SOFTWARE MDM ORIENTADO A EDUCACIÓN

I.E.S. Leopoldo Queipo

Elio Cabrera Piñar

Contenido

Introducción y justificación

En los últimos años los dispositivos móviles han ido introduciéndose poco a poco en el ámbito educativo hasta llegar al punto de haberse convertido en una herramienta fundamental para la construcción de conocimiento e incrementar el nivel de interactividad con los alumnos. Eso por eso que surge la necesidad de

administrar, monitorizar y asegurar dichos dispositivos. Para cubrir esta necesidad aparece el **software MDM** (Mobile Device Management).

A lo largo de proyecto trataremos de comprender, evaluar y comparar las distintas soluciones existentes para gestionar dispositivos móviles.

El software MDM nos permitirá administrar, monitorizar y asegurar nuestro inventario de dispositivos móviles de una forma centralizada y homogénea; solucionando así, el problema de fragmentación que ocurre al intentar gestionar grupos de dispositivos de distintas plataformas y/o hardware como son los dispositivos móviles.

En las siguientes páginas, definiremos una serie de necesidades suponiendo que vamos a necesitar administrar dispositivos móviles en el ámbito educativo.

También compararemos las distintas soluciones existentes en el mercado y elegiremos la más adecuada, elaborando después un análisis exhaustivo de sus capacidades, así como ilustrando algunos ejemplos de uso en un centro educativo real.

Objetivos

A continuación definiremos los objetivos que el software elegido tendrá que satisfacer, nos centraremos en el control de contenidos, la seguridad y la posibilidad de gestionar usuarios con distintos roles.

- Usuarios y roles. La solución elegida tendrá que ser capaz de gestionar múltiples usuarios, asociados o no a un dispositivo con distintos permisos según rol. Como mínimo necesitaremos tres roles: **Alumno, Profesor y Administrador.**
- Gestión remota del dispositivo. Actualizaciones de software, bloqueo de pantalla, cambio de contraseña, instalación remota y masiva de aplicaciones, reestablecer a valores de fácbrica, etc...
- Monitorización. Informes de aplicaciones instaladas, ubicación del dispositivo, estado (batería, almacenamiento, encedido/apagado), control de la navegación…
- Seguridad. Detección de dispositivos modificados (root/jailbreak), alertas en base a ubicación, software obsoleto y demás.
- Compartir dispositivos. Puede darse el caso de que en una determinada clase haya más alumnos que dispositivos disponibles.

Usuarios y roles

Tal y como hemos comentado, necesitaremos tres roles con capacidades distintas que procedemos a explicar:

- Alumno. El alumno no debería tener acceso a ciertas características del dispositivo, así como cambiar ciertos ajustes o modificar los datos de otro alumno en caso de que el dispositivo sea compartido.
- Profesor. El profesor debería ser capaz de:
    - Bloquear / desbloquear dispositivos

- Enviar notificaciones Push a uno o varios alumnos (por ejemplo, mandar un enlace).
- Activar / desactivar y cambiar ajustes del dispositivo, como por ejemplo localización, conexión wifi, etc…
- Restringir los contenidos disponibles, es decir, controlar la navegación web estableciendo listas blancas o negras, establecer las apps disponibles para descargar / usar, etc…
- Monitorizar la actividad del dispositivo. Controlar el estado del dispositivo (apagado o encendido, ubicación, estado de la batería, almacenamiento, etc…)
- Enviar archivos a los dispositivos.
- Enviar mails de forma masiva a los alumnos.
- Bloquear, cambiar la contraseña o borrar dispositivos.
- Forzar la instalación de aplicaciones de forma remota.

- Administrador. Además de todos los privilegios del profesor, el administrador además podrá:
  - Gestionar usuarios y permisos (tanto alumnos como profesores).
  - Añadir y eliminar dispositivos.
  - Establecer políticas comunes a grupos de usuarios.

Análisis del contexto

El auge de los dispositivos móviles

Como ya hemos comentado antes, el auge de los dispositivos móviles ha transformado la sociedad, cambiándola de forma significativa en todos sus ámbitos, incluyendo el educativo.

Los dispositivos móviles nos permiten estar conectados de forma permanente, en cualquier parte, y esto nos ofrece gran cantidad de nuevas herramientas para docentes y alumnos. Para aprovechar todas estas nuevas herramientas cada vez más centros dotan a sus alumnos de dispositivos para uso durante las clases, de forma que el docente puede enriquecer la sesión con material interactivo y audiovisual. Del mismo modo, los alumnos pueden entregar ejercicios y colaborar e intercambiar información de forma inmediata.

