(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 805 278**

(51) Int. CI.:

H04W 4/00 (2008.01)
G06F 21/88 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **07.11.2007 PCT/US2007/083943**

(87) Fecha y número de publicación internacional: **22.05.2008 WO08060920**

(96) Fecha de presentación y número de la solicitud europea: **07.11.2007 E 07868687 (0)**

(97) Fecha y número de publicación de la concesión europea: **06.05.2020 EP 2095254**

(54) Título: **Inutilizar y bloquear un dispositivo por vía aérea**

(30) Prioridad:

15.11.2006 US 560048

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.02.2021

(73) Titular/es:

QUALCOMM INCORPORATED (100.0%)
5775 Morehouse Drive
San Diego, CA 92121-1714, US

(72) Inventor/es:

WELINGKAR, BHARAT y
PRASAD, SRIKIRAN

(74) Agente/Representante:

SALVÀ FERRER, Joan

DESCRIPCIÓN

Inutilizar y bloquear un dispositivo por vía aérea

REFERENCIA CRUZADA A SOLICITUDES RELACIONADAS

[0001] La presente solicitud reivindica prioridad con respecto a la solicitud de patente de Estados Unidos de América n.º 11/560.048 que lleva por título *Over-the-Air Device Kill Pill and Lock* ("Inutilizar y bloquear un dispositivo por vía aérea"), presentada el 15 de noviembre de 2006. La presente aplicación contiene materia que puede estar relacionada con la materia contenida en las siguientes solicitudes pendientes de tramitación de propiedad común: la solicitud de patente de Estados Unidos de América n.º 11/560.040, presentada el 15 de noviembre de 2006 y que lleva por título *Over-the-Air Device Services and Management* ("Servicios y administración de dispositivos por vía aérea"); la solicitud de patente de Estados Unidos de América n.º 11/560.045, presentada el 15 de noviembre de 2006 y que lleva por título *Dynamic Resource Management* ("Administración dinámica de recursos"), la solicitud de patente de Estados Unidos de América n.º 11/560.052, presentada el 15 de noviembre de 2006 y que lleva por título *Device-Side Data De-Duping* ("Eliminación de duplicados de datos del lado del dispositivo") y la solicitud de patente de Estados Unidos de América n.º 11/560.084, presentada el 15 de noviembre de 2006 y titulada *Server-Controlled Heartbeats* ("Latidos controlados por el servidor").

ANTECEDENTES

[0002] Un dispositivo informático típico del lado del cliente, como por ejemplo un dispositivo informático y de comunicaciones móvil, depende de varias entidades dispares para los servicios y la administración del dispositivo cliente. Por ejemplo, un usuario del dispositivo cliente puede necesitar un ordenador de escritorio para acceder a un sitio web de facturación proporcionado por un proveedor de servicios para el dispositivo cliente. Para servicios de datos, el usuario puede tener que acceder a un sitio web administrado por una organización a la que está asignado el dispositivo cliente. Sin embargo, para otros servicios, el usuario puede tener que acceder a un sitio web asociado con un fabricante del dispositivo cliente.

[0003] Además, es posible que varios puntos de interfaz deban estar disponibles para el usuario con el fin de que el usuario tenga acceso a un conjunto completo de servicios y administración disponibles para el dispositivo cliente. Por ejemplo, pueden adquirirse determinados servicios a través del dispositivo cliente. Es posible que se tengan que adquirir otros servicios utilizando un sitio web de escritorio. Aún más, otros servicios específicos pueden estar disponibles solo a través de llamadas a un representante de atención al cliente. Además, se pueden obtener determinadas actualizaciones para el dispositivo cliente accediendo a un sitio web suministrado por un fabricante del dispositivo cliente.

[0004] A medida que se introducen entidades proveedoras de servicios adicionales en un sistema para admitir las operaciones y la funcionalidad del dispositivo cliente, la complejidad –al menos desde la perspectiva del usuario– aumenta proporcionalmente y, en consecuencia, resulta más difícil mantener y administrar completamente el dispositivo cliente.

[0005] En la solicitud de patente de Estados Unidos de América n.º 2004/224665 A1 se describe la restricción del acceso a los datos de usuario en un dispositivo móvil cuando se pierde o es robado dicho dispositivo.

SUMARIO

[0006] De acuerdo con al menos un aspecto de una o más realizaciones descritas en el presente documento, un sistema incluye: una interfaz de instrucciones configurada para recibir una instrucción de un usuario para restringir el acceso a los datos de usuario almacenados en un dispositivo informático móvil; y una interfaz de transmisión configurada para transmitir de forma inalámbrica un comando informático ejecutable por el dispositivo informático móvil, donde se genera el comando informático en respuesta a la instrucción para restringir el acceso a los datos de usuario.

[0007] De acuerdo con al menos otro aspecto de una o más realizaciones descritas en el presente, un método para administrar un dispositivo cliente incluye: recibir una instrucción de un usuario para restringir el acceso a los datos de usuario almacenados en el dispositivo cliente; autenticar el usuario; como respuesta a una autenticación correcta, generar un comando de restricción correspondiente a la instrucción recibida; y transmitir de forma inalámbrica el comando de restricción para su ejecución por el dispositivo cliente.

[0008] De acuerdo con al menos otro aspecto de una o más realizaciones descritas en el presente, un dispositivo informático móvil incluye: un primer módulo configurado para recibir de forma inalámbrica un primer comando y configurado además para, en respuesta a la recepción del primer comando, bloquear datos de usuario en el dispositivo informático móvil para que se no se pueda acceder a ellos usando el dispositivo informático móvil; y un segundo

módulo configurado para recibir de forma inalámbrica un segundo comando y configurado además para, en respuesta a la recepción del segundo comando, borrar los datos de usuario en el dispositivo informático móvil.

[0009] Las características y ventajas descritas en el presente no son exhaustivas y, en particular, un gran número de características y ventajas adicionales resultarán evidentes para los expertos en la materia a la vista de la siguiente descripción. Además, cabe señalar que el lenguaje utilizado en el presente se ha seleccionado principalmente para fines de legibilidad y didácticos y puede que no se haya seleccionado para circunscribir la presente invención. La invención está definida por las reivindicaciones adjuntas.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

[0010] En la Figura 1 se muestra un diagrama de alto nivel de un sistema de servicios y administración de dispositivos por vía aérea de acuerdo con una realización de la presente invención.

En la Figura 2 se muestra un diagrama a nivel de componentes de un sistema de servicios y administración de dispositivos por vía aérea de acuerdo con una realización de la presente invención.

En la Figura 3 se muestra un diagrama a nivel de módulos de un servidor de administración de cuentas y un dispositivo informático del lado del cliente de acuerdo con una realización de la presente invención.

En la Figura 4 se muestra un diagrama de transición de estados de acuerdo con una realización de la presente invención.

En la Figura 5 se muestra un subsistema de un sistema de servicios y administración de dispositivos por vía aérea de acuerdo con una realización de la presente invención.

En la Figura 6 se muestra un diagrama a nivel de módulos de un servidor de aplicaciones web y un dispositivo informático del lado del cliente de acuerdo con una realización de la presente invención.

En la Figura 7 se muestra un subsistema de un sistema de servicios y administración de dispositivos por vía aérea de acuerdo con una realización de la presente invención.

En la Figura 8 se muestra un proceso de flujo de acuerdo con una realización de la presente invención.

En la Figura 9 se muestra un subsistema de un sistema de servicios y administración de dispositivos por vía aérea de acuerdo con una realización de la presente invención.

En la Figura 10 se muestra un proceso de flujo de acuerdo con una realización de la presente invención.

En la Figura 11 se muestra un diagrama a nivel de módulos de un servidor de sincronización y un dispositivo informático del lado del cliente de acuerdo con una realización de la presente invención.

En la Figura 12 se muestra un proceso de flujo de acuerdo con una realización de la presente invención.

En las Figuras 13-28 se muestran varias capturas de pantalla de acuerdo con una o más realizaciones de la presente invención.

[0011] Cada una de las figuras a las que se hace referencia anteriormente representa una realización de la presente invención a título ilustrativo únicamente. Los expertos en la materia reconocerán fácilmente a partir de la siguiente descripción que pueden usarse una o más realizaciones de los métodos, estructuras y sistemas ilustrados en el presente sin abandonar los principios de la presente invención.

DESCRIPCIÓN DETALLADA

[0012] En la siguiente descripción de realizaciones de la presente invención se exponen numerosos detalles específicos para proporcionar una comprensión más exhaustiva de la presente invención. No obstante, resultará evidente para un experto en la materia que la presente invención se puede llevar a la práctica sin uno o más de estos detalles específicos. En otros casos, no se han descrito en detalle características bien conocidas para no complicar innecesariamente la descripción.

[0013] En general, las realizaciones de la presente invención se refieren a un sistema para proporcionar servicios y administración de dispositivos informáticos del lado del cliente. En particular, en una o más realizaciones, se proporciona un conjunto de servicios y administración por vía aérea para dispositivos informáticos móviles, los cuales incluyen dispositivos informáticos portátiles de mano. Entre los ejemplos de dispositivos informáticos portátiles de

mano figuran los teléfonos móviles/celulares, los Asistentes Digitales Personales (PDA, *Personal Digital Assistant*), los dispositivos portátiles de correo electrónico y otros dispositivos informáticos que tienen un factor de forma adecuado para su uso en mano. Sin embargo, se observa que, en otras realizaciones, uno o más de los diversos principios descritos a continuación pueden aplicarse igualmente a otros tipos de dispositivos informáticos del lado del cliente, como por ejemplo estaciones de trabajo, ordenadores de escritorio y ordenadores portátiles.

[0014] En la Figura 1 se muestra un sistema de servicios y administración de dispositivos por vía aérea 100 de acuerdo con una realización de la presente invención. Este sistema 100 incluye un dispositivo informático del lado del cliente (que también se denomina en el presente un “dispositivo cliente”) 102, por ejemplo, un teléfono móvil/celular, un asistente digital personal, un dispositivo de correo electrónico portátil, un ordenador de escritorio o un ordenador portátil. En general, el dispositivo cliente 102 puede ser cualquier tipo de dispositivo que sea capaz de comunicarse con otro dispositivo para obtener servicios y/o datos.

[0015] Un lado del servidor del sistema 100 incluye un servidor de aplicaciones web 104, un servidor de administración de cuentas 106 y un servidor de sincronización 108. Más adelante se describe en mayor detalle cada uno de estos servidores 104, 106 y 108, haciendo referencia a las Figuras 2-28.

[0016] Los servidores 104, 106 y 108 pueden estar configurados para su implementación en hardware y/o software. Por ejemplo, el servidor de aplicaciones web 104 puede estar asociado con un sistema informático físico dedicado únicamente a proporcionar servicios del servidor de aplicaciones web 104. Sin embargo, en una o más de otras realizaciones adicionales, el servidor de aplicaciones web 104 puede estar asociado con el software residente en un sistema informático particular que no está dedicado únicamente a proporcionar servicios del servidor de aplicaciones web 104.

[0017] Además, aunque se muestran el servidor de aplicaciones web 104, el servidor de administración de cuentas 106 y el servidor de sincronización 108 como separados en la Figura 1, la funcionalidad de uno o más de los servidores 104, 106 y 108 puede combinarse con la de otro de los servidores 104, 106 y 108. Además, la ubicación de uno o más de los servidores 104, 106 y 108 puede ser la misma que la de otro de los servidores 104, 106 y 108. Por ejemplo, el servidor de administración de cuentas 106 y el servidor de sincronización 108 pueden estar alojados en la misma máquina.

[0018] En una o más realizaciones, los servidores 104, 106 y 108 pueden estar ubicados remotamente entre sí. En algunos de dichos casos, los servidores 104, 106 y 108 pueden comunicarse entre sí a través de una red de área local (LAN, *Local Area Network*). Por ejemplo, si los servidores 104, 106 y 108 residen dentro o forman parte de una organización específica, los servidores 104, 106 y 108 pueden comunicarse a través de una red empresarial y/o a través de una interconexión punto a punto. Además, en una o más de otras realizaciones adicionales, los servidores 104, 106 y 108 pueden comunicarse entre sí a través de una red de área amplia (WAN, *Wide Area Network*). Por ejemplo, los servidores 104, 106 y 108 pueden comunicarse entre sí a través de Internet utilizando solicitudes y respuestas del protocolo de transporte de hipertexto (HTTP, *Hypertext Transport Protocol*). Más específicamente, por ejemplo, los servidores 104, 106 y 108 pueden comunicarse entre sí utilizando mensajes basados en lenguaje de marcado extensible (XML, *Extensible Markup Language*).

[0019] Además, cabe señalar que cada uno de los servidores 104, 106 y 108 puede ser diseñado, mantenido, administrado y/o entregado por una o más de varias entidades. Por ejemplo, el servidor de sincronización 108 puede ser administrado por el fabricante del dispositivo cliente 102. En otro ejemplo, el servidor de aplicaciones web 104 y/o el servidor de administración de cuentas 108 pueden diseñarse y/o entregarse por contrato con un fabricante del dispositivo cliente 102. Además, en otro ejemplo adicional, uno o más de los servidores 104, 106 y 108 pueden ser diseñados y/o administrados por un proveedor de servicios configurado para proporcionar servicios de voz y/o datos a un usuario del dispositivo cliente 102. En otro ejemplo adicional, uno o más de los servidores 104, 106 y 108 pueden ser administrados y/o diseñados para una organización a la que pertenecen una pluralidad de dispositivos cliente 102 o con la que están asociados de otra forma.

[0020] En la Figura 2 se muestra un diagrama a nivel de componentes del sistema 100. El dispositivo cliente 102 se comunica con el servidor de aplicaciones web 104, el servidor de administración de cuentas 106 y el servidor de sincronización 108 a través de una red 202. En general, la red 202 es cualquier medio a través del cual el dispositivo cliente 102 puede comunicarse de forma inalámbrica con uno o más del servidor de aplicaciones web 104, el servidor de administración de cuentas 106 y el servidor de sincronización 108. En otras palabras, el dispositivo cliente 102 es capaz de comunicarse de forma inalámbrica con la red 202 a la que uno o más de entre el servidor de aplicaciones web 104, el servidor de administración de cuentas 106 y el servidor de sincronización 108 están conectados operativamente. Es en este sentido que el sistema 100 puede describirse como un sistema “por vía aérea”: los servicios y las características de administración de los servidores 104, 106 y 108 se proporcionan de forma inalámbrica al dispositivo cliente 102, donde el dispositivo cliente 102 representa un punto de interfaz central a través del cual un usuario del dispositivo cliente 102 puede acceder a dichos servicios y características de administración (en lugar de que el usuario tenga que acceder a un sistema distinto al del dispositivo cliente 102).

[0021] Además, se observa que el sistema 100 puede ser una red *push*, una red *pull* o una combinación de las mismas. En una red *push*, uno o más de los servidores 104, 106 y 108 envían datos al dispositivo cliente 102. En una red *pull*, uno o más de los servidores 104, 106 y 108 envían datos al dispositivo cliente 102 previa solicitud de los datos por el dispositivo cliente 102.

[0022] En una o más realizaciones, la red 202 puede ser al menos en parte una red de telefonía móvil. En otro ejemplo, la red 202 puede ser al menos en parte una red de datos inalámbrica. Además, en otro ejemplo adicional, la red 202 puede ser al menos en parte una red de radio. En otro ejemplo adicional, la red 202 puede ser al menos en parte una red wifi (*Wireless Fidelity*). Además, en una o más realizaciones, la red 202 puede ser al menos en parte una red basada en Internet. Aún más, la información transferida entre el dispositivo cliente 102 y uno o más de entre el servidor de aplicaciones web 104, el servidor de administración de cuentas 106 y el servidor de sincronización 108 pueden encriptarse usando técnicas de encriptado de datos estándar de la industria (por ejemplo, SSL de 128 bits) Además, los datos específicos del usuario almacenados en uno o más de entre el servidor de aplicaciones web 104, el servidor de administración de cuentas 106 y el servidor de sincronización 108 pueden encriptarse usando técnicas de encriptado de datos estándar en el sector.

[0023] Por lo que respecta también a la Figura 2, el servidor de aplicaciones web 104 incluye, al menos en parte, un componente de administración de recursos 204 y componente de “inutilización (*kill pill*) y bloqueo” 206. El componente de administración de recursos 204, tal y como se describe más adelante con referencia a las Figuras 7 y 8, puede usarse para administrar centralmente los recursos (por ejemplo, los tipos de datos) usados por las aplicaciones 218 residentes en el dispositivo cliente 102. El componente de inutilización y bloqueo 206, como se describe en mayor detalle más adelante haciendo referencia a las Figuras 9 y 10, puede usarse para borrar y/o bloquear los datos residentes en el dispositivo cliente 102.

[0024] El servidor de administración de cuentas 106 incluye, al menos en parte, un componente de “motor de latidos” 212 y un componente de motor de estado 214. El componente de motor de estado 214, como se describe en mayor detalle más adelante haciendo referencia a la Figura 4, puede usarse para mantener información de estado y realizar un seguimiento de cambios de estado del dispositivo cliente 102. El componente de motor de latidos 212, como se describe en mayor detalle más adelante haciendo referencia a la Figura 5, puede usarse para controlar un protocolo de actualización seguido por el dispositivo cliente 102.

[0025] Por lo que respecta también a la Figura 2, el servidor de sincronización 108 incluye, al menos en parte, un componente de copia de seguridad/restauración 208. El componente de copia de seguridad/restauración 208, como se describe en mayor detalle más adelante haciendo referencia a la Figura 11, puede usarse para hacer una copia de seguridad de los datos y restaurarlos en el dispositivo cliente 102.

[0026] El dispositivo cliente 102 incluye utilidades del sistema 216, aplicaciones 218 y un componente de eliminación de datos duplicados 210. El uso y la operación de las utilidades del sistema 216 y las aplicaciones 218 serán evidentes a la vista de la descripción en el presente. El componente de eliminación de datos duplicados 210, como se describe en mayor detalle más adelante haciendo referencia a la Figura 12, puede usarse para detectar y/o eliminar instancias de tipos de datos redundantes.

[0027] A continuación se describirán en mayor detalle el servidor de aplicaciones web 104, el servidor de administración de cuentas 106 y el servidor de sincronización 108. Específicamente, la descripción más adelante que hace referencia a las Figuras 3-5 se refiere al servidor de administración de cuentas 106, la descripción más adelante que hace referencia a las Figuras 6-10 se refiere al servidor de aplicaciones web 104 y la descripción más adelante que hace referencia a las Figuras 11 y 12 se refiere al servidor de sincronización 108. Cabe señalar que, aunque las diversas funcionalidades se describen más adelante en asociación con uno de los servidores 104, 106 y 108, dicha descripción se presenta principalmente en aras de una mayor claridad, y como tal, no limita las formas en que las diferentes funcionalidades descritas pueden asignarse a uno o más de los servidores 104, 106 y 108. Asimismo, el servidor de administración de cuentas 106, el servidor de aplicaciones web 104, el servidor de sincronización 108 y el dispositivo cliente 102 se describen, haciendo referencia a las Figuras 3, 6 y 11, y tienen módulos, donde un “módulo” es cualquier programa, lógica y/o funcionalidad implementados en hardware y/o software.

Servidor de administración de cuentas

[0028] En la Figura 3 se muestra un diagrama del servidor de administración de cuentas 106 y el dispositivo cliente 102 de acuerdo con una realización de la presente invención. En general, el servidor de administración de cuentas 106 sirve como un punto central de administración de cuentas al que uno o más proveedores, proveedores de servicios, fabricantes de dispositivos y similares pueden conectarse para interactuar con una cuenta asociada con el dispositivo cliente 102.

[0029] Como se muestra en la Figura 3, el servidor de administración de cuentas 106 incluye un componente de transporte HTTP 314 y un componente de transporte de servicio de mensajes cortos (SMS) 316. El dispositivo cliente 102 incluye, de manera similar, un componente de transporte HTTP 318 y un componente de transporte SMS 320. Los componentes de transporte HTTP 314 y 318 pueden usarse para comunicaciones HTTP/S. Además, en una o más realizaciones, pueden utilizarse los componentes de transporte HTTP 314 y 318 para admitir un protocolo simple de acceso a objetos (SOAP, *Simple Object Access Protocol*), el cual puede ser usado para intercambiar mensajes basados en XML. Pueden utilizarse los componentes de transporte SMS 316 y 320 para admitir comunicaciones de mensajes SMS. Cabe señalar que los mensajes SMS pueden comunicarse en la forma que se conoce como mensajes de "texto".

[0030] Además, se muestra que el dispositivo cliente 102 tiene una pluralidad de bibliotecas. Una "biblioteca" puede definirse como una colección de subrutinas y funciones almacenadas en uno o más archivos, generalmente de forma compilada, para enlazar con otros programas. En particular, en la Figura 3, el dispositivo cliente 102 incluye una biblioteca de administración de cuentas 322 que puede usarse para interconectar recursos y funcionalidad con los proporcionados por el servidor de administración de cuentas 106. Además, el dispositivo cliente 102 incluye una biblioteca de sincronización 324 que puede usarse para interconectar recursos y funcionalidad con los proporcionados por el servidor de sincronización 108 (descrito más adelante con referencia a las Figuras 11 y 12).

[0031] El dispositivo cliente 102 también incluye una biblioteca de registros de cuentas 326, una biblioteca de autenticación 328, una biblioteca de texto 330, una biblioteca de registros de eventos 332, una biblioteca de programación 334 y una biblioteca de latidos 336. El uso y la función de las bibliotecas 326, 328, 330, 332, 334 y 336 quedarán claros a la vista de la descripción que se presenta a continuación y que hace referencia a las Figuras 3-28. Además, una o más de las bibliotecas 326, 328, 330, 332, 334 y 336 pueden ser reutilizables en el sentido de que pueden usarse en conexión con las funcionalidades del servidor de aplicaciones web 104, el servidor de administración de cuentas 106, el servidor de sincronización 108 o cualquier combinación de los mismos.

[0032] Al menos en un aspecto de una o más realizaciones descritas en el presente, el servidor de administración de cuentas 106 facilita la creación/registro e inicio de sesión en una cuenta mantenida para el dispositivo cliente 102. Tradicionalmente, para configurar una cuenta, un usuario tiene que llamar a un representante de atención al cliente, llevar a cabo a un proceso de configuración en tiempo real con un representante en un minorista o proveedor de servicios del dispositivo cliente, o acceder a Internet para realizar un proceso de configuración disponible a través de un sitio web de un minorista, fabricante o proveedor de servicios. Aquí, en una o más realizaciones, el usuario del dispositivo cliente 102 puede configurar una cuenta para su dispositivo cliente 102 completamente (o casi completamente) mediante el uso del dispositivo cliente 102, como se describe a continuación.

[0033] Por lo que respecta ahora a una descripción de las formas en que pueden usarse el servidor de administración de cuentas 106 y el dispositivo cliente 102, en un aspecto, una vez que un usuario del dispositivo cliente 102 se registra en el servidor de administración de cuentas 106 (por ejemplo, se crea una cuenta para ese usuario), es posible que ese usuario no tenga que volver a crear otra cuenta de usuario, incluso si sustituye el dispositivo cliente 102, cambia la plataforma del dispositivo cliente 102 y/o se pierden o corrompen datos en el dispositivo cliente 102. Por lo tanto, puede considerarse que dicha administración de cuentas centralizada es un servicio proporcionado por el sistema 100.

[0034] Una vez que se ha instalado un software de cliente particular en el dispositivo cliente 102 (la descarga y la instalación se describen más adelante haciendo referencia a la Figura 6), se puede iniciar el software de cliente, de forma que el usuario del dispositivo cliente 102 tiene la opción de registrarse para una nueva cuenta o iniciar sesión en una cuenta existente (véase, por ejemplo, la Figura 13). Si el usuario elige registrarse para una nueva cuenta, se le solicita que introduzca la información de registro de la cuenta. Dicha información puede incluir, por ejemplo, su nombre, la dirección de su casa y/o trabajo, el número de teléfono de su casa y/o trabajo, el número de la seguridad social, el número de su permiso de conducir o tarjeta de identificación, su nombre de usuario, su contraseña y una dirección alternativa de correo electrónico (por ejemplo, una dirección de correo diferente a la asociada con el dispositivo cliente 102). También se puede solicitar al usuario que especifique preguntas y respuestas de comprobación, las cuales se utilizarán para recuperar un nombre de usuario y/o contraseña olvidados (véase, por ejemplo, la Figura 14). La información de registro se envía de forma inalámbrica a través de la red 202 (como se muestra en la Figura 2) al servidor de administración de cuentas 106. Si la cuenta se crea correctamente, se puede notificar al usuario en consecuencia; por el contrario, si la cuenta no se crea correctamente, se le puede presentar al usuario información de error que posiblemente contendrá instrucciones para volver a introducir parte o toda la información de registro.

[0035] Si el usuario tiene una cuenta existente, puede indicarlo y a continuación se le solicitará su dirección de correo electrónico y contraseña. La dirección de correo electrónico, la contraseña y un número de teléfono del dispositivo cliente 102 se comunican después a través de la red 202 (como se muestra en la Figura 2) al servidor de administración de cuentas 106. Tras la validación de la cuenta del usuario mediante un módulo de verificación de correo electrónico 306 y un módulo de verificación de número de teléfono 310 en el servidor de administración de

cuentas 106, se le puede solicitar al usuario que realice una copia de seguridad o restauración de datos (véase, por ejemplo, la Figura 15). Como se describe de forma más detallada a continuación haciendo referencia a la Figura 11, el servicio de copia de seguridad de datos permite al usuario hacer una copia de seguridad inalámbrica de los datos en su dispositivo cliente 102 en un almacén de datos del lado del servidor (no mostrado). Además, como se describe de forma más detallada más adelante, haciendo referencia a la Figura 11, el servicio de restauración de datos permite al usuario restaurar datos de forma inalámbrica en su dispositivo cliente 102 desde un almacén de datos del lado del servidor (no mostrado).

