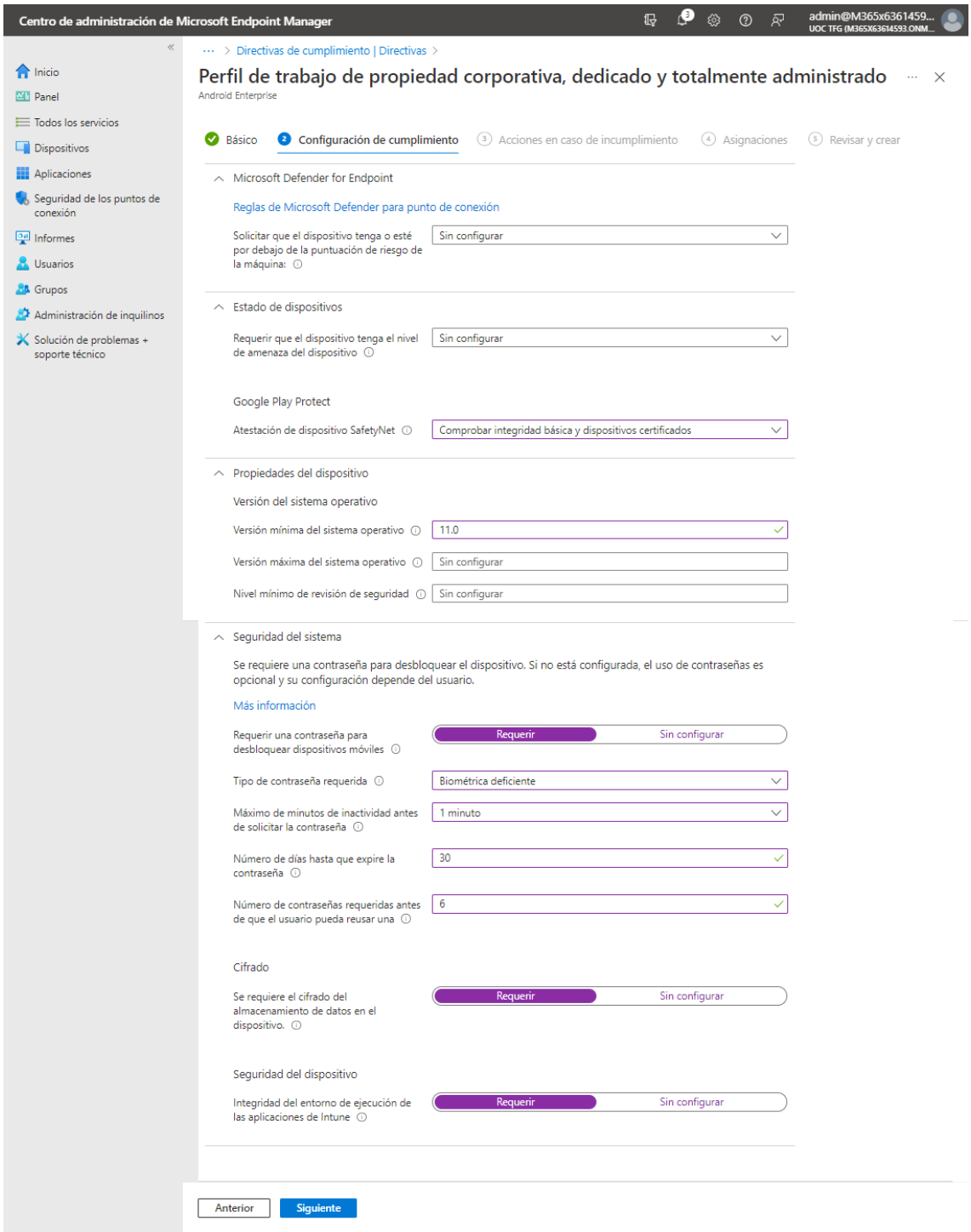
En este caso, al crear la directiva, se selecciona “Android Enterprise” como plataforma y “Perfil de trabajo de propiedad corporativa, dedicado y totalmente administrado” como tipo de perfil.



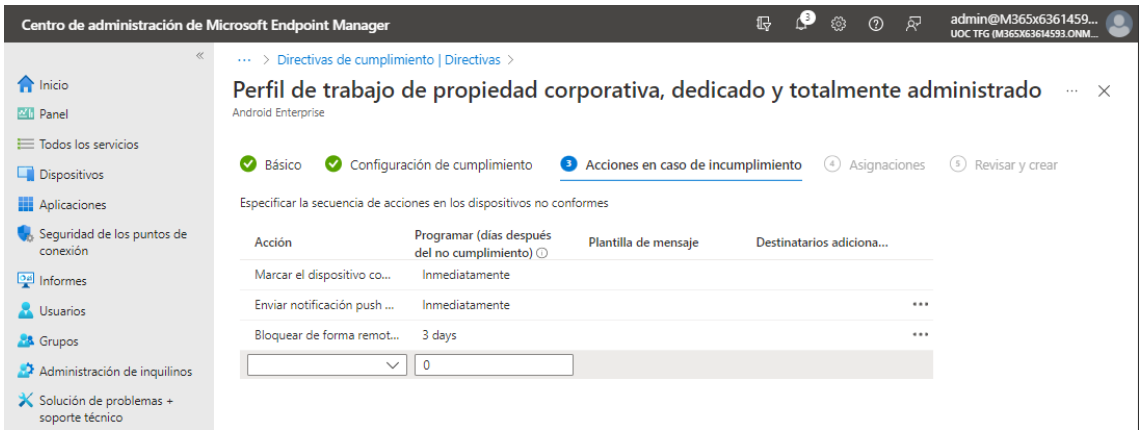
En el primer paso se indica el nombre y la descripción de la directiva.



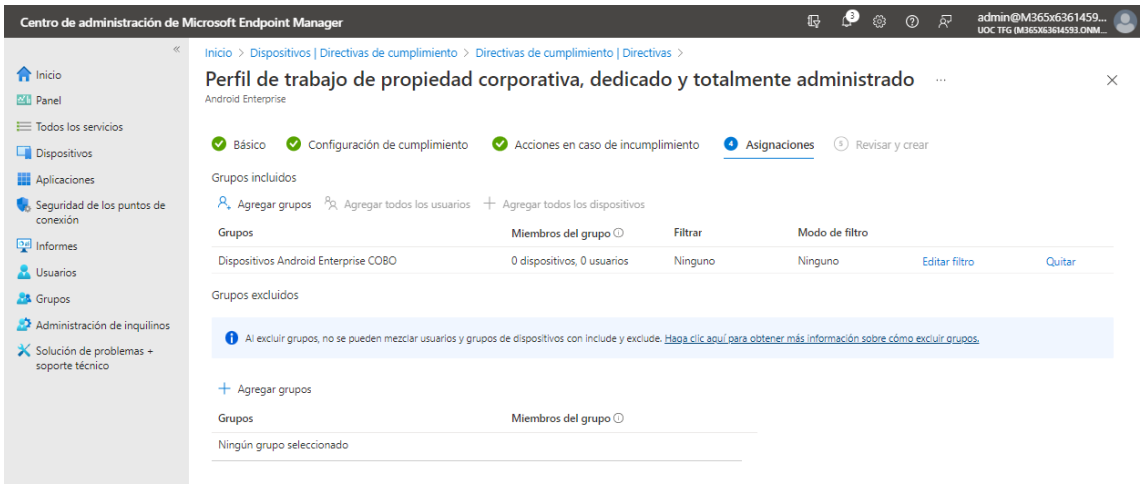
En el segundo paso se configuran los parámetros que los dispositivos deben cumplir para ser conformes. En este caso, se requiere que la versión mínima de sistema operativo sea la 11.0 (publicada en septiembre de 2020), que el dispositivo esté protegido mediante contraseña y biometría, con un periodo de inactividad de 1 minuto hasta bloquearse, que la contraseña expire cada 30 días y no se puedan reutilizar las 6 anteriores, y que tanto el cifrado del almacenamiento del dispositivo como la integridad del entorno de ejecución de las aplicaciones de Intune estén habilitados.



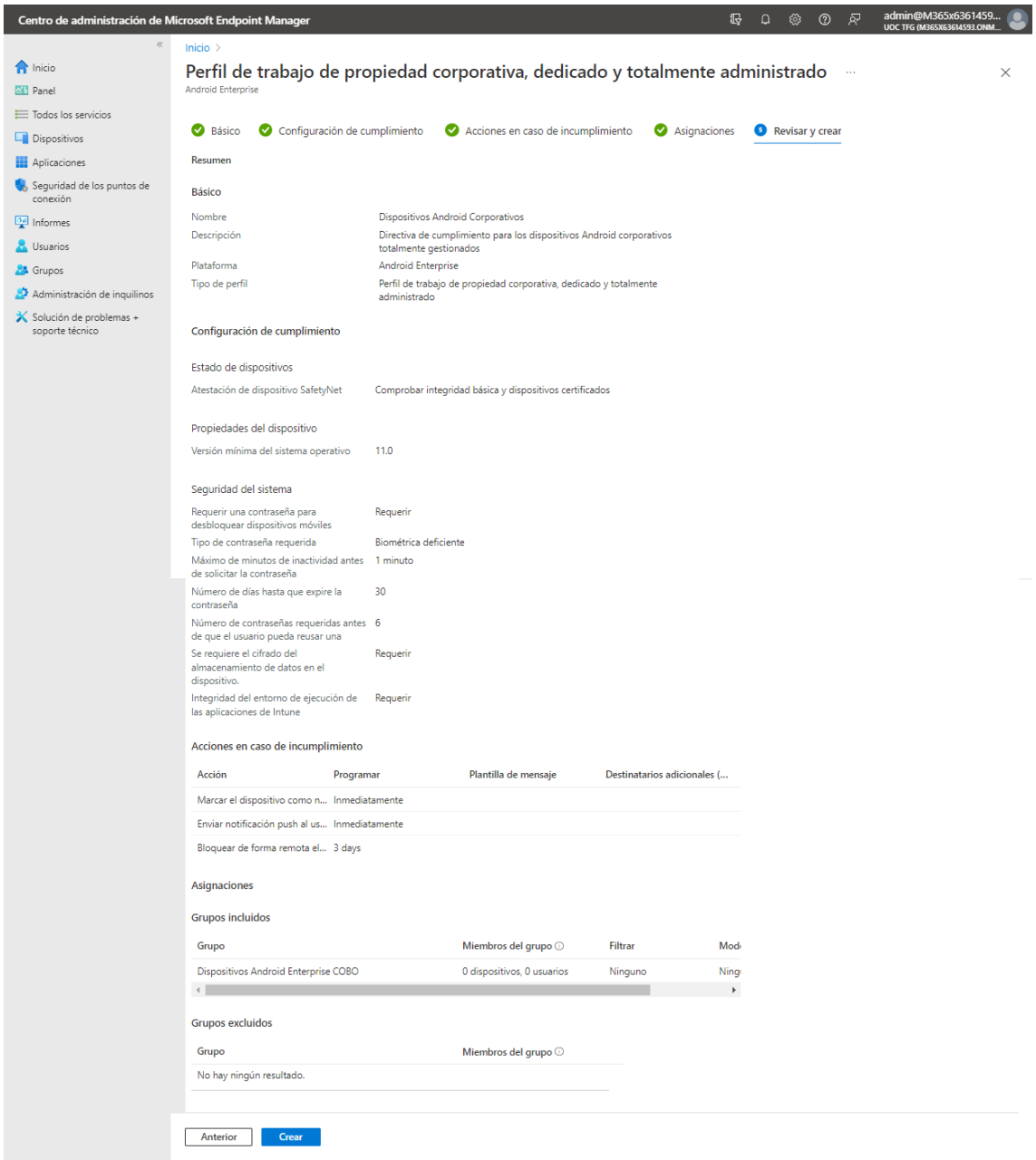
En el tercer paso de creación de la directiva se configuran las acciones a realizar por Intune en caso de no que esta no se cumpla: marcar inmediatamente el dispositivo como no conforme, enviar una notificación push al usuario y bloquear el dispositivo de forma remota si pasados 3 días se mantiene como no conforme.



En el cuarto paso, se asigna la directiva al grupo en el cual se encontrarán los dispositivos y usuarios sobre los que se aplicará: Dispositivos Android Enterprise COBO.

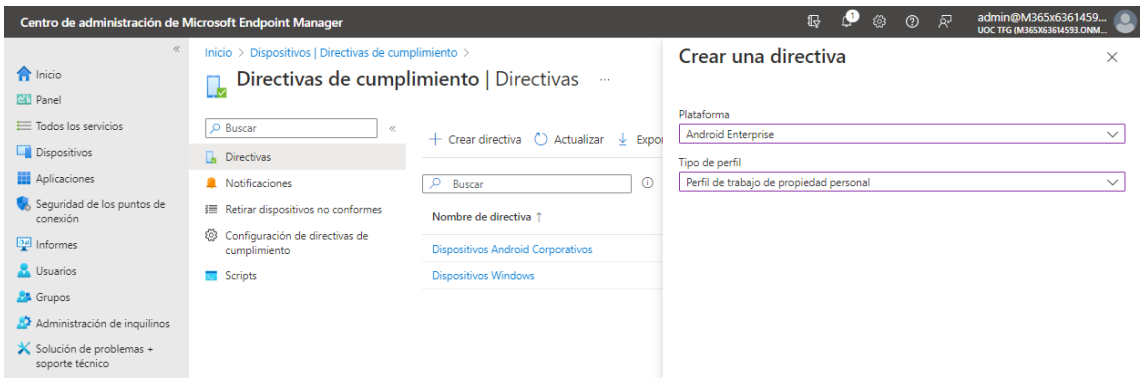


Por último, se revisan los detalles de la directiva y se realiza la creación.

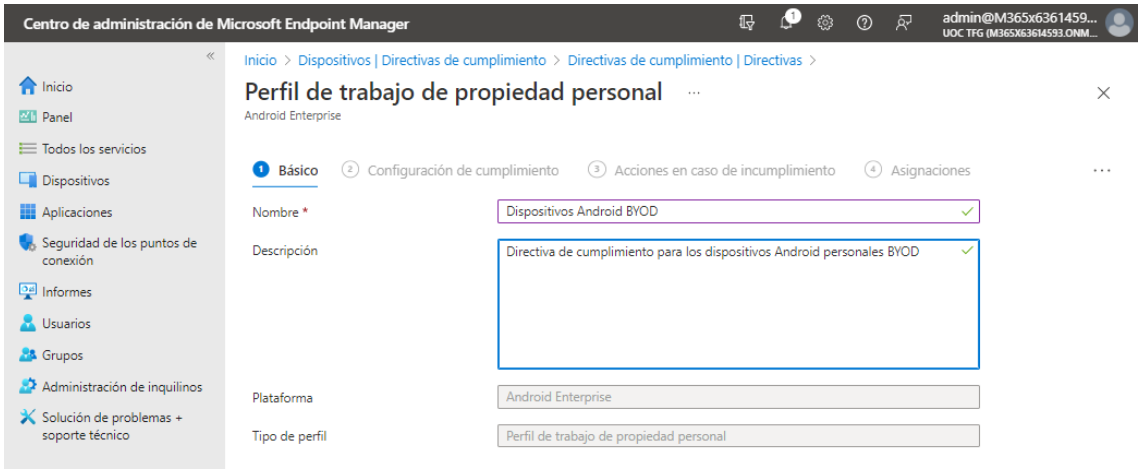

Centro de administración de Microsoft Endpoint Manager
admin@M365x6361459...
UOC TFG (M365X63614593.ONM...
Inicio
Panel
Todos los servicios
Dispositivos
Aplicaciones
Seguridad de los puntos de conexión
Informes
Usuarios
Grupos
Administración de inquilinos
Solución de problemas + soporte técnico
Inicio >
Perfil de trabajo de propiedad corporativa, dedicado y totalmente administrado
Android Enterprise
Básico
Configuración de cumplimiento
Acciones en caso de incumplimiento
Asignaciones
Revisar y crear
Resumen
Básico
Nombre
Dispositivos Android Corporativos
Descripción
Directiva de cumplimiento para los dispositivos Android corporativos totalmente gestionados
Plataforma
Android Enterprise
Tipo de perfil
Perfil de trabajo de propiedad corporativa, dedicado y totalmente administrado
Configuración de cumplimiento
Estado de dispositivos
Atestación de dispositivo SafetyNet
Comprobar integridad básica y dispositivos certificados
Propiedades del dispositivo
Versión mínima del sistema operativo
11.0
Seguridad del sistema
Requerir una contraseña para desbloquear dispositivos móviles
Requerir
Tipo de contraseña requerida
Biométrica deficiente
Máximo de minutos de inactividad antes de solicitar la contraseña
1 minuto
Número de días hasta que expire la contraseña
30
Número de contraseñas requeridas antes de que el usuario pueda reusar una
6
Se requiere el cifrado del almacenamiento de datos en el dispositivo.
Requerir
Integridad del entorno de ejecución de las aplicaciones de Intune
Requerir
Acciones en caso de incumplimiento
Acción
Programar
Plantilla de mensaje
Destinatarios adicionales (...
Marcar el dispositivo como n...
Inmediatamente
Enviar notificación push al us...
Inmediatamente
Bloquear de forma remota el...
3 days
Asignaciones
Grupos incluidos
Grupo
Miembros del grupo
Filtrar
Dispositivos Android Enterprise COBO
0 dispositivos, 0 usuarios
Ninguno
Grupos excluidos
Grupo
Miembros del grupo
No hay ningún resultado.
Anterior
Crear

Dispositivos Android Enterprise BYOD

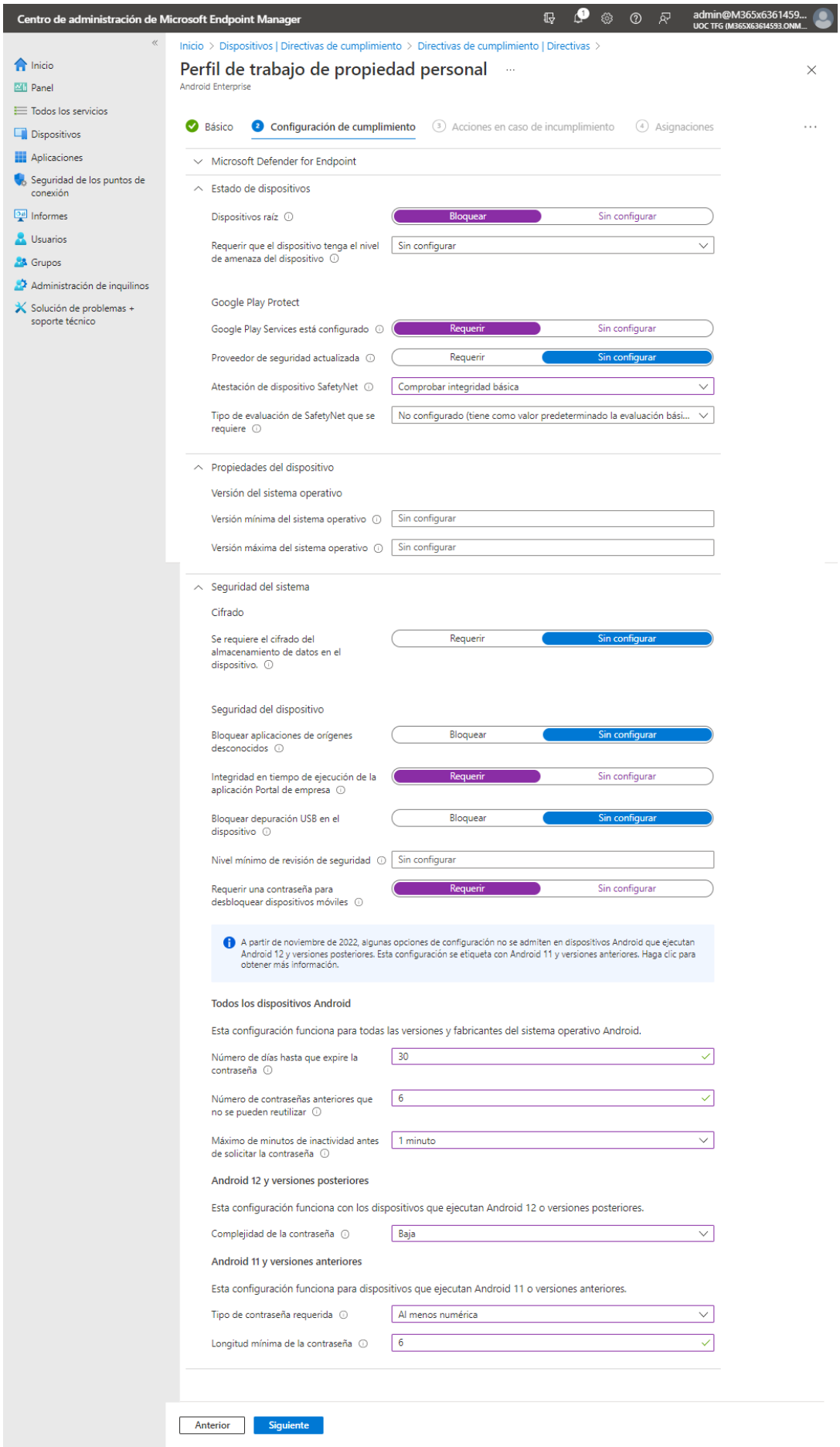
Para los dispositivos Android Enterprise BYOD, al crear la directiva, se selecciona “Android Enterprise” como plataforma y “Perfil de trabajo de propiedad personal” como tipo de perfil.



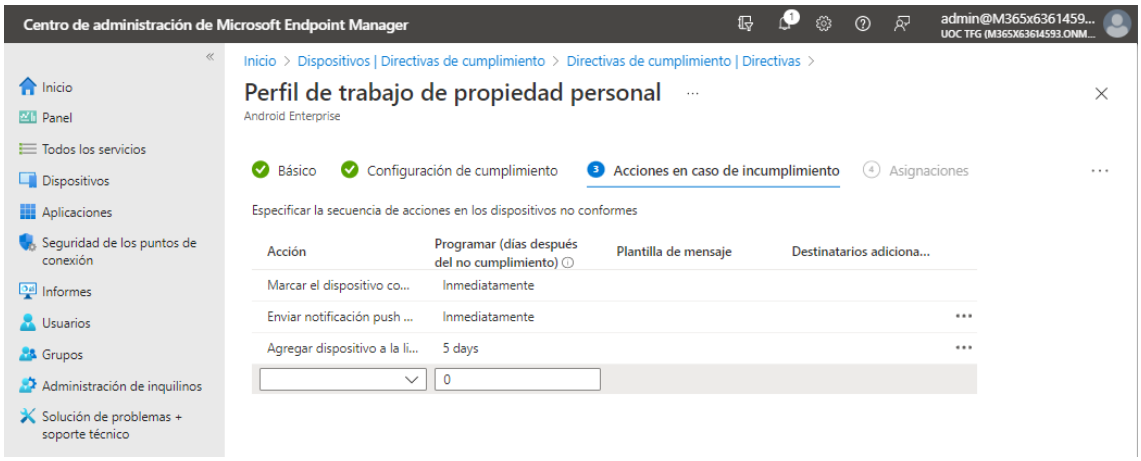
Como es habitual, en el primer paso se indica el nombre y la descripción de la directiva.



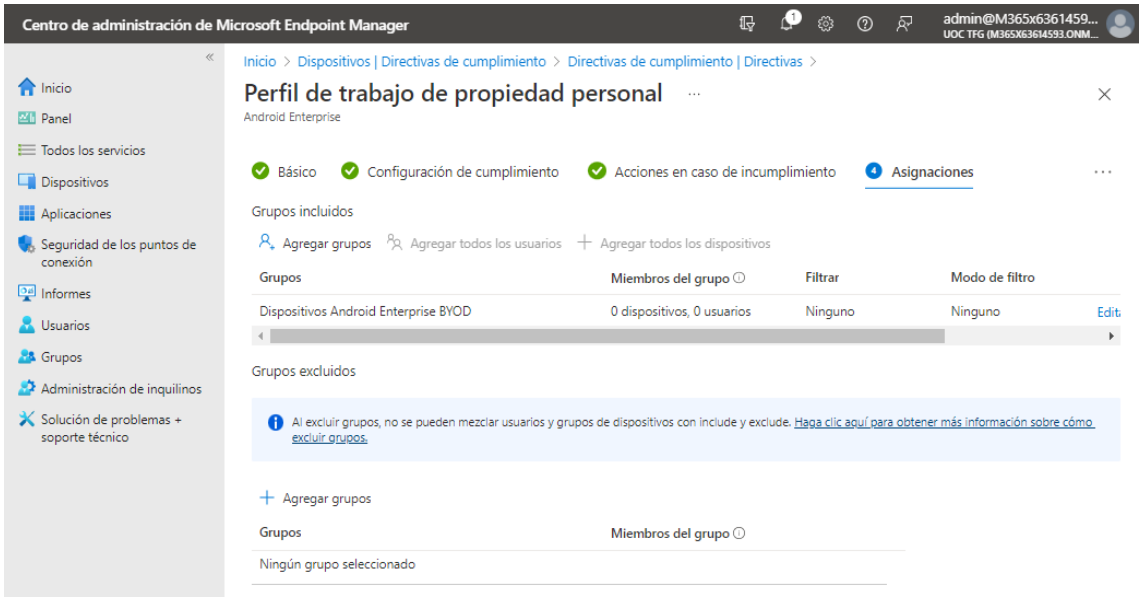
En el segundo paso, se especifican los requisitos que deben cumplir los dispositivos a los que vaya destinada la directiva de cumplimiento. A grandes rasgos, se bloqueadn los dispositivos que estén liberados (con acceso root), se requiere que Google Play Services esté configurado y que la atestación de dispositivo Safetynet compruebe la integridad básica, que la integridad en tiempo de ejecución de la aplicación Portal de empresa esté habilitada y que el dispositivo disponga de una contraseña al menos numérica de mínimo 6 dígitos.


Centro de administración de Microsoft Endpoint Manager
admin@M365x6361459...
UOC TFG (M365X63614593.ONM...
Inicio
Panel
Todos los servicios
Dispositivos
Aplicaciones
Seguridad de los puntos de conexión
Informes
Usuarios
Grupos
Administración de inquilinos
Solución de problemas + soporte técnico
Inicio > Dispositivos | Directivas de cumplimiento > Directivas de cumplimiento | Directivas >
Perfil de trabajo de propiedad personal
Android Enterprise
Básico
Configuración de cumplimiento
Acciones en caso de incumplimiento
Asignaciones
Microsoft Defender for Endpoint
Estado de dispositivos
Dispositivos raíz
Bloquear
Sin configurar
Requerir que el dispositivo tenga el nivel de amenaza del dispositivo
Sin configurar
Google Play Protect
Google Play Services está configurado
Requerir
Sin configurar
Proveedor de seguridad actualizada
Requerir
Sin configurar
Atestación de dispositivo SafetyNet
Comprobar integridad básica
Tipo de evaluación de SafetyNet que se requiere
No configurado (tiene como valor predeterminado la evaluación básí...
Propiedades del dispositivo
Versión del sistema operativo
Versión mínima del sistema operativo
Sin configurar
Versión máxima del sistema operativo
Sin configurar
Seguridad del sistema
Cifrado
Se requiere el cifrado del almacenamiento de datos en el dispositivo.
Requerir
Sin configurar
Seguridad del dispositivo
Bloquear aplicaciones de orígenes desconocidos
Bloquear
Sin configurar
Integridad en tiempo de ejecución de la aplicación Portal de empresa
Requerir
Sin configurar
Bloquear depuración USB en el dispositivo
Bloquear
Sin configurar
Nivel mínimo de revisión de seguridad
Sin configurar
Requerir una contraseña para desbloquear dispositivos móviles
Requerir
Sin configurar
A partir de noviembre de 2022, algunas opciones de configuración no se admiten en dispositivos Android que ejecutan Android 12 y versiones posteriores. Esta configuración se etiqueta con Android 11 y versiones anteriores. Haga clic para obtener más información.
Todos los dispositivos Android
Esta configuración funciona para todas las versiones y fabricantes del sistema operativo Android.
Número de días hasta que expire la contraseña
30
Número de contraseñas anteriores que no se pueden reutilizar
6
Máximo de minutos de inactividad antes de solicitar la contraseña
1 minuto
Android 12 y versiones posteriores
Esta configuración funciona con los dispositivos que ejecutan Android 12 o versiones posteriores.
Complejidad de la contraseña
Baja
Android 11 y versiones anteriores
Esta configuración funciona para dispositivos que ejecutan Android 11 o versiones anteriores.
Tipo de contraseña requerida
Al menos numérica
Longitud mínima de la contraseña
6
Anterior
Siguiente

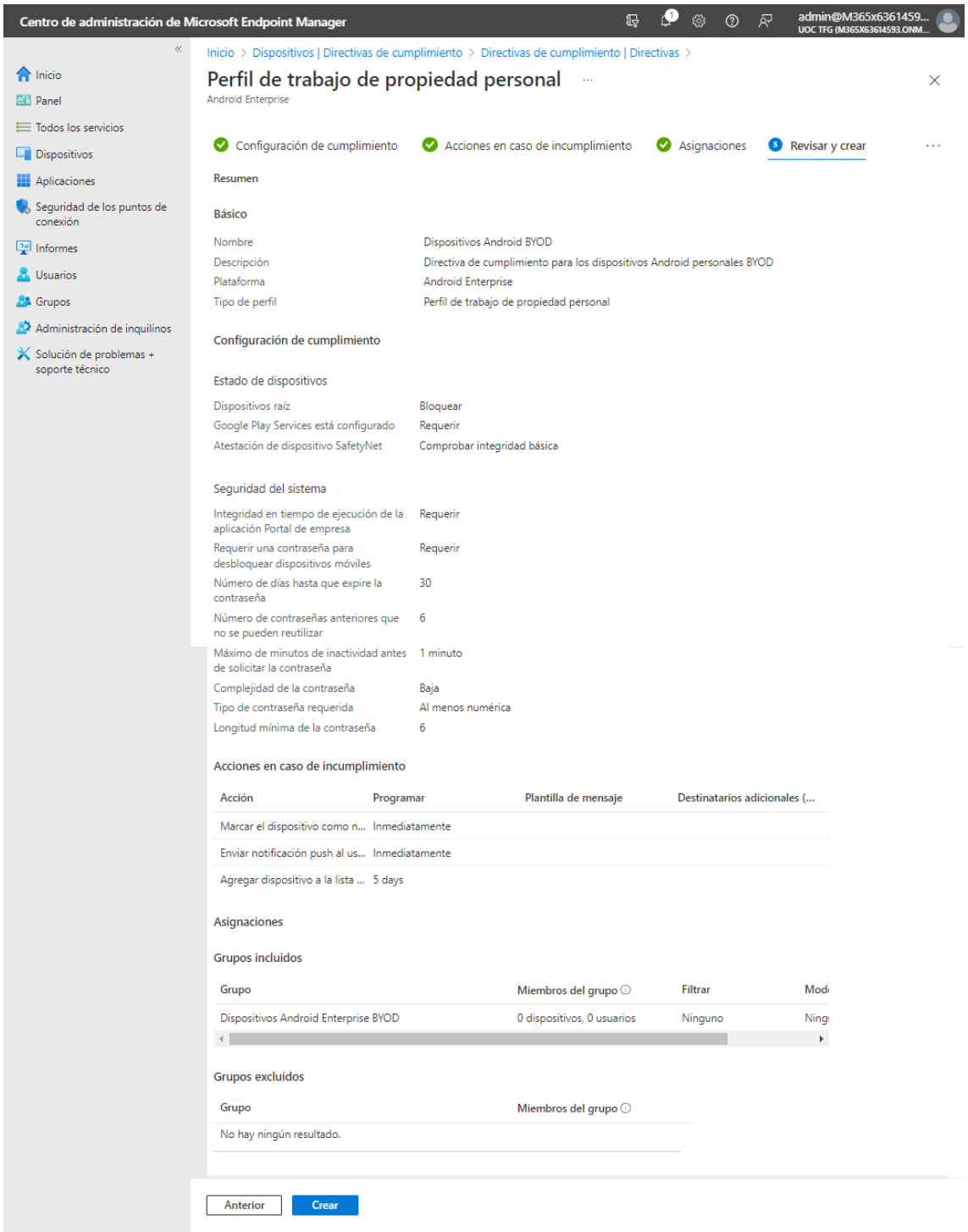
En el tercer paso, se configuran las acciones en caso de incumplimiento de la directiva: marcar inmediatamente el dispositivo como no conforme y enviar notificación push al usuario, y agregar el dispositivo a la lista de retirada pasados 5 días.



En el cuarto paso, se agregan los grupos a los que se aplicará la directiva de cumplimiento: Dispositivos Android Enterprise BYOD.

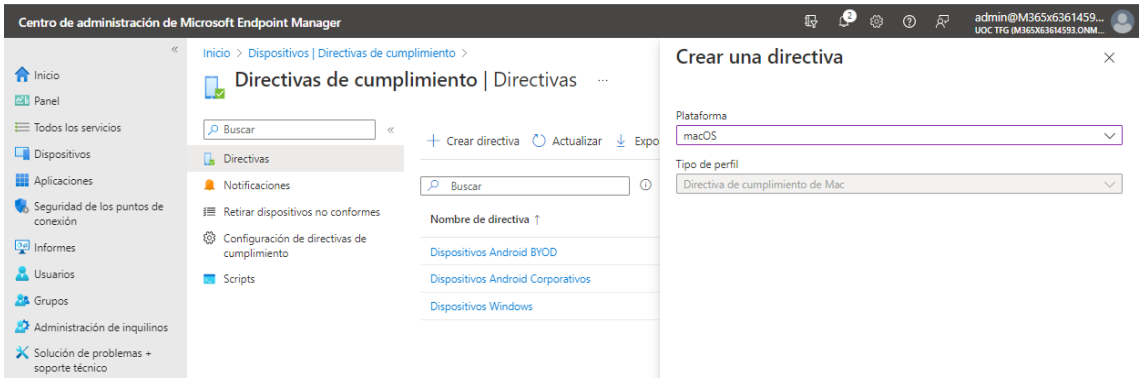


Para finalizar, se revisan los detalles de la directiva y se realiza la creación de esta.

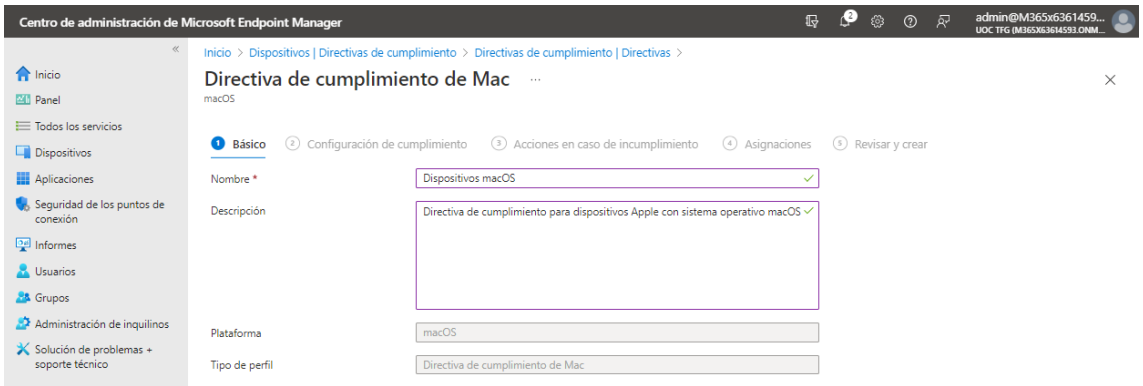

Centro de administración de Microsoft Endpoint Manager
admin@M365x6361459...
UOC TFG (M365X63614593.ONM...
Inicio
Panel
Todos los servicios
Dispositivos
Aplicaciones
Seguridad de los puntos de conexión
Informes
Usuarios
Grupos
Administración de inquilinos
Solución de problemas + soporte técnico
Inicio > Dispositivos | Directivas de cumplimiento > Directivas de cumplimiento | Directivas >
Perfil de trabajo de propiedad personal
Android Enterprise
Configuración de cumplimiento
Acciones en caso de incumplimiento
Asignaciones
Revisar y crear
Resumen
Básico
Nombre Dispositivos Android BYOD
Descripción Directiva de cumplimiento para los dispositivos Android personales BYOD
Plataforma Android Enterprise
Tipo de perfil Perfil de trabajo de propiedad personal
Configuración de cumplimiento
Estado de dispositivos
Dispositivos raíz Bloquear
Google Play Services está configurado Requerir
Atestación de dispositivo SafetyNet Comprobar integridad básica
Seguridad del sistema
Integridad en tiempo de ejecución de la aplicación Portal de empresa Requerir
Requerir una contraseña para desbloquear dispositivos móviles Requerir
Número de días hasta que expire la contraseña 30
Número de contraseñas anteriores que no se pueden reutilizar 6
Máximo de minutos de inactividad antes de solicitar la contraseña 1 minuto
Complejidad de la contraseña Baja
Tipo de contraseña requerida Al menos numérica
Longitud mínima de la contraseña 6
Acciones en caso de incumplimiento
Acción Programar Plantilla de mensaje Destinatarios adicionales (...
Marcar el dispositivo como n... Inmediatamente
Enviar notificación push al us... Inmediatamente
Agregar dispositivo a la lista ... 5 days
Asignaciones
Grupos incluidos
Grupo Miembros del grupo Filtrar
Dispositivos Android Enterprise BYOD 0 dispositivos, 0 usuarios Ninguno
Grupos excluidos
Grupo Miembros del grupo
No hay ningún resultado.
Anterior
Crear

- **Dispositivos Apple macOS**

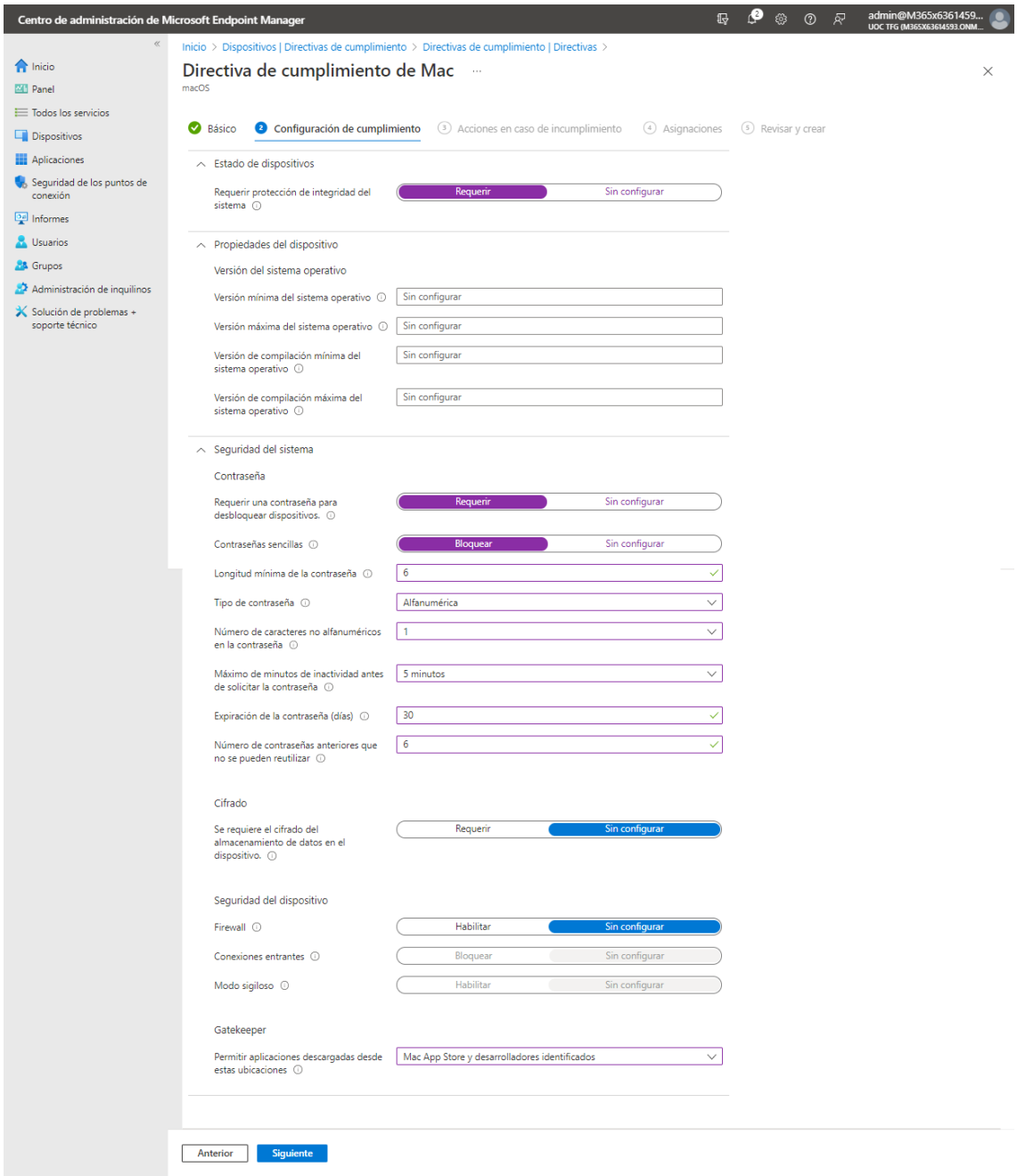
Para crear la directiva de los dispositivos Apple con sistema operativo macOS es necesario seleccionar macOS en la plataforma.



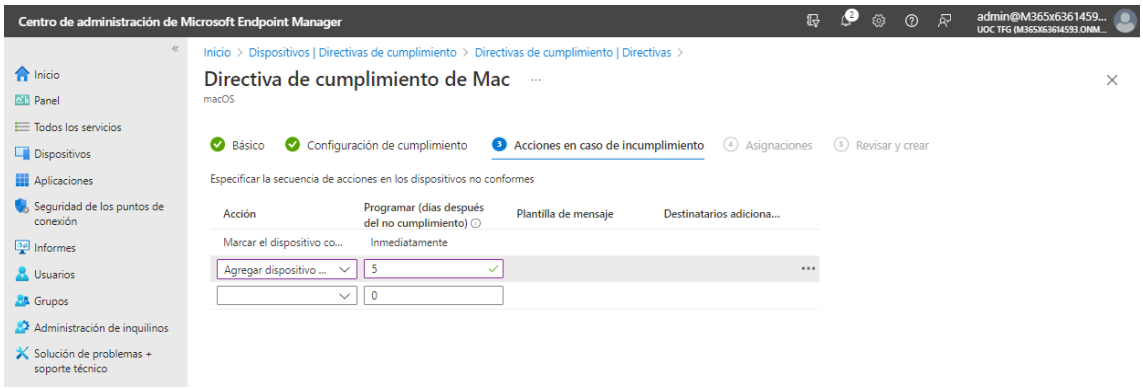
De igual forma que en las directivas creadas anteriormente, en el primer paso se indican el nombre y la descripción de la directiva.



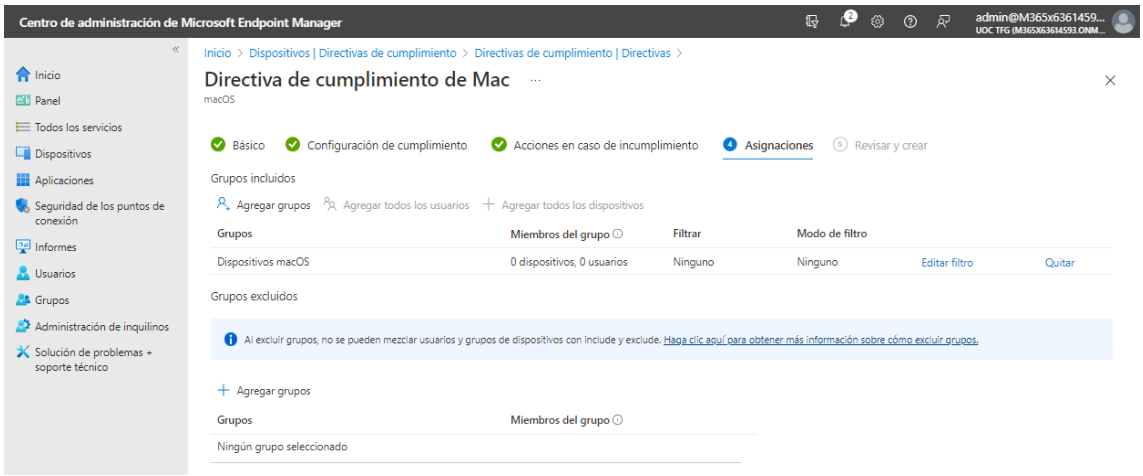
En el segundo paso, se especifican las configuraciones requeridas de la directiva. La política de contraseñas configurada es la misma que para el resto de dispositivos ya configurados anteriormente. Además, se requiere protección de integridad del sistema y solo se permiten las aplicaciones descargadas desde Mac App Store y de desarrolladores identificados.



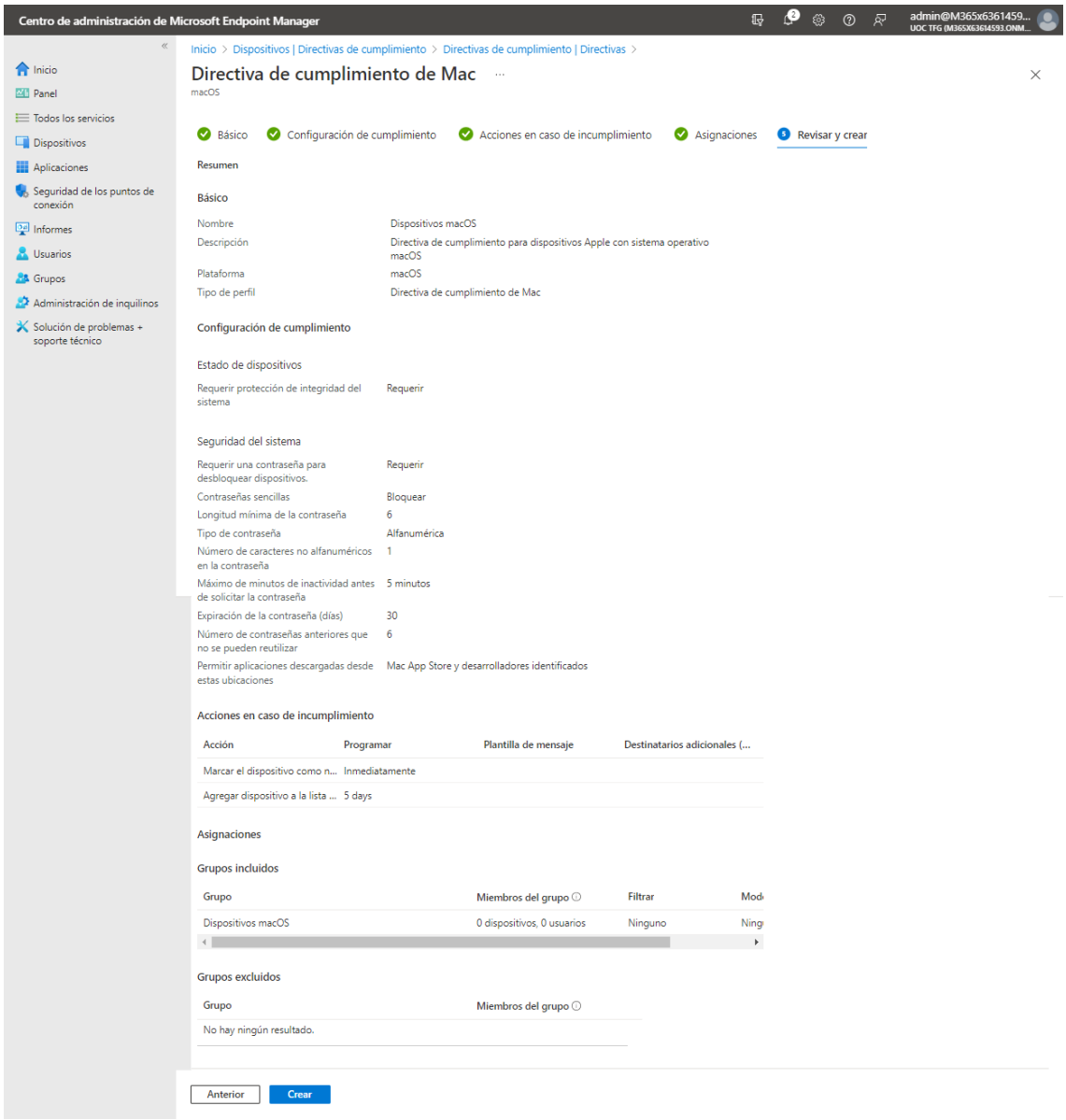
En el paso 3, se definen las acciones en caso de incumplimiento: marcar el dispositivo como no conforme inmediatamente y agregarlo a la lista de retirada si pasados 5 días se mantiene como no conforme.



En el paso 4 se asignan los grupos a los que se les aplicará la directiva de cumplimiento y los que estarán excluidos. En este caso, la directiva se aplicará al grupo “Dispositivos macOS”.

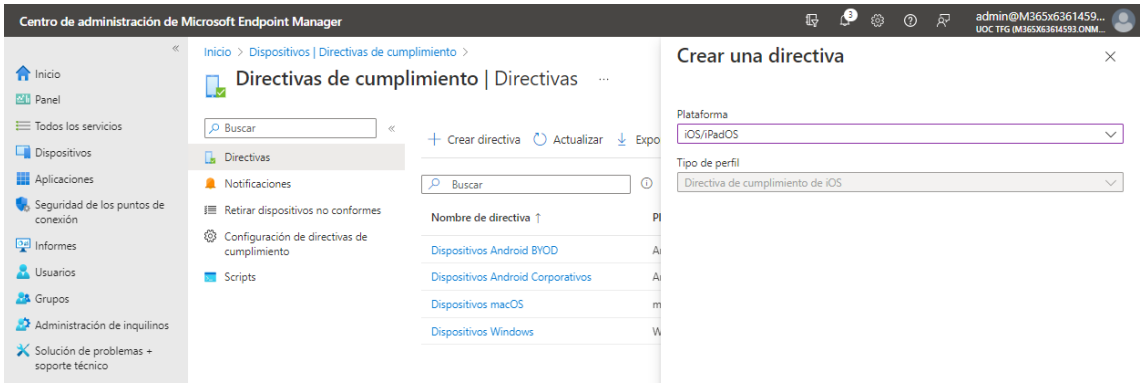


Por último, se revisan los detalles de la directiva de cumplimiento y se ordena la creación.


Centro de administración de Microsoft Endpoint Manager
admin@M365x6361459...
UOC TFG (M365X63614593.ONM...
Inicio
Panel
Todos los servicios
Dispositivos
Aplicaciones
Seguridad de los puntos de conexión
Informes
Usuarios
Grupos
Administración de inquilinos
Solución de problemas + soporte técnico
Inicio > Dispositivos | Directivas de cumplimiento > Directivas de cumplimiento | Directivas >
Directiva de cumplimiento de Mac
macOS
Básico
Configuración de cumplimiento
Acciones en caso de incumplimiento
Asignaciones
Revisar y crear
Resumen
Básico
Nombre
Dispositivos macOS
Descripción
Directiva de cumplimiento para dispositivos Apple con sistema operativo macOS
Plataforma
macOS
Tipo de perfil
Directiva de cumplimiento de Mac
Configuración de cumplimiento
Estado de dispositivos
Requerir protección de integridad del sistema
Requerir
Seguridad del sistema
Requerir una contraseña para desbloquear dispositivos.
Requerir
Contraseñas sencillas
Bloquear
Longitud mínima de la contraseña
6
Tipo de contraseña
Alfanumérica
Número de caracteres no alfanuméricos en la contraseña
1
Máximo de minutos de inactividad antes de solicitar la contraseña
5 minutos
Expiración de la contraseña (días)
30
Número de contraseñas anteriores que no se pueden reutilizar
6
Permitir aplicaciones descargadas desde estas ubicaciones
Mac App Store y desarrolladores identificados
Acciones en caso de incumplimiento
Acción
Programar
Plantilla de mensaje
Destinatarios adicionales (...
Marcar el dispositivo como n...
Inmediatamente
Agregar dispositivo a la lista ...
5 days
Asignaciones
Grupos incluidos
Grupo
Miembros del grupo
Filtrar
Dispositivos macOS
0 dispositivos, 0 usuarios
Ninguno
Grupos excluidos
Grupo
Miembros del grupo
No hay ningún resultado.
Anterior
Crear

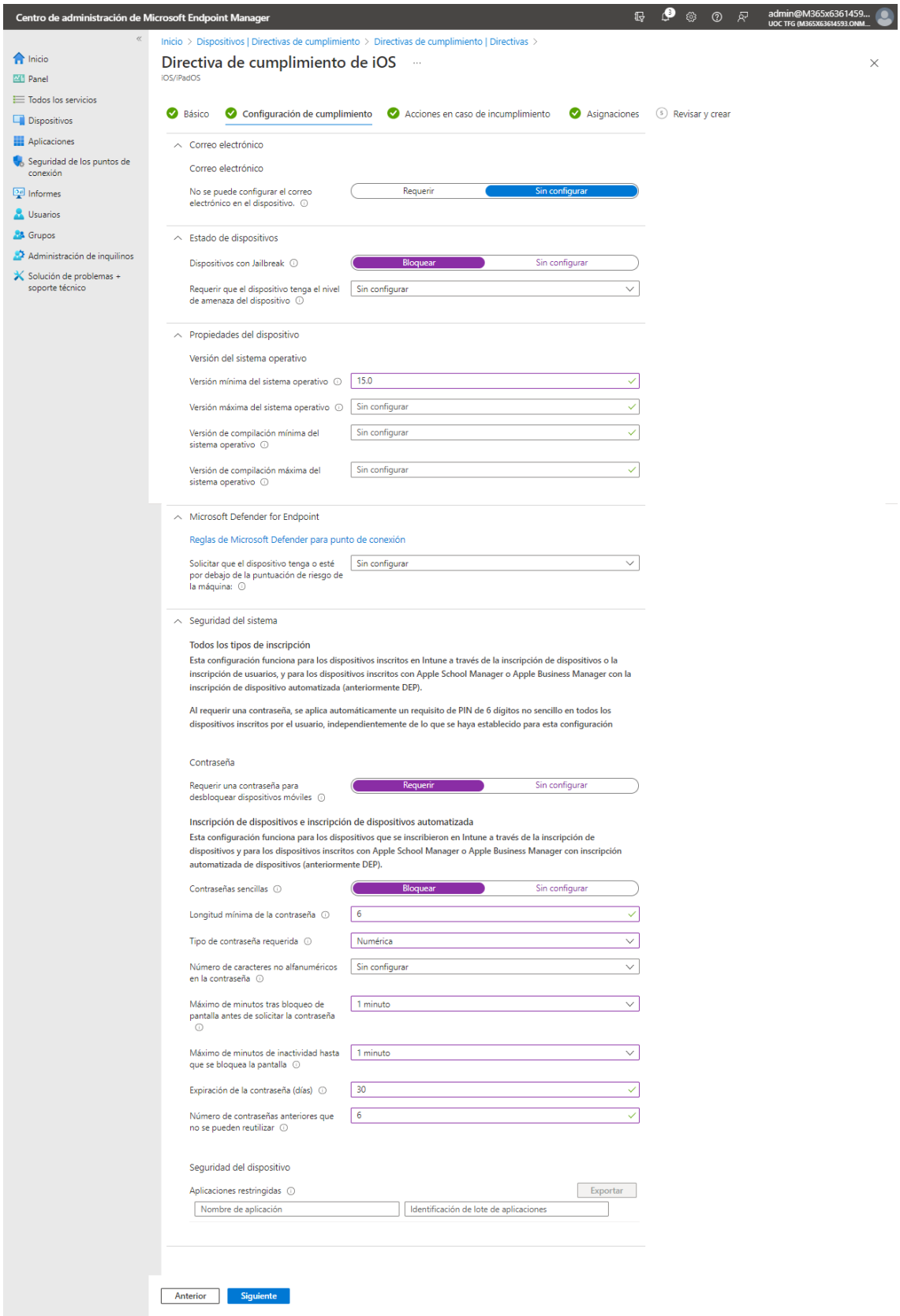
- **Dispositivos Apple iOS e iPadOS**

Al crear la nueva directiva de cumplimiento se debe seleccionar “iOS/iPadOS” como Plataforma.



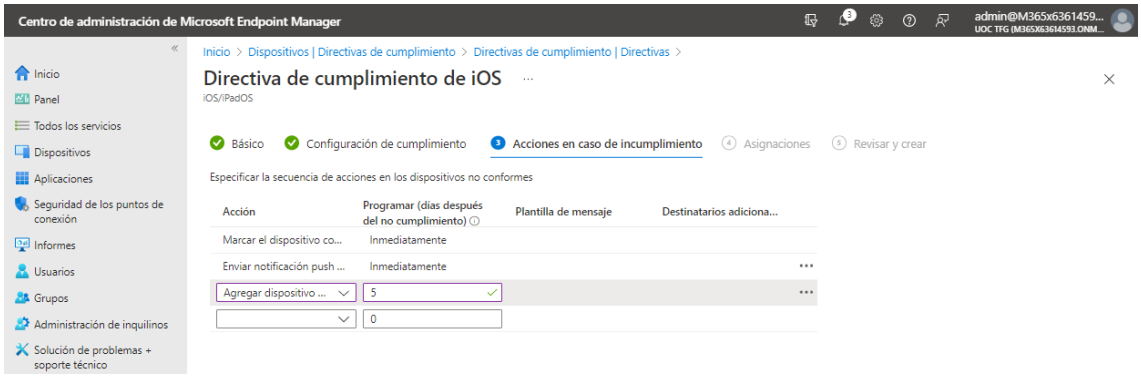
En el primer paso, se indica el nombre y la descripción de la directiva.

En el segundo paso se configuran los requisitos que deben cumplir los dispositivos. La política de contraseñas requerida es la misma que en los demás perfiles, a excepción de que no se requieren caracteres alfanuméricos al tratarse de dispositivos móviles. Además, no se permiten los dispositivos liberados (jailbreak) y la versión de sistema operativo mínima es la 15.0 (publicada en 2021 y aplicable a dispositivos iPhone a partir del 6S e iPad a partir del Air 2, lanzados en 2015 y 2014 respectivamente).

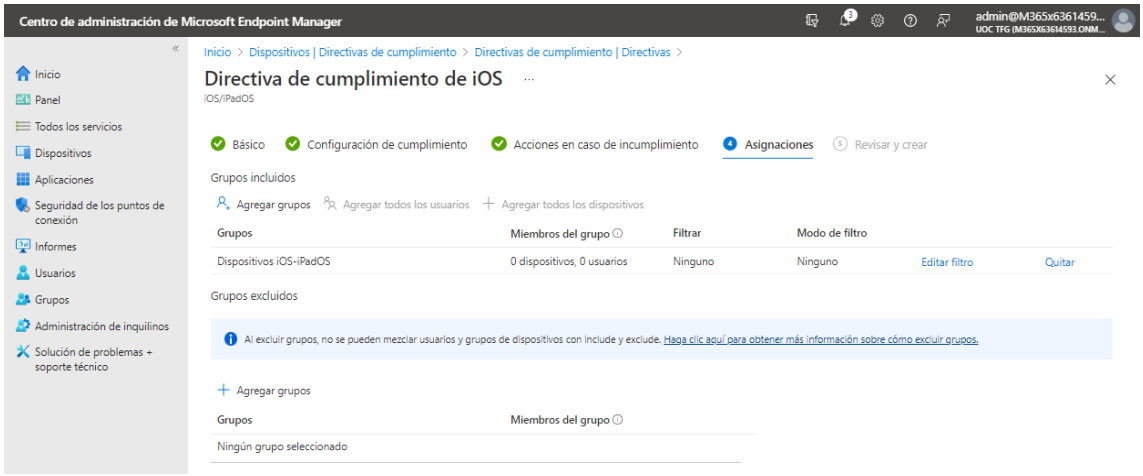


En el tercer paso, se especifican las acciones a realizar en caso de incumplimiento de la directa: marcar el dispositivo inmediatamente como no

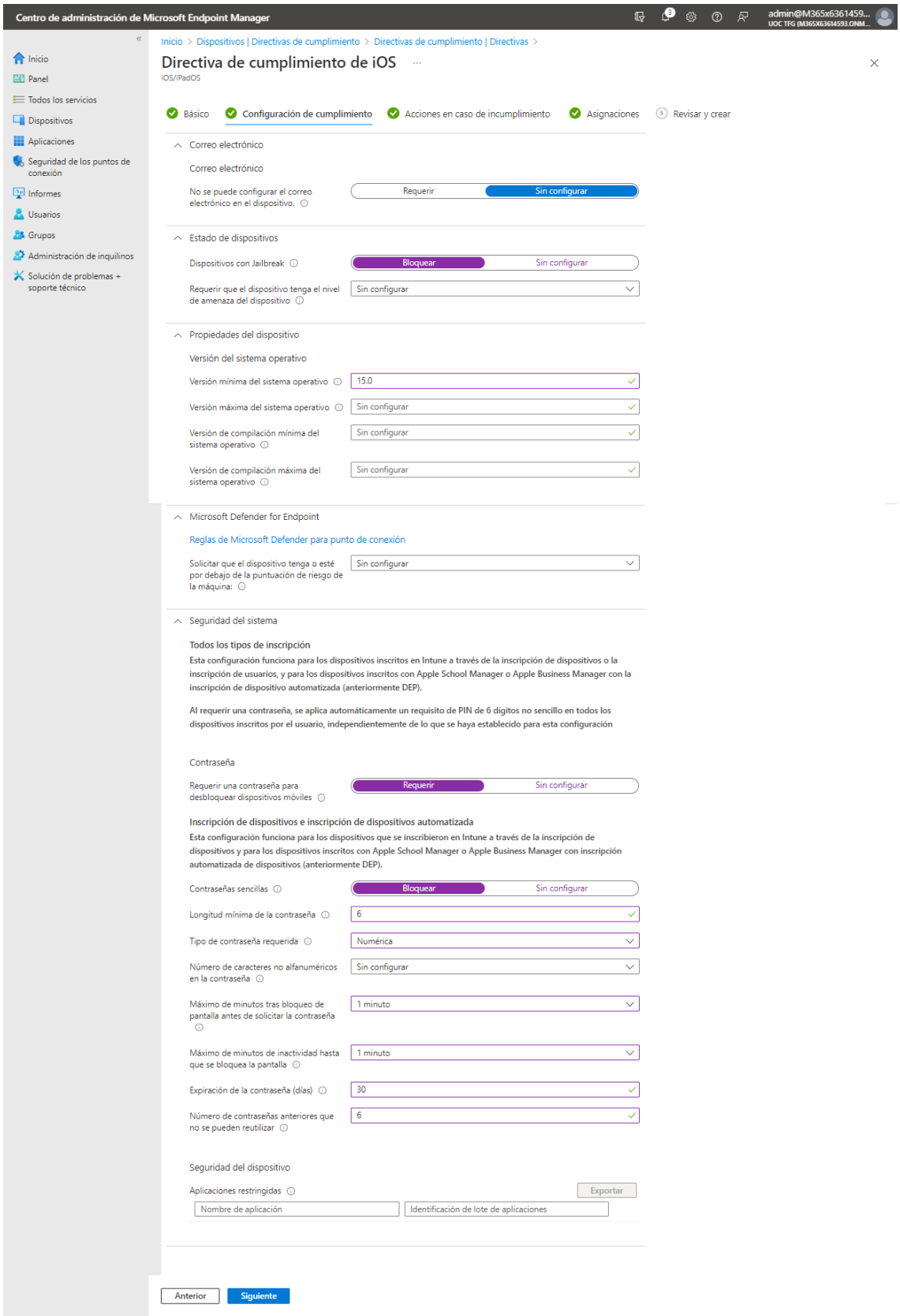
conforme y enviar notificación push al usuario, y agregar el dispositivo a la lista de retirada si se mantiene como no conforme pasados 5 días.



En el cuarto paso, se asigna la directiv al grupo sobre el que se aplicará: “Dispositivos iOS-iPadOS”.

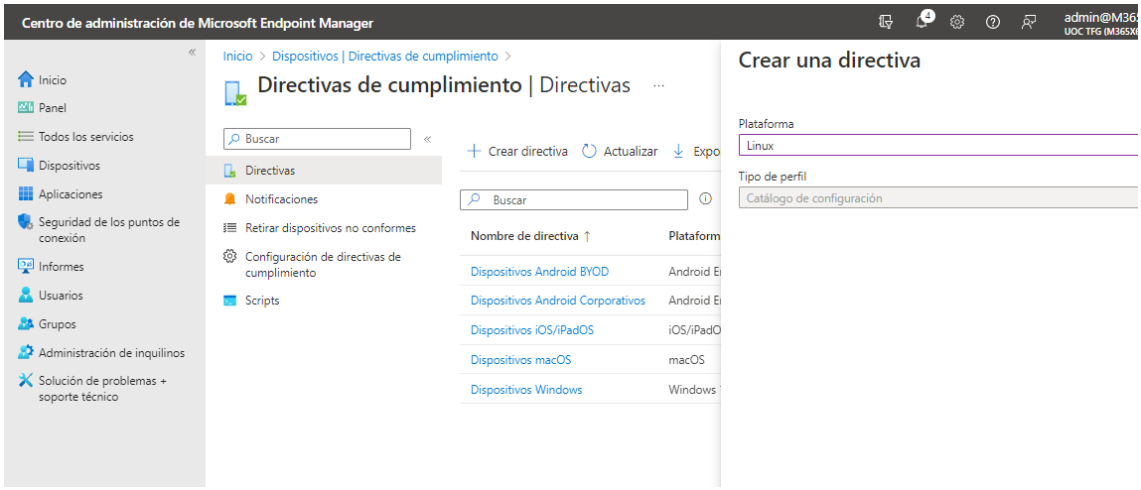


Por último, se revisan los detalles de la directiva y se realiza la creación.

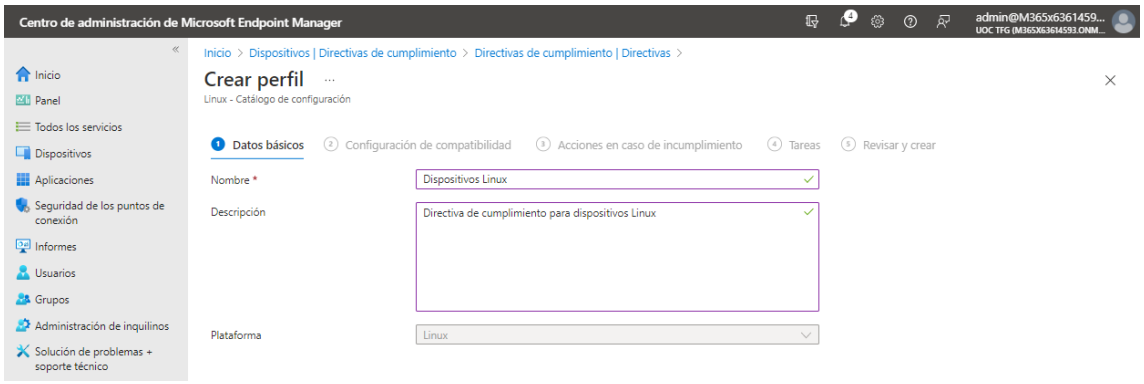

Centro de administración de Microsoft Endpoint Manager
admin@M365x6361459...
UOC TFG (M365X6361459.ONM...
Inicio
Panel
Todos los servicios
Dispositivos
Aplicaciones
Seguridad de los puntos de conexión
Informes
Usuarios
Grupos
Administración de inquilinos
Solución de problemas + soporte técnico
Inicio > Dispositivos | Directivas de cumplimiento > Directivas de cumplimiento | Directivas >
Directiva de cumplimiento de iOS
iOS/iPadOS
Básico
Configuración de cumplimiento
Acciones en caso de incumplimiento
Asignaciones
Revisar y crear
Correo electrónico
Correo electrónico
No se puede configurar el correo electrónico en el dispositivo.
Requerir
Sin configurar
Estado de dispositivos
Dispositivos con Jailbreak
Bloquear
Sin configurar
Requerir que el dispositivo tenga el nivel de amenaza del dispositivo
Sin configurar
Propiedades del dispositivo
Versión del sistema operativo
Versión mínima del sistema operativo
15.0
Versión máxima del sistema operativo
Sin configurar
Versión de compilación mínima del sistema operativo
Sin configurar
Versión de compilación máxima del sistema operativo
Sin configurar
Microsoft Defender for Endpoint
Reglas de Microsoft Defender para punto de conexión
Solicitar que el dispositivo tenga o esté por debajo de la puntuación de riesgo de la máquina:
Sin configurar
Seguridad del sistema
Todos los tipos de inscripción
Esta configuración funciona para los dispositivos inscritos en Intune a través de la inscripción de dispositivos o la inscripción de usuarios, y para los dispositivos inscritos con Apple School Manager o Apple Business Manager con la inscripción de dispositivo automatizada (anteriormente DEP).
Al requerir una contraseña, se aplica automáticamente un requisito de PIN de 6 dígitos no sencillo en todos los dispositivos inscritos por el usuario, independientemente de lo que se haya establecido para esta configuración
Contraseña
Requerir una contraseña para desbloquear dispositivos móviles
Requerir
Sin configurar
Inscripción de dispositivos e inscripción de dispositivos automatizada
Esta configuración funciona para los dispositivos que se inscribieron en Intune a través de la inscripción de dispositivos y para los dispositivos inscritos con Apple School Manager o Apple Business Manager con inscripción automatizada de dispositivos (anteriormente DEP).
Contraseñas sencillas
Bloquear
Sin configurar
Longitud mínima de la contraseña
6
Tipo de contraseña requerida
Numérica
Número de caracteres no alfanuméricos en la contraseña
Sin configurar
Máximo de minutos tras bloqueo de pantalla antes de solicitar la contraseña
1 minuto
Máximo de minutos de inactividad hasta que se bloquea la pantalla
1 minuto
Expiración de la contraseña (días)
30
Número de contraseñas anteriores que no se pueden reutilizar
6
Seguridad del dispositivo
Aplicaciones restringidas
Exportar
Nombre de aplicación
Identificación de lote de aplicaciones
Anterior
Siguiente

- **Dispositivos Linux**

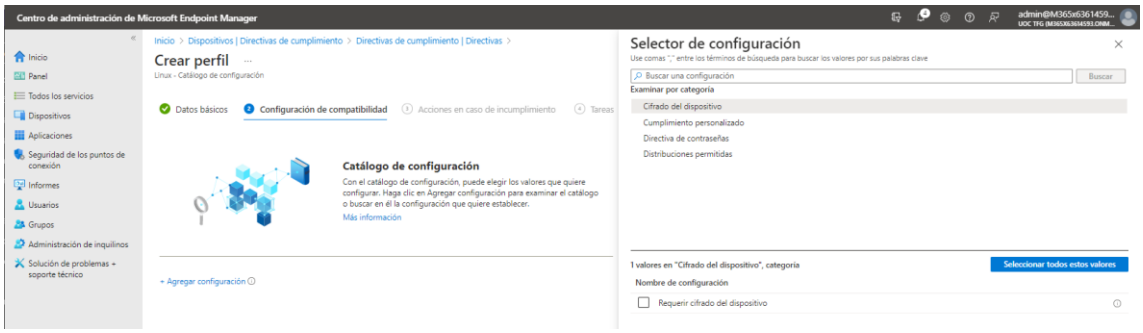
Para crear la directiva de cumplimiento de dispositivos Linux se debe seleccionar “Linux” como plataforma.



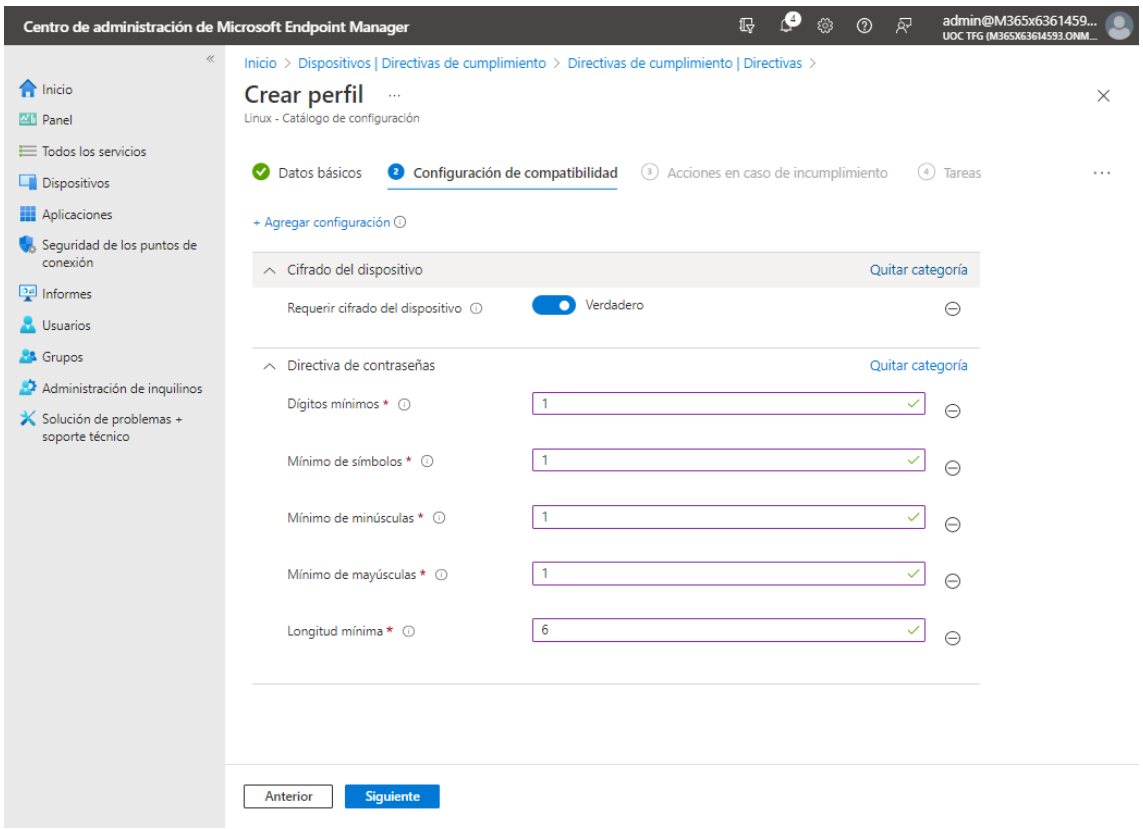
Primero, se indica el nombre y la descripción de la directiva.



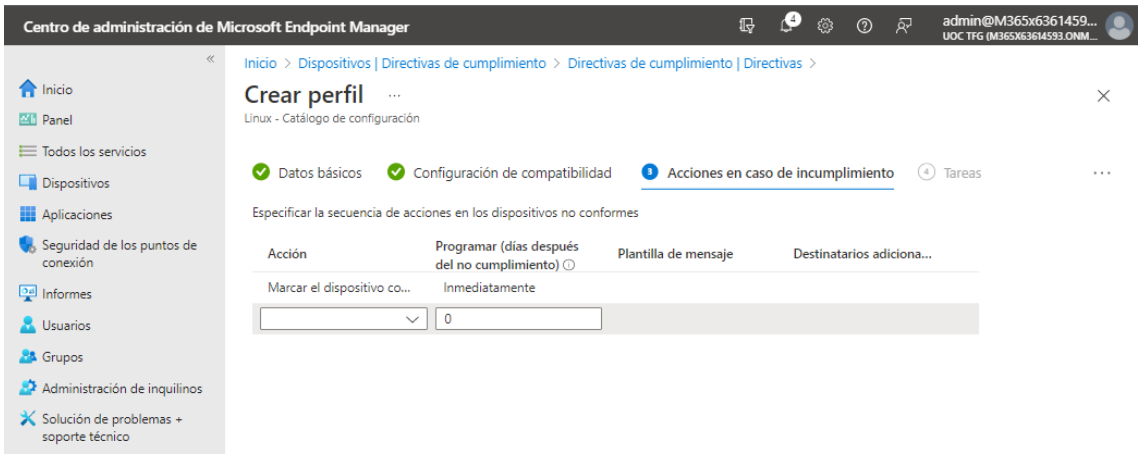
A continuación, se deben indicar las configuraciones que se desea que cumplan los dispositivos a los que se les asigne la directiva. A diferencia de en las directivas anteriores, para los dispositivos Linux existe un catálogo de configuración en el que se seleccionan los parámetros que se quieren añadir a la directiva y su configuración individual.



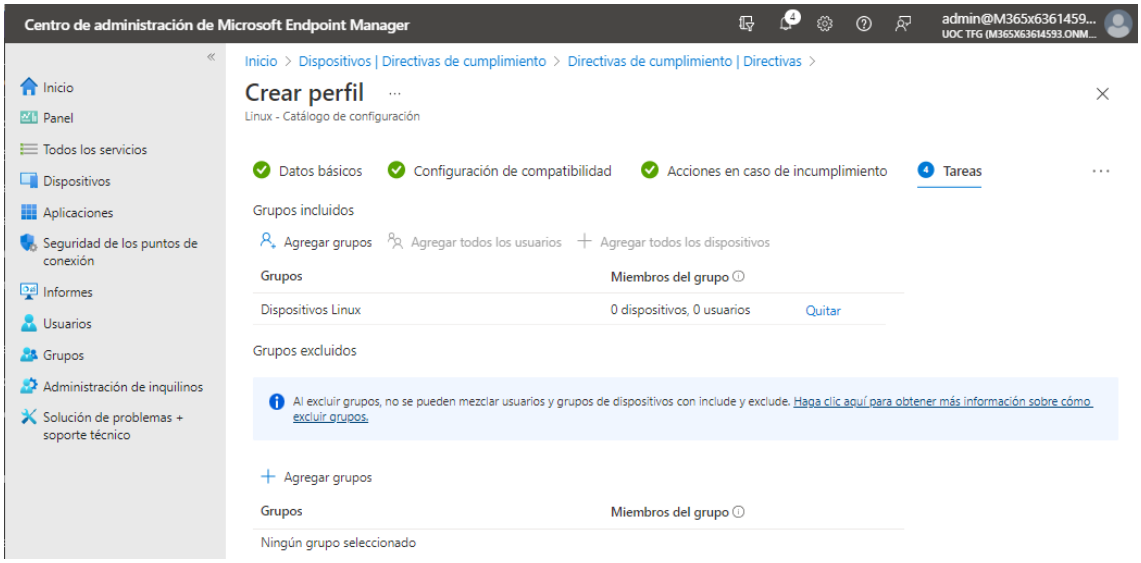
En este caso, se quiere controlar que el dispositivo tenga el cifrado habilitado y que la complejidad de la contraseña sea de al menos 6 caracteres incluyendo una mayúsucla, una minúscula, un número y un símbolo.



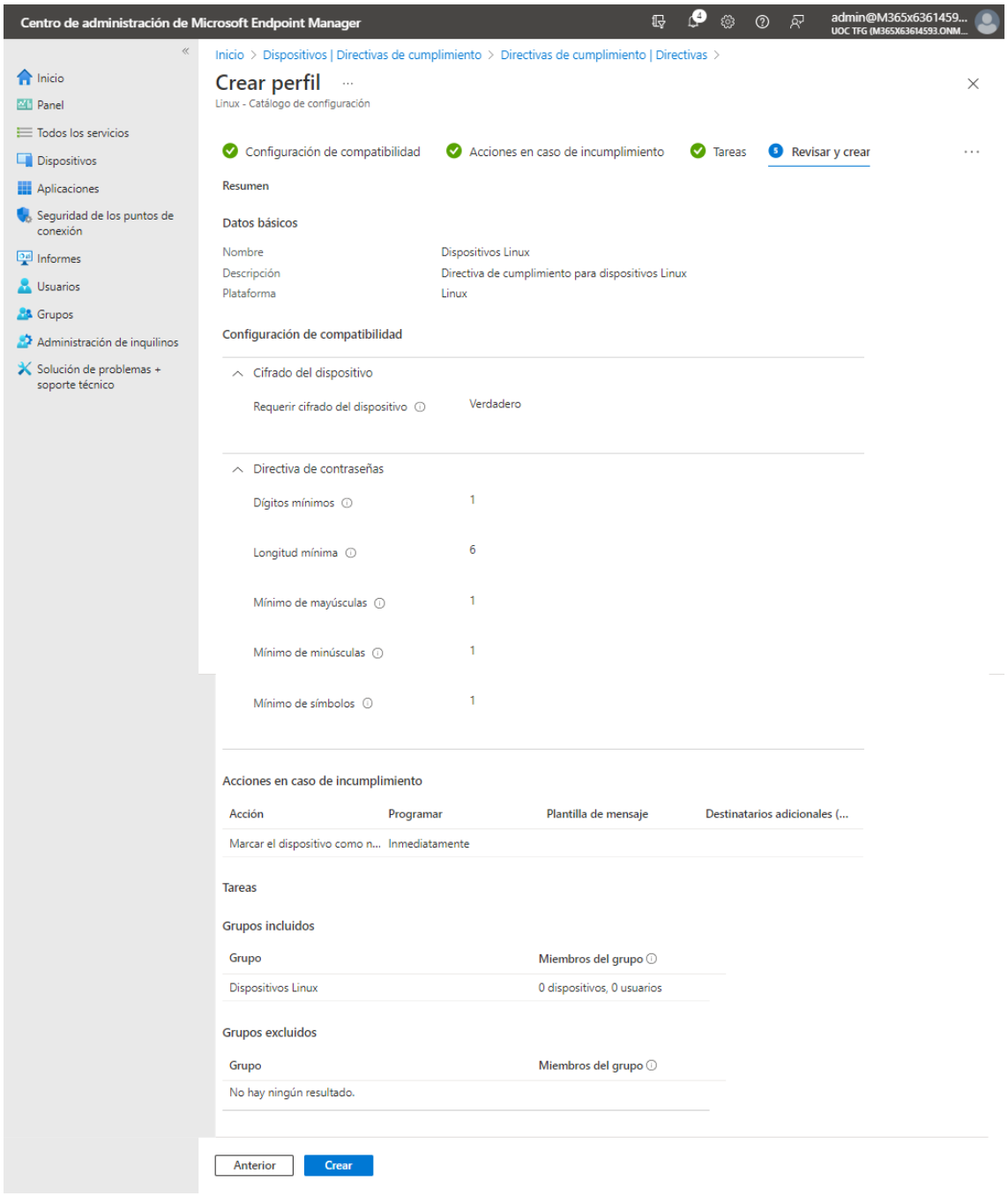
En el tercer paso, se indica que los dispositivos que no cumplan los requisitos de la directiva deben marcarse como no conformes inmediatamente.