Esta nueva situación nos plantea la necesidad de que exista un control y monitorización de todos los dispositivos, sin olvidar la gestión remota; ya que gestionar de forma individual los dispositivos sería ineficiente además de una pesadilla logística.

Al igual que ocurre con otros dispositivos, como PC's y portátiles, la aproximación más eficiente será la de disponer de un software que nos permita llevar a cabo las tareas de administración y gestión de forma centralizada y homogénea para los dispositivos móviles independientemente de su plataforma, versión y hardware.

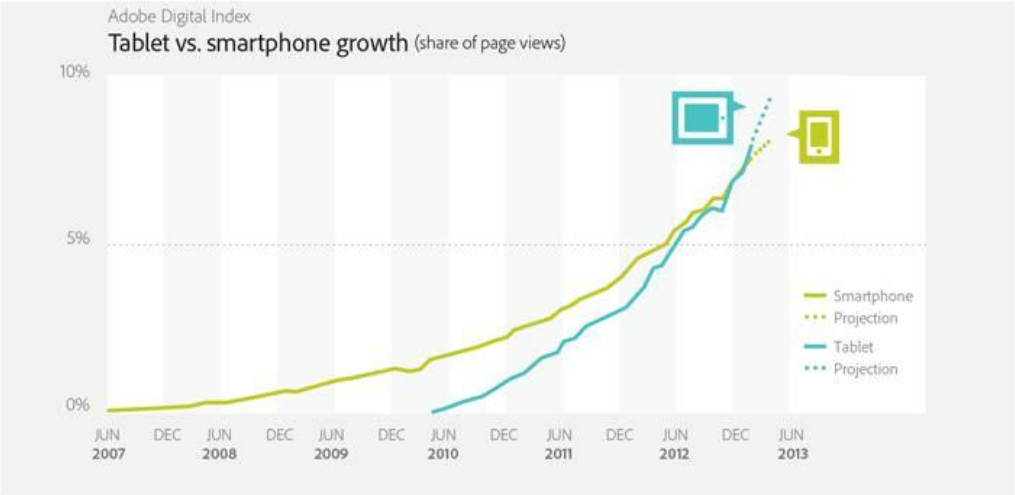


Figura 1. Crecimiento de smartphones y tablets de 2007 a 2013

Estado del mercado

A fin de tener los criterios adecuados a la hora de seleccionar la solución que más se ajuste a nuestras necesidades, primero estudiaremos cuáles son las plataformas más extendidas en nuestro país, ya que las plataformas más utilizadas gozarán de más software disponible, soporte y conocimiento del usuario.

Sistemas Operativos más usados en España

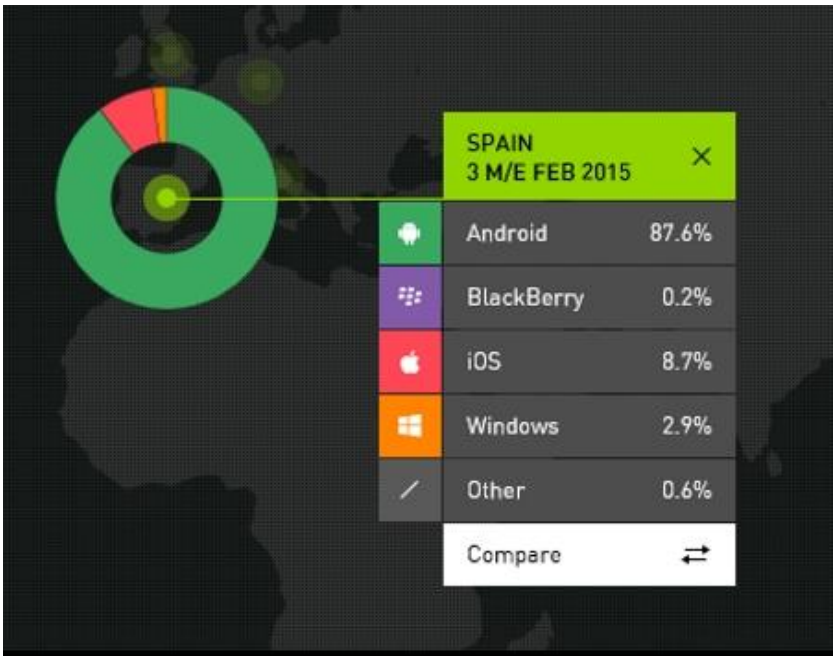


Figura 2. Cuota de mercado en España.

Como se puede apreciar, en nuestro país el Sistema Operativo dominante es Android, seguido muy de lejos por iOS, esto debe a una mayor cantidad de dispositivos Android existentes en el mercado y a otros factores que no comentaremos por alejarse demasiado del ámbito de nuestro proyecto.

