

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 982 293**

51 Int. Cl.:

H04W 4/30 (2008.01)

H04W 4/021 (2008.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **01.11.2018** **PCT/GB2018/053167**

87 Fecha y número de publicación internacional: **09.05.2019** **WO19086880**

96 Fecha de presentación y número de la solicitud europea: **01.11.2018** **E 18800744 (7)**

97 Fecha y número de publicación de la concesión europea: **29.05.2024** **EP 3777257**

54 Título: **Funcionalidad de bloqueo en un dispositivo inteligente**

30 Prioridad:

03.11.2017 US 201715802583

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

15.10.2024

73 Titular/es:

BLACKOUT TECHNOLOGIES GROUP LTD
(100.0%)
Craven House, 16 Northumberland Avenue
London WC2N 5AP, GB

72 Inventor/es:

WATSON, CHARLES;
HADLEY, MARK y
ASTLE, MICHAEL DAVID

74 Agente/Representante:

ISERN JARA, Jorge

ES 2 982 293 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Funcionalidad de bloqueo en un dispositivo inteligente

- 5 La presente divulgación se refiere a un procedimiento para bloquear la funcionalidad en un dispositivo inteligente. En particular, la divulgación se refiere a un procedimiento para bloquear aplicaciones y/o funciones tal como una cámara o un navegador de un dispositivo inteligente. La presente divulgación también se refiere a un sistema y sus componentes que realizan el procedimiento.
- 10 Muchas empresas pierden productividad debido a que los empleados utilizan dispositivos electrónicos durante el horario laboral para asuntos personales. Existen muchas técnicas para que las empresas controlen el uso de los ordenadores, por ejemplo, las PC conectadas a la red de la empresa.
- 15 Trae tu propio dispositivo (BYOD) se está convirtiendo en una práctica cada vez más común en las empresas, en las que los empleados utilizan su propio dispositivo inteligente, por ejemplo, un teléfono móvil, para trabajar. Esto puede ahorrar costos a la empresa, ya que no necesita suministrar ni mantener una serie de dispositivos para sus empleados. Sin embargo, existe la posibilidad de que se pierda productividad con los acuerdos BYOD, ya que es más probable que los empleados utilicen su propio dispositivo inteligente para uso personal durante el horario laboral si se les permite ser vistos usando sus propios dispositivos para trabajar. Si el dispositivo del empleado no
- 20 está conectado a la red de la empresa y, por ejemplo, utiliza Internet móvil, entonces es difícil para los empleadores controlar si los empleados están utilizando sus propios dispositivos inteligentes para trabajar o para uso personal durante el horario laboral.
- 25 Además, el uso de BYOD en el lugar de trabajo puede tener graves implicaciones de seguridad. Algunas aplicaciones y funciones son particularmente vulnerables a los ataques cibernéticos y algunas permiten a los usuarios difundir intencionalmente o por error información comercial confidencial.
- 30 El documento 2015/237193 A1 divulga un procedimiento de acuerdo con el preámbulo de la reivindicación 1. El documento US 2017/149795 A1 divulga un dispositivo, sistema y procedimiento para permitir a los padres ver y rastrear las actividades de sus hijos con teléfonos inteligentes, incluido el acceso y la extracción de datos de o sobre aplicaciones de mensajería de texto, aplicaciones de redes sociales, navegadores web y aplicaciones para compartir imágenes.
- 35 El documento US 2016/0034699 a Sasaki divulga un sistema en el que, cuando un usuario intenta abrir una unidad de adquisición de información (por ejemplo, una cámara) en un dispositivo móvil, el dispositivo entra en contacto con un servidor con información sobre la ubicación del dispositivo y el servidor determina, en base a la ubicación, si se debe permitir que las unidades de adquisición de información se abran y envíen esta información al dispositivo. El documento US 2015/0327011 a Fairbanks divulga un sistema y procedimiento para rastrear el tiempo que los empleados utilizan los dispositivos móviles que porta cada empleado.
- 40 De acuerdo con un primer aspecto, la invención proporciona un procedimiento para bloquear una o más aplicación(ones) y/o función(ones) en un dispositivo inteligente, en el que el dispositivo inteligente comprende un receptor GPS y uno o más dispositivos receptores inalámbricos. El procedimiento comprende, en el dispositivo inteligente: detectar, mediante una aplicación de control que se ejecuta en el dispositivo inteligente, el movimiento
- 45 del dispositivo inteligente hacia o desde una región predeterminada en base a los datos recibidos por el receptor GPS y/o uno o más de los dispositivos receptores inalámbricos; y bloquear una o más aplicación(ones) y/o función(ones) en el dispositivo inteligente cuando el dispositivo inteligente está dentro de la región predeterminada. El dispositivo inteligente está configurado para comunicarse con un servidor. El procedimiento se caracteriza por: el dispositivo inteligente envía al servidor un conjunto de parámetros actuales del dispositivo inteligente que se aplican actualmente o son detectados por el dispositivo inteligente; en el que el conjunto de parámetros comprende: algunos o todos los permisos de aplicación actuales para la aplicación de control, el estado actual de activación de uno o más dispositivos receptores inalámbricos del dispositivo inteligente y el estado actual de un conmutador de anulación manual de la aplicación de control en el dispositivo inteligente.
- 50
- 55 Por lo tanto, la invención permite el bloqueo de aplicación(ones) y/o función(ones) cuando el dispositivo inteligente se encuentra en una determinada región, tal como el lugar de trabajo. Esto mejora la seguridad, por ejemplo, evitando que los empleados difundan información confidencial de forma intencionada o errónea, y reduce el tiempo de trabajo perdido debido a que los empleados utilizan aplicaciones y/o funciones de sus teléfonos en el lugar de trabajo.
- 60 Por lo tanto, la invención permite que el bloqueo comience cuando se detecta el movimiento del dispositivo inteligente hacia la región predeterminada y luego las aplicaciones se bloquean mientras el dispositivo inteligente está en la región predeterminada.
- 65 El paso de bloquear puede comprender bloquear una o más aplicación(ones) y/o función(ones)s predeterminadas. Es decir, el bloqueo puede realizarse en forma de una "lista negra" de aplicaciones que no puede usarse cuando el

dispositivo inteligente se encuentra en la región predeterminada.

El paso de bloqueo puede comprender bloquear todas las aplicaciones y/o funciones en el dispositivo inteligente excepto una o más aplicación(ones) y/o función(ones) predeterminadas cuando el dispositivo inteligente está dentro de la región predeterminada. Es decir, el bloqueo puede realizarse en forma de una "lista blanca" de aplicaciones que son las únicas aplicaciones/funciones que se permiten usar cuando el dispositivo inteligente está en la región predeterminada.

Estos conceptos de "lista negra" y "lista blanca" son aplicables a todas las diversas realizaciones y aspectos de la invención descrita en la presente memoria. Por lo tanto, cuando se describe el bloqueo de aplicación(ones) y/o función(ones), esto puede utilizar los conceptos particulares de lista negra o lista blanca como se describió anteriormente.

Los sistemas operativos de los dispositivos inteligentes normalmente permitirán un acceso restringido a los usuarios habituales y un acceso de nivel superior a aquellos con privilegios de administrador o de nivel raíz. El acceso restringido tiene como objetivo en parte evitar que un usuario afecte las funciones necesarias para el funcionamiento estable del dispositivo inteligente. Por ejemplo, a un usuario normal generalmente se le impedirá acceder a las funciones que determinan la asignación de memoria o cómo funciona una pantalla táctil, o cómo el teléfono se registra en una red celular. Estas aplicaciones y funciones a las que no puede acceder un usuario normal (uno sin privilegios de acceso especiales) están fuera del alcance de la presente divulgación. Es decir, las "aplicaciones" y "funciones" a las que se hace referencia en la presente memoria generalmente se refieren a aquellas aplicaciones y funciones que pueden ser bloqueadas por un usuario que no tiene privilegios de administrador o de nivel raíz. En la industria, tales aplicaciones y funciones se denominan comúnmente "administrables" (es decir, "aplicaciones administrables" y "funciones administrables"), en el sentido de que un usuario normal puede administrar esas aplicaciones sin permisos de acceso especiales a través de la configuración del dispositivo o el registro y uso de un sistema MDM.

Como se indicó anteriormente, la invención bloquea aplicación(ones) y/o función(ones) en base a la ubicación del dispositivo inteligente. Preferentemente, sin embargo, la(s) aplicación(ones) y/o función(ones) se bloquean adicionalmente en base a si una hora se encuentra dentro de un período de tiempo predeterminado. Por lo tanto, el procedimiento puede comprender además determinar una hora actual, en donde una o más aplicación(ones) y/o función(ones) se bloquean tanto cuando el dispositivo inteligente está dentro de la región predeterminada como cuando la hora actual está dentro de un período de tiempo predeterminado. Por lo tanto, el procedimiento puede comprender determinar si una hora actual está dentro del período de tiempo predeterminado. En una realización preferente, un servidor con el que el dispositivo inteligente puede comunicarse determina si una hora actual está dentro del período de tiempo predeterminado en base a la hora de un reloj del servidor.

El dispositivo inteligente y un servidor con el que el dispositivo inteligente puede comunicarse pueden comprender cada uno un reloj. En el caso de una lista negra como se describió anteriormente, una o más aplicación(ones) y/o función(ones) predeterminadas pueden bloquearse cuando el dispositivo inteligente se encuentra dentro de la región predeterminada y cuando transcurre un tiempo determinado por uno o ambos de los relojes que está dentro de un período de tiempo predeterminado. O, en el caso de una lista blanca como se describió anteriormente, todas las aplicaciones y/o funciones del dispositivo inteligente, excepto una o más aplicación(ones) y/o función(ones) predeterminadas, pueden bloquearse cuando ambos dispositivos inteligentes están dentro la región predeterminada y cuando una hora determinada a partir de uno o ambos relojes está dentro de un período de tiempo predeterminado.

Si el servidor comprende un reloj, el procedimiento puede comprender además que el servidor determine la hora actual a partir del reloj y envíe la hora actual a la aplicación de control del dispositivo inteligente.

Por tanto, de acuerdo con un aspecto adicional, la invención proporciona un procedimiento para bloquear aplicaciones y/o funciones en un dispositivo inteligente que está configurado para comunicarse con un servidor, en el que el dispositivo inteligente comprende un receptor GPS y uno o más dispositivos receptores inalámbricos; el procedimiento que comprende: determinar una hora actual; detectar, mediante una aplicación de control que se ejecuta en el dispositivo inteligente, el movimiento del dispositivo inteligente hacia o desde una región predeterminada; y bloquear una o más aplicación(ones) y/o función(ones) en el dispositivo inteligente cuando el dispositivo inteligente está dentro de la región predeterminada.

En el caso de bloquear una o más aplicación(ones) y/o función(ones) predeterminadas, la invención prevé el bloqueo de solo una aplicación y/o función predeterminada. Sin embargo, la invención normalmente puede incluir el bloqueo de más de una aplicación y/o función predeterminada. Además, en el caso de bloquear todas las aplicaciones y/o funciones excepto una o más aplicación(ones) y/o función(ones) predeterminadas, la invención prevé la excepción del bloqueo de solo una aplicación y/o función predeterminada. Sin embargo, la invención normalmente puede incluir la excepción del bloqueo de más de una aplicación y/o función predeterminada. Por lo tanto, en la presente memoria a menudo se hace referencia a múltiples aplicaciones y/o funciones. También se hace referencia a un conjunto predeterminado de aplicaciones y/o funciones.

Al bloquear aplicaciones y/o funciones en base tanto a la ubicación espacial como al tiempo, el bloqueo de aplicaciones/funciones se puede controlar más estrictamente. Por ejemplo, el dispositivo inteligente puede ser el dispositivo inteligente de un empleado. Un empleador puede desear que se bloqueen aplicaciones y/o funciones mientras el empleado está en el trabajo. Al definir una región predeterminada en relación con el lugar de trabajo y definir un tiempo predeterminado en relación con las horas de trabajo, el bloqueo de aplicaciones se puede implementar particularmente con precisión. La implementación precisa es muy importante ya que los empleadores querrían asegurarse de que las aplicaciones/funciones estén correctamente bloqueadas en el lugar de trabajo para proporcionar las ventajas de estas, pero tanto los empleadores como los empleados no desearían que las aplicaciones/funciones se bloqueen por error cuando el empleado no está en el trabajo.

Preferentemente, el servidor comprende un reloj y el procedimiento comprende además que el servidor determine la hora actual a partir del reloj y envíe la hora actual a la aplicación de control del dispositivo inteligente para evitar que un usuario intente eludir el bloqueo de la aplicación modificando la hora del reloj del dispositivo inteligente.

El uno o más dispositivos receptores inalámbricos puede ser cualquier dispositivo combinado que tenga funcionalidad de receptor. Por ejemplo, los dispositivos receptores inalámbricos pueden comprender además una funcionalidad de transmisión. Los dispositivos receptores inalámbricos pueden ser transceptores.

El uno o más dispositivos receptores inalámbricos pueden incluir un dispositivo receptor Bluetooth y/o un dispositivo receptor Wi-Fi y/o un dispositivo receptor de red celular. De acuerdo con lo anterior, un dispositivo receptor Bluetooth puede ser un transceptor Bluetooth, un dispositivo receptor Wi-Fi puede ser un transceptor Wi-Fi y un dispositivo receptor de red celular puede ser un transceptor de red celular.

Los dispositivos GPS y receptores inalámbricos pueden considerarse como "sensores" que proporcionan datos de ubicación.

El bloqueo de aplicaciones/funciones también puede describirse como filtrado de aplicaciones/funciones. Las aplicaciones/funciones bloqueadas pueden considerarse funcionalidad deshabilitada, mientras que las aplicaciones/funciones desbloqueadas pueden considerarse funcionalidad habilitada.

De acuerdo con la discusión anterior, la(s) aplicación(ones) y/o función(ones) predeterminada(s) que están bloqueadas pueden denominarse lista negra. La lista negra puede incluir, por ejemplo, aplicaciones como Facebook, WhatsApp e Instagram. Otras aplicaciones que pueden bloquearse pueden ser aplicaciones que controlan funciones de nivel inferior del dispositivo inteligente, como el control de la óptica de la cámara y CCD. Una función que puede bloquearse puede incluir una cámara. Otra función que puede bloquearse puede incluir un navegador. Estas funciones pueden bloquearse a nivel del sistema. Las aplicaciones y funciones pueden describirse en conjunto como "funcionalidad" o "funciones" del dispositivo inteligente. En el caso de esta opción, es decir, "bloquear una o más aplicación(ones) y/o función(ones) predeterminada(s) en el dispositivo inteligente cuando el dispositivo inteligente está dentro de la región predeterminada", el procedimiento puede incluir bloquear esa(s) aplicación(ones) y/o función(ones), excepto otra(s) aplicación(ones) y/o función(ones) y, de hecho, excepto todas las demás aplicación(ones) y/o función(ones).

Del mismo modo, una o más aplicación(ones) y/o función(ones) predeterminadas que no están bloqueadas (cuando todas las demás aplicaciones y/o funciones sí lo están) pueden denominarse lista blanca. La lista blanca puede incluir, por ejemplo, un programa de correo electrónico del trabajo.

La(s) aplicación(ones) y/o función(ones) predeterminada(s) pueden seleccionarse por un administrador, por ejemplo un empleador. El administrador puede seleccionar las aplicaciones y/o funciones en el servidor, y luego el servidor puede enviar esta lista predeterminada de aplicaciones y/o funciones al dispositivo inteligente.

Esto permite a los empleadores garantizar que las aplicaciones y/o funciones que no son relevantes para el trabajo del empleado no estén disponibles en el dispositivo de ese empleado cuando el empleado se encuentra dentro de la región predeterminada (por ejemplo, el lugar de trabajo) y durante un período de tiempo predeterminado (por ejemplo, horas de trabajo).

El dispositivo inteligente normalmente puede ser un teléfono inteligente, una tableta o un reloj inteligente. Preferentemente, el dispositivo inteligente tiene un sistema operativo Android o iOS.

Los datos recibidos por el receptor GPS y/o uno o más dispositivos receptores inalámbricos proporcionan una indicación de la ubicación del dispositivo inteligente.

Por tanto, el paso de detectar movimiento dentro o fuera de una región predeterminada en base a los datos recibidos por el receptor GPS y/o uno o más de los dispositivos receptores inalámbricos comprende obtener una indicación de la ubicación del dispositivo inteligente a partir de los datos.

El paso de detectar movimiento dentro o fuera de una región predeterminada puede comprender determinar la

ubicación espacial actual del dispositivo inteligente usando los datos de GPS y/o datos de uno o más de los dispositivos receptores inalámbricos (por ejemplo, Wi-Fi, Bluetooth); y evaluar si esta ubicación cae dentro o fuera de la región predeterminada.

Determinar la ubicación espacial actual y evaluar si se encuentra dentro o fuera de la región predeterminada puede ser parte de una única etapa. Por ejemplo, si un dispositivo Bluetooth recibe datos que indican que se ha detectado una baliza Bluetooth particular, y si la región predeterminada se define como aquella en la que esa baliza Bluetooth particular es detectable, entonces al detectar la baliza Bluetooth se sabe que el dispositivo inteligente está dentro de la región predeterminada.

La región predeterminada puede comprender al menos una de las siguientes áreas: una región espacial 2D definida por un conjunto predeterminado de coordenadas GPS; una región espacial 2D definida por una única coordenada GPS predeterminada y un radio desde esa coordenada GPS; una región en la que el dispositivo receptor inalámbrico detecta un identificador de red predeterminado. El identificador de red predeterminado puede ser un SSID o UUID. En el caso de un UUID, puede ser un UUID de baliza Bluetooth de baja energía (BLE).