[0036] Asimismo, en una o más realizaciones, en el caso de que el usuario (o un administrador) haya cambiado un número de teléfono del dispositivo cliente 102, cuando el usuario elige iniciar sesión en su cuenta existente, el nuevo número de teléfono, junto con la dirección de correo electrónico y la contraseña introducidas por el usuario, son comunicadas de forma inalámbrica al servidor de administración de cuentas 106. El servidor de administración de cuentas 106 después detecta el nuevo número de teléfono asociado con la dirección de correo electrónico y contraseña del usuario previamente conocidas y actualiza la cuenta del usuario para reflejar el nuevo número de teléfono. Al usuario entonces se le pueden presentar las opciones de realizar una copia de seguridad y/o restaurar datos, como se ha descrito anteriormente.

[0037] Si el usuario olvida la contraseña de su cuenta, el usuario lo podrá indicar, como corresponde, utilizando el software de cliente. Esta indicación, junto con la dirección de correo electrónico del usuario (véase, por ejemplo, la Figura 16), son enviadas al servidor de administración de cuentas 106, que a su vez recupera las preguntas de comprobación especificadas por el usuario durante el registro de la cuenta y las comunica de forma inalámbrica al dispositivo cliente 102 para que el usuario las pueda contestar (véase, por ejemplo, la Figura 17). Si el servidor de administración de cuentas 106 valida las respuestas del usuario a las preguntas de comprobación, dicho servidor de administración de cuentas 106 puede solicitar al usuario que introduzca una nueva contraseña (véase, por ejemplo, la Figura 18). El servidor de administración de cuentas 106 después actualiza la cuenta del usuario para reflejar la nueva contraseña.

[0038] Si el usuario no puede responder a sus preguntas de comprobación correctamente o en un número predeterminado de intentos permitidos, el servidor de administración de cuentas 106, a través de un módulo de restablecimiento de contraseña 304, puede notificar al usuario que su contraseña debe ser restablecida por correo electrónico (véase, por ejemplo, la Figura 19). En este caso, el módulo de restablecimiento de contraseña 304 envía un hipervínculo a la dirección de correo electrónico del usuario. A continuación, el usuario, ya sea desde el dispositivo cliente 102 o desde otro sistema informático (por ejemplo, un ordenador de escritorio o un ordenador portátil) puede hacer clic en el hipervínculo, lo que dirige al usuario de forma eficaz a través de un proceso de restablecimiento de contraseña para crear una nueva contraseña. La nueva contraseña se comunica al módulo de restablecimiento de contraseña 304, que a su vez restablece la contraseña de la cuenta del usuario, por consiguiente.

[0039] La descripción anterior, con respecto a cómo un usuario del dispositivo cliente 102 puede registrarse o iniciar sesión en una cuenta en el servidor de administración de cuentas 106, representa casos de uso. Una de las aplicaciones de software del lado del cliente 338 que facilita y admite estos casos de uso puede tener ciertos atributos, requisitos y características, como se describe a continuación. Cuando se inicia esta aplicación de software de cliente, el cliente primero puede asegurarse de que el dispositivo cliente 102 es un dispositivo admitido. En otras palabras, el cliente puede verificar que el dispositivo cliente 102 se encuentra incluido en una lista de dispositivos indicados como admitidos por el sistema 100. Si el dispositivo cliente 102 no es admitido, el usuario puede ser dirigido a un sitio web informativo (alojado, por ejemplo, por el servidor de aplicaciones web 104) para obtener más instrucciones.

[0040] Suponiendo que el dispositivo cliente 102 sea admitido, al iniciar la aplicación de software de cliente, se puede mostrar al usuario un acuerdo de licencia de usuario final (EULA, *End-User License Agreement*). En una o más realizaciones, la aplicación de software de cliente garantiza que el usuario pueda desplazarse por toda la pantalla y leer el acuerdo de licencia de usuario final. Además, se puede proporcionar al usuario la opción de aceptar o rechazar el acuerdo de licencia de usuario final. Aún más, el acuerdo de licencia de usuario final puede informar al usuario de los acuerdos de facturación y otras tarifas por el uso de uno o más de los servicios suministrados en el sistema 100. En caso de que el usuario se niegue a aceptar los términos del acuerdo de licencia de usuario final, la aplicación de software de cliente se cerrará, impidiendo así al usuario acceder a servicios particulares ofrecidos en el sistema 100. En inicios posteriores de la aplicación de software de cliente, la aplicación de software de cliente puede volver a mostrar el acuerdo de licencia de usuario final e impedir que el usuario acceda a servicios específicos hasta que acepte los términos del acuerdo de licencia de usuario final.

[0041] En el caso más probable de que el usuario acepte los términos del acuerdo de licencia de usuario final, la aplicación de software de cliente puede pasar a uno o más de los pasos de inicio de sesión/registro descritos anteriormente. Cabe señalar que, si se acepta el acuerdo de licencia de usuario final, el acuerdo de licencia de usuario final puede no ser mostrado en inicios posteriores; sin embargo, el usuario aún puede tener la opción de ver el acuerdo de licencia de usuario final en cualquier momento.

[0042] Cuando la aplicación de software de cliente se ejecuta en el dispositivo cliente 102 y el usuario elige registrar una nueva cuenta, el cliente proporciona una interfaz de registro. Mientras tanto, el cliente puede verificar si ya existe una cuenta con el número de teléfono del dispositivo cliente 102 (observando que este número de teléfono es probablemente un identificador único para la cuenta) en el servidor de administración de cuentas 106. Si se encuentra una cuenta con el mismo número de teléfono en el servidor de administración de cuentas 106, el cliente puede solicitar al usuario que confirme si desea iniciar sesión en lugar de registrarse. Si el usuario selecciona iniciar sesión, el cliente presenta una interfaz de inicio de sesión; de lo contrario, si el usuario selecciona registrar una nueva cuenta, el cliente presenta una interfaz de registro de cuenta. Además, se observa que en una o más realizaciones se puede usar un identificador único distinto al del dispositivo cliente 102. Por ejemplo, el identificador único puede ser el número de serie del dispositivo cliente 102 o la dirección de control de acceso a medios (MAC, *Media Access Control*).

[0043] Después de que el usuario haya completado el registro correctamente, el cliente puede indicar que el registro del servidor ha sido correcto y puede proporcionar al usuario una opción para configurar y/o iniciar una copia de seguridad de datos. En el caso de un inicio de sesión correcto, el cliente puede consultar al servidor de administración de cuentas 106 para determinar si el usuario tiene una copia de seguridad de los datos existentes que puede restaurarse en el dispositivo cliente 102. Si el usuario tiene una copia de seguridad de los datos existentes válida, el cliente puede preguntar al usuario si desea iniciar una restauración de datos. Además, si el usuario ha realizado una copia de seguridad de los datos, pero los datos no pueden restaurarse en el dispositivo cliente 102 (debido, por ejemplo, a un cambio en el sistema operativo (SO) desde la última copia de seguridad de datos), el usuario puede ser informado de que no se pueden migrar los datos y que el usuario necesita “empezar desde cero” en el dispositivo cliente 102 con respecto a copias de seguridad si el usuario desea continuar con el inicio de sesión. Si el usuario no tiene datos de copia de seguridad existentes, el cliente puede requerir que el usuario realice una copia de seguridad de sus datos, como si se tratara de un usuario que se acaba de registrar.

[0044] En una o más realizaciones, el cliente debe permitir que un nuevo usuario se registre en el sistema 100, y más particularmente, en el servidor de administración de cuentas 106. Durante el registro, se puede solicitar al usuario una dirección de correo electrónico. El cliente y/o el servidor de administración de cuentas 106 pueden validar que la dirección de correo electrónico es una dirección de correo electrónico con formato estándar; como mínimo, el cliente puede verificar la presencia de una arroba, “@”, y servidor de administración de cuentas 106 puede realizar una validación más completa. Además, el servidor de administración de cuentas 106 puede validar la dirección de correo electrónico registrada como única en el sistema 100. Aún más, el cliente puede informar al usuario que se enviará un correo electrónico de validación a la dirección de correo electrónico proporcionada para instar al usuario a introducir una dirección de correo electrónico válida.

[0045] Además, durante el registro, se puede solicitar al usuario una contraseña. Puede requerirse un formato de contraseña que tenga un número mínimo y/o un número máximo de caracteres. Asimismo, se puede solicitar al usuario que introduzca su contraseña para garantizar la entrada correcta de la contraseña. El cliente también puede requerir que la contraseña contenga letras y números.

[0046] Además, durante el registro, se le puede pedir al usuario el nombre del país en el que tiene pensado utilizar el dispositivo cliente 102. Esta acción puede ser respaldada con la presentación una lista desplegable de nombres de países.

[0047] Además, durante el registro, se puede preguntar al usuario si desea recibir mensajes promocionales de marketing y/o de publicidad. En una o más realizaciones, la opción predeterminada puede ser optar por no recibir dichos mensajes.

[0048] También, como se ha descrito anteriormente, se pueden hacer al usuario preguntas de comprobación. En una o más realizaciones, se puede solicitar al usuario que seleccione al menos dos preguntas de comprobación y especifique sus respuestas a las mismas. Por ejemplo, se pueden seleccionar las preguntas de comprobación de entre las siguientes: nombre de la primera escuela; nombre de la primera mascota; nombre de la calle en la que creció; ciudad de nacimiento del padre; ciudad de nacimiento de la madre; nombre de la abuela; marca/modelo; y/o nombre del primer empleador.

[0049] Después de que el usuario haya terminado de introducir la información de registro para una nueva cuenta, el cliente puede comunicar de forma inalámbrica la información de registro al servidor de administración de cuentas 106. Sin embargo, en una o más de otras realizaciones, la información de registro puede comunicarse de forma inalámbrica a medida que se introduce la información de registro. Si el cliente no puede comunicar de forma inalámbrica la información de registro al servidor de administración de cuentas 106 debido a problemas de comunicación o disponibilidad del servidor, el cliente puede presentar un mensaje al usuario pidiéndole que intente registrarse de nuevo más tarde. En tales casos, el usuario puede ser informado de que los valores introducidos se han guardado y que el usuario puede intentarlo de nuevo, por ejemplo, haciendo clic en el botón “reintentar”.

[0050] Además, durante la creación/registro de la cuenta, el dispositivo cliente 102 puede enviar adicionalmente, por ejemplo, los siguientes datos al servidor de administración de cuentas 106: número de teléfono móvil; operadora; una identidad internacional de equipo móvil (IMEI, *International Mobile Equipment Identity*) y/o un número de serie electrónico (ESN, *Electronic Serial Number*); versión de firmware; versión de software; versión de hardware; número de identificación de sincronización ("SyncID"); base de datos de operadora; número de serie del dispositivo; y/o modelo del dispositivo.

[0051] En el caso de una interfaz de inicio de sesión, el cliente puede solicitar al usuario que introduzca un correo electrónico y una contraseña. Después de un cierto número de intentos incorrectos, el usuario puede ser dirigido a preguntas de comprobación. Además, en una o más realizaciones, se puede proporcionar al usuario la opción de ir directamente a preguntas de comprobación en cualquier momento en que se solicite al usuario sus credenciales de inicio de sesión. Si se produce un error en el inicio de sesión, se puede informar al usuario del error de autenticación y se le puede permitir que lo intente de nuevo.

[0052] Se envían el correo electrónico y la contraseña introducidos por el usuario al servidor de administración de cuentas 106 para la validación de la cuenta. Si se encuentra la dirección de correo en el servidor de administración de cuentas 106, el servidor de administración de cuentas 106 puede intentar utilizar el correo electrónico y la contraseña para la validación de la cuenta. Si el correo electrónico se encuentra en el servidor de administración de cuentas 106 y la validación de la cuenta no es correcta debido a la contraseña introducida por el usuario, el cliente puede permitir que el usuario vuelva a introducir la contraseña y puede además proporcionar una opción de restablecimiento de contraseña.

[0053] Además, durante la secuencia de inicio de sesión, se puede verificar el número de teléfono del dispositivo cliente 102, comparándolo con el número de teléfono registrado en la cuenta. Si el número de teléfono tomado del dispositivo cliente 102 no es el mismo que el número de teléfono registrado en la cuenta, el servidor de administración de cuenta 106 puede actualizar la cuenta con este nuevo número de teléfono. Si el cliente no puede recuperar el número de teléfono desde el dispositivo cliente 102, el cliente puede iniciar un servicio de mensajes cortos (SMS) con el servidor de administración de cuentas 106 y verificar el número de teléfono registrado de la cuenta.

[0054] En caso de que el usuario intente transferir una cuenta existente al dispositivo cliente 102 con un nuevo número de teléfono (tomado del dispositivo cliente 102) y el nuevo número de teléfono deseado ya esté asociado con una cuenta activa existente en el sistema 100, el sistema 100 puede intentar transferir el número de teléfono al nuevo usuario utilizando un método de confirmación por SMS.

[0055] Como se ha descrito anteriormente, cuando se solicitan al usuario las credenciales de inicio de sesión, el cliente puede solicitar al usuario que restablezca la contraseña mediante preguntas de comprobación. Para hacer esto, el servidor de administración de cuentas 106 puede identificar al usuario mediante número de teléfono o correo electrónico para determinar con precisión las preguntas y respuestas de comprobación correspondientes. El usuario puede iniciar un restablecimiento de contraseña respondiendo, por ejemplo, al menos a dos preguntas de comprobación que el usuario seleccionó y respondiendo durante el registro, como se ha descrito anteriormente. Además, en una o más realizaciones, el servidor de administración de cuentas 106 puede restringir el número de intentos de restablecimiento a través de preguntas de comprobación permitidos para una cuenta de usuario particular.

[0056] Si el usuario puede responder correctamente a las preguntas de comprobación, se puede solicitar al usuario una nueva contraseña y luego se le puede pedir que confirme la nueva contraseña. Cuando esto ocurre, el servidor de administración de cuentas 106 actualiza, en consecuencia, la contraseña de la cuenta del usuario.

[0057] Si el usuario no puede responder a las preguntas de comprobación correctamente, se puede enviar un correo electrónico a la dirección de correo electrónico registrada del usuario con instrucciones sobre cómo realizar un restablecimiento de contraseña basado en la web. El correo electrónico enviado puede contener un hipervínculo que apunta a un sitio web de restablecimiento de contraseñas. Además, el hipervínculo puede contener un *token* (autentificador) que confirma la identidad del usuario que solicita el restablecimiento de la contraseña. En una o más realizaciones, este *token* solo puede ser válido durante un tiempo limitado y puede ser válido para usarse en un solo restablecimiento de contraseña. Además, se observa que el sitio web de restablecimiento de contraseñas puede ser admitido por navegadores web móviles y de escritorio. Si el usuario es validado mediante un *token* que se ha pasado, el sitio web de restablecimiento de contraseñas puede solicitar al usuario que introduzca y confirme una nueva contraseña. El sitio web de restablecimiento de contraseñas puede permitir al usuario restablecer la contraseña y las preguntas de comprobación como una función combinada. Además, el sitio web de restablecimiento de contraseñas puede confirmar al usuario que la contraseña se ha restablecido si el restablecimiento de la contraseña es correcto. Si se accede al sitio web de restablecimiento de contraseñas desde el dispositivo cliente 102, después de que se complete el restablecimiento de contraseña, el cliente puede realizar un inicio automático en la pantalla de inicio de sesión. Por otro lado, si se accede al sitio web de restablecimiento de contraseñas desde un ordenador de escritorio o portátil, después de que se complete el restablecimiento de contraseña, se puede indicar al usuario que vuelva a iniciar sesión en el dispositivo cliente 102 utilizando la nueva contraseña. Después de restablecer o cambiar la

contraseña, el servidor de administración de cuentas 106 puede enviar un correo electrónico a la dirección de correo electrónico del usuario informándole que se ha actualizado la contraseña e instándole a ponerse en contacto con el servicio de atención al cliente si el usuario no tenía la intención de cambiar la contraseña. Además, después de cualquier restablecimiento o cambio de contraseña, el servidor de administración de cuentas 106 puede hacer expirar todos los *tokens* de restablecimiento de contraseña emitidos previamente para el dispositivo cliente 102.

[0058] En una o más realizaciones, durante un proceso de inicio de sesión, el cliente puede reenviar información del dispositivo. El servidor de administración de cuentas 106 puede entonces registrar esta información. Si el número de teléfono del usuario ha cambiado, el servidor de administración de cuentas 106 puede notificar al usuario que se cambiará el número de teléfono de su cuenta y puede proporcionar al usuario la opción de cancelar el inicio de sesión.

[0059] Después de un registro o inicio de sesión correctos, el cliente puede almacenar en una biblioteca de autenticación 328 un *token* que puede usarse para autenticar el usuario en futuras transacciones con el servidor de administración de cuentas 106. Dicho *token* puede no incluir ningún dato identificable del usuario. Además, dicho *token* puede no ser transferible a otro dispositivo. Aún más, el servidor de administración de cuentas 106 puede ser capaza de hacer expirar el *token* y obligar al usuario a volver a iniciar la sesión. Aún más, los *tokens* previamente existentes se pueden eliminar después de un inicio de sesión o registro correctos.

[0060] Además, el cliente puede detectar si un número de teléfono del dispositivo cliente 102 cambia durante el uso continuo. Si el número de teléfono del dispositivo cliente 102 cambia, el cliente puede hacer expirar un *token* de inicio de sesión anterior y, por lo tanto, requerir que el usuario vuelva a iniciar una sesión.

[0061] En una o más realizaciones, el cliente puede proporcionar al usuario la capacidad de actualizar los datos de usuario (por ejemplo, su nombre, correo electrónico y contraseña). Si el usuario cambia su dirección de correo electrónico, es posible que deba volver a confirmar la nueva dirección de correo electrónico. Además, es posible que el usuario no pueda cambiar una dirección de correo electrónico a una dirección de correo electrónico que ya esté asociada con una cuenta activa.

[0062] Todavía con respecto a la Figura 3, el servidor de administración de cuentas 106 incluye un módulo de eliminación de cuentas 308 que proporciona la eliminación de cuentas. La eliminación de la cuenta puede producirse al enviar un correo electrónico iniciado por un operador o el administrador a la dirección de correo electrónico registrada del usuario y solicitar al usuario que haga clic en un enlace en el correo electrónico. Después de eliminar una cuenta con este mecanismo, el servidor de administración de cuentas 106 puede enviar un correo electrónico de confirmación al usuario informándole que su cuenta ha sido eliminada.

[0063] El servidor de administración de cuentas 106 también incluye un modelo de estado de cuenta 302. El modelo de estado de cuenta 302 corresponde al motor de estado 214 mostrado en la Figura 2. En general, en una o más realizaciones, el servidor de administración de cuentas 106 puede asociar un estado de cuenta con cada una de una pluralidad de cuentas registradas en el servidor de administración de cuentas 106.

[0064] Por lo que respecta ahora a la Figura 4, se puede denominar “Estado 0” a un estado “inactivo pendiente de verificación de número de teléfono”. Cuando el número de teléfono registrado de una cuenta recién registrada o con respecto a la cual se acaba de iniciar sesión existe en otra cuenta activa, la nueva cuenta puede colocarse en el Estado 0. Además, si el cliente no puede recuperar un número de teléfono para una cuenta recién registrada, se puede colocar la nueva cuenta en el Estado 0. Además, en una o más realizaciones, el servidor de administración de cuentas 106 puede permitir que el cliente se autentique con una cuenta que se encuentra en el Estado 0, pero puede no permitirse ninguna otra funcionalidad hasta que se produzca la verificación del número de teléfono. Después de la verificación correcta del número de teléfono, una cuenta en el Estado 0 puede pasar al Estado A (como se describe en mayor detalle más adelante). Si un proceso de verificación de número de teléfono no se ha completado correctamente dentro de un periodo de tiempo predeterminado (por ejemplo, 7 días), una cuenta en el Estado 0 puede pasar al Estado D (como se describe en mayor detalle más adelante).

[0065] Todavía con respecto a la Figura 4, se puede denominar “Estado A” al estado “activo pendiente de verificación”. Una cuenta recién registrada puede estar en el Estado A si su número de teléfono registrado no está ya en otra cuenta (es decir, no se encuentra en el Estado 0). Además, el servidor de administración de cuentas 106 puede permitir que el cliente se autentique con una cuenta que se encuentra en el Estado A, pero puede que no se permita cierta funcionalidad. Por ejemplo, una cuenta en el Estado A puede ser capaz de realizar una copia de seguridad de los datos, pero es posible que no pueda realizar las funcionalidades de restauración de datos y de inutilización y bloqueo (como se describe en mayor detalle más adelante). Después de la verificación correcta del número de teléfono y el correo electrónico, una cuenta en el Estado A puede pasar al Estado B (como se describe en mayor detalle más adelante). Si no se ha completado un proceso de verificación de número de teléfono o correo electrónico dentro de un periodo de tiempo predeterminado (por ejemplo, 7 días), una cuenta en el Estado A puede pasar al Estado D (como se describe en mayor detalle más adelante). Además, si el usuario se pone en contacto con un operador, administrador

o agente de atención al cliente para eliminar su cuenta, una cuenta en el Estado A puede pasar al Estado E (como se describe en mayor detalle más adelante) utilizando el módulo de eliminación de cuentas 308 descrito anteriormente.

[0066] Con respecto aún al diagrama de transición de estados mostrado en la Figura 4, un “Estado B” puede denominarse un estado “activo”. En general, una cuenta en el Estado B ha completado correctamente los procesos de verificación de número de teléfono y correo electrónico. En una o más realizaciones, el servidor de administración de cuentas 106 puede permitir que el cliente se autentique con una cuenta que se encuentra en el Estado B. Además, el servidor de administración de cuentas 106 puede permitir que el cliente realice funcionalidades de copias de seguridad y restauración de datos e inutilización y bloqueo (como se describe en mayor detalle más adelante) si la cuenta se encuentra en el Estado B. Una cuenta en el Estado B puede pasar al Estado C (como se describe en mayor detalle más adelante) cuando se cambia un número de teléfono o una dirección de correo electrónico asociados (por ejemplo, cuando se transfirió una cuenta a un nuevo número o el usuario cambió la dirección de correo electrónico de la cuenta). Si el usuario se pone en contacto con el operador, el administrador o el agente de atención al cliente para eliminar su cuenta, una cuenta en el Estado B puede pasar al Estado E (como se describe en mayor detalle más adelante) utilizando el módulo de eliminación de cuentas 308 descrito anteriormente.

[0067] Todavía con respecto a la Figura 4, se puede denominar un “Estado C” a un estado “activo pendiente de nueva verificación”. En una o más realizaciones, una cuenta en el Estado C solo puede proceder del Estado B, como se muestra en la Figura 4. Además, el servidor de administración de cuentas 106 puede permitir que el cliente se autentique con una cuenta que se encuentra en el Estado C. Además, el servidor de administración de cuentas 106 puede permitir que el cliente lleve a cabo funcionalidades de copia de seguridad y restauración de datos e inutilización y bloqueo (como se describe en mayor detalle más adelante) si la cuenta se encuentra en el Estado C. Después de la verificación correcta del número de teléfono y el correo electrónico, una cuenta en el Estado C puede pasar al Estado B. Si la verificación del número de teléfono o correo electrónico no se produce dentro de un periodo predeterminado de tiempo (por ejemplo, 7 días), una cuenta en el Estado C puede pasar al Estado D (como se describe en mayor detalle más adelante). Si el usuario se pone en contacto con el operador, el administrador o el agente de atención al cliente para eliminar su cuenta, una cuenta en el Estado C puede pasar al Estado E (como se describe en mayor detalle más adelante) utilizando el módulo de eliminación de cuentas 308 descrito anteriormente.

[0068] Con respecto aún al diagrama de transición de estados mostrado en la Figura 4, un “Estado D” puede denominarse un estado “bloqueado”. Una cuenta que no ha completado el proceso de verificación de número de teléfono y correo electrónico dentro de un periodo de tiempo predeterminado (por ejemplo, 7 días) puede pasar al Estado D. En una o más realizaciones, el servidor de administración de cuentas 106 puede permitir que el cliente se autentique con una cuenta que se encuentra en el Estado D, pero determinadas funcionalidades pueden no estar permitidas. Por ejemplo, una cuenta en el Estado D puede no ser capaz de llevar a cabo funcionalidades de copia de seguridad y restauración de datos e inutilización y bloqueo (como se describe en mayor detalle más adelante). Además, después de que el usuario inicie y complete correctamente la verificación de número de teléfono y correo electrónico, una cuenta en el Estado D puede pasar al Estado B.

[0069] Todavía con respecto a la Figura 4, puede denominarse un “Estado E” a un estado “deshabilitado/eliminado”. El servidor de administración de cuentas 106 puede cambiar una cuenta al Estado E si el usuario ha solicitado eliminar su cuenta utilizando el módulo de eliminación de cuentas 308 descrito anteriormente. Además, el servidor de administración de cuentas 106 puede no permitir que el cliente se autentique con una cuenta que se encuentra en el Estado E. Además, una cuenta en el Estado E puede no ser capaz de llevar a cabo funcionalidades de copia de seguridad y restauración de datos e inutilización y bloqueo (como se describe en mayor detalle más adelante)) Además, el servidor de administración de cuentas 106 puede eliminar la información de registro de usuario y los datos de copia de seguridad de una cuenta en el Estado E. En una o más realizaciones, los datos de los que se ha hecho una copia de seguridad pueden ser completamente irrecuperables.

