Estudio de plataformas MDM en arquitecturas distribuidas

Judit Antoranz García

Resumen—La empresa TMB se encuentra en pleno proceso de adquisición de dispositivos móviles para el parque empresarial, conllevando esto un aumento considerable en la gestión y configuración de los mismos.Con el análisis y estudio de la plataforma utilitzada, VMWare Workspace ONE, se pretende conseguir una mejora cualitativa en la gestión de los dispositives móviles permitiendo una creación de usuarios y grupos con unas características específicas para cada uno, así como la creación e implementación de políticas de seguridad para cada uno de los grupos. Finalmente se pretende conseguir establecer un plan de migración eficaz y eficiente entre los modos de gestión Legacy y Entreprise para los dispositivos Android. Este plan de migración debe permitir migrar los dispositivos al modo Enterprise utilizando el modo Work Managed o el modo COPE. El proyecto resulta beneficioso para la empresa ya que le proporciona soluciones eficientes en la creación de usuarios, Smart Groups, implementación de perfiles de seguridad y migración de dispositivos. Esta eficiencia queda demostrada en la semiautomatización de las tareas y el aumento de la cantidad de dispositivos migrados en una sola operación de migración.

Palabras clave— Mobile Device Management (MDM), políticas de Seguridad, migración de dispositivos, Transports Metropolitans de Barcelona (TMB), VMWare Workspace ONE, Organization Groups, Legacy, Enterprise.

Abstract—The company TMB is in the process of acquiring Mobile devices for the business park, leading to a considerable increase in their management and configuration of devices. With the analysis and study of the platform used, VMWare Workspace ONE, aims to advise a qualitative improvement in the management of Mobile devices allowing the creation of users and groups with specific characteristics for each one, as well as the creation and implementation of security policies for each of the groups. Finally, the aim is to establis han optimal and eficient migration plan between Legacy and Enterprise management modes for Android devices. This migration plan should allow devices to be migrated to Enterprise mode using either Work Managed or Corporate Owned Personally Enabled (COPE) mode. The developed project is beneficial for the company as it provides efficient solutions in the creation of users, Smart Groups, implementation of security profiles and device migration. This efficiency is demonstrated in the semi-automation of tasks and the increase in the number of migrated devices in a single migration operation.

Index Terms— Mobile Device Management (MDM), security policies, Device migration, Barcelona Metropolitan Transport (TMB), VMWare Workspace ONE, Organization Groups, Legacy, Enterprise.

1 Introducción

1.1 ¿Qué son las plataformas MDM?

En la actualidad la mayor parte de las empresas utilizan los dispositivos móviles como una herramienta más de trabajo de la que disponen, a través de la cual utilizan aplicaciones y servicios específicos que ayudan y favorecen el desarrollo de su actividad empresarial. El uso de este tipo de dispositivos ha aportado una serie de ventajas que han favorecido la flexibilidad y movilidad de los trabajadores, así como la eficiencia, eficacia y la reducción de costos en la actividad empresarial. De igual manera esto también ha aportado una serie de desventajas puesto que estos dispositivos tienen que ser gestionados y administrados para un uso correcto y la trata de sus fallos así como la seguridad del dispositivo.

A raíz de este suceso surgieron las plataformas MDM con el objetivo de administrar una gran cantidad y diversidad de dispositivos y usuarios de forma escalable y consistente, incrementando el soporte a dispositivos, su seguridad y las funcionalidades corporativas sin perjudicar el uso del dispositivo para el usuario final.

Así, de forma genérica, se puede definir una plataforma MDM como un conjunto de aplicaciones y configuraciones del dispositivo, políticas corporativas y certificados junto con una infraestructura de backend, con el objetivo de simplificar y mejorar la administración de los dispositivos de usuario final.

Las plataformas MDM (Mobile Device Management) conforman un tipo específico de software que se dedica a la gestión y administración de dispositivos móviles como smartphones, tablets, ordenadores portátiles y ordenadores de sobremesa. Normalmente, estas plataformas se implementan juntamente con productos de terceros, que usualmente pertenecen a los propios productores de los dispositivos a gestionar [1].

- E-mail de contacto: judit.antoranz@e-campus.uab.cat
- Mención realizada: Enginyeria de Computadors
- Trabajo tutorizado por: Eduardo César Galobardes (CAOS – Computer Architecture and Operative Systems)
- Curso 2020/21

El uso de este tipo de plataformas está implementado mayormente en empresas de gran tamaño debido a la complejidad de la gestión de un parque móvil con una gran cantidad de dispositivos, así como la segregación de datos, la securización de emails, documentos y dispositivos empresariales.

1.2 Características de las plataformas MDM

Algunas de las funciones principales de las plataformas MDM son las siguientes y quedan reflejadas de forma resumida en la Fig 1:

- Configurar el dispositivo para un repositorio concreto de aplicaciones y realizar una instalación masiva de estas.
- Configurar el dispositivo para una serie de funciones y políticas de seguridad empresariales específicas.
- Actualización del dispositivo, de las aplicaciones, de las funciones y de las políticas de seguridad.
- Monitorización del equipo para realizar un control del uso de éste.
- Rastreo del equipo para su localización en caso de pérdida o extravío.
- Realizar un diagnóstico de los fallos del dispositivo o de la seguridad que puedan comprometer el dispositivo o los datos sensibles.

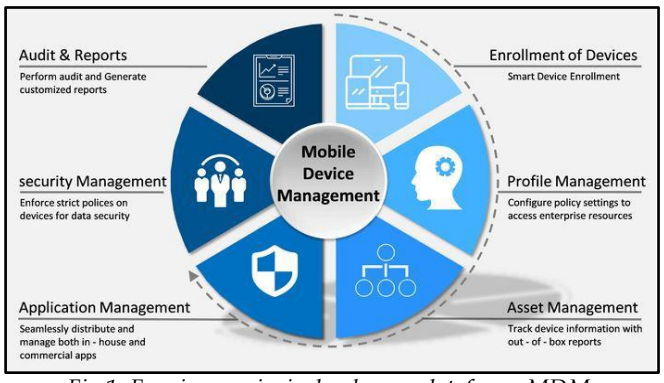


Fig 1. Funciones principales de una plataforma MDM

Principalmente, las plataformas MDM tienen una serie de características comunes en lo que refiere a su arquitectura. Estas están compuestas por:

- Un servidor, a partir del cual se pueden administrar los usuarios, dispositivos, políticas de seguridad y contenido de los dispositivos.
- Un agente cliente, que se instala en el dispositivo móvil para recibir e implementar las instrucciones que se le envían desde el servidor.
- Características de seguridad móvil como [2]:
    - **Secure email:** permite integrar el email corporativo.
    - **Secure docs:** permite la restricción o deshabilita el uso de la copia de documentos fuera del contenedor seguro de la empresa. También restringe el reenvío, el adjuntar o guardar documentos en enlaces externos o dispositivos de memoria extraíbles, maximizando así la seguridad de los datos.
    - **Secure browser:** permite que se eviten la mayor parte de riesgos potenciales mediante el filtrado de URL y el uso del navegador dentro del contenedor seguro de la empresa.
    - **Secure application catalog:** permite a la empresa distribuir, administrar y actualizar aplicaciones en los dispositivos de los usuarios finales usando un repositorio, restringiendo el uso de aplicaciones que podrían comprometer la seguridad tanto del dispositivo como de los datos empresariales.

