(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 794 407**

(51) Int. CI.:

G06F 21/60 (2013.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **27.12.2016 E 16207027 (0)**

(97) Fecha y número de publicación de la concesión europea: **04.03.2020 EP 3188069**

(54) Título: **Sistema de permisos basado en red**

(30) Prioridad:

28.12.2015 US 201562272003 P
07.07.2016 US 201615204866

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
18.11.2020

(73) Titular/es:

PALANTIR TECHNOLOGIES, INC. (100.0%)
100 Hamilton Avenue, Suite 300
Palo Alto, California 94301, US

(72) Inventor/es:

ELLIOT, MARK;
ZHAO, JASON;
SCHIMPF, BRIAN;
MEACHAM, JACOB;
GELMI, MARCO;
DUFFIELD, BENJAMIN;
SGUERA, SAVINO;
BAKER, JAMES;
RICKARDS, NEIL;
CAMPANINI, JAVIER;
CHEN, QINFENG;
CICERONE, DEREK y
ZIEBART, NATHAN

(74) Agente/Representante:

TORNER LASALLE, Elisabet

DESCRIPCIÓN

Sistema de permisos basado en red

Referencia cruzada con solicitudes relacionadas

La presente solicitud reivindica la prioridad de la solicitud de patente provisional U.S. con nº de serie 62/272.003, presentada el 28 de diciembre de 2015 y la prioridad de la solicitud de patente U.S. con nº de serie 15/204.866, presentada el 7 de julio de 2016.

Campo técnico

El contenido dado a conocer en la presente memoria versa acerca de permisos de acceso a recursos de datos. En particular, realizaciones ejemplares versan acerca de sistemas y procedimientos para registrar y evaluar directrices asociadas con recursos de datos en un entorno de red de ordenadores.

Antecedentes

Los sistemas de ordenador normales incluyen un sistema de ficheros para controlar cómo se almacenan y recuperan los datos. Los sistemas convencionales de ficheros mantienen la información con relación al permiso de acceso de usuario junto con cada recurso almacenado para controlar la capacidad de los usuarios a acceder a los recursos. Por ejemplo, se puede permitir que un usuario visualice y cambie un recurso particular mientras que puede permitirse a otro usuario únicamente visualizar el recurso. En algunos casos, múltiples programas de aplicación pueden compartir un acceso común a recursos incluidos en un único sistema de ficheros. Por ejemplo, un paquete de aplicaciones de red puede proporcionar una interfaz común que proporciona a un usuario diversas funcionalidades relacionadas que permiten al usuario interactuar con un repositorio común de objetos de datos compartidos por el paquete de aplicaciones. En estos casos, cada programa de aplicación es normalmente responsable de evaluar si un usuario tiene permiso para acceder a un recurso incluido en el sistema de ficheros en función de la información de permiso de acceso de usuario mantenida junto con el recurso. No solo da lugar esta implementación convencional a redundancias meticulosas en el desarrollo de tal aplicación, sino que también presenta el potencial de una gestión incoherente de los permisos de acceso de usuario en cada una de las aplicaciones.

Una desventaja adicional de los sistemas convencionales de ficheros es la gestión de los recursos con dependencias de otros recursos. Debido a que se mantiene la información de permisos de cada recurso junto con el propio recurso, para determinar si un usuario puede acceder a un recurso con dependencias, el evaluador debe recorrer todo el árbol de dependencias del recurso para alcanzar la determinación correcta. Como resultado de este flujo de trabajo de muchas lecturas, se utilizan los recursos de cómputo de forma ineficaz debido al número de frases de órdenes que deben ser ejecutados para determinar el permiso de acceso real del usuario, lo que, a su vez, da lugar a una degradación del rendimiento del sistema.

El documento US 2004/0010607 A1 da a conocer un sistema en el que un servidor Web toma decisiones informadas en función de normas por defecto y/o específicas de si devolver recursos solicitados a un usuario final. Un módulo de soporte lógico incluido en el servidor Web consulta a un servidor de acceso acerca de si el usuario está autorizado para acceder a un recurso solicitado. A su vez, el servidor de acceso consulta a un directorio los criterios apropiados de autorización para el recurso solicitado. El servidor de acceso recupera los criterios de autorización del recurso y responde a la consulta del módulo de soporte lógico del servidor Web. Las normas especifican las condiciones en las que se permite o deniega el acceso a los recursos solicitados, y a qué usuarios finales se aplican estas condiciones.

El documento US 2001/0007133 A1 da a conocer una técnica para mantener la seguridad en un entorno informático distribuido. Un gestor de directrices ubicado en un servidor mantiene y distribuye unas directrices de seguridad, y un controlador de aplicaciones ubicado en un cliente gestiona el acceso a componentes asegurables, según especifican las directrices de seguridad. Los objetos pueden organizarse en una jerarquía de objetos. Si se concede a un usuario un cierto privilegio en un objeto precursor, entonces se le concede automáticamente el privilegio sobre todos los objetos derivados. En otras palabras, se heredan los privilegios de objetos precursores a derivados.

Sumario

La presente invención se define mediante las reivindicaciones independientes, teniendo en cuenta, debidamente, cualquier elemento que sea equivalente a un elemento especificado en las reivindicaciones. Las reivindicaciones dependientes versan acerca de elementos ópticos de algunas realizaciones de la presente invención.

Breve descripción de los dibujos

Diversos de los dibujos adjuntos simplemente ilustran realizaciones ejemplares de la presente divulgación y no se concibe que limiten su alcance a las realizaciones ilustradas. Al contrario, se concibe que estos ejemplos abarquen alternativas, modificaciones y equivalentes que puedan estar incluidos en el alcance de la divulgación.

La FIG. 1 es un diagrama de red que muestra una sistema de red que comprende un grupo de servidores de aplicaciones en comunicación con un sistema de concesión y denegación de permisos basado en red configurado para registrar y evaluar los derechos de acceso para recursos de datos de acceso común por parte del grupo de servidores de aplicaciones, según una realización ejemplar.

La FIG. 2 es un diagrama de bloques que ilustra diversos componentes del sistema de concesión y denegación de permisos basado en red, que se proporciona como parte del sistema de red, coherente con algunas realizaciones.

La FIG. 3 es un diagrama de flujo que ilustra un procedimiento para registrar unas directrices asociadas con un recurso de datos, según algunas realizaciones ejemplares.

La FIG. 4 es un diagrama de interfaz que ilustra una porción de una interfaz para registrar unas directrices asociadas con un recurso de datos, según algunas realizaciones ejemplares.

La FIG. 5 es un diagrama de estructura de datos que ilustra elementos de un objeto de directrices mantenido en una base de datos del sistema de concesión y denegación de permisos basado en red, según algunas realizaciones ejemplares.

La FIG. 6 es un diagrama de estructura de datos que ilustra un gráfico de recursos mantenido en una base de datos del sistema de concesión y denegación de permisos basado en red, según algunas realizaciones.

La FIG. 7 es un diagrama de flujo que ilustra un procedimiento para procesar permisos de acceso asociados con un recurso de datos, según algunas realizaciones.

La FIG. 8 es un diagrama de bloques que ilustra un entorno ejemplar de red en el que puede operar el sistema de concesión y denegación de permisos basado en red, según algunas realizaciones.

La FIG. 9 es una representación esquemática de una máquina en la forma ejemplar de un sistema de ordenador en el que puede ejecutarse un conjunto de instrucciones para provocar que una máquina lleve a cabo una cualquiera o más de las metodologías expuestas en la presente memoria.

Descripción detallada

Se hará referencia ahora en detalle a realizaciones ejemplares específicas para llevar a cabo el contenido inventivo de la presente divulgación. En la siguiente descripción, se definen detalles específicos para proporcionar una comprensión exhaustiva del contenido. Se apreciará que se pueden poner en práctica las realizaciones sin algunos de estos detalles específicos, o sin ninguno de ellos.

Las realizaciones ejemplares versan acerca de un sistema de concesión y denegación de permisos basado en red y de procedimientos empleados, de ese modo, para gestionar los permisos de acceso asociados con los recursos de datos. Según se utiliza en la presente memoria, un “recurso de datos” puede incluir cualquier elemento de dato o de código (por ejemplo, un objeto de datos) que puede ser utilizado por uno o más programas de ordenador. En realizaciones ejemplares, se almacenan los recursos de datos en una o más bases de datos de red y son susceptibles de ser objeto de acceso por aplicaciones alojadas en servidores que comparten un acceso común a la base de datos de la red.

Aspectos de la presente divulgación implican directrices de registro asociadas con los recursos de datos. Las directrices definen permisos de acceso de un usuario o grupo de usuarios con respecto a un recurso de datos. Como parte del procedimiento para registrar directrices, el sistema de concesión y denegación de permisos proporciona una interfaz a usuarios (por ejemplo, al comunicar un conjunto de instrucciones legibles por un ordenador a un dispositivo del usuario) que permite a los usuarios especificar los permisos de acceso asociados con un recurso de datos. En consecuencia, la interfaz incluye un campo para identificar el recurso de datos (por ejemplo, utilizando un identificador de recursos globalmente únicos), campos para identificar usuarios (por ejemplo, utilizando un identificador de usuario) y campos para especificar el permiso de acceso de cada usuario identificado con respecto al recurso identificado.

Una vez que el usuario introduce y envía las directrices al sistema de concesión y denegación de permisos, el sistema de concesión y denegación de permisos registra las directrices con respecto al recurso de datos. Al registrar cada directriz, el sistema de concesión y denegación de permisos crea o actualiza un objeto de directrices asociado con el recurso de datos en una base de datos de directrices en la que se mantienen otros objetos de directrices asociados con otros recursos de datos. Además, el sistema de concesión y denegación de permisos mantiene una representación de la jerarquía de permisos del recurso de datos que se actualiza para reflejar directrices nuevas o actualizadas. De esta forma, el sistema de concesión y denegación de permisos mantiene unas directrices eficaces para cada recurso de datos debido a que el objeto de datos que representa las directrices incluye información de directrices para todo el árbol jerárquico y, como tal, el objeto contiene toda la información necesaria para determinar el permiso de acceso de un usuario con respecto a un recurso particular de datos.

Aspectos adicionales de la presente divulgación implican la evaluación de los permisos de acceso de un usuario con respecto a recursos compartidos de datos. El sistema de concesión y denegación de permisos evalúa los permisos del usuario en respuesta a las solicitudes de acceso que pueden ser recibidas procedentes de una cualquiera de múltiples aplicaciones alojadas en servidores vinculados comunicativamente (por ejemplo, mediante una red) al sistema de concesión y denegación de permisos. Cada solicitud de acceso identifica un recurso de datos y un usuario que solicita el acceso al recurso de datos. El sistema de concesión y denegación de permisos evalúa el permiso de acceso del usuario identificado accediendo a la información de directrices incluida en un objeto de directrices asociado con el recurso de datos y almacenado en la base de datos de directrices. La información de directrices almacenada en el objeto de directrices incluye directrices asociadas explícitamente con el recurso de datos al igual que directrices asociadas implícitamente con el recurso de datos gracias a la dependencia del recurso de datos con respecto a otros recursos de datos. El sistema de concesión y denegación de permisos comunica una respuesta a la aplicación, desde la que se recibió la solicitud de acceso, que incluye el permiso de acceso del usuario. El permiso de acceso incluye una o más operaciones que el usuario está autorizado a llevar a cabo con respecto a los recursos de datos. En algunos casos, los permisos de acceso pueden incluir operaciones que son específicas a la aplicación desde la que se recibió la solicitud de acceso.

La FIG. 1 es un diagrama de red que muestra un sistema 100 de red que comprende una plataforma 102 de procesamiento de datos en comunicación con un sistema 104 de permisos basado en red configurado para registrar y evaluar permisos de acceso para recursos de datos a los cuales el grupo de servidores 106-108 de aplicaciones comparten un acceso común, según una realización ejemplar. De acuerdo con algunas realizaciones, el sistema 100 de red puede emplear una arquitectura cliente-servidor, aunque el presente contenido inventivo no está limitado, por supuesto, a tal arquitectura, y podría igualmente bien encontrar aplicación en un sistema de arquitectura dirigida por eventos, distribuido o de dispositivos del mismo nivel, por ejemplo. Además, se apreciará que aunque se exponen diversos componentes funcionales del sistema 100 de red en el sentido singular, se pueden emplear múltiples casos de uno o más de los diversos componentes funcionales.

La plataforma 102 de procesamiento de datos incluye un grupo de servidores, específicamente los servidores 106-108, que alojan aplicaciones 109 -111 de red, respectivamente. Las aplicaciones 109-111 de red alojadas en la plataforma 102 de procesamiento de datos pueden componer colectivamente un paquete de aplicaciones que proporciona a usuarios del sistema 100 de red un conjunto de funcionalidades relacionadas, aunque independientes, que son accesibles por una interfaz común. Por ejemplo, las aplicaciones 109-111 de red pueden componer un paquete de herramientas de aplicaciones de soporte lógico que pueden ser utilizadas para analizar datos para desarrollar diversas percepciones acerca de los datos, y visualizar diversas métricas asociadas con los datos. Para ahondar en este ejemplo, se puede utilizar la aplicación 109 de red para analizar datos para desarrollar métricas particulares con respecto a información incluida en el mismo, mientras que se utiliza la aplicación 110 de red para formar representaciones gráficas de tales métricas. Se apreciará que aunque la FIG. 1 ilustra que la plataforma 102 de procesamiento de datos incluye un número particular de servidores, el contenido dado a conocer en la presente memoria no está limitado a ningún número particular de servidores y, en otras realizaciones, pueden incluirse un número menor o mayor de servidores y aplicaciones.

Cada uno de los servidores 106-108 se encuentra en comunicación con el sistema 104 de permisos basado en red a través de una red 112 (por ejemplo, Internet o una intranet). Se muestra, además, que cada uno de los servidores 106-108 se encuentra en comunicación con un servidor 114 de base de datos que facilita el acceso a una base 116 de datos de recursos a través de la red 112, aunque en otras realizaciones, los servidores 106-108 pueden acceder a la base 116 de datos de recursos directamente, sin la necesidad de un servidor 114 de base de datos. La base 116 de datos de recursos almacena recursos de datos que puede ser utilizada por una cualquiera de las aplicaciones 109-111 alojadas en la plataforma 102 de procesamiento de datos.

Para acceder a los recursos de datos desde la base 116 de datos de recursos, los servidores 106-108 transmiten solicitudes de acceso mediante la red 112 al sistema 104 de permisos basado en red. Una solicitud de acceso incluye un identificador de recurso de datos y un identificador de usuario correspondiente a un usuario (también denominado en la presente memoria “usuario solicitante”) que está utilizando una de las aplicaciones 109-111 para acceder al recurso de datos (también denominado en la presente memoria “aplicación solicitante”). El sistema 104 de permisos basado en red puede incluir una interfaz para programación de aplicaciones (API) u otra interfaz de máquina para recibir tales solicitudes de acceso procedentes del servidor 106-108 que aloja la aplicación solicitante 109-111.

Tras recibir una solicitud de acceso para un recurso particular de datos, el sistema 104 de permisos basado en red accede a un objeto de directrices almacenado por separado asociado con el recurso particular de datos. Los objetos de directrices están almacenados en una base de datos del sistema 104 de permisos basado en red, que se mantiene independientemente de la base 116 de datos de recursos.

Un objeto de directrices es una estructura de datos que incluye un identificador (por ejemplo, un identificador de recursos globalmente únicos) del recurso de datos con el que está asociado, un identificador de un recurso de datos precursor del que depende el recurso de datos (denominado “identificador precursor”) e información de directrices que incluye identificadores de recursos dependientes. La información de directrices también incluye uno o más

frases de órdenes que especifican operaciones que el usuario está autorizado o no a llevar a cabo con respecto al recurso de datos en función del cumplimiento de una o más condiciones. Las operaciones autorizadas pueden ser aplicables globalmente al sistema 100 de red, o pueden ser específicas a una cualquiera de las aplicaciones 109-111 de red.

El sistema 104 de permisos basado en red utiliza la información de directrices en el objeto correspondiente de directrices para determinar los permisos de acceso del usuario con respecto al recurso de datos. Una vez que el sistema 104 de permisos basado en red determina el permiso de acceso del usuario con respecto al recurso de datos, el sistema 104 de permisos basado en red comunica a la aplicación solicitante una respuesta a la solicitud de acceso. Más específicamente, el sistema 104 de permisos basado en red comunica uno o más paquetes de datos (por ejemplo, información legible por un ordenador) al servidor que aloja la aplicación solicitante como una respuesta a la solicitud de acceso. La respuesta a la solicitud de acceso incluye los permisos de acceso del usuario solicitante identificado con respecto al recurso de datos. Los permisos de acceso del usuario solicitante puede incluir una o más operaciones autorizadas que puede llevar a cabo el usuario sobre el recurso de datos.

En consecuencia, el sistema 104 de permisos basado en red hace de sistema centralizado de concesión y denegación de permisos para que la plataforma 102 de procesamiento de datos evalúe los permisos de acceso de usuarios del sistema 100 de red con respecto al recurso de datos almacenado en la base 116 de datos de recursos. De esta forma, el sistema 104 de permisos basado en red obvia la necesidad de las aplicaciones 109 - 111 de red para que tenga distintos sistemas dedicados de concesión y denegación de permisos. Como resultado, las aplicaciones 109-111 de red pueden operar y funcionar con independencia mutua mientras que mantienen la coherencia de los recursos de datos compartidos con respecto a los permisos de acceso del usuario.

