

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 963 388**

51 Int. Cl.:

H04L 9/40 (2012.01)

H04W 12/00 (2011.01)

H04L 67/2876 (2012.01)

H04W 12/04 (2011.01)

H04W 12/63 (2011.01)

H04W 12/65 (2011.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **16.01.2009** **PCT/CA2009/000046**

87 Fecha y número de publicación internacional: **27.06.2017** **WO09089626**

96 Fecha de presentación y número de la solicitud europea: **16.01.2009** **E 09701800 (6)**

97 Fecha y número de publicación de la concesión europea: **25.10.2023** **EP 2238777**

54 Título: **Virtualización securizada de la capa de presentación para dispositivos de comunicación inalámbrica de mano**

30 Prioridad:

16.01.2008 US 21357 P

09.09.2008 US 95387 P

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

26.03.2024

73 Titular/es:

BLACKBERRY LIMITED (100.0%)

2200 University Avenue East

Waterloo, ON N2K 0A7, CA

72 Inventor/es:

ANDRESS, MARK;

DIETRICH, TREVOR;

DIXON, KEVIN y

NOBLE, DUNCAN

74 Agente/Representante:

ELZABURU, S.L.P

ES 2 963 388 T3

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

DESCRIPCIÓN

Virtualización securizada de la capa de presentación para dispositivos de comunicación inalámbrica de mano

Campo

5 La presente invención se refiere en general a comunicaciones a través de dispositivos de comunicación inalámbrica de mano y a un sistema y un método para la virtualización securizada de una capa de presentación de dicho dispositivo en un punto extremo tal como un ordenador portátil u otro aparato de presentación.

Antecedentes de la invención

10 Las organizaciones y empresas, tanto públicas como privadas (incluidas, entre otras, instituciones gubernamentales, empresariales, educativas, sanitarias y otras) hacen frente a muchos desafíos relacionados con la securización de activos de información al tiempo que intentan apoyar a los trabajadores móviles mediante el uso de tecnologías informáticas inalámbricas en rápida evolución. Las opciones son costosas y complicadas. Los trabajadores móviles desean permanecer conectados con sus empresas cuando están en situación de movilidad y, a menudo, dependen de dispositivos de comunicación inalámbrica de mano, como teléfonos celulares, PDAs, etc., para mensajería y otras aplicaciones.

15 BlackBerry® de Research In Motion Ltd. se destaca como el dispositivo móvil dominante y la infraestructura de soporte en la que confían los departamentos de IT para su autenticación con el fin de acceder de forma segura a activos de información - tanto en el dispositivo como en la empresa. Otros dispositivos móviles de mano y/o sistemas correspondientes disponibles comercialmente incluyen Palm Treo, Pocket PC y otros dispositivos que ejecutan Good Mobile Messaging e Intranet de Motorola Good Technology Group, Motorola, Nokia, Palm Treo y otros dispositivos
20 que ejecutan el *software* Seven de Seven Networks, Inc., el iPhone de Apple, dispositivos que ejecutan la plataforma Mobile 5 (M5) de Microsoft y dispositivos que ejecutan la plataforma Android de Google Inc., entre otros.

25 Los dispositivos BlackBerry son dispositivos de comunicación inalámbrica de mano que comprenden interfaces de teclado y pantalla relativamente pequeñas. La fortaleza de estos dispositivos radica en sus capacidades de comunicación seguras y fiables. No están destinados a ser dispositivos informáticos de propósito general. A menudo, los trabajadores móviles tienen tanto un dispositivo BlackBerry como un dispositivo informático portátil para satisfacer todas sus necesidades.

30 Las organizaciones han invertido significativamente en una infraestructura segura para acceso remoto con tecnologías como: Citrix, RSA ID y Redes Privadas Virtuales (VPN) para permitir que los ordenadores portátiles y otros dispositivos informáticos ubicados remotamente se conecten de manera segura a la empresa (es decir, a las redes privadas de las organizaciones a través de la Internet pública). Además, algunas organizaciones dotan a sus trabajadores móviles de "Air Cards" para permitir que sus ordenadores portátiles se conecten a la empresa, utilizando la infraestructura de seguridad de turno (por ejemplo, VPNs), a través de las mismas redes inalámbricas (por ejemplo, redes celulares) que admiten el BlackBerry. Sin embargo, en general, muchas personas con ordenadores portátiles que requieren acceso remoto más allá del correo electrónico también tienen un BlackBerry - un conducto ya de confianza hacia la empresa.

35 Las organizaciones prefieren no gestionar tecnologías dispares que logren los mismos resultados. Las organizaciones líderes tienen una visión de "independencia de los puntos extremos"; esto significa que las organizaciones pueden permitir que sus usuarios seleccionen y utilicen cualquier ordenador de punto extremo que deseen como dispositivo informático personal propio, dejando que el usuario se ocupe del mantenimiento de ese ordenador y lo mantenga libre de virus, permitiéndoles usar el ordenador tanto para uso laboral como personal, al tiempo que los activos de la
40 empresa permanecen controlados, monitorizados y securizados.

45 En situaciones en las que la empresa no gestiona el ordenador de punto extremo, existe la preocupación por la posibilidad de que queden olvidados datos confidenciales en el ordenador de punto extremo (por ejemplo, PC, ordenador portátil). En situaciones en las que los datos se desplazan del dispositivo de mano de un usuario a las aplicaciones residentes del ordenador de punto extremo (por ejemplo, Microsoft Word o Excel), existe el riesgo de que archivos temporales que contienen dichos datos pudieran dejarse olvidados después de que finalice la sesión del usuario.

50 Por lo tanto, es deseable proporcionar una solución que permita al usuario móvil conectarse desde un ordenador portátil u otro aparato de presentación que sea capaz de ejecutar un navegador web, a su dispositivo de comunicación inalámbrica de mano (por ejemplo, un BlackBerry). Al virtualizar la capa de presentación del dispositivo de mano y ejecutar las aplicaciones en el dispositivo de mano, utilizando el ordenador portátil como dispositivo de presentación, los usuarios pueden aprovechar la conexión segura con la empresa desde el dispositivo de mano. El ordenador portátil puede aprovechar la tecnología de acceso por radiocomunicaciones del dispositivo portátil para conectarse a una red inalámbrica y trabajar con las capacidades de comunicación segura del dispositivo de mano para autenticarse en la red privada de la empresa. También puede ser deseable que no quede ningún rastro de datos (es decir, "cero
55 residuos") de información confidencial en el ordenador portátil u otro ordenador de punto extremo. El documento US 2002/163895 A1 da a conocer un sistema que incluye un dispositivo de pasarela inalámbrico acoplado a una red y que incluye un primer dispositivo inalámbrico que proporciona una primera señal de radiocomunicaciones de corto alcance

al dispositivo de pasarela inalámbrico, en el que el dispositivo de pasarela inalámbrico incluye un componente de *software* administrador de red para acceder a información de la red en respuesta a la primera señal de radiocomunicaciones de corto alcance.

El documento US 2003/177384 A1 da a conocer un servidor *proxy* dividido multicanal que incluye un servidor *proxy* dividido dispuesto detrás de un cortafuegos en una parte privada de la red de comunicaciones de datos y un cliente *proxy* dividido dispuesto en un dispositivo informático de cliente posicionado externamente con respecto a la parte privada de la red de comunicaciones de datos, en donde se establece un túnel entre el cliente *proxy* dividido y el servidor *proxy* dividido para alojar tráfico de datos de IP entre una aplicación de cliente en el dispositivo informático de cliente y una aplicación de servidor correspondiente en la parte privada de la red de comunicaciones de datos.

El documento GB 2 423 895 A se refiere al acceso a datos mediante el uso de un dispositivo de telecomunicaciones móviles, en el que el dispositivo de telecomunicaciones móviles está acoplado a un aparato de procesamiento de datos. Se accede a los datos utilizando una interfaz de usuario del aparato de procesamiento de datos, en donde la interfaz de usuario puede implementarse mediante un navegador web. El aparato de procesamiento de datos incluye un agente de servicios telefónicos que controla comunicaciones entre el dispositivo de telecomunicaciones móviles y el aparato de procesamiento de datos.

El documento US 2006/0203758 A1 se refiere a un terminal móvil que comprende una pantalla local para visualizar datos multimedia. El terminal móvil recibe datos multimedia a través de una primera interfaz inalámbrica y transmite los datos multimedia recibidos a una pantalla externa a través de una segunda interfaz inalámbrica, por ejemplo si la calidad de la pantalla externa es superior a la calidad de la pantalla local.

Compendio

Según un aspecto de la invención, se proporciona un método para comunicar datos. El método comprende acoplar un dispositivo de comunicación inalámbrica de mano con un aparato de presentación para virtualizar una capa de presentación del dispositivo de mano para un usuario, en el que el dispositivo de comunicación inalámbrica está configurado para comunicar datos de forma segura dentro de una red inalámbrica pública y una red de área local privada. El aparato y el dispositivo de mano definen un servidor *proxy* dividido de modo que el aparato también esté configurado para comunicar datos de forma segura dentro de la red inalámbrica pública a través del dispositivo de mano. El aparato y el dispositivo de comunicación inalámbrica están acoplados comunicativamente para la comunicación de datos a través de un *proxy* dividido. El método comprende además ejecutar una interfaz de usuario en dicho aparato para virtualizar la capa de presentación y permitir al usuario trabajar selectivamente con las comunicaciones de datos utilizando dicha comunicación de datos segura con la red de área local privada desde el dispositivo de comunicación inalámbrica.

Según otro aspecto, se proporciona un sistema de comunicación de datos. El sistema comprende un dispositivo de comunicación inalámbrica de mano configurado para comunicar datos de forma segura a través de una red inalámbrica pública y una red de área local privada; y un aparato de presentación para virtualizar una capa de presentación del dispositivo de mano para un usuario. El aparato y el dispositivo de mano están acoplados comunicativamente para la comunicación de datos a través de un *proxy* dividido de manera que el aparato también está configurado para comunicar datos de forma segura dentro de la red inalámbrica pública a través del dispositivo de mano. El aparato está provisto de una interfaz de usuario para virtualizar la capa de presentación y permitir al usuario trabajar selectivamente con las comunicaciones de datos utilizando dicha comunicación de datos segura con la red de área local privada desde el dispositivo de comunicación inalámbrica.

De acuerdo con otro aspecto más, se proporciona un medio de almacenamiento legible por ordenador que tiene instrucciones ejecutables por ordenador almacenadas en el mismo para adaptar un dispositivo de mano inalámbrico y un aparato de presentación para comunicaciones de datos, en donde el dispositivo inalámbrico está configurado para comunicar datos de forma segura dentro de una red inalámbrica pública y una red de área local privada. Las instrucciones incluyen primeros medios de código para adaptar el dispositivo de mano y segundos medios de código para adaptar el aparato de manera que cuando los primeros y segundos medios de código son ejecutados por procesadores respectivos del dispositivo de mano y el aparato, el dispositivo de mano y el aparato se acoplan comunicativamente para la comunicación de datos a través de un *proxy* dividido de modo que el aparato también esté configurado para comunicar datos de forma segura dentro de la red inalámbrica pública a través del dispositivo de mano. Además, los segundos medios de código proporcionan al aparato una interfaz de usuario para virtualizar una capa de presentación del dispositivo de mano y permiten a un usuario trabajar selectivamente con las comunicaciones de datos utilizando dicha comunicación de datos segura con la red de área local privada desde el dispositivo de comunicación inalámbrica.

Estas y otras características resultarán evidentes para aquellos con conocimientos habituales en la materia.

Breve descripción de los dibujos

A continuación se describirá una realización de la invención a modo de ejemplo únicamente con referencia a los siguientes dibujos en los que:

La Fig. 1 es un diagrama de bloques que muestra un ejemplo de red de comunicación en el que un aparato de presentación está acoplado a través de un dispositivo de mano a una red de área local empresarial;

La Fig. 2 es un diagrama de bloques de módulos de memoria respectivos que muestra un modelo de *software* para el dispositivo de mano y el aparato de presentación;

5 La Fig. 3 es una vista de una pantalla de interfaz de usuario representativa de un visor de capa de presentación de acuerdo con una realización;

La Fig. 4 es un diagrama de flujo que muestra operaciones para inicializar y configurar el aparato de presentación para ver datos desde el dispositivo de mano;

10 La Fig. 5 es un diagrama de flujo que muestra operaciones para enviar un correo electrónico desde el aparato de presentación a través del dispositivo de mano;

Las Figs. 6A y 6B son realizaciones alternativas respectivas de la red de comunicación de la Fig. 1;

La Fig. 7 es un diagrama de flujo que muestra operaciones para obtener un archivo adjunto de un correo electrónico en un formato de aplicación asociada (es decir, nativo);

15 La Fig. 8 es un diagrama de flujo que muestra operaciones para configurar una parte de la red de comunicación para comunicaciones cifradas de acuerdo con una realización;

La Fig. 9 es un diagrama de flujo que muestra el descubrimiento automatizado de ajustes de *proxy* de red estáticos según una realización;

La Fig. 10 es un diagrama de flujo que muestra el descubrimiento automatizado de ajustes de *proxy* de red dinámicos de acuerdo con una realización;

20 La Fig. 11 es un diagrama de flujo que muestra el descubrimiento automatizado de ajustes de *proxy* de red dinámicos de acuerdo con otra realización;

La Fig. 12 es un diagrama de bloques de una realización que muestra la ejecución de aplicaciones en un entorno de ejecución contenido o contenedor que comprende una máquina virtual;

25 La Fig. 13 es un diagrama de bloques de otra realización que muestra la ejecución de aplicaciones en un entorno de ejecución contenido o contenedor que comprende una máquina virtual;

La Fig. 14 es un diseño representativo de una pantalla de una interfaz de usuario según una realización;

La Fig. 15 es un diseño representativo de una pantalla de una interfaz de usuario de una realización del sistema de archivos;

30 La Fig. 16 es un diseño representativo de una pantalla de una interfaz de usuario de otra realización del sistema de archivos; y

La Fig. 17 es un diagrama de flujo de la inicialización y el funcionamiento de aplicaciones de acuerdo con una realización del entorno de ejecución contenido.

35 La Fig. 18 es un diagrama de bloques de una realización adicional de un dispositivo de mano y una aplicación de presentación acoplados configurados de manera que el aparato de presentación de punto extremo puede leer y escribir datos en un módulo de almacenamiento en el dispositivo de mano pero sin embargo no quedan datos en el aparato de presentación;

La Fig. 19 es un diagrama de bloques de una realización de una red de comunicación que incluye una zona de aterrizaje corporativa, externa a una red corporativa, para datos de un dispositivo de mano; y

40 La Fig. 20 es un diagrama de flujo de operaciones para comunicar datos desde el dispositivo de mano a la red corporativa, a través de la zona de aterrizaje corporativa, de acuerdo con una realización.

Por conveniencia, números iguales en la descripción se refieren a estructuras equivalentes en los dibujos.

Descripción detallada

45 De acuerdo con varios aspectos, la conectividad y la seguridad de los dispositivos de mano (HD) inalámbricos se pueden aprovechar para proporcionar un aparato de presentación (PA), como un ordenador portátil, con la capacidad de comunicarse de forma segura con una red privada de una empresa. Un servidor *proxy* dividido, con parte del mismo ejecutándose en el HD y parte ejecutándose en el PA, implementa un *Proxy* de Internet/Web totalmente compatible con el HTTP 1.1 para acoplar el PA para la comunicación a través del HD. Específicamente, el *proxy* dividido brinda soporte para el pragmático encabezamiento *keep-alive*, el método CONNECT, el uso compartido de conexiones de

socket y la agrupación de hilos, con el fin de permitir un entorno de navegación completamente funcional. Un entorno de este tipo permite el acceso a aplicaciones comerciales basadas en la web que se construyen sobre tecnologías estándar de Internet sin la necesidad de volver a renderizar o reescribir las interfaces de usuario para adaptarlas al HD. Además, se consigue que las aplicaciones de Intranet basadas en la web sean accesibles de forma segura sin necesidad de tecnologías adicionales de VPN y de acceso remoto.

Ampliar el *proxy* de HTTP del HD para brindar acceso a los recursos del HD, a través de un navegador y recursos de renderización en una combinación de XML/HTML/JavaScript y otras tecnologías de presentación web, permite que el HD actúe como un servidor web "personal" liviano. Preferiblemente se proporciona una aplicación de "visor" para acceder a las aplicaciones del HD, tales como correo electrónico y contactos, de modo que la capa de presentación se virtualice a través del PA y un usuario pueda trabajar selectivamente con las funciones de comunicación de datos. No es necesario almacenar datos de aplicaciones de forma persistente en el PA. En una realización, cuando el HD y el PA dejan de comunicarse (por ejemplo, debido a una pérdida de Bluetooth u otra conexión de comunicación como se describe más adelante), la aplicación de visor del PA se cierra automáticamente y no quedan datos del HD.

En una realización, las comunicaciones entre el dispositivo de mano y el aparato de presentación se pueden securizar firmemente. Utilizando la conexión segura del HD a la red inalámbrica y un túnel de TLS seguro habilitado por el *proxy* dividido, se puede intercambiar de forma segura una clave privada para securizar la conexión entre el HD y el PA. El HD puede solicitar una clave privada pseudoaleatoria de un servidor de claves (por ejemplo, acoplado detrás del cortafuegos de la LAN de la empresa). El servidor de claves responde al HD con la clave privada pseudoaleatoria y un *token* de autenticación de tercer factor pseudoaleatorio adicional. El *token* del tercer factor se presenta al usuario (por ejemplo, mostrándolo en la pantalla del HD). El lado HD del *proxy* dividido ahora tiene la clave privada que se utilizará para securizar el canal entre este y el lado PA del *proxy* dividido. Se puede solicitar al usuario que introduzca en la interfaz de *proxy* dividido del lado PA o en la aplicación de visor el *token* de autenticación de tercer factor presentado en el HD. A continuación, el lado PA establece una conexión segura de TLS con el mismo servidor de claves, esta vez proporcionando el *token* de autenticación de tercer factor y, a cambio, recibe la misma clave privada que se entregó al HD. Por lo tanto, ambos lados del *proxy* dividido recuperan la misma clave privada de forma segura. A continuación, ambos lados del *proxy* dividido pueden intercambiar datos cifrados de alta seguridad utilizando la clave privada.

En una realización, se puede configurar una unidad de almacenamiento *flash* combinada con Bluetooth/USB para proporcionar componentes ejecutables para la invención, así como capacidades de radiocomunicaciones de corto alcance de Bluetooth al aparato de presentación. La unidad de almacenamiento *flash* puede proporcionar un módulo de almacenamiento para código ejecutable para el visor y *proxy* dividido del lado PA, etc., así como para datos transitorios, de modo que no sea necesario utilizar los dispositivos de almacenamiento persistentes nativos del aparato de presentación. La retirada de la unidad de almacenamiento *flash* puede provocar el cese automático del *proxy* dividido y la virtualización de la capa de presentación (por ejemplo, el visor). De manera similar, detener las comunicaciones de corto alcance entre el dispositivo de mano y el aparato (por ejemplo, moviendo el dispositivo de mano o el aparato para que los dispositivos queden fuera de alcance mutuo) también puede desencadenar el cese automático. Si bien puede ser preferible comunicarse a través de Bluetooth y usar un dispositivo de Bluetooth consistente y una pila asociada, también se pueden usar otras capacidades de comunicación, como la capacidad de Bluetooth nativa de un dispositivo de presentación o un acoplamiento en serie por cable a través de USB, etc. Aún en una realización adicional, se puede usar una unidad de almacenamiento *flash* sin Bluetooth para proporcionar un módulo de almacenamiento para el código ejecutable para el visor y *proxy* dividido del lado PA, etc., así como para datos transitorios de modo que no sea necesario usar los dispositivos de almacenamiento persistentes nativos del aparato de presentación. La retirada de esta unidad de almacenamiento *flash* puede provocar el cese automático del *proxy* dividido y la virtualización de la capa de presentación (por ejemplo, el visor). El dispositivo de mano se puede conectar mediante una conexión por cable (por ejemplo, USB serie). La retirada de la conexión también puede provocar automáticamente el cese.

En una realización, se puede crear un espacio de sistema de archivos virtual (VFS) de manera que, para los componentes de ejecución del lado PA, el mismo aparente ser un espacio de almacenamiento en el lado PA, mientras que el espacio es un punto de montaje a través de la capa de transporte en el sistema de archivos del HD. Esto permite que los componentes de ejecución del PA funcionen como si un sistema de archivos normal estuviese prestando soporte a la ejecución cuando, en realidad, los datos se recuperan y guardan de forma segura en el HD. Cuando un HD se conecta al PA a través del *proxy* dividido, las aplicaciones (por ejemplo, aplicaciones de terceros comúnmente disponibles) pueden funcionar normalmente sin saber que están contestando al módulo de memoria del HD. En otras palabras, las aplicaciones de terceros pueden funcionar sin necesidad de readaptaciones y pueden cargarse desde el PA directamente o a través del Visor de PA y, de hecho, incluso pueden cargarse desde el módulo de memoria en el HD.

Servicios de WebDAV por encima de los componentes de VFS pueden permitir que se pueda acceder al módulo de memoria *flash* del HD mientras no está en modo de almacenamiento masivo. Alternativamente, no se establece el montaje de la unidad de VFS y solo las aplicaciones compatibles con WebDAV pueden acceder a los datos del HD a través del conducto de VFS.

Estas y otras características serán evidentes para aquellos con conocimientos habituales en la materia.

La Fig. 1 ilustra la red 100 de comunicación representativa en la que un dispositivo 102 de comunicación inalámbrica de mano (en adelante HD 102) está acoplado de forma inalámbrica para una comunicación segura a través de redes externas 106 y 110 a la red interna de una empresa, concretamente una red de área local (LAN) privada 112. De acuerdo con una realización de la invención, una capa de presentación (que se analiza más adelante) del HD 102 se virtualiza en un aparato de presentación (PA) 104, concretamente un ordenador portátil, para acoplar de ese modo el PA 104 a la LAN 112.

El PA 104 y el HD 102 se comunican a través del acoplamiento 103. En una realización, el acoplamiento comprende un acoplamiento de comunicación inalámbrica de corto alcance, preferiblemente a través de Bluetooth® como se describe más adelante en el presente documento. Aquellos con conocimientos habituales en la materia apreciarán que estos aparatos se pueden acoplar para una comunicación utilizando otra tecnología tal como comunicación en serie por cable (USB, RS 232, etc.), entre otras. En una realización preferida, una unidad 103A de almacenamiento *flash* combinada con Bluetooth/USB está acoplada al PA 104 para proporcionar componentes ejecutables para la invención, así como el PA 104 con capacidades de comunicación de Bluetooth.

El HD 102 se comunica de forma inalámbrica a través de una red de área amplia inalámbrica (WWAN) 106 tal como una red de telefonía celular (por ejemplo, GSM/GPRS, EDGE u otra red similar) o una red de área local inalámbrica (WLAN) (por ejemplo, red 802.11 o Wi-MAX (no mostrada)). Como es bien sabido, las comunicaciones de datos de HD a través de la WWAN 106 son admitidas por una red de servicios del dispositivo de mano (por ejemplo, BlackBerry® Network) representada por la infraestructura 108 para transmitir datos entre el HD 102 y la LAN 112 u otros HD (no mostrados). La LAN 112 y la infraestructura 108 de red de servicios de HD pueden acoplarse para la comunicación a través de la red externa (Internet) 110 o una red privada (no mostrada).

A modo de ejemplo, los componentes de la LAN 112 pueden comprender un cortafuegos 114, un servidor empresarial 116 de dispositivos de mano, un servidor 118 de correo electrónico empresarial y un servidor *proxy* adicional 130 o servidores 130-1, 130-2, ... 130-n. Otros componentes de la red LAN pueden incluir servidor(es) de aplicaciones, servidor(es) *backend*, bases de datos, etc. (por ejemplo, por cada servidor representativo 120) para proporcionar contenido a dispositivos en la LAN, incluido el HD 102. En algunas realizaciones, se puede proporcionar una pluralidad de servidores *proxy* 130-1, 130-2, ... 130-n, por ejemplo, en los que servidores respectivos gestionan solicitudes respectivas en respuesta a un tipo de solicitud. En otras realizaciones, se puede proporcionar un único servidor *proxy* (por ejemplo, 130) para gestionar todos los tipos. Una persona con conocimientos habituales en la técnica apreciará que se omiten diversas infraestructuras de redes públicas e inalámbricas para mayor claridad.

