

Ciclo
Administración de Sistemas Informáticos en Red

Proyecto
Software MDM (Mobile Device Management)

Alumno
Ernesto Álvarez Siles

Índice

[Introducción y justificación](#)

[Objetivos](#)

[Análisis del contexto](#)

[Desarrollo del contenido](#)

[Protocolo de despliegue](#)

[Fase de inicio.](#)

[Fase de estudio.](#)

[Fase de implementación](#)

[Operaciones y mantenimiento](#)

[Fin de ciclo](#)

[Ejemplos de aplicaciones MDM](#)

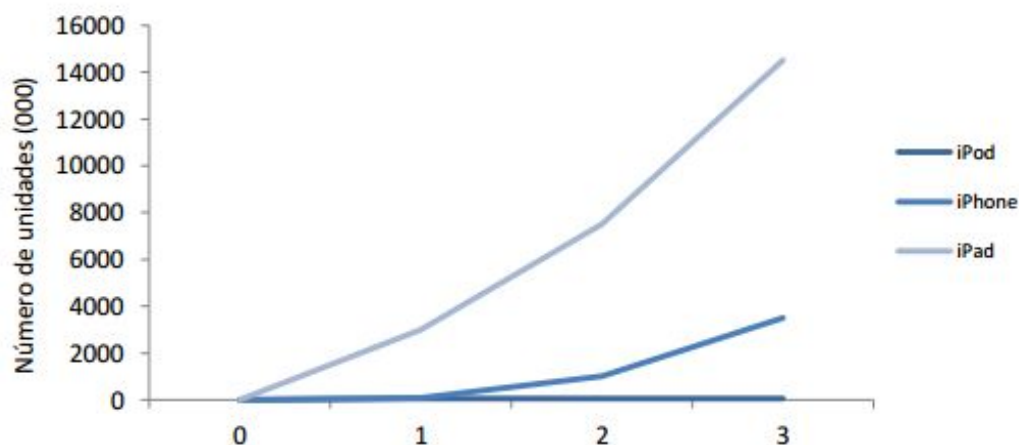
[Conclusión y valoración personal](#)

[Bibliografía y fuentes de consulta](#)

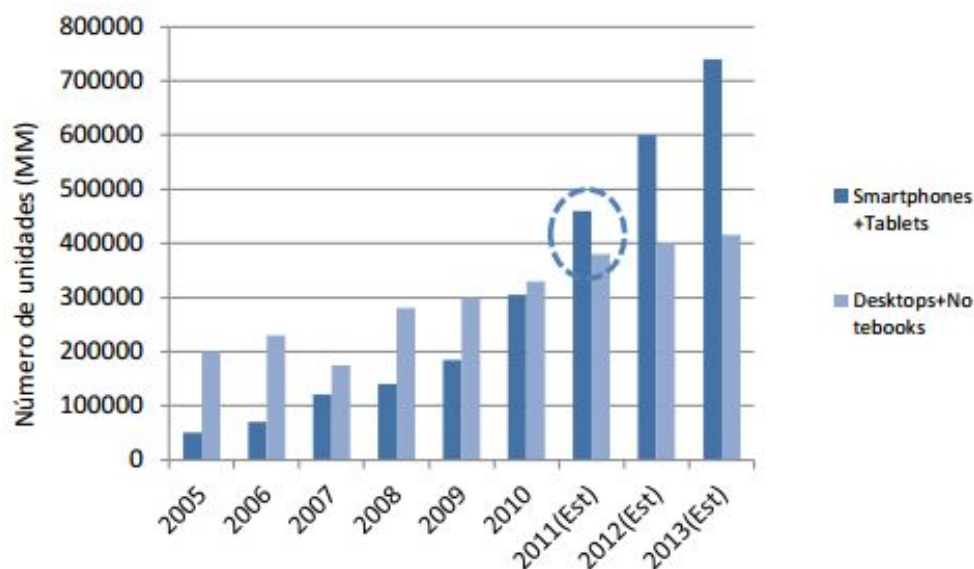
Introducción y justificación

La proliferación y el uso de forma común de dispositivos móviles (teléfonos inteligentes, tabletas...) por parte de la mayoría de la población y la diversidad de aplicaciones que hoy en día existen para dichos dispositivos, permiten darle un uso intensivo por parte de los usuarios en los más diversos escenarios, tanto de ocio como de trabajo o en los estudios.