Según se muestra, el sistema 100 de red también incluye un dispositivo cliente 118 en comunicación con la plataforma 102 de procesamiento de datos y el sistema 104 de permisos basado en red a través de la red 106. El dispositivo cliente 118 comunica e intercambia datos con la plataforma 102 de procesamiento de datos.

El dispositivo cliente 118 puede ser cualquiera de una variedad de tipos de dispositivos que incluyen al menos un medio de visualización, un procesador y capacidades de comunicaciones que proporcionan acceso a la red 106 (por ejemplo, un teléfono inteligente, un ordenador de tipo tableta, un asistente digital personal (PDA), un dispositivo de navegación personal (PND), un ordenador portátil, un ordenador de sobremesa, un ordenador portátil u ordenador súper portátil de red, o un dispositivo informático que se puede llevar puesto), y puede ser operado por un usuario (por ejemplo, una persona) para intercambiar datos con otros componentes del sistema 100 de red que pertenecen a diversos aspectos y funciones asociados con el sistema 100 de red y sus usuarios. Los datos intercambiados entre el dispositivo cliente 118 y la plataforma 102 de procesamiento de datos implican funciones seleccionadas por un usuario disponibles a través de una o más interfaces de usuario (UI). Las UI pueden estar asociadas específicamente con un cliente Web (por ejemplo, un navegador) o una aplicación 109-111 que se ejecuta en el dispositivo cliente 118 que se encuentra en comunicación con la plataforma 102 de procesamiento de datos. Por ejemplo, el sistema 104 de permisos basado en red proporciona interfaces de usuario a un usuario del dispositivo cliente 118 (por ejemplo, comunicando un conjunto de instrucciones legibles por un ordenador al dispositivo cliente 118 que provocan que el dispositivo cliente 118 represente visualmente las interfaces de usuario) que permiten al usuario registrar directrices asociadas con los recursos de datos almacenados en la base 116 de datos de recursos.

La FIG. 2 es un diagrama de bloques que ilustra diversos componentes del sistema 104 de permisos basado en red, que se proporcionan como parte del sistema 100 de red, coherente con algunas realizaciones. Para evitar ofuscar el contenido inventivo con un detalle innecesario, se han omitido de la FIG. 2 diversos componentes funcionales (por ejemplo, módulos y motores) que no son relevantes para transmitir una comprensión del contenido inventivo. Sin embargo, un experto reconocerá inmediatamente que se pueden soportar diversos componentes funcionales adicionales por medio del sistema 104 de permisos basado en red para facilitar la funcionalidad adicional que no se describe específicamente en la presente memoria.

Como comprenderán los expertos en las técnicas informáticas relevantes, cada componente funcional (por ejemplo, módulo) ilustrado en la FIG. 2 puede implementarse utilizando soporte físico (por ejemplo, un procesador de una máquina) o una combinación de lógica (por ejemplo, instrucciones ejecutables de soporte lógico) y de soporte físico (por ejemplo, memoria y procesador de una máquina) para ejecutar la lógica. Además, los diversos componentes funcionales mostrados en la FIG. 2 pueden residir en un único ordenador (por ejemplo, un ordenador portátil), o pueden distribuirse en varios ordenadores en diversas disposiciones, tales como arquitecturas basadas en la nube. Además, se apreciará que aunque se exponen los componentes funcionales (por ejemplo, módulos) de la FIG. 2 en el sentido singular, en otras realizaciones, se pueden emplear múltiples casos de uno o más de los módulos.

Se muestra que el sistema 104 de permisos basado en red incluye un módulo 200 de interfaz, un módulo 202 de registro y un módulo 204 de evaluación, todos configurados para comunicarse entre sí (por ejemplo, mediante un *bus*, memoria compartida, un conmutador, o interfaces para programación de aplicaciones (API)). Los módulos mencionados anteriormente del sistema 104 de permisos basado en red puede, además, acceder a una base 206 de datos de directrices y a un registro 208 de operaciones de auditoría. Cada uno de la base 206 de datos de directrices y del registro 208 de operaciones de auditoría reside en un soporte de almacenamiento legible por una

máquina del sistema 104 de permisos basado en red. La base 206 de datos de directrices y el registro 208 de operaciones de auditoría pueden mantenerse con independencia mutua.

El módulo 200 de interfaz recibe solicitudes de diversos dispositivos (por ejemplo, los servidores 106-108) y comunica respuestas apropiadas a los dispositivos solicitantes. El módulo 200 de interfaz proporciona interfaces para permitir que dispositivos soliciten acceso a recursos de datos almacenados en la base 116 de datos de recursos. Por ejemplo, el módulo 200 de interfaz puede recibir solicitudes de acceso para recursos de datos en forma de una solicitud de interfaz para programación de aplicaciones (API).

El módulo 200 de interfaz también proporciona interfaces de usuario a usuarios del sistema 100 de red (por ejemplo, comunicando un conjunto de instrucciones legibles por un ordenador a dispositivos de ordenador de los usuarios). El módulo 200 de interfaz también recibe una entrada del usuario a través de tales interfaces de usuario, y pasa la entrada recibida del usuario al componente aplicable del sistema 104 de permisos basado en red. Como ejemplo, el módulo 200 de interfaz proporciona interfaces de usuario para permitir que los usuarios registren y modifiquen directrices asociadas con los recursos de datos almacenados en la base 116 de datos de recursos. A continuación, con referencia a la FIG. 4, se expone un ejemplo de tales interfaces de usuario proporcionadas por el módulo 200 de interfaz.

Las directrices forman la base del modelo de seguridad del sistema 104 de permisos basado en red. Cada directriz está compuesta por un conjunto de frases de instrucciones no ordenadas, y cada frase de órdenes da como resultado un valor booleano bien de “VERDADERO” o de “FALSO” e incluye: una operación o un conjunto de operaciones que se ve afectado por la frase de órdenes, una acción que ha de emprenderse con la operación especificada y una condición utilizada para determinar la aplicación a operaciones especificadas de la aplicación especificada.

Para cada recurso de datos almacenado en la base 116 de datos de recursos de datos, el sistema 104 de permisos basado en red mantiene una estructura de datos en la base 206 de datos de directrices que incluye un gráfico sencillo de recursos diseñado para emular estructuras básicas similares a un sistema de ficheros y también acomodar dependencias de recursos relacionados. Cada nodo en el gráfico de recursos representa un recurso de datos. De esta forma, el sistema 104 de permisos basado en red mantiene una representación de la jerarquía de permisos de un recurso de datos en un objeto unificado sencillo que puede ser evaluado de forma aislada. En consecuencia, el objeto de directrices proporciona un árbol jerárquico de permisos de acceso en un formato ordenado, de manera que el módulo 204 de evaluación solo necesite las directrices eficaces para determinar los permisos de un usuario.

El módulo 202 de registro es responsable de registrar directrices asociadas con recursos de datos almacenados en la base 116 de datos de recursos. Como parte del procedimiento de registro, el módulo 202 de registro recibe y procesa datos de registro de directrices enviados por usuarios a través de interfaces de usuario proporcionadas por el módulo 200 de interfaz (por ejemplo, proporcionando un conjunto de instrucciones legibles por un ordenador a dispositivos de ordenador de los usuarios) que permiten que los usuarios registren y modifiquen directrices asociadas con los recursos de datos.

Durante el procedimiento de registro, un usuario puede interactuar con diversos elementos de interfaz (por ejemplo, mediante uno o más dispositivos de entrada) de interfaces de usuario para especificar datos de registro de directrices incluyendo: un identificador de recurso correspondiente a un recurso de datos, y unas directrices asociadas con el recurso de datos. Cada directriz puede incluir un identificador de usuario o un conjunto de identificadores de usuarios correspondiente a un usuario o a un grupo de usuarios, aunque se apreciará que en algunos casos, unas directrices pueden ser indiferentes en cuanto al usuario (por ejemplo, permitir el acceso antes del 25 de diciembre de 2015). Cada directriz especifica operaciones que se autoriza que lleven a cabo usuarios con respecto al recurso de datos. Tras determinar que se autoriza al usuario crear unas nuevas directrices o modificar unas directrices existentes, el módulo 202 de registro registra las directrices especificadas por el usuario.

Al registrar unas directrices, el módulo 202 de registro almacena un objeto de directrices en la base 206 de datos de directrices. Cada objeto de directrices es una estructura de datos que está vinculada con un recurso de datos, aunque los objetos de directrices y los recursos de datos se mantienen por separado - los objetos de directrices se almacenan en la base 206 de datos de directrices y los recursos de datos se almacenan en la base 116 de datos de recursos -. Cada objeto de directrices incluye: un identificador de recurso correspondiente al recurso de datos con el que se asocia las directrices; uno o más identificadores precursores, identificando cada uno de los cuales un recurso precursor de datos del que depende el recurso de datos, si es aplicable; y unas directrices asociadas con el recurso de datos.

Cada directriz incluye una o más frases de órdenes que especifican operaciones particulares que se autoriza a un usuario a llevar a cabo con respecto a un recurso particular de datos. En particular, cada frase de órdenes incluye un campo para cada operación (o conjunto de operaciones), una acción y una condición. El campo de operación corresponde a una operación que se autoriza a un usuario a llevar a cabo con respecto al recurso de datos. Cada operación puede ser aplicable globalmente al sistema 104 de permisos basado en red o puede estar relacionada específicamente con una de las aplicaciones 109-111 de red.

Cada frase de órdenes se ejecuta según el cumplimiento de las condiciones particulares incluidas en el mismo. Como ejemplo, la condición puede especificar un identificador de usuario particular correspondiente a un usuario permitido, y se cumple la condición si el identificador de usuario del usuario solicitante se corresponde con el identificador de usuario del usuario permitido. Como otro ejemplo, la condición puede ser una condición temporal, tal como un intervalo de tiempo en el que un usuario solicitante puede acceder al recurso de datos y, de esta forma, se pueden utilizar las condiciones para proporcionar una fecha (o una hora) de caducidad para unas directrices. Condiciones ejemplares adicionales soportadas por el sistema 104 de permisos basado en red incluyen: una condición de DEPENDIENTE para comprobar si las operaciones resultantes de las dependencias contienen todas las operaciones especificadas por la condición, o cualquiera de ellas; una condición de GRUPO para comprobar si un usuario posee todos los grupos especificados por la condición, o cualquiera de ellos; una condición de NO para negar el resultado de otra condición; una condición de O que toma dos o más condiciones y comprueba si cualquiera de ellas da como resultado un valor verdadero; una condición de Y que toma dos o más condiciones y comprueba si todas ellas dan como resultado un valor verdadero; una condición de USUARIO para comprobar si el usuario solicitante es el usuario permitido; y una condición de TIPO DE USUARIO que comprueba si el usuario de del tipo permitido (por ejemplo, usuario o servicio). Se comprenderá que las condiciones soportadas por el sistema 104 de permisos basado en red pueden ser extensible y, por lo tanto, no están limitadas a los anteriores ejemplos a los que se ha hecho referencia. Lo que sigue es un ejemplo de tal combinación: “NO(USUARIO=X)”; “Y(USUARIO=X, GRUPO=Y)”.

Las acciones incluidas en el campo de acción definen un comportamiento asociado con una frase de órdenes particular, tal como permitir o denegar la capacidad de un usuario para llevar a cabo una operación. Además, las acciones pueden incluir invalidaciones especiales de otras acciones en la cadena de herencia de directrices del recurso de datos. Como ejemplo, las acciones pueden incluir lo siguiente: una acción de PERMITIR que concede una operación especificada a un contexto actual si la condición da como resultado “VERDADERO”; una acción de DENEGAR que deniega una operación especificada si la condición da como resultado “VERDADERO” a una acción de PERMITIR-A-LA-FUERZA que concede operaciones especificadas como una invalidación especial y provoca que el sistema ignore todas las acciones de DENEGAR y de DENEGAR-A-LA-FUERZA, si la condición da como resultado “VERDADERO”; una acción de DENEGAR-A-LA-FUERZA que deniega operaciones especificadas a no ser que sea invalidada explícitamente por una frase de órdenes de PERMITIR-A-LA-FUERZA; una condición de PERMITIR-EN-DERIVADOS o DENEGAR-EN-DERIVADOS que se aplica únicamente cuando es heredada (por ejemplo, en vez de decir que un usuario tiene (o no tiene) derechos en un nodo específico en el gráfico, un recurso puede estar configurado para conceder (o denegar) el acceso únicamente a nodos derivados). Se comprenderá que las acciones soportadas por el sistema 104 de permisos basado en red pueden ser extensibles, y por lo tanto no están limitadas, a los ejemplos a los que se ha hecho referencia anteriormente. Con referencia a la FIG. 3 a continuación se exponen detalles adicionales con relación al procedimiento de registro llevado a cabo por el módulo 202 de registro, según algunas realizaciones ejemplares.

El módulo 204 de evaluación está configurado para evaluar los permisos de acceso del usuario con respecto a recursos de datos almacenados en la base 116 de datos de recursos. La evaluación de los permisos de acceso del usuario, en la mayoría de casos, es activada por la recepción de una solicitud de acceso recibida por medio de una API procedente de una aplicación de red soportada por el sistema 104 de permisos basado en red (por ejemplo, las aplicaciones 109-111 de red). La solicitud de acceso incluye un identificador de recurso de datos correspondiente al recurso de datos para el cual se está solicitando el acceso, y un identificador de usuario correspondiente al usuario solicitante. En algunos casos, la solicitud de acceso puede incluir, además, uno o más filtros identificando una o más operaciones particulares o conjuntos de operaciones que son de interés.

Al evaluar un permiso de acceso de un usuario con respecto a un recurso particular de datos, el módulo 204 de evaluación accede a un objeto de directrices asociado con el recurso de datos desde la base 206 de datos de directrices. Para evaluar el permiso de acceso del usuario solicitante a un recurso particular de datos, el módulo 204 de evaluación lleva a cabo una evaluación primero en profundidad y luego sigue un modelo sencillo de herencia. Durante la evaluación, el módulo 204 de evaluación realiza un seguimiento de múltiples conjuntos de operaciones correspondientes a las acciones expuestas anteriormente. En un ejemplo, el módulo 204 de evaluación realiza un seguimiento de: 1) frases de órdenes de PERMITIR; 2) frases de órdenes de DENEGAR-A-LA-FUERZA; y 3) frases de órdenes de PERMITIR-A-LA-FUERZA.

En cada nodo del gráfico de recursos incluido en el objeto de directrices almacenado en la base 206 de datos de directrices, el módulo 204 de evaluación evalúa el recurso precursor de datos, entonces lleva a cabo una evaluación concisa de las dependencias (por ejemplo, dependencias evaluadas únicamente si una condición requiere los resultados), entonces evalúa el nodo local (por ejemplo, el recurso de datos para el cual se evalúa el permiso de acceso) y luego una fusión de los resultados precursores y locales.

En el nivel de solicitud más alto, el módulo 204 de evaluación colapsa los conjuntos de operaciones objeto de seguimiento en un único conjunto. El procedimiento para colapsar los conjuntos de operaciones objeto de seguimiento incluye la creación de un conjunto vacío y añadiendo todas las operaciones permitidas explícitamente en el conjunto vacío. Entonces, el módulo 204 de evaluación elimina todas las operaciones denegadas explícitamente. Durante esta operación, se utiliza una operación especial para eliminar todas las operaciones

concedidas anteriormente. Entonces, el módulo 204 de evaluación añade todas las frases de órdenes de PERMITIR-A-LA-FUERZA al conjunto.

Tras determinar los permisos de acceso de un usuario, el módulo 204 de evaluación comunica una respuesta a una solicitud recibida de acceso a una aplicación 109-111 de red solicitante (por ejemplo, mediante una llamada apropiada a la API). La respuesta incluye un conjunto de operaciones que se autoriza que lleve a cabo el usuario con respecto al recurso de datos. En casos en los que la solicitud de acceso incluye filtros de operación, la respuesta comunicada a la aplicación solicitante 109-111 puede incluir únicamente aquellas operaciones de interés a la aplicación 109-111 y, como tal, la generación de la respuesta puede incluir la omisión de una porción del conjunto de todas las operaciones que se autoriza que lleven a cabo usuarios con respecto al recurso de datos. En función de la respuesta recibida del módulo 204 de evaluación, la aplicación solicitante 109-111 puede bien permitir o bien inhabilitar una o más operaciones que el usuario puede llevar a cabo con respecto al objeto de datos dependiendo de los permisos de acceso determinados del usuario.

Para cada solicitud de acceso recibida, el módulo 204 de evaluación crea y almacena un registro de operaciones de solicitudes de acceso en un registro 208 de operaciones de auditoría. Cada registro de operaciones de solicitudes de acceso incluye un identificador de recurso, un identificador de usuario, permisos determinados de acceso del usuario, un identificador del solicitante (por ejemplo, la dirección IP) y un sello de tiempo.