Por lo tanto, el paso de detectar movimiento dentro o fuera de la región predeterminada en base a los datos recibidos por el receptor GPS y/o uno o más de los dispositivos receptores inalámbricos puede comprender determinar si una coordenada GPS de la ubicación del dispositivo inteligente está dentro de una región espacial 2D definida por un conjunto predeterminado de coordenadas GPS. Puede comprender determinar si la coordenada GPS de la ubicación del dispositivo inteligente está dentro de una región espacial 2D definida por una única coordenada GPS predeterminada y un radio desde esa coordenada GPS. Puede comprender determinar si el dispositivo receptor inalámbrico del dispositivo inteligente detecta un identificador de red predeterminado, tal como un SSID de Wi-Fi o un UUID de baliza Bluetooth de baja energía. Un experto en la técnica podría implementar fácilmente estas etapas en una aplicación de control.

La región predeterminada puede comprender una superposición de más de una de las áreas antes mencionadas. Por ejemplo, la región predeterminada puede comprender tanto una región espacial 2D definida por un conjunto de coordenadas GPS como una región en la que el dispositivo receptor inalámbrico puede detectar un identificador de red predeterminado (por ejemplo, la red Wi-Fi del lugar de trabajo). Al detectar movimiento dentro o fuera de una región predeterminada que comprende ambas áreas, no importa si, por ejemplo, la recepción GPS es deficiente. Esto se debe a que la aplicación puede detectar movimiento dentro/fuera de la región espacial 2D mediante el identificador de red.

Preferentemente, el procedimiento comprende que el servidor reciba datos del dispositivo que indican que el dispositivo se ha movido a una región predeterminada, y que el servidor determine en base a esta información que una o más aplicación(ones) y/o función(ones) predeterminadas deben bloquearse o que todas las aplicaciones y/o funciones deben bloquearse excepto una o más aplicación(ones) y/o función(ones) predeterminadas, y el servidor envía esta decisión al dispositivo.

Por lo tanto, preferentemente el procedimiento puede comprender además que la aplicación de control envíe datos relacionados con el movimiento del dispositivo inteligente dentro o fuera de la región predeterminada al servidor. El procedimiento puede comprender además que el servidor determine, en base a estos datos, si la(s) aplicación(ones) y/o función(ones) deben bloquearse en el dispositivo inteligente. El procedimiento puede comprender además que el servidor se comunique con el dispositivo inteligente para proporcionar instrucciones para bloquear aplicación(ones) y/o función(ones), en donde el bloqueo se lleva a cabo en respuesta a estas instrucciones.

Esto puede permitir que la lista de aplicación(ones) y/o función(ones) predeterminadas se establezca centralmente en el servidor, por ejemplo, por un administrador. Por lo tanto, si se identifica una nueva aplicación o función que debe bloquearse mientras se encuentra en la región predeterminada, entonces el administrador puede agregar esa aplicación o función en el lado del servidor para que el bloqueo de esta nueva aplicación/función no requiera acción por parte del usuario del dispositivo inteligente. Esto también puede facilitar la tarea de garantizar que varios dispositivos inteligentes (administrados por el mismo servidor) bloqueen las aplicaciones correctas.

Cuando el servidor recibe datos relacionados con el movimiento del dispositivo inteligente fuera de la región predeterminada, el servidor puede determinar si una hora actual está dentro de un período de tiempo predeterminado y además usar esto para determinar si la(s) aplicación(ones) y/o función(ones) deberían bloquearse. Por ejemplo, si el dispositivo inteligente se ha movido a la región predeterminada y la hora actual está dentro del período de tiempo predeterminado, entonces el servidor puede determinar que la(s) aplicación(ones) y/o función(ones) deben bloquearse. Luego, el servidor puede comunicar instrucciones al dispositivo inteligente o a la aplicación de control en el dispositivo inteligente para bloquear aplicación(ones) y/o función(ones).

El período de tiempo predeterminado puede seleccionarse por un administrador, por ejemplo un empleador. El administrador puede establecer el período de tiempo predeterminado en el servidor. El servidor puede enviar esto al dispositivo inteligente.

El procedimiento puede comprender además los pasos de:

- a. el servidor determina si los parámetros actuales del dispositivo inteligente se ajustan a un conjunto predeterminado de parámetros; y
- b. cuando los parámetros actuales del dispositivo inteligente no se ajustan al conjunto predeterminado de parámetros, enviar una notificación al dispositivo inteligente para indicarle al dispositivo inteligente o a un usuario del dispositivo inteligente que ajuste los parámetros actuales del dispositivo aplicados en el dispositivo.

Esto puede mejorar la funcionalidad de la aplicación de control y garantizar el cumplimiento del usuario con la implementación del procedimiento. Por ejemplo, si el servidor determina que el estado actual de activación de un dispositivo receptor inalámbrico está apagado cuando debería estar encendido, se le indica al dispositivo inteligente (o al usuario del dispositivo inteligente) que lo encienda. Esto evitaría, por ejemplo, que un usuario intente eludir el bloqueo de aplicaciones en su dispositivo desactivando Bluetooth.

El procedimiento puede comprender el paso de que el servidor envíe notificaciones al dispositivo inteligente para configurar o actualizar la región predeterminada.

Esto permite a un administrador establecer o modificar la región predeterminada en un único punto, el servidor, y luego el servidor actualiza las regiones predeterminadas correspondientes para cada dispositivo (por ejemplo, el dispositivo de cada empleado) que está configurado para realizar el procedimiento.

Cuando se determina que los permisos actuales de la aplicación de control no se ajustan a los permisos de la aplicación de control del conjunto predeterminado de parámetros, el procedimiento puede comprender el paso de que el servidor envíe una notificación al dispositivo inteligente para iniciar la comunicación con el servidor.

Cuando se determina que el estado de activación del receptor GPS y el o cada dispositivo receptor inalámbrico no se ajusta a un estado de activación deseado, el procedimiento puede comprender el paso de que el servidor envíe una notificación al dispositivo inteligente para notificar a un usuario que cambie el estado de activación de cada uno de los receptores GPS y de cada dispositivo receptor inalámbrico que se determina que no se ajusta a un estado de activación deseado.

El procedimiento puede comprender además que el dispositivo inteligente envíe al servidor uno o más de: identificadores de red para cualquier red inalámbrica que detecte el dispositivo inteligente, balizas visibles y coordenadas GPS actuales del dispositivo inteligente.

El dispositivo inteligente puede estar asociado con un primer usuario, y el servidor puede mantener un registro de los permisos actuales de la aplicación de control para la aplicación de control en el dispositivo inteligente; y cuando se determina que los permisos de la aplicación de control no se ajustan a los permisos de la aplicación de control del conjunto predeterminado de parámetros más de un número predeterminado de veces, el servidor envía una alerta a un segundo usuario que identifica al primer usuario.

Esto permite auditar el cumplimiento de un empleado con el funcionamiento de la aplicación de control. Si un empleado determinado no ha otorgado (repetidamente) los permisos correctos a la aplicación de control, el servidor puede alertar a un administrador (es decir, a un segundo usuario).

El dispositivo inteligente puede estar asociado con un primer usuario, y el servidor puede mantener un registro de la frecuencia con la que el dispositivo inteligente se comunica con el servidor; y cuando la frecuencia cae por debajo de una frecuencia predeterminada, el servidor envía una alerta a un segundo usuario que identifica al primer usuario.

El dispositivo inteligente puede estar asociado con un primer usuario y el servidor puede mantener un registro de la última vez que el dispositivo inteligente se comunicó con el servidor. Cuando la duración desde la última vez que el dispositivo inteligente se comunicó con el servidor excede una duración predeterminada, el servidor puede enviar una alerta a un segundo usuario que identifique al primer usuario.

Esto permite otra forma de auditar el cumplimiento de los empleados con el funcionamiento de la aplicación de control, en la que se puede alertar a un administrador sobre el hecho de que el dispositivo de un empleado no se ha registrado recientemente con el servidor.

El procedimiento puede comprender además desbloquear aplicaciones bloqueadas cuando la aplicación de control detecta el movimiento del dispositivo inteligente fuera de la región predeterminada. El desbloqueo puede basarse además en si la hora actual está fuera del período de tiempo predeterminado. En otras palabras, el procedimiento puede comprender determinar cuándo una ubicación del dispositivo inteligente sale de la región predeterminada y cuándo el tiempo cae fuera del período de tiempo predeterminado, y cuando se satisfacen ambas condiciones, el procedimiento comprende desbloquear (por ejemplo, habilitar) una o más aplicación(ones) y/o función(ones) que han sido bloqueadas en el dispositivo inteligente.

La aplicación de control lleva a cabo el paso de detectar el movimiento del dispositivo inteligente fuera de una región predeterminada. El dispositivo inteligente puede enviar datos relacionados con el movimiento del dispositivo inteligente fuera de la región predeterminada al servidor. El servidor puede determinar, en base a estos datos, si la(s) aplicación(ones) y/o función(ones) actualmente bloqueadas en el dispositivo inteligente deben desbloquearse. Generalmente, si el dispositivo inteligente se ha movido fuera de la región predeterminada, entonces el servidor determinará que la(s) aplicación(ones) y/o función(ones) actualmente bloqueadas deben desbloquearse. Luego, el servidor se comunicará con el dispositivo inteligente o la aplicación de control en el dispositivo inteligente para proporcionar instrucciones para desbloquear aplicación(ones) y/o función(ones) bloqueadas en particular, o incluso todas la(s) aplicación(ones) y/o función(ones) bloqueadas, en el que el desbloqueo se realiza en respuesta a estas instrucciones.

Cuando el servidor recibe datos relacionados con el movimiento del dispositivo inteligente fuera de la región predeterminada, el servidor puede determinar si una hora actual está dentro de un período de tiempo predeterminado y además usar esto para determinar si la(s) aplicación(ones) y/o función(ones) actualmente bloqueadas deben desbloquearse. Por ejemplo, si el dispositivo inteligente se ha movido fuera de la región predeterminada y la hora actual está fuera del período de tiempo predeterminado, entonces el servidor puede determinar que la(s) aplicación(ones) y/o función(ones) actualmente bloqueadas deben desbloquearse. Luego, el servidor puede indicarle al dispositivo inteligente o a la aplicación de control en el dispositivo inteligente que desbloquee ciertas aplicación(ones)/función(ones) bloqueadas o todas las aplicación(ones)/función(ones) bloqueadas.

En cuanto al bloqueo de aplicaciones en el dispositivo inteligente, éste podrá realizarse mediante la aplicación de control. Sin embargo, el experto apreciará fácilmente que la implementación particular puede depender del sistema operativo del dispositivo inteligente. Por ejemplo, la funcionalidad de bloqueo normalmente deberá implementarse de manera diferente para un sistema operativo Android que para un iOS. Más adelante se describen ejemplos particulares para Android y iOS en relación con las Figuras.

En un aspecto adicional, la invención proporciona un dispositivo inteligente de acuerdo con la reivindicación 11. En un aspecto adicional, se proporciona un sistema que comprende el dispositivo inteligente y un servidor de acuerdo con la reivindicación 12.

En el sistema, el servidor y/o el dispositivo inteligente comprenden preferentemente un reloj. El dispositivo inteligente se puede configurar para bloquear una o más aplicación(ones) y/o función(ones) en el dispositivo inteligente, adicionalmente, en base a si la hora actual del reloj se encuentra dentro de un período de tiempo predeterminado.

Preferentemente, el servidor puede configurarse y reconfigurarse para definir la región predeterminada y/o el período de tiempo predeterminado, y/o la(s) aplicación(ones)/función(ones) predeterminada(s). Preferentemente, el servidor puede configurarse para comunicarse con el dispositivo inteligente para establecer la región predeterminada, el período de tiempo predeterminado y/o una o más aplicación(ones)/función(ones).

El servidor puede contener instrucciones editables ejecutables por ordenador para definir la región predeterminada y/o el período de tiempo predeterminado y/o una o más aplicación(ones)/función(ones); y el servidor puede contener instrucciones editables ejecutables por ordenador para comunicarse con el dispositivo inteligente para establecer la región predeterminada y/o el período de tiempo predeterminado y/o una o más aplicación(ones)/función(ones).

Este procedimiento y sistema de la invención pueden aumentar la productividad de un usuario del dispositivo inteligente al bloquear aplicaciones y/o funciones que distraen (por ejemplo, aplicaciones de noticias, aplicaciones de redes sociales, aplicaciones de citas, aplicaciones de juegos, funcionalidad de cámara) mientras el usuario está en una área predeterminada durante un tiempo predeterminado (por ejemplo, en el trabajo, durante las horas de trabajo). La seguridad de la información también aumenta. Ventajosamente, el bloqueo es "inteligente" porque la funcionalidad regresa cuando el usuario está fuera del área predeterminada (por ejemplo, cuando viaja al trabajo o sale a almorzar) y está en su tiempo personal.

Por ejemplo, un empleador puede instituir una política BYOD condicionada a que dichos dispositivos tengan instalada la aplicación de control. Luego, el empleador puede configurar el servidor para identificar el área predeterminada (por ejemplo, el lugar de trabajo) y el período de tiempo predeterminado (por ejemplo, horas de trabajo), y puede establecer qué aplicaciones y/o funciones están permitidas/bloqueadas en el dispositivo del usuario.

Una pluralidad de dispositivos inteligentes diferentes (por ejemplo, pertenecientes a diferentes empleados de la misma empresa) pueden conectarse al mismo servidor (por ejemplo, gestionarse o configurarse por esa empresa). Esto permite a la empresa establecer y actualizar una política común que se aplica a todos los dispositivos inteligentes que utilizan los empleados como parte del esquema BYOD.

En el sistema, el o cada dispositivo receptor inalámbrico puede ser uno de un dispositivo receptor Bluetooth (por ejemplo, un transceptor Bluetooth), un dispositivo receptor Wi-Fi (por ejemplo, un transceptor Wi-Fi) y un dispositivo

receptor de red celular (por ejemplo, un transceptor de red celular). Esto permite establecer la región predeterminada de diversas maneras. Cuando el dispositivo receptor inalámbrico es un dispositivo receptor Bluetooth, la región predeterminada puede definirse mediante una baliza Bluetooth. Cuando el dispositivo receptor inalámbrico es un dispositivo receptor Wi-Fi, la región predeterminada puede definirse como la región en la que el dispositivo inteligente detecta una red Wi-Fi específica.

En términos del receptor GPS, la región predeterminada puede definirse mediante coordenadas GPS.

La mayoría de los dispositivos inteligentes modernos tendrán los tres tipos de dispositivos receptores (GPS, Wi-Fi y Bluetooth), lo que permite definir la región predeterminada de múltiples maneras, lo que aumenta la flexibilidad del sistema.

Además de las ventajas descritas anteriormente en relación con la seguridad de la información y el aumento de la productividad, una ventaja técnica particular de los procedimientos y sistemas de la presente invención puede ser que el dispositivo inteligente puede funcionar más rápido y/o tener una mayor duración de la batería.

El servidor puede contener instrucciones editables ejecutables por ordenador para definir la región predeterminada. El servidor puede contener instrucciones editables ejecutadas por ordenador para comunicarse con el dispositivo inteligente para establecer la región predeterminada.

El servidor y/o el dispositivo inteligente pueden comprender un reloj, y en donde las instrucciones ejecutables por ordenador del dispositivo inteligente pueden bloquear una o más aplicación(ones) y/o función(ones) en el dispositivo inteligente, adicionalmente, en base a si una hora actual del reloj está dentro de un período de tiempo predeterminado.

El o cada dispositivo receptor inalámbrico puede ser uno de entre un dispositivo receptor Bluetooth, un dispositivo receptor Wi-Fi y un dispositivo receptor de red celular.

El servidor puede contener instrucciones ejecutables por ordenador que hacen que el servidor se comunice con el dispositivo inteligente para establecer la región predeterminada y/o el período de tiempo predeterminado.

La ubicación predeterminada podrá determinarse parcialmente en términos negativos. Es decir, es posible especificar una región donde se desbloquean las aplicaciones que esté dentro de una región donde se bloquean las aplicaciones. Por ejemplo, una empresa podría designar una cafetería o sala de descanso como un lugar donde los empleados tengan uso ilimitado de sus dispositivos inteligentes. Para hacer esto, se puede determinar una primera región (por ejemplo, usando una latitud/longitud GPS y un radio); y se puede definir una segunda región dentro de la primera región, usando opcionalmente una baliza (por ejemplo, una baliza Bluetooth de baja energía), en donde la región predeterminada se define restando la segunda región de la primera región.

Cuando el dispositivo inteligente puede detectar la baliza Bluetooth, esto puede hacer que desactive el bloqueo de aplicaciones a pesar de que el dispositivo inteligente se encuentre dentro de la primera región. Cuando el usuario se mueve (dentro de la primera región) fuera del alcance de la baliza Bluetooth, se puede restablecer el bloqueo de la aplicación. Dicho de otra manera, la región predeterminada puede contener uno o más "agujeros" de manera que un usuario que está dentro del límite más externo de la región predeterminada, puede, no obstante, estar fuera de la región predeterminada en virtud de estar ubicado en un agujero dentro de la región predeterminada.

Se pueden usar balizas iBeacon o Eddystone para implementar una baliza Bluetooth de baja energía para definir la primera región o para definir la segunda región (es decir, un agujero en la región predeterminada).

La hora predeterminada podrá establecerse en el servidor durante el horario laboral y en días laborables.

El tiempo predeterminado se puede configurar de manera diferente para el dispositivo inteligente de cada usuario.

De esta forma, no es necesario que todos los usuarios registrados en un mismo servidor compartan los mismos horarios predeterminados. Esta característica permite que la aplicación de control y/o el servidor tengan en cuenta diferentes horarios de trabajo y/o días festivos (vacaciones) de los empleados.