El servidor empresarial 116 de HD proporciona un enlace centralizado entre dispositivos inalámbricos, aplicaciones empresariales y redes inalámbricas, para proporcionar comunicaciones inalámbricas seguras y datos corporativos a usuarios móviles. Las características importantes incluyen cifrado de extremo a extremo y admisión de aplicaciones inalámbricas para correo electrónico, calendario y libreta de direcciones. El servidor empresarial de HD incluye preferiblemente integración con aplicaciones empresariales como Exchange de Microsoft®, IBM® Lotus® Domino® o Novell® Groupwise®, etc.

En una realización en la que el HD 102 comprende un dispositivo BlackBerry, el servidor empresarial 116 de HD comprende preferiblemente un Servidor Empresarial de BlackBerry que "ofrece cifrado del Estándar de Cifrado Avanzado (AES) o el Estándar de Cifrado de Datos Triple (3DES) de extremo a extremo que ayuda a garantizar la confidencialidad e integridad de la información transmitida de forma inalámbrica desde detrás del cortafuegos a dispositivos inalámbricos en el campo". Además, el Servidor Empresarial de BlackBerry proporciona acceso al correo electrónico basándose en un envío sin solicitud previa [*push*]; calendario, contactos, tareas y notas; mensajería instantánea; aplicaciones y servicios basados en la web y aplicaciones empresariales. Se pueden utilizar otros servidores relacionados (no mostrados, por ejemplo, MDS Empresarial de BlackBerry) para proporcionar admisión de datos móviles a los dispositivos de mano (por ejemplo, HD 102) para proporcionar contenido desde los servidores 120 de forma inalámbrica. Aunque se ilustran como componentes independientes de la LAN 112, las personas con conocimientos habituales apreciarán que se pueden configurar varias combinaciones de *hardware/software* para proporcionar tales capacidades.

De acuerdo con características preferidas de la invención, se puede proporcionar un cifrado de extremo a extremo de modo que o bien 1) los datos se cifren entre los dos lados del *proxy* dividido y a continuación bien se almacenen en el HD o bien se transmitan inmediatamente desde el HD al servidor de destino utilizando otro transporte seguro - ya sea una conexión de 3DES/AES segura (por ejemplo, a través del BES) o una conexión de SSL o TLS o bien 2) que el PA haya establecido una conexión de TLS, a través de la capacidad de tunelización del *proxy* dividido (descrita más adelante), directamente al servidor de destino. Por lo tanto, en una configuración de red donde un servidor de soporte, como un servidor BES para 3DES/AES, no está disponible (no se muestra), se puede sustituir por una conexión de SSL desde el HD al servidor de destino.

La Fig. 2 es un diagrama de bloques de dispositivos de almacenamiento informáticos tales como memoria (200A y 200B, en conjunto 200) para cada uno del HD 102 y el PA 104 que ilustra un modelo de componentes de *software* para llevar a cabo la invención de acuerdo con una realización. El sistema operativo (O/S) 204 de HD representa soporte nativo para capacidades del dispositivo. En una realización, el O/S 204 proporciona al menos los servicios básicos de una Configuración Limitada de Dispositivos Conectados (CLDC) que define el conjunto básico de interfaces

de programación de aplicaciones y una máquina virtual para dispositivos con recursos limitados como teléfonos móviles, buscapersonas y asistentes digitales personales convencionales. Cuando se combina con un perfil como el Perfil de Dispositivos de Información Móviles (MIDP), proporciona una plataforma Java sólida para desarrollar aplicaciones que se ejecuten en dispositivos con memoria, poder de procesamiento y capacidades gráficas limitados.

5 El O/S 204 proporciona APIs para acceder a almacenamiento persistente rudimentario y, como mínimo, una arquitectura de conector similar a J2ME para acceso básico a funciones/servicios de comunicación del Protocolo de Internet.

10 El Entorno 212 de Trabajo de *Servlet* de HD se basa en métodos básicos de notificación de eventos (por ejemplo, a través de APIs 216 de HD) para indicar cuándo se han producido eventos tales como ha llegado un correo nuevo, se ha eliminado un correo, etc. y otros eventos del calendario, contactos, según su disponibilidad. Cuando no haya un modelo de evento disponible, para emular eventos para el lado PA se implementarán otros mecanismos para sondear los módulos de almacenamiento del administrador de información personal (PIM) (no mostrados) con el fin de determinar los cambios.

15 La Aplicación 214 de HD de Virtualización de Capa de Presentación (Aplicación 214 de HD) es un componente de *software* que proporciona funcionalidad y una interfaz de usuario en el HD 102 para permitir al usuario establecer una conexión de comunicación con el PA 104 a través del acoplamiento 103 y lanzar el Visor 230 de PA. La Aplicación 214 de HD también permite al usuario cerrar la conexión de comunicación, reconectarse, salir de la aplicación, hacer que la Aplicación 214 de HD se ejecute en segundo plano en el HD 102 o solicitar un canal seguro entre el HD 102 y el PA 104.

20 El Entorno 212 de Trabajo de *Servlet* y *Proxy* Dividido de HD es un componente de *software* que implementa el lado HD de un servidor *proxy* dividido y con el Entorno 228 de Trabajo de *Servlet* y *Proxy* Dividido de PA ejecutándose en el PA 104 facilita las comunicaciones entre el HD 102 y el PA 104. En una realización preferida, el *proxy* dividido proporciona una capa de transporte basada en XML (componente 208 de Transporte de HD) que aísla las comunicaciones basadas en flujos de capa superior de las complejidades de las comunicaciones de puertos serie a través de Bluetooth 206 y proporciona una multiplexación altamente escalable a través del transporte único. Una biblioteca de flujos (Flujos 210 de HD) permite a las capas superiores simplemente leer y escribir datos en el otro lado del *proxy* (228) como si fuera cualquier otro flujo de Java. Esta disposición también aísla a las capas superiores de los detalles de si las comunicaciones a través del acoplamiento de Bluetooth están cifradas o no. Se entenderá que "capas superiores" aquí se refiere a aplicaciones/funciones de capa de aplicación que transmiten datos de aplicación formateados tales como en un protocolo basado en XML para presentación remota o traducción de instrucciones de capa de presentación/visualización con el fin de renderizar una visualización en el PA 104 remoto.

El Entorno 212 de Trabajo de *Servlet* y *Proxy* Dividido de HD proporciona además un servidor *proxy* web 212A que utiliza Flujos 210 de HD e implementa:

35 • un mecanismo sofisticado de compartición de *sockets* de TCP para aprovechar al máximo las conexiones de red disponibles en el dispositivo de mano utilizando la agrupación de conexiones, mecanismos de *keep-alive*, canalización [*pipelining*] de solicitudes y capacidades de retransmisión;

40 • una capacidad de tunelización que se coordina con el otro lado del *proxy* dividido 228 para implementar el método CONNECT de acuerdo con el protocolo HTTP 1.1 para uso con aplicaciones basadas en navegador y otras aplicaciones del lado PA que requieren que el *proxy* dividido pase datos al servidor de destino sin inspección - es decir, tunelización fiable de datos opacos que pueden o no estar cifrados;

45 • admisión completa del protocolo HTTP 1.1 en coordinación con el lado PA del *proxy* dividido 228. El lado PA 228 realiza el procesamiento de encabezamientos antes de su transmisión al lado HD para optimizar solicitudes para el lado HD y reducir la cantidad de procesamiento de encabezamientos del lado HD. Se proporcionan sugerencias al lado HD sobre si abrir o no una nueva conexión o intentar reutilizar una conexión para el mismo punto extremo. Además, el lado PA está configurado preferiblemente para filtrar y denegar solicitudes para ciertas aplicaciones/agentes de usuario conocidos que consumen mucho ancho de banda a través de la conexión de HTTP (por ejemplo, Skype, MSN, etc.).

El Entorno 212 de Trabajo de *Servlet* y *Proxy* Dividido de HD también proporciona un servidor 212B de *Servlet* que utiliza la biblioteca Flujos 210 de HD. El Servidor 212B de *Servlet* :

50 • determina si las solicitudes al HD a través de los flujos 210 son para recursos/*servlets* locales (recursos en el dispositivo de mano) o deben retransmitirse a recursos de Intranet/Internet a través del servidor *proxy* web;

• implementa un grupo de hilos para garantizar un límite controlable en la cantidad de hilos que se ejecutan en el dispositivo de mano dentro del servidor de *servlet* para adaptarse a las limitaciones de conexión con la red inalámbrica y limitar las excepciones de sobrecarga de recursos; y,

55 • proporciona un entorno de trabajo de *servlet* para añadir componentes personalizados que aprovechan todo el entorno de trabajo del servidor de *servlet* al subclasificar la clase de *servlet* y codificar la funcionalidad incremental como si fuera un componente de *software* de HD "nativo" típico.

El Entorno 212 de Trabajo de *Servlet* y *Proxy* Dividido de HD también proporciona una capa de seguridad operativa selectivamente que, cuando está "activada", extiende las comunicaciones cifradas al *proxy* dividido 228 del lado PA.

Como se analiza más adelante con referencia a las Figs. 4B y 5, en la realización preferida, la capacidad de seguridad obtiene de forma segura una clave privada y un *token* de autenticación de tercer factor de un servidor de confianza ya sea en la empresa o en Internet. Una vez que se recibe la clave privada, el Entorno 212 de Trabajo de *Servlet* y *Proxy* Dividido de HD informa al Entorno 228 de Trabajo de *Servlet* y *Proxy* Dividido de PA, ya sea manualmente a través del usuario o pasando el *token* mediante programación, que 228 debe solicitar la misma clave proporcionando el *token* al servidor de claves. Una vez que el Entorno 228 de Trabajo de *Servlet* y *Proxy* Dividido de PA ha recibido la clave, informa al Entorno 212 de Trabajo de *Servlet* y *Proxy* Dividido de HD y todas las comunicaciones posteriores se cifran usando la clave privada en la capa 208 de transporte de modo que las capas superiores no necesitan ser conscientes de que los datos se están cifrando y descifrando.

El Entorno 228 de Trabajo de *Servlet* y *Proxy* Dividido de PA es el otro lado del *proxy* dividido y comparte código en común con el Entorno 212 de Trabajo de *Servlet* y *Proxy* Dividido de HD y coordina la implementación del HTTP 1.1. Cuando el Entorno 212 de Trabajo de *Servlet* y *Proxy* Dividido de HD lo solicita, el lado PA 228 lanza el Visor 230 de PA y facilita comunicaciones a través del transporte 224, 208, entre el Visor 230 de PA y el HD 102.

El Entorno 228 de Trabajo de *Servlet* y *Proxy* Dividido de PA monitoriza la conexión con el túnel 234 de claves y si el túnel se rompe, el Visor de PA se cierra inmediatamente. El túnel se rompe cuando: 1) el HD 102 sale del alcance de las comunicaciones de Bluetooth de corto alcance; 2) el usuario de HD apaga la conexión desde el dispositivo de mano a través de la aplicación 214 de HD; 3) el usuario de HD apaga directamente la conexión 206 de Bluetooth; o 4) cada vez que se extrae la unidad de almacenamiento *flash* de Bluetooth del PA 104.

El Entorno 228 de Trabajo de *Servlet* y *Proxy* Dividido de PA proporciona dos *proxies*: un *proxy* 228A de visor para el Visor de PA para virtualización de aplicaciones del HD y un *Proxy* 228B de Navegador para cualquier navegador de Internet como Mozilla Firefox® o Microsoft Internet Explorer para una funcionalidad completa de navegador web. El *Proxy* 228A de Visor está construido sobre la misma biblioteca de flujos (componente 226 de flujos de PA) que el código del *proxy* dividido 212 del Lado HD (es decir, Flujos 208 de HD) y, por lo tanto, construido sobre el mismo transporte de XML (componente 224 de Transporte de PA) a través de Bluetooth 222 que el código 212 del Lado HD. El *Proxy* 228A de Visor expone las interfaces de programación de aplicaciones (API) 216 de las aplicaciones de HD nativas a la aplicación 230 de Visor de PA a través de XML. Las API 216 de HD incluyen preferiblemente APIs para correo electrónico, calendario y/o libreta de direcciones/contactos, entre otros, proporcionados por aplicación(es) de comunicación de datos en el HD 102. Dichas aplicaciones de comunicación de datos (no mostradas) en el HD 102 a menudo se sincronizan con la cuenta de usuario de la LAN 112 del usuario, por ejemplo, en el servidor 118 de correo electrónico.

Como se ha señalado, el *Proxy* 228B de Navegador proporciona una interfaz de *proxy* de HTTP 1.1 configurable para navegadores de Internet estándar, por ejemplo 232. Por ello, proporciona acceso inalámbrico a Internet (ya sea "vinculado" a través del servidor empresarial 116 del dispositivo de mano y de acuerdo con cualquier restricción y/o monitorización de tráfico que pueda imponer o "abierto" sin restricciones y, por lo general, eludiendo el servidor 116, que en una realización puede incluir un servidor MDS Empresarial de BlackBerry) para el Navegador 232 traduciendo y retransmitiendo solicitudes de HTTP al Servidor *Proxy* Web 212A de HD a través del transporte (224 y 208). La parte del Entorno 228 de Trabajo de *Servlet* y *Proxy* Dividido de PA correspondiente al *Proxy* 228A de Navegador se puede configurar para permitir que el usuario o personal de IT niegue a ciertos agentes de usuario, tales como Skype, MSN u otros agentes que pueden no ser deseables, tener acceso a los servicios del *proxy* dividido.

El Visor 230 de PA es una aplicación de tipo cliente que proporciona una interfaz de usuario para las API 216 de HD acopladas. El Visor 230 de PA renderiza una interfaz gráfica de usuario operada por XML presentada al mismo por la aplicación 214 de HD y el *proxy* dividido 212 de HD. En una realización, el Visor 230 de PA es una aplicación basada en Windows .NET. El Visor 230 de PA presenta al usuario de PA 104 una interfaz para manipular los datos que se visualizan y para enviar solicitudes de vuelta al lado HD 212 para APIs 216 de HD. A continuación se describe una vista representativa con referencia a la Fig. 3.

El Monitor 220 de PA es una aplicación que permite al usuario de PA 104 lanzar todos los componentes del lado PA (222-234) de forma coordinada y monitorizar su estado. Si algún componente falla, por ejemplo, porque se interrumpe la comunicación con el HD 102, el monitor 220 de PA notifica al usuario y proporciona instrucciones de reparación cuando sea posible. Además, como se ha descrito anteriormente, el Monitor 220 de PA intenta cerrar el Visor 230 de PA elegantemente en el caso en que se vea que el túnel 234 de claves se ha venido "abajo". En una realización, el Monitor 220 de PA es una aplicación basada en Windows .NET.

El túnel 234 de claves comprende un componente de *software* "ligero" que se ejecuta en el PA 102 y sirve como un túnel simple entre la pila 222A del componente de Bluetooth 222 y el Entorno 228 de Trabajo de *Servlet* y *Proxy* Dividido de PA. El túnel 234 de claves notifica el estado de conectividad a través del flujo de salida estándar del proceso y transporta datos de un lado a otro entre la pila 222A y el Entorno 228 de Trabajo de *Servlet* y *Proxy* Dividido de PA. En un lado del túnel, los datos se leen y escriben a través de una interfaz de puerto serie (puerto com) en la pila 222A de Bluetooth y en el otro lado hay una conexión de TCP al Entorno 228 de Trabajo de *Servlet* y *Proxy*

Dividido de PA.

Como se ha descrito anteriormente, se puede configurar una unidad combinada 103A de almacenamiento *flash* y llave electrónica de USB/Bluetooth para acoplarse al PA 104 para proporcionar componentes ejecutables así como capacidades de comunicación de Bluetooth. La unidad combinada puede permitir el uso de una interfaz de Bluetooth consistente y una pila para componentes de comunicación (por ejemplo, túnel 234 de claves) en el PA 104 en lugar de depender de cualquier capacidad de Bluetooth nativa del PA 104).

La Fig. 3 es un diseño 300 de pantalla de interfaz de usuario representativo de una realización del Visor 230 de PA. La vista 300 muestra una ilustración representativa de una interfaz de usuario de correo electrónico, similar a una experiencia de interfaz de usuario de escritorio, que incluye tres partes principales, a saber, el área 330 de barra de herramientas superior, y dos partes inferiores para controles 332 y un área 332 de visualización de datos principal. El área 330 de barra de herramientas incluye una parte 302 de título y una o más barras de herramientas (por ejemplo, 304, 306 y 308). Una barra de herramientas particular puede ser contextual con respecto a la interfaz de usuario activa que se está renderizando. Por ejemplo, en la barra 308 de herramientas para presentar la aplicación de correo electrónico del HD, se proporciona contextualmente una interfaz 310 de búsqueda para buscar correo electrónico. Los controles 332 pueden incluir una interfaz contextual para explorar o manipular datos visualizados en el área 332 de visualización de datos principal. Por ejemplo, se puede proporcionar una jerarquía de carpetas o una vista 314 de árbol para explorar datos de correo como es bien conocido. En el modo de vista de calendario (no se muestra), se pueden visualizar los meses del calendario. En una vista de Inicio (no se muestra), se puede mostrar información de estado relacionada con el HD (por ejemplo, señal inalámbrica, duración de la batería, propietario, etc.) y el estado de la conexión del HD al PA. En la misma se pueden proporcionar controles (por ejemplo, entradas de usuario de estilo radio o botón) para controlar aspectos de la experiencia de virtualización de la capa de presentación de HD-PA. Un ejemplo incluye un control para especificar si se usa la conexión del HD para navegación web u otra conexión disponible para el PA 104.

Los controles 318-324 proporcionan interfaces convenientes para invocar la visualización de datos particulares en el área 334 de visualización de datos principal o (por ejemplo, 326) para lanzar interfaces de usuario externas tales como el navegador web 232.

El área 334 de visualización principal se puede dividir en más de una parte, como en la vista 300 de Correo. La vista 300 muestra una lista de correo electrónico que comprende datos resumidos en la parte superior 316 y vistas previas de correos electrónicos individuales que incluyen una parte del cuerpo del correo electrónico específico (si corresponde) en la parte inferior 328. La selección de un correo electrónico en particular puede abrir el correo electrónico en una ventana emergente independiente, como es bien conocido. Aunque no se muestra, una vista de calendario o vista de contactos puede no dividir el área de visualización y mostrar todos los datos en una parte no dividida del área 332. Al igual que otras interfaces de usuario, se puede navegar por el visor 230 de PA usando un dispositivo señalador y/o entradas de teclado para moverse entre los controles, seleccionar control e invocar acciones. Al hacer clic en un control "nuevo" de la barra 306 de herramientas se puede invocar una ventana emergente de redacción de correo electrónico, por ejemplo.

Es importante destacar que el Visor de PA obtiene principalmente sus datos de correo, contactos, calendario, etc. de datos almacenados en el HD 102 o disponibles de otro modo en el HD 102. Debido a los recursos limitados (por ejemplo, almacenamiento y ancho de banda) del HD 102, un usuario de HD puede tener sólo un subconjunto del correo electrónico del usuario almacenado en el HD 102. Es posible que más datos de correo electrónico permanezcan disponibles para el usuario a través del servidor 118 de correo electrónico, por ejemplo a través de una interfaz de correo electrónico diferente tal como a través de Outlook o el correo Web en un ordenador de escritorio (no mostrado). A menudo, sólo una parte de un correo electrónico particular se almacena en el HD 102. La aplicación de HD asociada puede permitir la recuperación selectiva de más datos (por ejemplo, a través de una interfaz de orden Más o Todo). El visor 230 de PA ofrece preferentemente una funcionalidad similar.

Preferiblemente, los respectivos entornos 212 y 228 de trabajo de *proxy* dividido y *servlet* proporcionan un sistema de archivos virtual. Un sistema de archivos de este tipo ayuda con la transferencia organizada de datos/archivos particularmente entre el PA 104 y el HD 102. De acuerdo con un primer modelo para mover datos/ archivos del PA 104 al HD 102:

(a) Los archivos que se transferirán del PA 104 al HD 102 para su almacenamiento en el HD 102 o para adjuntarlos posteriormente a un correo electrónico saliente se almacenan primero en un directorio raíz en el módulo 103A de memoria extraíble del PA (es decir, unidad de almacenamiento *flash* y llave electrónica de Bluetooth combinadas) de manera similar a cómo cualquier otra aplicación guardaría un archivo de datos en cualquier otro sistema de archivos. Como el módulo 103A de memoria es extraíble, no quedan datos en el PA 104 ni siquiera en el caso de que el archivo no se transfiera con éxito al HD 102;

(b) El Visor 230 de PA a continuación envía una solicitud basada en XML al Servidor 212B de *Servlet* de HD que contiene como parte de la carga útil un URL correspondiente al recurso almacenado en la llave electrónica 103A. Por ejemplo `res:///path/filename;`

(c) Cuando el Servidor 212B de *Servlet* de HD procesa una solicitud que contiene un elemento con un URL como se indica en el punto (b) anterior, realiza una solicitud de regreso al Servidor 228B de *Servlet* PA utilizando el URL proporcionado;

5 (d) El esquema `res://` indica que la respuesta debe tratarse como un flujo binario sin formato y el flujo virtual se cierra cuando se devuelven todos los datos del archivo;

(e) En el caso de que el recurso se adjunte a un correo electrónico, se incorpora a la construcción del correo electrónico utilizando las API 216 de HD;

10 (f) En el caso de que el recurso deba guardarse en el módulo de memoria de HD para su posterior manipulación a través de otras aplicaciones (ya sea en el HD 102 o en el PA 104), los datos se almacenan en el módulo de memoria persistente del HD a través de las API 216 de HD;

(g) El recurso se retira del módulo 103A de memoria de PA.

15 De acuerdo con un segundo modelo para transferir datos/archivos desde el PA 104 al HD 102 pero de manera segura, se llevan a cabo operaciones similares a las descritas con referencia al primer modelo. Sin embargo, para aquellos casos en los que no es aceptable tener un recurso guardado de forma transitoria e insegura en el módulo 103A de memoria:

(a) El recurso se cifra usando la misma clave que se obtiene para securizar el transporte de comunicaciones entre el HD 102 y el PA 104 (como se describe con referencia a las Figs. 4B y 6) - por lo tanto, se indica cuándo está habilitado el transporte seguro de extremo a extremo;

(b) El mismo URL (por ejemplo, `res:///path/filename`) se envía al *Servlet* 212B de HD;

20 (c) El recurso se extrae del servidor del *Servlet* 228B de PA como en el primer modelo anterior;

(d) El recurso se descifra utilizando la clave segura;

(e) El recurso se guarda en el HD 102 y/o se envía como un archivo adjunto de correo electrónico de la misma manera que la descrita anteriormente.

25 En el caso de que los archivos se almacenen en la llave electrónica 103A en formato cifrado, si los datos no se transmiten completamente al HD y no se descifran antes de que se detenga la sesión, el archivo no podrá descifrarse nuevamente a menos que se almacene un historial de claves (por ejemplo, en el módulo de memoria de HD). Se puede usar una marca de tiempo del archivo cifrado en la llave electrónica 103A para su indexación en un historial de claves con el fin de determinar la clave apropiada para descifrar el archivo después de recuperarlo del módulo 103A de memoria de PA.

30 El sistema de archivos virtual puede proporcionar dos o más particiones para el almacenamiento de datos. Una partición puede ser un medio extraíble conectado por USB que puede montarse mediante el sistema de archivos de cualquier sistema operativo estándar y al que pueden acceder aplicaciones de terceros, como saben los expertos en la técnica. Una segunda puede ser un sistema de archivos que sólo puede montarse utilizando el servidor *proxy* dividido de la presente invención. Las dos o más particiones podrían implementarse en la misma unidad de
35 almacenamiento *flash*. Alternativamente, las particiones se pueden implementar en distintas unidades de almacenamiento *flash*.

40 En una realización, con referencia a la Fig. 12, el entorno de tiempo de ejecución comprende dos zonas 1202, 1203. La aplicación del Visor 230 de PA está escrita en un lenguaje (por ejemplo, Java) tal que en la primera zona 1202 puede residir dentro del mismo entorno de ejecución o contenedor operativo 1204 (por ejemplo, una Máquina Virtual Java) que aplicaciones 1206 de terceros escritas en ese mismo lenguaje, que el Visor 230 de PA también usa para renderizar archivos adjuntos y otros datos. Las aplicaciones 1206 de terceros utilizadas por el Visor 230 de PA pueden restringirse mediante las políticas y otras configuraciones del contenedor 1204, que también contiene el Visor 230 de PA, según lo determine la empresa. Como ejemplo, esta zona de contenedor podría implementarse como un archivo
45 Jar en el caso de que el lenguaje sea Java y el contenedor sea una Máquina Virtual Java. La segunda zona 1203 incluye un sistema de archivos que se puede montar mediante el sistema de archivos de cualquier sistema operativo estándar y puede ser accesible para aplicaciones 1210 de terceros que no residen en el contenedor y que no están sujetas a las políticas y configuraciones de la empresa como lo es la primera zona 1202. Las aplicaciones no contenidas (por ejemplo, navegadores estándar 1208) y el contenedor 1204 pueden operar con el Entorno 228 de Trabajo de *Servlet* y *Proxy* Dividido de PA y el Entorno 212 de Trabajo de *Servlet* y *Proxy* Dividido de HD, que a su
50 vez utilizan el Túnel 234 de Claves como se ha explicado anteriormente.