La FIG. 3 es un diagrama de flujo que ilustra un procedimiento 300 para registrar unas directrices asociadas con un recurso de datos, según algunas realizaciones ejemplares. El procedimiento 300 se implementa en instrucciones legibles por un ordenador para su ejecución mediante uno o más procesadores, de forma que las operaciones del procedimiento 300 sean llevadas a cabo, en parte o completamente, por medio del sistema 104 de permisos basado en red; en consecuencia, a continuación se describe el procedimiento 300 a modo de ejemplo con referencia al mismo. Sin embargo, se apreciará que al menos algunas de las operaciones del procedimiento 300 pueden ser desplegadas en diversas configuraciones distintas de soporte físico, y no se pretende que el procedimiento 300 esté limitado al sistema 104 de permisos basado en red.

En la operación 305, el módulo 200 de interfaz proporciona una interfaz de registro de directrices a un dispositivo de ordenador para registrar unas directrices asociadas con un recurso de datos. Por ejemplo, el módulo 200 de interfaz puede proporcionar un conjunto de instrucciones legibles por un ordenador al dispositivo cliente 118 que provocan que el dispositivo de ordenador represente visualmente la interfaz de registro de directrices.

Como ejemplo de la interfaz de registro de directrices proporcionada por el módulo 200 de interfaz, la FIG. 4 es un diagrama de interfaz que ilustra una porción de una interfaz 400 de usuario para registrar unas directrices asociadas con un recurso de datos, según algunas realizaciones ejemplares. Según se muestra, la interfaz 400 de usuario incluye un campo 402 en el que un usuario que se conecta introduce un identificador de usuario (por ejemplo, nombre, nombre de usuario, una dirección de correo electrónico, un número de teléfono u otro identificador tal) o un identificador de grupo de usuarios. La interfaz 400 de usuario incluye, además, un elemento gráfico 404, específicamente un menú desplegable, para especificar los permisos de acceso del usuario identificado o del grupo de usuarios.

Según se muestra, la interfaz 400 de usuario también representa visualmente permisos existentes de acceso del usuario incluidos en las directrices del recurso de datos. Por ejemplo, la interfaz 400 de usuario representa visualmente un identificador 406 de usuario (el nombre del usuario) correspondiente a un usuario que tiene permiso para acceder al recurso de datos. En particular, el identificador 406 de usuario está enumerado como un “propietario” del recurso de datos, lo que indica que el usuario tiene privilegios administrativos con respecto al recurso de datos. Adicionalmente, la interfaz 400 de usuario incluye un identificador 408 de grupo de usuarios correspondiente a un grupo de usuarios que tienen permisos de acceso con respecto al recurso de datos. En particular, el grupo de usuarios identificado por el identificador 408 de grupo de usuarios está autorizado a editar el recurso de datos.

El botón 410 es utilizado por el usuario que se conecta para enviar las directrices al módulo 202 de registro. Más específicamente, tras la selección por parte del usuario del botón 410, el módulo 200 de interfaz proporciona al módulo 202 de registro un registro de directrices para el recurso de datos. Con referencia de nuevo a la FIG. 3, en la operación 310, el módulo 204 de evaluación recibe el registro de directrices asociado con el recurso de datos. El registro de directrices incluye un identificador de usuario y los permisos especificados de acceso del usuario con respecto al recurso de datos.

En la operación 315, el módulo 204 de evaluación evalúa los permisos de acceso del usuario que se conecta. En particular, el módulo 204 de evaluación determina si el usuario que se conecta está autorizado para editar las directrices asociadas con el recurso de datos. A continuación se exponen con referencia a la FIG. 7 detalles adicionales del procedimiento de evaluación de los permisos de acceso de usuario, según algunas realizaciones ejemplares.

En la operación 320, el módulo 202 de registro registra las directrices asociadas con el recurso de datos en función de los permisos de acceso del usuario que se conecta que autorizan al usuario que se conecta a modificar las

directrices del recurso de datos. En casos en los que el recurso de datos no tiene unas directrices existentes, el registro de las directrices incluye la creación y el almacenamiento de un objeto de directrices asociado con el recurso de datos en la base 206 de datos de directrices. En casos en los que el recurso de datos tiene unas directrices existentes, el registro de las directrices incluye la actualización de un objeto de directrices asociado con el recurso de datos que se almacena en la base 206 de datos de directrices. El objeto almacenado o actualizado de directrices incluye las frases de órdenes incluidas en las directrices especificadas por el usuario que se conecta mediante la interfaz de registro de directrices.

Como ejemplo, la FIG. 5 es un diagrama de estructura de datos que ilustra elementos de un objeto 502 de directrices asociado con un recurso 500 de datos, según algunas realizaciones ejemplares. El recurso 500 de datos se almacena en la base 116 de datos de recursos mientras que el objeto 502 de directrices se almacena en la base 206 de datos de directrices. El objeto 502 de directrices incluye un identificador 504 de recurso que identifica el recurso 500 de datos. El objeto 502 de directrices incluye, además, un campo de identificador precursor 506 que incluye un identificador de recursos de datos precursores del que depende el recurso 500 de datos. En casos en los que el recurso 500 de datos no tiene ninguna dependencia, el identificador precursor 506 incluye una entrada nula.

El objeto 502 de directrices incluye, además, unas directrices 508 que comprenden un conjunto de frases de instrucciones no ordenadas 510-5*n*0. Al mantener el identificador precursor 506 en el objeto 502 de directrices asociado con el recurso 500 de datos, el sistema 104 de permisos basado en red es capaz de hacer un seguimiento de la cadena de herencia del recurso 500 de datos. La cadena de herencia del recurso 500 de datos incluye un recurso precursor de datos (otros recursos de datos de los que depende el recurso 500 de datos) junto con recursos derivados de datos (otros recursos de datos que dependen del recurso 500 de datos). En consecuencia, las frases de órdenes 510-5*n*0 incluyen frases de órdenes asociadas explícitamente con el recurso 500 de datos. Las frases de órdenes que están asociadas implícitamente con el recurso 500 de datos mediante herencia de la dependencia del recurso 500 de datos en el recurso precursor identificado en el campo de identificador precursor 506 pueden ser evaluados accediendo al objeto de directrices asociado con el recurso precursor. La frase de órdenes 510 incluye una acción 512, una condición 514 y una operación 516. La acción 512 define el comportamiento asociado con la frase de órdenes 510. Se utiliza la condición 514 para determinar la aplicación de la acción 512 a la operación 516. La operación 516 es la operación afectada por la frase de órdenes 510. La acción 510 puede especificar bien que se permite o se deniega que el usuario lleve a cabo la operación 516 en función de si se cumple la condición 514. El sistema 104 de permisos basado en red puede soportar, además, acciones que invalidan otras operaciones especificadas.

En casos en los que el recurso 500 de datos para el cual se ha enviado un registro de directrices incluye una dependencia de otro recurso de datos, el módulo 204 de evaluación actualiza una representación jerárquica de los permisos de acceso del recurso 500 de datos según las directrices recibidas durante el registro de las directrices, que puede incluir la aplicación de las directrices registradas a otros recursos de datos en la cadena de herencia del recurso 500 de datos. En consecuencia, el registro de las directrices puede incluir la modificación de objetos de directrices asociado con recursos de datos (por ejemplo, recursos precursor y derivado de datos) en la cadena de herencia para que incluyan al menos una porción de la pluralidad de frases de órdenes de permisos provenientes de las directrices recién registradas.

Como ejemplo, la FIG. 6 es un diagrama de estructura de datos que ilustra un gráfico 600 de recursos mantenido en la base 206 de datos de directrices del sistema 104 de permisos basado en red, según algunas realizaciones. El gráfico 600 de recursos puede mantenerse para cada uno de los recursos de datos almacenados en la base 116 de datos de recursos de datos. Cada gráfico de recursos puede mantenerse de forma independiente de los objetos de directrices o como parte de los objetos de directrices. Por ejemplo, el gráfico 600 de recursos puede almacenarse como parte del objeto 502 de directrices.

Los nodos individuales en el gráfico 600 de recursos representa recursos de datos, aunque los nodos no incluyen ellos mismos el contenido de los recursos de datos que representan. Por ejemplo, el gráfico 600 de recursos se almacena en la base 206 de datos de directrices del sistema 104 de permisos basado en red mientras que cada uno de los recursos 500, 602 y 604 de datos son almacenados por separado en la base 116 de datos de recursos.

Según se muestra, el gráfico 600 de recursos incluye una representación de una cadena de herencia del recurso 500 de datos. En particular, el gráfico 600 de recursos incluye una representación de una dependencia del recurso 500 de datos con respecto a los recursos precursores 602 de datos. Además, el gráfico 600 de recursos incluye una representación de un recurso derivado - recurso 604 de datos - que depende del recurso 500 de datos. Al registrar unas nuevas directrices asociadas con el recurso 500 de datos, el módulo 202 de registro puede actualizar unas directrices eficaces asociadas con el recurso 604 de datos para que incluya al menos una porción de las frases de órdenes 510-5*n*0 incluidas en las directrices asociadas con el recurso 500 de datos. Al mantener unas directrices eficaces asociadas con el recurso de datos, el sistema 104 de permisos basado en red hace seguimiento de permisos heredados de acceso a recursos dependientes de datos. Por lo tanto, al mantener una representación de unas directrices eficaces de la cadena de herencia del recurso 500 de datos, el sistema 104 de permisos basado en red mantiene toda la información de directrices con respecto a un recurso particular de datos en un objeto de directrices asociado con el recurso de datos, de forma que el módulo 204 de evaluación del sistema 104 de

permisos basado en red solo necesite leer un único nodo para calcular los permisos de acceso de todo el gráfico 600 de recursos.

La FIG. 7 es un diagrama de flujo que ilustra un procedimiento 700 para procesar permisos de acceso asociados con un recurso de datos, según algunas realizaciones. El procedimiento 700 se implementa en instrucciones legibles por un ordenador para su ejecución mediante uno o más procesadores, de forma que se lleven a cabo las operaciones del procedimiento 700 en parte o completamente por medio del sistema 104 de permisos basado en red; en consecuencia, a continuación se describe el procedimiento 700 a modo de ejemplo con referencia al mismo. Sin embargo, se apreciará que al menos algunas de las operaciones del procedimiento 700 pueden ser desplegadas en diversas otras configuraciones de soporte físico, y no se concibe que el procedimiento 700 esté limitado al sistema 104 de permisos basado en red.

En la operación 705, el módulo 200 de interfaz recibe una solicitud de acceso a un recurso de datos. Por ejemplo, el módulo 200 de interfaz puede recibir una solicitud de acceso procedente de una de las aplicaciones 109-111 de red mediante una llamada a la API para acceder al recurso 500 de datos. La solicitud de acceso incluye un identificador de recurso (por ejemplo, el identificador 504 de recurso) correspondiente al recurso de datos (por ejemplo, el recurso 500 de datos) y un identificador de usuario correspondiente al usuario solicitante. El identificador de usuario puede ser o incluir, por ejemplo, un nombre, un nombre de usuario, una dirección de correo electrónico, un número de empleado o cualquier otro identificador único adecuado para identificar al usuario. En coherencia con algunas realizaciones, como parte de la recepción de la solicitud de acceso, el módulo 200 de interfaz recibe un testigo de portador, que es una cadena criptográficamente segura que representa un usuario. El sistema 104 de permisos basado en red puede interactuar con diversos servicios de red de usuario (por ejemplo, mediante intercambios de datos por la red 112) que comprueban la validez del testigo, y devuelven un objeto de usuario que incluye el identificador de usuario.

En la operación 710, el módulo 204 de evaluación accede a un objeto de directrices (por ejemplo, el objeto 502 de directrices) asociado con el recurso de datos desde la base 206 de datos de directrices en respuesta a la recepción de la solicitud de acceso al recurso de datos. Por ejemplo, tras la recepción de una solicitud de acceso al recurso 500 de datos, el módulo 204 de evaluación accede al objeto 502 de directrices desde la base 206 de datos de directrices. Según se ha expuesto anteriormente, el objeto de directrices incluye una lista de frases de instrucciones no ordenadas que definen los permisos de acceso del usuario solicitante con respecto al objeto de directrices. El objeto de directrices puede incluir frases de órdenes registradas explícitamente en asociación con el recurso de datos al igual que frases de órdenes heredadas por el recurso de datos en función de una dependencia de otros recursos de datos.

En la operación 715, el módulo 204 de evaluación evalúa los permisos de acceso del usuario identificado con respecto al recurso identificado de datos en función de la información incluida en el objeto de directrices. El permiso de acceso del usuario con respecto al recurso de datos hace referencia a un conjunto de operaciones que se autoriza que lleve a cabo el usuario sobre el recurso de datos. En consecuencia, la evaluación del permiso de acceso del usuario incluye la determinación de un conjunto de operaciones que se autoriza que el usuario lleve a cabo con respecto al recurso de datos, que depende de si se cumplen las condiciones incluidas en el conjunto de frases de órdenes incluido en las directrices. Por lo tanto, la evaluación del permiso de acceso del usuario puede incluir la determinación de si se cumplen las condiciones incluidas en el conjunto de frases de órdenes. Como ejemplo, una frase de órdenes en las directrices puede incluir una condición que especifica un identificador particular de usuario correspondiente a un usuario permitido, y la determinación de que se cumple la condición en función de que el identificador de usuario del usuario solicitante se corresponda con el identificador de usuario del usuario permitido. Como otro ejemplo, una frase de órdenes en las directrices puede incluir una condición temporal que especifique como un intervalo de tiempo durante el cual un usuario solicitante puede acceder al recurso de datos, y la determinación de que se cumple la condición en función de si se recibe la solicitud de acceso durante el intervalo de tiempo.

Al evaluar el permiso de acceso de un usuario con respecto a un recurso particular de datos, el módulo 204 de evaluación accede a un objeto de directrices asociado con el recurso de datos desde la base 206 de datos de directrices. Para evaluar el permiso de acceso del usuario solicitante a un recurso particular de datos, el módulo 204 de evaluación lleva a cabo una evaluación primero en profundidad y luego sigue un modelo sencillo de herencia. En cada nodo del gráfico de recursos incluido en el objeto de directrices almacenado en la base 206 de datos de directrices, el módulo 204 de evaluación evalúa en primer lugar el recurso precursor de datos, entonces lleva a cabo una evaluación concisa de las dependencias (por ejemplo, solo se evalúan las dependencias si una condición requiere los resultados), luego evalúa el nodo local (por ejemplo, el recurso de datos para el cual se está evaluando el permiso de acceso) y devuelve una fusión de resultados precursor y local. En el nivel más alto de solicitud, el módulo 204 de evaluación colapsa los conjuntos de operación objeto de seguimiento en un único conjunto. El procedimiento para colapsar los conjuntos de operación objeto de seguimiento incluye la creación de un conjunto vacío añadiendo todas las operaciones permitidas explícitamente en el conjunto vacío. Entonces, el módulo 204 de evaluación elimina todas las operaciones denegadas explícitamente. Durante esta operación, se utiliza una operación especial para eliminar todas las operaciones concedidas anteriormente. Entonces, el módulo 204 de

evaluación añade todas las frases de órdenes de permiso de invalidación (por ejemplo, las frases de órdenes PERMITIR-A-LA-FUERZA) al conjunto.

En la operación 720, el módulo 204 de evaluación funciona junto con el módulo 200 de interfaz para comunicar a la aplicación solicitante (por ejemplo, mediante una llamada a la API) una respuesta a la solicitud de acceso. La respuesta a la solicitud de acceso incluye el permiso de acceso del usuario y, en consecuencia, la respuesta incluye un conjunto de operaciones que se autoriza que lleve a cabo el usuario con respecto a la aplicación. En función de los permisos de acceso incluidos en la respuesta, la aplicación solicitante puede bien conceder o bien denegar el acceso del usuario al recurso de datos, que puede incluir bien la habilitación o bien la inhabilitación de ciertas operaciones o funcionalidades de la aplicación solicitante.

En la operación 725, el módulo 204 de evaluación crea un registro de operaciones de la solicitud de acceso. El registro de operaciones de la solicitud de acceso incluye una indicación de la recepción de la solicitud de acceso, una hora correspondiente a la recepción de la solicitud de acceso, un identificador del usuario y el permiso de acceso determinado del usuario. En la operación 730, el módulo 204 de evaluación almacena el registro de operaciones en el registro 208 de operaciones de auditoría.

La FIG. 8 es un diagrama de bloques que ilustra un entorno ejemplar 800 de red en el que puede operar el sistema 104 de permisos basado en red, según algunas realizaciones. Según se muestra, el entorno 800 de red incluye: una aplicación 802; un almacén 804 de objetos conectado con una base 806 de datos; un motor 808 de búsqueda consciente de las directrices conectado con una base 810 de datos; y el sistema 104 de permisos basado en red. Cada uno de los componentes funcionales a los que se ha hecho referencia anteriormente del entorno de red puede implementarse utilizando soporte físico (por ejemplo, un procesador de una máquina) o una combinación de lógica (por ejemplo, instrucciones ejecutables de soporte lógico) y de soporte físico (por ejemplo, memoria y un procesador de una máquina) para ejecutar la lógica. Además, cada uno de los diversos componentes funcionales puede residir en un único ordenador (por ejemplo, un servidor) o pueden distribuirse entre varios ordenadores en diversas disposiciones, tales como arquitecturas basadas en la nube.