A parte de las características genéricas, las plataformas MDM también pueden contener una serie de características adicionales, dependiendo siempre del tipo de plataforma elegida. La característica más destacable de éstas, utilizada en la plataforma usada por TMB, es la configuración VPN que permite tunelizar las comunicaciones a través de un proxy seguro.

1.3 Problema a tratar

El problema a tratar en este proyecto surge a causa del gran aumento de dispositivos en el parque móvil de TMB y que éstos necesitan estar gestionados de forma eficiente, generando tipos de perfiles más específicos para cada tipo de departamento adecuándose a las necesidades de cada uno de estos. Otra causa de esta problemática viene dada por la obsolescencia, antes de lo previsto e indicado por VMWare, del modo de gestión Legacy, que obliga a una rápida migración de los dispositivos de un modo a otro con todo lo que ello supone como fallos en la migración, pérdida de capacidad de gestión (debido al uso del modo COPE y la actual ley de protección de datos) o por perdida de funcionalidades debido al nuevo modo de gestión.

El problema que trata este proyecto tiene dos partes bien diferenciadas entre si pero interrelacionadas, una primera parte de análisis de la arquitectura de VMWare Workspace ONE y de la organización a nivel de parque móvil y una segunda parte de realización de perfiles, políticas de seguridad y planes de migración de dispositivos de un modo de gestión a otro.

La primera parte del problema consiste en analizar la arquitectura de la plataforma MDM de VMWare Workspace ONE. Después se deberá analizar cómo está organizada la estructura del parque móvil de TMB dentro de ésta y cuáles son las funcionalidades utilizadas de la plataforma. Algunas de las funcionalidades a analizar serán el proceso de creación de los usuarios y a qué parte de la organización se asignan (Departamento de oficinas, Metro, Bus, etc.), también cómo se dan de alta los dispositivos y qué funcionalidades se permiten que tengan activadas o si el propio dispositivo se incorpora a una whitelist o blacklist. Finalmente como parte más importante se

deben analizar las políticas de seguridad aplicadas a los distintos tipos de usuarios y dispositivos en función de la parte de la organización a la que pertenecen.

La segunda parte del problema consiste en:

- Crear un perfil de usuario.
- Crear un Smart Group para agrupar un conjunto de usuarios.
- Hacer el enrollment de nuevos dispositivos.
- Crear una serie de políticas de seguridad para aplicar a un usuario, dispositivo o a un grupo de cualquiera de estos dos.
- Analizar los dos modos de gestión actuales que existen para dispositivos Android con VMWare Workspace ONE, que son Legacy y Enterprise.
- Dentro de Enterprise existen dos modos diferenciados que son COPE y Work Managed, entre los cuales se deberá decidir cuál de ellos es el más adecuado a aplicar en un conjunto de dispositivos concretos.
- Realizar el diseño de un plan de migración de los dispositivos del modo de gestión Legacy al modo Enterprise.

Este documento que describe la realización del proyecto está compuesto de las siguientes partes descritas en orden:

- Objetivo del proyecto.
- Estado del arte.
- Metodología.
- ¿Qué es VMWare Workspace ONE?
- Desarrollo.
- Resultados y conclusiones.
- Agradecimientos.
- Bibliografía.
- Anexos.

2 Objetivos

A continuación se exponen los diferentes tipos de objetivos de este proyecto, divididos entre generales y específicos, siendo los específicos otros objetivos a conseguir dentro de los generales. Estos son:

- **O.G.1.** Búsqueda de distintas plataformas MDM en el mercado y compararlas con las utilizadas en TMB.
- **O.G.2.** Analizar el problema principal a resolver, que es la migración de los dispositivos del modo de gestión Legacy al modo Enterprise.
- **O.G.3.** Crear usuarios y agruparlos en una OG o Smart Group en función de las características.
    - **O.E.1.** Creación de usuarios y de un manual de usuario sobre la creación.
    - **O.E.2.** Agrupación de usuarios y creación de un manual de usuario sobre la agrupación.
- **O.G.4.** Dar de alta dispositivos y vincularlos a un usuario.
    - **O.E.3.** Dar de alta un dispositivo y creación de un manual sobre cómo dar de alta un dispositivo.
    - **O.E.4.** Vincular un dispositivo a un usuario y creación de un manual de usuario sobre cómo realizar la vinculación.
- **O.G.5.** Análisis de las políticas de seguridad.
    - **O.E.5.** Análisis de las distintas políticas de seguridad aplicadas.
    - **O.E.6.** Analizar para qué colectivos se utiliza una política u otra.
- **O.G.6.** Análisis de los modos de gestión de dispositivos.
    - **O.E.7.** Análisis del modo Legacy.
    - **O.E.8.** Análisis del modo Enterprise.
- **O.G.7.** Definición de un perfil y políticas de seguridad para un dispositivo genérico de personal de oficinas.
    - **O.E.7.** Restricciones de funcionalidad, acceso, datos y aplicaciones para la definición de un perfil o política.
    - **O.E.8.** Definición de una política de seguridad o elección de una ya existente.
- **O.G.8.** Definición de un plan de migración de dispositivos de modo Legacy a modo Enterprise.
    - **O.E.7.** Definición de un plan de migración.
    - **O.E.8.** Realización de la migración para un banco de dispositivos de prueba y realización de un manual de usuario.

3 Estado del arte

Debido al aumento constante en la adquisición de dispositivos móviles, de escritorio y robustos por parte de la gran mayoría de empresas, éstas se han encontrado en la tesitura de tener que gestionar éstos en un parque móvil cada vez mayor. Actualmente existen las plataformas MDM para este tipo de gestión y administración de dispositivos, variando entre ellas el tipo de funcionalidades que poseen.

De todas las plataformas MDM que existen actualmente en el mercado cabe distinguir algunas de ellas en concreto ya que son las mejor valoradas por las empresas que las utilizan. A continuación se describen las plataformas más relevantes y sus principales características y se pueden ver en la Tabla 1 la comparativa entre ellas:

- **Miradore** [5]: es una herramienta que permite administrar los dispositivos de forma sencilla, rápida y barata. Permite dar de alta dispositivos, securizarlos y hacer un seguimiento y gestión para Android, iOS, Windows y MacOS. En lo referente a seguridad de datos, permite crear un contenedor seguro para los datos de empresa. También permite habilitar restricciones y configuración de perfiles para el uso de distintas funcionalidades. Finalmente, permite programar la instalación o actualización de software y la consulta de informes sobre el uso del dispositivo.

- **ManageEngine [6]**: es una herramienta que permite

dar de alta y autenticar dispositivos empresariales de BYOD (Bring Your Own Device) así como configurar perfiles para establecer políticas de seguridad a nivel Wi-Fi o VPN. Permite también el control remoto de los dispositivos para resolución de incidencias y monitorización de estos. En cuanto a la gestión de aplicaciones, permite la distribución y actualización masiva de estas, también tiene un repositorio de aplicaciones de las que realizar la distribución masiva y se pueden crear listas de aplicaciones personales o empresariales.