Las aplicaciones de control pueden comunicarse con servicios en línea que proporcionan un sistema de informe de fallos. Esto puede permitir que varias partes (por ejemplo, el usuario, el empleador o el administrador del servidor) identifiquen errores en el sistema general.

Hay varias situaciones en las que la aplicación de control, a través del dispositivo inteligente, puede configurarse para señalar algo al servidor. Estas situaciones incluyen:

conectarse/desconectarse de una red Wi-Fi, entrar o salir de una región predeterminada (por ejemplo, pasar una geocerca), un escaneo periódico en busca de balizas, verificar periódicamente si algún servicio VPN se está ejecutando en el dispositivo inteligente, verificar periódicamente si la aplicación de control tiene los permisos de la

aplicación correctos, verificar los estados de Wi-Fi y Bluetooth del dispositivo inteligente y verificar la ubicación del dispositivo.

5 La aplicación de control puede requerir que transcurra un tiempo determinado (por ejemplo, 30 segundos) antes de determinar que el dispositivo inteligente 40 está dentro de la región predeterminada.

Esto puede garantizar que el dispositivo inteligente 40 esté efectivamente dentro de la región predeterminada y que no se haya cometido ningún error breve al determinar la ubicación del dispositivo inteligente.

10 La aplicación de control puede configurarse para solicitar los permisos de ubicación necesarios desde el dispositivo inteligente para acceder a los servicios de ubicación.

La aplicación de control se puede configurar para verificar, con una frecuencia configurable, si los permisos requeridos y los servicios activos están disponibles.

15 Los servicios de ubicación en dispositivos inteligentes permiten determinar la ubicación del dispositivo inteligente mediante la detección de una o más de: señales de datos celulares (por ejemplo, con qué torres de telefonía celular puede comunicarse el dispositivo inteligente), señales de Wi-Fi, redes GPS y balizas Bluetooth, el acceso a varios servicios de ubicación diferentes puede permitir que la aplicación de control detecte con mayor precisión el movimiento del dispositivo inteligente dentro o fuera de la región predeterminada.

20 Los dispositivos inteligentes pueden estar "supervisados" o "no supervisados". Un dispositivo supervisado permite al supervisor un mayor nivel de acceso al sistema operativo que se le otorga a un usuario (donde el supervisor y el usuario son personas diferentes). Por ejemplo, las organizaciones que poseen una gran cantidad de dispositivos inteligentes que se distribuyen a su personal, a menudo registrarán los dispositivos inteligentes de la organización como "supervisados" para permitir a la empresa un mayor nivel de control sobre el dispositivo inteligente que el empleado. Los dispositivos inteligentes no supervisados son dispositivos inteligentes que no están supervisados. Los dispositivos no supervisados normalmente serán dispositivos inteligentes adquiridos por el empleado para uso personal.

30 El servidor puede tener un mayor nivel de control sobre los dispositivos inteligentes supervisados en comparación con los dispositivos inteligentes no supervisados. Por ejemplo, en un dispositivo supervisado que ejecuta iOS, las aplicaciones individuales pueden estar en la lista blanca o lista negra. En un dispositivo no supervisado, es posible que la inclusión en listas negras o listas blancas solo se base en categorías amplias de aplicaciones, por ejemplo, en base a la clasificación por edades, que se describe a continuación.

35 Un dispositivo inteligente no supervisado que ejecute iOS puede inscribirse en un MDM sin encabezado que permite, por ejemplo, bloquear todas las aplicaciones en el dispositivo inteligente que se hayan descargado de la App Store de Apple, en base a una política de clasificación por edades.

40 Actualmente, la App Store de Apple tiene clasificaciones de edad para aplicaciones de 4+ (es decir, adecuadas para usuarios mayores de cuatro años), 9+, 12+, 17+ y "Sin clasificación". Por lo tanto, la MDM sin encabezado puede, por ejemplo, indicarle al dispositivo inteligente que bloquee todas las aplicaciones con una clasificación de edad superior a 4+.

45 La presente divulgación proporciona ejemplos detallados para implementar el procedimiento y el sistema en dispositivos inteligentes que ejecutan iOS fabricado por Apple Inc. y Android fabricado por Google Inc. La aplicación de control puede funcionar de manera muy similar para diferentes variantes de estos sistemas operativos. iOS tiene varias versiones diferentes. De manera similar, Android tiene una gran cantidad de variantes, en particular, variantes que son modificadas por terceros para utilizar el sistema Android base junto con otras funciones programadas por ese tercero. Por lo tanto, en otro aspecto, la aplicación de control está configurada para ejecutarse en dispositivos inteligentes que ejecutan iOS, Android y cualquier variante de estos.

50 Se apreciará fácilmente que las diversas características opcionales y preferidas de ciertas realizaciones descritas anteriormente pueden usarse por separado o en cualquier combinación, y son aplicables a todos los aspectos de la invención.

55 Ahora se describirán ciertas realizaciones de la presente invención en mayor detalle, solo a modo de ejemplo, con referencia a las figuras adjuntas en las que:

60 La Figura 1 muestra una vista en planta de tres edificios; y
 La Figura 2 muestra una vista en planta de tres edificios con una región circular definida;
 La Figura 3 muestra un diagrama de flujo del proceso seguido por una aplicación de control para determinar si bloquear/permitir aplicaciones y/o funciones;
 65 La Figura 4 muestra un diagrama de secuencia para actualizar la región predeterminada desde un servidor al dispositivo inteligente;

La Figura 5 muestra un diagrama de arquitectura del proceso de bloqueo de aplicaciones y/o funciones en un dispositivo inteligente que ejecuta iOS de Apple;

La Figura 6 muestra un diagrama de arquitectura del proceso de bloqueo de aplicaciones y/o funciones en un dispositivo inteligente que ejecuta el sistema operativo Android;

La Figura 7 muestra una vista esquemática de los enlaces de comunicación entre: un servidor, un dispositivo inteligente que ejecuta iOS, un dispositivo inteligente que ejecuta Android y una interfaz de control (remota) para el servidor;

La Figura 8 muestra un diagrama de flujo para operaciones en segundo plano realizadas por una aplicación de control ilustrativa;

Las Figuras 9A y 9B muestran un diagrama de flujo para el funcionamiento de una aplicación de control ilustrativa que se ejecuta en iOS;

La Figura 10 muestra un diagrama de flujo del bucle de operación principal para el control ilustrativo de la Figura 9;

La Figura 11 muestra un diagrama de flujo para verificar los permisos de ubicación para la aplicación de control ilustrativa de las Figuras 9A/9B; y

Las Figuras 12A y B muestran un diagrama de flujo de la configuración inicial para la aplicación de control ilustrativa de la Figura 9.

La siguiente descripción describe el bloqueo de múltiples aplicaciones y/o funciones. Sin embargo, de la descripción anterior se apreciará que la invención incluye el bloqueo de solo una aplicación y/o función. La siguiente descripción se refiere simplemente a realizaciones preferentes particulares.

La Figura 1 muestra una vista en planta de tres edificios 10, 20, 30. El primero de los edificios 10 es el lugar de trabajo de un empleado de una empresa que opera la realización descrita. Los otros dos edificios 20, 30 pueden ser otros lugares de trabajo de diferentes empresas. Varios emisores inalámbricos 10a-c están asociados con el primer edificio 10. Los otros edificios 20, 30 también pueden tener sus propios emisores inalámbricos 20a, 30a. Los emisores inalámbricos pueden ser, por ejemplo, un dispositivo Wi-Fi tal como un enrutador Wi-Fi o extensores Wi-Fi, o un dispositivo Bluetooth, tal como una baliza Bluetooth. El empleado tiene un dispositivo móvil inteligente (por ejemplo, un teléfono inteligente, una tableta, un ordenador portátil, etc.) 40, que puede estar en cualquier lugar del área mostrada. Está en comunicación inalámbrica con el servidor 50 dentro del primer edificio 10, que es operado por la empresa. El servidor (que puede denominarse en la presente memoria "Servidor de interrupciones") ejecuta software que puede usarse para controlar el acceso a otras aplicaciones y funciones del dispositivo inteligente 40 del empleado.

La Figura 2 corresponde a la Figura 1, excepto que muestra una región circular 16 centrada en un punto 12 definido por coordenadas GPS.

La empresa con sede en el primer edificio 10 quiere permitir a los empleados utilizar sus propios dispositivos inteligentes en el lugar de trabajo, limitando al mismo tiempo el acceso a determinadas aplicaciones y/o funciones en esos dispositivos cuando el empleado está en el lugar de trabajo y durante el horario laboral, para mejorar productividad de los trabajadores. Para lograr esto, el empleador puede pedir a los empleados que descarguen un programa informático (aplicación) en sus dispositivos inteligentes. Por ejemplo, a un empleado se le puede enviar un mensaje a su dispositivo inteligente invitándole a descargar la aplicación desde un enlace concreto.

Una vez instalada, la aplicación (que puede denominarse "aplicación de control") configura el dispositivo inteligente 40 para entrar en contacto con el servidor 50 en respuesta a ciertos eventos, tales como la llegada de una notificación push o un movimiento detectado dentro o fuera de una región predeterminada (ver más abajo), en cuyo punto, el dispositivo inteligente 40 transmite al servidor 50 datos con respecto al estado actual del dispositivo inteligente 40. En particular, el dispositivo inteligente 40 envía datos que incluyen: los permisos actuales de la aplicación de control, el estado actual de activación del receptor GPS y todos los dispositivos receptores inalámbricos, y el estado actual de un conmutador de anulación manual de la aplicación de control en el dispositivo inteligente 40. Estos pasos se analizan más adelante en relación con la Figura 4.

La aplicación y el servidor 50 están configurados para cooperar para realizar los siguientes pasos, mostrados en la Figura 3:

Paso 100: determinar una ubicación del dispositivo inteligente;

Paso 102: determinar la hora actual;

Paso 104: verificar si la hora actual está dentro de un período de tiempo predeterminado;

Paso 106: verificar si la ubicación está dentro de una región predeterminada;

Paso 108: si la hora actual está dentro de un período de tiempo predeterminado y la ubicación está dentro de una región predeterminada, entonces un conjunto predeterminado de aplicaciones y/o funciones (lista negra) se bloquean en el dispositivo inteligente o todas las aplicaciones y/o funciones excepto para un conjunto predeterminado de aplicaciones (lista blanca) están bloqueadas en el dispositivo inteligente; de lo contrario

Paso 110: desactivar cualquier bloqueo de aplicaciones y/o funciones (es decir, desbloquear esas aplicaciones y/o funciones).

En otras realizaciones, es posible que el paso 104 no se lleve a cabo y, por lo tanto, el paso 108 puede implicar un bloqueo basado únicamente en la ubicación. Estos pasos se describirán con más detalle a continuación, haciendo referencia a la realización en la que se realiza el paso 104.

5 Las decisiones sobre cuándo activar o desactivar el bloqueo de aplicaciones y/o funciones en el dispositivo inteligente 40 las toma el software que se ejecuta en el servidor 50, en base a los datos recibidos desde el dispositivo inteligente. Por lo tanto, en relación con el Paso 100, el dispositivo inteligente enviará datos relacionados con el movimiento detectado dentro o fuera de la región predeterminada. El dispositivo inteligente 40 también puede
10 enviar los identificadores de red para todas las redes inalámbricas que detecta el dispositivo inteligente 40 y cualquier baliza visible (por ejemplo, balizas Bluetooth). En base a la información recibida (Pasos 104 y 106), el servidor 50 luego se comunica con el dispositivo inteligente o la aplicación de control en el dispositivo inteligente 40 para indicarle al dispositivo inteligente 40 o a la aplicación de control en el dispositivo inteligente 40 que bloquee o desbloquee aplicaciones y/o funciones en el dispositivo inteligente 40 (Paso 108). Más adelante se describen implementaciones ilustrativas de la funcionalidad de bloqueo para iOS y Android en relación con las Figuras 5 y 6.

15 Como resultado de lo anterior, cuando un empleado está, por ejemplo, en el lugar de trabajo durante el horario laboral, el dispositivo inteligente 40 se configura (mediante la aplicación de control) para bloquear el acceso del usuario a ciertas aplicaciones y/o funciones.

20 La determinación de la ubicación del dispositivo (Paso 100) está relacionada con la definición de la región predeterminada utilizada en el Paso 106, por lo que ahora se describen juntas con más detalle.

La región predeterminada puede definirse de diferentes maneras. Por ejemplo, en la Figura 1, el empleador puede definir la región predeterminada como un área definida por un conjunto de coordenadas GPS que definen la forma del edificio 10. En este caso, un empleado con un dispositivo inteligente 40 en la ubicación A estaría dentro de la
25 región predeterminada y, por lo tanto, durante un periodo de tiempo predeterminado, por ejemplo, horas de trabajo, la aplicación de control estaría activa bloqueando ciertas aplicaciones y/o funciones o permitiendo ciertas aplicaciones y/o funciones en el dispositivo inteligente de un empleado, según corresponda.

30 Alternativa o adicionalmente, la región predeterminada puede definirse como un área definida por una única coordenada GPS 12 y un radio 14, definiendo de esta manera una región circular 16, como se muestra en la Figura 2. Esta región puede extenderse más allá del edificio 10 y, en consecuencia, un empleado en la ubicación A o en la ubicación B estaría dentro de la región predeterminada.

35 La región predeterminada puede comprender una o más áreas definidas de diferentes maneras. La región predeterminada puede ser una superposición de tales áreas o una agregación de tales áreas. Por ejemplo, la región predeterminada puede comprender un área definida por un conjunto de coordenadas GPS y un área definida por una única coordenada GPS y un radio. Por tanto, si un empleado se encuentra dentro de una región predeterminada que comprende una superposición o agregación de cualquiera de una pluralidad de áreas por lo tanto definidas, la
40 aplicación de control en el dispositivo inteligente 40 del empleado estaría activa en el bloqueo.

Alternativa, o adicionalmente, la región predeterminada puede definirse como cualquier lugar en el que el dispositivo inteligente 40 pueda detectar una red inalámbrica en particular, por ejemplo, cuando está dentro del alcance de cualquiera de los emisores inalámbricos 10a-c (Figura 1).

45 En este ejemplo, la región predeterminada se define como cualquier lugar donde un dispositivo inteligente 40 propiedad de un empleado del primer edificio 10 pueda detectar los emisores inalámbricos 10a-c del primer edificio.

Los dispositivos inteligentes normalmente pueden detectar varios emisores inalámbricos sin conectarse a ninguno de ellos. Los emisores inalámbricos 20a, 30a del segundo y tercer edificios 20, 30 no están asociados con la empresa del primer edificio 10. Por lo tanto, incluso si un dispositivo inteligente 40 detecta estos emisores inalámbricos 20a, 30a, no definen la región predeterminada. Por lo tanto, el dispositivo inteligente 40 de un empleado del primer edificio 10 en la ubicación C puede detectar la red inalámbrica 20a pero, siempre que el dispositivo inteligente 40 no pueda detectar ninguno de los emisores inalámbricos 10a-c del primer edificio 10,
55 entonces la ubicación C está fuera la región predeterminada. El experto apreciará fácilmente cómo configurar la aplicación de control para distinguir entre emisores inalámbricos que definen la región predeterminada y emisores inalámbricos no relacionados con la región predeterminada, por ejemplo, en virtud de un identificador particular.

De manera similar, si un empleado de una empresa del segundo edificio 20 (que también implementa este sistema) está en la ubicación A con su dispositivo inteligente 40, entonces su dispositivo inteligente 40 puede detectar uno o todos los emisores inalámbricos 10a-c del primer edificio 10 pero, a menos que su dispositivo inteligente 40 pueda detectar el emisor inalámbrico 20a del segundo edificio, la ubicación A está fuera de la región predeterminada para el dispositivo inteligente 40 de ese empleado.

65 Dicho de otra manera, cada dispositivo inteligente 40 puede configurarse para utilizar diferentes procedimientos para identificar regiones predeterminadas. Por lo tanto, un primer dispositivo inteligente 40 puede tener una región

predeterminada definida por la coordenada GPS 12 y el radio 14, como se muestra en la Figura 2. Un segundo dispositivo inteligente 40' puede tener una región predeterminada definida por su capacidad de detectar un emisor inalámbrico 30a determinado.

La aplicación de control recopila por lo tanto datos relacionados con la ubicación del dispositivo inteligente 40, por ejemplo, datos GPS de un receptor GPS y/o datos relacionados con la detección de un identificador de red, por ejemplo, de un dispositivo receptor inalámbrico tal como un dispositivo receptor Bluetooth, dispositivo receptor Wi-Fi o dispositivo receptor de red celular. Los dispositivos GPS y receptores inalámbricos pueden considerarse como "sensores" que proporcionan datos de ubicación. La aplicación de control evalúa, en base a los datos de ubicación, si la ubicación se encuentra dentro de la región predeterminada. Si es así, la aplicación de control contacta con el servidor 50.

La hora actual (Paso 102) puede determinarse a partir de un reloj en el servidor 50 o en el dispositivo inteligente 40. Preferentemente, la hora se determina a partir de un reloj en el servidor 50 para evitar la elusión del usuario al cambiar el reloj en su dispositivo inteligente 40. Luego, la aplicación de control determina si el tiempo cae dentro de un período durante el cual se requiere el bloqueo (Paso 104), por ejemplo, durante el horario laboral normal de la empresa.

Suponiendo que sea necesario, el bloqueo de aplicaciones y/o funciones (Paso 108) puede efectuarse mediante la aplicación de control o mediante la interacción del servidor con el dispositivo inteligente. La forma en que se realiza el bloqueo puede depender del sistema operativo que se ejecuta en el dispositivo inteligente, por ejemplo, iOS o Android. Más adelante se describen realizaciones de la funcionalidad de bloqueo.