La aplicación 802 es una aplicación basada en Web en comunicación bien con el almacén 804 de objetos o bien con el motor 808 de búsqueda consciente de las directrices, o con ambos. Por ejemplo, se puede utilizar la aplicación 802, que puede corresponderse con una cualquiera de las aplicaciones 109-111 de red, para analizar datos para desarrollar diversas percepciones acerca de los datos, y visualizar diversas métricas asociadas con los datos.

El almacén 804 de objetos está construido sobre la base 806 de datos. En coherencia con algunas realizaciones, el almacén 804 de objetos puede ser seguro, estar compartimentalizado y/o almacenar pares de clave/valor. Se pueden asegurar datos utilizando testigos de autentificación y se pueden comprobar los permisos de acceso utilizando el sistema 104 de permisos basado en red. El almacén 804 de objetos puede estar compartimentalizado organizando un intervalo de claves y valores asociados en un espacio nominal. En una realización, las claves pueden ser cadenas.

Los usuarios del almacén 804 de objetos pueden introducir una etiqueta de versión en operaciones para forzar actualizaciones atómicas de clave única. En una realización, las etiquetas de versión pueden habilitar contadores, y se puede incrementar un contador si hay un anterior incremento. En otra realización, si el almacén 804 de objetos recibe una etiqueta de versión para una operación, las operaciones pueden no ser idempotentes (por ejemplo, una segunda llamada de la operación puede provocar un error si tiene éxito la primera llamada de la operación). En una realización adicional, si el almacén 804 de objetos no recibe una etiqueta de versión para una operación, el almacén 804 de datos puede realizar la aseveración de que la operación será idempotente (por ejemplo, el estado resultante y el comportamiento de la llamada serán idénticos, o se garantiza que se apliquen sus efectos secundarios).

Cuando el almacén 804 de datos almacena un objeto, también se puede añadir el objeto en una tabla en la base 806 de datos, y el objeto puede ser transmitido a un canal de notificaciones sin que medie solicitud (por ejemplo, mediante una API de llamada de respuesta definida en el almacén 804 de datos). El motor 808 de búsqueda consciente de las directrices puede recibir la o las notificaciones (por ejemplo, mediante una API dedicada a la escucha de eventos). En una realización, se pueden transmitir eventos sin que medie solicitud a un único URL por receptor configurado.

El almacén 804 de objetos puede tener un punto final que puede ser utilizado por los usuarios para ANUNCIAR formularios de múltiples partes de objetos que han de ser insertados. En una realización, el punto final puede insertar atómicamente el objeto. En otra realización, el punto final puede determinar el o los compartimentos, la o las claves y/o la o las versiones relevantes del conjunto de cabeceras en el cuerpo del formulario.

El almacén 804 de datos puede indexar datos escritos en el motor 808 de búsqueda consciente de las directrices. En algunas realizaciones, el motor 808 de búsqueda consciente de las directrices puede permitir una búsqueda más rápida que el almacén 804 de objetos. En algunas realizaciones, el motor 808 de búsqueda consciente de las directrices puede ser un servicio de búsqueda con respaldo de búsquedas elásticas. En algunas realizaciones, el motor 808 de búsqueda consciente de las directrices puede tener esquemas y listas de control de acceso a nivel de objetos (por ejemplo, en función del sistema 104 de permisos basado en red). El motor 808 de búsqueda consciente

de las directrices puede respaldar la aplicación 802 y/o indexar objetos arbitrarios del almacén 804 de objetos. El motor 808 de búsqueda consciente de las directrices puede exponer una API de consultas de búsqueda. Por ejemplo, el motor 808 de búsqueda consciente de las directrices puede exponer una API de consultas de búsquedas elásticas, añadiendo, de ese modo, una capa de seguridad encima del servicio de búsqueda (por ejemplo, búsqueda elástica) al igual que una API de indexación para otros servicios para indexar objetos arbitrarios.

El motor 808 de búsqueda consciente de las directrices también puede indexar identificadores de recursos accesibles a un usuario en el nodo 812 de lectura. En algunas realizaciones, el nodo 812 de lectura puede permitir una búsqueda más rápida que el motor 808 de búsqueda consciente de las directrices sin el nodo 812 de lectura. Para cada solicitud de acceso al sistema 104 de permisos basado en red, el nodo 812 de lectura también puede almacenar un identificador de usuario y un identificador de recurso. Tras la recepción de una consulta de búsqueda procedente de un usuario, el motor 808 de búsqueda consciente de las directrices puede consultar el nodo 812 de lectura con un identificador de usuario correspondiente al usuario solicitante. El nodo 812 de lectura responde al motor 808 de búsqueda consciente de las directrices con una lista de todos los identificadores de recursos accesibles al identificador de usuario, que representa únicamente un subconjunto de los registros en la base 810 de datos. El motor 808 de búsqueda consciente de las directrices puede consultar a la base 810 de datos para que ejecute la consulta de búsqueda únicamente en el subconjunto de registros que contienen los identificadores de recursos devueltos por el nodo 812 de lectura. De esta forma, el motor 808 de búsqueda consciente de las directrices puede evitar la ejecución de la consulta de búsqueda contra cada registro en la base 810 de datos y verificar cada resultado consultado de la base 810 de datos con el sistema 104 de permisos basado en red para confirmar que el usuario puede acceder al resultado consultado. El nodo 812 de lectura puede proporcionar, además, a los usuarios una opción de utilizar un posfiltrado para ciertos casos de usos sensibles.

En algunas realizaciones, para cada solicitud de acceso al sistema 104 de permisos basado en red, el nodo 812 de lectura puede almacenar, además, información de la versión (por ejemplo, una hora correspondiente a la recepción de la solicitud de acceso, la etiqueta de la versión o el número de la versión). En algunas realizaciones, el usuario puede tolerar una latencia o diferencia especificada en valores entre la información de la versión almacenada en el nodo 812 de lectura y la información de la versión almacenada en el sistema 104 de permisos basado en red. En algunas realizaciones, el nodo 812 de lectura, la aplicación 802 y/o el motor 808 de búsqueda consciente de las directrices pueden aceptar una entrada de umbral por un usuario como la latencia o la diferencia especificada en valores entre la información de la versión almacenada en el nodo 812 de lectura y el sistema 104 de permisos basado en red. Si la latencia o diferencia especificada en valores entre la información de la versión almacenada en el nodo 812 de lectura y la información de la versión almacenada en el sistema 104 de permisos basado en red supera el umbral introducido, el motor 808 de búsqueda consciente de las directrices puede interrogar a la base 810 de datos sin limitar la consulta de búsqueda a los identificadores de recursos devueltos por el nodo 812 de lectura.

La FIG. 9 es una representación esquemática de una máquina en la forma ejemplar de un sistema de ordenador en el que puede ejecutarse un conjunto de instrucciones para provocar que la máquina lleve a cabo una cualquiera o más de las metodologías expuestas en la presente memoria. Específicamente, la FIG. 9 muestra una representación esquemática de la máquina 900 en la forma ejemplar de un sistema, en el que pueden ejecutarse las instrucciones 902 (por ejemplo, soporte lógico, un programa, una aplicación, una miniaplicación, una app, un controlador u otro código ejecutable) para provocar que la máquina 900 lleve a cabo una cualquiera o más de las metodologías expuestas en la presente memoria. Por ejemplo, las instrucciones 902 incluyen código ejecutable que provoca que la máquina 900 ejecute los procedimientos 300 y 700. De esta forma, estas instrucciones 902 transforman la máquina genera no programada en una máquina particular programada para llevar a cabo las funciones descritas e ilustradas de la forma descrita en la presente memoria. La máquina 900 puede operar como un dispositivo autónomo o puede acoplarse (por ejemplo, en red) con otras máquinas.

A modo de ejemplo no limitante, la máquina 900 puede comprender o corresponderse con una televisión, un ordenador (por ejemplo, un ordenador servidor, un ordenador cliente, un ordenador personal (PC), un ordenador de tipo tableta, un ordenador de sobremesa o un ordenador súper portátil de red), un decodificador (STB), un asistente personal digital (PDA), un sistema multimedia de entretenimiento (por ejemplo, un receptor de audio/vídeo), un teléfono móvil, un teléfono inteligente, un dispositivo móvil, un dispositivo que se puede llevar puesto (por ejemplo, un reloj inteligente), un reproductor multimedia portátil o cualquier máquina con capacidad para emitir señales de audio y con capacidad para ejecutar las instrucciones 902, secuencialmente o de otra forma, que especifican las acciones que han de ser emprendidas por la máquina 900. Además, aunque solo se ilustra una única máquina 900, también se interpretará que el término “máquina” incluye una colección de máquinas 900 que ejecutan, individual o conjuntamente, las instrucciones 902 para llevar a cabo una cualquiera o más de las metodologías expuestas en la presente memoria.

La máquina 900 puede incluir procesadores 904, una memoria 906, una unidad 908 de almacenamiento y/o componentes 910 de I/O, que pueden estar configurados para comunicarse entre sí, tal como mediante un *bus* 912. En una realización ejemplar, los procesadores 904 (por ejemplo, una unidad central de procesamiento (CPU), un procesador de ordenador con juego reducido de instrucciones (RISC), un procesador de ordenador con juego completo de instrucciones (CISC), una unidad de procesamiento gráfico (GPU), un procesador de señales digitales (DSP), un circuito integrado para aplicaciones específicas (ASIC), un circuito integrado de radiofrecuencia (RFIC),

otro procesador, o cualquier combinación adecuada de los mismos) pueden incluir, por ejemplo, el procesador 914 y el procesador 916 que pueden ejecutar instrucciones 902. Se concibe que el término “procesador” incluya procesadores de múltiples núcleos que pueden comprender dos o más procesadores independientes (denominados a veces “núcleos”) que pueden ejecutar instrucciones simultáneamente. Aunque la FIG. 9 muestra múltiples procesadores, la máquina 900 puede incluir un único procesador con un único núcleo, un único procesador con múltiples núcleos (por ejemplo, un procesador de múltiples núcleos), múltiples procesadores con un único núcleo, múltiples procesadores con múltiples núcleos o cualquier combinación de los mismos.

Tanto la memoria 906 (por ejemplo, una memoria principal u otro almacenamiento de memoria) como la unidad 908 de almacenamiento son accesibles a los procesadores 904, tal como mediante el *bus* 912. La memoria 906 y la unidad 908 de almacenamiento almacenan las instrucciones 902 que implementan una cualquiera o más de las metodologías o funciones descritas en la presente memoria. En algunas realizaciones, la base 112 de datos de recursos reside en la unidad 908 de almacenamiento. Las instrucciones 902 también pueden residir, completa o parcialmente, en la memoria 906, en la unidad 908 de almacenamiento, en al menos uno de los procesadores 904 (por ejemplo, en la memoria de almacenamiento temporal del procesador), o en cualquier combinación de los mismos, durante la ejecución de las mismas por medio de la máquina 900. En consecuencia, la memoria 906, la unidad 908 de almacenamiento y la memoria de los procesadores 904 son ejemplos de soportes legibles por una máquina.

Según se utiliza en la presente memoria, “soporte legible por una máquina” significa un dispositivo con capacidad para almacenar instrucciones y datos temporal o permanentemente y puede incluir, sin limitación, memoria de acceso aleatorio (RAM), memoria de solo lectura (ROM), memoria de almacenamiento intermedio, memoria *flash,* soportes ópticos, soportes magnéticos, memoria de almacenamiento temporal, otros tipos de almacenamiento (por ejemplo, memoria de solo lectura borrable y programable (EEPROM)) o cualquier combinación adecuada de los mismos. Se debería interpretar que la expresión “soporte legible por una máquina” incluye un único soporte o múltiples soportes (por ejemplo, una base de datos centralizada o distribuida o memorias de almacenamiento temporal y servidores asociados) con capacidad para almacenar instrucciones 902. También se debe interpretar que la expresión “soporte legible por una máquina” incluya cualquier soporte, o combinación de múltiples soportes, que es capaz de almacenar instrucciones (por ejemplo, instrucciones 902) para su ejecución por una máquina (por ejemplo, la máquina 900), de forma que las instrucciones, cuando son ejecutadas por uno o más procesadores de la máquina 900 (por ejemplo, los procesadores 904), provoquen que la máquina 900 lleve a cabo una cualquiera o más de las metodologías descritas en la presente memoria (por ejemplo, los procedimientos 300 y 700). En consecuencia, un “soporte legible por una máquina” hace referencia a un único aparato o dispositivo de almacenamiento, al igual que a sistemas de almacenamiento o redes de almacenamiento “basados en la nube” que incluyen múltiples aparatos o dispositivos de almacenamiento. La expresión “soporte legible por una máquina” excluye las señales *per se*.

Además, el “soporte legible por una máquina” es no transitorio, porque no implementa una señal de propagación. Sin embargo, no se interpretará que la calificación del soporte tangible legible por una máquina como “no transitorio” signifique que el soporte no tenga capacidad de movimiento - se debería considerar que el soporte es transportable desde una ubicación física hasta otra -. Adicionalmente, dado que el soporte legible por una máquina es tangible, se puede considerar que el soporte es un dispositivo legible por una máquina.

Los componentes 910 de I/O pueden incluir una amplia variedad de componentes para recibir una entrada, proporcionar una salida, producir una salida, transmitir información, intercambiar información, capturar mediciones, etcétera. Los componentes específicos 910 de I/O que se incluyen en una máquina particular dependerán del tipo de máquina. Por ejemplo, las máquinas portátiles tales como los teléfonos móviles probablemente incluirán un dispositivo de entrada táctil u otro mecanismo tal de entrada, mientras que una máquina servidora sin monitor probablemente no incluirá tal dispositivo de entrada táctil. Se apreciará que los componentes 910 de I/O pueden incluir muchos otros componentes que no se muestran específicamente en la FIG. 9. Los componentes 910 de I/O están agrupados según la funcionalidad simplemente para simplificar la siguiente exposición y la agrupación no es limitante de ninguna forma. En diversas realizaciones ejemplares, los componentes 910 de I/O pueden incluir componentes 918 de entrada y componentes 920 de salida. Los componentes 918 de entrada pueden incluir componentes de entrada alfanumérica (por ejemplo, un teclado, una pantalla táctil configurada para recibir una entrada alfanumérica, un teclado fotoóptico u otros componentes de entrada alfanumérica), componentes de entrada basados en puntero (por ejemplo, un ratón, una almohadilla táctil, un mando de bola, una palanca de mando, un sensor de movimiento u otro instrumento de puntero), componentes de entrada táctil (por ejemplo, un botón físico, una pantalla táctil que proporciona la ubicación y/o la fuerza del contacto o gestos táctiles u otros componentes de entrada táctil), componentes de entrada de audio y similares. Los componentes 920 de salida pueden incluir componentes visuales (por ejemplo, un medio de visualización tal como un panel de pantalla de plasma (PDP), un medio de visualización de diodos emisores de luz (LED), una pantalla de cristal líquido (LCD), un proyector o un tubo de rayos catódicos (CRT), componentes acústicos (por ejemplo, altavoces), componentes hápticos (por ejemplo, un motor vibratorio, mecanismos de resistencia), otros generadores de señales, etcétera.

La comunicación puede implementarse utilizando una amplia variedad de tecnologías. Los componentes 910 de I/O pueden incluir componentes 922 de comunicaciones operables para acoplar la máquina 900 con una red 924 o con

dispositivos 926 mediante el acoplamiento 928 y el acoplamiento 930, respectivamente. Por ejemplo, los componentes 922 de comunicaciones pueden incluir un componente de interfaz de red u otro dispositivo adecuado para interconectarse con la red 924. En ejemplos adicionales, los componentes 922 de comunicaciones pueden incluir componentes de comunicaciones alámbricas, componentes de comunicaciones inalámbricas, componentes de comunicaciones celulares, componentes de comunicaciones de campo cercano (NFC), componentes de Bluetooth® de baja energía), componentes de WiFi® y otros componentes de comunicaciones para proporcionar una comunicación mediante otras modalidades. Los dispositivos 926 pueden ser otra máquina o cualquiera de una amplia variedad de dispositivos periféricos (por ejemplo, un dispositivo periférico acoplado mediante un *bus* serie universal (USB)).

Módulos, componentes y lógica

En la presente memoria se describe que ciertas realizaciones incluyen lógica o un número de componentes, módulos o mecanismos. Los módulos pueden constituir bien módulos de soporte lógico (por ejemplo, código implementado en un soporte legible por una máquina o en una señal de transmisión) o bien módulos de soporte físico. Un módulo de soporte físico es una unidad tangible con capacidad para llevar a cabo ciertas operaciones y puede estar configurada o dispuesta de cierta forma. En realizaciones ejemplares, uno o más sistemas de ordenador (por ejemplo, un sistema de ordenador autónomo, cliente o servidor) o uno o más módulos de soporte físico de un sistema de ordenador (por ejemplo, un procesador o un grupo de procesadores) pueden estar configurados por soporte lógico (por ejemplo, una aplicación o una porción de aplicación) como un módulo de soporte físico que opera para llevar a cabo ciertas operaciones según se describe en la presente memoria.

