(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 719 442**

(51) Int. CI.:

G06F 21/51 (2013.01)
G06F 8/61 (2008.01)
G06F 21/60 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **03.03.2014 PCT/US2014/019793**

(87) Fecha y número de publicación internacional: **12.09.2014 WO14137865**

(96) Fecha de presentación y número de la solicitud europea: **03.03.2014 E 14713293 (0)**

(97) Fecha y número de publicación de la concesión europea: **16.01.2019 EP 2965255**

(54) Título: **Limitación de aplicaciones de empresa y ajustes en dispositivos**

(30) Prioridad:

06.03.2013 US 201313787420

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
10.07.2019

(73) Titular/es:

MICROSOFT TECHNOLOGY LICENSING, LLC (100.0%)
One Microsoft Way
Redmond, WA 98052, US

(72) Inventor/es:

KARAA, HASSEN;
HEALY, MICHAEL;
FLEGG, BRETT D.A.;
DHAWAN, GAURAV y
SUTHERLAND, JEFFREY

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Limitación de aplicaciones de empresa y ajustes en dispositivos

Antecedentes

Antecedentes y técnica relevante

Los ordenadores y los sistemas informáticos han afectado casi a todos los aspectos de la vida moderna. Los ordenadores están generalmente involucrados en la gestión del trabajo, ocio, servicios médicos, transporte, entretenimiento, hogar, etc.

Además, la funcionalidad del sistema informático se puede potenciar mediante la capacidad de un sistema informático para interconectarse con otros sistemas informáticos a través de conexiones de red. Las conexiones de red pueden incluir, pero no se limitan a, conexiones a través de Ethernet cableado o inalámbrico, conexiones celulares, o incluso conexiones de ordenador a ordenador a través de conexiones en serie, en paralelo, de USB, u otras. Las conexiones permiten que un sistema informático acceda a servicios en otros sistemas informáticos y que reciba rápida y eficientemente datos de aplicación a partir de otros sistemas informáticos.

Las redes actuales han permitido que se conecten en red muchos tipos nuevos y diferentes de dispositivos. Una de las principales tendencias en la TI en los últimos años ha sido el impulso hacia una “orientación al consumidor de TI”, que es una expresión que describe cómo la tecnología de consumo, de teléfonos a PC, está permeando en toda forma y modo en las organizaciones empresariales. Y cada vez más, los dispositivos que están apareciendo son propiedad y responsabilidad del empleado más que de la organización para la que este trabaja. Esto se observa, sobre todo, en la categoría de los dispositivos de tipo teléfono inteligente, pero más recientemente también en tabletas u otros factores de forma de dispositivo portátil que están apareciendo cada vez más en el lugar de trabajo. A medida que las organizaciones adoptan la orientación al consumidor, las TI han de considerar cuánto control pueden ejercer las mismas sobre el dispositivo de un usuario, ya sea este una propiedad personal o propiedad de la empresa, y cuánta gestión del dispositivo es “lo suficientemente buena”.

El dispositivo puede ser sustraído o el dispositivo puede alojar una aplicación móvil que resulta ser un troyano que recopila contraseñas guardadas o registra pulsaciones de teclas y otros datos. Por lo tanto, puede haber un deseo de controlar qué datos y aplicaciones se pueden almacenar en el dispositivo. No obstante, puesto que el dispositivo se puede usar para fines personales, y no solo fines empresariales, también puede haber un cierto deseo por parte del usuario por hacer que las aplicaciones y los datos personales no estén bajo el control de la empresa. Las soluciones previas o bien son demasiado férreas con la gestión y toman un control completo sobre los dispositivos de los usuarios o bien son demasiado suaves con la gestión y la seguridad, permitiendo un acceso sin apenas trabas por parte de un usuario de recursos de empresa usando sus dispositivos.

La materia objeto reivindicada en el presente documento no está limitada a realizaciones que resuelvan desventaja alguna o que operen únicamente en entornos tales como los anteriormente descritos. En su lugar, estos antecedentes se proporcionan únicamente para ilustrar un área de tecnología ejemplar en la que pueden ponerse en práctica algunas realizaciones descritas en el presente documento.

La técnica anterior relevante en el campo técnico está representada por el documento US 2012/129503 A1, que desvela un procedimiento para gestionar y controlar la implementación de aplicaciones alojadas en dispositivos móviles en un entorno de empresa.

Breve resumen

Una realización ilustrada en el presente documento incluye un procedimiento de instalación de aplicaciones y de establecimiento de la configuración en un dispositivo. El procedimiento incluye recibir una entrada de usuario. La entrada de usuario indica un nivel de control que un usuario desea dar a una empresa sobre un dispositivo. El procedimiento incluye adicionalmente determinar, basándose en el nivel de control indicado por el usuario, un conjunto de aplicaciones que se permite instalar en el dispositivo. El conjunto de aplicaciones que se permite instalar en el dispositivo está limitado por el nivel de control indicado por el usuario. El procedimiento incluye adicionalmente autorizar la instalación del conjunto de aplicaciones en el dispositivo al tiempo que se restringe la instalación de otras aplicaciones que estarían autorizadas si el usuario hubiera seleccionado un nivel diferente de control que el usuario desea dar a la empresa sobre el dispositivo.

Este resumen se proporciona para introducir una selección de conceptos en una forma simplificada, que se describen adicionalmente a continuación en la descripción detallada. No se pretende que este resumen identifique características clave o características esenciales de la materia objeto reivindicada, ni se pretende que se use como una ayuda para determinar el ámbito de la materia objeto reivindicada.

Características y ventajas adicionales se expondrán en la descripción que sigue y, en parte, serán obvias a partir de la descripción, o se pueden aprender mediante la práctica de las enseñanzas en el presente documento. Las características y ventajas de la invención se pueden realizar y obtener por medio de los instrumentos y

combinaciones particularmente señalados en las reivindicaciones adjuntas. Las características de la presente invención se harán más plenamente evidentes a partir de la siguiente descripción y las reivindicaciones adjuntas, o se pueden aprender mediante la práctica de la invención tal como se expone en lo sucesivo en el presente documento.

Breve descripción de los dibujos

Para describir la manera en la que pueden obtenerse las ventajas y características anteriormente descritas, así como otras ventajas y características, se presentará una descripción más particular de la materia objeto brevemente descrita por referencia a realizaciones específicas que se ilustran en los dibujos adjuntos. Entendiendo que estos dibujos representan únicamente realizaciones típicas y que, por lo tanto, no se ha de considerar que limiten el ámbito, se describirán y explicarán realizaciones con detalle y especificidad adicional a través del uso de los dibujos adjuntos, en los que:

la figura 1 ilustra un entorno que incluye una red de empresa y un dispositivo conectado a la red de empresa;
la figura 2 ilustra una interfaz de usuario para autenticar a un usuario en una red de empresa;
la figura 3 ilustra una interfaz de usuario para que un usuario seleccione aplicaciones de empresa para su instalación en un dispositivo;
la figura 4 ilustra un flujo de mensajes para instalar aplicaciones de empresa en un dispositivo;
la figura 5 ilustra un procedimiento de instalación de aplicaciones en un dispositivo; y
la figura 6 ilustra un procedimiento de instalación de aplicaciones y de establecimiento de la configuración en un dispositivo.

Descripción detallada

Algunas realizaciones descritas en el presente documento incluyen una funcionalidad para gestionar dispositivos que, en algunas realizaciones, pueden ser dispositivos de propiedad personal que se usan en un entorno de empresa. En particular, un dispositivo puede ser controlado generalmente por un usuario y no por la empresa, pero se puede seguir usando en el entorno de empresa con un control apropiado en el dispositivo. En particular, la empresa puede ejercer un control sobre determinados aspectos del dispositivo, al tiempo que se permite que el usuario controle otros aspectos del dispositivo sin interferencia o intromisión por parte de la empresa. Este enfoque de gestión equilibra satisfacer las necesidades de seguridad de la empresa al tiempo que se mantiene el control del usuario sobre el dispositivo y minimizar cualquier impacto del rendimiento del dispositivo. Algunas realizaciones abordan cómo entregar la configuración y el software que necesitan los usuarios en el contexto empresarial, como aplicaciones y acceso a datos en cualquier dispositivo, con el suficiente control de TI para aseverar que el dispositivo es de confianza, al tiempo que se evita comprometer la privacidad del usuario en su dispositivo.

Diversas realizaciones pueden mostrar diversos aspectos. Por ejemplo, algunas realizaciones pueden implementar una experiencia de inscripción en la que un usuario puede pasar por un componente de SO integrado para conectarse al entorno de trabajo de empresa. Alternativa o adicionalmente, algunas realizaciones pueden mostrar una colección de cantidad limitada de inventario que es suficiente para evaluar la seguridad del dispositivo pero no suficiente para tomar el control del dispositivo y entrometerse en la privacidad del usuario. Alternativa o adicionalmente, algunas realizaciones pueden mostrar una distribución de aplicaciones a petición con reconocimiento de rendimiento en la que se usa un servicio de notificación para iniciar la instalación de aplicaciones. Alternativa o adicionalmente, algunas realizaciones pueden mostrar desconexión con respecto a una empresa que bloquea todas las aplicaciones y/o restablece los ajustes obtenidos de la empresa.