Para determinar qué aplicaciones y/o funciones deben bloquearse en el paso 108, se puede determinar un conjunto de aplicaciones y/o funciones permitidas como una lista blanca, es decir, el empleador prepara una lista de aplicaciones y/o funciones que están permitidas que se pueden utilizar durante el horario laboral y en el lugar de trabajo, y todas las demás aplicaciones y/o funciones están bloqueadas de forma predeterminada.

Alternativamente, el conjunto de aplicaciones y/o funciones puede determinarse como una lista negra, es decir, el empleador prepara una lista de aplicaciones y/o funciones que deben bloquearse durante el horario laboral y en el lugar de trabajo, y todas las demás aplicaciones y/o funciones están permitidas de forma predeterminada.

Un dispositivo inteligente 40 puede funcionar más rápido o tener una duración de batería más larga como consecuencia del bloqueo de aplicaciones y/o funciones de la manera proporcionada por la presente divulgación.

Es una característica general de los sistemas operativos (SO) de dispositivos inteligentes que cualquier aplicación requiere varios "permisos" para interactuar con el dispositivo y con otras aplicaciones. Normalmente, cuando un usuario descarga una aplicación, el dispositivo inteligente 40 alerta al usuario sobre qué permisos de aplicación se requieren para el correcto funcionamiento de esa aplicación descargada. Por ejemplo, es común que las aplicaciones requieran acceso a Internet para poder mostrar anuncios a los usuarios que utilizan la aplicación. También es común que una aplicación solicite acceso a los contactos del usuario almacenados en el dispositivo inteligente 40 si esa aplicación tiene funcionalidad para compartir datos con otros (por ejemplo, enviando un mensaje de texto o correo electrónico a los dispositivos de otros usuarios desde esa aplicación).

Para implementar el procedimiento descrito anteriormente a través de una aplicación, es importante que la aplicación de control tenga los permisos correctos.

En consecuencia, el servidor 50 recibe una lista de los permisos de aplicación de control requeridos. La aplicación de control comunica una lista de permisos actuales de la aplicación de control al servidor 50. La lista de permisos actuales de la aplicación de control puede considerarse como un tipo de "parámetros actuales del dispositivo inteligente". El servidor 50 puede verificar si los permisos actuales de la aplicación de control coinciden con la lista de permisos de la aplicación de control requeridos. Si el dispositivo inteligente 40 no tiene los permisos correctos de la aplicación de control, el servidor 50 puede enviar una notificación push al dispositivo inteligente 40 para solicitar al dispositivo inteligente 40 que se comuniquen con el servidor 50. Luego, el servidor 50 envía información a la aplicación de control para notificar al usuario que necesita ajustar sus permisos o hacer que la aplicación de control ajuste los permisos automáticamente. Las notificaciones automáticas pueden ser realizadas, por ejemplo, por el servicio Urban Airship.

La Figura 4 muestra un diagrama de secuencia de este proceso. Las acciones en el dispositivo inteligente 40 se muestran a la izquierda y las acciones en el servidor 50 están a la derecha.

Paso 200: un usuario, por ejemplo un administrador, establece los parámetros predeterminados (por ejemplo, permisos de aplicación de control requeridos) en el servidor 50.

Paso opcional 201a: el servidor 50 solicita al dispositivo inteligente 40 que envíe una lista de parámetros actuales. Estos parámetros incluyen: permisos de aplicaciones de control actuales establecidos en el dispositivo inteligente

40; el estado actual de activación del o cada dispositivo receptor inalámbrico del dispositivo inteligente 40; y el estado actual de un conmutador de anulación manual de la aplicación de control en el dispositivo inteligente 40. El servidor 50 también puede solicitar identificadores de red para cualquier red inalámbrica que sea detectada por el dispositivo inteligente 40.

Paso 201: la aplicación de control envía la lista de parámetros actuales al servidor 50, incluidos los permisos actuales de la aplicación de control y opcionalmente los identificadores de red, de acuerdo con la solicitud.

Paso 202: el servidor 50 verifica si los parámetros actuales se ajustan a un conjunto predeterminado de parámetros.

Paso 203: si los parámetros actuales no se ajustan al conjunto predeterminado de parámetros (por ejemplo, si los permisos de la aplicación de control actual no se ajustan a los permisos de la aplicación de control requeridos), entonces el servidor 50 envía una notificación al dispositivo inteligente 40 que contiene el conjunto predeterminado de parámetros (es decir, especificar los permisos de la aplicación de control necesarios).

Paso 204: el dispositivo inteligente 40 aplica entonces los parámetros o solicita a un usuario que aplique el conjunto predeterminado de parámetros, según sea necesario. Por lo tanto, dado que los parámetros incluyen permisos de aplicaciones de control actuales, el dispositivo inteligente 40 aplica los permisos de aplicaciones de control predeterminados o solicita al usuario que lo haga.

Si un usuario tiene permisos incorrectos de manera persistente, esto podría indicar que está intentando eludir la aplicación cuando se encuentra en el lugar de trabajo durante el horario laboral. Por lo tanto, se puede implementar un procedimiento de auditoría en el que, si se determina que los permisos de la aplicación para un dispositivo inteligente 40 dado son incorrectos más de un cierto número de veces (por ejemplo, 5 veces, o en 5 días hábiles diferentes), el servidor 50 puede enviar una alerta a un segundo usuario, por ejemplo un supervisor de la empresa, para identificar el dispositivo inteligente 40 y su propietario y alertar al segundo usuario de que esta persona puede estar intentando eludir la funcionalidad de la aplicación de control.

Alternativamente, un usuario puede intentar eludir la aplicación de control impidiendo que la aplicación de control entre en contacto con el servidor 50 (por ejemplo, desactivando todos los sistemas de comunicación inalámbrica en su dispositivo inteligente 40). Por lo tanto, el servidor 50 puede almacenar una o ambas de la frecuencia con la que la aplicación de control se conecta al servidor 50 y un tiempo (duración) desde que el dispositivo inteligente 40 se conectó por última vez al servidor 50. Si la frecuencia de contacto es demasiado baja, el servidor 50 puede alertar a un segundo usuario, por ejemplo, un supervisor, de que el usuario puede estar intentando eludir la aplicación de control. Si el tiempo transcurrido desde la última comunicación desde la aplicación de control es demasiado largo, el servidor 50 puede alertar a un segundo usuario, por ejemplo un supervisor, de que el usuario puede estar intentando eludir la aplicación de control.

Como se mencionó anteriormente, la implementación particular del procedimiento y sistema dependerá del sistema operativo que se ejecuta en el dispositivo inteligente 40. En particular, la implementación de la funcionalidad de bloqueo será diferente para iOS y Android.

A continuación se describe una implementación de la aplicación de control 42a que está configurada para ejecutarse en iOS producida por Apple Inc. con referencia a la Figura 5. No tiene capacidad para bloquear o desbloquear directamente aplicaciones y/o funciones (en otras palabras, activar o desactivar filtros de aplicaciones) ni para determinar directamente el estado de bloqueo (es decir, el estado de los filtros). En cambio, para ello depende de los elementos del lado del servidor. Los dispositivos inteligentes iOS 40 pueden inscribirse en un sistema de gestión de dispositivos móviles implementado por el servidor 50. Esto permite que el sistema MDM administre el dispositivo inteligente. Por lo tanto, el dispositivo inteligente 40 puede denominarse "dispositivo gestionado".

A continuación se describe una implementación de la aplicación de control 42b que está configurada para ejecutarse en el sistema operativo Android producido por Google Inc., con referencia a la Figura 6. A diferencia del sistema iOS, es totalmente responsable de la implementación del bloqueo (es decir, implementar filtros para controlar el bloqueo/desbloqueo de ciertas aplicaciones/funciones). Esto se debe a que, en Android, las aplicaciones tienen un control potencial mucho mayor sobre otras aplicaciones.

Considerando primero la realización de iOS, la Figura 5 muestra un diagrama de arquitectura del proceso de bloqueo de aplicaciones en un dispositivo inteligente 40 que ejecuta iOS de Apple. En esta realización, los dispositivos inteligentes iOS 40 que tienen la aplicación de control 42a instalada en estos se inscriben en un sistema de gestión de dispositivos móviles implementado por un servidor 50. El servidor utiliza las funciones de MDM de iOS para controlar la funcionalidad disponible (por ejemplo, las aplicaciones y/o funciones que están bloqueadas/no bloqueadas) en los dispositivos administrados como se describió anteriormente.

En iOS, es posible que un dispositivo (por ejemplo, el dispositivo inteligente 40) esté inscrito en uno o ninguno de los sistemas MDM a la vez. Inscribirse en un sistema MDM permite que el sistema MDM administre el dispositivo inteligente 40 de varias maneras, incluyendo desactivar/activar aplicaciones, la cámara y el navegador web Safari.

Hay dos mecanismos de control. El sistema MDM puede requerir que un dispositivo aplique o elimine cualquier número de 'Perfiles de configuración'. Deshabilitar aplicaciones, la cámara y el navegador Safari son consecuencias de aplicar perfiles de configuración.

- 5 Los sistemas MDM también pueden aplicar comandos a dispositivos. Los comandos suelen ser cambios de estado, como hacer que un dispositivo inteligente 40 instale una determinada aplicación o poner el dispositivo en modo "perdido".

10 La aplicación de control recopila datos relacionados con la ubicación del dispositivo inteligente 40 como se describió anteriormente, por ejemplo, usando sensores tales como un receptor GPS, un dispositivo receptor Bluetooth, un dispositivo receptor Wi-Fi o un dispositivo receptor de red celular. El movimiento hacia o desde una región predeterminada se puede detectar en base a los datos de este sensor como se describió anteriormente, y esto permite que se le indique al MDM que configure la funcionalidad permitida del dispositivo (por ejemplo, si/qué aplicaciones se van a bloquear) en el dispositivo gestionado. En términos de implementación específica, en función de la versión exacta de iOS que se ejecuta en el dispositivo inteligente 40 y el nivel de gestión permitida, la MDM puede indicarle al dispositivo inteligente 40 que instale o elimine perfiles de configuración que controlan la disponibilidad de aplicaciones y/o funciones del dispositivo.

20 El proceso de bloqueo de aplicaciones se ilustra en la Figura 5.

El flujo de operaciones es el siguiente:

25 Paso 1: Se produce un evento que hace que la aplicación de control 42a, a través del dispositivo inteligente 40, entre en contacto con el servidor 50 (ref 1). Este evento puede ser la detección, por parte de la aplicación de control 42a, del movimiento del dispositivo inteligente 40 hacia o desde una región conocida (definida, por ejemplo, por coordenadas GPS o por proximidad/detección de una red inalámbrica, etc.). Alternativamente, el evento puede ser un evento programado periódicamente, tal como una instrucción diaria para entrar en contacto con el servidor 50. La aplicación de control 42a envía al menos: los permisos actuales de la aplicación de control 42a, el estado actual de activación del receptor GPS y todos los dispositivos receptores inalámbricos, y el estado actual de un conmutador de anulación manual en el dispositivo inteligente 40. Si la aplicación de control 42a ha detectado movimiento del dispositivo inteligente 40 dentro o fuera de la región, la aplicación de control lo comunicará al servidor 50.

30 Paso 2: El servidor 50 recibe la información y determina, en base a esa información y la hora de acuerdo con el reloj del servidor 50, qué aplicaciones y/o funciones en el dispositivo inteligente 40 deben bloquearse. El servidor 50 envía una instrucción 2 al MDM que contiene una lista de qué aplicaciones, si las hay, que deberían bloquearse en el dispositivo inteligente 40.

Paso 3: La MDM ordena (ref. 3) al APNS que envíe un mensaje de "activación" 7 al dispositivo inteligente 40.

Paso 4: El APNS acusa recibo (ref. 8) de la instrucción de envío de mensaje al MDM.

Paso 5: La MDM reconoce (ref. 9) la instrucción del servidor 50.

40 Paso 6: El servidor 50 devuelve (ref. 6) los permisos actuales de la aplicación de control 42a, el estado actual de activación del receptor GPS y todos los dispositivos receptores inalámbricos, y el estado actual de un conmutador de anulación manual al dispositivo inteligente 40.

Paso 7: El APNS envía un mensaje de "activación" (ref. 7 nuevamente) al dispositivo inteligente 40. Esto es asíncrono con el paso 6.

45 Paso 8: El dispositivo inteligente 40, al recibir el mensaje de "activación" del APNS, entra en contacto con la MDM (ref. 8 nuevamente) para recuperar una lista de qué funcionalidad (aplicaciones y/o funciones) deben bloquearse o desbloquearse en el dispositivo inteligente 40. La funcionalidad bloqueada también puede considerarse funcionalidad deshabilitada; la funcionalidad desbloqueada puede considerarse como funcionalidad habilitada. Por lo tanto, las aplicaciones/funciones bloqueadas también pueden considerarse aplicaciones/funciones deshabilitadas; las aplicaciones/funciones desbloqueadas también pueden considerarse aplicaciones/funciones habilitadas.

50 Paso 9: La MDM envía (ref. 9 nuevamente) al dispositivo inteligente 40 una lista de qué funcionalidades (aplicaciones y/o funciones) deben bloquearse/desbloquearse (deshabilitarse/habilitarse) y el dispositivo inteligente ajusta su configuración en consecuencia.

55 Como se indicó anteriormente, en una realización alternativa, la aplicación 42b puede ejecutarse en el sistema operativo Android. La aplicación de control para Android puede tener un alto nivel de permisos para afectar el funcionamiento de otras aplicaciones. Actualmente existe una variación en el campo de las versiones y dispositivos del sistema operativo Android compatibles que pueden requerir el uso de una combinación de técnicas para lograr el bloqueo de aplicaciones y/o funciones. La aplicación de control configurada para ejecutarse en Android puede lograr el bloqueo de aplicaciones mediante dos enfoques:

- 65 1. Servicios de Accesibilidad. La aplicación de control 42a guía al usuario a través del proceso de conceder permiso para que la aplicación de control detecte cuando otras aplicaciones pasan a primer plano y pueda "taparlas" para impedir su uso.

2. Servicios VPN. La aplicación de control 42a también solicitará al usuario que otorgue los permisos necesarios

para evitar que las aplicaciones bloqueadas se comuniquen directamente con cualquier red.

En función de su disponibilidad en la versión específica del sistema operativo Android de un dispositivo, la aplicación de control 42a puede usar una combinación de servicios del sistema Android para evitar la interacción con aplicaciones bloqueadas a través de la interfaz de usuario principal, notificaciones u otras formas de mensajería de la aplicación. Estos incluyen servicios de accesibilidad, servicios VPN y acceso a la lista de procesos en ejecución.

Actualmente, en Android, las aplicaciones tienen un nivel mucho mayor de control potencial sobre otras aplicaciones en el mismo dispositivo inteligente (por ejemplo, dispositivo inteligente 40). Por esta razón, una implementación de la aplicación de control configurada para ejecutarse en Android no requiere la misma influencia en todo el dispositivo que en el caso de iOS. En cambio, la aplicación de control que se ejecuta en Android requiere un alto nivel de permisos para afectar el funcionamiento de otras aplicaciones. El bloqueo del uso del navegador y de la cámara se puede realizar bloqueando las aplicaciones utilizadas para abrir esas funciones. Para estos dispositivos, el proceso de entrar en contacto con el servidor 50 y bloquear aplicaciones y/o funciones puede implementarse de acuerdo con el siguiente proceso ilustrado en la Figura 6:

Paso 1: Se produce un evento que hace que la aplicación de control 42b, a través del dispositivo inteligente 40, entre en contacto (ref. 1) con el servidor 50. La aplicación de control 42b envía al menos: los permisos actuales de la aplicación de control 42b, el estado actual de activación del receptor GPS y todos los dispositivos receptores inalámbricos, y el estado actual de un conmutador de anulación manual en el dispositivo inteligente 40. Si la aplicación de control 42b ha detectado movimiento del dispositivo inteligente 40 dentro o fuera de la región, la aplicación de control lo comunicará al servidor 50.

Paso 2: El servidor 50 recibe la información y determina a partir de ahí qué aplicaciones en el dispositivo inteligente 40 deben bloquearse. El servidor 50 responde (ref. 2) al dispositivo inteligente 40 con una lista de qué aplicaciones y/o funciones, si las hay, deberían bloquearse en el dispositivo inteligente 40. La aplicación de control 42b aplica entonces estos bloques en el dispositivo inteligente 40.

En función de la disponibilidad de los servicios del sistema Android en la versión específica del sistema operativo Android que se ejecuta en el dispositivo inteligente 40, se utiliza una combinación de servicios del sistema para evitar la interacción con aplicaciones y/o funciones bloqueadas a través de la interfaz de usuario principal, notificaciones u otras formas de mensajería de aplicaciones. Estos incluyen servicios de accesibilidad, servicios VPN y acceso a la lista de procesos en ejecución.

Algunas realizaciones de la divulgación permiten el bloqueo de funciones tales como una cámara y/o un navegador (por ejemplo, el navegador predeterminado). En una implementación de la aplicación de control para un dispositivo inteligente 40 que ejecuta iOS, la cámara o el navegador (por ejemplo, el navegador Safari) se pueden desactivar a nivel del sistema. En otras palabras, se realiza un bloqueo a nivel del sistema. Esto se puede hacer cuando el servidor se comunica con el dispositivo inteligente (no con la aplicación de control) y le indica al dispositivo inteligente que bloquee/desbloquee ciertas funciones como la cámara o el navegador (es decir, cambie la funcionalidad habilitada/deshabilitada). Esto sería una cuestión de implementación sencilla para el experto. Alternativamente, una aplicación que opera la cámara o una aplicación del navegador puede bloquearse como parte del bloqueo de aplicaciones descrito anteriormente. En una implementación para un dispositivo inteligente 40 que ejecuta Android, no se lleva a cabo el bloqueo a nivel de sistema. En cambio, las aplicaciones del navegador y de la cámara no pueden abrirse. Este es un bloqueo extendido a nivel de aplicación.

