(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 733 433**

(51) Int. CI.:

***G06F 21/30*** (2013.01)
***G06F 21/60*** (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **17.08.2012 PCT/US2012/051491**

(87) Fecha y número de publicación internacional: **21.03.2013 WO13039649**

(96) Fecha de presentación y número de la solicitud europea: **17.08.2012 E 12832406 (8)**

(97) Fecha y número de publicación de la concesión europea: **10.04.2019 EP 2756445**

(54) Título: **Protección del uso de datos en dispositivos informáticos**

(30) Prioridad:

**15.09.2011 US 201113233032**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**29.11.2019**

(73) Titular/es:

**MICROSOFT TECHNOLOGY LICENSING, LLC (100.0%)**
**One Microsoft Way**
**Redmond, WA 98052, US**

(72) Inventor/es:

**BRENNAN, DAVID JOHN;**
**DESAI, ADITI y**
**RAMANATHAN, RAJESH**

(74) Agente/Representante:

**CARPINTERO LÓPEZ, Mario**

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

## DESCRIPCIÓN

Protección del uso de datos en dispositivos informáticos

**Antecedentes**

Recientes tendencias informáticas han mostrado un paso de ordenadores tradicionales de sobremesa a dispositivos informáticos móviles. Los dispositivos informáticos móviles, tales como ordenadores portátiles, pequeños ordenadores portátiles, tabletas y teléfonos móviles, proporcionan la conveniencia de portabilidad y de rendimiento que es capaz de ejecutar tareas habituales, incluyendo el correo electrónico, la navegación por Internet, el procesamiento de textos, la edición de fotografías, el consumo de contenidos, etcétera. Sin embargo, la naturaleza móvil de estos dispositivos plantea retos singulares en comparación con los ordenadores de sobremesa.

Los dispositivos informáticos móviles a menudo almacenan o permiten el acceso a datos sensibles, tales como datos relacionados con una empresa. Por ejemplo, es cada vez más común que un individuo utilice un dispositivo informático móvil para tareas tanto personales como relacionadas con una empresa. Cuando el individuo se desplaza (por ejemplo, al trabajo o desde el mismo), los datos sensibles de la empresa pueden estar expuestos a múltiples redes de comunicaciones, incluyendo redes celulares y redes Wi-Fi, algunas de las cuales pueden ser inseguras. Esto puede plantear un riesgo de seguridad a la empresa debido a la posibilidad de que el dispositivo informático móvil comparta involuntaria o intencionalmente datos de la empresa cuando se encuentra fuera de la red de la empresa.

A menudo se implementan directrices y los controles de seguridad de datos para dispositivos móviles en un intento por eliminar o, al menos, mitigar las inquietudes mencionadas anteriormente y otras relacionadas con la seguridad. Estos controles y directrices de seguridad se implementan utilizando un planteamiento de todo o nada. Muchos usuarios optan por el planteamiento de nada si se les permite, debido a la sobrecarga adicional impuesta por directrices generales que, a menudo, afectan de forma adversa a la idoneidad de uso de sus dispositivos para datos personales. Normalmente, sin embargo, estos controles y directrices de seguridad son impuestos a expensas de una menor idoneidad de uso con respecto al acceso a datos personales.

Es con respecto a estas y otras consideraciones que se presenta la divulgación aquí presentada.

El documento US 2006/224742 A1 versa acerca de técnicas para imponer una directriz de seguridad en dispositivos móviles en función de parámetros dinámicos. Un sistema de seguridad de múltiples capas y/o de múltiples modos proporciona una seguridad independiente de la plataforma para controlar el acceso a datos almacenados en al menos un servidor. Las directrices de seguridad son almacenadas en el servidor y sincronizadas con un dispositivo móvil. La imposición de las directrices de seguridad permite al dispositivo móvil acceder a una red y a datos únicamente si opera en conformidad con directrices proporcionadas en el sistema de seguridad.

El documento US 2006/120526 A1 versa acerca de un control de acceso a ficheros en función de la información de origen. Se describen técnicas para proteger datos accesibles por uno o más dispositivos móviles utilizando directrices de seguridad basadas en criterios tales como la información de origen asociada con datos y una ubicación asociada con un entorno de red en el que opera cada dispositivo móvil.