- **VMWare Workspace ONE** [7]: es una herramienta que sirve para gestionar y distribuir aplicaciones de forma sencilla y segura entre los dispositivos. Permite la gestión unificada de dispositivos móviles, de escritorio, robustos o IoT (Internet of Things) para dispositivos iOS, Android, Windows 10, MacOS y Chrome entre muchas otras. Una ventaja que implementa es el acceso único de inicio de sesión y sin contraseña en las aplicaciones del contenedor seguro. Permite la verificación continua de los usuarios y dispositivos para ofrecer una mayor seguridad. Finalmente, establece y aplica políticas de seguridad de datos y acceso para todas las aplicaciones, dispositivos y ubicaciones.

	Gestión de informes	Gestión de dispositivos	Programación de sincronización	Gestión de software	Gestión de datos
Miradore	X	X	NO	X	X
ManageEngine MDM Plus	X	X	X	X	X
VMWare Workspace ONE	X	X	X	X	X

Tabla 1. Tabla comparativa plataformas MDM

Para la realización de este proyecto se utilizará la plataforma VMWare Workspace ONE, ya que es la plataforma que utiliza la empresa TMB. Esta plataforma se eligió mediante un concurso público para la elección de proveedor de plataforma y servicios.

4 METODOLOGÍA

Para el desarrollo de este proyecto se va a utilizar la metodología KANBAN [3], que consiste en la gestión de trabajo mediante tareas, identificando los recursos que van a ser necesarios para el desarrollo de cada una de éstas, las fechas de inicio y de finalización y los miembros del equipo asignados a cada tarea. Esta metodología maximiza el proceso visual de saber qué hay que hacer, cuándo y la cantidad de trabajo que va a suponer, además de mejorar el proceso evolutivo del proyecto.

Los principales motivos de la elección de esta metodología son:

- Limitar la cantidad de trabajo en curso debido al uso de recursos.
- Facilidad a la hora de realizar el seguimiento del trabajo y comprobar el estado de las tareas [Anexo 1].
- Organizar de forma visual todas las tareas del proyecto [Anexo 2].
- Dirigir y gestionar el flujo de trabajo en función de las necesidades (tiempo, recursos, etc.).
- Observar las posibilidades de mejora de rendimiento en cuanto a la distribución y realización de tareas siguiendo las fechas de entrega de éstas.

La herramienta que se va a utilizar para la organización de las tareas del proyecto es Microsoft Planner [4] por lo explicado anteriormente, además, porque facilita el seguimiento por parte de ambos tutores sobre el estado del proyecto y además permite la compartición de ficheros relacionados con cada tarea.

5. ¿QUÉ ES VMWARE WORKSPACE ONE?

A continuación se va a explicar qué es VMWare Workspace ONE, para qué sirve y cuáles son sus principales características, para así poder comprender mejor cómo se va a desarrollar el proytecto.

VMWare Workspace ONE [8] es una plataforma de trabajo que permite distribuir y gestionar dispositivos móviles y de escritorio de una forma sencilla y segura. Esta plataforma permite gestionar el control de acceso, las aplicaciones instaladas y utilizadas y los propios terminales multiplataforma

Algunas de las características más destacables e importantes de esta plataforma son:

- Permite crear nuevos usuarios y asignarle unas aplicaciones y dispositivos en tiempo rápido.
- Generar y aplicar perfiles de seguridad que garantizan o deniegan el acceso a aplicaciones, dispositivos y ubicaciones.
- Acceso a la información corporativa de forma segura.
- Acceso sencillo y único a todas las aplicaciones del usuario.
- Proporciona unas herramientas de trabajo como email, calendario, archivos y redes sociales.
- Las aplicaciones permiten a los empleados trabajar de una forma más colaborativa en tiempo real ya que se pueden integrar junto con las herramientas que ya utilizan.
- Posibilidad de gestión tanto de dispositivos estrictamente empresariales como dispositivos BYOD, siempre gestionando únicamente el espacio de datos empresariales creado en el dispositivo.
- Acceso sencillo a aplicaciones multiplataforma, ya que una vez se ha autenticado el usuario a través de Workspace ONE tienen acceso al catálogo de aplicaciones empresariales personalizado.
- Acceso único (SSO) y la autenticación multifactor.

- Seguridad de datos debido al acceso condicional, que se consigue mediante la combinación de la gestión de dispositivos y las identidades que permiten garantizar el grado de seguridad de la autenticación, la red, la ubicación y la conformidad de los dispositivos.
- Funcionalidad de automatización y distribución de aplicaciones en tiempo real, ya que aprovecha la tecnología UEM para permitir que se distribuyan de forma automática las aplicaciones y se actualicen sobre la marcha. A esta tecnología además se le une la virtualización de Horizon que mejora la seguridad y la conformidad.

VMWare Workspace ONE es una plataforma que permite realizar la gestión de usuarios, Smart Groups, dispositivos, perfiles de seguridad y migraciones mediante distintos modos de gestión. A continuación se describen los dos modos de gestión principales que se utilizan actualmente, que son el modo Legacy en proceso de obsolescéncia y el modo Enterprise.

5.1 Modo de gestión Android Legacy

El modo de gestión Legacy [9] hace referencia a la integración de dispositivos Android con VMWare Workspace ONE, este tipo de dispositivos pueden optar por no usar el registro con Google y son incapaces de comunicarse con Google Play o utilizan un SO Android 5.0 o inferior.

Con este modo de gestión se puede realizar una serie de tareas, que son las siguientes:

- Se puede establecer políticas de cumplimiento y perfiles de seguridad a grupos concretos o usuarios de la organización empresarial.
- Se puede integrar las apps empresariales con Airwatch Sotware Development Kit para mejorar su funcionalidad.
- Se puede autorizar a los usuarios finales a realizar tareas por si mismos para ahorrar tiempo y recursos.

A pesar de ser un modo de gestión creado para la gestión de dispositivos con SO Android 5.0 o inferior, éste soporta los SO que aparecen en la *Tabla 2*.

SO	4.4.X Kit Kat	5.0.X Lollipop	5.1.X Lillipop	6.0.X Marshmallow
SO	7.0.X Nougat	8.0.X Oreo	9.0 Pie	10.0

Tabla 2. SO soportados por Android Legacy

También cabe indicar que tienen mayor capacidad de administración las OEMs que aparecen en la Tabla 3.

OEMs	Samsung	LG	Lenovo	Barnes and Noble Nook
OEMs	Sony	Panasonic	Intel	Nexus
OEMs	Amazon	HTC	Asus	Motorola

Tabla 3. OEMs soportadas por Android Legacy

¿Qué se puede hacer con Android Legacy?

Configuración de dispositivos:

Se pueden configurar dispositivos con Android Legacy siempre y cuando se cumplan una serie de requisitos:

- **Google ID con su ID de dispositivo correspondiente**: permite integrar y buscar apps en Google Play Store.
- **Permisos de administrador:** permite crear perfiles, políticas y administrar dispositivos con la consola de Workspace ONE UEM.
- **URL para el Enrollment:** dirige directamente al entorno de enrollment y a la pantalla de inicio de este.
- **Group ID:** asocia el dispositivo con el rol corporativo.
- **Credenciales:** autentica al administrador y al usuario en el entorno de Workspace ONE UEM.

Perfiles de Andorid Legacy

Los perfiles aseguran un uso correcto de los dispositivos, protección de datos sensibles y funcionalidad para el puesto de trabajo. Con los perfiles se pueden establecer una serie de restricciones en el uso de los dispositivos, cosa que permite tener diversos perfiles creados para restringir diferentes tipos de funcionalidades en relación con el tipo de usuario que va a utilizar el dispositivo. Hay que tener en cuenta que si se aplican dos o más perfiles con conflicto de restricciones, entonces el dispositivo aplicará la configuración más restrictiva.