En una realización de la invención, cuando un usuario (por ejemplo, un empleado) desea hacer uso de la aplicación de control (por ejemplo, como condición de una política BYOD por parte del empleador), el usuario puede descargar la aplicación de control y registrar su dispositivo inteligente 40 con el servidor 50, de manera que el dispositivo inteligente 40 reciba la configuración correcta con respecto a aplicaciones y/o funciones bloqueadas, aplicaciones y/o funciones permitidas, área predeterminada, hora predeterminada, etc., según lo establecido en el servidor 50, por ejemplo, por el empleador. Tras un registro exitoso, la aplicación de control recupera la configuración actual del servidor 50 y luego entra en un bucle de eventos. En este bucle de eventos, la aplicación de control contacta al servidor cuando ocurre un evento en particular, por ejemplo, cuando los datos relevantes del sensor han cambiado o cuando ha pasado un tiempo en particular desde el último contacto. La Figura 8, que se analizará en detalle a continuación, muestra una serie de eventos diferentes, cada uno de los cuales hace que el dispositivo inteligente 40 (intente) entrar en contacto con el servidor 50.

Más específicamente, los tipos de eventos no urgentes pueden incluir el movimiento del dispositivo inteligente 40 desde o hacia la proximidad de la región predeterminada y el primer plano de la aplicación actual en uso por el usuario. Los tipos de eventos urgentes pueden ser la recepción de una notificación push remota desde el servidor 50 y/o cuando un usuario cambia el estado del conmutador de anulación manual en la UI de la aplicación de control.

Cuando ocurre cualquiera de los eventos anteriores, la aplicación de control recopilará todos los datos relevantes (lista de balizas visibles, coordenadas GPS actuales, SSID de red actual, etc.), todos los estados relevantes del dispositivo (permisos, estado de activación de Bluetooth, etc.) y los enviará junto con el estado actual del conmutador de anulación manual al servidor 50. El servidor 50 responderá con la configuración correcta actual

completa y el estado esperado de bloqueo de aplicaciones (es decir, activación del filtro).

Parte de la configuración del servidor 50 será una cantidad mínima de tiempo que la aplicación de control deberá esperar antes de entrar en contacto con el servidor 50 en respuesta a un evento no urgente. Esto se podrá configurar por cliente (por ejemplo, por empleador) y permitirá a los administradores lograr el equilibrio adecuado entre la latencia de bloqueo de aplicaciones y la carga del sistema y el impacto en la batería del dispositivo.

En términos de que la aplicación de control entre en contacto con el servidor 50 después de que haya transcurrido un tiempo en particular desde el último contacto, la aplicación de control se ejecuta en segundo plano en el dispositivo inteligente 40, informando información sobre el estado del dispositivo inteligente 40 al servidor con una frecuencia determinada por el servidor 50.

Las Figuras 7-12 muestran implementaciones detalladas de la aplicación de control que se ejecuta en dispositivos inteligentes 40.

La Figura 7 muestra una vista de alto nivel del sistema que muestra los enlaces de comunicación entre un dispositivo inteligente Android 40 y el servidor 50, y entre un dispositivo inteligente iOS 40 y el servidor 50 (y un MDM 66), y entre un navegador o dispositivo del administrador dedicado (perteneciente, por ejemplo, al empleador) y el servidor 50.

El servidor 50 mostrado en la Figura 7 contiene varios módulos diferentes para proporcionar diferentes funciones. Estos incluyen una API de usuario 52, un sistema de gestión de bases de datos relacionales (RDBMS) 54, una API de administrador 56 y una interfaz de administración web 58. La interfaz de administración web puede permitir que un usuario (por ejemplo, un empleador) acceda al servidor 50 de forma remota para establecer políticas específicas (horas predeterminadas, áreas predeterminadas, listas blancas, listas negras, etc.) para dispositivos inteligentes 40 registrados con ese servidor 50.

En esta realización, el servidor 50 implementa una cola de mensajes 60 para enviar mensajes/actualizaciones a los dispositivos inteligentes 40 de los usuarios. La cola de mensajes 60 se implementa utilizando el sistema de notificaciones push de Urban Airship 62. La cola de mensajes 60 también se comunica con el servicio de correo electrónico Sparkpost 61. El sistema de notificación push 62 se comunica con la aplicación de control que se ejecuta en los dispositivos inteligentes del usuario 40. Las aplicaciones de control se comunican con Crashlytics 64, que es un servicio que proporciona un sistema de informes de fallos. La gestión de dispositivos inteligentes 40 que ejecuta iOS se dirige a través de un sistema de gestión de dispositivos móviles (MDM) 66, como se describió anteriormente. La MDM 66 comprende una API de gestión 68, un sistema de gestión de bases de datos relacionales (RDBMS) 70 y una cola del Servicio de notificaciones push de Apple (APNS) 72, que se comunica con el APNS 74, que, a su vez, se comunica con el dispositivo inteligente 40. El dispositivo iOS 40 se comunica con una API de MDM 76 en la MDM 66. Un administrador se comunica con la interfaz de administración web 58 a través de un navegador 82 que se ejecuta en un dispositivo del cliente 80 (por ejemplo, una PC).

La Figura 8 muestra un diagrama de flujo que muestra un conjunto de procesos (mostrados en cuadros a la izquierda y en la parte superior de la figura) que se ejecutan en segundo plano en una implementación de la invención (es decir, aspectos no visibles para el usuario del dispositivo inteligente 40)). Esto representa situaciones en las que la aplicación de control, a través del dispositivo inteligente 40, se comunica con el servidor 50 para señalar algún evento detectado por la aplicación de control. Estas situaciones son: el dispositivo inteligente 40 que se conecta/desconecta de una red Wi-Fi 84, el dispositivo inteligente 40 entra o sale de una región predeterminada (por ejemplo, geocerca) 86a, 86b, una exploración periódica en busca de balizas 88 por parte del dispositivo inteligente 40, verificar periódicamente si algún servicio VPN se está ejecutando 90 en el dispositivo inteligente 40, verificar periódicamente si la aplicación de control tiene los permisos de aplicación correctos 92a, verificar los estados de Wi-Fi 92b y Bluetooth 92c activos en el dispositivo inteligente 40 y verificar la ubicación 92d del dispositivo inteligente 40.

La aplicación de control implementa un tiempo de permanencia de 30 segundos para determinar que el dispositivo inteligente 40 efectivamente ha entrado en la región predeterminada antes de implementar el bloqueo de la aplicación. Al salir de la región predeterminada, la aplicación desbloquea inmediatamente las aplicaciones bloqueadas.

La exploración periódica de balizas 88 ocurre cada 3 minutos. La verificación para determinar si algún servicio VPN se está ejecutando 90 en el dispositivo inteligente 40 ocurre cada 5 minutos. En este paso 90, si es necesario y posible, la aplicación de control reinicia el servicio VPN.

La aplicación de control implementa subrutinas de escucha para determinar inmediatamente si se implementan los permisos correctos de la aplicación 92a, verificando el estado de Wi-Fi 92b y Bluetooth 92c, verificando la configuración de accesibilidad del sistema operativo 92d y la configuración de notificación 92e.

Cuando es necesario, el servidor 50 envía notificaciones silenciosas a la aplicación de control para

bloquear/desbloquear aplicaciones 94 o para modificar la configuración 96 de la aplicación de control.

Las Figuras 9A y 9B muestran un diagrama de flujo del ciclo de ejecución de la aplicación en un dispositivo inteligente 40 que ejecuta iOS a partir de la primera instalación de la aplicación de control en un dispositivo inteligente iOS 40. (Las Figuras 9A y 9B son partes del mismo diagrama de flujo dividido en dos páginas. Para mostrar claramente los vínculos, varias flechas de flujo que se extienden desde los pasos que se muestran en la Figura 9A están marcadas como A-E y estas corresponden a las flechas de flujo A-E en la Figura 9B).

En estos diagramas, donde una flecha de flujo va a varias acciones (por ejemplo, vea la flecha que sale del cuadro "Aplicación iniciada por el usuario"), las acciones se realizan en orden de arriba hacia abajo en la orientación que se muestra en el diagrama. Es decir, en el ejemplo de la flecha que se extiende desde el bloque "Aplicación iniciada por el usuario", la aplicación pasa a "¿Está registrada?" primero y luego, si corresponde, "Configurar flujo", "Verificar flujo de permiso de ubicación", etc.

Como se muestra en la Figura 9A, una vez que la aplicación de control se instala en el paso S901 y luego el usuario la inicia en el paso S902, la aplicación de control comienza determinando si el dispositivo inteligente 40 está registrado con el servidor 50 en el paso S903.

Si es así, la aplicación de control verifica que puede entrar en contacto con el servidor 50 en el paso S904 y, si es así, la aplicación de control ingresa al bucle de Operación Principal 1000, discutido en detalle a continuación con respecto a las Figuras 10-12B.

Si la aplicación de control no puede entrar en contacto con el servidor 50, genera un mensaje de falla/error (paso S905).

Si la aplicación de control no está registrada con el servidor 50, la aplicación de control primero ingresa al flujo de configuración 1200, descrito a continuación con referencia a las figuras 12A y 12B, y luego ingresa al flujo de verificación de permiso de ubicación 1100, descrito a continuación con referencia a la Figura 11.

En el paso S906, si el inicio de la aplicación o la puesta en primer plano fueron causados por el usuario que tocó el "Recordatorio de permiso de ubicación" (parte del flujo de verificación de permiso de ubicación, que se analiza a continuación en relación con la Figura 11), entonces, en el paso S907, la aplicación redirige al usuario a la aplicación Configuración en el dispositivo inteligente 40 para que el usuario pueda establecer los permisos necesarios.

Estos pasos se realizan en orden cada vez que se inicia la aplicación de control o cuando el usuario la pone en primer plano.

La Figura 9B muestra las acciones de la aplicación de control cuando se ejecuta en segundo plano. En esta situación, el flujo comienza en el paso S908 en el que la aplicación de control verifica si el dispositivo inteligente 40 está registrado con el servidor 50 y, de ser así, comienza el bucle de operación principal 1000. De lo contrario, la aplicación de control intenta entrar en contacto con el servidor 50 en el paso S904 y, si no puede, genera un mensaje de fallo/error (paso S905), es decir, como anteriormente, cuando la aplicación está en primer plano.

Si la aplicación de control no está registrada con el servidor 50, entonces la aplicación de control ingresa al flujo de verificación de permiso de ubicación 1100.

En el paso S908, si, mientras está en segundo plano, el sistema operativo suspende la aplicación de control por cualquier motivo, entonces la aplicación de control puede reiniciarse automáticamente (paso S910) cuando el sistema operativo determina que se ha producido una actualización de ubicación significativa o detecta la entrada del dispositivo inteligente dentro/fuera de la región predeterminada.

Si el usuario o el sistema operativo finalizan la aplicación de control (paso S909), entonces el usuario debe reiniciar manualmente la aplicación de control (es decir, volver al paso S102) o reiniciarla mediante una actualización significativa de la ubicación o detectando la entrada del dispositivo inteligente dentro/fuera de la región predeterminada.

La Figura 10 representa el bucle de operación principal 1000 de la aplicación de control, es decir, su procedimiento de operación. El procedimiento comienza en el paso S1001 con la aplicación de control en el dispositivo inteligente 40 monitoreando la entrada/salida en la región predeterminada. Además, la aplicación de control espera (paso S1002) en el bucle de operación a que ocurra una de las siguientes cosas:

Una actualización del servidor 50 que cambia la región predeterminada 1003;

Se recibe 1004 una notificación push silenciosa desde el servidor 50;

La aplicación de control se pone en primer plano por el usuario 1005;

El usuario cambia un conmutador de filtro manual en la aplicación de control que le permite deshabilitar explícitamente la aplicación y cualquier filtrado activo de aplicaciones 1006. El uso de este conmutador por parte

del usuario se registra en el servidor 50;

El dispositivo inteligente 40 cambia para conectarse a una red Wi-Fi 1007 diferente;

Un cambio en las Autorizaciones de notificación de usuario 1008;

Un cambio en los Permisos de Ubicación 1009 (es decir, autorización en el dispositivo inteligente 40 para usar los Servicios de Ubicación) - en este punto, la aplicación de control ingresa primero al Flujo de Verificación de Permiso de Ubicación 1100;

Un cambio en el estado de la región de baliza o geocerca 1010 (es decir, entrada o salida de la región predeterminada, según lo detectado por el receptor GPS o por la detección/no detección de una baliza de interés, es decir, una baliza que define al menos parcialmente la región predeterminada);

Un cambio en el estado de activación de Bluetooth en el dispositivo inteligente 40 1011 (es decir, encender o apagar un receptor Bluetooth) o un cambio de una/la baliza a la que está conectado el dispositivo inteligente a través de Bluetooth o la detección de una baliza de interés;

Un cambio del dispositivo inteligente a un modo de baja energía 1012; o

Cambio de estado de actualización en segundo plano 1013 (es decir, una configuración cambiada por el usuario en cuanto a si las aplicaciones se pueden actualizar en segundo plano).

En el paso S1014, si la aplicación de control detecta uno de: una actualización del servidor 50 que cambia la región predeterminada 1003; una notificación push silenciosa desde el servidor 50 1004; la aplicación de control está en primer plano por el usuario 1005; o el usuario cambia un conmutador de filtro manual 1006, luego la aplicación de control entra en contacto con el servidor 50 y espera instrucciones de este. Luego, el servidor 50 identifica si la aplicación de control ha fallado o no o si no hay cambios en la lista de regiones (paso S1015a). Si la aplicación de control no ha fallado, el servidor 50 envía (paso S1015a) a la aplicación de control una actualización de la lista de regiones, es decir, una actualización de las regiones predeterminadas.

Si no hay cambios en la región predeterminada, la aplicación de control vuelve al paso de esperar en el bucle de operación a que ocurra uno de los eventos antes mencionados (es decir, paso S1002).

Si hay un cambio en la región predeterminada, la aplicación de control pasa al paso de monitorear la entrada/salida de la nueva región predeterminada (es decir, actualizada) (es decir, el paso S1001).

En cualquiera de los otros eventos 1007-1013 antes mencionados, la aplicación de control verifica si todas las áreas ("regiones") se han determinado en el paso S1016. La aplicación de control tiene una lista de áreas de interés (por ejemplo, una coordenada GPS + radio, una lista de balizas Wi-Fi y Bluetooth, etc.) que conforman la región predeterminada. Un área se señala como "indeterminada" cuando actualmente no está claro para la aplicación si el dispositivo inteligente 40 está dentro o fuera de esa área (por ejemplo, si el receptor GPS aún no ha obtenido una posición exacta sobre la ubicación del dispositivo inteligente). Un área se señala como "determinada" cuando la aplicación de control sabe definitivamente si el dispositivo inteligente 40 está o no dentro de la región predeterminada. Si no se han determinado todas las regiones, el flujo vuelve al paso S1002. Si se han determinado todas las regiones, la aplicación de control entra en contacto con el servidor 50 en el paso S1018.

La Figura 11 muestra el flujo de verificación de permiso de ubicación 1100. Esta Figura detalla el flujo de pasos cuando la aplicación de control solicita los permisos de ubicación necesarios (es decir, acceso a servicios de ubicación) desde un dispositivo inteligente 40 que ejecuta iOS. Los servicios de ubicación en dispositivos inteligentes iOS (y Android) 40 permiten determinar la ubicación del dispositivo inteligente 40 detectando señales de datos celulares, señales de Wi-Fi, redes GPS y/o balizas Bluetooth, como se describió anteriormente, y la aplicación de control está configurada para utilizar los servicios de ubicación para determinar la ubicación del dispositivo inteligente 40 con respecto a la(s) región(ones) predeterminada(s).

El flujo de verificación de permisos de ubicación comienza en el paso S1101 en el que la aplicación de control primero verifica si al usuario se le ha solicitado previamente que proporcione los permisos de ubicación necesarios.

En caso contrario, el flujo finaliza (paso S1102).

Si es así, el siguiente paso (paso S1103) es que la aplicación de control determine si los Permisos de Ubicación otorgados por el usuario son realmente los necesarios para el correcto funcionamiento de la aplicación de control.

Si los permisos no son correctos, la aplicación de control verifica si ya está programado un recordatorio para recordarle al usuario que establezca los permisos de ubicación correctos en el sistema operativo en el paso S1104. Si no se establece ningún recordatorio, la aplicación de control programa un recordatorio para el usuario (paso S1105) y el flujo finaliza.

Si los permisos de ubicación son correctos, entonces la aplicación de control cancela cualquier recordatorio pendiente al usuario con respecto a los permisos de ubicación para la aplicación de control (paso S1106) y el flujo finaliza.

Las Figuras 12A y 12B representan el flujo de pasos para configurar inicialmente la aplicación en un dispositivo

inteligente 40 que ejecuta iOS. En "Inicio", la aplicación se ejecuta por primera vez y la aplicación inicialmente verifica si el dispositivo inteligente 40 está registrado con un servidor en particular 50. El proceso continúa a partir de ahí y se describe en detalle a continuación. (Las Figuras 12A y 12B son partes del mismo diagrama de flujo dividido en dos páginas. Para mostrar claramente los vínculos, varias flechas de flujo que se extienden desde los pasos mostrados en la Figura 12A están marcadas como F-K y corresponden a las flechas de flujo F-K en la Figura 12B. Es decir, por ejemplo, después del paso de "El usuario permite/deniega permisos", en la Figura 12A, el diagrama de flujo continúa a lo largo de la flecha "K" hasta el paso de "¿Son correctos los permisos?" que se muestra en la Figura 12B, etc.) En este flujo, la aplicación de control primero verifica si el dispositivo inteligente 40 está registrado con el servidor 50 (paso S1201). Si es así, la aplicación de control verifica si los permisos de aplicación requeridos se han solicitado previamente (paso S1202).