[0070] Por lo que respecta ahora de forma más general a la Figura 4, el servidor de administración de cuentas 106 puede cambiar una cuenta al Estado 0 cuando el usuario transfiere su número de teléfono y ese número de teléfono existe en otra cuenta. Además, el servidor de administración de cuentas 106 puede cambiar una cuenta de la siguiente manera si el usuario transfiere su número de teléfono y ese número de teléfono no está en otra cuenta: Estados 0 y A pasan a Estado A; Estado B pasa a Estado C; Estado C permanece en Estado C; y Estado D permanece en Estado D.

[0071] Además, en una o más realizaciones, el servidor de administración de cuentas 106 puede verificar que una dirección de correo electrónico y/o un número de teléfono enviados recientemente (observándose que un número de teléfono se toma directamente del dispositivo cliente 102 y no es introducido por el usuario) es único en todo el sistema 100. Si el usuario intenta registrar una cuenta utilizando una dirección de correo electrónico que se ha verificado anteriormente, se puede informar al usuario que la dirección de correo electrónico ya se está utilizando y se le pueden presentar opciones de restablecimiento de contraseña (en cuyo caso se supone que el usuario debe iniciar sesión, no registrarse). Si el usuario intenta registrar una cuenta utilizando un número de teléfono que ya está asociado con otra cuenta activa existente (en los Estados A, B o C), el servidor de administración de cuentas 106 puede permitir que el

usuario se registre y luego puede marcar la cuenta como Estado 0 hasta que se confirme el número de teléfono. Si el número de teléfono se confirma mediante, por ejemplo, un mensaje SMS, se puede eliminar el número de teléfono de una cuenta anterior y la cuenta se puede colocar en el Estado 0. El cliente puede permitir que el usuario "recupere" su cuenta iniciando un proceso de verificación de SMS, como se describe más adelante. Se puede enviar un correo electrónico a la cuenta anterior notificando al usuario que el número de teléfono se ha transferido a una cuenta nueva. Si el número de teléfono no puede confirmarse mediante un mensaje SMS, la cuenta puede ser deshabilitada.

[0072] Después de un registro correcto, el cliente puede enviar un mensaje SMS de confirmación al servidor de administración de cuentas 106 para verificar su número de teléfono. El mensaje SMS puede contener suficiente información de identificación y autenticación de cuenta para que el servidor de administración de cuentas 106 realice una o más comprobaciones de seguridad necesarias. Si el servidor de administración de cuentas 106 no recibe la confirmación por SMS, el servidor de administración de cuentas 106 puede notificar al cliente para solicitar al usuario que vuelva a enviar el mensaje SMS periódicamente hasta que se reciba el mensaje de confirmación SMS.

[0073] Si el servidor de administración de cuentas 106 no recibe confirmación durante un periodo de tiempo específico después del registro, el servidor de administración de cuentas 106 puede cambiar el estado de la cuenta al Estado D. Si la cuenta del usuario está deshabilitada porque el número de teléfono no puede confirmarse, el cliente puede dirigir al usuario a un sitio web de soporte técnico. Más en concreto, por ejemplo, el cliente puede notificar al usuario a través de una alerta de que su cuenta ha sido desactivada y puede dirigir al usuario a un sitio web de soporte técnico.

[0074] Después de que se introduce un nuevo correo electrónico mediante un nuevo registro o mediante un cambio de dirección de correo electrónico iniciado por el usuario, el servidor de administración de cuentas 106 puede validar esa dirección de correo electrónico. El servidor de administración de cuentas 106 puede enviar un mensaje de correo electrónico a la nueva dirección de correo electrónico solicitando al usuario que confirme la dirección. El mensaje de correo electrónico puede incluir un hipervínculo con un *token* que el usuario puede seleccionar para establecer un vínculo con un sitio web de confirmación de correo electrónico. El sitio web de confirmación de correo electrónico puede ser admitido por navegadores web de escritorio y móviles. Si transcurre un periodo de tiempo predeterminado y el usuario aún no ha confirmado la dirección de correo electrónico, el cliente puede notificar al usuario a través de una alerta que la dirección de correo electrónico no ha sido verificada. El cliente puede dar al usuario la opción de volver a introducir la dirección de correo electrónico en este momento. Además, el cliente puede proporcionar al usuario una opción para que se le reenvíe un correo electrónico de confirmación. Además, el cliente puede aconsejar al usuario que revise las carpetas y los filtros de correo electrónico no deseado o *spam* si el correo electrónico aún no se ha recibido.

[0075] Si transcurre otro periodo de tiempo predeterminado y el usuario aún no ha confirmado la dirección de correo electrónico, el servidor de administración de cuentas 106 puede cambiar la cuenta del usuario al Estado D. En este caso, el cliente puede notificar al usuario que el cliente está deshabilitado hasta que se verifique la dirección de correo electrónico. Además, el cliente puede dar al usuario la opción de volver a introducir la dirección de correo electrónico en este momento. Aún más, el cliente puede proporcionar al usuario una opción para que se le reenvíe un correo electrónico de confirmación. Además, el cliente puede aconsejar al usuario que revise las carpetas y los filtros de correo electrónico no deseado si el correo electrónico aún no se recibe. Si el usuario puede completar un restablecimiento de contraseña por correo electrónico, como se ha descrito anteriormente, antes de acceder al enlace de verificación de correo electrónico, el servidor de administración de cuentas 106 puede marcar el proceso de verificación de correo electrónico como completado.

[0076] Por lo que respecta de nuevo a la Figura 3, el servidor de administración de cuentas 106 incluye un módulo de administrador de latidos 312. El módulo de administrador de latidos 312 corresponde al motor de latidos 212 mostrado en la Figura 2. En la Figura 5 se muestra más particularmente un subsistema asociado con el módulo de administrador de latidos 312.

[0077] Por lo general, un componente del lado del cliente envía lo que se conoce como "ping" o "latido" a un servidor para que el servidor sepa que el componente del lado del cliente está activo y funcionando. Tales pings convencionales son enviados periódicamente y regularmente por el componente del lado del cliente. Aquí, en una o más realizaciones, en general, el dispositivo cliente 102 envía pings a una frecuencia y/o formato especificados y cambiables dinámicamente por el servidor de administración de cuentas 106.

[0078] Como se muestra en la Figura 5, el dispositivo cliente 102 tiene un módulo de actualización 340 que se utiliza para recuperar y recibir actualizaciones del servidor de administración de cuentas 106. Estas actualizaciones pueden ser, por ejemplo, actualizaciones del sistema operativo, actualizaciones de seguridad, actualizaciones de servicio, actualizaciones de aplicaciones, actualizaciones de datos, actualizaciones de bibliotecas, actualizaciones de controladores y/o actualizaciones de protocolos de comunicación. El módulo de actualización 340 busca actualizaciones mediante el uso de lo que se denomina "pings" o "latidos", como se ha descrito anteriormente. En una o más realizaciones, dichos latidos pueden estar especialmente formateados o pueden ser simplemente solicitudes

HTTP estructuradas. En una o más realizaciones adicionales, los latidos pueden comunicarse a través de mensajes SMS. En aún una o más realizaciones adicionales, los latidos pueden comunicarse a través de uno o más canales de datos y/o voz disponibles.

[0079] En general, una aplicación del dispositivo cliente 102 puede intentar buscar actualizaciones en el servidor de administración de cuentas 106 de forma regular o periódica (por ejemplo, diariamente) para ver si hay una o más actualizaciones disponibles y registrar un "latido" con el servidor de administración de cuentas 106. Por consiguiente, el dispositivo cliente 102 puede tener una biblioteca (no mostrada) que administra la programación para un proceso de latido. Como parte de sus latidos, el cliente puede proporcionar información de identidad al servidor de administración de cuentas 106. Además, por ejemplo, el latido puede incluir información sobre una versión de software utilizada por el dispositivo cliente 102, el tiempo de un último intento de copia de seguridad de datos, un estado de verificación de correo electrónico, un estado de verificación de SMS, información del estado de la cuenta, un *token* de identidad de la cuenta y/o el siguiente latido programado.

[0080] El ping del dispositivo cliente 102, empaquetado y dependiente de una biblioteca de latidos 336, es recibido por el módulo de administrador de latidos 312 que reside en el servidor de administración de cuentas 106. Si hay una actualización disponible para el dispositivo cliente 102, el módulo de administrador de latidos 312 envía consiguientemente la actualización al módulo de actualización 340 para que el dispositivo cliente 102 la procese/ejecute.

[0081] El servidor de administración de cuentas 106 está conectado operativamente a un almacén de datos de tiempos de retraso 502 o contiene dentro de sí un almacén de datos de tiempos de retraso 502. El almacén de datos de tiempos de retraso 502 incluye una colección de tiempos de retraso configurables y/o predeterminados. Estos tiempos de retraso, configurables a través de un módulo de configuración de retraso 504, son utilizados por el módulo de administrador de latidos 312 para indicar al dispositivo cliente 102 cómo y cuándo el dispositivo cliente 102 debe enviar pings futuros. Por ejemplo, la respuesta del módulo de administrador de latidos 312 puede incluir información en su respuesta sobre cuánto tiempo debe esperar el dispositivo cliente 102 antes de intentar un próximo ping. Si el cliente no puede realizar un latido en un momento solicitado por algún motivo, puede cancelar ese latido y volver a intentarlo de nuevo en la frecuencia predeterminada (por ejemplo, a diario). En consecuencia, al controlar una frecuencia de ping, el servidor de administración de cuentas 106 puede, por ejemplo, ralentizar los pings del dispositivo cliente 102 si el servidor de administración de cuentas 106 está experimentando una alta carga de tráfico (por ejemplo, una mayor demanda interna o externa de recursos informáticos).

[0082] Además, la respuesta del módulo de administrador de latidos 312 puede incluir información en su respuesta sobre cómo se debe enviar un próximo ping desde el dispositivo cliente 102. Por ejemplo, el módulo de administrador de latidos 312 puede indicar al dispositivo cliente 102 que debe producirse un próximo ping a través de un mensaje SMS en lugar de una solicitud HTTP. En otro ejemplo, el módulo de administrador de latidos 312 puede indicar al dispositivo cliente 102 que se debe enviar un próximo ping a través de un canal de voz particular en lugar de por una solicitud HTTP. De esta manera, por ejemplo, se pueden enviar latidos desde el dispositivo cliente 102 en una red alternativa (por ejemplo, una red wifi), incluso si una red inicialmente seleccionada (por ejemplo, una red de telefonía móvil) no está disponible. Por lo tanto, en general, un componente del lado del servidor (en el presente, el servidor de administración de cuentas 106) controla el latido de un componente del lado del cliente (en el presente, el dispositivo cliente 102). Además, al administrar los latidos del dispositivo cliente 102 y saber cuándo se espera recibir latidos del dispositivo cliente 102, el servidor de administración de cuentas 106 puede usarse para realizar un seguimiento de si el dispositivo cliente 102 está funcionando y "vivo" (por ejemplo, está operativo y/o activo).

[0083] En una o más realizaciones, el tiempo de retraso especificado en una respuesta al dispositivo cliente 102 puede variar según la operadora, el grupo, el dispositivo y/o la plataforma. Por ejemplo, un tiempo de retraso en una respuesta a un dispositivo cliente 102 que forma parte de un primer grupo puede ser mayor que un tiempo de retraso especificado en una respuesta a otro dispositivo cliente (no mostrado) que forma parte de otro grupo. Como se ha descrito anteriormente, los tiempos de retraso pueden almacenarse en el almacén de datos de tiempos de retraso 502. Uno o más de estos tiempos de retraso pueden tener valores predeterminados y, además, uno o más de estos tiempos de retraso pueden ajustarse dinámicamente según las necesidades y/o los objetivos de rendimiento.

[0084] Además, en una o más realizaciones, una respuesta del módulo de administrador de latidos 312 puede indicar al dispositivo cliente 102 un desencadenador de eventos que debería hacer que el dispositivo cliente 102 enviara un latido. Por ejemplo, el módulo de administrador de latidos 312 puede indicar que cuando el dispositivo cliente 102 envía un correo electrónico saliente, el dispositivo cliente 102 en ese momento también debe enviar un latido al servidor de administración de cuentas 106. En otro ejemplo, el módulo de administrador de latidos 312 puede indicar que el dispositivo cliente 102 debería enviar un latido cada vez que se envía un mensaje SMS desde el dispositivo cliente 102.

[0085] Cuando se indica que una actualización está disponible, el cliente puede preguntarle al usuario si desea descargar e instalar la actualización. Por ejemplo, el cliente puede notificar al usuario a través de una alerta que guía

al usuario al cuadro de diálogo de una aplicación. Además, en una o más realizaciones, si se detecta una actualización, el cliente puede no permitir intentos de realizar actividades adicionales del servidor hasta que se instale la actualización. Además, si hay una actualización disponible, el cliente puede preguntarle al usuario si desea descargar e instalar la actualización de inmediato o desea que se le recuerde que debe descargar la actualización más tarde. Si el usuario elige descargar e instalar la actualización inmediatamente, el cliente puede descargar e instalar la actualización en segundo plano (por ejemplo, el usuario aún puede usar la funcionalidad de teléfono del dispositivo cliente 102 sin ser interrumpido). Si el usuario elige que se le recuerde que debe realizar la actualización más tarde (por ejemplo, después de que haya pasado un número determinado de días), el cliente puede volver a preguntarle al usuario en ese momento. Además, por ejemplo, después de proporcionar un número específico de recordatorios, el cliente puede informar al usuario que no se lo recordará de nuevo y que el usuario deberá descargar e instalar la actualización manualmente. Además, en una o más realizaciones, el cliente puede proporcionar una configuración de preferencias para permitir que se descarguen actualizaciones futuras sin preguntar al usuario.

Servidor de aplicaciones web

[0086] En la Figura 6 se muestra un diagrama del servidor de aplicaciones web 104 y el dispositivo cliente 102 de acuerdo con una realización de la presente invención. El servidor de aplicaciones web 104 puede alojar un sitio web de escritorio 602 y/o un sitio web móvil 604 para proporcionar información sobre un producto, servicio y conjunto de aplicaciones de administración ofrecido por el sistema 100 a un usuario del dispositivo cliente 102. En otras palabras, una entidad, por ejemplo, un proveedor de servicios, fabricante de dispositivos y/o minorista, puede confiar al sitio web de escritorio 602 y/o el sitio web móvil 604 la transmisión pública de información sobre los productos y/o servicios ofrecidos por el sistema 100.

[0087] El servidor de aplicaciones web 106 también incluye un componente de transporte HTTP/S 614 y un componente de transporte SMS 616 para interactuar respectivamente con el componente de transporte HTTP/S 318 y el componente de transporte SMS 320 que residen en el dispositivo cliente 102. Estos componentes de transporte 614, 616, 318 y 320 pueden admitir, por ejemplo, una o varias de las diversas comunicaciones admitidas entre el dispositivo cliente 102 y el servidor de administración de cuentas 106.

[0088] Para que el dispositivo cliente 102 tenga la funcionalidad descrita en el presente, puede ser necesario que el dispositivo cliente 102 tenga instalado el software de cliente apropiado. En una o más realizaciones, el usuario puede acceder al sitio web de escritorio 602 y/o al sitio web móvil 604. El usuario introduce su número de teléfono móvil y operadora y solicita el software de cliente (véase, por ejemplo, la Figura 20). A su vez, el usuario recibe un mensaje SMS en el dispositivo cliente 102, donde el mensaje SMS puede incluir un enlace web a una página de descarga móvil (véase, por ejemplo, la Figura 21), posiblemente admitida por un módulo de descarga de cliente 606 residente en el servidor de aplicaciones web 104. El usuario puede hacer clic en el enlace web y se inicia el navegador móvil del usuario. A continuación, el usuario puede ser llevado a un sitio de descarga móvil que detecta el sistema operativo del dispositivo cliente 102 y comienza la descarga del instalador de cliente apropiado (véanse, por ejemplo, las Figuras 22 y 23). El instalador de cliente se ejecuta en el dispositivo cliente 102 tras la descarga (véase, por ejemplo, la Figura 24). Posteriormente, el cliente se inicia después de la instalación y registro/inicio de sesión, como se ha descrito anteriormente.

[0089] Además, en una o más realizaciones, el cliente puede instalarse a través de un dispositivo de almacenamiento en el que está almacenado el software de cliente disponible para la instalación. Por ejemplo, en una o más realizaciones, el dispositivo de almacenamiento puede ser una tarjeta SD (*Secure Digital*). En ese caso, se puede proporcionar al usuario una tarjeta SD que contiene un instalador de cliente para un sistema operativo del dispositivo cliente 102. A continuación, el usuario inserta la tarjeta SD en el dispositivo cliente 102, y el dispositivo cliente 102 a su vez realiza la instalación apropiada. Tras la instalación, el cliente se inicia y se le puede solicitar al usuario que realice el registro/inicio de sesión, como se ha descrito anteriormente.

[0090] Aún más, en una o más realizaciones, el cliente puede descargarse e instalarse a través de un sitio web móvil. En tal caso, el usuario puede abrir un navegador web en el dispositivo cliente 102. El usuario puede entonces navegar al sitio web apropiado para descargar el cliente. El usuario puede elegir comenzar la descarga del cliente. Además, en una o más realizaciones, la página de descarga móvil puede detectar el sistema operativo del dispositivo cliente 102 y entregar el instalador de cliente apropiado. El instalador de cliente puede ejecutarse en el dispositivo cliente 102 después de la descarga. El cliente, por consiguiente, se instala y comienza el registro/inicio de sesión, como se ha descrito anteriormente.

[0091] Como se ha descrito anteriormente, el servidor de aplicaciones web 104 puede transmitir información de productos y/o servicios con respecto al sistema 100. Además, el servidor de aplicaciones web 104 puede facilitar la distribución de un instalador de cliente a través de un mensaje SMS. Además, el servidor de aplicaciones web 104 puede proporcionar una interfaz para que el usuario envíe el número de teléfono móvil y la operadora del usuario. Aún más, el servidor de aplicaciones web 104 puede incluir un mecanismo para evitar que usuarios malintencionados envíen mensajes SMS repetidos.

[0092] Como se ha descrito anteriormente, una vez que el usuario ha introducido un número de teléfono móvil y una operadora, el servidor de aplicaciones web 104 puede enviar un mensaje SMS al dispositivo cliente 102, donde el mensaje SMS incluye un enlace a un sitio de aterrizaje móvil. En una o más realizaciones, el servidor de aplicaciones web 104 puede utilizar un agregador de SMS (no mostrado) para enviar mensajes SMS. Después de que se envía un mensaje SMS, el servidor de aplicaciones web 104 puede proporcionar al usuario información sobre los próximos pasos que el usuario tomará: recibir el SMS y realizar el proceso de instalación del cliente.

[0093] En una o más realizaciones, el sitio web móvil 604 puede ser capaz de determinar un sistema operativo del dispositivo cliente 102. El sitio web móvil 604 puede proporcionar la descarga directa del instalador de cliente apropiado para el dispositivo cliente 102 a través de un sitio de descarga móvil. Además, el sitio web móvil 604 puede proporcionar un sitio de descarga móvil para entregar una descarga móvil y servir como destino para enlaces SMS enviados a usuarios desde el sitio web de escritorio 602. Además, en una o más realizaciones, el sitio de descarga móvil puede comenzar automáticamente la descarga de un instalador apropiado al dispositivo cliente 102. En tales casos, el sitio de descarga móvil puede detectar el sistema operativo del dispositivo cliente 102.

[0094] Asimismo, en una o más realizaciones, la aplicación cliente y los archivos de componentes relacionados pueden entregarse en forma de un instalador de cliente autoextraíble que puede ejecutarse en el dispositivo cliente 102. Más en concreto, en una o más realizaciones, el instalador de cliente puede comprobar si hay suficiente memoria en el dispositivo cliente 102 antes de realizar la instalación. Además, el instalador de cliente puede realizar comprobaciones para asegurarse de que el dispositivo cliente 102 sea un tipo de dispositivo admitido. También, el instalador de cliente puede detectar qué componentes ya están en el dispositivo cliente 102 y puede no sobrescribir ninguna información del usuario o componentes del cliente preexistentes a menos que se actualicen componentes particulares. Además, como se ha descrito anteriormente, el instalador de cliente puede ejecutarse, por ejemplo, desde el dispositivo cliente 102 o desde un dispositivo de almacenamiento (por ejemplo, una tarjeta SD). Además, el instalador de cliente puede eliminarse automáticamente del dispositivo cliente 102 (pero no del dispositivo de almacenamiento) después de una instalación correcta.

[0095] Por lo que respecta aún a la Figura 6, el servidor de aplicaciones web 104 incluye un módulo administrador de recursos 608. En la Figura 7 se muestra un subsistema asociado con el módulo administrador de recursos 608. En general, la administración de recursos, como se describe más adelante, facilita uno o más servicios mediante los cuales los recursos de datos a los que hacen referencia las aplicaciones de software residentes en los dispositivos cliente servidos por el sistema 100 pueden actualizarse a nivel del servidor y transmitirse a los dispositivos cliente basándose, por ejemplo, en el tipo de dispositivo, la operadora y/o el grupo.

[0096] El servidor de aplicaciones web 104 está conectado operativamente a un almacén de datos de recursos 702, o contiene dentro de sí mismo un almacén de datos de recursos 702. El almacén de datos de recursos 702 incluye recursos como, por ejemplo, cadenas de texto, mapas de bits, códigos, imágenes, cadenas de caracteres y/o metadatos, los cuales pueden usarse en conexión con aplicaciones o interfaces de usuario en el dispositivo cliente 102. En general, un recurso es cualquier forma de datos estáticos.

[0097] Durante el uso y la operación del dispositivo cliente 102 se pueden producir errores específicos o situaciones desconocidas. Cuando se produce tal error o situación desconocida, el usuario del dispositivo cliente 102 puede registrar el error con un componente basado en el servidor. Por ejemplo, el usuario puede acceder a un departamento de soporte técnico o proporcionar comentarios de garantía de calidad. La información proporcionada por el usuario puede ponerse a disposición de un administrador (u operador o agente de servicio de atención al cliente) que tenga acceso al módulo de configuración de recursos 704 que se muestra en la Figura 7. El administrador puede entonces determinar si el error indicado por el usuario es frecuente y/o significativo en relación con otros tipos de errores. El administrador también puede asignar el error a un recurso particular almacenado en el almacén de datos de recursos 702.

[0098] De manera regular o periódica (por ejemplo, en función de algún proceso programado), el módulo administrador de recursos 608 puede generar automáticamente un paquete de recursos para su despliegue en el dispositivo cliente 102 (y en otros dispositivos cliente). De esta forma, el paquete de recursos se genera automáticamente para incluir recursos a los que se hace referencia con frecuencia. En otras palabras, el paquete de recursos puede generarse automáticamente para incluir recursos “imprescindibles” para el dispositivo cliente 102. El archivo de recursos puede enviarse al dispositivo cliente 102 por vía aérea a través de, por ejemplo, un mensaje SMS. Los expertos en la materia observarán que tal mecanismo de generación y envío de archivos de recursos de generación automática evita la necesidad de que el dispositivo cliente 102 sea enviado o inicialmente instalado con una multitud de recursos que consumen recursos (que generalmente incluyen texto, gráficos, encabezados de interfaz de usuario o cualquier otra cosa que pueda mostrarse), algunos de los cuales el dispositivo cliente 102 puede no necesitar posteriormente. Por lo tanto, al menos en un aspecto, los recursos se añaden al dispositivo cliente 102 “según sea necesario”.

[0099] Cuando un archivo de recursos del módulo administrador de recursos 608 es recibido por vía aérea en el dispositivo cliente 102, se activa un módulo de actualización 340 para recibir una notificación de que hay una actualización disponible. El módulo de actualización 340 a continuación toma el archivo de recursos y lo instala en la biblioteca de textos 330, de modo que cuando el dispositivo cliente 102 indica posteriormente un error (de un tipo que se ha experimentado previamente), un recurso correspondiente a ese error está disponible para su uso en la biblioteca de textos 330.

[0100] En la Figura 8 se muestra un proceso de flujo de un proceso de administración de recursos de acuerdo con una realización de la presente invención. El proceso comienza cuando, en el cliente, se indica un error 850. Si un recurso está disponible localmente para ese error (determinado, por ejemplo, a través de la referencia a la biblioteca de textos 330) 852, la operación del cliente continúa haciendo referencia a ese recurso 854.

[0101] Si un recurso para un error indicado no está disponible 852, se notifica al servidor 856 la aparición de ese error. Dicha notificación puede ocurrir a través de uno o más de varios mecanismos. Por ejemplo, el usuario puede enviar una notificación del error por correo electrónico o mensaje SMS. En otro ejemplo, el usuario puede acceder a una página web específica para registrar el error con un administrador.

[0102] Una vez que se recibe la notificación de la aparición del error a nivel del servidor, se identifica 858 la asignación del recurso o los recursos a ese error. Si el servidor no determina que el error se produce con frecuencia 860, esos recursos asignados al error recibido pueden enviarse al cliente 862, con lo cual el cliente instala los recursos recibidos 864 y la operación del cliente continúa haciendo referencia al recurso o a los recursos apropiados 854. Sin embargo, si se determina que el error ocurre con frecuencia 860, el servidor marca el recurso o los recursos apropiados para que se incluyan en la siguiente compilación del archivo de recursos 866. A continuación, en el momento programado apropiadamente, el archivo de recursos se genera automáticamente 868 y se envía al cliente, después de lo cual el cliente instala el archivo de recursos 870 y la operación del cliente procede a hacer referencia al recurso o a los recursos apropiados 854.

