Gestión de dispositivos y datos corporativos en iOS

Presentación

Empresas de todo el mundo están motivando la productividad de sus empleados con el iPhone y el iPad.

Contenido

Para que la estrategia móvil tenga éxito, es fundamental conseguir un equilibrio entre el control del equipo de TI y las opciones para usuarios. Al personalizar los dispositivos iOS con sus propias apps y contenidos, los usuarios los ven como si fueran suyos y asumen más responsabilidades, lo que hace que sean más productivos y se impliquen más. Esto se consigue gracias al entorno de gestión de Apple, que separa los datos personales de los del trabajo para que la empresa pueda gestionar los datos y apps corporativos aparte. Además, los usuarios saben cómo se están gestionando sus dispositivos y están tranquilos porque su privacidad está a salvo.

Este documento ofrece pautas para que el departamento de TI pueda mantener el control esencial y los usuarios puedan seguir utilizando las mejores herramientas para trabajar. Es un complemento de la «Guía de referencia sobre la implantación de iOS», un documento técnico online con información completa sobre la implantación y gestión de dispositivos iOS en la empresa.

La «Guía de referencia sobre la implantación de iOS» se encuentra disponible en help.apple.com/deployment/ios.

Fundamentos de la gestión

iOS facilita enormemente las implantaciones de iPhone y iPad, pues incorpora técnicas que permiten simplificar la configuración de cuentas, configurar políticas, distribuir apps y aplicar restricciones a los dispositivos a distancia.

Nuestro modelo de gestión

El entorno de gestión de Apple es la base de la gestión de dispositivos móviles. Al estar integrado en iOS, las organizaciones pueden centrar la gestión en lo relevante, con una intervención mínima y sin dar prioridad al bloqueo de prestaciones o a la desactivación de funciones. Como resultado, el entorno de gestión de Apple permite que las soluciones de gestión de dispositivos móviles (MDM) de terceros puedan controlar con más precisión los dispositivos, apps y datos. Pero lo más importante es que la empresa mantiene el control necesario sin que se resientan la experiencia de los empleados ni su privacidad.

Es posible que otros métodos de gestión de dispositivos se refieran a las funciones de MDM con otros nombres, como «gestión de la movilidad empresarial (EMM)» o «gestión de aplicaciones móviles (MAM)». Todas estas soluciones persiguen un mismo objetivo: gestionar los dispositivos y los datos corporativos de la organización de forma inalámbrica. Como el entorno de gestión

de Apple está integrado en iOS, no se necesita ninguna aplicación agente del proveedor de la solución de MDM.

Separación de datos profesionales y personales

No importa si la organización usa dispositivos propiedad de la empresa o de los usuarios: el departamento de TI podrá gestionarlos sin interferir en la productividad de los empleados. Los datos profesionales y personales se gestionan por separado, sin perjudicar la experiencia del usuario. Esto da más libertad a los empleados, que pueden tener en sus dispositivos tanto las apps de productividad más novedosas como las apps corporativas. iOS lo consigue sin usar soluciones de terceros —por ejemplo, contenedores—, que frustran a los usuarios y empeoran su experiencia.

Distintos modelos de gestión

En otras plataformas, se suelen crear contenedores para solucionar problemas que no se producen en iOS. Algunos contenedores usan una estrategia de doble persona, que crea dos entornos independientes que se ejecutan en el mismo dispositivo. Otros se centran en la contenerización de las propias apps a través de la integración mediante código o de soluciones de empaquetado de apps. Todos estos métodos pueden mermar la productividad de los usuarios, que tienen que iniciar y cerrar sesión en varios espacios de trabajo o añadir una dependencia en el código propietario que suele provocar incompatibilidades de las apps con las actualizaciones del sistema operativo.

Las organizaciones que ya no usan contenedores ven que los controles de gestión que incorpora iOS ofrecen una experiencia óptima para los usuarios y aumentan su productividad. Para evitar posibles complicaciones para los usuarios que utilizan los dispositivos tanto en casa como en el trabajo, se pueden usar controles de políticas que gestionen el flujo de datos de forma sencilla en segundo plano.

Gestión de los datos corporativos

Con iOS, no es necesario bloquear los dispositivos, ya que sus tecnologías clave permiten controlar el flujo de los datos corporativos entre las apps y evitan la fuga de información a las apps o servicios de nube personales del usuario.

Contenido gestionado

El contenido gestionado permite instalar, configurar, gestionar y eliminar dominios, libros, cuentas y apps internas personalizadas y del App Store.