Los usuarios quieren acceder a Internet independientemente de su localización y del dispositivo que estén usando. El siguiente gráfico muestra la tendencia y aceleración de esta mentalidad: iPad, en un trimestre, llegó al nivel de ventas que a iPhone le costó tres trimestres conseguir (Fuente: Apple).



En el año 2011 la venta de Pc's y notebooks se vió superada por la de smartphones y tablets. Teniendo en cuenta los tiempos de reposición, se estima que en este año el parque desplegado de dispositivos móviles sea superior al de Pc's. (Fuente: Informe KPBC - Top 10 mobile trends).



Esta evolución, terminará por sustituir las actuales aulas de informática existentes en colegios e institutos, a las que el alumno se tiene que desplazar con la consiguiente pérdida de tiempo y el ruido generado, molestando a los demás alumnos del centro, por las tabletas que tienen sobre lo anterior la ventaja de ser dispositivos personales que lleva el alumno consigo y que puede utilizar en todo momento, además de un menor coste de mantenimiento e incluso del propio dispositivo.

En el ámbito de la enseñanza también han visto en las tabletas y su amplio mercado de aplicaciones unas enormes posibilidades educativas y una oportunidad de ayudar a aumentar la productividad de los alumnos.

En centros educativos con un número significativo de alumnos que utilicen este tipo de aparatos diariamente, se hace engorrosa la tarea de actualizar dichos dispositivos con nuevas versiones o con nuevas aplicaciones si se hace de uno en uno. Por lo tanto, es imprescindible la ayuda de este tipo de aplicaciones que permiten la actualización e instalación masiva de aplicaciones a distancia y en todos los dispositivos a la vez o a elección del administrador, la monitorización de la actividad de los alumnos en cuanto a su uso, la localización en caso necesario, la seguridad, sincronización de archivos, borrado remoto, etc. , la gestión de las aulas por parte de los profesores y el uso de los dispositivos por parte de los alumnos según los parámetros definidos por el profesor.

Objetivos

El objetivo de este proyecto es analizar las prestaciones de dichas aplicaciones, denominadas MDM (Mobile Device Management), realizar una comparativa teniendo en cuenta varios parámetros y que dicho estudio nos ayude a decidir cuál de ellas nos convendría más usar en nuestro ámbito concreto y según nuestras necesidades. En el caso que nos ocupa, la enseñanza, para cubrir dichas necesidades el software debe permitir o debe cumplir las siguientes especificaciones o prestaciones:

- Administración centralizada de grupos de usuarios/dispositivos (administradores, profesores y alumnos) que se puedan utilizar para asignar políticas de seguridad, reglas de conformidad, ubicaciones, configuración de privacidad y distribuir aplicaciones y documentos.
- Distribución de aplicaciones por parte del administrador.
- Políticas de seguridad independientes por grupo de dispositivos definidas por los profesores y distribuidas por el administrador, por ejemplo políticas de contraseñas de desbloqueo de las tablets.
- Reglas de conformidad definidas por los profesores y que los dispositivos tienen que cumplir en todo momento. Las reglas de conformidad se definen a partir de las políticas de seguridad.
- Registro de conformidad a revisar por el administrador, que indica si efectivamente los dispositivos han sido actualizados para cumplir las reglas de conformidad..
- Informes de estado de los dispositivos
- Inventario de dispositivos.
- Inversión a realizar para conseguir la funcionalidad deseada.

Una vez realizada la comparativa y teniendo en cuenta el mercado al que va destinado, llegaría el momento de elegir cuál de las aplicaciones se adapta más como

apoyo al uso de tabletas en los IES y cómo aplicarlo mediante un protocolo de instalación que puede agruparse en cinco fases bien definidas:

- Fase de inicio: Identificación de necesidades según las características del centro, número de dispositivos, tipo de alumnado, etc.
- Fase de estudio de la solución: Estudio del grado de cumplimiento del MDM con las necesidades del centro, definidas en la fase anterior.
- Fase de implementación: Apoyándose en el MDM configurar e instalar todo el software necesario para su uso en las aulas.
- Operaciones y mantenimiento: Uso diario de dispositivos y solución de la problemática que puede surgir con dicho uso, como olvido de contraseñas, actualización de apps, etc....
- Fin de ciclo: Reinicio de dispositivos para asignación a nuevos alumnos o reciclado según las normas medioambientales en caso de desecho.