[0103] Refiriéndose de nuevo a la Figura 7, en una o más realizaciones, el dispositivo cliente 102 puede realizar una recuperación de recursos “previa petición”. Por ejemplo, si se produce una ocurrencia continua o frecuente de un tipo particular de error, el dispositivo cliente 102 puede, a través del módulo administrador de recursos 608, recuperar el recurso o los recursos apropiados del almacén de datos de recursos 702. En otras palabras, el dispositivo cliente 102 puede realizar un seguimiento de cuántas veces se produce un tipo específico de error sin estar en una compilación de archivo de recursos enviada desde el módulo administrador de recursos 608. Cuando se alcanza un umbral de ocurrencias de ese error, el dispositivo cliente 102 solicita y obtiene el recurso o los recursos apropiados del almacén de datos de recursos 702. Además, cuando recupera el recurso, ese recurso puede ser “marcado” como utilizado con frecuencia, de modo que el recurso se incluya en la próxima generación automática de un archivo de recursos.

[0104] Además, en una o más realizaciones, el dispositivo cliente 102 puede recuperar un recurso y no marcar el recurso como utilizado frecuentemente. En tal caso, ese recurso puede ser supervisado para determinar la frecuencia con la que se solicita/recupera, y se puede enviar una alerta a un administrador si una tendencia de solicitudes para el recurso indica que ese recurso debe incluirse en la próxima compilación del archivo de recursos. Además, los expertos en la materia observarán que en una o más de las otras realizaciones, se puede automatizar el proceso de supervisar las tendencias de solicitud de recursos y determinar si se incluye el recurso en la compilación de un archivo de recursos.

[0105] Además, los recursos en el almacén de datos de recursos 702 pueden personalizarse en función de, por ejemplo, la operadora, el grupo, el tipo de dispositivo y/o el conjunto de aplicaciones. Por ejemplo, si el dispositivo cliente 102 pertenece a un determinado grupo que tiene un dominio informático más bajo que otro grupo, entonces un recurso asociado con un mensaje de error puede ajustarse para proporcionar instrucciones de error más detalladas, en comparación con otro grupo que se considera que tiene un mayor dominio informático. Por lo tanto, de esa forma los códigos de error pueden asignarse dinámicamente a recursos específicos.

[0106] Haciendo referencia de nuevo a la Figura 6, el servidor de aplicaciones web 104 incluye un módulo de bloqueo del dispositivo 610 y un módulo de borrado del dispositivo 612. En la Figura 9 se muestra un subsistema asociado con el módulo de bloqueo del dispositivo 610 y el módulo de borrado del dispositivo 612. En general, estos módulos 610 y 612, junto con los módulos homólogos en el dispositivo cliente 102 que se describen más adelante en mayor detalle, facilitan los servicios de “inutilización (*kill pill*) y bloqueo” proporcionados por el sistema 100. La disponibilidad de uno o más de estos servicios puede resultar útil, por ejemplo, si el usuario pierde, extravía o se encuentra lejos del dispositivo cliente 102. Puede haber datos de usuario en el dispositivo cliente 102 a los que el usuario quiera restringir el acceso en una situación en la que el usuario no esté en posesión o control directo del dispositivo cliente 102. Por lo tanto, en tales casos, los servicios de “inutilización y bloqueo” que se describen a continuación permiten al usuario restringir de forma remota la accesibilidad a los datos de usuario almacenados en el dispositivo cliente 102 sin tener que desactivar completamente el dispositivo cliente 102 o desactivar una cuenta

asociada con el dispositivo cliente 102. Entre los ejemplos de datos de usuario figuran los datos de calendario, los datos de contactos, los datos de tareas, los datos de notas, los datos de marcadores de navegador, los datos de acceso directo para la aplicación del teléfono (por ejemplo, los datos de números de marcación rápida), los datos de registro de llamadas, los datos de configuración de aplicaciones y los datos del historial de mensajes SMS.

[0107] Una vez que el usuario completa el registro, como se ha descrito anteriormente, se puede informar al usuario que el dispositivo cliente 102 ahora está activado para el servicio de inutilización y bloqueo. Se puede realizar un bloqueo de dispositivo remoto utilizando el módulo de bloqueo del dispositivo 610 a través de una interfaz de usuario de inutilización y bloqueo 804. Para hacerlo, en una o más realizaciones, el usuario (o un administrador) puede acceder al sitio web de escritorio 602, introducir su número de teléfono y contraseña de cuenta, y elegir una opción de bloqueo de dispositivo. El usuario puede tener la opción de enviar un mensaje al dispositivo cliente 102, donde este mensaje puede mostrarse siempre que alguien intente acceder al dispositivo cliente 102. El comando de “bloqueo” se envía al dispositivo cliente 102 y el servidor de aplicaciones web 104 espera a recibir una confirmación. Cuando una aplicación de bloqueo 608 en el dispositivo cliente 102 recibe el comando de bloqueo, la contraseña para el dispositivo cliente 102 se establece en la contraseña de la cuenta y el dispositivo cliente 102 se bloquea. En otras palabras, por ejemplo, cuando la aplicación de bloqueo 608 recibe el comando de bloqueo, se ejecuta el comando, cuyo resultado es bloquear los datos de usuario en el dispositivo cliente 102 para que sean inaccesibles mediante el uso del dispositivo cliente 102.

[0108] Si el servidor de aplicaciones web 104 no recibe ninguna confirmación de que un comando de bloqueo se ha ejecutado con éxito después de un periodo de tiempo, puede reenviarse el comando de bloqueo. Si aún no tiene éxito después de varios intentos, se envía un correo electrónico al usuario que indica que no se pudo bloquear el dispositivo cliente 102. Por otro lado, si tiene éxito, el usuario recibe un correo electrónico de confirmación.

[0109] Además, en una o más realizaciones, si el servidor de aplicaciones web 104 no recibe una confirmación de ejecución correcta del comando de bloqueo, el servidor de aplicaciones web 104 puede solicitar al servidor de administración de cuentas 106 que transmita continuamente mensajes al dispositivo cliente 102 para aumentar una frecuencia de ping del dispositivo cliente 102 (como se ha descrito anteriormente). Cuando el dispositivo cliente 102 recibe estas señales del servidor de administración de cuentas 106 y se recibe un próximo ping desde el dispositivo cliente 102, el comando de bloqueo puede enviarse inmediatamente al dispositivo cliente 102 para su ejecución. De esta manera, tan pronto como el dispositivo cliente 102 sea visible para la red, se puede enviar un comando de bloqueo al dispositivo cliente 102. Por lo tanto, incluso si el dispositivo cliente 102 está sin conexión a la red (*off-line*) durante un periodo de tiempo, aún se puede invocar una funcionalidad de bloqueo tan pronto como el dispositivo cliente 102 se vuelva a conectar a la red.

[0110] Además, se puede enviar un comando de inutilización remota utilizando el módulo de borrado del dispositivo 612 a través de la interfaz de usuario de inutilización y bloqueo 804. En este caso, el usuario (o un administrador) va al sitio web de escritorio 602, introduce su número de teléfono y contraseña de cuenta, y elige una opción de inutilización. Se le puede pedir al usuario que confirme su decisión de enviar el comando de inutilización y se le puede proporcionar una opción para iniciar una copia de seguridad de datos remota antes de enviar el comando de inutilización. Se envía el comando de inutilización al dispositivo cliente 102, y posteriormente una aplicación de eliminación de datos 808 en el dispositivo cliente 102 borra todos (o al menos una parte) de los datos de usuario en el dispositivo cliente 102 y restablece en el dispositivo cliente 102 la configuración de fábrica incluso si, por ejemplo, una copia de seguridad de datos solicitada no tiene éxito según las preferencias del usuario. Además, por ejemplo, una vez que la aplicación de eliminación de datos 808 recibe un comando de inutilización, los datos de usuario pueden borrarse con independencia de si el dispositivo cliente 102 está conectado a una red de servicios. De esta manera, una vez que se recibe un comando de inutilización, la ejecución del comando de inutilización no puede detenerse desconectando el dispositivo cliente 102 de la red (por ejemplo, la red 202 en la Figura 2).

[0111] Si el servidor de aplicaciones web 104 no recibe una confirmación de que un comando de inutilización enviado se haya ejecutado correctamente después de un determinado periodo de tiempo, se puede reenviar el comando de inutilización. Si, después de varios intentos, aún no se ha ejecutado correctamente, se puede enviar un correo electrónico al usuario indicando que no se pudo implementar correctamente el comando de inutilización. Por otro lado, si se ejecuta correctamente, el usuario recibe un correo electrónico de confirmación.

[0112] Además, en una o más realizaciones, si el servidor de aplicaciones web 104 no recibe una confirmación de ejecución correcta del comando de inutilización, el servidor de aplicaciones web 104 puede solicitar al servidor de administración de cuentas 106 que transmita continuamente mensajes al dispositivo cliente 102 para aumentar una frecuencia de ping del dispositivo cliente 102 (como se ha descrito anteriormente). Cuando el dispositivo cliente 102 recibe estas señales del servidor de administración de cuentas 106 y se recibe un próximo ping desde el dispositivo cliente 102, a continuación, puede enviarse inmediatamente el comando de inutilización al dispositivo cliente 102 para su ejecución. De esta manera, tan pronto como el dispositivo cliente 102 sea visible a través de la red, se puede enviar un comando de inutilización al dispositivo cliente 102. Por lo tanto, incluso si el dispositivo cliente 102 no tiene conexión

a la red (*off-line*) durante un periodo de tiempo, puede invocarse una funcionalidad de inutilización tan pronto como el dispositivo cliente 102 se vuelva a conectar a la red.

[0113] En una o más realizaciones, el comando de bloqueo y/o inutilización descritos anteriormente pueden enviarse al dispositivo cliente 102 de acuerdo con una configuración del dispositivo cliente 102. Por ejemplo, el comando de bloqueo y/o inutilización pueden enviarse de acuerdo con un sistema operativo del dispositivo cliente 102. En otro ejemplo, el comando de bloqueo y/o inutilización pueden enviarse de acuerdo con un tipo de dispositivo cliente 102. Al generar el comando de bloqueo y/o inutilización de acuerdo con uno o más detalles del dispositivo cliente 102, se puede lograr el reconocimiento y la ejecución adecuados del comando de bloqueo y/o inutilización.

[0114] Por lo que respecta al módulo de bloqueo del dispositivo 610 y al módulo de borrado del dispositivo 612 alojados en el servidor de aplicaciones web 104, el sitio web de escritorio correspondiente 602 solo puede permitir al usuario realizar una función de inutilización y bloqueo si la cuenta del usuario está activa (en Estado B o C). Si la cuenta del usuario no se encuentra en el Estado B o C, el sitio web de escritorio 602 puede mostrar un mensaje de error de inicio de sesión y no permitir que el usuario realice una función de inutilización y bloqueo.

[0115] Además, el sitio web de escritorio 602 puede proporcionar una interfaz de usuario 804 para emitir comandos de inutilización y bloqueo. Como se ha descrito anteriormente, para hacerlo, el sitio web de escritorio 602 puede requerir que el usuario introduzca un número de teléfono y contraseña de cuenta. El sitio web de escritorio 602 puede autenticar el número de teléfono del usuario y la contraseña de la cuenta antes de enviar un comando de bloqueo o inutilización.

[0116] Además, en una o más realizaciones, el sitio web de escritorio 602 puede permitir “bloquear de nuevo” el dispositivo cliente 102 con una nueva contraseña (si el dispositivo ya está bloqueado, el usuario puede ser capaz de restablecer la contraseña por correo electrónico y después bloquear de nuevo el dispositivo cliente 102 con la nueva contraseña).

[0117] Como se desprende de la descripción anterior, el sitio web de escritorio 602 puede permitir al usuario elegir entre un comando de inutilización o bloqueo para enviar al dispositivo cliente 102. Por motivos de seguridad, en una o más realizaciones, el sitio web de escritorio 602 puede no permitir que el usuario emita un comando de inutilización si la contraseña del usuario se ha restablecido dentro de un periodo de tiempo predeterminado (por ejemplo, 24 horas). Además, en una o más realizaciones, siempre se puede permitir el bloqueo del dispositivo, con independencia de la hora del último cambio de contraseña.

[0118] En una o más realizaciones, el comando de inutilización o bloqueo puede enviarse como un mensaje SMS (encriptado) propagado a través de una puerta de enlace de agregador de SMS (no mostrada). El sitio web de escritorio 602 puede incluir información en el mensaje SMS enviado al cliente que permite al cliente autenticar la solicitud. Además, el sitio web de escritorio 602 puede requerir que el usuario realice una confirmación antes de enviar un comando de inutilización y puede recordarle al usuario los efectos de la inutilización.

[0119] Cuando el usuario solicita un bloqueo del dispositivo, el sitio web de escritorio 602 puede permitir que el usuario introduzca un mensaje que se mostrará en la pantalla de bloqueo del dispositivo cliente 102. Cuando el usuario solicita un bloqueo del dispositivo, el sitio web de escritorio 602 puede permitir que el usuario introduzca un número de teléfono que se transmitirá al dispositivo cliente 102, tras lo cual ese número de teléfono puede mostrarse en la pantalla de bloqueo del dispositivo en un esfuerzo para solicitar a una persona que está accediendo al dispositivo cliente 102 llamar a ese número de teléfono (véase, por ejemplo, la Figura 28).

[0120] Como se ha descrito anteriormente, el servidor de aplicaciones web 104 puede reenviar comandos de bloqueo e inutilización al dispositivo cliente 102 si el servidor de aplicaciones web 104 no recibe un mensaje de ejecución correcta del dispositivo cliente 102. En una o más realizaciones, el servidor de aplicaciones web 104 puede, por ejemplo, tener el siguiente programa de reintentos: 1.er reintento: 1 minuto; 2.º reintento: 5 minutos; 3.er reintento: 30 minutos; 4.º reintento: 2 horas; 5.º reintento: 6 horas; 6.º reintento: 12 horas; y 7.º reintento: 24 horas. Si fallan todos los reintentos, el servidor de aplicaciones web 104 puede notificar al usuario enviando un correo electrónico a la dirección de correo electrónico de la cuenta del usuario.

[0121] Además, en una o más realizaciones, cuando se solicita una inutilización, el usuario puede tener la opción de solicitar una copia de seguridad de datos antes de la ejecución de la inutilización. Se puede suministrar al usuario una opción de especificar si la inutilización debe continuar, incluso cuando la copia de seguridad de los datos no se ejecuta correctamente inicialmente. Cuando se solicita un bloqueo del dispositivo, el usuario puede tener la opción de solicitar una copia de seguridad del dispositivo como parte del comando de bloqueo. Por ejemplo, el dispositivo cliente 102 puede bloquearse y los datos de usuario en el dispositivo cliente 102 pueden transmitirse de forma inalámbrica a un almacén de datos remoto. Posteriormente, el dispositivo cliente 102 también puede ser “inutilizado” (por ejemplo, borrando los datos de usuario, como se ha descrito anteriormente) mientras se encuentra en el estado bloqueado. De esta manera, el bloqueo del dispositivo cliente 102 evita que una persona en posesión del dispositivo cliente 102

intente sortear o evitar una operación de bloqueo, copia de seguridad de datos y/o inutilización. Al recibir la confirmación del dispositivo cliente 102 de un bloqueo o inutilización con éxito del dispositivo, el servidor de aplicaciones web 104 puede enviar un correo electrónico para notificar al usuario la acción o las acciones específicas tomadas.

[0122] Si se confirma la entrega de un mensaje SMS, pero no se recibe ningún mensaje de confirmación del dispositivo cliente 102 después de un determinado periodo de tiempo, el servidor de aplicaciones web 104 puede notificar al usuario por correo electrónico que se recibió el mensaje SMS, pero no se recibió confirmación del dispositivo.

[0123] Con respecto a una inutilización como se usa en una o más realizaciones, la aplicación de borrado 808 puede ser capaz de recibir y procesar un mensaje SMS con formato especial para iniciar la actividad de la inutilización. Además, la aplicación de borrado 808 puede autenticar la inutilización sirviéndose de la información proporcionada por el servidor de aplicaciones web 104 en el mensaje SMS. Además, al recibir el mensaje SMS, el cliente puede iniciar una copia de seguridad de datos si el usuario ha elegido hacerlo. Durante el proceso de copia de seguridad, si se genera un error en la copia de seguridad debido a algún error o se cancela manualmente, el cliente aún puede ejecutar el comando de inutilización. Cuando se realiza una función de inutilización, el cliente puede aún borrar aplicaciones y datos en el dispositivo cliente 102, por ejemplo, sobrescribiendo el contenido en la memoria y después llevando a cabo un restablecimiento completo a la configuración predeterminada de fábrica. Después de que se haya ejecutado la inutilización y se haya realizado el restablecimiento completo del dispositivo cliente 102, el cliente puede volver a bloquear el dispositivo cliente 102 con la contraseña de su cuenta. Además, el cliente puede notificar su estado al servidor de aplicaciones web 104 antes de que comience el procedimiento final de la inutilización. Si el cliente no puede entrar en contacto con el servidor de aplicaciones web 104, el cliente puede continuar con el proceso de inutilización si el usuario ha indicado tal preferencia al enviar la inutilización.

[0124] Por lo que respecta al bloqueo del dispositivo, el cliente puede ser capaz de recibir y procesar un mensaje SMS con formato especial para iniciar una función de bloqueo del dispositivo. La aplicación de bloqueo 806 puede autenticar la solicitud de bloqueo del dispositivo utilizando la información proporcionada por el servidor de aplicaciones web 104 en el mensaje SMS. Al recibir el mensaje SMS, el cliente puede iniciar una copia de seguridad de datos si el usuario ha elegido realizar esta acción. Además, al recibir el mensaje SMS, el cliente bloquea el dispositivo cliente 102. Además, la aplicación de bloqueo 806 puede presentar en una pantalla del dispositivo cliente 102 un mensaje que indica que el dispositivo cliente 102 está bloqueado. Es posible que el cliente no permita que un usuario omita la pantalla sin introducir la contraseña correcta (véase, por ejemplo, la Figura 28). En particular, el cliente puede permitir que un usuario introduzca una contraseña de cuenta para desbloquear el dispositivo cliente 102. Además, si el servidor de aplicaciones web 104 ha transmitido un mensaje personalizado especificado por el usuario, el cliente muestra ese mensaje en la pantalla de visualización de bloqueo. Aún más, si el servidor de aplicaciones web 104 ha transmitido un número de teléfono especificado por el usuario, el cliente puede permitir que el usuario llame a ese número de teléfono con el dispositivo cliente 102 (véase, por ejemplo, la Figura 28). Más en concreto, en una o más realizaciones, ese número de teléfono puede no mostrarse realmente al autor de la llamada. Además, el cliente puede permitir el uso del dispositivo cliente 102 para llamar a los servicios de emergencia (véase, por ejemplo, la Figura 28).

[0125] En la Figura 10 se muestra un proceso de flujo de acuerdo con una realización de la presente invención. En concreto, se muestra un proceso de flujo para ejemplos de servicios de inutilización y bloqueo. En el lado del servidor (por ejemplo, el servidor de aplicaciones web 104), un usuario solicita que se envíe un comando de bloqueo o inutilización a su dispositivo cliente (por ejemplo, el dispositivo cliente 102) 950. Junto con la solicitud, el usuario puede especificar instrucciones concretas. Entre los ejemplos de instrucciones adicionales que se pueden solicitar figuran si se debe realizar una copia de seguridad de datos antes de ejecutar una operación de inutilización, si se debe realizar una copia de seguridad de datos antes de ejecutar una operación de bloqueo, un número de teléfono al que llamar si una persona intenta usar una funcionalidad de teléfono del dispositivo cliente, y si se debe eliminar un bloqueo en los datos de usuario en el dispositivo cliente después de un periodo de tiempo predeterminado.

[0126] Cuando se reciben la solicitud y las instrucciones del usuario (o después de recibirlas), el lado del servidor intenta autenticar el usuario utilizando las credenciales proporcionadas por el usuario 952. Dicha autenticación puede implicar localizar una cuenta de usuario para el dispositivo cliente. Suponiendo que el usuario solicitante está autenticado, el lado del servidor genera un comando de bloqueo o un comando de inutilización 954. El comando puede generarse de acuerdo con una especificación del dispositivo cliente, como se indica en la cuenta de usuario ubicada a través de la autenticación del usuario. En otras palabras, el comando puede generarse específicamente para el dispositivo cliente previsto.

[0127] A continuación, se transmite el comando de bloqueo o inutilización de forma inalámbrica desde el lado del servidor a una dirección del dispositivo cliente 956. Tras la recepción inalámbrica en el dispositivo cliente, el dispositivo cliente descifra el comando y determina si el comando es un comando de bloqueo 960. Si se ha recibido un comando de bloqueo 960, el dispositivo cliente determina si se ha proporcionado una instrucción para realizar una copia de seguridad de los datos antes de bloquear el dispositivo cliente 962. Cabe señalar que en una o más realizaciones

adicionales, se puede invocar sistemáticamente una copia de seguridad de datos sin una solicitud particular del usuario. Si se requiere o solicita una copia de seguridad de los datos, se hace una copia de seguridad de datos de usuario en el dispositivo cliente de forma inalámbrica en un almacén de datos remoto 964. Después, el dispositivo cliente bloquea el dispositivo cliente para que no se pueda acceder a los datos de usuario en el dispositivo cliente usando el dispositivo cliente 966.

[0128] En caso de que el dispositivo cliente reciba un comando de inutilización 968, el dispositivo cliente puede bloquearse automáticamente, como se ha descrito anteriormente (teniendo en cuenta que, si el comando recibido no es un comando de bloqueo o un comando de inutilización, el comando se procesa de otra forma 982). El dispositivo cliente determina si se ha proporcionado una instrucción para realizar una copia de seguridad de datos antes de borrar los datos de usuario en el dispositivo cliente 970. Cabe señalar que en una o más realizaciones adicionales, se puede invocar sistemáticamente una copia de seguridad de datos sin una solicitud particular del usuario. Si se requiere o solicita una copia de seguridad de los datos, se lleva a cabo una copia de seguridad de los datos de usuario en el dispositivo cliente de forma inalámbrica en un almacén de datos remoto 972. Después, el dispositivo cliente borra los datos de usuario en el dispositivo cliente 974.

[0129] Es importante señalar que en una o más realizaciones, se puede enviar un comando de inutilización o bloqueo a un dispositivo cliente desde el servidor de aplicaciones web 104, aunque ese dispositivo cliente no pueda sincronizar datos a través del servidor de aplicaciones web 104. En otras palabras, la capacidad de enviar un comando de inutilización o bloqueo no está limitada por el motor o los motores de sincronización utilizados por el dispositivo cliente 102 para sincronizar datos. Por ejemplo, en una o más realizaciones, las funcionalidades del comando de inutilización y bloqueo pueden ser admitidas, específicas y/o dependientes de un fabricante de dispositivos, a diferencia de un proveedor de terceros que ofrece soluciones de sincronización de datos para el dispositivo.

[0130] Además, en una o más realizaciones, el usuario puede elegir qué datos se bloquearán o deshabilitarán. Por ejemplo, el usuario puede solicitar que solo se borren los datos críticos en lugar de todos los datos de usuario. En otro ejemplo, el usuario puede permitir que determinados tipos de datos permanezcan desbloqueados, mientras especifica otros tipos de datos que se bloquearán como parte de la operación de bloqueo iniciada por el usuario.

[0131] Si la operación de bloqueo o inutilización tiene éxito 976, el dispositivo cliente envía de forma inalámbrica una indicación de éxito al lado del servidor 980. De lo contrario, el dispositivo cliente envía de forma inalámbrica una indicación de error al lado del servidor 978. A continuación, el lado del servidor notifica al usuario 958 en consecuencia. Se puede proporcionar la notificación al usuario, por ejemplo, por correo electrónico, mensaje automatizado a un número de teléfono almacenado de la casa o el trabajo, correo postal o un sitio web al que puede acceder el usuario.

Servidor de sincronización

[0132] En la Figura 11 se muestra un diagrama del servidor de sincronización 108 y el dispositivo cliente 102 de acuerdo con una realización de la presente invención. El servidor de sincronización 108 incluye un módulo de copia de seguridad de datos 902, un módulo de restauración de datos 904 y un almacén de datos 906, cada uno de los cuales se describe en mayor detalle a continuación.

[0133] El servidor de sincronización 106 también incluye un componente de transporte HTTP/S 914 y un componente de transporte SMS 916 para interactuar respectivamente con el componente de transporte HTTP/S 318 y el componente de transporte SMS 320 que residen en el dispositivo cliente 102. Estos componentes de transporte 914, 916, 318 y 320 pueden admitir, por ejemplo, una o más de las diversas comunicaciones admitidas entre el dispositivo cliente 102 y el servidor de administración de cuentas 106 (o el servidor de aplicaciones web 104). Además, por ejemplo, se pueden producir las operaciones de copia de seguridad y restauración de datos entre el dispositivo cliente 102 y el servidor de sincronización 108 usando mensajes de lenguaje de marcado de sincronización (SyncML) enviados a través de HTTP/S. Además, en una o más realizaciones, las operaciones de copia de seguridad y restauración de datos entre el dispositivo cliente 102 y el servidor de sincronización 108 pueden producirse usando un protocolo basado en información pública y privada (PAPI, *Public and Private Information*) sobre HTTP/S.

[0134] El módulo de copia de seguridad de datos 902, el módulo de restauración de datos 904 y el módulo de almacenamiento de datos 906 admiten los servicios de copia de seguridad y restauración de datos proporcionados por el sistema 100. Como se ha descrito anteriormente, una vez que el usuario completa el registro, se le presenta la opción de hacer una copia de seguridad de los datos en su dispositivo cliente 102. Si el usuario elige iniciar una copia de seguridad de datos, se le puede informar cuánto tiempo se tardará en realizar la copia de seguridad de datos y en cuánto tráfico de datos se incurrirá. Si el usuario lo aprueba, se inicia la copia de seguridad de datos y se puede mostrar un indicador de progreso de la copia de seguridad de datos con una opción de cancelación (véase, por ejemplo, la Figura 25). Los datos particulares de los que se realiza una copia de seguridad pueden variar. Al completar con éxito la copia de seguridad de datos, se informa al usuario en consecuencia (véase, por ejemplo, la Figura 26).