El documento US 2009/247125 A1 versa acerca del control del acceso de recursos de ordenador de dispositivos móviles clientes. Se puede controlar, configurar o coordinar una sistema de bloqueo para uno o más recursos de ordenador de los dispositivos móviles clientes mediante un sistema de gestión de amenazas u otro sistema centralizado. Los recursos de ordenador pueden incluir una pluralidad de programas de aplicación de soporte lógico, dispositivos de comunicaciones, dispositivos de manipulación de datos, dispositivos de almacenamiento de datos y similares. Unos dispositivos de gestión central pueden establecer parámetros de control de acceso a aplicaciones por parte de individuos o de grupos en los muchos clientes móviles dentro su control según una directriz empresarial. La directriz empresarial puede requerir que cualquier programa que proporcione acceso a sitios de red o a un correo electrónico empresarial deba estar protegido por contraseña. La configuración para el control de acceso al recurso de ordenador para una pluralidad de dispositivos móviles clientes debe ser flexible en términos de qué recursos de ordenador están bloqueados y protegidos por contraseña. El dispositivo móvil cliente puede estar completamente bloqueado, completamente desbloqueado, parcialmente bloqueado con algunos recursos de ordenador bloqueados y otros desbloqueados. El dispositivo móvil cliente puede tener distintas contraseñas para distintos recursos bloqueados de ordenador, la misma contraseña para todos los recursos bloqueados de ordenador, una contraseña para el dispositivo móvil cliente y similares.

**Sumario**

El objeto de la presente invención es mejorar la seguridad de las técnicas de la técnica anterior.

Este objeto se soluciona mediante el contenido de las reivindicaciones independientes.

Las realizaciones preferentes se definen mediante las reivindicaciones dependientes.

En la presente memoria se describen conceptos y tecnologías para proteger el uso de datos en dispositivos informáticos. Según los conceptos y las tecnologías divulgados en la presente memoria, se aplican directrices y controles de seguridad a datos específicos en vez de a todo el dispositivo que contiene los datos. Los datos específicos puede ser cualquier tipo de dato incluyendo, sin limitación, datos de la empresa y datos personales. Este enfoque proporciona un equilibrio entre la necesidad de la empresa de seguridad y de control de los datos y la necesidad de un facilidad de uso y de un control de los datos personales. Además, este enfoque permite a un usuario establecer de forma selectiva su directriz de acceso a datos para acceder a datos personales asociados con diversos servicios de consumo. Por ejemplo, un usuario puede establecer la petición de una contraseña para un acceso a un servicio de correo electrónico, pero no requerir ninguna contraseña u otro mecanismo de autentificación para acceder a fotografías, música o algún otro dato. Los conceptos y las tecnologías divulgados en la presente memoria proporcionan controles para datos sensibles utilizando diversos requisitos de contraseña, mantenimiento selectivo de datos en memoria intermedia, transmisión de datos, almacenamiento temporal de datos y/o condiciones predefinidas en las que se deben borrar los datos o se ha de hacer que se vuelvan inaccesibles.

Según un aspecto, un ordenador está configurado para recibir una definición para una directriz configurada para controlar el acceso a los datos en un dispositivo informático, almacenar la directriz y enviar la directriz al dispositivo informático, en el que se controla el acceso a los datos según la directriz. En algunas realizaciones, la directriz incluye una directriz de bloqueo que incluye instrucciones que especifican uno o más niveles de bloqueo, cada uno de los cuales permite un acceso a los datos o a una porción de los mismos en respuesta a la recepción de una credencial válida de autentificación. En algunas realizaciones, la directriz incluye una directriz de control del almacenamiento que incluye instrucciones que dictan el almacenamiento de los datos en el dispositivo informático. La directriz de control del almacenamiento puede indicar si los datos pueden ser mantenidos en memoria intermedia en el dispositivo informático, puede indicar durante cuánto tiempo pueden ser mantenidos en memoria intermedia los datos en el dispositivo informático, puede indicar durante cuánto tiempo pueden almacenarse los datos en el dispositivo informático, cuándo y cómo pueden transmitirse los datos al dispositivo, y desde el mismo, o puede indicar una o más condiciones en las que se deben borrar los datos o se ha de hacer que se vuelvan inaccesibles.

Según otro aspecto, un ordenador, tal como un dispositivo informático móvil, está configurado para recibir una directriz, recibir una solicitud de datos específicos asociados con la directriz, y permitir o denegar el acceso a los datos específicos según la directriz. La directriz puede ser una directriz de bloqueo o una directriz de control del almacenamiento según se ha descrito anteriormente.