Acceso y seguridad del dispositivo:

Se pueden configurar perfiles que aseguren que el acceso al dispositivo está limitado a los usuarios autorizados.

Los perfiles permiten establecer funcionalidades de seguridad que limiten el acceso a datos sensibles como el email, ficheros o contenido empresarial y de igual forma permite tomar acciones administrativas cuando un usuario instala o desinstala aplicaciones concretas.

5.2 Modo de gestión Android Enterprise

El modo de gestión Enterprise [10] hace referencia a la integración de dispositivos Android con VMWare Workspace ONE, este tipo de dispositivos utilizan un SO Android 5.0 o superior.

Para poder usar el modo de gestión Enterprise se necesita cumplir una serie de requisitos, que son los siguientes:

- Usar alguno de los SO Android de la Tabla 4.
- Requisitos de enrollment:
  - Dirección de email corporativa.

  - Credenciales de nombre de usuario y contraseña que garanticen acceso a VMWare Workspace ONE UEM.
- Requisitos de red:
  - Cumplir con los requisitos de las reglas del firewall para dispositivos (poder acceder a ciertos endpoints para garantizar acceso a aplicaciones y servicios).

SO	5.X.X	6.X.X	7.X.X	8.X.X	9.X.X	10.X.X

Tabla 4. SO soportados por Android Enterprise.

Modos de los dispositivos

El modo Enterprise permite configurar completamente los dispositivos para uso exclusivo de trabajo. Los diferentes modos de gestión dependen de la propiedad del dispositivo y son los siguientes:

- **Work Profile:** el dispositivo es BYOD y por tanto crea en él un espacio para los datos y aplicaciones de trabajo que son lo único que se podrá administrar y configurar.
- **Work Managed Device:** restringe el uso del dispositivo para uso corporativo.
  - **COPE:** Es un dispositivo corporativo pero a éste se le crean dos espacios: uno para uso corporativo y otro para uso personal.
  - **Work Managed Device Without Google Play Services:** uso exclusivo corporativo sin acceso a los servicios de Google Play.

Modo Work Profile:

En el dispositivo se encontrarán los iconos diferenciados para las aplicaciones de uso corporativo y las de uso personal, es decir, se podrán encontrar dos iconos de Google Chrome, uno normal para el uso personal y otro con la insignia roja que denota que es para uso corporativo. A pesar de que pueda parecer que se ha instalado dos veces la aplicación, no es cierto, se encuentra instalada una sola vez, con dos iconos generados y con almacenamiento separado para los datos corporativos.

El uso de Workspace ONE Intelligent Hub únicamente existe en el espacio de datos del Work Profile, para garantizar que no hay ningún tipo de control sobre las aplicaciones y datos personales.

De igual manera algunos ajustes muestran la diferencia entre la configuración personal y la corporativa. Las diferentes configuraciones pueden observarse en los ajustes siguientes:

- **Credenciales:** se pueden observar los certificados para la autenticación de usuario en dispositivos gestionados.
- **Cuentas:** se puede observar la Google Account vinculada al Work Profile.
- **Aplicaciones:** se puede observar la lista de todas las aplicaciones instaladas en el dispositivo.
- **Seguridad:** se puede observar el estatus de la encriptación del dispositivo.

Modo Work Managed Device:

En este modo de gestión el dispositivo está gestionado totalmente por VMWare Workspace ONE UEM y en este caso existe únicamente un espacio de datos de uso exclusivamente empresarial.

En este caso el usuario tendrá acceso a las aplicaciones preinstaladas en el dispositivo y que están pendientes de activación. Si el usuario desea instalar alguna aplicación más deberá solicitar permiso al administrador y esta aplicación deberá ser aceptada. Si el dispositivo sufre un unenrolling del modo Work Managed, este sufrirá un autoreset a valores de fábrica.

6. DESARROLLO

Para poder tener una visión más clara sobre las plataformas MDM se crea un entorno de desarrollo y pruebas real en VMWare Workspace ONE para poder ver reflejada toda la parte práctica realizada. Para poder realizar todos los objetivos, hay que distribuir el proyecto en diversos aparados para su desarrollo, se distribuirá de la siguiente forma:

- Se generarán, en el modo de gestión Legacy, unos usuarios para unos empleados de nuevo ingreso en la empresa (O.G.3. y O.E.1.).
- Se crearán diversos Smart Groups para agrupar a los usuarios según unos criterios establecidos (O.G.1 y O.E.2.).
- Se asignarán y darán de alta los correspondientes dispositivos móviles correspondientes (O.G.4.).
- Se crearán unos perfiles de seguridad para aplicarlos a los Smart Groups (O.G.5 y O.G.7.).
- Se crearán unos planes de migración de esos dispositivos al nuevo modo de gestión Enterprise (O.G.6 y O.G.8.).

Para realizar todo lo mencionado anteriormente, ha sido necesario un perfil de superusuario para la creación, gestión y actualización de todo el banco de pruebas existente. Para realizar las configuraciones y alta se han utilizado unos dispositivos móviles Samsung Xcover 4.

6.1 Creación del entorno de pruebas

Inicialmente se creó un espacio personal de trabajo dentro de la estructura de trabajo de TMB en VMWare Workspace ONE para poder desarrollar ahí el banco de pruebas para el proyecto. Dicho banco de pruebas tiene una nomenclatura propia para que este se pueda diferenciar del resto de departamentos, la nomenclatura es "ZZZ-TFG-Antoranz". En el interior de esta OG, que está dentro de la OG principal de la empresa, se han creado dos OG hijas para poder separar y diferenciar los elementos que pertenecerán al modo de gestión Legacy y los de

Enterprise.

6.2 Creación de los usuarios

Después de tener creada la estructura principal, se procedió a crear los usuarios del banco de pruebas, que son usuarios asignados a un directorio empresarial para ser gestionados ahí. Para poder crear los usuarios deben cumplirse unos prerrequisitos previos como son la existencia del directorio al que se les va a asignar, políticas de contraseña configuradas y atributos de usuario requeridos para el directorio concreto. Una vez creado el usuario, éste deberá crear una contraseña nueva para él y el usuario será añadido a los grupos existentes en función de los atributos que el usuario y el grupo comparten.

Los usuarios siguen la misma nomenclatura que la OG en la que se trabaja y por tanto sus nombres son "ZZZ-TFG-Antoranz-UserX" y así sucesivamente para cada uno de los 5 usuarios que se crearon. En este caso se decidió crear 5 porque se consideró que eran usuarios suficientes para realizar todas las pruebas necesarias.

El proceso de creación de los usuarios se describe detalladamente en el manual de usuario creado, aunque en dicho proceso existen unas pautas comunes para la creación de cualquier tipo de usuario. La estructura básica de un usuario es la que se puede observar en el Anexo 3.

6.3 Creación de los Smart Groups

Una vez se tuvieron creados los usuarios se crearon los Smart Groups necesarios para contener a un grupo de usuarios en él. Un Smart Group es un grupo configurable, en el cual se puede determinar las plataformas, dispositivos, usuarios que podrán pertenecer a él. Estos Smart Groups siempre deben pertenecer a la estructura corporativa.