[0135] Además, en una o más realizaciones, se puede realizar automáticamente una copia de seguridad de los datos de usuario de acuerdo con un programa concreto. Aún más, en una o más realizaciones, se puede realizar una copia de seguridad de los datos de usuario “según sea necesario”. Además, el usuario puede iniciar manualmente una copia de seguridad de los datos. En tales casos, el usuario puede realizar cambios en datos específicos en el dispositivo cliente 102 y elegir realizar una copia de seguridad de los datos modificados. En otras palabras, en una o más realizaciones, se puede realizar una copia de seguridad de los cambios incrementales en los datos de usuario en lugar de todos los datos de usuario residentes en el dispositivo cliente 102.

[0136] En algunos casos, el usuario puede restaurar los datos a un dispositivo cliente “limpio” (por ejemplo, un nuevo dispositivo) con datos procedentes de una copia de seguridad de un dispositivo cliente utilizado anteriormente. Esto ocurre cuando el usuario inicia sesión en una cuenta existente en su nuevo dispositivo cliente. A continuación, el servidor de sincronización 108 puede detectar que el usuario ha realizado previamente una copia de seguridad de los datos en el servidor de sincronización 108. Después, el cliente ofrece al usuario la opción de iniciar una restauración. El usuario puede entonces iniciar la restauración, tras lo cual se informa al usuario del tiempo y el uso de datos antes de que comience la restauración. Después se inicia la restauración y se puede mostrar un indicador de progreso de restauración. Los datos de destino se restauran al dispositivo cliente 102. Además, en una o más realizaciones, los datos existentes localmente en el dispositivo cliente 102 se combinan con los datos almacenados en el servidor de sincronización 108. Una vez completada la restauración, se informa al usuario de la restauración correcta de los datos.

[0137] En algunos casos, el usuario puede migrar a un dispositivo cliente de generación más reciente que tiene el mismo sistema operativo que el dispositivo cliente utilizado anteriormente. Aquí, el usuario lleva a cabo una copia de seguridad de datos en el dispositivo antiguo. El usuario puede adquirir e instalar el software de cliente en el nuevo dispositivo cliente, como se ha descrito anteriormente. A continuación, se pueden restaurar los datos de la copia de seguridad en el nuevo dispositivo.

[0138] Los tipos de datos que se pueden incluir en la copia de seguridad y luego restaurarse posteriormente incluyen, entre otros: un calendario; contactos; tareas; notas; marcadores de navegador; accesos directos de aplicaciones telefónicas, incluidos números de marcación rápida; registros de llamadas; configuraciones de aplicaciones; e historial de mensajes SMS.

[0139] En la Figura 27 se muestra un ejemplo de una captura de pantalla de copia de seguridad de datos de acuerdo con una realización de la presente invención. El cliente puede mostrar una hora y fecha de una última copia de seguridad correcta y cualquier condición de error, si es necesario. Cuando el usuario elige realizar una copia de seguridad de datos, si el usuario no ha realizado una restauración en el dispositivo cliente 102 (porque el cliente se registró o inició sesión la última vez), el cliente puede realizar una copia de seguridad de datos (una “copia de seguridad limpia”) antes de una purga. Cuando el cliente realiza la copia de seguridad limpia, los datos de los que se había realizado una copia de seguridad previamente en el servidor de sincronización 108 pueden purgarse y reemplazarse con los datos de los que se ha realizado una copia de seguridad más recientemente. Además, si existen datos en el servidor de sincronización 108, el cliente puede advertir al usuario que se sobrescribirán los datos existentes.

[0140] Además, como se ha descrito anteriormente, el cliente puede realizar copias de seguridad incrementales. Si el usuario ya ha realizado una copia de seguridad o restauración en el dispositivo cliente 102 (desde que el cliente se registró o inició sesión por última vez), el cliente puede realizar una copia de seguridad incremental. Durante la copia de seguridad incremental, el cliente solo puede hacer una copia de seguridad de los datos que se han modificado desde la última copia de seguridad o restauración desde el servidor de sincronización 108. Además, el cliente puede hacer una copia de seguridad de los cambios de datos a nivel de campo, en lugar de a nivel de registro o de base de datos/archivo.

[0141] Además, en una o más realizaciones, las copias de seguridad iniciadas por el usuario pueden deshabilitar otras actividades del dispositivo que pueden interrumpir la copia de seguridad de datos. Si una copia de seguridad de datos supera el tiempo de espera, se puede mostrar un mensaje de error y se pueden (re)habilitar otras actividades detenidas previamente en el dispositivo. Además, se puede impedir que el usuario abandone una aplicación de copia de seguridad. Se puede ofrecer al usuario una opción de cancelación que proporciona la cancelación instantánea de una copia de seguridad en curso y (re)habilita otras actividades del dispositivo detenidas previamente.

[0142] En una o más realizaciones, se puede realizar una copia de seguridad automática después de que el dispositivo cliente 102 haya estado inactivo durante un determinado periodo de tiempo. Si se interrumpe una copia de seguridad de datos, la copia de seguridad de datos puede cancelarse de inmediato automáticamente y pasar el control a una aplicación solicitante o a una aplicación predeterminada (si no hay ninguna aplicación solicitante). Si la copia de seguridad de datos se cancela automáticamente, el cliente puede volver a intentar realizar copias de seguridad en segundo plano.

[0143] Además, en una o más realizaciones, las copias de seguridad de datos pueden realizarse en un subproceso que no sea de bloqueo. Si el cliente es la aplicación activa durante una copia de seguridad de datos, el cliente puede

mostrar información de progreso al usuario, incluido el tipo de datos del que se está realizando una copia de seguridad actualmente y un porcentaje general de finalización. Además, el cliente puede ser capaz de continuar una copia de seguridad de datos incluso si el usuario cambia los datos de destino durante la copia de seguridad de datos. Aún más, en una o más realizaciones, el usuario puede ser capaz de iniciar una llamada telefónica saliente o recibir una llamada telefónica entrante cuando se está realizando una copia de seguridad de datos. Además, el usuario puede ser capaz de iniciar la actividad de datos cuando se realiza una copia de seguridad de datos. En tales casos, la copia de seguridad de datos puede cancelarse y el cliente puede volver a intentar la copia de seguridad de datos más tarde. Además, el usuario puede ser capaz de cancelar un proceso de copia de seguridad de datos desde dentro del cliente.

[0144] Como se ha descrito anteriormente, el usuario puede iniciar una copia de seguridad de datos manual. Por ejemplo, el cliente puede informar al usuario del tiempo y el uso de datos proyectados para la actividad de copia de seguridad antes de que comience la actividad y puede darle al usuario la opción de cancelar. Si el cliente está realizando una copia de seguridad inicial iniciada manualmente (es decir, el usuario no realizó una copia de seguridad de datos cuando se registró por primera vez), el cliente puede presentar al usuario una pantalla de configuración de programación de copia de seguridad.

[0145] Además, en una o más realizaciones, el cliente puede ser capaz de iniciar copias de seguridad automáticas. Se pueden realizar las copias de seguridad automáticas según un programa configurable por el usuario. Si el usuario aún no ha realizado una copia de seguridad inicial, es posible que no se realice una copia de seguridad automática. Además, se pueden realizar las copias de seguridad automáticas, por ejemplo, “después de cualquier cambio”, diariamente, semanalmente, mensualmente o nunca, según especifique el usuario. Si el usuario selecciona “después de cualquier cambio”, el cliente puede intentar realizar una copia de seguridad automática cada vez que se modifiquen datos específicos. Además, el cliente puede esperar hasta que el dispositivo cliente 102 esté inactivo antes de intentar una copia de seguridad de datos “después de cualquier cambio”. Tales copias de seguridad de datos no pueden realizarse más de una vez en un periodo de tiempo específico. Los cambios de datos realizados durante este periodo de espera pueden agruparse y realizarse cuando finaliza el periodo de espera. Si el usuario no selecciona “después de cualquier cambio” o “manual”, el cliente puede intentar realizar copias de seguridad automáticas durante un tiempo aleatorio (basado en la hora local del dispositivo) dentro de una franja horaria especificada por la preferencia de “hora del día” del usuario: “mañana” (*morning*) es desde las 6.00 horas a las 12.00 horas; “tarde” (*afternoon*) es desde las 12.00 horas a las 18.00 horas; “última hora” (*evening*) es desde las 18.00 horas a las 24.00 horas; y “durante la noche” (*overnight*) es desde las 24.00 horas a las 6.00 horas. Además, se pueden intentar realizar copias de seguridad automáticas en una programación con independencia de si el usuario ha realizado copias de seguridad manuales adicionales. Además, las copias de seguridad automáticas solo se pueden realizar cuando el dispositivo cliente 102 ha entrado en un modo de suspensión y ha estado suspendido durante un periodo de tiempo específico.

[0146] Asimismo, en una o más realizaciones, el cliente puede proporcionar al usuario una o más de las siguientes configuraciones –que el usuario puede configurar– para la copia de seguridad automática: “después de cualquier cambio”; “una vez al día”; “una vez por semana”; “una vez al mes”; y “manual”. Si el usuario nunca ha realizado una copia de seguridad de datos, una selección “manual” puede ser la configuración predeterminada. Además, se puede presentar al usuario durante una copia de seguridad inicial una opción para establecer una programación de copia de seguridad “automática”; el valor automatizado predeterminado puede establecerse en “diario”. Cuando la programación de copia de seguridad automática se establece en “diaria”, “semanal” o “mensual”, puede estar disponible una preferencia adicional de “hora del día”. Los valores posibles pueden incluir, por ejemplo, “mañana” (*morning*), “tarde” (*afternoon*), “última hora” (*evening*) y “durante la noche” (*overnight*), donde una configuración predeterminada puede establecerse en “durante la noche”. Además, las opciones de preferencia pueden incluir una opción de “no realizar copia de seguridad mientras se está en modo itinerante”, donde la configuración predeterminada puede establecerse para dejar esta opción sin marcar. Además, esta preferencia solo puede ser aplicable para una copia de seguridad automática y no para una copia de seguridad manual.

[0147] Además, en una o más realizaciones, el cliente puede indicar un estado general de copia de seguridad de datos en una pantalla principal usando una característica visual (por ejemplo, un icono de color). Por ejemplo, el cliente puede usar un icono verde para indicar que se ha realizado una copia de seguridad correcta de los datos de usuario dentro de un periodo de tiempo determinado desde la última copia de seguridad automática programada. Si el usuario realiza una copia de seguridad manualmente, el cliente puede mostrar un icono verde si el usuario ha realizado una copia de seguridad dentro de un último periodo de tiempo especificado. Aún más, el cliente puede usar, por ejemplo, un icono amarillo para indicar que no se ha realizado nunca una copia de seguridad de los datos de usuario o que no se ha realizado una copia de seguridad recientemente. Además, por ejemplo, el cliente puede usar un icono rojo para indicar que el último intento de copia de seguridad tuvo como resultado un error grave.

[0148] En una o más realizaciones, el cliente puede realizar una o más de las siguientes comprobaciones antes de un proceso de copia de seguridad de datos. El servidor de sincronización 108 puede permitir que el cliente realice una copia de seguridad de datos si la cuenta del usuario es provisional o está activa. Además, si la cuenta del usuario está deshabilitada, el cliente puede mostrar un mensaje de error de inicio de sesión y cancelar la actividad de copia de seguridad. Además, el cliente puede validar un *token* con el servidor de sincronización 108 para autenticar el

usuario antes de realizar la actividad de copia de seguridad de datos. Si la validación produce un error y la aplicación se está ejecutando en primer plano, el cliente puede mostrar un cuadro de diálogo de reintento de inicio de sesión, que puede presentar al usuario la posibilidad de restablecer su contraseña o autenticarse a través del servidor de administración de cuentas 106. Si el usuario puede autenticarse a través del cuadro de diálogo de reintento de inicio de sesión, el cliente puede continuar con el proceso de copia de seguridad de datos. Si el usuario no puede autenticarse a través del diálogo de reintento de inicio de sesión, el cliente puede tratar la copia de seguridad de datos como cancelada. Además, si la validación produce un error y una aplicación se está ejecutando en segundo plano, el cliente puede notificar al usuario a través de una notificación del sistema que la autenticación ha producido un error. Cuando el usuario se autentica correctamente en el sistema, se pueden eliminar las notificaciones pendientes del sistema. Si la validación produce un error, el cliente puede no intentar otra copia de seguridad automática hasta que se solucione la condición de error.

[0149] Además, en una o más realizaciones, el cliente puede confirmar que una radio está encendida. Si la radio no está encendida y el cliente se está ejecutando en primer plano, el cliente puede indicar al usuario si desea encender la radio. Si el usuario selecciona “sí”, el cliente enciende la radio y continúa. Si el usuario selecciona “no”, el cliente puede cancelar el proceso de copia de seguridad de datos y mostrar un mensaje de error. Si la radio no está encendida y el cliente se está ejecutando en segundo plano, el cliente puede cancelar el proceso de copia de seguridad de datos y notificar al usuario sobre el error. En este caso, el cliente puede iniciar una copia de seguridad de datos automáticamente la próxima vez que la radio esté encendida y el dispositivo cliente 102 entre en modo de suspensión. Es posible que el cliente no inicie otra copia de seguridad automática hasta que se encienda la radio.

[0150] Además, en una o más realizaciones, el cliente puede confirmar que el dispositivo cliente 102 se encuentra dentro del rango de cobertura de datos. Si el dispositivo cliente 102 está fuera del rango de cobertura de datos y el cliente se está ejecutando en primer plano, el cliente puede cancelar el proceso de copia de seguridad de datos y mostrar un mensaje de error. Si el dispositivo cliente 102 está fuera del rango de cobertura de datos y el cliente se está ejecutando en segundo plano, el cliente puede cancelar el proceso de copia de seguridad de datos y, en consecuencia, notificar al usuario. El cliente puede iniciar un proceso de copia de seguridad de datos automáticamente cuando se ha corregido la condición. Además, el cliente puede no iniciar otra copia de seguridad automática hasta que se corrija la condición.

[0151] Además, en una o más realizaciones, el cliente puede determinar si el dispositivo cliente 102 se encuentra en modo itinerante. Si se establece como “verdadera” una preferencia de “no realizar copia de seguridad mientras se está en modo itinerante” y el cliente se ejecuta en segundo plano, el cliente puede cancelar el proceso de copia de seguridad de datos. El cliente puede iniciar un proceso de copia de seguridad de datos automáticamente cuando se corrige esta condición. Además, el cliente puede no iniciar otra copia de seguridad automática hasta que se corrija la condición.

[0152] Además, en una o más realizaciones, el cliente puede confirmar que una batería se encuentra en un nivel suficiente para completar una copia de seguridad de datos. Si la batería no tiene un nivel suficiente y el cliente se está ejecutando en primer plano, el cliente puede cancelar el proceso de copia de seguridad de datos y mostrar un mensaje de error. Si el nivel de batería no es suficiente y el cliente se está ejecutando en segundo plano, el cliente puede cancelar el proceso de copia de seguridad de datos y notificar al usuario en consecuencia. Además, el cliente puede iniciar una copia de seguridad de datos automáticamente cuando se tiene el suficiente nivel de batería. Asimismo, el cliente puede no iniciar otra copia de seguridad automática hasta que se tenga el nivel suficiente de batería. Si el cliente se ejecuta en primer plano y se produce un error en la actividad de copia de seguridad por algún motivo, el cliente puede notificar al usuario que la copia de seguridad de datos ha producido un error. Si el cliente se ejecuta en segundo plano y se produce un error en el proceso de copia de seguridad de datos por algún motivo, es posible que el cliente no notifique de inmediato al usuario.

[0153] Asimismo, en una o más realizaciones, el cliente puede llevar a cabo, por ejemplo, el siguiente programa de reintentos después de encontrar un error desconocido en la copia de seguridad de datos: 1.er reintento: 1 minuto; 2.º reintento: 5 minutos; 3.er reintento: 30 minutos; 4.º reintento: 2 horas; 5.º reintento: 6 horas; 6.º reintento: 12 horas; y 7.º reintento: 24 horas. Si se producen errores en todos los reintentos, el cliente puede notificar al usuario según corresponda.

[0154] Además, en una o más realizaciones, el cliente puede borrar las alertas generadas por las notificaciones del sistema si la copia de seguridad de datos se realiza correctamente. Además, si el cliente se encuentra en el proceso de un programa de reintentos, se pueden rechazar otras copias de seguridad automáticas. Aún más, si se realiza correctamente una copia de seguridad de datos, se pueden cancelar los reintentos pendientes. Aún más, el cliente puede mostrar información sobre el ciclo de reintentos, incluida la cantidad de errores, la hora del último error, la hora programada del siguiente intento y el motivo del error.

[0155] Además, en una o más realizaciones, la pantalla principal de la aplicación del cliente puede indicar la intensidad de la señal de datos del dispositivo y el nivel de batería.

[0156] Además, en una o más realizaciones, el servidor de sincronización 108 puede ser capaz de detectar cuentas de copia de seguridad inactivas. Cuando el servidor de sincronización 108 detecta una cuenta de copia de seguridad inactiva, el servidor de sincronización 108 puede notificar a un titular de cuenta por correo electrónico que su cuenta de copia de seguridad está inactiva y que los datos de usuario de los que se ha realizado una copia de seguridad se eliminarán después de un determinado periodo de tiempo si el usuario no realiza actividades adicionales de copia de seguridad o de restauración. Si no se realizan actividades adicionales de copia de seguridad o restauración en la cuenta inactiva dentro de este periodo determinado de tiempo, los datos de usuario de los que se ha realizado una copia de seguridad pueden eliminarse del servidor de sincronización 108. En este caso, el servidor de sincronización 108 puede enviar un correo electrónico al usuario indicando que sus datos de usuario se han eliminado del servidor de sincronización 108 e informando al usuario que puede volver a iniciar sesión y realizar una nueva copia de seguridad inicial si el usuario desea continuar utilizando el servicio. Cuando los datos de copia de seguridad del usuario se eliminan debido a la inactividad, no se elimina necesariamente la cuenta del usuario.

[0157] Cuando se inicia una actividad de restauración, el cliente puede recuperar datos de destino y restaurar todos esos datos al dispositivo cliente 102. En una o más realizaciones, la restauración puede ser realmente una operación de sincronización bidireccional. Además, la operación de restauración se puede realizar en segundo plano.

[0158] Durante una operación de restauración, si el cliente está activo, el cliente puede mostrar el estado al usuario, incluido el tipo de datos que se está restaurando actualmente y un porcentaje de finalización general. Además, durante una operación de restauración, el cliente puede evitar que se inicie una copia de seguridad automática hasta que se complete el proceso de restauración.

[0159] Aún más, en una o más realizaciones, durante una operación de restauración, el cliente puede proporcionar al usuario la posibilidad de pausar la operación de restauración. Cuando se encuentra en pausa, las actividades de restauración pueden ponerse en espera. Además, cuando se encuentra en pausa, el cliente puede proporcionar al usuario la capacidad de reiniciar la operación de restauración. Además, cuando se encuentra en pausa, el cliente puede suspender una copia de seguridad automática y deshabilitar una copia de seguridad manual de datos hasta que se complete la operación de restauración.

[0160] Además, en una o más realizaciones, antes de que comience una operación de restauración, el cliente puede informar al usuario de lo siguiente. El usuario puede ser informado de que los datos locales y la configuración se restaurarán en el dispositivo cliente 102. Además, se puede presentar al usuario una estimación del tiempo y el uso de datos necesarios para realizar la restauración. Además, el usuario puede ser informado de la hora y fecha en que se realizó la última copia de seguridad exitosa. Además, el usuario puede tener la oportunidad de cancelar la operación de restauración en este punto.

[0161] Asimismo, en una o más realizaciones, el cliente puede ser capaz de realizar una operación de restauración después de un inicio de sesión inicial del dispositivo. Después de que el usuario haya iniciado sesión en el dispositivo cliente 102 por primera vez, el cliente puede ofrecer al usuario la posibilidad de realizar una operación de restauración si el usuario tiene datos de copia de seguridad existentes en el servidor de sincronización 108 que pueden restaurarse en el dispositivo cliente 102. Si el usuario no tiene una copia de seguridad de los datos en el servidor de sincronización 108, el cliente no ofrece al usuario la opción de realizar una operación de restauración. Si el cliente no puede determinar si el usuario tiene una copia de seguridad de los datos en el servidor de sincronización 108, el cliente funciona como si hubiera datos disponibles en el servidor de sincronización 108 para restaurar. Si el usuario elige restaurar y no existen datos de copia de seguridad en el servidor de sincronización 108, el cliente puede informar al usuario que no se restauraron datos en el dispositivo cliente 102.

[0162] En una o más realizaciones, el cliente puede realizar las siguientes comprobaciones antes de una operación de restauración. El servidor de sincronización 108 solo puede permitir que el cliente lleve a cabo una operación de restauración si la cuenta del usuario se encuentra en el Estado B o C. Si la cuenta del usuario no se encuentra en el Estado B o C, el cliente puede mostrar un mensaje de error de inicio de sesión y cancelar la actividad de restauración.

[0163] Además, en una o más realizaciones, el cliente puede confirmar que una radio está encendida. Si la radio no está encendida, el cliente debe preguntar al usuario si quiere encender la radio. Si el usuario selecciona “sí”, el cliente enciende la radio y procede con una operación de restauración. Si el usuario selecciona “no”, el cliente puede cancelar la actividad de restauración y mostrar un mensaje de error. El cliente puede ofrecer al usuario la opción de volver a intentar la operación de restauración más tarde.

[0164] Además, en una o más realizaciones, el cliente puede confirmar que el dispositivo cliente 102 está dentro del rango de cobertura de datos. Si el dispositivo cliente 102 está fuera del rango de cobertura de datos, el cliente puede cancelar la actividad de restauración y mostrar un mensaje de error. El cliente puede ofrecer al usuario la opción de volver a intentar la operación de restauración más tarde.

[0165] Aún más, en una o más realizaciones, el cliente puede confirmar que la batería tiene suficiente carga para completar una operación de restauración. Si la batería no tiene el nivel suficiente, el cliente puede cancelar la actividad de restauración y mostrar un mensaje de error según corresponda. El cliente puede ofrecer al usuario la opción de volver a intentar la operación de restauración más tarde.

[0166] Además, en una o más realizaciones, el cliente puede confirmar que el dispositivo cliente 102 tiene suficiente memoria disponible para completar la operación de restauración. Si no hay suficiente memoria disponible, el cliente puede cancelar la actividad de restauración y mostrar un mensaje de error según corresponda. El cliente puede ofrecerle al usuario la opción de volver a intentar la operación de restauración más tarde.

[0167] En una o más realizaciones, si el cliente no puede iniciar un proceso de restauración por alguna razón, el cliente puede notificar al usuario que la restauración ha producido un error. El cliente puede ofrecerle al usuario la opción de volver a intentar la operación de restauración más tarde.

[0168] Además, en una o más realizaciones, durante una operación de restauración, si la actividad de restauración produce un error por algún motivo, el cliente puede pausar la operación de restauración y seguir un programa de reintentos. Cuando se encuentra en pausa, el cliente puede proporcionar al usuario la capacidad de reiniciar la operación de restauración. Además, cuando se encuentra en pausa, el cliente puede suspender una copia de seguridad automática y desactivar una copia de seguridad manual hasta que se complete el proceso de restauración.

[0169] Además, en una o más realizaciones, el cliente puede realizar, por ejemplo, el siguiente programa de reintentos después de encontrar un error de restauración desconocido: 1.er reintento: 1 minuto; 2.º reintento: 5 minutos; 3.er reintento: 30 minutos; 4.º reintento: 2 horas; 5.º reintento: 6 horas; 6.º reintento: 12 horas; y 7.º reintento: 24 horas. Si todos los reintentos producen errores, el cliente puede notificar al usuario según corresponda.

[0170] Además, en una o más realizaciones, el cliente puede admitir la migración (copia de seguridad desde un dispositivo, restauración a otro) desde un dispositivo cliente admitido a un dispositivo cliente diferente que ejecute el mismo sistema operativo. Además, el cliente puede convertir un formato de datos de los que se ha realizado una copia de seguridad según sea necesario para que cuando se restaure, esté en el formato adecuado para el dispositivo de destino. Además, en una o más realizaciones, el cliente puede no permitir que el usuario restaure datos de un sistema operativo a un sistema operativo diferente. Aún más, el cliente puede no restaurar configuraciones no aplicables cuando migra a un tipo diferente de dispositivo.

[0171] Además, en una o más realizaciones, el cliente puede restaurar los datos de tal manera que las actividades de sincronización periódicamente en curso por parte del usuario no se vean afectadas negativamente y no se creen duplicados en el cliente. Si el usuario ha realizado una operación de sincronización inicial y está intentando realizar una restauración, el cliente puede preguntarle al usuario si los datos del servidor o del dispositivo deberían ganar en caso de conflicto.

[0172] Después de una operación de restauración correcta, el cliente puede informar al usuario que la operación de restauración fue correcta a través de una alerta. Además, después de una restauración correcta, el cliente puede continuar con las copias de seguridad automáticas programadas.

[0173] Además, durante una operación de restauración, el cliente puede fusionar datos existentes en el dispositivo cliente 102 con datos recuperados. De esta manera, mediante el uso de un módulo de eliminación de datos duplicados 908, el proceso de restauración no crea duplicados. Por lo general, los datos duplicados pueden detectarse y eliminarse a nivel del servidor. Aquí, en una o más realizaciones, y posiblemente bajo el control del servidor de sincronización 108, se produce la eliminación de datos duplicados en el dispositivo cliente 102. En otras palabras, el módulo de eliminación de duplicados 908, al recibir de forma inalámbrica datos de usuario de los que previamente se realizó una copia de seguridad, puede detectar y eliminar elementos de datos redundantes para que solo quede una instancia de un elemento de datos particular. Los ejemplos de datos de usuario que pueden ser procesados por el módulo de eliminación de duplicados 908 incluyen datos de calendario, datos de contactos, datos de tareas, datos de notas, datos de marcadores de navegador, datos de acceso directo a aplicaciones de teléfono (por ejemplo, datos de números de marcación rápida), datos del registro de llamadas, datos de configuraciones de aplicaciones y datos del historial de mensajes SMS.