En cualquier caso, entre los dos principales SO's suman un 96.3% de cuota de mercado, por lo que podemos descartar los demás por ser irrelevantes.

Desarrollo del contenido

Como ya hemos comentado, el objetivo de este proyecto es comparar y evaluar las distintas soluciones que existen y elegir la más adecuada a los objetivos planteados.

Para esto hemos elegido varios candidatos que seleccionamos tras una primera búsqueda y filtrado de este tipo de software.

Airwatch

Airwatch es una solución ofrecida por VMWare. Sin duda es una de las más utilizadas y conocidas. Aparece en los primeros resultados de búsqueda de este tipo de software y es mencionado en prácticamente todos los artículos que hablan del tema. Es propiedad de una de las grandes empresas del sector, por lo que podemos decir que se trata de un proyecto que inspira estabilidad y la seguridad de tener a todo un gigante tecnológico detrás.

Precios y licencias

Consta de una serie de modalidades o paquetes que incluyen distintos servicios dependiendo de las necesidades del cliente. Si desean conocerse sus precios puede visitarse el siguiente enlace:

Precios y paquetes

Hay que resaltar que no consta con modalidad gratuita, aunque puede solicitarse una prueba gratuita de 30 días, para ello hay que rellenar un formulario y esperar a que un comercial se ponga en contacto (yo aún sigo esperando).

Prueba gratuita

Características

- Permite gestionar todo tipo de dispositivos, no solo móviles. Desde PC's a sistemas embebidos, máquinas industriales, etc… Este punto no nos interesa demasiado realmente ya que sólo necesitaremos gestionar dispositivos móviles, y esta es una característica que comparten todas las soluciones MDM.
- Soporta prácticamente todos los SO's existentes para dispositivos móviles: Android, iOS, Mac OS, Blackberry, Symbian y Windows. Como se ha comentado antes, nos centraremos en iOS y Android.
- BYOD (Trae tu propio dispositivo). Permite administrar todo tipo de hardware, de forma que en una empresa cada trabajador utilice su móvil/Tablet personal pudiendo separar de forma segura sus datos, cuentas y archivos personales de las profesionales. Para ello cuenta con lo que llaman contenedores, mediante los cuales, podemos tener, por ejemplo, la cuenta de correo corporativa separada de nuestro correo personal, así como aplicaciones y archivos.
- Administración remota del dispositivo. Pueden programarse actualizaciones masivas, instalar aplicaciones de forma remota, así como modificar ajustes en el dispositivo.
- Gestión de aplicaciones. Además de poder instalar de forma remota apps, puede configurarse una App Store empresarial donde publicar las aplicaciones de uso interno que serán utilizadas, sin necesidad de publicarlas en App Sotre oficiales.
- Monitorización. Tendremos en tiempo real todo tipo de información referente a los dispositivos: batería, ubicación, versión de SO, aplicaciones instaladas… Así como definir alertas en base a estos valores. Por ejemplo, podemos definir un recinto mediante coordenadas GPS y configurar una alerta para que nos avise cuando un dispositivo sale de dicho perímetro. Otro punto importante es que podemos controlar la navegación, estableciendo listas negras/blancas acerca de las webs que se pueden visitar.

- Correo electrónico. Nos permitirá establecer unos ajustes para el cliente de correo electrónico comunes a todos los usuarios/grupos que queramos, de forma que si tenemos un servidor de correo propio en el centro, podemos configurar los dispositivos de forma casi inmediata todos a la vez.
- Gestión de usuarios, políticas y roles. Como se comentó en el apartado de objetivos, necesitamos tipos de usuarios con permisos muy específicos. Con esta solución esto no será un problema, ya que permite configurar políticas comunes a los distintos grupos de usuarios que tengamos. De forma que podamos añadir/quitar permisos de forma granulada a nuestros usuarios.

Método de instalación / despliegue

Airwatch nos permite elegir entre dos modalidades, una basada en la nube, y otra en la sede:

- Distribución basada en la nube: Airwatch nos concederá unos credenciales mediante los cuales accederemos a un portal de administración **alojado fuera de nuestros servidores** y desde el que administraremos todos los servicios.
- En la sede: Se procederá a la descarga del software de servidor necesario y se desplegará en la red del centro.

Conclusión

Estamos ante una completísima solución diseñada para el mundo **corporativo** ofrece muchísimas características que realmente no necesitamos, y carece de otras, debido a que no son necesarias en un entorno empresarial pero sí en uno educativo.

Por tanto, aunque si bien podría adecuarse a nuestras necesidades, Airwatch no será la solución más eficiente.