A continuación, se asigna la directiva al grupo “Dispositivos Linux”.

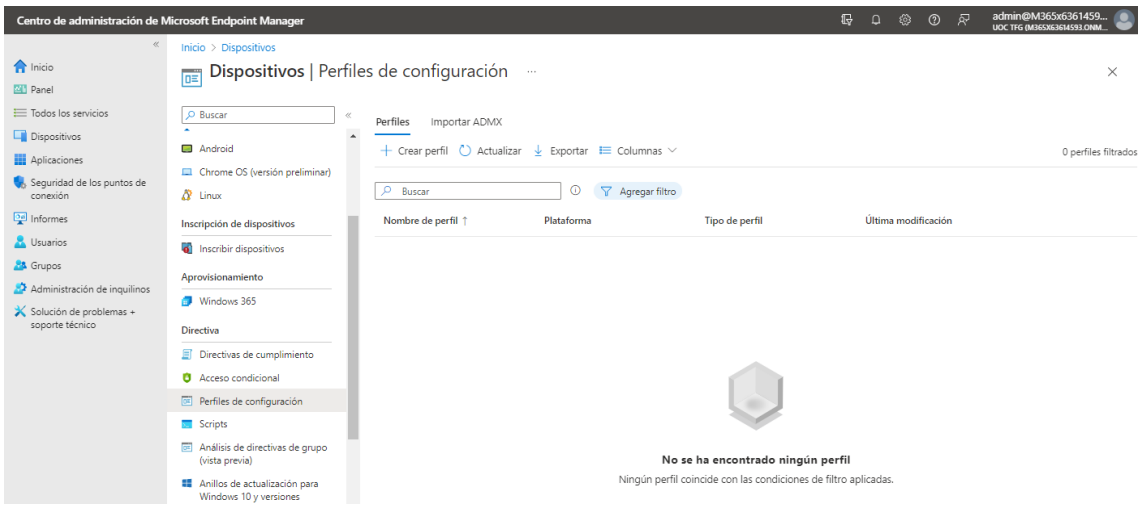


Por último, se revisa que los detalles de la directiva de cumplimiento sean correctos y se ordena la creación.


Centro de administración de Microsoft Endpoint Manager
admin@M365x6361459...
UOC TFG (M365X63614593.ONM...
Inicio
Panel
Todos los servicios
Dispositivos
Aplicaciones
Seguridad de los puntos de conexión
Informes
Usuarios
Grupos
Administración de inquilinos
Solución de problemas + soporte técnico
Inicio > Dispositivos | Directivas de cumplimiento > Directivas de cumplimiento | Directivas >
Crear perfil
Linux - Catálogo de configuración
Configuración de compatibilidad
Acciones en caso de incumplimiento
Tareas
Revisar y crear
Resumen
Datos básicos
Nombre
Dispositivos Linux
Descripción
Directiva de cumplimiento para dispositivos Linux
Plataforma
Linux
Configuración de compatibilidad
Cifrado del dispositivo
Requerir cifrado del dispositivo
Verdadero
Directiva de contraseñas
Dígitos mínimos
1
Longitud mínima
6
Mínimo de mayúsculas
1
Mínimo de minúsculas
1
Mínimo de símbolos
1
Acciones en caso de incumplimiento
Acción
Programar
Plantilla de mensaje
Destinatarios adicionales (...
Marcar el dispositivo como n...
Inmediatamente
Tareas
Grupos incluidos
Grupo
Miembros del grupo
Dispositivos Linux
0 dispositivos, 0 usuarios
Grupos excluidos
Grupo
Miembros del grupo
No hay ningún resultado.
Anterior
Crear

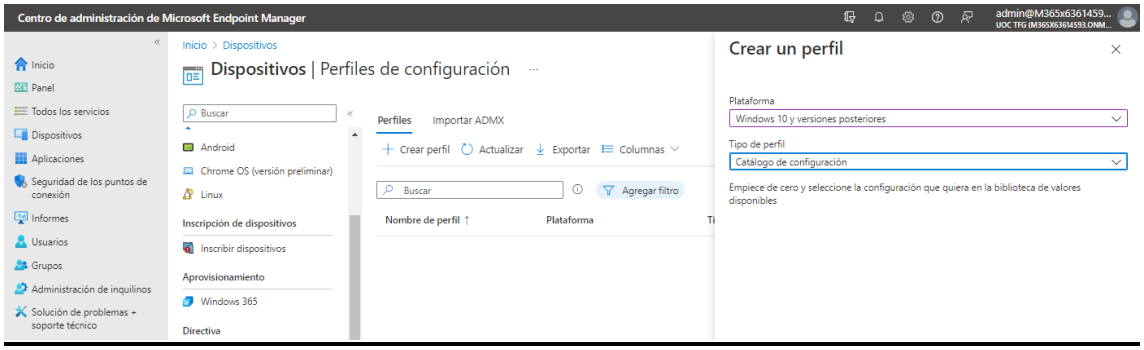
Anexo 6. Creación de perfiles de configuración

La creación de perfiles de configuración en Microsoft Intune se puede llevar a cabo desde “Perfiles de configuración”, dentro del menú Dispositivos.



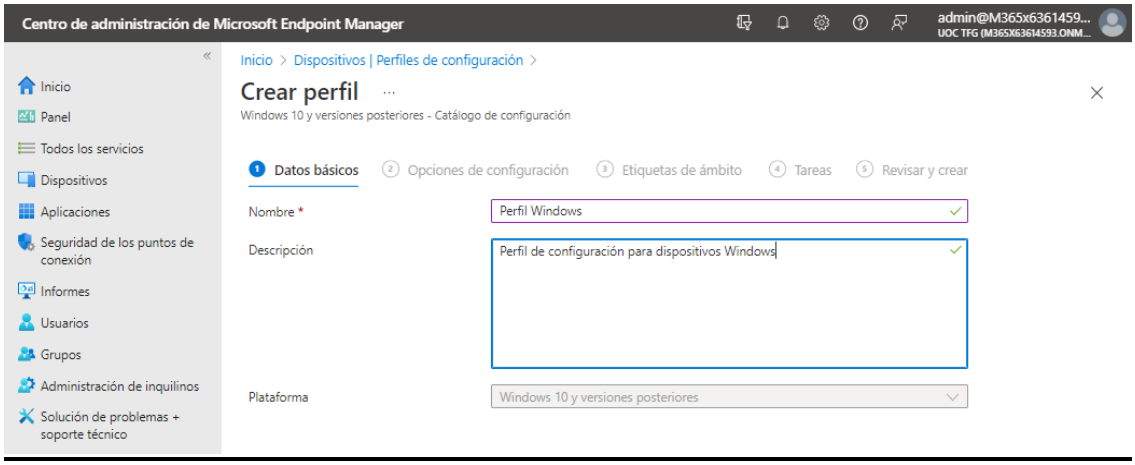
- **<u>Dispositivos Windows</u>**

En primer lugar, se debe indicar la plataforma y elegir el tipo de perfil deseado, si aplica.

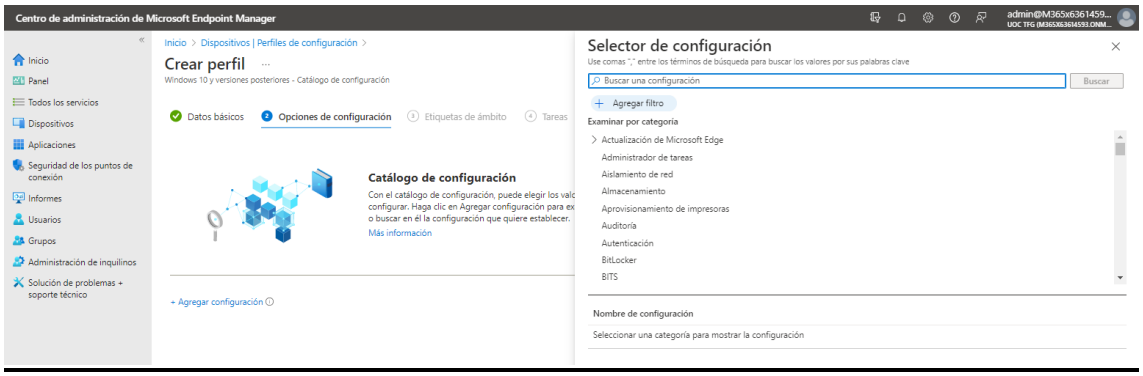


En este caso, se ha seleccionado “Windows 10 y versiones posteriores” como plataforma, y “Catálogo de configuración” como tipo de perfil. La diferencia entre “Catálogo de configuración” y “Plantillas” es que en el primero se pueden agregar configuraciones de diferente tipo al mismo perfil, mientras que si se selecciona “Plantillas” solo se puede seleccionar una plantilla de un tipo concreto de configuración para el perfil (como por ejemplo VPN o Wi-Fi).

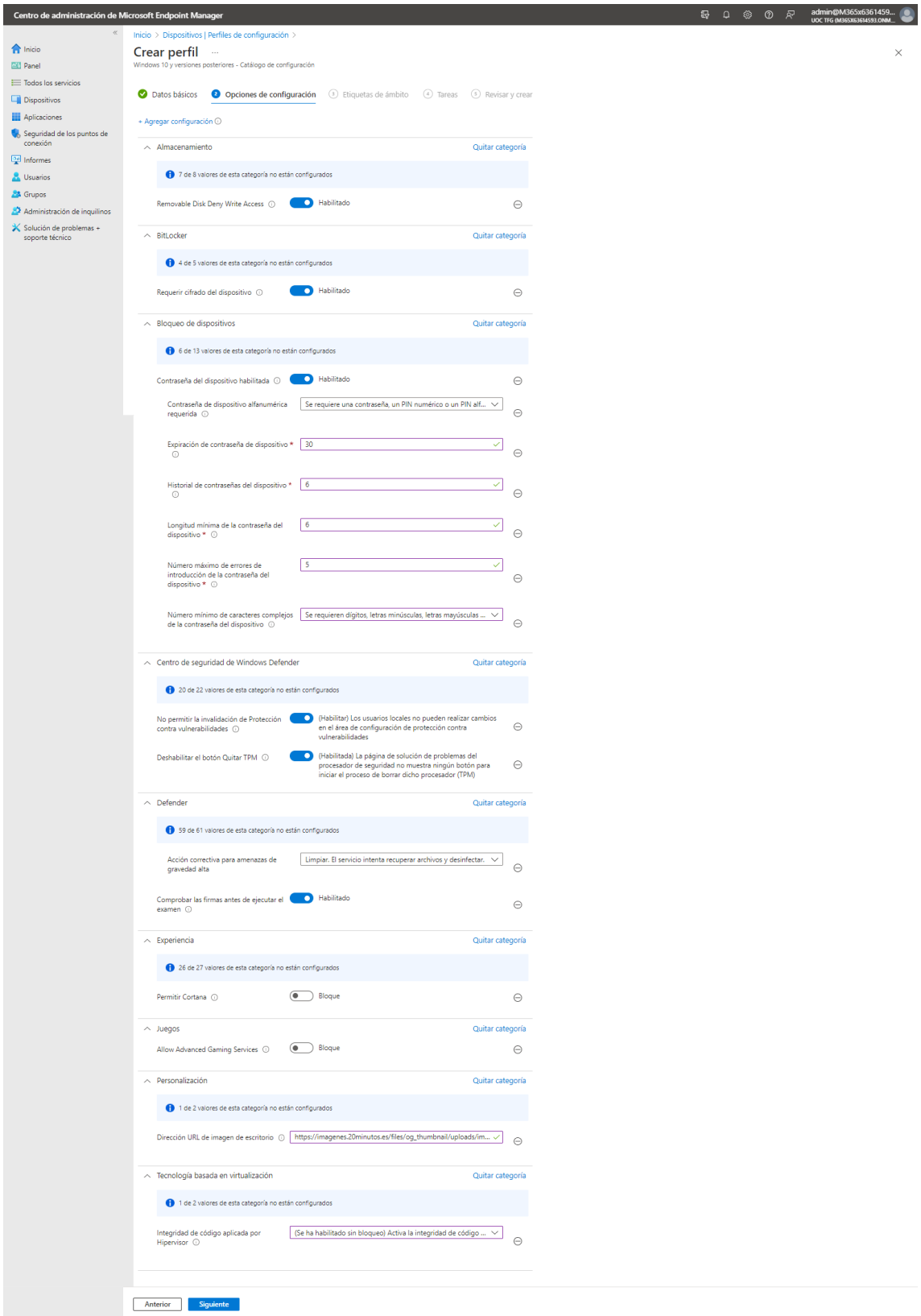
A continuación, como es habitual, se indica el nombre y la descripción del perfil en el primer paso.



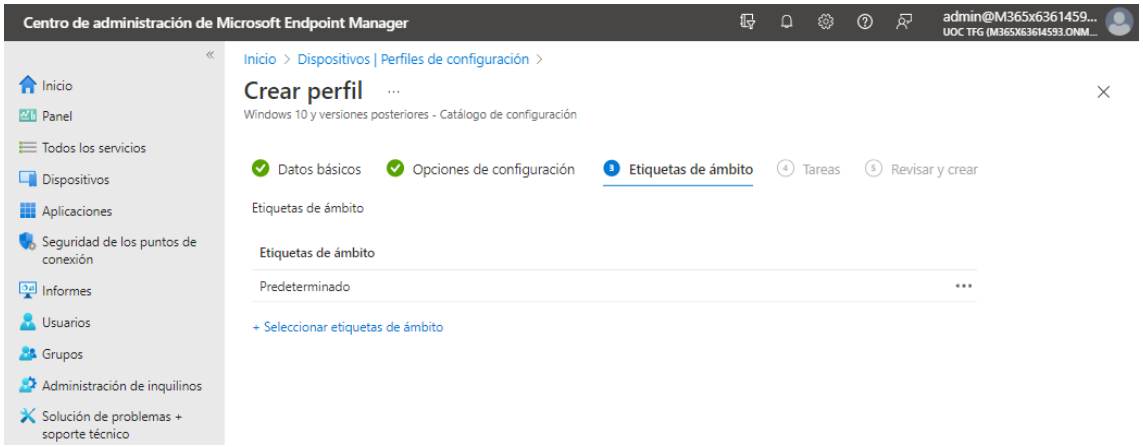
Después, se seleccionan las configuraciones que se deseen añadir al perfil de configuración, de entre todas las disponibles.



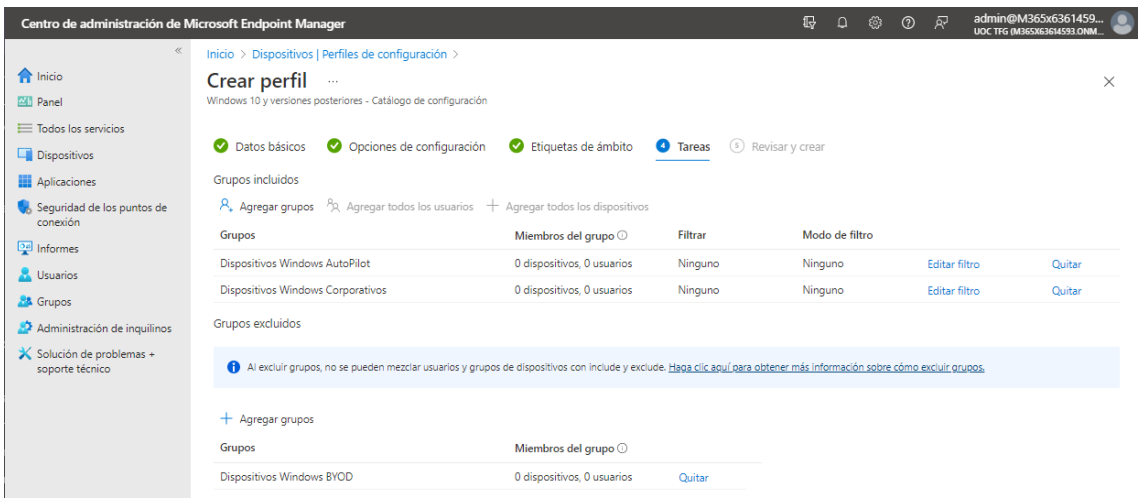
Una vez añadidas, se configuran todos los parámetros de las configuraciones elegidas.

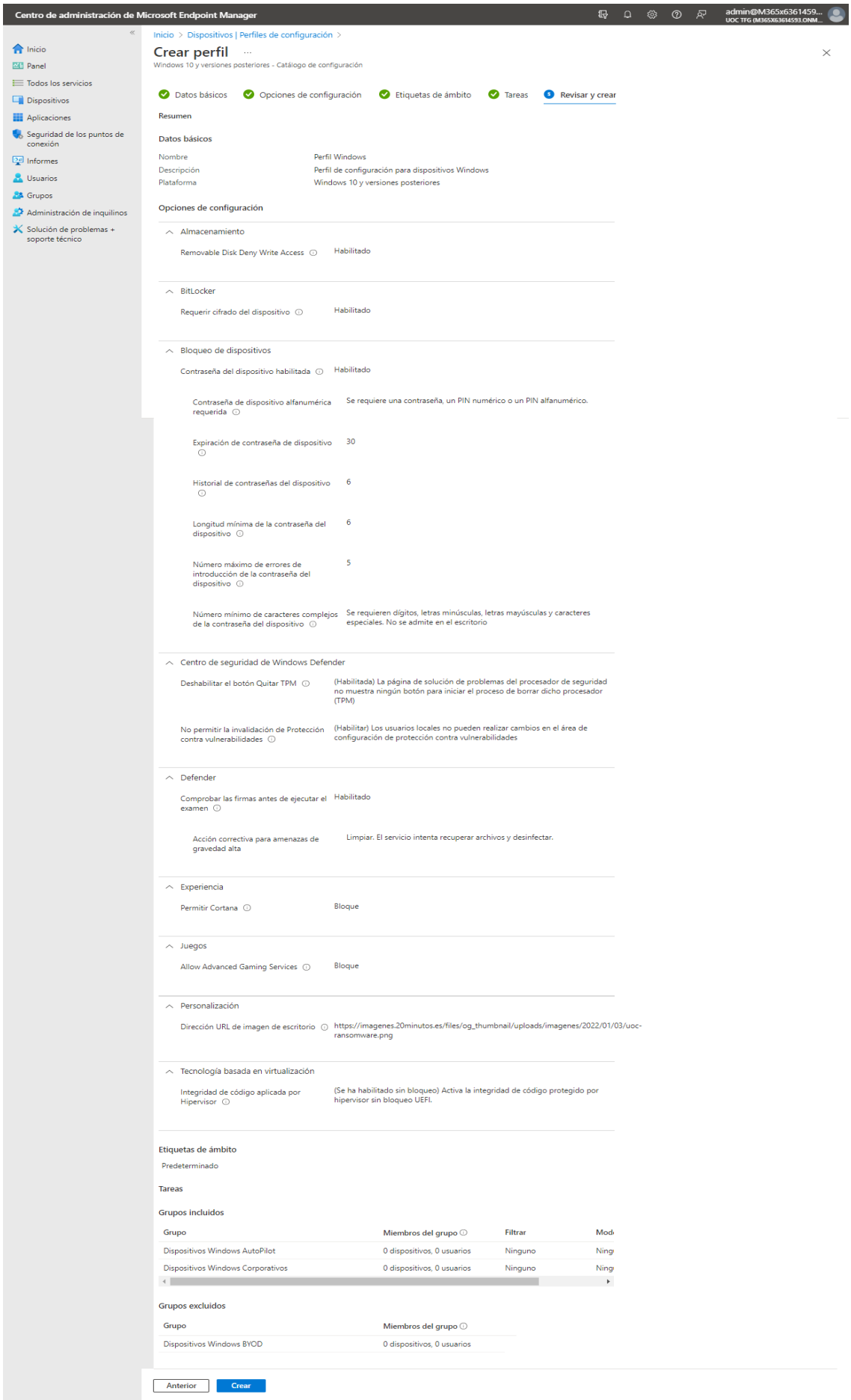

Centro de administración de Microsoft Endpoint Manager
admin@M365x6361459...
UOC TFG (M365X63614593.ONM...
Inicio
Panel
Todos los servicios
Dispositivos
Aplicaciones
Seguridad de los puntos de conexión
Informes
Usuarios
Grupos
Administración de inquilinos
Solución de problemas + soporte técnico
Inicio > Dispositivos | Perfiles de configuración >
Crear perfil
Windows 10 y versiones posteriores - Catálogo de configuración
Datos básicos
Opciones de configuración
Etiquetas de ámbito
Tareas
Revisar y crear
+ Agregar configuración
Almacenamiento
Quitar categoría
7 de 8 valores de esta categoría no están configurados
Removable Disk Deny Write Access
Habilitado
BitLocker
Quitar categoría
4 de 5 valores de esta categoría no están configurados
Requerir cifrado del dispositivo
Habilitado
Bloqueo de dispositivos
Quitar categoría
6 de 13 valores de esta categoría no están configurados
Contraseña del dispositivo habilitada
Habilitado
Contraseña de dispositivo alfanumérica requerida
Se requiere una contraseña, un PIN numérico o un PIN alf...
Expiración de contraseña de dispositivo *
30
Historial de contraseñas del dispositivo *
6
Longitud mínima de la contraseña del dispositivo *
6
Número máximo de errores de introducción de la contraseña del dispositivo *
5
Número mínimo de caracteres complejos de la contraseña del dispositivo
Se requieren dígitos, letras minúsculas, letras mayúsculas ...
Centro de seguridad de Windows Defender
Quitar categoría
20 de 22 valores de esta categoría no están configurados
No permitir la invalidación de Protección contra vulnerabilidades
(Habilitar) Los usuarios locales no pueden realizar cambios en el área de configuración de protección contra vulnerabilidades
Deshabilitar el botón Quitar TPM
(Habilitada) La página de solución de problemas del procesador de seguridad no muestra ningún botón para iniciar el proceso de borrar dicho procesador (TPM)
Defender
Quitar categoría
59 de 61 valores de esta categoría no están configurados
Acción correctiva para amenazas de gravedad alta
Limpiar. El servicio intenta recuperar archivos y desinfectar.
Comprobar las firmas antes de ejecutar el examen
Habilitado
Experiencia
Quitar categoría
26 de 27 valores de esta categoría no están configurados
Permitir Cortana
Bloque
Juegos
Quitar categoría
Allow Advanced Gaming Services
Bloque
Personalización
Quitar categoría
1 de 2 valores de esta categoría no están configurados
Dirección URL de imagen de escritorio
https://imagenes.20minutos.es/files/og_thumbnail/uploads/im...
Tecnología basada en virtualización
Quitar categoría
1 de 2 valores de esta categoría no están configurados
Integridad de código aplicada por Hipervisor
(Se ha habilitado sin bloqueo) Activa la integridad de código ...
Anterior
Siguiente

En el tercer paso, se pueden añadir etiquetas de ámbito. Las etiquetas de ámbito sirven para delegar permisos en Intune, mediante el control de acceso basados en roles (RBAC, del inglés Role-Based Access Control) en el que se basa la herramienta. Por ejemplo, se podrían definir una serie de etiquetas para cada ubicación y que los administradores de dichas ubicaciones solo tuviesen permisos sobre los objetos con esas etiquetas, evitando que pudieran modificar configuraciones de otros sitios.



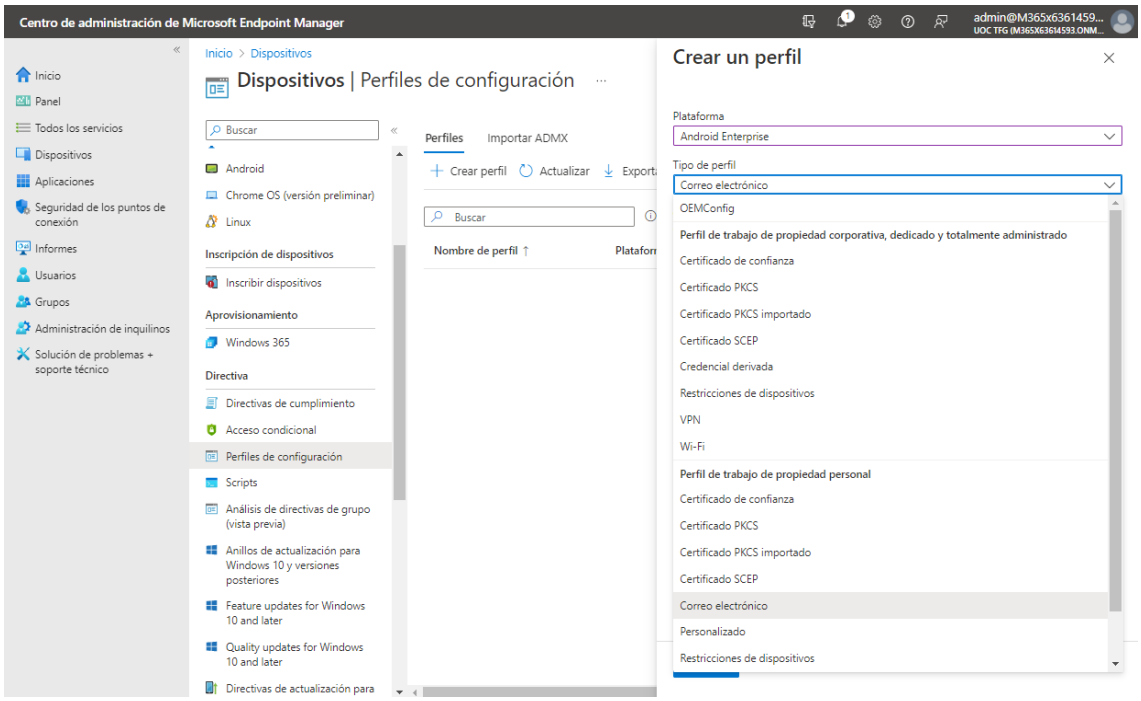
Para finalizar, se asigna el perfil a los grupos en los que se va a aplicar, se revisan los detalles del perfil y se procede a su creación. En este caso, se ha excluido el perfil de configuración del grupo “Dispositivos Windows BYOD” para evitar que se les apliquen las configuraciones requeridas en los dispositivos corporativos.



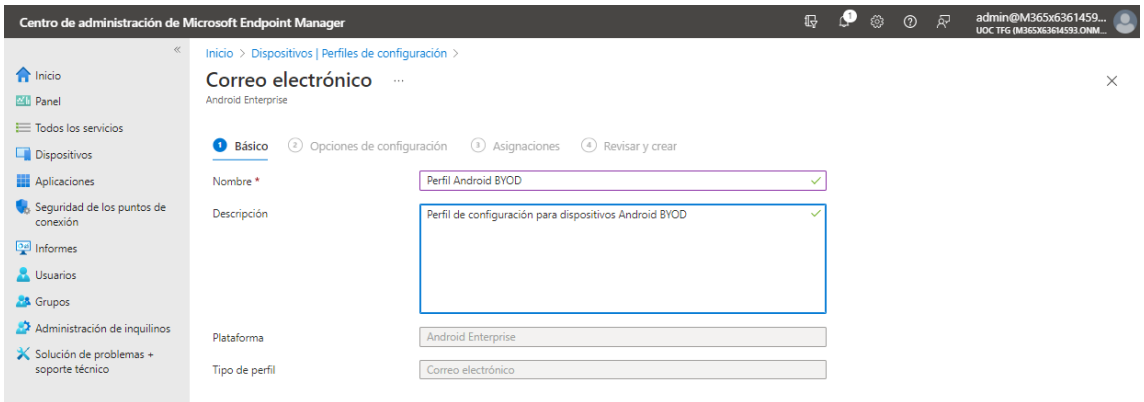

Centro de administración de Microsoft Endpoint Manager
admin@M365x6361459...
UOC TFG (M365X63614593.ONM...
Inicio
Panel
Todos los servicios
Dispositivos
Aplicaciones
Seguridad de los puntos de conexión
Informes
Usuarios
Grupos
Administración de inquilinos
Solución de problemas + soporte técnico
Inicio > Dispositivos | Perfiles de configuración >
Crear perfil
Windows 10 y versiones posteriores - Catálogo de configuración
Datos básicos
Opciones de configuración
Etiquetas de ámbito
Tareas
Revisar y crear
Resumen
Datos básicos
Nombre Perfil Windows
Descripción Perfil de configuración para dispositivos Windows
Plataforma Windows 10 y versiones posteriores
Opciones de configuración
Almacenamiento
Removable Disk Deny Write Access Habilitado
BitLocker
Requerir cifrado del dispositivo Habilitado
Bloqueo de dispositivos
Contraseña del dispositivo habilitada Habilitado
Contraseña de dispositivo alfanumérica requerida Se requiere una contraseña, un PIN numérico o un PIN alfanumérico.
Expiración de contraseña de dispositivo 30
Historial de contraseñas del dispositivo 6
Longitud mínima de la contraseña del dispositivo 6
Número máximo de errores de introducción de la contraseña del dispositivo 5
Número mínimo de caracteres complejos de la contraseña del dispositivo Se requieren dígitos, letras minúsculas, letras mayúsculas y caracteres especiales. No se admite en el escritorio
Centro de seguridad de Windows Defender
Deshabilitar el botón Quitar TPM (Habilitada) La página de solución de problemas del procesador de seguridad no muestra ningún botón para iniciar el proceso de borrar dicho procesador (TPM)
No permitir la invalidación de Protección contra vulnerabilidades (Habilitar) Los usuarios locales no pueden realizar cambios en el área de configuración de protección contra vulnerabilidades
Defender
Comprobar las firmas antes de ejecutar el examen Habilitado
Acción correctiva para amenazas de gravedad alta Limpiar. El servicio intenta recuperar archivos y desinfectar.
Experiencia
Permitir Cortana Bloque
Juegos
Allow Advanced Gaming Services Bloque
Personalización
Dirección URL de imagen de escritorio https://imagenes.20minutos.es/files/og_thumbnail/uploads/imagenes/2022/01/03/uoc-ransomware.png
Tecnología basada en virtualización
Integridad de código aplicada por Hipervisor (Se ha habilitado sin bloqueo) Activa la integridad de código protegido por hipervisor sin bloqueo UEFI.
Etiquetas de ámbito
Predeterminado
Tareas
Grupos incluidos
Grupo
Miembros del grupo
Filtrar
Dispositivos Windows AutoPilot
0 dispositivos, 0 usuarios
Ninguno
Dispositivos Windows Corporativos
0 dispositivos, 0 usuarios
Ninguno
Grupos excluidos
Grupo
Miembros del grupo
Dispositivos Windows BYOD
0 dispositivos, 0 usuarios
Anterior
Crear

- **Dispositivos Android BYOD**

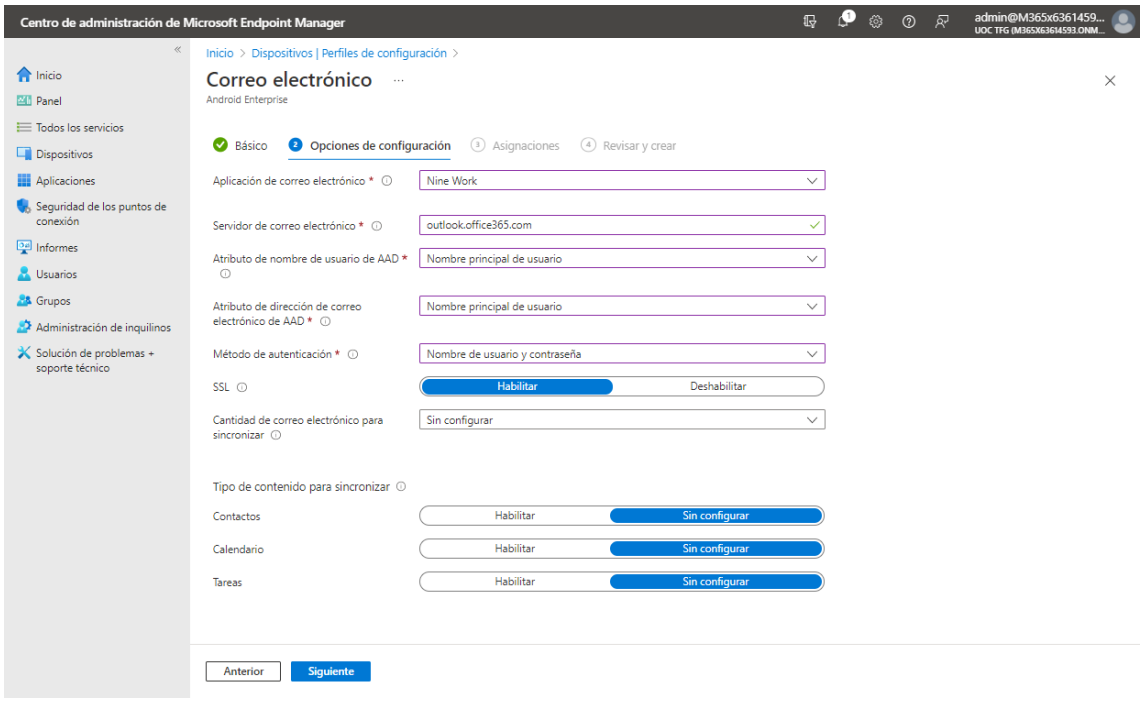
Para crear el perfil de configuración de los dispositivos Android Enterprise se debe seleccionar “Android Enterprise” en plataforma y seleccionar un tipo de perfil de los disponibles. En este caso, se ha optado por el de “Correo electrónico” para los dispositivos con perfil de trabajo en dispositivo de propiedad personal (BYOD).



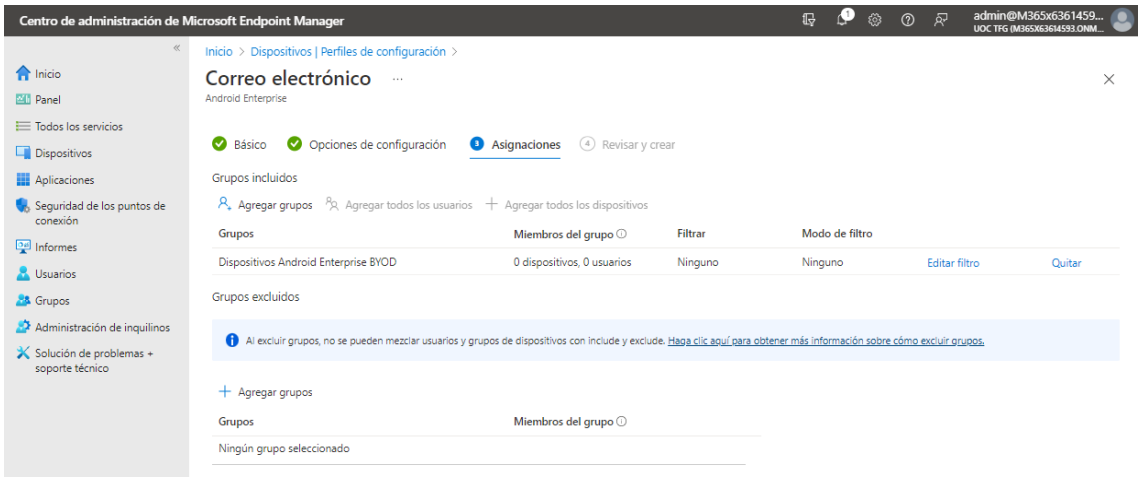
En el primer paso, se introduce el nombre del perfil y la descripción.

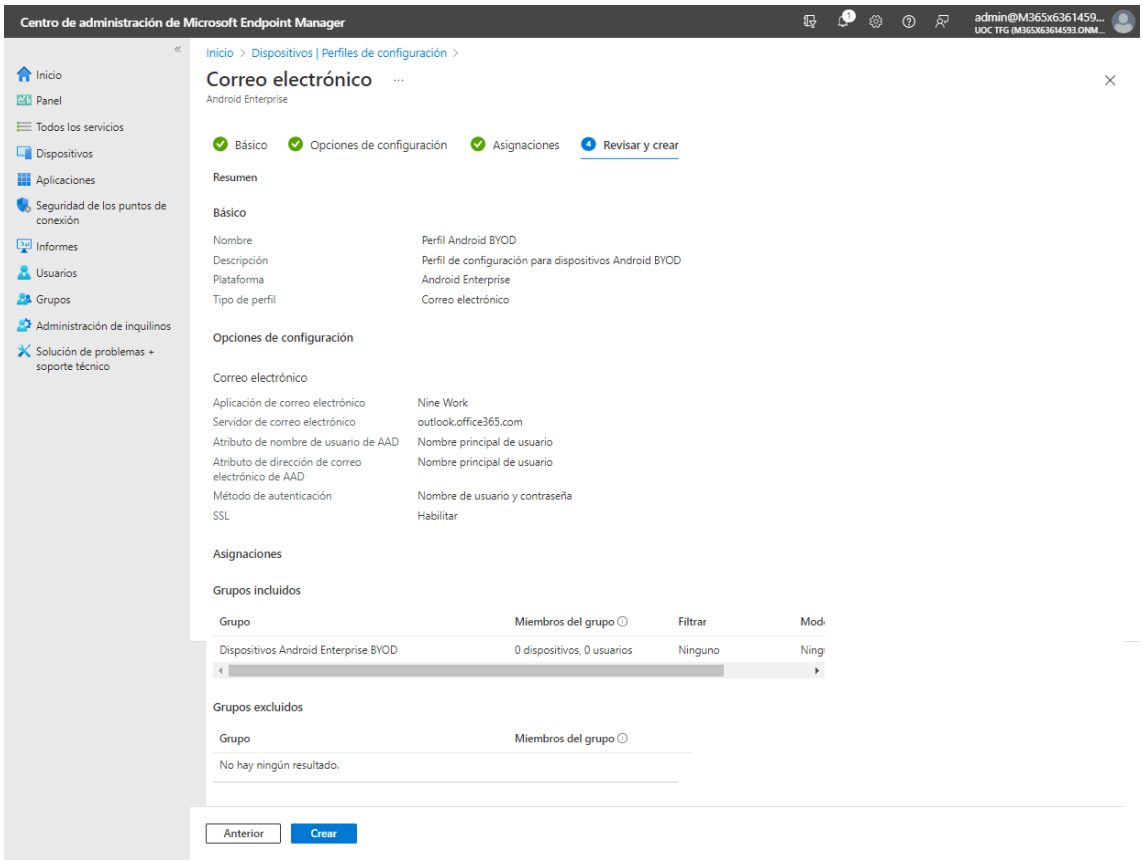


En el segundo paso, se indican los parámetros de configuración del perfil.



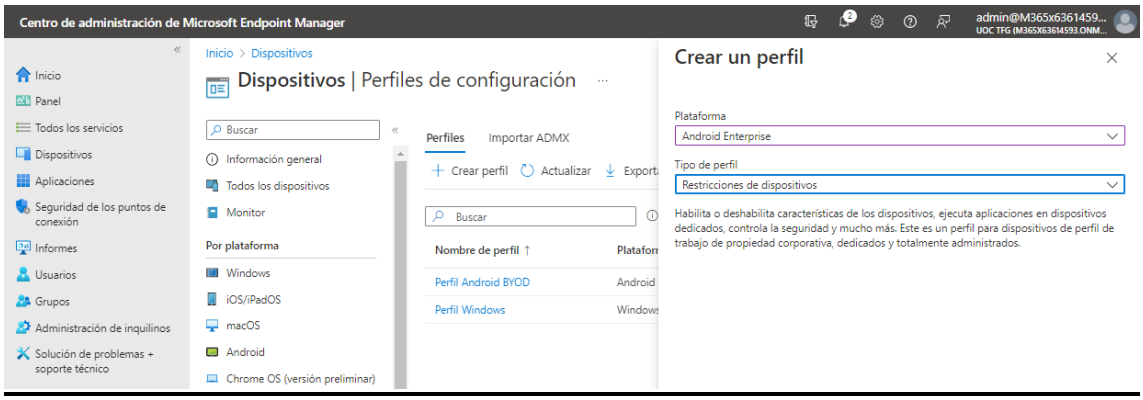
Por último, se asigna al grupo deseado (“Dispositivos Android Enterprise BYOD”) y se revisan los detalles antes de ejecutar la creación del perfil.



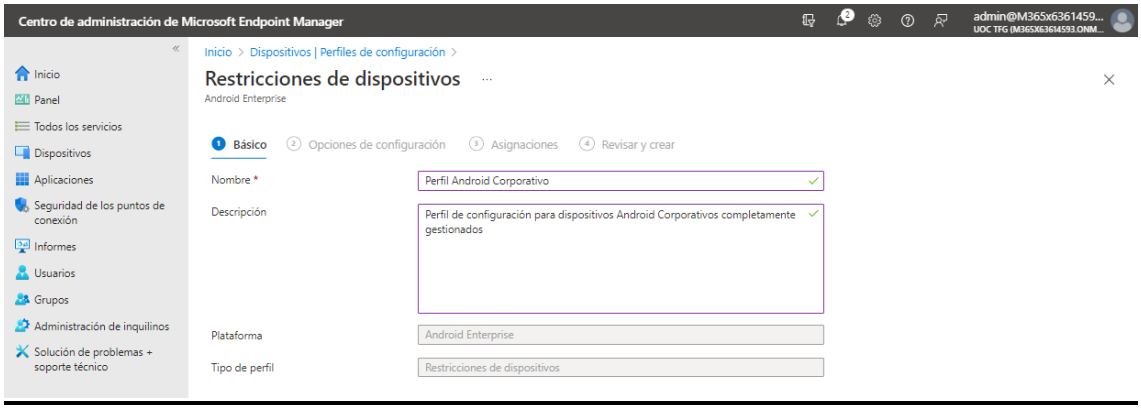


- **<u>Dispositivos Android Corporativos</u>**

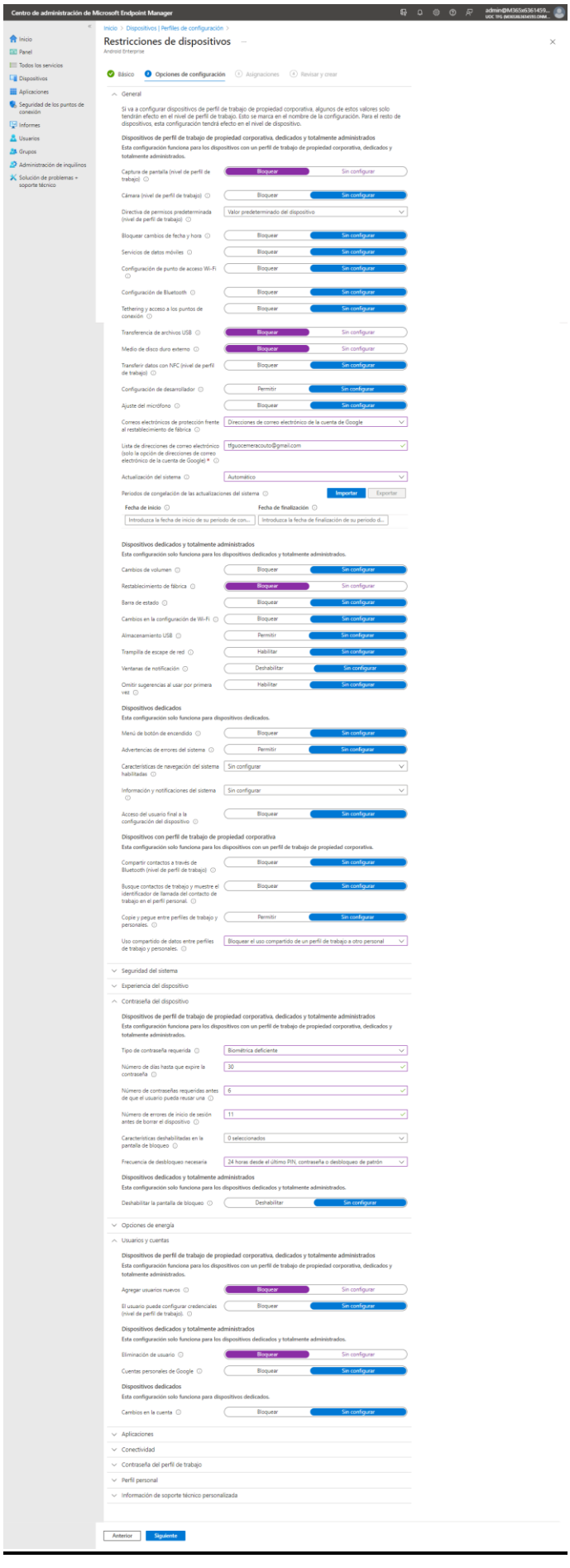
La creación del perfil de configuración de los dispositivos Android Enterprise corporativos es similar a la de los BYOD, con la diferencia de que hay que seleccionar un tipo de perfil de los que se encuentran bajo Perfil de trabajo de propiedad corporativa, dedicado y totalmente administrado. En este caso, se ha seleccionado “Restricciones de dispositivos”.



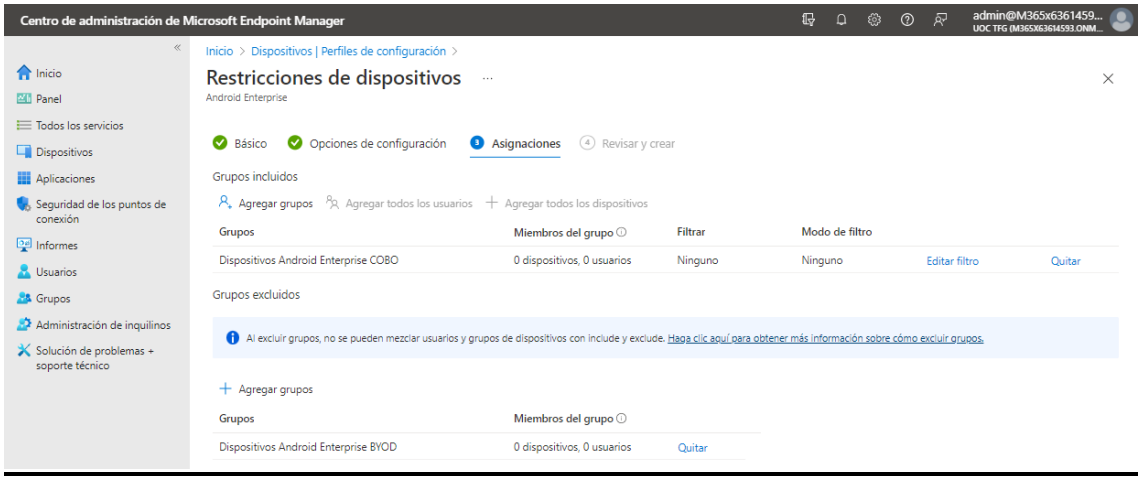
De nuevo, el primer paso de la creación del perfil consiste en indicar el nombre y la descripción del mismo.

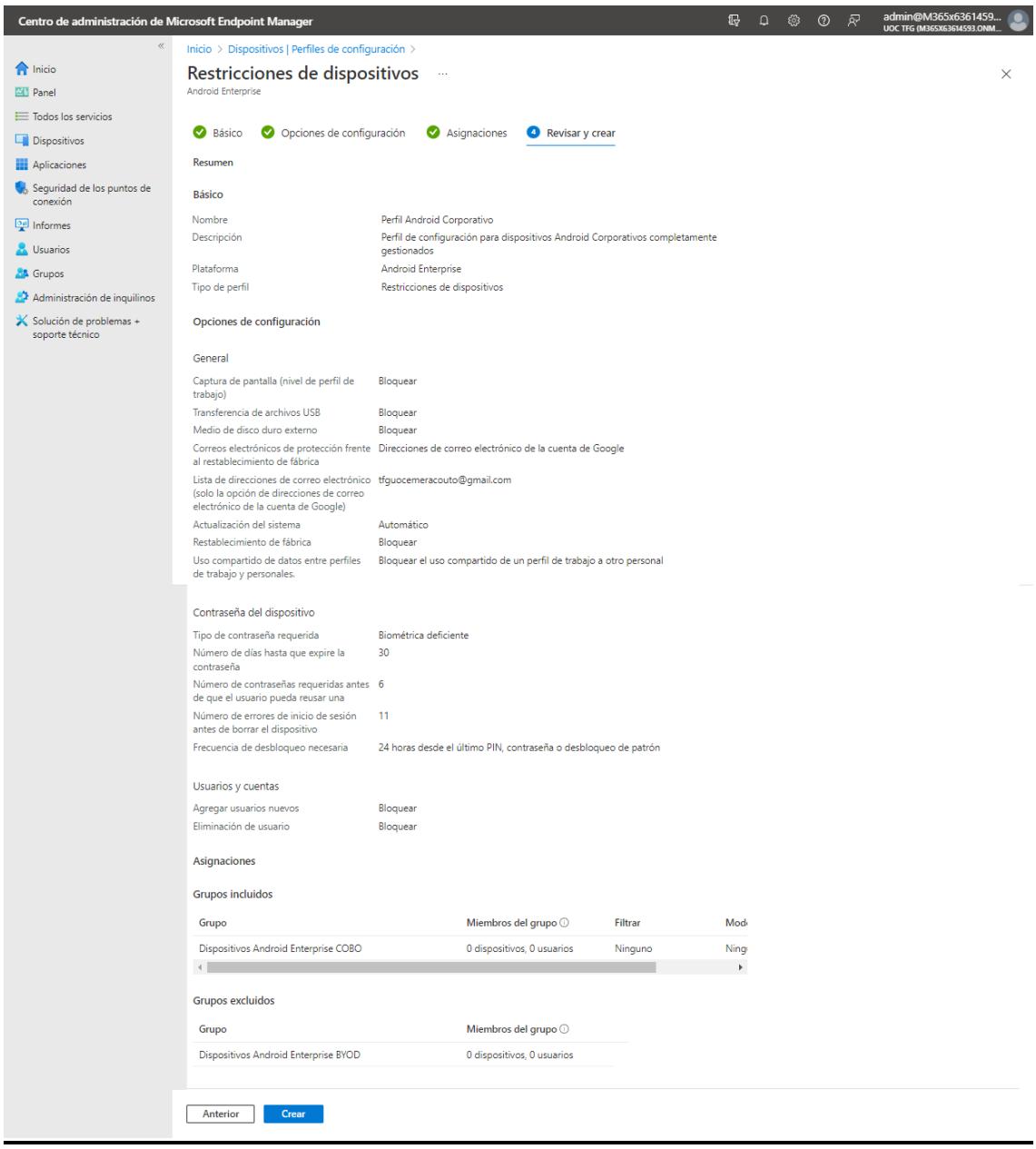


Después, se deben configurar los parámetros deseados de la configuración de restricción de dispositivos, tal y como se muestra en la siguiente imagen.


Centro de administración de Microsoft Endpoint Manager
Inicio > Dispositivos | Perfiles de configuración >
Restricciones de dispositivos
Android Enterprise
Básico
Opciones de configuración
Asignaciones
Revisar y crear
General
Si va a configurar dispositivos de perfil de trabajo de propiedad corporativa, algunos de estos valores solo tendrán efecto en el nivel de perfil de trabajo. Esto se marca en el nombre de la configuración. Para el resto de dispositivos, esta configuración tendrá efecto en el nivel de dispositivo.
Dispositivos de perfil de trabajo de propiedad corporativa, dedicados y totalmente administrados
Esta configuración funciona para los dispositivos con un perfil de trabajo de propiedad corporativa, dedicados y totalmente administrados.
Captura de pantalla (nivel de perfil de trabajo)
Cámara (nivel de perfil de trabajo)
Directiva de permisos predeterminada (nivel de perfil de trabajo)
Valor predeterminado del dispositivo
Bloquear cambios de fecha y hora
Servicios de datos móviles
Configuración de punto de acceso Wi-Fi
Configuración de Bluetooth
Tethering y acceso a los puntos de conexión
Transferencia de archivos USB
Medio de disco duro externo
Transferir datos con NFC (nivel de perfil de trabajo)
Configuración de desarrollador
Ajuste del micrófono
Correos electrónicos de protección frente al restablecimiento de fábrica
Direcciones de correo electrónico de la cuenta de Google
Lista de direcciones de correo electrónico (solo la opción de direcciones de correo electrónico de la cuenta de Google) *
tfguocemeracouto@gmail.com
Actualización del sistema
Automático
Periodos de congelación de las actualizaciones del sistema
Importar
Exportar
Fecha de inicio
Fecha de finalización
Introduzca la fecha de inicio de su periodo de con...
Introduzca la fecha de finalización de su periodo d...
Dispositivos dedicados y totalmente administrados
Esta configuración solo funciona para los dispositivos dedicados y totalmente administrados.
Cambios de volumen
Restablecimiento de fábrica
Barra de estado
Cambios en la configuración de Wi-Fi
Almacenamiento USB
Trampilla de escape de red
Habilitar
Ventanas de notificación
Deshabilitar
Omitir sugerencias al usar por primera vez
Dispositivos dedicados
Esta configuración solo funciona para dispositivos dedicados.
Menú de botón de encendido
Advertencias de errores del sistema
Características de navegación del sistema habilitadas
Sin configurar
Información y notificaciones del sistema
Acceso del usuario final a la configuración del dispositivo
Dispositivos con perfil de trabajo de propiedad corporativa
Esta configuración solo funciona para los dispositivos con un perfil de trabajo de propiedad corporativa.
Compartir contactos a través de Bluetooth (nivel de perfil de trabajo)
Busque contactos de trabajo y muestre el identificador de llamada del contacto de trabajo en el perfil personal.
Copie y pegue entre perfiles de trabajo y personales.
Uso compartido de datos entre perfiles de trabajo y personales.
Bloquear el uso compartido de un perfil de trabajo a otro personal
Seguridad del sistema
Experiencia del dispositivo
Contraseña del dispositivo
Dispositivos de perfil de trabajo de propiedad corporativa, dedicados y totalmente administrados
Esta configuración funciona para los dispositivos con un perfil de trabajo de propiedad corporativa, dedicados y totalmente administrados.
Tipo de contraseña requerida
Biométrica deficiente
Número de días hasta que expire la contraseña
30
Número de contraseñas requeridas antes de que el usuario pueda reusar una
6
Número de errores de inicio de sesión antes de borrar el dispositivo
11
Características deshabilitadas en la pantalla de bloqueo
0 seleccionados
Frecuencia de desbloqueo necesaria
24 horas desde el último PIN, contraseña o desbloqueo de patrón
Dispositivos dedicados y totalmente administrados
Esta configuración solo funciona para los dispositivos dedicados y totalmente administrados.
Deshabilitar la pantalla de bloqueo
Opciones de energía
Usuarios y cuentas
Dispositivos de perfil de trabajo de propiedad corporativa, dedicados y totalmente administrados
Esta configuración funciona para los dispositivos con un perfil de trabajo de propiedad corporativa, dedicados y totalmente administrados.
Agregar usuarios nuevos
El usuario puede configurar credenciales (nivel de perfil de trabajo).
Dispositivos dedicados y totalmente administrados
Esta configuración solo funciona para los dispositivos dedicados y totalmente administrados.
Eliminación de usuario
Cuentas personales de Google
Dispositivos dedicados
Esta configuración solo funciona para dispositivos dedicados.
Cambios en la cuenta
Aplicaciones
Conectividad
Contraseña del perfil de trabajo
Perfil personal
Información de soporte técnico personalizada
Anterior
Siguiente

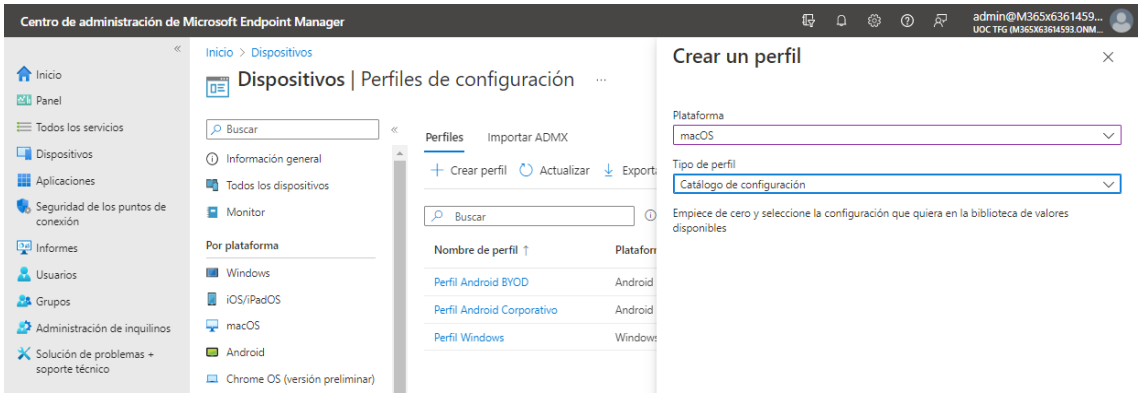
Por último, se asigna el perfil al grupo deseado y se ordena la creación.



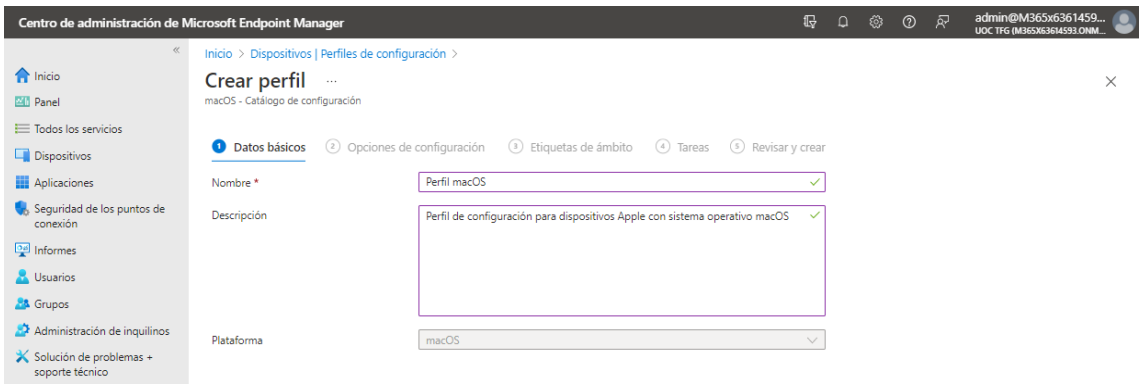


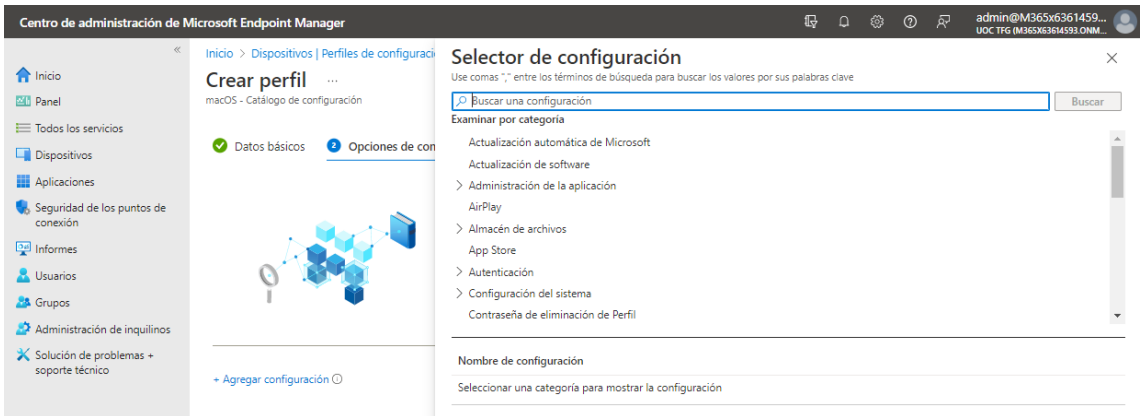
- **Dispositivos macOS**

La creación de un perfil de configuración para dispositivos Apple con sistema operativo macOS es similar a la de los dispositivos Windows, debiendo seleccionar “macOS” en Plataforma y “Catálogo de configuración” o “Plantillas” como tipo de perfil.

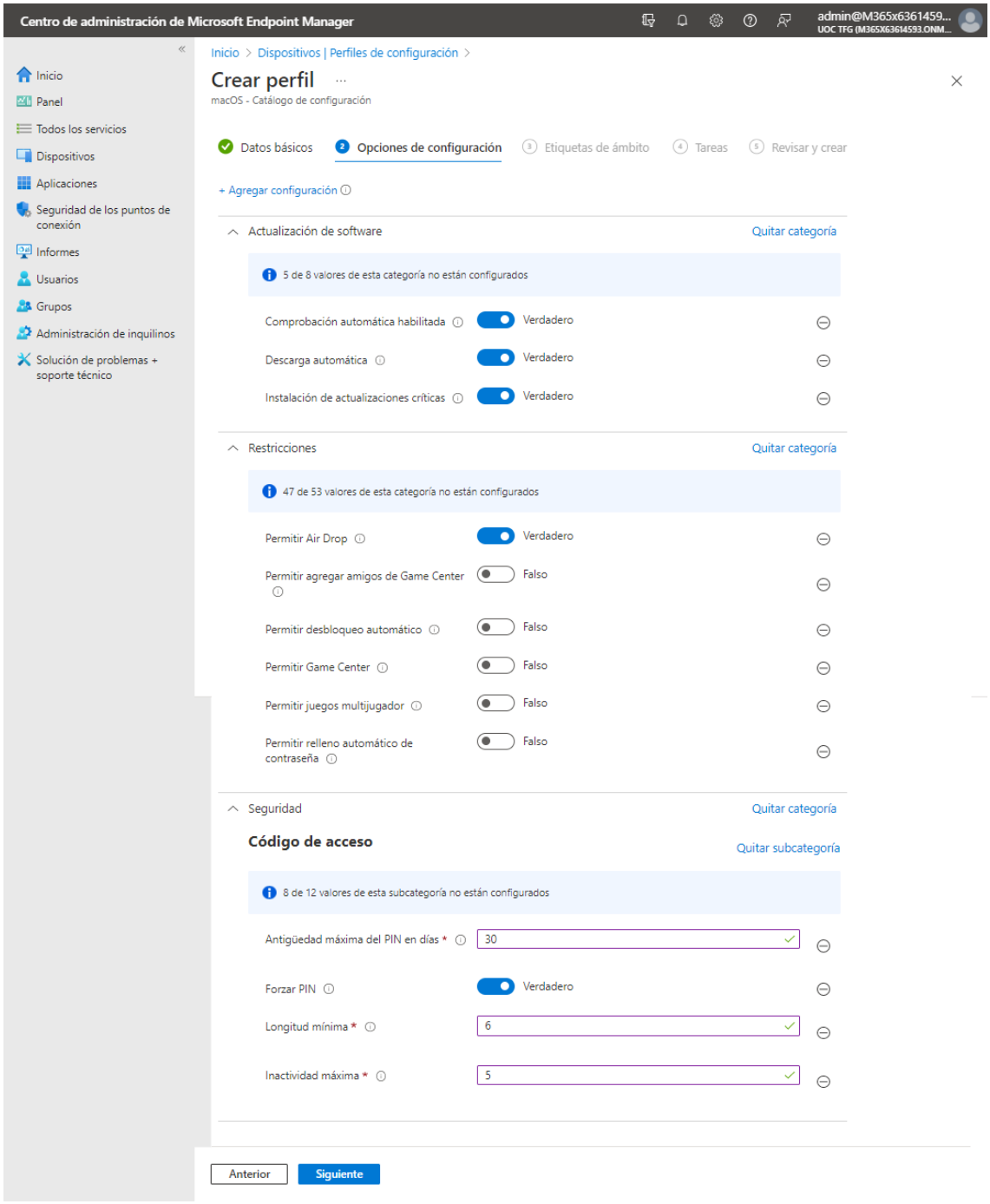


Una vez definido el tipo de perfil, se indica su nombre y descripción y, después, se seleccionan las configuraciones sobre las que se quiere actuar.

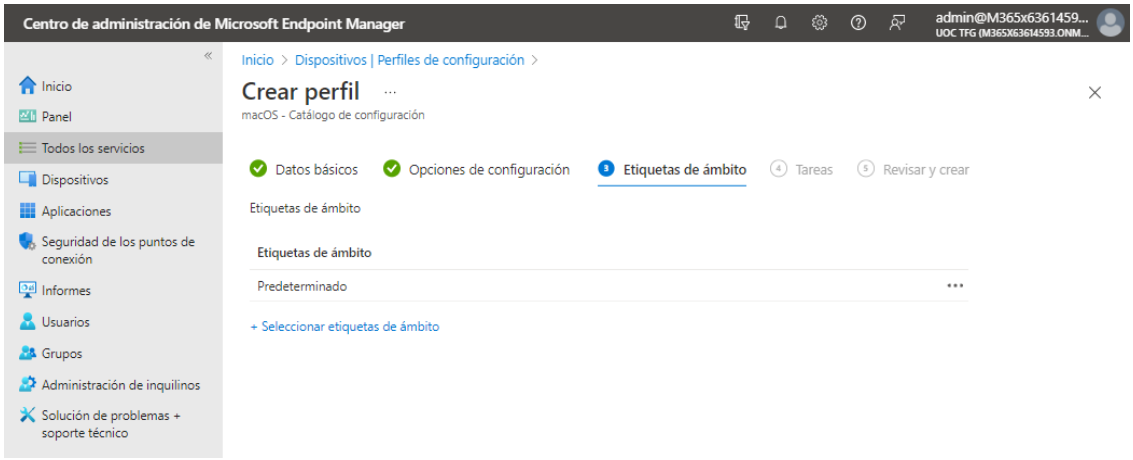




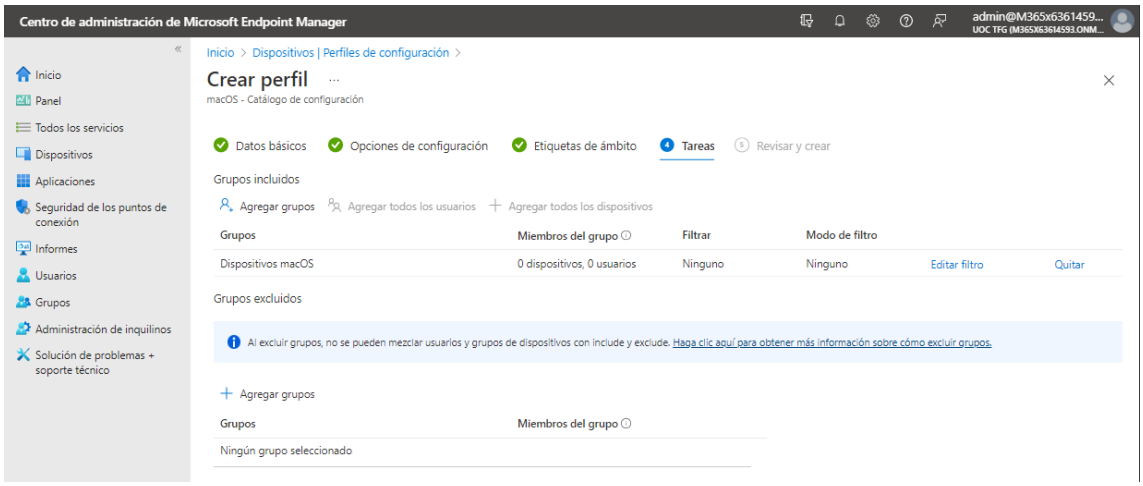
A continuación, se definen lo parámetros de las configuraciones elegidas.

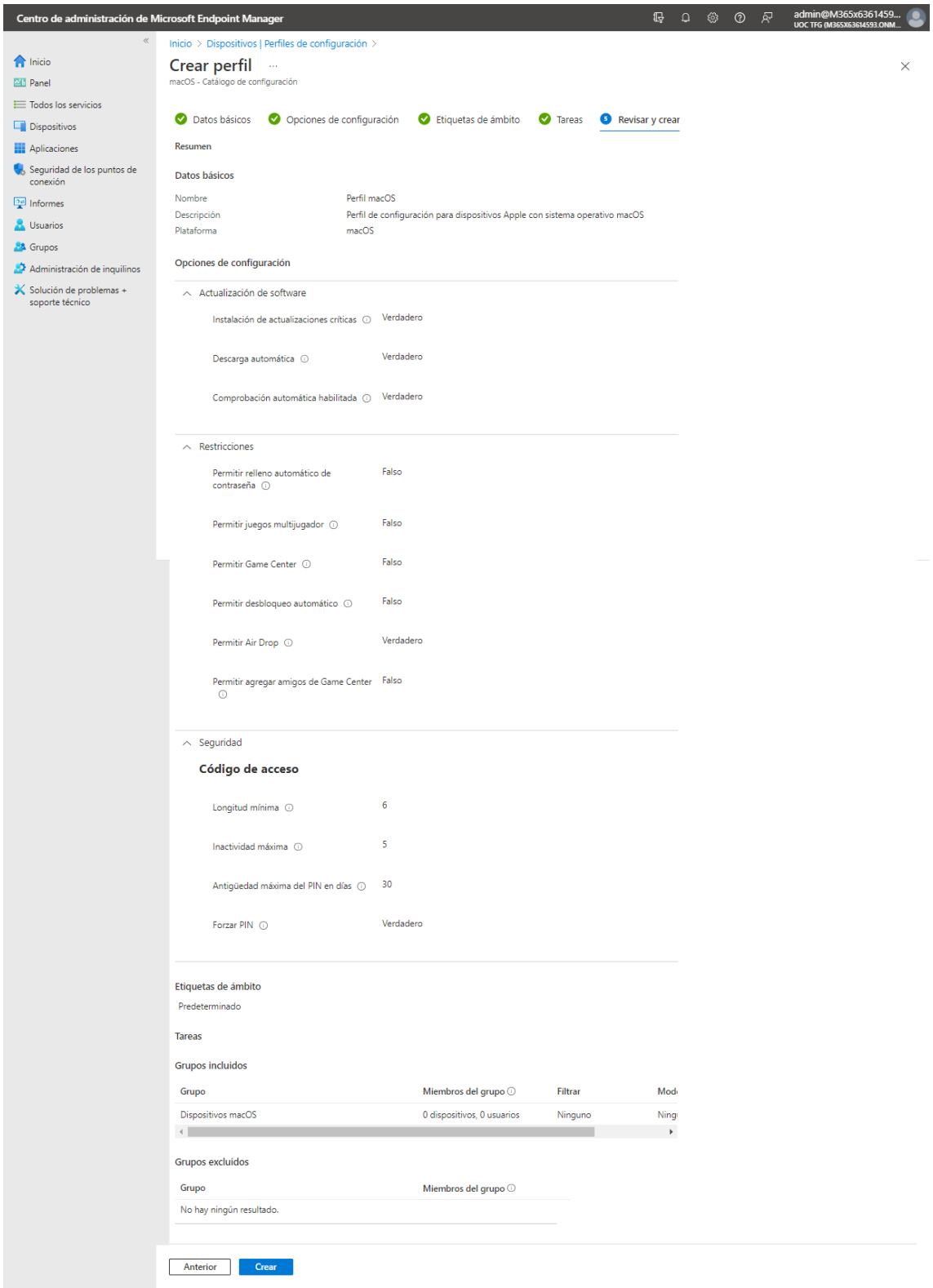


Los perfiles de macOS también permiten asignar etiquetas de ámbito, para delegar permisos de administración.



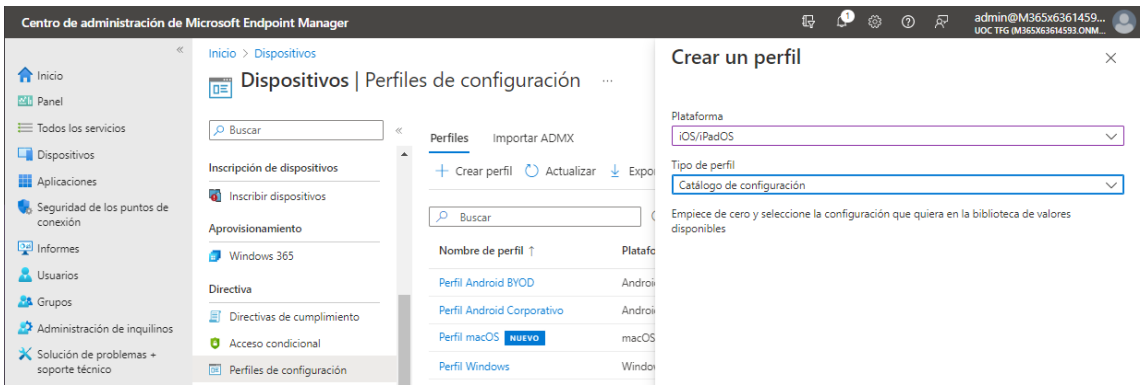
Para finalizar, se asigna el perfil a los grupos deseados y se realiza la creación del perfil.



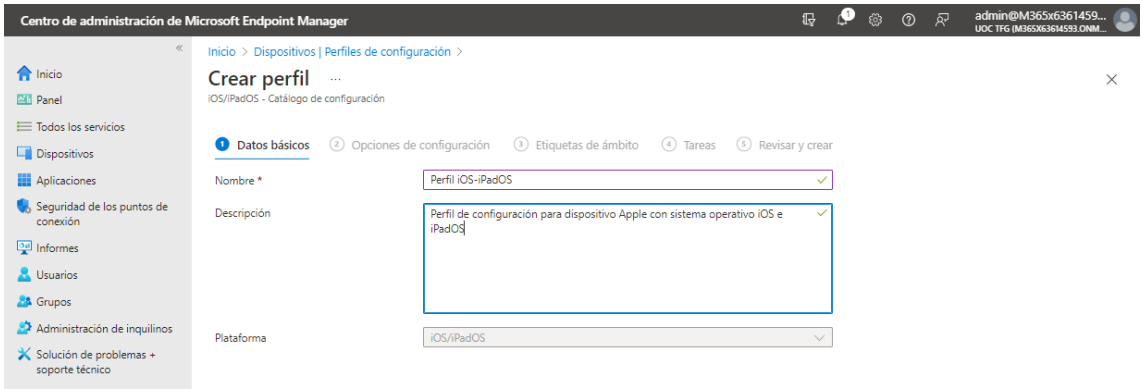

Centro de administración de Microsoft Endpoint Manager
admin@M365x6361459...
UOC TFG (M365X63614593.ONM...
Inicio
Panel
Todos los servicios
Dispositivos
Aplicaciones
Seguridad de los puntos de conexión
Informes
Usuarios
Grupos
Administración de inquilinos
Solución de problemas + soporte técnico
Inicio > Dispositivos | Perfiles de configuración >
Crear perfil
macOS - Catálogo de configuración
Datos básicos
Opciones de configuración
Etiquetas de ámbito
Tareas
Revisar y crear
Resumen
Datos básicos
Nombre
Perfil macOS
Descripción
Perfil de configuración para dispositivos Apple con sistema operativo macOS
Plataforma
macOS
Opciones de configuración
Actualización de software
Instalación de actualizaciones críticas
Verdadero
Descarga automática
Verdadero
Comprobación automática habilitada
Verdadero
Restricciones
Permitir relleno automático de contraseña
Falso
Permitir juegos multijugador
Falso
Permitir Game Center
Falso
Permitir desbloqueo automático
Falso
Permitir Air Drop
Verdadero
Permitir agregar amigos de Game Center
Falso
Seguridad
Código de acceso
Longitud mínima
6
Inactividad máxima
5
Antigüedad máxima del PIN en días
30
Forzar PIN
Verdadero
Etiquetas de ámbito
Predeterminado
Tareas
Grupos incluidos
Grupo
Miembros del grupo
Filtrar
Dispositivos macOS
0 dispositivos, 0 usuarios
Ninguno
Grupos excluidos
Grupo
Miembros del grupo
No hay ningún resultado.
Anterior
Crear

- **Dispositivos iOS e iPadOS**

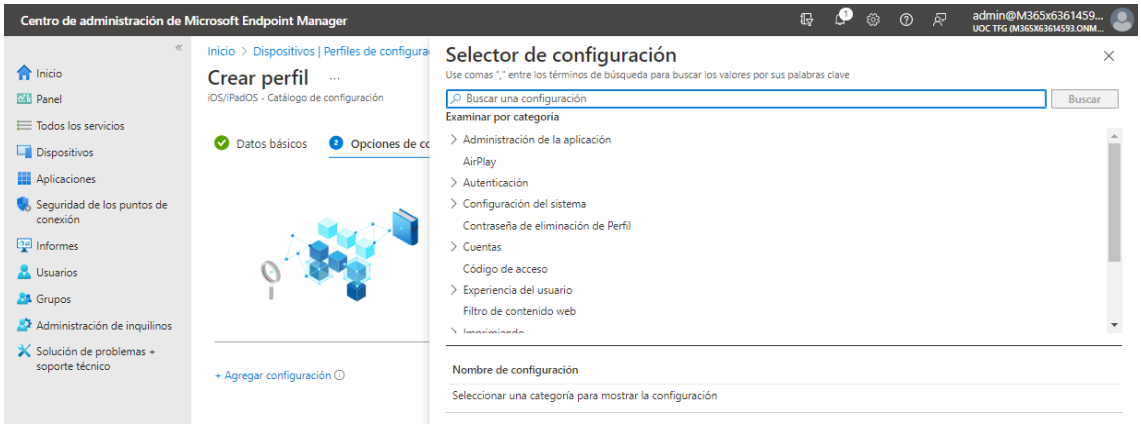
La creación de los perfiles de configuración para los dispositivos Apple con sistemas operativos iOS e iPadOS también es similar a la de los dispositivos Windows y macOS, permitiendo elegir Plantillas o Catálogo de configuración.



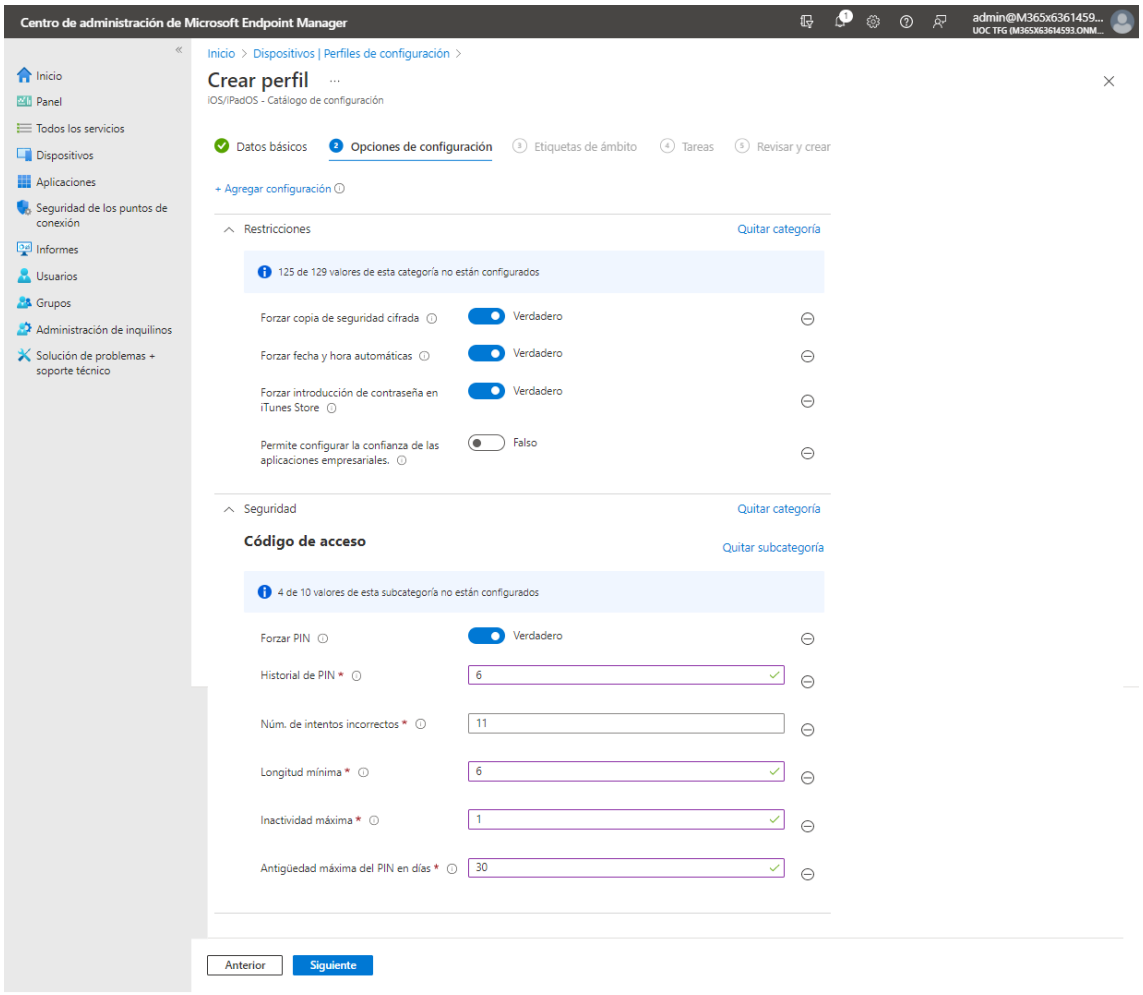
En el primer paso, se introduce el nombre y la descripción del perfil.