En otra realización, mostrada en el diagrama de bloques de la Fig. 13, también se proporcionan dos zonas 1302, 1303. La aplicación del Visor 230 está escrita en un lenguaje (AJAX o JavaScript, por ejemplo) tal que en la primera partición 1302 puede residir dentro del mismo contenedor operativo 1304 (por ejemplo, una Máquina Virtual Java) que aplicaciones 1306 de terceros (por ejemplo, Office Suite) escritas en ese mismo lenguaje o en uno compatible (por

ejemplo, AJAX o JavaScript), que el Visor 230 también utiliza para renderizar archivos adjuntos y otros datos. Una aplicación 1308 (por ejemplo, un navegador de Java) en el contenedor y el Visor 230 pueden compartir la misma información de autenticación de modo que al navegador se le permita acceder a recursos empresariales utilizando el *proxy* dividido (212, 228). Por ejemplo, un navegador 1308 de Java que reside dentro del mismo contenedor 1304 que el Entorno 228 de Trabajo de *Servlet* y *Proxy* Dividido de PA puede proporcionar la información de autenticación en un encabezamiento 1310 de solicitud de HTTP al Entorno 228 de Trabajo de *Servlet* y *Proxy* Dividido de PA, y de este modo se le concede acceso a los recursos empresariales a través del Túnel 234 de Claves y el Entorno 212 de Trabajo de *Servlet* y *Proxy* Dividido de HD. Sin embargo, una aplicación 1312 en la segunda zona 1303, es decir, no en el contenedor 1304, no tendrá acceso a la información de autenticación disponible en el contenedor 1304 y No se le permitirá acceder a los recursos de la empresa (porque no podrá proporcionar información de autenticación adecuada) utilizando el *proxy* dividido 228.

En las dos realizaciones anteriores (mostradas en las Figs. 12 y 13), el Visor 230 puede programarse utilizando un lenguaje compatible con (y que reside en el mismo contenedor que) una aplicación de terceros que utiliza para renderizar archivos adjuntos y otros datos en un dispositivo de mano.

La Fig. 14 es una vista o diseño de pantalla de interfaz de usuario representativo de una realización del Visor 230 de PA en funcionamiento en el que se incorpora una partición de memoria. La vista 230 muestra una ilustración representativa de una interfaz de usuario de sistema de archivos, similar a una experiencia de interfaz de usuario de escritorio, que incluye tres partes principales, concretamente el área 1430 de barra de herramientas superior, y dos partes inferiores para controles 1432 y un área 1434 de visualización de datos principal. El área 1430 de barra de herramientas incluye una parte 1402 de título y una o más barras de herramientas (por ejemplo, 1404, 1406 y 1408). Una barra de herramientas particular puede ser contextual con respecto a la interfaz de usuario activa que se está renderizando. Por ejemplo, la barra 1408 de herramientas para presentar la aplicación de navegador de archivos del HD, una interfaz 1410 de búsqueda se proporciona contextualmente para buscar archivos en el explorador de archivos. Los controles pueden incluir una interfaz contextual para explorar o manipular datos visualizados en el área 1434 de visualización de datos principal, como se ha explicado con referencia a la Fig. 3 anterior.

La parte principal 1434 de la vista 230 muestra la separación visual del sistema de archivos en el Espacio Corporativo 1445 y el Espacio Personal 1446. Los archivos (datos) del Espacio Corporativo no se pueden copiar ni guardar en el Espacio Personal (por ejemplo, arrastrando y soltando, cortar/pegar, etc.), pero los archivos del Espacio Personal se pueden guardar o copiar en el Espacio Corporativo. Asimismo, las aplicaciones de terceros que residan fuera del contenedor tampoco podrán acceder a archivos del Espacio Corporativo.

La Fig. 15 muestra una captura de pantalla de una realización del sistema de archivos en funcionamiento en el Visor 230 de PA. Usando el *software* Explorador de Archivos de Microsoft Windows (por ejemplo), el usuario puede navegar fácilmente a los archivos en el HD. Se pueden distinguir claramente el Espacio Corporativo (carpeta 1502) y el Espacio Personal (carpeta 1504). Cualquier archivo (por ejemplo, 1506) presente en el Espacio Corporativo (carpeta 1502) puede mostrarse en el panel 1508 de visualización (por ejemplo, cuando el foco está en la carpeta 1502). El árbol 1510 de directorios se proporciona en otro panel 1512 de visualización, que puede ser visible en la misma ventana 1514 que el panel 1508 de visualización. Si un usuario intenta acceder a archivos en el Espacio Personal (carpeta 1504) (por ejemplo, a través del *software* Explorador de Archivos), al usuario se le presentará la aplicación adecuada para el tipo de archivo al que se esté accediendo (no se muestra).

La Fig. 16 es una captura de pantalla que muestra resultados de ejemplo cuando un usuario intenta abrir un archivo cifrado 1506 que reside en el Espacio Corporativo (carpeta 1502) en una situación en la que el *software* Explorador de Archivos del usuario no reside en ni tiene acceso al contenedor. Debido a que el *software* de explorador de archivos del usuario no reside en el contenedor, no puede descifrar archivos dentro del Espacio Corporativo (carpeta 1502). Como resultado, el archivo 1506 se visualiza 1602 en su forma cifrada 1604.

Alternativamente, la estructura de almacenamiento *flash* se puede configurar para que el Espacio Corporativo (carpeta 1502) no aparezca para aplicaciones fuera del contenedor (como, por ejemplo, para el programa Explorador de Archivos de Windows local con respecto al PA (no se muestra)). Esto se puede lograr: 1) estableciendo una unidad de almacenamiento *flash* completa en el HD como Espacio Corporativo, 2) no permitiendo que el Espacio Corporativo se use en modo de almacenamiento masivo y 3) escribiendo datos en el Espacio Corporativo a través de la infraestructura de *proxy* dividido de nuevo en el HD utilizando un protocolo privativo (VFS), de modo que visores de sistemas de archivos estándar, como el Explorador de Archivos de Windows, no reconozcan el sistema de archivos.

De manera similar, si un navegador reside en el contenedor ("Navegador de Extranet") y un segundo navegador reside fuera del contenedor ("Navegador de Internet"), solo el Navegador de Extranet podrá acceder a recursos de la empresa. La Fig. 17 muestra un diagrama de flujo de un ejemplo de un escenario de este tipo en el que se lanzan ambos navegadores. En la práctica, un usuario sólo puede lanzar uno u otro navegador.

Con referencia a la Fig. 17, el *Proxy* Dividido 228 de PA determina la información de autenticación empresarial a partir del *Proxy* Dividido 212 de HD (paso 1700). A continuación, un usuario lanza dos navegadores (pasos 1701 y 1704) en el *Proxy* Dividido 228 de PA: un Navegador de Extranet y un Navegador de Internet. El Navegador de Extranet está codificado dentro del mismo contenedor (por ejemplo, en la misma JVM) que el Visor 230 de PA y puede estar sujeto

a las mismas restricciones y configuraciones dictaminadas por la empresa que el Visor 230 de PA. El Navegador de Internet no está dentro del mismo contenedor que el Visor 230 de PA. El *Proxy* Dividido 228 de PA pasa el código de autenticación al Navegador de Extranet cuando se lanza (paso 1702); no hay disponible ningún código de autenticación de este tipo para el Navegador de Internet (paso 1703) porque no está dentro del mismo contenedor que el Visor 230 de PA en el *Proxy* Dividido 228 de PA.

Cuando el Navegador de Extranet realiza una solicitud para un *servlet* que se ejecuta en el HD (paso 1706), la información de autenticación se confirma en el *Proxy* Dividido 228 de PA y la solicitud se procesa (paso 1705) en el *Proxy* Dividido 212 de HD. Si el usuario intenta realizar una solicitud de *servlet* en el dispositivo de mano desde el Navegador de Internet (paso 1712) (que puede no estar en el contenedor), el navegador no puede proporcionar la información de autenticación y, en consecuencia, se deniega la solicitud (paso 1711) en el *Proxy* Dividido 228 de PA. Cuando el Navegador de Extranet solicita recursos de Intranet, la información de autenticación se pasa al *Proxy* Dividido 228 de PA en el encabezamiento de las solicitudes de HTTP utilizando métodos conocidos por quienes están familiarizados con el protocolo. Se invoca la infraestructura del *Proxy* Dividido 228 de PA y la información de autenticación se propaga al servidor de destino, ya sea un servidor *proxy* adicional (pasos 1707, 1708) o el servidor de intranet de destino real que proporciona el recurso (pasos 1710, 1709). El uso de un servidor *proxy* adicional se explica en detalle posteriormente. A continuación, el servidor de destino o bien verificaría la información de autenticación en el encabezamiento de la solicitud de HTTP y denegaría la solicitud si la información de autenticación no está presente o bien, alternativamente, validaría la información de autenticación con una base de datos que tenga datos de autenticación registrados (que pueden ser proporcionados por el contenedor en la inicialización 1700, por ejemplo).

Alternativamente, en el momento de determinar el *proxy* adicional (con referencia todavía a la Fig. 12), el *Proxy* Dividido 228 de PA podría determinar si el *proxy* adicional está designado como un *proxy* de intranet (es decir, para acceder a datos o aplicaciones empresariales) o un *proxy* de Internet (no mostrado). Si se trata de un *proxy* de intranet, el *Proxy* Dividido 228 de PA denegaría la solicitud si la información de autenticación no se confirmase. Se podría utilizar un componente del lado del servidor para ayudar a tomar una determinación entre direcciones de intranet e Internet (por ejemplo, para determinar si la determinación se realiza en el servidor o si se envía sin solicitud previa una lista dinámica de dominios al contenedor). La empresa podría restringir aún más el acceso a ciertos dominios de Internet en función de la presencia o confirmación de la información de autenticación.

El uso de microalmacenamiento extraíble/actualizable, como tarjetas microSD y otros, es común para separar la compra de módulos de memoria con respecto a la compra de un dispositivo de mano. El beneficio que esto proporciona es que el módulo de memoria se puede actualizar, de 4 GB a 32 GB, por ejemplo, sin dejar de utilizar el mismo dispositivo de mano. Los nuevos dispositivos de comunicación inalámbrica, como el iPhone™ y el BlackBerry Bold™, también se venden con módulos de memoria *flash* no extraíbles. Uno de los beneficios de este módulo de memoria adicional no extraíble es que se pueden enviar con o sin solicitud previa grandes cantidades de datos al dispositivo de comunicación inalámbrica y residir en este módulo de memoria sin dejar de ser controlados por la empresa a través de la infraestructura móvil (por ejemplo, los datos de BlackBerry pueden ser borrados de forma remota por la empresa). Además, este módulo de memoria puede ser o no direccionable/legible mediante soportes de USB estándar conectados en PCs (o Mac, etc.). Por ejemplo, BlackBerry tiene la capacidad (por ejemplo, a través de políticas de IT) de deshabilitar el dispositivo de comunicación inalámbrica para que no muestre este módulo de memoria interno como una unidad estándar (por ejemplo, Modo de Almacenamiento Masivo Desactivado) cuando el dispositivo de comunicación inalámbrica se conecta a un PC/portátil a través de cable de USB. En algunos escenarios, es deseable hacer que el módulo de memoria extraíble esté disponible adicionalmente, en cualquier punto extremo, para datos tanto personales como corporativos, preservando al mismo tiempo la seguridad de los datos corporativos.

Se crean desafíos asociados cuando se originan datos en el punto extremo y los mismos se cifran en el módulo de almacenamiento de HD, o por ejemplo, como se ha descrito con referencia a las Figs. 12-13 anteriormente. A menudo se desea, y en algunos contextos empresariales se requiere, que se realice una copia de seguridad de los datos con fines de recuperación. Además, es deseable escanear los datos en busca de virus - los datos originados en un punto extremo que no es de confianza podrían tener virus dentro de ellos, por lo que se recomienda escanear los datos antes de ser aceptados por detrás de un cortafuegos empresarial, por ejemplo para que otros los abran en plataformas de escritorio heredadas, como Microsoft Office. Es engorroso realizar copias de seguridad y escanear datos cifrados. Las claves, etc. se deben compartir y se debe realizar una copia de seguridad/mantenimiento de las mismas.

De acuerdo con una realización adicional, el HD y el PA pueden configurarse para proporcionar acceso a sistemas de archivos (por ejemplo, dentro de microSD u otro módulo de memoria incorporado) cuando el Modo de Almacenamiento Masivo está desactivado, lo que permite leer y escribir en el HD pero, sin embargo, forzando a que no se queden datos del HD en el PA.

La Fig. 18 es un diagrama de bloques de una realización adicional del HD 1802 y el PA 1804 configurados de manera que un PA 1804 de punto extremo puede leer y escribir datos en un módulo 1806 de almacenamiento en el HD pero, sin embargo, no quedan datos en el PA (por ejemplo, en el módulo 1808 de almacenamiento de punto extremo). Se proporciona un entorno de contención de datos para aplicaciones en el PA que restringe que las mismas almacenen datos, a no ser que sea de forma transitoria, o que comuniquen datos desde el PA a no ser que se produzca a través del sistema de archivos virtual. Aquellos con conocimientos habituales en la materia apreciarán que en la Fig. 18 sólo

se ilustran componentes físicos y de *software* seleccionados.

El PA 1804 comprende un módulo 1808 de almacenamiento físico (tal como una unidad de disco duro, *flash*, un grabador de discos ópticos, etc.), una(s) interfaz(es) 1810 de red que proporciona(n) acceso a una LAN o red pública (no mostrada), I/O estándar 1812 y una pluralidad de aplicaciones 1814 como paquetes de aplicaciones y navegadores. Normalmente, estas aplicaciones 1814 están configuradas para almacenar datos usando un servicio de I/O estándar 1810 en medios físicos tales como el 1808. Algunas pueden configurarse para acceder a recursos usando la interfaz 1810. El HD 1802 comprende medios 1806 de almacenamiento tales como una memoria *flash* no extraíble o *flash* extraíble (microSD u otro formato). De acuerdo con la presente realización, el HD 1802 y el PA 1804 están configurados para comunicarse de forma segura a través de un *proxy* dividido y un sistema de archivos virtual como se ha descrito con referencia a la Fig. 2 y adaptados como se describe a continuación para proporcionar acceso de WebDAV al módulo 1806 de almacenamiento. Para mayor comodidad, los componentes de lo descrito anteriormente se simplifican como componentes 1820A y 1820B del sistema de archivos virtual (VFS). WebDAV o creación y control de versiones distribuidas basadas en la web es un conjunto de extensiones del HTTP que permite a los usuarios editar y gestionar archivos de forma colaborativa en servidores remotos de la World Wide Web. Los sistemas operativos Microsoft™ y Apple™ brindan soporte de cliente de WebDAV para exploradores de archivos (por ejemplo, Windows Explorer™ y Mac Finder™).

El PA 1804 comprende además un controlador de filtro de bloques (BFD) 1822 y un sistema de monitorización de interfaces de red (NIMS) 1824. El BFD 1822 está configurado para filtrar y atrapar solicitudes de escritura de bloques de I/O estándar en un dispositivo de almacenamiento disponible para el PA (que no sea a través del VFS), dirigiendo los bloques a una memoria caché gestionada 1826 para almacenar temporalmente los datos. La memoria caché gestionada puede estar cifrada. La memoria caché se borra al reiniciar el PA y el PA se reinicia al final de una sesión. Las solicitudes de aplicaciones para leer en uno o más de los bloques almacenados en memoria caché se atrapan para obtener los datos de la memoria caché según sea necesario o del módulo 1808 de almacenamiento según sea necesario. De esta manera, los datos creados cuando el HD y el PA están acoplados y funcionando en comunicación (es decir, durante una "sesión") no pueden almacenarse en el PA 1804 más que de forma transitoria y de una manera que no es descifrable sin un índice apropiado mantenido por el BFD 1822. La memoria caché 1826 de datos puede mantenerse en una memoria (por ejemplo, una RAM no mostrada) o en un disco u otro módulo de almacenamiento que incluye el módulo 1828 de almacenamiento.

La I/O estándar que está destinada a una unidad conectada a la red y otro tráfico de red simplemente se bloquea en la medida en que el NIMS 1824 garantiza que las interfaces 1810 de red permanecen apagadas mientras una sesión está vigente para que el PA no se comunique más que con el HD a través del *proxy* dividido.

De acuerdo con la realización, el VFS 1820A y 1820B habilita aplicaciones (1814) que admiten I/O usando el protocolo WebDAV para acceder al módulo 1806 de almacenamiento de HD. Como se ha descrito anteriormente, el VFS 1820A y 1820B proporciona un servidor para admitir *servlets* que pueden configurarse para proporcionar servicios de WebDAV (por ejemplo, listado de directorios, propiedades, creación, eliminación, cambio de nombre, lectura y escritura de archivos), tales como métodos de RPC para implementar el acceso básico al sistema de archivos de acuerdo con la especificación de WebDAV. En lugar de proporcionar dicho acceso a un sistema de archivos en el PA 1804, el VFS está configurado para proporcionar el acceso al módulo 1806 de almacenamiento del HD 1802. Las aplicaciones 1814 que llevan a cabo una I/O basada en WebDAV encontrarán el servidor 1820A de VFS y podrán manipular archivos. En el espacio 1820A, 1806 de VFS. El VFS 1820B usa el protocolo de WebDAV en el PA 1804 y un protocolo privativo entre los dos puntos 1820A y 1820B de VFS por encima de la infraestructura de *proxy* dividido entre el PA y el HD (es decir, comunicaciones privativas a través de Bluetooth o conexión por cable de USB) para habilitar las operaciones del VFS. Si bien se prefiere el WebDAV ya que se trata de una especificación aceptada con numerosos componentes disponibles comercialmente que admiten la especificación, se podrían adoptar otros componentes de soporte del servicio de I/O, incluidos componentes privativos.

De acuerdo con otra realización para abordar los desafíos presentados por el uso de módulos de memoria *flash* o de otro tipo en el HD, se proporciona una configuración de red y un método para proporcionar unos medios para almacenar datos corporativos u otros datos confidenciales en un módulo de almacenamiento extraíble en el HD.

La Fig. 19 ilustra un diagrama de bloques de una realización de una red de comunicación en la que un aparato 104 de presentación está acoplado a un HD 102 que tiene un módulo 1902 de almacenamiento no extraíble y un módulo 1902R de almacenamiento extraíble. El HD 102 está acoplado a través de una infraestructura de red externa (por ejemplo, que incluye una red inalámbrica pública e Internet) a una red local o zona 1910 de aterrizaje corporativa del HD detrás de un cortafuegos 1914. La red 1910 comprende uno o más servidores 1902B que proporcionan espacio de almacenamiento personal para almacenar datos desde el HD 102 como se describe a continuación en la presente. La red 1910 está acoplada a la LAN empresarial 1912 a través del cortafuegos 1915. La LAN 1912 comprende uno o más servidores 1902C y un servidor 1920.

Aprovechando las capacidades de cifrado dentro de la solución del *proxy* dividido, los datos recibidos en formato no cifrado y almacenados en un módulo de memoria no extraíble pueden moverse a un módulo de almacenamiento extraíble y almacenarse en formato cifrado. Los datos que acaban de llegar al HD (por ejemplo, enviados con o sin solicitud previa desde una red corporativa) se almacenan primero en el módulo 1902 de memoria no extraíble (en

formato no cifrado). Sólo cuando están acoplados al PA 104 y en una sesión, son accesibles los datos del módulo 1902 de memoria no extraíble para las aplicaciones en el PA 104.

Una vez leídos inicialmente desde un módulo de memoria no extraíble, al usuario se le ofrece la opción de dejar los datos en el módulo de memoria interno más pequeño o transferir el archivo a los medios 1902R de almacenamiento extraíbles con el contenido cifrado mediante una tecnología de cifrado potente (AES, por ejemplo). Esta opción se puede invocar o bien explícitamente cuando el usuario realiza una acción específica para mover el archivo al módulo 1902R de memoria extraíble - por ejemplo, cuando se le solicita esto al detectar poco espacio libre - o bien implícitamente cada vez que un archivo del módulo 1902 de almacenamiento interno se modifica y se vuelve a guardar.

Una vez transferidos al módulo 1902R de memoria extraíble, los datos permanecen cifrados y, por lo tanto, solo se puede acceder a ellos a través del entorno seguro de *proxy* dividido - incluso si el módulo 1902R de memoria extraíble se retira y se coloca en otro dispositivo no empresarial (no mostrado), solo los archivos personales que no se hayan cifrado serán accesibles de forma general a través de medios estándar.

De manera similar a cómo el dispositivo de mano es una zona de aterrizaje de datos personales para datos provenientes de la empresa al usuario, hay una zona 1910 de aterrizaje creada detrás del cortafuegos 1914 pero fuera de la red corporativa general 1912, 1915. De esta manera, los datos pueden ser respaldados desde el dispositivo 102 de mano y almacenados transitoriamente en un espacio personal (1902B) dentro de la zona 1910 de aterrizaje corporativa que refleja los datos en el dispositivo de mano del empleado. En esta zona 1910 de aterrizaje corporativa, los datos se descifran, se escanean en busca de virus y se propagan a la red corporativa (1902C) para que estén disponibles para su integración en procesos normales de copias de seguridad/recuperación dentro de la empresa y para un acceso general para otros dentro de la red corporativa 1912 (p. ej. el servidor 1920).

La Fig. 20 es un diagrama de flujo de operaciones 2000 para comunicar datos desde el HD a la red corporativa, a través de la zona 1910 de aterrizaje de acuerdo con una realización. En el paso 2002, los Datos se almacenan en una memoria *flash* extraíble 1902R. Los datos se cifran como se ha descrito anteriormente. En el paso 2004, se activa la propagación de datos y los datos "sucios" se transfieren a la zona 1910 de aterrizaje. En 2006, los datos cifrados se descifran, se escanean en busca de virus y se transfieren a la LAN (o Intranet) empresarial 1912 (por ejemplo, para compartir y/o copias de seguridad). En 2007, se hace que los datos depurados estén disponibles en la Intranet, p. ej. en un sistema de archivos, base de datos, repositorio local, según corresponda sobre la base del tipo de datos o la aplicación asociada. En el paso 2008, los datos empresariales se modifican, por ejemplo, a través de unos medios heredados en el departamento de gestión interna de la empresa, según esté disponible a través de la Intranet. Los datos a los que están suscritos los usuarios de HDs (por ejemplo, 102) se identifican y se envían, sin solicitud previa, notificaciones de cambio a los HDs adecuados. En 2011, se recibe la notificación, se resuelven los conflictos y los datos se recuperan, con solicitud previa, y se almacenan en el módulo 1902 de memoria no extraíble en un formato no cifrado. El PA 104 (durante una sesión con el HD 102) se usa para modificar los datos en 2012 y las operaciones 2000 se repiten en el paso 2002.

La Fig. 4 es un diagrama de flujo de las respectivas operaciones 400 de arranque en el HD 102 y el PA 104 de acuerdo con una realización que establece una conexión entre estos dispositivos e inicia el visor 230 de PA con datos de PIM iniciales del HD 102.

En los pasos 402A y 402B, si aún no están emparejados, los dispositivos 102 y 103A se emparejan para una comunicación de Bluetooth como es bien conocido. En el paso 404A, los ejecutables iniciales se cargan desde el módulo 103A de almacenamiento en la versión de ejecución [*runtime*] del PA (por ejemplo, la RAM 200B). El Monitor 220 de PA se carga desde el módulo 103A de almacenamiento. El Monitor 220 de PA carga la pila de Bluetooth (222A), carga el *software* (234) de Claves que interactúa con la pila 222A y el Transporte (224) y el Entorno (228) de Trabajo de *Servlet* y *Proxy* Dividido y carga el Entorno (228) de Trabajo de *Servlet* y *Proxy* Dividido de PA. En el paso 406, el Monitor 220 de PA observa entonces la ejecución de estos componentes y si se determina que alguno se ha detenido, se intenta reiniciar a menos que se determine que la llave electrónica/Clave física 103A ha sido retirada, en cuyo caso monitoriza continuamente el PA 104 para comprobar la presencia de la Clave/llave electrónica antes de intentar reiniciar los componentes.