En diversas realizaciones, se puede implementar un módulo de soporte físico mecánica o electrónicamente. Por ejemplo, un módulo de soporte físico puede comprender circuitería o lógica dedicada que está configurada permanentemente (por ejemplo, como un procesador de uso especial, tal como una matriz de puertas de campo programable (FPGA) o un circuito integrado para aplicaciones específicas (ASIC)) para llevar a cabo ciertas operaciones. Un módulo de soporte físico también puede comprender lógica o circuitería programable (por ejemplo, que abarque un procesador de uso general u otro procesador programable) que está configurada temporalmente por soporte lógico para llevar a cabo ciertas operaciones. Se apreciará que la decisión puede implementar un módulo de soporte físico mecánicamente, en circuitería dedicada y configurada permanentemente, o en circuitería configurada temporalmente (por ejemplo, configurada por soporte lógico) puede verse influida por consideraciones de coste y de tiempo.

En consecuencia, se debería entender que la expresión “módulo de soporte físico” abarque una entidad tangible, ya sea una entidad que está construida físicamente, configurada permanentemente (por ejemplo, cableada) o configurada temporalmente (por ejemplo, programada) para operar de cierta forma y/o para llevar a cabo ciertas operaciones descritas en la presente memoria. Considerando realizaciones en las que los módulos de soporte físico están configurados temporalmente (por ejemplo, programados), cada uno de los módulos de soporte físico no necesita estar configurado o ejemplificado en un momento cualquiera en el tiempo. Por ejemplo, cuando los módulos de soporte físico comprenden un procesador de uso general configurado utilizando soporte lógico, el procesador de uso general puede estar configurado como módulos respectivos distintos de soporte físico en distintos momentos. El soporte lógico puede configurar, en consecuencia, un procesador, por ejemplo, para constituir un módulo particular de soporte físico en un momento en el tiempo y para constituir un distinto módulo de soporte físico en un distinto momento en el tiempo.

Los módulos de soporte físico pueden proporcionar información a otros módulos de soporte físico, y recibir información de los mismos. En consecuencia, se puede considerar que los módulos descritos de soporte físico pueden estar acoplados de forma comunicativa. Cuando existen simultáneamente múltiples de tales módulos de soporte físico, las comunicaciones pueden lograrse mediante una transmisión de señales (por ejemplo, a través de circuitos y *buses* apropiados que conectan los módulos de soporte físico). En realizaciones en las que múltiples módulos de soporte físico están configurados o ejemplificados en distintos momentos, se pueden lograr comunicaciones entre tales módulos de soporte físico, por ejemplo, mediante el almacenamiento y la recuperación de información en estructuras de memoria a las que tienen acceso los múltiples módulos de soporte físico. Por ejemplo, un módulo de soporte físico puede llevar a cabo una operación y almacenar la salida de esa operación en un dispositivo de memoria con el que está acoplado de forma comunicativa. Entonces, un módulo adicional de soporte físico puede, en un momento posterior, acceder al dispositivo de memoria para recuperar y procesar la salida almacenada. Los módulos de soporte físico también pueden iniciar comunicaciones con dispositivos de entrada o de salida, y pueden operar sobre un recurso (por ejemplo, una lista de información).

Las diversas operaciones de los procedimientos ejemplares descritos en la presente memoria pueden llevarse a cabo, al menos parcialmente, por medio de uno o más procesadores que están configurados temporalmente (por ejemplo, mediante soporte lógico) o configurados permanentemente para llevar a cabo operaciones relevantes. Tanto si están configurados temporal como permanentemente, tales procesadores pueden constituir módulos implementados por procesador que operan para llevar a cabo una o más operaciones o funciones. Los módulos a los que se hace referencia en la presente memoria pueden comprender, en algunas realizaciones ejemplares, módulos implementados por procesador.

De forma similar, los procedimientos descritos en la presente memoria pueden ser implementados, al menos parcialmente, mediante procesador. Por ejemplo, al menos algunas de las operaciones de un procedimiento pueden ser llevadas a cabo por medio de uno o más procesadores o de módulos implementados por procesador. El desempeño de ciertas de las operaciones puede distribuirse entre los uno o más procesadores, que no solo residen en una única máquina, sino que se despliegan en un número de máquinas. En algunas realizaciones ejemplares, el procesador o los procesadores pueden estar localizados en una única ubicación (por ejemplo, en un entorno doméstico, un entorno de oficina o una granja de servidores), mientras que en otras realizaciones los procesadores pueden distribuirse en un número de ubicaciones.

Los uno o más procesadores también pueden operar apoyando el desempeño de las operaciones relevantes en un entorno "informático en la nube" o como un "soporte lógico como servicio" (SaaS). Por ejemplo, al menos algunas de las operaciones pueden ser llevadas a cabo por medio de un grupo de ordenadores (como ejemplos de máquinas que incluyen procesadores), siendo estas operaciones accesibles mediante una red (por ejemplo, Internet) y mediante una o más interfaces apropiadas (por ejemplo, API).

Aparato y sistema electrónico

Se pueden implementar realizaciones ejemplares en circuitería electrónica digital, o en soporte físico de ordenador, en soporte lógico inalterable o en soporte lógico o en combinaciones de los mismos. Se pueden implementar realizaciones ejemplares utilizando un producto de programa de ordenador, por ejemplo, un programa de ordenador implementado de forma tangible en un transportador de información, por ejemplo, en un soporte legible por una máquina para ser ejecutado por un aparato de procesamiento de datos, o para controlar la operación del mismo, por ejemplo, un procesador programable, un ordenador o múltiples ordenadores.

Se puede escribir un programa de ordenador en cualquier forma de lenguaje de programación, incluyendo lenguajes compilado o interpretado, y puede desplegarse en cualquier forma, incluyendo como un programa autónomo o como un módulo, subrutina u otra unidad adecuada para ser utilizado en un entorno informático. Se puede desplegar un programa de ordenador para que sea ejecutado en un ordenador o en múltiples ordenadores en un sitio, o distribuido en múltiples sitios e interconectados por una red de comunicaciones.

En realizaciones ejemplares, las operaciones pueden llevarse a cabo por medio de uno o más procesadores programables que ejecutan un programa de ordenador para llevar a cabo funciones operando en datos introducidos y generando una salida. Las operaciones del procedimiento también pueden ser llevadas a cabo por medio de circuitería lógica de uso especial (por ejemplo, una FPGA o un ASIC), y un aparato de realizaciones ejemplares puede implementarse como tal.

El sistema informático puede incluir clientes y servidores. Un cliente y un servidor son generalmente remotos entre sí y, normalmente, interactúan mediante una red de comunicaciones. La relación cliente-servidor surge gracias a programas de ordenador que se ejecutan en los ordenadores respectivos y que tienen una relación de cliente-servidor entre sí. En realizaciones que despliegan un sistema informático programable, se apreciará que arquitecturas tanto de soporte físico como de soporte lógico merecen consideración. Específicamente, se apreciará que la elección de si implementar cierta funcionalidad en soporte físico confirmado permanentemente (por ejemplo, un ASIC), en soporte físico configurado temporalmente (por ejemplo, una combinación de soporte lógico y de un procesador programable) o en una combinación de soporte físico configurado permanentemente y temporalmente puede ser una elección de diseño. A continuación se definen arquitecturas de soporte físico (por ejemplo, una máquina) y de soporte lógico que pueden desplegarse en diversas realizaciones ejemplares.

Realizaciones ejemplares enumeradas

Las realizaciones de la presente invención se ejemplifican mediante las siguientes realizaciones ejemplares enumeradas (EEE):

EEE 1: Un procedimiento que comprende: recibir, procedente de una aplicación de red, una solicitud de acceso a un recurso de datos almacenado en una primera base de datos de red, incluyendo la solicitud de acceso un identificador de recurso y un identificador de usuario, identificando el identificador de recurso el recurso de datos, identificando el identificador de usuario un usuario de la aplicación de red; en respuesta a la recepción de la solicitud de acceso, procedente de una segunda base de datos de red, un objeto de directrices asociado con el recurso de datos utilizando el identificador de recurso, incluyendo el objeto de directrices una frase de órdenes, incluyendo la frase de órdenes una operación que puede llevarse a cabo con respecto al recurso de datos en función del cumplimiento de una o más condiciones; evaluar, utilizando un procesador de soporte físico, un permiso de acceso del usuario con respecto al recurso de datos en función de si se cumplen las una o más condiciones incluidas en el registro de directrices; y comunicar, a la aplicación de red, una respuesta a la solicitud de acceso, incluyendo la respuesta a la solicitud de acceso el permiso de acceso del usuario con respecto al recurso de datos.

EEE 2: El procedimiento de la EEE 1, que comprende, además: proporcionar, a un dispositivo cliente, una interfaz de usuario para registrar unas directrices, incluyendo la interfaz de usuario uno o más campos de entrada para recibir un registro de directrices; recibir, procedente del dispositivo cliente, un registro de directrices asociado con un recurso adicional de datos almacenado en la primera base de datos de red, incluyendo el registro de directrices un

identificador adicional de recurso y una pluralidad de frases de órdenes, identificando el identificador adicional de recurso el recurso adicional de datos, incluyendo cada una de la pluralidad de frases de órdenes de permisos una condición y una operación; y registrar unas directrices asociadas con el recurso adicional de datos en función del registro de directrices.

EEE 3: El procedimiento de la EEE 2, en el que el registro de las directrices incluye la creación y el almacenamiento, en la segunda base de datos de red, un objeto adicional de directrices asociado con el recurso adicional de datos.

EEE 4: El procedimiento de la EEE 3, en el que: el recurso adicional de datos depende del recurso de datos; y el objeto adicional de directrices incluye una estructura de datos que comprende un gráfico jerárquico de recursos que representa una dependencia del recurso adicional de datos del recurso de datos.

EEE 5: El procedimiento de la EEE 4, en el que el registro de las directrices incluye aplicar las directrices al recurso de datos modificando unas directrices eficaces asociadas con el recurso de datos para que incluya al menos una porción de la pluralidad de frases de órdenes incluidas en las directrices asociadas con el recurso adicional de datos.

EEE 6: El procedimiento de cualquiera de las EEE 1-5, en el que la solicitud de acceso es recibida procedente de una aplicación de red incluida en un paquete de aplicaciones de red, compartiendo el paquete de aplicaciones de red el acceso a la primera base de datos de red.

EEE 7: El procedimiento de la EEE 6, en el que el objeto de directrices incluye una pluralidad de frases de órdenes que incluye la frase de órdenes, definiendo al menos una frase de órdenes de la pluralidad de frases de órdenes una condición para permitir o denegar al usuario llevar a cabo una operación para una aplicación específica asociada con una aplicación particular de red entre el paquete de aplicaciones de red.

EEE 8: El procedimiento de la EEE 7, en el que la pluralidad de frases de órdenes incluye al menos una seleccionado del grupo que comprende: una primera frase de órdenes que concede al usuario permiso para llevar a cabo una primera operación en función del cumplimiento de una primera condición; una segunda frase de órdenes que deniega al usuario permiso para llevar a cabo una segunda operación en función del cumplimiento de una segunda condición; una tercera frase de órdenes que invalida el permiso de acceso concedido por una cuarta frase de órdenes; o una quinta frase de órdenes que invalida el permiso de acceso denegado por una sexta frase de órdenes.

EEE 9: El procedimiento de cualquiera de las EEE 1-8, que comprende, además: crear un registro de operaciones de la solicitud de acceso, incluyendo el registro de operaciones un identificador de la aplicación de red, el identificador de usuario, el permiso de acceso del usuario y un sello de tiempo; y almacenar el registro de operaciones de la solicitud de acceso en una tercera base de datos de red.

EEE 10: El procedimiento de cualquiera de las EEE 1-9, en el que: las una o más condiciones incluyen un identificador permitido de usuario, y el cumplimiento de las una o más condiciones se basa en que el identificador de usuario se corresponda con el identificador permitido de usuario.

EEE 11: El procedimiento de cualquiera de las EEE 1-10, en el que: las una o más condiciones incluyen una condición temporal que especifica un intervalo de tiempo, y el cumplimiento de las una o más condiciones se basa en que se reciba la solicitud de acceso durante el intervalo de tiempo.

EEE 12: El procedimiento de cualquiera de las EEE 1-11, en el que el permiso de acceso incluye una operación que se autoriza que lleve a cabo el usuario sobre el recurso de datos utilizando la aplicación de red.

EEE 13: Un sistema que comprende: uno o más procesadores de una máquina; un primer soporte legible por una máquina que almacena una pluralidad de objetos de directrices asociados con una pluralidad de recursos de datos, siendo la pluralidad de recursos de datos almacenados en una base de datos de red objeto de acceso por una o más aplicaciones de red alojadas en uno o más servidores; y un segundo soporte legible por una máquina que almacena instrucciones que, cuando son ejecutadas por los uno o más procesadores de la máquina, provocan que la máquina lleve a cabo operaciones que comprenden: recibir, procedente de una aplicación de red de entre la pluralidad de aplicaciones de red, una solicitud de acceso a un recurso de datos de entre la pluralidad de recursos de datos almacenados en la base de datos de red, incluyendo la solicitud de acceso un identificador de recurso y un identificador de usuario, identificando el identificador de recurso el recurso de datos, identificando el identificador de usuario un usuario de la aplicación de red; en respuesta a la recepción de la solicitud de acceso, acceder, desde el primer soporte legible por una máquina, un objeto de directrices asociado con el recurso de datos utilizando el identificador de datos, incluyendo el objeto de directrices una frase de órdenes, incluyendo la frase de órdenes una operación que puede llevarse a cabo con respecto al recurso de datos en función del cumplimiento de una o más condiciones; evaluar un permiso de acceso del usuario con respecto al recurso de datos en función de si se cumplen las una o más condiciones incluidas en el registro de directrices; y comunicar, a la aplicación de red, una respuesta a

la solicitud de acceso, incluyendo la respuesta a la solicitud de acceso el permiso de acceso del usuario con respecto al recurso de datos.

EEE 14: El sistema de la EEE 13, en el que las operaciones comprenden, además: proporcionar, a un dispositivo cliente, una interfaz de usuario para registrar unas directrices, incluyendo la interfaz de usuario uno o más campos de entrada para recibir un registro de directrices; recibir, procedente del dispositivo cliente, un registro de directrices asociado con el recurso de datos, incluyendo el registro de directrices el identificador de recurso y una pluralidad de frases de órdenes adicionales; y registrar unas directrices asociadas con el recurso de datos en función del registro de directrices.

EEE 15: El sistema de la EEE 14, en el que el registro de las directrices incluye actualizar el objeto de directrices asociado con el recurso de datos para que incluya la pluralidad de frases de órdenes adicionales.

EEE 16: El sistema de la EEE 14 o de la EEE 15, en el que: un recurso derivado depende del recurso de datos, y el registro de las directrices incluye la actualización de unas directrices eficaces asociadas con el recurso derivado, actualizándose las directrices eficaces para que incluyan al menos una porción de la pluralidad de frases de órdenes adicionales.

EEE 17: El sistema de cualquiera de las EEE 13-16, en el que el objeto de directrices incluye una estructura de datos que comprende un gráfico jerárquico de recursos que representa una dependencia del recurso de datos en al menos un recurso adicional de datos.

EEE 18: El sistema de cualquiera de las EEE 13-17, en el que las operaciones comprenden, además: crear un registro de operaciones de la solicitud de acceso, incluyendo el registro de operaciones un identificador de la aplicación de red, el identificador de usuario, el permiso de acceso del usuario y un sello de tiempo; y almacenar el registro de operaciones de la solicitud de acceso en una tercera base de datos de red.

EEE 19: El sistema de cualquiera de las EEE 13-18, en el que: las una o más condiciones incluyen un identificador permitido de usuario, y el cumplimiento de las una o más condiciones se basa en que el identificador de usuario se corresponda con el identificador permitido de usuario.

EEE 20: Un soporte de almacenamiento legible por una máquina que implementa instrucciones que, cuando son ejecutadas por al menos un procesador de una máquina, provocan que la máquina lleve a cabo operaciones que comprenden: recibir, procedente de una aplicación de red alojada en un servidor, una solicitud de acceso a un recurso de datos almacenado en una primera base de datos de red, incluyendo la solicitud de acceso un identificador de recurso y un identificador de usuario, identificando el identificador de recurso el recurso de datos, identificando el identificador de usuario un usuario de la aplicación de red; en respuesta a la recepción de la solicitud de acceso, acceder, desde una segunda base de datos de red, un objeto de directrices asociado con el recurso de datos utilizando el identificador de recurso, incluyendo el objeto de directrices una frase de órdenes, incluyendo la frase de órdenes una operación que puede llevarse a cabo con respecto al recurso de datos en función del cumplimiento de una o más condiciones; evaluar un permiso de acceso del usuario con respecto al recurso de datos en función de si se cumplen las una o más condiciones incluidas en el registro de directrices; y comunicar, a la aplicación de red, una respuesta a la solicitud de acceso, incluyendo la respuesta a la solicitud de acceso el permiso de acceso del usuario con respecto al recurso de datos.

Lenguaje

Aunque se han descrito las realizaciones de la presente invención con referencia a realizaciones ejemplares específicas, será evidente que se pueden realizar diversos cambios y modificaciones a estas realizaciones sin alejarse del ámbito más amplio del contenido inventivo. En consecuencia, se deben considerar la memoria y los dibujos en un sentido ilustrativo en vez de restrictivo. Los dibujos adjuntos que forman una parte de la presente memoria muestran, a modo ilustrativo, y no limitante, realizaciones específicas en las que puede ponerse en práctica el contenido. Las realizaciones ilustradas se describen con suficiente detalle para permitir que los expertos en la técnica pongan en práctica las enseñanzas dadas a conocer en la presente memoria. Se pueden utilizar y deducir otras realizaciones a partir de las mismas, de forma que se puedan realizar sustituciones y cambios estructurales y lógicos sin alejarse del ámbito de la presente divulgación. Por lo tanto, no se debe interpretar la descripción detallada en un sentido limitante, y el ámbito de diversas realizaciones solo está definido por las reivindicaciones adjuntas, junto con la gama completa de equivalentes a los que tienen derecho tales reivindicaciones.