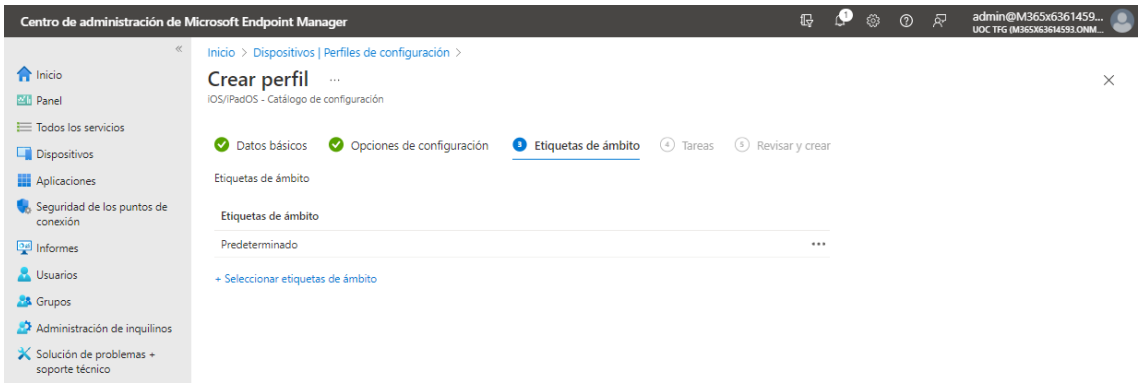
A continuación, se seleccionan las categorías de configuración deseadas.



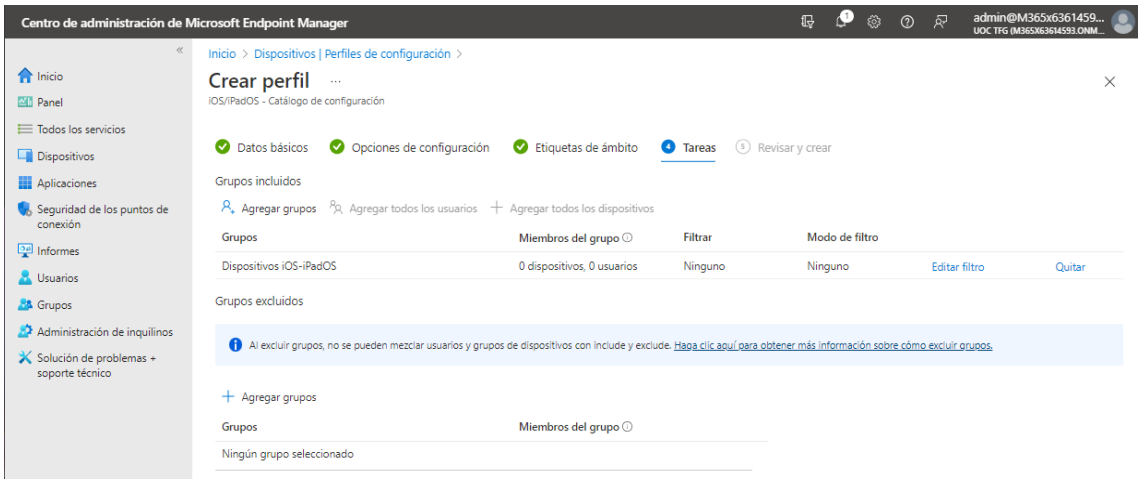
Después, se configuran los parámetros de configuración.

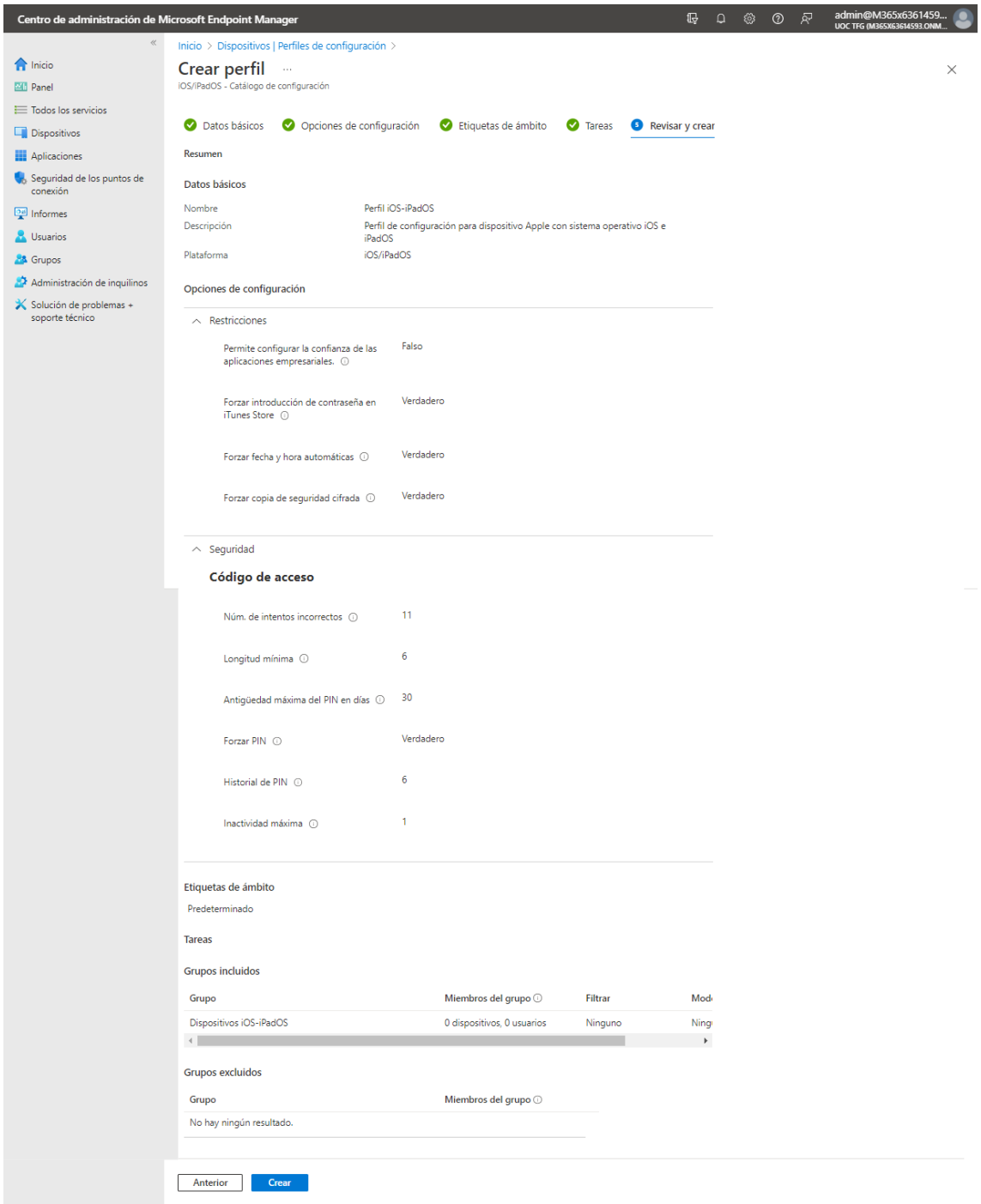


Se añaden las etiquetas de ámbito, en caso de ser necesario.



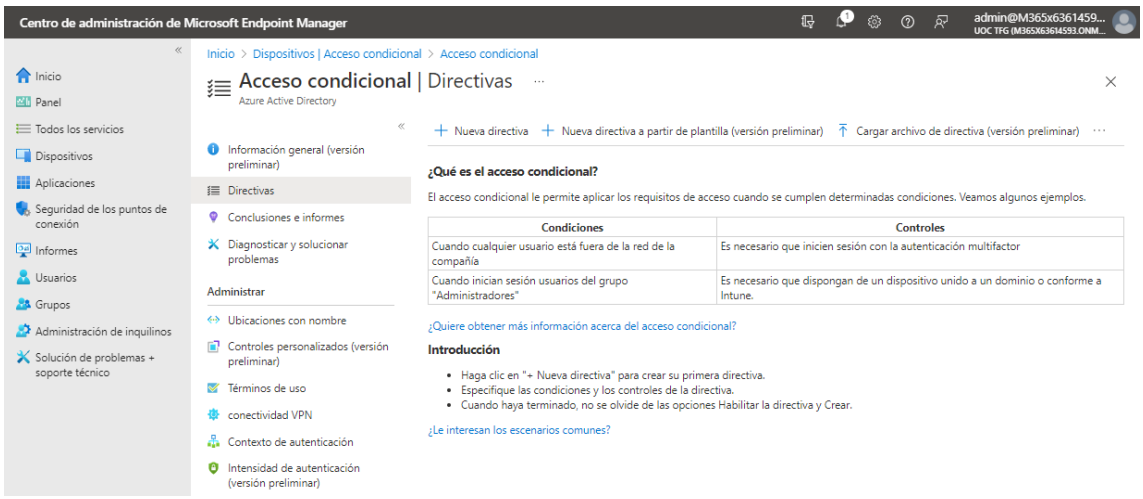
Y, por último, se asigna el perfil al grupo sobre el que se va a aplicar (“Dispositivos iOS-iPadOS”, en este caso) y se revisan los detalles de configuración antes de ordenar la creación del mismo.



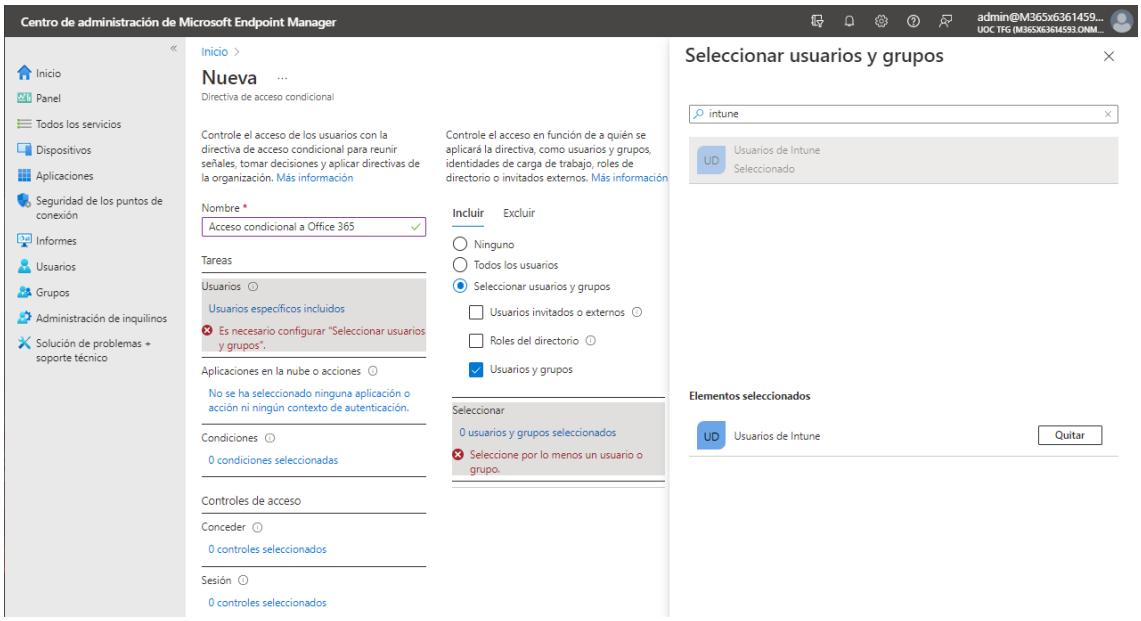

Centro de administración de Microsoft Endpoint Manager
admin@M365x6361459...
UOC TFG (M365X63614593.ONM...
Inicio
Panel
Todos los servicios
Dispositivos
Aplicaciones
Seguridad de los puntos de conexión
Informes
Usuarios
Grupos
Administración de inquilinos
Solución de problemas + soporte técnico
Inicio > Dispositivos | Perfiles de configuración >
Crear perfil
iOS/iPadOS - Catálogo de configuración
Datos básicos
Opciones de configuración
Etiquetas de ámbito
Tareas
Revisar y crear
Resumen
Datos básicos
Nombre
Perfil iOS-iPadOS
Descripción
Perfil de configuración para dispositivo Apple con sistema operativo iOS e iPadOS
Plataforma
iOS/iPadOS
Opciones de configuración
Restricciones
Permite configurar la confianza de las aplicaciones empresariales.
Falso
Forzar introducción de contraseña en iTunes Store
Verdadero
Forzar fecha y hora automáticas
Verdadero
Forzar copia de seguridad cifrada
Verdadero
Seguridad
Código de acceso
Núm. de intentos incorrectos
11
Longitud mínima
6
Antigüedad máxima del PIN en días
30
Forzar PIN
Verdadero
Historial de PIN
6
Inactividad máxima
1
Etiquetas de ámbito
Predeterminado
Tareas
Grupos incluidos
Grupo
Miembros del grupo
Filtrar
Dispositivos iOS-iPadOS
0 dispositivos, 0 usuarios
Ninguno
Grupos excluidos
Grupo
Miembros del grupo
No hay ningún resultado.
Anterior
Crear

Anexo 7. Creación de directiva de acceso condicional

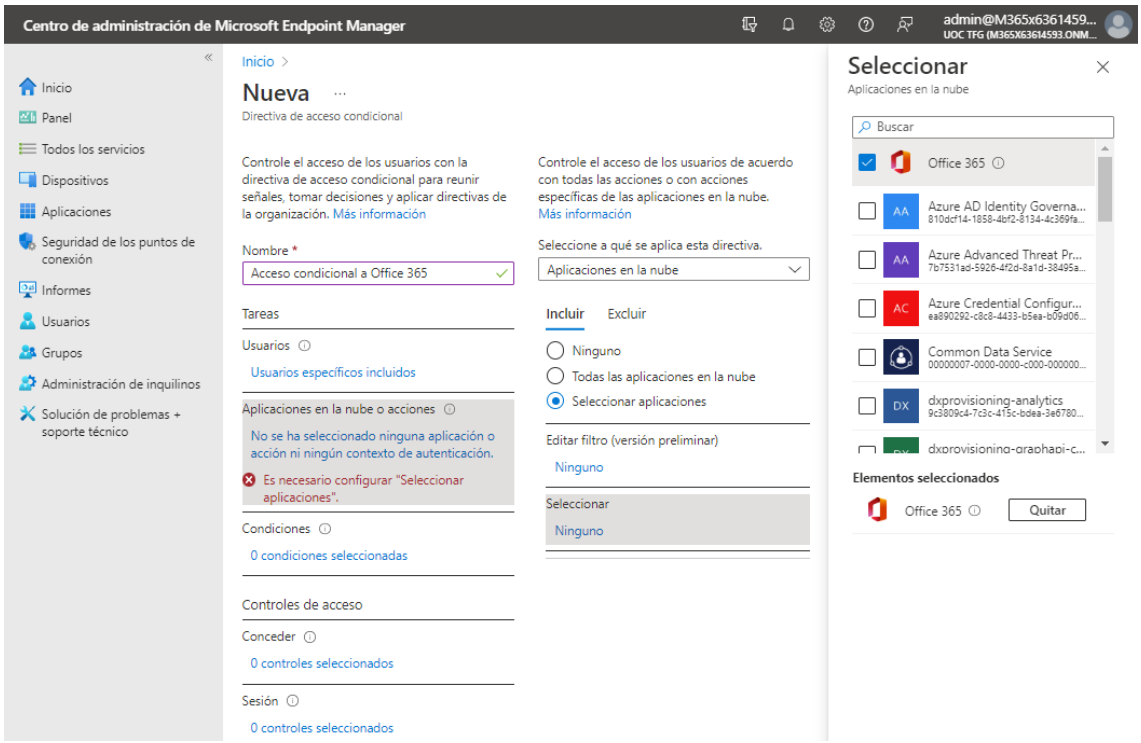
Para crear una directiva de acceso condicionales se debe acceder a Dispositivos/Acceso condicional/Directivas y hacer click en “Nueva directiva”.



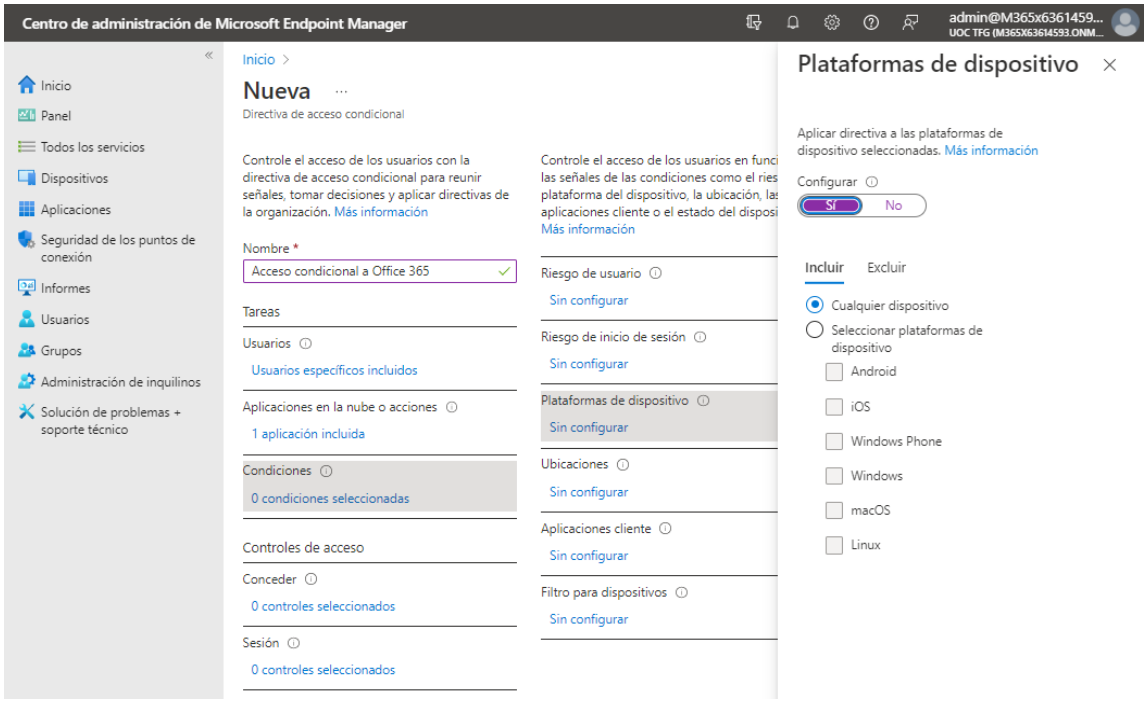
A continuación, se debe seleccionar a qué usuarios se le aplicará la directiva.

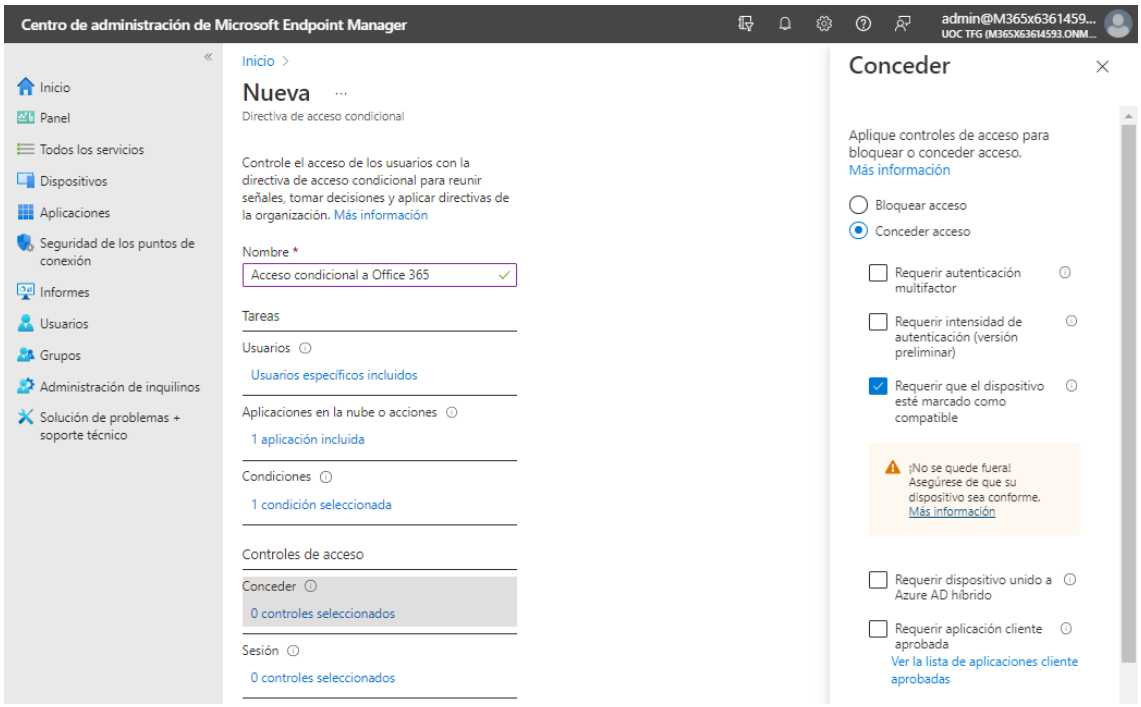


Después, se indican las aplicaciones en la nube o acciones sobre las que se quiere crear la directiva.

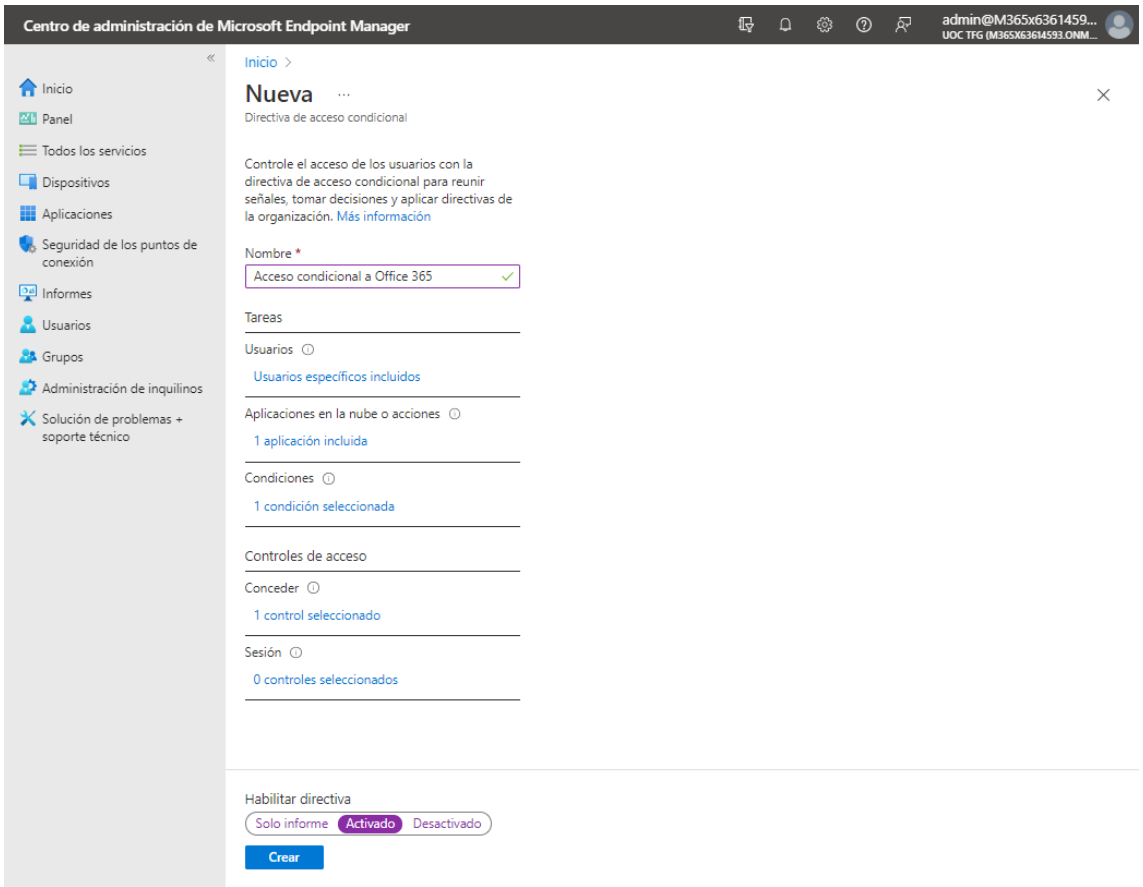


También es necesario indicar las condiciones de la directiva. En este caso consistirá en que cualquier dispositivo inscrito tiene que estar marcado como conforme en las directivas de cumplimiento aplicadas para obtener acceso a los recursos.





Por último, se habilita la directiva.

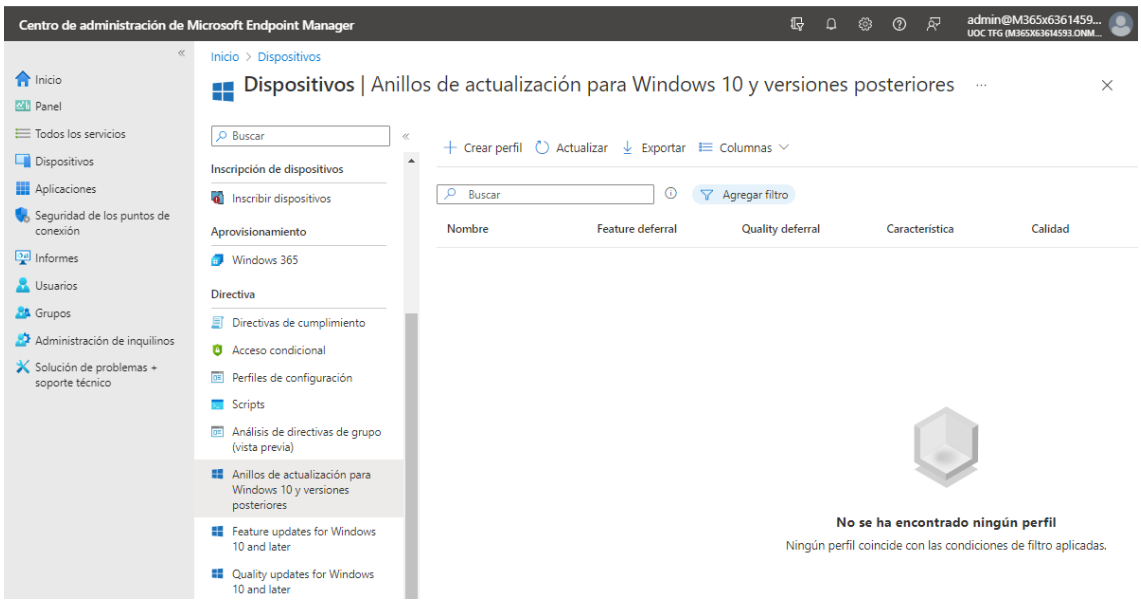


Anexo 8. Creación de perfiles de actualización

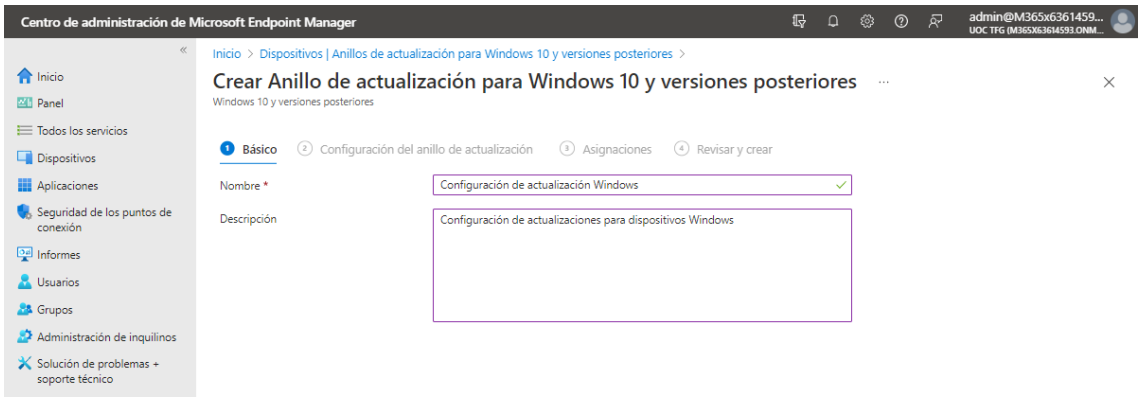
La creación de perfiles de actualización en Microsoft Intune se realiza desde el menú Dispositivos, seleccionando el tipo de directiva de actualización deseada en función de la plataforma.

- **Dispositivos Windows**

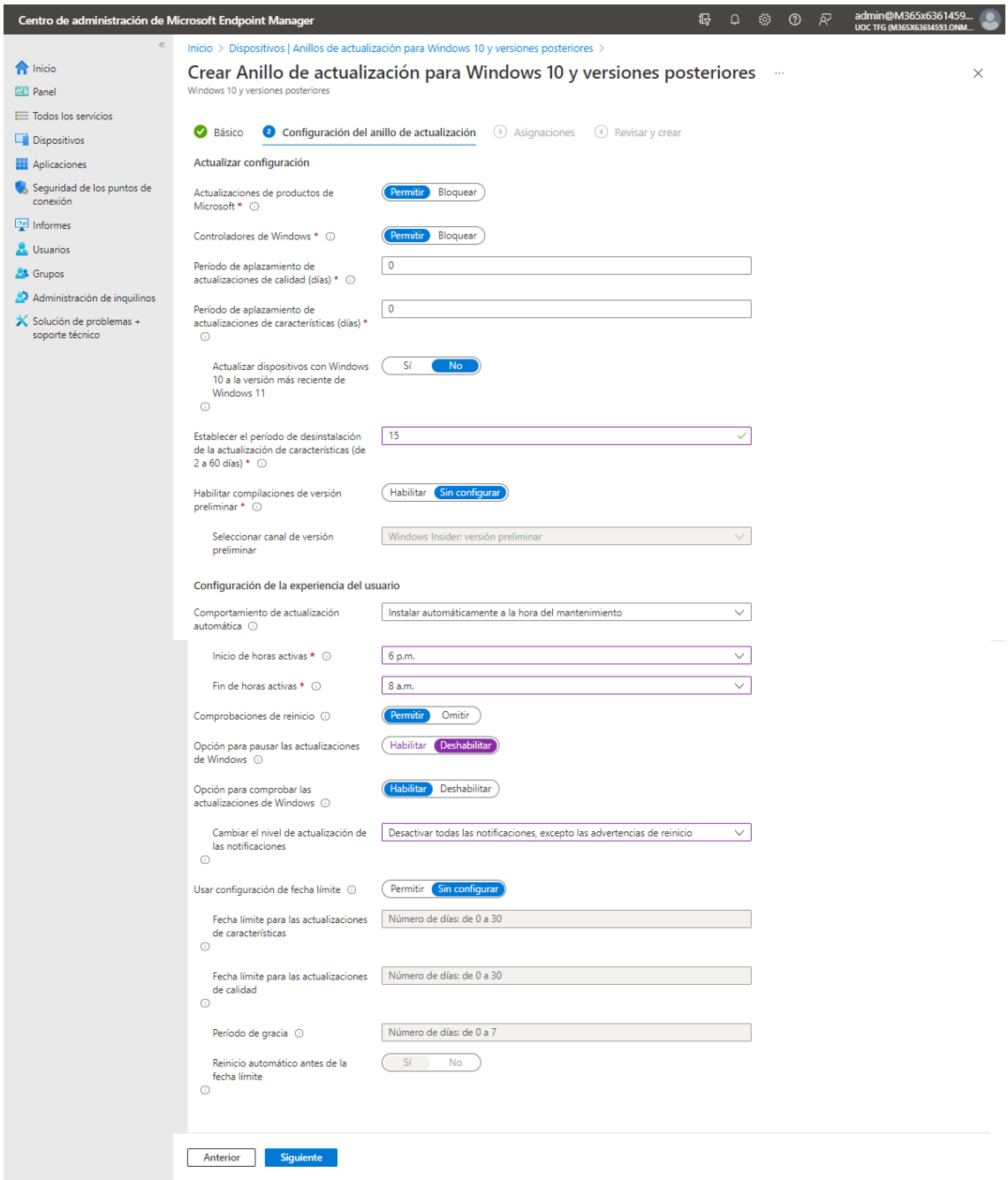
En primer lugar, se crea el perfil del tipo de directiva de actualización deseado de los tres disponibles para los dispositivos con sistema operativo Windows.



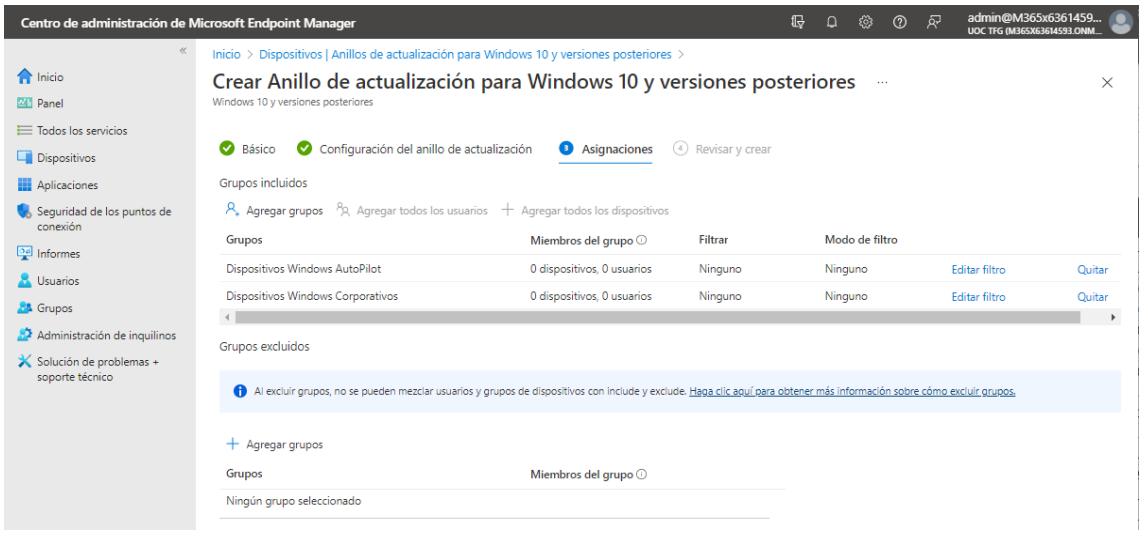
Se especifica el nombre y la descripción de la directiva.

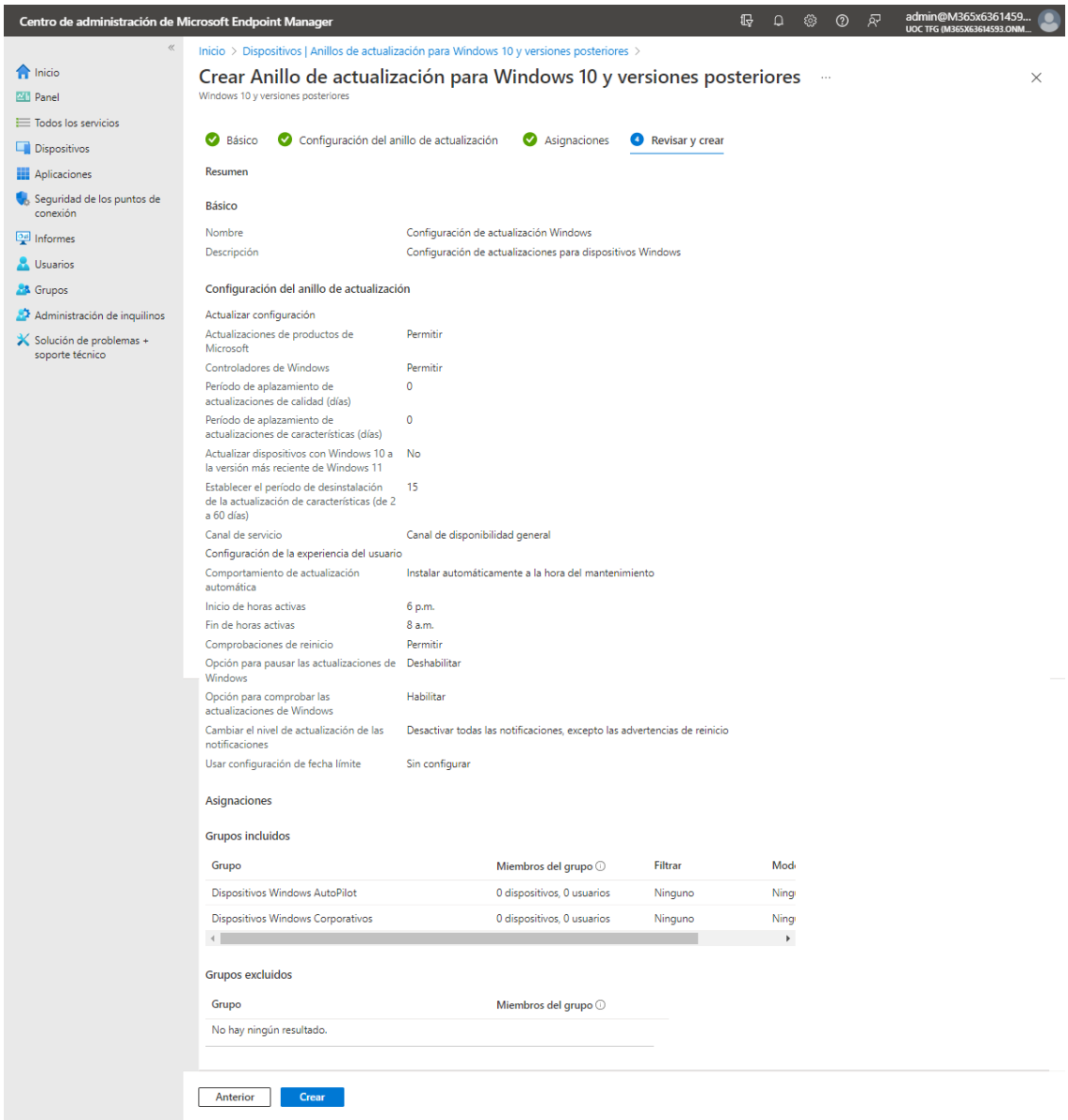


Se realizan las configuraciones deseadas.



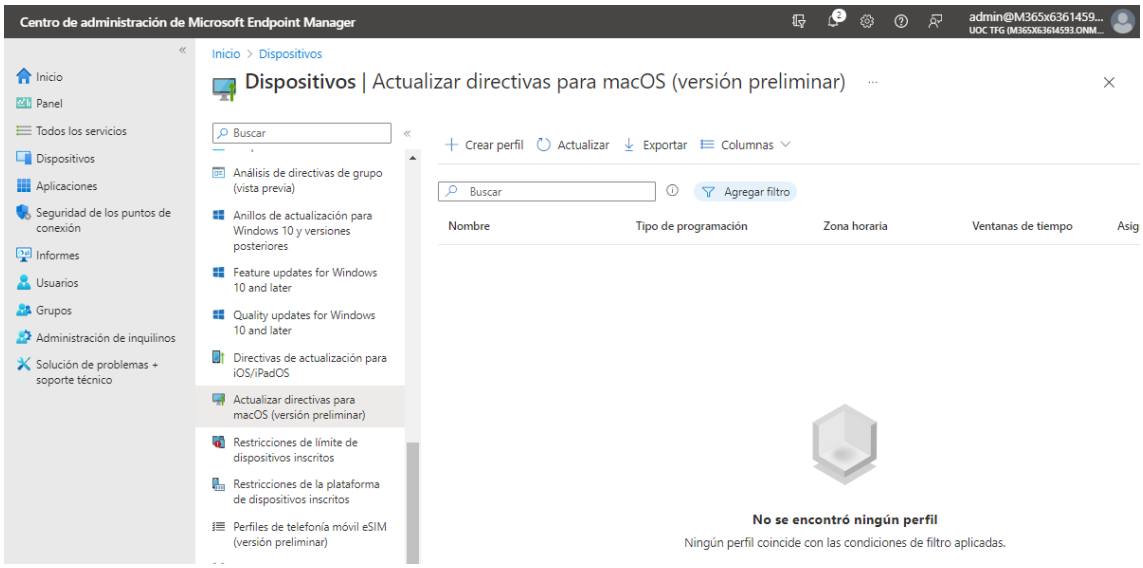
Por último, se asigna la directiva a los grupos en los que se quiera aplicar, se revisa el resumen con los detalles configurados y se lleva a cabo la creación.


Centro de administración de Microsoft Endpoint Manager
admin@M365x6361459...
UOC TFG (M365X63614593.ONM...
Inicio
Panel
Todos los servicios
Dispositivos
Aplicaciones
Seguridad de los puntos de conexión
Informes
Usuarios
Grupos
Administración de inquilinos
Solución de problemas + soporte técnico
Inicio > Dispositivos | Anillos de actualización para Windows 10 y versiones posteriores >
Crear Anillo de actualización para Windows 10 y versiones posteriores
Windows 10 y versiones posteriores
Básico
Configuración del anillo de actualización
3 Asignaciones
4 Revisar y crear
Grupos incluidos
Agregar grupos
Agregar todos los usuarios
Agregar todos los dispositivos
Grupos
Miembros del grupo
Filtrar
Modo de filtro
Dispositivos Windows AutoPilot
0 dispositivos, 0 usuarios
Ninguno
Ninguno
Editar filtro
Quitar
Dispositivos Windows Corporativos
0 dispositivos, 0 usuarios
Ninguno
Ninguno
Editar filtro
Quitar
Grupos excluidos
Al excluir grupos, no se pueden mezclar usuarios y grupos de dispositivos con include y exclude. Haga clic aquí para obtener más información sobre cómo excluir grupos.
Agregar grupos
Grupos
Miembros del grupo
Ningún grupo seleccionado

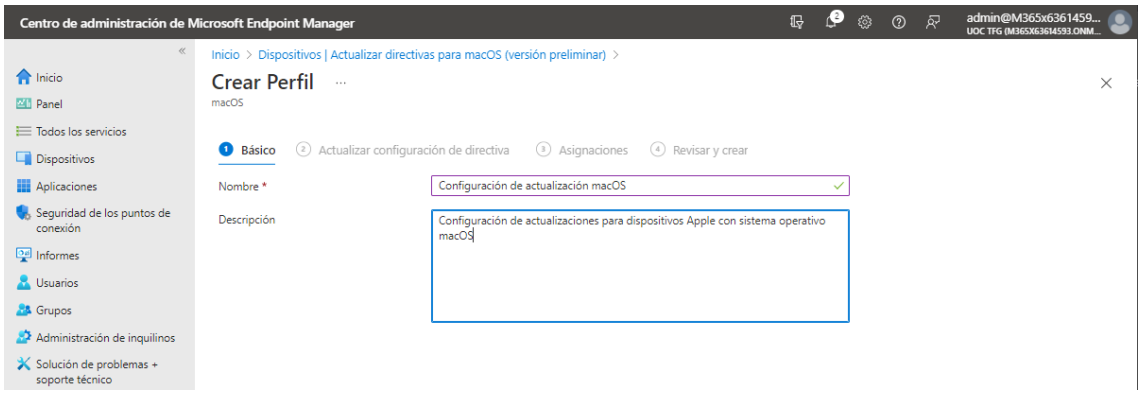

Centro de administración de Microsoft Endpoint Manager
admin@M365x6361459...
UOC TFG (M365X63614593.ONM...
Inicio
Panel
Todos los servicios
Dispositivos
Aplicaciones
Seguridad de los puntos de conexión
Informes
Usuarios
Grupos
Administración de inquilinos
Solución de problemas + soporte técnico
Inicio > Dispositivos | Anillos de actualización para Windows 10 y versiones posteriores >
Crear Anillo de actualización para Windows 10 y versiones posteriores
Windows 10 y versiones posteriores
Básico
Configuración del anillo de actualización
Asignaciones
4 Revisar y crear
Resumen
Básico
Nombre
Configuración de actualización Windows
Descripción
Configuración de actualizaciones para dispositivos Windows
Configuración del anillo de actualización
Actualizar configuración
Actualizaciones de productos de Microsoft
Permitir
Controladores de Windows
Permitir
Período de aplazamiento de actualizaciones de calidad (días)
0
Período de aplazamiento de actualizaciones de características (días)
0
Actualizar dispositivos con Windows 10 a la versión más reciente de Windows 11
No
Establecer el período de desinstalación de la actualización de características (de 2 a 60 días)
15
Canal de servicio
Canal de disponibilidad general
Configuración de la experiencia del usuario
Comportamiento de actualización automática
Instalar automáticamente a la hora del mantenimiento
Inicio de horas activas
6 p.m.
Fin de horas activas
8 a.m.
Comprobaciones de reinicio
Permitir
Opción para pausar las actualizaciones de Windows
Deshabilitar
Opción para comprobar las actualizaciones de Windows
Habilitar
Cambiar el nivel de actualización de las notificaciones
Desactivar todas las notificaciones, excepto las advertencias de reinicio
Usar configuración de fecha límite
Sin configurar
Asignaciones
Grupos incluidos
Grupo
Miembros del grupo
Filtrar
Dispositivos Windows AutoPilot
0 dispositivos, 0 usuarios
Ninguno
Dispositivos Windows Corporativos
0 dispositivos, 0 usuarios
Ninguno
Grupos excluidos
Grupo
Miembros del grupo
No hay ningún resultado.
Anterior
Crear

- **Dispositivos macOS**

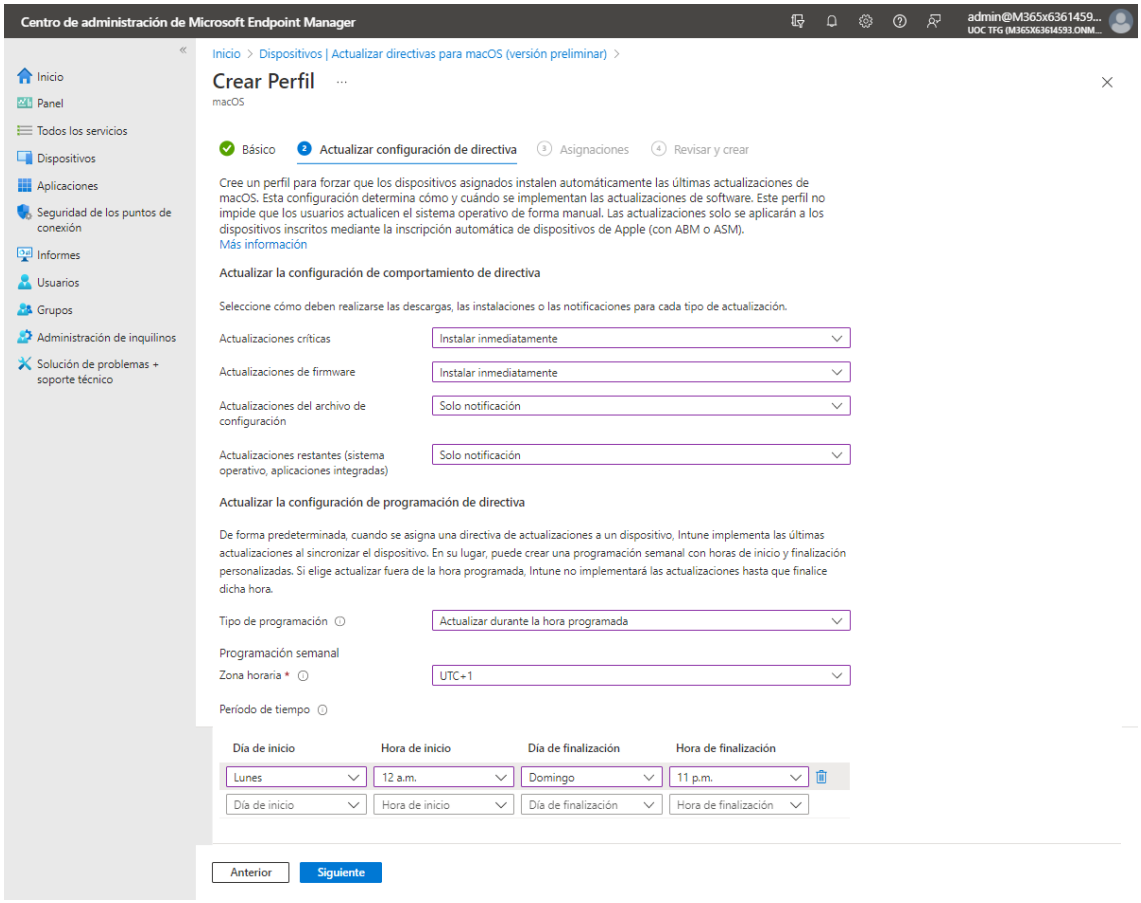
Para los dispositivos con sistema operativo macOS, sólo hay disponible un tipo de directiva de actualización.



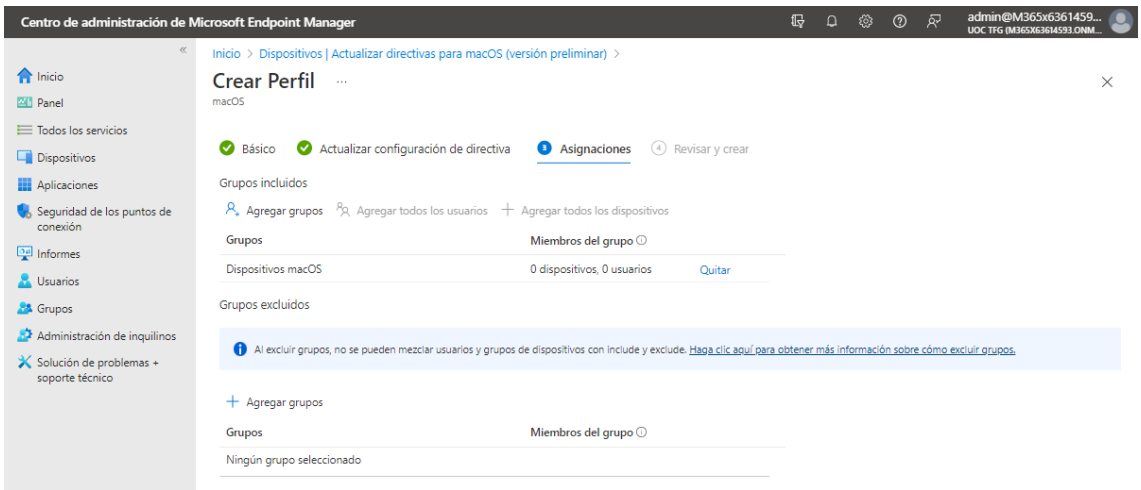
Al crear el perfil, se indica el nombre y la descripción del mismo en el primer paso, como es habitual.

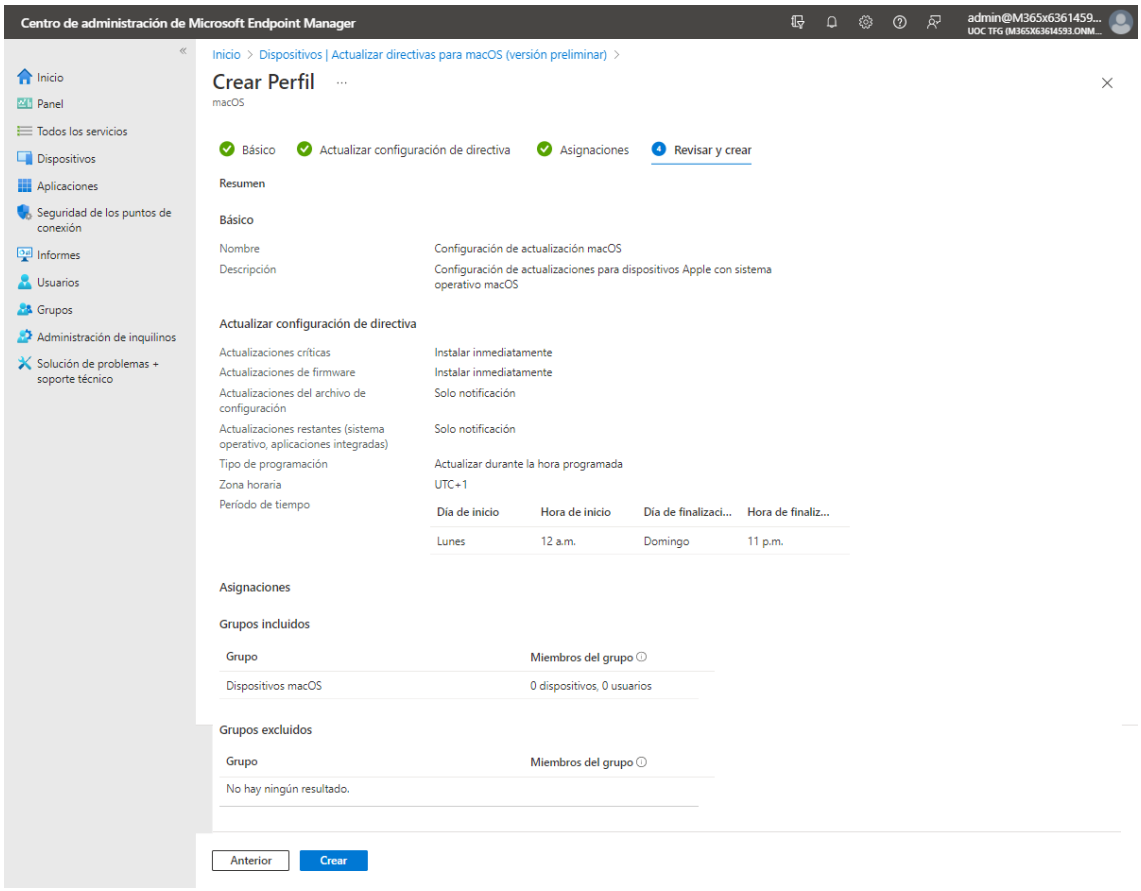


A continuación, se configura la directiva con los parámetros deseados.



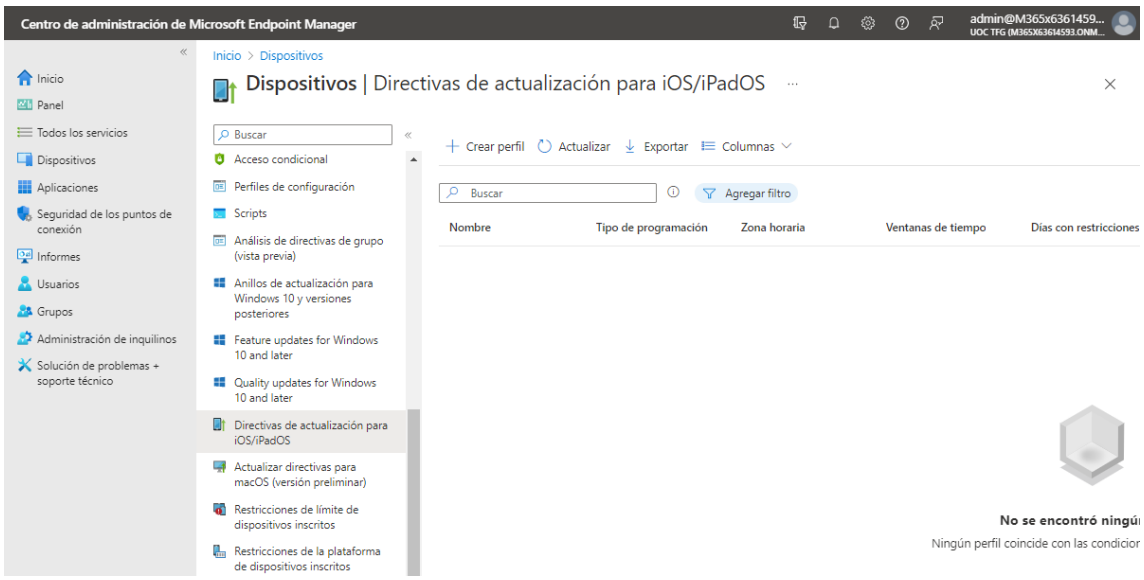
Para finalizar, se asigna el perfil a los grupos deseados y se realiza la creación.

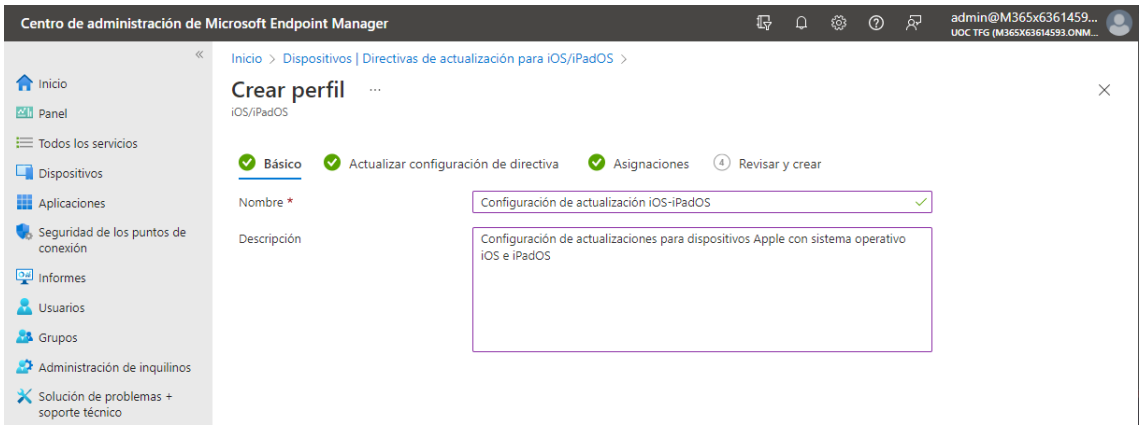




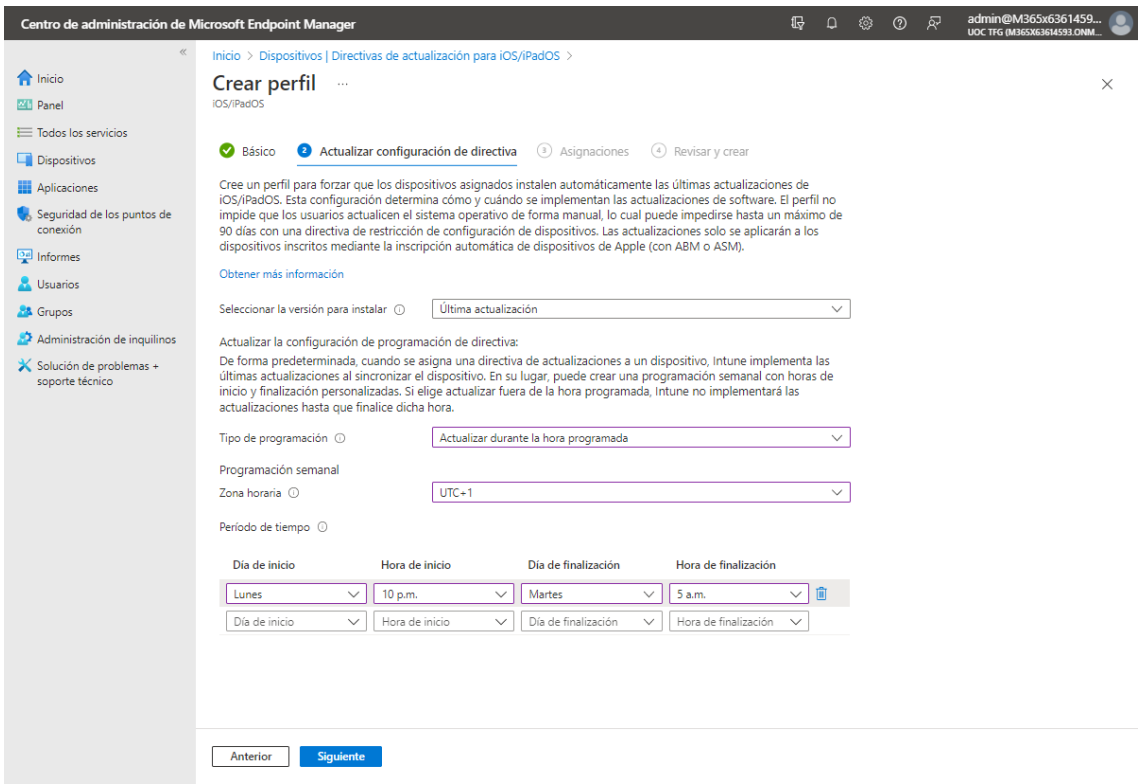
- **<u>Dispositivos iOS e iPadOS</u>**

Para los dispositivos con sistema operativo iOS e iPadOS también solo hay disponible un tipo de directiva de actualización, por lo que se crea el perfil.

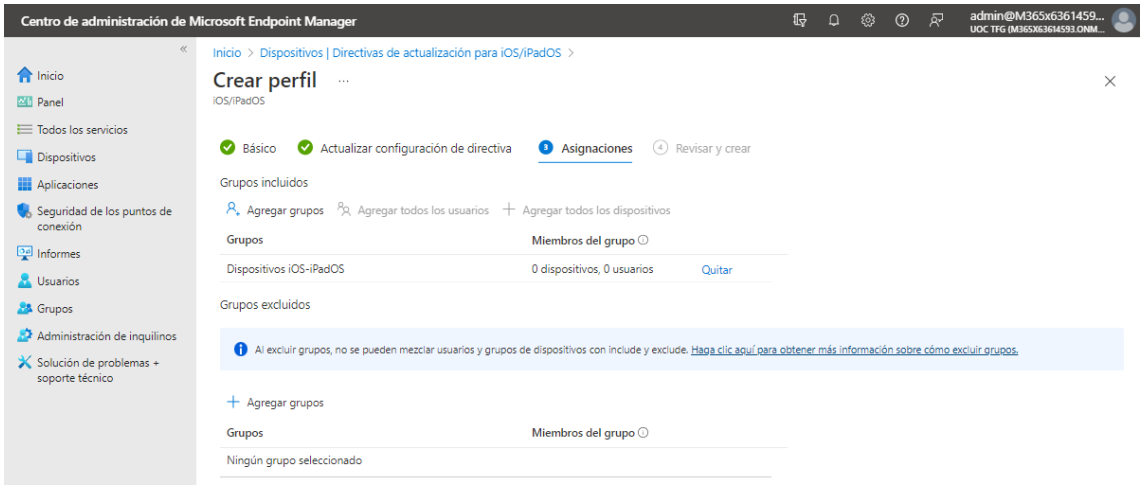


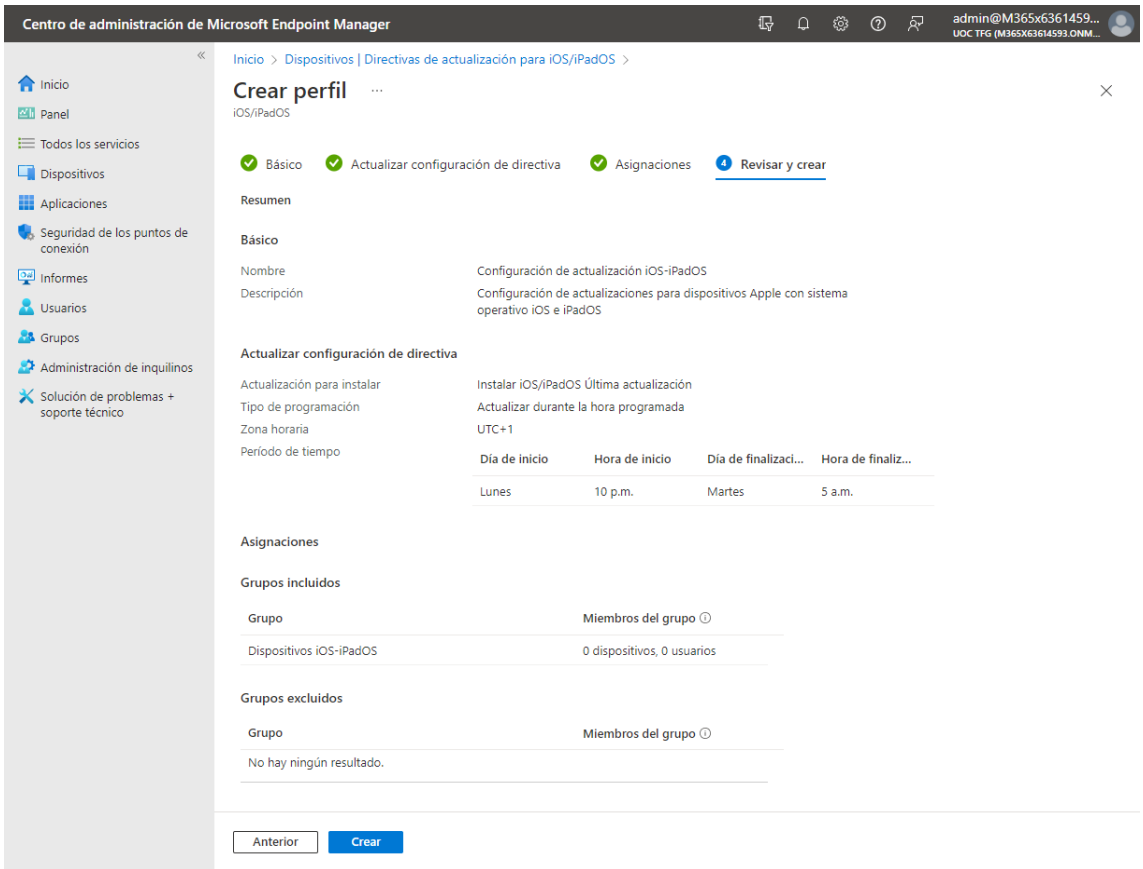


Tras introducir el nombre y descripción, se escogen las configuraciones deseadas.



Para finalizar, se asigna el perfil a los grupos deseados y se revisan los detalles configurados antes de ordenar la creación del mismo.



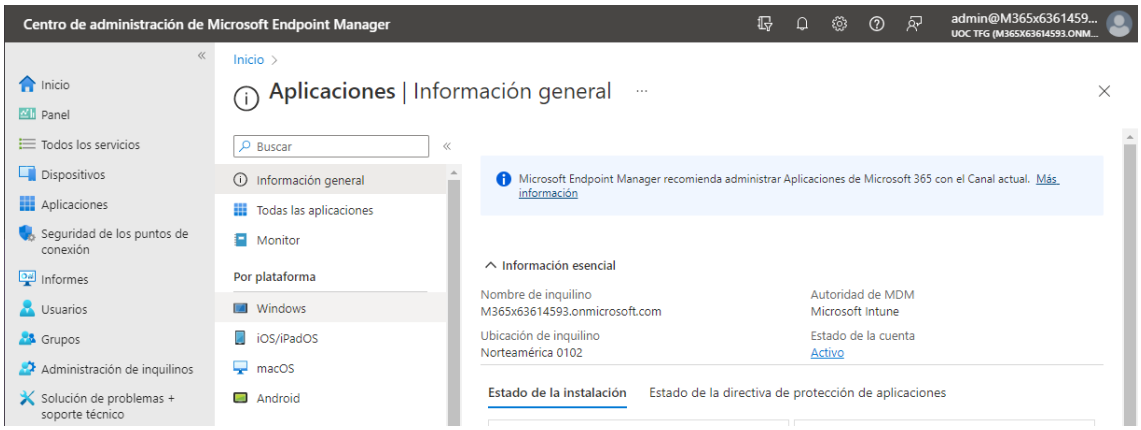


Anexo 9. Despliegue de aplicaciones por plataforma

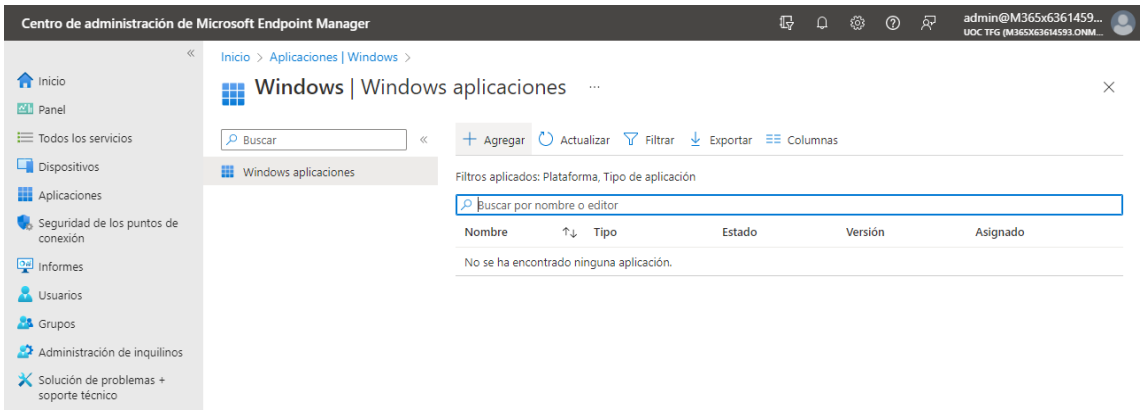
Microsoft Intune permite desplegar aplicaciones para los dispositivos con plataforma Windows, iOS/iPadOS, macOS y Android, accediendo a la plataforma deseada desde el menú “Aplicaciones”. A continuación, se detalla el proceso de despliegue para cada una de las plataformas.

- **Dispositivos Windows**

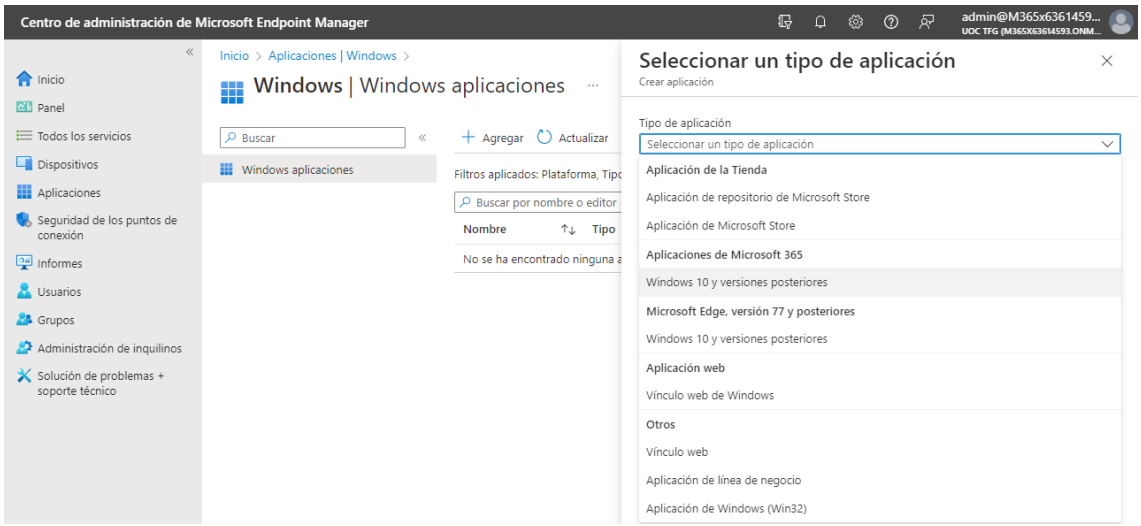
Para crear un despliegue de aplicación para dispositivos con sistema operativo Windows se debe seleccionar Windows dentro del menú “Aplicaciones”.



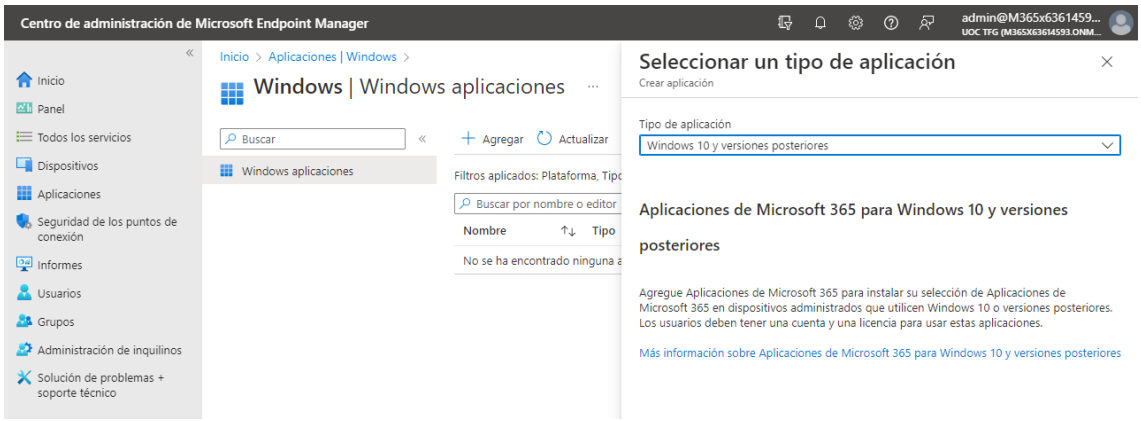
A continuación, se hace click en “Agregar”.



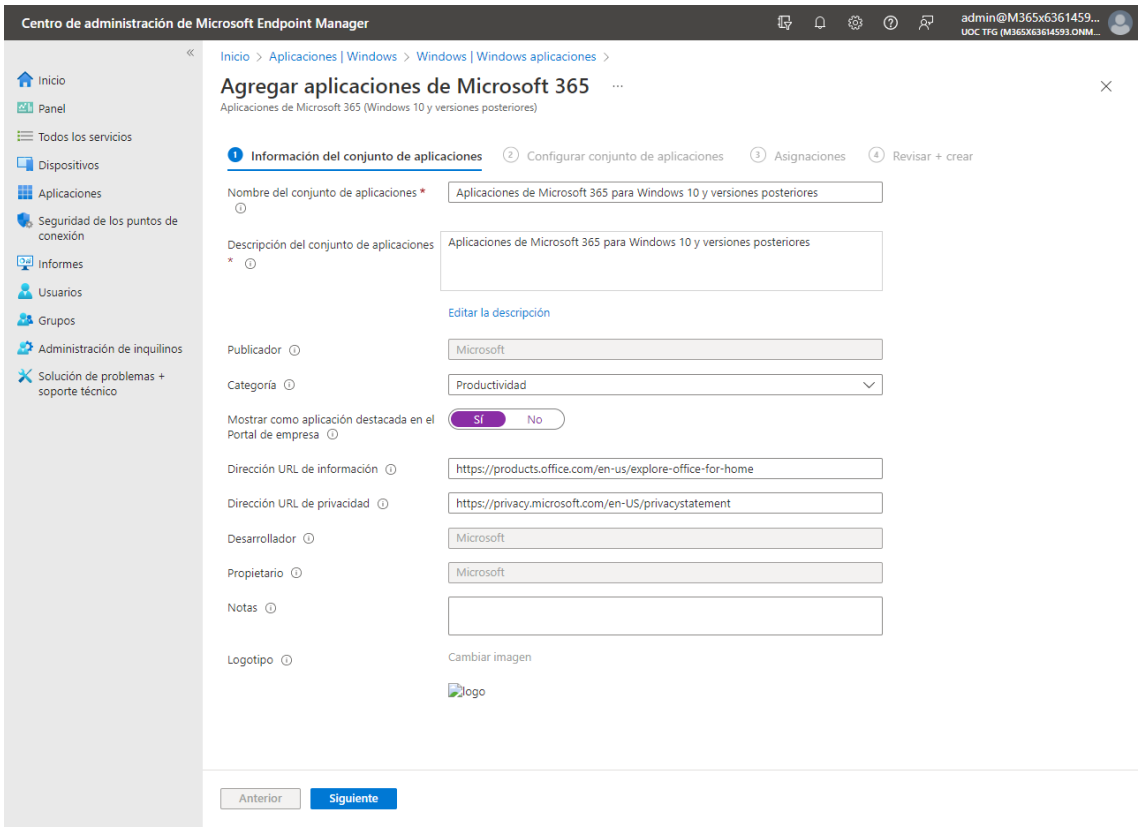
Se debe seleccionar un tipo de aplicación de los disponibles para la plataforma. Entre ellos, se encuentran aplicaciones de la tienda de Microsoft, aplicaciones de Microsoft 365, Microsoft Edge Chromium, aplicaciones web, aplicaciones de línea de negocio o aplicaciones clásicas Win32.

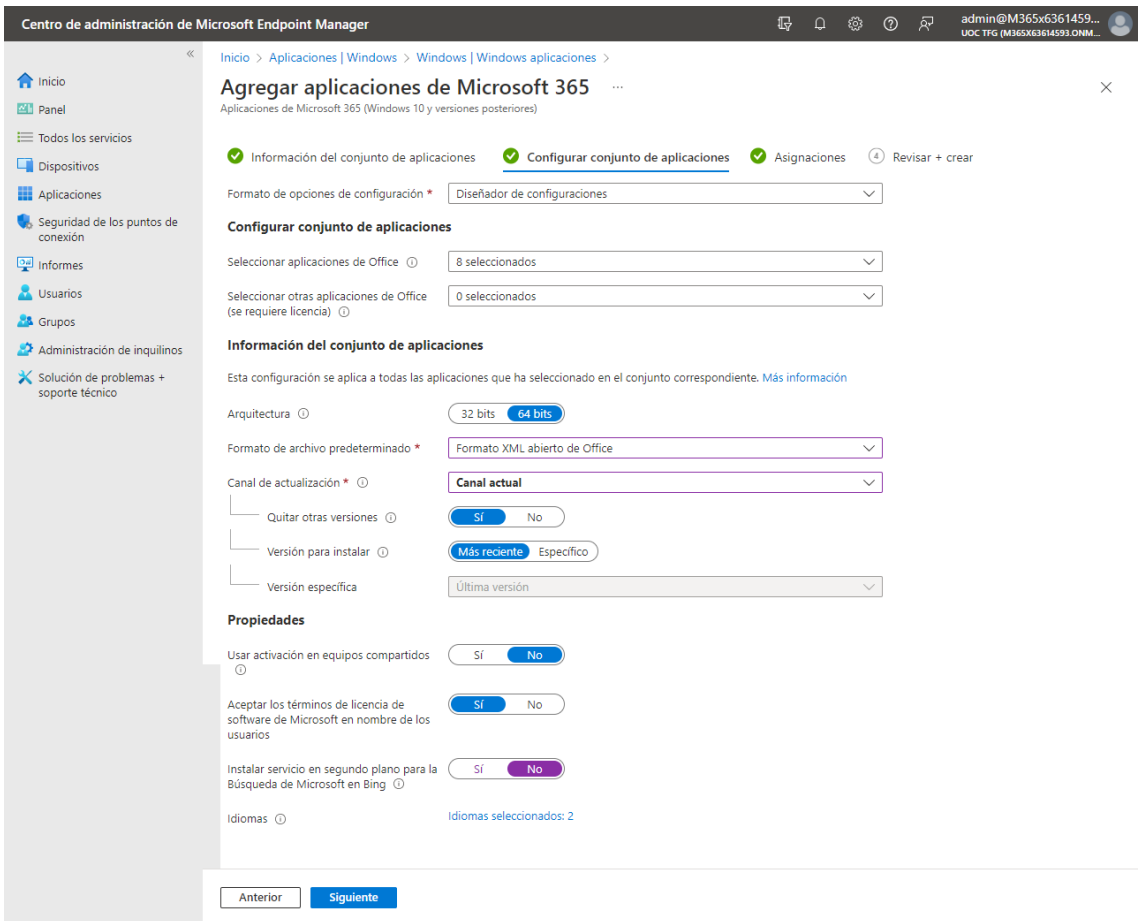


En este caso, la aplicación seleccionada es Microsoft 365 (anteriormente conocida como Microsoft Office).