Con el lado PA ejecutándose, el usuario ahora puede interactuar con la Aplicación (214) de HD y lanzar el Visor (230) de PA de forma remota. En el paso 404B, el usuario inicia la Aplicación 214 de HD e invoca una operación Conexión. Alternativamente, (no se muestra) si la Aplicación 24 de HD ya está conectada, el usuario puede invocar una operación Reinicio (por ejemplo, desde un menú). Utilizando las interfaces 216 de O/S de HD nativas, la Aplicación 214 de HD establece una conexión de Bluetooth de SPP con el PA 104 emparejado que ahora está a la escucha de conexiones del HD previamente emparejado y prepara el Transporte (208) de HD y los Flujos (210) de HD por encima de la conexión (206) de SPP una vez establecida. Una vez conectado, el HD inicializa el Entorno 212 de Trabajo de *Servlet* y *Proxy* Dividido de HD e inicia el Servidor (212B) de *Servlet* y el Servidor *Proxy* Web (212A) para usar los Flujos de HD ahora configurados con la conexión de SPP. En el paso 408B, se envía una solicitud de conexión simple a través del Transporte de HD y la misma es recibida por el Transporte de PA y se pasa al *Proxy* Dividido (228) de PA. En el paso 408A, el *Proxy* Dividido de PA valida la solicitud y carga el Visor 230 de PA en la Versión 200B de ejecución del PA.

Con el Visor 230 de PA ahora ejecutándose, busca instrucciones sobre cómo inicializarse. Preferiblemente, obtiene estas instrucciones de un archivo de configuración almacenado en el HD 102 (pasos 410A y 410B). En el caso de que la inicialización sea la primera vez que se lanza el Visor 230 de PA, es posible que no se encuentre ningún archivo de configuración y el Visor de PA puede usar ajustes predeterminados por primera vez. Los ajustes predeterminados se guardan nuevamente en el HD para que el usuario pueda cambiarlos posteriormente si lo desea como archivo de configuración (no se muestra). El Visor de PA realiza una solicitud de *servlet* 228B al Servidor 212B de *Servlet* de HD usando un URL correspondiente tal como `/viewer/getConfig` para recuperar la información de configuración. El archivo de configuración se procesa y los ajustes se mantienen con la memoria de ejecución del Visor de PA.

Con su información de configuración ahora fijada, el Visor 230 de PA realiza una solicitud para cargar la jerarquía 314 de navegación de carpetas tal como se puede visualizar en el lado izquierdo de la interfaz 300 de usuario enviando una solicitud al Servidor 212B de *Servlet* de HD usando un URL correspondiente tal como `/mail/getFolderList` por ejemplo (paso 412A). El Entorno 212 de Trabajo de *Servlet* de HD responde con un flujo de XML que le dice al Visor 230 de PA qué y cómo presentar la jerarquía 314 de navegación de carpetas (paso 412B).

Con la jerarquía de navegación fijada, el Visor de PA ahora puede ejecutar cualquier instrucción de configuración de arranque realizando solicitudes adicionales hacia el Servidor de *Servlet* de HD como lo indica su configuración (pasos 414A y 414B). Las instrucciones de arranque pueden incluir instrucciones para cargar varios datos de PIM desde el HD 102, como datos de mensajes (es decir, Bandeja de entrada, elementos enviados, etc. para las Carpetas de 314), datos de contacto y datos de calendario, etc. Por ejemplo: si está configurado para cargar los datos de la carpeta Bandeja de entrada en el arranque, se llama a una solicitud hacia el Servidor de *Servlet* de HD utilizando un URL correspondiente como `/mail/getMailList` con parámetros suficientes para identificar la carpeta para la cual se debe devolver la lista de correo y el modo en el que se debe devolver la lista (es decir, si la lista completa debe devolverse en un lote o si la lista debe paginarse).

Con el Visor 230 de PA ahora iniciado, configurado exclusivamente por la configuración del HD, e inicializando su visualización, el usuario es libre de interactuar y comenzar a leer el correo electrónico, buscar contactos, organizar el calendario y redactar nuevos mensajes como desee.

A medida que se producen eventos nuevos en el HD 102 (por ejemplo, mensajes recibidos, actualización de contactos, cambios de calendario, etc.), el Visor 230 de PA puede actualizarse para presentar los eventos. Preferiblemente se proporciona un modelo escuchador de eventos mediante el cual se puede informar, al Visor de PA, sobre cambios después del arranque. El modelo de eventos se puede aplicar no sólo al correo electrónico sino a cualquier evento que se produzca en el HD 104 para su visualización mediante la capa de presentación, proporcionando una arquitectura de escuchador para el tipo de recurso particular - por ejemplo, Calendario, Contactos, Correo, etc. Usando el correo electrónico como ejemplo:

(a) En el arranque, el Entorno 212 de Trabajo de *Servlet* de HD registra un `folderListener` (no mostrado) para cada carpeta 314 que pudiera recibir un mensaje nuevo enviado sin solicitud previa al HD;

(b) En el arranque, el Entorno 212 de Trabajo de *Servlet* de HD pone en marcha un hilo `EventProcessing` (no mostrado) que monitoriza mensajes de eventos de adición y eliminación para su transmisión al lado PA con el fin de presentarlos al usuario;

(c) Cuando se envía, sin solicitud previa, un mensaje al HD, se activa el `folderListener` y se proporciona el mensaje y la carpeta al escuchador;

(d) El escuchador construye un mensaje nuevo basado en XML y lo coloca en la cola de eventos salientes (no mostrada). Por ejemplo, el hilo `EventProcessor` realiza un POST de evento: `///mail/newMail` cuando llega un mensaje nuevo e incluye en la carga útil del POST un mensaje basado en XML que contiene información similar a los mensajes enviados al Visor 230 de PA en la inicialización;

(e) El hilo `EventProcessing` espera notificaciones del escuchador y comprueba periódicamente la cola en busca de eventos nuevos;

(f) A medida que el hilo `EventProcessing` detecta nuevos elementos en la cola, los empaqueta en un mensaje basado en XML y los envía al Lado PA para su presentación a través del visor 230.

Con respecto a la realización de la Fig. 18, se realizan operaciones de instalación y arranque similares para configurar el PA 1804. En la instalación, el BFD 1822 y el NIMS 1824 se instalan para redirigir respectivamente derechos de disco a la memoria caché gestionada 1826 y garantizar que las interfaces 1810 de red permanecen apagadas durante una sesión. Se define un "userid" del sistema operativo para su uso durante una sesión, al userid se le asignan ciertos derechos o privilegios y se le restringen otros. Por ejemplo, la capacidad de cambiar a un usuario diferente (por ejemplo, un usuario administrativo) durante una sesión se revoca o impide para frustrar intentos de eludir características de seguridad que impiden dejar datos en el PA 1804.

Al poner en marcha un PA, se inicia el Monitor 220 de PA para obtener una ejecución de una sesión. El userid se confirma con los derechos adecuados para que se apliquen las restricciones de tiempo de ejecución antes de que se

establezca una conexión con el HD 1802. El NIMS 1824 apaga las interfaces 1810 para impedir que un usuario (a sabiendas o sin saberlo, por ejemplo a través de un virus) tome datos recibidos a través de una conexión de una sesión y los emita a través de una conexión de red que no está gestionada por el HD y su infraestructura de red conectada. Se establece la conexión con el HD y el usuario del PA 1804 puede comenzar a utilizar el HD, por ejemplo, para acceder a recursos conectados empresariales a través del HD, correo electrónico, etc.

Durante el funcionamiento, el NIMS mantiene las interfaces apagadas. El BFD redirige las escrituras de disco (nivel de bloques) a la memoria caché gestionada 1826 como almacenamiento volátil, gestionando los bloques atrapados y escritos en la memoria caché para volver a servirlos en lecturas posteriores, etc. Al reiniciarse el sistema de un PA, el "almacenamiento volátil" se elimina, garantizando así que no queden detrás datos en el PA 1804 durante una sesión.

Al salir de la sesión, el PA se reinicia para eliminar los datos de la memoria caché y volver a un estado inicial anterior a la sesión.

Con una interpretación del arranque, la configuración y la inicialización iniciales, a continuación se describirán operaciones representativas para usar el visor 230 de PA. La Fig. 5 es un diagrama de flujo de operaciones 500 para redactar y enviar un correo electrónico usando el Visor 230 de PA.

En el paso 502, un usuario lanza una ventana de "mensaje nuevo" usando los controles del Visor de PA (por ejemplo, 306). El usuario redacta el correo electrónico, introduciendo destinatarios de Para, destinatarios de CC, destinatarios de CCO, la línea de Asunto y el cuerpo del mensaje según lo desee (paso 504). Cuando los contactos 324 han sido cargados en el arranque (típico) o manualmente por el usuario, al seleccionar la pestaña Contactos los contactos se pueden usar en una lista desplegable para facilitar la introducción de direcciones de correo electrónico utilizadas comúnmente;

En el paso 506, con el nuevo mensaje de correo redactado, el usuario presiona el control Enviar (por ejemplo, desde los controles 306). El Visor 230 de PA empaqueta el mensaje nuevo en una carga útil de XML y realiza un POST de los datos del mensaje al servidor 212B de *Servlet* de HD usando un URL correspondiente como /mail/sendMessage (paso 508). Para comodidad del usuario y de manera similar a la redacción y el envío de correo usando aplicaciones de correo utilizadas comúnmente, el correo electrónico en fase de borrador puede mantenerse en una carpeta Borrador (no mostrada) en la vista 314 de árbol de carpetas y el correo electrónico saliente (después de la invocación al envío) se puede mantener en una carpeta Bandeja de salida (no mostrada).

En el HD 102, la solicitud basada en XML es recibida por el Servidor 212B de *Servlet* de HD y la solicitud se pasa al *Servlet* apropiado dentro del Entorno 212 de Trabajo de *Servlet* (paso 510). El *Servlet* sendMessage desempaqueta el XML e interactúa con las API 216 de HD para crear un mensaje de correo electrónico estructurado apropiadamente para el HD y envía el mensaje por el transporte de correo electrónico del HD (paso 514). En los pasos 516 y 518, el *Servlet* sendMessage responde y el Visor de PA recibe una confirmación de que el mensaje de correo electrónico se mandó a la cola de salida del HD. Aunque no se muestra, el Visor 230 de PA recibe una notificación de evento para actualizar una carpeta de Elementos Enviados en la parte 314 del visor.

Se pueden realizar operaciones similares para otras actividades de mensajes tales como Responder/Responder a Todo, Reenviar, etc. Para responder a un mensaje, un usuario selecciona el mensaje deseado de la lista de mensajes 316 y hace clic derecho en él y selecciona "Responder" o "Responder a Todo" o usa los controles 304 del menú Acciones para hacer lo mismo o usa el botón apropiado en la barra 306 de botones. El Visor 230 de PA lanza la ventana de redacción de correo electrónico de manera similar a la anterior pero también completa de manera previa los Campos de Destinatarios, fija el asunto en "RE: " + asunto y, opcionalmente, realiza una solicitud al Servidor 212B de *Servlet* de HD para recuperar el contenido completo del mensaje original usando un URL correspondiente como /mail/fetchMessage, proporcionando parámetros apropiados para que el *Servlet* fetchMessage recupere el contenido del correo electrónico original usando las API 216 de HD necesarias. El Visor 230 de PA rellena previamente la ventana del cuerpo del mensaje con el mensaje original y marca el contenido como "Original". El usuario entonces es libre de editar cualquier parte del contenido del mensaje antes de presionar el botón "Enviar" 306. De manera similar, el Visor 230 de PA empaqueta el mensaje de respuesta en una carga útil de XML y realiza un POST de los datos del mensaje al Servidor 212B de *Servlet* de HD usando un URL correspondiente como /mail/replyToMessage que proporciona parámetros apropiados para que el *Servlet* replyToMessage utilice las API 214 de HD necesarias para construir un mensaje de correo electrónico en el HD 102 que represente una respuesta al mensaje original y para su emisión posteriormente al transporte de correo electrónico de HD para su puesta en cola. El *Servlet* de HD a continuación responde con una confirmación de que el mensaje se puso en cola para su transmisión.

Al reenviar un mensaje, las operaciones son similares a responder. Sin embargo, es preferible que el mensaje original no se recupere y el usuario no tenga la opción de modificar ninguna parte del contenido del mensaje original antes de enviarlo. Para garantizar que el lado HD pueda construir un mensaje saliente como un reenvío estructurado adecuadamente usando las API 216 de HD necesarias para construir un correo electrónico, se llama un URL correspondiente distinto similar a /mail/sendForwardMessage.

Cualquiera de los tipos de mensajes anteriores se puede guardar como borrador de mensaje en el módulo de memoria de HD. Los pasos son idénticos en cada caso, excepto que en lugar del URL para enviar el mensaje, el URL indica

que se debe guardar un borrador. Por ejemplo, el URL correspondiente /mail/saveForwardMessage indica al Entorno de Trabajo de *Servlet* del lado HD que utilice las API de HD necesarias para construir un mensaje con el formato adecuado que pueda reenviarse utilizando el transporte de correo electrónico de HD, pero que en su lugar simplemente almacene el mensaje como un borrador para su posterior edición adicional y su envío más tarde.

5 A menudo, un correo electrónico incluye un documento adjunto. Un documento adjunto puede comprender datos destinados a una aplicación específica. Ejemplos comunes son documentos de procesamiento de textos (por ejemplo, para MS Word), documentos de imagen (.tiff, .GIF, .jpeg) y documentos en formato de documento portátil (es decir, PDFs). Para reducir el consumo de ancho de banda inalámbrico, minimizar los requisitos de almacenamiento del HD y reducir los requisitos de renderización de datos del HD, la comunicación de datos de correo electrónico al dispositivo
10 de mano, por lo tanto, puede no incluir datos correspondientes a archivos adjuntos o (ya sea por petición del usuario de datos adjuntos o automáticamente) puede incluir solo datos reducidos. Por ejemplo, un archivo adjunto de un documento de procesamiento de textos puede incluir sólo texto limitado y datos de formato para el dispositivo de mano.

De manera ventajosa, el PA 104, especialmente en forma de ordenador portátil, normalmente tiene almacenamiento adecuado y aplicaciones nativas para trabajar con tales archivos adjuntos en formato nativo. La Fig. 6A ilustra una
15 realización alternativa 600 de la red 100 en la que los servidores acoplados a la LAN 112 son diferentes de la Fig. 1. La LAN 112 puede configurarse para incluir un servidor 602 de archivos adjuntos, por ejemplo usando protocolos IMAP o POP, para extraer un correo electrónico con su archivo adjunto del servidor 118 de correo electrónico, en una solicitud recibida del visor 230 de PA a través del HD 102, y entregar en formato nativo el archivo adjunto como respuesta al Visor 232 de PA a través del HD 102.

20 La Fig. 7 ilustra operaciones 700 para obtener un archivo adjunto de correo electrónico en su formato nativo usando el servidor 602. El Visor 230 de PA facilita que un usuario solicite selectivamente (no se muestra) un archivo adjunto particular asociado a un correo electrónico. A petición del usuario, el Visor de PA envía una solicitud de HTTP a través del *proxy* dividido (paso 702). La solicitud identifica el correo electrónico que tiene el archivo adjunto en el servidor 118 de correo electrónico. La solicitud se dirige a través del HD 102 a la LAN 112 y posteriormente a través del servidor
25 116 al servidor 402 de archivos adjuntos (paso 704). Como se ha señalado, el servidor 402 de archivos adjuntos tiene acceso al servidor 118 de correo electrónico a través de protocolos IMAP. El servidor 402 de archivos adjuntos obtiene el correo electrónico con el archivo adjunto del servidor 118 (paso 706), extrae el archivo adjunto (paso 708) y devuelve el archivo adjunto en su formato nativo en una respuesta de HTTP al Visor de PA (paso 710). El Visor de PA a continuación proporciona el archivo adjunto al usuario.

30 Se puede ofrecer a un usuario una opción para guardar archivos adjuntos en un módulo de memoria de PA - preferiblemente, esta opción se puede deshabilitar cuando lo requieran las implementaciones empresariales. Cuando una aplicación asociada está disponible en el PA para un tipo de archivo adjunto determinado, la misma se puede lanzar para renderizar el archivo adjunto para verlo y/o editarlo. Alternativamente, se pueden usar aplicaciones basadas en la web para hacer lo mismo:

35 (a) haciendo que el PA solicite que el archivo adjunto se mande a un servidor de aplicaciones compartido como docs.google.com o un tipo de servicio similar y posteriormente lanzando un navegador para el URL apropiado en el servidor de aplicaciones; o

(b) guardando el archivo adjunto en el módulo de memoria del HD, mandando el archivo adjunto guardado a un servidor de aplicaciones de manera similar al punto a) anterior y a continuación lanzando un navegador para el URL apropiado
40 en el servidor de aplicaciones de manera similar al punto a) anterior;

En otra realización, un servidor de archivos adjuntos puede configurarse de manera similar al servidor 602 de archivos adjuntos para recuperar, sin solicitud previa, el correo electrónico y su archivo adjunto y reenviar el archivo adjunto al Visor de PA solicitante. Por ejemplo, el Visor de PA se puede configurar para enviar solicitudes de archivos adjuntos al servidor de archivos adjuntos. Ese servidor de archivos adjuntos está configurado con una cuenta de correo electrónico para el HD y una capacidad de procesamiento de servidor de archivos adjuntos como se describe con
45 referencia al servidor 602. Para obtener el archivo adjunto, el correo electrónico de interés que contiene el(los) archivo(s) adjunto(s) se reenvía primero a través de la aplicación del PA al servidor de archivos adjuntos, a través de protocolos SMTP/SMIME estándar, a una cuenta de correo electrónico específica del HD. A continuación, el PA solicita el archivo adjunto de interés utilizando una solicitud de HTTP/S similar a la respuesta de solicitud descrita anteriormente con referencia a la Fig. 7. El servidor de archivos adjuntos recupera, sin solicitud previa, el correo electrónico y el archivo adjunto en formato nativo del servidor 118 de correo electrónico por detrás del cortafuegos 114 para proporcionar una respuesta al PA 104. Este servidor de archivos adjuntos puede ser uno alojado fuera de la empresa más allá de la LAN 112 o dentro del entorno de la LAN 112. Como entenderán las personas con conocimientos habituales en la técnica, un servidor alojado externamente puede requerir una seguridad diferente para
50 acceder al servidor 118 de correo electrónico por detrás del cortafuegos 114. Puede ser preferible alojar el servidor de archivos adjuntos dentro de la LAN 112 para cumplir con los estándares de IT de la empresa.

La Fig. 6B ilustra una realización alternativa 640 de la red 100 y la red 600 en la que la LAN 112 es nuevamente diferente. En esta realización 640, la LAN 112 comprende un Servidor 642 de Claves para cifrar las comunicaciones entre el PA 104 y el HD 102, proporcionando una clave de cifrado y un *token* de autenticación como se describe con

más detalle de acuerdo con la Fig. 8.

La Fig. 8 ilustra un diagrama de flujo de operaciones para cifrar una parte de una red de comunicación tal como la red 640. En el paso 802, usando la aplicación 214 de HD, el usuario realiza una solicitud de HTTP a través de la infraestructura inalámbrica segura del dispositivo de mano (a través del servidor 108 y 116) al Servidor 642 de Claves para obtener una clave privada.

En el paso 804, el Servidor 642 de Claves responde con una clave privada que comprende preferiblemente una matriz pseudoaleatoria generada de bytes (por ejemplo, un mínimo de 128 bits y configurable) y un *token* de autenticación de tercer factor que comprende una cadena pseudoaleatoria generada independiente de al menos 8 caracteres (configurables).

En el paso 806, la Aplicación 214 de HD recibe la clave y el *token* y visualiza el *token* que se introduce en el Visor 230 de PA. Alternativamente, el *token* podría pronunciarse para el usuario.

El Visor 230 de PA establece una Conexión segura de TLS 1.0 con el Servidor 642 de Claves por medio de los componentes de *software* del *proxy* dividido de PA descritos en la Fig. 2 y solicita la misma clave privada que se obtuvo en el paso 602 proporcionando el *token* en una solicitud de HTTPS/TLS (paso 808).

En el paso 810, el Servidor 642 de Claves usa el *token* para buscar la clave privada que se proporcionó en el paso 802 y devuelve esa clave en la respuesta a la solicitud. En el paso 812, una vez que el Visor 230 de PA recibe la clave privada, se proporciona al lado PA del *proxy* dividido 228 y se envía una solicitud al lado HD 212 indicando que todas las transmisiones de datos posteriores se cifrarán usando la clave privada recién obtenida.

Con referencia a las Figs. 1, 2 y 9-11, las comunicaciones desde una aplicación (por ejemplo, el navegador 232) en el PA 104 a un recurso de destino en Internet 110 o Intranet 112 normalmente viajan a través de al menos dos *proxies*. El primero es el servidor *proxy* dividido 212 y 228 y el segundo es el servidor empresarial 116 de HD. Este segundo *proxy* 116 también puede funcionar, por ejemplo, como cortafuegos 114. Las Figs. 9 a 11 ilustran operaciones para configurar y operar el servidor *proxy* dividido 212 y 228 para comunicarse con el tercer servidor *proxy* 130 o los servidores 130-1, 130-2, ... 130-n que proporcionan acceso a recursos de Internet o Intranet. El *proxy* 116 en la infraestructura inalámbrica se denomina "*Proxy* de 2º Nivel" en los diagramas de flujo de las Figs. 9 a 11. Es común que una empresa requiera que las comunicaciones desde el *proxy* 116 de infraestructura inalámbrica viajen a través de otro (tercer) *proxy* tal como el *proxy* 130 para obtener acceso a los recursos en Internet 110 o Intranet 112. Las empresas pueden dirigir además dichas comunicaciones (es decir, desde el *proxy* en la infraestructura inalámbrica) a través de diferentes *proxy* de tercer nivel 130-1, 130-2, ..., 130-n dependiendo del tipo o dirección del recurso solicitado. Los navegadores generalmente se configuran para acceder a los recursos de Internet o Intranet, ya sea configurándolos con una única dirección de *proxy* estática o configurándolos con un URL en un *script* que determina la dirección de *proxy* dada la dirección del recurso.

Las dos partes del *proxy* dividido, el Entorno 212 de Trabajo de *Servlet* y *Proxy* Dividido de HD (el "*Proxy* de HD") y el Entorno 228 de Trabajo de *Servlet* y *Proxy* Dividido de PA (el "*Proxy* de PA"), funcionan en conjunto para proporcionar un *proxy* con todas las funciones para el navegador 232. Por razones de rendimiento, el *Proxy* 212 de HD puede no procesar encabezamientos, sino que puede depender del *Proxy* 228 de PA para indicarle a qué dirección conectarse para recuperar el recurso solicitado. Al *Proxy* 212 de HD se le proporciona acceso a la red empresarial 112 a través del servidor empresarial 116 de HD que reside en la infraestructura inalámbrica. Por ello, los medios típicos disponibles para configurar un navegador en un PC para comunicarse con los recursos de Internet o Intranet en una empresa a través de un tercer *proxy* 130 no están inherentemente disponibles usando la configuración de *proxy* dividido.

La Fig. 9 ilustra un método para proporcionar acceso a recursos de Internet o Intranet a través del *proxy* de tercer nivel de acuerdo con una realización en la que la empresa requiere que todas las solicitudes de dichos recursos se dirijan a través de un único servidor *proxy* (es decir, 130). El servidor *proxy* 116 en la infraestructura inalámbrica pasa (por ejemplo, envía sin solicitud previa) un parámetro que representa la dirección del servidor *proxy* 130 de la empresa a HDs que gestiona y que están configurados para usar el servidor *proxy* dividido (bloque 902). El parámetro es recibido y almacenado en una base de datos de políticas local por el *Proxy* de HD que representa la dirección del servidor *proxy* 130 de la empresa (bloque 903). El *proxy* HD recupera este parámetro (bloque 904) y lo pasa al *proxy* de PA en la conexión inicial (bloques 906 y 908). Con el *Proxy* de PA ahora informado de la dirección del servidor *proxy* 130 de la empresa, el mismo puede indicarle al *Proxy* de HD que se conecte al servidor *proxy* 130 de la empresa en todas las solicitudes posteriores de recursos del navegador 232 en el PA (véase, por ejemplo, 910, 912, 914). En una realización alternativa, se puede omitir el paso 902 y proporcionar la dirección de *proxy* al *Proxy* de HD por otros medios, tales como introduciéndola a través de una interfaz de usuario.