La nomenclatura de los Smart Groups es la misma que la del resto de la OG del proyecto, siendo por tanto para cada Smart Group "ZZZ-TFG-Antoranz-Smart Group X". Inicialmente se vincularon los usuarios 1 y 2 al Smart Group 1, los usuarios 3 y 4 al Smart Group 2 y finalmente, el usuario 5 al Smart Group 3.

El contenido y estructura de un Smart Group necesario para el proyecto es el que se puede observar en el Anexo 4.

6.4 Device Enrollment

Posteriormente se hizo el Device Enrollment, que consiste en dar de alta primero un dispositivo dentro de la infraestructura empresarial para luego ser asignado a un usuario concreto y así poder ser gestionado y mantenido. En este caso el Enrollment se ha realizado a través de Intelligent Hub ya que permite la automatización de la mayor parte del proceso de Enrollment del dispositivo, reduciendo al máximo la interacción del gestor con la plataforma ya que sólo deberá introducirse la dirección de email del usuario para realizar el Enrollment.

Una vez más la nomenclatura sigue igual, siendo ésta "ZZZ-TFG-Antoranz-UserX's Device" para cada uno de los dispositivos. Estos tuvieron que ser dados de alta con su correspondiente IMEI y número de serie para vincular un dispositivo concreto a un usuario. Una vez indicados estos dos elementos del dispositivo, se tiene que asignar un usuario al dispositivo. Una vez se haya hecho esto, le llegará un email al usuario para confirmar que la vinculación se ha hecho de forma correcta.

6.5 Creación de los perfiles de seguridad

Finalmente se crearon dos perfiles de seguridad [11], uno para los dispositivos gestionados mediante Android Legacy, como se puede observar en el Anexo 5 y otro para los dispositivos gestionados mediante Android Enterprise. Aunque a rasgos generales podrían parecer dos perfiles muy similares, existen entre ellos algunas diferencias que son clave para ver la mejora que supone realizar la gestión con Android Enterprise respecto a hacerla con Android Legacy. Algunas de estas características permiten diferenciar en el modo Enterprise entre un dispositivo Work Managed y uno BYOD. Las opciones para un dispositivo de tipo Work Managed siempre serán más restrictivas respecto a un BYOD, puesto que un dispositivo de tipo BYOD conlleva que es un dispositivo tanto de uso corporativo como para uso personal. En el caso de un dispositivo BYOD, a causa de la ley de protección de datos, no podrán realizarse ciertos controles de gestión del dispositivo ya que es el propio usuario el que proporciona el dispositivo.

6.6 Creación de un plan de migración

Una vez creados todos los usuarios, que éstos habían sido asignados a un Smart Group, que se había realizado el Enrollment de los dispositivos vinculándolos a sus correspondientes usuarios y se habían creado y aplicado los perfiles de seguridad a todos los Smart Groups se procedió a realizar la migración de los dispositivos del modo de gestión Legacy al modo Enterprise. Para poder realizar esta migración se crearon dos OG dentro del entorno de pruebas, una para los dispositivos gestionados en modo Legacy y otro para los gestionados en modo Enterprise. Primero se configuró la OG de Enterprise para que al realizar un Enrollment de dispositivo este fuese en modo Enterprise y posteriormente se modificó la OG que gestionaba los Smart Groups para que fuese la correspondiente a Enterprise.

Cuando todos estos pasos estuvieron realizados se pudo realizar la migración propiamente dicha, como se puede observar en la Fig 2. La migración se pudo realizar de dos modos distintos, que están explicados detalladamente en el manual de usuario. Uno de los procesos de migración lo hará como "Work Managed" [12] y el otro como "Work Profile" [13]. En ambos procesos de migración, una vez finalizada esta se debe comprobar que ésta se había realizado correctamente mediante la com-

probación de dos campos que son “Platform” y “Android Management” en los que debe aparecer “Android” que indica que es Android Enterprise, sino aparecería como “Android (Legacy)” y en el segundo campo deberá aparecer “Work Profile” para tener la segunda confirmación que se está gestionando mediante Enterprise.

7. Resultados y conclusiones

Después del desarrollo del proyecto fue cuando se pudo realizar el análisis de los resultados obtenidos. Inicialmente se pudo observar que todas las tareas eran

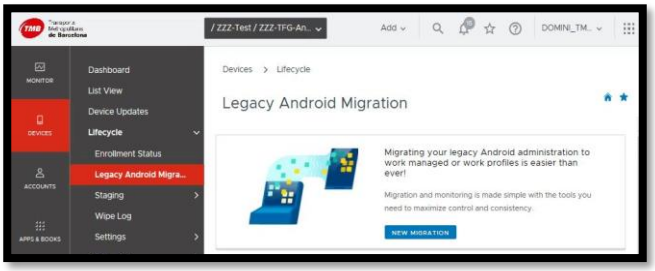


Fig 2. Pantalla de inicio de creación de un nuevo plan de migración.

sencillas de realizar siempre y cuando el administrador tuviese una base sólida de conocimientos de la plataforma MDM.

En lo referente a la creación de usuarios se pudo observar que esta es fácilmente mecanizable, ya que sólo hay que introducir unos datos básicos del usuario a crear y todos ellos ya son conocidos por la empresa. Además posee la ventaja que se puede relacionar con la de vinculación directa de un dispositivo si en vez de realizar un guardado directo se accede a la opción de “guardar y añadir un dispositivo”.

La tarea de creación de Smart Groups, debido al método que usa la empresa para la creación de los Smart Groups, que es mediante la opción de “Devices or Users”, permite vincular y añadir a un Smart Group unos usuarios o dispositivos ya dados de alta en el sistema. En algunos casos la empresa utiliza el tipo de creación mediante “criteria” que es más complejo. En este se deben seleccionar unos criterios concretos mediante los cuales se añadirían usuarios y/o dispositivos a un Smart Group y además permite añadir un dispositivo o usuario concreto mediante la pestaña "Additions".

En la tarea de Enrollment de los dispositivos se debía realizar el Enrollment de los dispositivos y este debe hacerse en dos pasos: uno inicial en la plataforma MDM en la que se indicaban los datos correspondientes al dispositivo y para los cuales se necesita acceso a ciertos datos del dispositivo como su IMEI y una segunda parte en la que se debe actuar directamente sobre el dispositivo. Es en esta segunda fase en la que se encontraron algunos problemas puesto que en el caso que no se posea, debe crearse una Google Account para el usuario para poder descargar la app Intelligent Hub para realizar el Enrollment. Posteriormente se debe asegurar una conexión a Internet fiable en el proceso de Enrollment del dispositivo para que el proceso no sufra interrupciones, ya que puede llegar a quedarse bloqueado en algún punto y tener que hacerle un hard reset al dispositivo para poder volver a comenzar a hacer el Enrollment.