- **Apps gestionadas.**Las apps instaladas mediante MDM se denominan «apps gestionadas». Pueden ser apps gratuitas o de pago del App Store, o apps internas personalizadas, y todas ellas pueden instalarse con MDM a través de una red inalámbrica. Las apps gestionadas suelen contener información confidencial y ofrecen más control que las apps descargadas por el usuario. El servidor de MDM puede eliminar por petición apps gestionadas y sus correspondientes datos o especificar qué apps deben eliminarse cuando se quite el perfil de MDM. Además, el servidor de MDM puede impedir que los datos de las apps gestionadas se incluyan en copias de seguridad de iTunes y iCloud.
- **Cuentas gestionadas.** MDM puede configurar automáticamente el correo y otras cuentas de los usuarios para ayudarles a tener sus equipos preparados rápidamente. En función de la solución de MDM y de su integración con los sistemas internos, las cargas útiles también pueden incluir varios datos del usuario, como nombre, dirección de correo y, si procede, identidades de certificado para tareas de autenticación y firma. MDM puede configurar los

siguientes tipos de cuentas: IMAP/POP, CalDAV, calendarios suscritos, CardDAV, Exchange ActiveSync y LDAP.

- **Libros gestionados.** MDM permite enviar automáticamente cualquier documento o libro en formato ePub o PDF a los dispositivos de los usuarios para que tengan todo lo que necesitan. Los libros gestionados pueden compartirse solo con otras apps gestionadas o enviarse por email desde cuentas gestionadas. Cuando los materiales dejen de ser necesarios, se borran en remoto y listo.
- **Dominios gestionados.** Las descargas de Safari se consideran documentos gestionados si tienen su origen en un dominio gestionado. Es posible gestionar direcciones URL y subdominios concretos. Por ejemplo, si un usuario descarga un PDF de un dominio gestionado, el PDF debe cumplir con todos los ajustes de documentos gestionados exigidos por el dominio. Las rutas que siguen al dominio se gestionan por omisión.

Distribución gestionada

Con la distribución gestionada, se puede usar la solución de MDM o Apple Configurator 2 para gestionar las apps y los libros comprados a través del Programa de Compras por Volumen (PCV). Para activar la distribución gestionada, primero es necesario vincular la solución de MDM con la cuenta del PCV mediante un identificador de seguridad. En cuanto el servidor de MDM se conecta al PCV, se pueden asignar apps directamente a un dispositivo sin necesidad de usar un ID de Apple. El usuario recibe un mensaje cuando las apps están listas para instalarse en el dispositivo. En el caso de los dispositivos supervisados, las apps se instalan sin ni siquiera preguntar al usuario.

Para conservar el control total sobre las apps con una solución MDM, hay que asignar las apps directamente a un dispositivo.

Configuración de apps gestionada

Con la configuración de apps gestionada, MDM usa el entorno de gestión integrado en iOS para configurar las apps durante o después de la implantación. En este entorno, los desarrolladores pueden identificar los ajustes de configuración que deben implementarse al instalar su app como una app gestionada. Los empleados pueden usar de inmediato las apps configuradas de este modo, sin que deban personalizar ninguna opción. Como no es necesario instalar ningún SDK propietario ni empaquetar ninguna app, el departamento de TI tiene la seguridad de que los datos corporativos de las apps están a salvo.

Con la configuración de apps gestionada, se pueden activar algunas funciones que los desarrolladores de apps pueden usar, por ejemplo, para configurar apps, borrarlas de forma remota, evitar que se hagan copias de seguridad o desactivar las capturas de pantalla.

Esta comunidad se dedica a ofrecer herramientas y prácticas recomendadas sobre las funciones nativas de los sistemas operativos móviles. Los principales proveedores de soluciones de MDM de esta comunidad han establecido una guía estándar para todos los desarrolladores de apps que usan la configuración de apps gestionada. Con estas pautas para configurar y proteger las apps móviles de forma más coherente, abierta y sencilla, la comunidad contribuye a aumentar la adopción de sistemas móviles en las empresas.

Se puede obtener más información sobre la AppConfig Community en www.appconfig.org.

Flujo de datos gestionado

Las soluciones de MDM ofrecen prestaciones específicas que permiten gestionar los datos corporativos con precisión para evitar la fuga de información a las apps o servicios de nube personales del usuario.