Spiceworks

Spiceworks es una solución basada en Ruby on Rails que pertenece a una empresa homónima con sede en Texas, EEUU. Además de ofrecer soluciones de software, es a su vez una inmensa red profesional orientada a nuevas tecnologías, lo que se traduce en una gran comunidad, soporte y documentación.

Precios y licencias

Al contrario que la solución de VMWare, el sistema de precios de Spiceworks es mucho más sencillo: tenemos dos modalidades a elegir, gratuita y Premium.

La modalidad Premium tiene un precio fijo establecido por dispositivo, por lo que podemos asegurarnos de que los servicios contratados se ajustan a nuestras necesidades reales, o dicho de otra forma, que pagamos sólo lo justo y necesario, manteniendo la posibilidad de escalabilidad.

La versión gratuita nos sirve para observar ligeramente las capacidades del software, aunque se encuentra muy limitada. No obstante, tenemos la posibilidad de solicitar una prueba gratuita de 30 días para asegurarnos de que las características Premium nos convencen. Otro punto a favor es que este proceso es totalmente automatizado, por lo que sólo es necesario rellenar un formulario para gozar de las ventajas Premium por un mes (sin esperar llamadas de comerciales).

Spiceworks - precios

Características

- Soporta todo tipo de tablets y móviles independientemente de su hardware.
- En cuanto a plataformas soportadas, únicamente iOS, Android y Windows Phone. Como ya hemos comentado, sólo nos interesan las dos primeras, de modo que por ahora nos vale.

- No soporta compartimentación de las cuentas, datos y archivos. Es decir, si el dispositivo personal es gestionado desde el centro, sus datos, cuentas y aplicaciones personales se verán comprometidas ya que el administrador tendrá acceso a todo tipo de configuraciones del dispositivo. No obstante, para el caso del email sí que ofrece compartimentación de forma que la cuenta corporativa (o en este caso del centro) nunca se vea "mezclada" con otras cuentas y archivos personales.
  Por lo tanto, siempre que los dispositivos sean proporcionados por el centro, la solución será válida. De otro modo no.
- Administración remota del dispositivo. Al igual que ocurre con Airwatch, este software permite la gestión remota prácticamente de forma total. Se pueden instalar y actualizar aplicaciones, cambiar ajustes del dispositivo (como por ejemplo activar la localización), bloquear y borrar el dispositivo… etc.
- Gestión de aplicaciones. Del mismo modo, también se pueden distribuir aplicaciones, a través de una tienda de apps propia, o bien a través del link de la aplicación a Play Store / App Store, o bien subiendo un archivo .apk o .ipa de la aplicación.
- Monitorización. Como suele ocurrir con estos tipos de software, incluye capacidades de monitorización e informes muy completas. Podemos definir nuestros propios informes de forma muy sencilla de forma que tengamos toda la información relevante a golpe de un click. También tenemos la posibilidad de definir alertas o como ellos lo llaman "monitores" que nos avisen siempre que se cumpla alguna condición definida por nosotros. Tal como que un dispositivo haya sido rooteado, haya salido del perímetro del centro, etc…
- Gestión de usuarios y roles. Este suele ser un rasgo común de todo el software de gestión de dispositivos móviles. Podremos definir usuarios asociados a dispositivos, definir políticas que apliquen permisos o configuraciones en base al grupo al que pertenece el usuario y demás.

Método de instalación / despliegue

Aquí sólo tenemos una opción, que es alojar físicamente nuestra aplicación en una máquina propia, es decir, no es un servicio basado en la nube; aunque una vez instalado, ofrece una interfaz web similar a la de sus competidores que nos permite gestionar todo a golpe de ratón.

Un punto a tener en cuenta importantísimo, es que sólo ofrecen versión de su software para **Windows**, de forma que si nos decantamos por esta solución tendremos que ceñirnos a este SO, ya sea en una máquina física o virtual (como es el caso de este proyecto para el que hemos obtenido resultados satisfactorios usando Virtualbox).

