(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 410 362**

(51) Int. CI.:

H04W 84/00 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **23.02.2005 E 05723626 (7)**

(97) Fecha y número de publicación de la concesión europea: **26.12.2012 EP 1726167**

(54) Título: **Sistema de copia de seguridad de datos de teléfono inalámbrico**

(30) Prioridad:

27.02.2004 US 789816

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
01.07.2013

(73) Titular/es:

FUSIONONE INC. (100.0%)
1 ALMADEN BOULEVARD, 11TH FLOOR
SAN JOSE, CA 95113, US

(72) Inventor/es:

ONYON, RICHARD y
STANNARD, LIAM

(74) Agente/Representante:

PÉREZ BARQUÍN, Eliana

DESCRIPCIÓN

Sistema de copia de seguridad de datos de teléfono inalámbrico

Antecedentes de la invención

Campo de la invención

La invención se refiere a la copia de seguridad y a la recuperación de datos almacenados en un teléfono inalámbrico, y en particular a un teléfono móvil que tiene capacidades de almacenamiento de datos.

Descripción de la técnica relacionada

Los dispositivos de comunicación inalámbrica, tal como los teléfonos móviles, se han expansionado más allá de lo que se considera meramente como mecanismos para comunicación. Muchos teléfonos incluyen características que habilitan la productividad personal, juegos, e incluso cámaras digitales. Los dispositivos que incluyen aplicaciones de productividad personal pueden incluir almacenamiento de datos para almacenar información personal del propietario dentro de los dispositivos de almacenamiento. Adicionalmente, los teléfonos tienen actualmente la capacidad de ejecutar programas de aplicación específicamente diseñados para entornos de tiempo de proceso basados en teléfono.

Toda la información personal de un individuo operada por, y almacenada por, un usuario, puede ser considerada dentro del "espacio de información personal" del usuario. En este contexto, un "espacio de información personal" es un almacén de datos de información personalizada por, y a favor de un usuario, que contiene tanto datos públicos que el usuario introduce en su espacio personal, como eventos privados del espacio, y otros objetos de datos tales como archivos de texto o archivos de datos que pertenecen al usuario y que son manejados por el usuario. El espacio de información personal está definido por el contenido que es específico de, y que está controlado por, un usuario, generalmente introducido por, o bajo el control del usuario individual, y que incluye eventos y datos "públicos", conocidos generalmente por otros, y eventos y datos "privados" que no se pretende que sean compartidos por los demás. Se debe reconocer que cada uno de los criterios mencionados con anterioridad no es exclusivo ni obligado, pero define características del término "espacio de información personal" según se utiliza dicho término en la presente memoria. En este contexto, dicha información incluye archivos electrónicos tales como bases de datos, archivos de texto, archivos de procesamiento de palabra, y otros archivos de aplicación específica, así como información de contacto en gestores de información personal, PDAs y teléfonos celulares.

Una dificultad a la que se enfrentan los usuarios consiste en que se puede consumir tiempo para introducir la información en un teléfono, y una vez introducida, la información puede ser objeto de pérdida. Si el teléfono se daña o simplemente lo pierde el usuario, el tiempo y el esfuerzo invertidos en introducir la información en el teléfono se pierden. Algunos teléfonos vienen con software y cables de conexión de datos que permiten que los usuarios introduzcan y hagan copias de seguridad de la información almacenada en un teléfono conectando físicamente el teléfono a un ordenador personal. Muchas de estas aplicaciones son proporcionadas por el fabricante del teléfono y están personalizadas para interactuar directamente con el teléfono. Es decir, el programa de aplicación está específicamente diseñado para que el teléfono recupere datos desde el teléfono y los almacene en una aplicación en un ordenador personal. Adicionalmente, algunos vendedores han intentado realizar sistemas de sincronización universal que interactúen con teléfonos a través del cable físico.

El problema de estos mecanismos de conexión física consiste en que el usuario debe recordar conscientemente conectar físicamente el teléfono al ordenador de una manera regular con el fin de asegurar que la información copiada en el ordenador sea precisa. Adicionalmente, el propio ordenador está sujeto a volatilidad. Los datos del ordenador pueden perderse o dañarse debido a fallos del hardware o del software.

Aunque los usuarios de teléfonos desean por lo general una funcionalidad incrementada de aplicaciones basadas en teléfono, también desean que las aplicaciones sean relativamente fáciles de usar. Incluso aplicaciones de utilidad basadas en un ordenador general, tales como aplicaciones de copia de seguridad de datos, son ventajosas si se disponen de modo que se ejecuten sin intervención significativa del usuario. Una aplicación que podría permitir a los usuarios de teléfonos inalámbricos hacer copias de seguridad de forma fácil y rápida de su información personal almacenada en el teléfono, podría ser de gran valor comercial y técnico.

El documento US 2003/134625 divulga un método de copia de seguridad de datos en una red, y un sistema que materializa dicho método, donde un teléfono móvil incluye una parte de memoria que almacena datos que van a ser copiados, así como programas configurados para transmitir y recuperar los datos copiados a través de circuitos inalámbricos. Una parte de control está configurada para procesar una petición de usuario para una operación de copia de seguridad de datos y transmitir o recibir los datos copiados. Una parte de circuito inalámbrico está configurada para convertir los datos copiados procesados por la parte de control en señales de radio y para transmitir las mismas, o para convertir las señales de radio recibidas en datos reconocibles por el teléfono móvil.

Sumario de la invención

La invención se define en las reivindicaciones.

Una realización proporciona un método implementado por un dispositivo de procesamiento en un teléfono inalámbrico para hacer copias de seguridad de la información personal almacenada en el teléfono inalámbrico. El método comprende: proporcionar, con la utilización de un agente de teléfono que incluya instrucciones operables por el dispositivo de procesamiento, un método de transmisión automatizada de datos de teléfono para transmitir cambios a un almacén de copia de seguridad, y un método de restauración para recuperar la información de seguridad desde el almacén de copia de seguridad para el inalámbrico; presentar en el teléfono inalámbrico, utilizando el agente de teléfono, una interfaz de contratación de cuenta de usuario de servicio de copia de seguridad para establecer una cuenta de usuario de servicio de copia de seguridad, una interfaz de programación de método de copia de seguridad para establecer el programa de copia de seguridad y una interfaz de recuperación para llamar al método de recuperación, incluyendo el teléfono inalámbrico un visualizador y uno o más botones pulsadores; y en respuesta a la activación del usuario, llamar mediante la interfaz de recuperación al método de recuperación para proporcionar cambios desde el almacén de copia de seguridad al teléfono inalámbrico.

Una realización de un agente de teléfono incluye instrucciones operables por un dispositivo de procesamiento de un teléfono inalámbrico para la copia de seguridad de información personal almacenada en el teléfono inalámbrico para llevar a cabo dicho método.

Una disposición de un método para almacenar información personal procedente de un teléfono inalámbrico en un almacén de copia de seguridad de una base de datos de almacenamiento de copia de seguridad, comprende: proporcionar a un teléfono inalámbrico, un agente de teléfono que incluya instrucciones operables mediante un procesador del teléfono inalámbrico. El agente de teléfono implementa un método de transmisión automática de datos del teléfono para transmitir cambios al almacén de copia de seguridad a través de un enlace de comunicaciones y un método de recuperación que restaura información de copia de seguridad desde el almacén de copia de seguridad para el teléfono inalámbrico, y presenta sobre el teléfono inalámbrico una interfaz de contratación de cuenta de usuario de servicio de copia de seguridad para establecer una cuenta de usuario de servicio de copia de seguridad, una interfaz de programación de método de copia de seguridad para establecer la programación de copia de seguridad y una interfaz de recuperación que llama al método de recuperación, incluyendo el teléfono inalámbrico un visualizador y uno o más botones pulsadores sobre el teléfono inalámbrico. En respuesta a la activación del usuario y a la interfaz de recuperación que llama al método, el método incluye proporcionar cambios desde el almacén de copia de seguridad al teléfono inalámbrico.

Una realización de un teléfono inalámbrico comprende un almacén de datos para almacenar información personal, un visualizador y uno o más botones pulsadores, comprendiendo además el teléfono inalámbrico: medios para creación de una cuenta de usuario automatizada, iniciada por un usuario a través de una interfaz de usuario en el teléfono inalámbrico, siendo los medios para creación operables para acceder a un sistema de copia de seguridad y para crear una cuenta de usuario en el sistema de copia de seguridad; medios para hacer automáticamente copias de seguridad y para transmitir cambios a través de un enlace de comunicaciones hasta el sistema de copia de seguridad a intervalos definidos por el usuario; y medios para recuperación llamados por el usuario a través de una interfaz de recuperación presentada sobre el teléfono inalámbrico, siendo los medios para recuperación operables para recuperar información de copia de seguridad desde el almacén de copia de seguridad hasta el teléfono inalámbrico.

Una realización proporciona un sistema para hacer copias de seguridad de datos en un teléfono inalámbrico que tiene un almacenamiento de datos que contiene información personal del usuario. La invención proporciona a un usuario un medio conveniente para asegurar que la información salvada en un teléfono inalámbrico, y el esfuerzo aplicado para asegurar que la informa ha sido introducida y es correcta, no se pierde en el propio teléfono si se pierde o se avería.

En una realización, el método puede incluir transmitir datos del teléfono al sistema de copia de seguridad a intervalos definidos por el usuario, o bien tras la recepción de una indicación desde un almacén de copia de seguridad de que han ocurrido cambios en los datos del almacén de datos. El indicador puede dar como resultado un barrido selectivo en el almacén de datos para determinar si han ocurrido cambios.

Una realización puede incluir el hecho de proporcionar una interfaz al almacén de datos a través de la web para alterar datos en el almacén de datos. Una realización puede incluir además proporcionar una interfaz de repetición y una interfaz de anti-borrado.

Una realización de una aplicación que forma el agente de teléfono, puede incluir un proceso repetitivo de información de teléfono que devuelva datos por la conexión inalámbrica a un estado existente en una fecha específica. La aplicación puede incluir además un proceso de registro anti-borrado. La aplicación puede incluir uno o más procesos que se ejecutan en un servidor, un agente BREW y/o un agente JAVA, o una aplicación diseñada para que opere en un dispositivo de propietario o un sistema operativo (por ejemplo, un sistema operativo Symbian).

Uno o más dispositivos de almacenamiento legibles con procesador pueden tener un código legible con procesador materializado en dichos dispositivos de almacenamiento legibles con procesador, siendo dicho código legible con procesador apto para programar uno o más procesadores para que lleven a cabo un método según se ha expuesto en lo que antecede.

Una realización puede proporcionar un sistema de copia de seguridad que use un identificador único de teléfono junto con información personal almacenada en relación con un usuario. El sistema de copia de seguridad puede asociar un identificador de teléfono único con un identificador de usuario único. El identificador de teléfono, el identificador de usuario o ambos pueden ser universalmente únicos. Un cliente SyncML existente, puede actuar por un teléfono como cliente de copia de seguridad y auto-crear la información de cuenta de usuario en el servidor.

Se pueden llevar a cabo realizaciones utilizando hardware, software, o una combinación de ambos hardware y software. El software usado para la presente invención puede estar almacenado en uno o más medios de almacenamiento legibles con procesador incluyendo las unidades de disco duro, CD-ROM, discos ópticos, discos flotantes, unidades de cinta, RAM, ROM u otros dispositivos de almacenamiento adecuados. En realizaciones alternativas, parte o todo el software puede ser sustituido por hardware dedicado incluyendo circuitos integrados según necesidades, matrices de puertas, FPGAs, PLDs, y ordenadores de propósito especial.

Estos y otros objetos y ventajas de la presente invención se pondrán más claramente de manifiesto a partir de la descripción que sigue en la que se expone la realización preferida de la invención junto con los dibujos.

Breve descripción de los dibujos

La invención va a ser descrita con respecto a varios ejemplos de realizaciones de la misma. Otras características y ventajas de la invención resultarán evidentes con referencia a la descripción y a los dibujos, en los que:

La figura 1 es un diagrama de bloques que ilustra el acoplamiento de un teléfono inalámbrico a un servidor de copia de seguridad utilizado conforme a la presente invención;

La figura 2 es un diagrama de flujo que ilustra cómo un usuario podría contratar y copiar inicialmente datos de copia de seguridad utilizando el sistema y la presente invención;

Las figuras 3a a 3q son imágenes de pantalla que ilustran cómo una interfaz de usuario podría permitir a un usuario contratar y copiar inicialmente datos en el sistema de la presente invención;

La figura 4 es un diagrama de flujo que ilustra un proceso de recuperación utilizado conforme a la presente invención;

Las figuras 5a a 5e ilustran una interfaz de usuario para conducir su proceso de recuperación conforme a la presente invención;

La figura 6 es un diagrama de flujo que ilustra una función de reversión utilizada conforme a la presente invención;

La figura 7 es un diagrama de flujo que ilustra la interacción del usuario con un gestor de información personal basado en web, para alterar los datos en el almacén de copia de seguridad y consiguientemente la información almacenada en el teléfono inalámbrico.

La figura 8 es una realización alternativa del proceso mostrado en la figura 7 que ilustra una interacción de usuario con un gestor de información personal en base a web, que modifica información de usuario almacenada en un teléfono inalámbrico;

La figura 9 es un diagrama de flujo que ilustra cómo pueden ocurrir dos estados diferentes de datos, y opciones para resolver esos estados;

La figura 10 ilustra un método para implementar un sistema de copia de seguridad usando un único identificador de teléfono asociado con datos de usuario;

La figura 11 ilustra un método para el uso de un cliente SyncML proporcionado por fabricante pre-aprovisionado en un teléfono, para comunicar con el servidor de copia de seguridad;

La figura 12 ilustra un método para la provisión de un cliente SyncML proporcionado por el fabricante en un teléfono, para comunicar con el servidor de copia de seguridad.