[0174] Además, en una o más realizaciones, puede no ser necesario que dos elementos de datos sean exactamente idénticos para que uno de los elementos sea eliminado por el módulo de eliminación de duplicados 908. Por ejemplo, si un primer elemento de datos del número de teléfono es “800-123-4567”, y un segundo elemento de datos del número de teléfono es “8001234567” u “(800) 123-4567”, el módulo de eliminación de duplicados 908 puede reconocer que los elementos de datos son idénticos para los datos de contacto del número de teléfono, en cuyo caso se elimina uno de los elementos de datos del número de teléfono. Además, en una o más realizaciones, el módulo de eliminación de duplicados 908 y la funcionalidad de eliminación de duplicados del sistema 100, en general, pueden

ocurrir automáticamente. En otras palabras, las diferencias entre los datos de usuario pueden resolverse automáticamente y sin consultar a un usuario.

[0175] Además, en una o más realizaciones, el módulo de eliminación de duplicados 908 puede ser capaz de detectar elementos de datos duplicados que se reciben a través de diferentes mecanismos de sincronización. Por ejemplo, los expertos en la materia observarán que varios proveedores ofrecen motores de sincronización. En general, dichos motores de sincronización sincronizan datos de diferentes tipos. Por ejemplo, puede usarse un motor de sincronización específico para sincronizar elementos de datos de contactos, calendario y notas, mientras que puede usarse otro motor de sincronización para sincronizar el historial de llamadas, los marcadores del navegador, los favoritos en el teléfono, los contactos, el calendario y los elementos de datos de notas. Por lo tanto, el dispositivo cliente 102 puede tener elementos de datos duplicados recibidos en respuesta a operaciones de sincronización realizadas con diferentes motores de sincronización. En una o más realizaciones, el módulo de eliminación de duplicados 908 es capaz de detectar elementos de datos duplicados incluso en vista del uso de diferentes motores de sincronización.

[0176] En la Figura 15 se muestra un proceso de flujo de una operación de eliminación de duplicados del lado del cliente de acuerdo con una realización de la presente invención. Inicialmente, en una base de datos particular, se lee un registro enésimo 750. Si se ha alcanzado el final de la base de datos 752, la operación de eliminación de duplicados finaliza 754. De lo contrario, si no se alcanza el final de la base de datos 752, se determina si el registro enésimo se ha eliminado 756. Si el registro se ha eliminado, “n” se incrementa 770 y el proceso retrocede y lee el nuevo registro enésimo 750.

[0177] Si el registro enésimo no se ha eliminado 756, se lee el siguiente registro 758. Si el siguiente registro marca el final de la base de datos 760, “n” se incrementa 770 y el proceso retrocede y lee el nuevo registro enésimo 750. De lo contrario, si no se ha alcanzado el final de la base de datos 760, se determina si el registro enésimo y el siguiente registro son del mismo tamaño 762. Si estos registros no son del mismo tamaño 762, se lee un nuevo registro siguiente 758 para su posterior comparación con el registro enésimo. Sin embargo, si el registro enésimo y el siguiente registro son del mismo tamaño 762, se realiza una comparación binaria en el registro enésimo y el siguiente registro 764. Si la comparación binaria indica que los registros no son idénticos 766, entonces se lee un nuevo siguiente registro 758 para la comparación posterior con el registro enésimo. Sin embargo, si la comparación binaria indica que el registro enésimo y el siguiente registro son idénticos 766, el siguiente registro se elimina 768 y se lee un nuevo siguiente registro 758 para la comparación posterior con el registro enésimo. Además, los expertos en la materia observarán que, de la manera descrita anteriormente, se puede realizar una operación de comparación binaria solo cuando sea necesaria (por ejemplo, después de la comparación de tamaños y otras comprobaciones) para evitar operaciones de comparación binaria innecesarias.

[0178] En una o más realizaciones, puede especificarse el conjunto de bases de datos sujetas a eliminación de duplicados, como se ha descrito anteriormente, en una lista de preferencias de usuario o administrador. Además, las preferencias pueden indicar los tipos de datos de los que se desean eliminar los duplicados. Diferentes tipos de bases de datos pueden corresponder a diferentes motores de sincronización utilizados por el dispositivo cliente 102 para realizar la sincronización de datos.

[0179] Si bien la invención se ha descrito con respecto a un número limitado de realizaciones, los expertos en la técnica, a la vista de la descripción anterior, apreciarán que se pueden concebir otras realizaciones que no abandonen el ámbito de la presente invención, tal y como se ha descrito en el presente. Por consiguiente, el ámbito de la presente invención debe estar limitado solo por las reivindicaciones adjuntas. Por ejemplo, en las realizaciones del sistema definido por cualquiera de las reivindicaciones 1 a 6 adjuntas o el método definido por cualquiera de las reivindicaciones 7 a 13 adjuntas, los datos de usuario pueden comprender al menos uno de los siguientes elementos: datos de calendario, datos de contactos, datos de tareas, datos de notas, datos de marcadores de navegador, datos de acceso directo a aplicaciones telefónicas, datos de números de marcación rápida, datos de registro de llamadas, datos de configuración de aplicaciones y datos del historial de mensajes SMS.

[0180] Las realizaciones del sistema definidas por cualquiera de las reivindicaciones adjuntas 1 a 6 pueden comprender un dispositivo cliente configurado para comunicarse de forma inalámbrica con al menos uno de los siguientes servidores: el servidor de aplicaciones web, el servidor de administración de cuentas y el servidor de sincronización a través de al menos uno de una solicitud HTTP, un mensaje SMS, un canal de voz y un canal de datos; y/o en el que el dispositivo informático es un dispositivo cliente; y/o el dispositivo informático es cualquiera de los siguientes: un teléfono móvil, un asistente digital personal, un dispositivo de correo electrónico portátil, un ordenador de escritorio y un ordenador portátil.

[0181] Las realizaciones del método definido por una cualquiera de las reivindicaciones adjuntas 7 a 13 en las que el dispositivo informático puede ser cualquiera de los siguientes: un teléfono móvil, un asistente digital personal, un dispositivo de correo electrónico portátil, un ordenador de escritorio y un ordenador portátil; y/o en el que el dispositivo informático es un dispositivo cliente; y/o el dispositivo informático es un dispositivo informático del lado del cliente.

[0182] Las realizaciones del dispositivo informático móvil definido por las reivindicaciones adjuntas 14 a 20 pueden ser cualquiera de las siguientes: un teléfono móvil, un asistente personal digital, un dispositivo de correo electrónico portátil y un ordenador portátil.

[0183] En realizaciones del sistema definido por cualquiera de las reivindicaciones adjuntas 1 a 6, la red de comunicaciones inalámbricas es al menos en parte cualquiera de las siguientes: una red de área amplia, una red de área local, una red de telefonía móvil, una red de radio, una red inalámbrica en malla y una red basada en Internet.

[0184] Una o más realizaciones pueden incluir un programa informático que comprende elementos de programa legibles por ordenador o máquina operativos para configurar un sistema y/o un dispositivo informático móvil de acuerdo con cualquiera de las reivindicaciones adjuntas 1 a 6 y/o 14 a 20 y/u operativos en un sistema y/o dispositivo informático móvil para implementar el método de cualquiera de las reivindicaciones adjuntas 7 a 13; y en particular materializado como un medio portador de programa informático que contiene el programa informático.

REIVINDICACIONES

1. Un sistema (100) que comprende:
un dispositivo informático que tiene una pantalla;
una interfaz de instrucciones configurada para recibir una instrucción de un usuario para restringir el acceso a los datos de usuario almacenados en el dispositivo informático; y
una interfaz de transmisión configurada para transmitir de forma inalámbrica (956) un comando informático ejecutable por el dispositivo informático, en donde se genera (954) el comando informático como respuesta a la instrucción de restringir el acceso a los datos de usuario, en donde la ejecución del comando informático tiene como resultado que el dispositivo informático lleve a cabo la restricción de la accesibilidad a los datos de usuario, y el comando informático se ejecuta con independencia de si el dispositivo informático está conectado a una red de servicios, en donde la ejecución del comando informático tiene como resultado que el dispositivo informático bloquee el acceso a los datos de usuario (966) mediante el uso del dispositivo informático, y en donde se puede acceder a una funcionalidad telefónica del dispositivo informático durante una restricción de la accesibilidad a los datos de usuario mediante el bloqueo del acceso a los datos de usuario desde el dispositivo informático, y la funcionalidad telefónica comprende el marcado de un número de teléfono especificado por el usuario, en donde el número de teléfono especificado por el usuario es recibido con la instrucción.

2. El sistema (100) de la reivindicación 1, en donde la ejecución del comando informático tiene como resultado que el dispositivo informático:
bloquee el acceso a los datos de usuario mediante el uso del dispositivo informático; y/o
borre los datos de usuario en el dispositivo informático, opcionalmente transmitiendo de forma inalámbrica una copia de los datos de usuario antes de borrar los datos de usuario.

3. El sistema (100) de la reivindicación 1, en donde:
el comando informático se comunica de manera inalámbrica en forma de un mensaje HTTP o un mensaje SMS, o ambos; y/o
el dispositivo informático está configurado para transmitir de forma inalámbrica una señal de estado que indica la finalización o el error de la restricción de accesibilidad a los datos de usuario; y/o
la interfaz de instrucciones está configurada además para autenticar el usuario antes de enviar de forma inalámbrica el comando informático al dispositivo informático; y/o
el comando informático no depende de un motor de sincronización utilizado por el dispositivo informático para sincronizar datos.

4. El sistema (100) de cualquiera de las reivindicaciones 1 a 3, en donde la funcionalidad telefónica comprende además desbloquear el dispositivo informático mediante la introducción de una contraseña de cuenta en la pantalla del dispositivo informático.

5. El sistema (100) de cualquiera de las reivindicaciones 1 a 4, en donde la funcionalidad telefónica comprende además el marcado de los servicios de emergencia.

6. El sistema (100) de cualquiera de las reivindicaciones 1 a 5, en donde el número de teléfono especificado por el usuario no es visible en la pantalla del dispositivo informático.

7. Un método para administrar un dispositivo informático que tiene una pantalla, el cual comprende:
la recepción de una instrucción de un usuario para restringir el acceso a los datos de usuario almacenados en el dispositivo informático;
la autenticación del usuario;
en respuesta a una autenticación correcta, la generación de un comando de restricción correspondiente a la instrucción recibida;
la transmisión de forma inalámbrica del comando de restricción al dispositivo informático para su ejecución por el dispositivo informático;
la ejecución del comando de restricción, en donde el comando de restricción se ejecuta con independencia de si el dispositivo informático está conectado a una red de servicios, en donde la ejecución del comando de restricción tiene como resultado que el dispositivo informático:
(a) bloquee el acceso a los datos de usuario mediante el uso del dispositivo informático; o
(b) bloquee el acceso a los datos de usuario mediante el uso del dispositivo informático y realizando una copia de seguridad inalámbrica de los datos de usuario en un almacén de datos remoto; y
permita que se pueda acceder a la funcionalidad telefónica del dispositivo informático durante la restricción de la accesibilidad a los datos de usuario al bloquear el acceso a los datos de usuario mediante el uso del dispositivo informático, y la funcionalidad telefónica comprende el marcado de un número de teléfono especificado por el usuario, en el que el número de teléfono especificado por el usuario se recibe con la instrucción.

8. El método de la reivindicación 7, que además comprende:
la recepción de una confirmación del dispositivo informático, indicando esta confirmación si el comando de restricción ha sido ejecutado correctamente por el dispositivo informático.

9. El método de la reivindicación 7 u 8, en donde la ejecución del comando de restricción tiene como resultado que el dispositivo informático:
borre los datos de usuario del dispositivo cliente; y/o
bloquee el acceso a los datos de usuario mediante el uso del dispositivo informático y borre los datos de usuario del dispositivo informático; y/o
bloquee el acceso a los datos de usuario mediante el uso del dispositivo informático, realice una copia de seguridad inalámbrica de los datos de usuario en un almacén de datos remoto y borre los datos de usuario del dispositivo informático.

10. El método de cualquiera de las reivindicaciones 7 a 9, en donde:
el comando de restricción se comunica de forma inalámbrica al dispositivo informático en forma de un mensaje HTTP y un mensaje SMS; y/o
el comando de restricción no depende de un motor de sincronización (108) utilizado por el dispositivo informático para sincronizar datos.

11. El método de cualquiera de las reivindicaciones 7 a 10, en donde la funcionalidad telefónica comprende además desbloquear el dispositivo informático mediante la introducción de una contraseña de cuenta en la pantalla del dispositivo informático.

12. El método de cualquiera de las reivindicaciones 7 a 11, en donde la funcionalidad telefónica comprende además el marcado de los servicios de emergencia.

13. El método de cualquiera de las reivindicaciones 7 a 12, en donde el número de teléfono especificado por el usuario no es visible en la pantalla del dispositivo informático.

14. Un dispositivo informático móvil que tiene una pantalla y comprende:
un primer módulo configurado para recibir de forma inalámbrica una instrucción y configurado además para, en respuesta a la recepción de la instrucción, bloquear el acceso a los datos de usuario en el dispositivo informático móvil utilizando el dispositivo informático móvil, y los datos de usuario se bloquean con independencia de si el dispositivo informático está conectado a una red de servicios; y
un segundo módulo configurado para habilitar la funcionalidad telefónica del dispositivo informático móvil, en donde el segundo módulo está configurado además para permitir la accesibilidad a la funcionalidad telefónica mientras el primer módulo ha bloqueado los datos de usuario al bloquear el acceso a los datos de usuario mediante el uso del dispositivo informático, y la funcionalidad telefónica comprende el marcado de un número de teléfono especificado por el usuario, en donde el número de teléfono especificado por el usuario es recibido con la instrucción.

15. El dispositivo informático móvil de la reivindicación 14, en donde la instrucción:
se recibe de forma inalámbrica en forma de un mensaje HTTP o un mensaje SMS, o ambos; y/o
no depende de un motor de sincronización (108) utilizado por el dispositivo informático móvil para sincronizar datos; y/o
se recibe de forma inalámbrica por el dispositivo informático móvil en respuesta a una instrucción de usuario recibida y autenticada en un sistema remoto.

16. El dispositivo informático móvil de cualquiera de las reivindicaciones 14 o 15, en donde el segundo módulo está configurado además para realizar de forma inalámbrica una copia de seguridad de los datos de usuario en un almacén de datos remoto antes de borrar los datos de usuario; y/o
en donde el primer módulo está configurado además para transmitir de forma inalámbrica una señal de estado que indica, o bien la finalización correcta, o bien un error en el bloqueo de los datos de usuario; y/o
en donde el segundo módulo está configurado además para transmitir de forma inalámbrica una señal de estado que indica, o bien la finalización correcta, o bien un error en el borrado de los datos de usuario.

17. El dispositivo informático móvil de cualquiera de las reivindicaciones 14 a 16, que además comprende:
un tercer módulo configurado para habilitar la funcionalidad telefónica del dispositivo informático móvil, en donde el tercer módulo está configurado además para permitir la accesibilidad a la funcionalidad telefónica mientras que el primer módulo ha bloqueado los datos de usuario o el segundo módulo ha borrado los datos de usuario, o se han realizado ambas acciones.

18. El dispositivo informático móvil de cualquiera de las reivindicaciones 14 a 17, en donde la funcionalidad telefónica comprende además desbloquear el dispositivo informático mediante la introducción de una contraseña de cuenta en la pantalla del dispositivo informático.

19. El dispositivo informático móvil de cualquiera de las reivindicaciones 14 a 18, en donde la funcionalidad telefónica comprende además el marcado de los servicios de emergencia.

20. El dispositivo informático móvil de cualquiera de las reivindicaciones 14 a 19, en donde el número de teléfono especificado por el usuario no es visible en la pantalla del dispositivo informático.

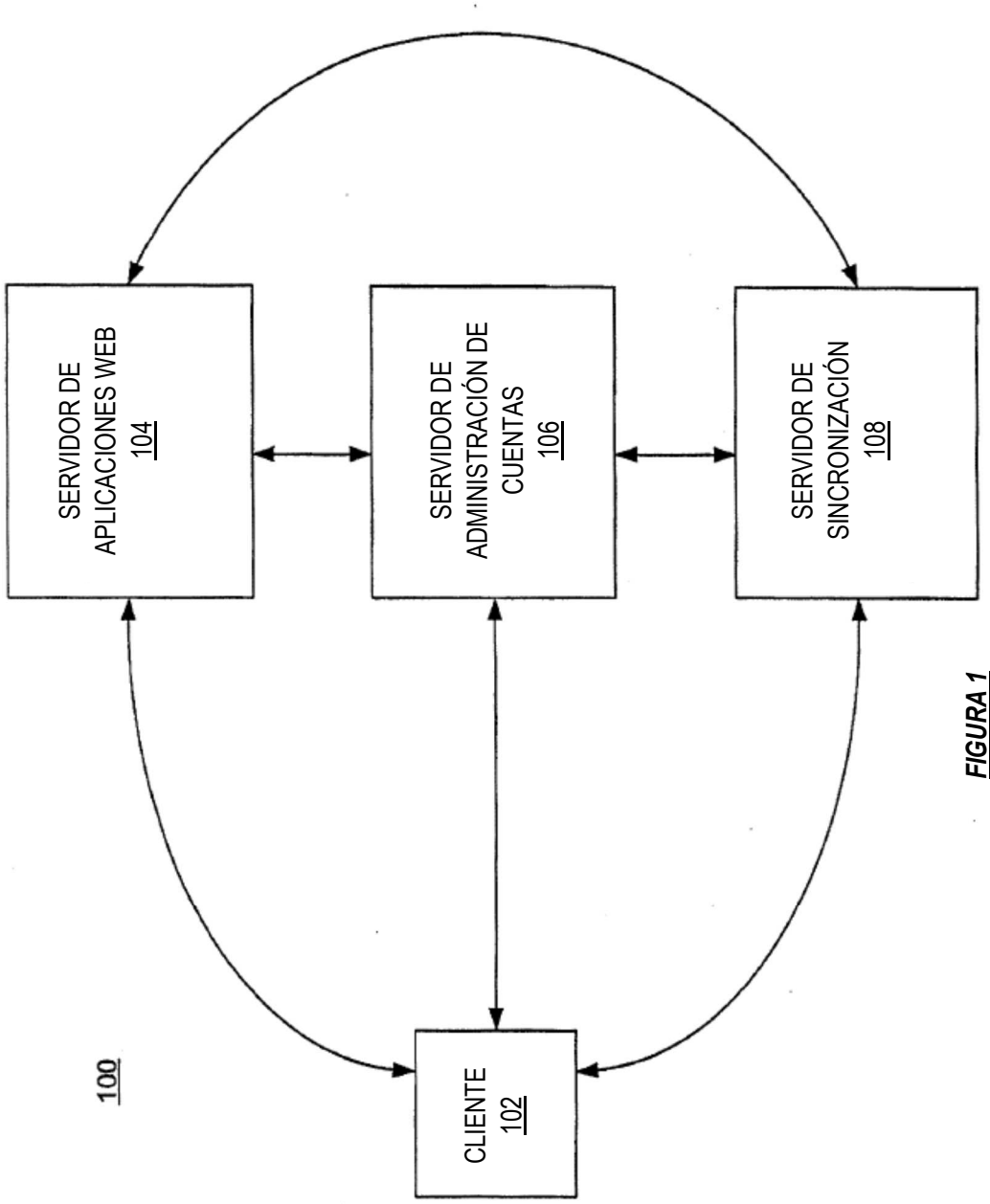
SERVIDOR DE APLICACIONES WEB 104
SERVIDOR DE ADMINISTRACIÓN DE CUENTAS 106
SERVIDOR DE SINCRONIZACIÓN 108
CLIENTE 102
100

FIGURA 1

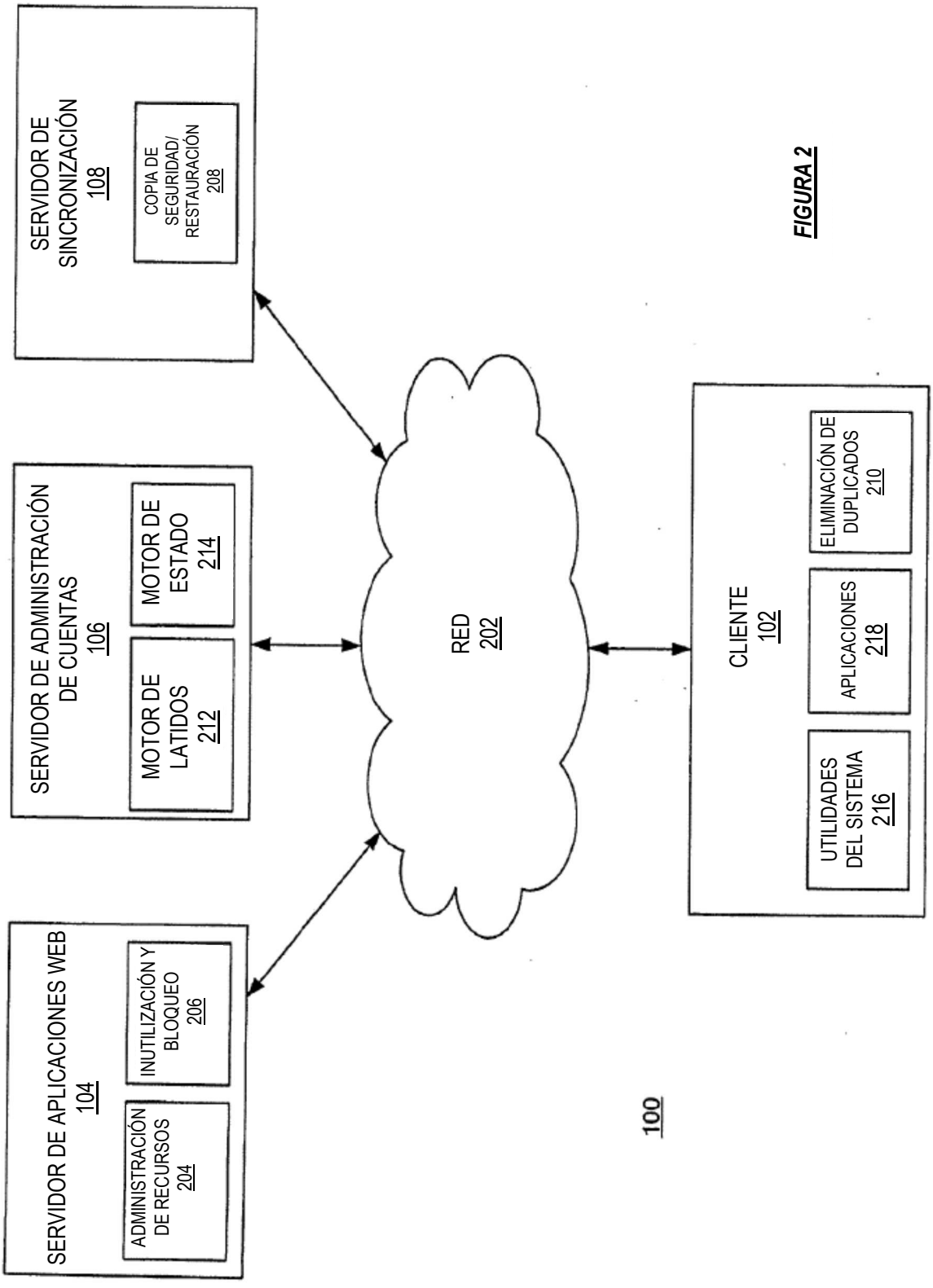
SERVIDOR DE SINCRONIZACIÓN 108
COPIA DE SEGURIDAD/ RESTAURACIÓN 208
SERVIDOR DE ADMINISTRACIÓN DE CUENTAS 106
MOTOR DE LATIDOS 212
MOTOR DE ESTADO 214
SERVIDOR DE APLICACIONES WEB 104
ADMINISTRACIÓN DE RECURSOS 204
INUTILIZACIÓN Y BLOQUEO 206
RED 202
CLIENTE 102
UTILIDADES DEL SISTEMA 216
APLICACIONES 218
ELIMINACIÓN DE DUPLICADOS 210
100