Para la realización de la tarea de creación de perfiles de seguridad hay que tener en cuenta una gran cantidad de casuísticas antes de realizar los perfiles. Primeramente debe tenerse claro cuál va a ser el ámbito en el que se van a usar los dispositivos y cómo van a estar estos gestionados, ya que se podrán permitir accesos a ciertas apps o datos a un grupo de empleados del departamento de RRHH pero en cambio estos no podrán tener acceso a documentación referente a la operativa que se lleva a cabo en LLAA (Líneas Automáticas) en caso de incidencia. También hay que ser conscientes del modo de gestión de dicho dispositivo ya que no será tratado del mismo modo un dispositivo BYOD de un director de departamento que un dispositivo Work Managed de un Técnico de Operación de Líneas Automáticas. Además hay que saber que a los dispositivos Samsung se les podrían aplicar directrices extras debido a Samsung Knox, pero en este proyecto no se ha abarcado esta posibilidad. Una vez conocidos todos los permisos, prohibiciones y modo de gestión del dispositivo se deben marcar todas y cada una de las casillas de cada elemento, como puede ser la autorización del uso de la cámara de fotos o poder acceder a páginas externas a la intranet empresarial. Este proceso es muy laborioso porque hay cientos de elementos a considerar y además para cada modo de gestión no están todos estos mismos elementos disponibles, cosa que dificulta el poder crear un perfil de seguridad único.

La última tarea que se realiza es el plan de migración de los dispositivos. Esta debe ser la última puesto que es necesario haber realizado todas las otras tareas para poder realizar ésta de forma correcta y sin tener que repetir el proceso. En este caso se encontraron algunas dificultades en el proceso de desarrollo puesto que de inicio se pensaba que se podría realizar la migración de dispositivos de una forma más automatizada y directa, pero en cambio, cuando se quiso realizar la migración del modo Legacy al modo Enterprise Work Managed se descubrió que no podía hacerse mediante la herramienta de migración, ya que esta sólo permite realizar una migración a “Work Profile” para cualquier tipo de dispositivo válido o bien permite hacer una migración a “Work Managed” pero sólo para dispositivos Zebra después de haber obtenido un vertificado Zebra para la empresa. Esto permitió observar que sólo podían hacerse dos cosas para poder migrar los dispositivos.

La primera es contraria a la metodología de trabajo de la empresa y consiste en migrar todos los dispositivos a modo “Work Profile”. Este modo que genera dos perfiles en el dispositivo, uno personal y otro de trabajo, cosa que dificulta y merma las capacidades de gestión y control de dispositivos empresariales debido al perfil perso-

nal en el dispositivo. En el perfil personal no se puede acceder a esa parte de los datos debido al hecho de que son de carácter personal y se incurriría en una violación de la Ley de Protección de Datos.

El segundo modo de migración de los dispositivos implica, debido a que no se puede realizar con la herramienta de migración automática, tener que realizar un Enterprise Wipe para todos y cada uno de los dispositivos. Esto, en cierta manera, puede automatizarse y realizarse en todos los dispositivos a la vez seleccionando todos los dispositivos a los que se le quiere realizar el Enterprise Wipe y realizándolo con el PIN del administrador en todos ellos una vez han sido selecciónados. La siguiente fase implica que después de realizar el Enterprise Wipe hay que realizar de nuevo el Enrollment de todos los dispositivos en modo Enterprise, cosa que es tremendamente laboriosa ya que estamos hablando de miles de dispositivos móviles y esto implicaría una cantidad de tiempo o de recursos humanos grandiosa. Además habría que comprobar que en todos y cada uno de los OG a los que pertenecen los dispositivos se puede realizar el Enrollment en modo Enterprise y en caso de no ser así debería modificarse esto en todos los OG o bien establecerlo el OG principal y hacer que fuese hereditario para todos los OG hijos.

Durante la realización de todas las tareas se ha visto que la organización de la plataforma es muy buena en lo siguiente:

- Permite una especificidad muy grande para poder realizar OG que sólo contienen a un grupo de empleados de un departamento.
- Perfiles de seguridad específicos que sólo sean aplicables a unos dispositivos que cumplan con unas características concretas.

Pero también tiene algunos errores que la llevan a perder efectividad y eficiencia en el uso de sus recursos, algunos de estos son:

- Los perfiles de seguridad específicos limitan la aplicación de perfiles de seguridad generales (la plataforma siempre aplica el perfil más restictivo).
- La dificultad de la migración automatizada y global ya que no se ha encontrado el modo de hacerlo mediante la herramienta de migración, cosa que implica un uso excesivo de horas en la migración así como un uso excesivo de recursos humanos para su realización.

Se podría concluir diciendo que en general el uso y aplicación de las distintas opciones que permite la plataforma MDM son correctos y eficaces, pero que estos podrían ser mucho mejores si se realizasen algunas tareas de otro modo o se investigase, mediante contacto directo con VMWare, cómo podría realizarse la migración a Android Enterprise de forma automatizada mediante la herramienta de migración o algún otro elemento de migración disponible en la plataforma.

AGRADECIMIENTOS

Me gustaría agradecer a Eduardo Cesar Galobardes toda su atención y motivación proporcionada no solo durante la realización de este Proyecto, sino durante todo mi desarrollo académico universitario. Igualmente me gustaría agradecer a todo el profesorado y en especial a los pertenecientes al departamento de CAOS todo el conocimiento y apoyo que han mostrado y brindado.

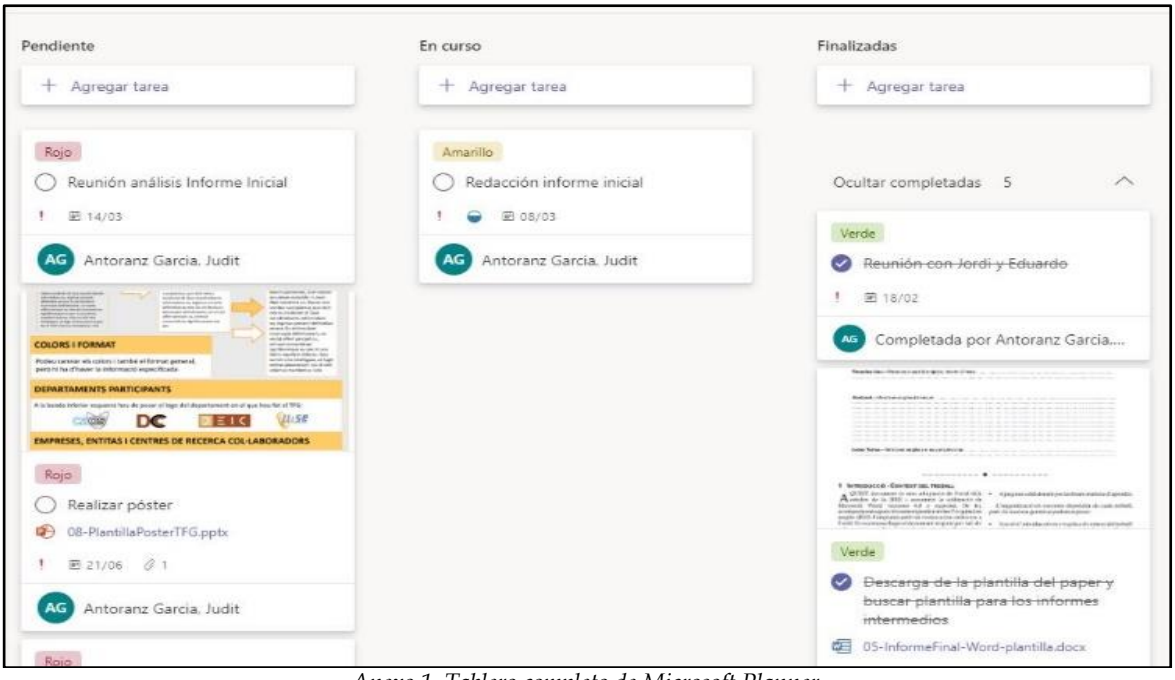
También me gustaría hacer una mención a mi tutor en la empresa, Jordi Esteve ya que me ha apoyado muchísimo y ayudado en todo lo que he necesitado y además, a Joan Carles Gallego por haberme ayudado a conseguir la oportunidad de poder realizar el TFG en TMB.