Si es así, se muestra al usuario la pantalla de verificación de configuración S1212a y la aplicación de control luego verifica si los permisos son correctos (en el paso S1203) y, de ser así, la aplicación de control se comunica con el servidor 50 para verificar si el dispositivo inteligente 40 está registrado correctamente en la MDM (en el paso S1204). Si el dispositivo está registrado incorrectamente en la MDM, se muestra al usuario un mensaje de Reintentar S1204a y se repite el paso S1204.

Una vez que se determina que el dispositivo inteligente 40 está registrado (en el paso S1205) en el MOM, se muestra al usuario la pantalla de Filtro manual (paso S1206) y el flujo finaliza.

Si el dispositivo inteligente 40 no está inscrito en la MDM, la aplicación de control determina si el usuario ha seguido previamente el enlace de MDM (paso S1207) y, de ser así, se le muestra al usuario un mensaje "MDM eliminado" (paso S1208) y se le indica que siga el enlace MDM (paso S1209), momento en el cual finaliza el flujo y el usuario queda en la aplicación Safari. Si el usuario no ha seguido previamente el enlace MDM, se le muestra el enlace MDM (paso S1210) y se le indica al usuario que lo siga (paso S1209), momento en el que finaliza el flujo y se deja al usuario en Safari aplicación. Cuando el usuario está inscrito en la MDM, el navegador de Internet de iOS, Safari, media la comunicación entre la aplicación de control y el servidor MDM 66.

Si la aplicación de control determina que los permisos de aplicación requeridos son incorrectos (en S1203), se informa al usuario en consecuencia (paso S1211) y se le dirige a la aplicación de configuración de iOS (paso S1212) para corregir esto, momento en el cual finaliza el flujo y el usuario se deja en la aplicación de configuración de iOS.

Si la aplicación de control determinó que no se han solicitado los permisos necesarios (en el paso S1202), la aplicación de control dirige al usuario a las pantallas relevantes (por ejemplo, pantallas de Acceso a la ubicación y/o Acceso a notificaciones) en el paso S1213, momento en el cual el usuario permite o deniega los permisos en el paso S1214. Si los permisos están permitidos, la aplicación de control verifica si los permisos son correctos en el paso S1215 y, si no, se muestra al usuario la pantalla "Permisos incorrectos" en el paso S1211 y el flujo continúa desde ese paso.

Si los permisos son correctos en el paso 1215, se muestra al usuario la pantalla de enlace MDM en el paso S1210 y el flujo continúa desde ese paso.

Si se deniegan los permisos, se le solicita nuevamente al usuario que permita los permisos correctos y esto se repite hasta que se acepten y el flujo continúe como se indicó anteriormente.

Si el dispositivo no está registrado, se le solicita al usuario que ingrese un código de autorización recibido del servidor 50 en el paso S1216, el usuario ingresa dicho código de autorización S1216a que la aplicación registra con el servidor S1216b, que luego se verifica con el servidor 50 S1217. Si el código es válido, entonces la aplicación de control se registra con el servidor 50 y la actividad se ramifica en dos flujos simultáneos: un primer flujo en el que la aplicación ingresa al bucle de operación principal, descrito anteriormente y un segundo flujo que pasa al paso 1213, descrito anteriormente. Si el código de autenticación no es válido, al usuario se le muestra un mensaje de error S1218 y el flujo vuelve al paso S1216.

REIVINDICACIONES

1. Un procedimiento para bloquear una o más aplicación(ones) y/o función(ones) en un dispositivo inteligente (40), en el que el dispositivo inteligente comprende un receptor GPS y uno o más dispositivos receptores inalámbricos; comprendiendo el procedimiento, en el dispositivo inteligente:

detectar, mediante una aplicación de control que se ejecuta en el dispositivo inteligente, el movimiento del dispositivo inteligente hacia o desde una región predeterminada (16) en base a los datos recibidos por el receptor GPS y/o uno o más de los dispositivos receptores inalámbricos; y
 bloquear una o más aplicación(ones) y/o función(ones) en el dispositivo inteligente cuando el dispositivo inteligente se encuentra dentro de la región predeterminada;
 en el que el dispositivo inteligente (40) está configurado para comunicarse con un servidor (50); y el procedimiento caracterizado por:

el dispositivo inteligente (40) envía al servidor (50) un conjunto de parámetros actuales del dispositivo inteligente que se aplican actualmente o son detectados por el dispositivo inteligente;
 en el que el conjunto de parámetros comprende: algunos o todos los permisos de aplicación actuales para la aplicación de control, el estado actual de activación de uno o más dispositivos receptores inalámbricos del dispositivo inteligente y el estado actual de un conmutador de anulación manual de la aplicación de control en el dispositivo inteligente.

2. El procedimiento de la reivindicación 1, en el que el paso de bloqueo comprende bloquear todas las aplicaciones y/o funciones en el dispositivo inteligente excepto una o más aplicación(ones) y/o función(ones) predeterminadas cuando el dispositivo inteligente (40) esté dentro de la región predeterminada (16).

3. El procedimiento de cualquier reivindicación anterior, que comprende además determinar una hora actual; y en el que una o más aplicación(ones) y/o función(ones) se bloquean cuando tanto el dispositivo inteligente (40) está dentro de la región predeterminada como la hora actual está dentro de un período de tiempo predeterminado.

4. El procedimiento como se reivindicó en la reivindicación 1, que comprende:

la aplicación de control envía datos relacionados con el movimiento del dispositivo inteligente (40) dentro o fuera de la región predeterminada (16) al servidor (50);
 el servidor (50) determina, en base a estos datos, si la(s) aplicación(ones) y/o función(ones) deben bloquearse en el dispositivo inteligente (40); y
 el servidor (50) se comunica con el dispositivo inteligente (40) para proporcionar instrucciones para bloquear aplicación(ones) y/o función(ones), en el que el bloqueo se lleva a cabo en respuesta a estas instrucciones.

5. El procedimiento de la reivindicación 1 o 4, que comprende además los pasos de:

el servidor (50) determina si los parámetros actuales del dispositivo inteligente se ajustan a un conjunto predeterminado de parámetros; y
 cuando los parámetros actuales del dispositivo inteligente no se ajustan al conjunto predeterminado de parámetros, enviar una notificación al dispositivo inteligente para instruir al dispositivo inteligente (40) o a un usuario del dispositivo inteligente (40) para ajustar los parámetros actuales del dispositivo aplicados en el dispositivo inteligente (40).

6. El procedimiento de la reivindicación 5, en el que, si se determina que los permisos de la aplicación de control no se ajustan a los permisos de la aplicación de control del conjunto predeterminado de parámetros, el procedimiento comprende el paso de que el servidor envíe una notificación al dispositivo inteligente (40) para iniciar la comunicación con el servidor (50).

7. El procedimiento de la reivindicación 4, 5 o 6, que comprende el paso de que el servidor (50) envíe notificaciones al dispositivo inteligente (40) para configurar o actualizar la región predeterminada (16).

8. El procedimiento de cualquiera de las reivindicaciones 1 y 4 a 7, en el que el dispositivo inteligente (40) está asociado con un primer usuario, y en el que el servidor (50) mantiene un registro de los permisos actuales de la aplicación de control; y
 cuando se determina que los permisos de la aplicación de control no se ajustan a los permisos de la aplicación de control del conjunto predeterminado de parámetros más de un número predeterminado de veces, el servidor envía una alerta a un segundo usuario que identifica al primer usuario.

9. El procedimiento de cualquiera de las reivindicaciones 1 y 4 a 8, en el que el dispositivo inteligente (40) está asociado con un primer usuario, y en el que el servidor (50) mantiene un registro de una frecuencia con la que el dispositivo inteligente (40) se comunicaba con el servidor (50); y

cuando la frecuencia cae por debajo de una frecuencia predeterminada, el servidor (50) envía una alerta a un segundo usuario que identifica al primer usuario.

- 5 10. El procedimiento de cualquiera de las reivindicaciones 1 y 4 a 9, en el que el dispositivo inteligente (40) está asociado con un primer usuario, y en el que el servidor (50) mantiene un registro de la última vez que el dispositivo inteligente (40) se comunica con el servidor (50); y cuando la duración desde la última vez que el dispositivo inteligente (40) se comunica con el servidor (50) excede una duración predeterminada, el servidor (50) envía una alerta a un segundo usuario que identifica al primer usuario.
- 10 11. Un dispositivo inteligente (40) que comprende un receptor GPS y uno o más dispositivos receptores inalámbricos; estando configurado el dispositivo inteligente para: detectar, mediante una aplicación de control (42a,b) que se ejecuta en el dispositivo inteligente, el movimiento del dispositivo inteligente (40) dentro o fuera de una región predeterminada en base a los datos recibidos por el receptor GPS y/o uno o más de los dispositivos receptores inalámbricos; y bloquear una o más aplicación(ones) y/o función(ones) en el dispositivo inteligente cuando el dispositivo inteligente se encuentra dentro de la región predeterminada; y caracterizado por:
20 el dispositivo inteligente configurado para enviar a un servidor (50) un conjunto de parámetros actuales del dispositivo inteligente que se aplican actualmente o son detectados por el dispositivo inteligente; en el que el conjunto de parámetros comprende: algunos o todos los permisos de aplicación actuales para la aplicación de control, el estado actual de activación de uno o más dispositivos receptores inalámbricos del dispositivo inteligente y el estado actual de un conmutador de anulación manual de la aplicación de control en el dispositivo inteligente.
- 25 12. Un sistema que comprende el dispositivo inteligente (40) de la reivindicación 11 y un servidor (50) en el que el dispositivo inteligente está configurado para comunicarse con el servidor cuando envía el conjunto de parámetros actuales del dispositivo inteligente.
- 30 13. El sistema de la reivindicación 12, en el que el servidor (50) contiene instrucciones editables ejecutables por ordenador para definir la región predeterminada; y en el que el servidor contiene instrucciones editables ejecutadas por ordenador para comunicarse con el dispositivo inteligente para establecer la región predeterminada.
- 35 14. El sistema de la reivindicación 12 o 13, en el que el servidor (50) y/o el dispositivo inteligente (40) comprende un reloj, y en el que las instrucciones ejecutables por ordenador del dispositivo inteligente bloquean una o más aplicación(ones) y/o función(ones) en el dispositivo inteligente en base adicionalmente a si una hora actual del reloj está dentro de un período de tiempo predeterminado.
- 40 15. El sistema de acuerdo con la reivindicación 12, 13 o 14, en el que el o cada dispositivo receptor inalámbrico es uno de entre un dispositivo receptor Bluetooth, un dispositivo receptor Wi-Fi y un dispositivo receptor de red celular.