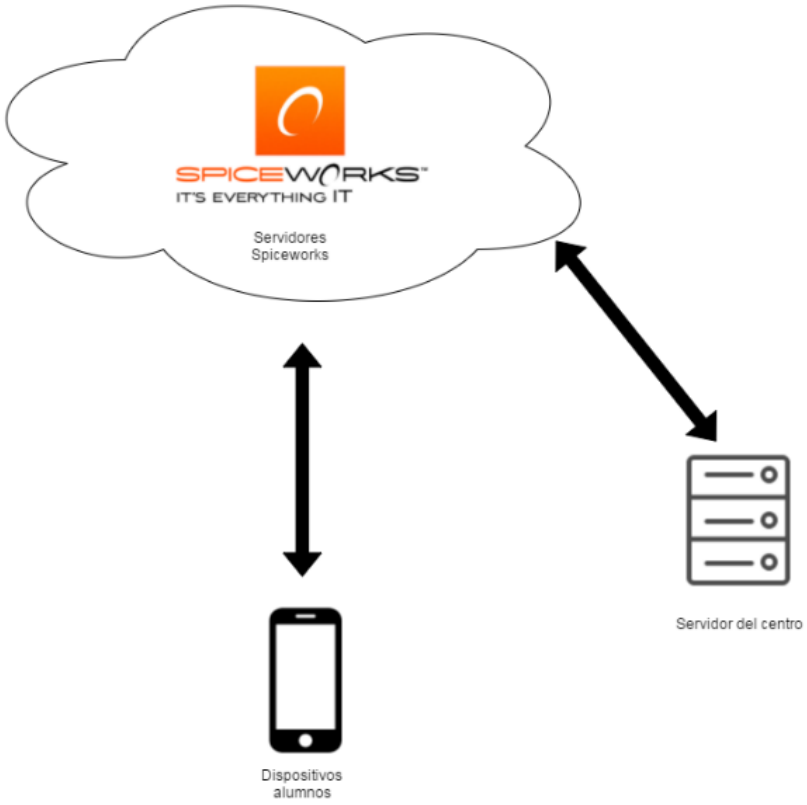
Conclusión

Spiceworks se trata de otra solución muy completa, se acerca bastante a nuestras necesidades, pero tiene dos puntos muy importantes en contra:

Primero, poca flexibilidad en cuanto a métodos de despliegue, nos vemos forzados a instalar el software en una de nuestras máquinas usando un SO muy específico.

Segundo, el rendimiento. Podemos decir que en base a las pruebas realizadas por el alumno tanto en la modalidad gratuita como en la Premium, la velocidad de respuesta es muy lenta; esto podría ser indiferente para ciertas características como pueden ser los informes, en cambio, si queremos bloquear o cambiar la contraseña del dispositivo de un alumno, es posible que los cambios se apliquen en un periodo no menor de 10 o 15 minutos. Esto se debe a que a pesar de que el servidor se encuentra alojado en nuestra red, la aplicación “cliente” que se encuentra en el dispositivo se comunica a través de internet (a fin de tener comunicación ya sea por red móvil o cualquier wifi).

El siguiente esquema ilustra la arquitectura que describimos:



Dado que Spiceworks cumple nuestros objetivos, podríamos considerarlo una solución válida, pero dada su falta de inmediatez en las comunicaciones y su escasa flexibilidad en cuanto a despliegue, consideraremos que **no es una solución válida** y pasamos al siguiente candidato.

Miradore

Se trata de una empresa con base en Finlandia que fue fundada en 2006, en su web comentan que su software es un proyecto con más de 15 años de antigüedad y centrada en Norteamérica, Europa, Oriente Próximo, África, Asia y el Pacífico (Así lo indican en su web).

Precios y licencias

Tenemos a nuestra disposición tres variantes: gratuita, business y enterprise, con características que van en aumento siendo la gratuita la más limitada y Enterprise la más completa.

Sus precios, al igual que Spiceworks, se basan en el número de dispositivos, con las ventajas que ello conlleva y que hemos comentado previamente.

En el siguiente enlace se pueden consultar sus precios:

Miradore - Precios

Características

- Soporta todo tipo de móviles y tablets, exactamente igual que Spiceworks.
- En cuanto a plataformas móviles, también soporta iOS, Android y Windows Phone.
- No soporta compartimentación de ningún tipo, por lo que no sería una buena opción en entornos BYOD (Bring Your Own Device – Trae tu propio dispositivo). Como asumimos que los dispositivos no serán personales sino que serán provistos por el centro, no daremos mucha importancia a este punto.
- Administración remota del dispositivo. Exactamente igual que sus competidores, goza de todas las características típicas en este tipo de software, que no vamos a detallar por no ser redundantes. Podemos resumirlo en que posee todas las herramientas de administración que necesitamos.
- Gestión de aplicaciones. Ídem, podemos instalar y actualizar aplicaciones de forma masiva y remota, incluso pudiendo personalizar el mensaje que aparece en el dispositivo previo a la instalación de la app.

Otra característica importantísima respecto a las aplicaciones, es el hecho de poder establecer listas blancas y negras para los dispositivos, usuarios y grupos (en iOS es más complicado pero ya hablaremos de esto mas adelante).