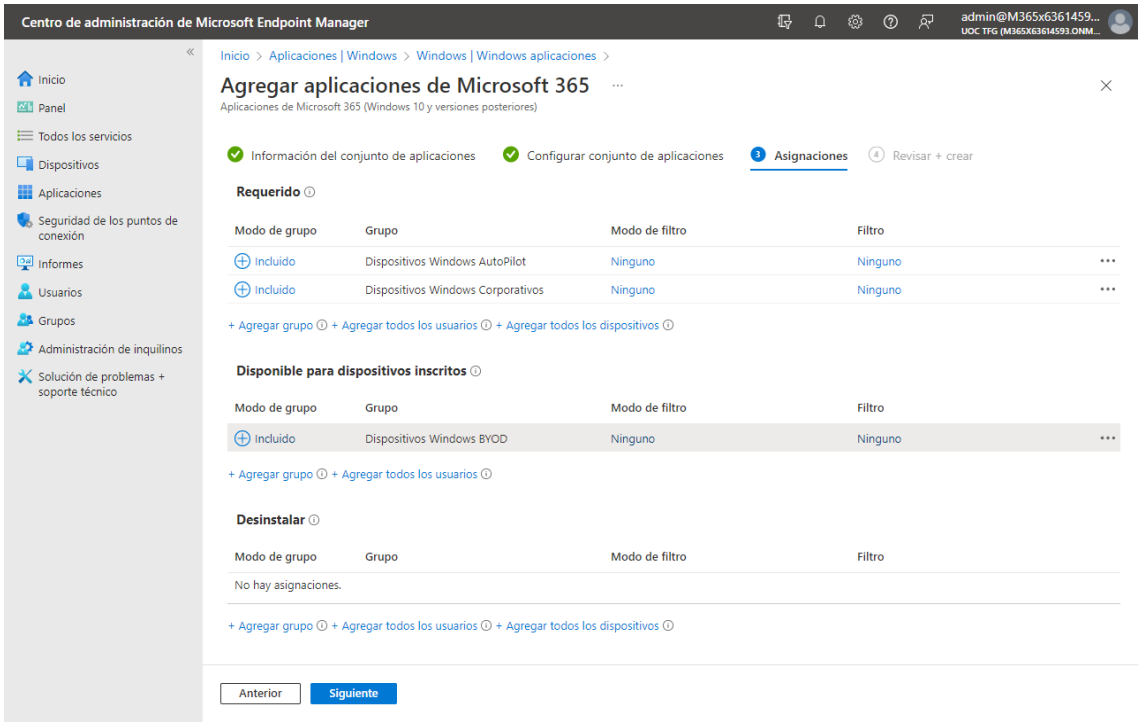


Una vez seleccionado el tipo de aplicación, se configuran los parámetros de la misma. Estos varían en función del tipo de aplicación elegida.

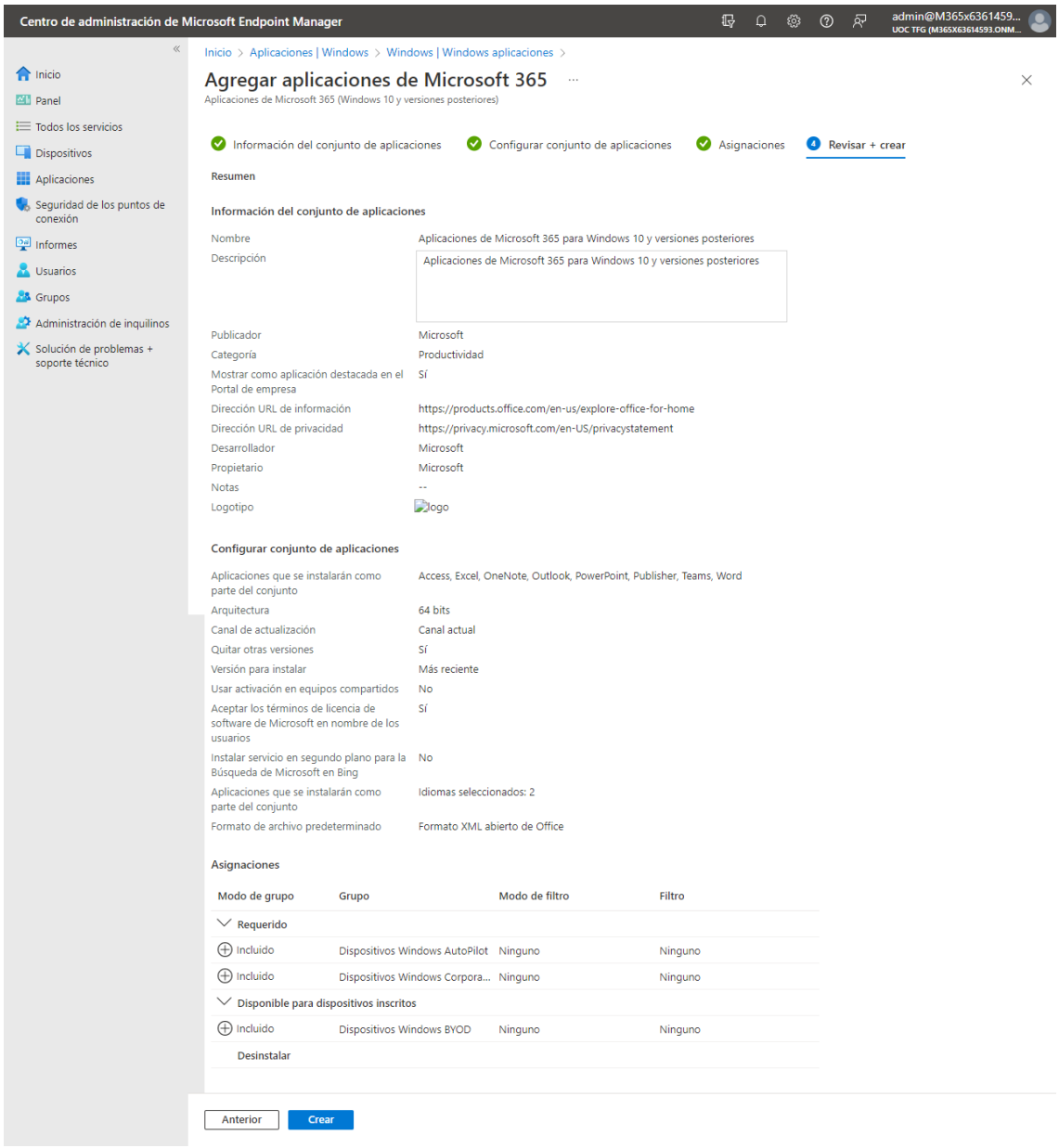

Centro de administración de Microsoft Endpoint Manager
admin@M365x6361459...
UOC TFG (M365X63614593.ONM...
Inicio
Panel
Todos los servicios
Dispositivos
Aplicaciones
Seguridad de los puntos de conexión
Informes
Usuarios
Grupos
Administración de inquilinos
Solución de problemas + soporte técnico
Inicio > Aplicaciones | Windows > Windows | Windows aplicaciones >
Agregar aplicaciones de Microsoft 365
Aplicaciones de Microsoft 365 (Windows 10 y versiones posteriores)
1 Información del conjunto de aplicaciones
2 Configurar conjunto de aplicaciones
3 Asignaciones
4 Revisar + crear
Nombre del conjunto de aplicaciones *
Aplicaciones de Microsoft 365 para Windows 10 y versiones posteriores
Descripción del conjunto de aplicaciones *
Aplicaciones de Microsoft 365 para Windows 10 y versiones posteriores
Editar la descripción
Publicador
Microsoft
Categoría
Productividad
Mostrar como aplicación destacada en el Portal de empresa
Sí
No
Dirección URL de información
https://products.office.com/en-us/explore-office-for-home
Dirección URL de privacidad
https://privacy.microsoft.com/en-US/privacystatement
Desarrollador
Microsoft
Propietario
Microsoft
Notas
Logotipo
Cambiar imagen
logo
Anterior
Siguiente


Centro de administración de Microsoft Endpoint Manager
admin@M365x6361459...
UOC TFG (M365X63614593.ONM...
Inicio
Panel
Todos los servicios
Dispositivos
Aplicaciones
Seguridad de los puntos de conexión
Informes
Usuarios
Grupos
Administración de inquilinos
Solución de problemas + soporte técnico
Inicio > Aplicaciones | Windows > Windows | Windows aplicaciones >
Agregar aplicaciones de Microsoft 365
Aplicaciones de Microsoft 365 (Windows 10 y versiones posteriores)
Información del conjunto de aplicaciones
Configurar conjunto de aplicaciones
Asignaciones
4 Revisar + crear
Formato de opciones de configuración *
Diseñador de configuraciones
Configurar conjunto de aplicaciones
Seleccionar aplicaciones de Office
8 seleccionados
Seleccionar otras aplicaciones de Office (se requiere licencia)
0 seleccionados
Información del conjunto de aplicaciones
Esta configuración se aplica a todas las aplicaciones que ha seleccionado en el conjunto correspondiente. Más información
Arquitectura
32 bits
64 bits
Formato de archivo predeterminado *
Formato XML abierto de Office
Canal de actualización *
Canal actual
Quitar otras versiones
Sí
No
Versión para instalar
Más reciente
Específico
Versión específica
Última versión
Propiedades
Usar activación en equipos compartidos
Sí
No
Aceptar los términos de licencia de software de Microsoft en nombre de los usuarios
Sí
No
Instalar servicio en segundo plano para la Búsqueda de Microsoft en Bing
Sí
No
Idiomas
Idiomas seleccionados: 2
Anterior
Siguiente

Para finalizar, se asigna la aplicación al grupo o grupos sobre los que se quiere aplicar y el modo en el que se instalará, si de forma requerida o estará disponible para su instalación en el portal de empresa.

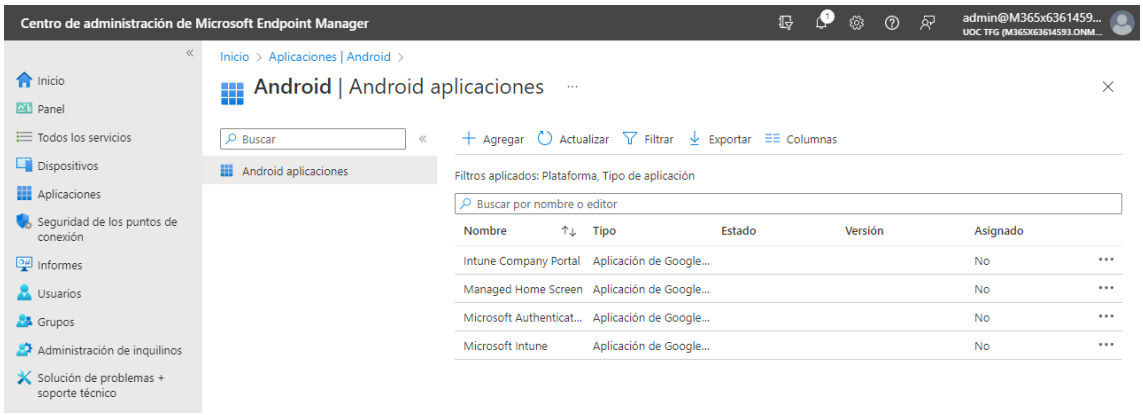


Se revisan los detalles de la configuración realizada para el despliegue de la aplicación y se lleva a cabo su creación.


Centro de administración de Microsoft Endpoint Manager
admin@M365x6361459...
UOC TFG (M365X63614593.ONM...
Inicio
Panel
Todos los servicios
Dispositivos
Aplicaciones
Seguridad de los puntos de conexión
Informes
Usuarios
Grupos
Administración de inquilinos
Solución de problemas + soporte técnico
Inicio > Aplicaciones | Windows > Windows | Windows aplicaciones >
Agregar aplicaciones de Microsoft 365
Aplicaciones de Microsoft 365 (Windows 10 y versiones posteriores)
Información del conjunto de aplicaciones
Configurar conjunto de aplicaciones
Asignaciones
4 Revisar + crear
Resumen
Información del conjunto de aplicaciones
Nombre
Aplicaciones de Microsoft 365 para Windows 10 y versiones posteriores
Descripción
Aplicaciones de Microsoft 365 para Windows 10 y versiones posteriores
Publicador
Microsoft
Categoría
Productividad
Mostrar como aplicación destacada en el Portal de empresa
Sí
Dirección URL de información
https://products.office.com/en-us/explore-office-for-home
Dirección URL de privacidad
https://privacy.microsoft.com/en-US/privacystatement
Desarrollador
Microsoft
Propietario
Microsoft
Notas
--
Logotipo
logo
Configurar conjunto de aplicaciones
Aplicaciones que se instalarán como parte del conjunto
Access, Excel, OneNote, Outlook, PowerPoint, Publisher, Teams, Word
Arquitectura
64 bits
Canal de actualización
Canal actual
Quitar otras versiones
Sí
Versión para instalar
Más reciente
Usar activación en equipos compartidos
No
Aceptar los términos de licencia de software de Microsoft en nombre de los usuarios
Sí
Instalar servicio en segundo plano para la Búsqueda de Microsoft en Bing
No
Aplicaciones que se instalarán como parte del conjunto
Idiomas seleccionados: 2
Formato de archivo predeterminado
Formato XML abierto de Office
Asignaciones
Modo de grupo
Grupo
Modo de filtro
Filtro
Requerido
Incluido
Dispositivos Windows AutoPilot
Ninguno
Ninguno
Incluido
Dispositivos Windows Corpora...
Ninguno
Ninguno
Disponible para dispositivos inscritos
Incluido
Dispositivos Windows BYOD
Ninguno
Ninguno
Desinstalar
Anterior
Crear

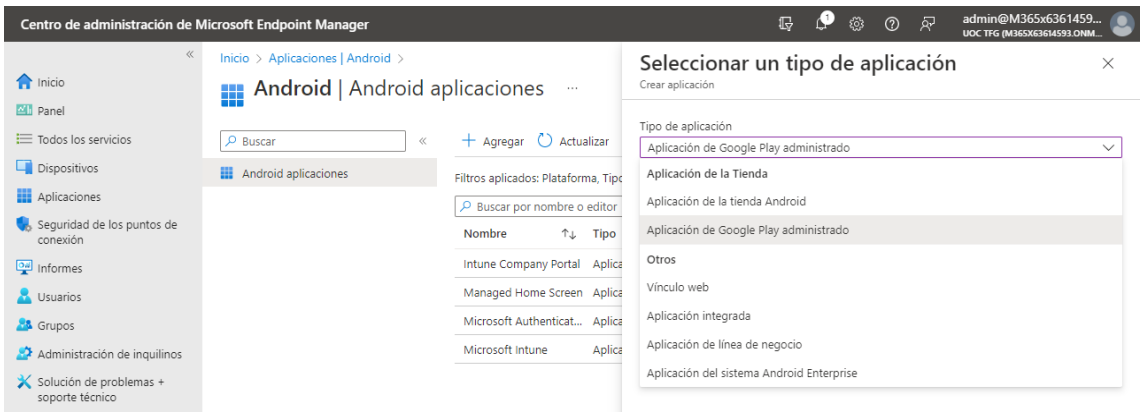
- **Dispositivos Android**

Para los dispositivos Android, se accede a la plataforma Android dentro del menú “Aplicaciones” y se hace click en “Agregar”.



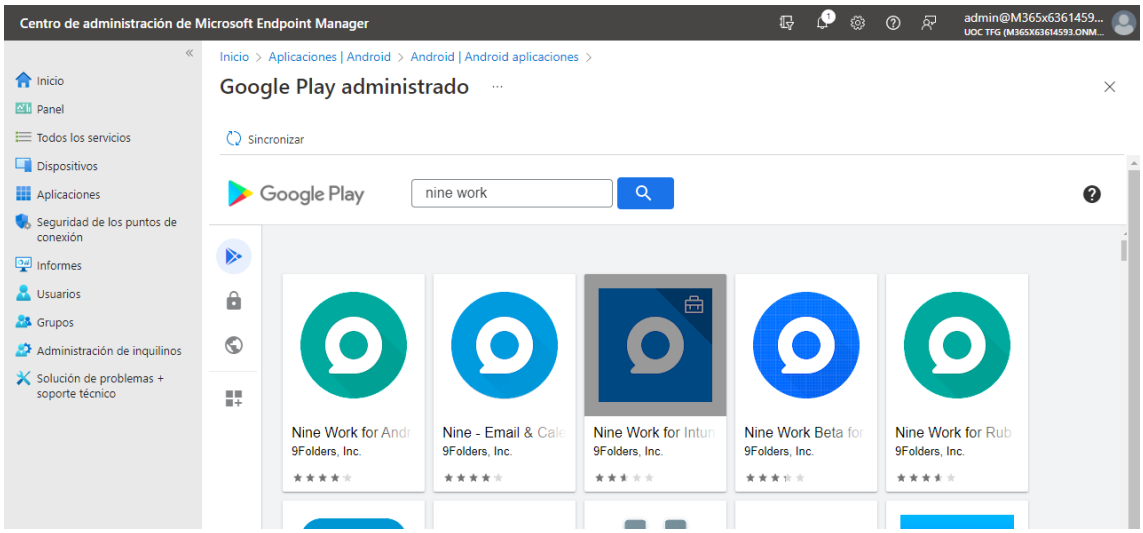
Como en el caso anterior, se selecciona el tipo de aplicación de las disponibles. En este caso, se quiere desplegar el gestor de correo “Nine Work”, para el que se ha creado un perfil de configuración previamente para los dispositivos Android Enterprise BYOD.

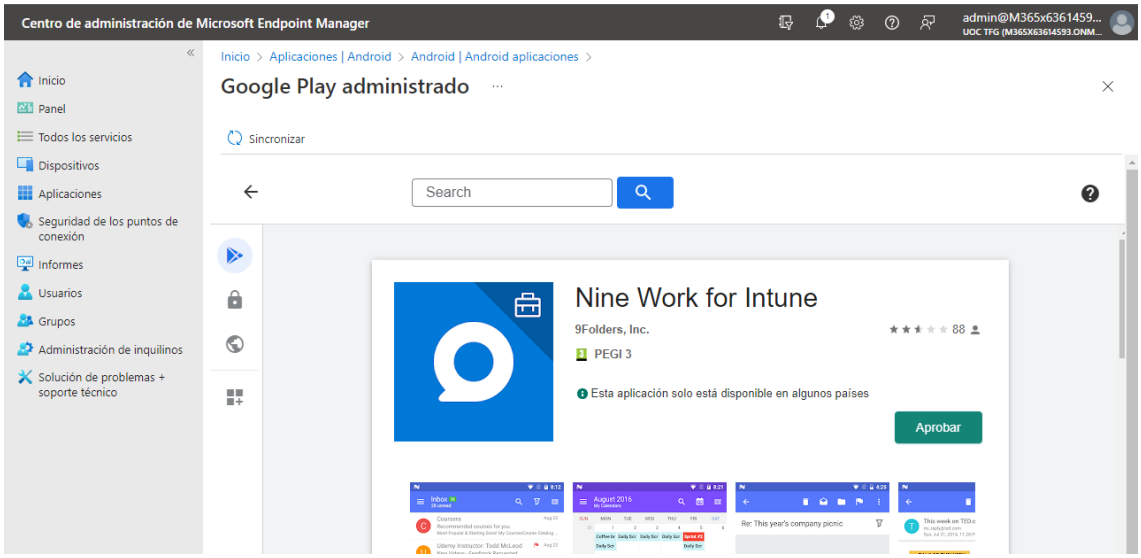
Por tanto, se selecciona “Aplicación de Google Play administrado” en el tipo de aplicación.



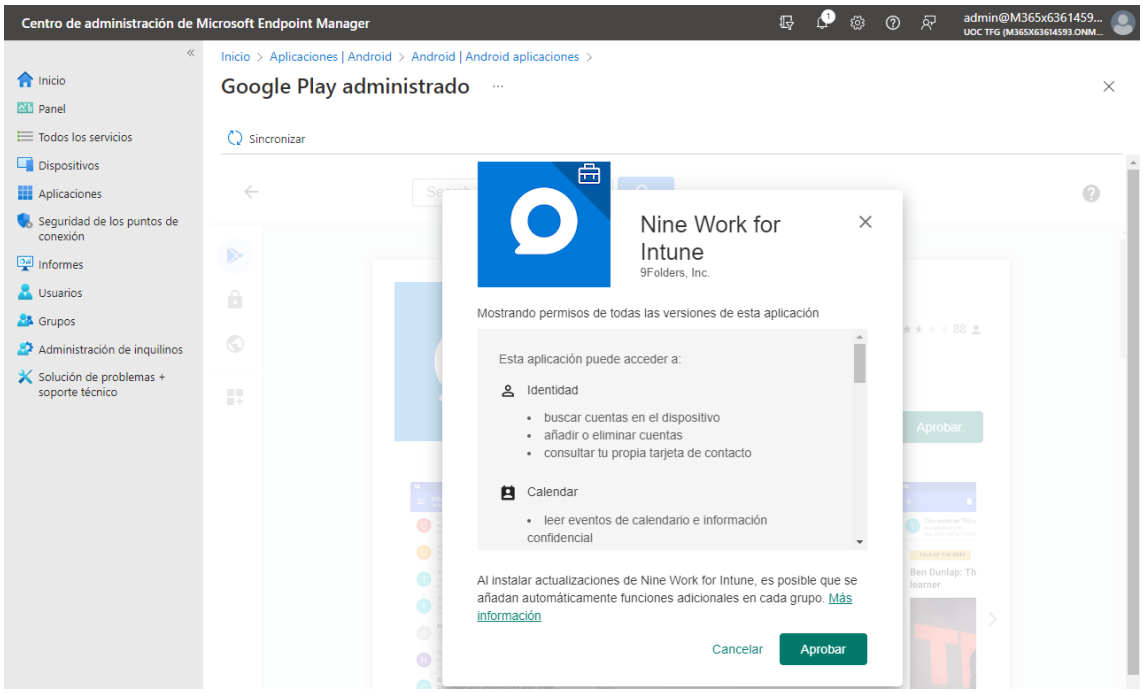
A continuación, se muestra Google Play Store embebido en el portal de administración de Intune, ya que se trata del Google Play administrado por la organización, independiente del Google Play Store público de la parte personal de los dispositivos.

Se busca la aplicación que se quiere desplegar y se aprueba.

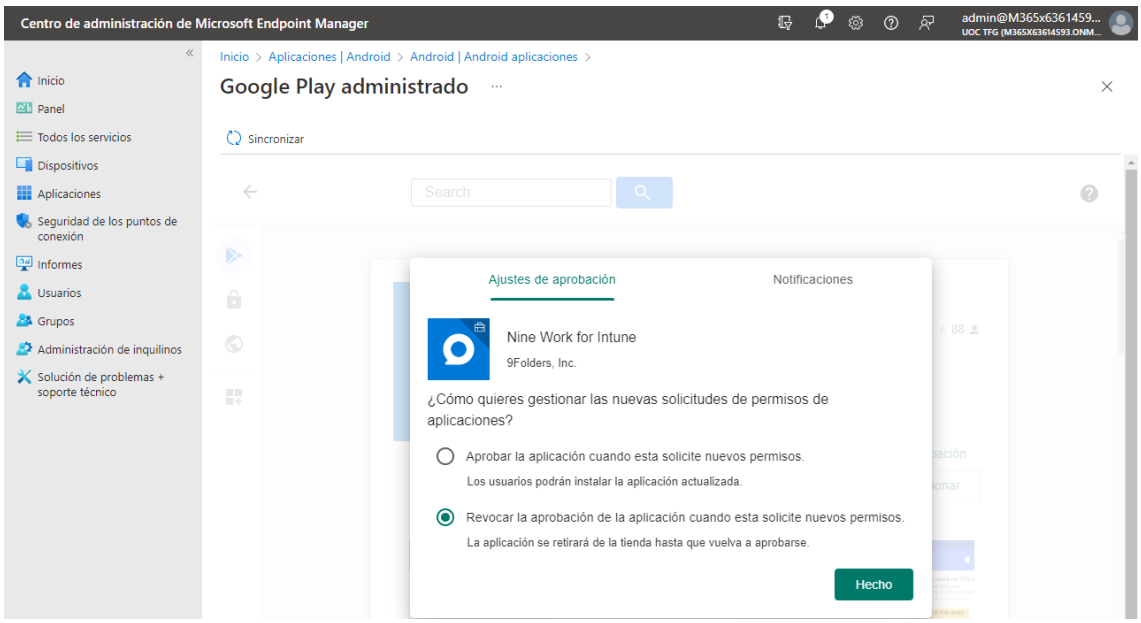




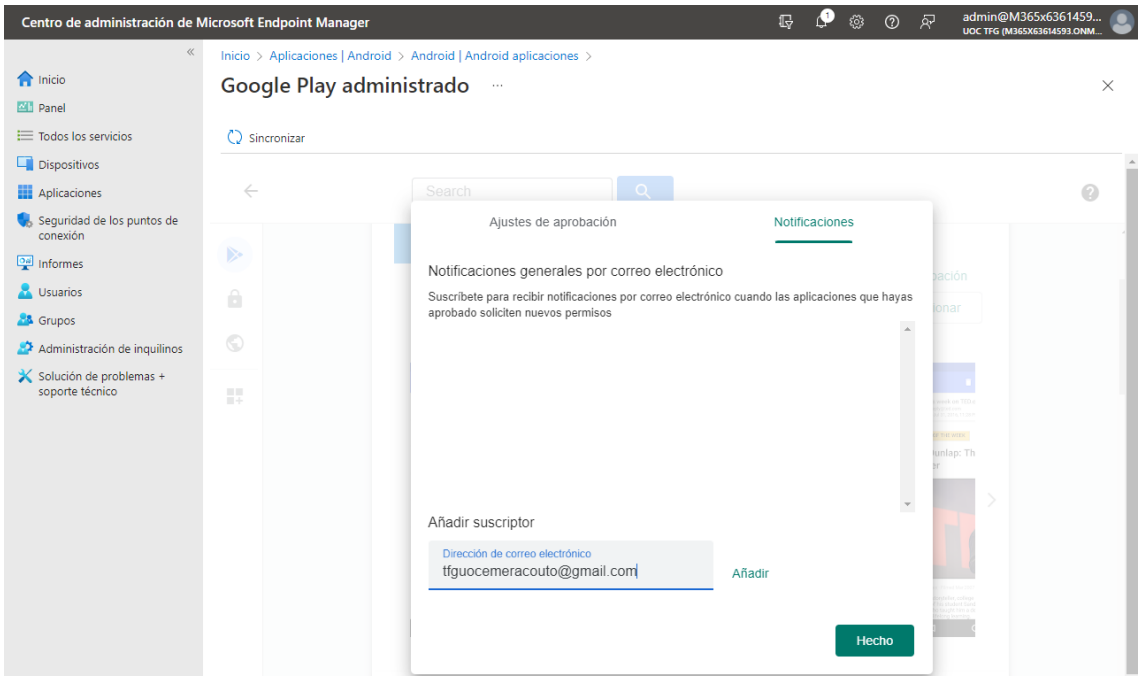
Se deben aprobar también los permisos que se le conceden a la aplicación. Así, el usuario no deberá hacerlo, ya que estarán previamente aprobados por la organización.



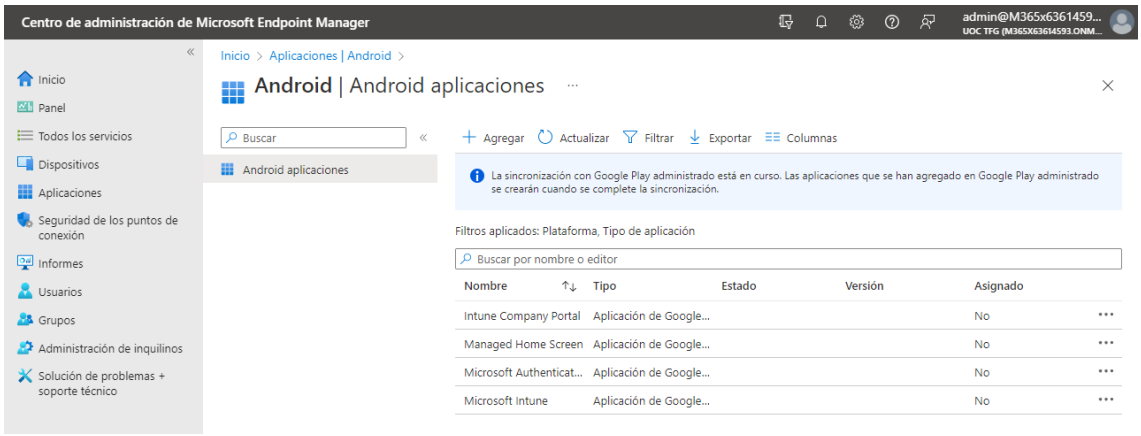
Además, se permite decidir el comportamiento sobre la aplicación desplegada en caso de que en un futuro solicite permisos adicionales a los ya aprobados por la organización. En este caso, se ha optado por revocar la aprobación, pues se desea supervisar los nuevos permisos requeridos y realizar la aprobación manual en caso de que cumplan con las medidas de seguridad y privacidad de la compañía.

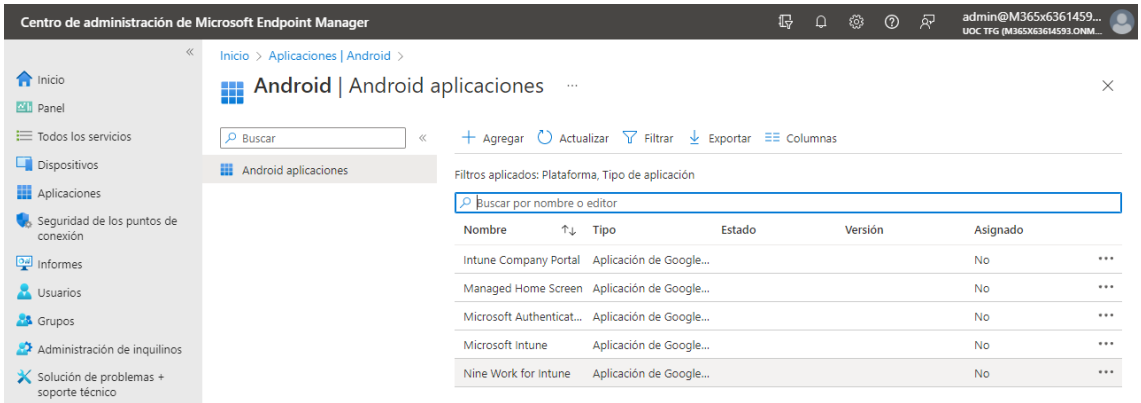


También se ha indicado la dirección de correo del administrador para que se le notifique ante futuros cambios.

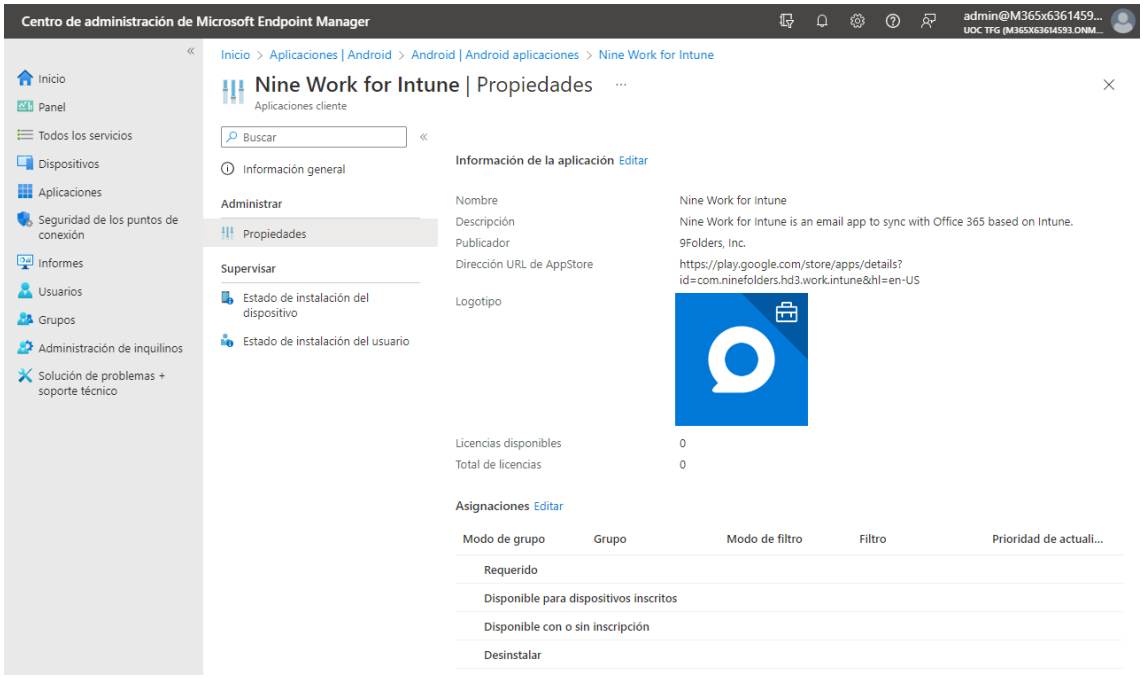


Una vez añadida la aplicación al catálogo de aplicaciones corporativas, se debe asignar al grupo sobre el que se instalará.

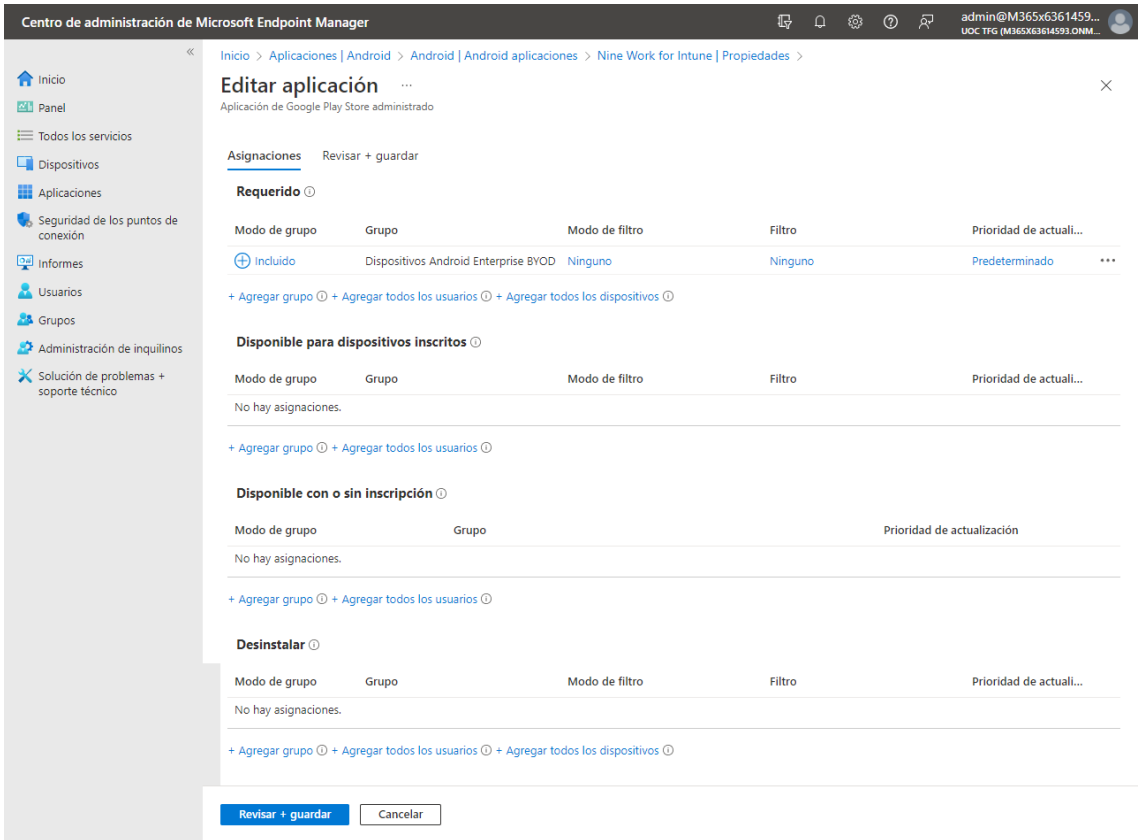




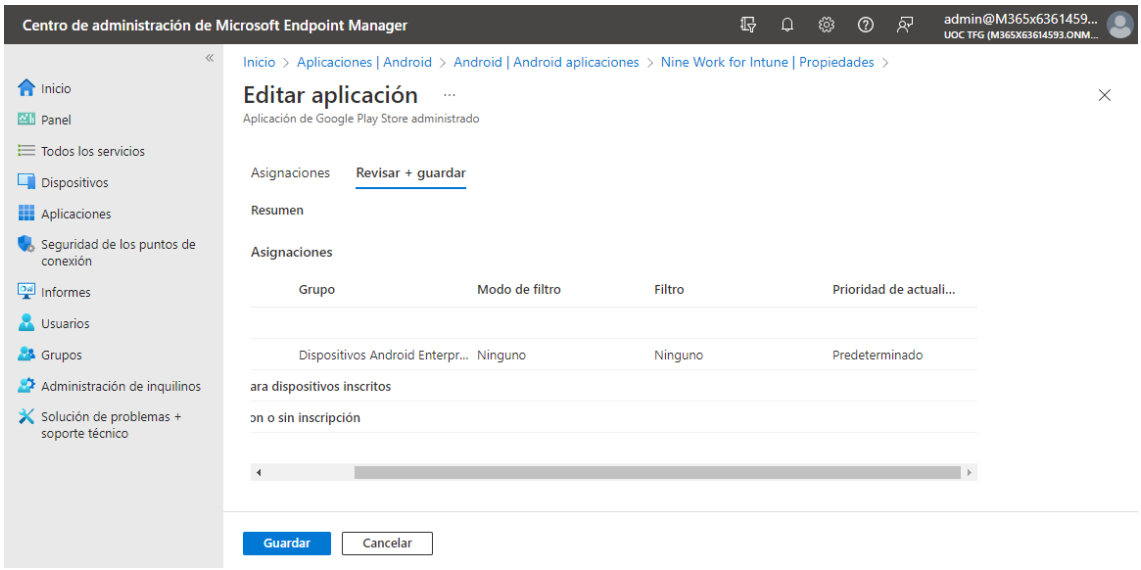
Para realizar la asignación, es necesario acceder a los detalles de la aplicación entrando en ella, simplemente pinchando en su nombre en la lista, y editar sus propiedades.



En las asignaciones, se indica el grupo y el tipo de despliegue.

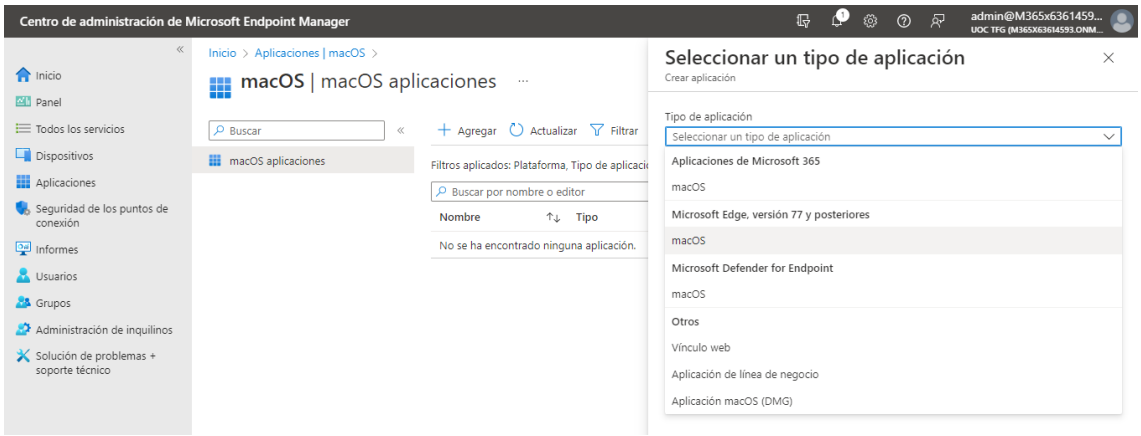


Por último, se revisan los cambios y se guardan.

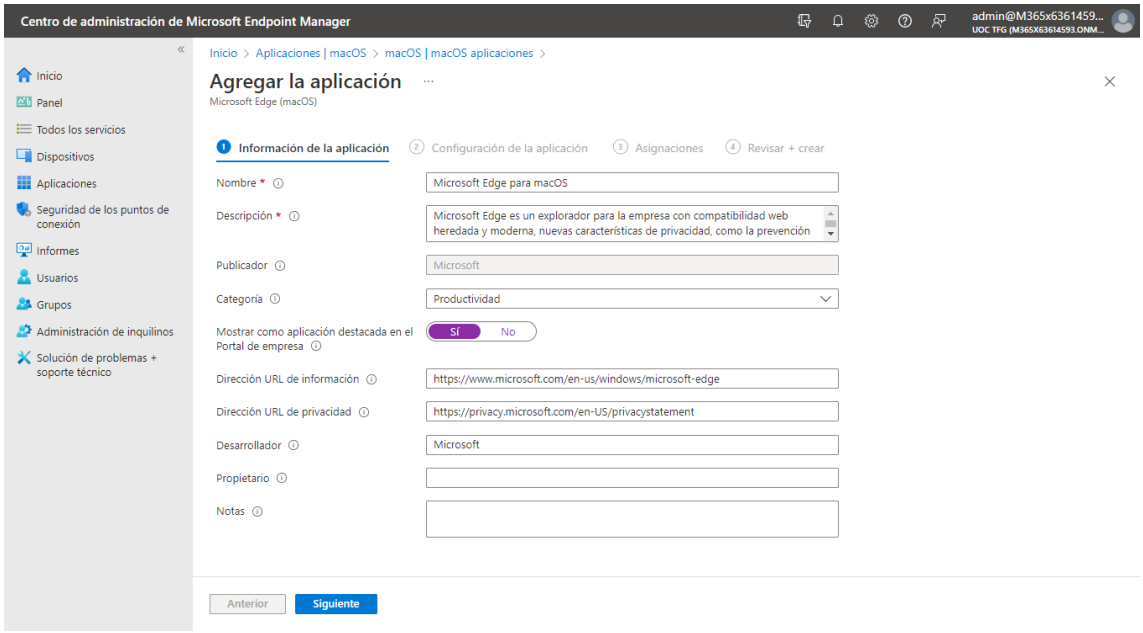


- **Dispositivos macOS**

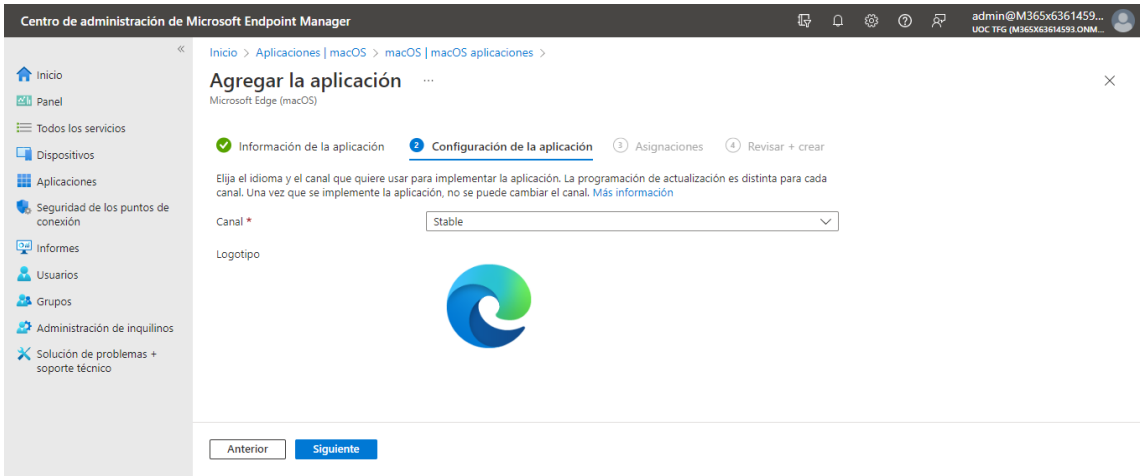
El proceso de creación de un despliegue de aplicación para dispositivos Apple con sistema operativo macOS es similar al de los dispositivos Windows, accediendo primero a “macOS” en el menú “Aplicaciones” y seleccionando después el tipo de aplicación tras hacer click en “Agregar”.



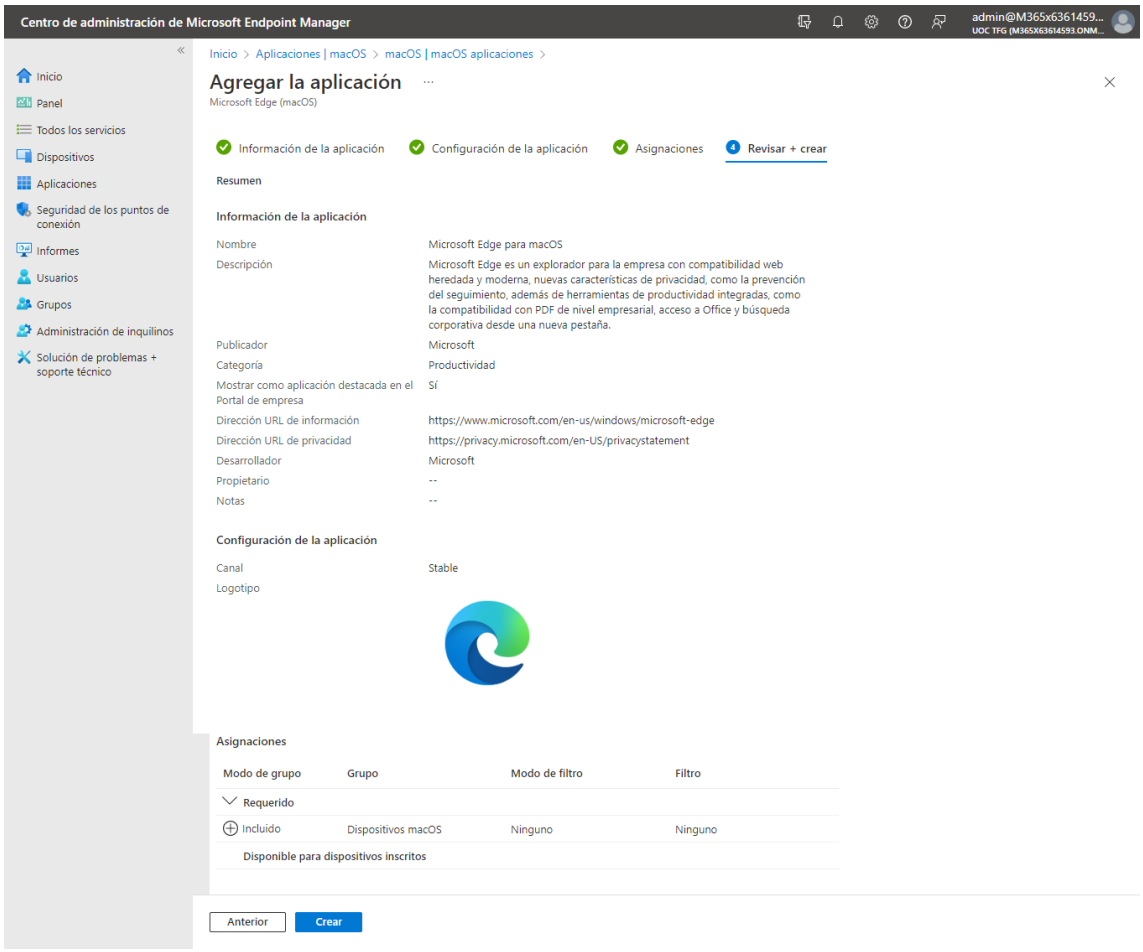
En este caso, la aplicación seleccionada es Microsoft Edge (Chromium).



Se configuran los parámetros de la aplicación, así como el canal y el logo.

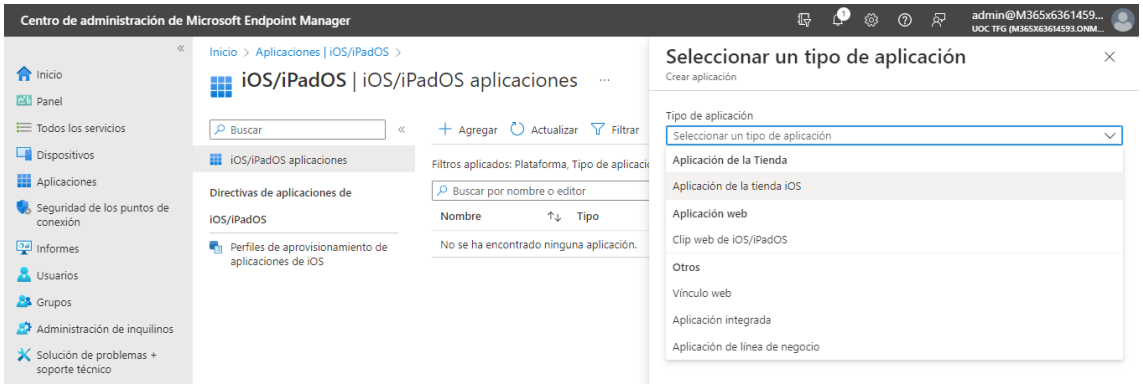


Por último, se añade el grupo (o grupos) sobre los que se quiere instalar la aplicación y el tipo de instalación deseada antes de revisar el resumen de la configuración y realizar la creación.

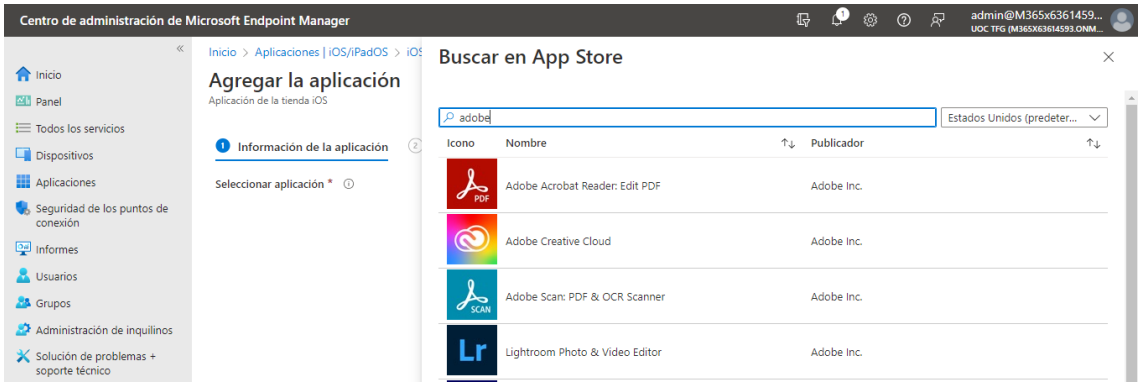


- **<u>Dispositivos iOS e iPadOS</u>**

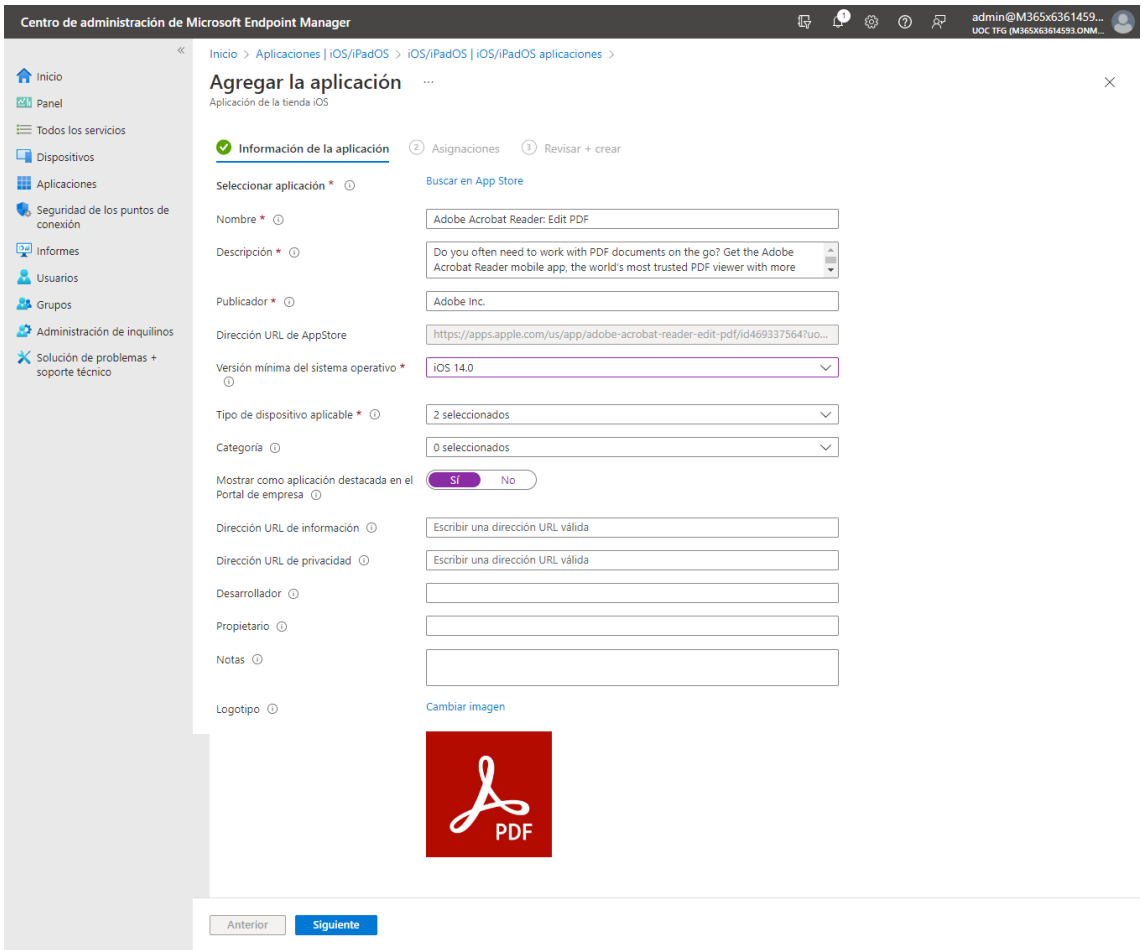
El despliegue de aplicaciones en dispositivos Apple con sistema operativo iOS e iPadOS también es similar al de los dispositivos Windows. Tras acceder a "iOS/iPadOS" dentro del menú "Aplicaciones", se selecciona el tipo de aplicación que se quiere desplegar.



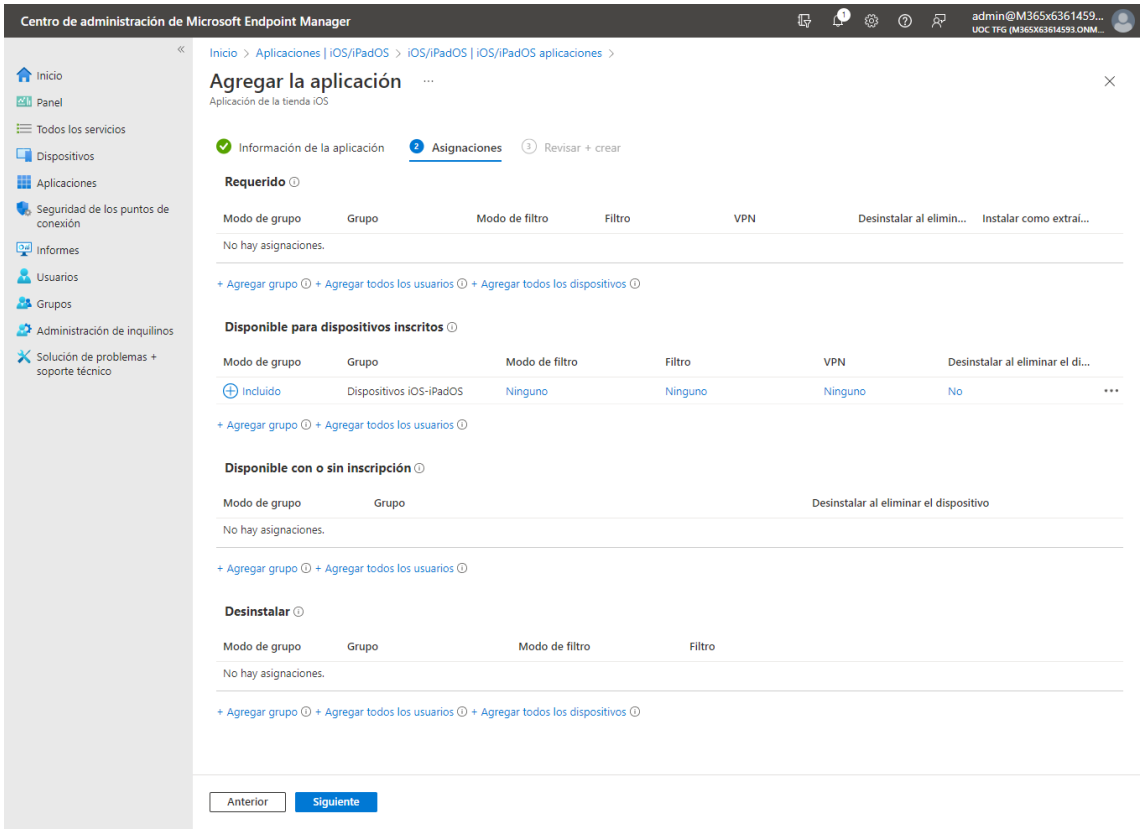
En este caso, la aplicación elegida es Adobe Acrobat Reader, de la tienda de aplicaciones Apple App Store.



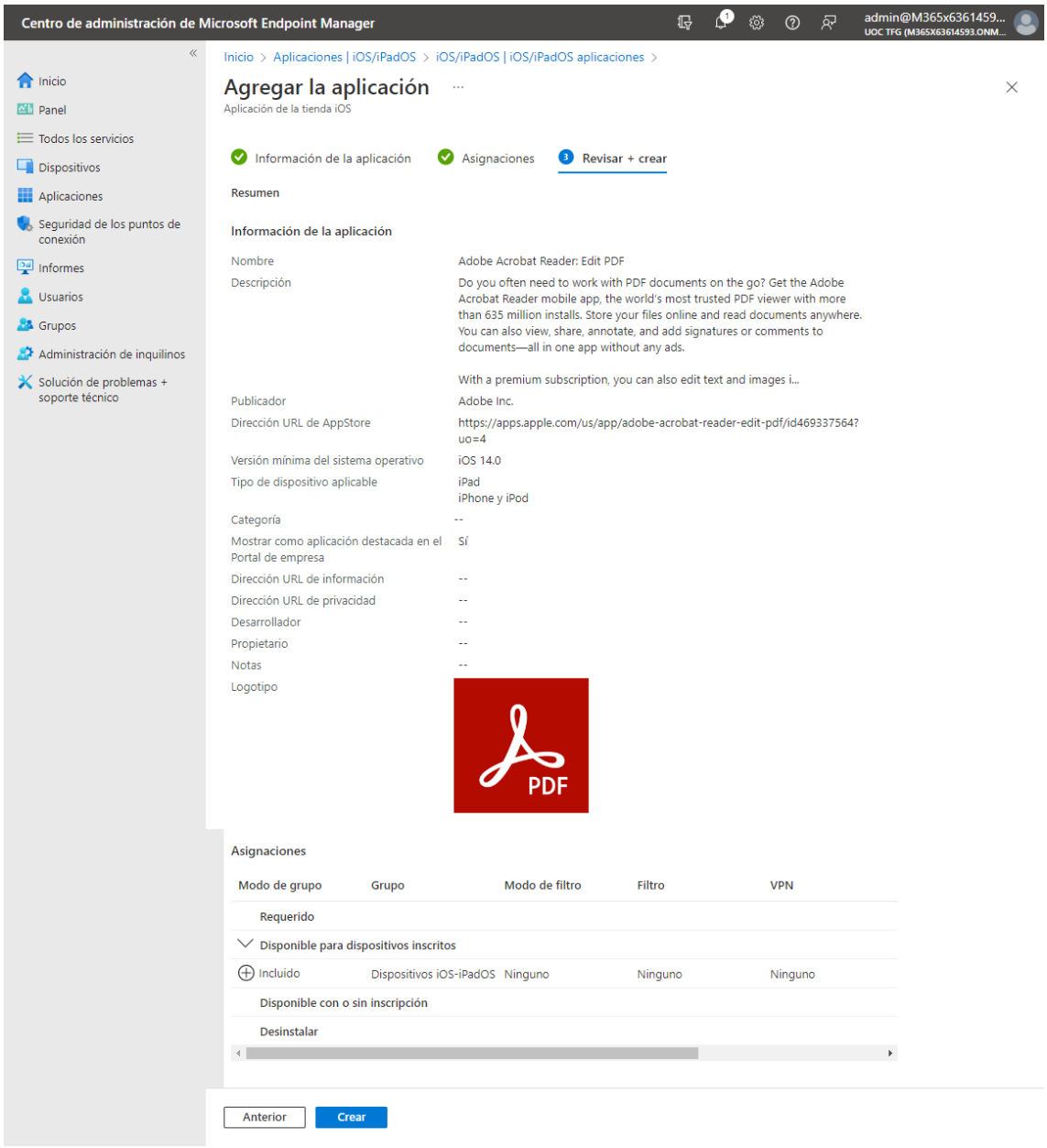
Se realizan las configuraciones deseadas sobre la aplicación (que varían dependiendo de la aplicación elegida).



Para finalizar, se asigna la aplicación y se elige el modo de despliegue (requerido o disponible).



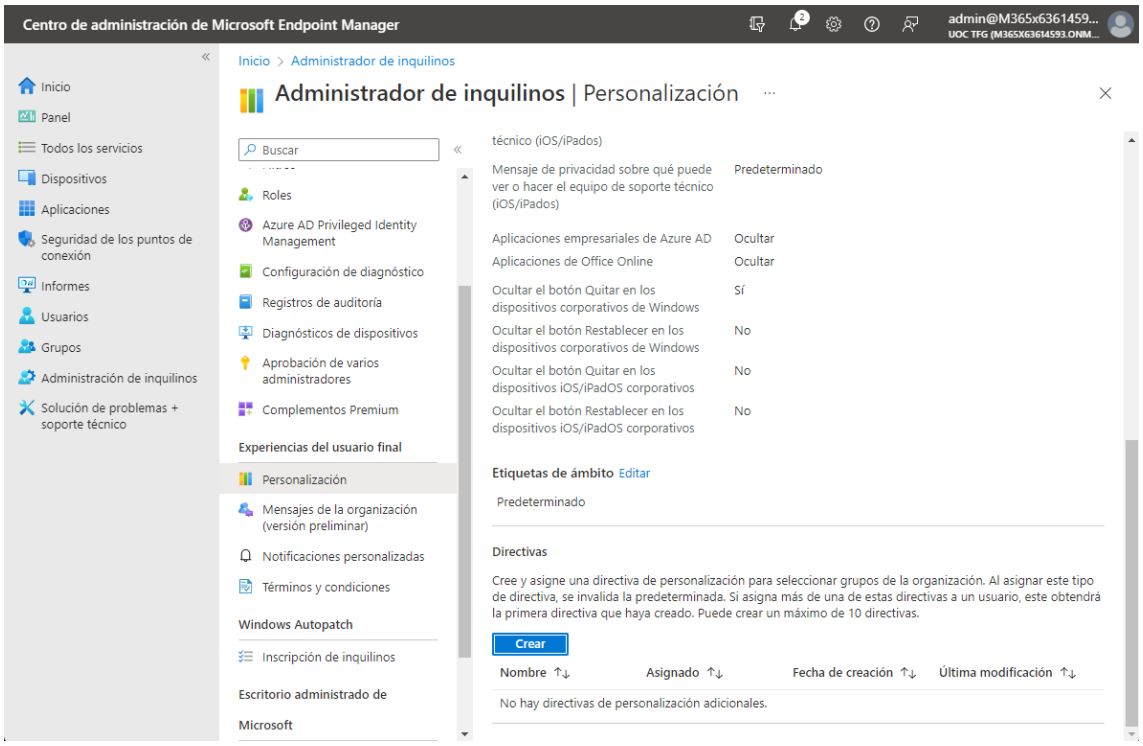
Se revisa el resumen de la configuración de la aplicación que se va a desplegar y se lleva a cabo la creación.


Centro de administración de Microsoft Endpoint Manager
admin@M365x6361459...
UOC TFG (M365X63614593.ONM...
Inicio
Panel
Todos los servicios
Dispositivos
Aplicaciones
Seguridad de los puntos de conexión
Informes
Usuarios
Grupos
Administración de inquilinos
Solución de problemas + soporte técnico
Inicio > Aplicaciones | iOS/iPadOS > iOS/iPadOS | iOS/iPadOS aplicaciones >
Agregar la aplicación
Aplicación de la tienda iOS
Información de la aplicación
Asignaciones
3 Revisar + crear
Resumen
Información de la aplicación
Nombre
Adobe Acrobat Reader: Edit PDF
Descripción
Do you often need to work with PDF documents on the go? Get the Adobe Acrobat Reader mobile app, the world's most trusted PDF viewer with more than 635 million installs. Store your files online and read documents anywhere. You can also view, share, annotate, and add signatures or comments to documents—all in one app without any ads.
With a premium subscription, you can also edit text and images i...
Publicador
Adobe Inc.
Dirección URL de AppStore
https://apps.apple.com/us/app/adobe-acrobat-reader-edit-pdf/id469337564?uo=4
Versión mínima del sistema operativo
iOS 14.0
Tipo de dispositivo aplicable
iPad
iPhone y iPod
Categoría
--
Mostrar como aplicación destacada en el Portal de empresa
Sí
Dirección URL de información
--
Dirección URL de privacidad
--
Desarrollador
--
Propietario
--
Notas
--
Logotipo
PDF
Asignaciones
Modo de grupo
Grupo
Modo de filtro
Filtro
VPN
Requerido
Disponible para dispositivos inscritos
Incluido
Dispositivos iOS-iPadOS
Ninguno
Ninguno
Ninguno
Disponible con o sin inscripción
Desinstalar
Anterior
Crear

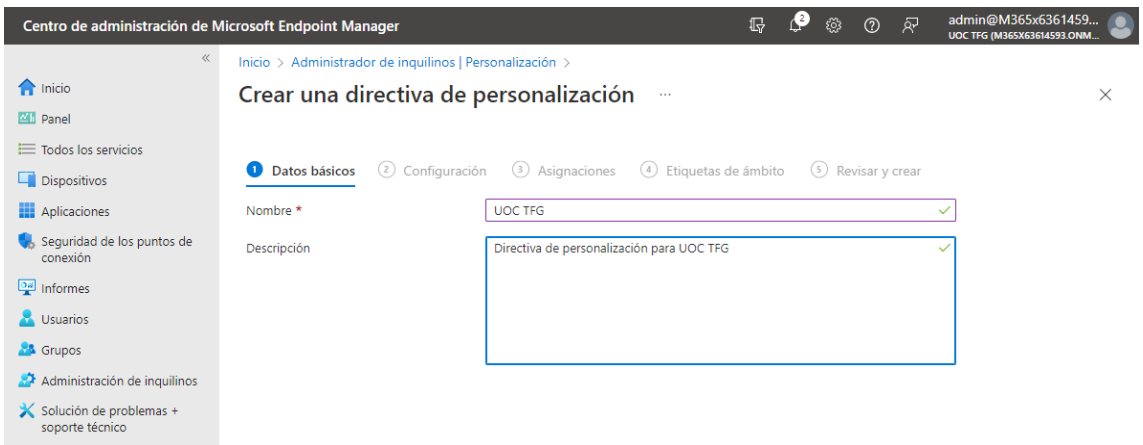
Anexo 10. Creación de directiva de personalización

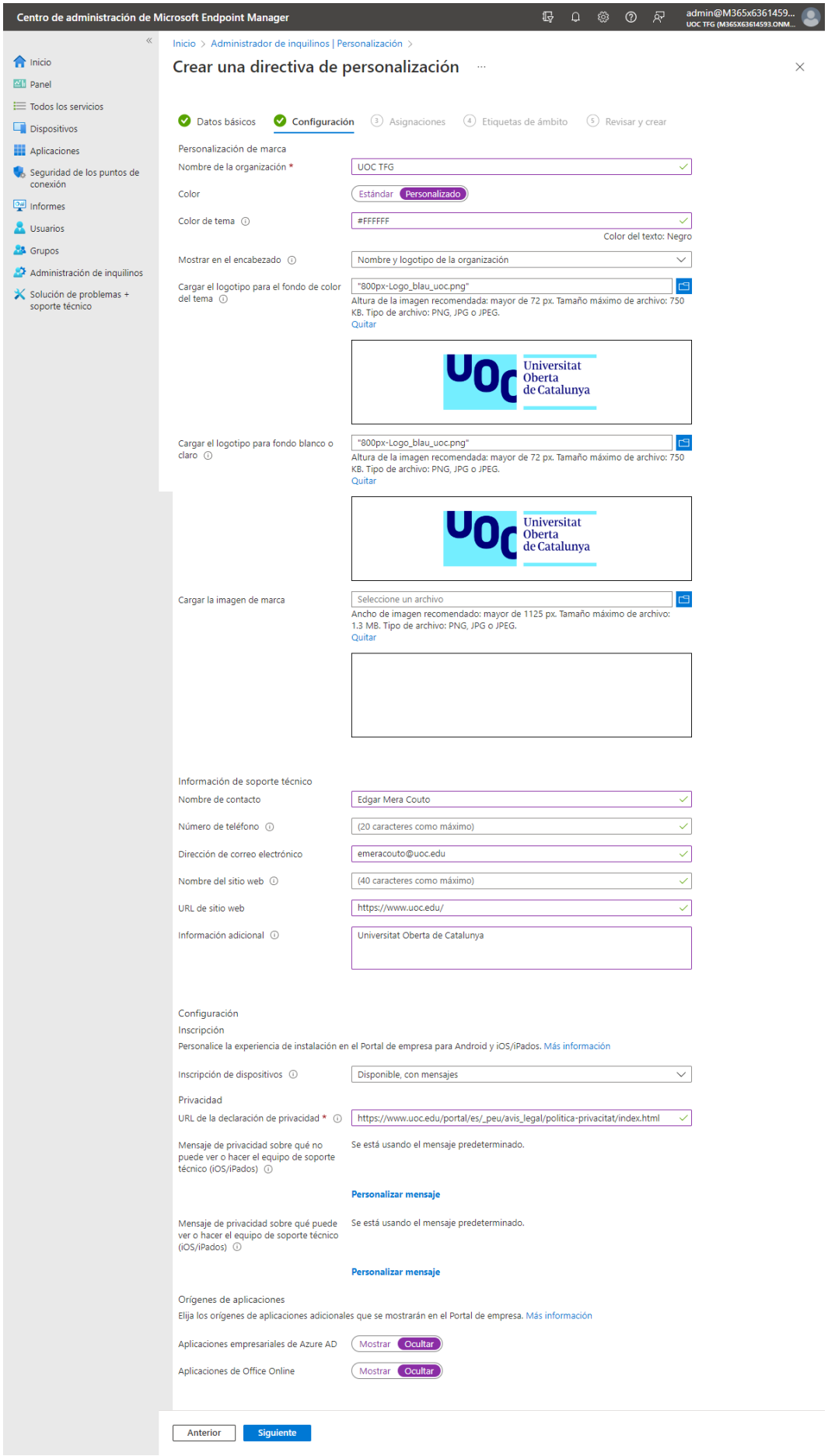
Las directivas de personalización permiten disponer de distintos tipos de experiencia de usuario en una misma empresa. Esto cobra sentido cuando, dentro de la misma organización, existen diferentes compañías que pertenecen al mismo grupo y se quiere realizar distinción entre ellas.

La creación de una directiva de personalización en Intune se puede llevar a cabo desde el apartado “Personalización”, en el menú “Administrador de inquilinos”, haciendo click en Crear.

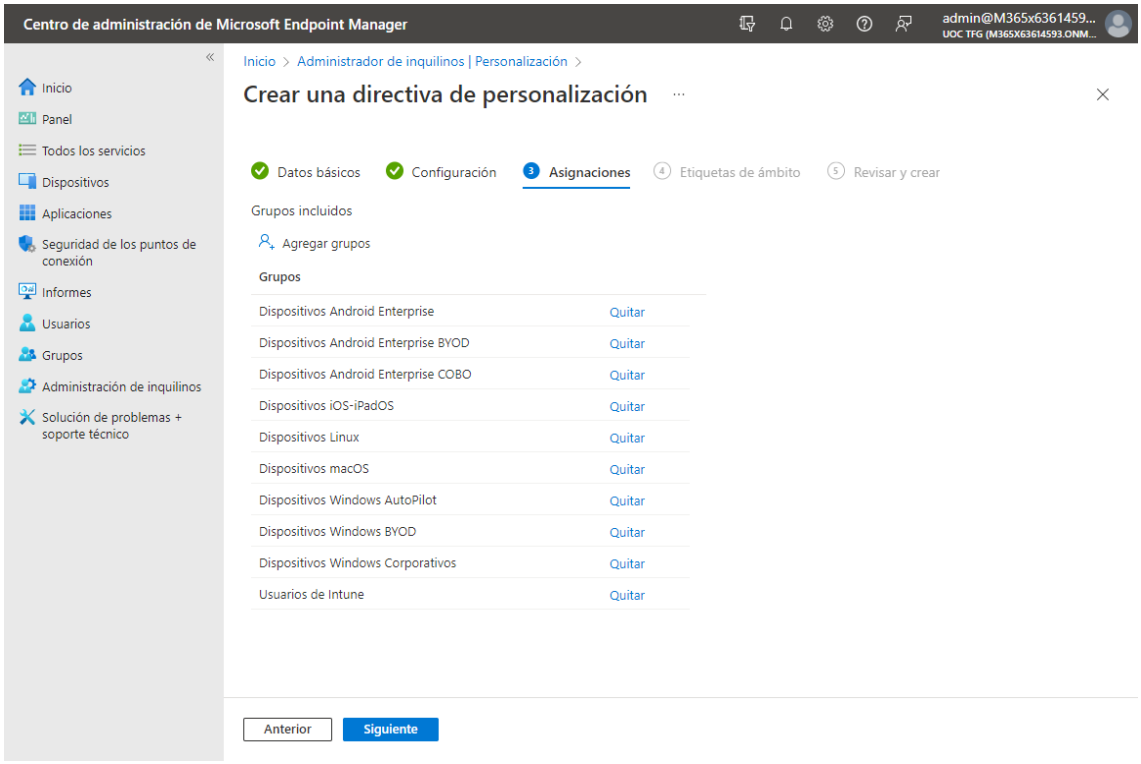


En el primer paso, se indica el nombre y la descripción de la directiva y, después, se configuran los aspectos de personalización deseados.

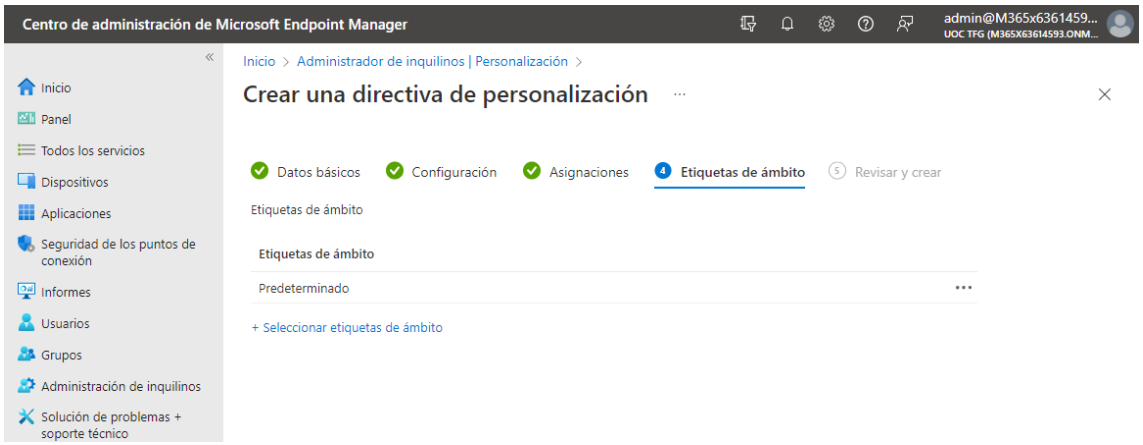



Centro de administración de Microsoft Endpoint Manager
admin@M365x6361459...
UOC TFG (M365X63614593.ONM...
Inicio
Panel
Todos los servicios
Dispositivos
Aplicaciones
Seguridad de los puntos de conexión
Informes
Usuarios
Grupos
Administración de inquilinos
Solución de problemas + soporte técnico
Inicio > Administrador de inquilinos | Personalización >
Crear una directiva de personalización
Datos básicos
Configuración
Asignaciones
Etiquetas de ámbito
Revisar y crear
Personalización de marca
Nombre de la organización *
UOC TFG
Color
Estándar
Personalizado
Color de tema
#FFFFFF
Color del texto: Negro
Mostrar en el encabezado
Nombre y logotipo de la organización
Cargar el logotipo para el fondo de color del tema
"800px-Logo_blau_uoc.png"
Altura de la imagen recomendada: mayor de 72 px. Tamaño máximo de archivo: 750 KB. Tipo de archivo: PNG, JPG o JPEG.
Quitar
Universitat Oberta de Catalunya
Cargar el logotipo para fondo blanco o claro
"800px-Logo_blau_uoc.png"
Altura de la imagen recomendada: mayor de 72 px. Tamaño máximo de archivo: 750 KB. Tipo de archivo: PNG, JPG o JPEG.
Quitar
Universitat Oberta de Catalunya
Cargar la imagen de marca
Seleccione un archivo
Ancho de imagen recomendado: mayor de 1125 px. Tamaño máximo de archivo: 1.3 MB. Tipo de archivo: PNG, JPG o JPEG.
Quitar
Información de soporte técnico
Nombre de contacto
Edgar Mera Couto
Número de teléfono
(20 caracteres como máximo)
Dirección de correo electrónico
emeracouto@uoc.edu
Nombre del sitio web
(40 caracteres como máximo)
URL de sitio web
https://www.uoc.edu/
Información adicional
Universitat Oberta de Catalunya
Configuración
Inscripción
Personalice la experiencia de instalación en el Portal de empresa para Android y iOS/iPados. Más información
Inscripción de dispositivos
Disponible, con mensajes
Privacidad
URL de la declaración de privacidad *
https://www.uoc.edu/portal/es/_peu/avis_legal/politica-privacitat/index.html
Mensaje de privacidad sobre qué no puede ver o hacer el equipo de soporte técnico (iOS/iPados)
Se está usando el mensaje predeterminado.
Personalizar mensaje
Mensaje de privacidad sobre qué puede ver o hacer el equipo de soporte técnico (iOS/iPados)
Se está usando el mensaje predeterminado.
Personalizar mensaje
Orígenes de aplicaciones
Elija los orígenes de aplicaciones adicionales que se mostrarán en el Portal de empresa. Más información
Aplicaciones empresariales de Azure AD
Mostrar
Ocultar
Aplicaciones de Office Online
Mostrar
Ocultar
Anterior
Siguiente

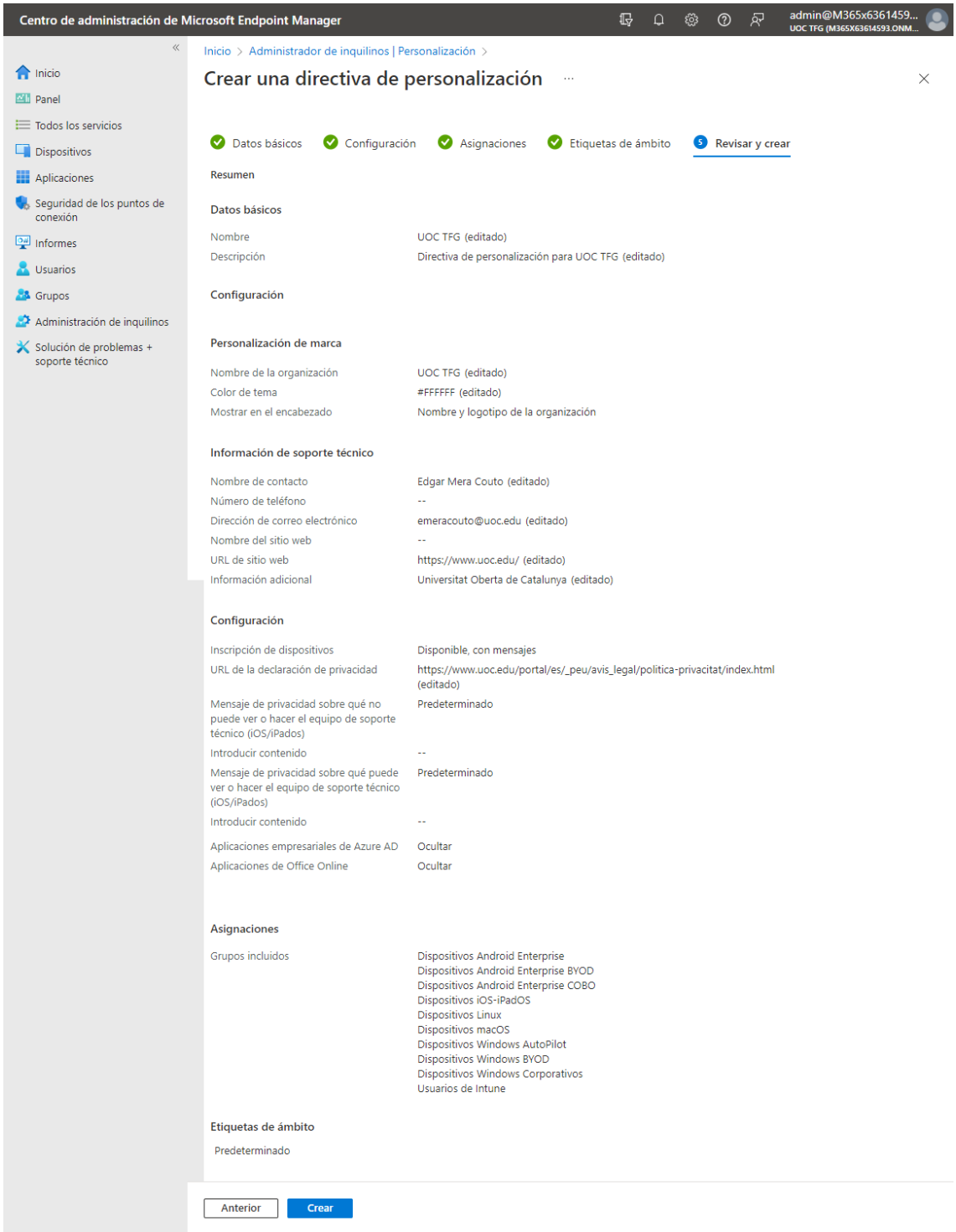
Una vez configurados los parámetros de personalización, se asigna la directiva a los grupos de la organización deseados.