Análisis del contexto

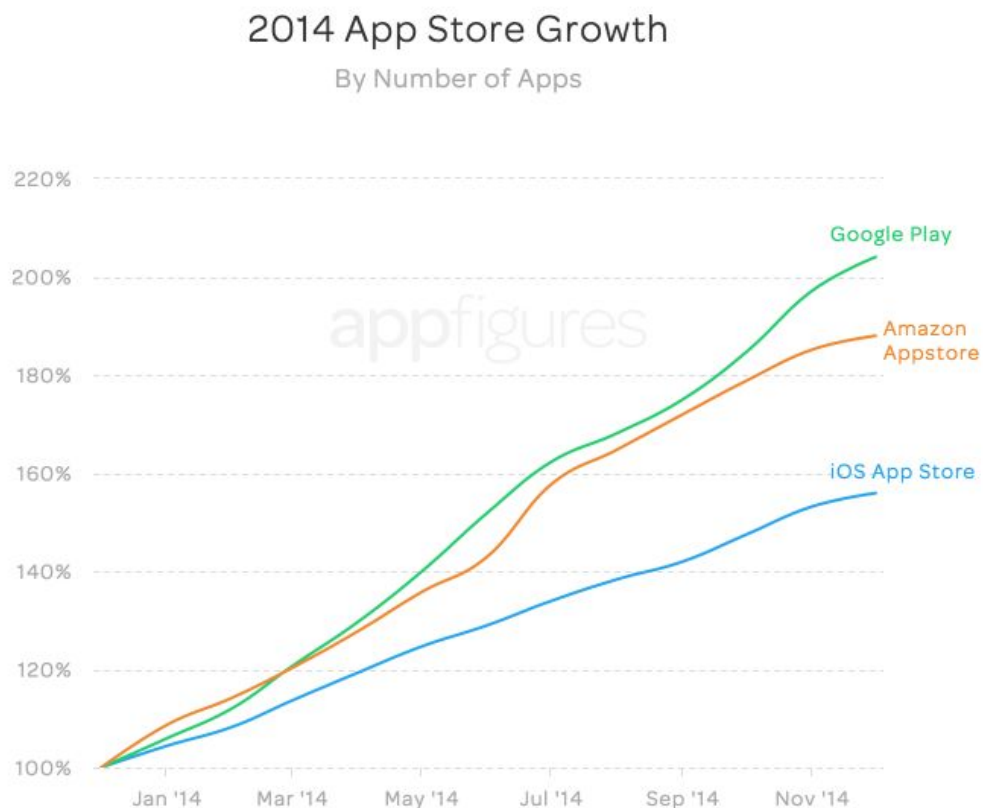
En el mercado actual existen una gran cantidad de estas aplicaciones de los tipos más diversos (gratuitas, de pago, con períodos de prueba) y con diferentes prestaciones (geolocalización, selección, instalación y actualización de aplicaciones, sincronización de archivos, etc.). Algunas empresas incluso han aprovechado esta diversificación para sacar sus propias líneas de producto que han denominado EMM (Enterprise Mobile Management). Este tipo de aplicaciones son horizontales, por lo que pretenden abarcar el mayor número de “targets” (objetivos) o clientes potenciales posibles. Esto quiere decir que hay que buscar siempre un compromiso, válido para el cliente, entre posibilidades del software y la forma de hacer las cosas por parte del cliente.

En nuestro caso, relacionado con la educación en los institutos de enseñanza secundaria, nos basamos en un contexto “tipo” generalizado, dando por hecho que se ha discutido con el TIC y el personal docente del centro cuáles son las necesidades concretas y qué se espera obtener de la implantación de un sistema de estas características, llegando a las siguientes conclusiones:

- Existen tres niveles de usuario dependiendo del rol o papel que desempeña cada uno: Administrador, Profesor y Alumno. La figura del administrador es imprescindible, ya que existen muchas funciones que están centralizadas en el uso de los MDM y que debe llevar a cabo una persona con buenos conocimientos de funcionamiento del software, descargando así de responsabilidades a los profesores. Los profesores definen qué es lo que se pretende obtener del uso de estas soluciones y los alumnos son los usuarios finales y los grandes beneficiados de esta forma de trabajo.
- Los dispositivos a usar serían tabletas de 10.1 pulgadas con sistema operativo Android, propiedad del centro. La elección de este tipo de dispositivo se debe al compromiso adecuado entre manejabilidad y tamaño y entre prestaciones + valor añadido y precio. En el siguiente gráfico se ve cómo ya en el 2014 Google Play superó a App Store en número de aplicaciones disponibles



En el gráfico siguiente se puede ver cómo en la tasa de crecimiento de las diferentes tiendas de aplicaciones, Google Play es la que crece más rápidamente.