Descripción detallada

La presente invención permite a un usuario hacer copia de seguridad inalámbricamente de la información personal almacenada en un teléfono celular utilizando un enlace de comunicación, tal como una red inalámbrica, a la cual puede ser conectado el teléfono. La aplicación da como resultado un proceso que se ejecuta generalmente en el fondo de la aplicación telefónica del usuario, y por lo tanto no inhibe el uso del teléfono del usuario.

La figura 1 ilustra una visión general de un sistema para implementar la presente invención. Según se muestra en la figura 1, un dispositivo de comunicación inalámbrica, tal como un teléfono 100, está conectado a un enlace de comunicaciones inalámbricas, tal como una red celular 150, para transmitir comunicaciones de voz y de datos a otros dispositivos que se acoplan a la red inalámbrica. Los datos pueden ser transmitidos por red en un número cualquiera de formatos conocidos. Se ha previsto también un servidor 160 que comunica a través de un enlace 185 inalámbrico con el teléfono a través de la red 150 inalámbrica. Alternativamente, el servidor 160 puede comunicar con el teléfono 100 a través de un servidor 195 de SyncML. El sistema de copia de seguridad incluye el agente 110, el almacén 150 de copia de seguridad en el servidor 160, y métodos implementados por el agente y el servidor para llevar a cabo funciones de copia de seguridad, recuperación e integridad de datos de la invención. Otros componentes discutidos en la presente memoria pueden ser incorporados también en el sistema en diversas realizaciones.

El teléfono 100 está dotado de una aplicación de copia de seguridad o agente 110. El agente 110 de copia de seguridad puede ser un cliente de comunicación SyncML designado para que interactúe con un servidor 195 de SyncML de acuerdo con versiones propuestas y aprobadas de la especificación SyncML OMA DS, incluyendo las extensiones propuestas (disponibles en http://www.openmobilealliance.org). Alternativamente, el agente 110 puede ser una aplicación diseñada para que comunique con el servidor 160 utilizando un cliente SyncML existente en el teléfono proporcionado por el fabricante de teléfonos (así como cualquier extensión que se necesite soportada por tal cliente), o una aplicación diseñada específicamente para comunicar con el servidor 160 a través de otro protocolo, incluyendo un protocolo de propietario. En una realización, el agente 110 es un cliente SyncML totalmente implementado y el servidor 160 incluye un servidor SyncML. En otra realización, la aplicación 110 es un agente sincronizado de dispositivo de aplicación de cliente tal como el que se divulga en la patente de Estados Unidos número 6.671.757. En otra realización más, la aplicación 110 es una aplicación de cliente que responde a efectos de control por medio de un navegador del teléfono, en el que la aplicación comprueba cambios en los datos del teléfono e implementa los procesos descritos en la presente memoria.

En general, una estructura de hardware adecuada para implementar el servidor 160, el servidor web 180 o el servidor 195 de SyncML, incluye un procesador 114, una memoria 104, un dispositivo 106 de almacenamiento no volátil, un dispositivo 110 de almacenamiento portátil, una interfaz de red 112 y dispositivo(s) 116 de E/S. La elección de procesador no es crítica en tanto que se elija un procesador adecuado con velocidad suficiente. La memoria 104 podría ser cualquier memoria de ordenador convencional conocida en el estado de la técnica. El dispositivo 106 de almacenamiento no volátil podría incluir una unidad de disco duro, CDROM, CDRW, tarjeta de memoria flash, o cualquier otro dispositivo de almacenamiento no volátil. El almacenamiento 108 portátil podría incluir una unidad de disco flotante o cualquier otro dispositivo de almacenamiento portátil. El sistema de ordenador puede incluir una o más interfaces de red 112. Un ejemplo de interfaz de red incluye una red conectada a una Ethernet o a otro tipo de LAN. El (los) dispositivo(s) 114 de E/S puede(n) incluir uno o más de entre los siguientes: teclado, ratón, monitor, pantalla de visualización, impresora, módem, etc. El software utilizado para llevar a cabo los métodos de la presente invención debe estar igualmente almacenado en un almacén 106 no volátil, en medios 110 de almacenamiento portátiles y/o en una memoria 104. El sistema de ordenador incluye también una base de datos 108, la cual puede estar almacenada en un almacén 106 no volátil. En realizaciones alternativas, la base de datos 108 está almacenada en la memoria 104, en el almacén 110 portátil o en otro dispositivo de almacenamiento que sea parte del sistema de la figura 1 o que esté en comunicación con el sistema de la figura 1. Se pueden usar también otras arquitecturas alternativas que sean diferentes de la representada en la figura 1. Diversas realizaciones, versiones y modificaciones de sistemas de la figura 1 pueden ser usadas para implementar un dispositivo de ordenador que ejecute la totalidad, o una parte, de la presente invención. Ejemplos de dispositivos de ordenador adecuados incluyen un ordenador personal, una estación de trabajo por ordenador, un ordenador portátil, un asistente digital personal, un localizador, un teléfono celular, un aparato inteligente o múltiples ordenadores, una red de área de almacenamiento, un conjunto de servidores, o cualquier otro dispositivo de computación adecuado. Puede existir un número cualquiera de servidores 160n, n+1, gestionados por un administrador de sistema que proporcione un servicio de copia de seguridad de acuerdo con la presente invención.

También se proporciona en el servidor 160 un almacén 150 de datos de copia de seguridad. El almacén de datos de copia de seguridad ha sido proporcionado en el espacio de memoria no volátil del servidor 160. Aunque solamente se ha mostrado un ordenador de almacenamiento de datos de copia de seguridad, se debe entender que el almacenamiento puede estar replicado en, o almacenado con, una pluralidad de ordenadores (160n, 160n+1) para asegurar que los datos presentes en los mismos están protegidos frente a pérdidas accidentales. Se debe entender que la representación del servidor 195 de SyncML y del servidor 180 de web no necesita que tales servidores sean proporcionados en un hardware físico diferente del servidor 160 de copia de seguridad.

De acuerdo con la invención el agente 110 de aplicación comunica información personal y cambios realizados en la información personal almacenada en el almacén de datos del teléfono 100 al servidor 160 a través de la red

inalámbrica. La comunicación de datos de usuario desde el dispositivo puede adoptar varias formas. Cuando el cliente es un cliente SyncML en comunicación con el servidor 160, la comunicación puede llevarse a cabo utilizando los estándares establecidos en la especificación SyncML. Los cambios son transmitidos en base a un registro-por-registro o de campo-por-campo. Alternativamente, la comunicación puede ocurrir a través de otro protocolo. En una realización alternativa, el agente 110 es una aplicación de auto-soporte diseñada para ser ejecutada como un agente JAVA o BREW, o cualquier otro dispositivo o agente específico de sistema operativo (tal como un agente operable en el sistema Operativo Symbian). Este agente puede incluir su propio cliente SyncML o bien interactuar con un cliente SyncML existente en el teléfono. Los cambios pueden ocurrir a nivel de campo o a nivel de byte. Realizaciones alternativas pueden comunicar por medio de protocolos alternativos a través del enlace de comunicaciones inalámbricas para almacenar información en la base de datos 510 de copia de seguridad.

El servidor 160 almacena datos de usuario en el almacén de copia de seguridad de una manera que asocia los datos con el usuario del teléfono. En una realización, los datos se almacenan en masa, es decir todos los registros y la información para el usuario se almacenan en forma de texto simple, o una copia de la base de datos completa del teléfono se almacena en el servidor. En esta realización, el servidor puede almacenar un número cualquiera de copias de los datos sobre una base de identificación por fechas. Alternativamente, el servidor 160 traduce esta información en registros de cambio, en una realización, conforme a las enseñanzas de la patente de Estados Unidos número 6.671.757. Esta información se almacena en el almacén de datos 510 de copia de seguridad del servidor 160. Esta información es almacenada en el almacén de datos utilizando un identificador único (UID) que asocia los datos con el usuario individual. El identificador puede ser un identificador cualquiera seleccionado aleatoriamente, siempre que el usuario sea identificado unívocamente, y los datos estén asociados con el usuario. Según un aspecto adicional, este UID de usuario puede ser un identificador universalmente único (UUID) creado de la manera que se describe en la patente 6.671.757 mencionada anteriormente o de otras maneras que permitan crear un sólo ID para un usuario dado.

El almacén de datos 150 puede consistir en cualquier forma de almacenamiento de datos para los datos de usuario. En una realización, el almacén de datos es una copia simple de la información almacenada en el dispositivo 100. En otra realización, el almacén de datos es una base de datos, tal como una base de datos de objeto o una base de datos de relación. En otra realización más, el almacén de datos es simplemente un contenedor de almacenamiento para registros de cambio creado conforme a la patente de Estados Unidos número 6.671.757.

Un servidor 180 web que permita a un usuario tener en un ordenador y otro dispositivo 190 un navegador web, puede estar dispuesto de manera que permita a un usuario configurar aspectos del sistema de la invención. El servidor 180 puede tener una configuración de hardware similar al ordenador 160 y puede comprender uno o más ordenadores físicos. Adicionalmente, el servidor 180 web puede estar integrado con el servidor 160.

En general, una primera realización del sistema descrito en lo que sigue presenta un sistema en el que ciertos aspectos del sistema de copia de seguridad de la presente invención son configurados a través de una interfaz de teléfono. En cada caso en que se utilice una interfaz de teléfono, el sistema puede ser configurado alternativamente por un usuario a través de una interfaz de web proporcionada por el servidor 180 de web por medio del dispositivo 190 de usuario.

La figura 2 ilustra cómo un usuario que interactúa con el sistema de la presente invención por primera vez, podría instalar la aplicación y contratar el servicio de copia de seguridad proporcionado por un administrador de sistema utilizando el servidor 160 de copia de seguridad y el teléfono 100 del usuario. En la realización de la figura 2, un usuario contrata un servicio de copia de seguridad proporcionado por un administrador de sistema utilizando el teléfono de usuario y la aplicación 100. Un proceso de contratación alternativa puede ser implementado teniendo el usuario que iniciar el servicio yendo a un sitio de World Wide Web administrado por el administrador de sistema y que interactúa con, o que es proporcionado por, el servidor 160 de sistema. Otro método más de contratación podría consistir en permitir al usuario contratar a través de un sitio de Protocolo de Aplicación Inalámbrica formateado de manera especial, al que se puede acceder mediante un navegador WAP con el teléfono 100. (Otra versión, que se discute más adelante en relación con las figuras 10-12, incluye la creación automática de una cuenta de usuario usando un identificador de teléfono único).

El administrador de sistema controla y mantiene el servidor 160, y proporciona el agente 110 para el teléfono. Alternativamente, el agente puede ser proporcionado por un fabricante de teléfonos y estar diseñado para comunicar con el servidor 160 (directamente o a través del servidor 195 syncML). El agente puede ser cargado previamente en el teléfono, con anterioridad a la distribución por el fabricante o portador de servicio inalámbrico, o proporcionado para su descarga por el administrador a través de la red inalámbrica. En la última realización, un usuario descarga inicialmente la aplicación desde un administrador de sistema a través del enlace 185 de comunicación. En general, las portadoras inalámbricas proporcionan ahora muchas formas de aplicaciones descargables para teléfonos inteligentes que tienen la capacidad de ejecutar las aplicaciones en BREW o en JAVA. BREW (Entorno de Rutina Binaria para Comunicación Inalámbrica) es una plataforma de desarrollo de aplicación de recurso abierto para dispositivos inalámbricos equipados con tecnología de acceso múltiple por división de código (CDMA). De igual modo, JAVA o J2ME (Micro Edición de Java 2) son plataformas similares de Sun Mycrosystems.

Una vez que la aplicación está instalada, en la etapa 202 de la figura 2, el usuario contacta con el sitio 160 de copia de seguridad utilizando el teléfono 100 y la aplicación 110. La manera en que esto podría ser presentado al usuario ha sido ilustrada en las figuras 3a y 3b. En la figura 3a se muestra una pantalla de bienvenida que invita al usuario a seleccionar el botón 2 del teléfono 300 inalámbrico para moverse hasta la "siguiente" pantalla mostrada en la figura 3b.

Como podrá comprender un experto medio en la materia, un teléfono 300 celular mostrado en las figuras 3a a 3q incluye botones "blandos" 302 y 304. Los objetos del menú que aparecen en la porción inferior de la pantalla indicados mediante los números de referencia 306 y 308, son los comandos que cambian en relación a la visualización y están controlados por la aplicación 110 (y de otros tipos) que se ejecuta en el teléfono 300 celular. En la figura 3a, se ha mostrado un botón de "siguiente" y un botón de "cancelar". Los botones 302 y 304 controlan las funciones "siguiente" y "cancelar", respectivamente.

Una vez que el usuario está de acuerdo en conectar con el sitio, según se muestra en la figura 3b, se presenta al usuario una pantalla que ilustra en teléfono conectando con la red inalámbrica. Se presenta el número móvil del usuario según se muestra con el número de referencia 312.

Volviendo a la figura 2, en la etapa 204, el usuario puede ser invitado a dar su conformidad a una licencia de software y a la licencia para el uso del servicio. Esto ha sido ilustrado en la figura 3c. Si el usuario no da su conformidad en la etapa 206, el proceso termina. Si el usuario está da su conformidad, entonces en la etapa 208, el teléfono descarga el número de usuario como un ID. En la etapa 210, el usuario selecciona y confirma un PIN. Esto ha sido ilustrado en las figuras 3d a 3f. En la figura 3d, el usuario introduce un Pin de registro en el teléfono y selecciona el siguiente comando presionando el botón blando 302. En la figura 3e, el teléfono muestra el PIN de entrada e invita al usuario a salvar el código pin. El usuario se mueve hasta la siguiente pantalla presionando el botón blando 302. Esta pantalla ha sido mostrada en la figura 3f, invitando al usuario a que seleccione una opción para que el servicio devuelva el PIN al teléfono por si el usuario olvida el PIN.