- **Gestión de apertura de archivos.** La gestión de apertura de archivos utiliza un conjunto de restricciones que impide que los adjuntos o documentos de orígenes gestionados se abran en destinos no gestionados, y viceversa.

  Por ejemplo, se puede impedir que los adjuntos de correos confidenciales correspondientes a una cuenta de correo gestionada se abran con apps personales del usuario. Solo las apps instaladas y gestionadas con MDM pueden abrir este documento de trabajo. Las apps personales no gestionadas ni siquiera aparecen en la lista de apps que pueden abrir el adjunto. Además de los libros, apps, cuentas y dominios gestionados, algunas extensiones respetan las restricciones de la gestión de apertura de archivos.

Para proteger los datos corporativos, solo las apps instaladas y gestionadas con MDM pueden abrir este documento de trabajo.

- **Gestión de extensiones.** Las extensiones de apps permiten que las apps de desarrolladores externos interactúen con otras apps e incluso con sistemas clave de iOS, como Centro de Notificaciones, lo que permite crear nuevos flujos de trabajo empresariales entre las apps. El uso de la gestión de apertura de archivos evita que las extensiones no gestionadas interactúen con las apps gestionadas. Estos son algunos ejemplos de extensiones:

– Las **extensiones para proveedores de documentos** permiten abrir archivos de una amplia variedad de servicios de nube con apps de productividad sin tener que hacer copias innecesarias.

– Las **extensiones de acción** permiten a los usuarios manipular o ver el contenido en el contexto de otra app. Por ejemplo, los usuarios pueden usar una acción para traducir el texto de un idioma a otro directamente en Safari.

– Las **extensiones de teclado personalizado** ofrecen teclados distintos de los que ya integra iOS. La gestión de apertura de archivos puede impedir el uso de teclados no autorizados en las apps corporativas.

– Las **extensiones de Hoy**, también llamadas «widgets», sirven para enviar información a la vista Hoy del Centro de Notificaciones. Es una forma fantástica de enviar información actualizada de una app al usuario, con interacciones simplificadas que permiten abrir la app para obtener más información.

– Las **extensiones de compartir** ofrecen a los usuarios una forma cómoda de compartir contenidos con otras entidades, como sitios web de redes sociales o servicios de carga de archivos. Por ejemplo, en una app que incluya un botón Compartir, los usuarios pueden elegir una extensión para compartir que represente el sitio web de una red social y publicar un comentario o cualquier otro contenido.

Opciones de gestión flexible

El entorno de gestión de Apple es flexible y ofrece un equilibrio entre la gestión de los dispositivos propiedad del usuario y la de los dispositivos propiedad de la empresa. Si se usa una solución de MDM de terceros en iOS, las opciones de gestión de dispositivos pueden ser de lo más variadas: desde aplicar una metodología muy abierta hasta configurar hasta el último detalle.

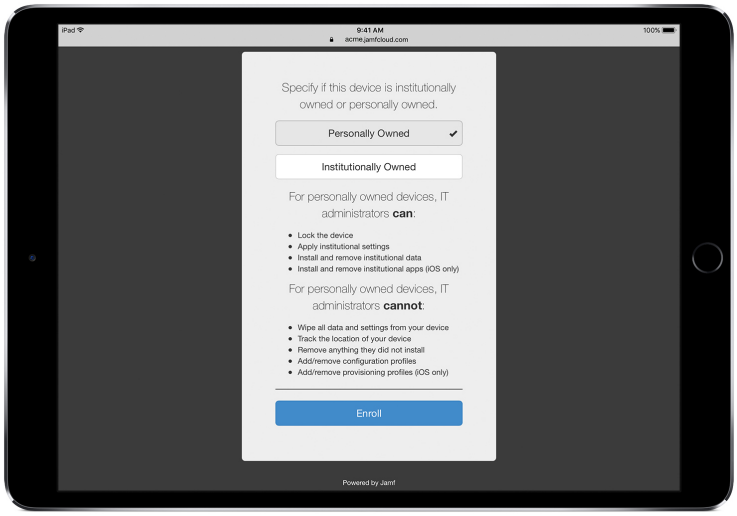
Modelos de propiedad

La gestión de los dispositivos y apps de la organización depende del modelo —o de los modelos — de propiedad de los dispositivos. Los dos modelos de propiedad de dispositivos iOS más habituales entre las empresas son: propiedad del usuario y propiedad de la empresa.