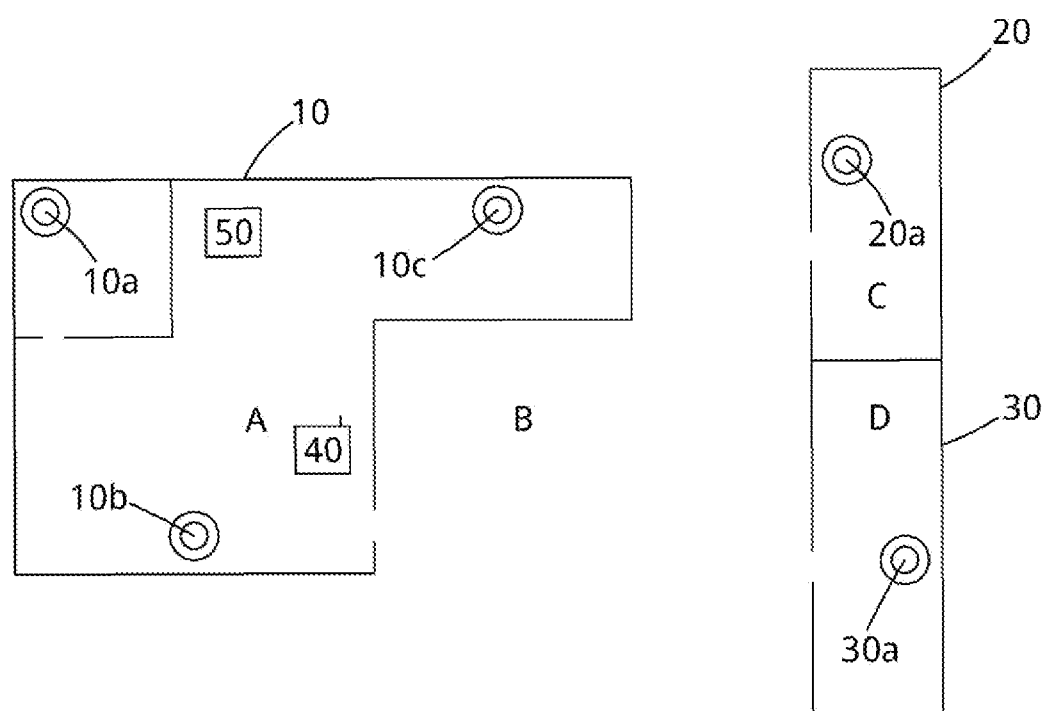


Figura 1

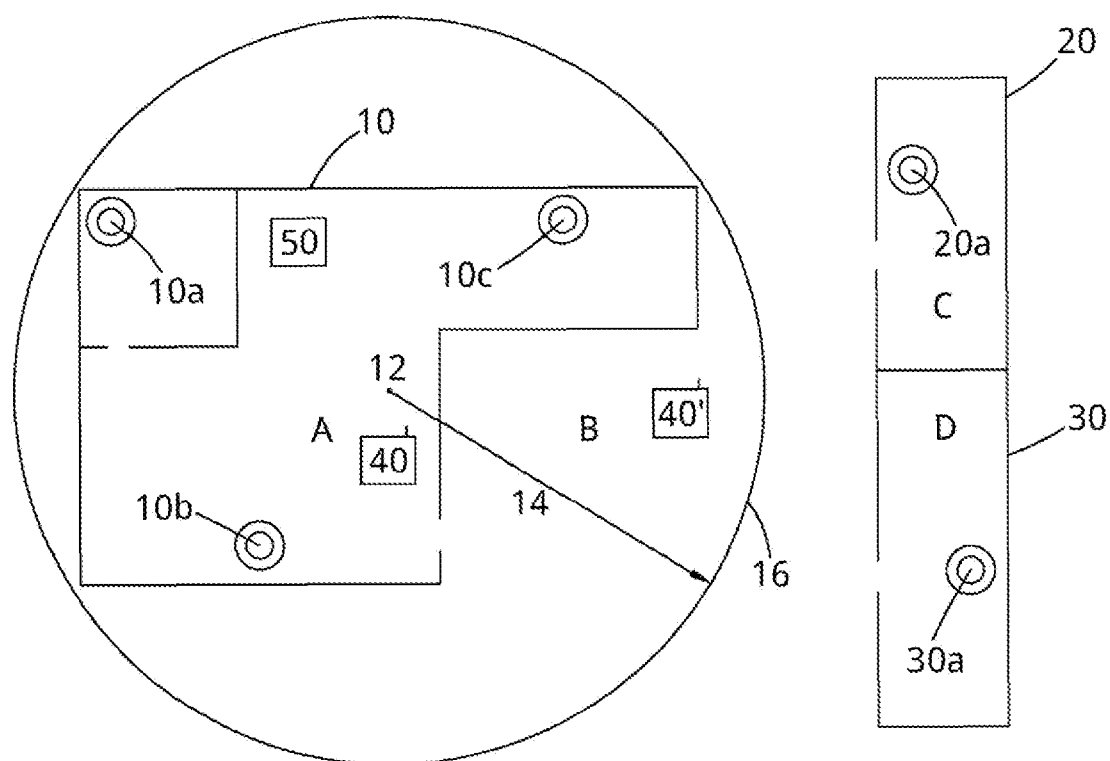


Figura 2

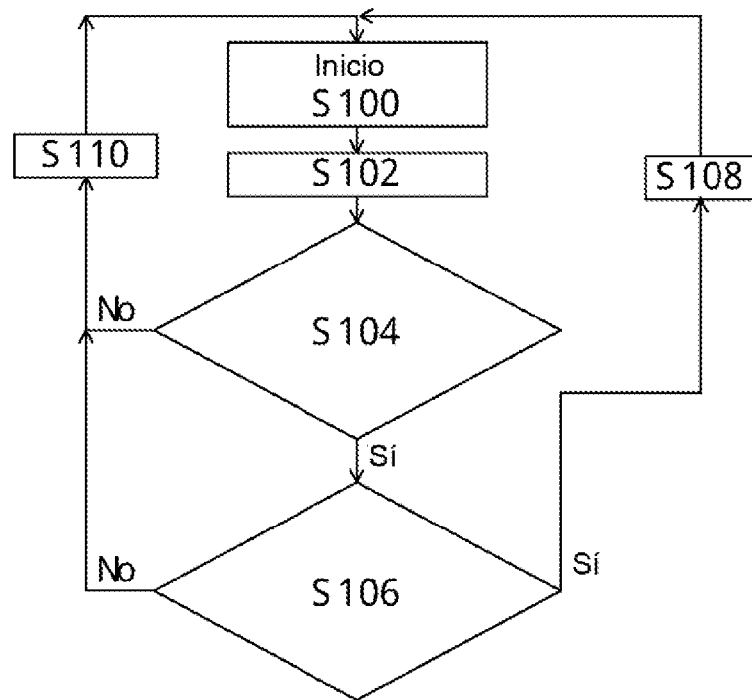


Figura 3

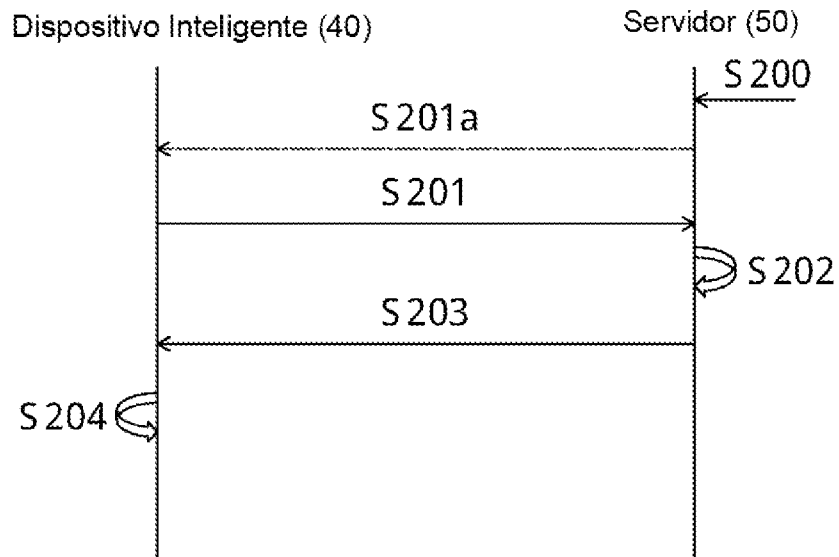


Figura 4

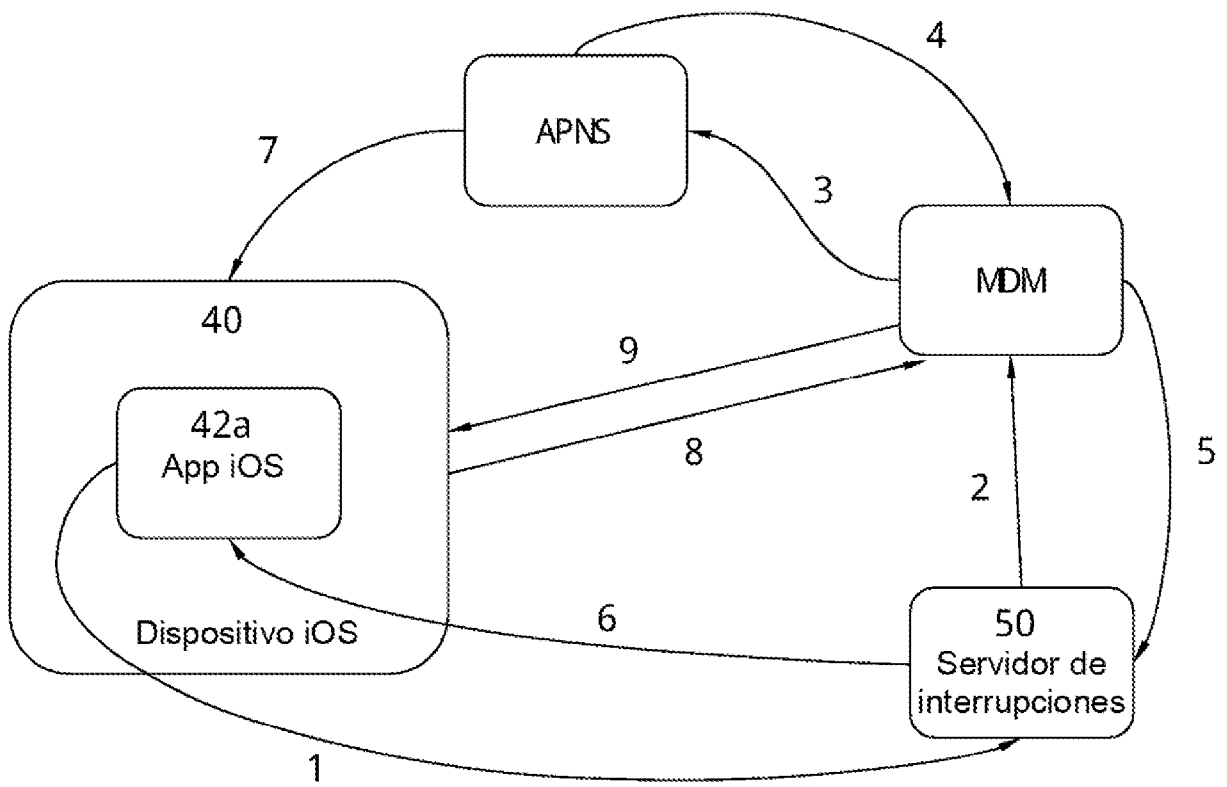


Figura 5

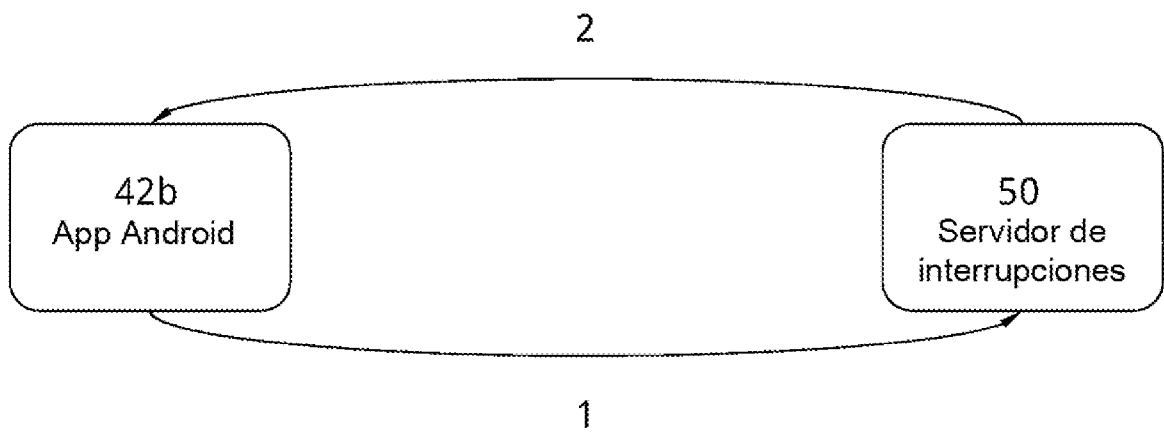


Figura 6

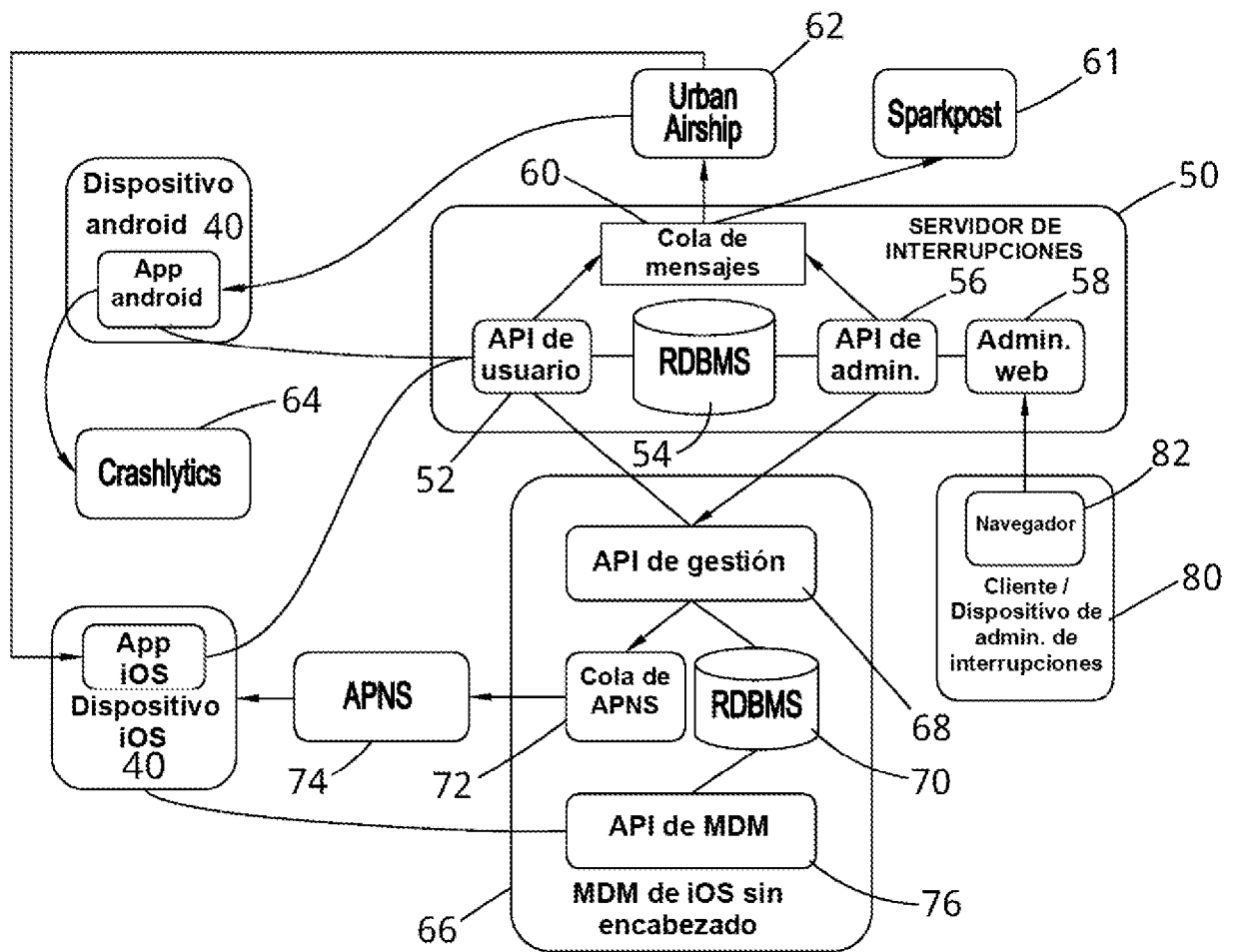


Figura 7