A continuación, se añaden las etiquetas de ámbito, en caso de ser necesario.



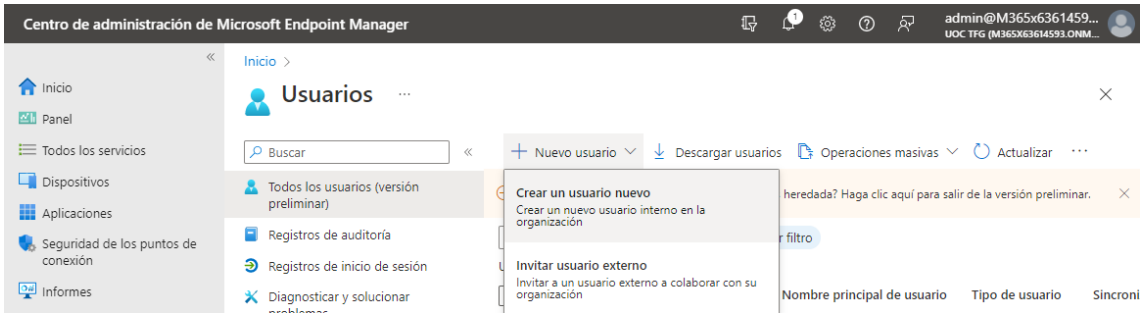
Por último, se revisan los detalles de la directiva configurados y ejecuta la creación de la misma.



Anexo 11. Creación de usuarios y asignación de licencias

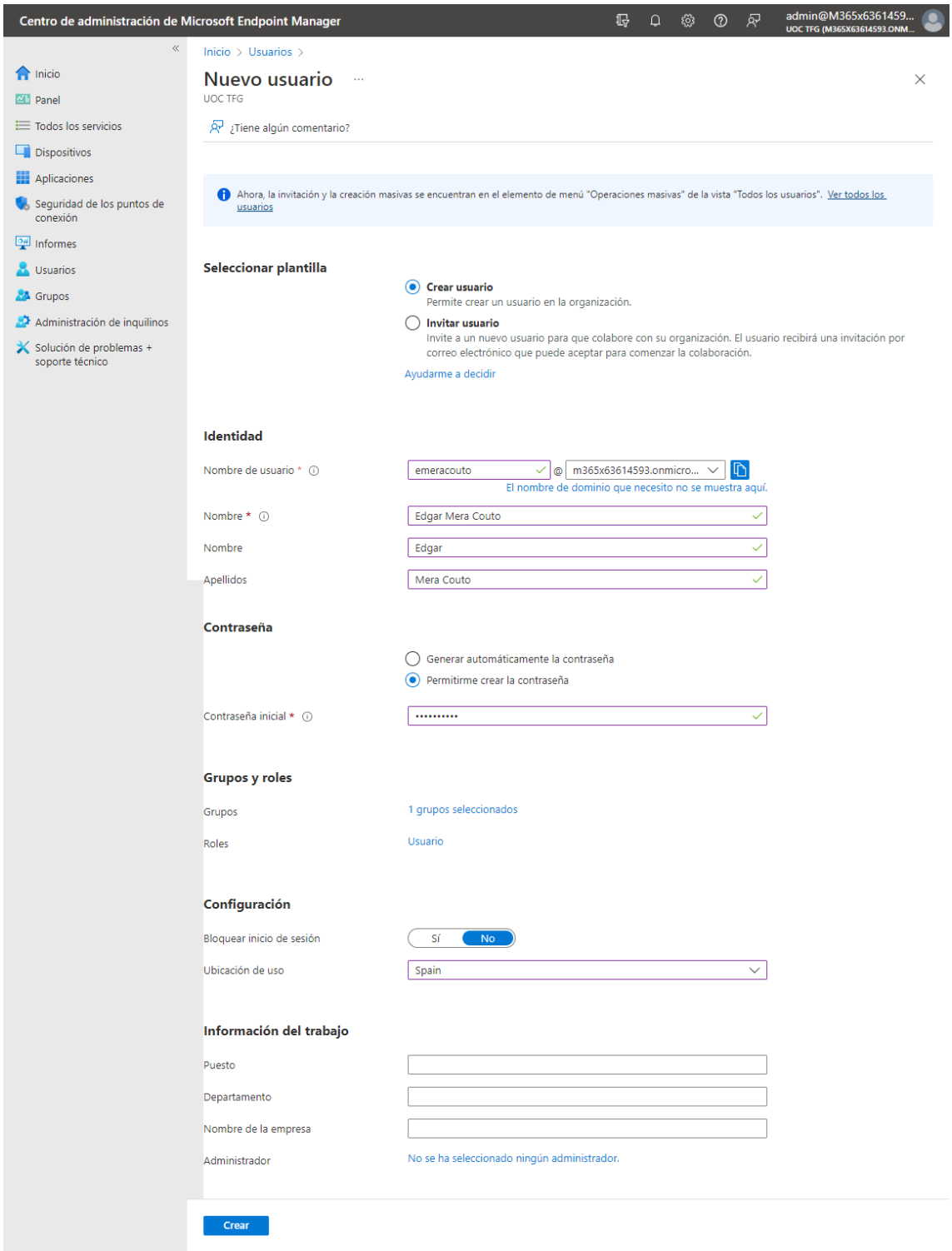
La creación de usuarios se puede llevar a cabo desde el propio portal de administración de Microsoft Intune o desde el de Azure Active Directory. En este caso, se ha optado por la primera opción.

Para crear un usuario se debe acceder al menú “Usuarios” en la consola de administración de Intune y hacer click en “Nuevo usuario”.

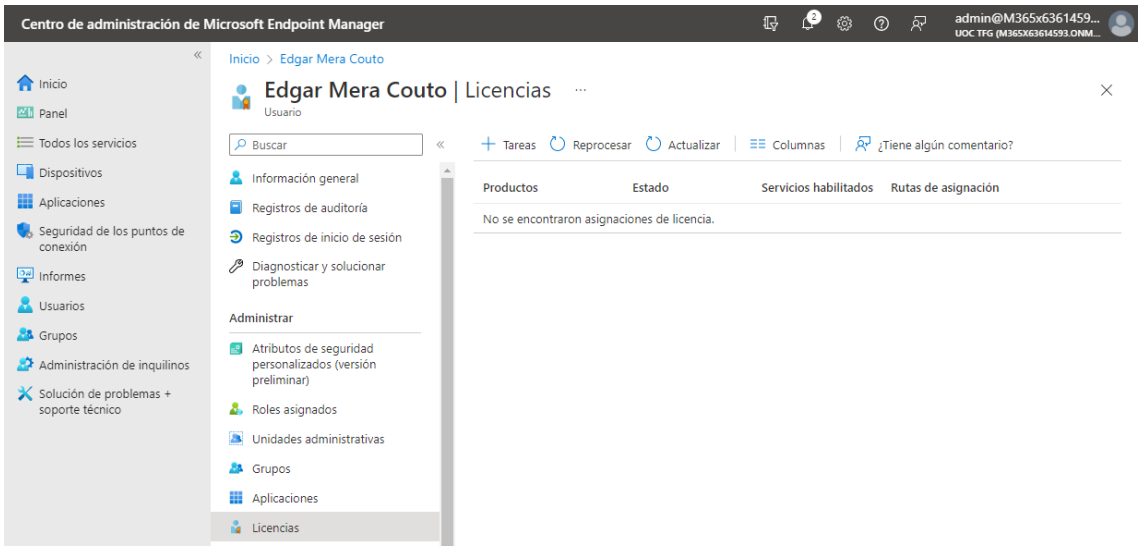


A continuación, se indican los datos del usuario a crear: nombre de inicio de sesión, nombre, apellidos, nombre completo a mostrar, contraseña inicial y ubicación. La contraseña deberá ser cambiada en el primer inicio de sesión del usuario por una que cumpla con las directivas de seguridad definidas por la organización.

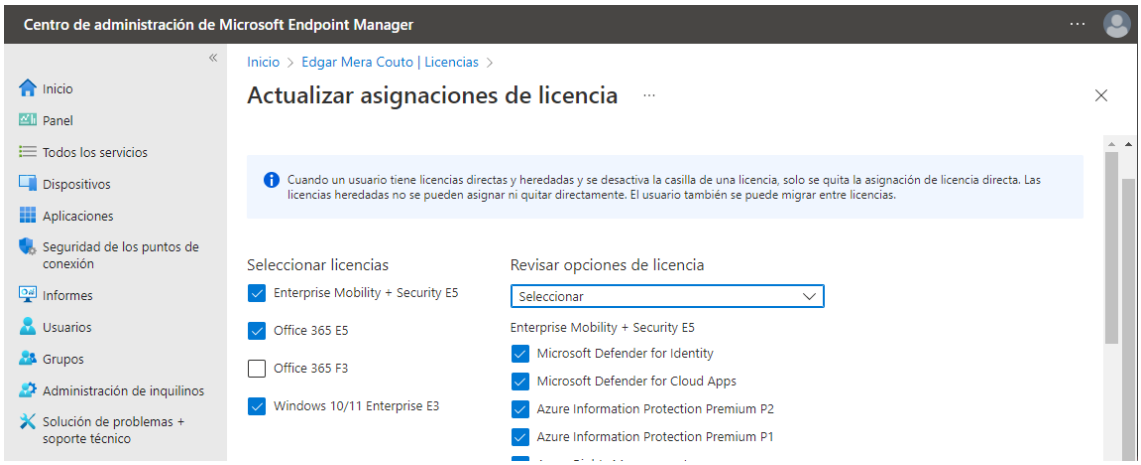
- Edgar Mera Couto:



Tras crear el usuario, se procede a asignar las licencias correspondientes. Para ello, se accede a las propiedades del usuario haciendo click en su nombre y entrando al apartado “Licencias” del menú de la izquierda.

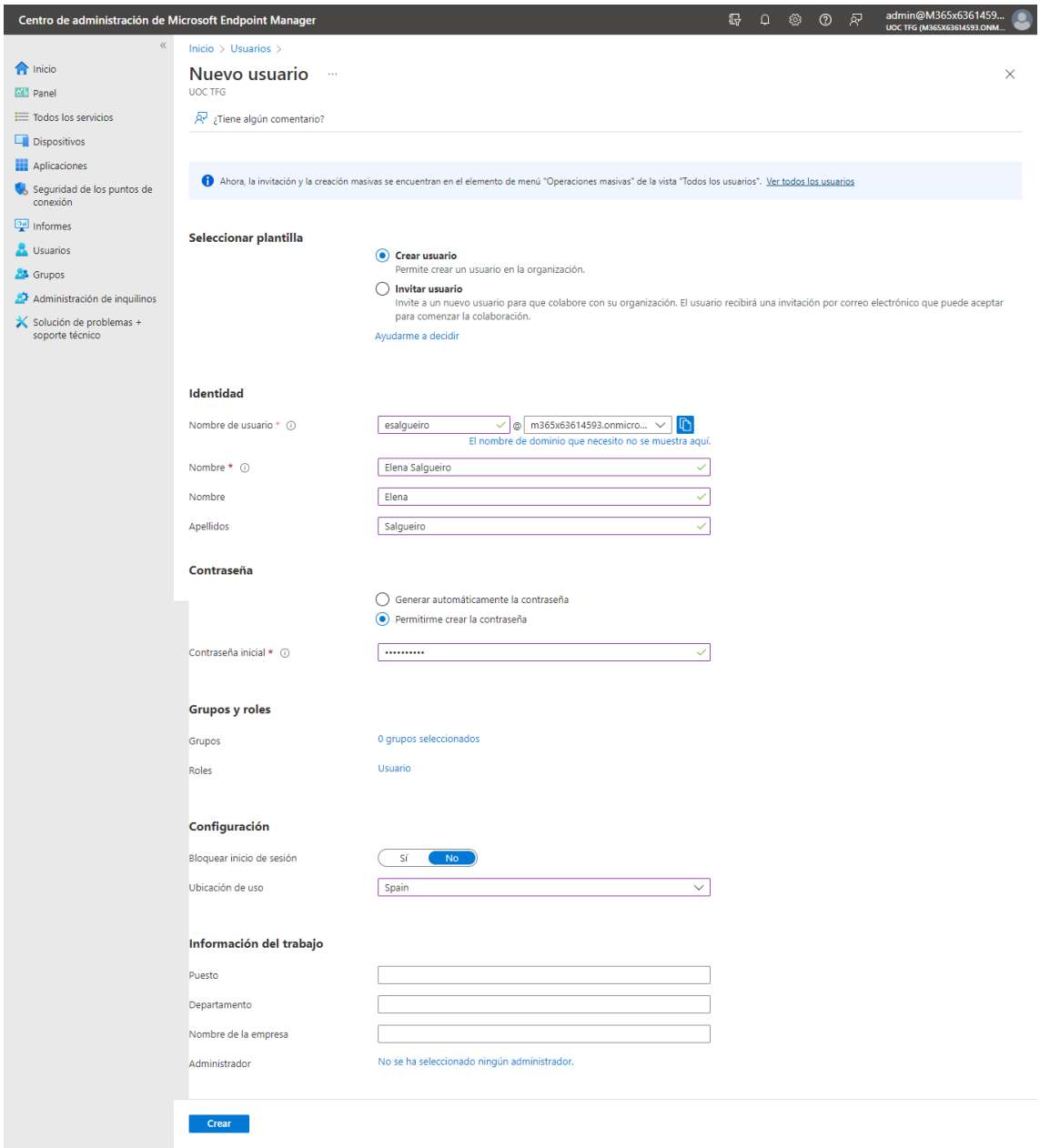


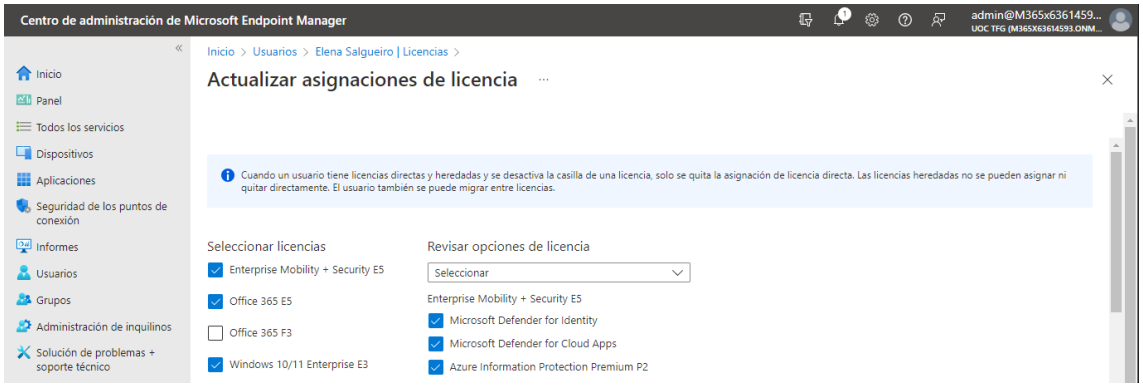
Después, se hace click en “Tareas” y se seleccionan las licencias deseadas, pudiendo elegir también los productos de cada licencia.



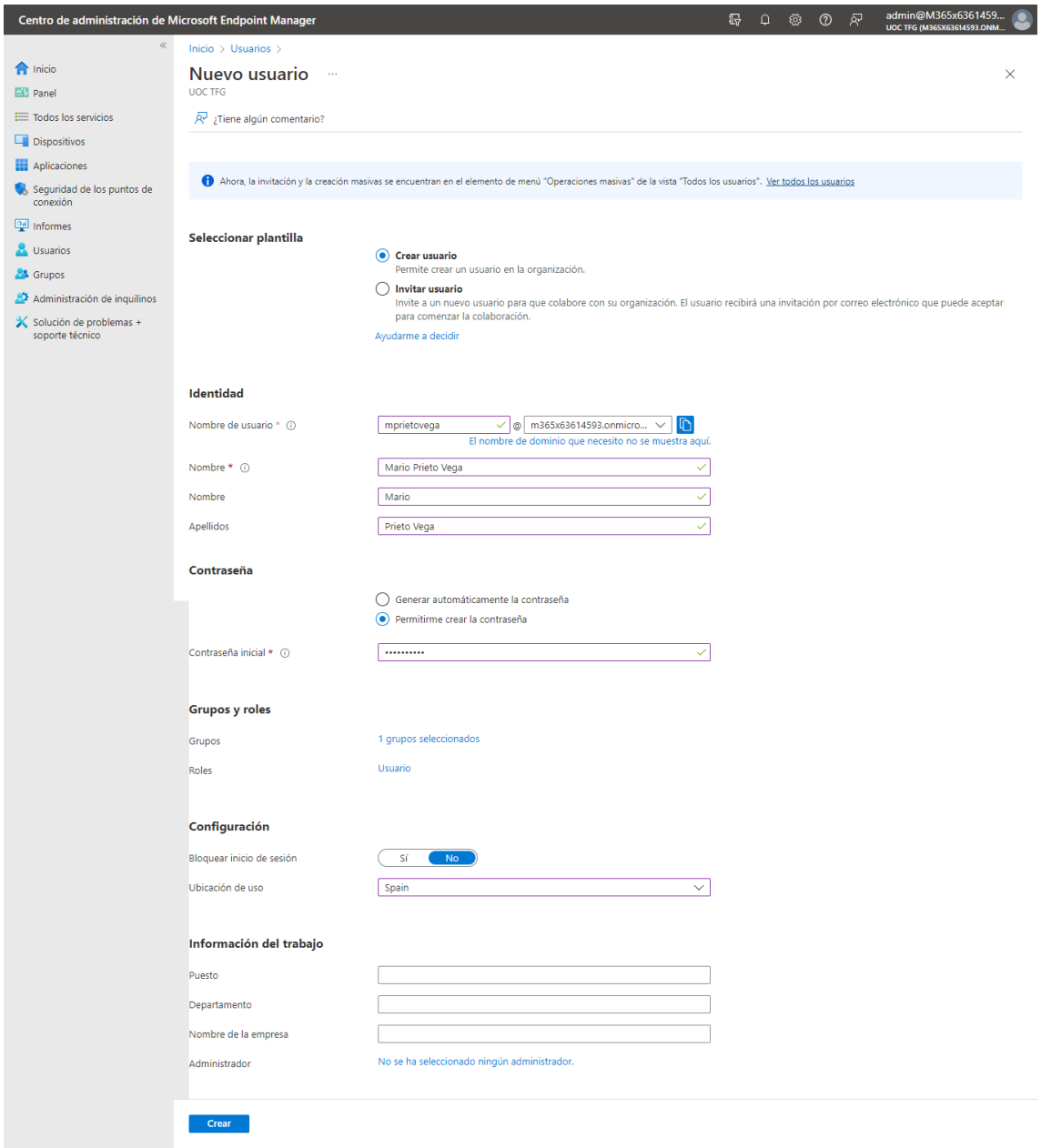
A continuación, se muestra el proceso de creación del resto de usuarios del entorno de laboratorio, siendo iguales al ya expuesto.

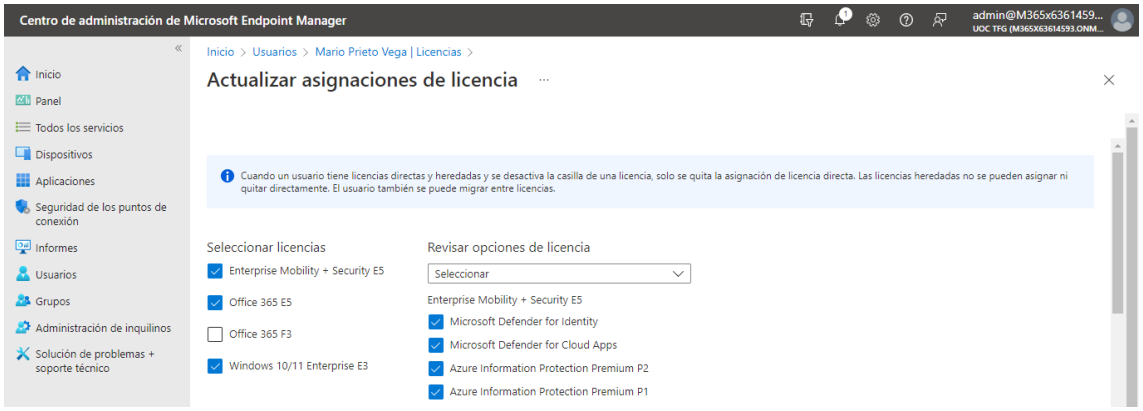
- Elena Salgueiro:



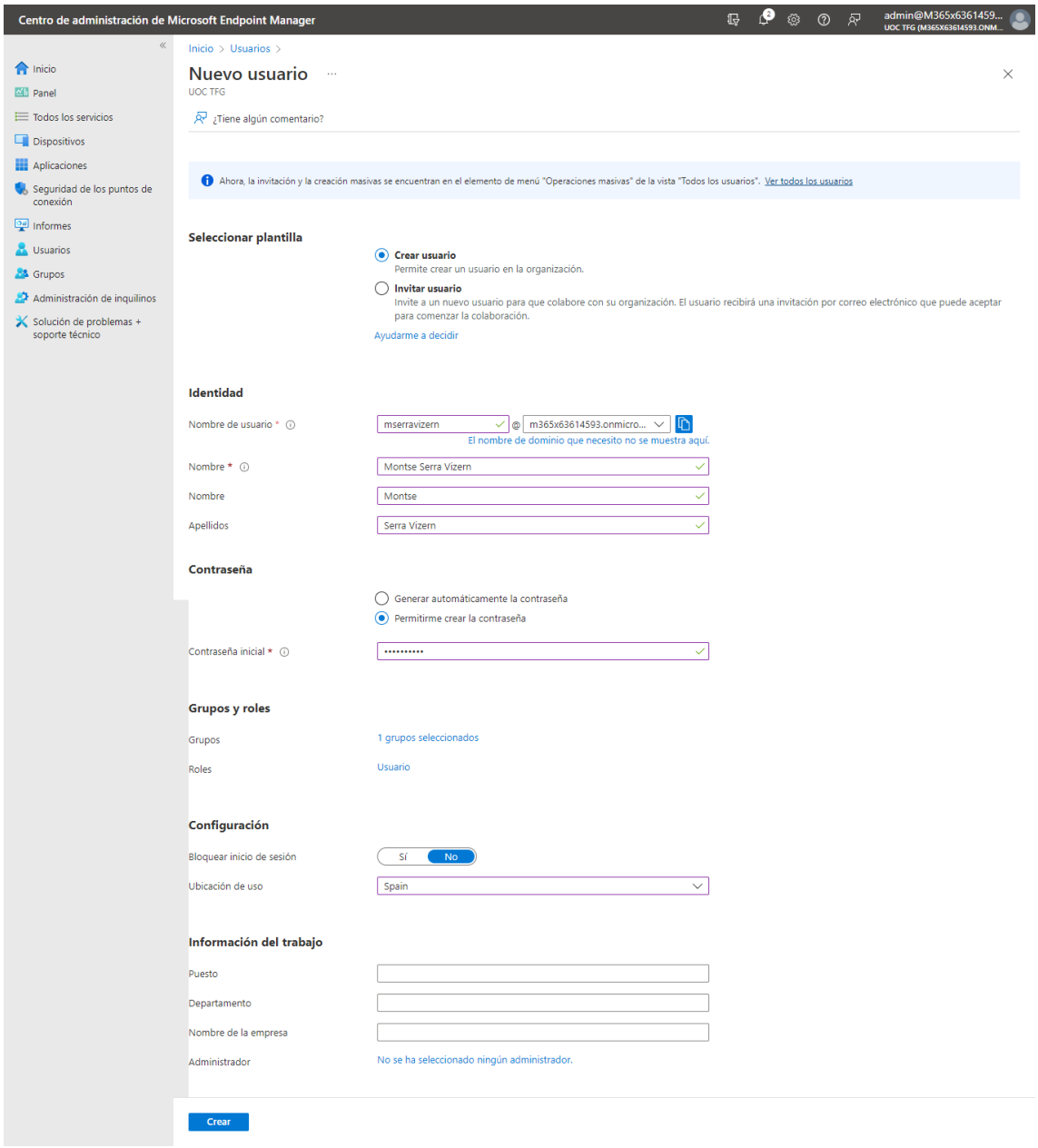


- Mario Prieto Vega:

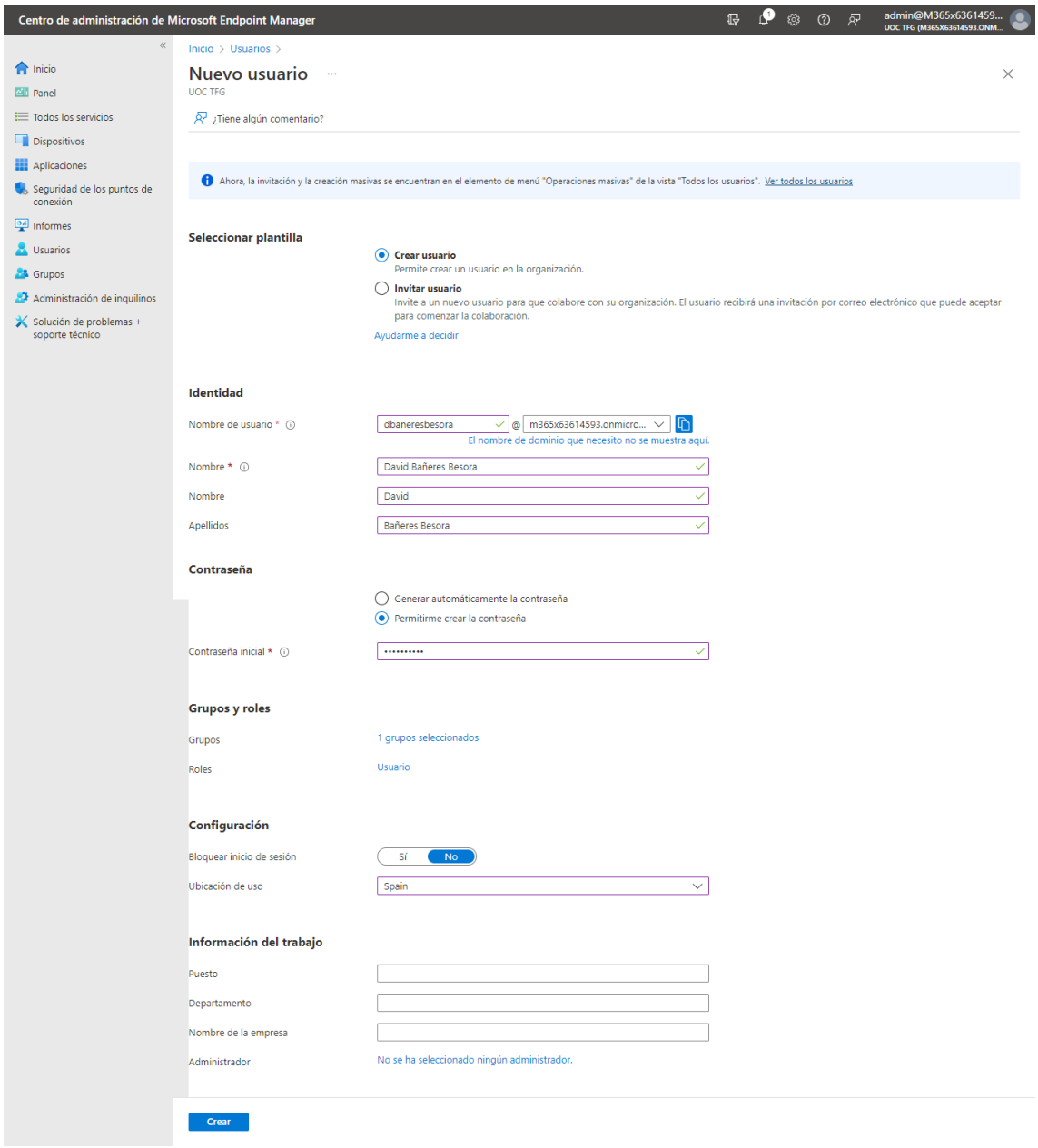


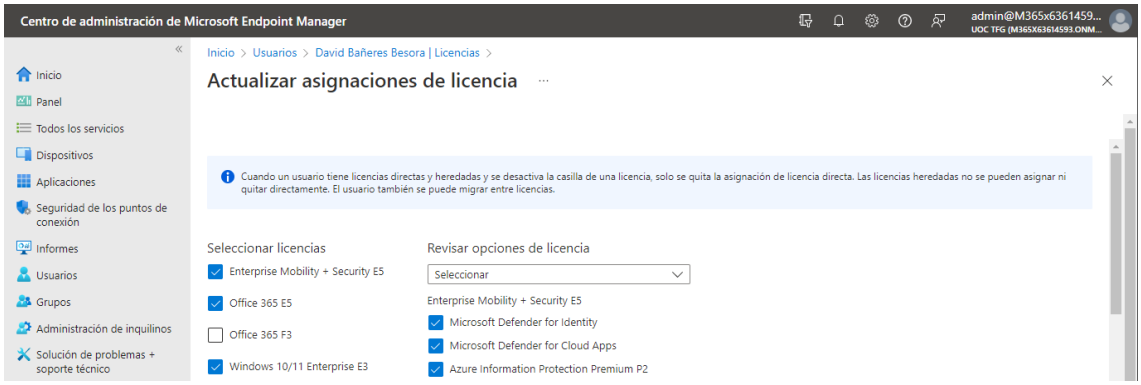


- Montse Serra Vizern:



- David Bañeres Besora:

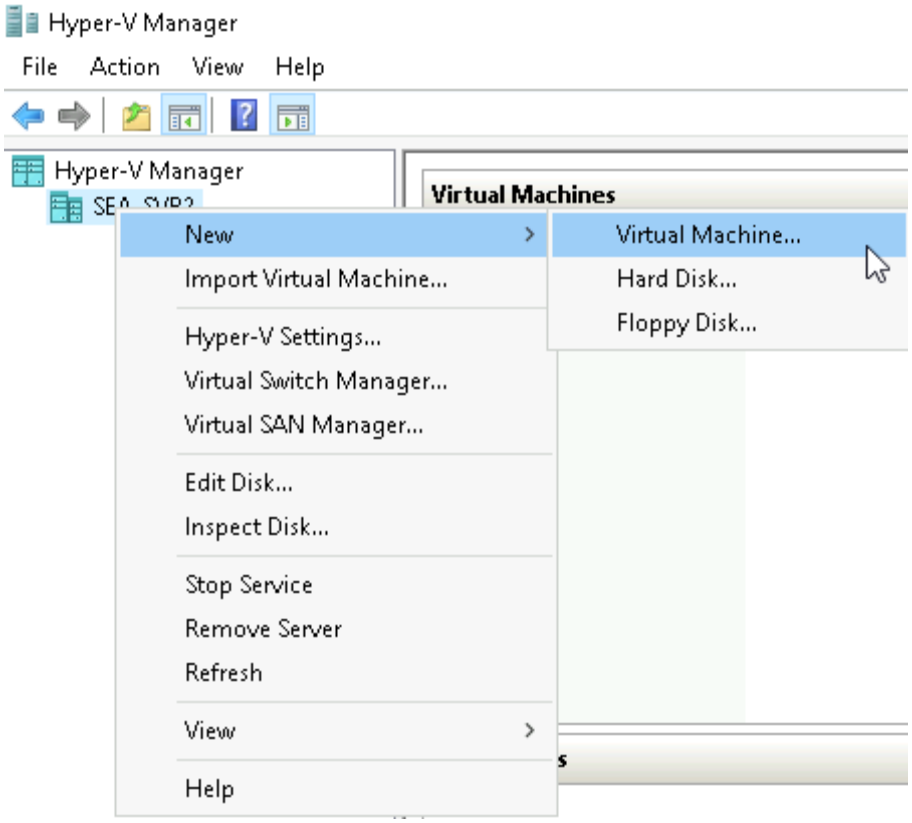




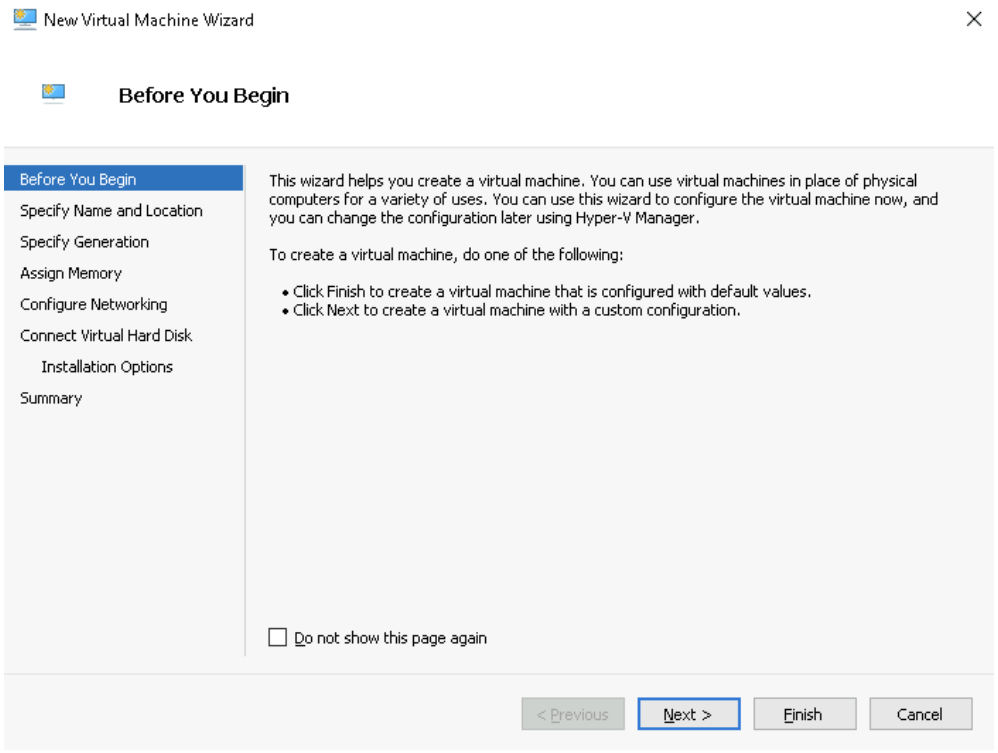
Anexo 12. Creación de máquina virtual Ubuntu

Para la creación de las máquinas virtuales se ha utilizado un servidor existente con sistema operativo Windows Server 2022 Datacenter y el rol de Hyper-V instalado.

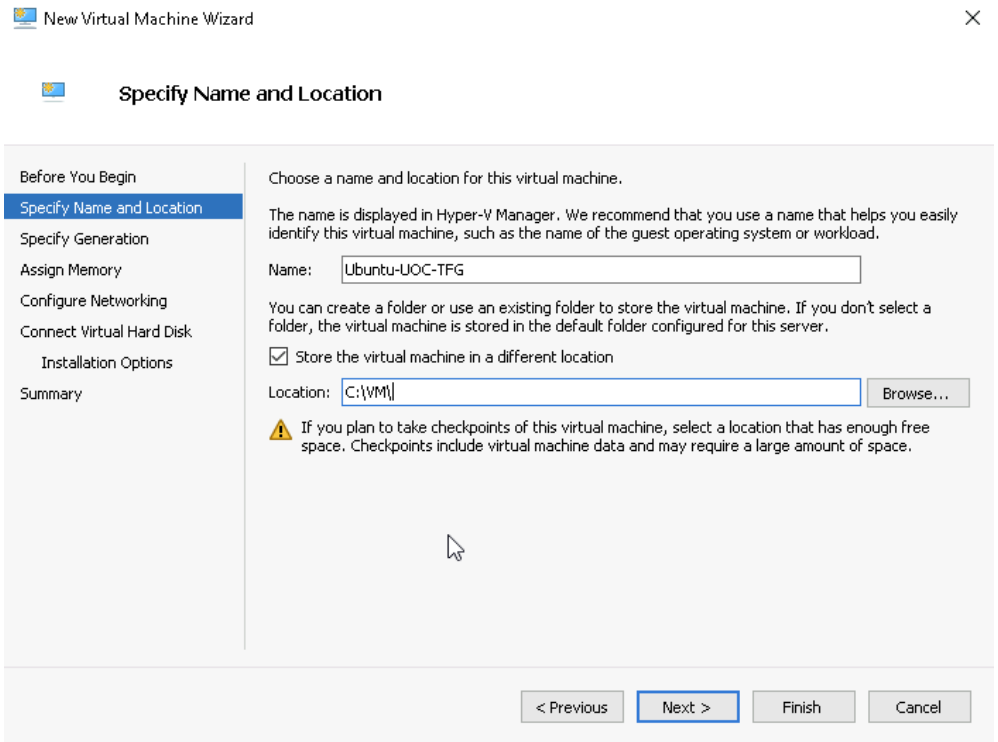
En primer lugar, se selecciona la opción New/Virtual Machine… del menú contextual del servidor Hyper-V.



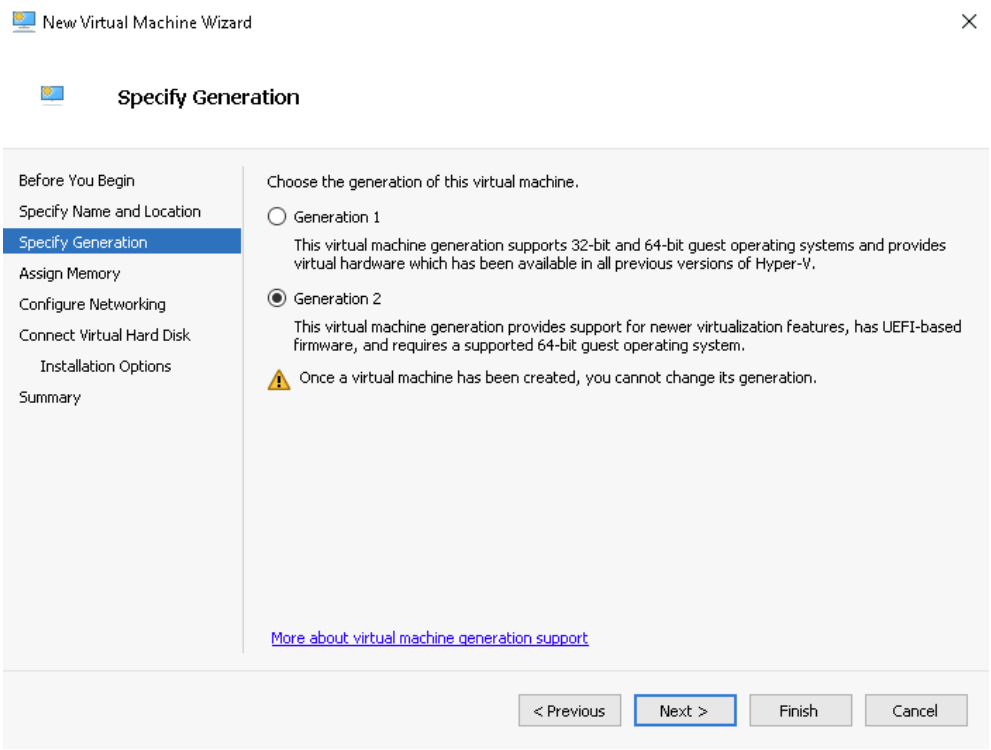
En el asistente de creación de máquina virtual, se hace click en “Next”.



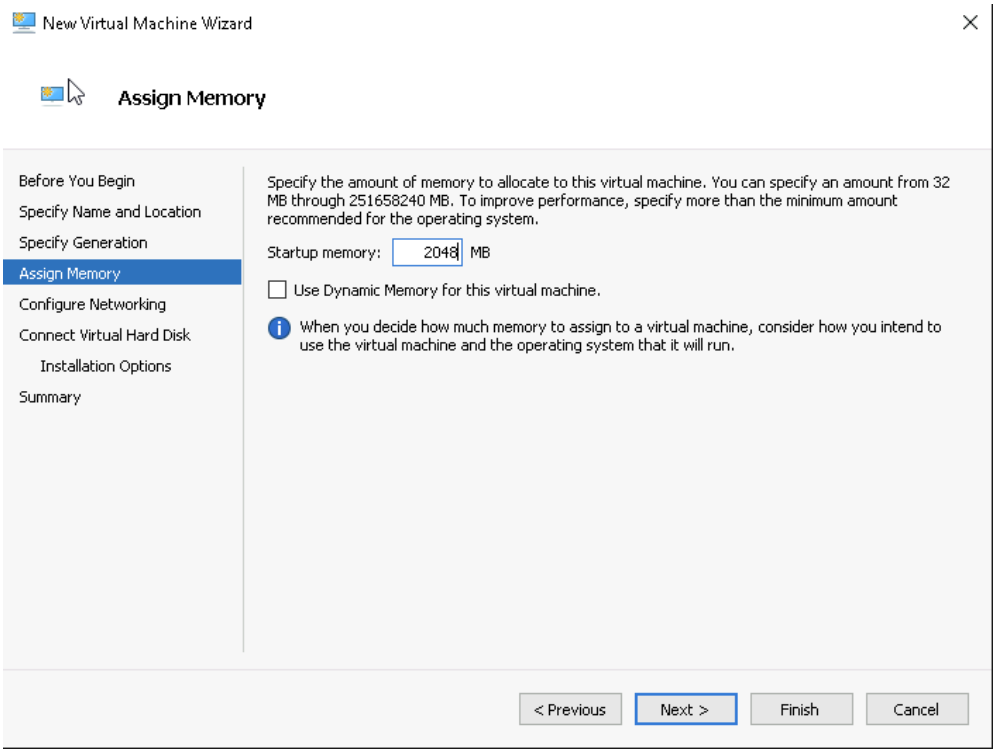
Se indica el nombre de la máquina virtual a crear y la ruta donde se alojarán los archivos.



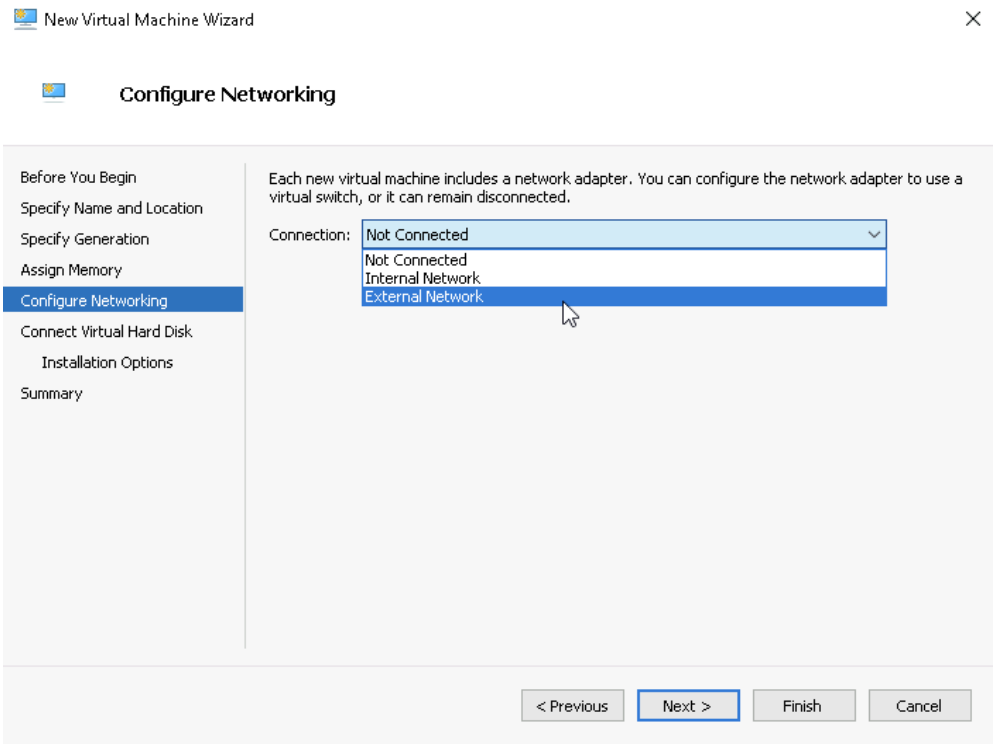
En generación, se selección “Generation 2”.



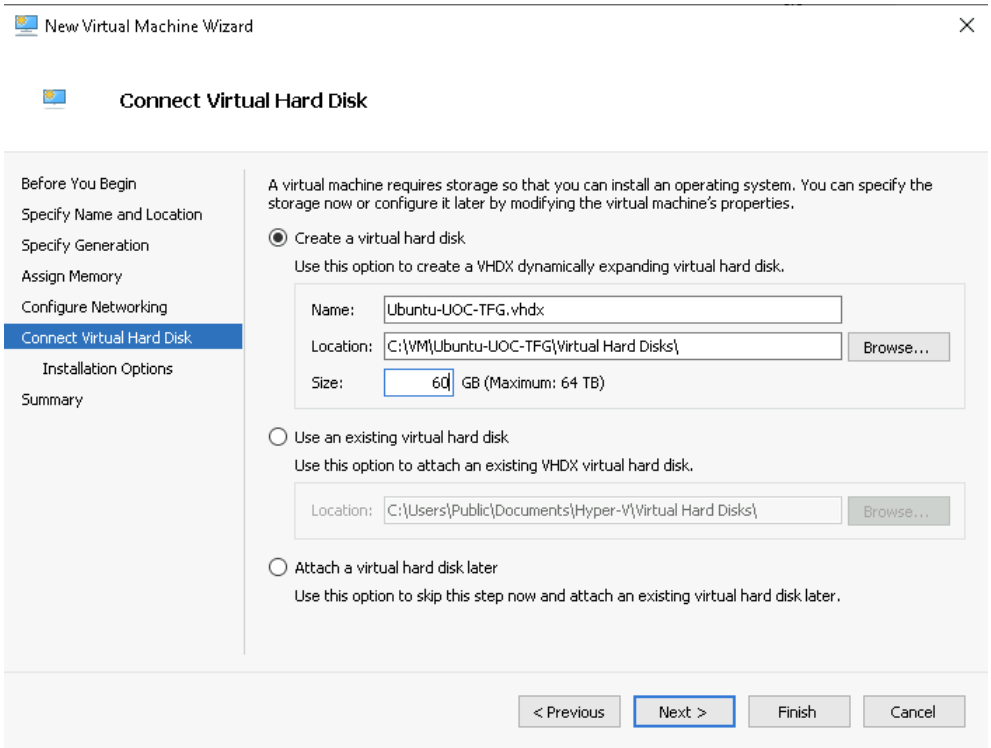
Se indica la memoria RAM de la que dispondrá la máquina virtual, 2 GB en este caso.



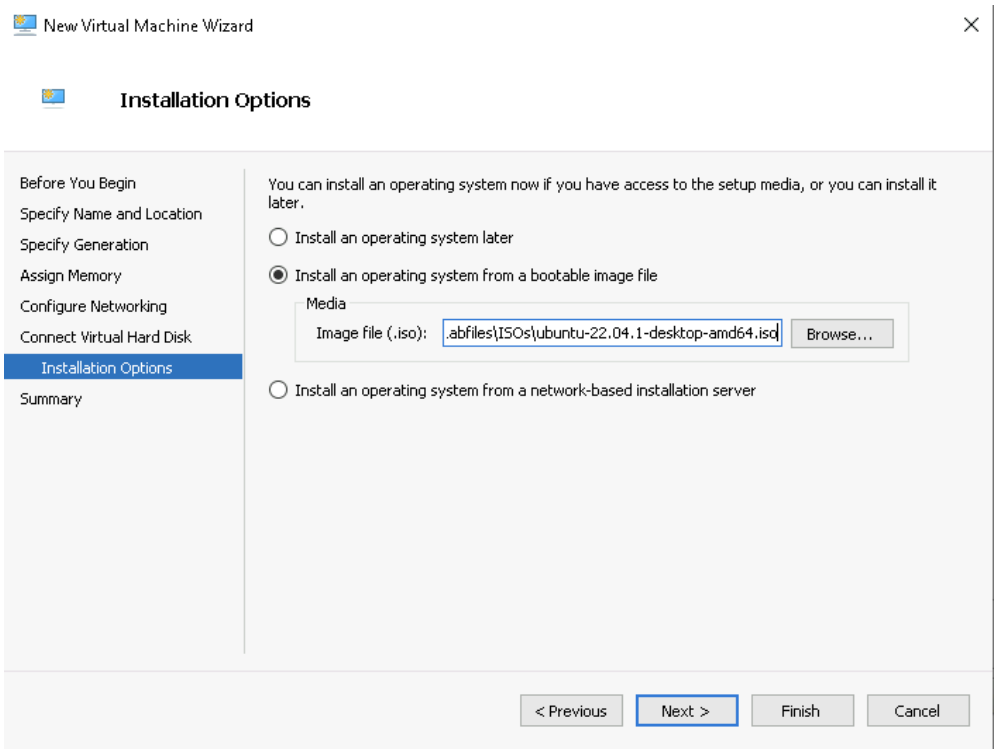
Se selecciona el adaptador de red que utilizará, “External Network”.



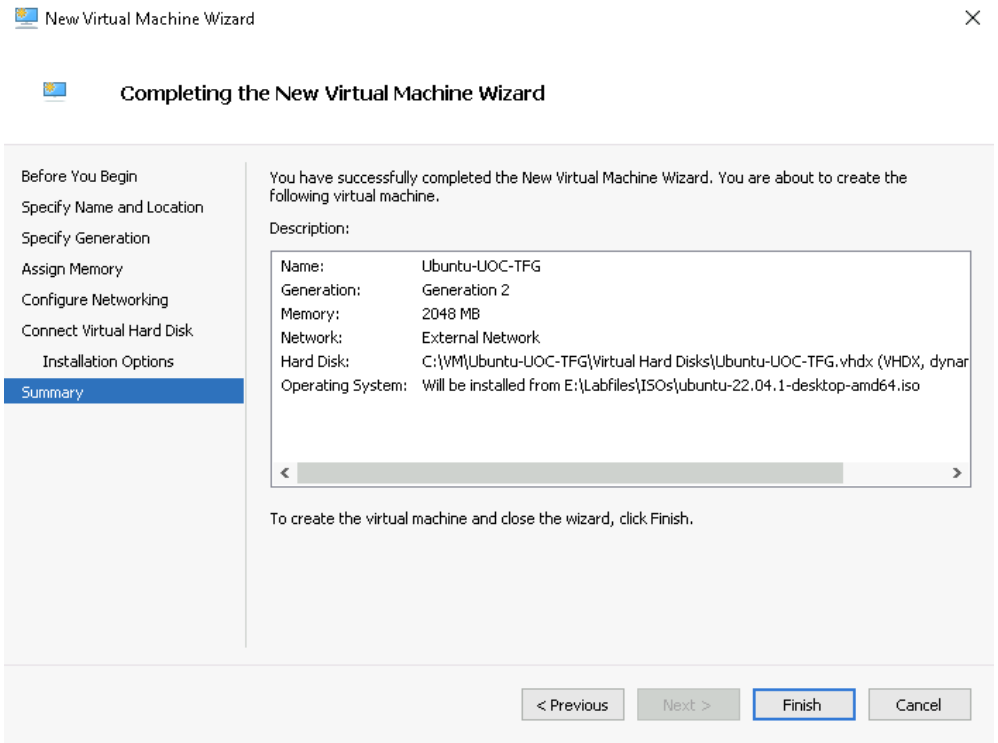
A continuación, se indica el nombre de disco duro, su ubicación y el tamaño.



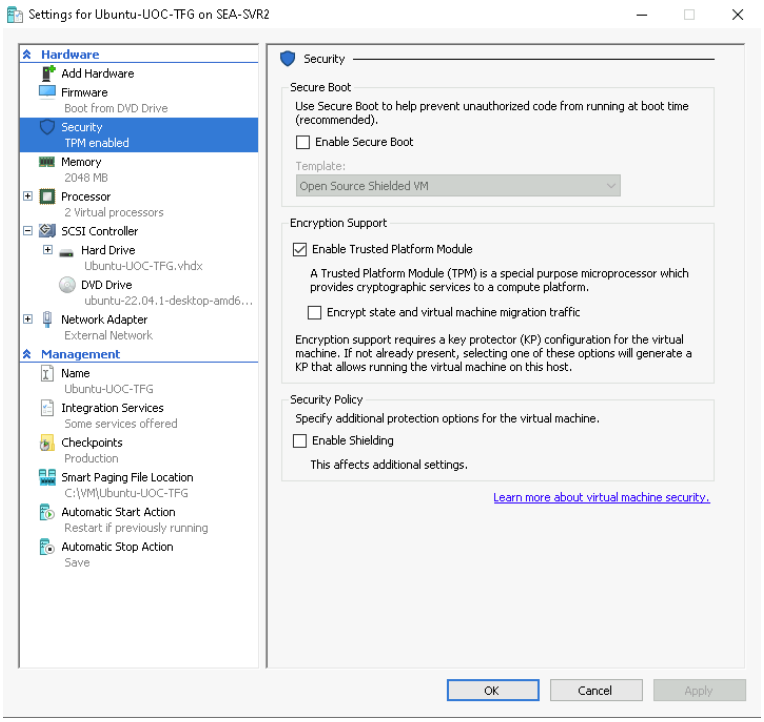
Por último, se selecciona cómo se va a realizar la instalación del sistema operativo. En este caso, mediante una imagen .iso, descargada de la web oficial de Ubuntu.



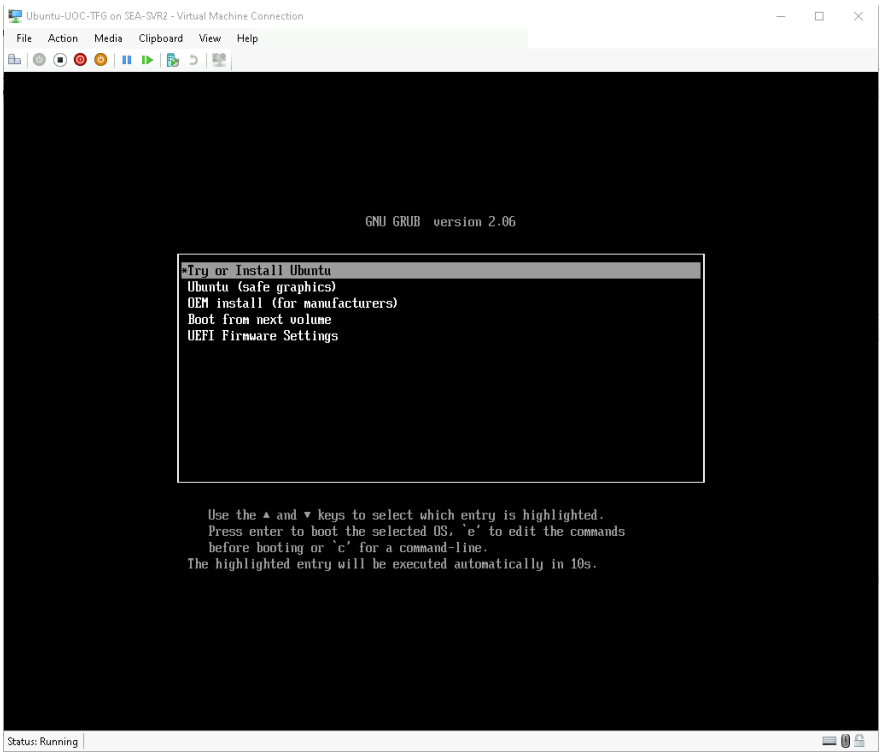
Se revisan los detalles de configuración elegidos y se pulsa en “Finish”.



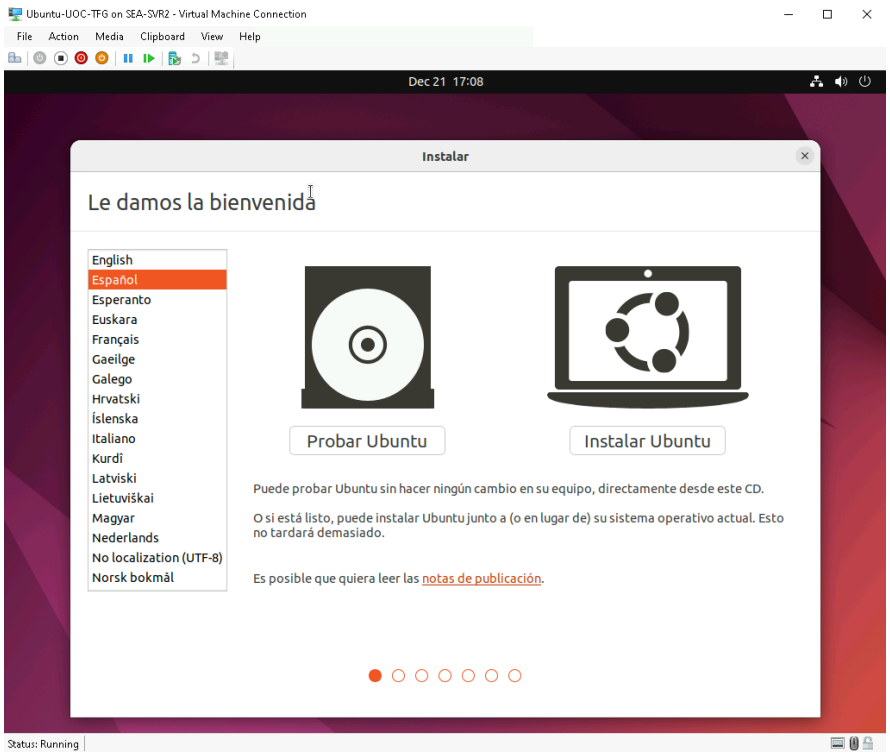
Como se trata de una máquina en la que se va a instalar un sistema operativo Linux, es necesario deshabilitar el arranque seguro (Secure Boot). Para ello, se accede a las propiedades de la máquina y se desmarca la opción en “Security”.

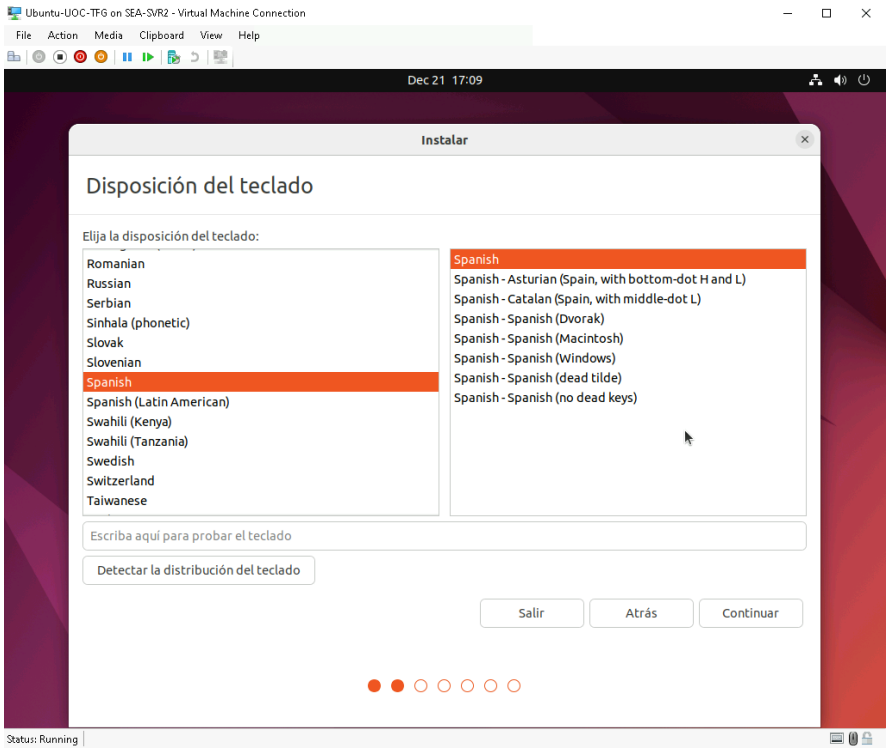


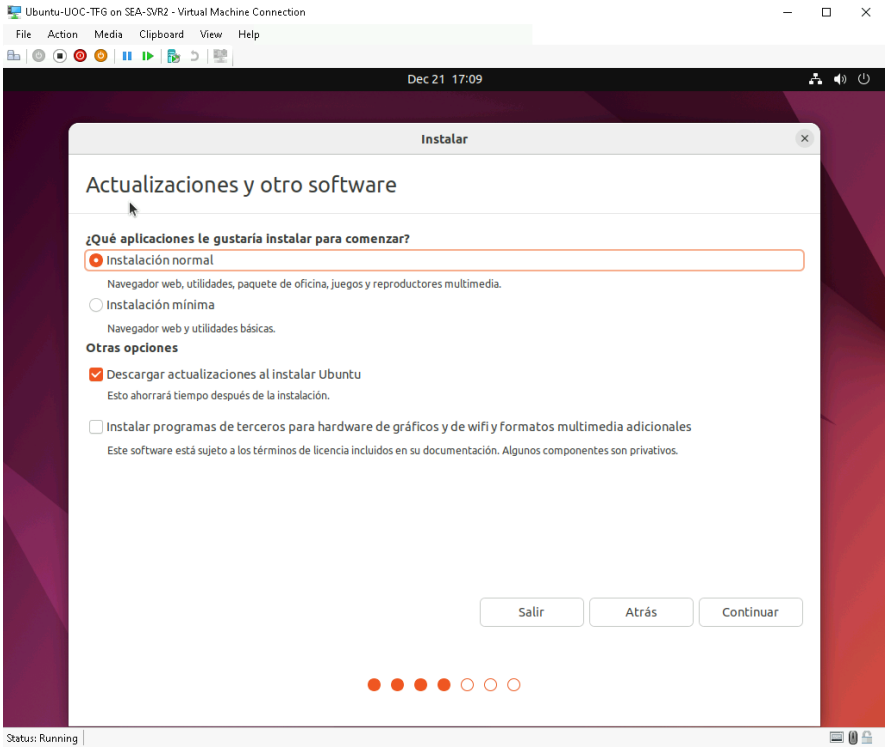
A continuación, se arranca la máquina virtual y se selecciona “Try or Install Ubuntu”.

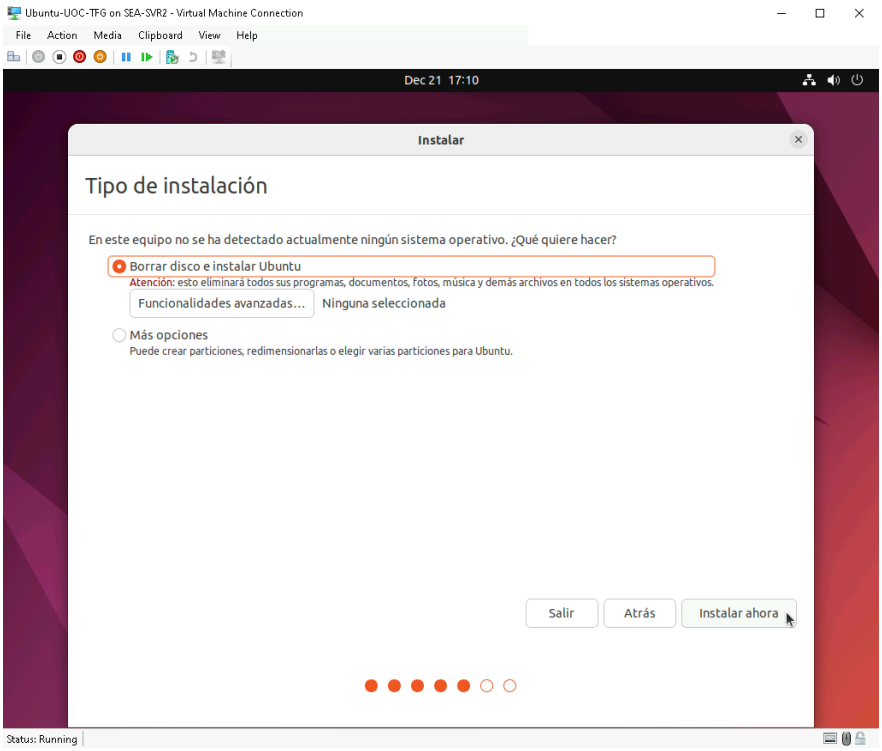


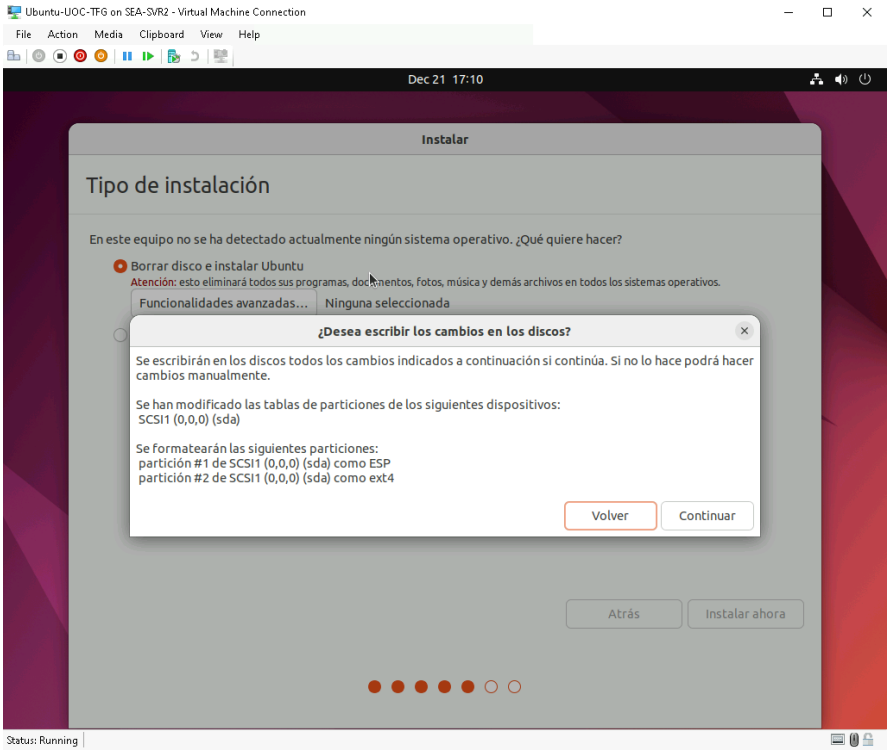
Se configuran las opciones deseadas del sistema operativo.

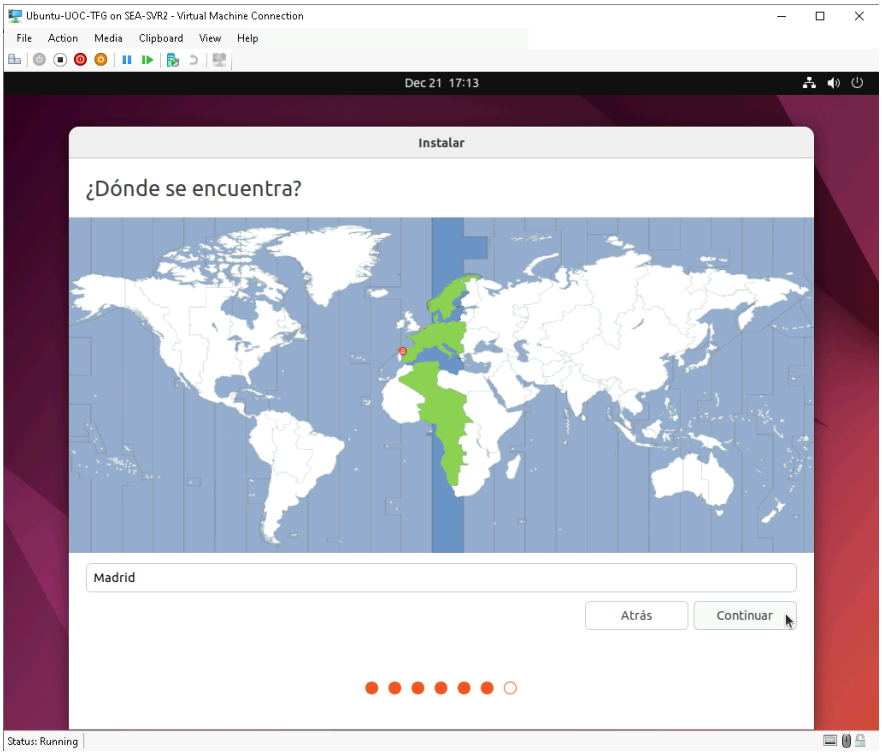




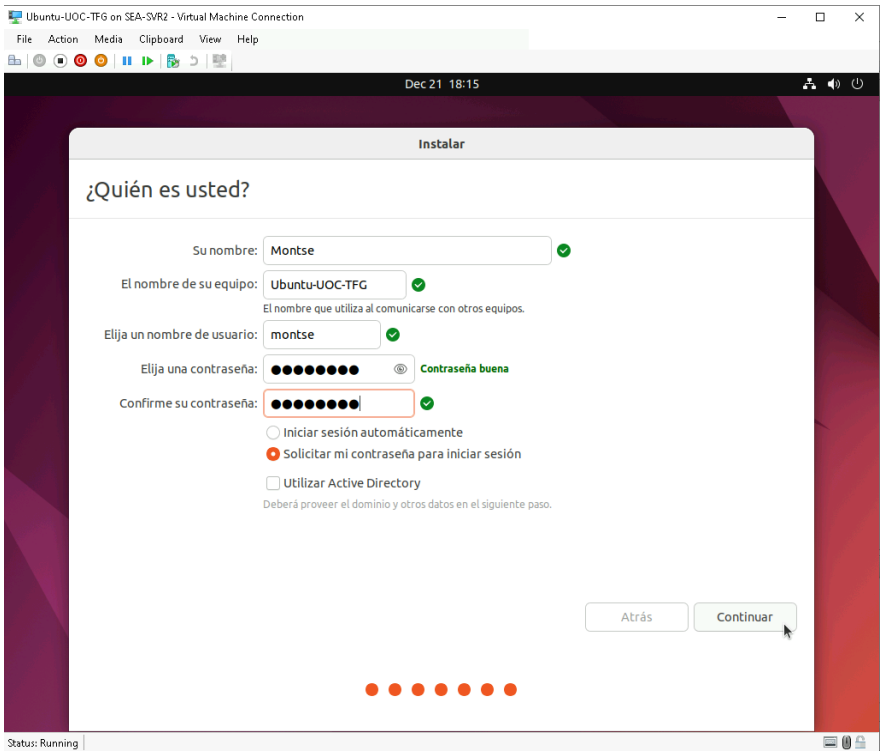

Ubuntu-UOC-TFG on SEA-SVR2 - Virtual Machine Connection
File Action Media Clipboard View Help
Dec 21 17:09
Instalar
Actualizaciones y otro software
¿Qué aplicaciones le gustaría instalar para comenzar?
Instalación normal
Navegador web, utilidades, paquete de oficina, juegos y reproductores multimedia.
Instalación mínima
Navegador web y utilidades básicas.
Otras opciones
Descargar actualizaciones al instalar Ubuntu
Esto ahorrará tiempo después de la instalación.
Instalar programas de terceros para hardware de gráficos y de wifi y formatos multimedia adicionales
Este software está sujeto a los términos de licencia incluidos en su documentación. Algunos componentes son privativos.
Salir
Atrás
Continuar
Status: Running

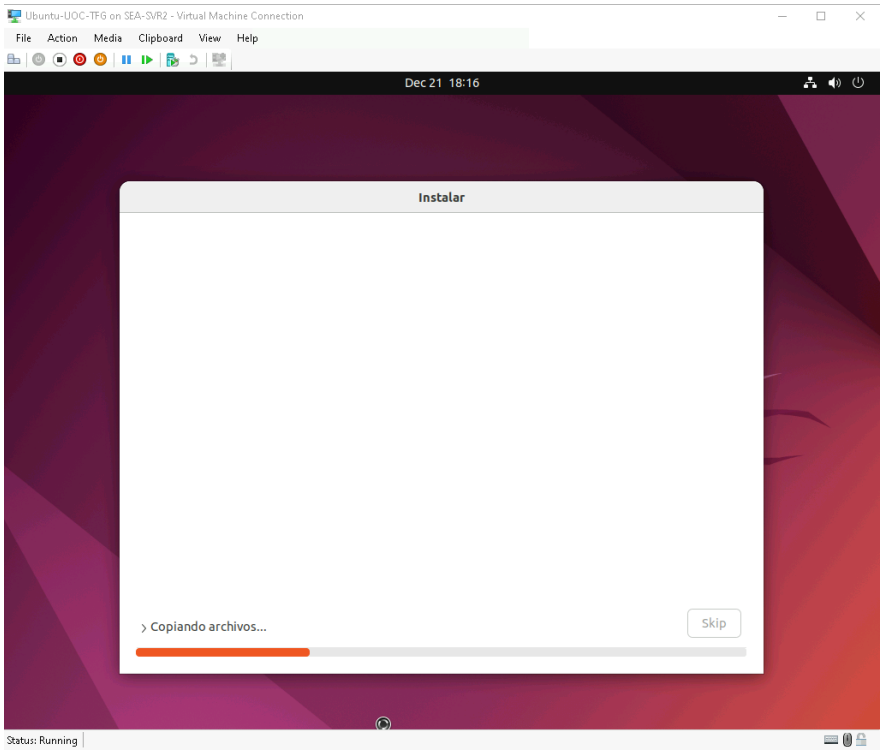

Ubuntu-UOC-TFG on SEA-SVR2 - Virtual Machine Connection
File Action Media Clipboard View Help
Dec 21 17:10
Instalar
Tipo de instalación
En este equipo no se ha detectado actualmente ningún sistema operativo. ¿Qué quiere hacer?
Borrar disco e instalar Ubuntu
Atención: esto eliminará todos sus programas, documentos, fotos, música y demás archivos en todos los sistemas operativos.
Funcionalidades avanzadas...
Ninguna seleccionada
Más opciones
Puede crear particiones, redimensionarlas o elegir varias particiones para Ubuntu.
Salir
Atrás
Instalar ahora
Status: Running

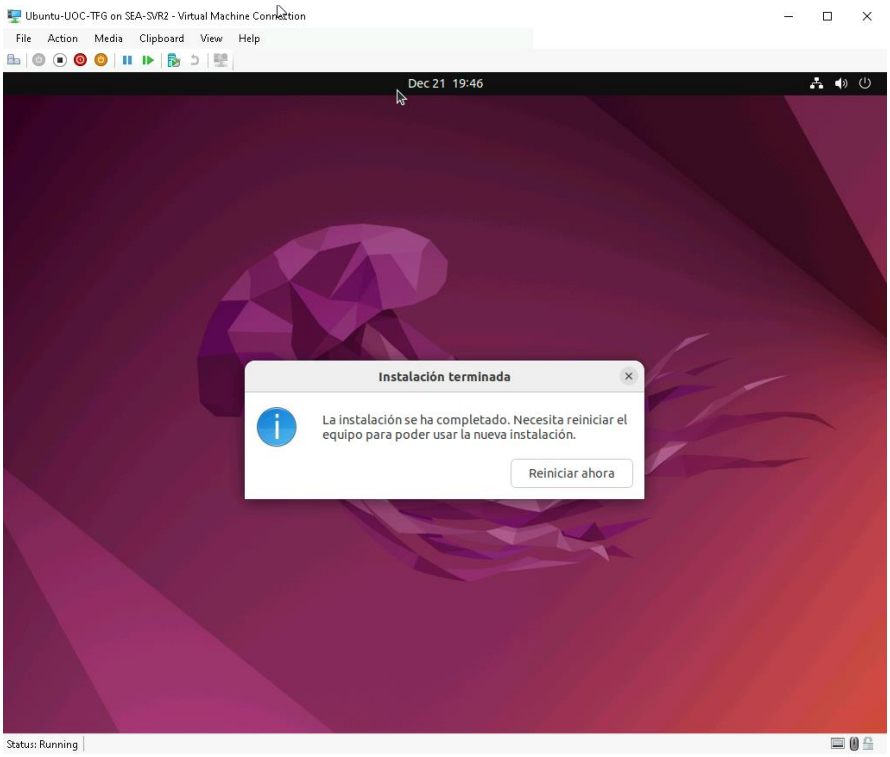

Ubuntu-UOC-TFG on SEA-SVR2 - Virtual Machine Connection
File Action Media Clipboard View Help
Dec 21 17:10
Instalar
Tipo de instalación
En este equipo no se ha detectado actualmente ningún sistema operativo. ¿Qué quiere hacer?
Borrar disco e instalar Ubuntu
Atención: esto eliminará todos sus programas, documentos, fotos, música y demás archivos en todos los sistemas operativos.
Funcionalidades avanzadas...
Ninguna seleccionada
¿Desea escribir los cambios en los discos?
Se escribirán en los discos todos los cambios indicados a continuación si continúa. Si no lo hace podrá hacer cambios manualmente.
Se han modificado las tablas de particiones de los siguientes dispositivos:
SCSI1 (0,0,0) (sda)
Se formatearán las siguientes particiones:
partición #1 de SCSI1 (0,0,0) (sda) como ESP
partición #2 de SCSI1 (0,0,0) (sda) como ext4
Volver
Continuar
Atrás
Instalar ahora
Status: Running


Ubuntu-UOC-TFG on SEA-SVR2 - Virtual Machine Connection
File Action Media Clipboard View Help
Dec 21 17:13
Instalar
¿Dónde se encuentra?
Madrid
Atrás
Continuar
Status: Running

Se indica el nombre de usuario local y contraseña, así como el nombre que tendrá el equipo, y se hace click en “Continuar” para que comience la instalación.







Una vez terminada la instalación, se hace click en “Reiniciar ahora” y el sistema operativo está listo para ser usado.

Anexo 13. Proceso de inscripción de dispositivos en Intune

- **Dispositivos Windows**

El proceso de inscripción de los dispositivos Windows es distinto dependiendo de si los dispositivos se van a inscribir directamente mediante AutoPilot, son dispositivos corporativos que se unen a Azure Active Directory o son dispositivos personales que se inscriben para poder tener acceso a los recursos empresariales (BYOD).

A continuación, se muestra el proceso de inscripción en los tres casos indicados.

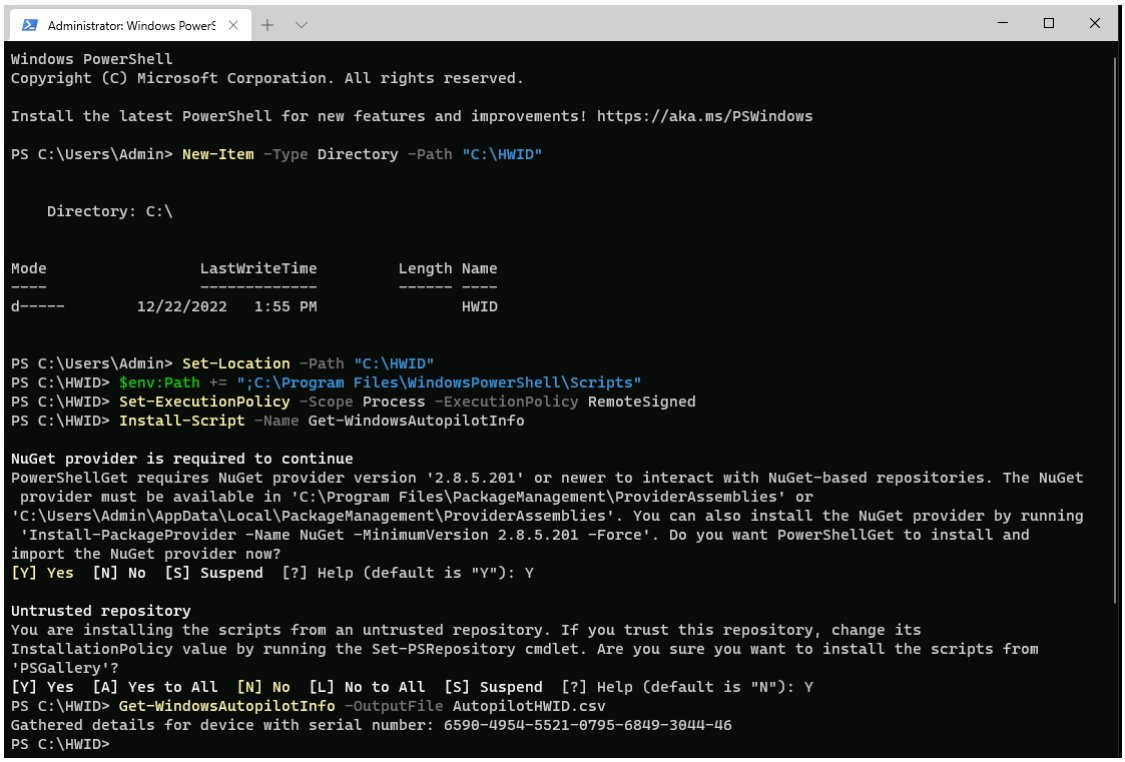
- Dispositivos Windows AutoPilot

Los dispositivos Windows AutoPilot son aquellos que se unen a Azure Active Directory cuando se encienden por primera vez y disponen de una conexión a Internet. Debido a la configuración de inscripción automática en Microsoft Intune, en cuanto se unen a Azure AD, se inscriben también en Intune.