Volviendo a la figura 2, a continuación de haber completado la etapa 210 en la figura 2, el usuario es invitado a establecer un programa de copia de seguridad en la etapa 212. Este proceso de establecimiento, es como se muestra en las figuras 3g a 3j. En la figura 3g, el usuario es invitado a establecer el programa presionando el botón blando 302. En la figura 3h, se presentan cuatro opciones para que el usuario seleccione un programa regularmente recurrente. Estas opciones son "cada día", "días de semana", "semanalmente" o "sin programación". Cuando el usuario selecciona el siguiente botón en la figura 3h, la pantalla de copia de seguridad diaria ha sido mostrada en la figura 3i. La copia de seguridad diaria permite al usuario establecer una hora específica para las copias de seguridad programadas con regularidad. Si el usuario elige una programación por días de semana, esta hora puede suceder también en el mismo intervalo cada día. Las programaciones semanales (selección 3 de la figura 3) funcionan de una manera similar. La opción de copia de seguridad "sin programar" permite al usuario hacer manualmente la copia de seguridad de la información en el teléfono iniciando manualmente la aplicación y enviando los cambios al almacén de copia de seguridad según se ha ilustrado en la etapa 222 de la figura 2. En otra realización más, la programación puede estar destinada a proporcionar datos de copia de seguridad al servidor cada vez que el usuario cambia información en el teléfono.

Según otra realización más, la programación está al menos parcialmente controlada por el servidor 160. En esta realización, cuando el usuario intenta establecer una hora de programación, el servidor 160 comprueba un registro mantenido por separado de las programaciones de transmisión de copia de seguridad de otros usuarios, para asegurar que se produce un equilibrio de carga de las transmisiones de varios usuarios en el servidor. Si, por ejemplo, un usuario desea enviar datos de copia de seguridad cada día a las 8 de la mañana, y un número de usuarios lo desean a la misma hora, el sistema puede instruir a la aplicación 110 para que altere si programa de manera que el programa no tenga impacto significativo para el usuario. Este cambio puede asegurar que el servidor 160 tiene suficiente ancho de banda de comunicaciones y potencia de procesamiento para gestionar peticiones coincidentes que pueden ocurrir a, o aproximadamente a, la misma hora de programación que la hora elegida por el usuario.

En otra realización, la programación de copia de seguridad está controlada totalmente por el servidor. En este aspecto, no se proporciona al usuario una selección de intervalo, y el servidor puede programar copias de seguridad por intervalo (en momentos regulares, irregulares o arbitrarios). En otra realización más, los datos de copia de seguridad son transmitidos en algún momento después de cada cambio en el almacén de datos del teléfono.

Volviendo de nuevo a la figura 2, una vez que se ha establecido la copia de seguridad programada en el etapa 212 de la figura 2, la información de copia de seguridad inicial debe ser almacenada en el servidor 160. Esto ocurre en la etapa 214 y se ha ilustrado en las figuras 3j a 3m. En la figura 3j, una vez que el establecimiento se ha completado, el usuario es invitado a presionar el "siguiente" botón blando 302 para iniciar el proceso de copia de seguridad inicial. Tras presionar el "siguiente" botón blando 302 según se muestra en la figura 3k, el teléfono conecta con el servidor 160 de copia de seguridad, y en la figura 3l se transmite la información al servidor de copia de seguridad. El campo de objetos 320 mostrado en la pantalla de la figura 3l mantiene un conteo total de los objetos que están siendo enviados al servidor 160 de copia de seguridad. Cuando la copia de seguridad está completa, la figura 3m muestra

la pantalla de estado presentada por el teléfono a la terminación del proceso de copia de seguridad.

En este punto, en la porción inferior de la pantalla, los botones blandos 302 y 304 presentan al usuario una opción "copia de seguridad ahora", que permite al usuario enviar información manualmente al teléfono según se ha indicado en la etapa 222 de la figura 2, y un botón de "opciones". El botón de "opciones" permite al usuario seleccionar diversas funciones administrativas según el proceso de copia de seguridad. Por ejemplo, las opciones podrían permitir al usuario cambiar la programación del proceso de copia de seguridad, debido a que la cuenta de número móvil del usuario que está identificada en el sistema 160 de copia de seguridad cambie el PIN de usuario, el acceso a la función de ayuda, o el acceso a información acerca del agente 110.

Volviendo a la figura 2, una vez que la pantalla de estado ha sido mostrada en las figuras 216, el usuario puede seguir usando este teléfono de la manera que el usuario está normalmente acostumbrado a hacerlo. En un instante de tiempo posterior, según se ha indicado mediante el intervalo de líneas de puntos entre las etapas 216 y 218, se alcanzará el intervalo de copia de seguridad establecido por el programa del usuario. En este punto, los cambios y adiciones y borrados serán enviados al almacén de copia de seguridad. Esto ha sido ilustrado en las figuras 3h a 3q. En la figura 3n, la aplicación puede presentar una pantalla de estado al usuario, en la figura 3o mostrar que está en conexión con el servidor 160 de copia de seguridad, en la figura 3p mostrar los objetos que están siendo copiados, y en la figura 3q mostrar el estado de la copia de seguridad como completado. Se debe entender que el intervalo 218 puede comprender, de hecho, un evento iniciado manualmente según se muestra en la etapa 222.

Se debe entender, además, que las etapas 218 y 220 pueden ocurrir en el fondo, y que no se proporcione ninguna información al usuario. Es decir, una vez que se ha alcanzado el intervalo de copia de seguridad, el teléfono puede descargar simplemente adiciones, borrados o cambios para el usuario y mantener un registro de cuándo se realizó su última copia de seguridad con el fin de que el usuario los pueda comprobar para asegurar que el proceso de copia de seguridad se está realizando sobre una base de regularidad. El tema de la interacción entre la aplicación y el usuario (por ejemplo, cuánta información proporciona la aplicación al usuario acerca de sus actividades), puede ser seleccionado por el usuario. En una realización alternativa, se puede proporcionar un indicador tal como un mensaje de información de "aparición repentina" a la terminación de la copia de seguridad. Los usuarios pueden seleccionar si, y con qué frecuencia, deben recibir mensajes de información.

La figura 4 muestra una visión general de un diagrama de flujo del proceso de recuperación utilizado de acuerdo con la presente invención. Las figuras 5a a 5e ilustran las etapas que un usuario podría ver en una interfaz de usuario durante el proceso de recuperación. En la etapa 402, el usuario activa la aplicación. Esto puede ocurrir, por ejemplo, cuando un usuario obtiene un nuevo teléfono o la memoria del teléfono normal del usuario ha sido borrada por alguna razón desconocida. Una vez que el usuario activa la aplicación, se presenta una pantalla de estado como la mostrada en la figura 5a.

Volviendo a la figura 4, en la etapa 404, el agente del dispositivo transmite el identificador único del usuario al servidor. En la etapa 406, el identificador ha sido indicado como que es el número de teléfono del usuario y éste identifica al usuario respecto al sistema de copia de seguridad. Alternativamente, el método puede incitar al usuario para que indique si el usuario ha establecido previamente una cuenta con el administrador del sistema y solicita el identificador y el PIN originales del usuario. Puesto que éste es un uso inicial de la aplicación en un teléfono que no contiene ningún dato de usuario, en una realización, el servidor puede reconocer que no hay datos presentes en el teléfono e invitar al usuario a realizar una recuperación, y la aplicación reconocerá rápidamente al usuario como un titular de cuenta en la etapa 406. La aplicación invitará a continuación a introducir un PIN en una etapa 420. Esto ha sido ilustrado en la figura 5c.

Una vez que el usuario introduce el PIN en la etapa 408, los datos serán restaurados en el dispositivo en la etapa 410. Esto ha sido ilustrado en la figura 5d, la cual indica al usuario que la aplicación está "recuperando" la información en el teléfono. La figura 5e muestra una pantalla de estado que presenta al usuario el hecho de que la información ha sido, de hecho, devuelta al teléfono del usuario.

Realizaciones alternativas del proceso de recuperación pueden ser también usadas. En una alternativa, el proceso de recuperación puede incluir proporcionar información a un teléfono que había tenido información introducida en el mismo más recientemente que el estado del almacén de copia de seguridad de los datos del usuario. Supóngase, por ejemplo que un usuario puede tener una cuenta creada con información en el almacén de copia de seguridad que crea un estado de copia de seguridad, por ejemplo "estado 1", en un momento dado. Si el usuario necesita realizar una restauración, tal como en caso de que el usuario pierda un teléfono y compre uno nuevo, el proceso de restauración podría simplemente proporcionar información de estado 1 al dispositivo. Si, no obstante, el usuario introduce manualmente información en el dispositivo, puede crear con ello una discordancia entre la información del estado 1 del almacén de copia de seguridad y los datos de teléfono introducidos más recientemente.

En este caso de discordancia, según una alternativa, la información de estado 1 puede ser proporcionar al teléfono mientras se ignora cualquier información nueva introducida por el usuario en el teléfono (haciendo con ello que la copia de seguridad se almacene en el contenedor de información principal y que ignore los cambios realizados en el teléfono). Según una segunda alternativa, el agente puede reconocer que el teléfono no es equivalente al teléfono

usado por el usuario para crear la información de estado 1 (utilizando, por ejemplo, un identificador único para el teléfono, tal como lo que se discute más adelante, o algún otro medio de identificación del nuevo estado de teléfono, tal como una selección de usuario). Una vez que el estado del teléfono ha sido establecido, la información personal del usuario almacenada en el teléfono es enviada al almacén de copia de seguridad, ejecutándose un proceso en el servidor que puede resolver discrepancias o duplicados, y escribiendo a continuación el nuevo estado de los datos del usuario en el teléfono. En otra alternativa, la información de ambos, dispositivo y almacén de copia de seguridad, puede ser fusionada. En esta última alternativa, existe la posibilidad de entradas duplicadas, y se puede proporcionar un mecanismo para tratar tales entradas duplicadas (tal como identificándolas para el usuario y requiriendo el duplicado que se debe mantener). La selección entre tales opciones debe ser proporcionada al usuario durante el proceso de establecimiento o bajo el menú de opciones de la aplicación o durante la recuperación, o en la web.

Adicionalmente, el sistema puede proporcionar opciones adicionales que permitan al usuario revertir los datos personales en una fecha y una hora particulares. Esta funcionalidad puede ser implementada según un número de maneras, pero es particularmente adecuada de usar en el sistema de la presente invención como implementada usando la tecnología de copia de seguridad divulgada en la solicitud de patente de Estados Unidos número 09/641.028, la solicitud de patente de Estados Unidos número 09/642.615 y la patente de Estados Unidos número 6.671.757. Las numerosas ventajas de la tecnología de copia de seguridad de datos que se describe en la patente de Estados Unidos número 6.671.757 han sido discutidas en la memoria de la misma. Sin embargo, se debe reconocer que usando tal tecnología, se pueden volver a crear datos de usuario en una fecha particular. Utilizando tal tecnología, el sistema empieza con un primer registro de cambio o paquete de datos identificado por un usuario, y posteriormente realiza las acciones definidas en el mismo sobre los datos almacenados en el mismo, buscando el cambio o la fecha en cuestión. Cuando se ha logrado dicho cambio, el objeto está “revertido”. En esta realización, se puede mantener un registro de mantenimiento con el fin de eliminar futuros cambios para este objeto desde los últimos registros de cambio asociados al usuario, o se puede apreciar el estado del registro en su estado revertido y añadir un nuevo registro de cambio de “modificar” al almacén de datos utilizando la reversión “versión actual” como base. Alternativamente, esta función puede ser implementada usando un número cualquiera de otras tecnologías, tal como una tecnología que almacene todos los cambios asociados al usuario, y durante la función de restauración solamente retorne los cambios más recientes o los datos establecidos recientemente para el usuario. Alterativamente, el almacén de datos puede almacenar un conjunto completo de datos por cada copia de seguridad que el usuario haga, aunque esto proporcione con frecuencia un esquema de datos relativamente intenso.

Esta opción de reversión, según se ha ilustrado en la figura 6, una vez que el uso activa la aplicación en la etapa 602, el teléfono envía el identificador único del usuario (en una realización, el número de teléfono) como identificador de usuario al almacén 510 de copia de seguridad en la etapa 660. En la etapa 608, la aplicación presenta al usuario una opción de revertir uno solo, o un grupo, de los contactos durante una fecha particular. Como etapa 608, una vez que el usuario introduce el PIN y la fecha de reversión, y selecciona uno solo o un grupo de contactos que han de ser revertidos, la aplicación restablece los datos desde el servidor de almacenamiento en la etapa 610. Alternativamente, el estado de los datos justamente con anterioridad a que se ejecute la reversión, puede ser en sí misma almacenada con anterioridad a que se lleve a cabo la función de reversión. En una realización adicional, el agente puede proporcionar una opción de “recordar PIN”, y almacenar el PIN localmente de modo que el usuario no necesite re-introducir el pin para cada reversión u otra función de identificación.

En realizaciones alternativas de la invención, una interfaz web puede permitir el acceso al almacén de copia de seguridad y el usuario puede implementar la función de reversión a través de la interfaz web. Por ejemplo, la interfaz puede presentar una lista de fechas de cada sincronización y el número de registros o campos sincronizados, y permitir que el usuario revierta un grupo de fecha individual o colectivo de contactos a su estado, en una fecha particular. Esta interfaz puede ser implementada también a través de una interfaz específica de WAP para el teléfono 100.