Dispositivos propiedad del usuario

En implantaciones con dispositivos propiedad de los usuarios, iOS permite a los usuarios personalizar la configuración de forma transparente, con la seguridad de que nadie de la empresa podrá tener acceso a sus datos personales.

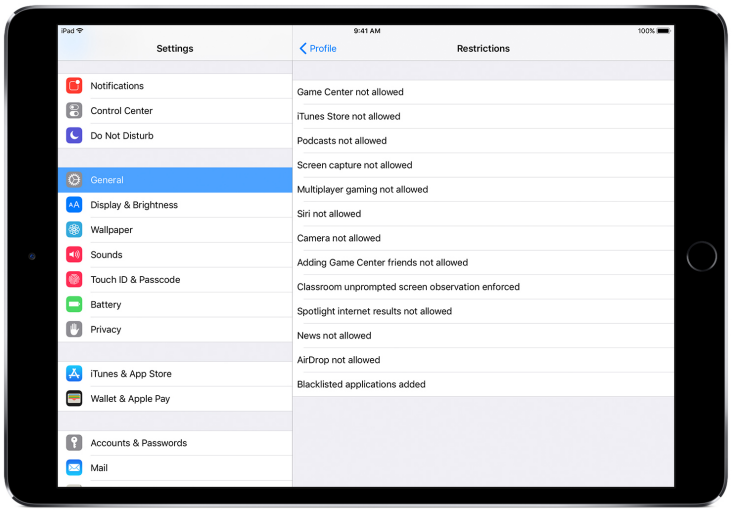
- **Aceptación o cancelación de la inscripción.**
  Incluso si los empleados utilizan sus dispositivos personales, pueden tener acceso a los servicios de Wi-Fi, correo y calendario de la empresa. Los usuarios simplemente deben aceptar la inscripción en la solución de MDM de la empresa. Cuando los usuarios se inscriben en MDM por primera vez con dispositivos iOS, se les informa del nivel de acceso que tiene el servidor de MDM a sus dispositivos y de las prestaciones que configurará. De este modo, obtienen información transparente sobre qué va a gestionar la empresa, y se establece una relación de confianza entre la organización y los usuarios. Es importante que los usuarios sepan que, si en algún momento se sienten incómodos con este tipo de gestión, pueden borrar el perfil de gestión de sus dispositivos para cancelar la inscripción. En tal caso, se eliminan todas las cuentas y apps corporativas que haya instalado el servidor de MDM.



Las soluciones de MDM de terceros suelen ofrecer una interfaz de usuario sencilla para que los empleados se sientan cómodos durante la inscripción.*

* Imagen cortesía de Jamf.

- **Mayor transparencia.** En cuanto los usuarios se inscriben en MDM, los empleados pueden ver fácilmente en Ajustes las apps, libros y cuentas que gestiona la empresa, así como las restricciones que se aplican. iOS etiqueta como gestionados todos los ajustes, cuentas y contenido de la empresa instalados con MDM.



En la interfaz de usuario de los perfiles de configuración de Ajustes, los usuarios pueden ver qué se ha configurado exactamente en sus dispositivos.

- **Privacidad del usuario.** Aunque el servidor de MDM te permite interactuar con los dispositivos iOS, queda restringido el acceso a ciertos ajustes e información de las cuentas. La organización puede gestionar las cuentas, los ajustes y la información proporcionados a través de MDM, pero no tiene acceso a las cuentas personales del usuario. De hecho, las mismas prestaciones que protegen los datos de las apps corporativas gestionadas hacen lo propio con el contenido personal del usuario, evitando así que esta información se mezcle con los datos de la empresa.

  Estos son algunos ejemplos de lo que un servidor de MDM de terceros puede y no puede ver en un dispositivo iOS personal:

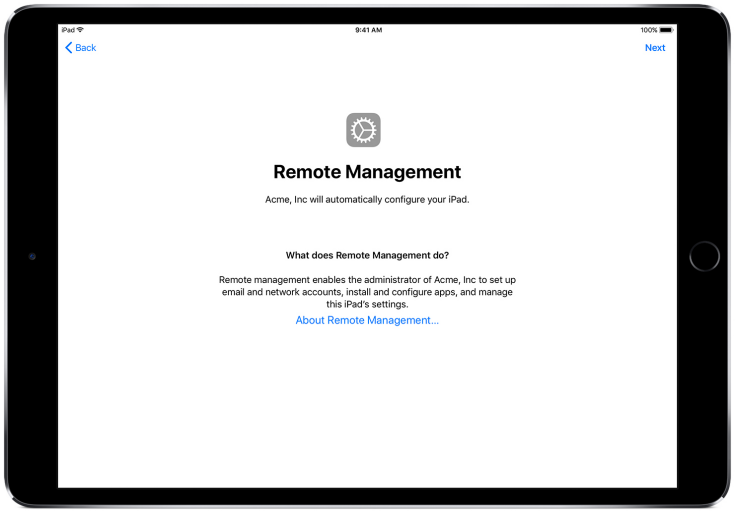
MDM puede ver:	MDM no puede ver datos personales como:
Nombre del dispositivo	Correo, calendarios y contactos personales o profesionales
Número de teléfono	Mensajes SMS o de iMessage
Número de serie	Historial de navegación de Safari
Número y nombre del modelo	Registros de llamadas telefónicas o FaceTime
Capacidad y espacio disponible	Notas y recordatorios personales
Número de versión de iOS	Frecuencia de uso de apps
Apps instaladas	Ubicación del dispositivo

- **Personalización de dispositivos.** Las empresas se han dado cuenta de que, cuando permiten la personalización de los dispositivos, los usuarios los ven como si fueran suyos y asumen más responsabilidades, lo que hace que sean más productivos porque les deja decidir qué apps y contenidos les van a ayudar a hacer mejor su trabajo.

Dispositivos propiedad de la empresa

En implantaciones con dispositivos propiedad de la empresa, se puede proporcionar un dispositivo a cada usuario —implantación personalizada—, o rotar los dispositivos entre los usuarios —implantación no personalizada—. Algunas prestaciones de iOS —como la inscripción automatizada, el bloqueo de ajustes de MDM, la supervisión de dispositivos y la VPN siempre activada— garantizan que los dispositivos se configuren según los requisitos de la organización. Así, la empresa tiene un mayor control y se asegura de que los datos corporativos queden a buen recaudo.

- **Inscripción automatizada.** El Programa de Inscripción de Dispositivos (PID) también permite automatizar la inscripción en MDM durante la configuración inicial de los dispositivos iPhone, iPad y Mac de la empresa. Si se quiere, la inscripción puede ser obligatoria y no eliminable. Los dispositivos también pueden ponerse en modo supervisado durante la inscripción, y se puede permitir que los usuarios se salten varios pasos de configuración básicos.



Con el PID, la solución de MDM configura automáticamente los dispositivos iOS en Asistente de Configuración.

- **Dispositivos supervisados.** La supervisión ofrece funciones de gestión adicionales para los dispositivos iOS propiedad de la empresa. Por ejemplo, permite filtrar las conexiones web a través de un proxy global para asegurarse de que el tráfico web de los empleados no sale de la red corporativa o para impedir que los usuarios restauren la configuración de fábrica en sus dispositivos.

Por omisión, los dispositivos iOS no están supervisados. Puedes utilizar el PID para activar el modo supervisado automáticamente o Apple Configurator 2 para hacerlo de forma manual.

Aunque de momento la empresa no se plantee usar las prestaciones reservadas a los dispositivos supervisados, puede ser útil configurar la supervisión en los dispositivos para poder aprovechar estas prestaciones más adelante. De lo contrario, los dispositivos ya implantados tendrán que borrarse. La supervisión no se limita a bloquear los dispositivos propiedad de la empresa, sino que los convierte en mejores herramientas al ampliar sus funciones de gestión. A largo plazo, la supervisión ofrece incluso más opciones a la empresa.

La Guía de referencia sobre la implantación de iOS contiene una lista completa de los ajustes supervisados.

Restricciones

iOS admite las siguientes categorías de restricciones, que se pueden configurar de forma inalámbrica para satisfacer las necesidades de la organización sin perjudicar la experiencia del usuario:

- AirPrint
- Instalación de las apps
- Uso de las apps
- App Aula
- Dispositivo
- iCloud
- Restricciones de usuario y de grupo de usuarios de Gestor de Perfiles
- Safari
- Ajustes de seguridad y privacidad
- Siri

Las siguientes categorías también tienen opciones que se pueden configurar mediante la solución de MDM:

- Ajustes de la inscripción en MDM automatizada
- Pantallas de Asistente de Configuración

Funciones de gestión adicionales

Consultas a dispositivos

Además de configurar dispositivos, un servidor de MDM tiene la posibilidad de enviar consultas a los dispositivos sobre sus datos, red, aplicaciones, estado de conformidad y otra información de seguridad. Esta información puede utilizarse para comprobar que los dispositivos siguen cumpliendo las políticas exigidas. El servidor de MDM determina la frecuencia con la que recopila dicha información.