Se puede hacer referencia, en la presente memoria, a tales realizaciones del contenido inventivo, individual o colectivamente, mediante el término “invención” simplemente en aras de la conveniencia y sin pretender limitar voluntariamente el ámbito de la presente solicitud a cualquier invención o concepto inventivo individual si se divulga, de hecho, más de uno. Por lo tanto, aunque se han ilustrado y descrito en la presente memoria realizaciones específicas, se debería apreciar que las realizaciones específicas mostradas pueden ser sustituidas por cualquier disposición calculada para lograr el mismo fin. Se concibe que la presente divulgación abarque cualquier adaptación o variación de diversas realizaciones, y todas ellas. Combinaciones de las anteriores realizaciones, y otras

realizaciones no descritas específicamente en la presente memoria, serán evidentes para los expertos en la técnica, tras el análisis de la anterior descripción.

Todas las publicaciones, las patentes y los documentos de patente a los que se ha hecho referencia en el presente documento están incorporados por referencia en la presente memoria en su totalidad, como si estuviesen incorporados individualmente por referencia. En el caso de usos incoherentes entre este documento y esos documentos así incorporados por referencia, se debería considerar el uso en las referencias incorporadas es suplementario al del presente documento; para incoherencias irreconciliables, el uso en el presente documento es el que manda.

En el presente documento, se utilizan los términos “un” o “una”, como es habitual en documentos de patente, para que incluyan uno o más de uno, con independencia de cualquier otro caso o uso de “al menos uno” o “uno o más”. En el presente documento, se utiliza el término “o” para hacer referencia a una falta de exclusividad o, de forma que “A” o “B” incluya “A pero no B”, “B pero no A” y “A y B”, a no ser que se indique lo contrario. En las reivindicaciones adjuntas, se utilizan las expresiones “que incluye” y “en el que” como los equivalentes en español corriente de las expresiones respectivas “que comprende” y “en el cual”. Además, en las siguientes reivindicaciones, las expresiones “que incluye” y “que comprende” son no limitantes; es decir, se sigue considerando que un sistema, dispositivo, artículo o procedimiento que incluye elementos además de los enumerados después de tal expresión se encuentra dentro del ámbito de esa reivindicación.

REIVINDICACIONES

1. Un procedimiento que comprende:

recibir (705), procedente de una aplicación (109, 110, 111) de red, una solicitud de acceso a un recurso (500) de datos almacenado en una primera base (116) de datos de red, incluyendo la solicitud de acceso un identificador (504) de recurso y un identificador (406) de usuario, identificando el identificador (504) de recurso el recurso (500) de datos, identificando el identificador (406) de usuario un usuario de la aplicación (109, 110, 111) de red; en respuesta a la recepción de la solicitud de acceso, utilizar el identificador (504) de recurso incluido en la solicitud de acceso para acceder (710), desde una segunda base (206) de datos de red, a un objeto (502) de directrices vinculado al recurso (500) de datos, incluyendo el objeto (502) de directrices unas directrices eficaces (508) para el recurso (500) de datos, incluyendo las directrices eficaces (508) al menos una frase de órdenes (510, 5*n*0) que (i) incluye una operación (516, 5*n*6) que puede llevarse a cabo con respecto al recurso (500) de datos en función del cumplimiento de una o más condiciones (514, 5*n*4), (ii) es heredada de al menos un recurso precursor (602) de datos del que depende el recurso (500) de datos, y (iii) es almacenada en el objeto (508) de directrices para el recurso (500) de datos; evaluar (715), utilizando un procesador (916) de soporte físico, un permiso de acceso del usuario con respecto al recurso (500) de datos en función de, al menos en parte, si se cumplen las una o más condiciones (514, 5*n*4) incluidas en la al menos una frase de órdenes (510, 5*n*0); y

comunicar (720) a la aplicación (109, 110, 111) de red, una respuesta a la solicitud de acceso, la respuesta a la solicitud de acceso que incluye el permiso de acceso del usuario con respecto al recurso (500) de datos.

2. El procedimiento de la reivindicación 1, que comprende, además:

proporcionar, a un dispositivo cliente (118), una interfaz (400) de usuario para registrar unas directrices, incluyendo la interfaz (400) de usuario uno o más campos de entrada para recibir un registro de directrices;
recibir, procedente del dispositivo cliente (118), un registro de directrices asociado con un recurso adicional (602) de datos almacenado en la primera base (116) de datos de red, incluyendo el registro de directrices un identificador de recurso adicional y una pluralidad de frases de órdenes, identificando el identificador adicional de recurso el recurso adicional (602) de datos, incluyendo cada una de la pluralidad de frases de órdenes una condición y una operación; y

registrar unas directrices asociadas con el recurso adicional (602) de datos en función del registro de directrices.

3. El procedimiento de la reivindicación 2, en el que el registro de las directrices incluye la creación y el almacenamiento, en la segunda base (206) de datos de red, un objeto adicional de directrices asociado con el recurso adicional (602) de datos.

4. El procedimiento de la reivindicación 3, en el que:

el recurso (500) de datos depende del recurso adicional (602) de datos; y

el objeto adicional de directrices incluye una estructura de datos que comprende un gráfico jerárquico (600) de recursos que representa una dependencia del recurso (500) de datos con respecto al recurso adicional (602) de datos.

5. El procedimiento de la reivindicación 4, en el que el registro de las directrices incluye la aplicación de las directrices al recurso (500) de datos modificando las directrices eficaces (508) asociadas con el recurso (500) de datos para que incluya al menos una porción de la pluralidad de frases de órdenes (510, 5*n*0) incluidas en las directrices asociadas con el recurso adicional (602) de datos.

6. El procedimiento de cualquiera de las reivindicaciones 1-5, en el que la solicitud de acceso es recibida desde una aplicación (109, 110, 111) de red incluida en un paquete de aplicaciones (109, 110, 111) de red, compartiendo el paquete de aplicaciones (109, 110, 111) de red el acceso a la primera base (116) de datos de red.

7. El procedimiento de la reivindicación 6, en el que el objeto (502) de directrices incluye una pluralidad de frases de órdenes (510, 5*n*0) que incluyen la frase de órdenes (510, 5*n*0), definiendo al menos una frase de órdenes (510, 5*n*0) de la pluralidad de frases de órdenes (510, 5*n*0) una condición (514, 5*n*4) para permitir o denegar al usuario llevar a cabo una operación (516, 5*n*6) para aplicaciones específicas asociada con una aplicación particular (109, 110, 111) de red de entre el paquete de aplicaciones (109, 110, 111) de red.

8. El procedimiento de la reivindicación 7, en el que la pluralidad de frases de órdenes (510, 5*n*0) incluye al menos una seleccionada del grupo que comprende:

una primera frase de órdenes (510, 5*n*0) que concede al usuario permiso para llevar a cabo una primera operación (516, 5*n*6) en función del cumplimiento de una primera condición (514, 5*n*4);

una segunda frase de órdenes (510, 5*n*0) que deniega al usuario permiso para llevar a cabo una segunda operación (516, 5*n*6) en función del cumplimiento de una segunda condición (514, 5*n*4);

una tercera frase de órdenes (510, 5*n*0) que invalida el permiso de acceso concedido por una cuarta frase de órdenes (510, 5*n*0); o

una quinta frase de órdenes (510, 5*n*0) que invalida el permiso de acceso denegado por una sexta frase de órdenes (510, 5*n*0).

9. El procedimiento de cualquiera de las reivindicaciones 1-8,

que comprende, además:

crear (725) un registro (208) de operaciones de la solicitud de acceso, incluyendo el registro (208) de operaciones un identificador de la aplicación (109, 110, 111) de red, el identificador (406) de usuario, el permiso de acceso del usuario y un sello de tiempo; y

almacenar (730) el registro (208) de operaciones de la solicitud de acceso en una tercera base de datos de red;

y/o en el que:

las una o más condiciones (514, 5*n*4) incluyen un identificador permitido de usuario, y

el cumplimiento de las una o más condiciones (514, 5*n*4) se basa en que el identificador (406) de usuario se corresponda con el identificador permitido de usuario;

y/o en el que:

las una o más condiciones (514, 5*n*4) incluyen una condición temporal que especifica un intervalo de tiempo, y el cumplimiento de las una o más condiciones (514, 5*n*4) se basa en que la solicitud de acceso sea recibida en el intervalo de tiempo;

y/o en el que:

el permiso de acceso incluye una operación (516, 5*n*6) que se autoriza que el usuario lleve a cabo sobre el recurso (500) de datos utilizando la aplicación (109, 110, 111) de red.

10. Un sistema que comprende:

uno o más procesadores (916) de una máquina;

un primer soporte legible por una máquina que almacena una pluralidad de objetos (502) de directrices asociado con una pluralidad de recursos (500) de datos, almacenada la pluralidad de recursos (500) de datos en una base (116) de datos de red a la que acceden una o más aplicaciones (109, 110, 111) de red alojadas en uno o más servidores (106, 107, 108); y

un segundo soporte legible por una máquina que almacena instrucciones que, cuando son ejecutadas por los uno o más procesadores (916) de la máquina, provocan que la máquina lleve a cabo operaciones que comprenden:

recibir (705), procedente de una aplicación (109, 110, 111) de red de entre la pluralidad de aplicaciones (109, 110, 111) de red, una solicitud de acceso a un recurso (500) de datos de entre la pluralidad de recursos (500) de datos almacenados en la base (116) de datos de red, incluyendo la solicitud de acceso un identificador (504) de recurso y un identificador (406) de usuario, identificando el identificador (504) de recurso el recurso (500) de datos, identificando el identificador (406) de usuario un usuario de la aplicación (109, 110, 111) de red;

en respuesta a la recepción de la solicitud de acceso, utilizando el identificador (504) de recurso incluido en la solicitud de acceso para acceder (710), desde el primer soporte legible por una máquina, a un objeto (502) de directrices vinculado al recurso (500) de datos, incluyendo el objeto (502) de directrices unas directrices eficaces (508) para el recurso (500) de datos, incluyendo las directrices eficaces (508) al menos una frase de órdenes (510, 5*n*0) que (i) incluye una operación (516, 5*n*6) que puede llevarse a cabo con respecto al recurso (500) de datos en función del cumplimiento de una o más condiciones (514, 5*n*4), (ii) es heredada del al menos un recurso precursor (602) de datos del que depende el recurso (500) de datos, y (iii) es almacenada en el objeto (508) de directrices para el recurso (500) de datos;

evaluar (715) un permiso de acceso del usuario con respecto al recurso (500) de datos en función, al menos en parte, de si se cumplen las una o más condiciones (514, 5*n*4) incluidas en la al menos una frase de órdenes (510, 5*n*0); y

comunicar (720), a la aplicación (109, 110,111) de red, una respuesta a la solicitud de acceso, incluyendo la respuesta a la solicitud de acceso el permiso de acceso del usuario con respecto al recurso (500) de datos.

11. El sistema de la reivindicación 10, en el que las operaciones comprenden, además:

proporcionar, a un dispositivo cliente (118), una interfaz (400) de usuario para registrar unas directrices, incluyendo la interfaz (400) de usuario uno o más campos de entrada para recibir un registro de directrices;
recibir, procedente del dispositivo cliente (118), un registro de directrices asociado con el recurso (500) de datos, incluyendo el registro de directrices el identificador (504) de recurso y una pluralidad de frases de órdenes adicionales; y

registrar unas directrices asociadas con el recurso (500) de datos en función del registro de directrices.

12. El sistema de la reivindicación 11,

en el que:

el registro de las directrices incluye actualizar el objeto (502) de directrices asociado con el recurso (500) de datos para que incluya la pluralidad de frases de órdenes adicionales;

y/o en el que:

un recurso derivado (604) depende del recurso (500) de datos, y

el registro de las directrices incluye actualizar unas directrices eficaces asociadas con el recurso derivado (604), siendo actualizadas las directrices eficaces para que incluyan al menos una porción de la pluralidad de frases de órdenes adicionales.

13. El sistema de cualquiera de las reivindicaciones 10-12,

en el que:

el objeto (502) de directrices incluye una estructura de datos que comprende un gráfico jerárquico (600) de recursos que representa una dependencia del recurso (500) de datos del al menos un recurso adicional (602) de datos;

y/o en el que las operaciones comprenden, además:

crear (725) un registro (208) de operaciones de la solicitud de acceso, incluyendo el registro (208) de operaciones un identificador de la aplicación (109, 110, 111) de red, el identificador (406) de usuario, el permiso de acceso del usuario y un sello de tiempo; y

almacenar (730) el registro (208) de operaciones de la solicitud de acceso en una tercera base de datos de red;

y/o en el que:

las una o más condiciones (514, 5*n*4) incluyen un identificador permitido de usuario, y

el cumplimiento de las una o más condiciones (514, 5*n*4) se basa en que el identificador (406) de usuario se corresponda con el identificador permitido de usuario.

14. Un soporte de almacenamiento legible por una máquina que implementa instrucciones que, cuando son ejecutadas por al menos un procesador (916) de una máquina, provocan que la máquina lleve a cabo las operaciones que comprenden:

recibir (705), procedente de una aplicación (109, 110, 111) de red alojada en un servidor (106, 107, 108), una solicitud de acceso a un recurso (500) de datos almacenado en una primera base (116) de datos de red, incluyendo la solicitud de acceso un identificador (504) de recurso y un identificador (406) de usuario, identificando el identificador (504) de recurso el recurso (500) de datos, identificando el identificador (406) de usuario un usuario de la aplicación (109, 110, 111) de red;

en respuesta a la recepción de la solicitud de acceso, utilizar el identificador (504) de recurso incluido en la solicitud de acceso para acceder (710), desde una segunda base (206) de datos de red, a un objeto (502) de directrices vinculado al recurso (500) de datos, incluyendo el objeto (502) de directrices unas directrices eficaces (508) para el recurso (500) de datos, incluyendo las directrices eficaces (508) al menos una frase de órdenes (510, 5*n*0) que (i) incluye una operación (516, 5*n*6) que puede llevarse a cabo con respecto al recurso (500) de datos en función del cumplimiento de una o más condiciones (514, 5*n*4), (ii) es heredada del al menos un recurso precursor (602) de datos del que depende el recurso (500) de datos, y (iii) es almacenada en el objeto (508) de directrices para el

recurso (500) de datos; evaluar (715) un permiso de acceso del usuario con respecto al recurso (500) de datos en función, al menos en parte, de si se cumplen las una o más condiciones (514, 5*n*4) incluidas en la al menos una frase de órdenes (510, 5*n*0); y

comunicar (720), a la aplicación (109, 110, 111) de red, una respuesta a la solicitud de acceso, incluyendo la respuesta a la solicitud de acceso el permiso de acceso del usuario con respecto al recurso (500) de datos.

15. El soporte de almacenamiento legible por una máquina de la reivindicación 14, en el que las instrucciones, cuando son ejecutadas por el al menos un procesador (916), provocan, además, que la máquina lleve a cabo operaciones que comprenden las operaciones enumeradas en cualquiera de las reivindicaciones 2-9.