Gestión de dispositivos de empresa

Con cada vez más personas proporcionando su propio hardware para el trabajo, “trae tu propio dispositivo” (BYOD) se está volviendo más común y los profesionales de TI desean tener la confianza en que pueden dar soporte a aquellos de sus clientes que siguen esta tendencia. La presencia de BYOD no cambia la necesidad de que los profesionales de TI gestionen, aseguren y sigan siendo responsables de los recursos de red de una organización. A menudo, las directivas escritas son ineficaces para imponer directivas de empresa.

Algunas realizaciones ilustradas en el presente documento pueden incluir una funcionalidad para gestionar un dispositivo de propiedad personal en una empresa al entregar los ajustes y el software que necesitan los usuarios, como aplicaciones y acceso a datos en cualquier dispositivo, con el suficiente control de TI para aseverar que el dispositivo es de confianza, al tiempo que se evita comprometer en modo alguno la privacidad del usuario en su dispositivo personal. Se ha de entender que los conceptos descritos en el presente documento también son aplicables a otros tipos de dispositivos que se usan en un ajuste de empresa, tales como dispositivos propiedad de la empresa en los que los usuarios esperan privacidad con respecto a una selección de aplicaciones, datos, ajustes, etc.

Haciendo referencia a continuación a la figura 1, se ilustra un dispositivo 102. El dispositivo 102 puede ser un dispositivo informático tal como un teléfono celular, PDA, tableta, portátil, u otro dispositivo que un usuario puede optar por conectar a una red de entorno de empresa 110. Algunas realizaciones integran un componente de gestión ligera (el agente 104) integrado en el sistema operativo 106 del dispositivo que se puede comunicar con una

infraestructura de gestión 108 en la red de empresa 110 para entregar unas aplicaciones de línea de empresa (LOB) (que a veces se denominan coloquialmente y en el presente documento como aplicaciones) a los usuarios.

La solución de gestión tiene dos porciones instaladas en cliente: el componente de gestión de sistema, que se puede denominar en el presente documento como agente 104; y una interfaz de usuario, que se puede denominar como portal de autoservicio, o SSP 112, que el usuario del dispositivo usa para navegar en busca de e instalar aplicaciones de LOB facilitadas al mismo. El SSP 112 se puede implementar en una serie de formas diferentes, tales como una aplicación en el dispositivo 102, una página/servicio web que se ejecuta en el navegador del usuario en el dispositivo 102, u otra interfaz. En particular, no es necesario que una solicitud para instalar una aplicación para el usuario del dispositivo 102 se origine en el propio dispositivo 102. En algunas realizaciones, esto se puede realizar a partir de otra máquina. En el ejemplo ilustrado, no obstante, ambas porciones de la solución de gestión instalada en el cliente se pueden diseñar para ser ciudadanos con buen comportamiento del sistema operativo 106 en términos de experiencia de usuario, gestión de alimentación/duración de la batería, reconocimiento de redes (para redes de uso medido), y la funcionalidad global.

El agente 104 realiza la mayor parte de la investigación y desarrollo difícil en el dispositivo de cliente 102. Este configura el dispositivo de cliente 102 para comunicarse con la infraestructura de gestión 108 de la organización; periódicamente, o por un cierto mecanismo desencadenante de la infraestructura de gestión 108, sincroniza con la infraestructura de gestión 108 para buscar cualquier aplicación de LOB actualizada y aplicar las últimas directivas de ajustes configuradas por la TI para el dispositivo 102; y maneja la descarga y la instalación reales de cualquier aplicación de LOB que desea instalar el usuario. Por último, si el usuario o el administrador opta por eliminar el dispositivo 102 de la infraestructura de gestión 108, este borra configuración del propio agente 104 y deshabilita, o borra de forma segura, toda aplicación de LOB que el usuario instalara del SSP 112.

Lo siguiente ilustra a continuación detalles adicionales con respecto a conectar el dispositivo de cliente 102 a la infraestructura de gestión 108. En algunas realizaciones, conectar un dispositivo de cliente 102 a la infraestructura de gestión 108 comienza con que un administrador de TI especifique el grupo de usuarios, tal como, por ejemplo, un grupo de usuarios de dominio de Active Directory® (AD) (facilitado por Microsoft® Corporation de Redmond, Washington) que están autorizados a conectar los dispositivos 108 en la empresa de red 110. El administrador también tiene la opción de especificar el número máximo de dispositivos permitidos por usuario u otras restricciones relacionadas con una directiva de inscripción por usuario. Por ejemplo, otras consideraciones de directivas de inscripción por usuario pueden especificar que un usuario solo se puede inscribir cuando está en una red particular, con autenticación de múltiples factores, dentro de un periodo de tiempo dado, etc. Tal como se ilustra en la figura 2, un usuario autorizado selecciona un enlace de aplicaciones de empresa 202 de una interfaz de usuario 200 y suministra sus credenciales de empresa 204. El agente 104 realiza entonces una consulta de servicio para localizar la infraestructura de gestión 108 de la organización.

Una vez que el agente 104 ha hallado la dirección correcta, este establece una conexión segura con la infraestructura de gestión 108 y autentica al usuario. Si el usuario se autentica con éxito y ha sido autorizado por el administrador a conectar dispositivos (por ejemplo, el dispositivo 102), la red de empresa 110 emite las órdenes correctas para configurar el agente 104 para sus comunicaciones en curso con la infraestructura de gestión 108. Una vez se ha completado, se insta al usuario a instalar el SSP 112 al tiempo que el agente 104 completa la conexión en el segundo plano. Como alternativa, el SSP 112 puede ser instalado automáticamente por la infraestructura de gestión en el momento de la inscripción. Mientras que en el ejemplo ilustrado, un usuario se ha autenticado ante la infraestructura de gestión 108, en realizaciones alternativas o adicionales, el propio dispositivo se puede autenticar ante la infraestructura de gestión. Por ejemplo, el dispositivo 102 se podría redirigir a un servicio de gestión que permitiría que el dispositivo se inscribiera en nombre de la empresa.

A continuación, el agente 104 inicia automáticamente una sesión con la infraestructura de gestión 108, usando los ajustes que ya obtuvo este. Esta sesión y toda sesión posterior se pueden realizar a través de una conexión segura. Esta sesión inicial completa el registro del dispositivo 102 con la red de empresa 110 al suministrar alguna información básica de dispositivo tal como el fabricante y el modelo del dispositivo 102, la versión de sistema operativo del dispositivo 102, capacidades de dispositivo, y otra información de hardware para el dispositivo 102. Esto permite que los administradores de TI supervisen qué tipos de dispositivos se están conectando a la organización, de tal modo que los mismos puedan mejorar las aplicaciones y servicios que estos entregan a los usuarios con el paso del tiempo.

A continuación de la sesión inicial, el agente 104 inicia la comunicación con la infraestructura de gestión 108 en dos circunstancias:

En primer lugar, como una tarea de mantenimiento que se ejecuta según una programación previamente establecida, o a partir de mecanismos desencadenantes de infraestructura de gestión u otros mecanismos desencadenantes, que no afecta a la experiencia de usuario. Las actividades realizadas durante estas sesiones de mantenimiento se centran en notificar información de hardware actualizada a la infraestructura de gestión 108, aplicar cambios a las directivas de ajustes para el dispositivo 102, notificar el cumplimiento de vuelta a la infraestructura de gestión 108 y aplicar actualizaciones de aplicaciones a las aplicaciones de LOB, o reintentar cualquier instalación de aplicaciones de LOB previamente fallida iniciada desde el SSP 112.

En segundo lugar, el agente 104 se comunicará con la infraestructura de gestión 108 en cualquier momento en el que el usuario inicie una instalación de aplicaciones a partir del SSP 112. En algunas realizaciones, estas sesiones iniciadas por el usuario están centradas únicamente en la instalación de aplicaciones y no realizan las actividades de mantenimiento y gestión descritas en el primer caso.

Con independencia de si una sesión es iniciada automáticamente por una tarea de mantenimiento programada o manualmente por el usuario, el dispositivo del cliente 102 continúa comportándose bien en relación con el estado de la batería en el dispositivo y sus condiciones de red actuales.

Gestión de directivas de ajustes

Tal como ya se ha analizado, el acceso a las aplicaciones de LOB habitualmente requiere que los sistemas cumplan con directivas básicas de seguridad y de protección de datos. A partir de la infraestructura de gestión 108, el administrador de TI es capaz de configurar un conjunto de directivas que este crea importantes para dar a la TI las garantías que necesitan sin afectar seriamente a la experiencia del usuario con su dispositivo. En particular, los administradores pueden imponer directivas de contraseñas y apagar determinados periféricos.

Además de las directivas configurables descritas anteriormente, el agente 104 también se puede usar para configurar automáticamente otros ajustes tales como ajustes de red, configuración de VPN, ajustes de WiFi, etc., de tal modo que el dispositivo 102 gestionado se puede conectar fácilmente con una red de empresa 110. Por último, el agente 104 también puede supervisar y realizar notificaciones acerca del cumplimiento del dispositivo 102 con un conjunto de directivas.

Aprovechando esta información de cumplimiento, los administradores de TI pueden controlar más eficazmente el acceso a los recursos corporativos en la red de empresa 110 si se determina que un dispositivo está en riesgo. Una vez más, la experiencia básica del usuario con el dispositivo se deja intacta y su privacidad personal se mantiene.