La figura 7 y la figura 8 muestran otra realización más de la presente invención en la que un usuario puede modificar opcionalmente los datos en el almacén de copia de seguridad utilizando una interfaz separada. En una realización, la interfaz es un gestor de información personal basado en World Wide Web que usa como fuente de datos para la información de almacén de copia de seguridad, o un espejo de tal información que se sincroniza con el almacén de copia de seguridad para modificar los datos en el almacén de copia de seguridad.

En la figura 7, en la etapa 702, se accede por una interfaz basada en web a los datos de información de copia de seguridad de la base de datos de copia de seguridad. En la etapa 704, el usuario modifica registros que se han generado inicialmente desde el teléfono 100 inalámbrico de usuario usando la interfaz web y los cambios son almacenados en la base de datos de copia de seguridad. En algún instante futuro, según se ha indicado mediante líneas discontinuas entre las etapas 704 y 706, el usuario (o el programador, en realizaciones de programación automática o controlada) activa la aplicación en el teléfono 100 y en la etapa 708, el teléfono transmite el identificador de usuario como número de teléfono al sistema. Una vez que el servidor 160 de sistema reconoce que ese usuario particular es un miembro del sistema, la opción de carga de contactos nuevos y cambiados que han sido cambiados por el acceso de web en la etapa 702, se presenta al usuario. Después de que el usuario introduce un número de información personal en la etapa 702, y confirma el proceso de carga, se instalan los datos en el

dispositivo en la etapa 712. Alternativamente, la carga no necesita ser confirmada, puede ser menos rápida, u opcionalmente estar pronta para el usuario. En otra realización, los cambios en el almacén 150 de datos pueden hacerse usando cualquiera de un número de productos comercialmente disponibles que permitan el acceso a los datos a una aplicación de gestor de información personal de software de usuarios, tal como la que se describe en la patente de Estados Unidos número 6.671.757. Tales productos extraen información desde gestores de información personal tales como Microsoft Outlook, y la transfieren a formatos alternativos que pueden ser leídos mediante otras aplicaciones.

La figura 8 muestra una realización alternativa del proceso de la figura 7. Las etapas 702 y 704 ocurren de igual modo que en el proceso ilustrado en la figura 7. En esta realización, la aplicación está activa en el fondo del teléfono y no se presenta al usuario con una opción hasta que el teléfono recibe un mensaje SMS en la etapa 808 indicando a la aplicación que han ocurrido los cambios en los datos del servidor. El SMS (Servicio de Mensaje Corto) es un servicio para el envío de mensajes de hasta 160 caracteres (224 caracteres si se utiliza el modo de 5 bits) a teléfonos móviles. A continuación, en la etapa 808, pueden ocurrir dos procesos opcionales. En la etapa 810, se puede presentar al usuario una opción para recuperar contactos nuevos y cambiados desde el servidor 160, y la información puede ser enviada, tras la introducción del PIN del usuario en la etapa 812 y la confirmación del proceso de carga. Cuando esto ocurre, los datos se instalan en el dispositivo en la etapa 814. Alternativamente, según se muestra mediante una línea en 816, una vez que el teléfono recibe el mensaje SMS indicativo de que se han producido los cambios en los datos del servidor, el agente interceptará el mensaje SMS y recuperará los cambios hechos en el almacén de datos a través de la interfaz de web automáticamente; los datos pueden ser instalados en el dispositivo sin ninguna intervención del usuario. Si la aplicación toma la ruta manual indicada por la línea 818 de proceso o la ruta automática indicada por la línea 816 de proceso, puede resultar una opción que el usuario seleccione, en un proceso de establecimiento, qué no ha sido descrito hasta ahora en el establecimiento de la aplicación, o qué ha sido configurado por el administrador de usuario.

En otra realización adicional, el agente 100 de teléfono puede no esperar por un mensaje SMS, sino que puede simplemente, de forma periódica, realizar un barrido selectivo en el servidor para determinar si se han producido cambios en el almacén de copia de seguridad.

En otra realización más, el barrido selectivo puede determinar si han ocurrido cambios en el teléfono con relación al almacén de datos de copia de seguridad, y transmitir esos cambios al almacén de datos. Esta realización se ha mostrado en la figura 9. Según se muestra en la misma, si un usuario modifica un registro en el teléfono en la etapa 902 y posteriormente modifica un registro en el almacén de copia de seguridad utilizando la interfaz web en la etapa 904, ambos cambios realizados con anterioridad ya sea en el almacén o ya sea en el teléfono son intercambiados con el otro dispositivo respectivo, estando los dos estados (estado 1 y estado 2) fuera de sincronización. En algún momento después de las modificaciones de las etapas 902 y 904 tal y como se ha indicado mediante la línea discontinua entre las etapas 902, 904 y 908, con la aplicación activa en el fondo del teléfono, podrá producirse alguna indicación de los cambios. Esto está representado en la etapa 908 y puede ocurrir que cuando el teléfono reciba un mensaje SMS indicativo de que los cambios han ocurrido, se produce el barrido selectivo mencionado del servidor, o se alcanza el intervalo de copia de seguridad temporizado. En esta etapa 808, se intercambian los cambios entre el teléfono y el almacén de copia de seguridad. Al igual que en la figura 8, los datos pueden ser intercambiados con la intervención del usuario (etapas 910 y 912) o sin ella (914). Adicionalmente, se puede producir el estado de conflicto discutido anteriormente con respecto al caso de discordancia, y las resoluciones discutidas anteriormente pueden estar asimismo implementadas en esta realización.

En otra realización adicional, el mensaje SMS puede dar instrucciones al teléfono para que descargue cualquier cambio realizado en el teléfono puesto que ésta es la última transmisión de copia de seguridad hasta el almacén de copia de seguridad.

Una realización adicional de la invención proporciona una automatización de los procesos de contratación, acceso a cuenta y copia de seguridad sobre un único identificador de teléfono o ID de teléfono que permita al sistema determinar información funcional más detallada acerca del teléfono. En esta realización, un UID de teléfono puede estar asociado a un UID de usuario. En una realización adicional, el UID de teléfono puede ser un ID de teléfono universalmente único (o UUID de teléfono). En una realización, el UUID de teléfono puede comprender un IMEI o un ESN. Cada teléfono GSM contiene un IMEI (número de Identidad Internacional de Equipo Móvil). Éste es un identificador único asignado a todos los dispositivos GSM. El IMEI es similar a un número de serie y es usado por la red para identificar el microteléfono (junto con el ID de SIM). El ID de SIM se proporciona en un Módulo de Identidad de Abonado que es una “tarjeta inteligente” de tamaño de sello pequeño usada en un teléfono GSM. La tarjeta SIM contiene un microchip que almacena datos que identifican al que llama para el proveedor de servicios de red. Los datos se utilizan también para encriptar transmisiones de voz y de datos, haciendo que sea prácticamente imposible escuchar llamadas. La SIM puede almacenar también información de librería del teléfono: números de teléfono y nombres asociados.

Los teléfonos CDMA tienen también un número de identificación individual, el ESN. Este número puede ser encontrado en la parte trasera de un microteléfono, bajo la batería, y normalmente es de una longitud de ocho dígitos, combinando letras y números.

La Asociación GSM (GSMA) tiene el papel de Administrador Decimal Global que asigna números de Identidad Internacional de Equipo Móvil (IMEI) a fabricantes para su uso en GSM. Los números de IMEI son asignados a teléfonos individuales por el fabricante y pueden identificar el tipo, la naturaleza y las características del teléfono al que se han asignado.

Un método para la utilización de un UID de teléfono asociado a los datos del usuario ha sido mostrado en la figura 10. En algún momento anterior a que los teléfonos sean distribuidos a un usuario en la etapa 1002, se asigna un UID de teléfono a un teléfono del usuario. El UID de teléfono puede comprender un IMEI u otro ID tal como un numero ESN tal y como se ha discutido en lo que antecede. Posteriormente, en la etapa 1004, el usuario adquiere el teléfono y presiona una opción de “copia de seguridad” en el teléfono. La opción de copia de seguridad puede ser proporcionada en un agente de aplicación tal y como se ha discutido con anterioridad, o en una aplicación específicamente diseñada para su uso en el teléfono, también discutida con anterioridad. Al iniciar la función de copia de seguridad en el teléfono en la etapa 1004, comenzará un proceso de copia de seguridad conforme a cualquiera de las realizaciones mencionadas anteriormente, pero permitirá que se cree automáticamente una cuenta de copia de seguridad usando un UID de teléfono y un UID de usuario. En la etapa 806, usando el UID del teléfono, el sistema puede determinar la caracterización (el tipo, las características, y la funcionalidad) del teléfono en base al UID de teléfono. Esto es particularmente cierto en casos de teléfonos GSM que hacen uso de un número de IMEI. Se comprenderá además que en la etapa 1004, el UID de usuario puede ser el ID de SIM que es proporcionado por el SIM en un teléfono GSM. Alternativamente, el UID de usuario puede ser el número de teléfono u otro identificador único cualquiera para el usuario.

En la etapa 808, una vez que son conocidos ambos UID de teléfono y UID de usuario, se puede contratar automáticamente una cuenta de copia de seguridad mediante el sistema sin necesidad de conocer información adicional del usuario. Alternativamente, se puede requerir información de autenticación adicional por parte del sistema, tal como la introducción de un PIN.

En la etapa 808, cada vez que el usuario almacena información de copia de seguridad en el almacén de datos de copia de seguridad, se puede registrar el UID de teléfono que especifica el teléfono desde el que se obtuvo la información. Con ello, el almacén de datos de copia de seguridad conocerá cuándo utiliza el usuario un teléfono alternativo que tenga un UID de teléfono diferente para almacenar información.

En la etapa 810, que puede estar separada en el tiempo de la etapa 808 según se ha indicado mediante una línea discontinua entre las etapas 808 y 810, el usuario inicia una transmisión de datos de copia de seguridad usando un nuevo UID de teléfono. Esto puede ocurrir, por ejemplo, cuando el usuario cambia una SIM a un nuevo teléfono de tecnología GSM, o en otro caso autentica, usando su UID de usuario, cualquier autenticación requerida por el sistema. La etapa 812 de autenticación puede ser opcional en casos en que la autenticación sea proporcionada por el ID de SIM o puede ser opcionalmente inhabilitada por el usuario.

Una vez que el sistema detecta, en la etapa 810, que el usuario ha proporcionado un nuevo UID de teléfono, en la etapa 814, el sistema registra el nuevo UID de teléfono en la etapa 816 y el sistema puede llevar a cabo automáticamente la restauración de datos de sistema transmitiendo cambios al nuevo teléfono. En la situación mostrada en las etapas 810 a 816, puesto que el usuario ha conmutado el UID del teléfono, el sistema conocerá que el estado de copia de seguridad más reciente llegó desde un teléfono diferente, y el UID del nuevo teléfono tendrá un estado de datos que no es normal.

De nuevo, al igual que en el caso de estado de datos de discordancia discutido con anterioridad, el usuario puede introducir datos en el nuevo teléfono con anterioridad a que se lleve a cabo la iniciación de la copia de seguridad en la etapa 810. En este caso, el comportamiento o la gestión de datos discutidos anteriormente con respecto al caso de discordancia, pueden ser aplicados de nuevo.

Las figuras 11 y 12 muestran dos alternativas a la manera en que se lleva a cabo la etapa 1004. De acuerdo con la presente invención, se puede producir cualquier comunicación entre el teléfono y el servidor 160 que sustenta el almacén de datos a través de un número cualquiera de protocolos. En una realización, se utiliza SyncML y en esa realización, el agente 110 puede tener un cliente SyncML integrado o se puede usar el cliente SyncML del fabricante proporcionado normalmente en el teléfono. Las figuras 11 y 12 muestran métodos para usar el cliente SyncML del fabricante.

En la figura 11, en la etapa 1004, se supone que el teléfono ha sido expedido con un cliente SyncML preconfigurado. Mediante la configuración previa, el cliente SyncML se expide con el teléfono de tal modo que presionando la opción de copia de seguridad (o sync) en el agente, el agente sync de los fabricantes de teléfonos tiene la información de identificación para acceder al servidor 495 SyncML mostrado en la figura 1. En la etapa 1102, en la que el teléfono se expide con un cliente SyncML configurado previamente, el UID de teléfono y el UID de usuario son enviados al servidor SyncML cuando el usuario presiona el botón de copia de seguridad en el teléfono. En la etapa 1106, la información de usuario y el UID del teléfono están asociados en un almacén de datos de copia de seguridad, y se establece una cuenta en la etapa 1108.

En la figura 12, el teléfono se expide sin cliente SyncML previamente configurado en la etapa 1202. Esto significa que en 1024, opcionalmente, el agente puede necesitar ser descargado e instalado en el teléfono en la etapa 1204. En la etapa 1206, tras la iniciación de la opción de copia de seguridad en la aplicación de teléfono, se puede enviar información de configuración por medio de un mensaje SMS al cliente SyncML del fabricante del teléfono que proporcione información de aprovisionamiento de configuración al cliente SyncML. Esto permite que el cliente SyncML del teléfono direccione el servidor 195 SyncML en la figura 1. A continuación, el proceso de establecimiento de cuenta en la etapa 1208 empieza a usar el UID del teléfono y el UID del usuario.

En la realización discutida con respecto a las figuras 10 a 12, la experiencia del usuario puede ser relativamente no obstructiva. Por ejemplo, el usuario necesita solamente presionar un botón blando de “copia de seguridad” en el teléfono para tener la información de establecimiento de cuenta transmitida al almacén de datos de copia de seguridad. Cualquier pérdida o cambio de SIM a un teléfono diferente, dará como resultado que el proceso de recuperación se lleve a cabo sin intervención de ningún usuario adicional.