- Debe existir una tableta por cada alumno, el cual se hace responsable del cuidado de la misma, así como de su carga para garantizar la disponibilidad.
- En cada tableta se deberá configurar una cuenta de correo electrónico, ya que es el medio mediante el cual el software realiza el registro (enrollment) del dispositivo en las bases de datos del servidor, además de ser imprescindible para la descarga de cualquier aplicación necesaria de los repositorios de aplicaciones de Google. En el caso de alumnos de edad inferior a 14 años, se deberá contar con el consentimiento del padre, madre o tutor según el artículo 13 de la LOPD.
- Los usuarios pertenecientes al grupo de administradores del servidor se deberán encargar del registro de los dispositivos en el servidor, altas de usuarios, definición de grupos de usuarios, grupos de dispositivos y

distribución de aplicaciones, para lo cual es recomendable una reunión al inicio del curso escolar.

- Los usuarios pertenecientes al grupo de profesores sólo se deberán encargar de verificar el cumplimiento de las políticas de seguridad de los dispositivos (el software cliente se encarga de indicar el grado de cumplimiento de cada dispositivo), distribuir documentos entre dispositivos o bien comunicar a los administradores cualquier cambio posterior en aplicaciones a instalar o eliminar y cambios en las políticas de seguridad.
- Los usuarios pertenecientes al grupo de alumnos son los responsables del mantenimiento de los dispositivos, así como de aplicar los cambios en las políticas de seguridad (sólo hay que seguir los pasos indicados por el cliente de la aplicación), actualizar los contenidos e instalar las aplicaciones. Todo esto lo indica el software cliente y tiene asistentes para realizar estas tareas fácilmente. También hay que tener en cuenta que hoy en día los alumnos, aunque sean de 13 años, están muy familiarizados con el uso de estos dispositivos.
- En definitiva, lo que se busca es tener un control total sobre las tabletas supervisado por administradores y profesores.

Todo esto hace que la enseñanza sea más productiva, dinámica, participativa y adaptada a las necesidades de cada clase, evitando pérdidas de tiempo por parte del profesorado realizando tareas de administración.

Desarrollo del contenido

La arquitectura de este tipo de software normalmente consiste en un agente, que se instala en cada uno de los dispositivos, un servidor desde el que se realizan las instalaciones, actualizaciones, etc. y una base de datos que almacena toda la información recabada de los dispositivos móviles.

Protocolo de despliegue

Para enfrentarse a la implantación hay que tomarlo como un proyecto con cinco fases:

- Fase de inicio.

Esta fase incluye las tareas que un centro debe realizar antes de diseñar una solución para dispositivos móviles: Identificar las necesidades de dispositivos móviles (cuantos se necesitan) y proporcionar una visión general de cómo debe adaptarse una solución de software a las necesidades del centro, dando forma a las políticas de seguridad y requerimientos funcionales. Esta fase de inicio la deben realizar entre el profesorado y los administradores. Se realiza una única vez y no es necesario repetirla hasta que por cualquier circunstancia se detecte que la solución adoptada ha quedado obsoleta.

- Fase de estudio.

Aquí se especifican las características técnicas del software y sus componentes, incluyendo los métodos de autenticación y cifrado para la protección de las comunicaciones y datos almacenados. También hay que evaluar los distintos tipos de dispositivos y sistemas operativos que van a ser usados y que se verán afectados por las políticas de seguridad definidas. En esta fase se deben elegir los elementos que se usarán en la implementación, tanto hardware como software, y la realizarían conjuntamente profesores y administradores. Al igual que la fase anterior, se realizaría una única vez y no se repetiría a menos que se detectase la obsolescencia de la solución elegida.