En algunas realizaciones, las directivas que pueden ser impuestas por la empresa u otras terceras partes pueden ser configurables por el usuario del dispositivo 102. Por ejemplo, un usuario puede desear aceptar algunas directivas al tiempo que rehúsa aceptar otras directivas que la empresa querría imponer. Por lo tanto, un usuario puede aceptar un nivel de control que el usuario desea dar a una empresa sobre el dispositivo. Este nivel de control indicado por el usuario del dispositivo 102 puede afectar a qué ajustes configura automáticamente la empresa en el dispositivo 102 y qué aplicaciones desea permitir la empresa que se instalen en el dispositivo 102.

Por ejemplo, si un usuario no desea aceptar todas las directivas que querría imponer la empresa, entonces el dispositivo 102 solo puede tener permitido instalar un conjunto limitado de aplicaciones en el dispositivo al tiempo que se restringe que este instale otras aplicaciones en el dispositivo. A modo de ilustración, el SSP 112 puede proporcionar una interfaz de usuario que permite que un usuario seleccione directivas que el usuario desea aceptar. Por ejemplo, la interfaz de usuario puede proporcionar una lista de directivas con un conjunto de casillas de verificación en las que el usuario puede seleccionar, al marcar casillas de verificación, qué directivas el usuario desea haber impuesto en el dispositivo 102. Como alternativa, una interfaz de asistente u otra interfaz se puede emplear para obtener información acerca de qué directivas desea haber impuesto el usuario en el dispositivo 102.

Las directivas de entre las que puede seleccionar el usuario pueden incluir, por ejemplo, restricciones en el dispositivo. Por ejemplo, tales restricciones pueden incluir artículos tales como requerir una contraseña en el dispositivo, requerir que determinadas aplicaciones o software se instalen en el dispositivo, requerir determinados ajustes en el dispositivo, limitar el dispositivo a su uso con determinados tipos o determinadas redes, etc.

Alternativa o adicionalmente, las directivas de entre las que puede seleccionar el usuario pueden incluir una directiva relacionada con los controles de acceso a datos en el dispositivo 102. Por ejemplo, el usuario puede indicar que la empresa es capaz de bloquear completamente el dispositivo, borrar todos los datos en el dispositivo, restablecer el dispositivo a los ajustes de fábrica, borrar todos los datos de empresa en el dispositivo, borrar datos asociados con determinadas aplicaciones en el dispositivo (tales como aplicaciones de empresa, aplicaciones de correo, etc.) etc.

Gestión de aplicaciones de LOB

El análisis previo se ha centrado en las mecánicas del dispositivo de cliente 102 y la infraestructura de gestión 108 junto con las necesidades del administrador de TI. No obstante, un aspecto importante de lo anterior es el beneficio que se puede proporcionar al usuario final al habilitar el acceso a sus aplicaciones de LOB.

Hay varias categorías y tipos diferentes de aplicaciones que una TI puede publicar para los usuarios en el SSP 112. Por ejemplo, una TI puede publicar: aplicaciones desarrolladas internamente, desarrolladas por la empresa; aplicaciones producidas por proveedores de software independientes que tienen licencia de la organización para su distribución interna; enlaces web que inician sitios web y aplicaciones basadas en web directamente en el navegador; enlaces a listados de aplicaciones en otros catálogos de aplicaciones (esta es una forma conveniente de para que una TI haga que los usuarios tomen conciencia de las aplicaciones de empresa útiles que están públicamente disponibles); etc.

Debido a que el usuario especificó sus credenciales corporativas como parte de la conexión inicial con la infraestructura de gestión 108, tal como se ilustra en la figura 2, el administrador de TI puede especificar entonces qué aplicaciones se publican a cada usuario individualmente. Como resultado, los usuarios solo ven aquellas aplicaciones que son aplicables a los mismos en el SSP 112. La figura 3 ilustra un ejemplo de la experiencia de usuario del SSP 112 para un usuario que navega en busca de aplicaciones de LOB en el SSP 112 para una empresa ficticia denominada “Woodgrove”.

En particular, algunas realizaciones se pueden implementar en un entorno de mercado cerrado de aplicaciones. En un entorno de ese tipo, el escenario de usuario habitual es que los usuarios solo tienen permitido instalar aplicaciones de entre un conjunto preaprobado de aplicaciones disponibles en un mercado autorizado. Por ejemplo, usando el dispositivo Windows Phone™ facilitado por Microsoft® Corporation de Redmond, Washington, un usuario solo es capaz habitualmente de instalar aplicaciones a partir del catálogo oficial de aplicaciones de Microsoft® que ofrece aplicaciones que se han evaluado y preaprobado para ser ofrecidas en el catálogo oficial de aplicaciones. En otras realizaciones, el entorno de mercado cerrado de aplicaciones puede ser cerrado en lo que respecta a determinados tipos de aplicaciones, pero abierto a otros tipos de aplicaciones. Por ejemplo, usando Windows 8 facilitado por Microsoft Corporation de Redmond, Washington, un usuario solo es capaz de instalar Aplicaciones de la Tienda de Windows de entre el catálogo oficial de aplicaciones en la interfaz de Windows 8 (tal como la ilustrada en la figura 3), mientras que otras aplicaciones se pueden instalar en la interfaz de escritorio con poca o ninguna restricción.

Algunas realizaciones se pueden ampliar para permitir que aplicaciones que son de un estilo o formato a ofrecer habitualmente en un entorno de mercado cerrado de aplicaciones, pero que no se ofrecen generalmente en el entorno de mercado cerrado de aplicaciones, sean no obstante “instaladas en modo de prueba” con el fin de permitir que aplicaciones para empresas específicas, no ofrecidas en el mercado cerrado, se instalen no obstante en el dispositivo 102. Por ejemplo, un dispositivo Windows® Phone sería capaz de instalar aplicaciones no ofrecidas en el catálogo oficial de aplicaciones. Como alternativa, un dispositivo con Windows® 8 sería capaz de instalar Aplicaciones de la Tienda de Windows, no disponibles en el catálogo oficial de aplicaciones.

En algunas realizaciones, esto, o habilitar determinados ajustes o funciones de gestión, se puede lograr mediante la instalación de una clave de instalación de prueba 114 en el dispositivo 102 que, siempre que la clave de instalación de prueba 114 sea válida, permite que el dispositivo 102 instale a modo de prueba las aplicaciones 116 a partir de un servidor de contenidos 118 de la infraestructura de gestión, en donde las aplicaciones 116 no se ofrecen generalmente en el mercado de aplicaciones cerrado 120, tales como las aplicaciones 122.

No obstante, aunque las aplicaciones 116 que se pueden instalar usando la clave de instalación de prueba 114 no se ofrecen generalmente en el mercado de aplicaciones cerrado 120, en algunas realizaciones, una autoridad central ha de seguir validando y autorizando que se instalen en el dispositivo las aplicaciones 116. Por ejemplo, la misma autoridad central que valida y autoriza las aplicaciones provistas en el mercado de aplicaciones cerrado 120 puede validar y autorizar las aplicaciones que se pretende instalar a modo de prueba en el dispositivo 102, siempre que el dispositivo 102 tenga una clave de instalación de prueba 114 válida (u otra indicación de que el dispositivo está autorizado a realizar instalaciones a modo de prueba de aplicaciones).

La clave de instalación de prueba 114 se puede obtener en una serie de formas diferentes. Por ejemplo, en algunas realizaciones, la clave de instalación de prueba 114 se puede adquirir del mercado de aplicaciones cerrado 120. En otras realizaciones, la clave puede ser adquirida por la empresa a partir de una autoridad central. En algunas realizaciones, una única clave de instalación de prueba 114 puede ser válida para un número particular de instalaciones en dispositivos. Por ejemplo, la clave de instalación de prueba se puede instalar en múltiples dispositivos diferentes en cualquier momento dado.

En algunas realizaciones, cuando el usuario opta por instalar una aplicación a partir del SSP 112, la solicitud se envía a la infraestructura de gestión 108 y se proporciona un enlace de descarga al agente 104. El agente 104 descarga entonces la aplicación, verifica la validez del contenido, comprueba la firma, e instala la aplicación. Todo esto tiene lugar habitualmente dentro de un plazo de segundos y, en general, es invisible para el usuario. En el caso de que tenga lugar un error durante cualquier parte de este proceso (por ejemplo, la ubicación del contenido no está disponible), el agente 104 pone en cola la aplicación para un reintento durante su siguiente sesión de mantenimiento regularmente programada. En cualquier caso, el agente 104 notifica el estado de la instalación de vuelta a la infraestructura de gestión 108. La figura 4 detalla esta interacción.