Una empresa puede requerir que el acceso a recursos de Internet o Intranet se enrute dinámicamente a través de diferentes *proxies* (por ejemplo, 130-1, 130-2, ..., 130-n) dependiendo de la naturaleza del recurso que se solicita. En tales situaciones, los navegadores suelen utilizar *scripts* para determinar el servidor *proxy* adecuado al que apuntar. La Fig. 10 ilustra un método para comunicarse en una red empresarial de este tipo utilizando la configuración de *proxy* dividido según una realización. El servidor empresarial 116 del servidor de HD en la infraestructura inalámbrica pasa (por ejemplo, envía sin solicitud previa) un parámetro que representa una dirección de URL de un *script* para

determinar el servidor *proxy* apropiado al que apuntar a HDs que son gestionados por él y que están configurados para usar el sistema de *proxy* dividido (bloque 1002). El HD recibe y almacena el parámetro en una base de datos de políticas local que representa la dirección de URL del *script* para determinar el servidor *proxy* apropiado al que apuntar (bloque 1003). El *Proxy de HD* recupera el parámetro (bloque 1004) y a continuación lo pasa al *Proxy de PA* en la conexión inicial (bloques 1006, 1008). A continuación, el *proxy de PA* recupera (bloque 1010) el *script* del *proxy* de interfaz inalámbrica usando el parámetro de URL y carga el *script* en un motor de *script* en tiempo de ejecución (bloque 1012). Cuando el *Proxy de PA* recibe una solicitud de HTTP (bloque 1014), el *Proxy de PA* pasa el URL de la solicitud a través del *script* para determinar la dirección del servidor *proxy* (bloque 1016). A continuación se formatea la solicitud (para especificar los Encabezamientos de HTTP y la dirección del *proxy* de interfaz inalámbrica) antes de ser enviada al *Proxy de HD* (bloque 1018). Después de esto, el *Proxy de HD* completa la solicitud de HTTP (bloque 1020) utilizando la dirección del servidor *proxy* resuelta. Con el *Proxy de PA* ahora informado de la ubicación del *script*, puede recuperar el *script* en el arranque a través del *proxy* en la red inalámbrica. Con el *script* cargado dinámicamente, el mismo permanece actualizado y el *Proxy de PA* puede continuar indicando al *Proxy de HD* que se conecte a direcciones dinámicamente en función de los resultados de la ejecución del *script*, dadas todas las solicitudes posteriores de recursos del navegador en el PA.

En otra realización del método de la Fig. 10 en el que las comunicaciones de red se enrutan dinámicamente a través de diferentes *proxies* dependiendo de la naturaleza del recurso que se solicita antes de acceder a los recursos de Internet o Intranet, se pueden omitir operaciones del bloque 1002. El HD puede recibir el parámetro por otros medios, como por ejemplo introduciéndolo a través de una interfaz de usuario.

Cuando una empresa requiere que las comunicaciones de red se enruten dinámicamente a través de diferentes *proxies* dependiendo de la naturaleza del recurso que se solicita, los *scripts* que normalmente se usan para determinar el servidor *proxy* apropiado al que apuntar pueden depender de información que solo está disponible cuando la aplicación que solicita el recurso está conectada directamente a la red de la empresa. Por ejemplo, una empresa puede requerir el uso de un determinado *proxy* si el dominio del recurso solicitado reside en el Sistema de Nombres de Dominio (DNS) de la empresa y, si no reside en el DNS, puede ser necesario un *proxy* diferente. La ejecución de un *script* en el HD o PA no resolverá correctamente la dirección del *proxy* a menos que el *script* acceda a la empresa para determinar el contenido del DNS.

En una realización, representada en la Fig. 11, se proporciona un método para determinar las direcciones apropiadas de las direcciones de los *proxies* empresariales 130-1, 130-2, ... 130-n en función del dominio o tipo de recurso o dirección a través de un *script* ejecutado en un servidor *proxy* en la infraestructura inalámbrica. Un parámetro que representa la dirección de URL de un *script* o método de *software* de *servlet* en el Servidor *Proxy* de 2º Nivel se pasa (por ejemplo, se envía sin solicitud previa) al HD (bloque 1102) por parte del servidor 116. El parámetro (por ejemplo, URL) se recibe y se almacena en una base de datos de políticas local (bloque 1130). Alternativamente, el *Proxy de HD* puede recibir la dirección de URL de un *script* o método de *software* de *servlet* por otros medios, como mediante entrada a través de una interfaz de usuario. El *proxy de HD* puede recuperar el URL (bloque 1104). Dada la dirección de un recurso solicitado, el método de *software* devolverá la dirección del *proxy* (por ejemplo, 130-1, 130-2, ..., 130-n) requerida por la empresa.

El parámetro puede pasarse desde el *Proxy de HD* al *Proxy de PA* en la conexión inicial (bloques 1106, 1108). Alternativamente, el *Proxy de HD* puede llamar al *script* y determinar la dirección del *proxy* sin la necesidad del *Proxy de PA*. El *Proxy de HD* (o el *Proxy de PA* si tiene el parámetro) puede llamar al método de *software* con la dirección del recurso como entrada (bloques 1112A, 1112B, 1112C). La dirección de *proxy* resultante se devuelve desde el *proxy* de infraestructura inalámbrica al *Proxy de PA* (bloque 1114) (y a continuación se almacena en memoria caché en el *Proxy de PA* si es necesario, bloque 1118). Los encabezamientos de HTTP y la dirección del *proxy* de infraestructura inalámbrica se formatean en la solicitud de HTTP original que a continuación se envía de vuelta al *Proxy de HD* (bloque 1118). El *Proxy de HD* a continuación completa la solicitud de HTTP (bloque 1120) usando la dirección de *proxy* resuelta. Con el *Proxy de PA* ahora informado de la dirección de URL del *script*, el mismo puede llamar al *servlet* (bloques 1112A, 1112B, 1112C) usando la solicitud de HTTP y resolver dinámicamente la dirección del *proxy* para acceder al recurso de HTTP. Además, ahora que el *Proxy de HD* (y posiblemente el *Proxy de PA*) está informado de la dirección del *proxy* de la empresa para una determinada solicitud de recurso, el *Proxy de HD* puede conectarse (o el *Proxy de PA* puede indicarle al *Proxy de HD* que se conecte) a la dirección de *proxy* de la empresa en todas las solicitudes posteriores de ese recurso del navegador del PA.

Como se ha señalado anteriormente, la virtualización de la capa de presentación se puede detener automáticamente en el PA 104 en respuesta a ciertos eventos, particularmente aquellos eventos que sugieren una oportunidad para que personas distintas al usuario tengan acceso a los datos virtualizados (por ejemplo, cuando el usuario no está cerca del PA 104). Por ejemplo, en las realizaciones ilustradas, el PA 104 y el HD 102 están acoplados a través de radiocomunicaciones de corto alcance y el PA 104 está provisto de una llave electrónica 103A de unidad de almacenamiento *flash* que almacena ejecutables que implementan aspectos de la invención. La conexión de Bluetooth entre el HD 102 y el PA 104 se puede detener, por ejemplo, cuando estos últimos salen fuera del alcance (por ejemplo, cuando el usuario aleja el HD 104 del PA 104). La conexión puede detenerse cuando la llave electrónica se retira del PA 104. En estas circunstancias, es probable que el usuario no desee que terceros tengan acceso a datos que puedan virtualizarse en un dispositivo de visualización de PA. Tales eventos preferentemente desencadenan una eliminación de datos virtualizados de la pantalla. Esto se puede lograr de diferentes maneras, incluido el apagado del visor 230 de

PA, por ejemplo.

La monitorización del estado de la conexión de HD-PA y de la conexión de la llave electrónica 103A al PA 104 se puede realizar de varias maneras. Por ejemplo, cuando el Monitor 220 de PA se lanza desde la llave electrónica 103A, reconoce su unidad de inicio/raíz. El monitor 220 de PA puede ser informado del estado de la conexión de Bluetooth (por ejemplo, a través de la pila 222A), pudiéndose presentar dicho estado al usuario. Al finalizar la conexión, el Monitor 220 de PA puede solicitar al usuario que lo apague. Se puede configurar una operación predeterminada de manera que si no se recibe respuesta dentro de un tiempo predeterminado, el Visor de PA se detiene automáticamente. Dicho temporizador permite a un usuario volver a establecer una conexión para continuar las operaciones y tiene en cuenta que un usuario haya abandonado las proximidades del PA 104 con el HD 102.

Si no hay conexión entre el PA 014 y el HD 102, el Monitor 220 de PA puede sondear el acceso a su raíz (llave electrónica 103A) y detener inmediatamente el Visor 230 de PA (y otros componentes que se deseen) si la llave electrónica 103A ya no está presente. El Monitor 220 de PA puede permanecer ejecutándose en espera de una conexión adicional. Si se vuelve a colocar la llave electrónica 103A y se inicia la conexión, se puede informar al monitor 220 de PA, tras lo cual se detiene el sondeo de la llave electrónica 103A y se reinician los componentes (por ejemplo, 224-230) según sea necesario. De manera similar, la pila 222A podría configurarse para monitorizar la presencia de la llave electrónica 103A cuando no hay una conexión disponible, e informar al Monitor 220 de PA de la misma para que invoque el apagado automático como se ha descrito anteriormente. La pila 222A podría permanecer en ejecución, realizando un sondeo para reabrir el dispositivo 103A. Una vez que la pila 222A abre con éxito el dispositivo 103A nuevamente, después de volver a introducirlo, se notifica al monitor 220 de PA que comience el ciclo de (re)inicio. Otras variaciones resultarán evidentes para aquellos con conocimientos habituales en la materia.

No se proporcionan diagramas detallados para el HD 102 y el PA 104, ya que los mismos serán conocidos por personas con conocimientos habituales en la técnica. El PA 104 puede comprender un ordenador portátil o PC u otro dispositivo informático con recursos suficientes para ejecutar un navegador y renderizar en un dispositivo de visualización la capa de presentación del HD. Este dispositivo no necesita tener acceso a la red inherente per se, ya que el HD puede proporcionarlo. Sin embargo, un PA incluirá una interfaz de I/O a través de la cual comunicarse con el HD y ésta puede incluir una capacidad de comunicación inherente de corto alcance, como Bluetooth inalámbrico o una interfaz de comunicación en serie (por ejemplo, USB). Como se muestra, se puede configurar una interfaz de USB (por ejemplo, a través de la llave electrónica 103A) para proporcionar capacidades de comunicación inalámbrica de corto alcance a un PA.

Los dispositivos adecuados que pueden configurarse como HD 102 son dispositivos de comunicación bidireccional que tienen capacidades avanzadas de comunicación de datos, incluida la capacidad de comunicarse con otros sistemas informáticos. Dependiendo de la funcionalidad proporcionada por dichos dispositivos, los mismos pueden denominarse dispositivo de mensajería de datos, buscapersonas bidireccional, teléfono celular con capacidades de mensajería de datos, aparato de Internet inalámbrico o dispositivo de comunicación de datos (con o sin capacidades de telefonía). En algunas realizaciones, un dispositivo de mano puede tener capacidades tanto de transceptor de Wi-Fi (o similar) como de transceptor celular y puede comunicarse en modos respectivos con cualquiera de una pluralidad de puntos de acceso y sistemas transceptores de estación base dentro de su área de cobertura geográfica. Un dispositivo de este tipo normalmente proporcionará una o más aplicaciones de comunicación de datos, tales como una aplicación de mensajería y/o un navegador. Una aplicación preferida que puede ser proporcionada por dicho dispositivo de mano puede ser una aplicación de administrador de información personal (PIM) que tiene la capacidad de organizar y gestionar elementos de datos para el usuario tales como, entre otros, correo electrónico, eventos de calendario, correos de voz, citas y elementos de tareas. Naturalmente, uno o más módulos de almacenamiento están disponibles en el dispositivo de mano para facilitar el almacenamiento de aplicaciones y datos. Preferiblemente, el dispositivo de mano incluye un subsistema de comunicaciones de corto alcance que proporciona comunicación entre el dispositivo de mano y diferentes sistemas o dispositivos, que no tienen que ser necesariamente dispositivos similares, tales como el PA 104. Por ejemplo, dicho subsistema puede incluir un módulo de comunicación de Bluetooth para proporcionar comunicación con sistemas y dispositivos habilitados de manera similar. El dispositivo de mano también puede incluir una interfaz de I/O para comunicaciones por cable, tal como una o más interfaces de comunicación en serie.

Aunque se muestran comunicándose de forma inalámbrica a través de Bluetooth en todas las realizaciones, el HD 102 y el PA 104 pueden acoplarse de otras maneras que preferiblemente proporcionen un caudal suficiente para admitir la aplicación que ejecutará el PA. Por ejemplo, se pueden acoplar de forma inalámbrica de acuerdo con otros protocolos, tales como el USB inalámbrico o se pueden acoplar en modo por cable. Aunque se han descrito principalmente con referencia a dispositivos de mano, las personas con conocimientos habituales en la técnica apreciarán que son adecuados otros dispositivos móviles de comunicación inalámbrica con atributos similares.

La ejecución de aplicaciones en un entorno de ejecución contenido tal como en las realizaciones de la Fig. 12 y la Fig. 13 se describen por separado de la realización de contención de datos de la Fig. 18. Sin embargo, se entiende que estas realizaciones pueden combinarse (por ejemplo, 12 y 18 o 13 y 18) de modo que las aplicaciones puedan ejecutarse en un contenedor y los datos puedan estar contenidos en el BFD. WebDAV se puede proporcionar por encima del VFS según se ha descrito.

5 Ventajosamente, el PA y el HD pueden acoplarse para virtualizar la capa de presentación del HD. Se proporciona acceso virtualizado a aplicaciones del HD y se proporciona acceso mediante navegador a la empresa e Internet. El uso de comunicaciones cifradas mantiene el mismo nivel de seguridad desde el HD hasta el Aparato de Presentación que desde la empresa hasta el HD. En muchos dispositivos de mano, incluidos dispositivos avanzados, las limitaciones inherentes a la memoria, los hilos, las conexiones de red y otros recursos hacen que sea muy difícil admitir un entorno de navegador completamente funcional. Para resolver otros problemas inherentes a las redes inalámbricas y a la renderización de páginas web basadas en HTML en dispositivos de mano muy pequeños, a menudo se utiliza un *proxy* de HTTP, del lado de la red, que transcodifica el HTML como parte de la infraestructura de red del dispositivo inalámbrico y reduce los requisitos de comunicación de datos, pero a expensas de una experiencia de HTTP 1.1 totalmente compatible. De acuerdo con la invención, los componentes del *proxy* dividido están habilitados para proporcionar y admitir protocolos estándar abiertos de Internet tales como SSL, TLS, HTTP/S y HTTP 1.1 completo.

10 Aunque en el presente documento se han descrito realizaciones específicas de la invención, los expertos en la técnica entenderán que, en las mismas, se pueden aplicar variaciones sin desviarse del alcance de la invención que se define en las reivindicaciones adjuntas.

15

REIVINDICACIONES

1. Un sistema (100) de comunicación de datos que comprende:

un dispositivo (102) de comunicación inalámbrica configurado para comunicar datos de forma segura a través de una red inalámbrica pública (106, 110) a una red (112) de área local privada;

5 un aparato (104) de presentación para virtualizar una capa de presentación del dispositivo (102) de comunicación inalámbrica para un usuario;

10 en el que el aparato (104) y el dispositivo (102) de comunicación inalámbrica están acoplados comunicativamente para la comunicación de datos a través de un *proxy* dividido de modo que el aparato (104) también está configurado para comunicar datos de forma segura dentro de la red inalámbrica pública (106, 110) a través del dispositivo (102) de comunicación inalámbrica, estando configurado el aparato (104) para ejecutar una interfaz de usuario con el fin de virtualizar la capa de presentación y permitir al usuario trabajar selectivamente con las comunicaciones de datos utilizando la comunicación de datos segura con la red (112) de área local privada desde el dispositivo (102) de comunicación inalámbrica; y una llave electrónica extraíble (103A) que comprende medios de almacenamiento y medios de radiocomunicaciones de corto alcance, estando configurada la llave electrónica (103A) para almacenar instrucciones y datos, estando configurado el aparato (104) para ejecutar las instrucciones y datos con el fin de facilitar las comunicaciones del *proxy* dividido con el dispositivo (102) de comunicación inalámbrica y estando configurada la llave electrónica (103A) para proporcionar además capacidades de comunicación de corto alcance para acoplar comunicativamente el aparato (104) y el dispositivo (102) de comunicación inalámbrica, en donde las instrucciones y datos configuran el aparato (104) para dejar de virtualizar la capa de presentación al producirse al menos una de:

20 (a) una retirada de la llave electrónica (103A); y

(b) una interrupción de las comunicaciones de corto alcance.

2. El sistema de la reivindicación 1, en el que el aparato (104) de presentación comprende un ordenador portátil y el dispositivo (102) de comunicación inalámbrica está configurado para comunicaciones de datos seguras con la red (112) de área local privada, de manera que el funcionamiento de la interfaz de usuario para virtualizar la capa de presentación acopla el ordenador portátil a la red (112) de área local privada para comunicaciones de datos seguras.

3. El sistema de la reivindicación 1 o 2, en el que el aparato (104) y el dispositivo (102) de comunicación inalámbrica están además acoplados comunicativamente para facilitar el intercambio de una dirección de *proxy* de red de comunicaciones con la que enrutar solicitudes de recursos de la red privada (112).

30 4. El sistema de cualquier reivindicación anterior, en el que el dispositivo (102) de comunicación inalámbrica está configurado para comunicar datos que comprenden mensajes electrónicos e incluye una interfaz de usuario de dispositivo de comunicación inalámbrica que tiene una capa de presentación configurada para visualizar y controlar los mensajes electrónicos; y en el que el aparato (104) comprende una interfaz (300) de usuario de aparato configurada para virtualizar la capa de presentación del dispositivo de comunicación inalámbrica configurada para visualizar y controlar los mensajes a través del aparato (104).

35 5. El sistema de cualquier reivindicación anterior, en el que el dispositivo (102) de comunicación inalámbrica y el aparato (104) están configurados para cifrar y descifrar comunicaciones respectivas de datos de *proxy* dividido intercambiadas entre ellos de acuerdo con una clave, estando configurado cada uno del dispositivo (102) de comunicación inalámbrica y el aparato (104) para obtener de forma segura la clave de un servidor (642) de claves acoplado a la red pública inalámbrica (106, 110) a través del dispositivo (102) de comunicación inalámbrica.

40 6. El sistema de la reivindicación 5, en el que el dispositivo (102) de comunicación inalámbrica está configurado para obtener la clave y un *token* de autenticación del servidor (642) de claves y presentar el *token* de autenticación al usuario para que el usuario lo use para solicitar la clave para el aparato (104), en el que el aparato (104) está configurado para recibir el *token* de autenticación del usuario y solicitar la clave del servidor (642) de claves mediante comunicaciones a través del dispositivo (102) de comunicación inalámbrica.

45 7. Un método para comunicar datos que comprende:

50 acoplar un dispositivo (102) de comunicación inalámbrica con un aparato (104) de presentación para virtualizar una capa de presentación del dispositivo (102) de comunicación inalámbrica para un usuario, en donde el dispositivo (102) de comunicación inalámbrica está configurado para comunicar datos de forma segura a través de una red inalámbrica pública (106, 110) a una red (112) de área local privada, definir mediante el aparato (104) y el dispositivo (102) de comunicación inalámbrica un servidor *proxy* dividido (212, 228) de un *proxy* dividido de manera que el aparato (104) también está configurado para comunicar datos de forma segura sobre la red inalámbrica pública (106, 110) a través del dispositivo (102) de comunicación inalámbrica, en donde el aparato (104) y el dispositivo (102) de comunicación inalámbrica están acoplados comunicativamente para la comunicación de datos mediante el *proxy* dividido; y ejecutar una interfaz (300) de usuario en el aparato (104) para virtualizar la capa de presentación y permitir al usuario trabajar selectivamente con las comunicaciones de datos utilizando la comunicación de datos segura con la red (112) de área

- 5 local privada desde el dispositivo (102) de comunicación inalámbrica, en el que el acoplamiento comprende usar, por parte del aparato, una llave electrónica extraíble (103A) que comprende medios de almacenamiento y medios de radiocomunicaciones de corto alcance, almacenando la llave electrónica (103A) instrucciones y datos para su ejecución por parte del aparato (104) con el fin de facilitar las comunicaciones de *proxy* dividido con el dispositivo (102) de comunicación inalámbrica y proporcionando además la llave electrónica (103A) capacidades de comunicación de corto alcance para acoplar comunicativamente el aparato (104) al dispositivo (102) de comunicación inalámbrica, y en el que las instrucciones y los datos configuran el aparato (104) para dejar de virtualizar la capa de presentación al producirse al menos una de una retirada de la llave electrónica (103A) y una interrupción de las comunicaciones de corto alcance.
- 10 8. El método de la reivindicación 7, en el que el dispositivo (102) de comunicación inalámbrica comunica datos que comprenden mensajes electrónicos e incluye una interfaz de usuario de dispositivo de comunicación inalámbrica que tiene una capa de presentación para visualizar y controlar los mensajes electrónicos; y en el que el aparato (104) comprende una interfaz (300) de usuario de aparato configurada para virtualizar la capa de presentación del dispositivo de comunicación inalámbrica con el fin de visualizar y controlar los mensajes mediante el aparato (104) y en el que el método comprende ejecutar la interfaz (300) de usuario de aparato para comunicar mensajes electrónicos desde el aparato (104).
- 15 9. El método de la reivindicación 8, en el que el dispositivo (102) de comunicación inalámbrica proporciona un entorno (212) de trabajo de *servlet* para procesar solicitudes y datos comunicados con el aparato (104).
- 20 10. El método de la reivindicación 8, en el que al menos algunos de los mensajes electrónicos están asociados a archivos adjuntos respectivos, definiéndose cada archivo adjunto de acuerdo con un formato de aplicación asociado respectivo; y en el que el método comprende hacer funcionar la interfaz (300) de usuario de aparato para solicitar a un servidor de archivos adjuntos que proporcione un archivo adjunto particular de acuerdo con su formato de aplicación asociado respectivo al aparato (104) mediante el servidor *proxy* dividido (212, 228).
- 25 11. El método de cualquiera de las reivindicaciones 7 a 10, en el que el dispositivo (102) de comunicación inalámbrica y el aparato (104) se configuran para cifrar y descifrar comunicaciones de datos de *proxy* dividido respectivas intercambiadas entre ellos de acuerdo con una clave y en el que el método comprende además obtener de forma segura la clave por parte de cada uno del dispositivo (102) de comunicación inalámbrica y el aparato (104) a partir de un servidor de claves acoplado a la red pública inalámbrica (106, 110) mediante el dispositivo (102) de comunicación inalámbrica.
- 30 12. Uno o más medios legibles por ordenador que comprenden instrucciones ejecutables por ordenador para adaptar un dispositivo inalámbrico (102) y un aparato (104) de presentación para comunicaciones de datos, en donde el dispositivo inalámbrico está configurado para comunicar datos de forma segura sobre una red inalámbrica pública (106, 110) a una red (112) de área local privada, comprendiendo las instrucciones primeros medios de código para adaptar el dispositivo (102) de comunicación inalámbrica y segundos medios de código para adaptar el aparato (104), de manera que cuando se ejecutan los primeros y segundos medios de código mediante procesadores respectivos del dispositivo (102) de comunicación inalámbrica y el aparato (104), el dispositivo (102) de comunicación inalámbrica y el aparato (104) se acoplan comunicativamente para la comunicación de datos mediante un *proxy* dividido de modo que el aparato (104) también está configurado para comunicar datos de forma segura dentro de la red inalámbrica pública (106, 110) a través del dispositivo (102) de comunicación inalámbrica, y en donde los segundos medios de código proporcionan al aparato (104) una interfaz de usuario para virtualizar una capa de presentación del dispositivo (102) de comunicación inalámbrica y permitir a un usuario trabajar selectivamente con las comunicaciones de datos utilizando la comunicación de datos segura con la red (112) de área local privada desde el dispositivo (102) de comunicación inalámbrica, en donde el dispositivo (102) de comunicación inalámbrica y el aparato (104) se acoplan comunicativamente para la comunicación de datos mediante una llave electrónica extraíble (103A) configurada para proporcionar capacidades de comunicación de corto alcance y para almacenar instrucciones y datos para su ejecución por el aparato (104) con el fin de facilitar las comunicaciones de *proxy* dividido con el dispositivo (102) de comunicación inalámbrica, en el que las instrucciones y los datos configuran el aparato (104) para dejar de virtualizar la capa de presentación al producirse al menos una de una retirada de la llave electrónica (103A) y una interrupción de las comunicaciones de corto alcance.