Adicionalmente, el administrador del almacén de datos de copia de seguridad puede realizar determinaciones acerca de cuántos datos se han de proporcionar al teléfono. Por ejemplo, si el teléfono que se identifica en base al UID del teléfono se sabe que es un dispositivo rico en funciones, el administrador puede hacer copia de todas las disposiciones que estén disponibles en los teléfonos, tal como calendario, tareas, y librería del teléfono. Si, tras la conmutación del UID del teléfono, el usuario cambia a un teléfono menos rico en funciones, el proveedor puede determinar que, por ejemplo, el nuevo teléfono tiene solamente una librería de direcciones, y proporcionar solamente los datos de librería de direcciones en la función de recuperación. El usuario no necesita proporcionar ninguna información de configuración al administrador durante este proceso.

La descripción detallada que antecede de la invención ha sido presentada a efectos de ilustración y de descripción. Ésta no pretende ser exhaustiva ni limitar la invención a la forma precisa en la que se ha descrito. Muchas modificaciones y variaciones son posibles en vista de la enseñanza anterior. Por ejemplo, tareas realizadas por el agente en el teléfono pueden ser llevadas a cabo por el servidor como resultado de una llamada a un código que esté en el servidor, instruyendo al servidor para que realice el método y devuelva datos al servidor. Adicionalmente, cuando el sistema requiere una autenticación, se puede proporcionar al usuario la opción de almacenar la información de autenticación en el teléfono o en el agente y no tener que introducir manualmente la autenticación cada vez que se requiera. Aún más, la autenticación puede ser transmitida por medio de un intercambio de mensajes SMS. Las funciones descritas en la presente memoria pueden estar asignadas al servidor o a un agente de teléfono o a una aplicación basada en la potencia de procesamiento disponible en el teléfono. Las realizaciones descritas fueron elegidas con el fin de explicar mejor los principios de la invención y su aplicación práctica para permitir con ello que otros expertos en la materia utilicen mejor la invención en diversas realizaciones y con diversas modificaciones según sean adecuadas para el uso particular contemplado. Se prevé que el alcance de la invención quede definido por las reivindicaciones anexas a la presente memoria.

REIVINDICACIONES

1.- Un método implementado por un dispositivo de procesamiento en un teléfono (100) inalámbrico para hacer copia de seguridad de información personal almacenada en el teléfono inalámbrico, comprendiendo el método:

proporcionar, usando un agente (110) de teléfono que incluye instrucciones operables por el dispositivo de procesamiento, un método de transmisión automatizada de datos de teléfono para transmitir cambios a un almacén (510) de copia de seguridad, y un método de restauración para recuperar información de copia de seguridad desde el almacén de copia de seguridad hasta el teléfono inalámbrico;

presentar en el teléfono inalámbrico, usando el agente de teléfono, una interfaz de establecimiento de cuenta de usuario de servicio de copia de seguridad, para establecer una cuenta de usuario de servicio de copia de seguridad, una interfaz de programación de método de copia de seguridad para establecer el programa de copia de seguridad, y una interfaz de recuperación para llamar al método de restauración, incluyendo el teléfono inalámbrico un visualizador y uno o más botones (302, 304); y

en respuesta a la activación del usuario, llamar con la interfaz de recuperación al método de restauración para proporcionar cambios desde el almacén de copia de seguridad hasta el teléfono inalámbrico.

2.- El método de la reivindicación 1, en el que el uno o más botones comprenden uno o más botones alfanuméricos y uno o más botones blandos, diferentes de los botones alfanuméricos, cambiando las funciones controladas por el uno o más botones blandos del teléfono inalámbrico bajo control del agente de teléfono.

3.- El método de la reivindicación 1, en el que la interfaz de establecimiento llama a un método que permite al usuario establecer una cuenta de copia de seguridad con un almacén de copia de seguridad.

4.- El método de la reivindicación 1, en el que la interfaz de programación establece un intervalo para enviar de manera regular información personal al almacén de copia de seguridad.

5.- El método de la reivindicación 1, en el que la interfaz de programación provoca la transmisión de la información personal al almacén de copia de seguridad tras una modificación de la información en el teléfono inalámbrico.

6.- El método de la reivindicación 1, en el que la interfaz de recuperación llama a un método para cargar toda la información almacenada en el almacén de copia de seguridad en el almacén de datos del teléfono inalámbrico.

7.- El método de la reivindicación 6, en el que el método incluye además proporcionar una interfaz de reversión en la interfaz de usuario del teléfono.

8.- El método de la reivindicación 7, en el que la interfaz de reversión llama un método que carga los cambios en base a una fecha particular.

9.- El método de la reivindicación 1, en el que el método incluye además proporcionar una interfaz anti-borrado.

10.- El método de la reivindicación 9, en el que la interfaz anti-borrado llama a un método que transmite un cambio asociado a un registro particular en un espacio de información personal del usuario.

11.- El método de la reivindicación 1, en el que dicha información personal comprende un almacén de datos de librería de direcciones, un almacén de datos de entradas de tareas, un almacén de datos de entradas de calendario, un almacén de datos de entradas de notas, un almacén de datos de entradas de alarma, un almacén de datos de diccionario según necesidad, un almacén de datos de email, un almacén de datos de tonos de llamada, o un almacén de datos multimedia para imágenes, sonidos, y películas.

12.- El método de l reivindicación 1, que comprende proporcionar acceso a al menos una de entre dicha interfaz de establecimiento, dicha interfaz de programación, y dicha interfaz de recuperación a través de un navegador de web o a través de un protocolo inalámbrico.

13.- Un método para almacenar información personal desde un teléfono (100) inalámbrico en un almacén (510) de copia de seguridad de una base de datos de almacenamiento de copia de seguridad, que comprende:

proporcionar a un teléfono inalámbrico, un agente (110) de teléfono que incluye instrucciones operables por un procesador del teléfono inalámbrico;

implementar un método de transmisión automatizada de datos de teléfono para transmitir cambios al almacén de copia de seguridad a través de un enlace comunicaciones, y un método de restauración que recupera información de copia de seguridad desde el almacén de copia de seguridad hasta el teléfono inalámbrico;

presentar en el teléfono inalámbrico una interfaz de establecimiento de cuenta de usuario de servicio de copia de seguridad para establecer una cuenta de usuario de servicio de copia de seguridad, una interfaz de programación de método de programación para establecer el programa de copia de seguridad y una interfaz de recuperación para llamar al método de restauración, incluyendo el teléfono inalámbrico un visualizador y uno o más botones (302, 304) en el teléfono inalámbrico; y

en respuesta a la activación del usuario y a la interfaz de recuperación que llama al método de restauración, proporcionar cambios desde el almacén de copia de seguridad hasta el teléfono inalámbrico.

14.- El método de la reivindicación 13, en el que el método incluye además aceptar información personal procedente del teléfono inalámbrico a intervalos definidos por el usuario a través de la interfaz de programación de método de copia de seguridad.

15.- El método de la reivindicación 13, en el que el método incluye además aceptar datos de establecimiento de cuenta de usuario procedentes de la interfaz de contratación de servicio del agente.

16.- El método de la reivindicación 13, en el que el método incluye además asignar un programa de intervalos de descarga al agente.

17.- El método de la reivindicación 16, en el que el método incluye además modificar el programa de intervalos para un equilibrio de carga entre una pluralidad de usuarios.

18.- El método de la reivindicación 13, que incluye demás proporcionar una notificación al agente sobre los cambios se han realizado en el almacén de copia de seguridad a través de una interfaz secundaria.

19.- El método de la reivindicación 18, en el que el agente de teléfono actualiza el almacén de datos en el teléfono inalámbrico tras la recepción de una notificación.

20.- El método de la reivindicación 19, en el que la notificación es un mensaje SMS o es el resultado de un barrido selectivo del almacén de copia de seguridad respecto a los cambios.

21.- Un agente de teléfono que incluye instrucciones operables por un dispositivo de procesamiento de un teléfono inalámbrico para hacer copia de seguridad de la información personal almacenada en el teléfono inalámbrico, para llevar a cabo el método de una cualquiera de las reivindicaciones 1 a 12.

22.- Un teléfono (110) inalámbrico que comprende un almacén de datos para almacenar información personal, un visualizador y uno o más botones (302, 204), comprendiendo además el teléfono inalámbrico:

medios (110) para la creación de una cuenta de usuario de forma automatizada, iniciada por un usuario a través de una interfaz de usuario del teléfono inalámbrico, siendo los medios para esta creación operables para acceder a un sistema de copia de seguridad y para crear una cuenta de usuario en el sistema de copia de seguridad;

medios (110) para hacer copia de seguridad automáticamente y transmitir cambios a través de un enlace de comunicaciones al sistema de copia de seguridad a intervalos definidos por el usuario; y

medios (110) para restablecimiento llamado por el usuario a través de una interfaz de recuperación presentada en el teléfono inalámbrico, siendo los medios para restablecimiento operables para recuperar información de copia de seguridad desde el almacén de copia de seguridad hasta el teléfono inalámbrico.

23.- El teléfono inalámbrico de la reivindicación 22, en el que los medios para creación son operables para acceder al sistema de copia de seguridad usando un identificador único para que el usuario cree una cuenta de usuario en el sistema de copia de seguridad.

24.- El teléfono inalámbrico de la reivindicación 22, en el que la interfaz de recuperación incluye un método de barrido selectivo que proporciona un estado de datos de usuario existente a modo de una fecha específica.

25.- El teléfono inalámbrico de la reivindicación 22, en el que la interfaz de recuperación incluye un método anti-borrado que proporciona al menos un objeto de datos restaurados previamente borrados por la acción de un usuario.

26.- El teléfono inalámbrico de la reivindicación 22, en el que al menos el método de copia de seguridad y el método de creación de cuenta son iniciados por el agente de teléfono de la reivindicación 20.

27.- El teléfono inalámbrico de la reivindicación 22, en el que los intervalos definidos por el usuario son alterables por medio de un administrador.

28.- El teléfono inalámbrico de la reivindicación 22, en el que los intervalos son regulares o los intervalos son

arbitrarios.

29.- El teléfono inalámbrico de la reivindicación 22, en el que el método de restauración opera en respuesta a un teléfono que se entiende que no tiene ningún dato ni ninguna cuenta de usuario existente.

30.- El teléfono inalámbrico de la reivindicación 22, en el que el método de creación de cuenta se lleva a cabo mediante el sistema de copia de seguridad a través de una interfaz secundaria proporcionada al usuario.

31.- El teléfono inalámbrico de la reivindicación 22, en el que dicho almacén de datos comprende un almacén de datos de librería de direcciones, un almacén de datos de entradas de tarea, un almacén de datos de entradas de calendario, un almacén de datos de entradas de notas, un almacén de datos de entradas de alarma, un almacén de datos de diccionario según necesidades, un almacén de datos de email, un almacén de datos de tonos de llamada, o un almacén de datos multimedia para imágenes, sonidos y películas.

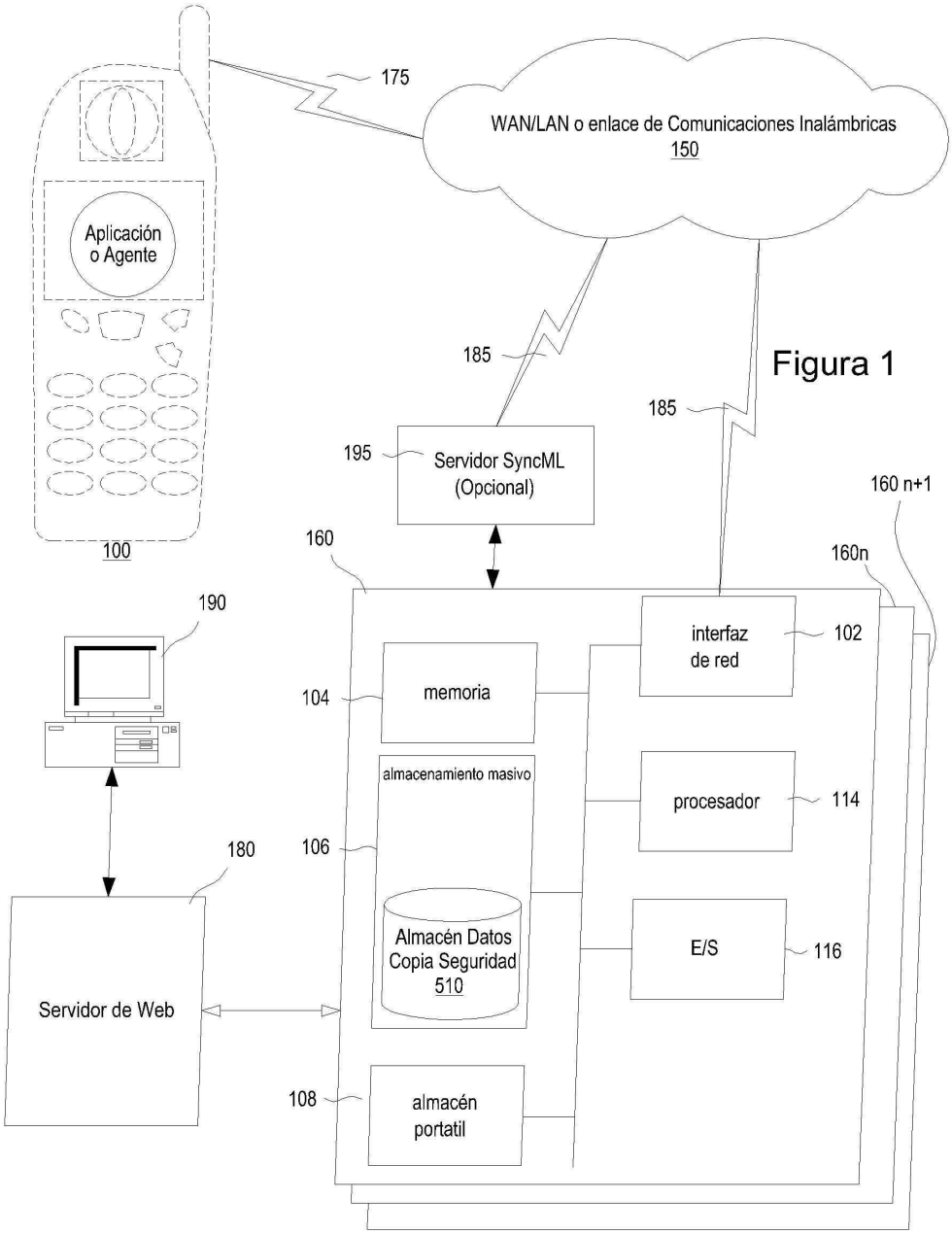

175
WAN/LAN o enlace de Comunicaciones Inalámbricas
150
Aplicación
o Agente
185
185
195
Servidor SyncML
(Opcional)
160 n+1
160
160n
100
190
interfaz
de red
102
104
memoria
almacenamiento masivo
procesador
114
106
180
Almacén Datos
Copia Seguridad
510
E/S
116
Servidor de Web
108
almacén
portatil