En particular, la figura 4 ilustra en 402 que el SSP 112 obtiene una lista de aplicaciones dirigidas a partir de un servicio de gestión 128 en la infraestructura de gestión 108. El servicio de gestión 128, tal como se ilustra en 404, en la infraestructura de gestión 108 envía una lista de aplicaciones de vuelta al SSP 112 en donde la lista de aplicaciones incluye una enumeración de aplicaciones disponibles para ser instaladas por el dispositivo 102. Tal como se ilustra en 406, el usuario 126 interacciona con el SSP 112 y solicita la instalación de una aplicación. Tal como se ilustra en 408, el SSP 112 solicita que la aplicación solicitada por el usuario sea instalada por el servicio de gestión 128. Tal como se ilustra en 410, el servicio de gestión 128 confirma la solicitud. Tal como se ilustra en 412, el SSP 112 da un toque al agente 104 indicando al agente que se debería instalar la aplicación seleccionada por el usuario 126. Tal como se ilustra en 414, el agente 104 confirma el toque al SSP 112. Tal como se ilustra en 416, el

agente 104 solicita detalles de aplicación y confirma la solicitud de instalación por el usuario 126 al servicio de gestión 128. Tal como se ilustra en 418, el servicio de gestión confirma las solicitudes de aplicación al agente 104. Tal como se ilustra en 420, el agente 104 solicita un contenido de aplicación a partir del servicio de contenidos 118 en la infraestructura de gestión 108. Tal como se ilustra en 422, el servicio de contenidos 118 devuelve el contenido de aplicación al agente 104 en el dispositivo 102. Tal como se ilustra en 424, el agente 104 se comunica con un gestor de paquetes 130 en el dispositivo 102 indicando que la aplicación se debería añadir para el usuario 126. Tal como se ilustra en 426, el gestor de paquetes 130 indica que la instalación de la aplicación se ha completado. Tal como se ilustra en 428, el agente 104 informa al servicio de gestión 128 de que la aplicación se ha instalado. Tal como se ilustra en 430, el servicio de gestión 128 confirma al agente 104 que se ha registrado la instalación de la aplicación seleccionada por el usuario.

En algunas realizaciones alternativas, el propio mercado de aplicaciones cerrado 120 puede tener determinados ofrecimientos de aplicaciones disponibles que solo están disponibles para los dispositivos con una clave de instalación de prueba instalada en el dispositivo 102. Por ejemplo, el mercado de aplicaciones cerrado 120 podría proporcionar un conjunto de aplicaciones 122 generalmente a los dispositivos, pero proporcionar aplicaciones adicionales 124 para su instalación a los dispositivos basándose en las claves de instalación de prueba instaladas en los dispositivos. Las aplicaciones adicionales disponibles para su instalación pueden depender de qué clave de instalación de prueba se instala en el dispositivo. Por lo tanto, el mercado de aplicaciones cerrado 120 podría mantener un conjunto de aplicaciones, en nombre de la empresa, para su instalación en dispositivos autorizados por la empresa.

Como parte de sus sesiones de mantenimiento regulares, el agente 104 realizará un inventario de qué aplicaciones de LOB están instaladas actualmente y notificará esa información de vuelta a la infraestructura de gestión 108 de tal modo que el administrador de TI puede gestionar eficazmente sus aplicaciones de LOB. En algunas realizaciones, solo las aplicaciones que se instalaron a través del SSP 112 y el dispositivo de cliente 102 se incluyen en este inventario a partir de un dispositivo. En algunas realizaciones, las aplicaciones generalmente disponibles instaladas a partir de un mercado de aplicaciones cerrado no se notifican como parte del inventario. En algunas realizaciones, el agente 104 se puede restringir solo a ser capaz de realizar un inventario de las aplicaciones de empresa 116 y no es capaz de realizar un inventario de las aplicaciones 122 en el dispositivo 102 que el usuario ha instalado para su uso personal.

En cualquier momento en el que el administrador de TI publique una actualización para una aplicación que se ha instalado en un dispositivo 102 autorizado por la empresa, el agente 104 descargará e instalará automáticamente la actualización durante su siguiente sesión de mantenimiento regular. Como alternativa, durante una ventana de mantenimiento regular, la infraestructura de gestión 108 puede detectar que una actualización está disponible y es aplicable, y como resultado, notificar al usuario.

Desconexión con respecto a la infraestructura de gestión 108

Se ilustran a continuación detalles acerca de cómo desconectar, de la infraestructura de gestión 108, un dispositivo. La desconexión puede ser iniciada o bien localmente por el usuario o bien remotamente por el usuario o el administrador de TI. Los usuarios pueden optar por desconectar por cualquiera de una serie de razones, incluyendo salir de la empresa u obtener un nuevo dispositivo y dejar de necesitar el acceso a sus aplicaciones de LOB en el dispositivo antiguo. Los administradores pueden optar por desconectar de un usuario el dispositivo después de que los mismos hayan salido de la empresa o debido a que, de forma regular, el dispositivo no está cumpliendo con la directiva de ajustes de seguridad de la organización. En otra realización alternativa, la empresa puede desconectar automáticamente un dispositivo de usuario 102 si el dispositivo no se ha conectado a la red de empresa 110 durante un periodo de tiempo dado.

Durante la desconexión, el agente 104 realiza una serie de acciones (y/o deja de poner en práctica una serie de acciones). Por ejemplo, el agente 104 retira el acceso a todas las aplicaciones que el usuario obtuvo de la empresa. En algunas realizaciones, el agente 104 puede bloquear el acceso a las aplicaciones 116 o puede eliminar completamente del dispositivo 102 las aplicaciones 116. El agente 104 deja de imponer las directivas de ajustes que ha aplicado la infraestructura de gestión 108. El agente 104 notifica la desactivación con éxito a la infraestructura de gestión 108 si el administrador inició el proceso. El agente 104 elimina la configuración del agente 104, incluyendo la tarea de mantenimiento programada. Una vez se ha completado, el agente 104 permanece inactivo a menos que el usuario lo reconecte a la infraestructura de gestión 108 u otra infraestructura de gestión.

El siguiente análisis se refiere a continuación a una serie de procedimientos y actos de procedimiento que se pueden realizar. Aunque los actos de procedimiento se pueden analizar en un determinado orden o ilustrarse en un diagrama de flujo como que tienen lugar en un orden particular, no se requiere ordenación particular alguna salvo que se exponga específicamente, o se requiera debido a que un acto depende de que se complete otro acto antes de que se realice el acto.

Haciendo referencia a continuación a la figura 5, se ilustra un procedimiento 500. El procedimiento 500 incluye actos para instalar aplicaciones en un dispositivo. El dispositivo está configurado en general para usarse en un entorno de mercado cerrado que solo permite que se instalen las aplicaciones generalmente disponibles del mercado cerrado.

El procedimiento 500 incluye determinar que el dispositivo ha sido autorizado a instalar aplicaciones fuera de un conjunto de aplicaciones generalmente disponibles en el mercado cerrado y a partir de un conjunto de aplicaciones disponibles solo a usuarios de una empresa particular (el acto 502). Por ejemplo, se puede poner en práctica el procedimiento 500, en el que determinar que el dispositivo ha sido autorizado a instalar aplicaciones fuera de un conjunto de aplicaciones generalmente disponibles en el mercado cerrado comprende determinar que se ha instalado una clave de instalación de prueba en el dispositivo. Un ejemplo de ese tipo se ilustra en la figura 1 mediante el uso de la clave de instalación de prueba 114 con el dispositivo 102.

El procedimiento 500 incluye adicionalmente determinar que una aplicación, que generalmente no está disponible en el mercado cerrado, ha sido verificada por una autoridad central (el acto 504). Se puede poner en práctica el procedimiento 500, en el que determinar que una aplicación que generalmente no está disponible en el mercado cerrado ha sido verificada por una autoridad central incluye determinar que la aplicación ha sido verificada por una autoridad central responsable del mercado cerrado. Por ejemplo, si Microsoft® dirige un mercado cerrado, pero la aplicación no es proporcionada por el mercado cerrado dirigido por Microsoft® Corporation, Microsoft® Corporation podría verificar, no obstante, la aplicación. Por ejemplo, tal como se ilustra en la figura 1, la entidad responsable de mantener el mercado 120 y verificar las aplicaciones 122 también puede verificar las aplicaciones 116 a pesar del hecho de que las aplicaciones 116 no se ofrecen en el mercado 120. Por lo tanto, las aplicaciones 116 disponibles en la red de empresa 110 no obstante tienen una cadena de autoridad con una autoridad central.

El procedimiento 500 incluye adicionalmente instalar la aplicación en el dispositivo a pesar del hecho de que el dispositivo está configurado en general para usarse en un entorno de mercado cerrado (en 506).

El procedimiento 500 puede incluir adicionalmente proporcionar una interfaz de usuario a un usuario para permitir que un usuario seleccione la aplicación de entre un conjunto de aplicaciones disponibles para dispositivos autorizados a conectar con la empresa particular; recibir una entrada de usuario que selecciona la aplicación; notificar a un servicio que el usuario ha seleccionado la aplicación; recibir una notificación a partir del servicio de que la aplicación está disponible para ser instalada; y en el que instalar la aplicación en el dispositivo se realiza de una forma que minimiza la alteración para el dispositivo. Ejemplos de esta funcionalidad se ilustran en la figura 3 y 4. En particular, la figura 3 ilustra una interfaz de usuario que se puede presentar a un usuario para permitir que un usuario seleccione aplicaciones para su instalación. La figura 4 ilustra un ejemplo de comunicación entre diversas entidades para permitir que un usuario indique qué aplicaciones querría instalar el usuario en el proceso para instalar las aplicaciones. En algunas de tales realizaciones, la aplicación se puede instalar cuando el dispositivo determina que este tiene suficientes recursos libres para instalar la aplicación sin afectar gravemente a la experiencia de usuario del dispositivo.