- Monitorización. Nos permitirá obtener todo tipo de información en tiempo real acerca de los dispositivos, incluso operador, estado de la batería, espacio libre en almacenamiento, ubicación, root, etc…
  En cuanto a informes, tiene una potente herramienta a través de la cual, crearemos informes usando un lenguaje que recuerda muy vagamente a SQL. Con dicho lenguaje podremos crear consultas y concatenarlas mediante operadores lógicos para crear informes lo más detallados y personalizados posibles.
  Ejemplo:

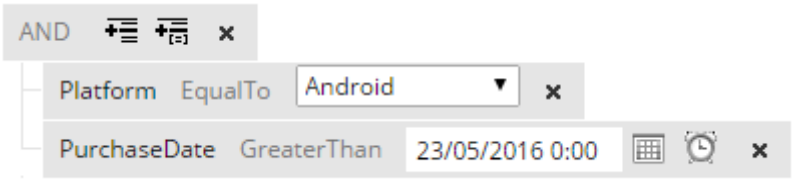


Figura 3. Ejemplo de sintaxis de informe.

- Gestión de usuarios y roles. Podemos definir distintos usuarios con sus correspondientes permisos, pero el punto fuerte de esta solución es la gestión de políticas de grupo, o como la aplicación los llama: Configuration Profiles (Perfiles de configuración).
  Dichos perfiles permiten de una sola vez y de forma centralizada, aplicar multitud de cambios en los dispositivos, tales como activar la localización, obligar al usuario a cambiar la contraseña del dispositivo por una que cumpla la política del centro, instalar aplicaciones de forma masiva y automática cuando un dispositivo se una a un grupo sobre el que está aplicada una política, etc…

  Esta característica recuerda mucho a las políticas de grupo de Active Directory, con lo que no podemos imaginar las posibilidades que ofrece.

Método de instalación / despliegue

El método de despliegue resulta muy sencillo ya que se trata de una solución basada en la nube. De forma que para ponernos en marcha sólo necesitamos registrarnos en su web, de forma que se nos proporcionará un dominio del tipo

nombredelproyecto.online.miradore.com

Sobra decir que este software puede ser gestionado desde cualquier dispositivo conectado a internet y que tenga un navegador compatible.

Conclusión

Miradore se trata de una solución que si bien no está orientada específicamente a la educación, cumple sobradamente con nuestras necesidades; sumando además su gran facilidad de uso, velocidad en cuanto a comunicaciones, plataformas soportadas y el hecho de gozar de modalidad gratuita.

Por esto, concluimos que Miradore se trata de una opción más que factible y que supera a las demás soluciones estudiadas, por lo que se recomienda su implantación en centros educativos.

Protocolos de actuación

En esta sección vamos a definir dos protocolos bien diferenciados:

1. Instalación del software y preparación de los dispositivos.
2. Asignación, entrega y recogida de los dispositivos de los alumnos.

Instalación del software y preparación de los dispositivos.

La instalación del software de gestión está explicada en cada uno de sus correspondientes apartados, por lo que no entraremos de nuevo en este tema.

Por otra parte, tal y como hemos definido en los objetivos, puede darse el caso de que varios alumnos tengan que compartir un dispositivo. Desgraciadamente, sólo una de las soluciones contempla este caso y no se trata de una solución idónea por otras razones que ya hemos explicado. Para solucionar este problema, recurriremos a una función incluida en Android a partir de la versión 4.2 que es la posibilidad de añadir múltiples usuarios a un dispositivo.

Existen tres tipos de cuentas de usuario disponibles en Android:

- Usuario principal. Idealmente este usuario será un administrador del centro, ya que será el único que podrá gestionar otras cuentas, así como definir qué aplicaciones están disponibles para los demás.
- Usuario secundario. A la hora de crear un nuevo usuario, se nos preguntará si será un usuario normal o limitado, elegiremos limitado para poder tener control sobre las aplicaciones disponibles.
- Invitado. Se trata de una cuenta normal, con la particularidad de que será borrada cuando se termine de usarla. No prestaremos mucha atención a esta opción porque no nos servirá de nada.

Preparación de dispositivos inicialmente para un curso escolar

El proceso para preparar un dispositivo será el siguiente:

1. El profesor/administrador vinculará una cuenta (preferiblemente del centro) al dispositivo en forma de cuenta principal. Se recomienda usar la misma cuenta para todos los dispositivos, ya que esto facilitará la instalación de las mismas aplicaciones y ajustes de red WiFi para todos los dispositivos (aunque esto es algo que luego se podrá hacer desde el software de gestión). Usando dicha cuenta se instalará la aplicación cliente propia del MDM (sin vincularla aún al servidor). Es MUY importante que el administrador establezca una contraseña de desbloqueo en el dispositivo, ya que si no cualquier alumno cambiar a la cuenta de administrador libremente.
2. Acto seguido se crearán las cuentas secundarias necesarias para los alumnos, eligiendo las aplicaciones disponibles (como mínimo deberá incluirse la aplicación de MDM)
3. Cada alumno tendrá que iniciar sesión la primera vez para vincular la cuenta del dispositivo a su cuenta Gmail. Idealmente cada alumno creará una cuenta específica para el curso siguiendo pautas establecidas por el profesorado, de forma que sea más fácil identificar a quién pertenece cada correo.