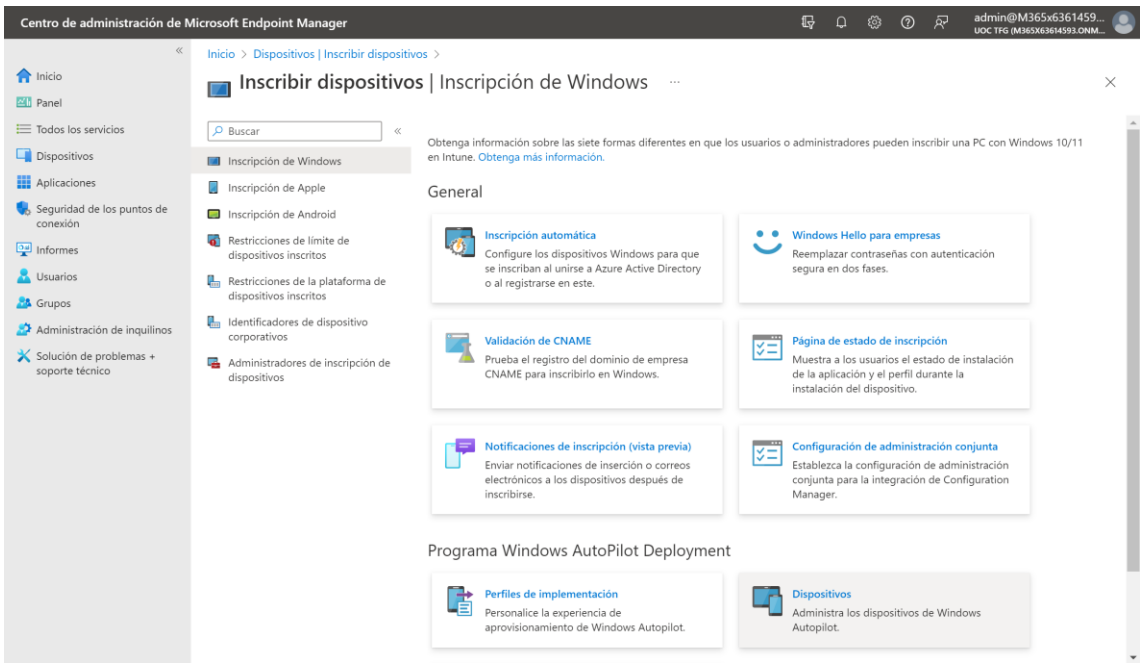
Para que el dispositivo se pueda inscribir mediante AutoPilot es necesario aprovisionarlo primero en Intune mediante su identificador único de HW. Esto lo puede realizar el proveedor del dispositivo en nombre de la organización o algún administrador de la propia organización.

El identificador de HW se puede extraer mediante un script proporcionado por Microsoft llamado Get-WindowsAutopilotInfo, disponible para su instalación en el repositorio NuGet de Microsoft. Al script se le pasa como parámetro un fichero de salida en formato .csv, en el cual se almacena la información de HW del equipo que será subida a Intune más adelante. El script debe ser ejecutado con privilegios de administrador.

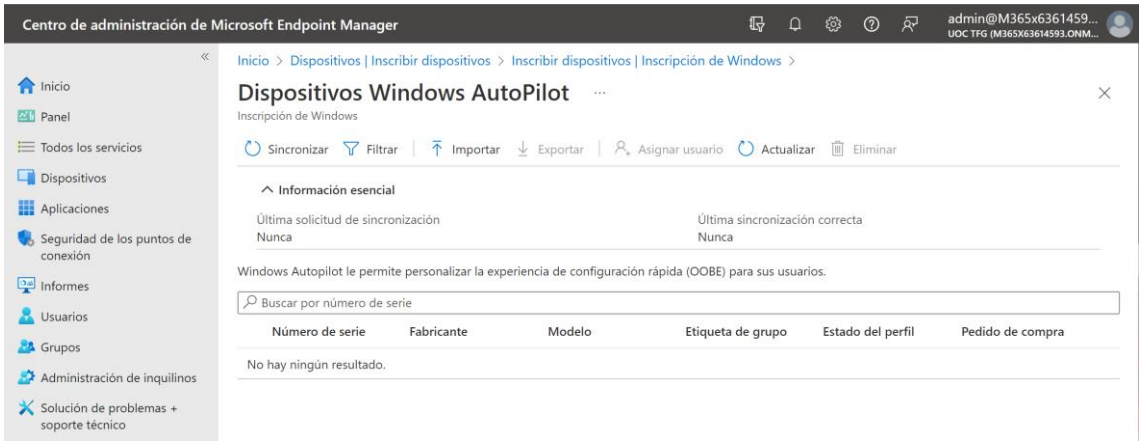
La siguiente captura muestra la ejecución del script para obtener el identificador único de HW del dispositivo.

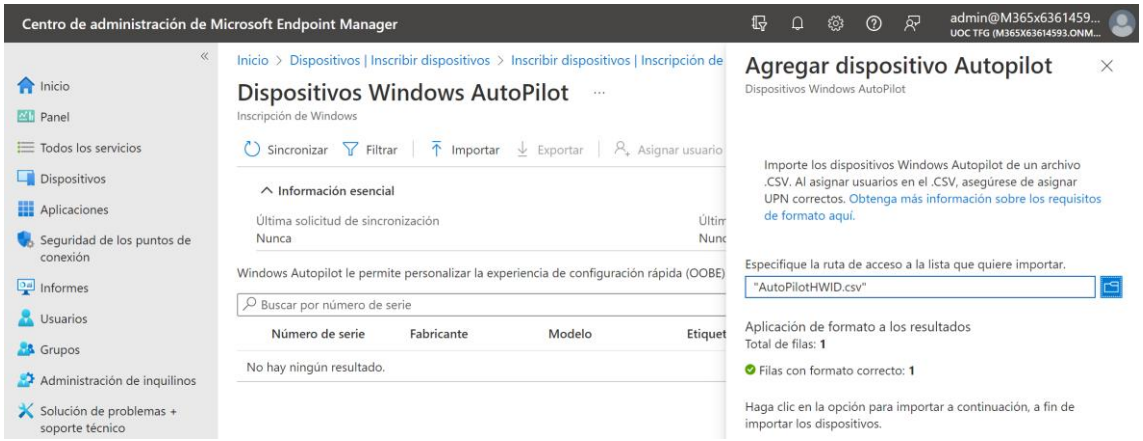


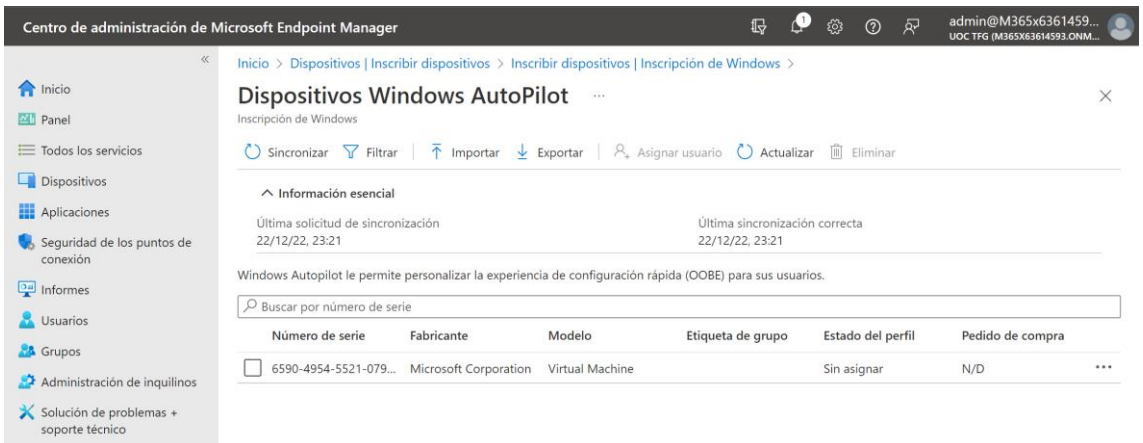
Una vez se dispone del fichero .csv con la información necesaria, se puede importar en Intune mediante el apartado “Dispositivos” del programa Windows AutoPilot Deployment, disponible en el menú Dispositivos/Inscribir dispositivos/Inscripción de Windows.



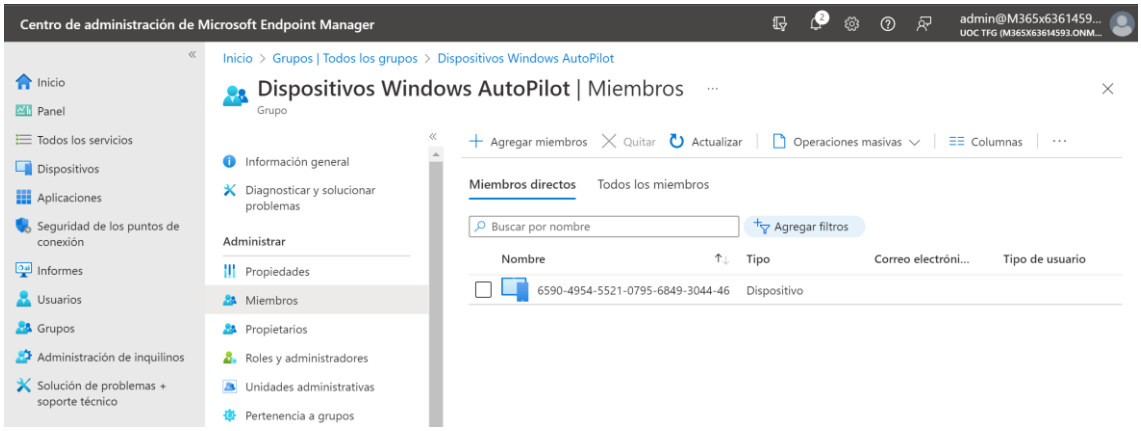
Para importar el archivo .csv, se hace click en “Importar” y se selecciona el archivo deseado.



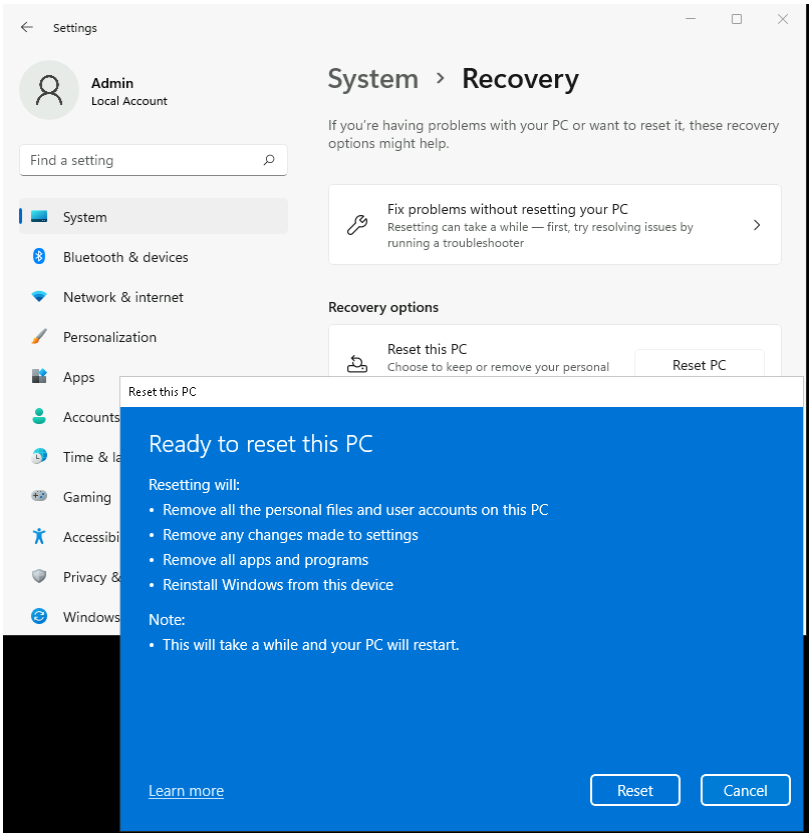




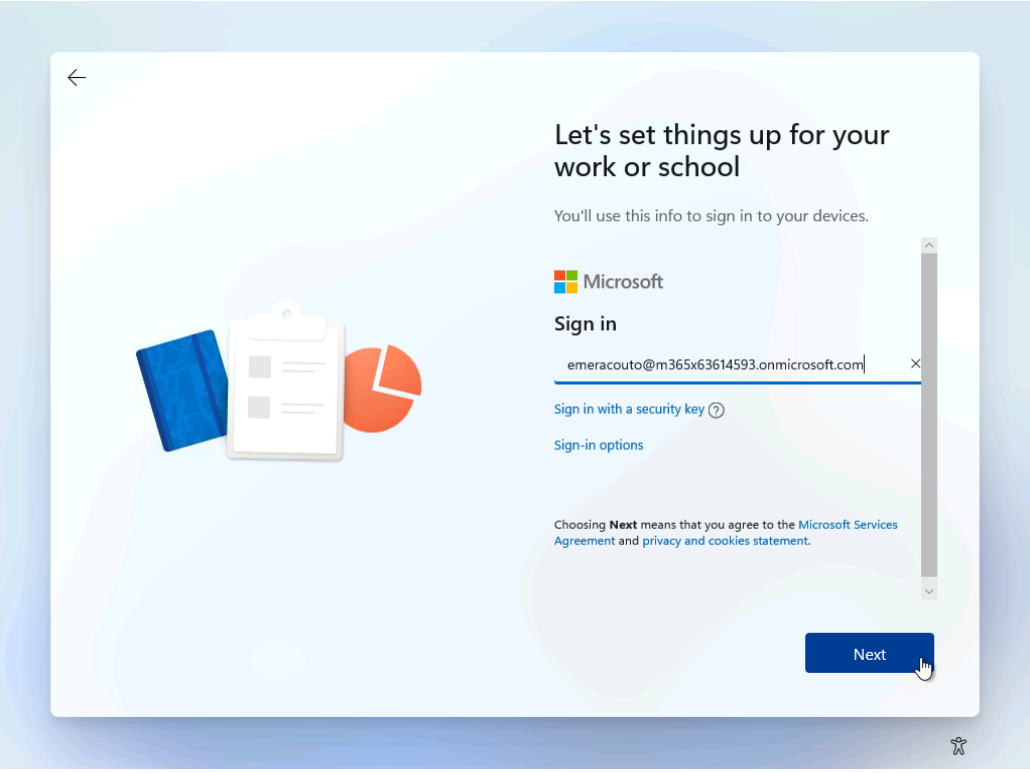
Por último, se añade el dispositivo al grupo “Dispositivos Windows AutoPilot”, que es el grupo que tiene asignado el perfil de implementación de Windows AutoPilot.

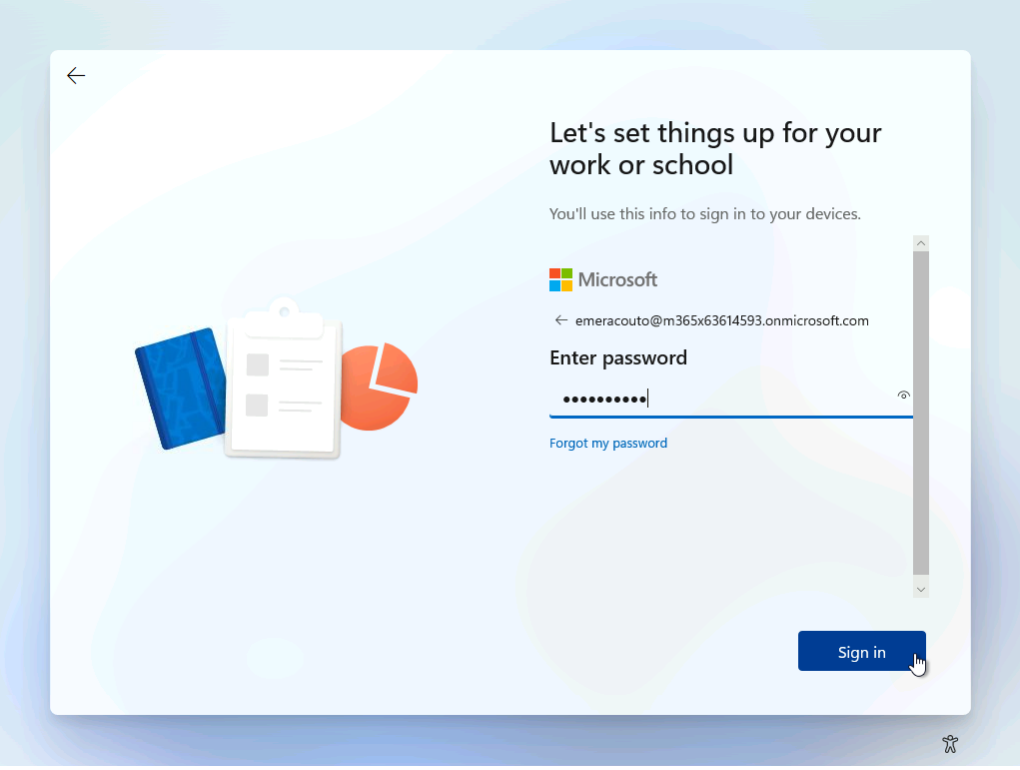


Ya en el dispositivo, en este caso una máquina virtual, se restablece el sistema operativo para que se inicie el proceso de inscripción automático en el primer arranque del sistema operativo. Esto no es necesario en dispositivos nuevos.

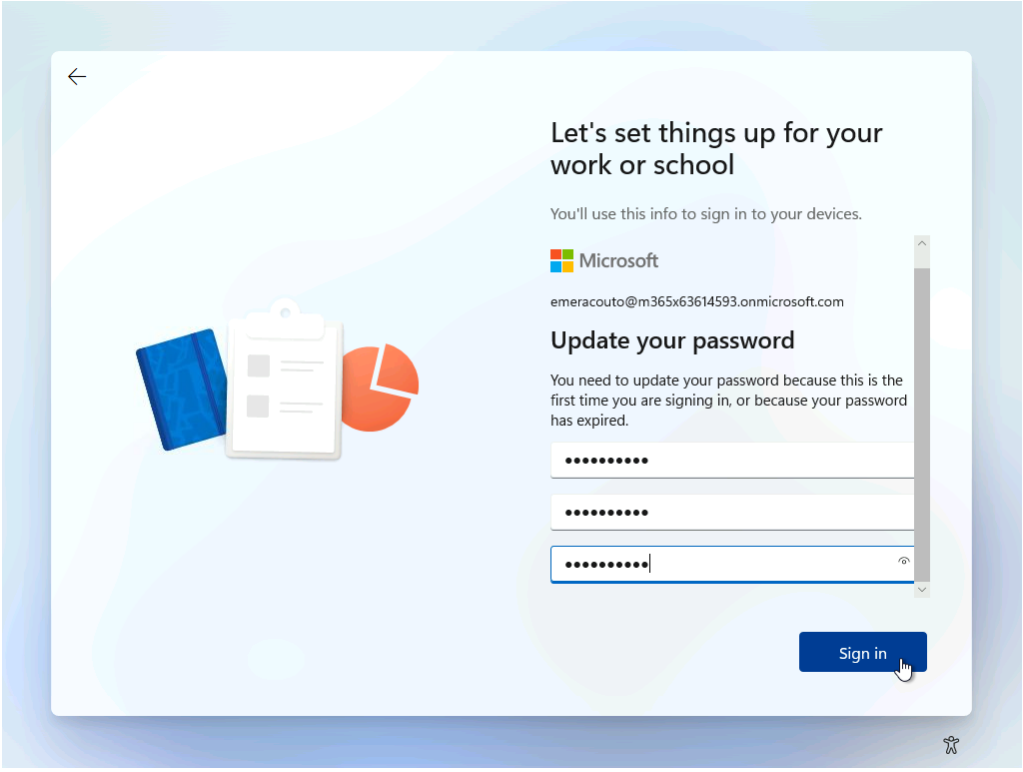


Tras el restablecimiento del sistema operativo a la configuración de inicio y conectar el equipo a Internet, el dispositivo contacta con los servidores de Microsoft y solicita las credenciales corporativas para unirse a la organización a la que está aprovisionado.

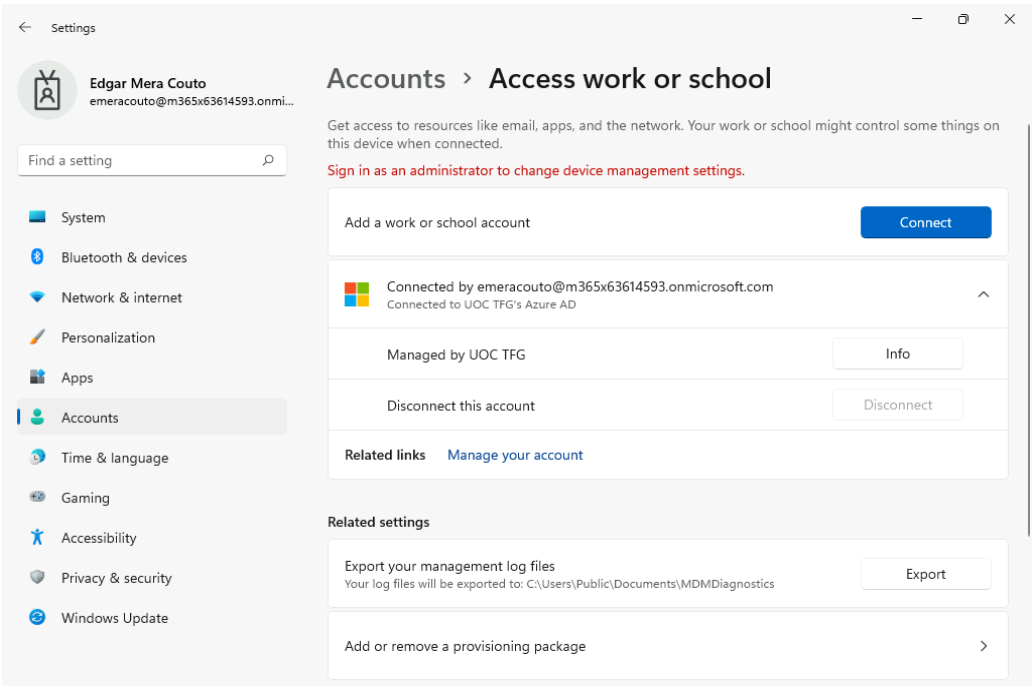


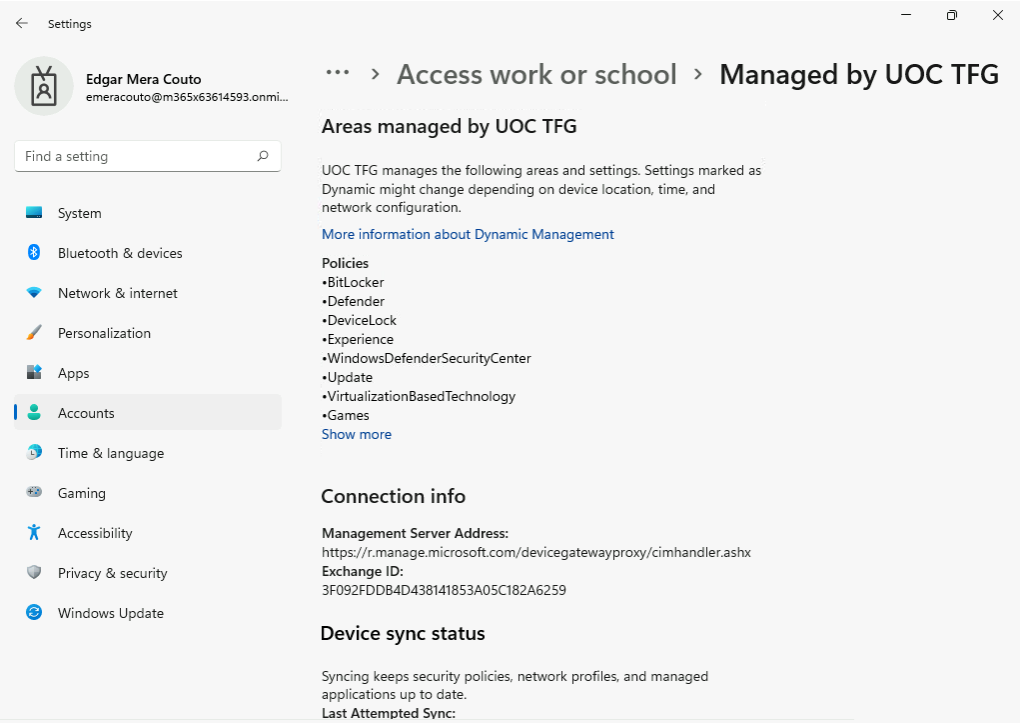


Como es la primera vez que Edgar inicia sesión, se le solicita que actualice la contraseña.



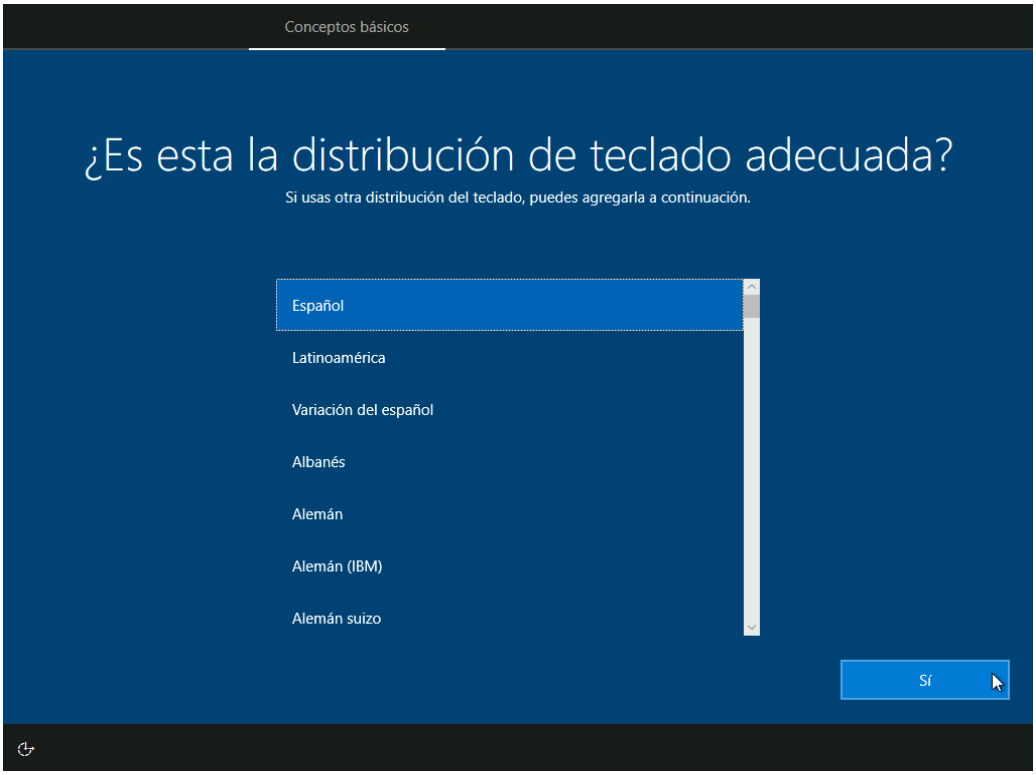
Tras la validación con las credenciales de Edgar, el equipo se une al tenant de UOC TFG y arranca sin mostrar ninguna opción de configuración adicional en la OOBE, pues ya ha sido configurado por la compañía en el perfil de implementación asignado. Además, se inscribe en Intune automáticamente.

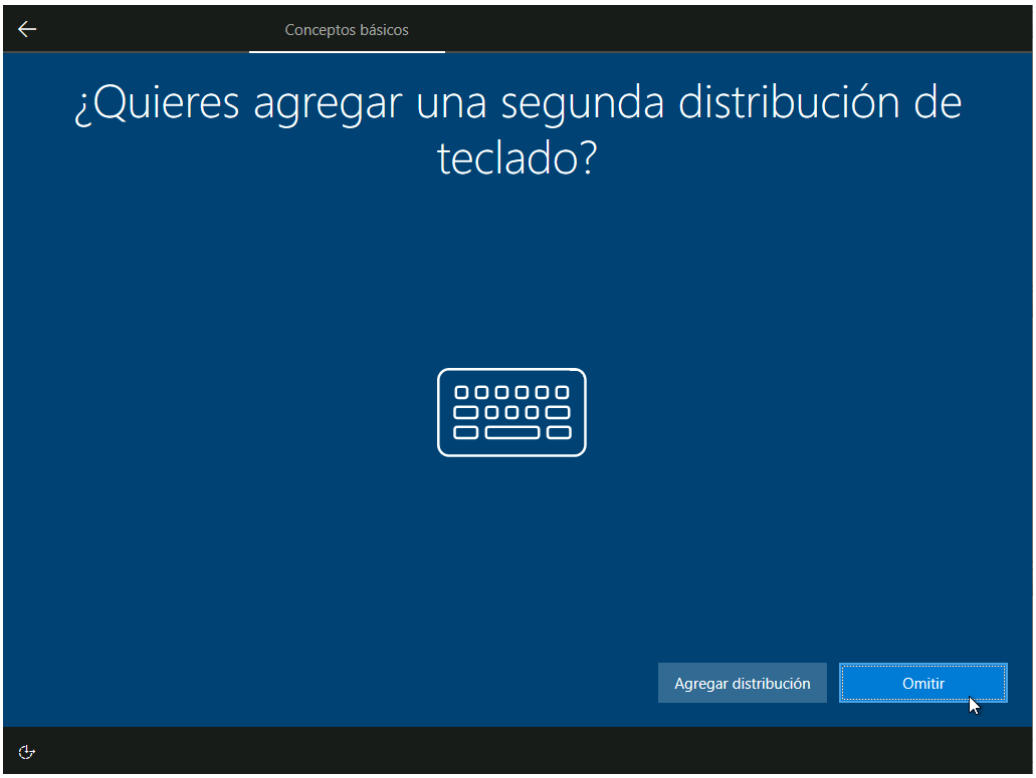




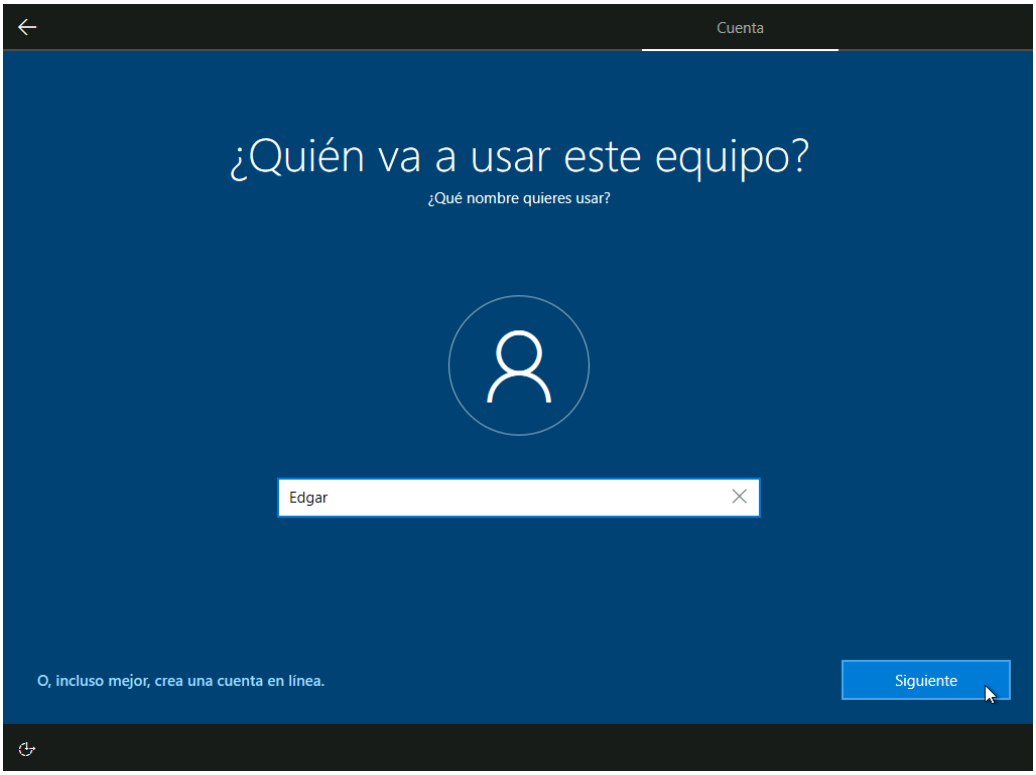
- Dispositivos Windows Corporativos

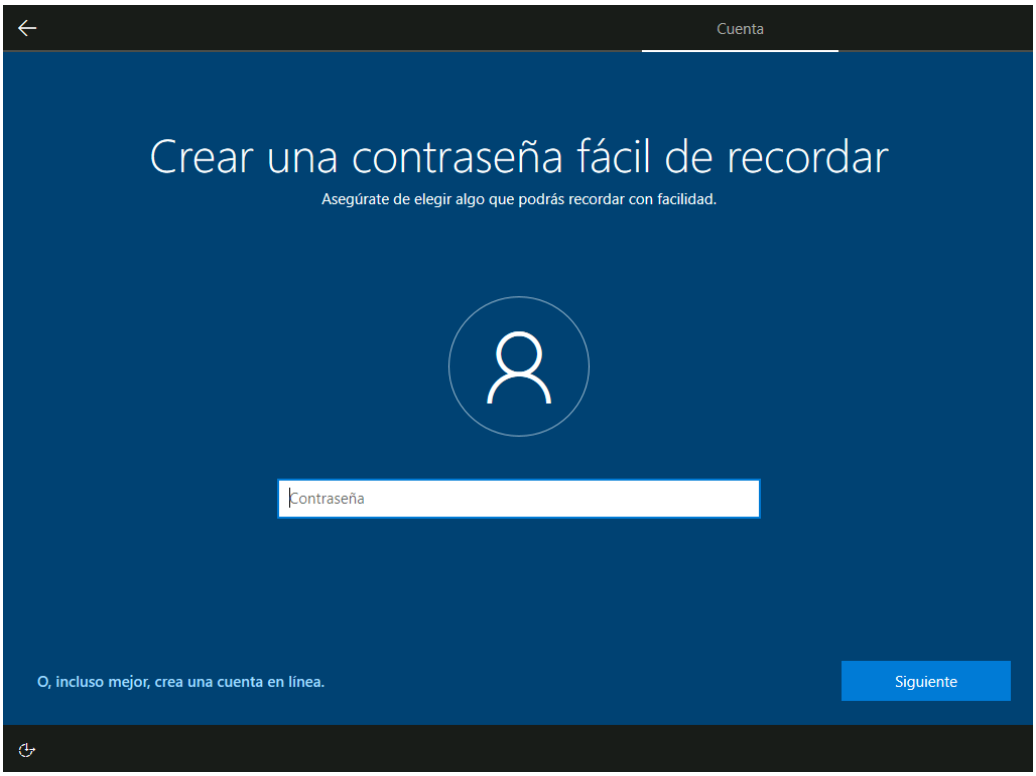
En los dispositivos Windows corporativos, la inscripción en Intune se realizará también de forma automática al unir el equipo a Azure AD. Esto se puede hacer durante el proceso OOBE, o desde la configuración del sistema operativo (como se muestra a continuación).



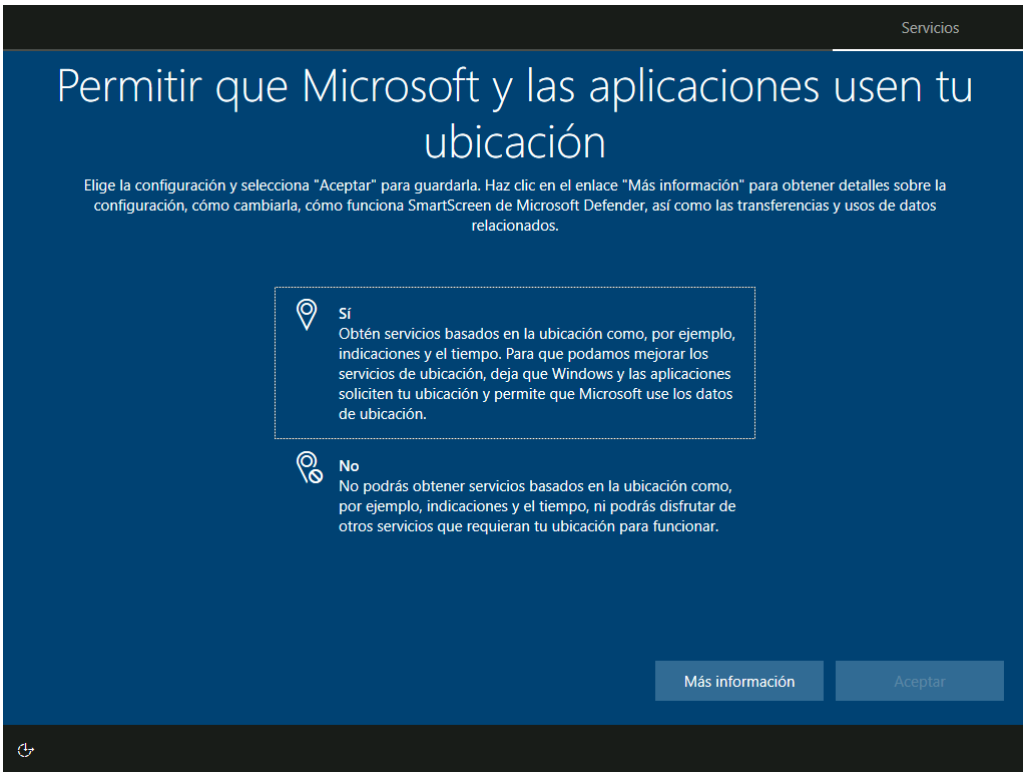


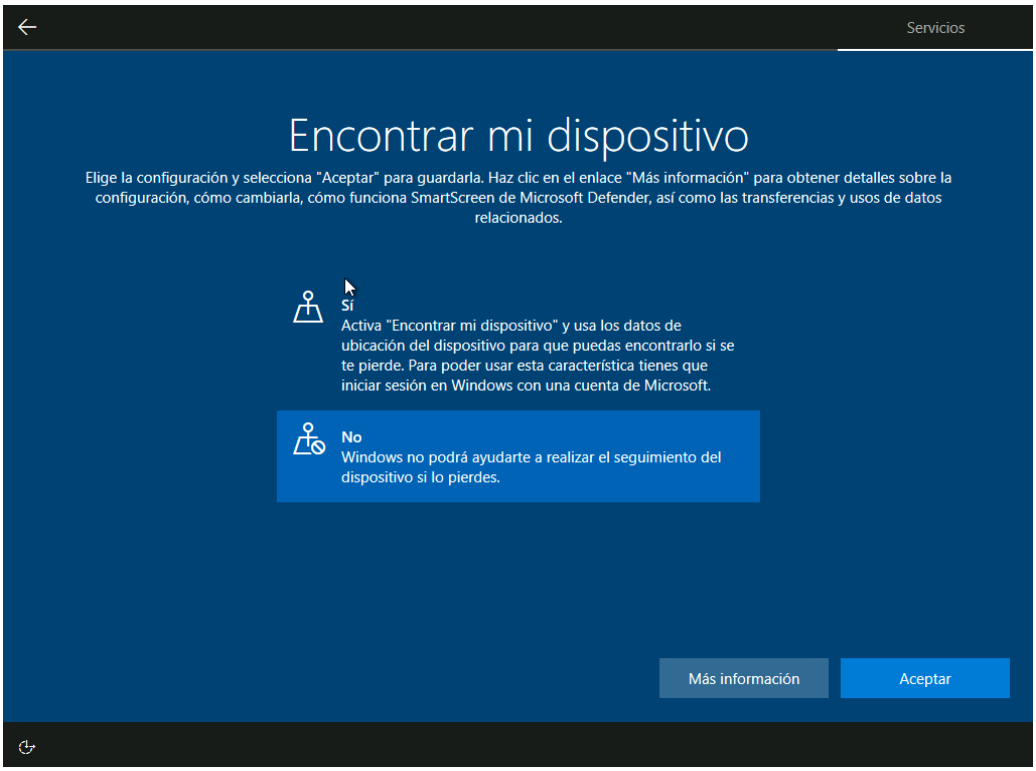
A diferencia del dispositivo preaprovisionado en AutoPilot, en este caso es posible crear una cuenta de usuario local.



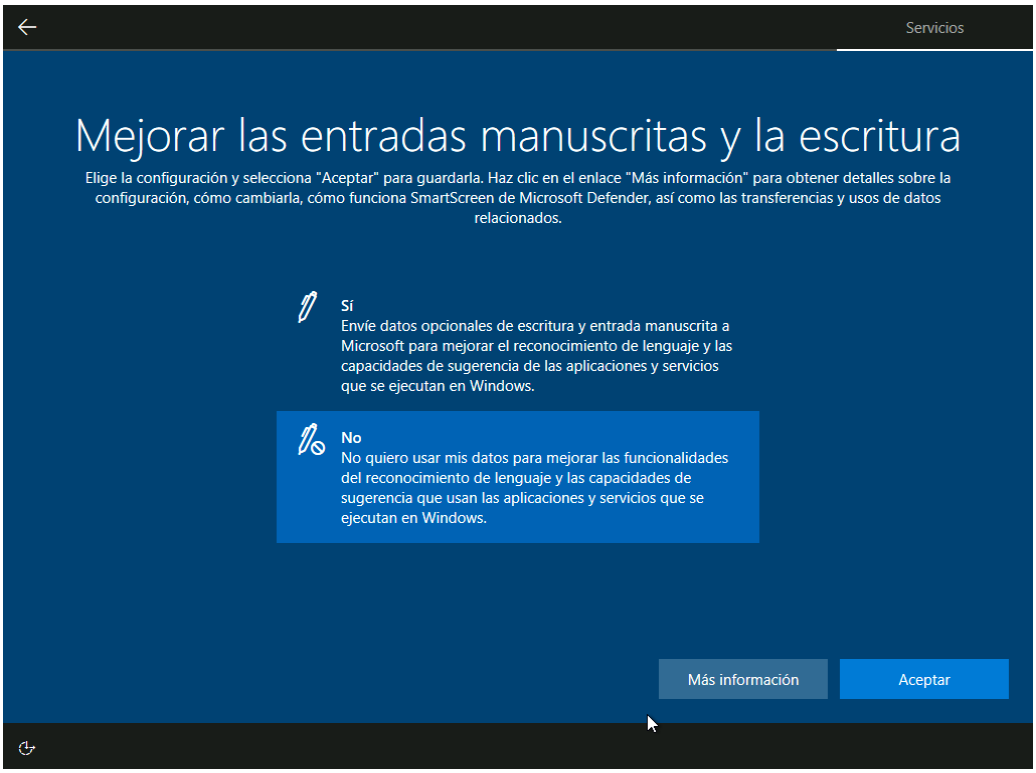


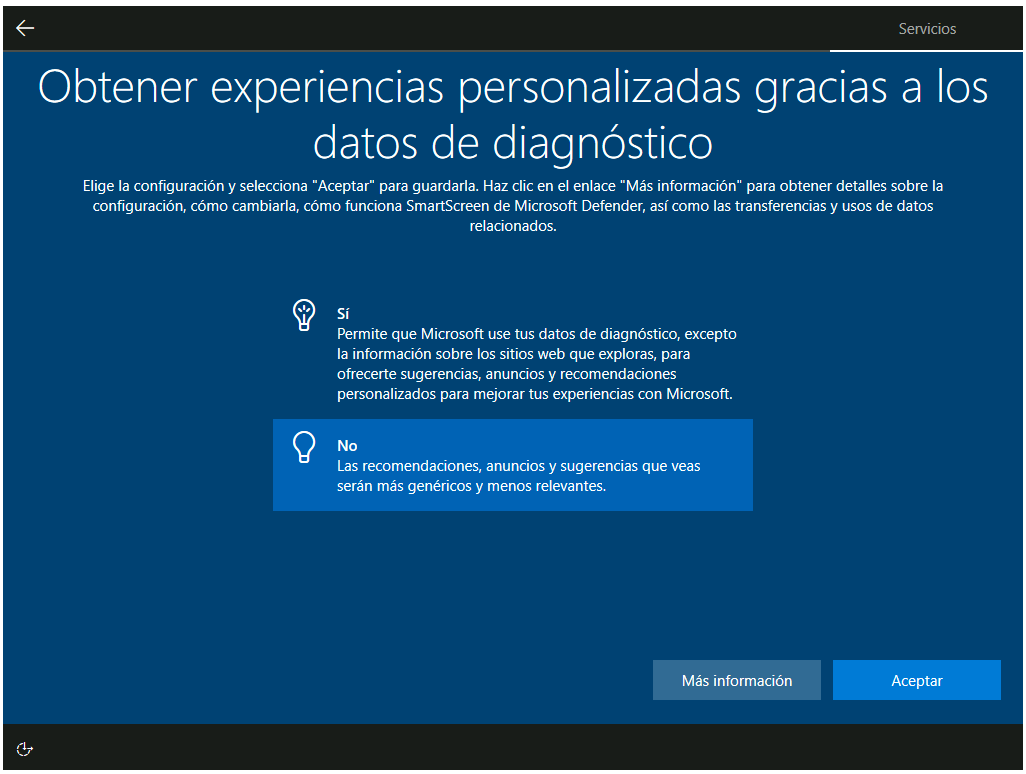
Una vez definidos el nombre de la cuenta local y la contraseña, se deben personalizar los ajustes del sistema operativo (ya preconfigurados en el caso de Windows AutoPilot, mediante el perfil de implementación).

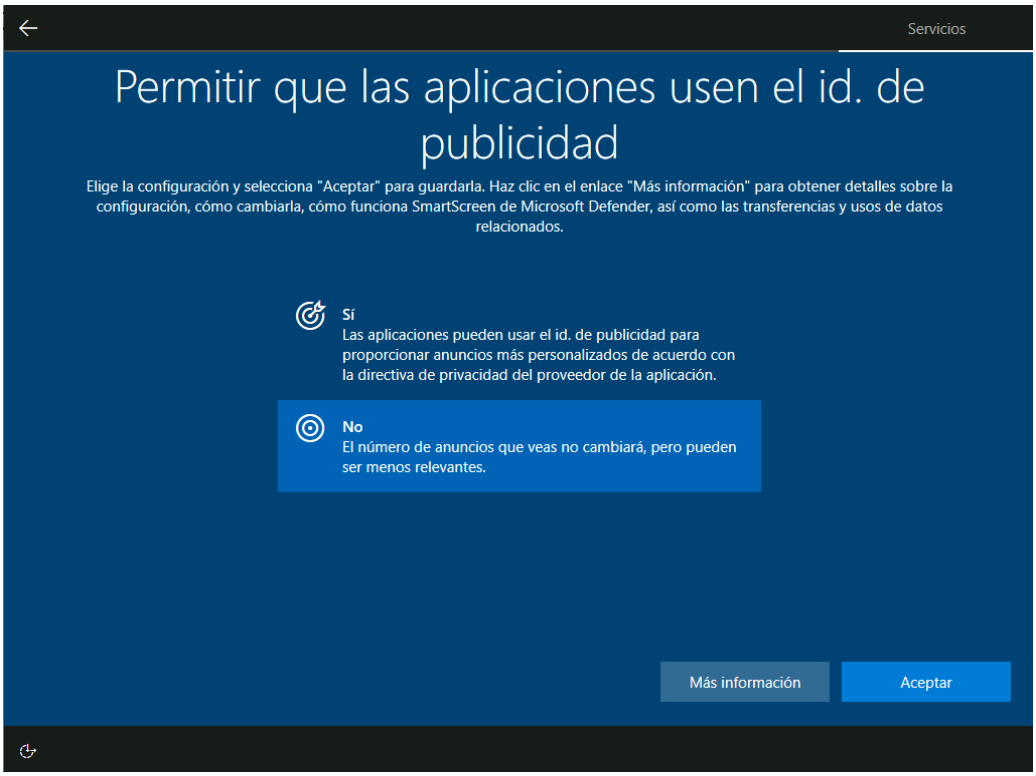


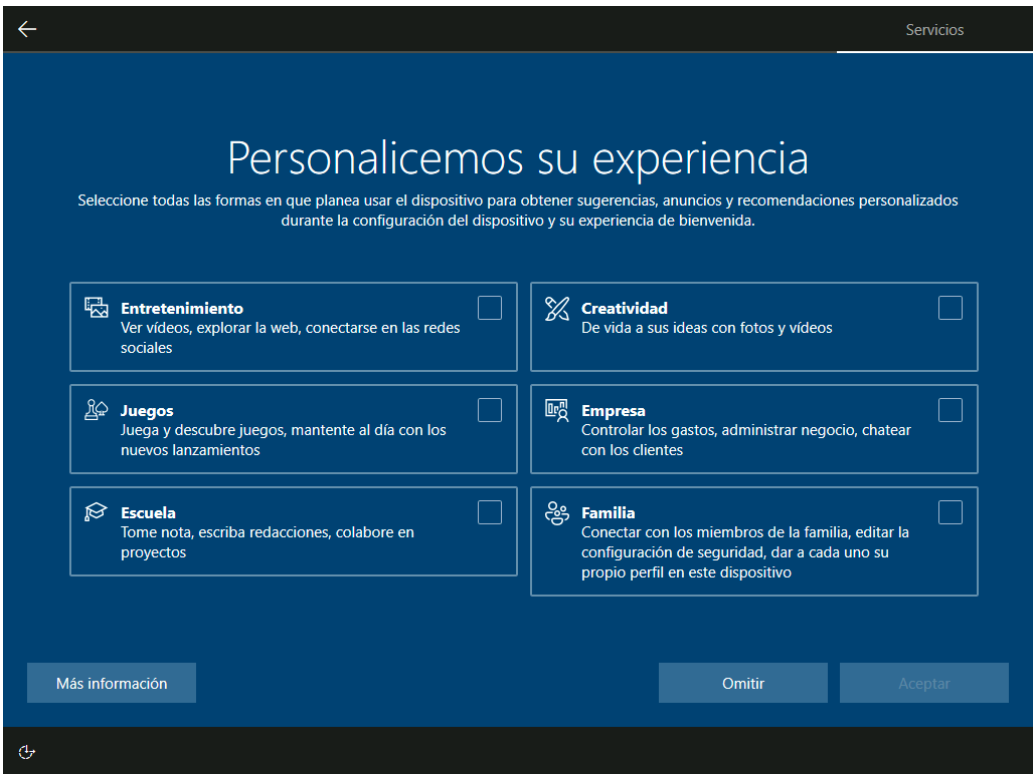

Servicios
Encontrar mi dispositivo
Elige la configuración y selecciona "Aceptar" para guardarla. Haz clic en el enlace "Más información" para obtener detalles sobre la configuración, cómo cambiarla, cómo funciona SmartScreen de Microsoft Defender, así como las transferencias y usos de datos relacionados.
Sí
Activa "Encontrar mi dispositivo" y usa los datos de ubicación del dispositivo para que puedas encontrarlo si se te pierde. Para poder usar esta característica tienes que iniciar sesión en Windows con una cuenta de Microsoft.
No
Windows no podrá ayudarte a realizar el seguimiento del dispositivo si lo pierdes.
Más información
Aceptar

Servicios
Enviar datos de diagnóstico a Microsoft
Elige la configuración y selecciona "Aceptar" para guardarla. Haz clic en el enlace "Más información" para obtener detalles sobre la configuración, cómo cambiarla, cómo funciona SmartScreen de Microsoft Defender, así como las transferencias y usos de datos relacionados.
Enviar Datos de diagnóstico requeridos y opcionales
Envíe información sobre los sitios web que explora y el uso de las aplicaciones y características, así como información adicional sobre el estado del dispositivo, la actividad del dispositivo e informes sobre la mejora de errores. Los datos de diagnóstico se usan para mantener Windows actualizado y protegido, solucionar problemas y realizar mejoras en los productos. Siempre se incluirán los datos de diagnóstico requeridos cuando elija Datos de diagnóstico opcionales. Independientemente su decisión, el dispositivo estará igualmente protegido y funcionará con normalidad.
Enviar Datos de diagnóstico requeridos
Envía únicamente información sobre el dispositivo, la configuración y las funcionalidades y si funciona
Más información
Aceptar

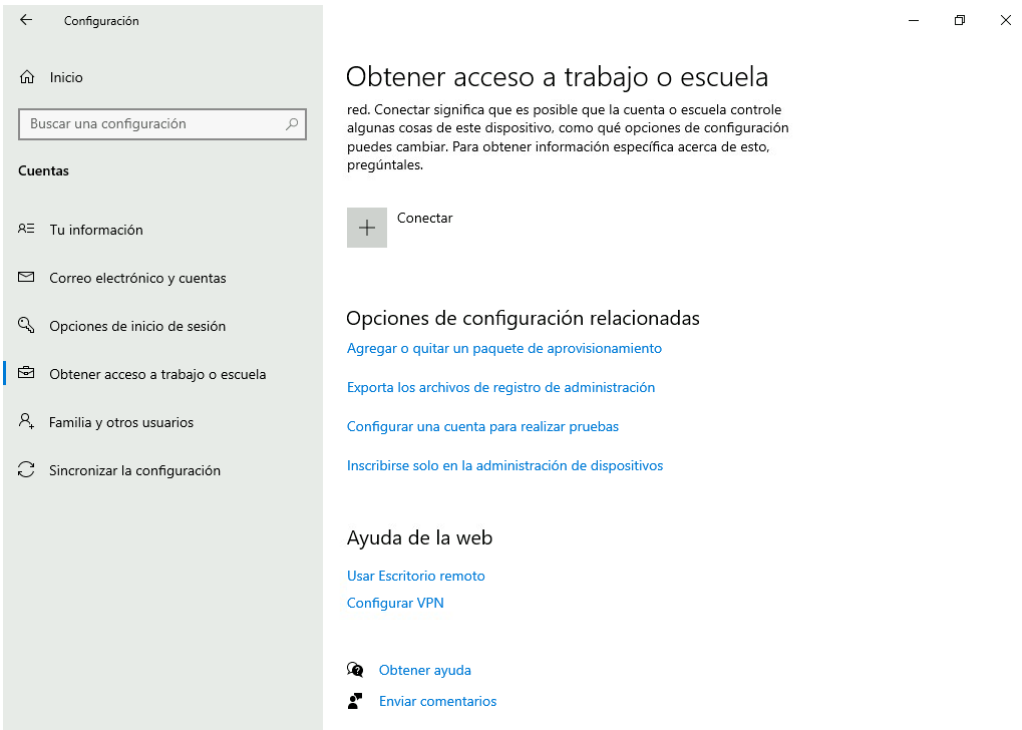

Servicios
Mejorar las entradas manuscritas y la escritura
Elige la configuración y selecciona "Aceptar" para guardarla. Haz clic en el enlace "Más información" para obtener detalles sobre la configuración, cómo cambiarla, cómo funciona SmartScreen de Microsoft Defender, así como las transferencias y usos de datos relacionados.
Sí
Envíe datos opcionales de escritura y entrada manuscrita a Microsoft para mejorar el reconocimiento de lenguaje y las capacidades de sugerencia de las aplicaciones y servicios que se ejecutan en Windows.
No
No quiero usar mis datos para mejorar las funcionalidades del reconocimiento de lenguaje y las capacidades de sugerencia que usan las aplicaciones y servicios que se ejecutan en Windows.
Más información
Aceptar


Servicios
Obtener experiencias personalizadas gracias a los datos de diagnóstico
Elige la configuración y selecciona "Aceptar" para guardarla. Haz clic en el enlace "Más información" para obtener detalles sobre la configuración, cómo cambiarla, cómo funciona SmartScreen de Microsoft Defender, así como las transferencias y usos de datos relacionados.
Sí
Permite que Microsoft use tus datos de diagnóstico, excepto la información sobre los sitios web que exploras, para ofrecerte sugerencias, anuncios y recomendaciones personalizados para mejorar tus experiencias con Microsoft.
No
Las recomendaciones, anuncios y sugerencias que veas serán más genéricos y menos relevantes.
Más información
Aceptar

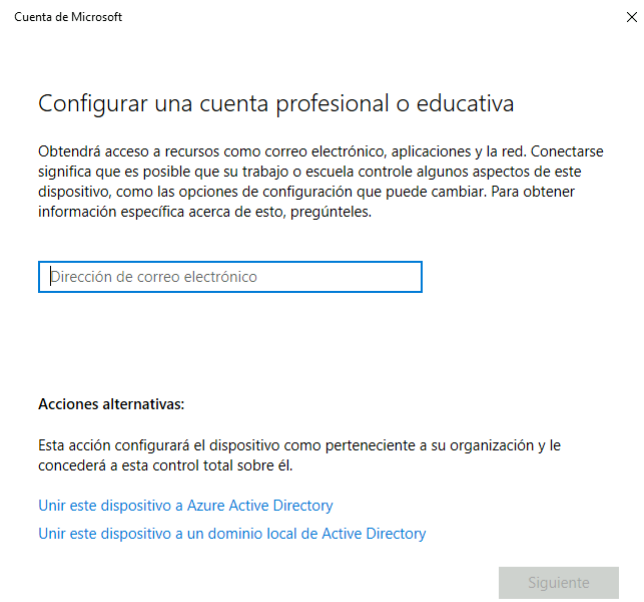

Servicios
Permitir que las aplicaciones usen el id. de publicidad
Elige la configuración y selecciona "Aceptar" para guardarla. Haz clic en el enlace "Más información" para obtener detalles sobre la configuración, cómo cambiarla, cómo funciona SmartScreen de Microsoft Defender, así como las transferencias y usos de datos relacionados.
Sí
Las aplicaciones pueden usar el id. de publicidad para proporcionar anuncios más personalizados de acuerdo con la directiva de privacidad del proveedor de la aplicación.
No
El número de anuncios que veas no cambiará, pero pueden ser menos relevantes.
Más información
Aceptar


Servicios
Personalicemos su experiencia
Seleccione todas las formas en que planea usar el dispositivo para obtener sugerencias, anuncios y recomendaciones personalizados durante la configuración del dispositivo y su experiencia de bienvenida.
Entretenimiento
Ver vídeos, explorar la web, conectarse en las redes sociales
Creatividad
De vida a sus ideas con fotos y vídeos
Juegos
Juega y descubre juegos, mantente al día con los nuevos lanzamientos
Empresa
Controlar los gastos, administrar negocio, chatear con los clientes
Escuela
Tome nota, escriba redacciones, colabore en proyectos
Familia
Conectar con los miembros de la familia, editar la configuración de seguridad, dar a cada uno su propio perfil en este dispositivo
Más información
Omitir
Aceptar

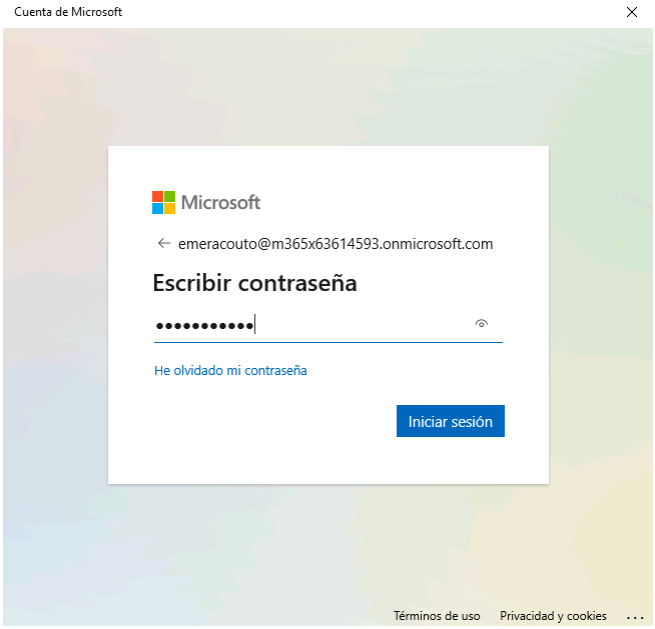
Una vez finalizada la configuración del sistema operativo mediante el OOBE, se debe unir el dispositivo a Azure Active Directory mediante la opción “Obtener acceso al trabajo o la escuela” del menú Cuentas de la configuración del sistema.

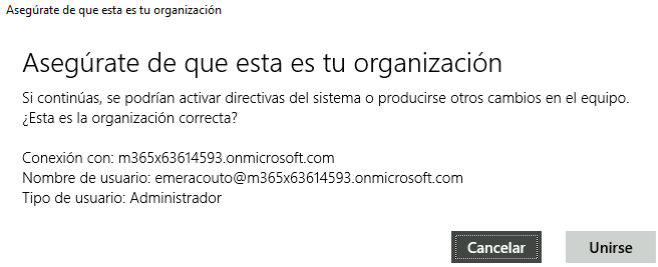


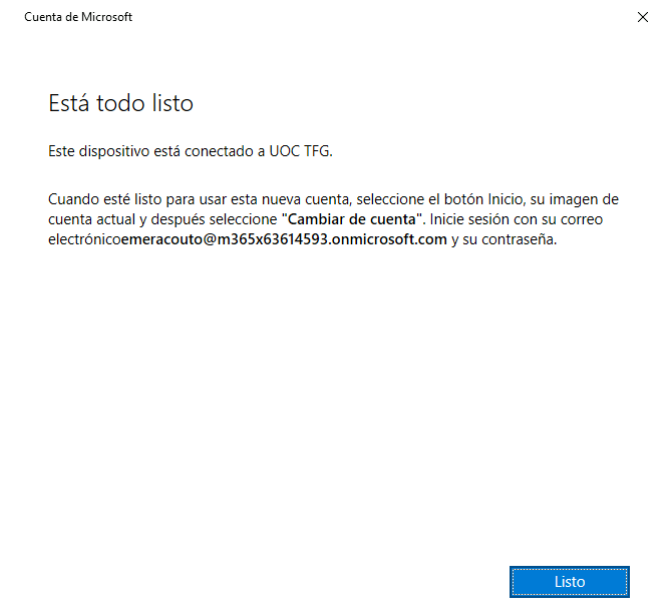
En la configuración de cuenta profesional o educativa, se debe seleccionar la opción inferior: “Unir este dispositivo a Azure Active Directory”.

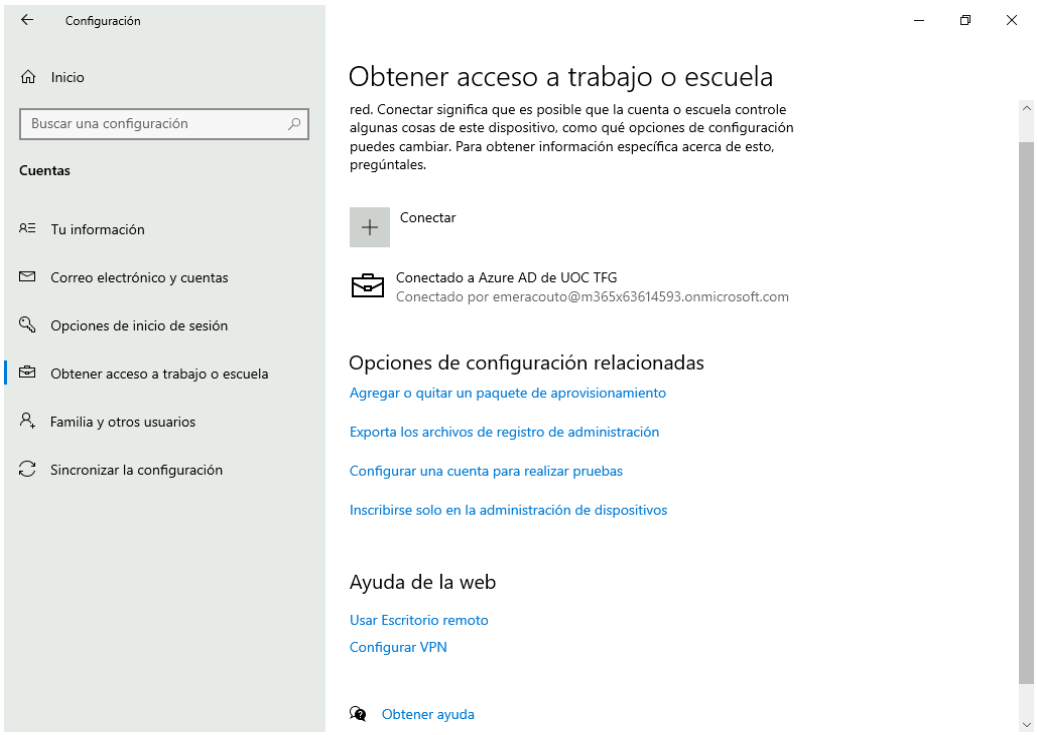


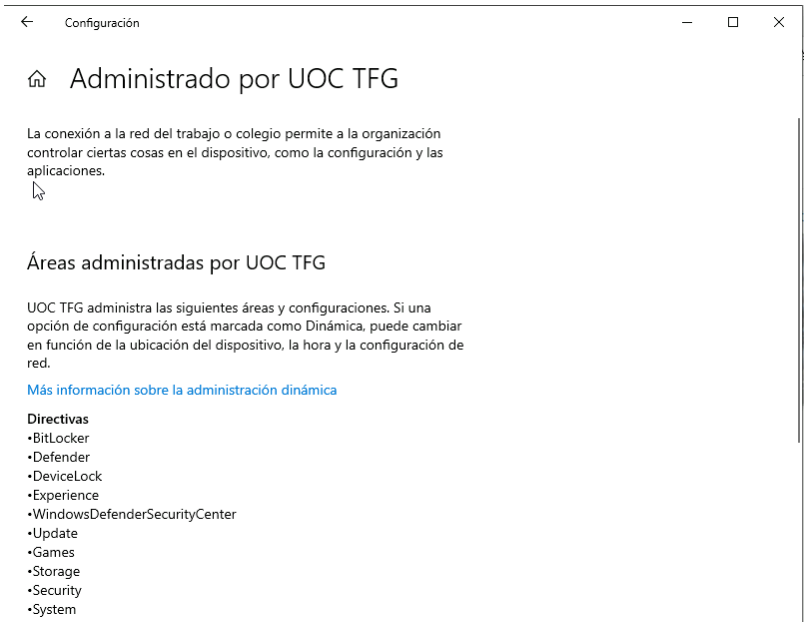
Tras introducir las credenciales corporativas, el dispositivo se une a Azure AD correctamente y, por tanto, también se inscribe en Intune.



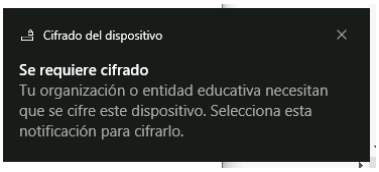

Asegúrate de que esta es tu organización
Asegúrate de que esta es tu organización
Si continúas, se podrían activar directivas del sistema o producirse otros cambios en el equipo.
¿Esta es la organización correcta?
Conexión con: m365x63614593.onmicrosoft.com
Nombre de usuario: emeracouto@m365x63614593.onmicrosoft.com
Tipo de usuario: Administrador
Cancelar
Unirse

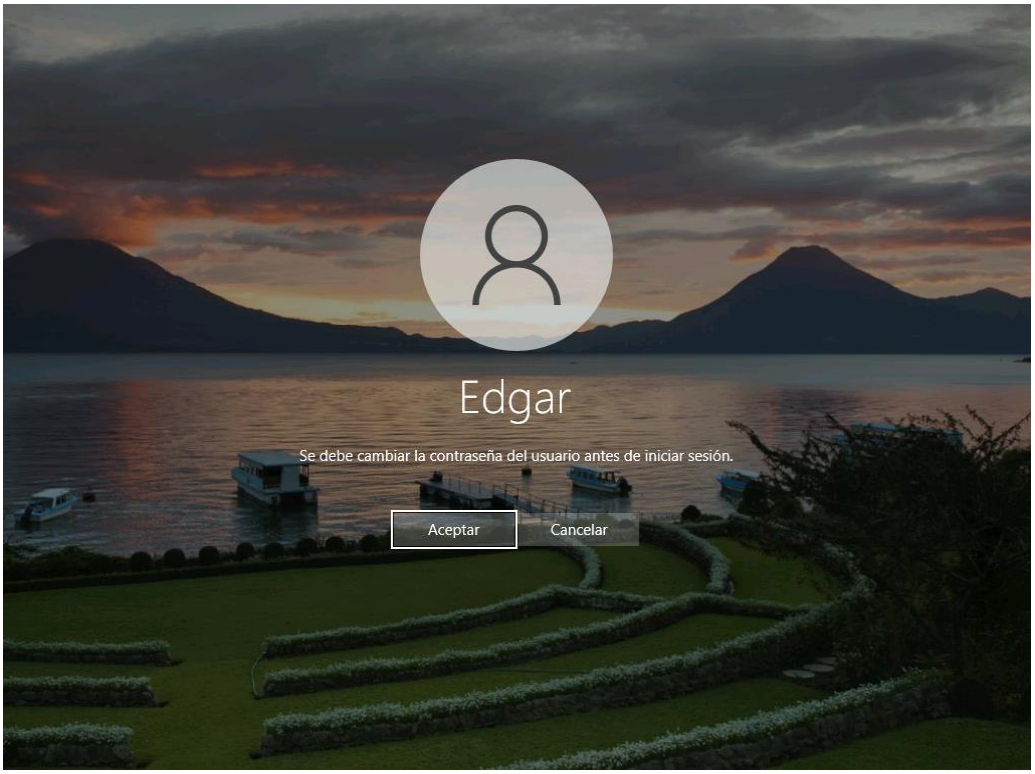

Cuenta de Microsoft
Está todo listo
Este dispositivo está conectado a UOC TFG.
Cuando esté listo para usar esta nueva cuenta, seleccione el botón Inicio, su imagen de cuenta actual y después seleccione "Cambiar de cuenta". Inicie sesión con su correo electrónicoemeracouto@m365x63614593.onmicrosoft.com y su contraseña.
Listo


Configuración
Inicio
Buscar una configuración
Cuentas
Tu información
Correo electrónico y cuentas
Opciones de inicio de sesión
Obtener acceso a trabajo o escuela
Familia y otros usuarios
Sincronizar la configuración
Obtener acceso a trabajo o escuela
red. Conectar significa que es posible que la cuenta o escuela controle algunas cosas de este dispositivo, como qué opciones de configuración puedes cambiar. Para obtener información específica acerca de esto, pregúntales.
Conectar
Conectado a Azure AD de UOC TFG
Conectado por emeracouto@m365x63614593.onmicrosoft.com
Opciones de configuración relacionadas
Agregar o quitar un paquete de aprovisionamiento
Exporta los archivos de registro de administración
Configurar una cuenta para realizar pruebas
Inscribirse solo en la administración de dispositivos
Ayuda de la web
Usar Escritorio remoto
Configurar VPN
Obtener ayuda



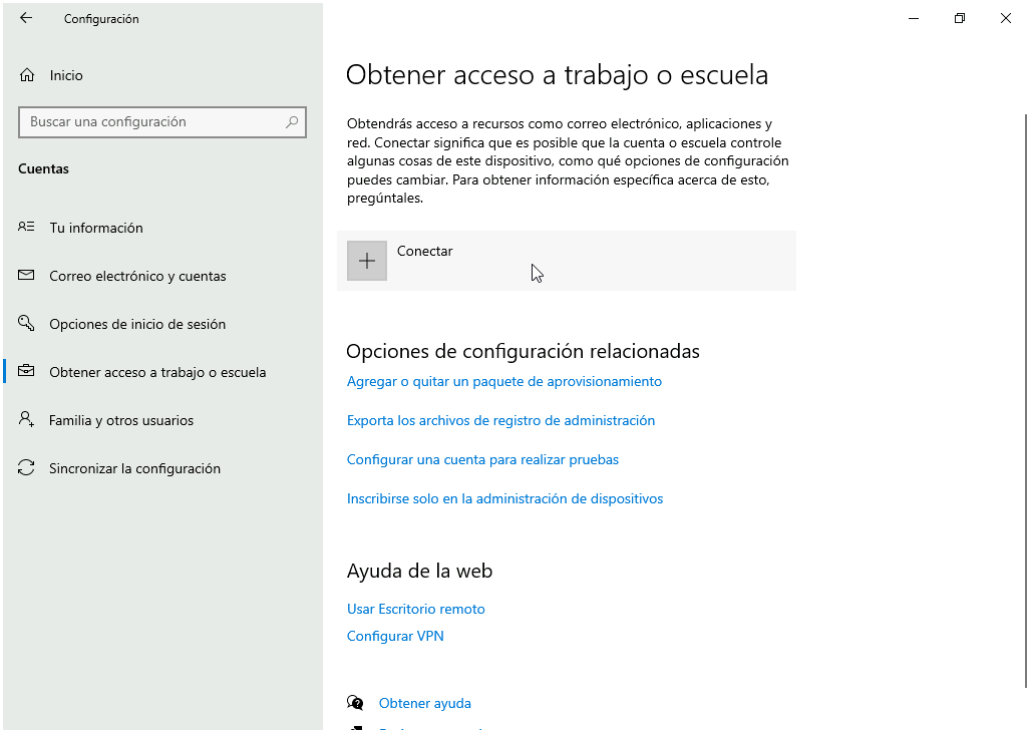
Como se aprecia en las siguientes capturas, las directivas de la organización se aplican mediante Intune y es necesario cifrar el dispositivo y cambiar la contraseña del usuario, al no cumplir con los requisitos de complejidad.



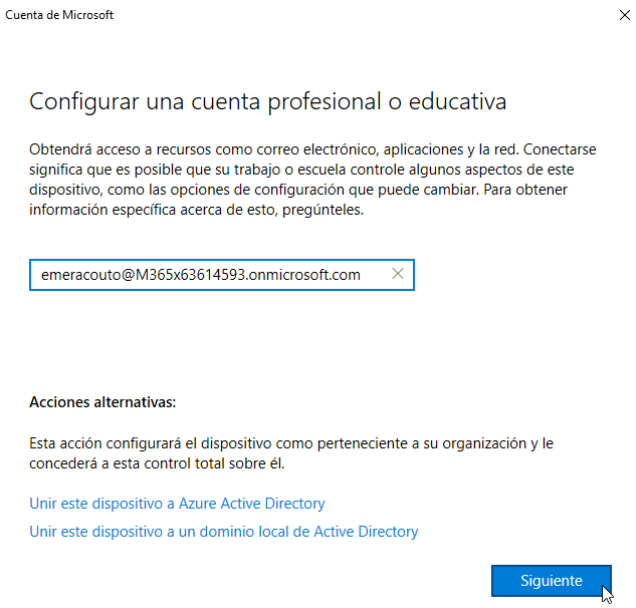


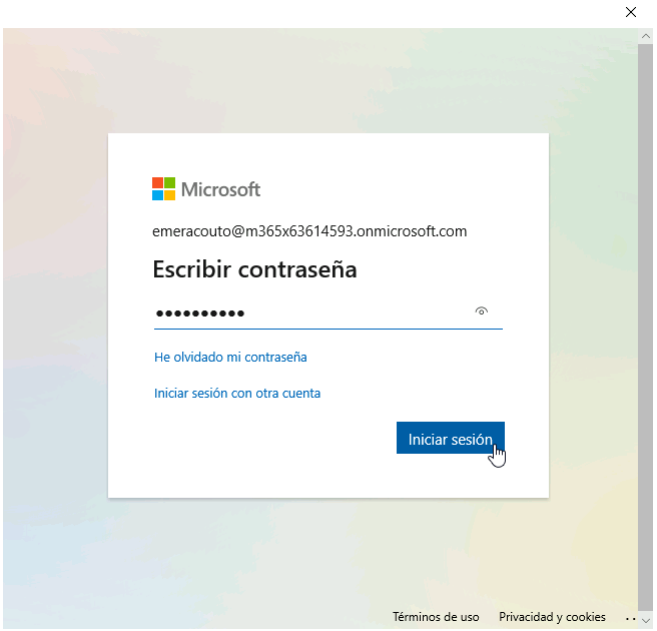
- Dispositivos Windows BYOD

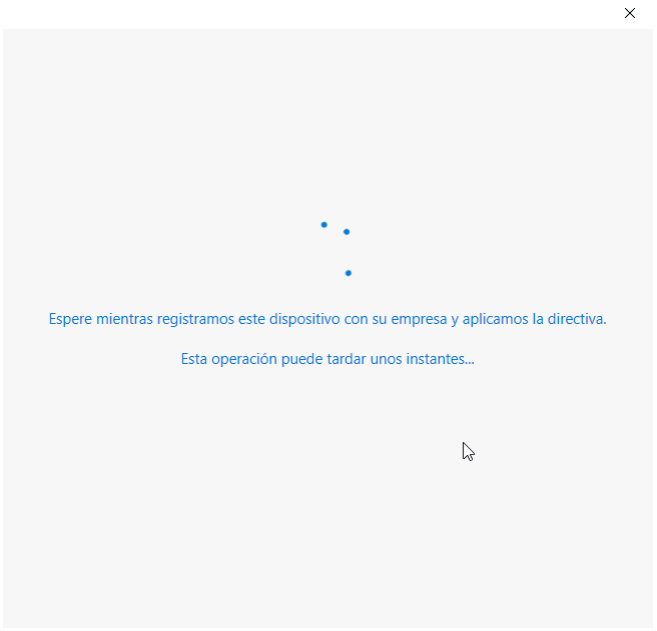
El usuario introduce sus credenciales corporativas en el menú “Obtener acceso a trabajo o escuela” del apartado Cuentas de la configuración del sistema.

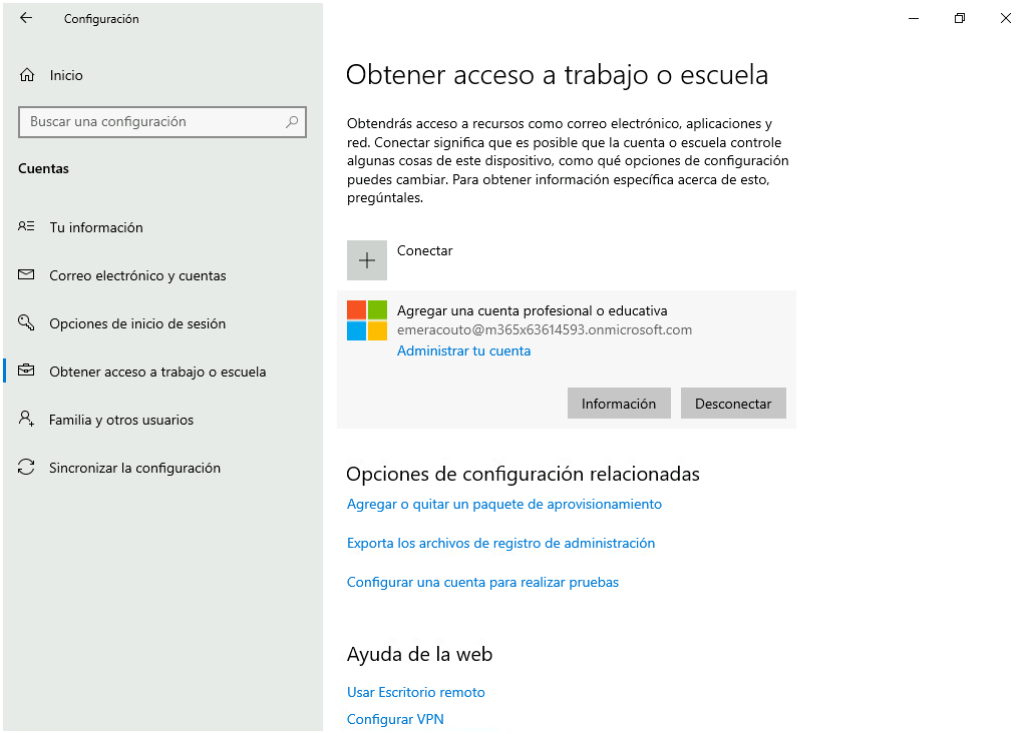


A diferencia de en los dispositivos corporativos, no se une el equipo al dominio de Azure AD, solo se registra y se inscribe en Microsoft Intune.