Figura 1

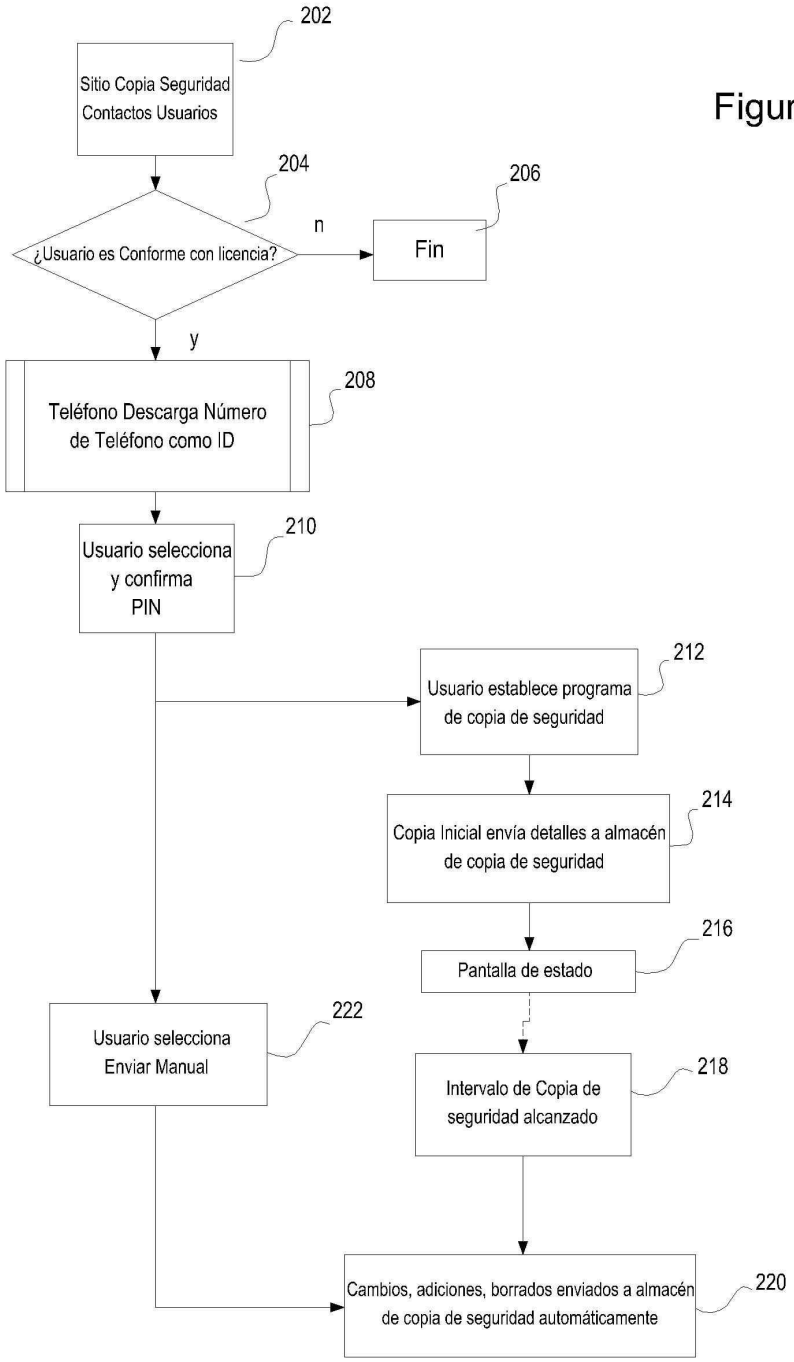

202
Sitio Copia Seguridad Contactos Usuarios
204
¿Usuario es Conforme con licencia?
n
206
Fin
y
208
Teléfono Descarga Número de Teléfono como ID
210
Usuario selecciona y confirma PIN
212
Usuario establece programa de copia de seguridad
214
Copia Inicial envía detalles a almacén de copia de seguridad
216
Pantalla de estado
222
Usuario selecciona Enviar Manual
218
Intervalo de Copia de seguridad alcanzado
220
Cambios, adiciones, borrados enviados a almacén de copia de seguridad automáticamente

Figura 2

Figura 3a

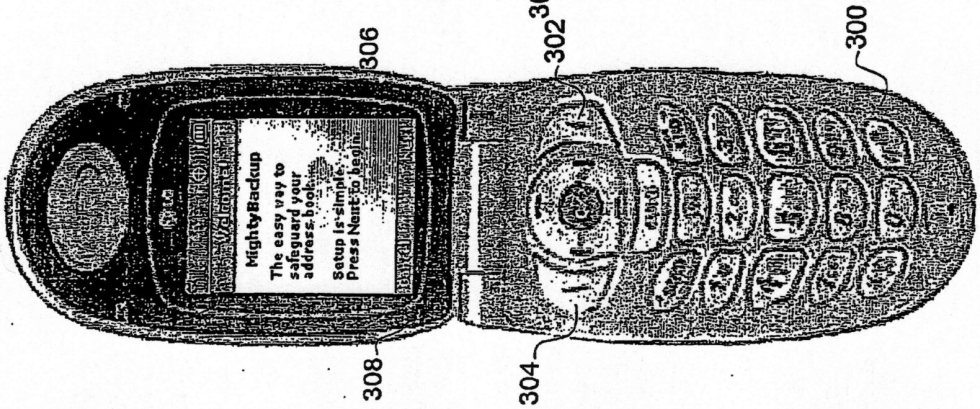


Figura 3b

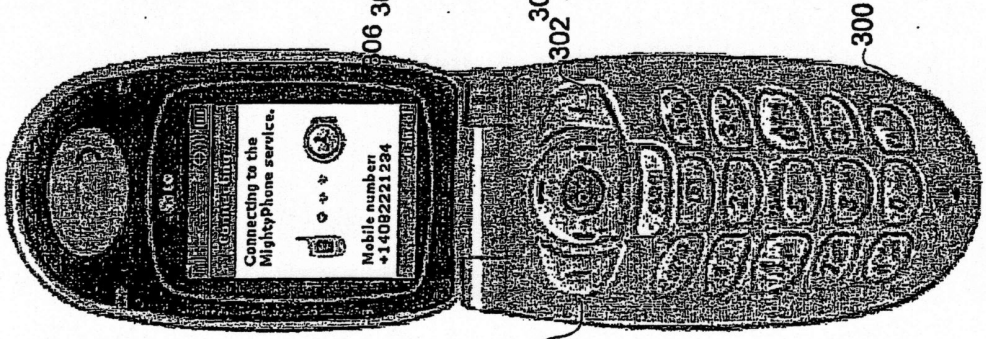


Figura 3c

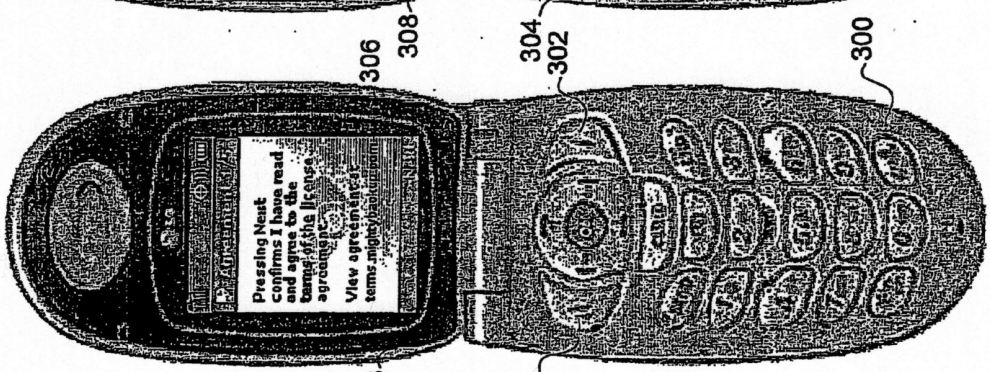


Figura 3d

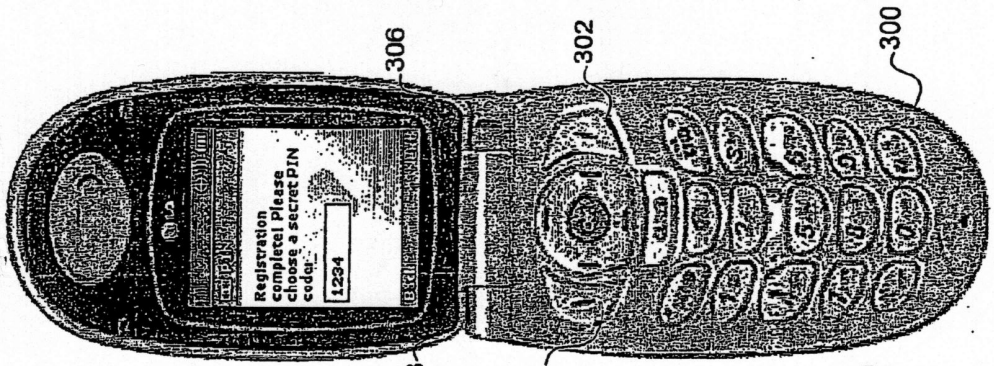


Figura 3e

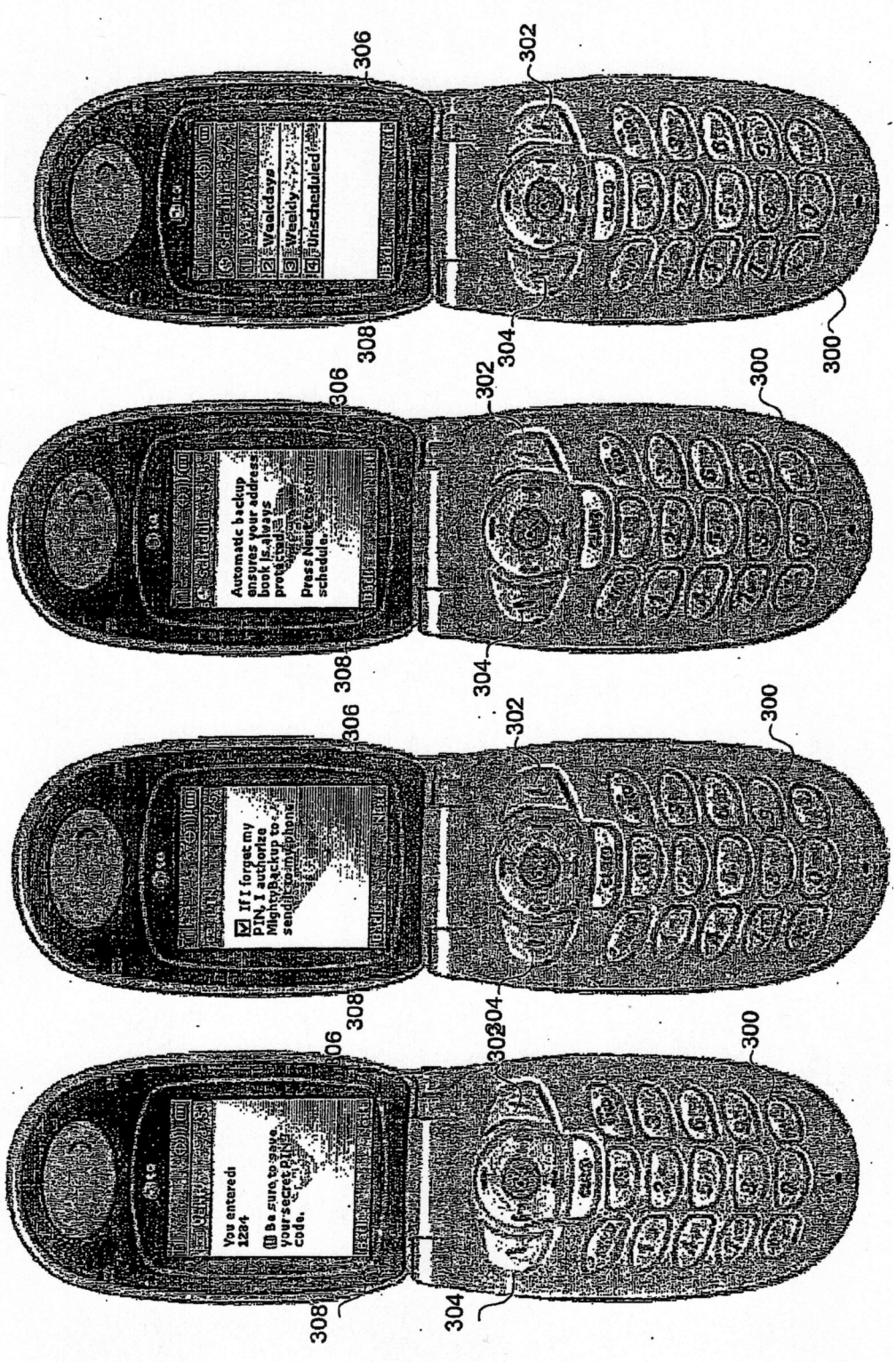


Figura 3f

Figura 3g

Figura 3h

Figura 3i

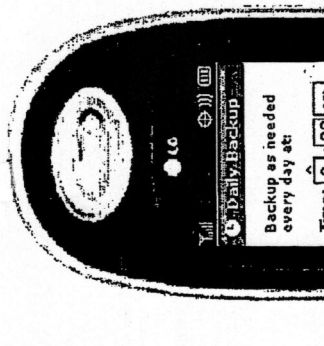


Figura 3j

Figura 3k

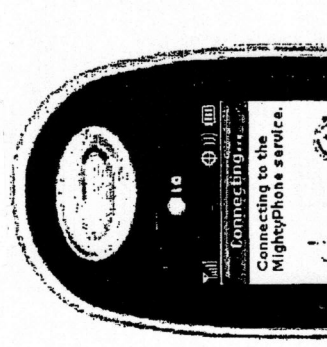
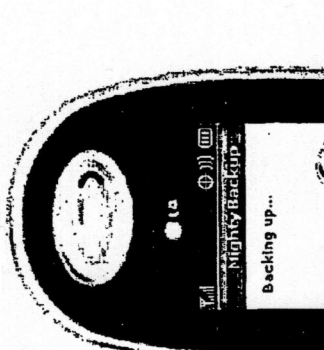