50

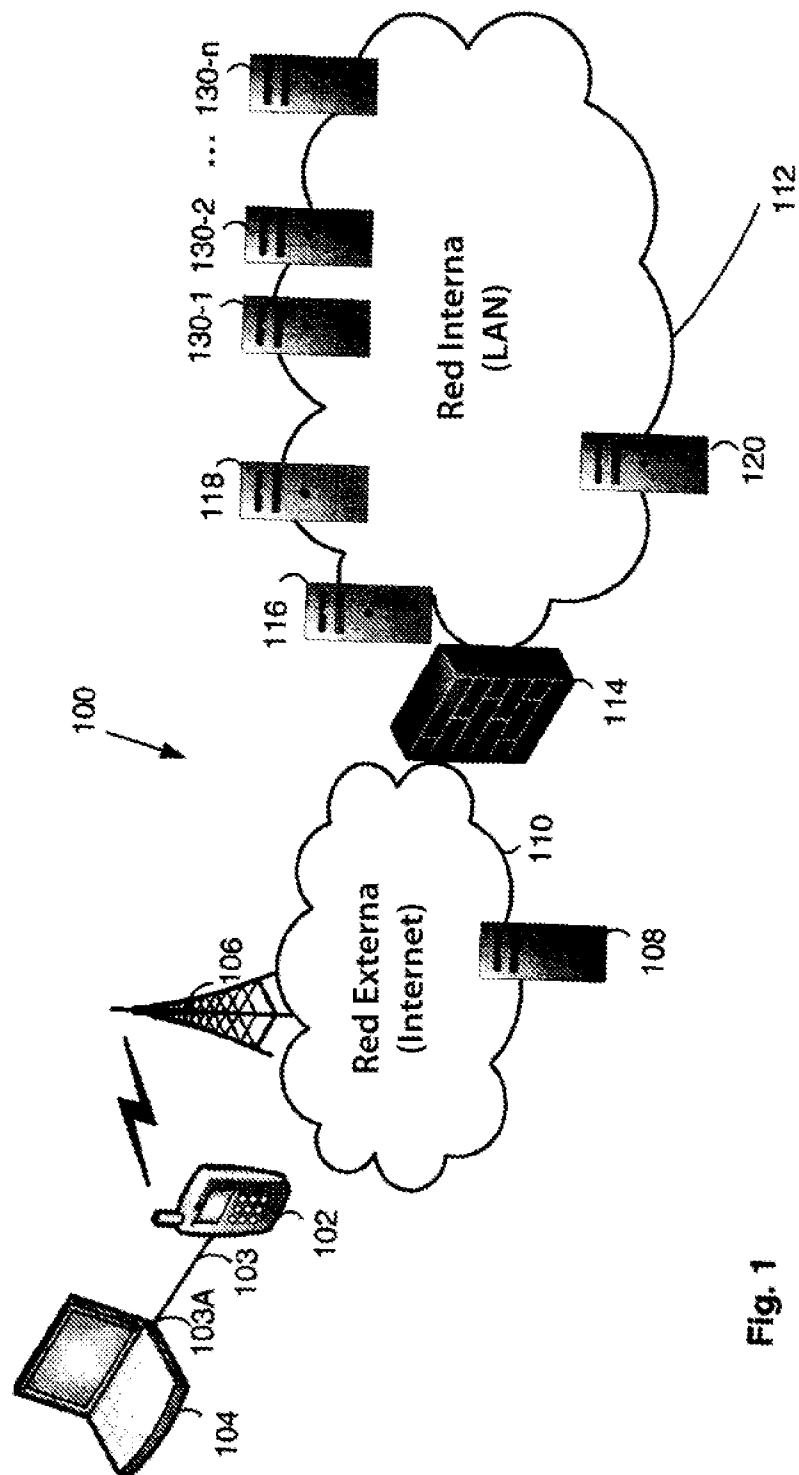


Fig. 1

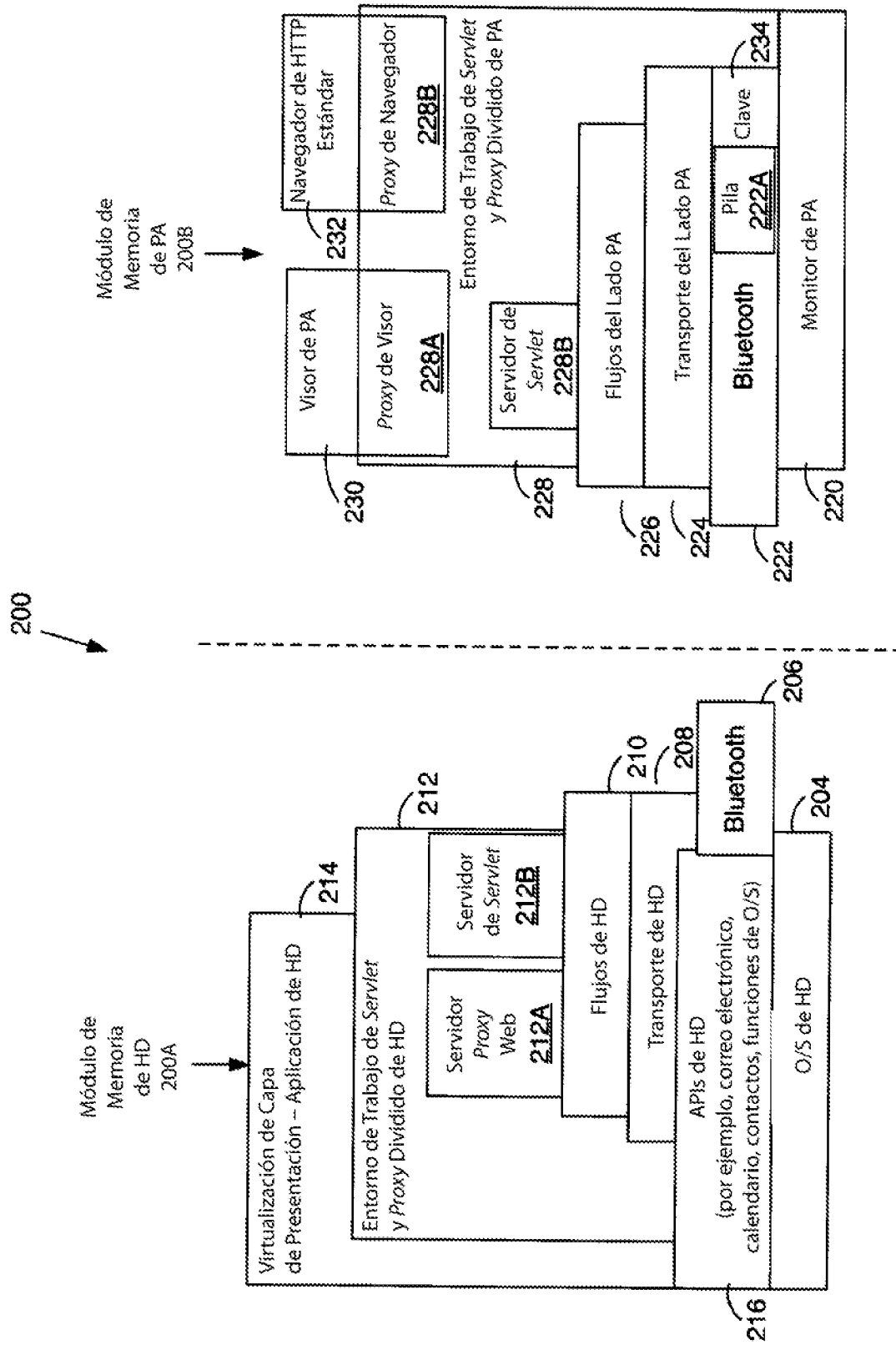


Fig. 2

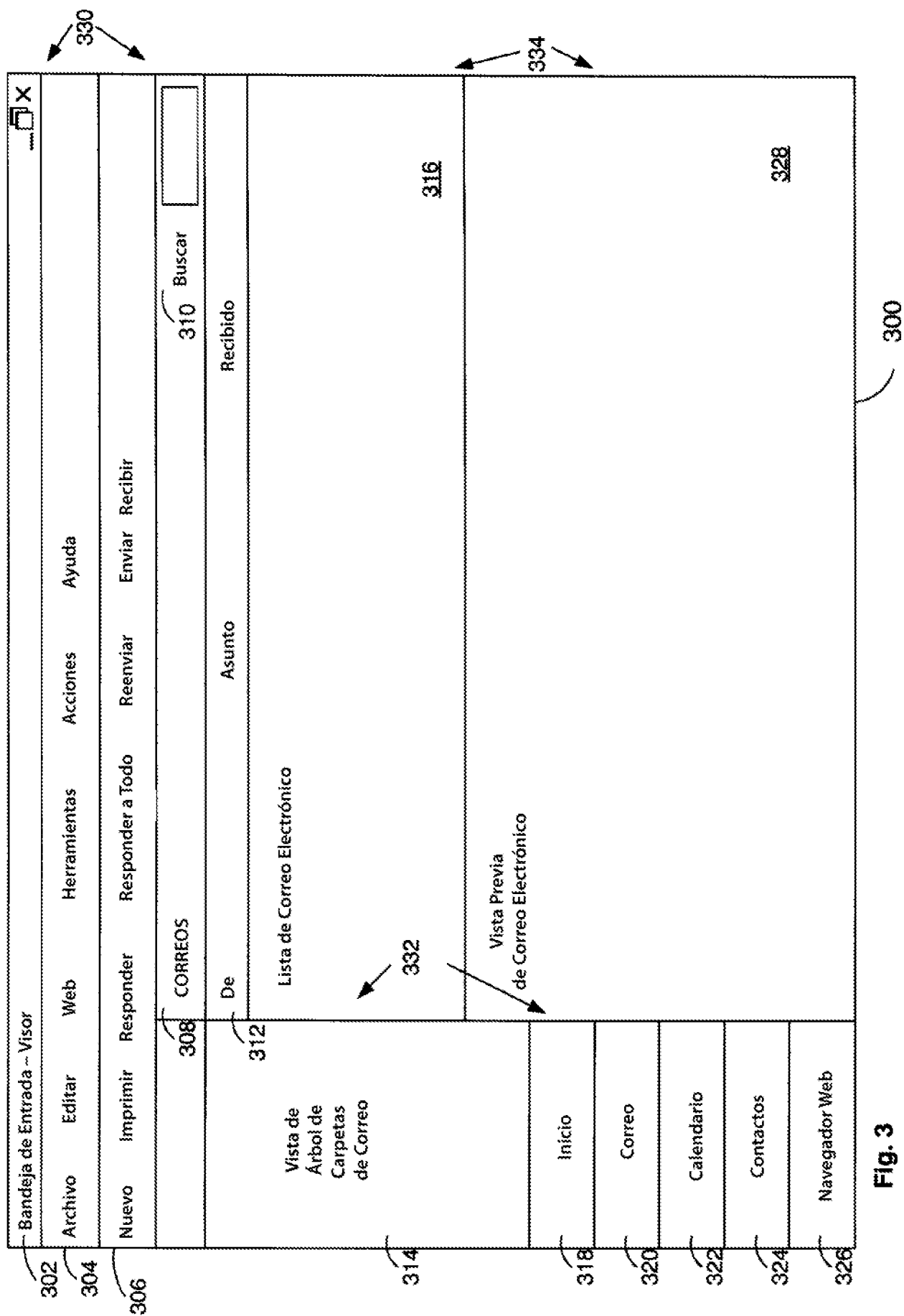


Fig. 3

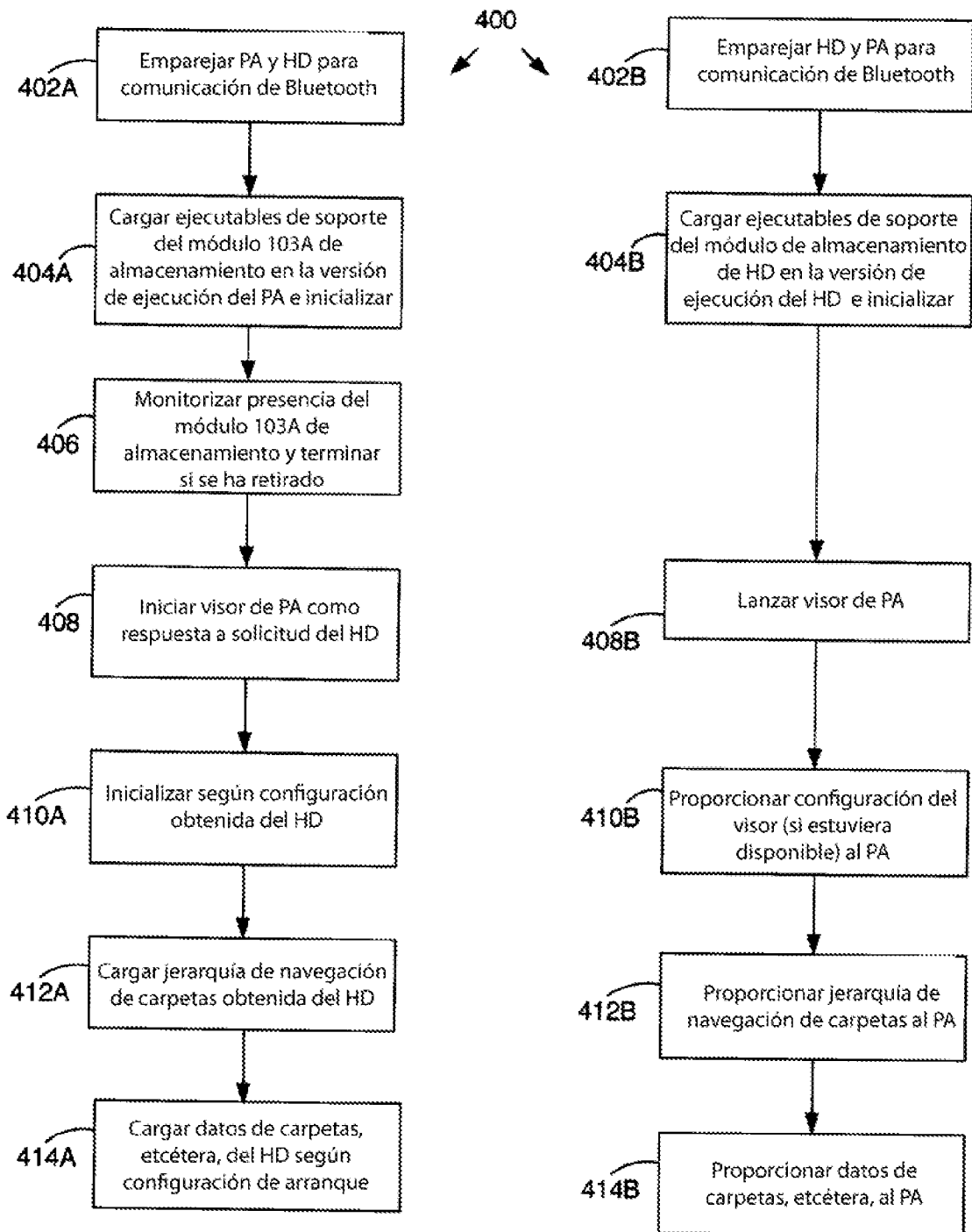


Fig. 4

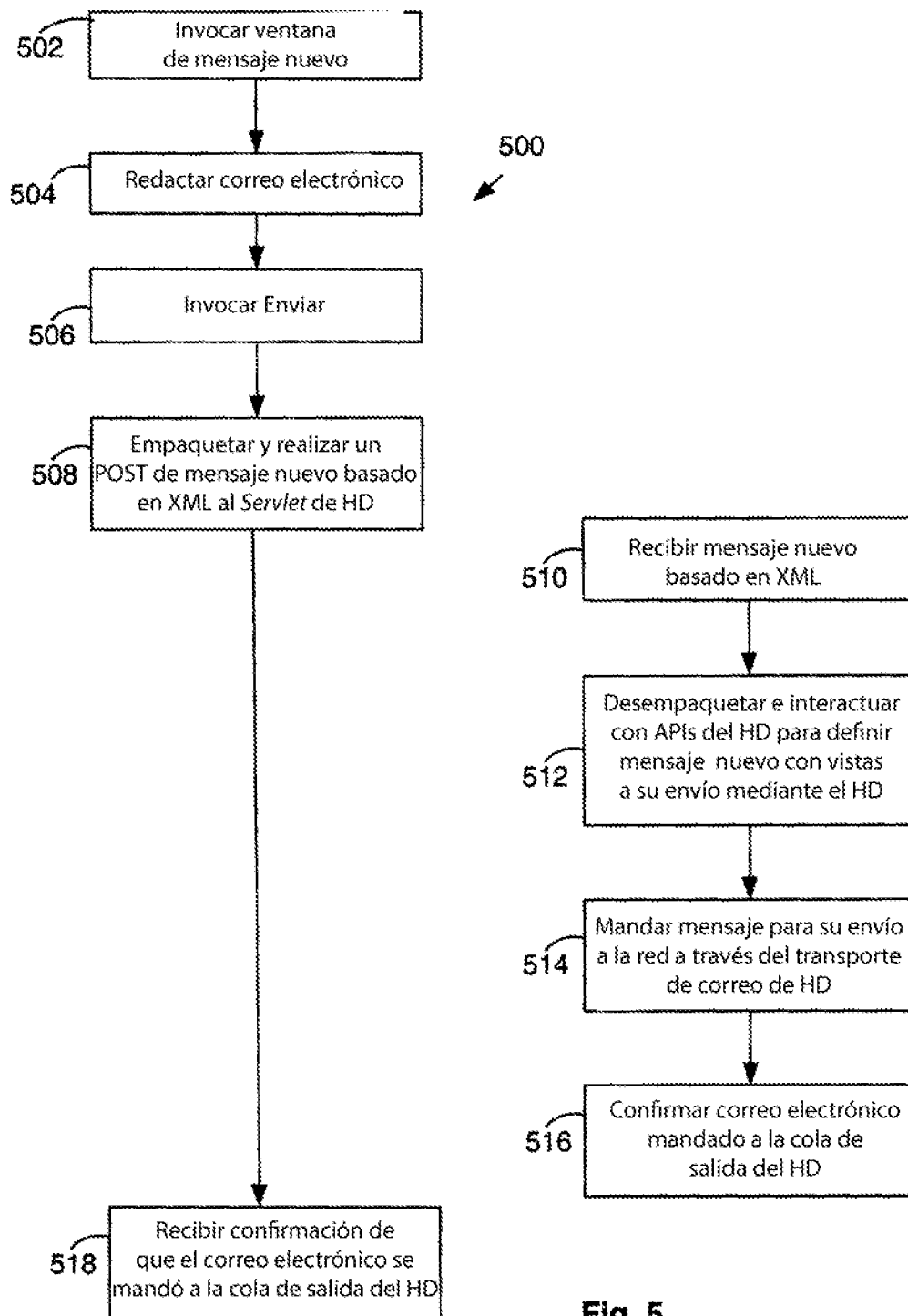


Fig. 5

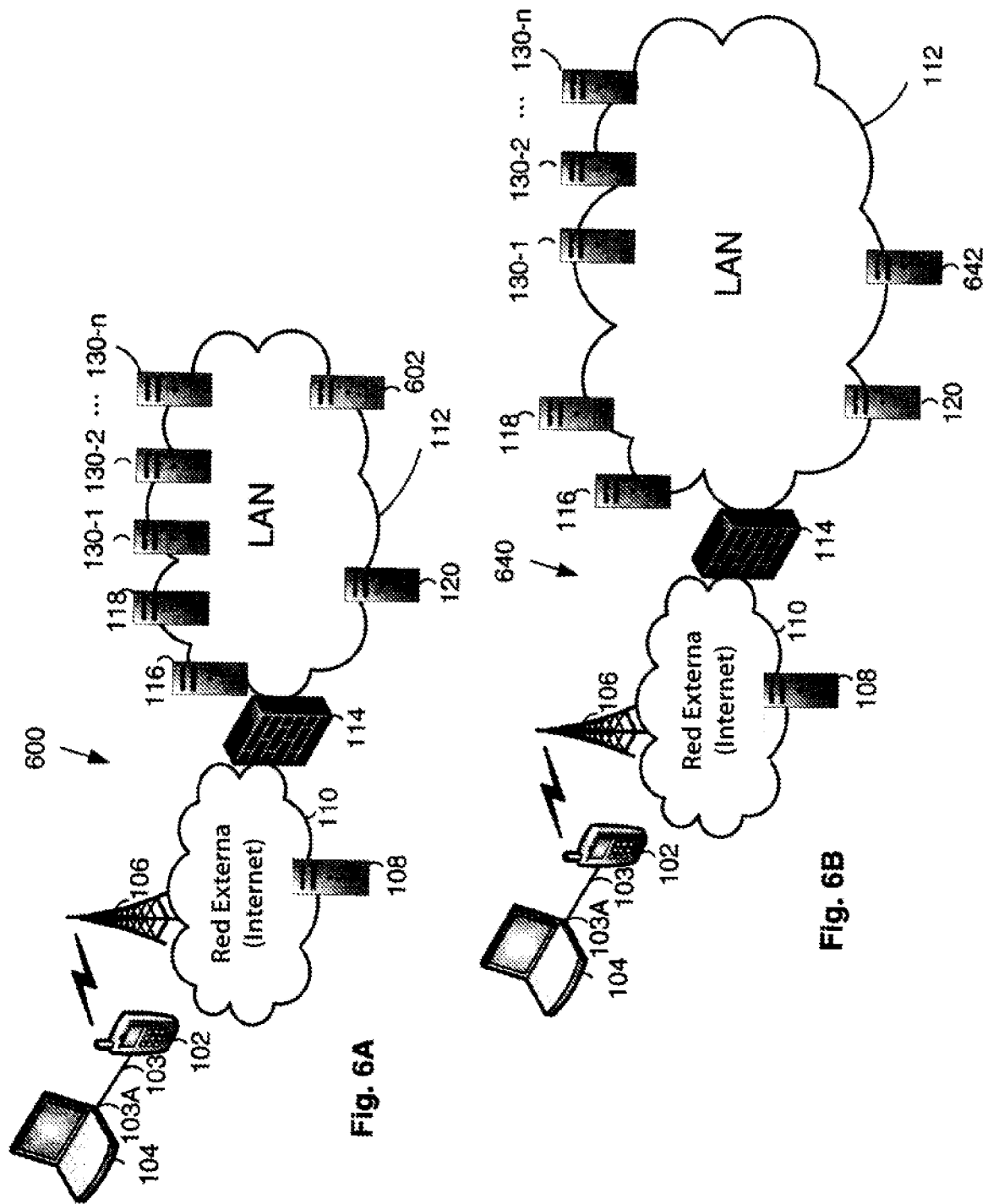


Fig. 6A

Fig. 6B

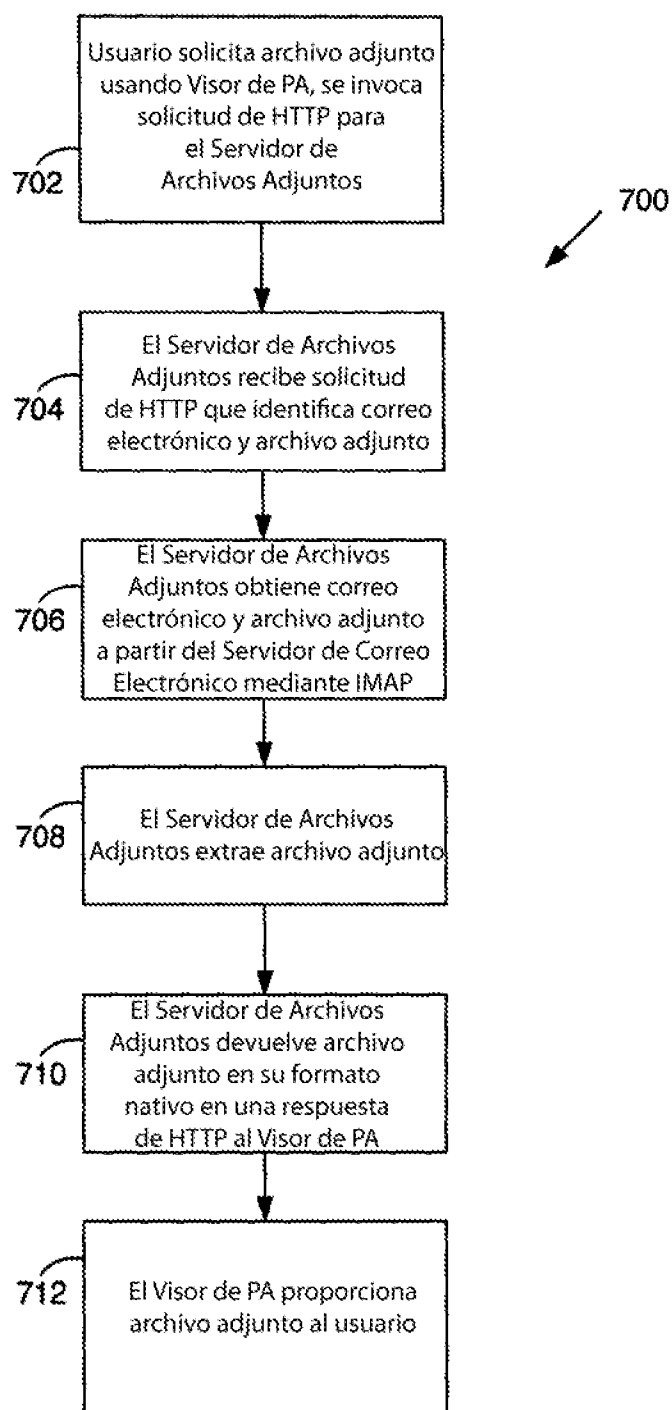
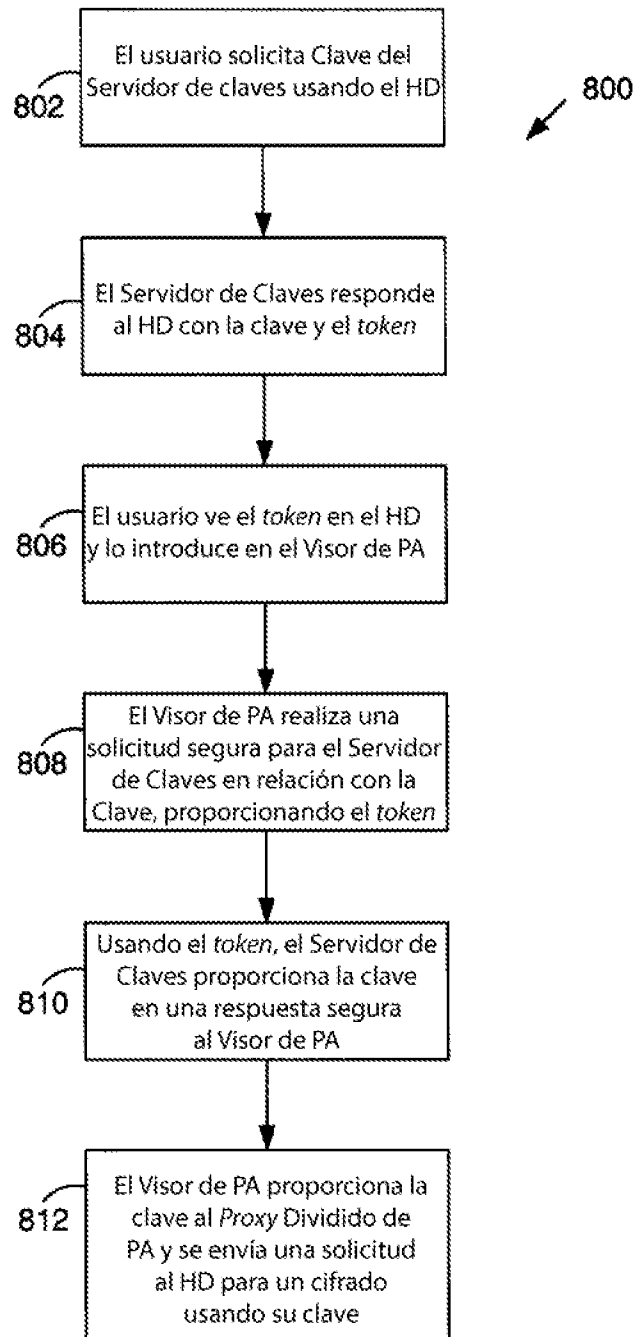