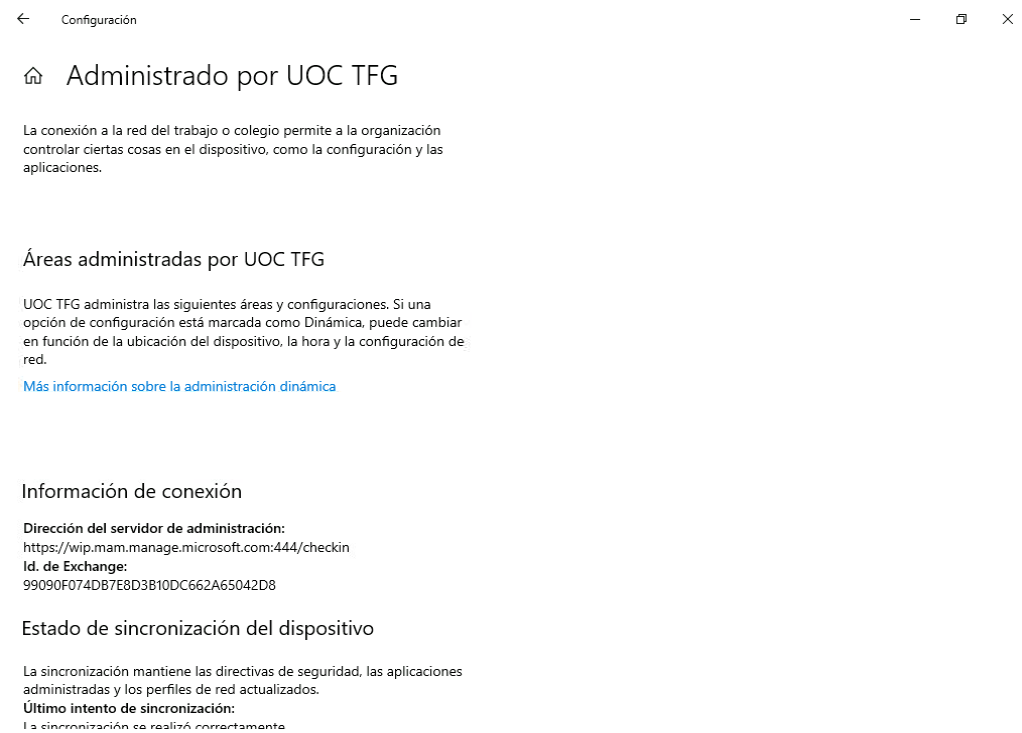



Microsoft
emeracouto@m365x63614593.onmicrosoft.com
Escribir contraseña
He olvidado mi contraseña
Iniciar sesión con otra cuenta
Iniciar sesión
Términos de uso
Privacidad y cookies


Espere mientras registramos este dispositivo con su empresa y aplicamos la directiva.
Esta operación puede tardar unos instantes...

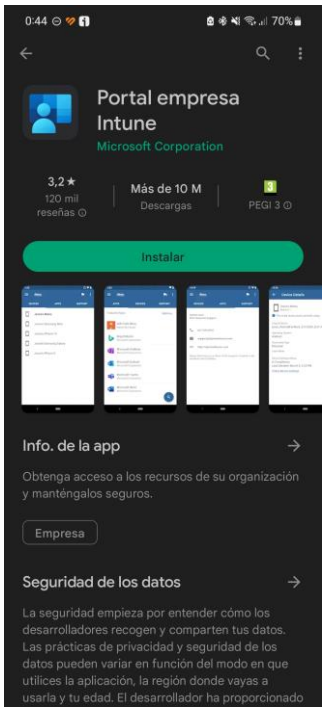


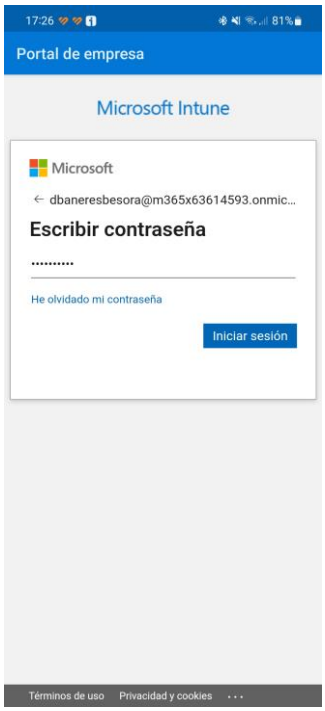
Tal y como se aprecia en la siguiente imagen, se administran ciertas áreas y configuraciones, no el dispositivo en sí.



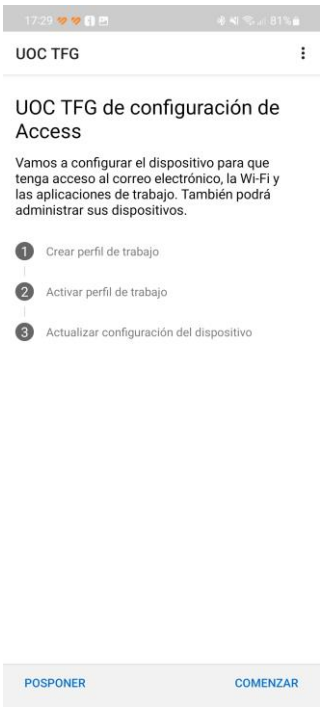
- **Dispositivos Android BYOD**

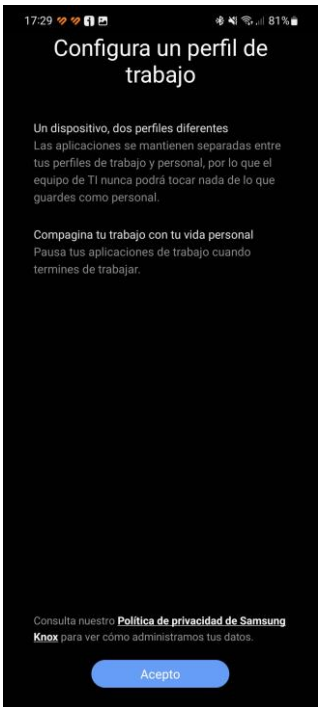
El usuario se descarga la aplicación “Portal empresa Intune” desde Google Play Store e introduce sus credenciales corporativas.

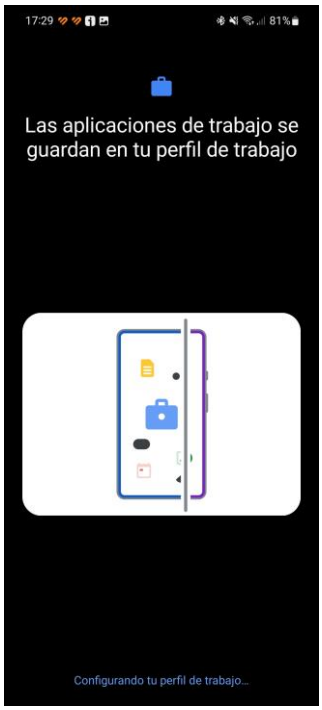


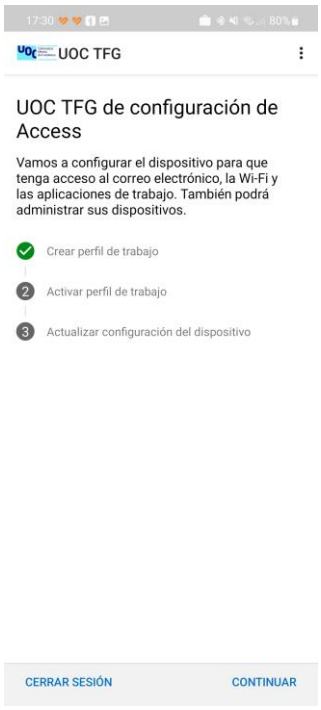


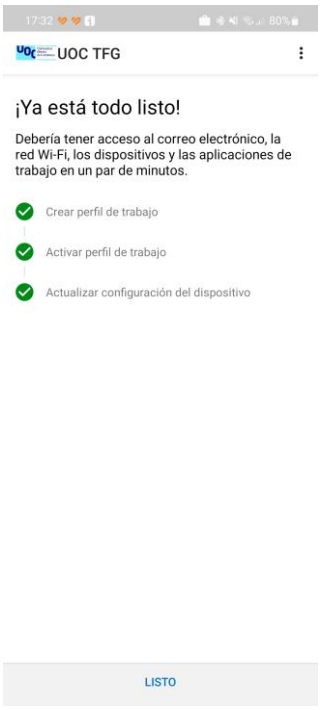
A continuación, revisa los privilegios que la organización tendrá sobre el dispositivo y permite la creación del perfil de trabajo en este.



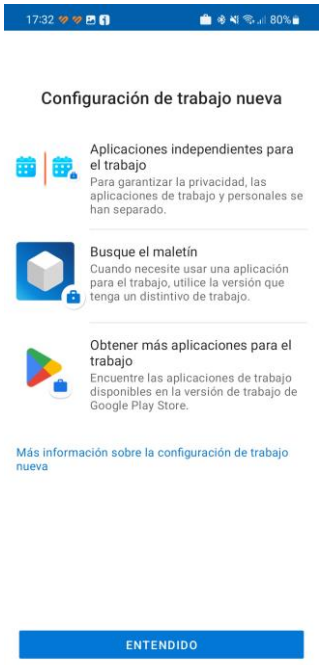


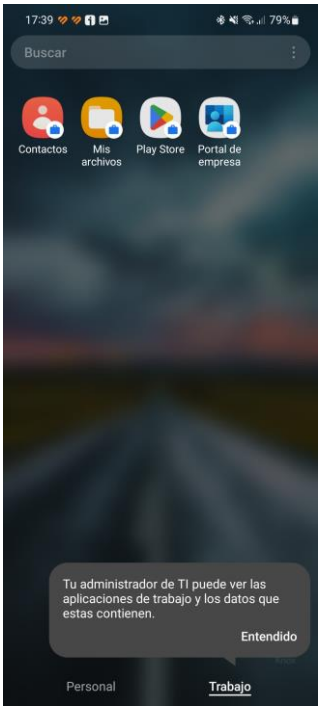




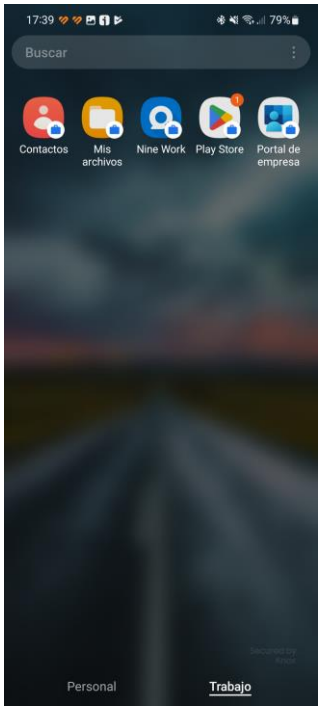


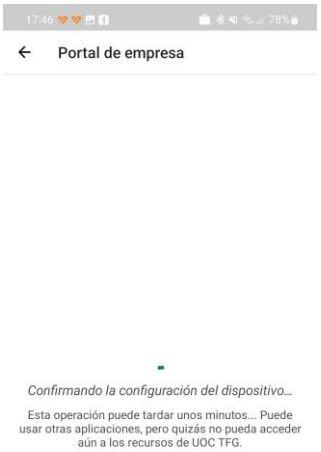
Una vez creado el perfil de trabajo, el dispositivo Android cuenta con dos espacios diferenciados, el Personal y el de Trabajo. En el primero se mantienen las aplicaciones que el usuario ya tenía instaladas, y en el de trabajo se instalarán las de la organización. Así, el dispositivo contará con dos Google Play Store, la personal con la cuenta del usuario, y la corporativa con la de la organización.

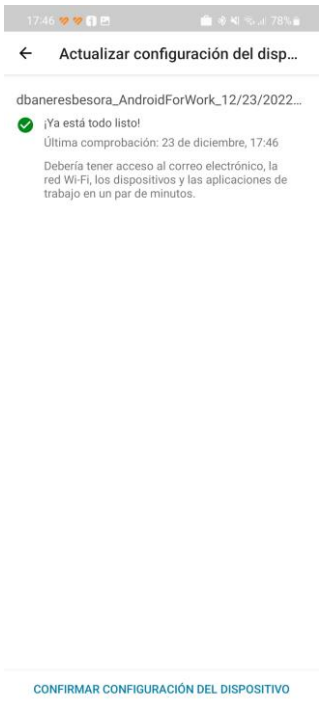


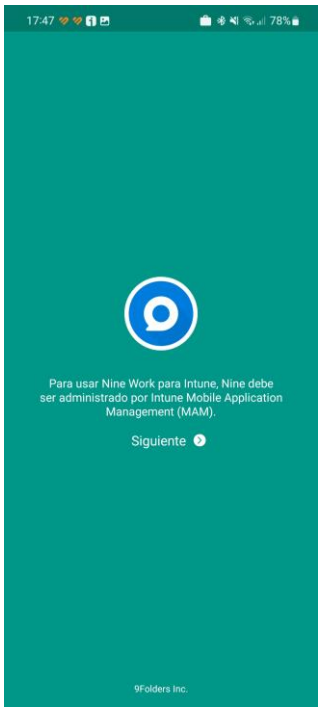


Por último, se instalan las aplicaciones corporativas en el perfil de trabajo (Nine Work, desplegada expresamente) y se aplican las configuraciones asignadas.





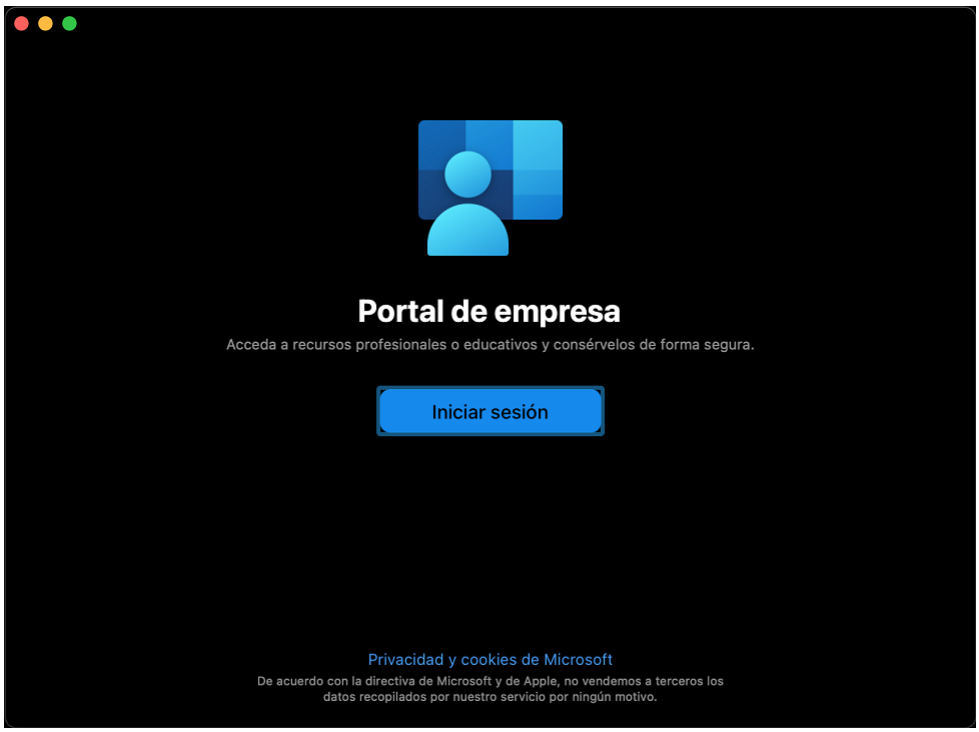


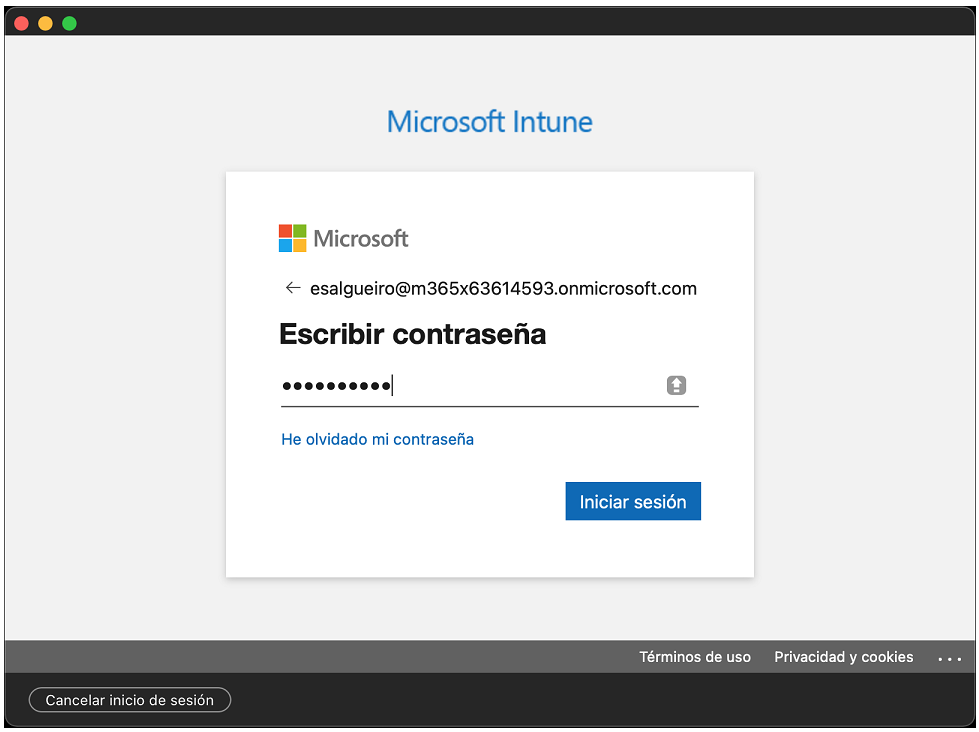


Tal y como muestra la última imagen, la aplicación Nine Work está preconfigurada con la cuenta de correo del usuario debido al perfil de configuración aplicado a los dispositivos Android Enterprise BYOD.

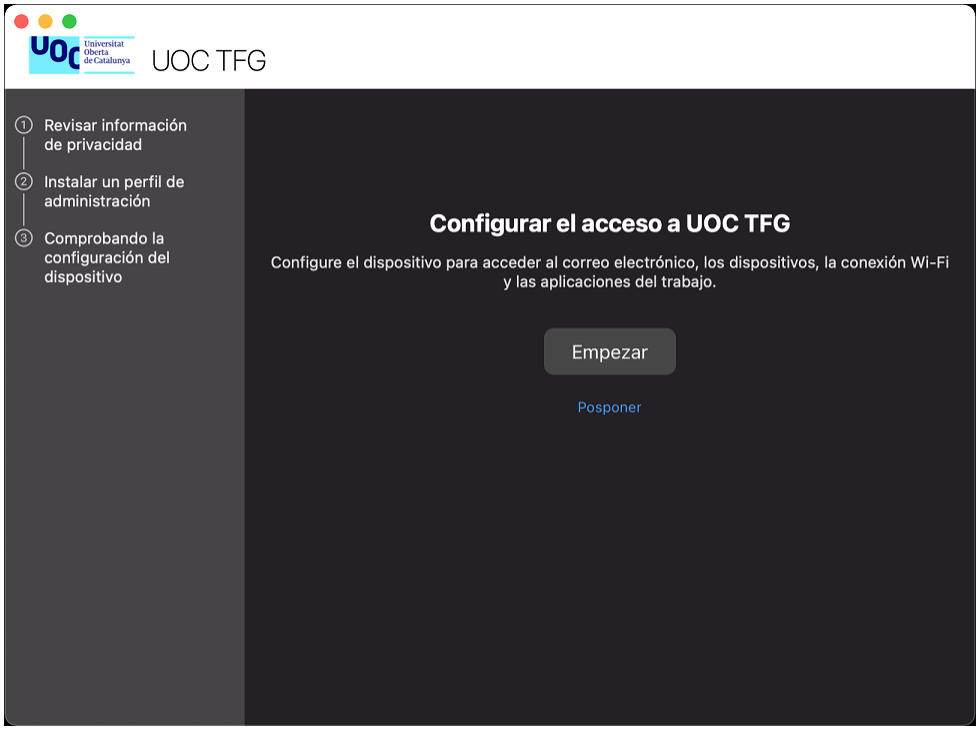
- **Dispositivos macOS**

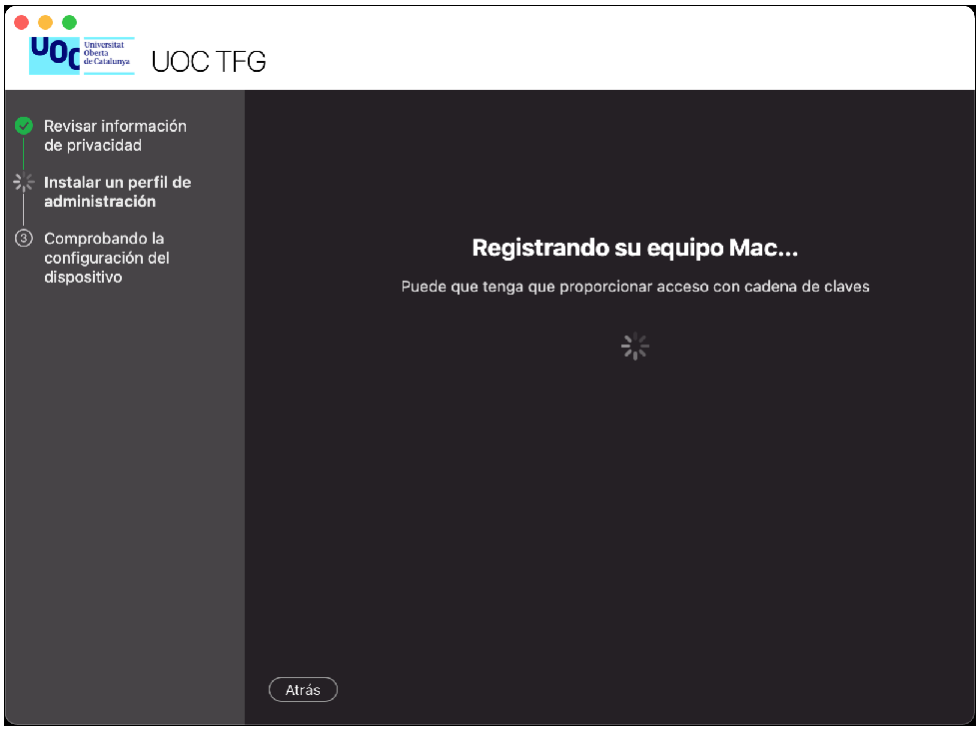
El usuario descarga la aplicación Portal de empresa desde la dirección https://go.microsoft.com/fwlink/?linkid=853070 y la instala. Después, la ejecuta y se valida con sus credenciales corporativas.



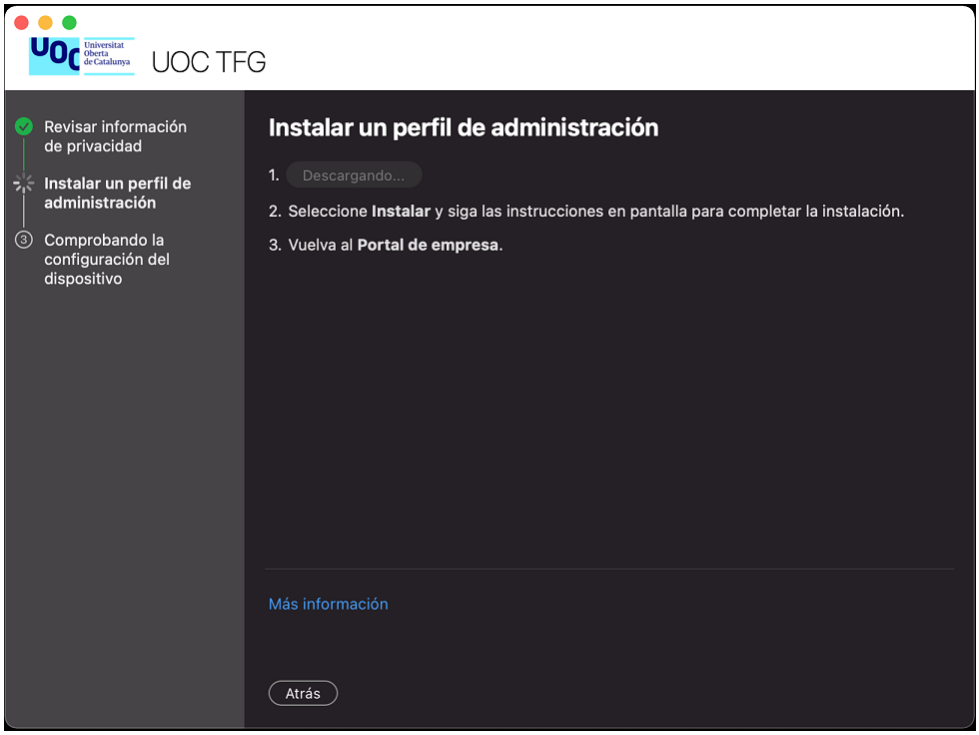


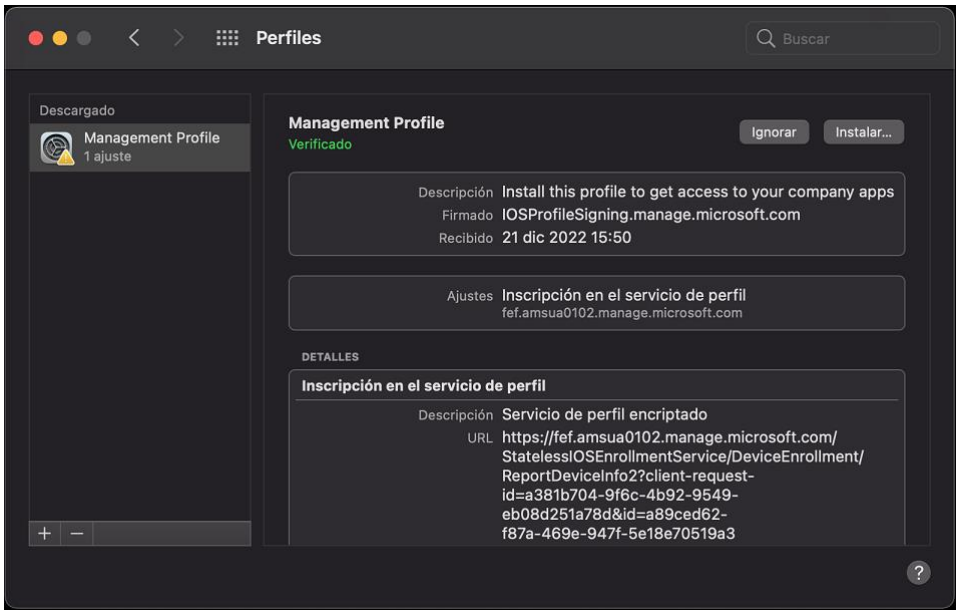
A continuación, configura la inscripción del dispositivo en Intune, revisando los permisos que tendrá la organización sobre él.

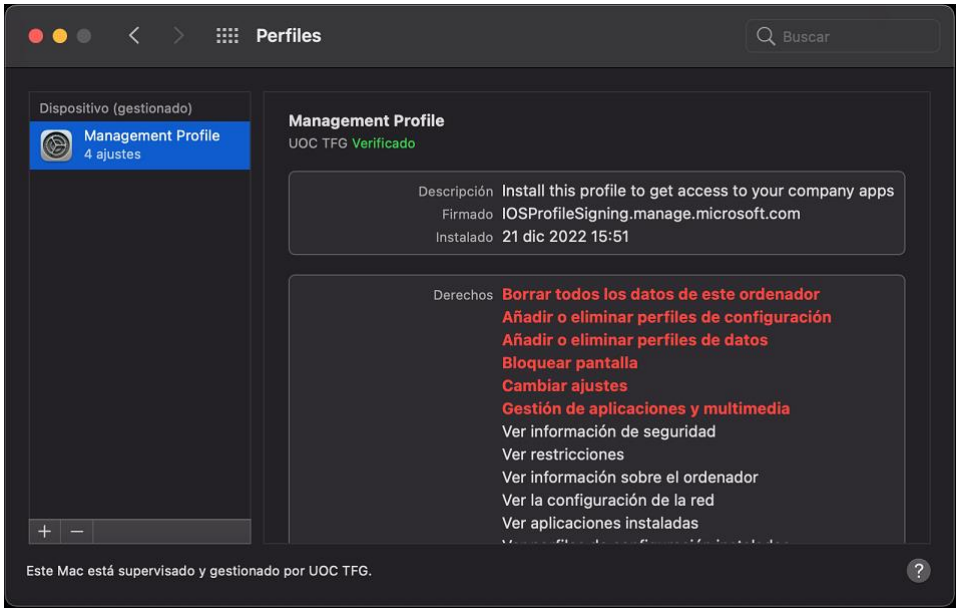


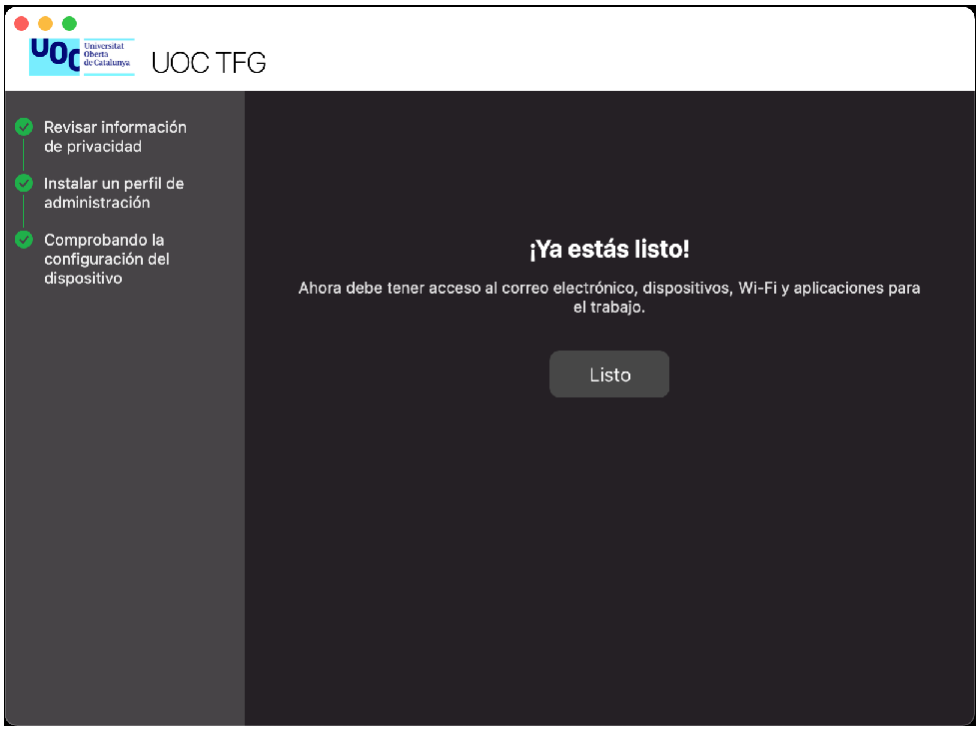


Una vez registrado el dispositivo en Intune, se debe instalar el perfil de administración en el equipo.

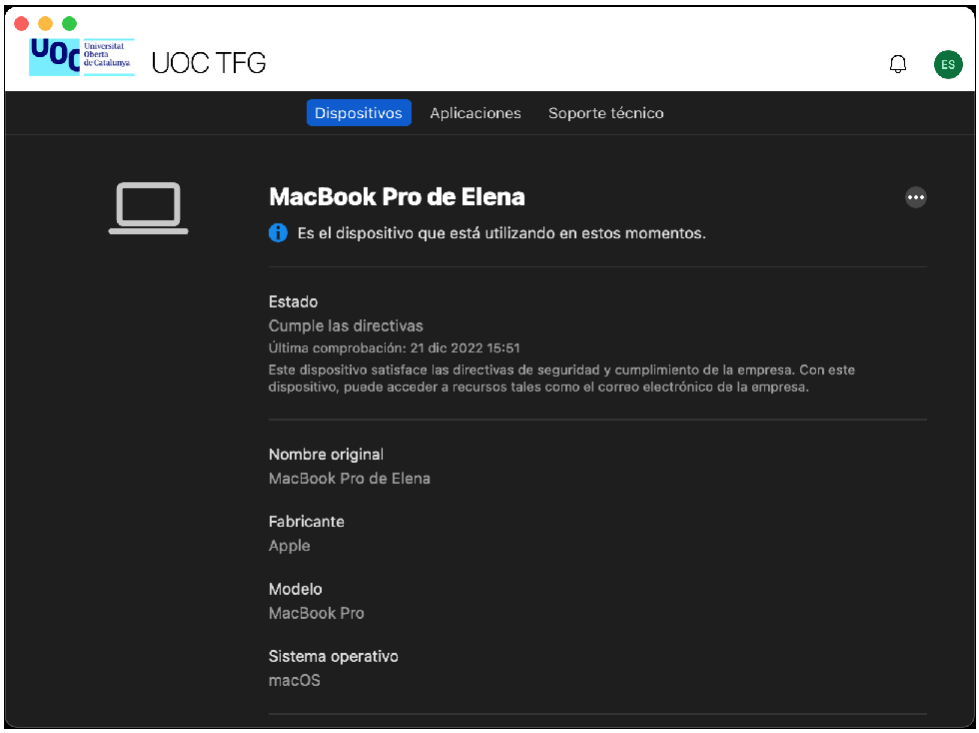



Perfiles
Buscar
Descargado
Management Profile
1 ajuste
Management Profile
Verificado
Ignorar
Instalar...
Descripción Install this profile to get access to your company apps
Firmado IOSProfileSigning.manage.microsoft.com
Recibido 21 dic 2022 15:50
Ajustes Inscripción en el servicio de perfil
fef.amsua0102.manage.microsoft.com
DETALLES
Inscripción en el servicio de perfil
Descripción Servicio de perfil encriptado
URL https://fef.amsua0102.manage.microsoft.com/StatelessIOSEnrollmentService/DeviceEnrollment/ReportDeviceInfo2?client-request-id=a381b704-9f6c-4b92-9549-eb08d251a78d&id=a89ced62-f87a-469e-947f-5e18e70519a3


Perfiles
Buscar
Dispositivo (gestionado)
Management Profile
4 ajustes
Management Profile
UOC TFG Verificado
Descripción Install this profile to get access to your company apps
Firmado IOSProfileSigning.manage.microsoft.com
Instalado 21 dic 2022 15:51
Derechos Borrar todos los datos de este ordenador
Añadir o eliminar perfiles de configuración
Añadir o eliminar perfiles de datos
Bloquear pantalla
Cambiar ajustes
Gestión de aplicaciones y multimedia
Ver información de seguridad
Ver restricciones
Ver información sobre el ordenador
Ver la configuración de la red
Ver aplicaciones instaladas
Este Mac está supervisado y gestionado por UOC TFG.

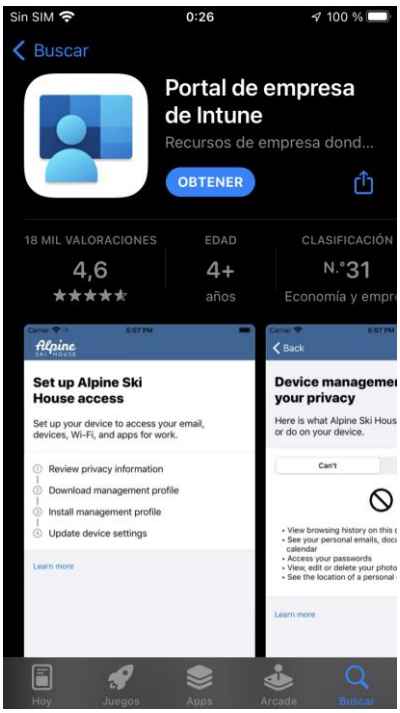


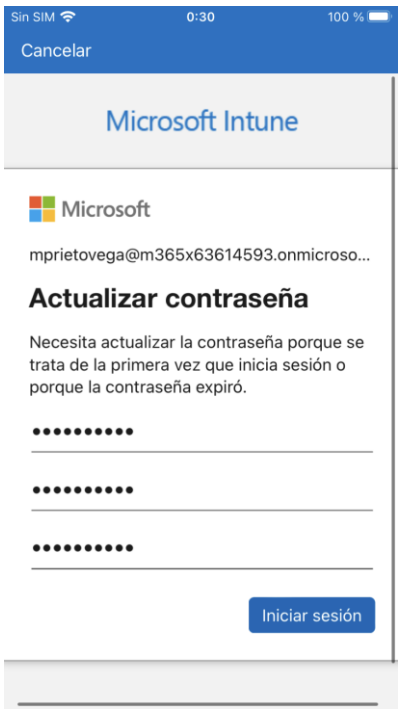
Por último, la aplicación muestra si el dispositivo es conforme o no con las directivas de cumplimiento de la compañía y, por tanto, puede acceder a los recursos corporativos.



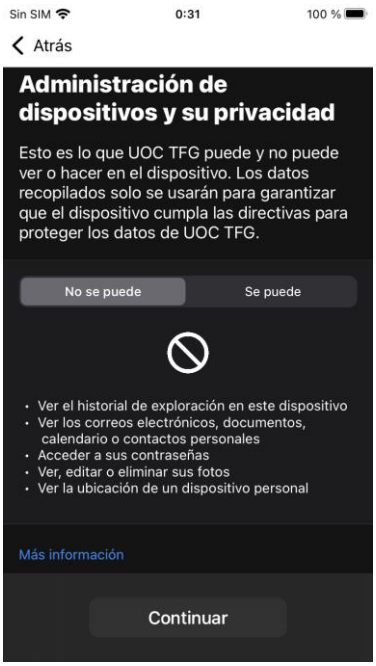
- **Dispositivos iOS e iPadOS**

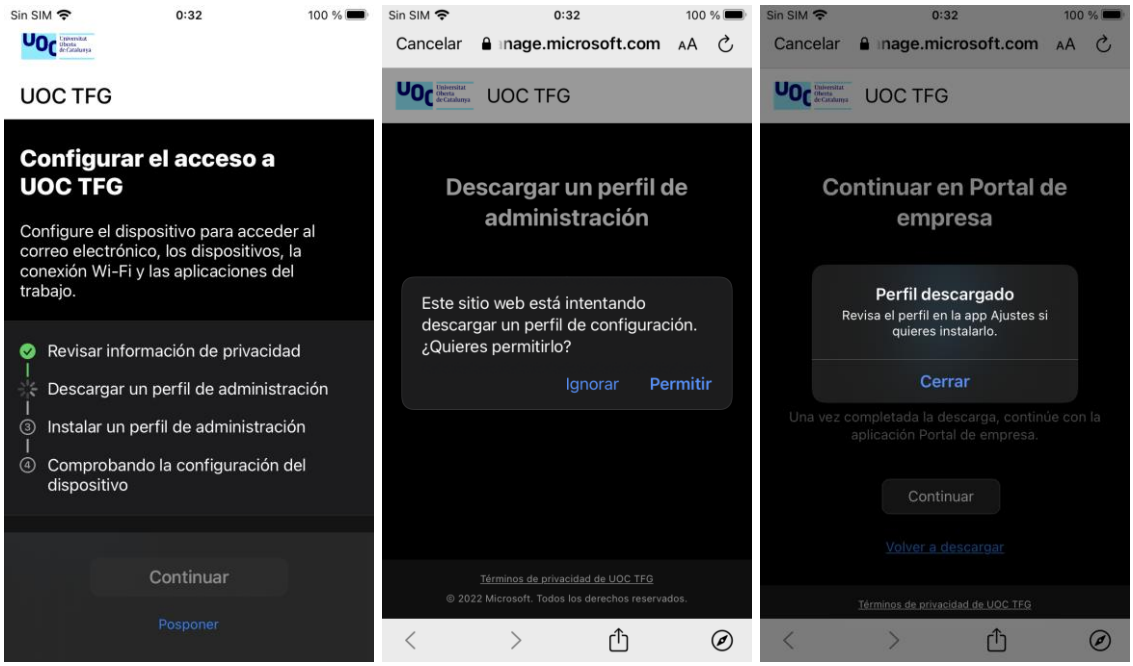
De igual forma que en los dispositivos Apple con sistema operativo macOS, el usuario debe descargar la aplicación Portal de empresa de Intune para inscribir el dispositivo. En este caso, la aplicación está disponible en la Apple App Store.



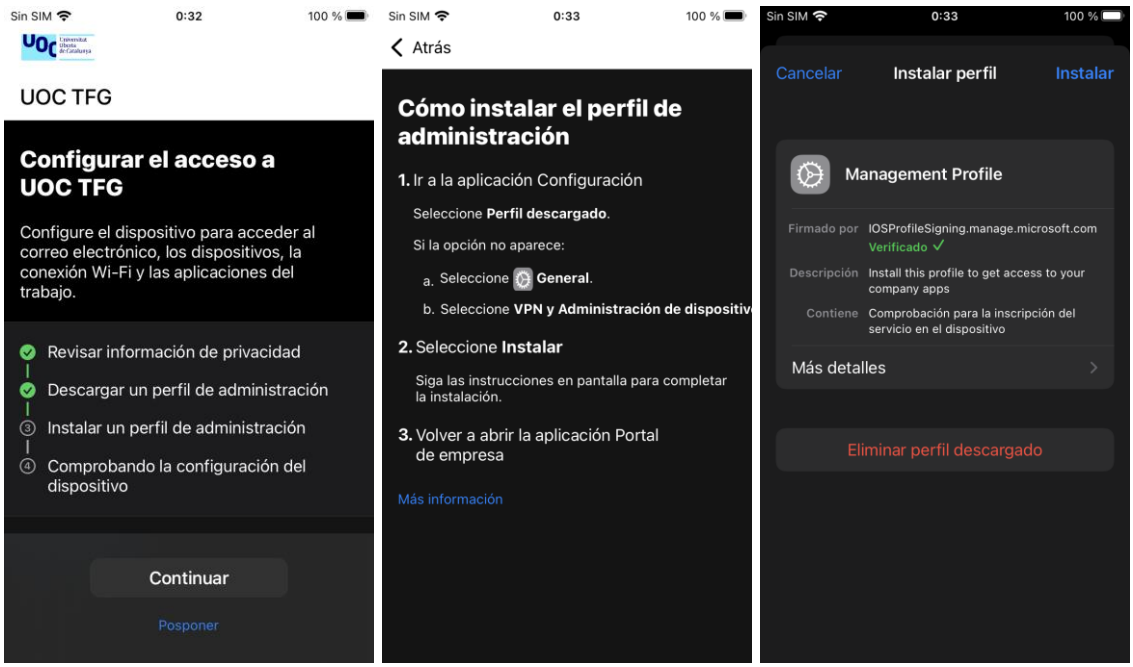


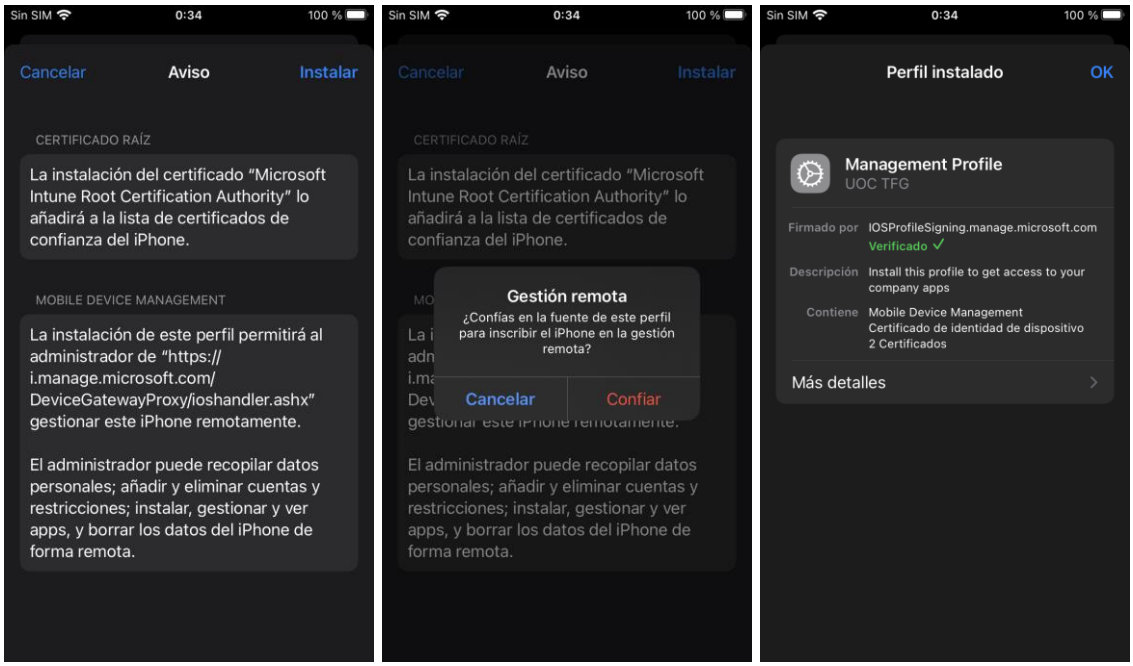
Tras validarse con las credenciales corporativas, se debe revisar la información de privacidad y descargar un perfil de administración.



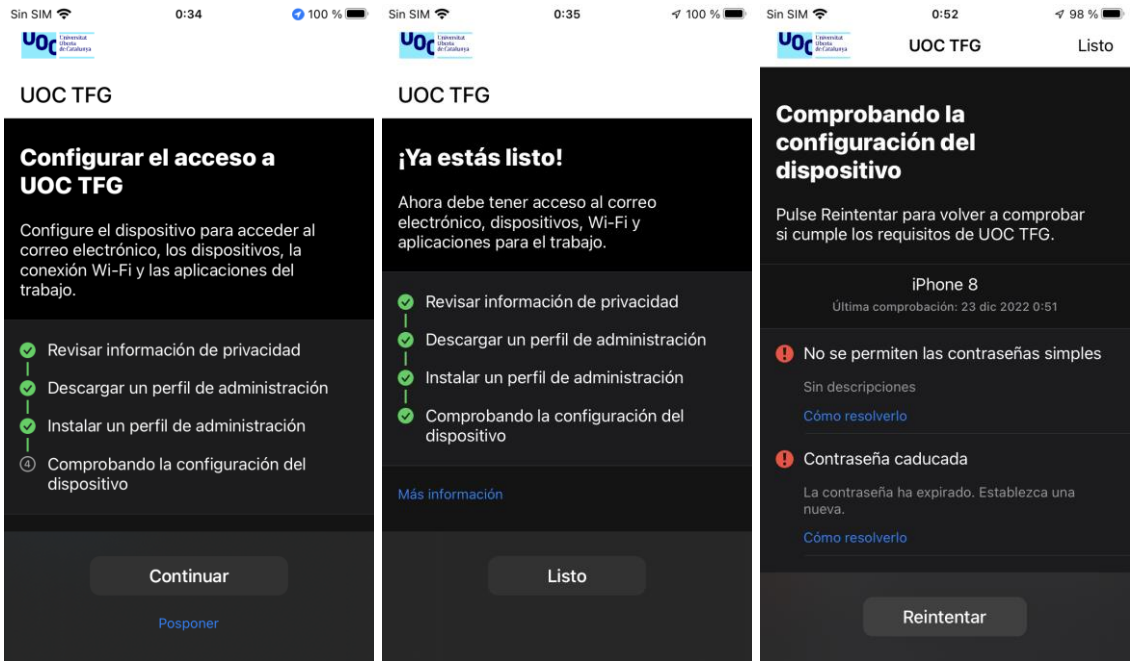


Después, se debe instalar el perfil de administración.

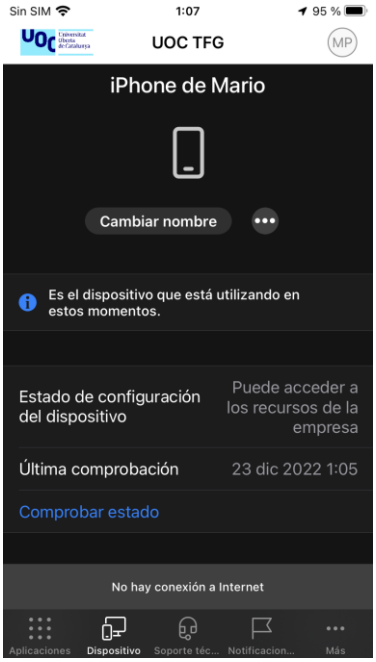




A continuación, la aplicación comprueba la configuración del dispositivo.



Por último, es necesario solventar las configuraciones que no cumplen con las directivas de cumplimento de la organización para que el dispositivo pueda tener acceso a los recursos corporativos. Una vez corregidas, se debe ejecutar de nuevo la comprobación de la configuración del dispositivo, bien manualmente o esperando a que la aplicación lo haga de forma automática según su programación.



- **Dispositivos Linux**

Para instalar la aplicación Microsoft Intune se debe ejecutar un terminal e instalar Curl mediante el comando “sudo apt install curl gpg”.

A continuación, se introducen los siguientes comandos en el orden indicado:

curl https://packages.microsoft.com/keys/microsoft.asc | gpg --dearmor > microsoft.gpg

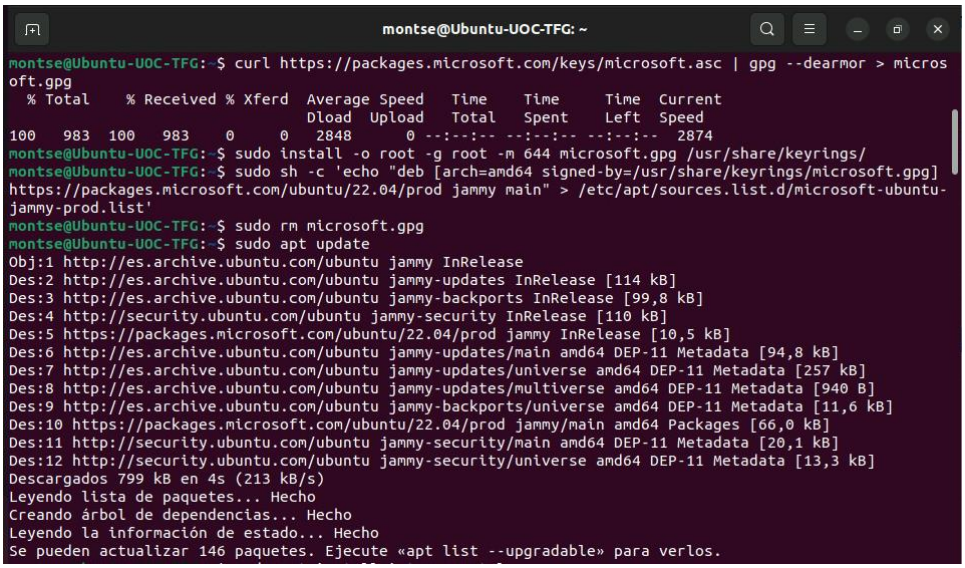
sudo install -o root -g root -m 644 microsoft.gpg /usr/share/keyrings/

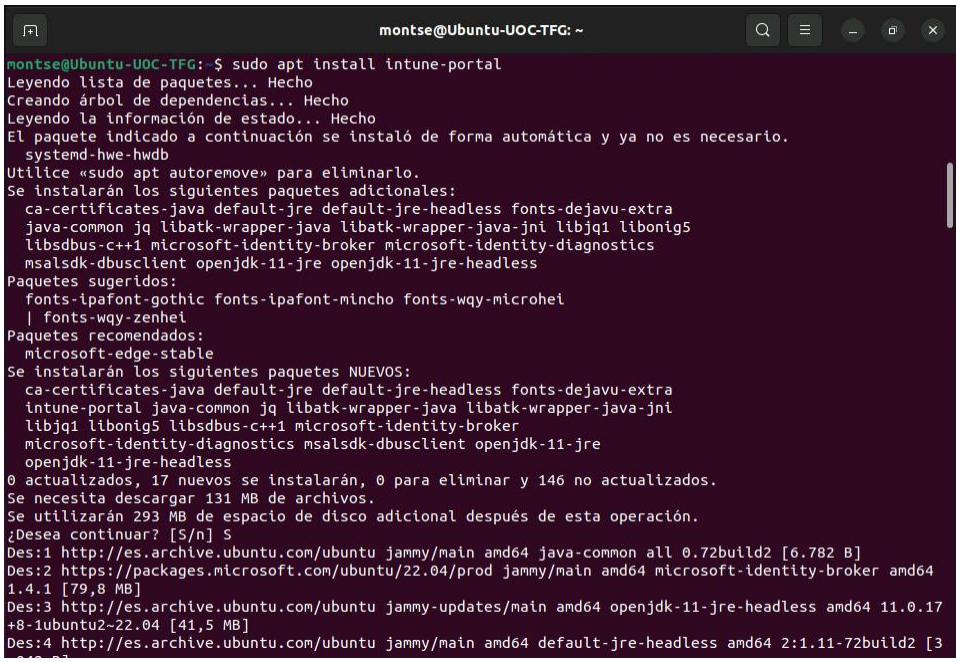
sudo sh -c 'echo "deb [arch=amd64 signed-by=/usr/share/keyrings/microsoft.gpg] https://packages.microsoft.com/ubuntu/22.04/prod jammy main" > /etc/apt/sources.list.d/microsoft-ubuntu-jammy-prod.list'

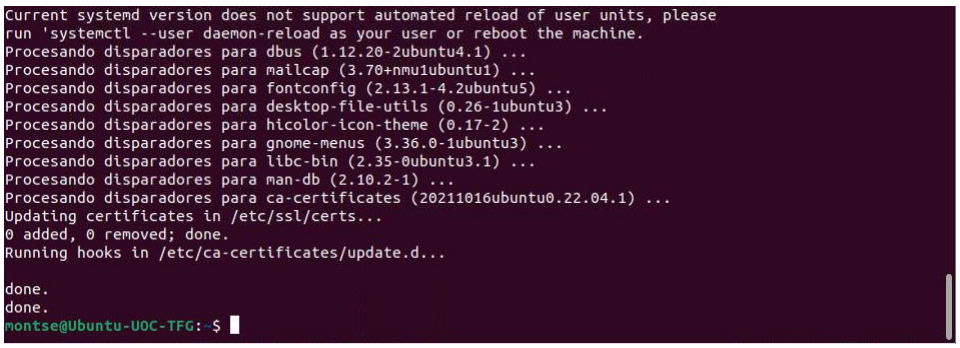
sudo rm microsoft.gpg

sudo apt update

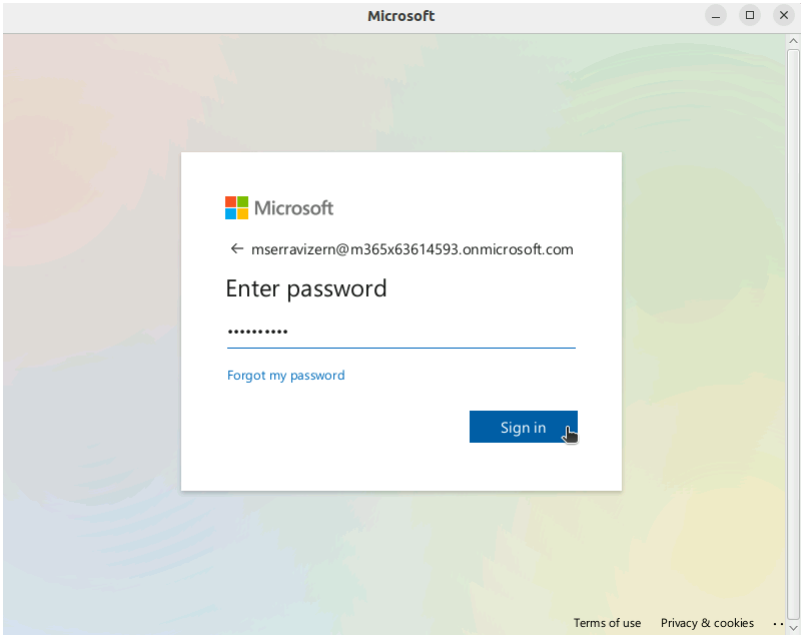
sudo apt install intune-portal

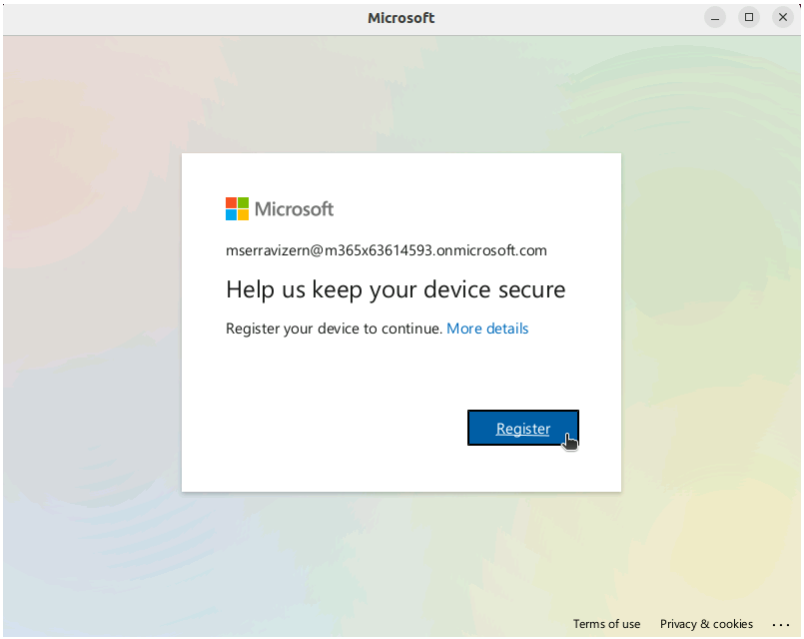




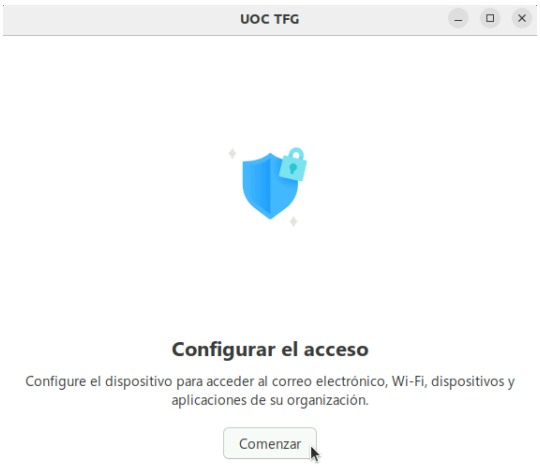


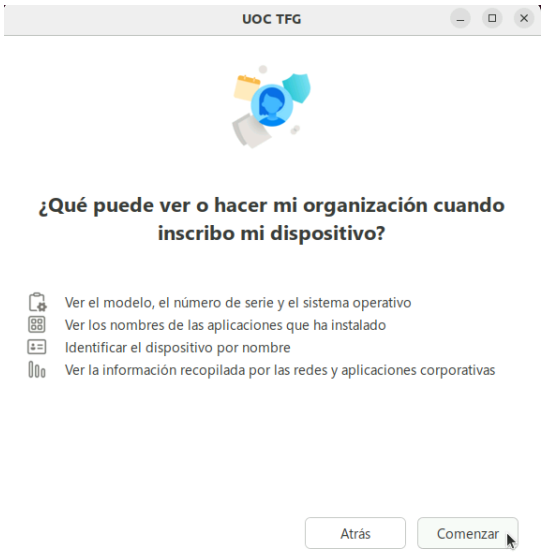
Una vez terminada la instalación, es necesario reiniciar el equipo. Tras el reinicio, se ejecuta la aplicación Microsoft Intune y se introducen las credenciales corporativas.



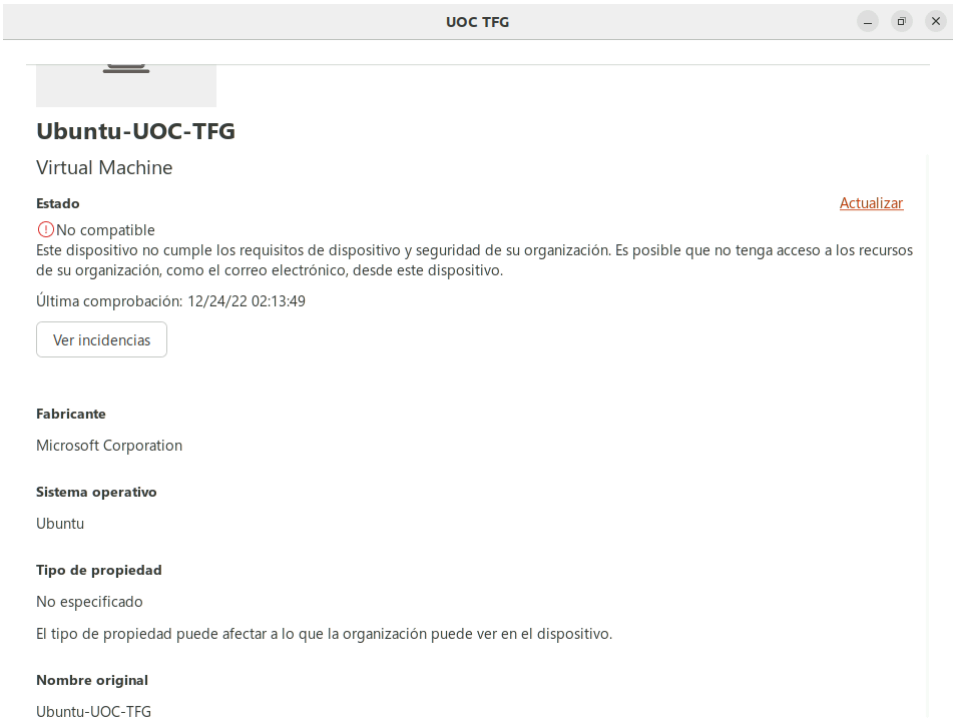


A continuación, se revisa la información que puede ver la empresa del dispositivo una vez inscrito en Microsoft Intune y se realiza la inscripción.





Tras aceptar la inscripción, el dispositivo se inscribe en Intune y se puede consultar su estado de cumplimiento en la aplicación instalada, comprobando si cumple con las directivas de la organización para acceder a los recursos corporativos.



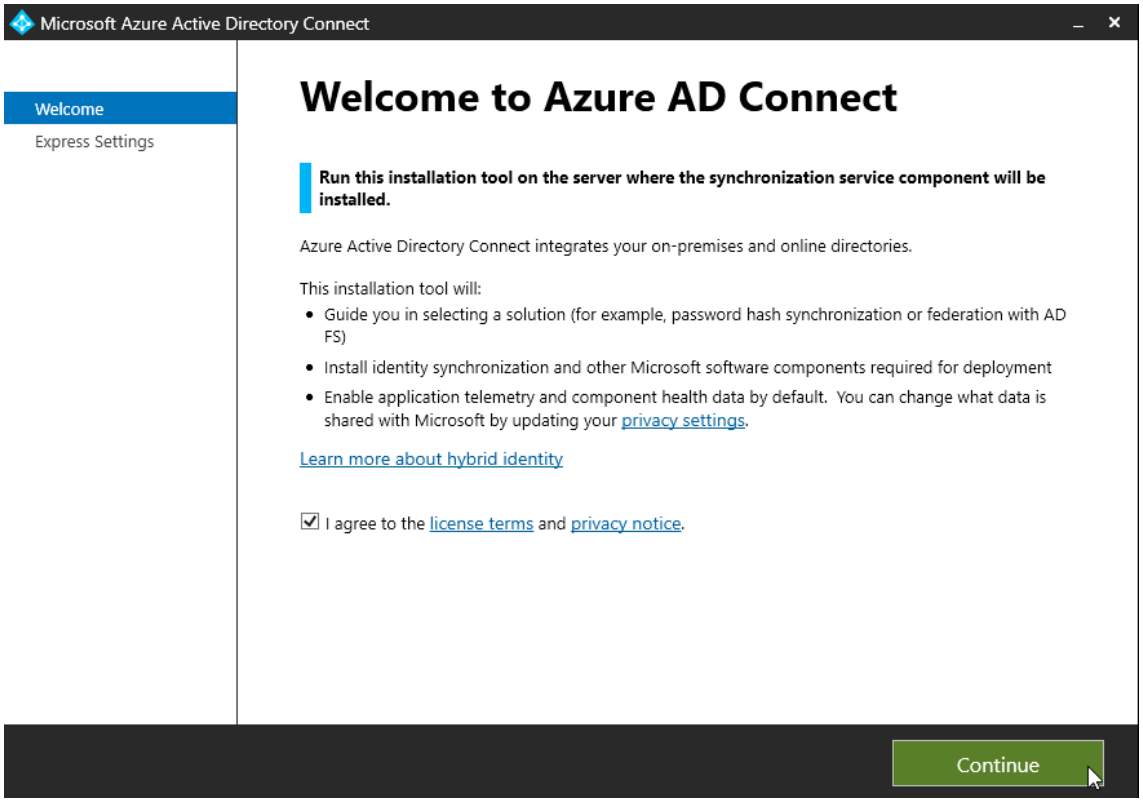
Anexo 14. Proceso de integración de Intune con MECM

Para integrar Microsoft Intune y Microsoft Endpoint Configuration Manager es necesario disponer de credenciales de administrador en ambas soluciones, así como credenciales de administrador de dominio (para el dominio on-premises) y de administrador global para el tenant de Azure AD. Los dispositivos deben tener una identidad en Azure AD para poder ser inscritos en Intune, por lo que deben estar registrados, unidos, o unidos de forma híbrida mediante el domino on-premises. En este caso, se ha optado por la última opción.

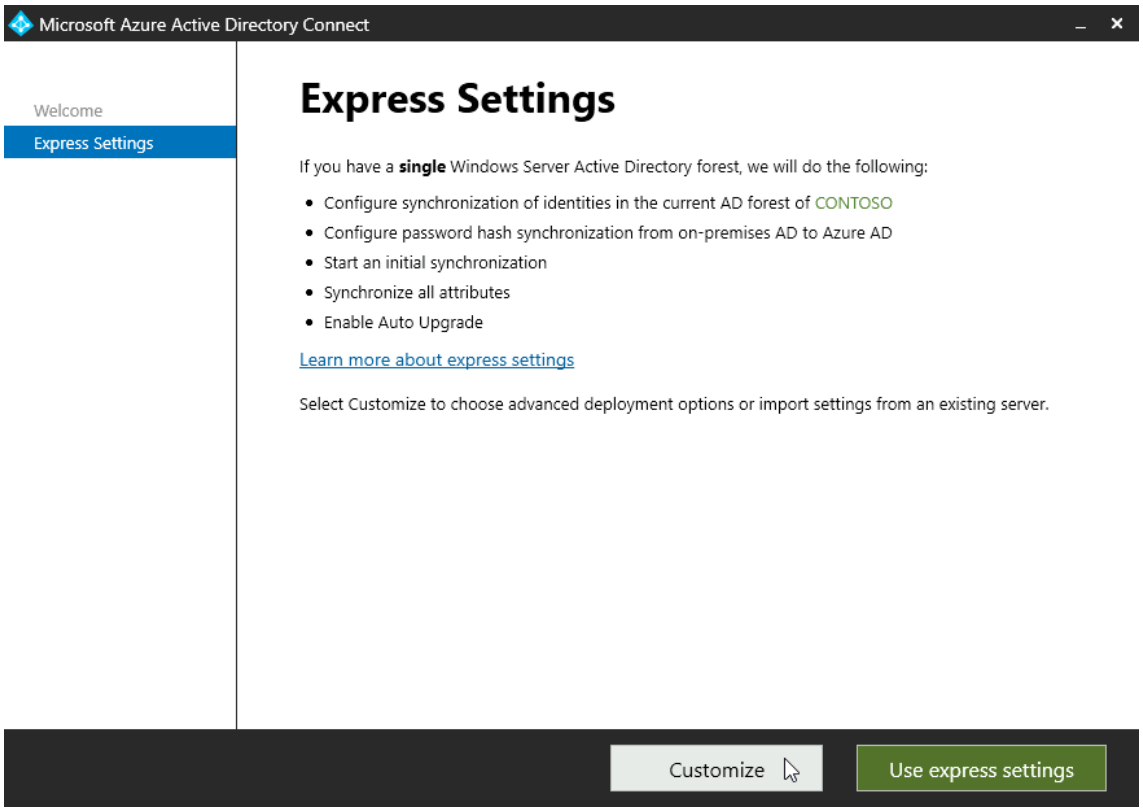
- **Instalación de Azure AD Connect**

En primer lugar, es necesario instalar la herramienta llamada “Azure AD Connect”, que permitirá sincronizar el dominio on-premises con el de Azure. Para ello, se descarga la aplicación desde la siguiente dirección y se instala en cualquiera de los servidores unidos al dominio on-premises:
https://www.microsoft.com/en-us/download/details.aspx?id=47594

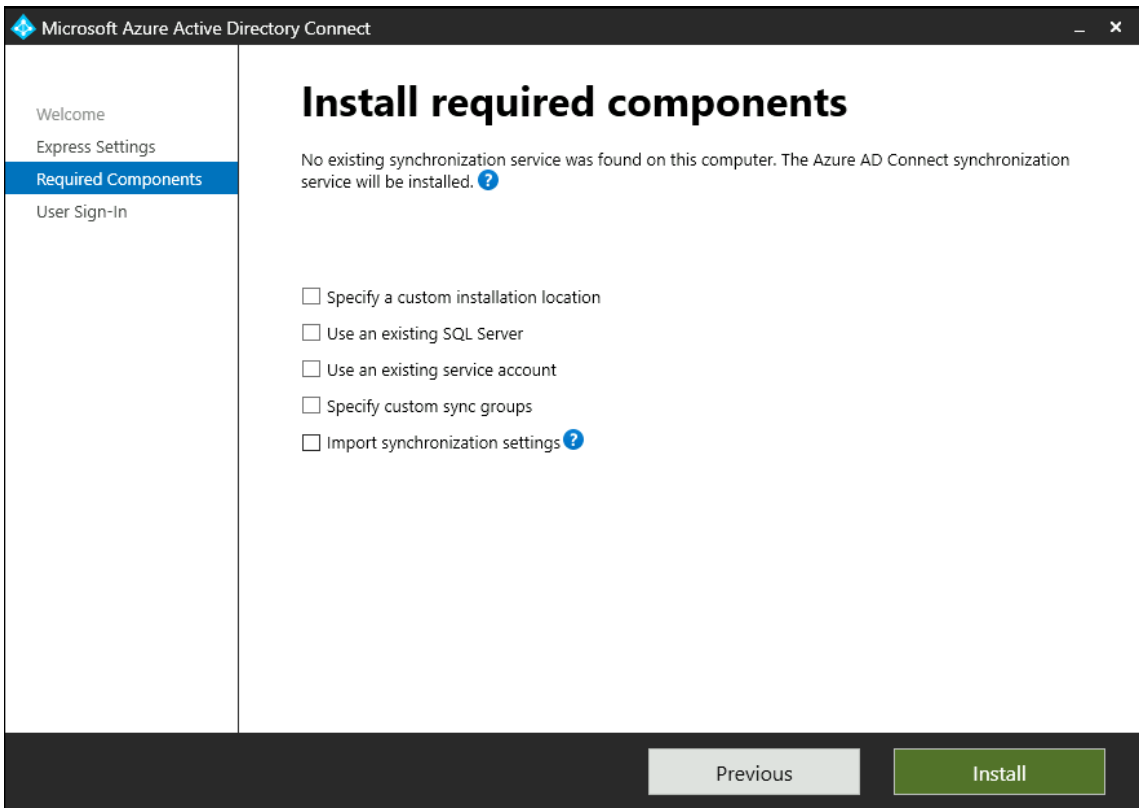
Una vez ha terminado la instalación, que es totalmente desatendida al ejecutar el archivo .msi, se ejecuta automáticamente el asistente de configuración, en el que el primer paso es aceptar los términos de licencia.



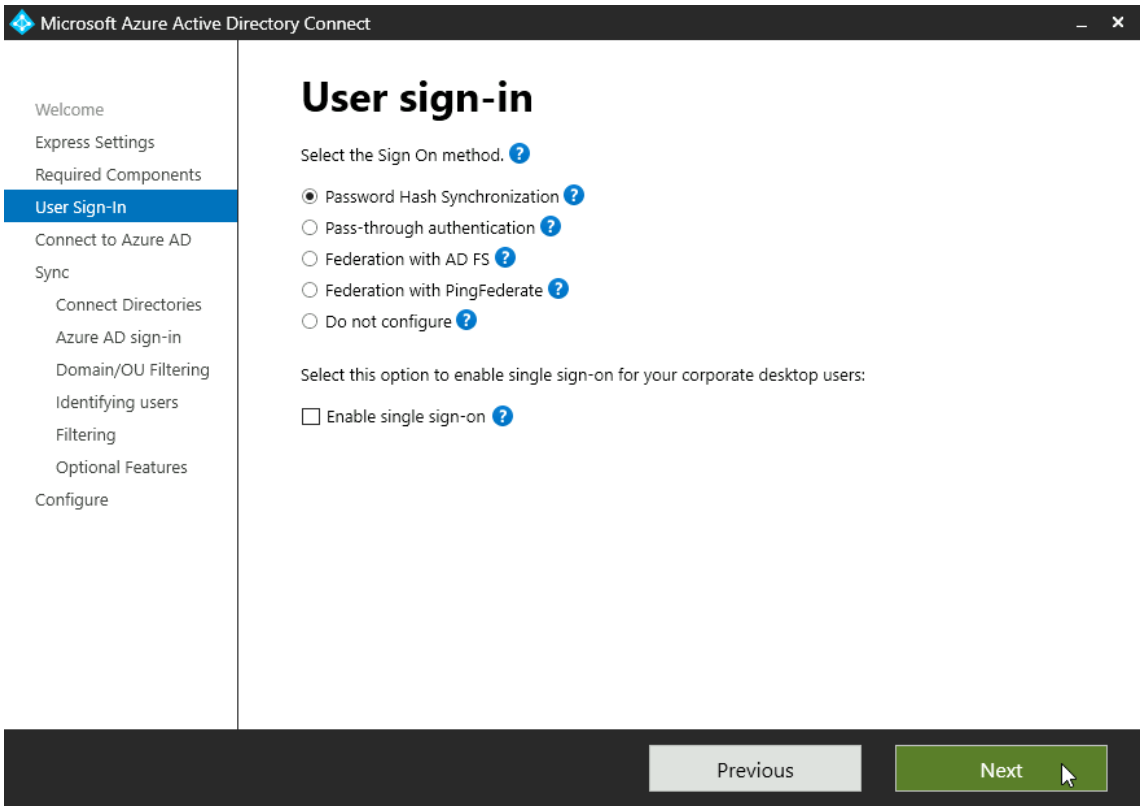
A continuación, se escoge la opción de personalización mediante el botón “Customize”.



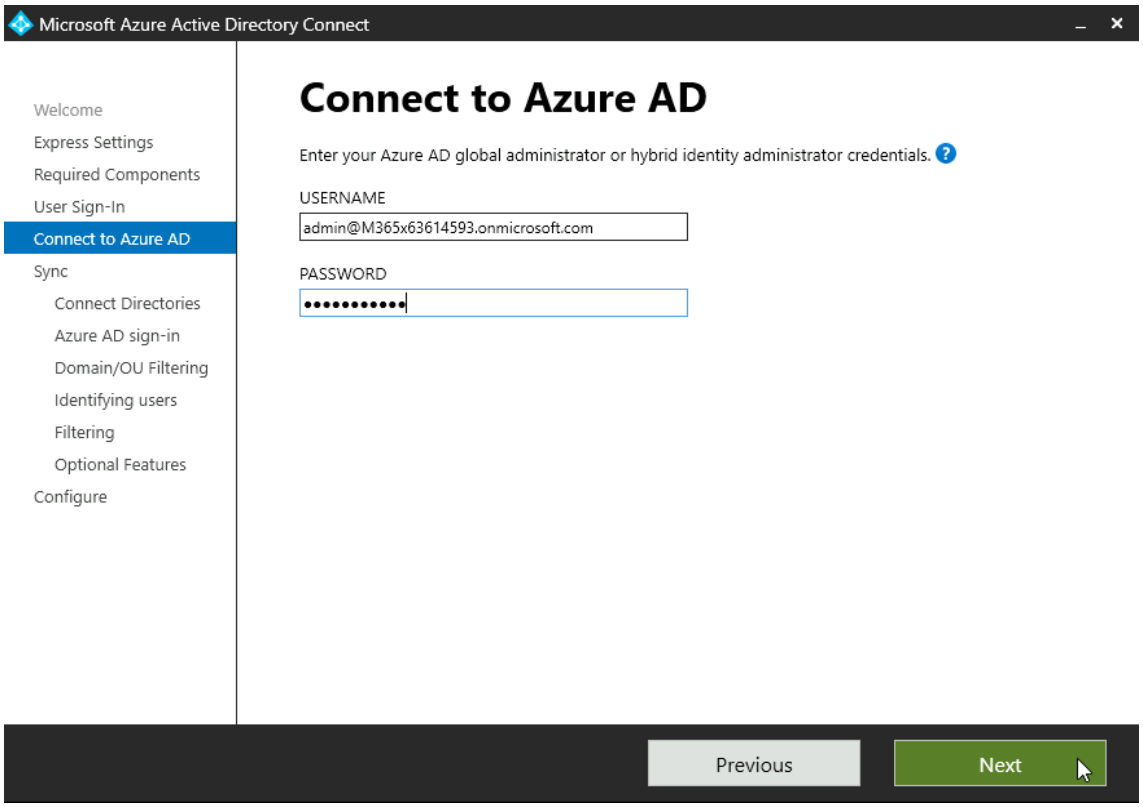
La configuración de instalación de los componentes requeridos se mantiene por defecto.



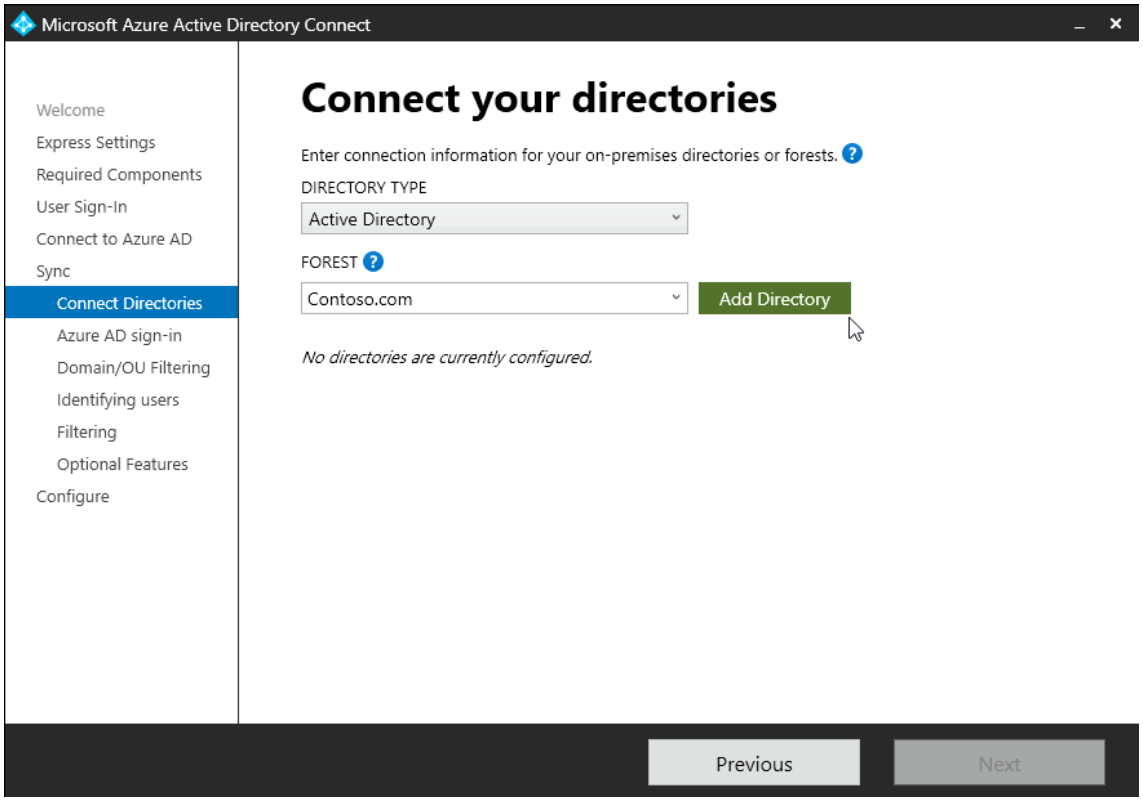
La configuración de inicio de sesión se mantiene como “Password Hash Synchronization”.