Estos son algunos ejemplos del tipo de información que se puede consultar en un dispositivo iOS:

- Detalles del dispositivo (nombre)
- Modelo, versión de iOS y número de serie
- Información de red

- Estado de itinerancia y direcciones MAC
- Aplicaciones instaladas
- Nombre de app, versión y tamaño
- Datos de seguridad y conformidad
- Certificados, políticas y ajustes instalados
- Estado de cifrado

Tareas de gestión

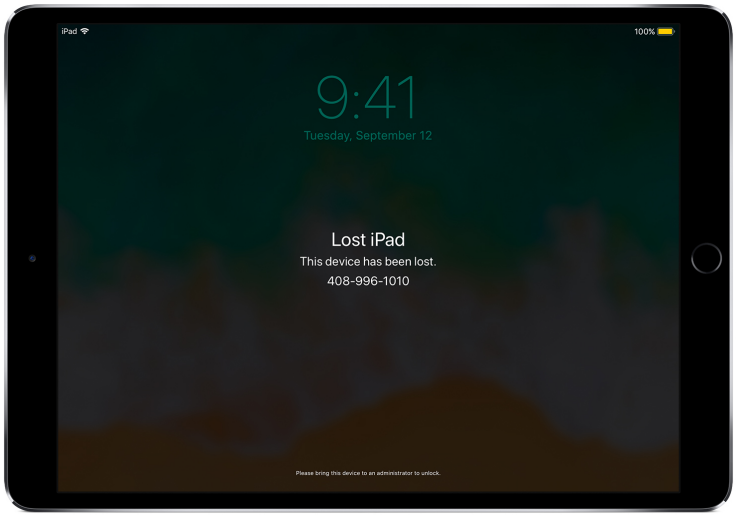
Cuando un dispositivo está gestionado, un servidor de MDM puede ejecutar una amplia variedad de tareas administrativas, como cambiar la configuración automáticamente sin interacción del usuario, actualizar iOS en dispositivos protegidos por código, bloquear o borrar un dispositivo a distancia, o quitar el bloqueo por código para que los usuarios puedan restablecer contraseñas olvidadas. Un servidor de MDM también puede indicar a un dispositivo iOS que inicie o finalice una sesión de Duplicación AirPlay con un destino determinado.

Modo Perdido

Con iOS 9.3 o posterior, la solución de MDM puede poner un dispositivo en modo Perdido a distancia. Esto bloquea el dispositivo y permite mostrar un mensaje con un número de teléfono en la pantalla de bloqueo.

Con el modo Perdido, MDM puede consultar a distancia la última ubicación en la que los dispositivos supervisados perdidos o robados tenían conexión. Para usar el modo Perdido no es necesario que esté activado Buscar mi iPhone.

Si MDM desactiva el modo Perdido a distancia, el dispositivo se desbloquea y se recoge su ubicación. Para garantizar la transparencia, el usuario recibe una notificación sobre la desactivación del modo Perdido.



Cuando se usa MDM para activar el modo Perdido en un dispositivo extraviado, el dispositivo se bloquea, se pueden mostrar mensajes en la pantalla y se determina su ubicación.

Bloqueo de Activación

Con iOS 7.1 o posterior, MDM puede activar Bloqueo de Activación cuando un usuario activa Buscar mi iPhone en un dispositivo supervisado. Así, la empresa puede beneficiarse de la función antirrobo Bloqueo de Activación o impedir su activación si, por ejemplo, un usuario se va de la empresa sin borrar Bloqueo de Activación con su ID de Apple.

La solución de MDM puede recuperar el código de cancelación y permitir que el usuario active Bloqueo de Activación en el dispositivo, teniendo en cuenta lo siguiente:

- Si Buscar mi iPhone está activado cuando la solución de MDM permite Bloqueo de Activación, este se activa en ese momento.
- Si Buscar mi iPhone está desactivado cuando la solución de MDM permite Bloqueo de Activación, este se activa la próxima vez que el usuario active Buscar mi iPhone.

Resumen

El entorno de gestión de iOS combina lo mejor de ambos mundos: el equipo de TI puede configurar, gestionar y proteger los dispositivos y controlar los datos corporativos que circulan por ellos, y los usuarios pueden trabajar a pleno rendimiento en sus dispositivos favoritos.