- Fase de implementación

En esta fase se configuran los equipos para que cumplan los requerimientos funcionales y de seguridad, incluidas las políticas de seguridad, instalando y comprobando el funcionamiento de un dispositivo piloto, incluyendo las restricciones en la navegación definidas por el proxy del centro educativo. Esta fase la realizarían los administradores y sería supervisada por el profesorado. Se debería realizar al comienzo de cada curso antes del comienzo de las clases.

- Operaciones y mantenimiento

Esta fase abarca la vigilancia por parte del profesorado del cumplimiento de las políticas de seguridad por parte de los alumnos (instalación y configuración de los dispositivos por parte de los alumnos según las indicaciones del software cliente MDM del dispositivo mediante mensajes push) y funcionamiento e idoneidad de las aplicaciones elegidas para su uso. Esta fase estaría vigente durante todo el curso.

- Fin de ciclo

Esta fase tiene lugar cuando hay que reasignar las tabletas a otros alumnos procediendo a su borrado e instalación limpia de sistema y aplicaciones, o bien los dispositivos han finalizado su vida útil y hay que definir las acciones a tomar para el cumplimiento de la legalidad vigente en cuanto a materia medioambiental a la hora de proceder a su destrucción o reciclado. El administrador sería la figura encargada de esta fase y se realizaría al final de cada curso.

Ejemplos de aplicaciones MDM

Existen muchas opciones en el mercado. A continuación se nombran las más utilizadas con algunas de sus características más importantes:

- AirWatch MDM



Multiplataforma (iOS, Android, Windows Phone).

Licencia de pago. Prueba gratuita 30 días.

Consola de administración única.

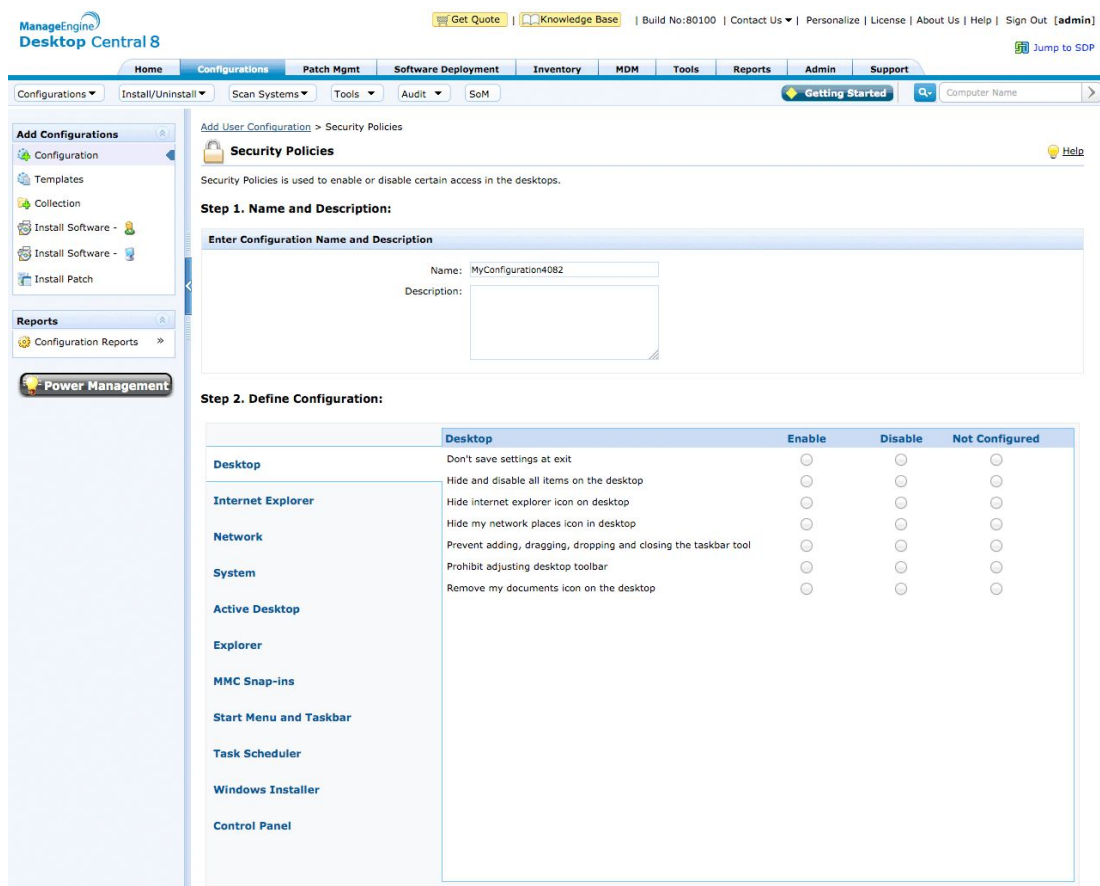
Administración de aplicaciones móviles.