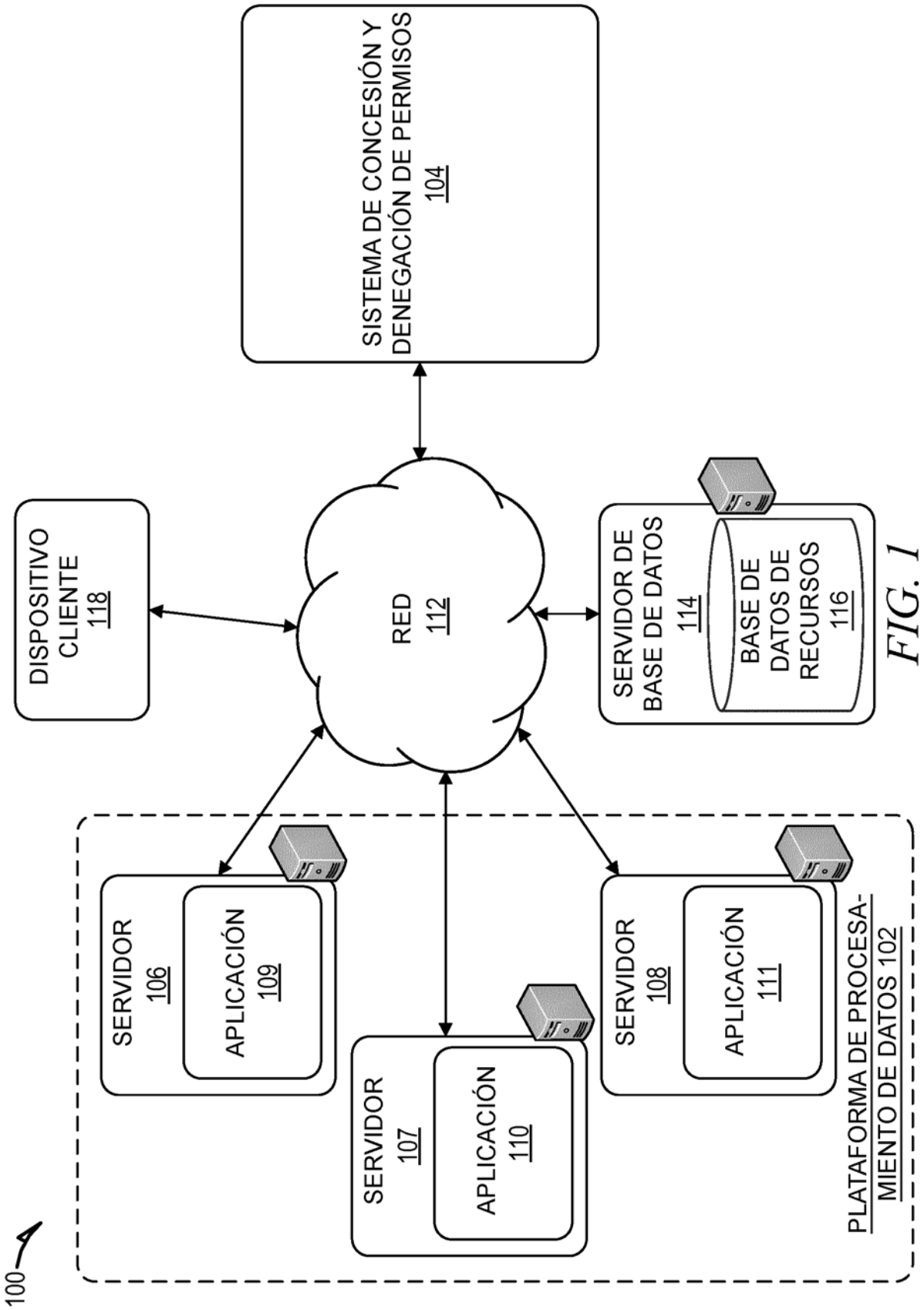
100
SISTEMA DE CONCESIÓN Y DENEGACIÓN DE PERMISOS 104
DISPOSITIVO CLIENTE 118
RED 112
SERVIDOR DE BASE DE DATOS 114
BASE DE DATOS DE RECURSOS 116
SERVIDOR 106
APLICACIÓN 109
SERVIDOR 107
APLICACIÓN 110
SERVIDOR 108
APLICACIÓN 111
PLATAFORMA DE PROCESAMIENTO DE DATOS 102

FIG. 1

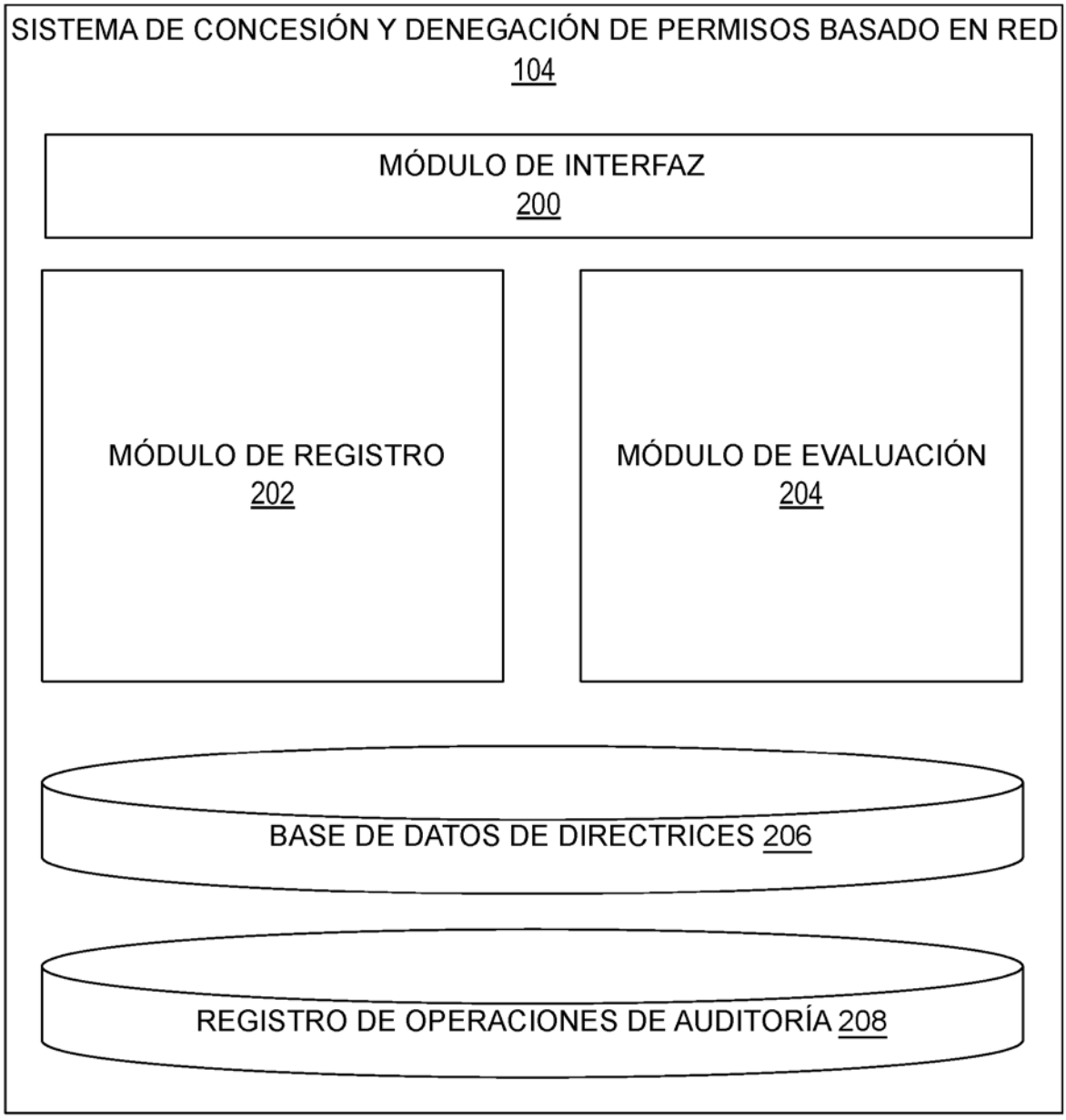
SISTEMA DE CONCESIÓN Y DENEGACIÓN DE PERMISOS BASADO EN RED
104
MÓDULO DE INTERFAZ
200
MÓDULO DE REGISTRO
202
MÓDULO DE EVALUACIÓN
204
BASE DE DATOS DE DIRECTRICES 206
REGISTRO DE OPERACIONES DE AUDITORÍA 208

FIG. 2

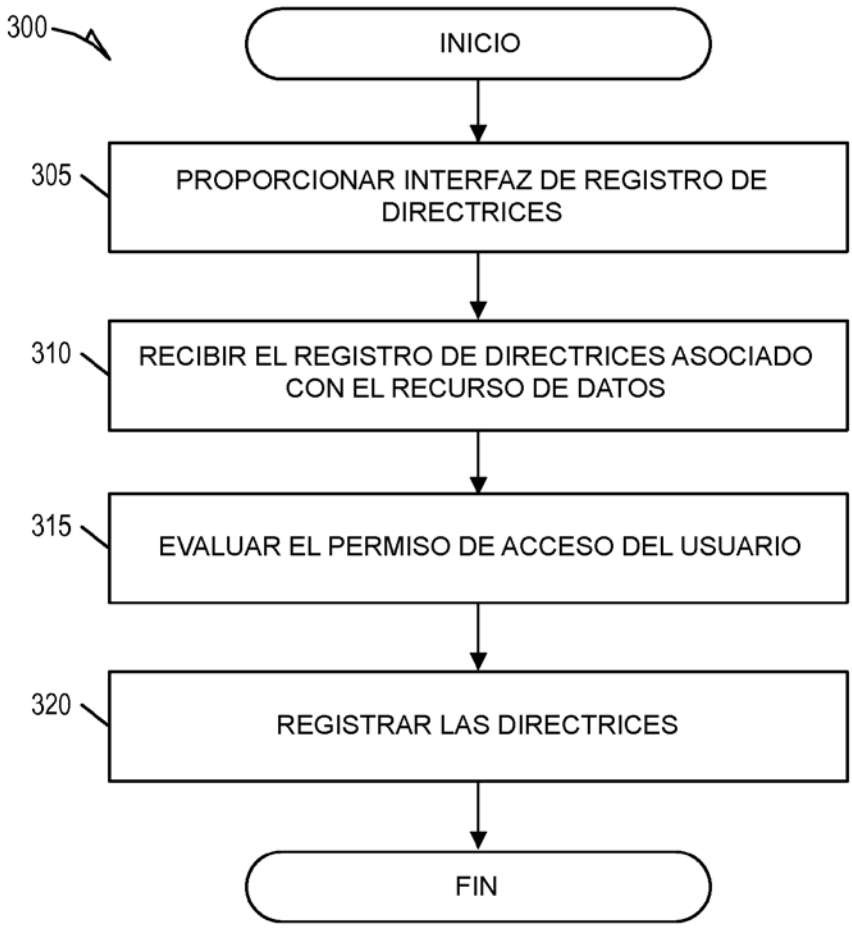
300
INICIO
305
PROPORCIONAR INTERFAZ DE REGISTRO DE DIRECTRICES
310
RECIBIR EL REGISTRO DE DIRECTRICES ASOCIADO CON EL RECURSO DE DATOS
315
EVALUAR EL PERMISO DE ACCESO DEL USUARIO
320
REGISTRAR LAS DIRECTRICES
FIN

FIG. 3

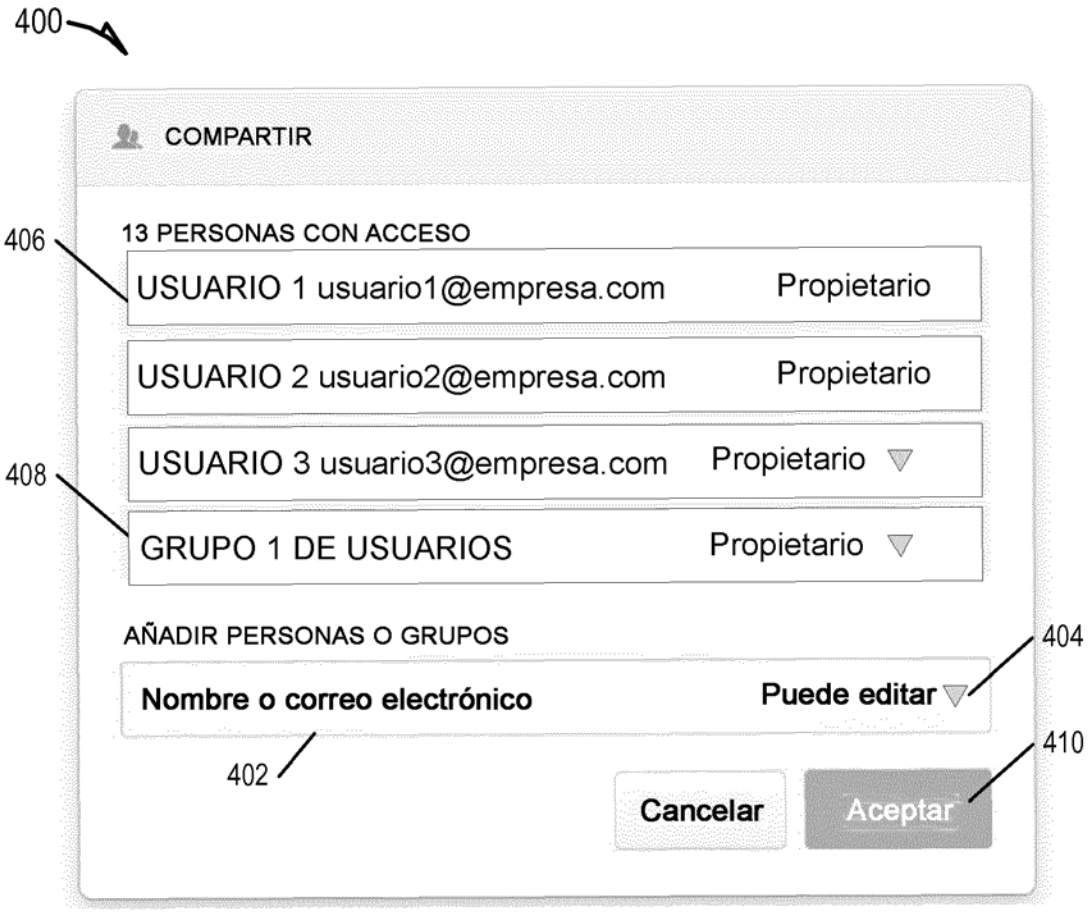
400
COMPARTIR
406
13 PERSONAS CON ACCESO
USUARIO 1 usuario1@empresa.com
Propietario
USUARIO 2 usuario2@empresa.com
Propietario
USUARIO 3 usuario3@empresa.com
Propietario
408
GRUPO 1 DE USUARIOS
Propietario
AÑADIR PERSONAS O GRUPOS
404
Nombre o correo electrónico
Puede editar
402
410
Cancelar
Aceptar

FIG. 4

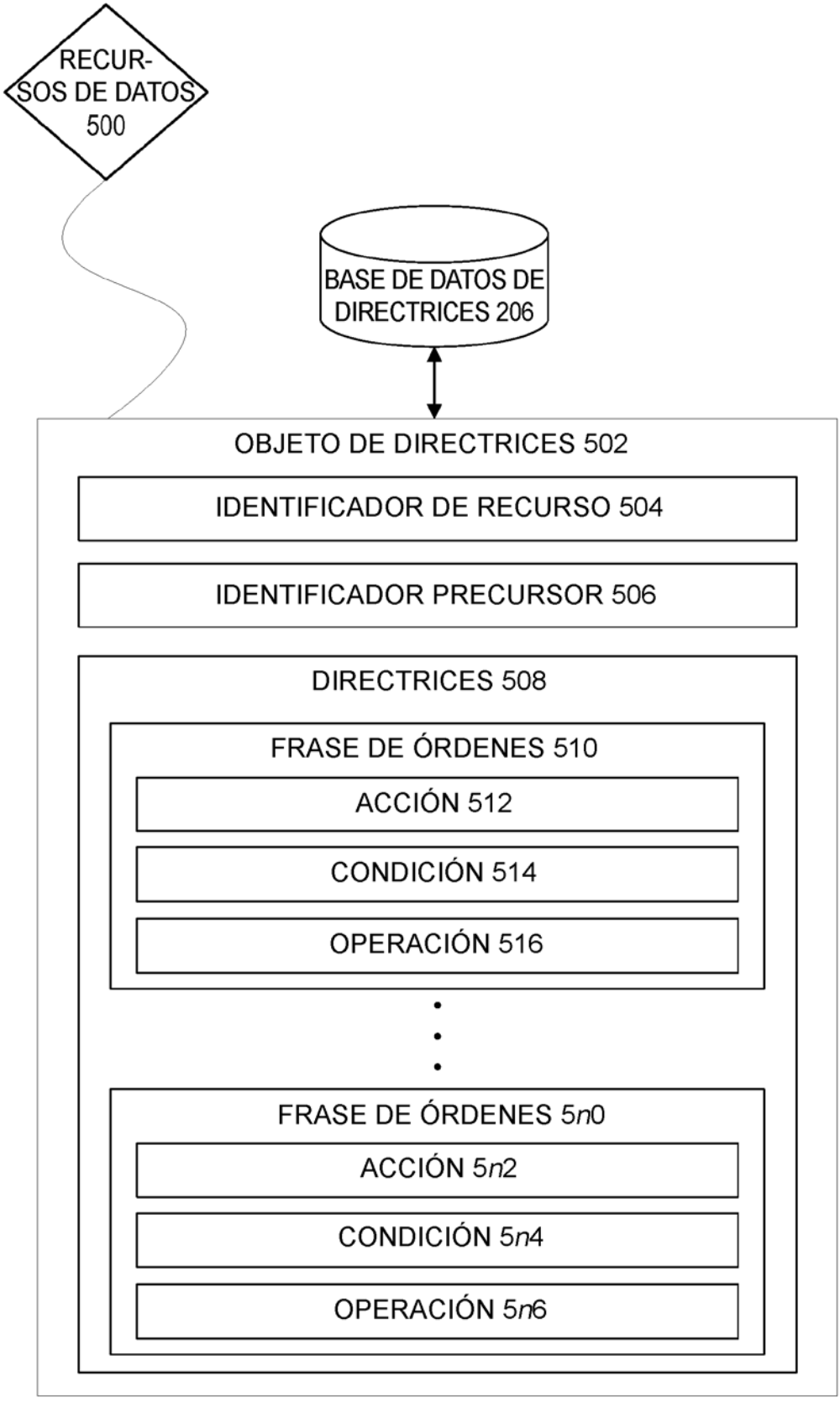
RECUR-
SOS DE DATOS
500
BASE DE DATOS DE
DIRECTRICES 206
OBJETO DE DIRECTRICES 502
IDENTIFICADOR DE RECURSO 504
IDENTIFICADOR PRECURSOR 506
DIRECTRICES 508
FRASE DE ÓRDENES 510
ACCIÓN 512
CONDICIÓN 514
OPERACIÓN 516
FRASE DE ÓRDENES 5n0
ACCIÓN 5n2
CONDICIÓN 5n4
OPERACIÓN 5n6