FIGURA 2

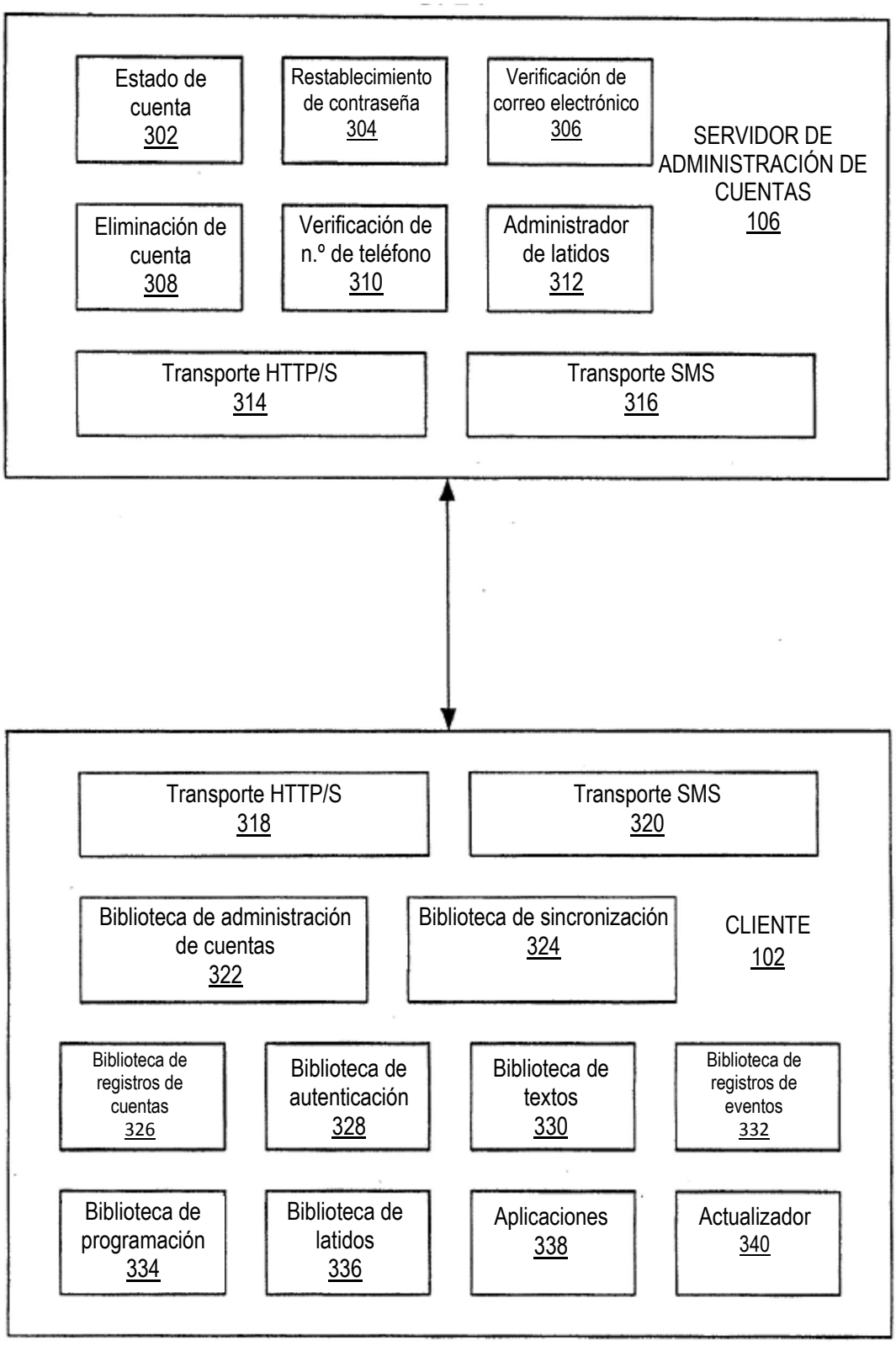
Estado de cuenta 302
Restablecimiento de contraseña 304
Verificación de correo electrónico 306
SERVIDOR DE ADMINISTRACIÓN DE CUENTAS 106
Eliminación de cuenta 308
Verificación de n.º de teléfono 310
Administrador de latidos 312
Transporte HTTP/S 314
Transporte SMS 316
Transporte HTTP/S 318
Transporte SMS 320
Biblioteca de administración de cuentas 322
Biblioteca de sincronización 324
CLIENTE 102
Biblioteca de registros de cuentas 326
Biblioteca de autenticación 328
Biblioteca de textos 330
Biblioteca de registros de eventos 332
Biblioteca de programación 334
Biblioteca de latidos 336
Aplicaciones 338
Actualizador 340

FIGURA 3

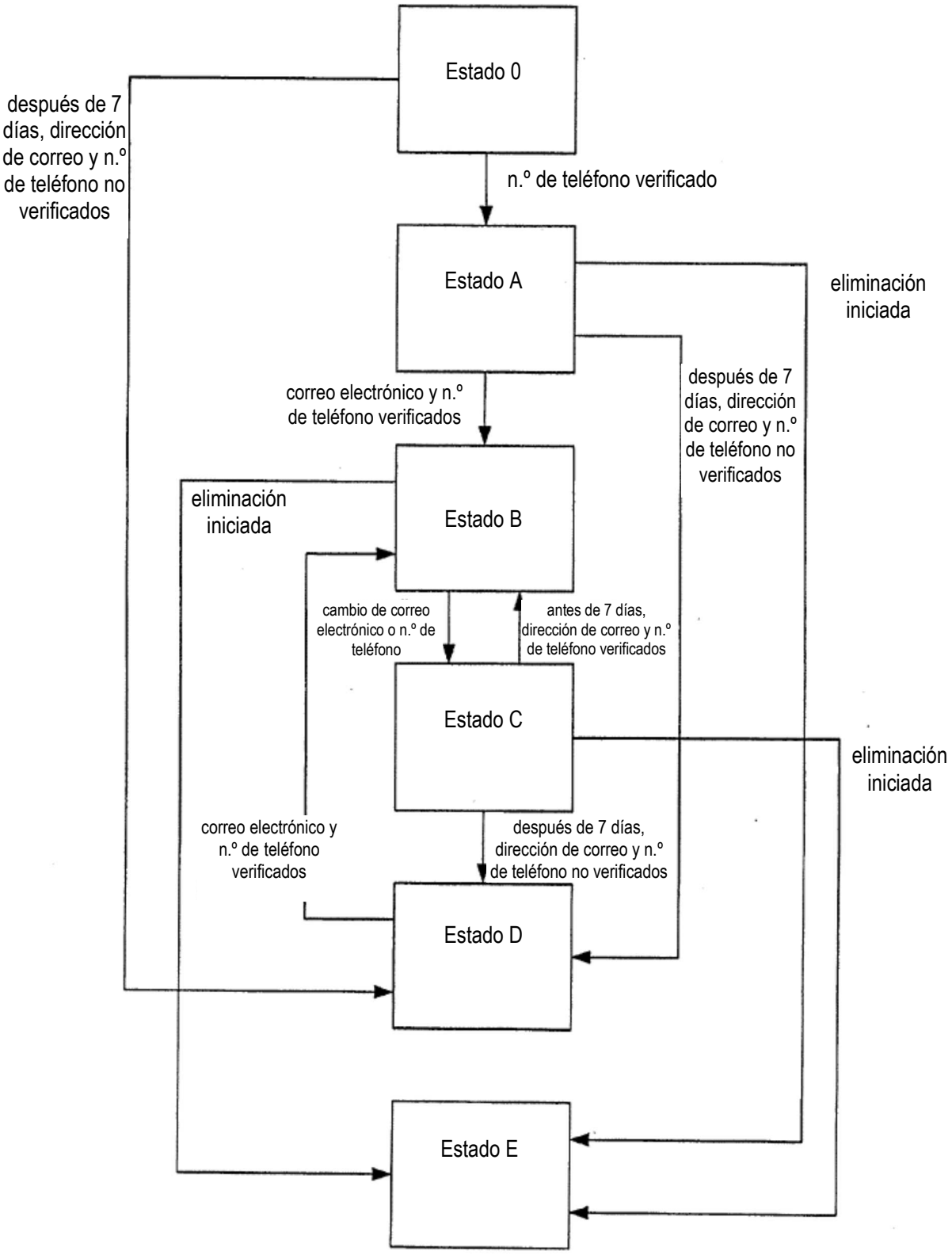
Estado 0
después de 7 días, dirección de correo y n.º de teléfono no verificados
n.º de teléfono verificado
Estado A
eliminación iniciada
después de 7 días, dirección de correo y n.º de teléfono no verificados
correo electrónico y n.º de teléfono verificados
eliminación iniciada
Estado B
cambio de correo electrónico o n.º de teléfono
antes de 7 días, dirección de correo y n.º de teléfono verificados
Estado C
eliminación iniciada
correo electrónico y n.º de teléfono verificados
después de 7 días, dirección de correo y n.º de teléfono no verificados
Estado D
Estado E

FIGURA 4

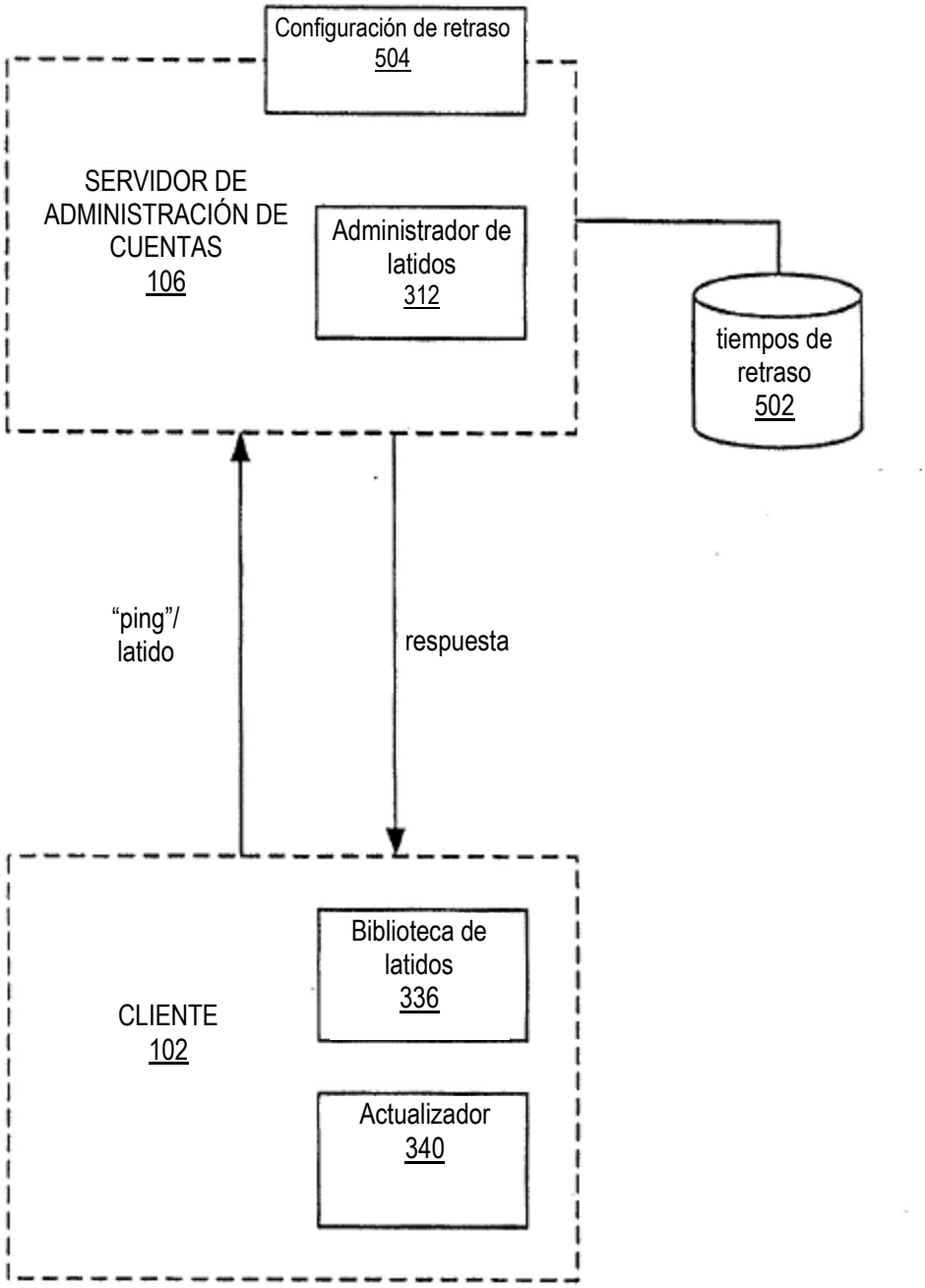
Configuración de retraso
504
SERVIDOR DE ADMINISTRACIÓN DE CUENTAS
106
Administrador de latidos
312
tiempos de retraso
502
"ping"/ latido
respuesta
CLIENTE
102
Biblioteca de latidos
336
Actualizador
340

FIGURA 5

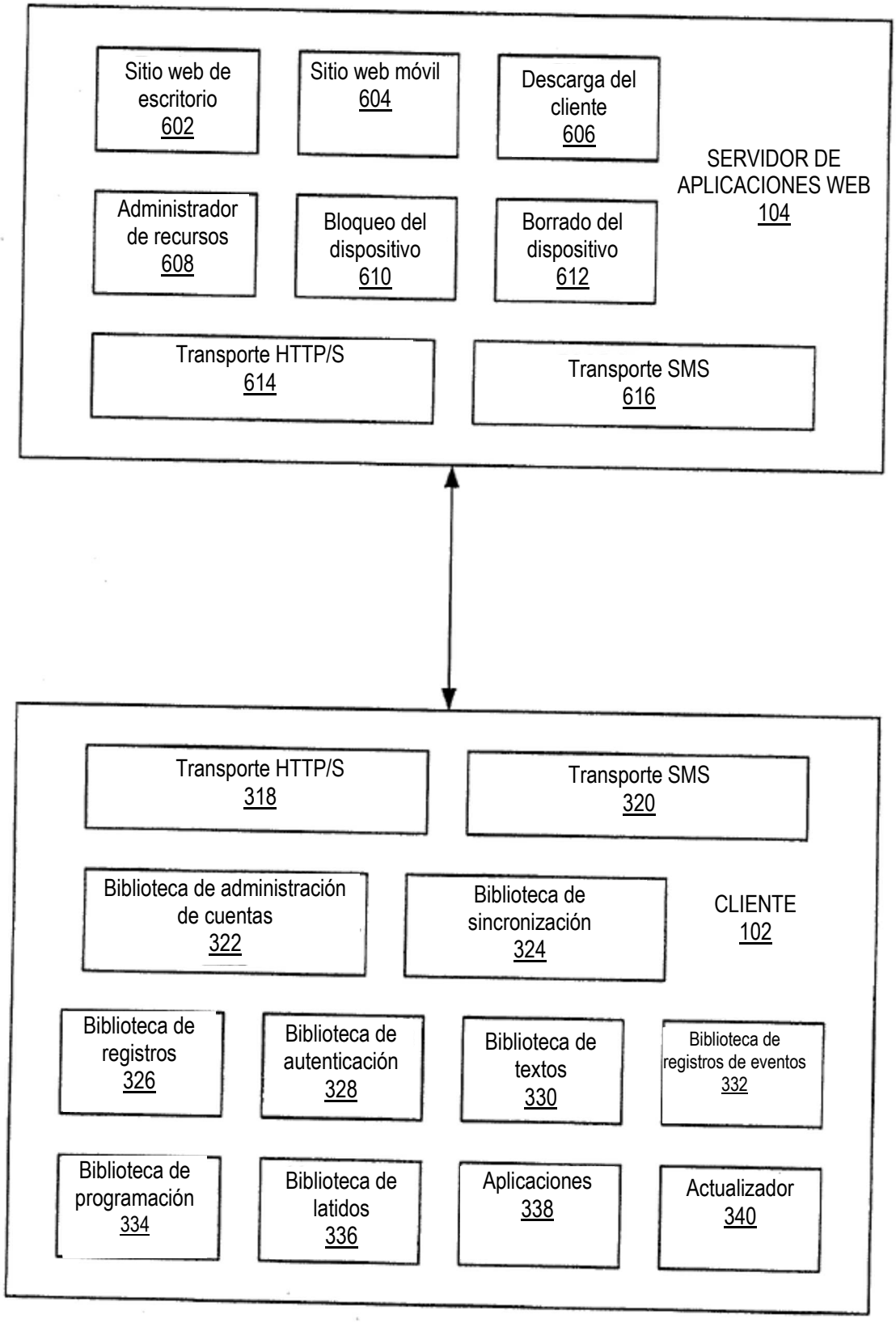
Sitio web de escritorio 602
Sitio web móvil 604
Descarga del cliente 606
SERVIDOR DE APLICACIONES WEB 104
Administrador de recursos 608
Bloqueo del dispositivo 610
Borrado del dispositivo 612
Transporte HTTP/S 614
Transporte SMS 616
Transporte HTTP/S 318
Transporte SMS 320
Biblioteca de administración de cuentas 322
Biblioteca de sincronización 324
CLIENTE 102
Biblioteca de registros 326
Biblioteca de autenticación 328
Biblioteca de textos 330
Biblioteca de registros de eventos 332
Biblioteca de programación 334
Biblioteca de latidos 336
Aplicaciones 338
Actualizador 340

FIGURA 6

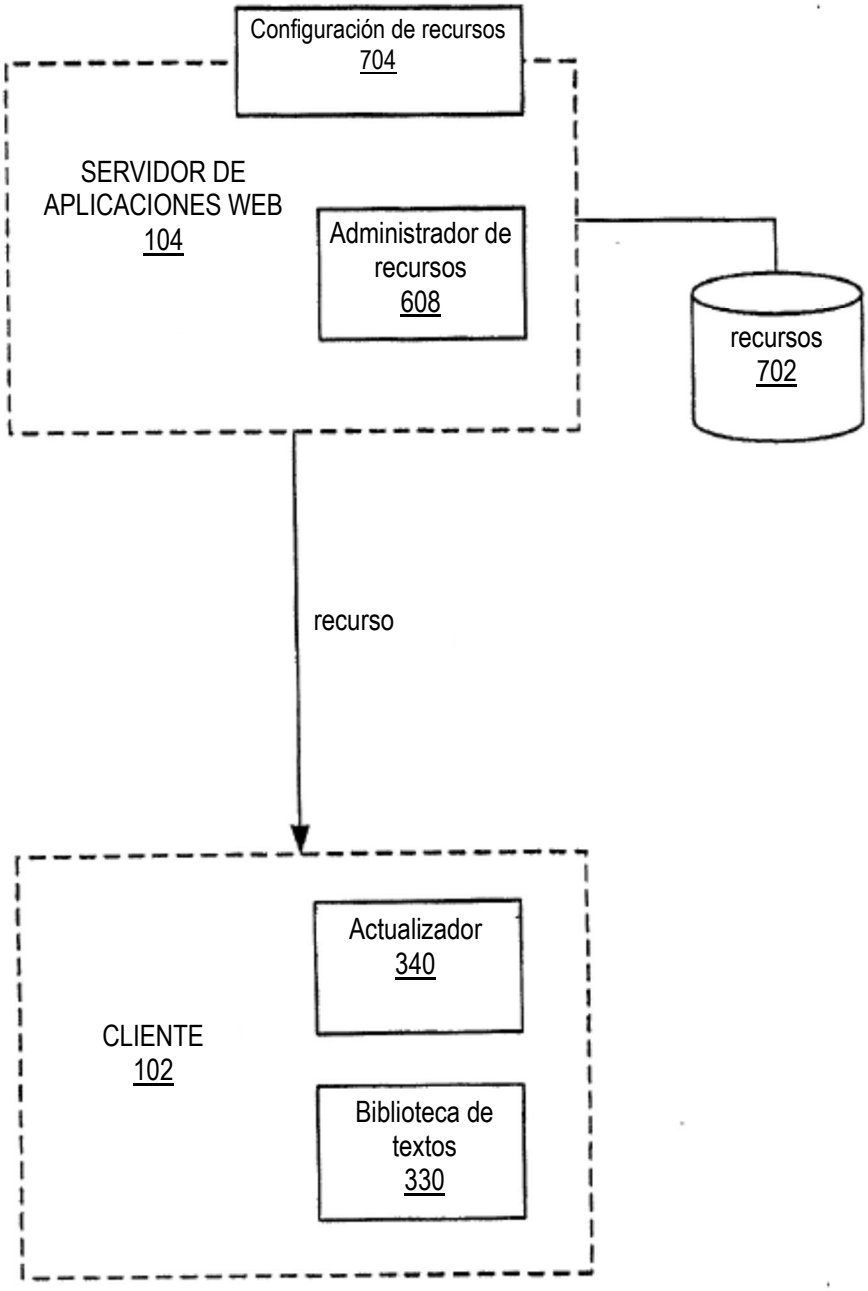
Configuración de recursos
704
SERVIDOR DE APLICACIONES WEB
104
Administrador de recursos
608
recursos
702
recurso
Actualizador
340
CLIENTE
102
Biblioteca de textos
330

FIGURA 7

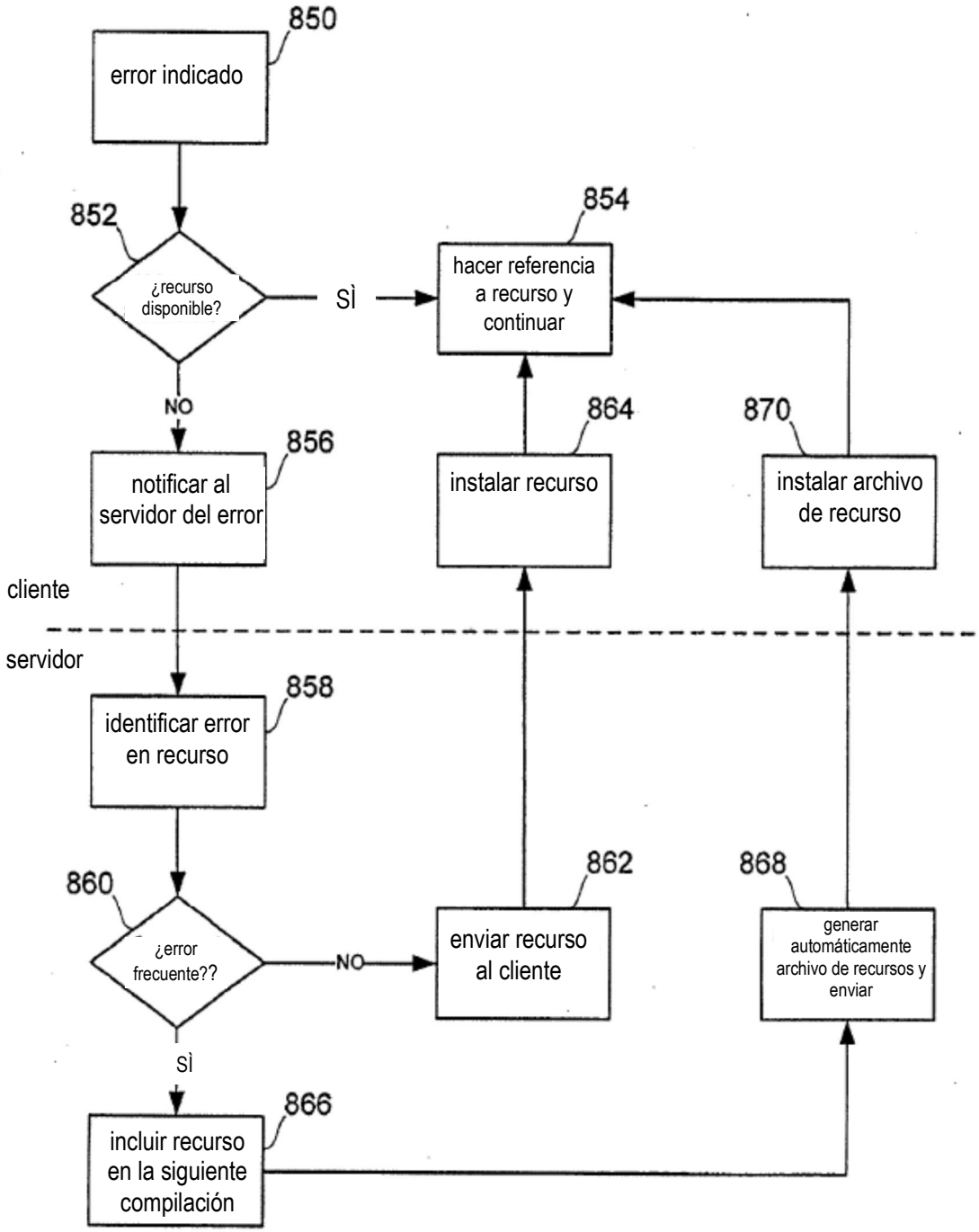
850
error indicado
852
¿recurso disponible?
SÌ
854
hacer referencia a recurso y continuar
NO
856
notificar al servidor del error
864
instalar recurso
870
instalar archivo de recurso
cliente
servidor
858
identificar error en recurso
860
¿error frecuente??
NO
862
enviar recurso al cliente
868
generar automáticamente archivo de recursos y enviar
SÌ
866
incluir recurso en la siguiente compilación

FIGURA 8

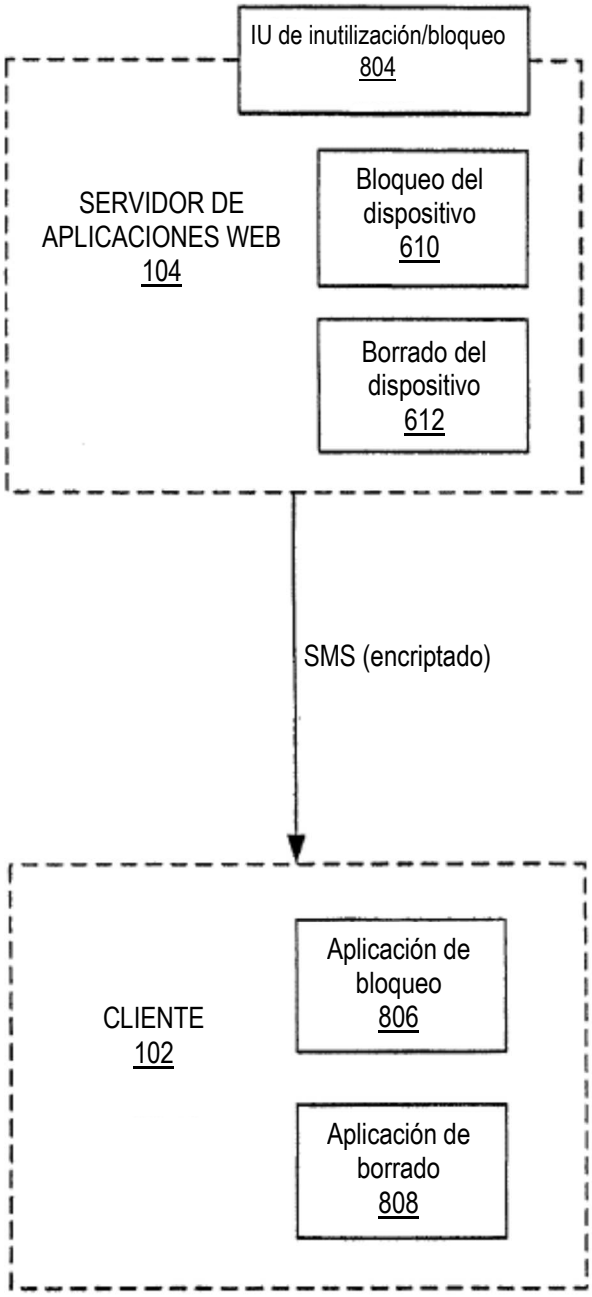
IU de inutilización/bloqueo
804
SERVIDOR DE APLICACIONES WEB
104
Bloqueo del dispositivo
610
Borrado del dispositivo
612
SMS (encriptado)
CLIENTE
102
Aplicación de bloqueo
806
Aplicación de borrado
808