El procedimiento 500 puede incluir adicionalmente mantener una enumeración de aplicaciones a partir del conjunto de aplicaciones disponibles solo a usuarios de una empresa particular que se han instalado en el dispositivo. En particular, se puede mantener un manifiesto en el dispositivo 102 y el agente 104 que enumera las diversas aplicaciones que se han instalado en el dispositivo 102. Esto se puede usar para notificar, a una autoridad central de empresa, información acerca de qué aplicaciones se instalan en el dispositivo 102.

El procedimiento 500 puede incluir adicionalmente proporcionar una notificación a un administrador de organización. La notificación puede incluir una enumeración de todas las aplicaciones a partir del conjunto de aplicaciones disponibles solo a usuarios de una empresa particular que se han instalado en el dispositivo sin identificar en la notificación otras aplicaciones que se han instalado en el dispositivo. Por ejemplo, la notificación puede identificar cualquiera de las aplicaciones 116 que se han instalado en el dispositivo 102 pero no identificará aplicación alguna seleccionada de entre el conjunto de aplicaciones 122 que se han instalado en el dispositivo 102.

El procedimiento 500 incluye adicionalmente diversos actos para retirar el dispositivo 102 de la red de empresa 110. Por ejemplo, el procedimiento 500 puede incluir desautorizar el dispositivo de tal modo que el dispositivo ya no puede instalar aplicaciones de entre el conjunto de aplicaciones disponibles solo a usuarios de una empresa particular; deshabilitar o eliminar toda aplicación de entre el conjunto de aplicaciones disponibles solo a usuarios de una empresa particular que ya se haya instalado en el dispositivo; y hacer inaccesibles los datos asociados con cualquier aplicación de entre el conjunto de aplicaciones disponibles solo a usuarios de una empresa particular que ya se han instalado en el dispositivo. En algunas realizaciones, esto se puede realizar en respuesta a que el dispositivo no entre en contacto con una infraestructura de gestión durante un periodo de tiempo predeterminado. En realizaciones alternativas o adicionales, esto se puede realizar en respuesta a que un usuario indique el deseo de desconectar el dispositivo de la empresa. En aún otra realización adicional o alternativa, esto se puede realizar en respuesta a que un administrador indique el deseo de desconectar el dispositivo de la empresa.

Haciendo referencia a continuación a la figura 6, se ilustra un procedimiento 600. El procedimiento 600 incluye actos para instalar aplicaciones y establecer la configuración en un dispositivo. El procedimiento 600 incluye recibir una entrada de usuario de un usuario de un dispositivo, indicando la entrada de usuario un nivel de control que el usuario desea dar a una empresa sobre el dispositivo (el acto 602). Se puede poner en práctica el procedimiento 600, en el que la entrada de usuario comprende que un usuario indique que la empresa puede imponer una o más restricciones en el dispositivo. Por ejemplo, las una o más restricciones pueden incluir una o más de requerir una contraseña, requerir que determinadas aplicaciones se instalen en el dispositivo, limitar el acceso del dispositivo a determinadas

redes o similares. Alternativa o adicionalmente, se puede poner en práctica el procedimiento 600, en el que la entrada de usuario comprende que un usuario indique que la empresa puede controlar el acceso a datos en el dispositivo. Por ejemplo, la entrada de usuario puede indicar que la empresa puede realizar uno o más de bloquear el dispositivo, borrar todos los datos de usuario en el dispositivo, restablecer el dispositivo a los ajustes de fábrica, borrar todos los datos de empresa en el dispositivo, borrar datos asociados con determinadas aplicaciones en el dispositivo, o similares. Se puede poner en práctica el procedimiento 600, en el que la entrada de usuario comprende que un usuario seleccione una pluralidad de artículos de entre una lista predeterminada, tal como una lista de casillas de verificación, que el usuario desea dejar que la empresa controle o restrinja en el dispositivo.

El procedimiento 600 incluye adicionalmente determinar, basándose en el nivel de control indicado por un usuario, un conjunto de aplicaciones que el usuario tiene permitido instalar en el dispositivo (el acto 604). El conjunto de aplicaciones que el usuario tiene permitido instalar en el dispositivo está limitado por el nivel de control indicado por el usuario.

El procedimiento 600 incluye adicionalmente autorizar al dispositivo a instalar el conjunto de aplicaciones al tiempo que se restringe que el dispositivo instale otras aplicaciones que estarían autorizadas si el usuario hubiera seleccionado un nivel diferente de control que el usuario desea dar a la empresa sobre el dispositivo (el acto 606). Por ejemplo, un dispositivo, tal como el dispositivo 102, puede tener permitido instalar algunas aplicaciones, pero no otras aplicaciones basándose en el ajuste de usuario y el nivel de control que el usuario desea permitir que tenga la empresa sobre el dispositivo 102. En algunas realizaciones, se puede poner en práctica el procedimiento 600, en el que el dispositivo está configurado en general para usarse en un entorno de mercado cerrado que solo permite que las aplicaciones generalmente disponibles del mercado cerrado se instalen en el dispositivo, pero el dispositivo está autorizado a instalar aplicaciones fuera de un conjunto de aplicaciones generalmente disponibles en el mercado cerrado y en el que el conjunto de aplicaciones están disponibles solo a usuarios de la empresa particular.

Además, los procedimientos pueden ser puestos en práctica por un sistema informático que incluye uno o más procesadores y medios legibles por ordenador tales como memoria informática. En particular, la memoria informática puede almacenar instrucciones ejecutables por ordenador que, cuando son ejecutadas por uno o más procesadores, dan lugar a que se realicen diversas funciones, tales como los actos enumerados en las realizaciones.

Algunas realizaciones de la presente invención pueden comprender o utilizar un ordenador de fin especial o de fin general que incluye hardware informático, tal como se analiza con mayor detalle en lo sucesivo. Las realizaciones dentro del ámbito de la presente invención también incluyen medios físicos y otros legibles por ordenador para llevar a cabo o almacenar instrucciones ejecutables por ordenador y/o estructuras de datos. Tales medios legibles por ordenador pueden ser cualquier medio disponible que pueda accederse por un sistema informático de fin general o de fin especial. Medios legibles por ordenador que almacenan instrucciones ejecutables por ordenador son medios de almacenamiento físico. Medios legibles por ordenador que llevan instrucciones ejecutables por ordenador son medios de transmisión. Por lo tanto, a modo de ejemplo, y no como limitación, las realizaciones de la invención pueden comprender al menos dos clases diferentes de manera distinta de medios legibles por ordenador: medios de almacenamiento legibles por ordenador físicos y medios legibles por ordenador de transmisión.

Medios de almacenamiento legible por ordenador físicos incluyen RAM, ROM, EEPROM, CDROM u otro almacenamiento de disco óptico (tales como CD, DVD, etc.), almacenamiento de disco magnético u otros dispositivos de almacenamiento magnético, o cualquier otro medio que puede usarse para almacenar medios de código de programa deseado en forma de instrucciones ejecutables por ordenador o estructuras de datos y que puede accederse por un ordenador de fin general o de fin especial.

Una “red” se define como uno o más enlaces de datos que posibilitan el transporte de datos electrónicos entre sistemas informáticos y/o módulos y/u otros dispositivos electrónicos. Cuando se transfiere o proporciona información a través de una red u otra conexión de comunicaciones (ya sea de cableado permanente, inalámbrica, o una combinación de cableado permanente o inalámbrica) a un sistema informático, el sistema informático visualiza de manera apropiada la conexión como un medio de transmisión. Medio de transmisión puede incluir una red y/o enlaces de datos que pueden usarse para llevar medios de código de programa deseados en forma de instrucciones ejecutables por ordenador o estructuras de datos y que puede accederse por un ordenador de fin general o de fin especial. Se incluyen también combinaciones de lo anterior dentro del ámbito de los medios legibles por ordenador.

Además, tras alcanzar diversos componentes de sistema informático, los medios de código de programa en forma de instrucciones ejecutables por ordenador o estructuras de datos pueden transferirse automáticamente desde los medios legibles por ordenador de transmisión a los medios de almacenamiento legibles por ordenador físicos (o viceversa). Por ejemplo, las instrucciones ejecutables por ordenador o estructuras de datos recibidas a través de una red o enlace de datos pueden almacenarse en memoria intermedia en RAM en un módulo de interfaz de red (por ejemplo, un “NIC”), y a continuación transferirse eventualmente a la RAM de sistema informático y/o a medios de almacenamiento físicos legibles por ordenador menos volátiles en un sistema informático. Por lo tanto, los medios de almacenamiento físicos legibles por ordenador pueden incluirse en componentes de sistema informático que también (o incluso principalmente) utilizan medios de transmisión.

Instrucciones ejecutables por ordenador comprenden, por ejemplo, instrucciones y datos que provocan que un

ordenador de fin general, un ordenador de fin especial o un dispositivo de procesamiento de fin especial realice una cierta función o grupo de funciones. Las instrucciones ejecutables por ordenador pueden ser, por ejemplo, códigos binarios, instrucciones de formato intermedio tales como lenguaje ensamblador, o incluso código fuente. Aunque se ha descrito la materia objeto en lenguaje específico a características estructurales y/o actos metodológicos, se ha de entender que la materia objeto definida en las reivindicaciones adjuntas no está necesariamente limitada a las características o actos anteriormente descritos. En su lugar, las características y actos descritos se desvelan como formas de ejemplo de implementación de las reivindicaciones.