Administración de contenido móvil.

Administración de correo electrónico móvil.

Administración de navegación.

– Manage Engine MDM



Multiplataforma (iOS, Android, Windows Phone).

Licencia gratuita hasta 1 técnico y 25 dispositivos.

Registro manual o autoregistro con dos niveles de autenticación.

Administrador de aplicaciones.

Administrador de perfiles.

Administrador de seguridad.

Administrador de correo electrónico.

Administrador de inventario.

Auditorías e informes.

Soporta autenticación Active Directory.

– **MobileEther MDM**



Protección de dispositivos móviles y seguridad web en una única solución.

Control de redes sociales.

Administrador de aplicaciones.

Monitorización y seguridad de datos en la nube.

Integración con Active Directory.

Soporta Apple DEP (Device Enrollment Program).

Cumplimiento preciso de políticas de seguridad.

– **SysAid MDM**



Inscripción de dispositivos Android e iOS de forma inalámbrica (OTA), tanto del centro como de los alumnos (BYOD).

Crear, asignar y modificar políticas personalizadas para los dispositivos.

Empleo de configuración WiFi y de correo electrónico creados previamente.

Aplicación de código de acceso que permite resetear, bloquear y borrar los dispositivos.

Trazabilidad de las aplicaciones instaladas con aplicación de monitorización

Protección de datos críticos.

– **Spiceworks MDM (Maas360)**



Este software permite:

- Tener un inventario de todos los dispositivos móviles en un sólo lugar. Soporta iOS, Android y Windows Phone. Registrando un dispositivo móvil obtiene toda la información del aparato, como tipo de dispositivo, sistema operativo utilizado, etc.
- Monitorear los dispositivos obteniendo información actualizada en tiempo real, pudiendo saber las aplicaciones que se instalan, etc., incluso creando alertas para dispositivos desactualizados, códigos de acceso deshabilitados, etc.
- Crear informes y estadísticas personalizadas de uso, averías, etc.

La versión de pago (Premium) permite, además de las características anteriores:

Bloquea y borra dispositivos perdidos o robados. Además puede usar la característica del portal MaaS360 que permite cambiar los códigos de acceso, gestionar la configuración del dispositivo e incluso establecer un contenedor de correo seguro para proteger los datos de los usuarios.

- Autenticar usuarios en Active Directory con códigos de acceso de un sólo uso, configurar políticas de cumplimiento para administrar el comportamiento del usuario, controlar fácilmente cuentas de correo electrónico, acceso WiFi y VPN.
- Acceso a aplicaciones corporativas o aplicaciones aprobadas por el administrador, con la posibilidad de distribuir y administrar fácilmente dichas aplicaciones en todos los dispositivos, incluso creando listas blancas / negras de aplicaciones según sea necesario para satisfacer la política móvil del centro de enseñanza.

En la tabla de la página siguiente se puede deducir de una forma objetiva el grado de cumplimiento del software respecto a las necesidades:

Característica / Software	Descripción comentario
Registro sencillo mediante correo electrónico	Los dispositivos se registran en la base de datos mediante servicios de mensajes, correo electrónico o un URL personalizado.
Autenticación LDAP	Proporciona acceso mediante el Protocolo Ligero de Acceso a Directorios.
Registros masivos	Inscripción de tabletas en la base de datos de registros, de forma masiva
Configuración correo	Gestión centralizada del correo electrónico
Configuración calendario	Gestión centralizada del calendario
Configuración Wi-Fi	Gestión centralizada de las conexiones Wi-Fi a las que la tableta puede tener acceso
Restringir cámaras	Habilitar o deshabilitar elementos de hardware o características como captura de pantallas.
Restablecer contraseñas	Obligar a los usuarios a establecer o restablecer contraseñas de acceso a las tablets
Soporte por control remoto	Para proporcionar soporte del centro de atención al usuario
Localizar dispositivos	Proporciona la ubicación de cualquier tableta basándose en GPS
Bloquear dispositivos	Puede enviar remotamente una orden de bloqueo de la tableta para que haya que introducir de nuevo la contraseña de acceso.
Limpieza selectiva	Limpiar de forma selectiva datos proporcionados por el centro, dejando intactos los del usuario. Ideal para entornos BYOD.
Reglas de conformidad en tiempo real	Crear reglas de conformidad en tiempo real con acciones automatizadas, por ejemplo, forzar a establecer una contraseña.
Portal de ayuda entre usuarios	Portal de autoservicio que permite que los usuarios se ayuden entre ellos.
Resúmenes gráficos de actividad	Utilización de paneles de instrumentos de inteligencia de movilidad para obtener resúmenes gráficos de operaciones y conformidad