Fig. 7

**Fig. 8**

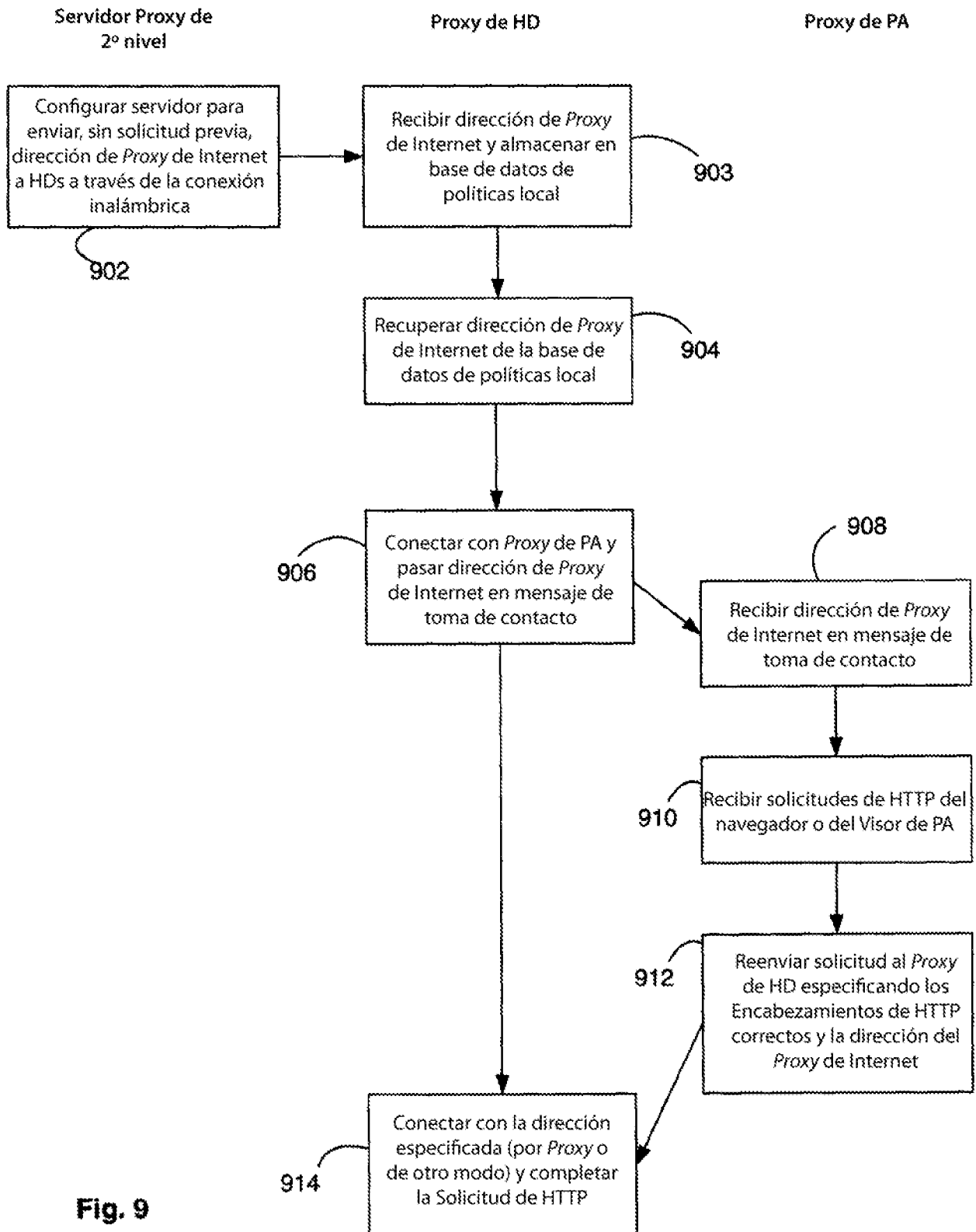


Fig. 9

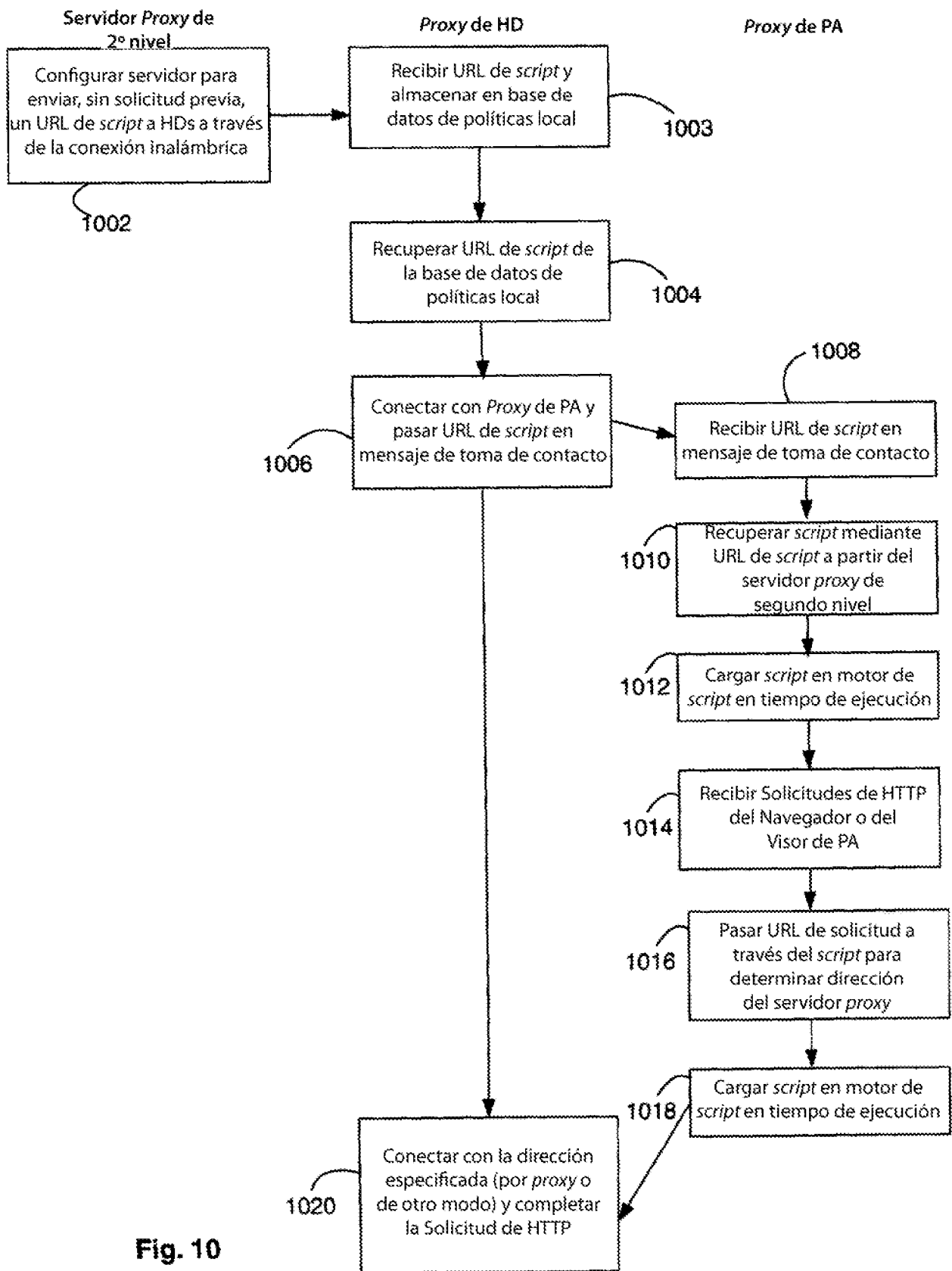


Fig. 10

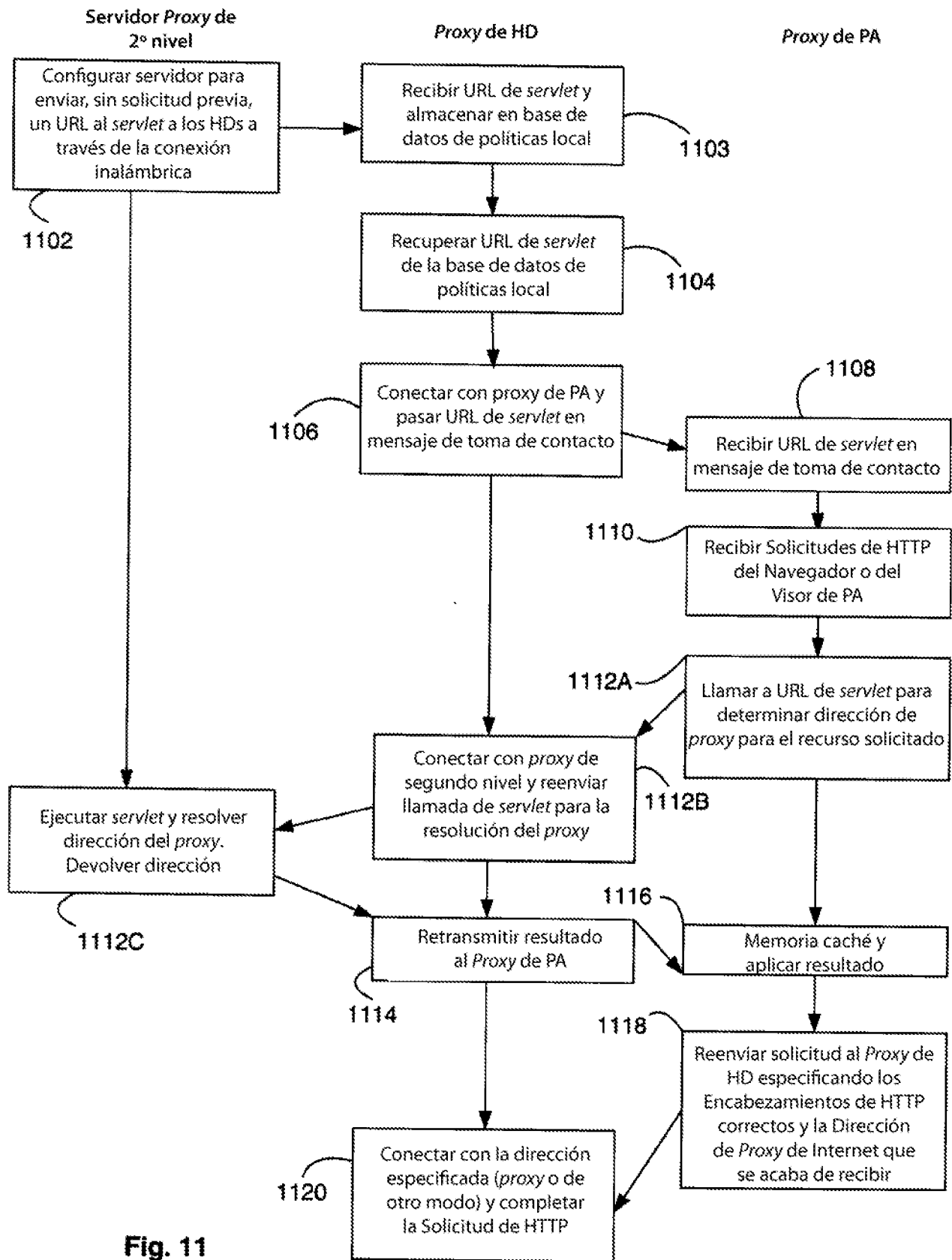


Fig. 11

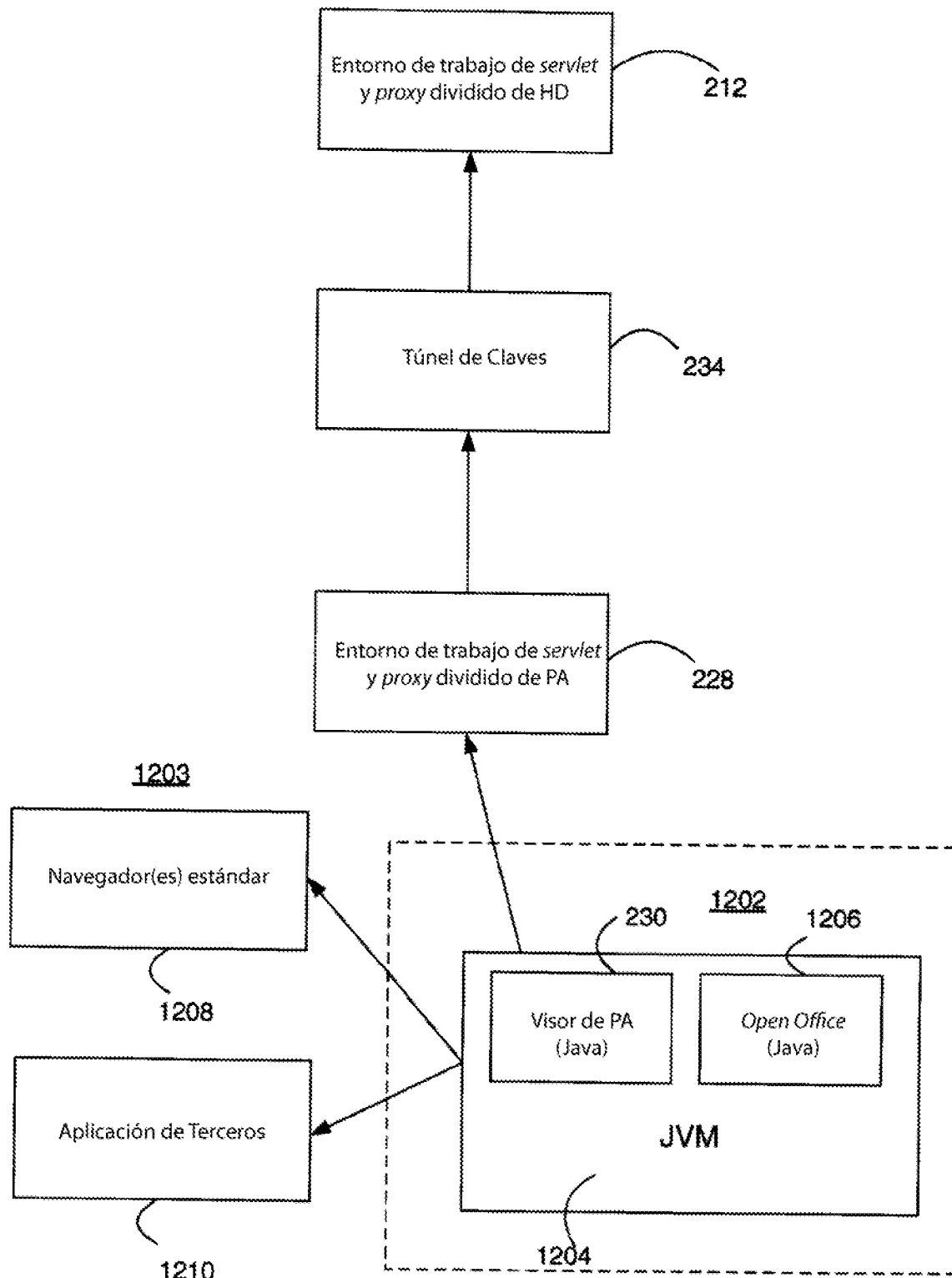


Fig. 12

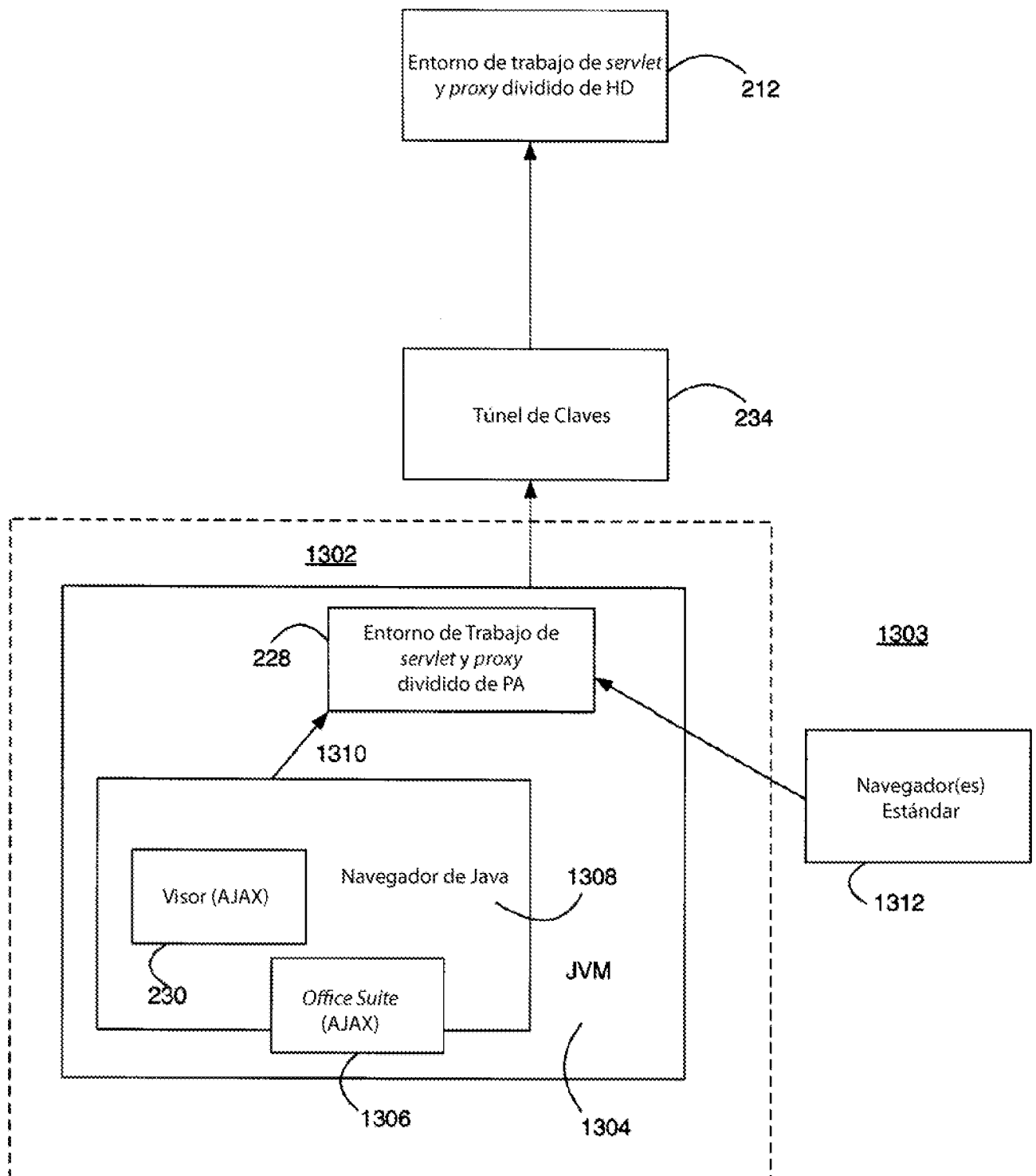


Fig. 13

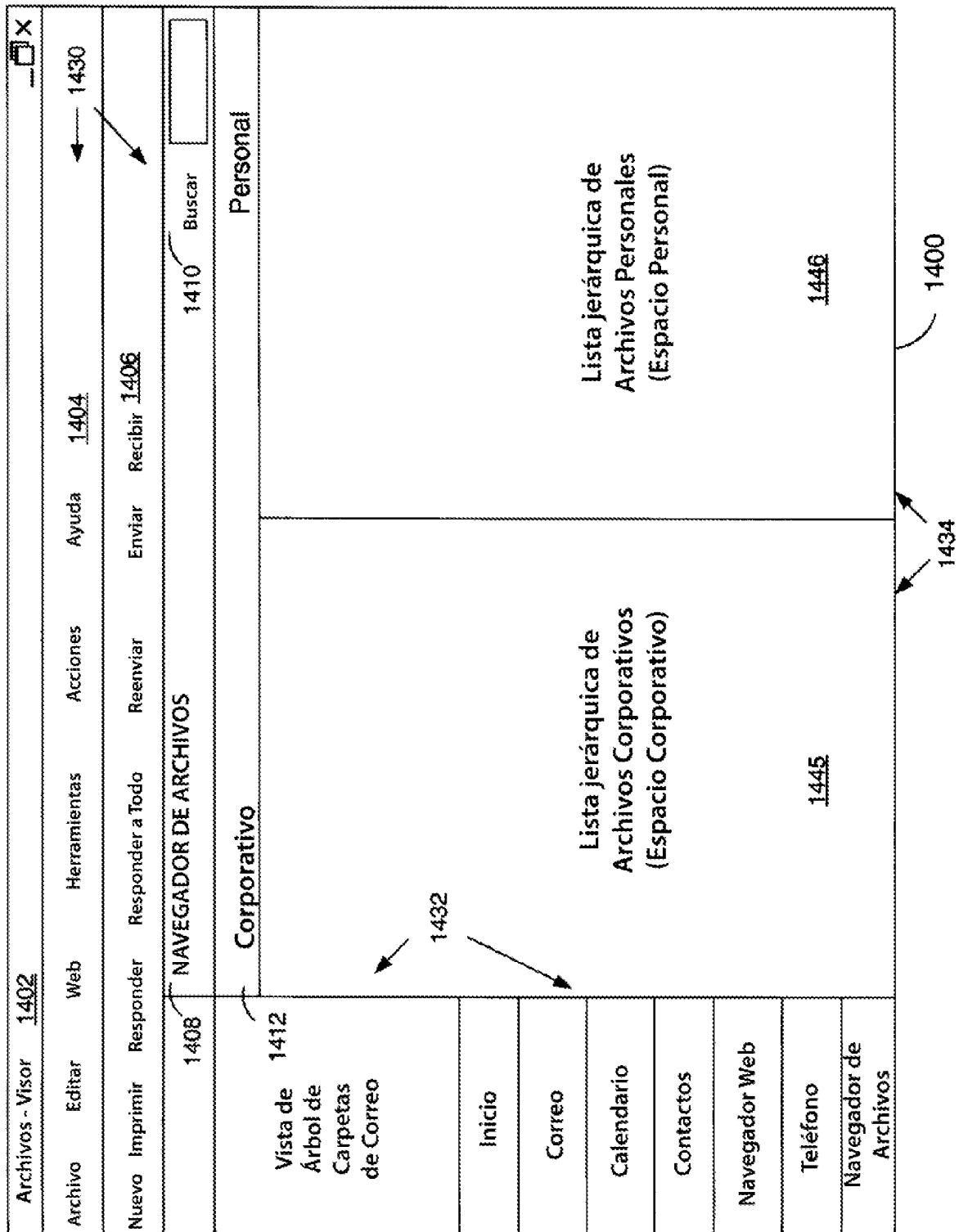