Los expertos en la materia apreciarán que la invención puede ponerse en práctica en entornos informáticos de red con muchos tipos de configuraciones de sistema informático, incluyendo, ordenadores personales, ordenadores de sobremesa, ordenadores portátiles, procesadores de mensajes, dispositivos portátiles, sistemas multiprocesador, electrónica de consumo basada en microprocesador o programable, PC de red, miniordenadores, ordenadores centrales, teléfonos móviles, PDA, buscapersonas, encaminadores, conmutadores y similares. La invención puede ponerse en práctica también en entornos de sistema distribuidos donde los sistemas informáticos locales y remotos, que están enlazados (ya sea por enlaces de datos de cableado permanente, enlaces de datos inalámbricos, o por una combinación de enlaces de datos de cableado permanente e inalámbricos) a través de una red, ambos realizan tareas. En un entorno de sistema distribuido, los módulos de programa pueden localizarse tanto en dispositivos de almacenamiento de memoria locales como remotos.

Alternativa o adicionalmente, lo descrito funcionalmente en el presente documento puede ser realizado, al menos en parte, por uno o más componentes lógicos de hardware. Por ejemplo, y sin limitación, tipos ilustrativos de componentes lógicos de hardware que se pueden usar incluyen Disposiciones de puertas programables in situ (FPGA), Circuitos Integrados para Programas específicos (ASIC), Productos Convencionales para Programas específicos (ASSP), sistemas de tipo Sistema sobre chip (SOC), Dispositivos Lógicos Programables Complejos (CPLD), etc.

La presente invención se puede materializar en otras formas específicas sin apartarse de sus características. Las realizaciones descritas han de considerarse en todos los aspectos solo como ilustrativas y no restrictivas. El ámbito de la invención se indica, por lo tanto, por las reivindicaciones adjuntas en lugar de por la descripción anterior. Todos los cambios que entren dentro del significado y el rango de equivalencia de las reivindicaciones se han de considerar englobados dentro de su ámbito.

REIVINDICACIONES

1. Un procedimiento de instalación de aplicaciones y de establecimiento de la configuración en un dispositivo, comprendiendo el procedimiento:

recibir (602) una entrada de usuario, indicando la entrada de usuario un nivel de control que un usuario desea dar a una empresa sobre un dispositivo, en el que la entrada de usuario comprende que un usuario seleccione una pluralidad de artículos de entre una lista predeterminada que el usuario desea dejar que la empresa controle o restrinja en el dispositivo;
determinar (604), basándose en el nivel de control indicado por la entrada de usuario, un conjunto de aplicaciones que se permite instalar en el dispositivo, en el que el conjunto de aplicaciones que se permite instalar en el dispositivo está limitado por el nivel de control indicado por el usuario; y
autorizar (606) la instalación del conjunto de aplicaciones en el dispositivo al tiempo que se restringe la instalación de otras aplicaciones que estarían autorizadas si el usuario hubiera seleccionado un nivel diferente de control que el usuario desea dar a la empresa sobre el dispositivo.

2. El procedimiento de la reivindicación 1, en el que la entrada de usuario comprende que un usuario indique que la empresa puede imponer una o más restricciones en el dispositivo.

3. El procedimiento de la reivindicación 2, en el que la una o más restricciones incluyen una o más de requerir una contraseña, requerir que determinadas aplicaciones se instalen en el dispositivo, limitar el acceso del dispositivo a determinadas redes, requerir que se active un cifrado en el dispositivo, requerir que haya instalado un antivirus, requerir que el antivirus esté actualizado, requerir que el dispositivo satisfaga una versión de SO mínima, requerir que una contraseña en el dispositivo tenga un determinado nivel de complejidad, requerir que una contraseña en el dispositivo tenga unos determinados requisitos de historial, requerir que el hardware del dispositivo esté configurado de una determinada forma, requerir que una cámara en el dispositivo esté deshabilitada o requerir que el Bluetooth en el dispositivo esté deshabilitado.

4. El procedimiento de la reivindicación 1, en el que la entrada de usuario comprende que un usuario indique que la empresa puede controlar el acceso a datos en el dispositivo.

5. El procedimiento de la reivindicación 4, en el que la entrada de usuario indica que la empresa puede realizar uno o más de bloquear el dispositivo, borrar todos los datos de usuario en el dispositivo, restablecer el dispositivo a los ajustes de fábrica, borrar todos los datos de empresa en el dispositivo, o borrar datos asociados con determinadas aplicaciones en el dispositivo.

6. El procedimiento de la reivindicación 1, en el que el dispositivo está configurado en general para ser usado en un entorno de mercado cerrado que solo permite que se instalen en el dispositivo las aplicaciones generalmente disponibles del mercado cerrado, pero el dispositivo está autorizado a instalar aplicaciones fuera de un conjunto de aplicaciones generalmente disponibles en el mercado cerrado y en el que el conjunto de aplicaciones están disponibles solo a usuarios de la empresa particular.