Informes inventario hardware	Informes detallados de inventario de hardware, agrupando si se quiere mediante características, como versión del Sistema Operativo, marca o modelo de la tableta.
Informes inventario software	Informes detallados de inventario de software, indicando las qué apps están instaladas en qué dispositivos, etc.
Vistas de dispositivos para diagnosticar y resolver problemas	Vistas predefinidas en el panel de control para poder diagnosticar y resolver problemas en las tablets.
Precio	La mayoría de los fabricantes dan precio mediante presupuesto personalizado. No aparecen precios en las webs.

Característica / Software	Maas360	AirWatch MDM	SysAid MDM
Registro sencillo mediante correo electrónico	Si	Si	Si
Autenticación LDAP	Si	No especificado	No especificado
Registros masivos	Si	No especificado	Si
Configuración correo	Si	Si	Si
Configuración calendario	Si	Si	No especificado
Configuración Wi-Fi	Si	Si	Si
Restringir cámaras	Si	No especificado	No especificado
Restablecer contraseñas	Si	Si	Si
Soporte por control remoto	Si	No especificado	No especificado
Localizar dispositivos	Si	Si	Si
Bloquear dispositivos	Si	Si	Si
Limpieza selectiva	Si	Si	Si

Reglas de conformidad en tiempo real	Si	Si	Si
Portal de ayuda entre usuarios	Si	No	No
Resúmenes gráficos de actividad	Si	Si	Si
Informes inventario hardware	Si	Si	Si
Informes inventario software	Si	Si	Si
Vistas de dispositivos para diagnosticar y resolver problemas	Si	Si	No
Precio	Preguntar	13.000€/año*	Preguntar

* El precio contempla la versión más económica para 250 dispositivos.