Figura 3l



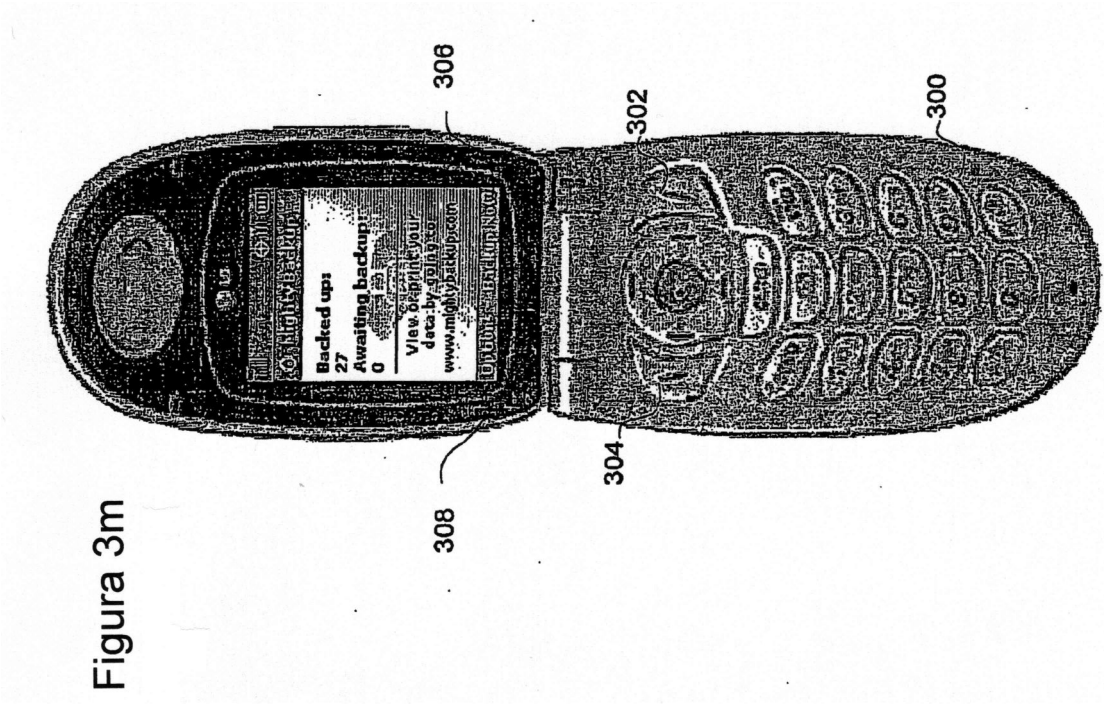

306
302
300
304
308
Backed up:
27
Awaiting backup:
0
View online your
data by going to
www.mobilybackup.com

Figura 3m

Figura 3n

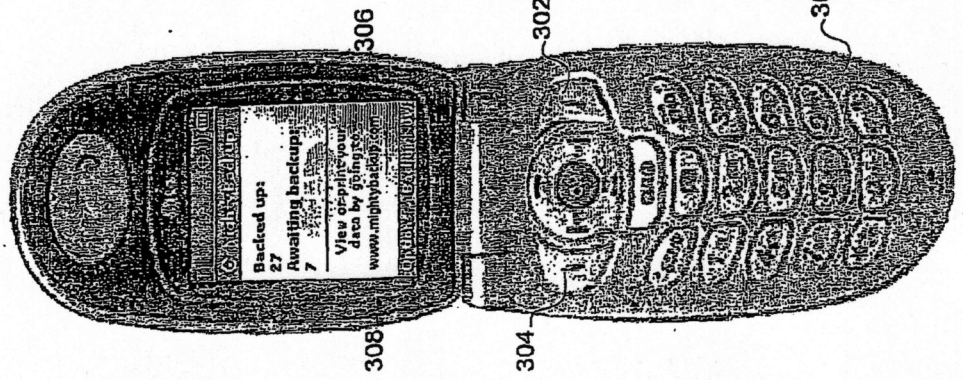


Figura 3o

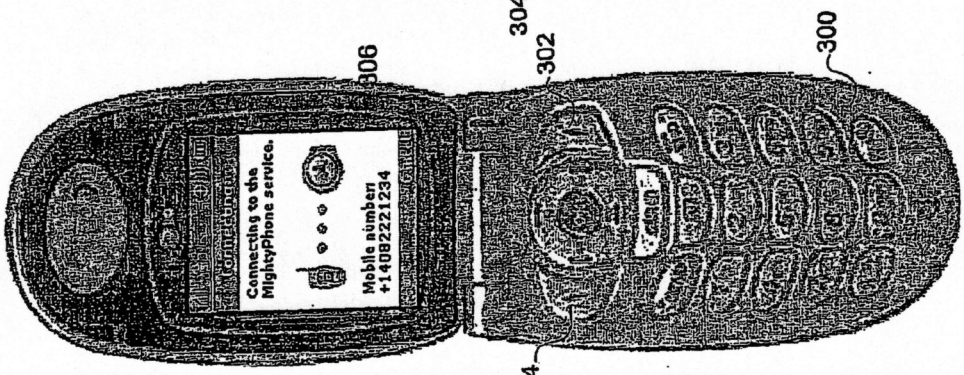


Figura 3p

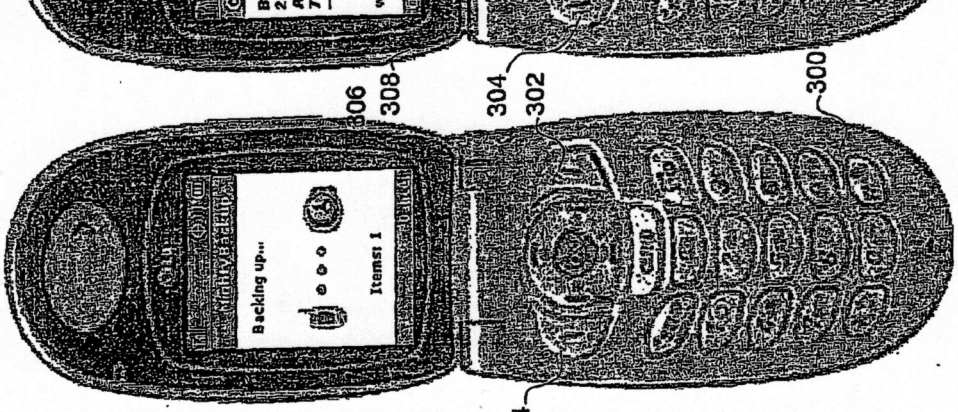
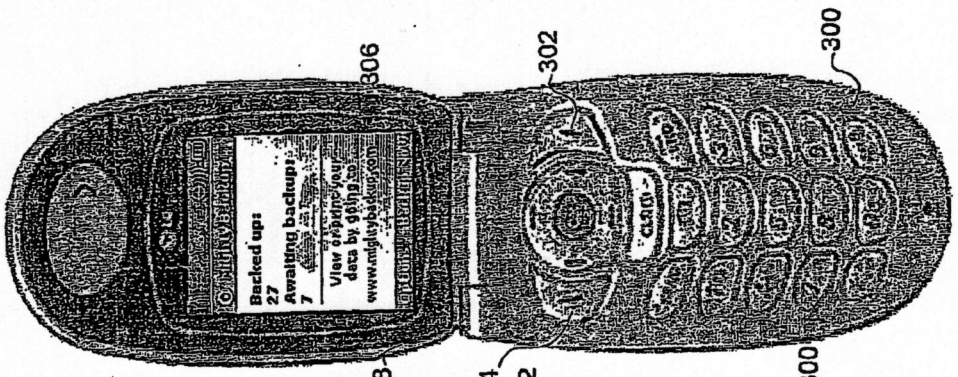