BIBLIOGRAFIA

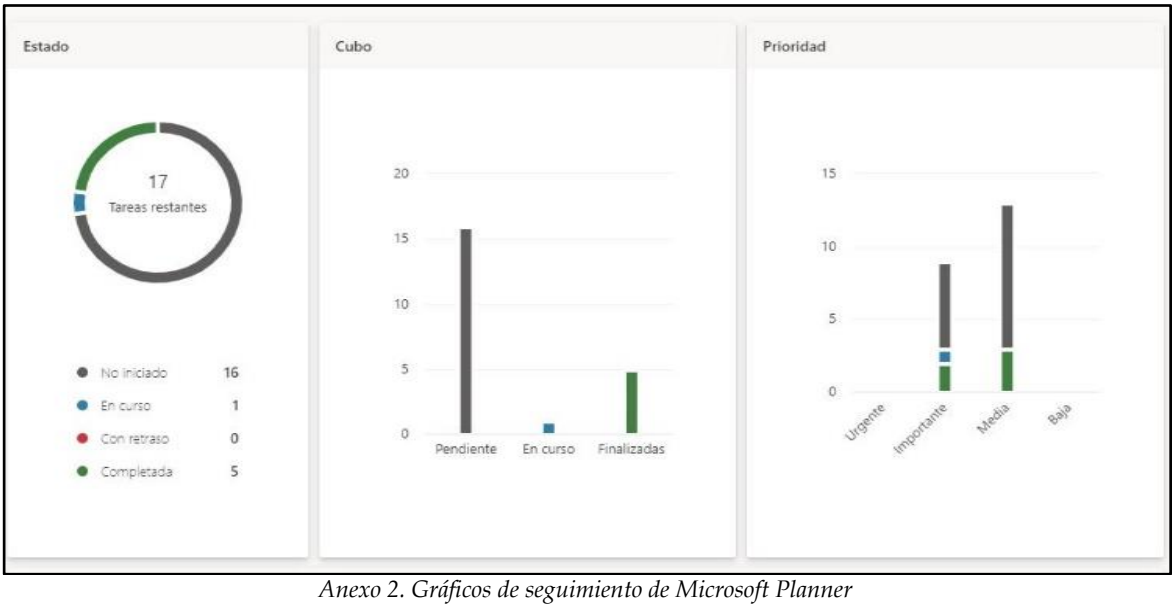
[1] Markus Pierer. Mobile Device Management. https://www.etonline-digitallibrary.com/bitstream/123456789/2169/1/1220.pdf. Pages 27-28, Springer Vieweg, 2016. Springer Fachmedien Wiesbaden.
[2] Workspace ONE UEM Architecture. https://techzone.vmware.com/resource/workspace-one-uem-architecture
[3] Metodología KANBAN https://es.wikipedia.org/wiki/Kanban_(desarrollo)
[4] Uso de Microsoft Planner https://support.microsoft.com/es-ES/office/build-your-plan-88716b3a-da46-43c0-8770-8b93e8c0959c?ui=es-ES&rs=es-ES&ad=ES#ID0EABAAA=Planes
[5] MDM Miradore https://www.miradore.com/es/
[6] MDM ManageEngine https://www.manageengine.com/es/
[7] MDM VMWare Workspace ONE https://www.vmware.com/es/products/workspace-one.html
[8] ¿Qué es VMWare Workspace ONE? https://www.vmware.com/content/dam/digitalmarketing/vmware/es/pdf/products/workspace-one/vmware-workspace-one-datasheet.pdf
[9] Modo de gestión Android Legacy https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/2001/WS1_Android_Legacy_Platform.pdf
[10] Modo de gestión Android Enterprise: https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/2001/WS1_Android_Platform.pdf
[11] Perfiles de seguridad: https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/1909/UEM_Managing_Devices/GUID-AWT-DEVICEPROFILESOVERVIEW.html
[12] Migration to Enterprise: https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/Android_Platform/GUID-AndroidMigrationLegacyMigrationConcept.html
[13] Migration tool : https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/Android_Platform/GUID-AndroidMigrationMigrateUsingMigrationTool.html