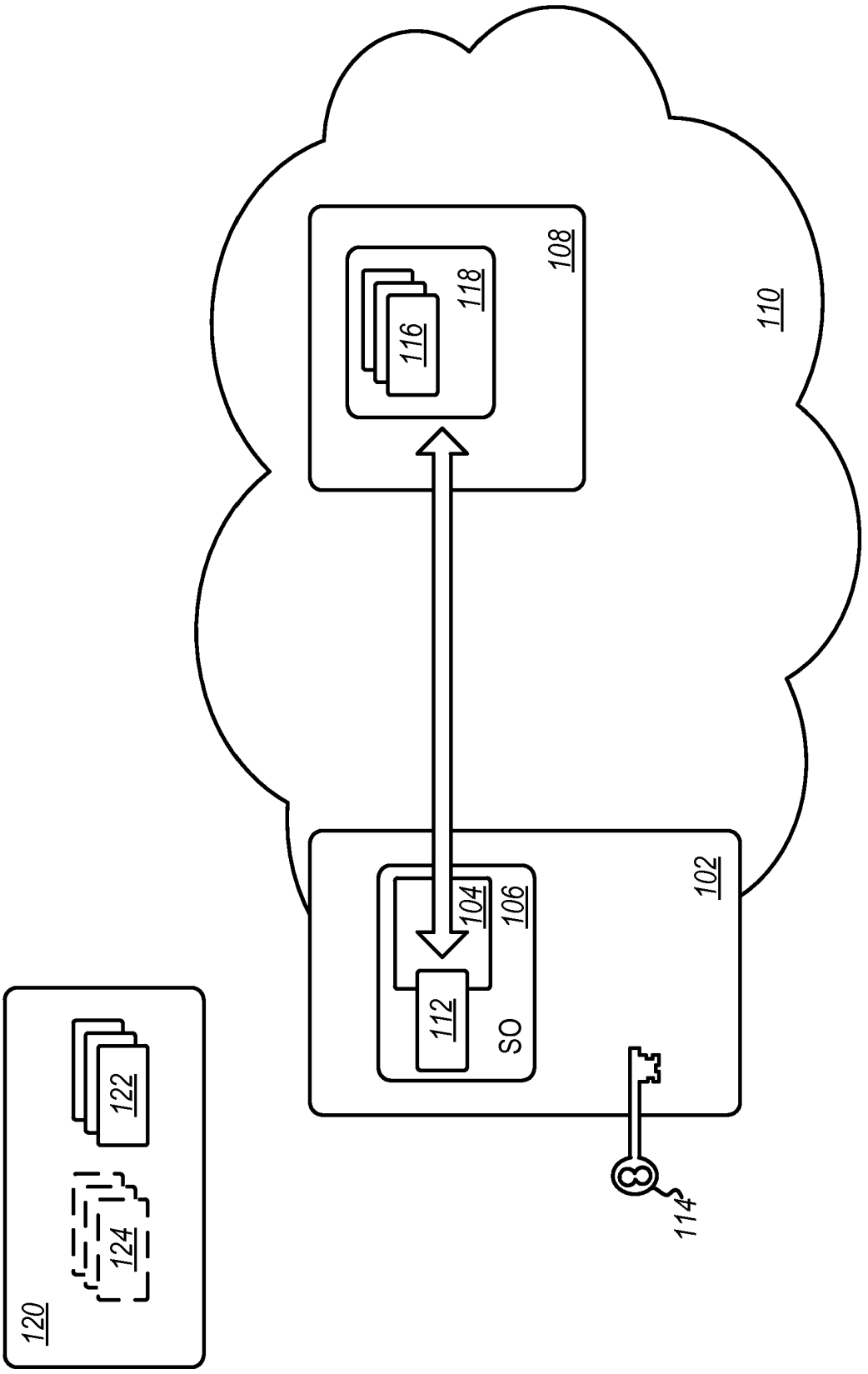

FIG. 1

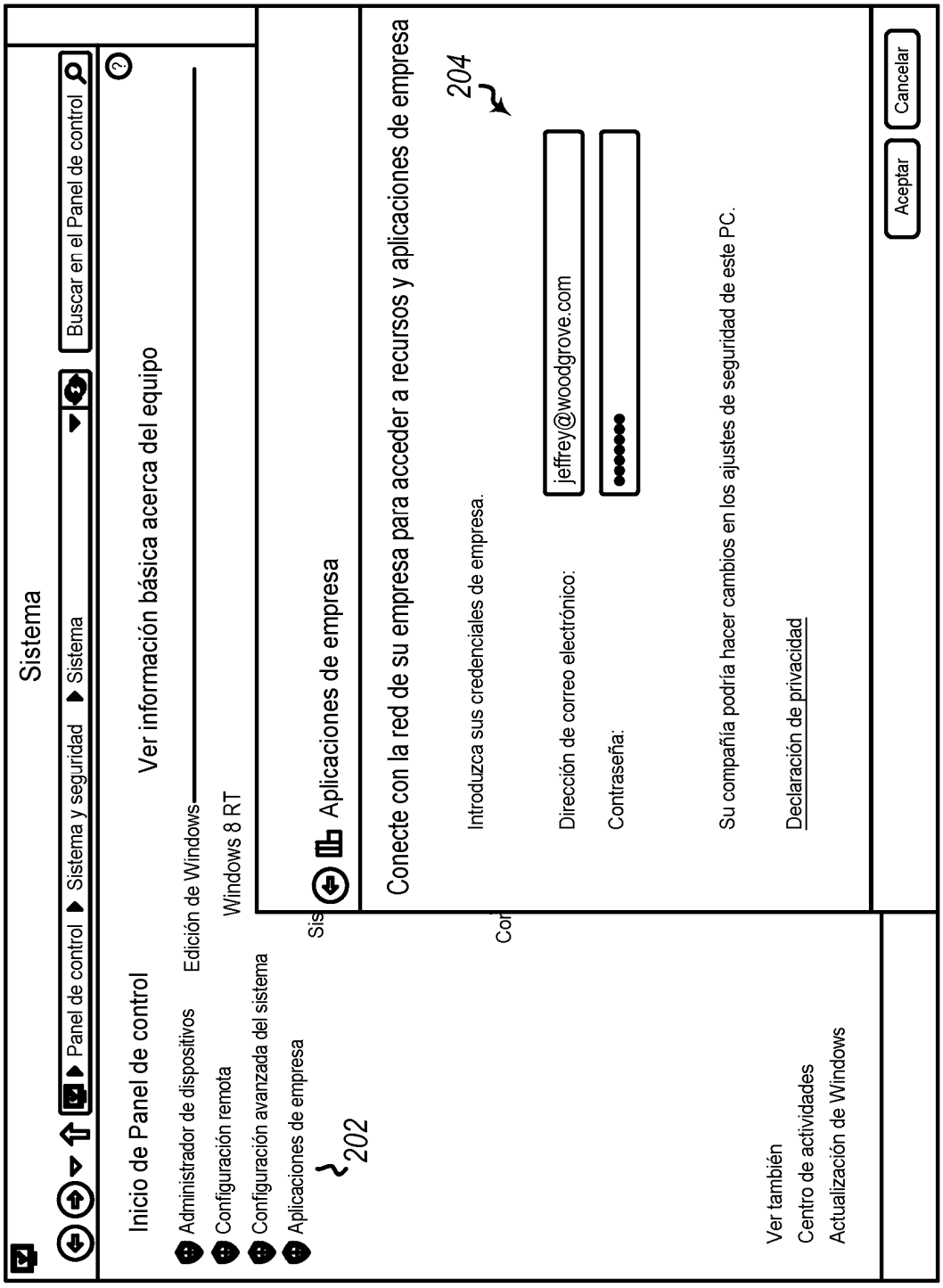
Sistema
Panel de control ▸ Sistema y seguridad ▸ Sistema
Buscar en el Panel de control
Inicio de Panel de control
Administrador de dispositivos
Configuración remota
Configuración avanzada del sistema
Aplicaciones de empresa
202
Ver información básica acerca del equipo
Edición de Windows
Windows 8 RT
Aplicaciones de empresa
Conecte con la red de su empresa para acceder a recursos y aplicaciones de empresa
204
Introduzca sus credenciales de empresa.
Dirección de correo electrónico:
jeffrey@woodgrove.com
Contraseña:
Su compañía podría hacer cambios en los ajustes de seguridad de este PC.
Declaración de privacidad
Aceptar
Cancelar
Ver también
Centro de actividades
Actualización de Windows
200

FIG. 2

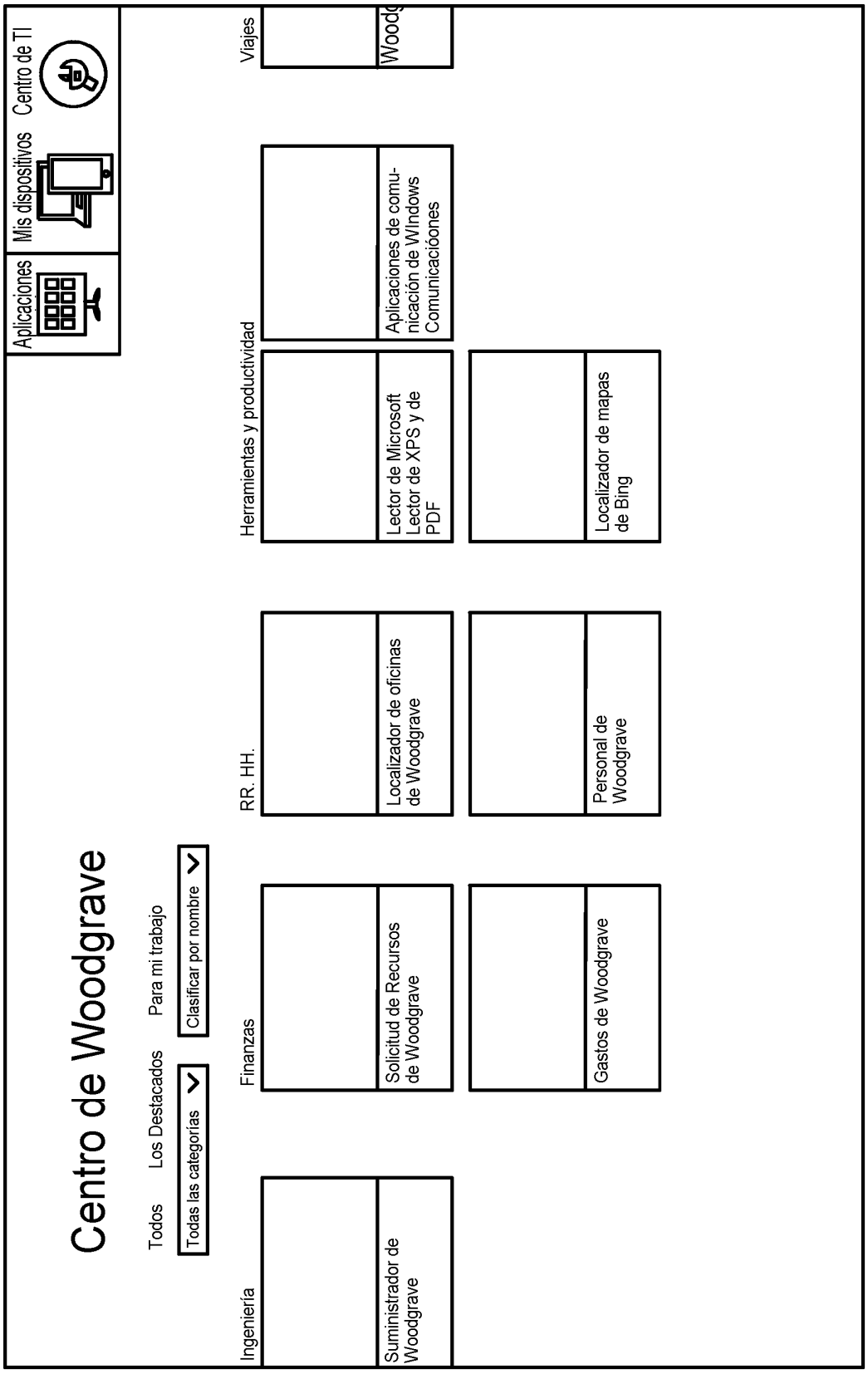
Aplicaciones
Mis dispositivos
Centro de TI
Centro de Woodgrave
Todos
Los Destacados
Para mi trabajo
Todas las categorías
Clasificar por nombre
Ingeniería
Finanzas
RR. HH.
Herramientas y productividad
Viajes
Suministrador de Woodgrave
Solicitud de Recursos de Woodgrave
Localizador de oficinas de Woodgrave
Lector de Microsoft Lector de XPS y de PDF
Aplicaciones de comunicación de Windows Comunicaciones
Gastos de Woodgrave
Personal de Woodgrave
Localizador de mapas de Bing