   Ejemplo: xprimerapellido.queipo@gmail.com siendo la x la inicial del nombre.
4. Se vincula cada dispositivo al software de gestión, de forma que si hay varias cuentas de usuario en un mismo dispositivo habrá que repetir el proceso para cada cuenta. Miradore facilita esto gracias a la posibilidad de enviar un correo de forma masiva a todos los usuarios con usuario y claves temporales para vincularse o mejor aún, activar una opción llamada Self Service Enrollment: de forma que podemos definir un PIN común para que los alumnos puedan darse de alta sin intervención del administrador. **Nota: En caso de dispositivos compartidos, en la vista de dispositivos aparecerá un dispositivo por alumno, es decir, tendremos dispositivos "repetidos". Esto se debe a que a la**

compartimentación que Android incluye actúa de cada forma que cada app de Miradore funciona de forma independiente.

5. Establecer contraseña para cada alumno, para evitar que un alumno se loguee en nombre de otro. Es posible establecer una política desde el software de gestión que pida al usuario cambiar / establecer la contraseña de desbloqueo. Por lo que se recomienda establecer dicha política antes de que los alumnos se vinculen. **NOTA: Debido a restricciones del SO, no es posible forzar al usuario a cambiarla, sólo es posible mostrar una notificación pidiendo al usuario que establezca la contraseña.**

Procedimiento de entrega y recogida para una sesión de clase

Gracias al software de gestión tendremos un inventario de dispositivos, así como qué dispositivos están activos. Si se desea, se puede añadir más control estableciendo un protocolo mediante el cual el alumno deja constancia escrita del dispositivo recogido.

- Los alumnos proceden a recoger sus dispositivos asignados (firmando o no)
- Comienza la sesión de clase: el profesor envía los contenidos, enlaces notificaciones, etc. necesarios para complementar la actividad. Si es necesario podrá bloquear los dispositivos o enviar notificaciones push con mensajes definidos por él.
- Termina la sesión: los alumnos proceden a entregar los dispositivos y dejar o no constancia de la entrega.

Conclusión y valoración personal

Nota importante sobre iOS

Antes de llegar a las conclusiones, debemos dejar clara una particularidad muy importante acerca de iOS. Y es que estos dispositivos son muy restrictivos a la

hora de permitirnos el control remoto. Existen muchas funciones que hemos descrito en este proyecto que dependen que el dispositivo sea puesto en un modo especial llamado

“modo supervisado”

Ni siquiera Apple distribuye mucha información de forma pública sobre este modo, pero lo que sabemos es que:

- El modo supervisado nos permite instalar o desinstalar aplicaciones de forma silenciosa, es decir, el usuario no será notificado de ninguna forma.
- Será posible establecer listas negras/blancas de aplicaciones.
- Para acceder a este modo, es necesario tener una cuenta corporativa en el programa de desarrolladores de Apple.
- Contar con un vendedor de productos Apple autorizado (Apple reseller) que nos provea de los dispositivos que vamos a utilizar, identificando la compra con nuestro id en el programa de desarrolladores.

Debido a que consideramos que esto es un escollo importante, ya que añade muchas trabas al proceso y nos fuerza a usar dispositivos nuevos (no podemos aprovechar dispositivos previamente adquiridos por el centro), estimamos que no es recomendable utilizar dispositivos iOS, por lo menos mientras se requieran funciones que sólo estén disponibles a través del modo gestionado (como es el caso).

Candidatos interesantes descartados

En este apartado comentaremos dos soluciones que, si bien se acercan muchísimo a nuestros objetivos, constan de algún tipo de limitación que las elimina directamente de “la competición” por convertirse en nuestro software MDM seleccionado.

TabAlive

A simple vista es la herramienta perfecta. Fue desarrollada específicamente para educación, tiene todas las funciones que necesitamos y puede accederse a ellas de forma muy fácil. Consta de tres roles predefinidos (Alumno, Profesor, Administrador) y además consta de herramientas específicas para ayudar al desarrollo de la clase.

El motivo de haber sido descartada es doble: Primero está limitada solamente a tablets, y como asumimos que se requiere administrar tanto smartphones como tablets, esta es una limitación excluyente. La segunda es que a pesar de tener disponible una demo gratuita, no ha sido posible ponerse en contacto con ellos para solicitarla.

No obstante, el alumno reconoce que puede tratarse de una opción muy interesante y recomienda un estudio detallado de la solución.