FIG. 5

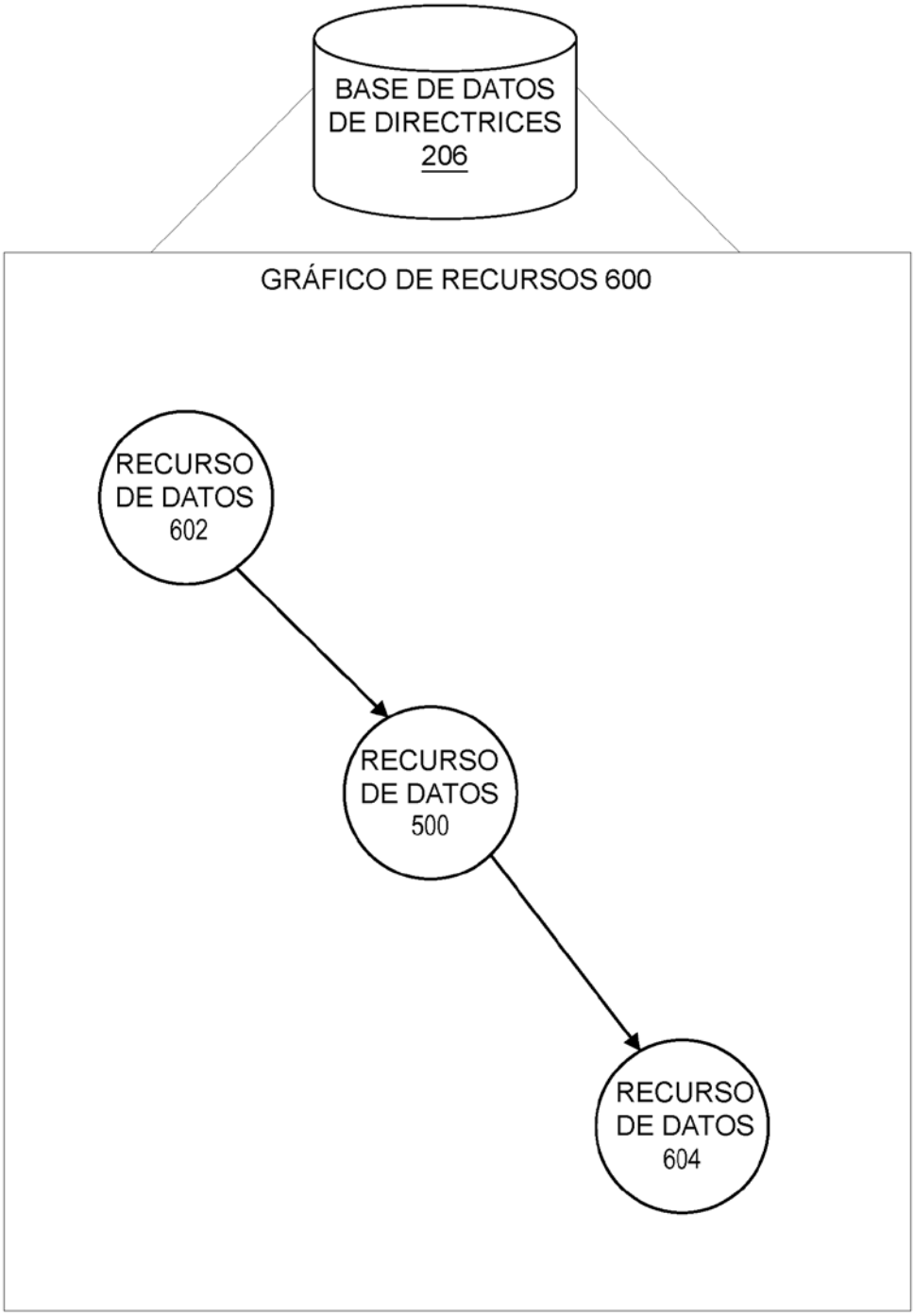
BASE DE DATOS
DE DIRECTRICES
206
GRÁFICO DE RECURSOS 600
RECURSO
DE DATOS
602
RECURSO
DE DATOS
500
RECURSO
DE DATOS
604

FIG. 6

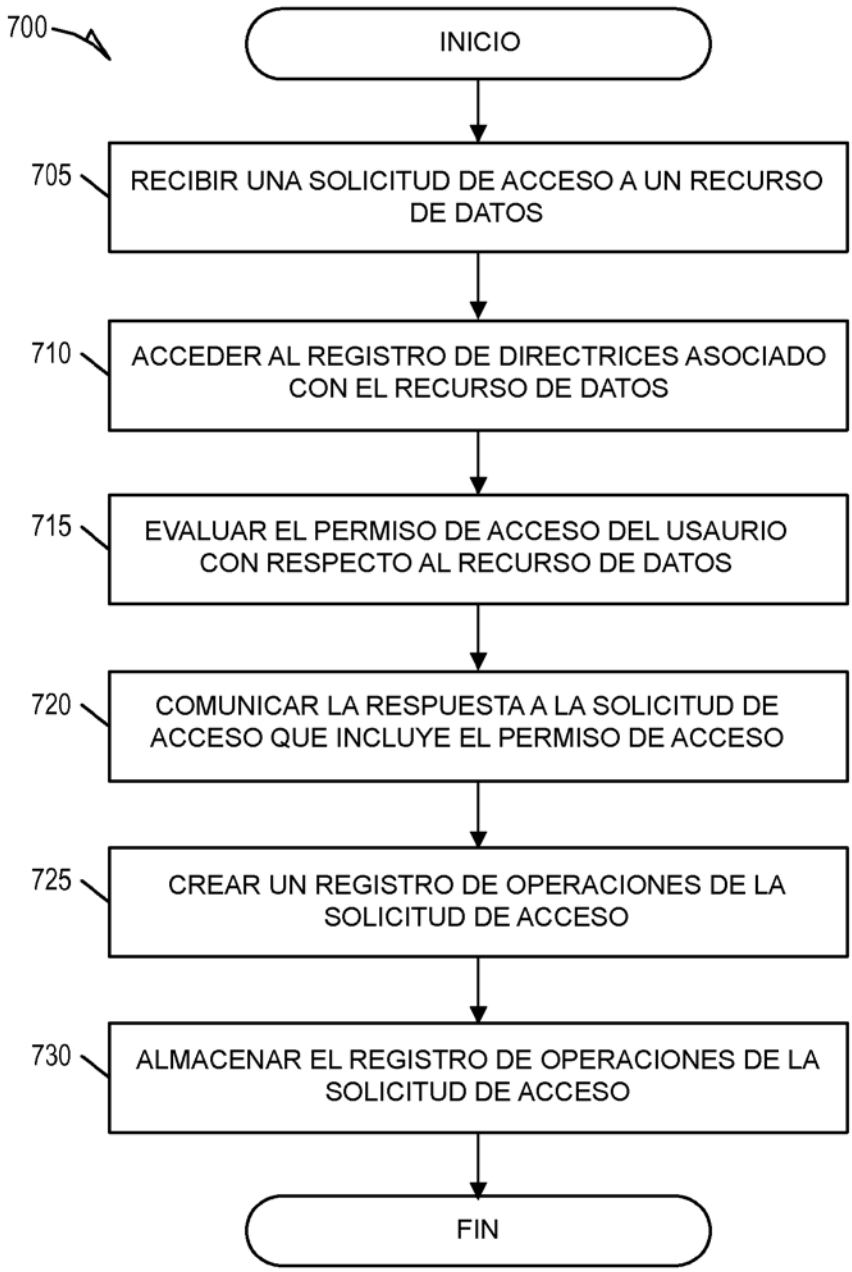
700
INICIO
705
RECIBIR UNA SOLICITUD DE ACCESO A UN RECURSO DE DATOS
710
ACCEDER AL REGISTRO DE DIRECTRICES ASOCIADO CON EL RECURSO DE DATOS
715
EVALUAR EL PERMISO DE ACCESO DEL USAURIO CON RESPECTO AL RECURSO DE DATOS
720
COMUNICAR LA RESPUESTA A LA SOLICITUD DE ACCESO QUE INCLUYE EL PERMISO DE ACCESO
725
CREAR UN REGISTRO DE OPERACIONES DE LA SOLICITUD DE ACCESO
730
ALMACENAR EL REGISTRO DE OPERACIONES DE LA SOLICITUD DE ACCESO
FIN

FIG. 7

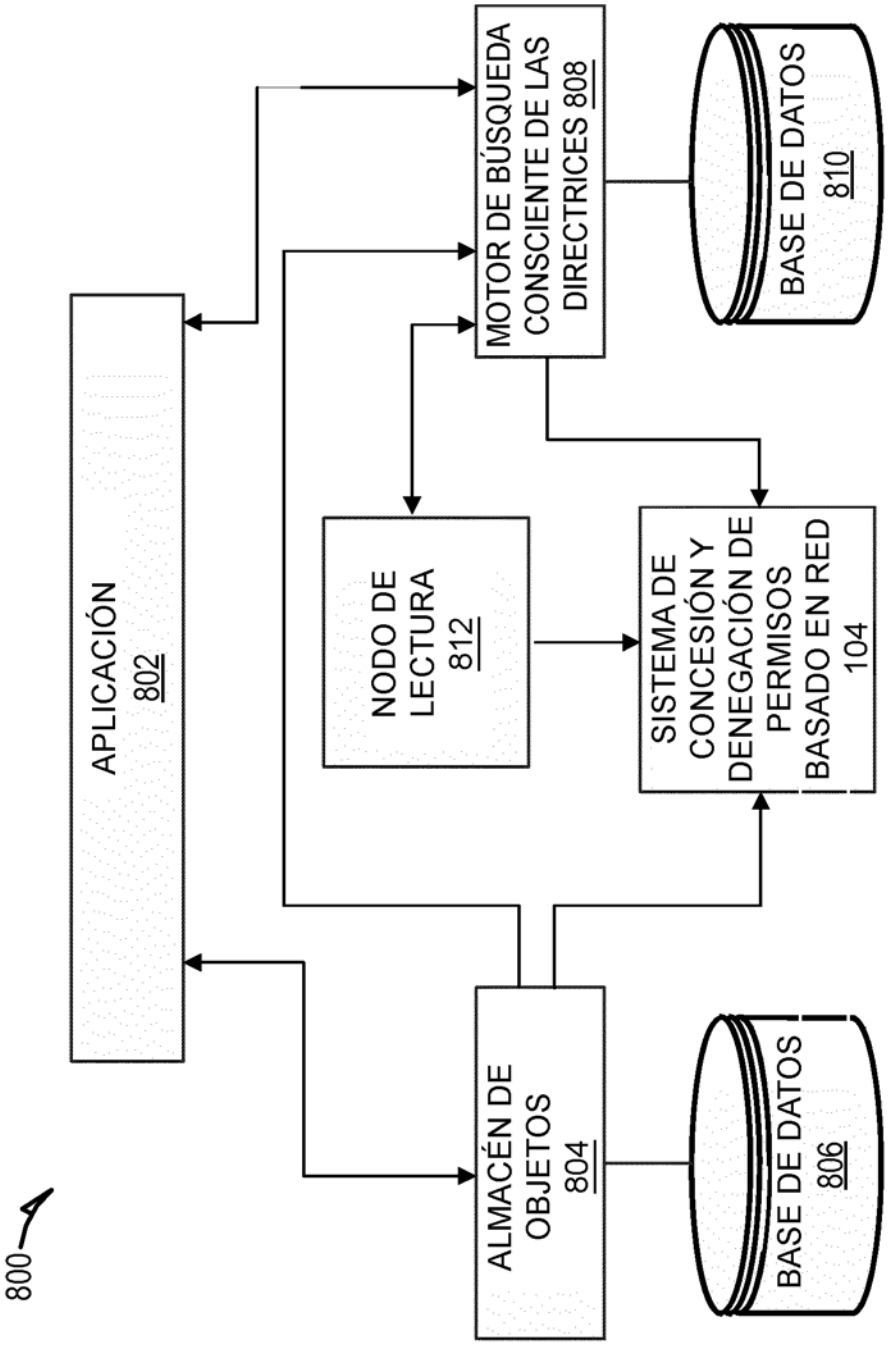
800
APLICACIÓN
802
MOTOR DE BÚSQUEDA CONSCIENTE DE LAS DIRECTRICES 808
BASE DE DATOS
810
NODO DE LECTURA
812
SISTEMA DE CONCESIÓN Y DENEGACIÓN DE PERMISOS BASADO EN RED
104
ALMACÉN DE OBJETOS
804
BASE DE DATOS
806

FIG. 8

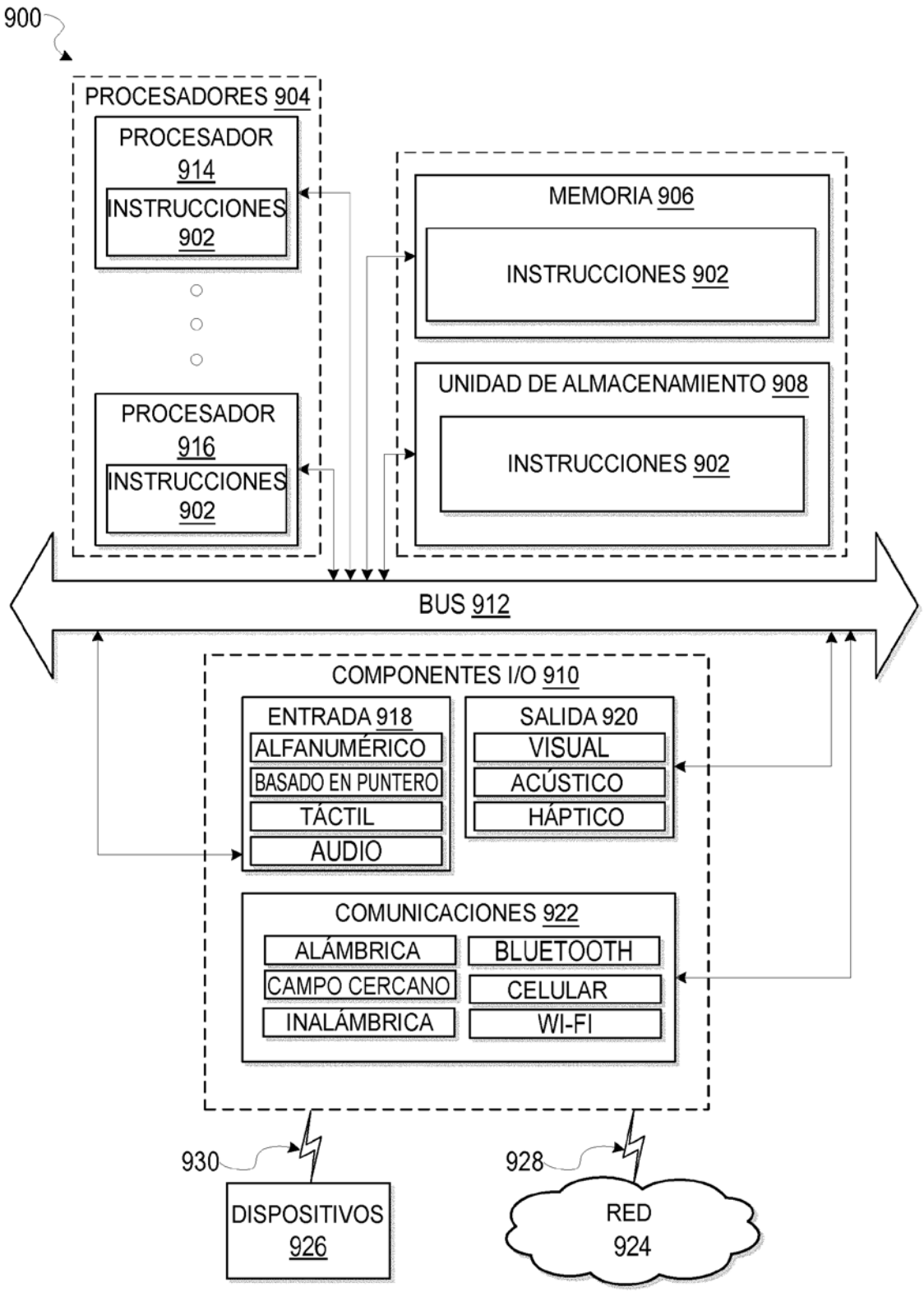
900
PROCESADORES 904
PROCESADOR 914
INSTRUCCIONES 902
PROCESADOR 916
INSTRUCCIONES 902
MEMORIA 906
INSTRUCCIONES 902
UNIDAD DE ALMACENAMIENTO 908
INSTRUCCIONES 902
BUS 912
COMPONENTES I/O 910
ENTRADA 918
ALFANUMÉRICO
BASADO EN PUNTERO
TÁCTIL
AUDIO
SALIDA 920
VISUAL
ACÚSTICO
HÁPTICO
COMUNICACIONES 922
ALÁMBRICA
CAMPO CERCANO
INALÁMBRICA
BLUETOOTH
CELULAR
WI-FI
930
DISPOSITIVOS 926
928
RED 924

FIG. 9