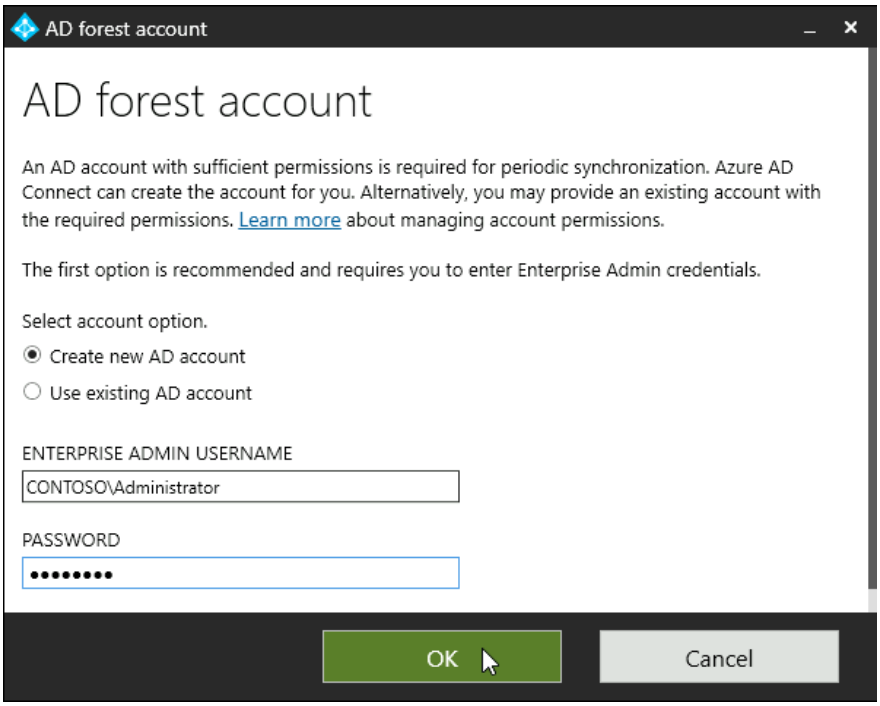
Después, se introducen las credenciales de un administrador global de Azure.

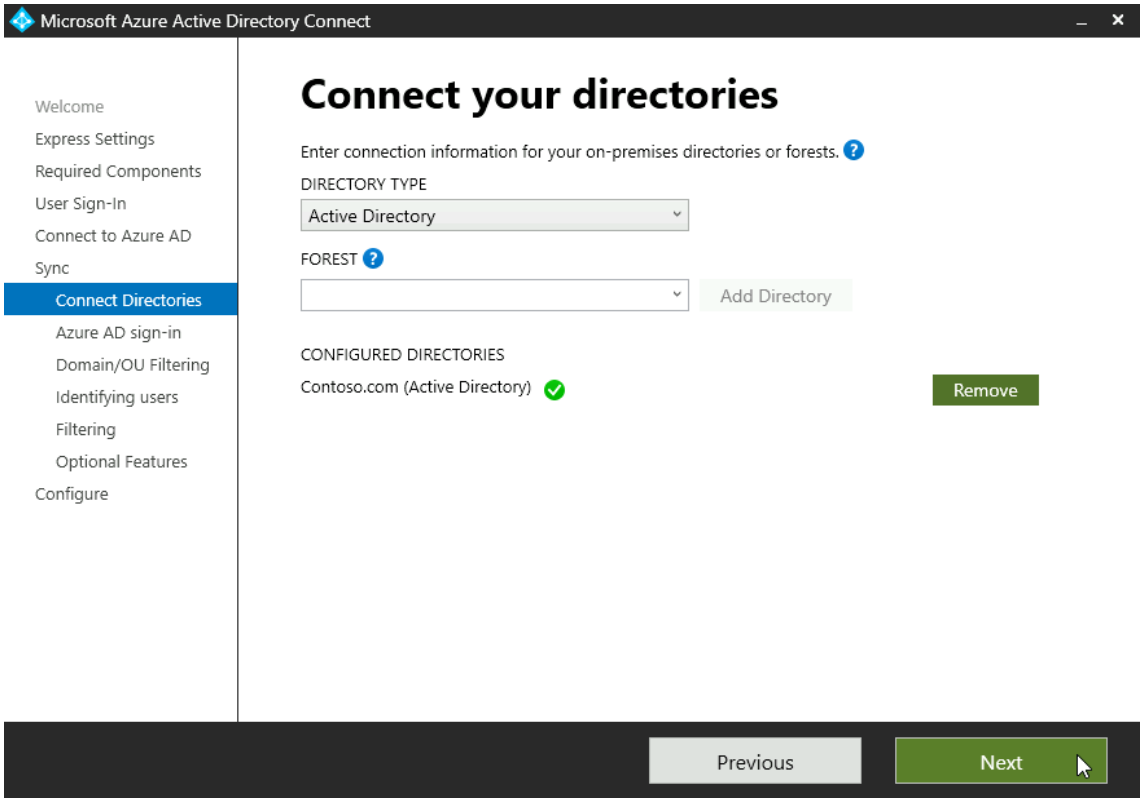


Se introducen las credenciales del administrador del dominio on-premises haciendo click en “Add Directory”.

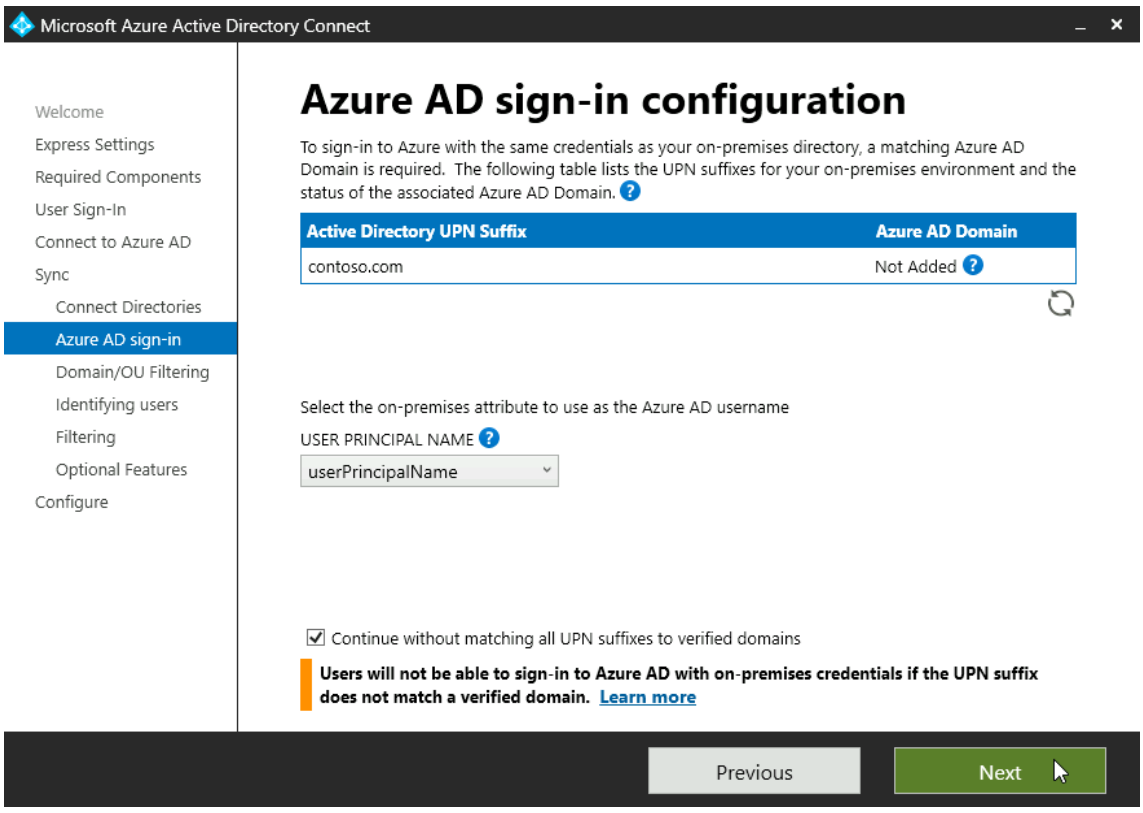


Se solicita la creación de una nueva cuenta de usuario en el dominio on-premises que será la encargada de realizar la sincronización de los directorios.

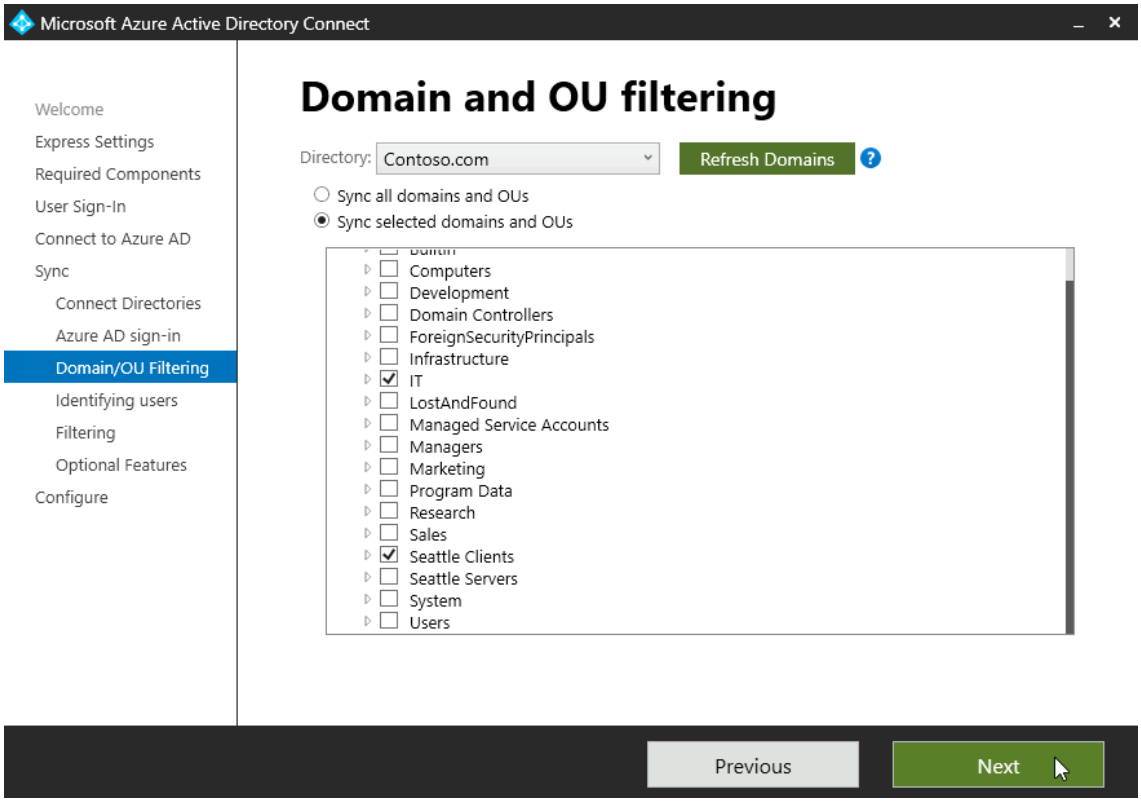




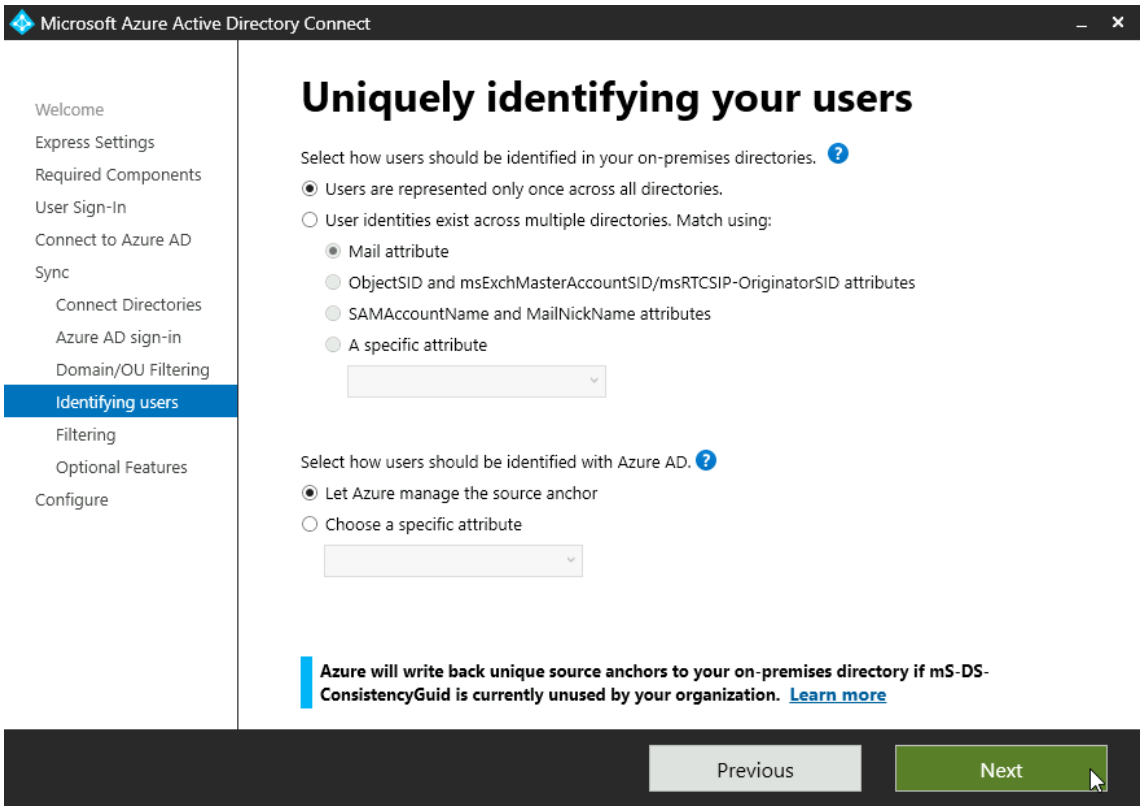
Se selecciona el atributo “userPrincipalName” como atributo on-premises para usar como nombre de usuario en Azure AD.



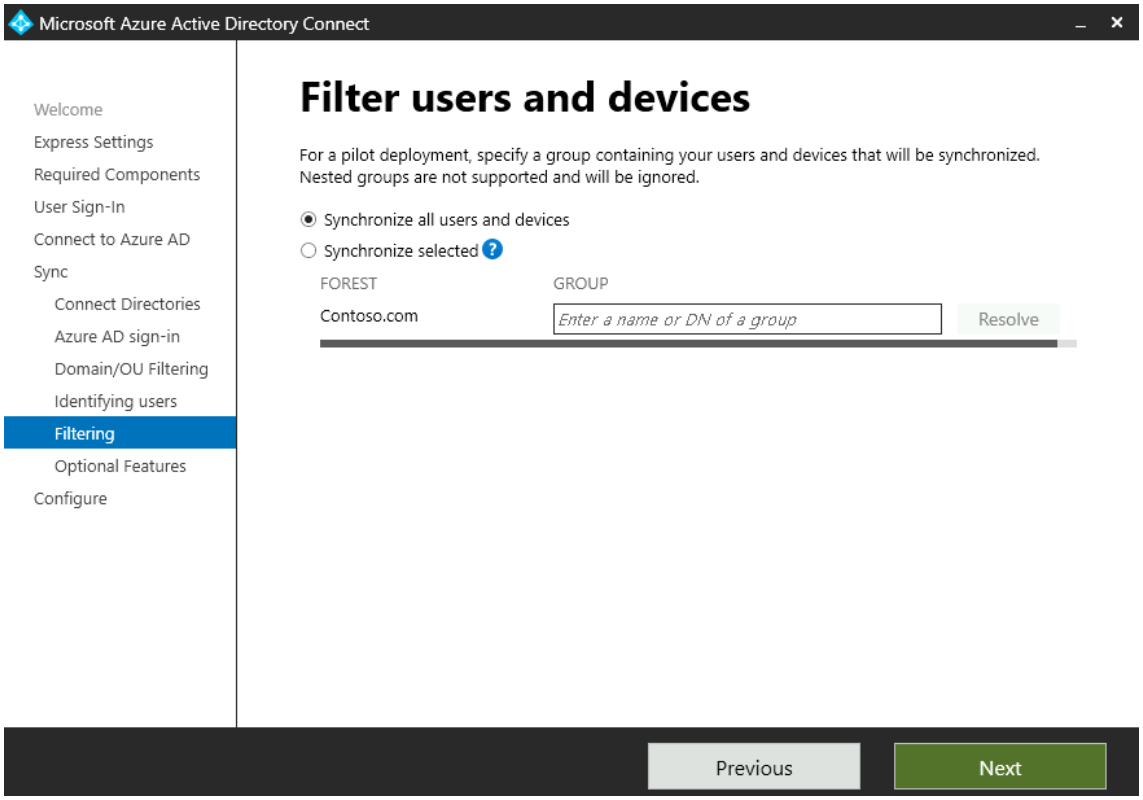
A continuación, se seleccionan las OU del dominio que se quiere sincronizar. En este caso, se ha seleccionado “IT” y “Seattle Clients”, que es donde se encuentran los dispositivos que se registrarán.



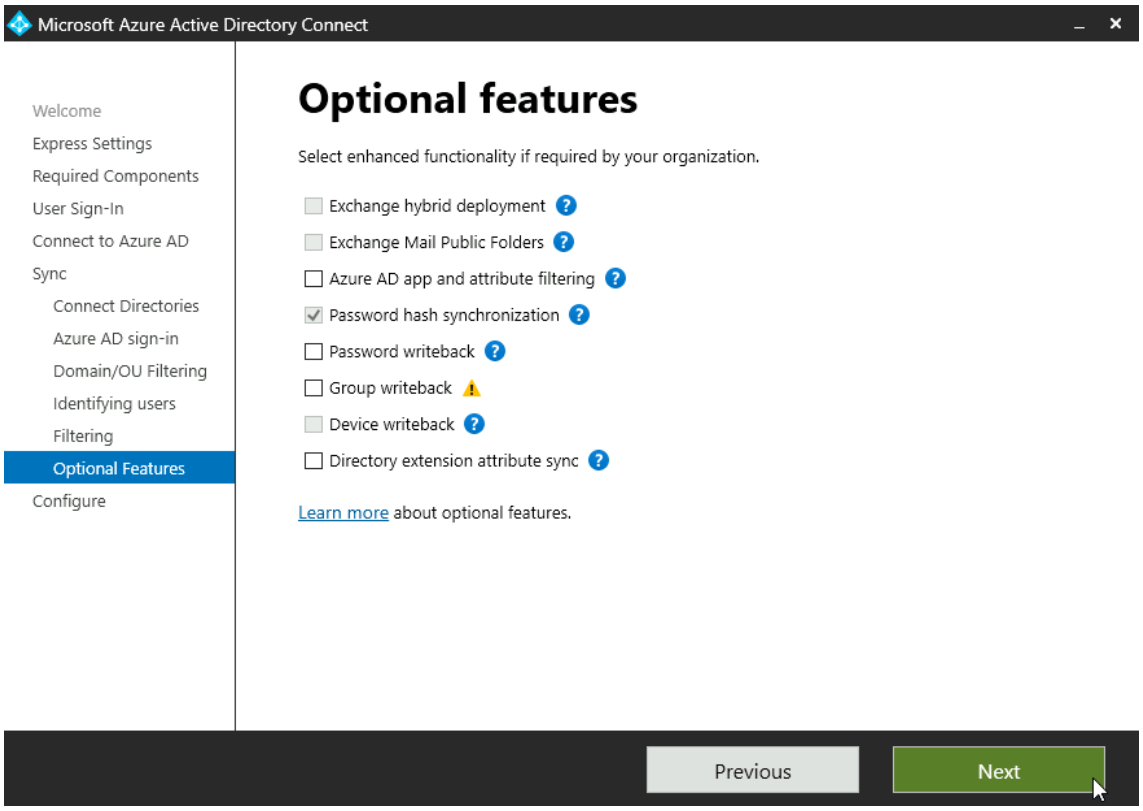
La configuración de identificación única de usuarios se mantiene por defecto.



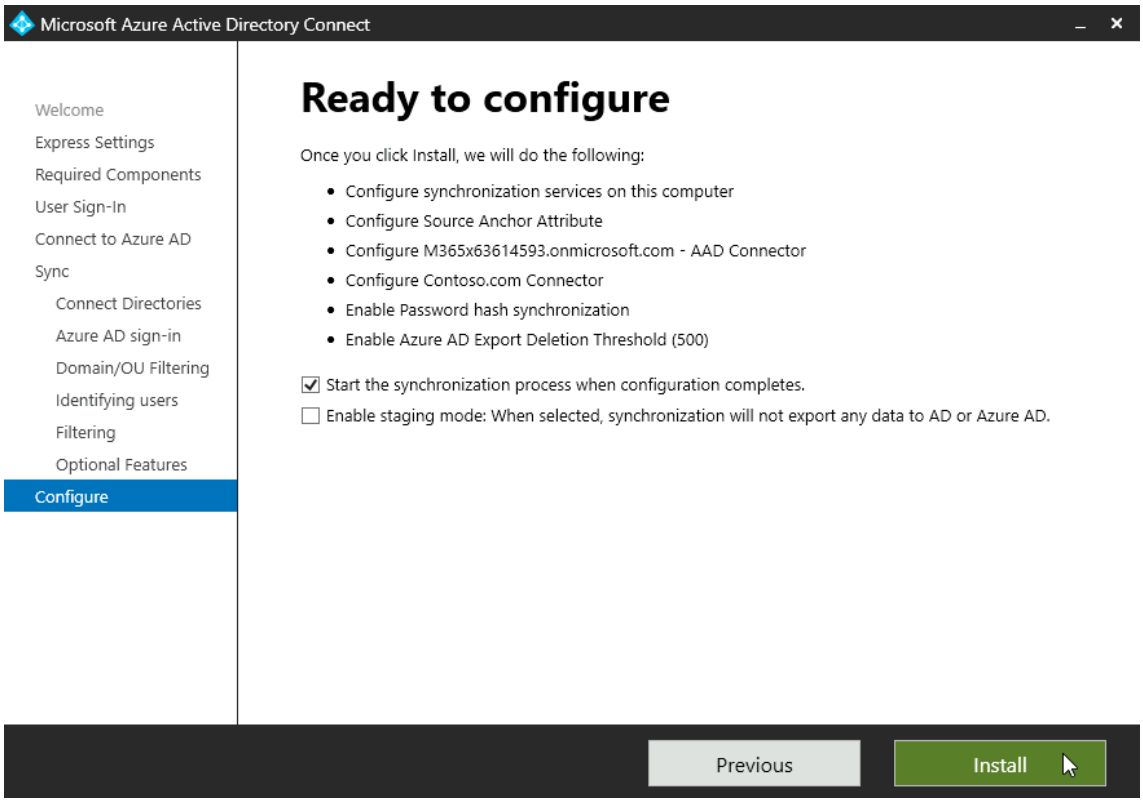
No se realiza ningún filtrado de usuarios ni dispositivos, pues ya se han seleccionado previamente los que se quieren sincronizar.



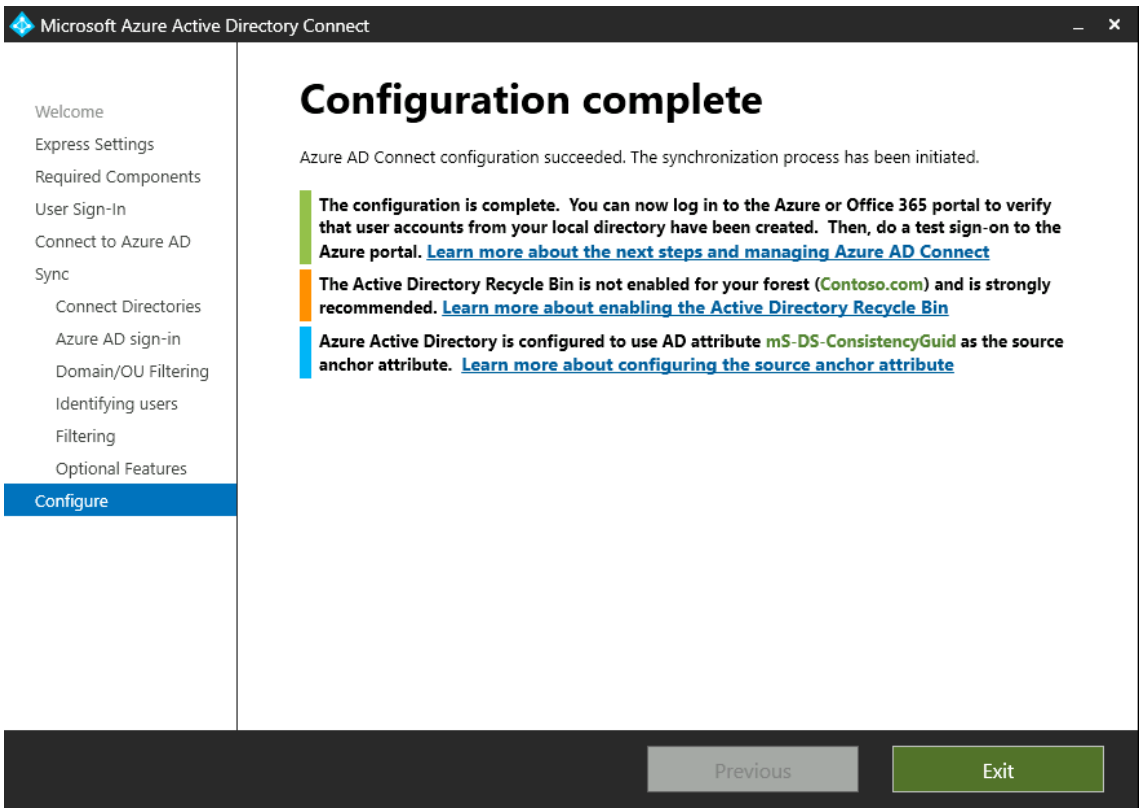
Para terminar, se mantienen por defecto las funcionalidades opcionales.



Se revisan las opciones configuradas y se realiza la instalación, dejando marcada la opción de que empiece la sincronización una vez esta termine.

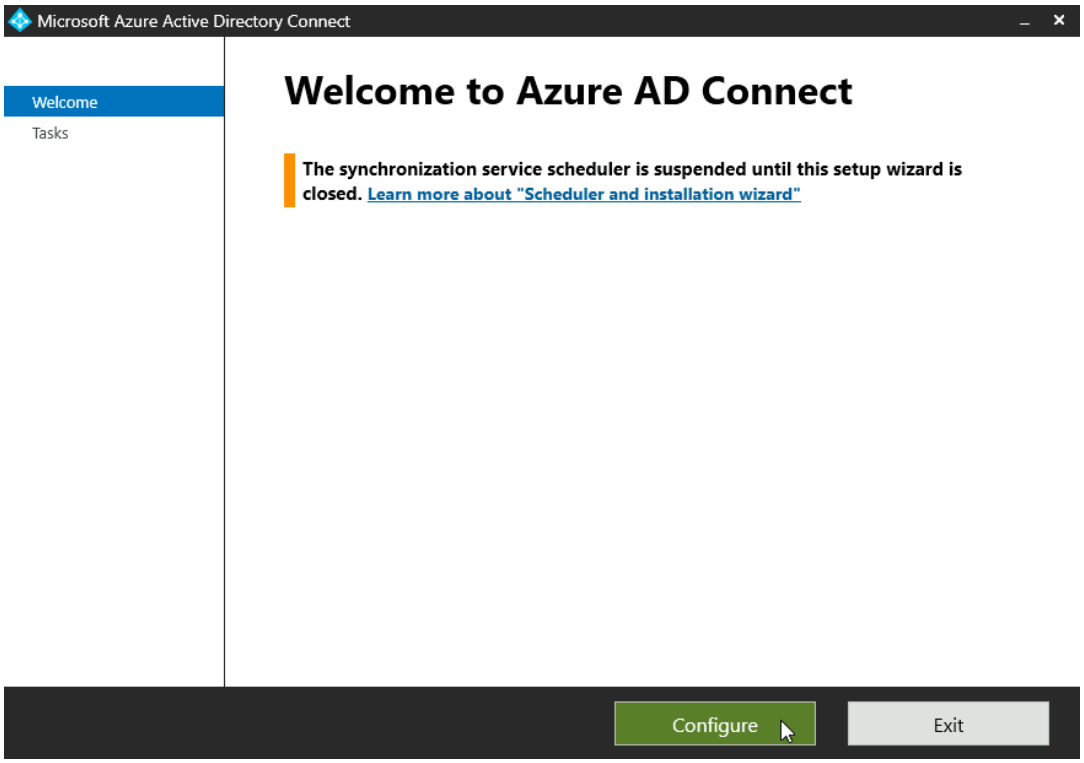


Un mensaje de configuración completada aparece tras la instalación.

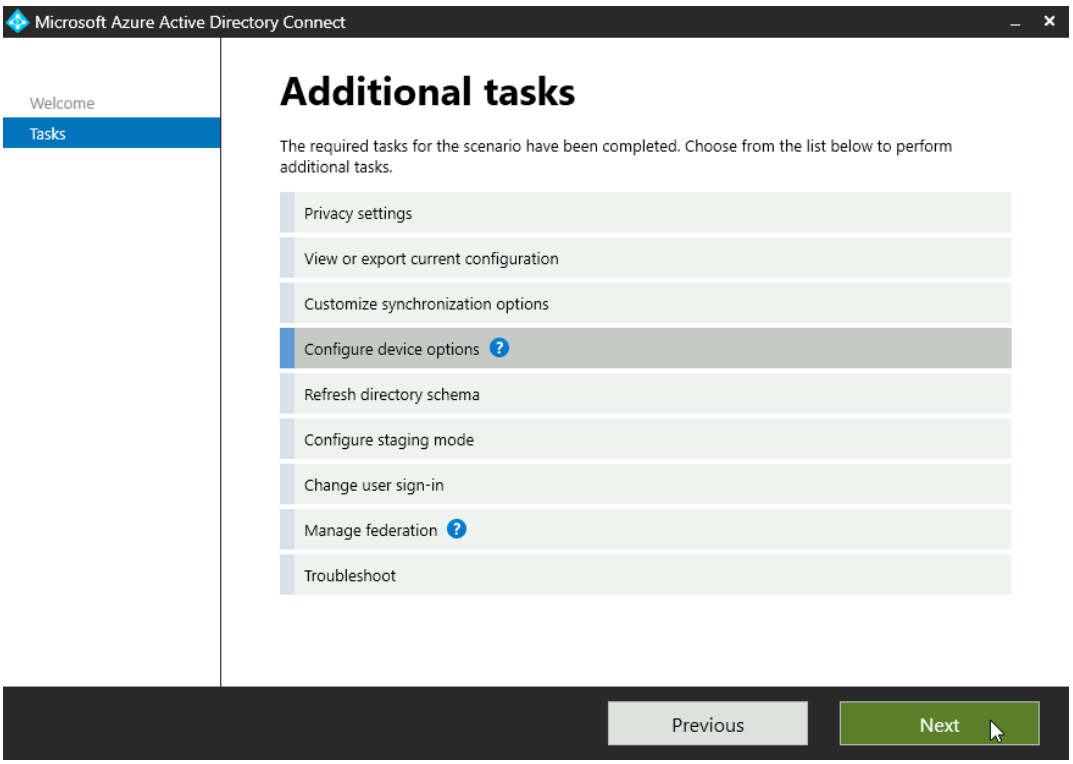


- **Configuración de unión híbrida a Azure AD**

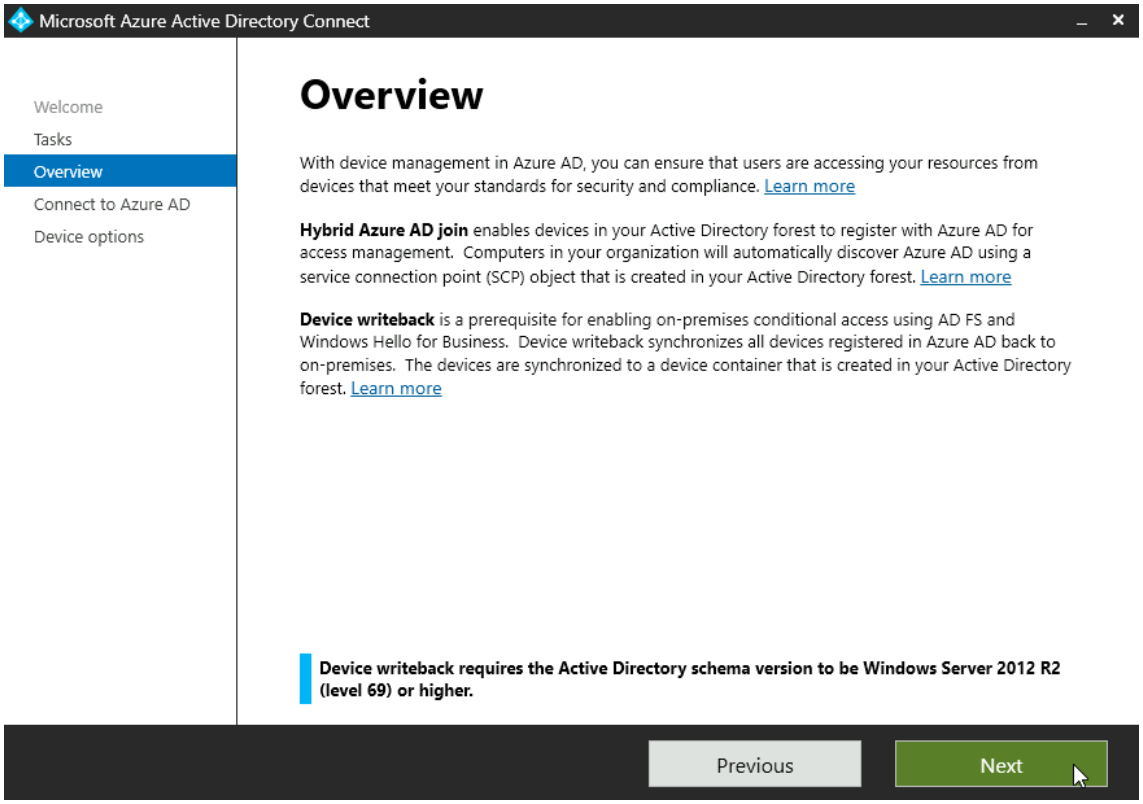
En segundo lugar, se debe configurar la unión híbrida a Azure AD de los dispositivos ya unidos al dominio on-premises. Para ello, se ejecuta la aplicación “Azure AD Connect” y se vuelve a configurar.



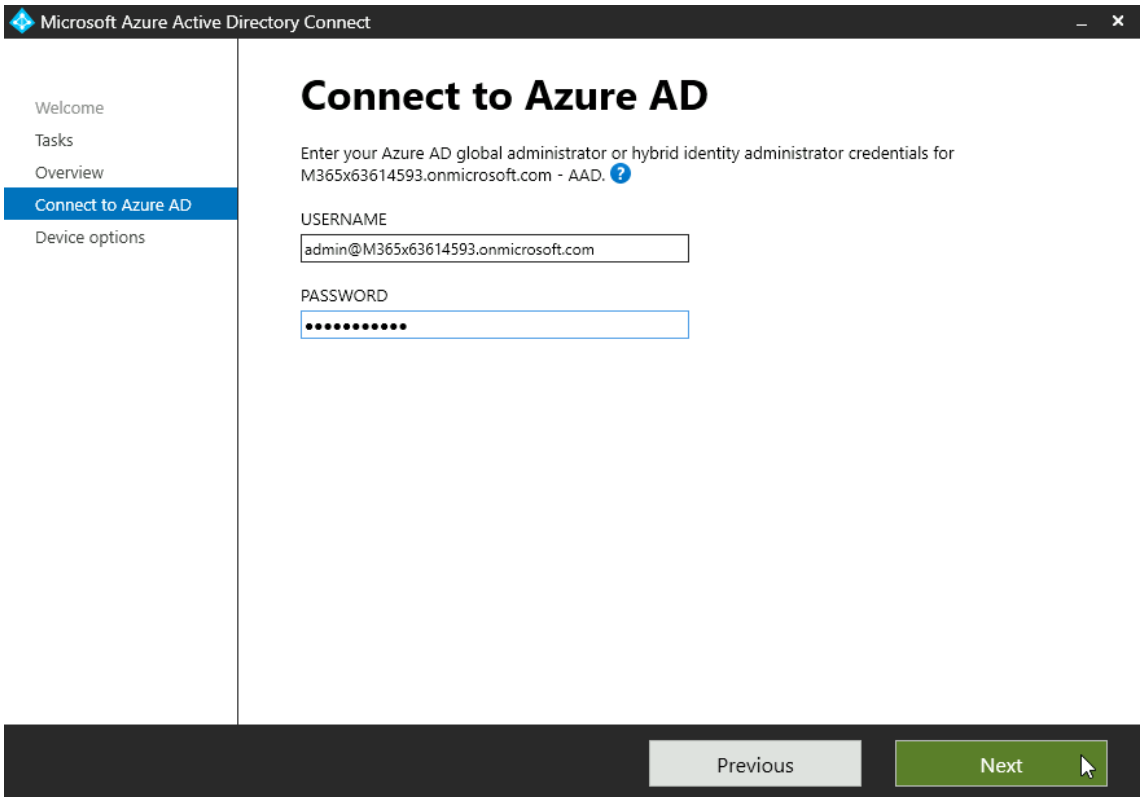
Se selecciona la opción “Configure Device Options” y se pulsa “Next”.



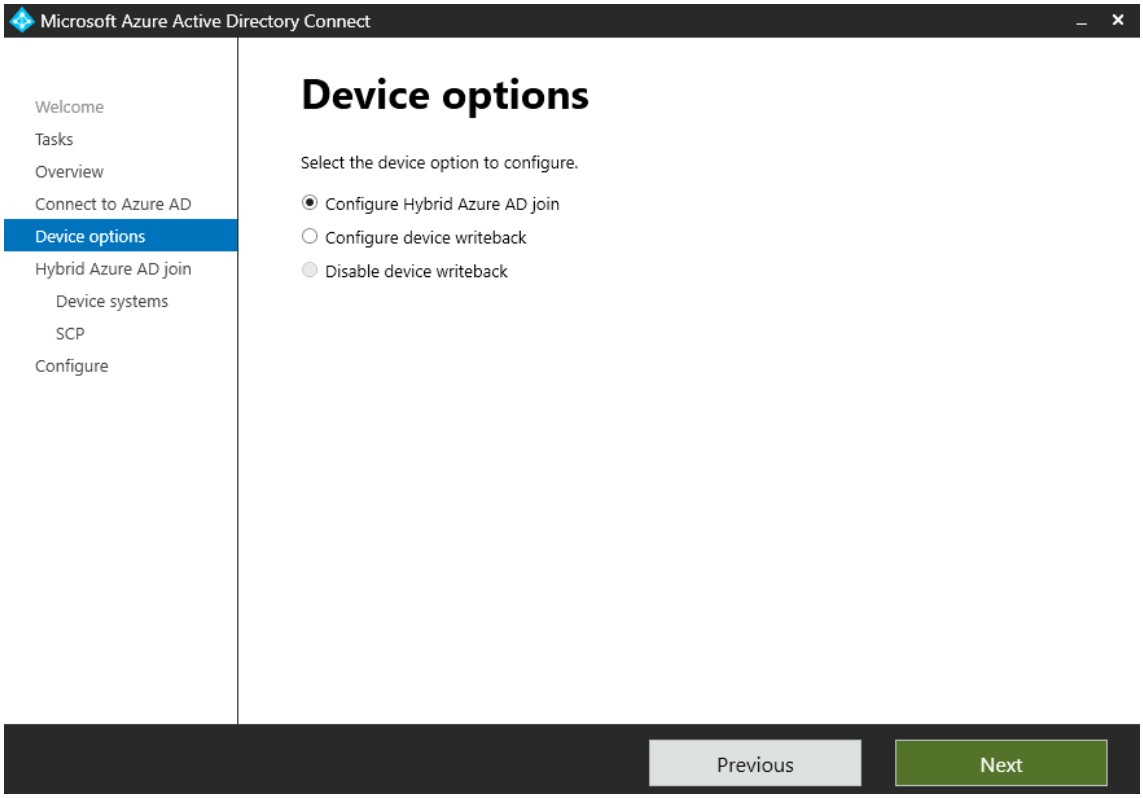
En la ventana de Overview, se pulsa en “Next”.



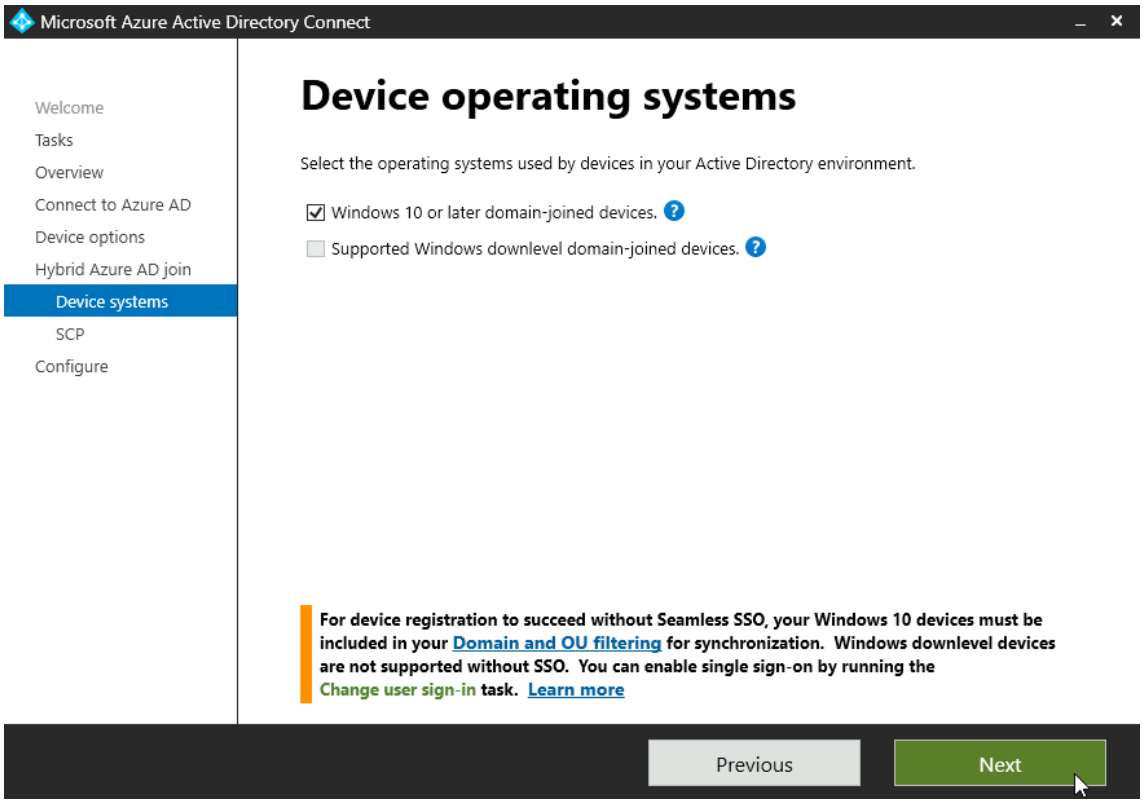
Se introducen las credenciales del administrador global de Azure AD.



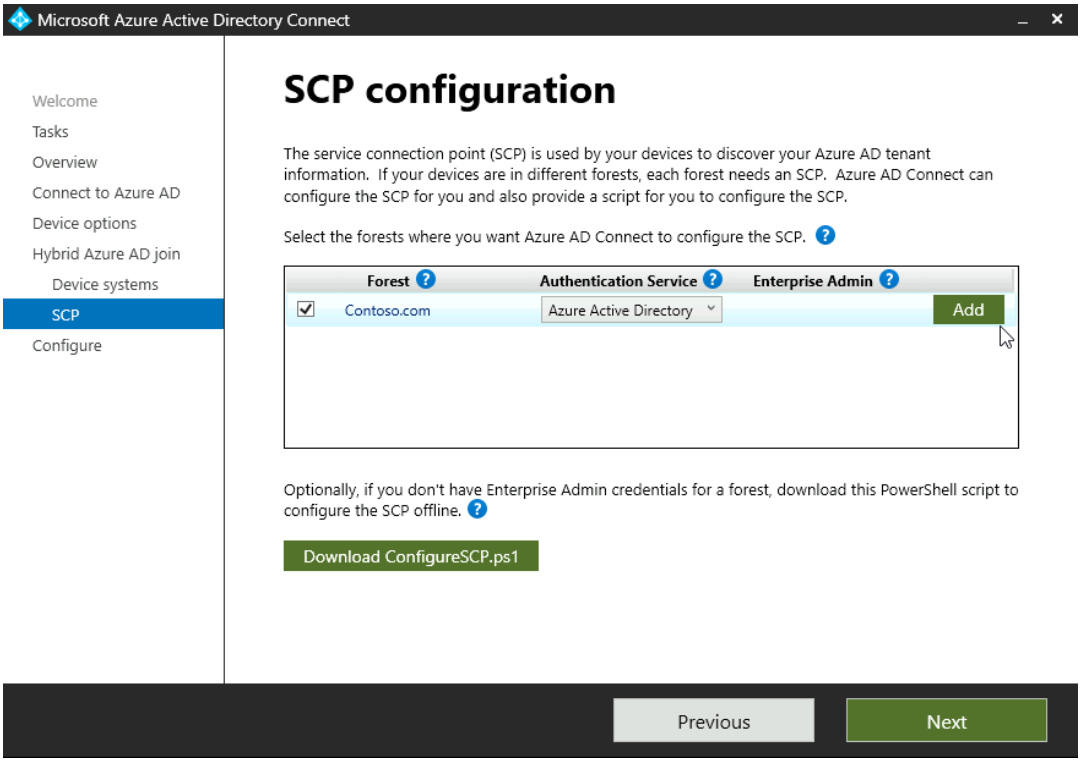
Se selecciona la opción “Configure Hybrid Azure AD join” y se pulsa Next.



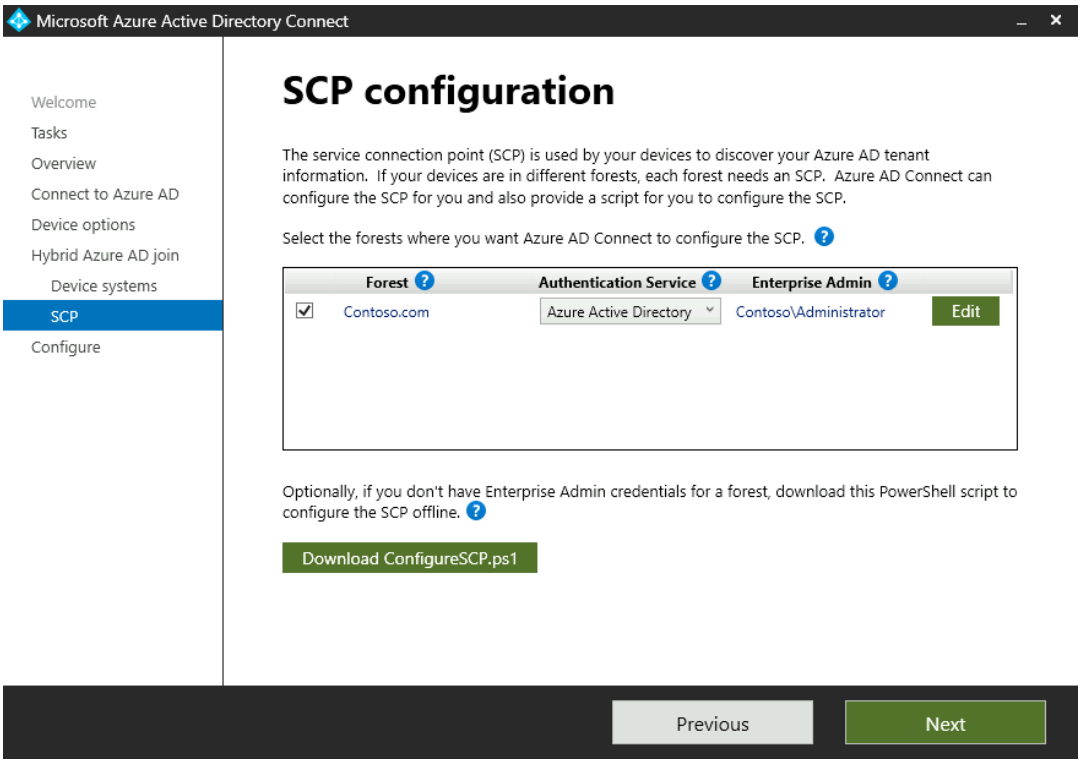
Se selecciona la opción “Windows 10 or later domain-joined devices.



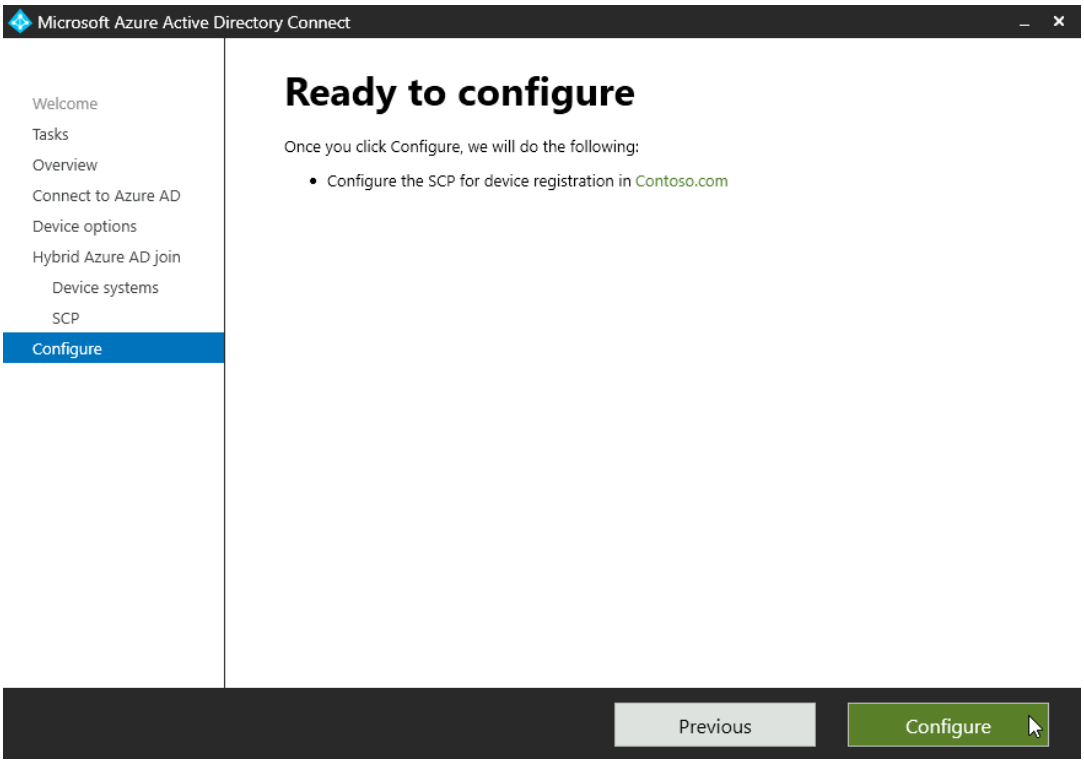
A continuación, se debe configurar el servicio de punto de conexión (SCP) para el bosque on-premises. Así, se marca el bosque, se selecciona “Azure Active Directory” en el desplegable de “Authentication Service” y se pulsa en “Add”.



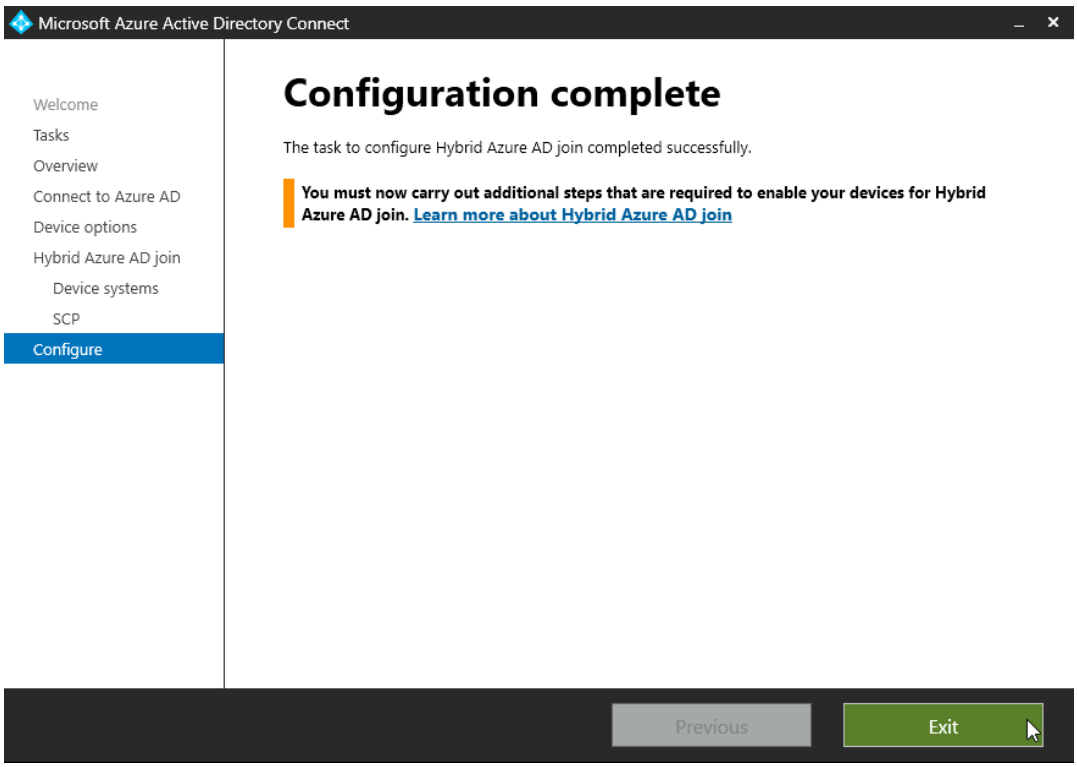
Tras introducir las credenciales del administrador empresarial, se pulsa en Next.



Por último, se pulsa en “Configure” para realizar la configuración definida.



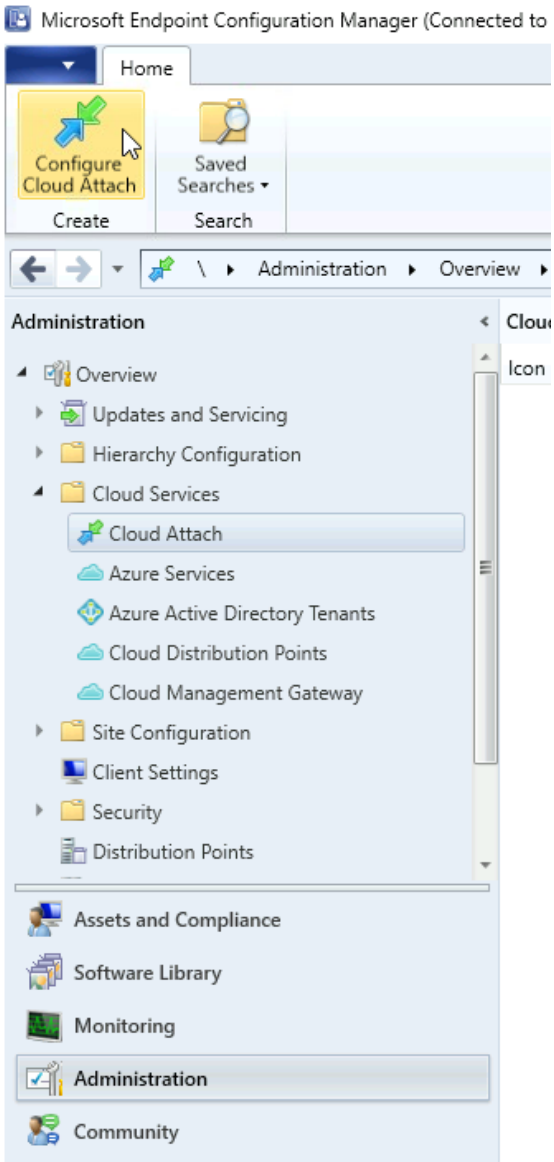
Tras la configuración, se muestra un mensaje conforme se ha realizado correctamente.



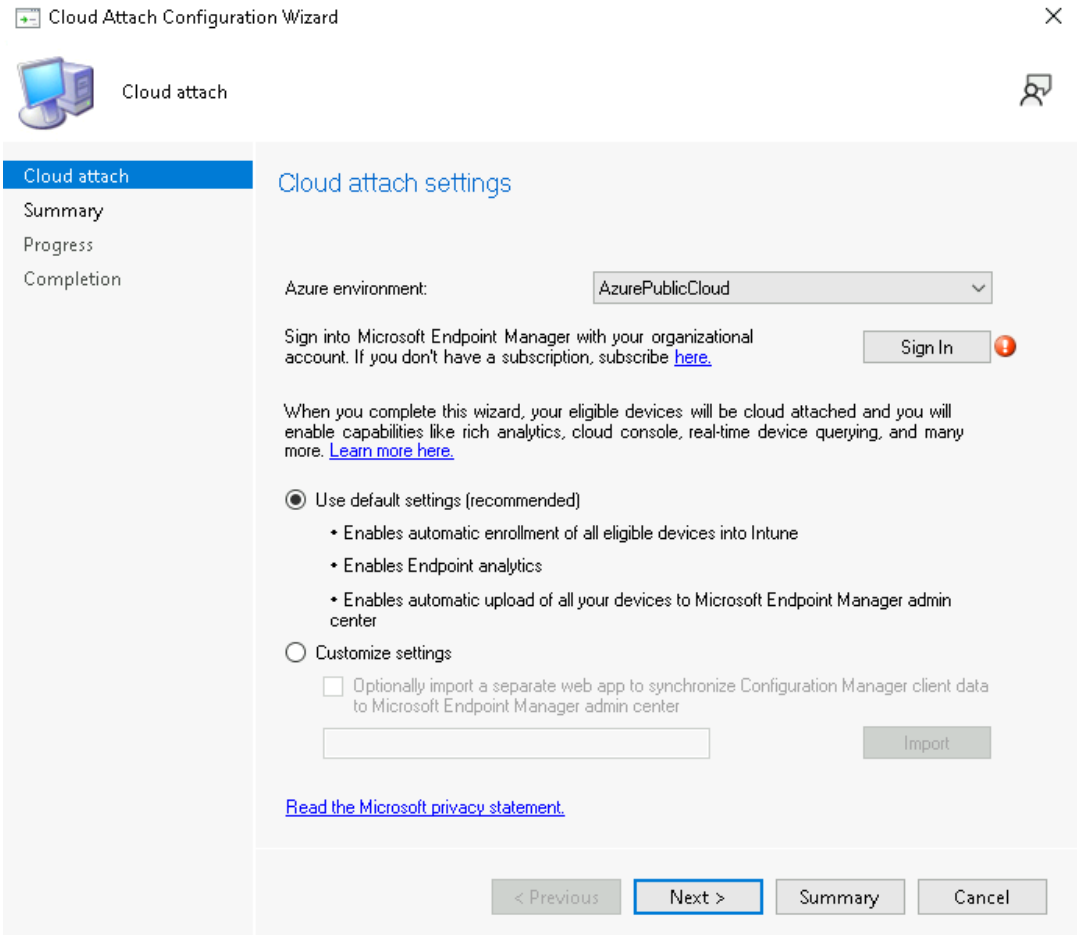
Una vez hecha la configuración, es necesario que los dispositivos se reinicien y se ejecute el ciclo de sincronización de directorios de Azure AD Connect, programado por defecto cada 30 minutos (se puede forzar con un comando powershell), para que los dispositivos se unan de manera hibrida en Azure AD.

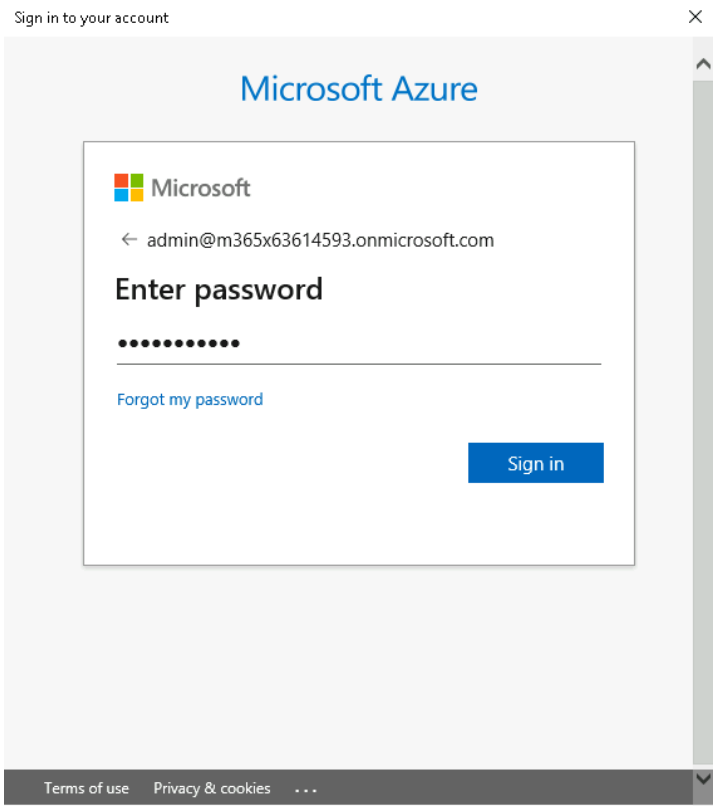
- **Vinculación del tenant de Azure AD en MECM**

En tercer lugar, se debe vincular el tenant de Azure AD en MECM, por lo que hay que acceder a Administration/Cloud Services/Cloud Attach y hacer click en “Configure Cloud Attach”.

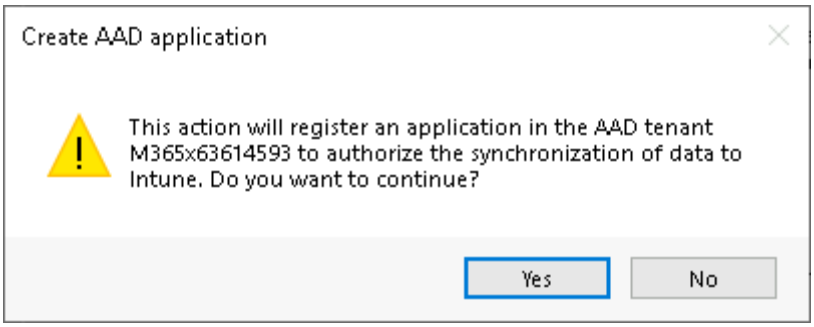


En el asistente, es necesario introducir las credenciales de un administrador global del tenant de Azure AD al pulsar en el botón “Sign In” y después pulsar en “Next >”.

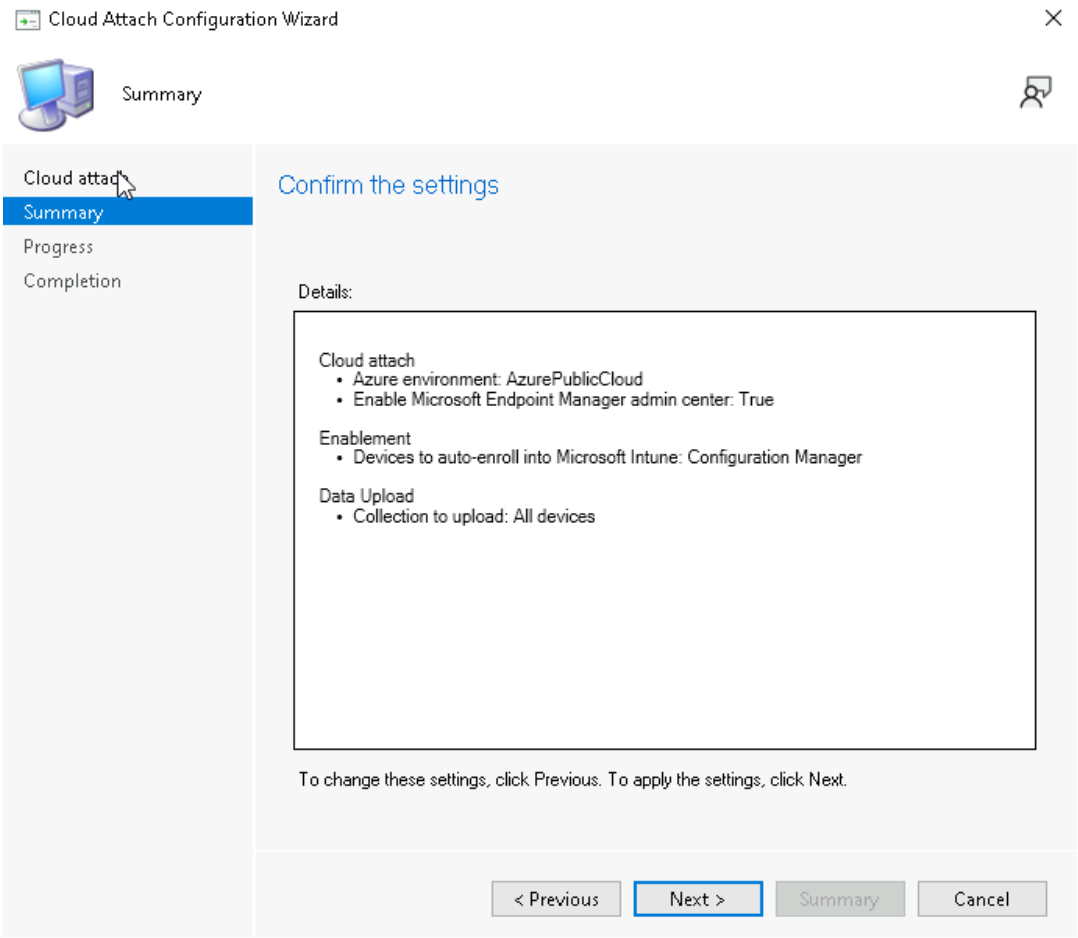




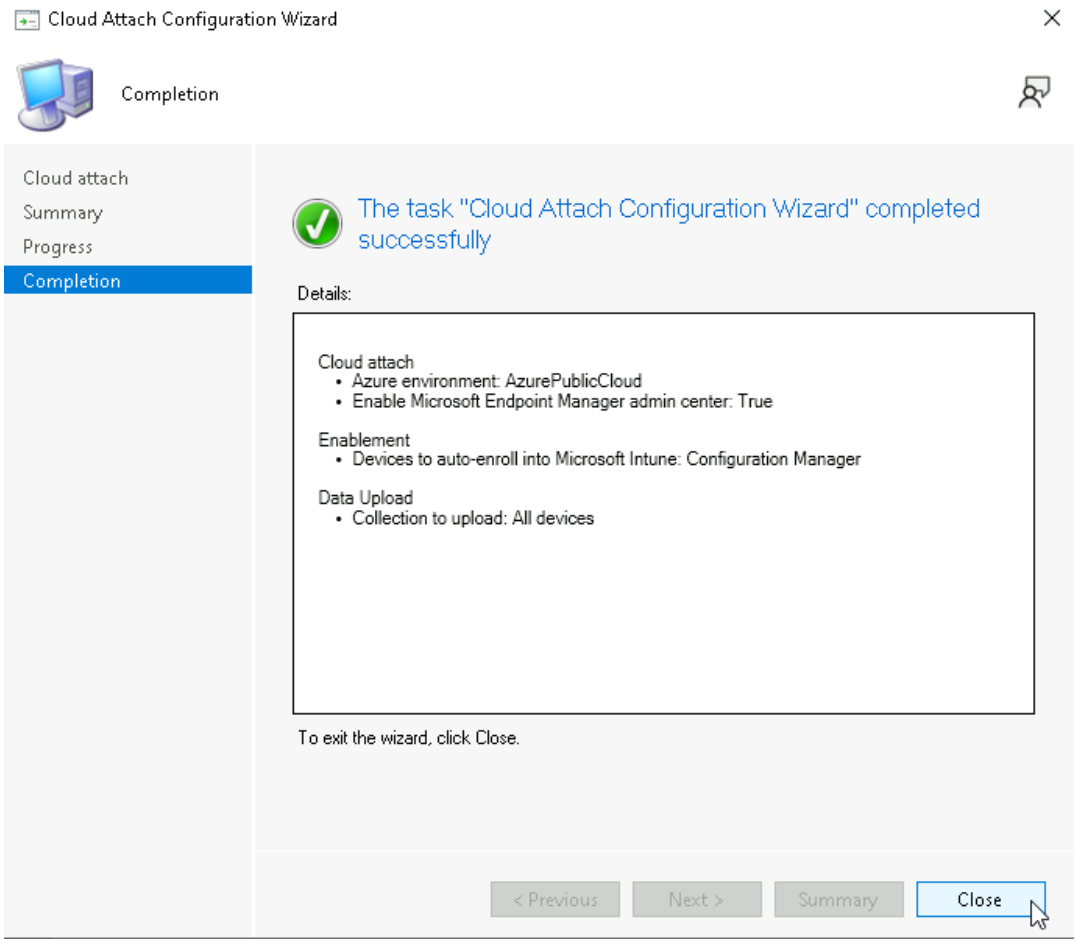
A continuación, se debe aceptar el mensaje conforme se va a registrar la aplicación en el tenant de Azure AD.



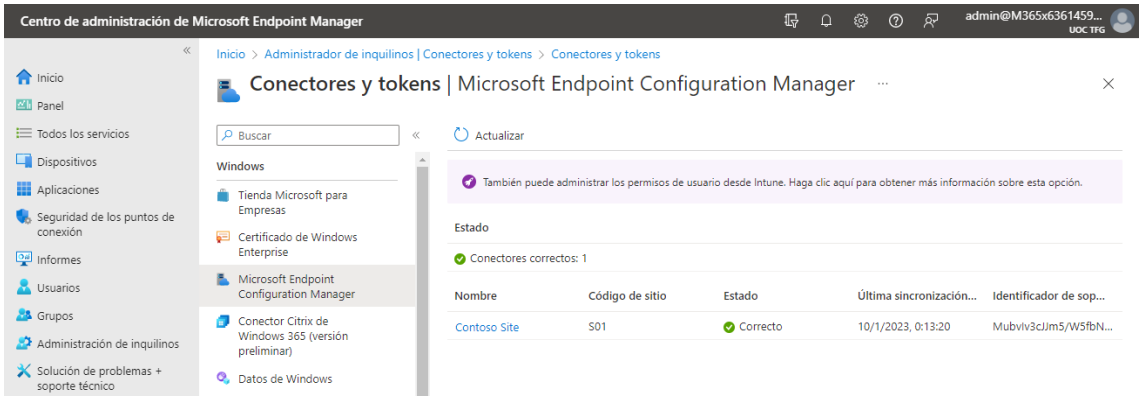
Se revisan los detalles de la configuración realizada y pulsa en “Next >”.



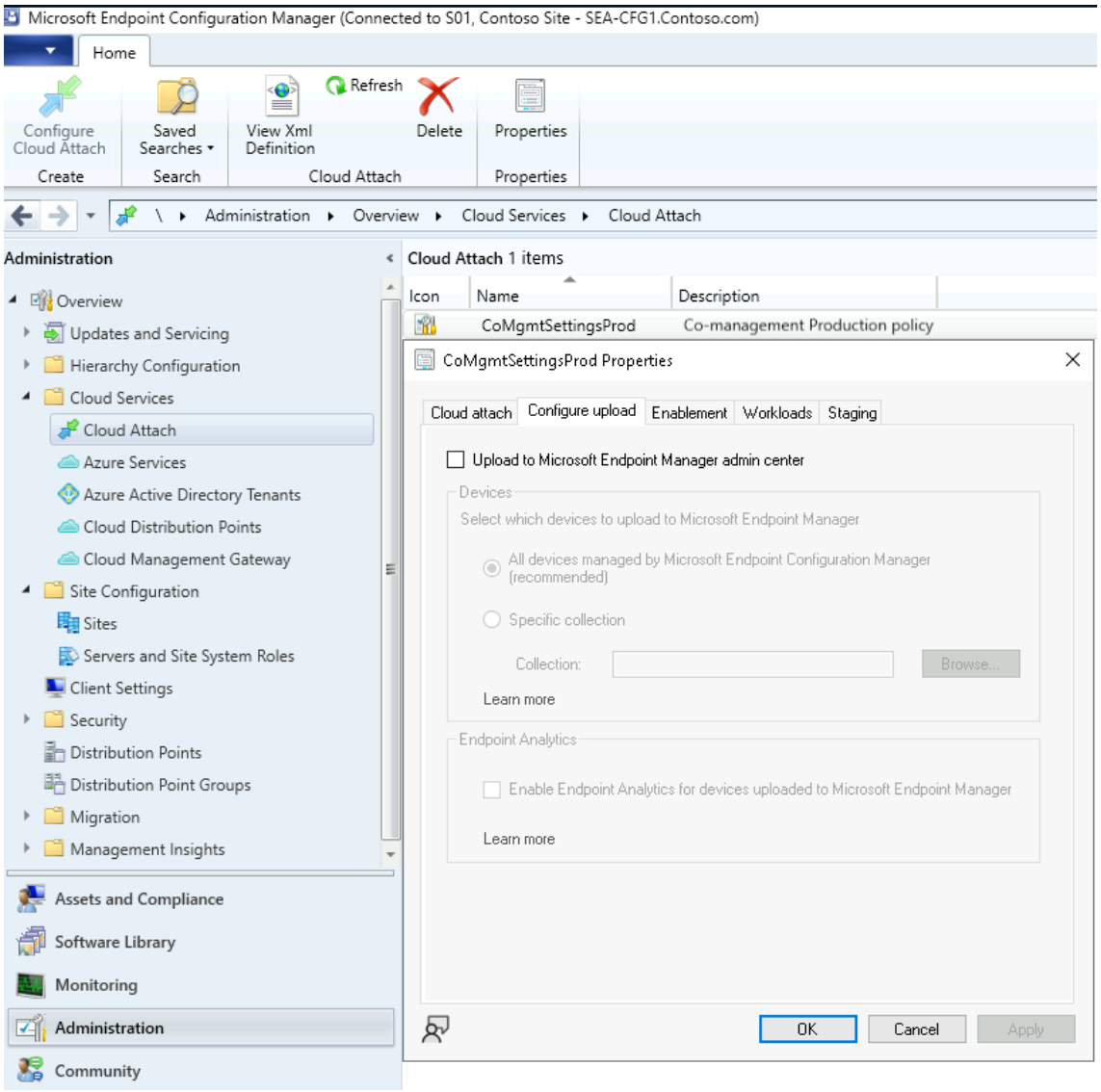
Si la vinculación con el tenant de Azure AD ha sido correcta, aparecerá un mensaje indicando lo siguiente.

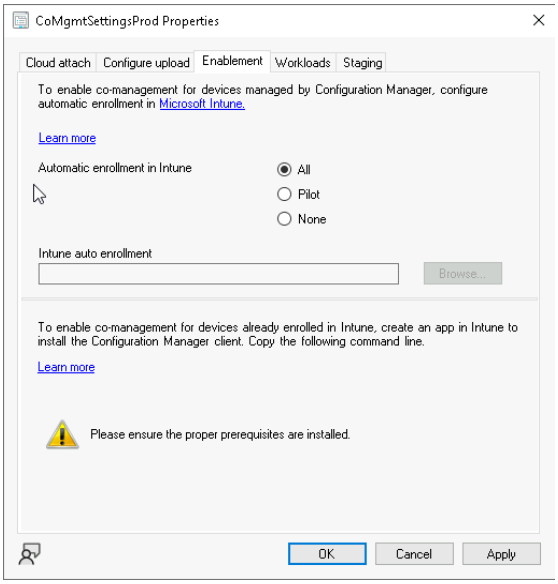


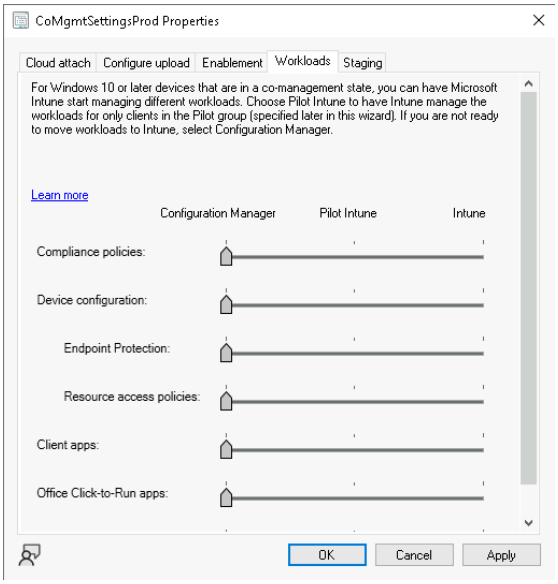
El estado de conexión también se puede consultar desde el portal de administración de Intune, en el apartado “Microsoft Endpoint Configuration Manager” del menú “Administración de inquilinos/Conectores y tokens”.

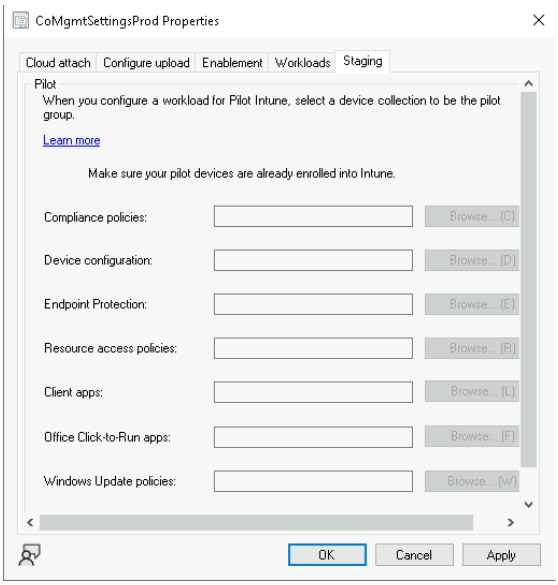


A continuación, se puede gestionar desde la consola de administración de MECM qué dispositivos se quieren integrar en Intune y qué áreas van a estar gestionados por cada herramienta. Para ello, es necesario ver las propiedas de la política llamada CoMgmtSettingsProd, en “Cloud Attach”.


Microsoft Endpoint Configuration Manager (Connected to S01, Contoso Site - SEA-CFG1.Contoso.com)
Home
Configure Cloud Attach
Create
Saved Searches
Search
View Xml Definition
Refresh
Delete
Cloud Attach
Properties
Properties
Administration
Overview
Cloud Services
Cloud Attach
Cloud Attach 1 items
Icon
Name
Description
CoMgmtSettingsProd
Co-management Production policy
CoMgmtSettingsProd Properties
Cloud attach
Configure upload
Enablement
Workloads
Staging
Upload to Microsoft Endpoint Manager admin center
Devices
Select which devices to upload to Microsoft Endpoint Manager
All devices managed by Microsoft Endpoint Configuration Manager (recommended)
Specific collection
Collection:
Browse...
Learn more
Endpoint Analytics
Enable Endpoint Analytics for devices uploaded to Microsoft Endpoint Manager
Learn more
OK
Cancel
Apply
Assets and Compliance
Software Library
Monitoring
Administration
Community


CoMgmtSettingsProd Properties
Cloud attach
Configure upload
Enablement
Workloads
Staging
To enable co-management for devices managed by Configuration Manager, configure automatic enrollment in Microsoft Intune.
Learn more
Automatic enrollment in Intune
All
Pilot
None
Intune auto enrollment
Browse...
To enable co-management for devices already enrolled in Intune, create an app in Intune to install the Configuration Manager client. Copy the following command line.
Learn more
Please ensure the proper prerequisites are installed.
OK
Cancel
Apply


CoMgmtSettingsProd Properties
Cloud attach
Configure upload
Enablement
Workloads
Staging
For Windows 10 or later devices that are in a co-management state, you can have Microsoft Intune start managing different workloads. Choose Pilot Intune to have Intune manage the workloads for only clients in the Pilot group (specified later in this wizard). If you are not ready to move workloads to Intune, select Configuration Manager.
Learn more
Configuration Manager
Pilot Intune
Intune
Compliance policies:
Device configuration:
Endpoint Protection:
Resource access policies:
Client apps:
Office Click-to-Run apps:
OK
Cancel
Apply


CoMgmtSettingsProd Properties
Cloud attach
Configure upload
Enablement
Workloads
Staging
Pilot
When you configure a workload for Pilot Intune, select a device collection to be the pilot group.
Learn more
Make sure your pilot devices are already enrolled into Intune.
Compliance policies:
Browse... (C)
Device configuration:
Browse... (D)
Endpoint Protection:
Browse... (E)
Resource access policies:
Browse... (R)
Client apps:
Browse... (L)
Office Click-to-Run apps:
Browse... (F)
Windows Update policies:
Browse... (W)
OK
Cancel
Apply