Figura 3q



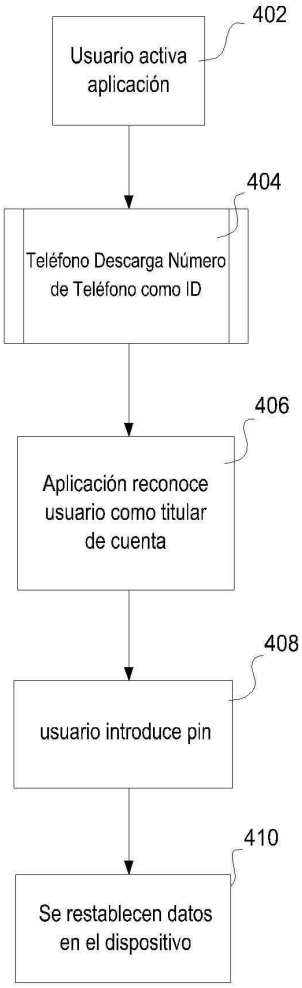


Figura 4

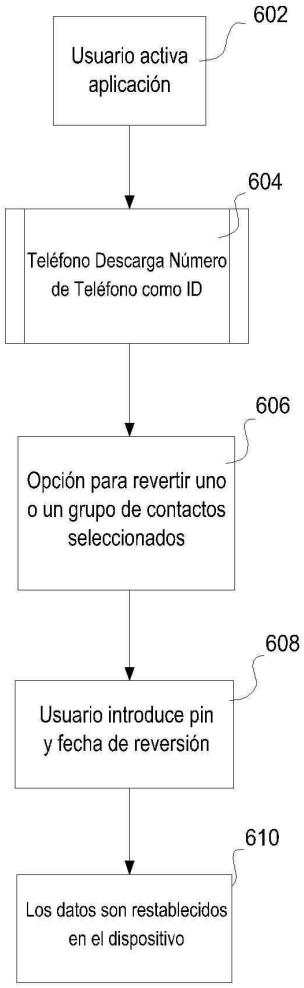


Figura 6

Figura 5a

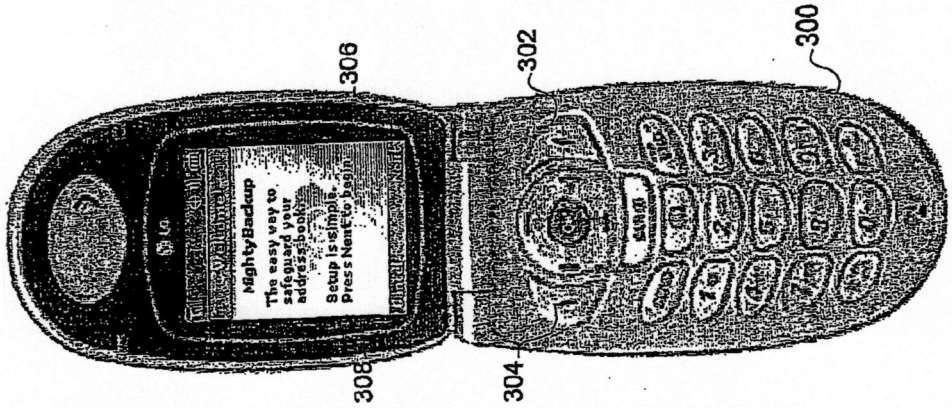


Figura 5b

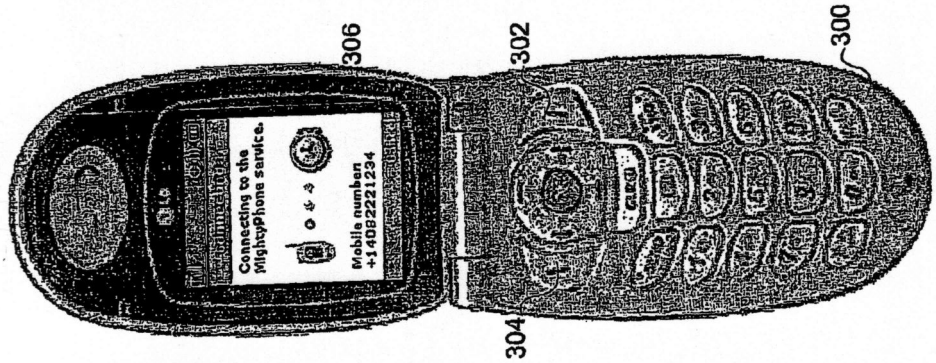


Figura 5c

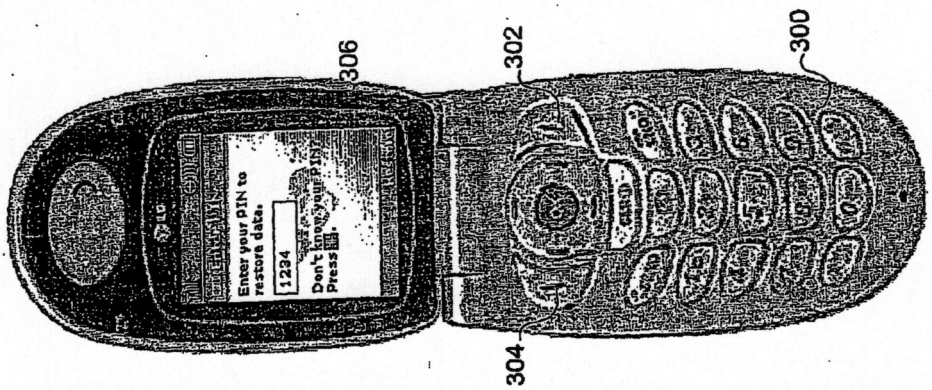


Figura 5e

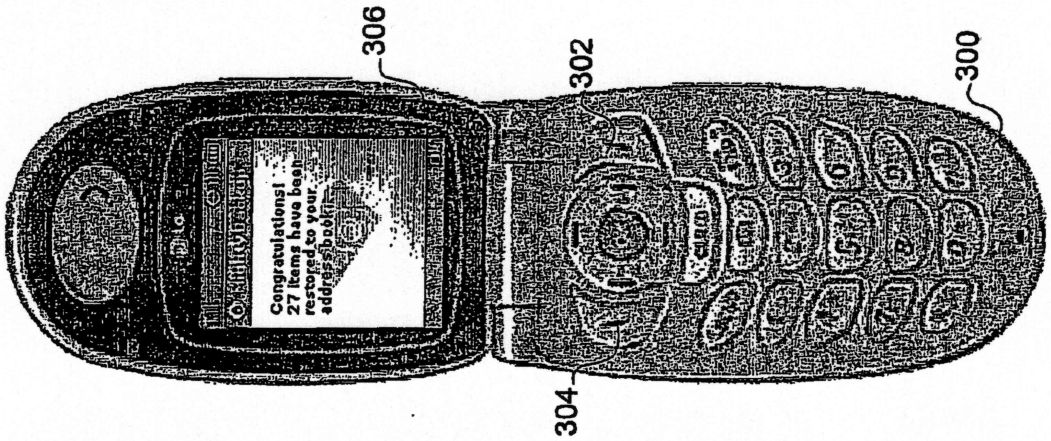


Figura 5d

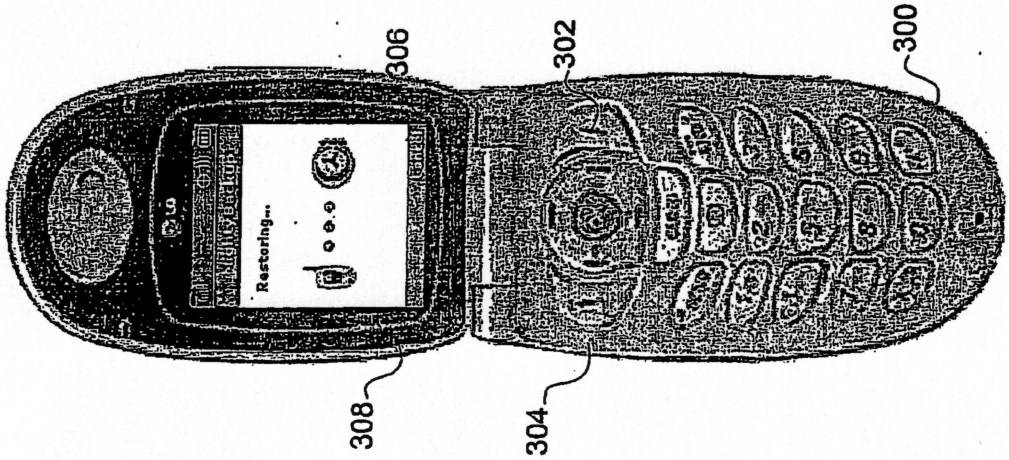


Figura 7

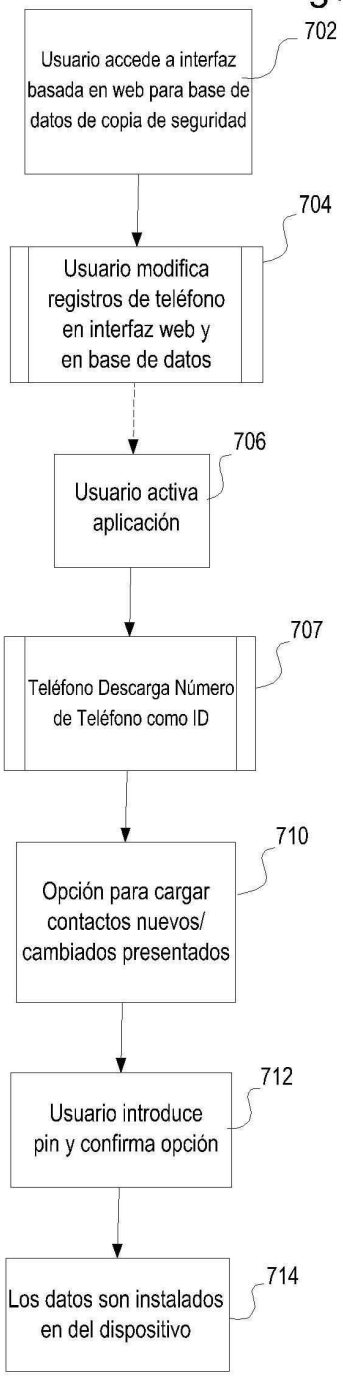


Figura 8

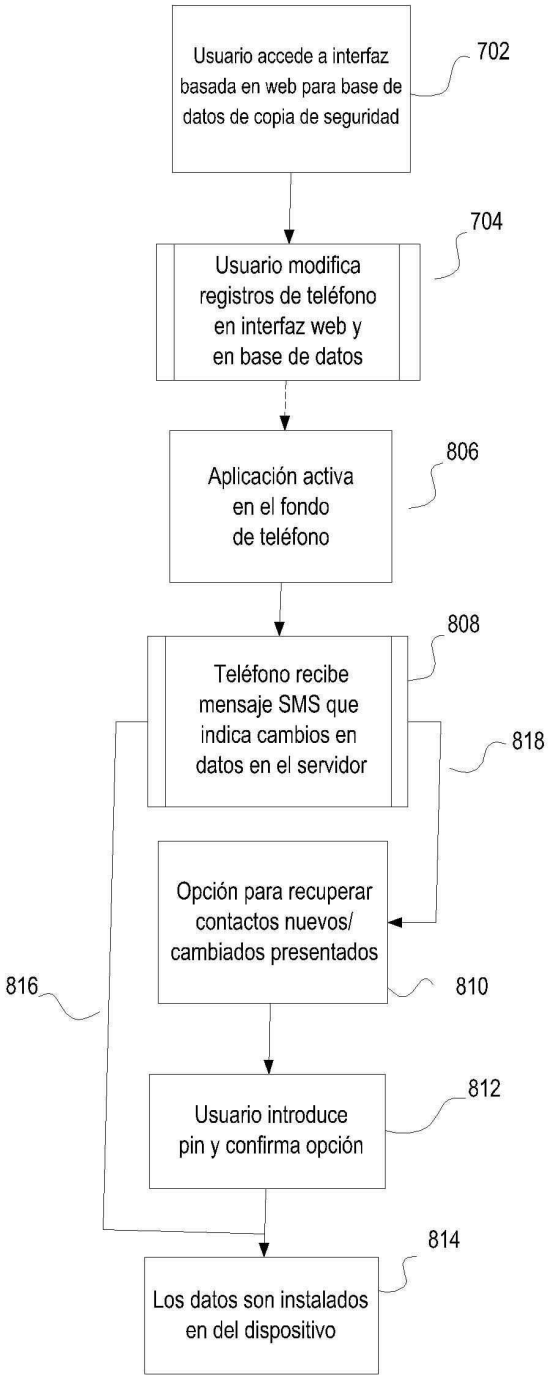


Figura 9

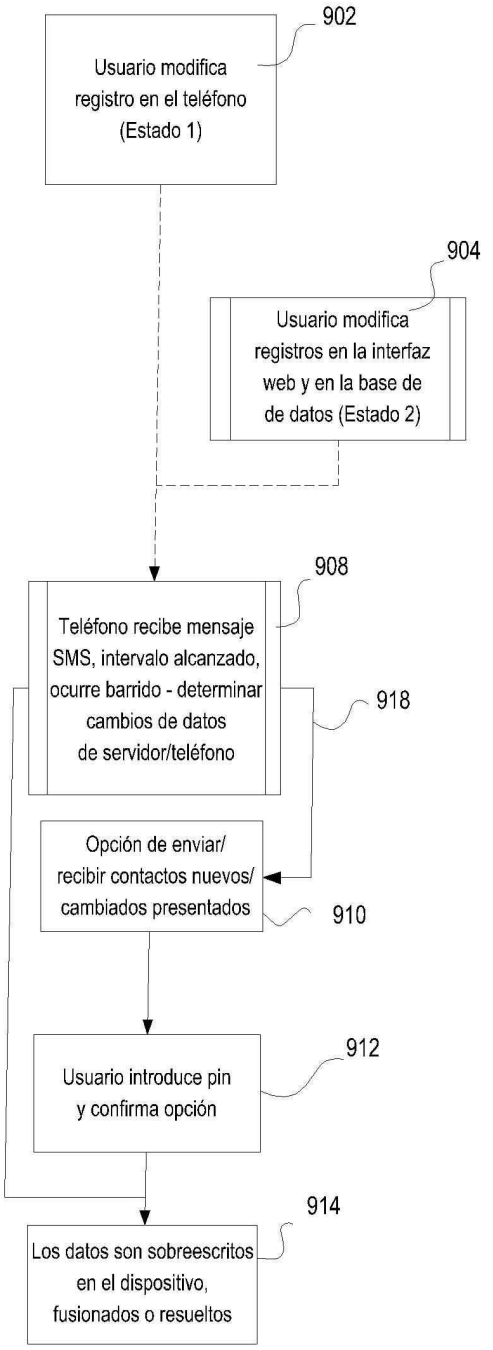


Figura 10

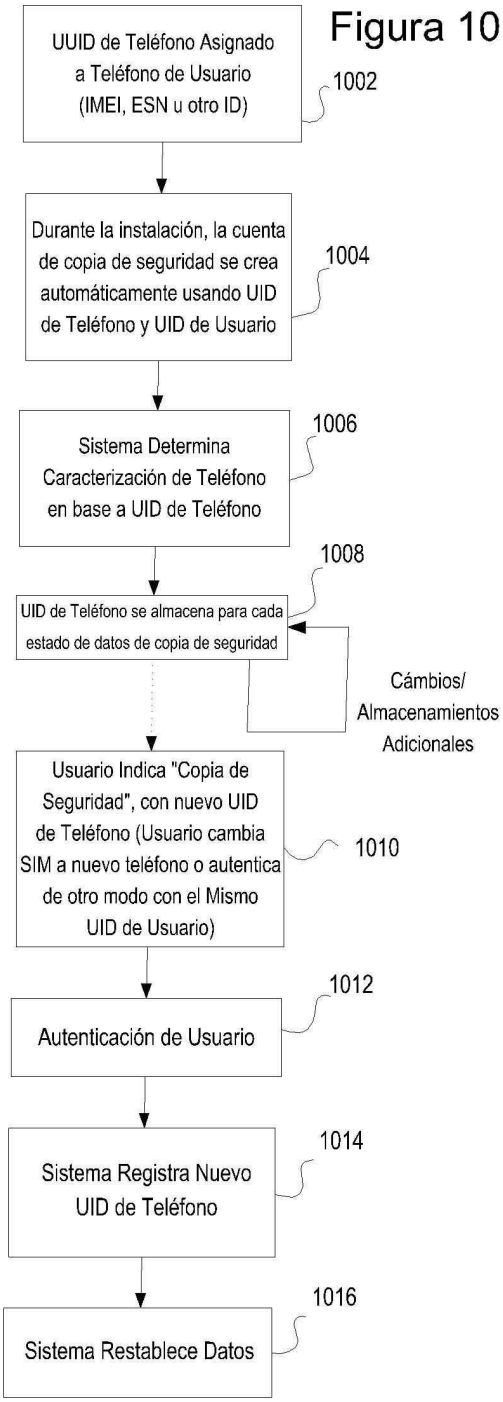


Figura 11

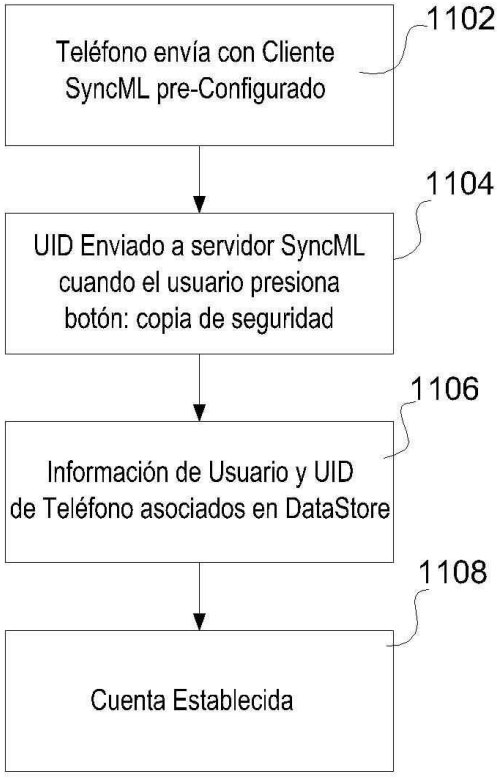


Figura 12