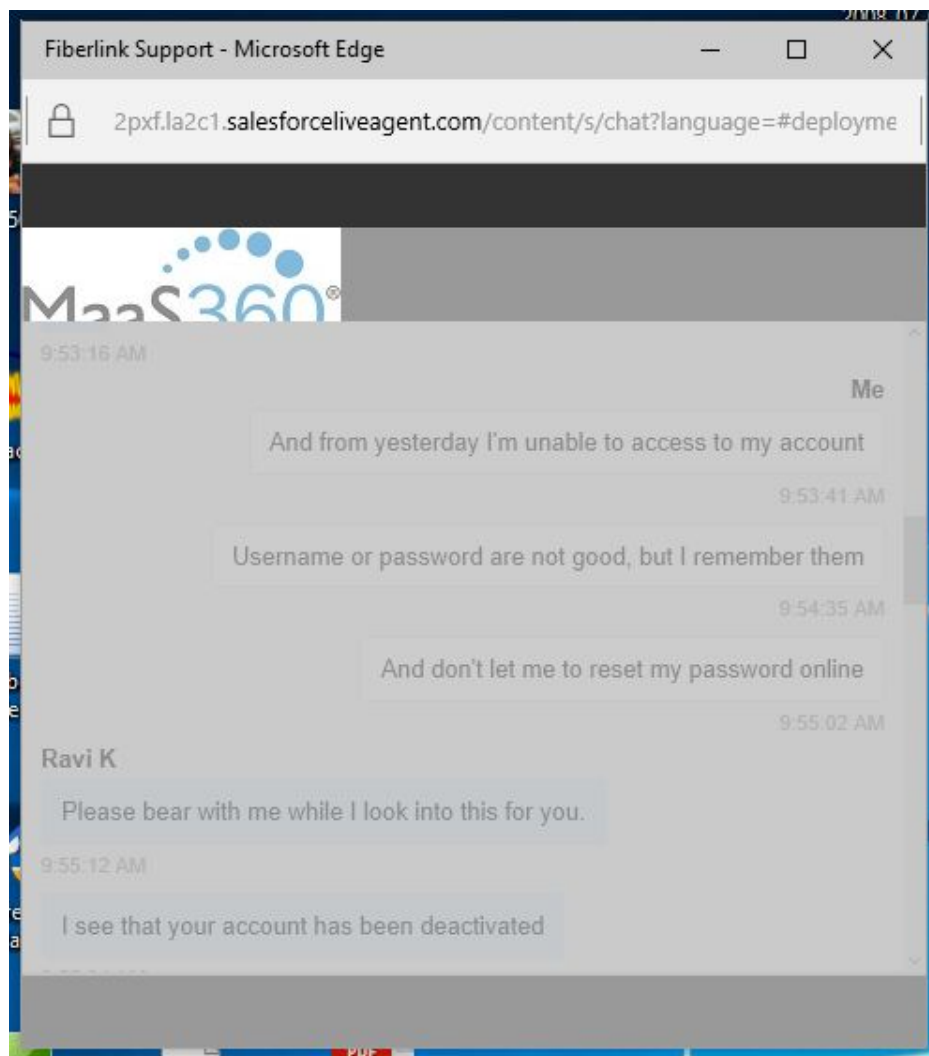
Como ejemplo de uso, en un documento anexo se ha realizado la instalación y algunas pruebas de la versión gratuita del software Spiceworks MDM, basado en MaaS360 (desarrollado por Fiberlink, una compañía de IBM), ya que, además de gratuita, parece ser lo suficientemente completa como para satisfacer nuestras necesidades. La instalación se realiza tanto en el servidor como en un smartphone Android y tableta Apple.

Conclusión y valoración personal

La digitalización de la educación es un hecho desde hace unos años. El propio Ministerio de Educación ha invertido muchos recursos en su programa Escuela 2.0, un proyecto de integración de las Tecnologías de la Información y Comunicación en los centros educativos, creando las aulas digitales dotando de recursos TIC a los alumnos y profesores (ordenadores personales, pizarras digitales interactivas, etc), garantizando la conectividad a Internet, y promoviendo la formación del profesorado. La inclusión de las tabletas en el aula gestionadas por un software MDM sería el siguiente paso lógico para la digitalización de la educación, que aunque todavía hay pocos proyectos en marcha, cada vez son más las empresas que ven en esta parcela de mercado una oportunidad de negocio debido a la expansión que se puede prever en la implantación de estas soluciones en los centros educativos.

En las webs consultadas, es bastante difícil averiguar detalles muy concretos sobre el funcionamiento del software, ya que las compañías intentan que se contacte con ellos para programar demos online y así ofrecer sus mejores argumentos de venta para justificar el elevado precio de estas soluciones. La mayoría de ellos aseguran tener precios especiales para entornos educativos, pero es imposible de averiguar si no es mediante un presupuesto personalizado, para lo cual suelen pedir los datos del cliente final, incluido C.I.F.

Esta filosofía se lleva hasta tal extremo que al mes de crear la cuenta de prueba la han deshabilitado, obligando a contactar con ellos para poder habilitarla de nuevo. En la imagen se ve el fondo gris porque es como se queda la pantalla del chat una vez el interlocutor ha cerrado la sesión:



Bibliografía y fuentes de consulta

https://es.wikipedia.org/wiki/Mobile_device_management

<http://www.telecomunicacionesparagerentes.com/10-soluciones-de-gestion-de-dispositivos-moviles-mdm-para-entornos-byod-i/>

<http://www.spiceworks.com/free-mobile-device-management-mdm-software/>

<https://portal.fiberlink.com/emc/>

<https://www.air-watch.com/es/soluciones/administracion-de-dispositivos-moviles>

<https://www.manageengine.com/mobile-device-management/>

https://resources.iboss.com/mobile_security/mdm_mobileether.html

<https://www.sysaid.com/es/it-service-management-software/it-asset-management/mobile-device-management>

<http://atsistemas.com/expresat/2013/02/como-implantar-sistema-de-gestion-de-dispositivos-moviles-mdm/#>

<http://www.ite.educacion.es/escuela-20>