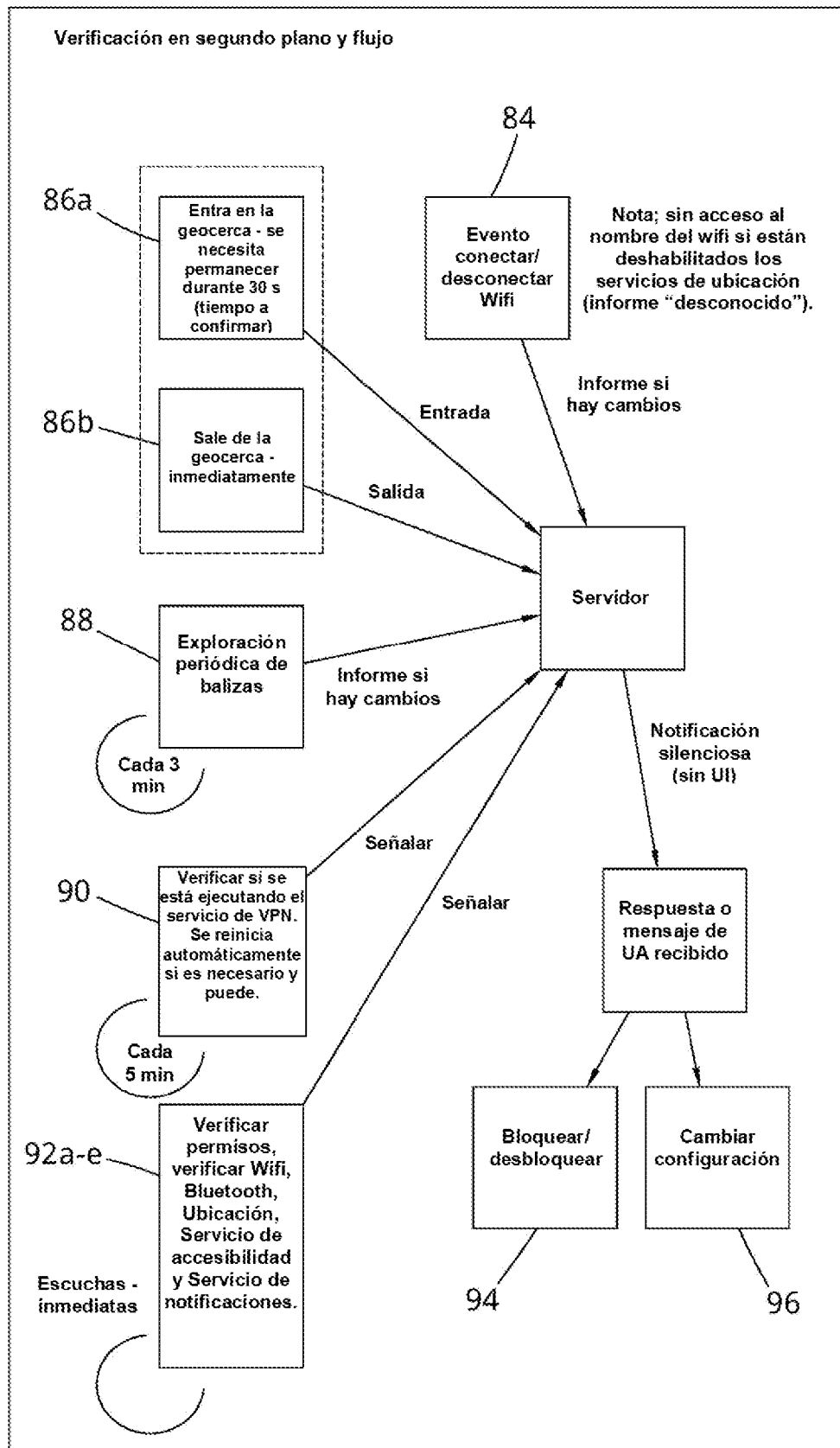


Figura 8

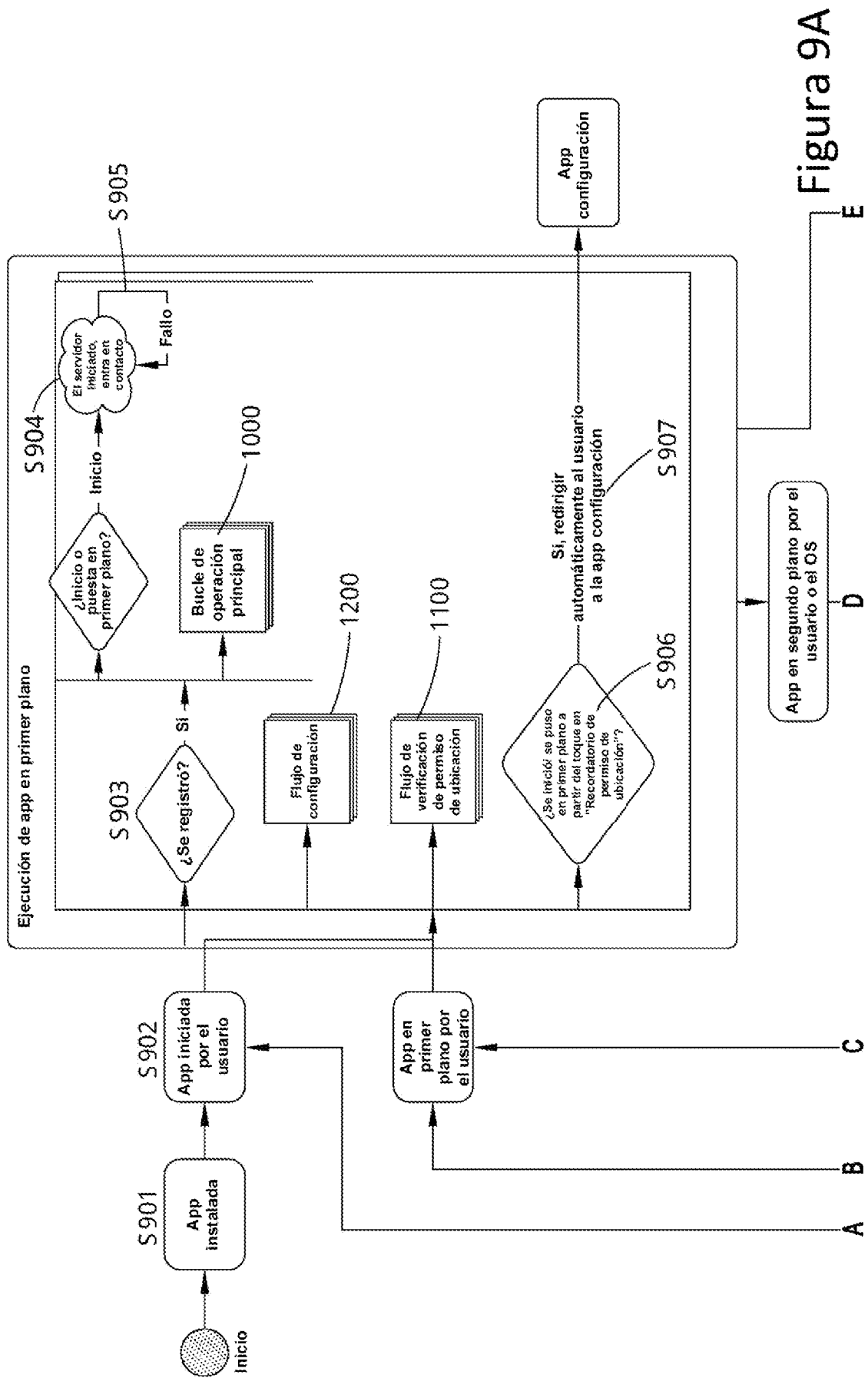


Figura 9A

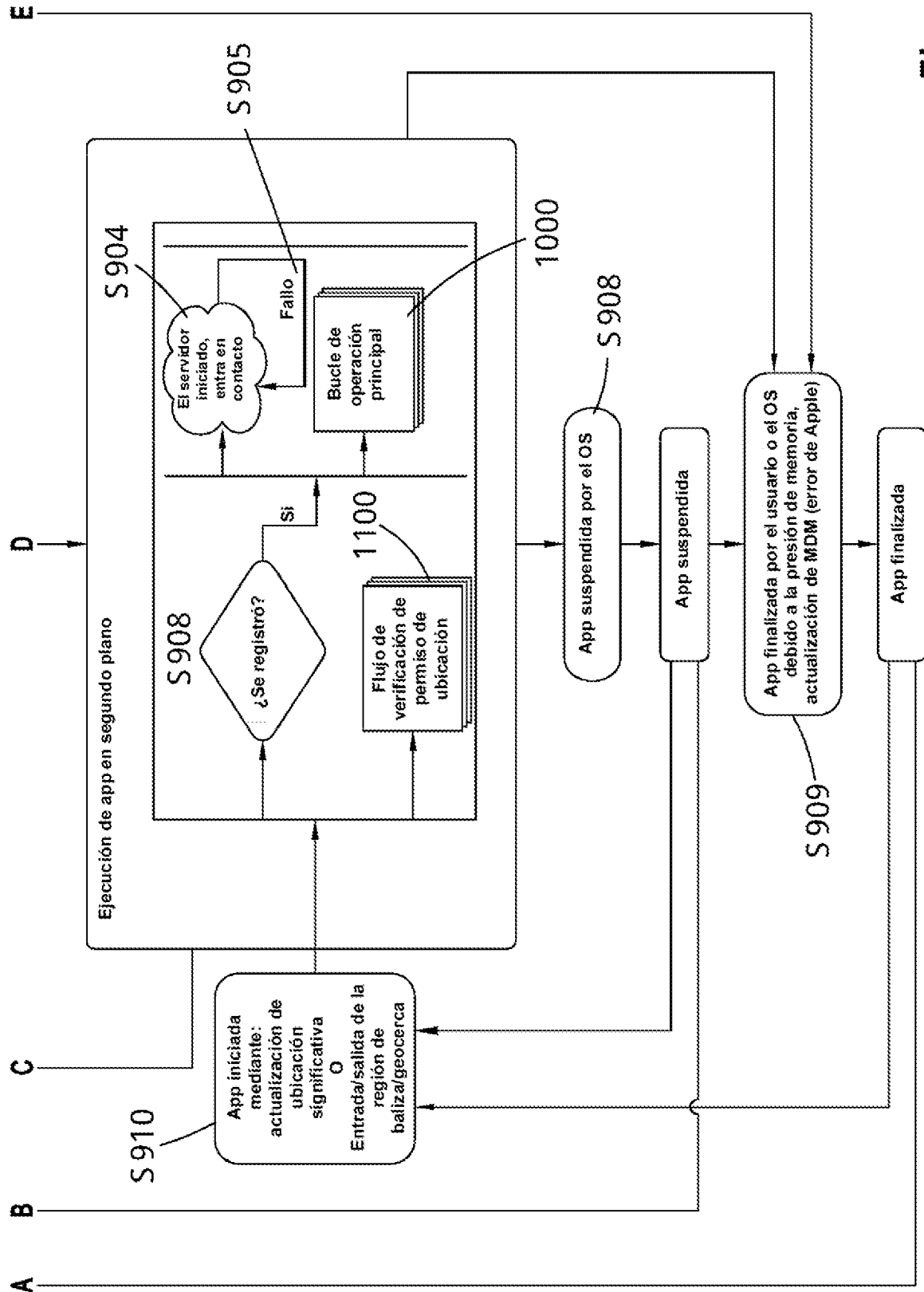


Figura 9B

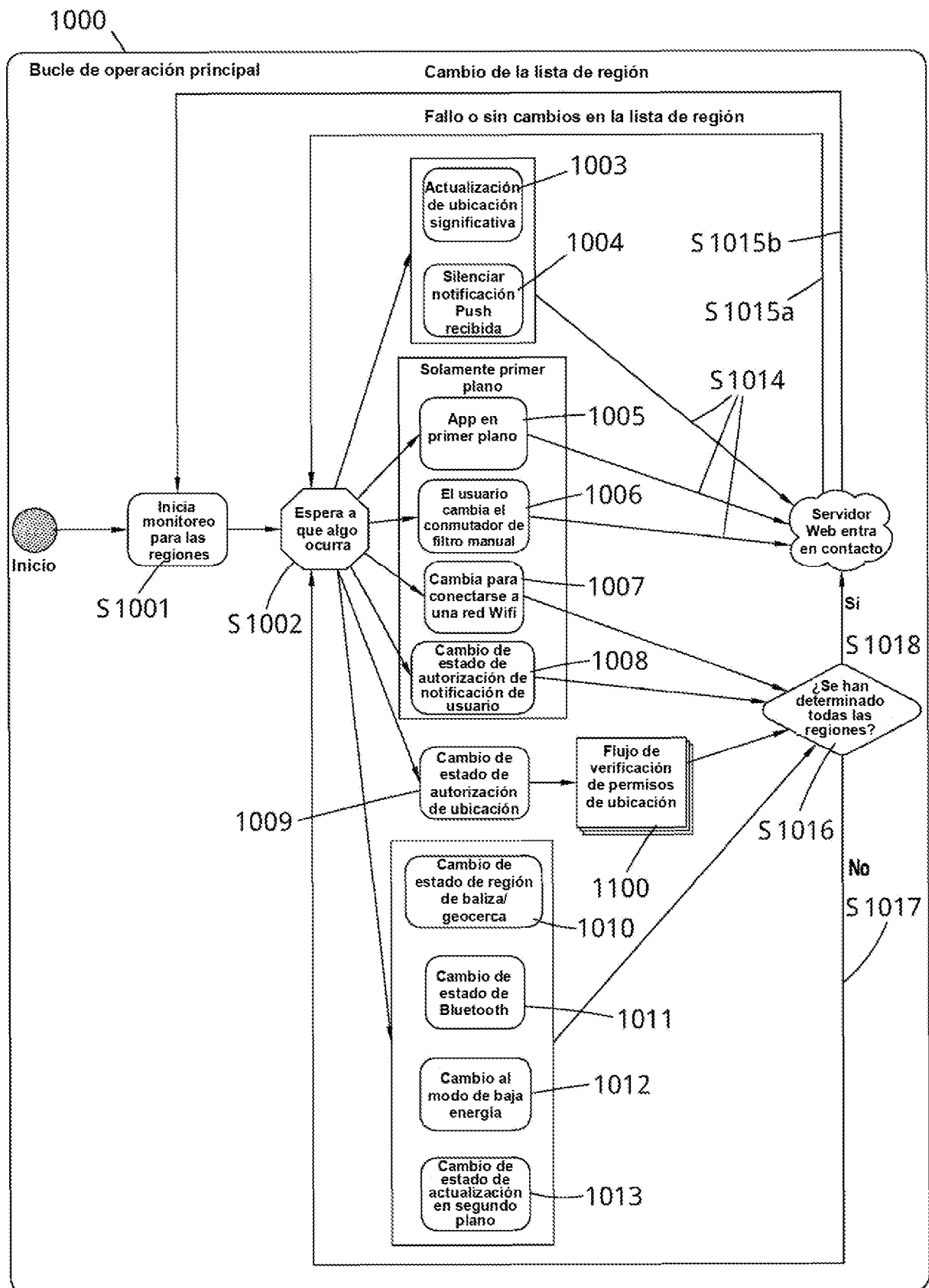


Figura 10

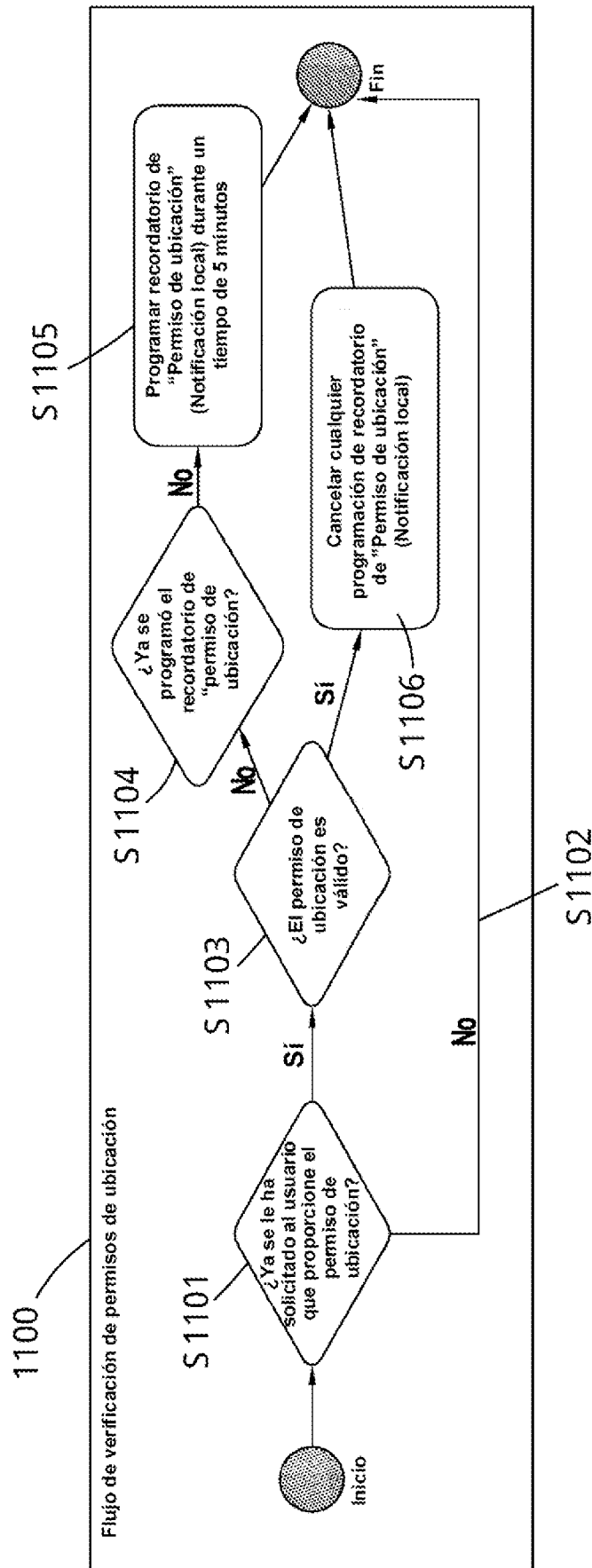
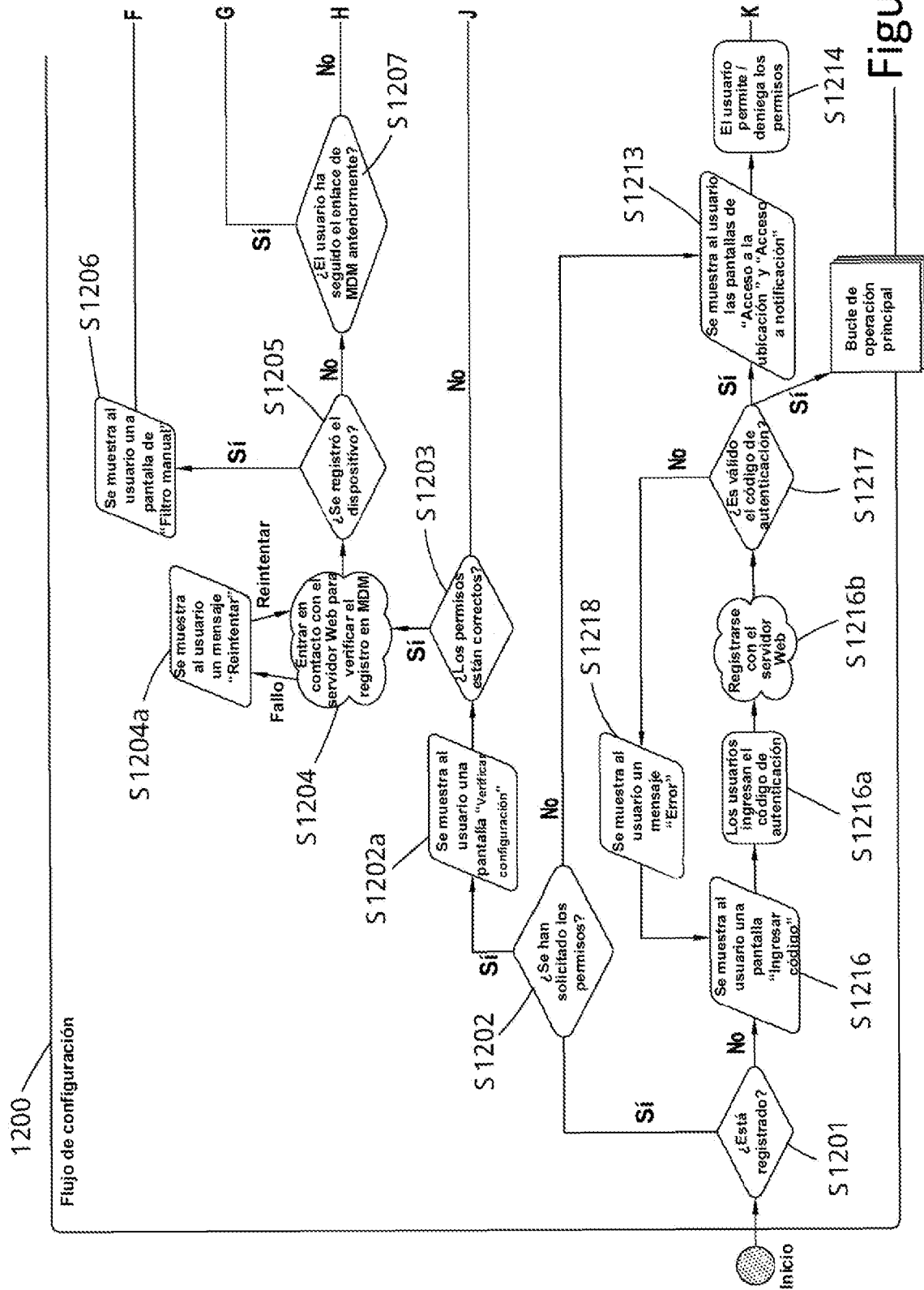


Figura 11



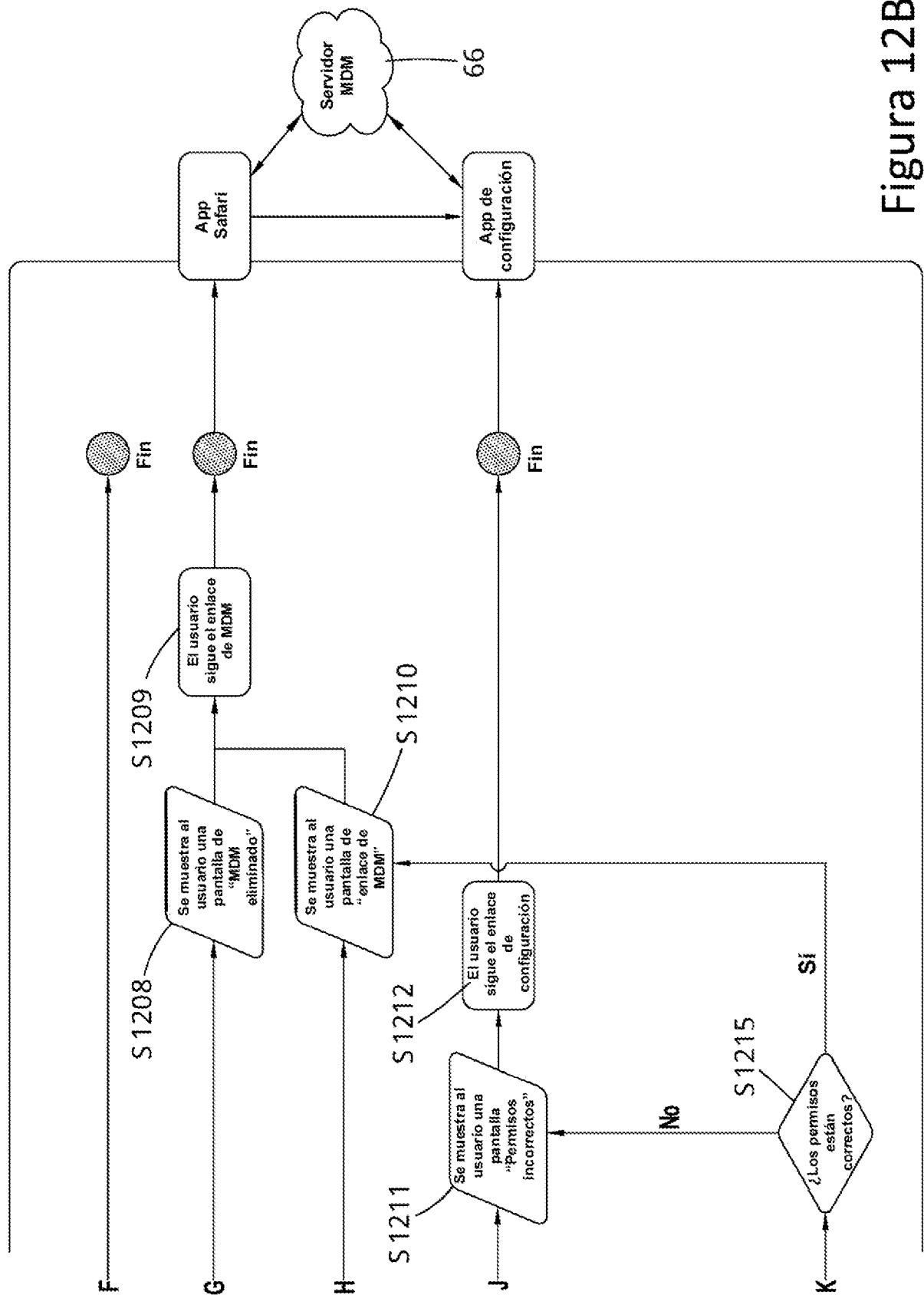


Figura 12B