FIGURA 9

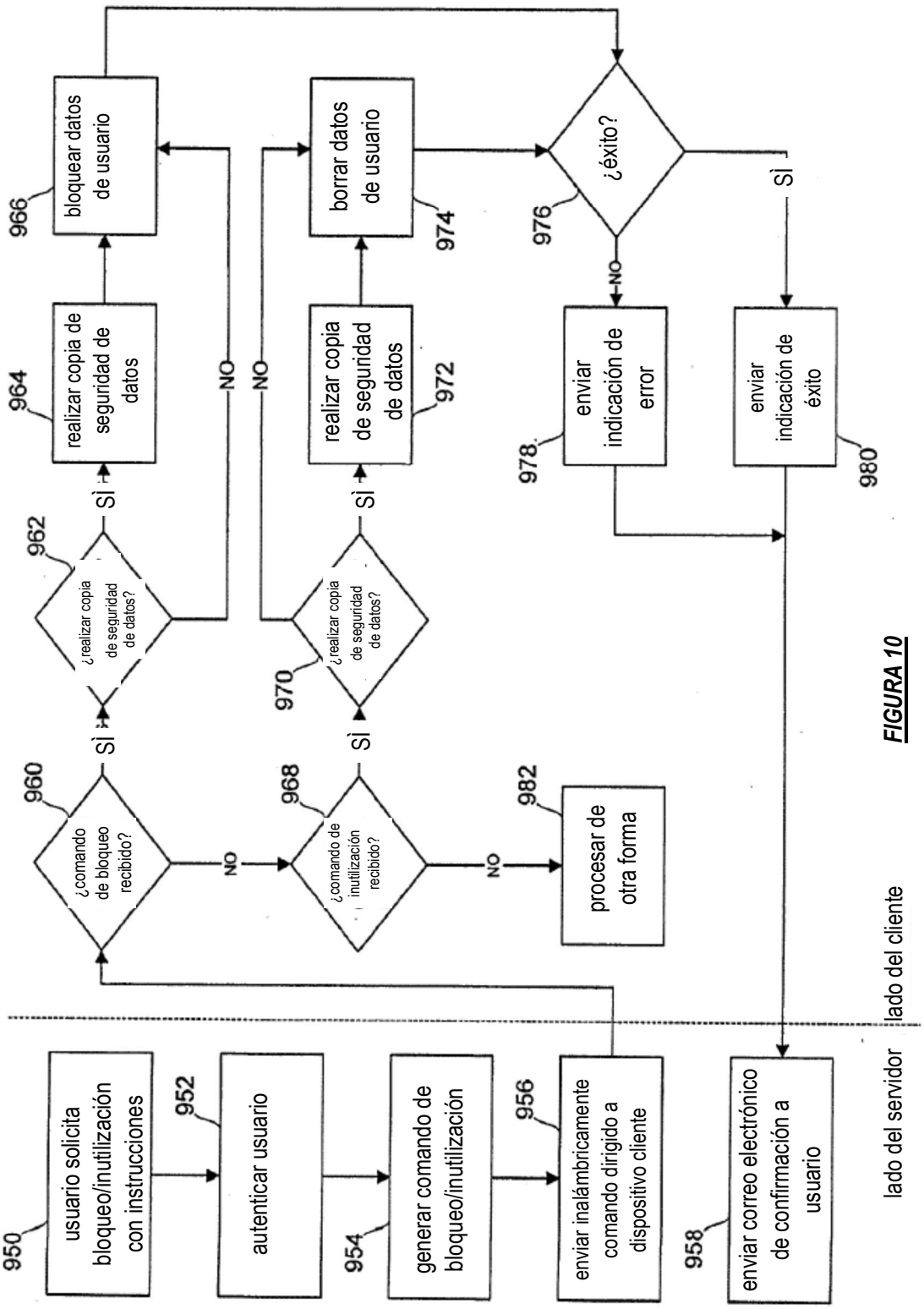
lado del cliente
lado del servidor
950
usuario solicita bloqueo/inutilización con instrucciones
952
autenticar usuario
954
generar comando de bloqueo/inutilización
956
enviar inalámbricamente comando dirigido a dispositivo cliente
958
enviar correo electrónico de confirmación a usuario
960
¿comando de bloqueo recibido?
962
¿realizar copia de seguridad de datos?
964
realizar copia de seguridad de datos
966
bloquear datos de usuario
968
¿comando de inutilización recibido?
970
¿realizar copia de seguridad de datos?
972
realizar copia de seguridad de datos
974
borrar datos de usuario
976
¿éxito?
978
enviar indicación de error
980
enviar indicación de éxito
982
procesar de otra forma
SÌ
NO

FIGURA 10

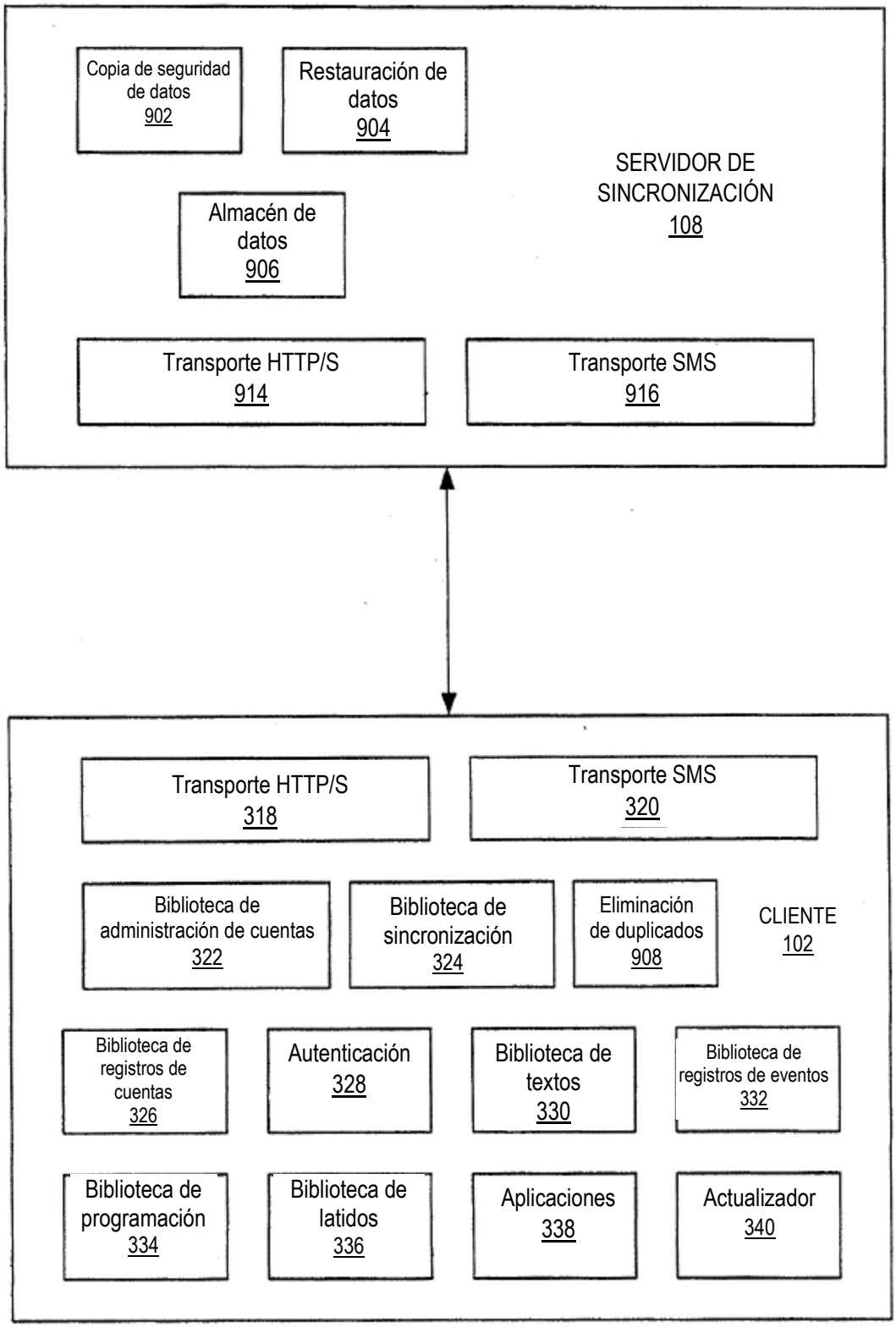
Copia de seguridad de datos 902
Restauración de datos 904
SERVIDOR DE SINCRONIZACIÓN 108
Almacén de datos 906
Transporte HTTP/S 914
Transporte SMS 916
Transporte HTTP/S 318
Transporte SMS 320
Biblioteca de administración de cuentas 322
Biblioteca de sincronización 324
Eliminación de duplicados 908
CLIENTE 102
Biblioteca de registros de cuentas 326
Autenticación 328
Biblioteca de textos 330
Biblioteca de registros de eventos 332
Biblioteca de programación 334
Biblioteca de latidos 336
Aplicaciones 338
Actualizador 340

FIGURA 11

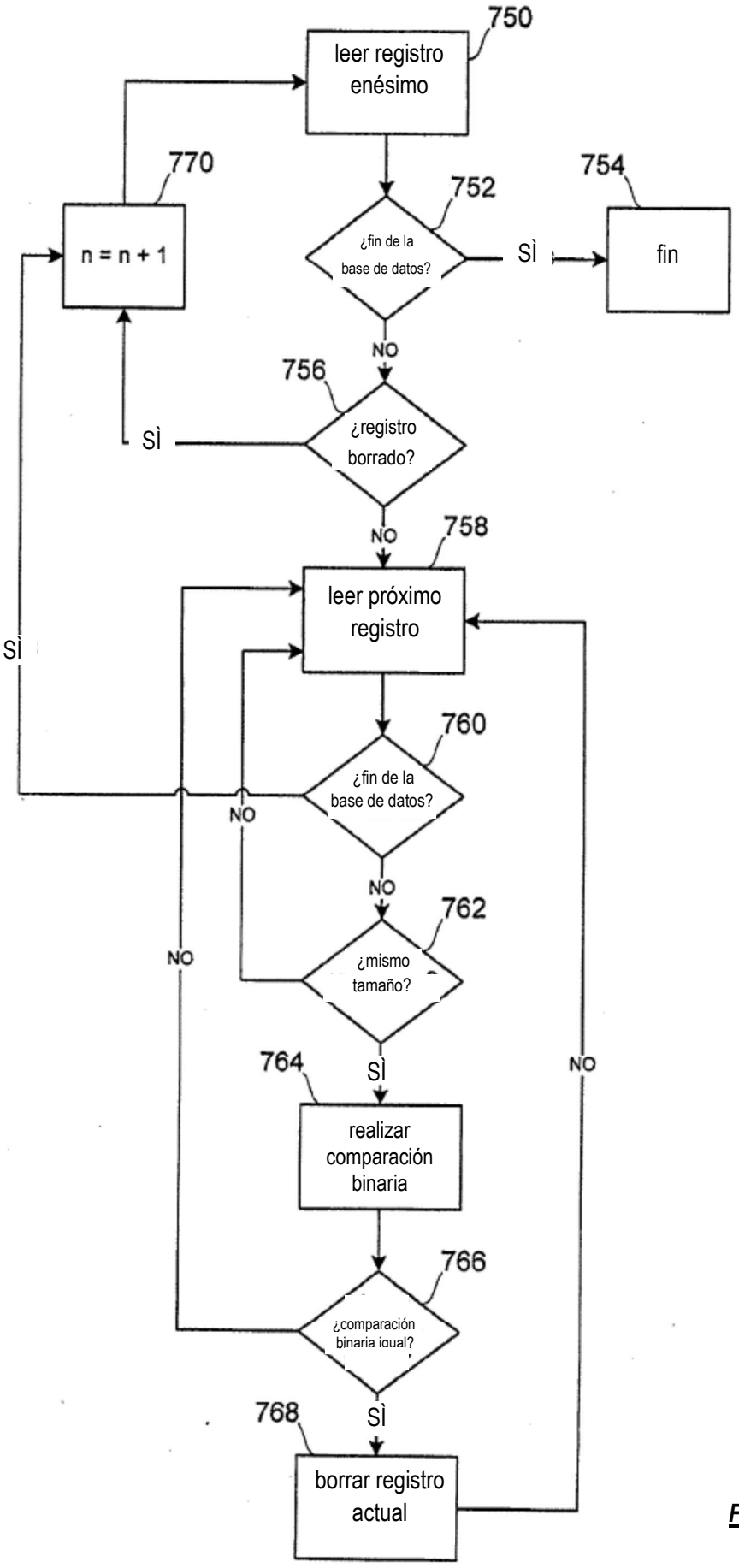
750
leer registro enésimo
770
n = n + 1
752
¿fin de la base de datos?
SÌ
754
fin
NO
756
¿registro borrado?
SÌ
NO
758
leer próximo registro
SÌ
760
¿fin de la base de datos?
NO
NO
762
¿mismo tamaño?
NO
764
SÌ
realizar comparación binaria
NO
766
¿comparación binaria igual?
768
SÌ
borrar registro actual

FIGURA 12

FIGURA 13

FIGURA 14

FIGURA 15

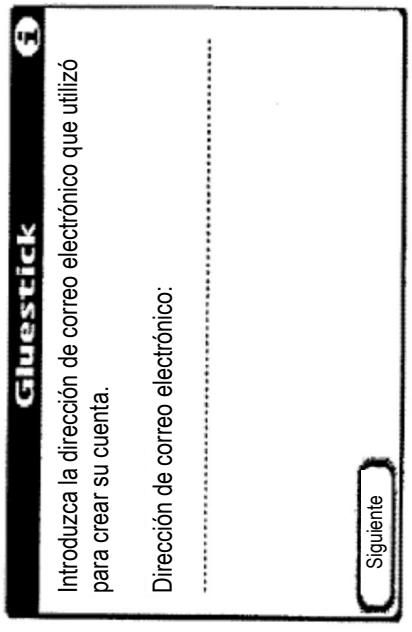

FIGURA 16

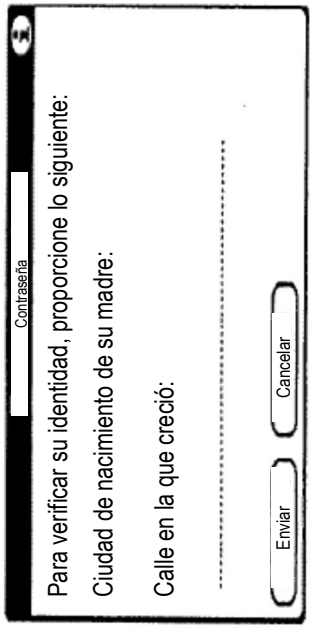

FIGURA 17

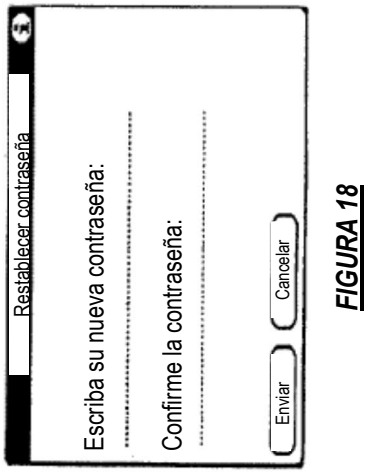

FIGURA 18

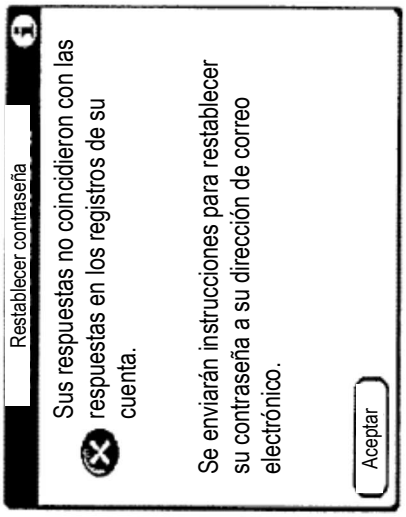

FIGURA 19

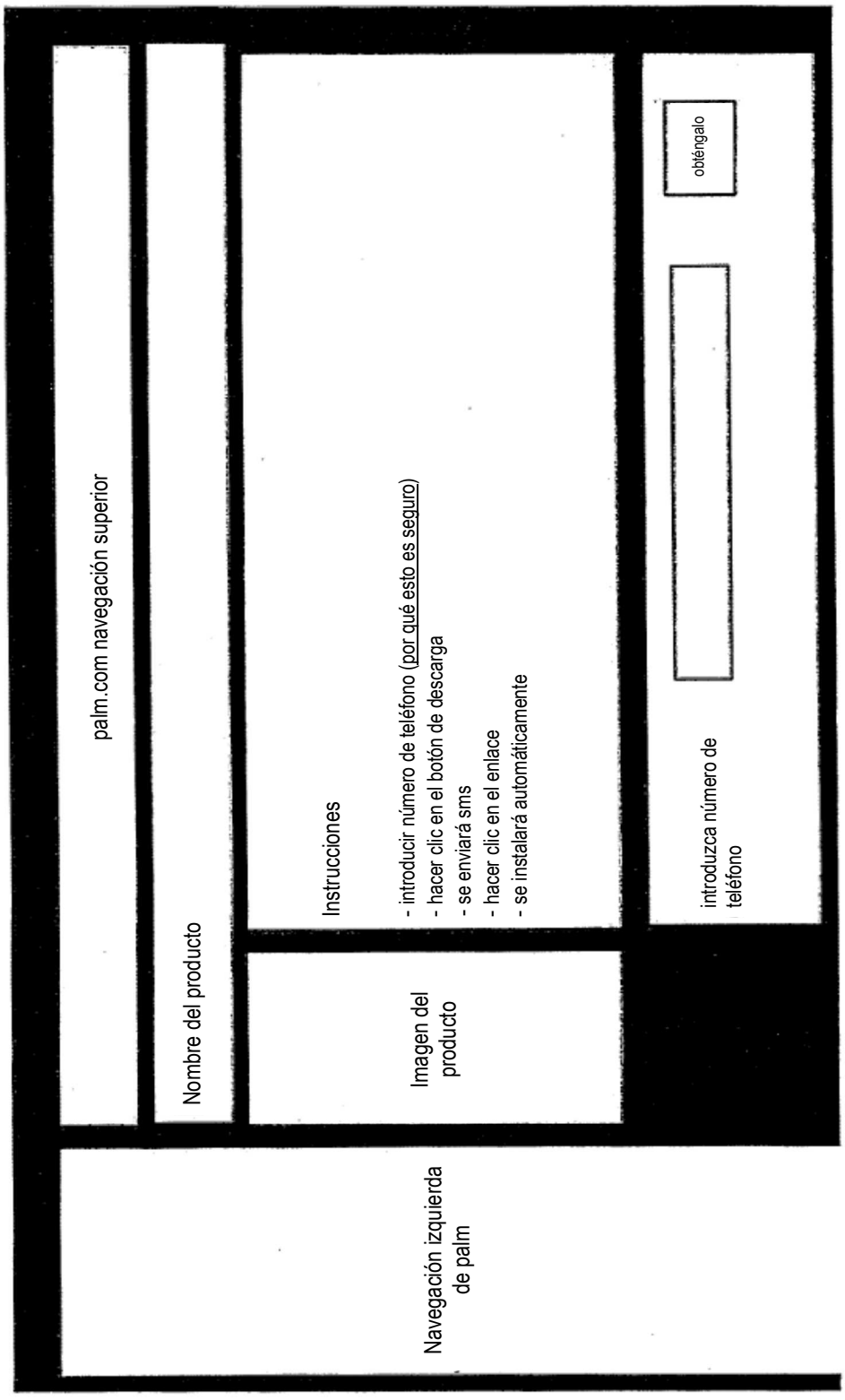
palm.com navegación superior
Nombre del producto
Instrucciones
- introducir número de teléfono (por qué esto es seguro)
- hacer clic en el botón de descarga
- se enviará sms
- hacer clic en el enlace
- se instalará automáticamente
Imagen del producto
introduzca número de teléfono
obténgalo
Navegación izquierda de palm

FIGURA 20

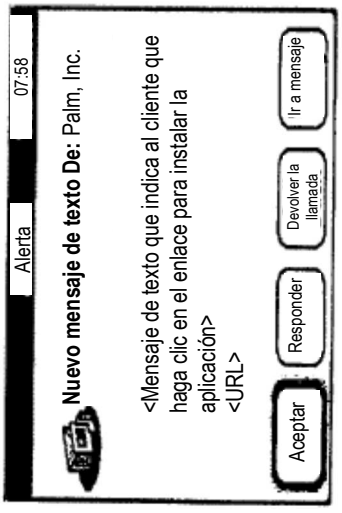

FIGURA 21

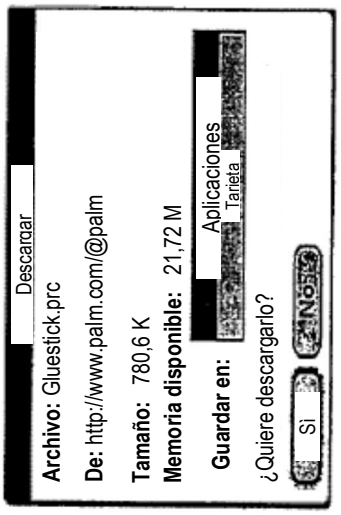

FIGURA 22

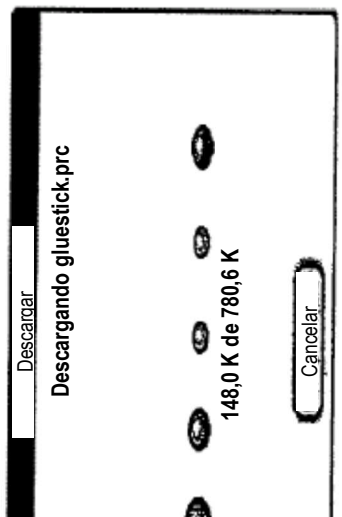

FIGURA 23

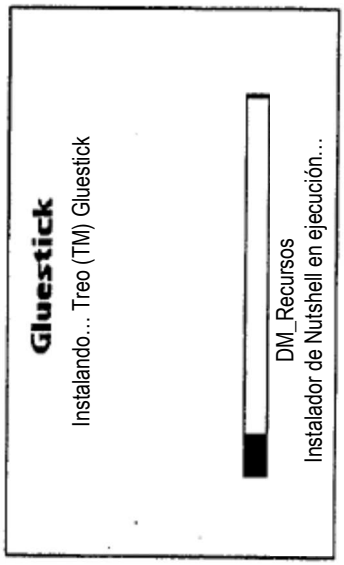

FIGURA 24

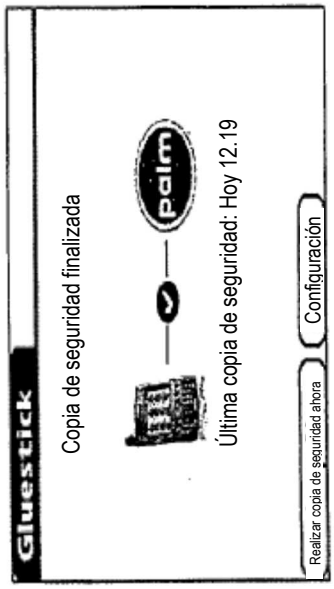

FIGURA 26

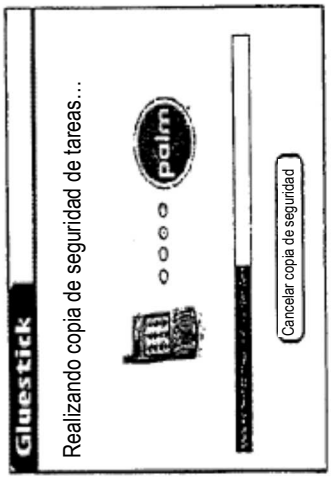

FIGURA 25

FIGURA 28

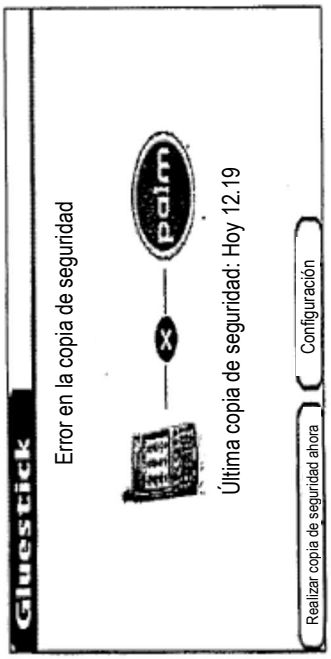

FIGURA 27