Cellabus

Se trata de otra solución desarrollada específicamente para educación, también se ajusta mucho a nuestros objetivos y parece gozar de una interfaz sencilla e intuitiva, pero queda descartada automáticamente al soportar **solamente dispositivos iOS.**

Resumen y conclusión final

Como sabemos, los dispositivos móviles se han convertido en una herramienta omnipresente que nos permite estar continuamente conectados. Como en todos los ámbitos de la vida, el ámbito educativo también se ha visto afectado por este cambio,

surgiendo así nuevas necesidades en cuanto a administración y gestión de dispositivos móviles.

A lo largo de este trabajo hemos explorado tres soluciones muy completas diseñadas para entornos empresariales pero que pueden ser aprovechadas para el ámbito educativo con relativa facilidad. Nos hemos decantado por recomendar Miradore por tratarse de una solución que consta con las características necesarias, además de estar basada en la nube (con el consiguiente ahorro en infraestructura), su facilidad de uso y su precio. Esto no quiere decir que no puedan existir otras soluciones igualmente válidas, pero a criterio del alumno esta es la más eficiente y asequible.

Como también se ha apuntado, hemos detectado que desplegar dispositivos iOS resulta más complicado, teniendo que ejecutar muchos más pasos e involucrar a terceros para obtener un resultado similar. Por esto se recomienda utilizar solamente Android en los dispositivos que vayan a ser gestionados de forma remota, ya que permiten un control más detallado con menos esfuerzo.

Otro apunte importante es que, como el lector habrá podido apreciar, no se ha hecho hincapié alguno en la forma de despliegue de los dispositivos móviles. Esto es debido a que resulta bastante trivial, en cada una de las soluciones el proceso es el mismo: descargar una aplicación cliente, introducir una clave temporal y esperar.

A continuación se adjunta una tabla comparativa que nos servirá para tener visión de conjunto y poder comparar de un vistazo las diferentes opciones que nos ofrecen las soluciones estudiadas.

	Airwatch	Spiceworks	Miradore
Android	Si	Si	Si
iOS	Si	Si	Si
Hardware	Todo tipo de dispositivos	Smartphones y tablets	Smartphones y tablets
Usuarios y roles	Administrador, administrador con privilegios limitados y usuario final. Permite administrar los permisos de forma granulada.	Administrador, reporting (solo genera informes), Helpdesk Admin, Helpdesk Tech.	Administrador, editor y usuario final
Bloqueo remoto	Si	Si	Si
Borrado remoto	Si	Si	Si
Cambios en configuración remotos	Todos, no impide que el usuario haga cambios.	Todos, no impide que el usuario haga cambios.	Todos, no impide que el usuario haga cambios.
Instalación de apps	Sí, de forma silenciosa o no. Con origen en App Store o archivo .ipa/.apk	Sí, con notificación y confirmación del usuario. Con origen en App Store o archivo .ipa/.apk	Sí, con notificación y confirmación del usuario. Con origen en App Store o archivo .ipa/.apk
Configurar app store propia para el centro	Si	Si	No
Actualización de apps	Si	Si	Si
Listas negras de apps	Si	Si***	Si***
Listas blancas de apps	Si	Si***	Si***
Informes	Totalmente configurables, permite almacenarlos y ejecutarlos bajo demanda o periódicamente	Totalmente configurables, permite almacenarlos y ejecutarlos bajo demanda o periódicamente	Totalmente configurables, permite almacenarlos y ejecutarlos bajo demanda o periódicamente
Alertas	De todo tipo, se pueden definir reglas basadas en cualquier dato medible.	De todo tipo, se pueden definir reglas basadas en cualquier dato medible.	De todo tipo, se pueden definir reglas basadas en cualquier dato medible.
Navegación segura	Control total sobre el	No. No permite controlar el	No. No permite controlar el

	contenido. Permite forzar un proxy e incluso desactivar el cifrado para interceptar las conexiones.	tráfico de los dispositivos. Sólo muestra las aplicaciones instaladas en él.	tráfico de los dispositivos. Sólo muestra las aplicaciones instaladas en él.
Detección de root / jailbreak	Si.	Si.	Si.
Compartimentación	Si	No	No
Soporte de dispositivos compartidos	Si	No**	No**
Infraestructura	SaaS* o local	Local, sólo Windows.	SaaS

* Software as Service, lo que comúnmente llamamos servicio en la nube.

** Aunque el software no soporta explícitamente dispositivos compartidos, en el protocolo de despliegue se explica la solución adoptada para solventar esto.

*** Se trata de una característica sólo disponible en modalidad premium

Bibliografía y fuentes de consulta

Enlaces de interés

Referencias bibliográficas