Fig. 14

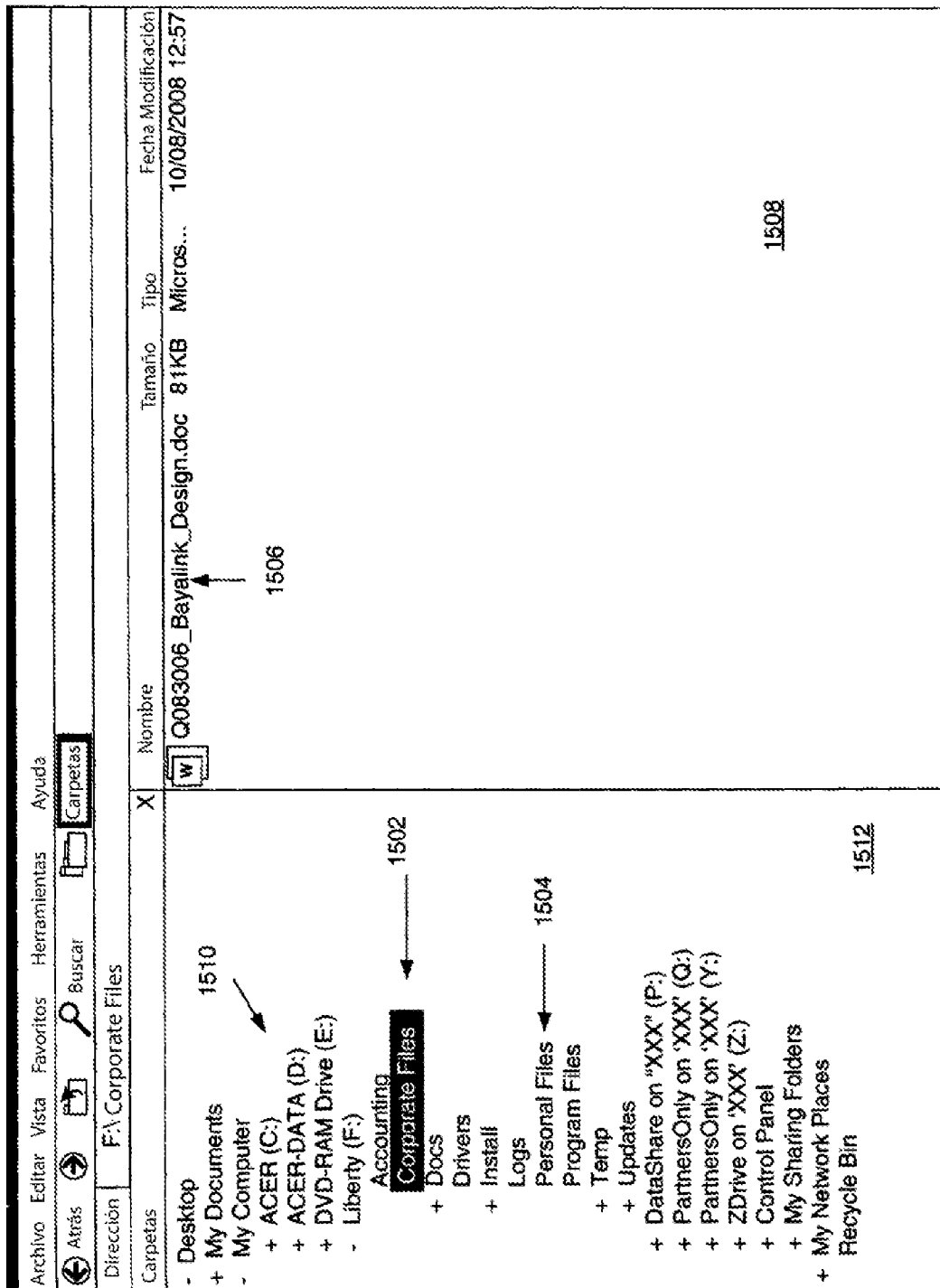


Fig. 15

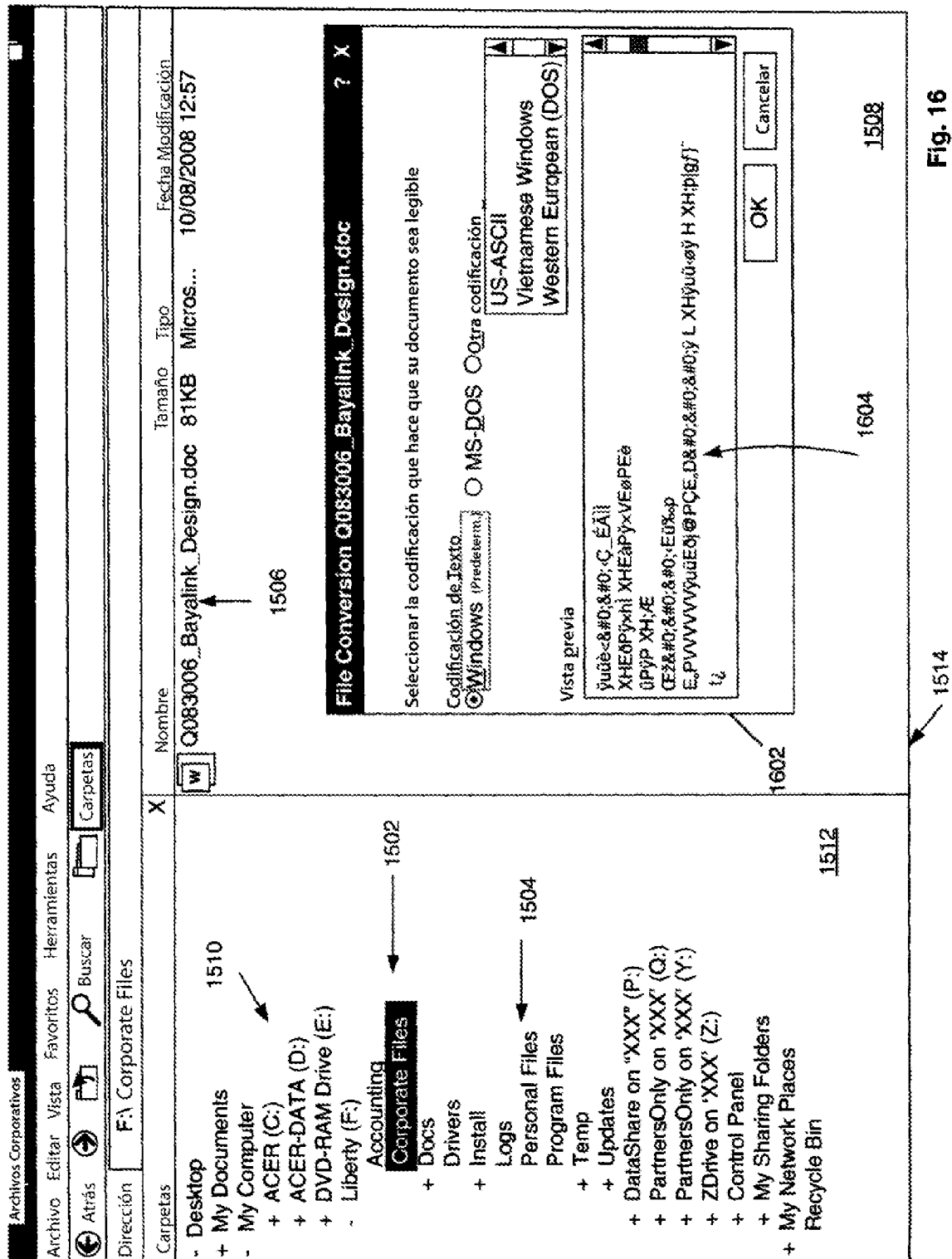


Fig. 16

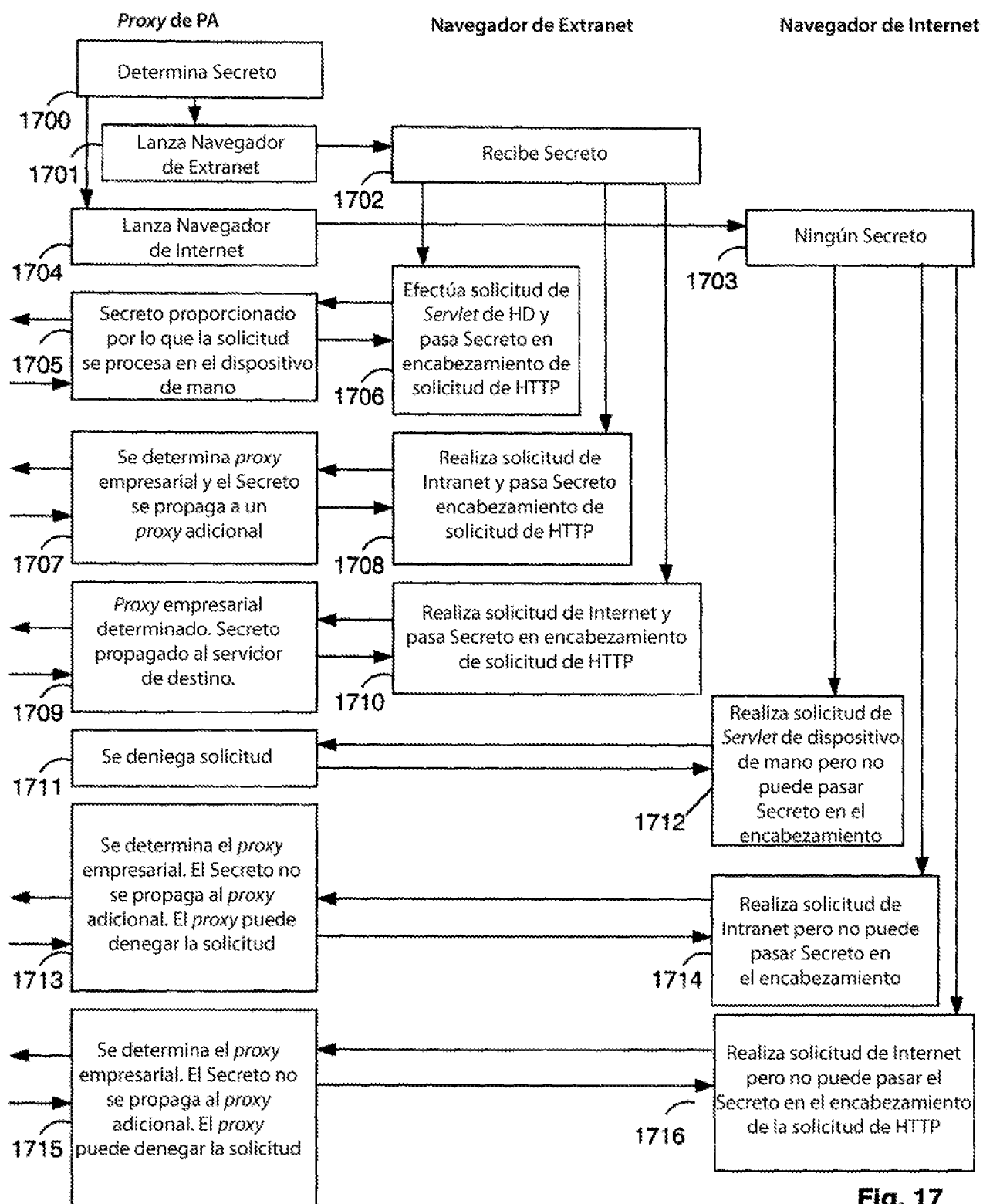


Fig. 17

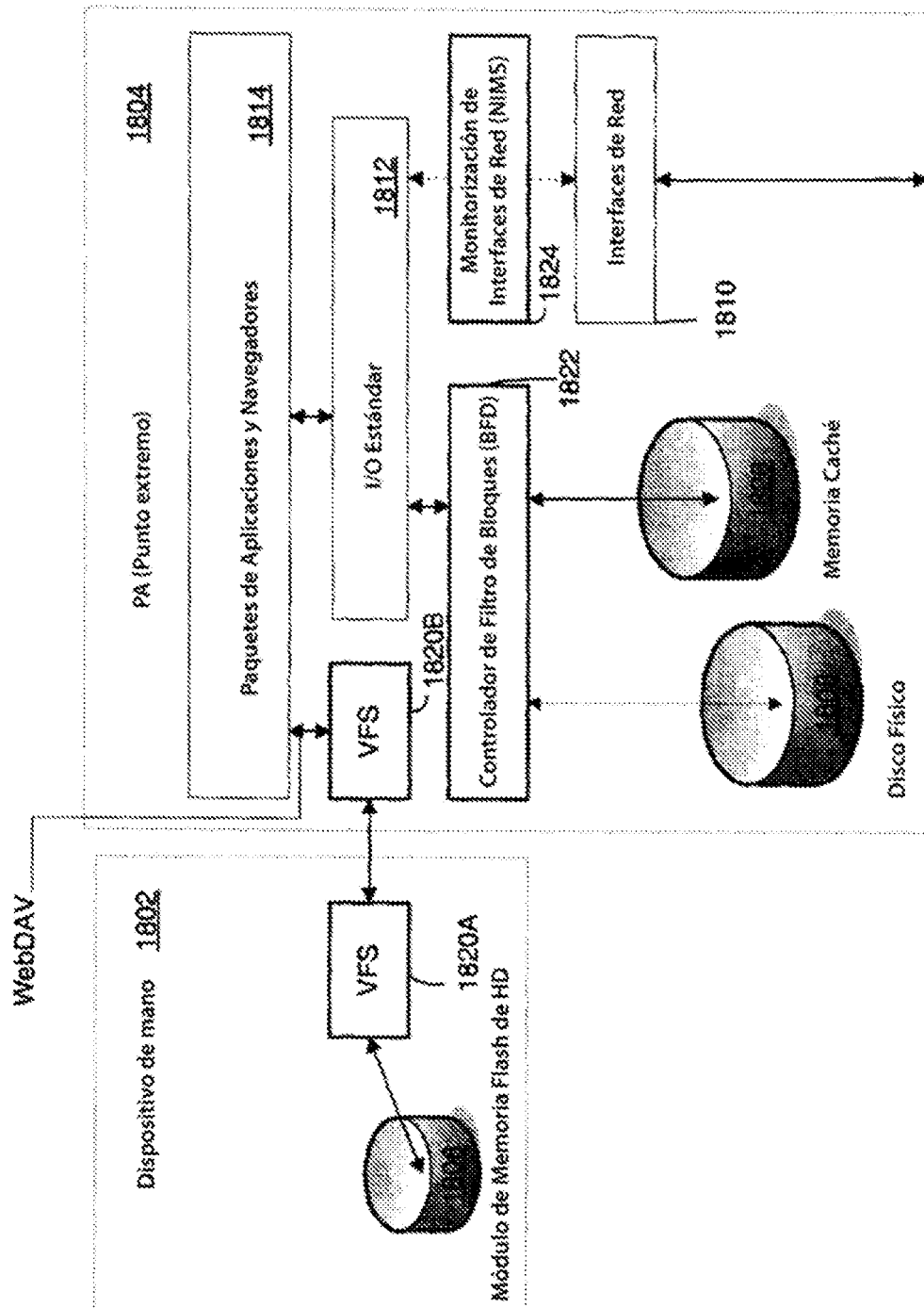


Fig. 18

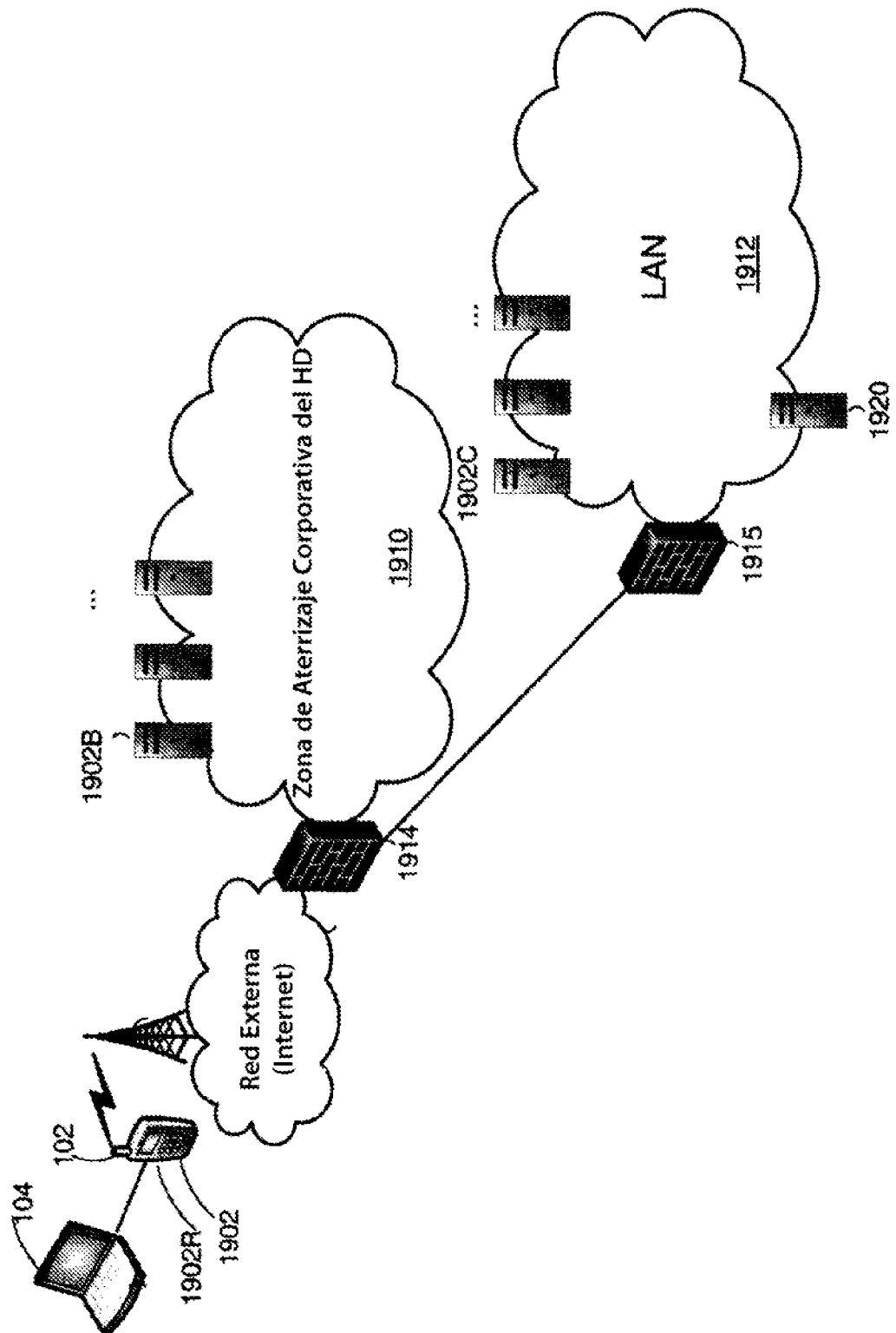


Fig. 19

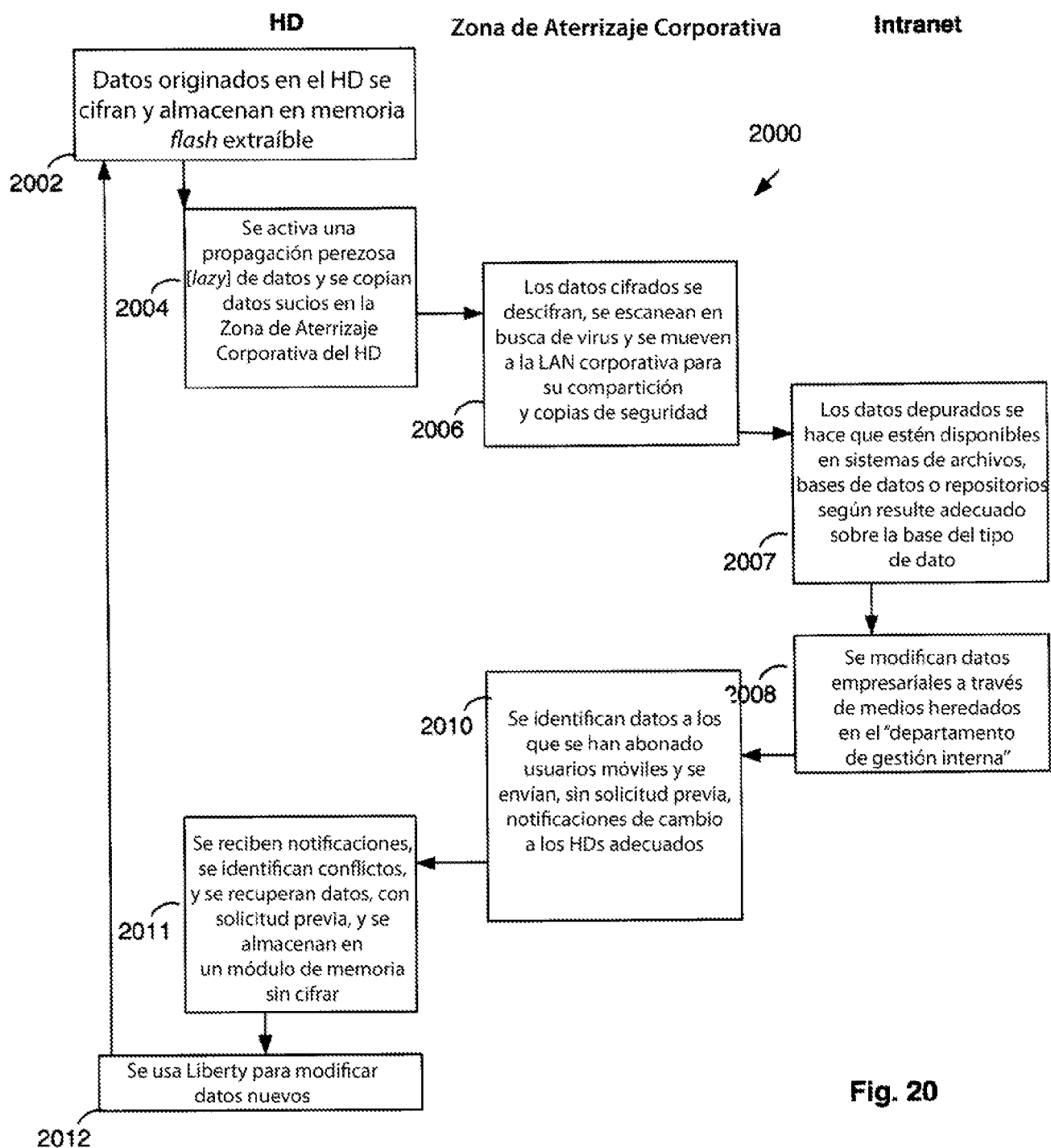


Fig. 20