FIG. 3

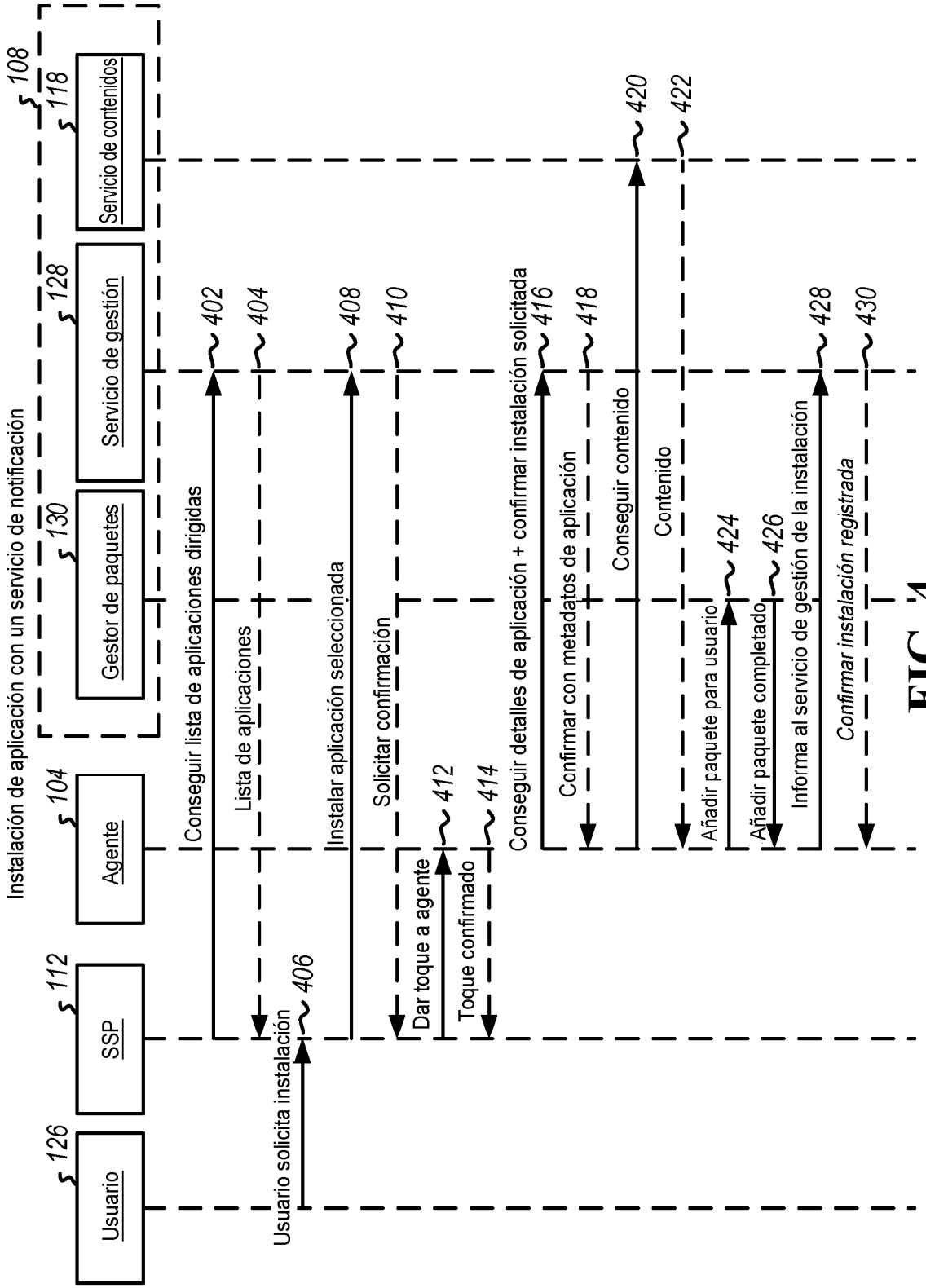
Instalación de aplicación con un servicio de notificación
108
Usuario
126
SSP
112
Agente
104
Gestor de paquetes
130
Servicio de gestión
128
Servicio de contenidos
118
Usuario solicita instalación
406
Conseguir lista de aplicaciones dirigidas
402
Lista de aplicaciones
404
Instalar aplicación seleccionada
408
Solicitar confirmación
410
Dar toque a agente
412
Toque confirmado
414
Conseguir detalles de aplicación + confirmar instalación solicitada
416
Confirmar con metadatos de aplicación
418
Conseguir contenido
420
Contenido
422
Añadir paquete para usuario
424
Añadir paquete completado
426
Informa al servicio de gestión de la instalación
428
Confirmar instalación registrada
430

FIG. 4

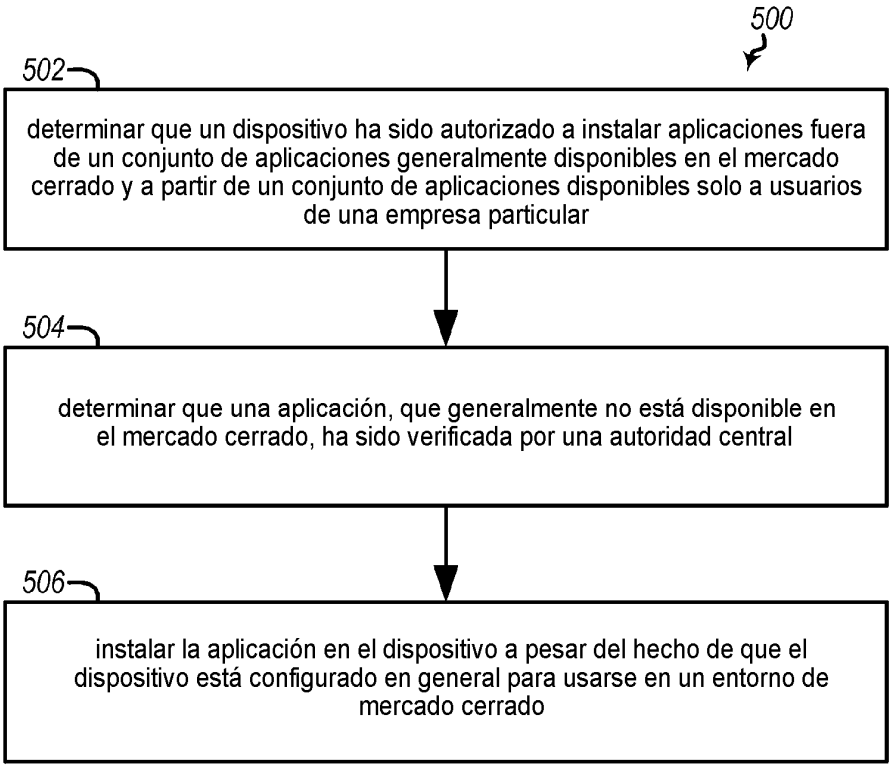
500
502
determinar que un dispositivo ha sido autorizado a instalar aplicaciones fuera de un conjunto de aplicaciones generalmente disponibles en el mercado cerrado y a partir de un conjunto de aplicaciones disponibles solo a usuarios de una empresa particular
504
determinar que una aplicación, que generalmente no está disponible en el mercado cerrado, ha sido verificada por una autoridad central
506
instalar la aplicación en el dispositivo a pesar del hecho de que el dispositivo está configurado en general para usarse en un entorno de mercado cerrado

FIG. 5

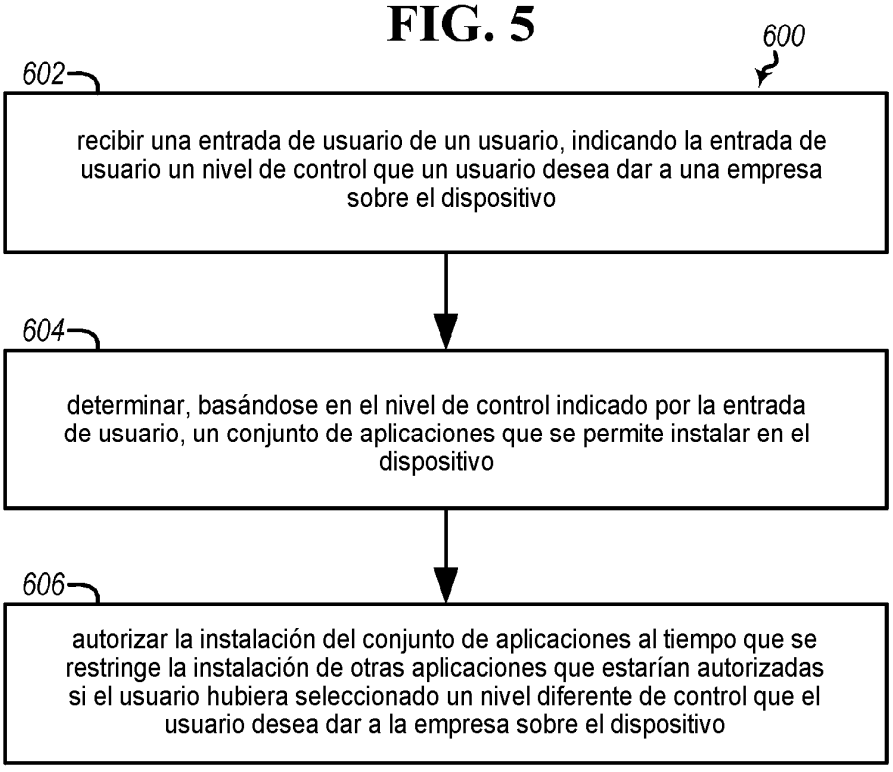
600
602
recibir una entrada de usuario de un usuario, indicando la entrada de usuario un nivel de control que un usuario desea dar a una empresa sobre el dispositivo
604
determinar, basándose en el nivel de control indicado por la entrada de usuario, un conjunto de aplicaciones que se permite instalar en el dispositivo
606
autorizar la instalación del conjunto de aplicaciones al tiempo que se restringe la instalación de otras aplicaciones que estarían autorizadas si el usuario hubiera seleccionado un nivel diferente de control que el usuario desea dar a la empresa sobre el dispositivo

FIG. 6