APÉNDICE

A1. USO DE MICROSOFT PLANNER

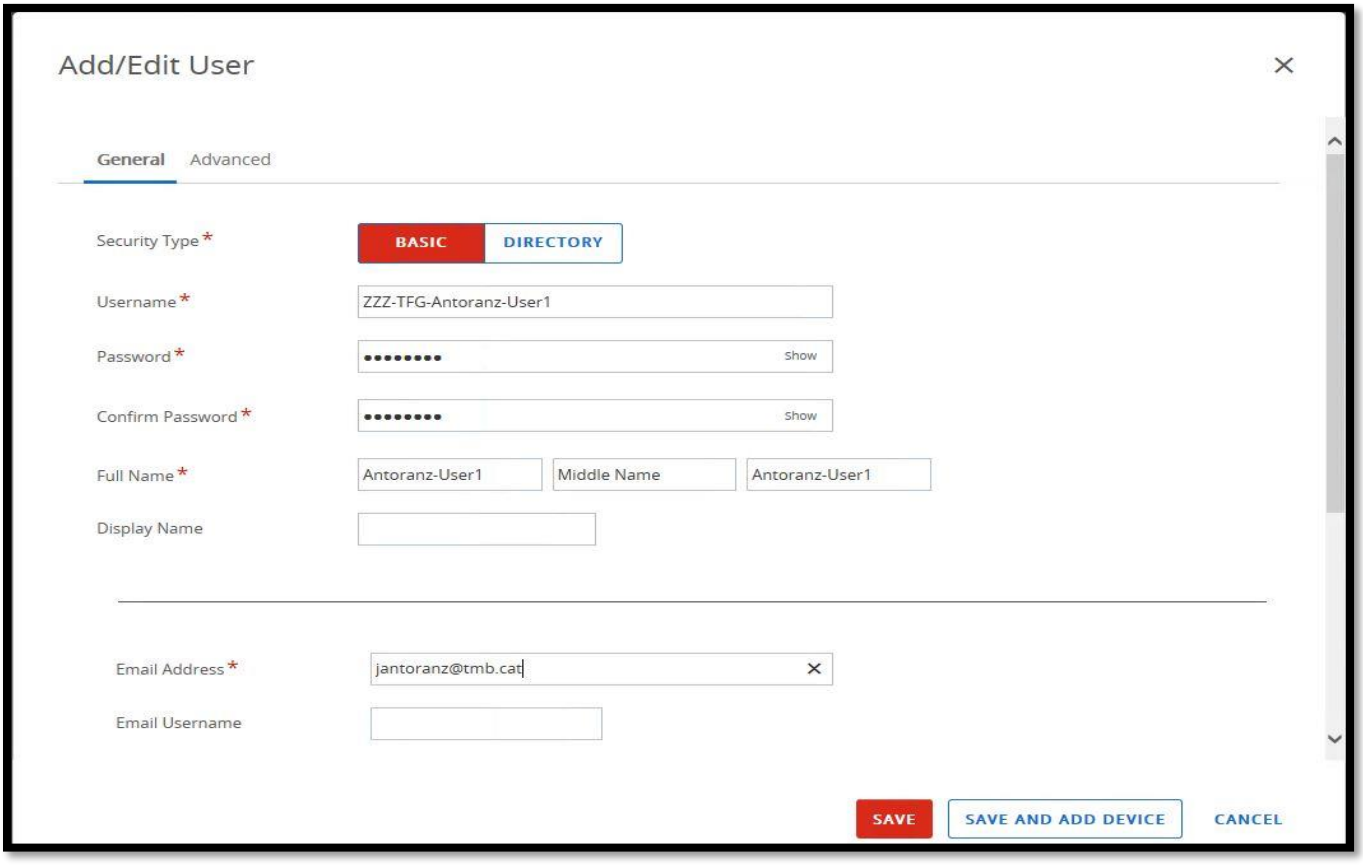


Anexo 1. Tablero completo de Microsoft Planner



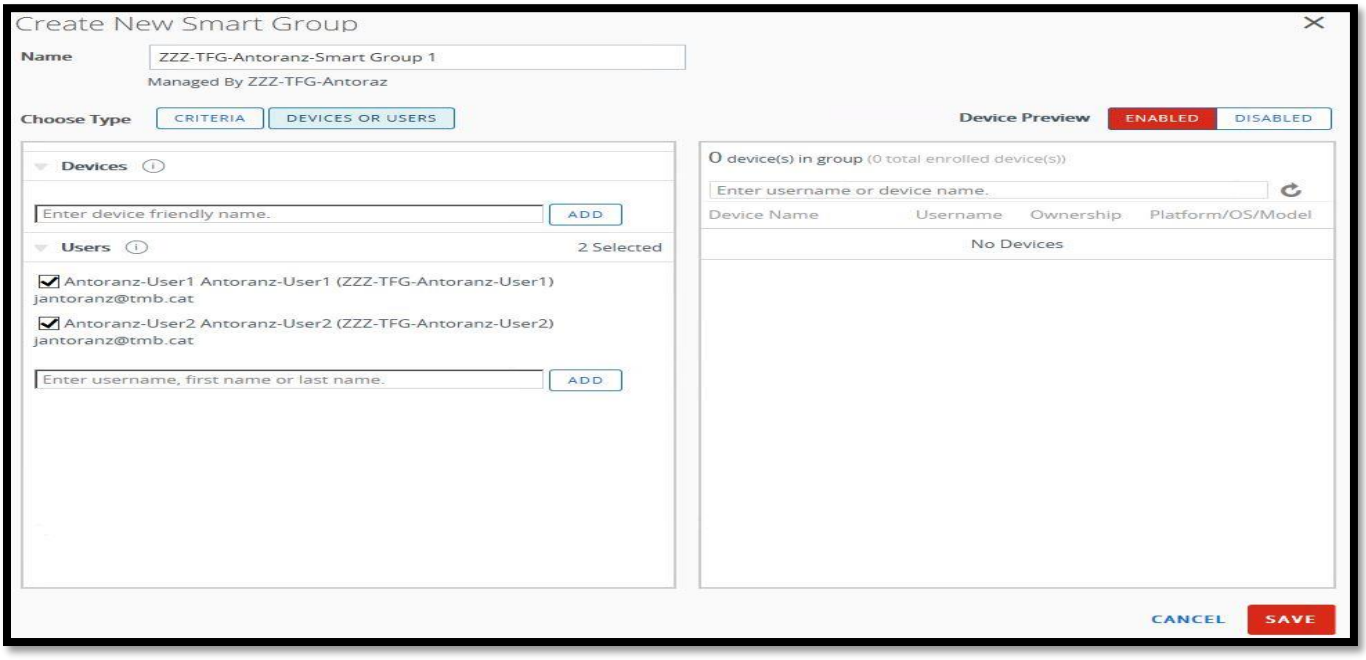
Anexo 2. Gráficos de seguimiento de Microsoft Planner

A2. CREACIÓN DE LOS USUARIOS



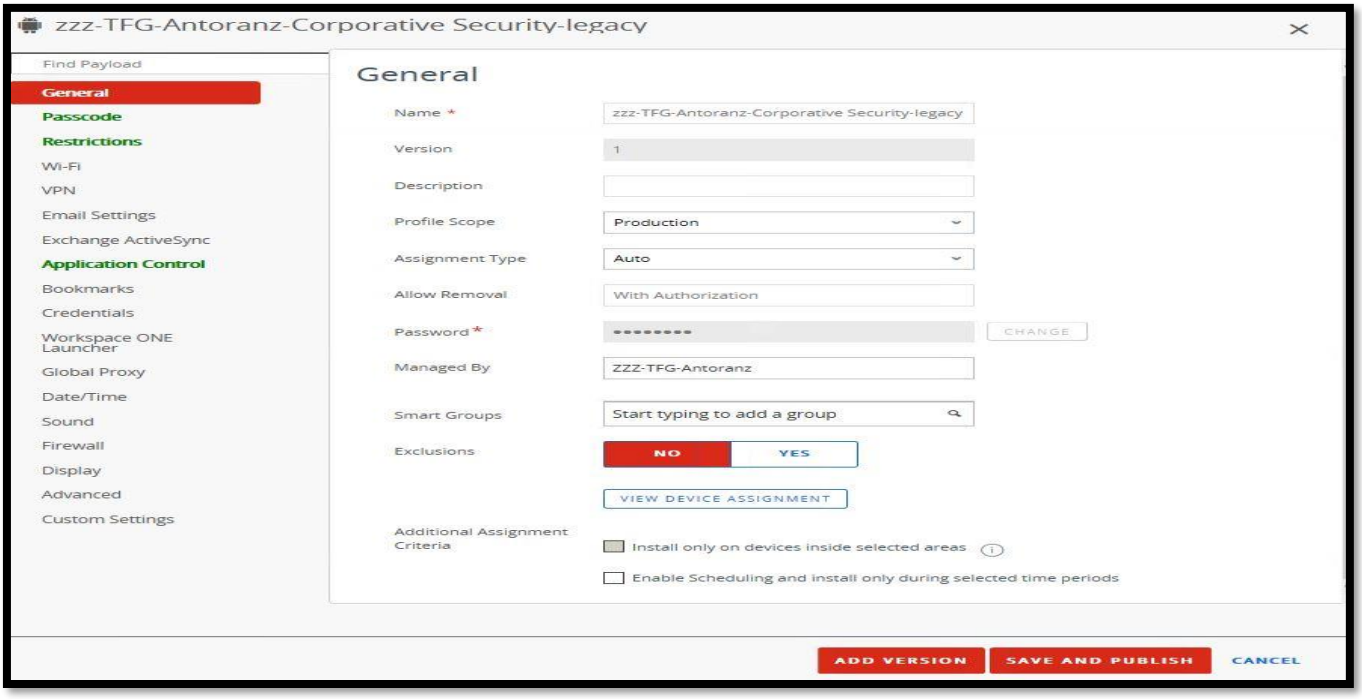
Anexo 3. Estrucutra básica de un usuario.

A3. CREACIÓN DE LOS SMART GROUPS



Anexo 4. Estructura básica de un Smart Group

A4. CREACIÓN DE UN PERFIL DE SEGURIDAD



Anexo 5. Estructura básica de creación de un perfil de seguridad.