Según otro aspecto más, un dispositivo informático móvil está configurado para almacenar datos personales asociados con un usuario del dispositivo informático móvil, almacenar datos de la empresa asociados con una empresa, almacenar una o más directrices, que controlan el acceso a los datos de la empresa, recibir una solicitud de datos de al menos una porción de los datos de la empresa, y permitir de forma selectiva el acceso a la porción de los datos de la empresa según las una o más directrices sin inhibir el acceso a los datos personales.

Se debería apreciar que el contenido descrito anteriormente puede ser implementado como un aparato controlado por un ordenador, un proceso de ordenador, un sistema informático, o como un artículo de fabricación tal como un medio de almacenamiento legible por un ordenador. Estas y otras diversas características serán evidentes a partir de una lectura de la siguiente descripción detallada y de un repaso de los dibujos asociados.

Se proporciona este sumario para presentar una selección de conceptos de forma simplificada que se describen adicionalmente en la descripción detallada. No se concibe que este sumario identifique características clave o características esenciales del contenido reivindicado, ni se prevé que este sumario sea utilizado para limitar el alcance del contenido reivindicado. Además, el contenido reivindicado no está limitado a las implementaciones que solucionan cualquiera de las desventajas, o todas ellas, que se hacen notar en cualquier parte de la presente divulgación.

**Breve descripción de los dibujos**

La FIGURA **1** es un diagrama del sistema que ilustra un entorno operativo ejemplar para las diversas realizaciones divulgadas en la presente memoria.

La FIGURA **2** es un diagrama que ilustra una jerarquía de almacenamiento de documentos de la empresa, según una realización ejemplar.

La FIGURA **3** es un diagrama que ilustra una jerarquía de almacenamiento del dispositivo informático móvil, según realizaciones ejemplares.

La FIGURA **4** es un diagrama de flujo que muestra aspectos de un procedimiento para crear y gestionar directrices, según una realización ejemplar.

La FIGURA **5** es un diagrama de flujo que muestra aspectos de un procedimiento para imponer una directriz en un servidor de datos, según una realización ejemplar.

La FIGURA **6** es un diagrama de flujo que muestra aspectos de un procedimiento para proporcionar datos y una directriz asociada a un dispositivo informático móvil, según una realización ejemplar.

La FIGURA **7** es un diagrama de flujo que muestra aspectos de un procedimiento para imponer una directriz en un dispositivo informático móvil, según una realización ejemplar.

La FIGURA **8** es un diagrama de arquitectura de ordenador que ilustra una arquitectura ejemplar de soporte físico y de soporte lógico de ordenador para un sistema informático con capacidad para implementar aspectos de las realizaciones presentadas en la presente memoria.

**Descripción detallada**

La siguiente descripción detallada está dirigida a conceptos y a tecnologías para proteger el uso de datos en dispositivos informáticos. Según los conceptos y las tecnologías descritos en la presente memoria, se aplican directrices y controles de seguridad a datos específicos en vez de a todo el dispositivo que contiene los datos. Más específicamente, los conceptos y las tecnologías divulgados en la presente memoria proporcionan controles para datos sensibles utilizando diversos requisitos de contraseña, un mantenimiento selectivo de datos en memoria intermedia, un almacenamiento temporal de datos y/o condiciones predefinidas en las que se deben borrar los datos o se ha de hacer que se vuelvan inaccesibles. Los conceptos y las tecnologías divulgados en la presente memoria se describen, en ocasiones, en el contexto de un control de acceso a los datos de la empresa. Sin embargo, se debería comprender que los conceptos y las tecnologías divulgados en la presente memoria pueden ser utilizados, adicional o alternativamente, para controlar el acceso a otros tipos de datos.

Aunque el contenido descrito en la presente memoria es presentado en el contexto general de módulos de programa que se ejecutan junto con la ejecución de un sistema operativo y de programas de aplicación en un sistema de ordenador, los expertos en la técnica reconocerán que se pueden llevar a cabo otras implementaciones en combinación con otros tipos de módulos de programa. En general, los módulos de programa incluyen rutinas, programas, componentes, estructuras de datos y otros tipos de estructuras que llevan a cabo tareas específicas o implementan tipos particulares de datos abstractos. Además, los expertos en la técnica apreciarán que el contenido descrito en la presente memoria puede ser puesto en práctica con otras configuraciones del sistema de ordenador, incluyendo dispositivos de mano, sistemas de múltiples procesadores, electrónica de consumo programable o basada en microprocesadores, miniordenadores, ordenadores centrales y similares.

En la siguiente descripción detallada, se hace referencia a los dibujos adjuntos que forman una parte de la presente memoria, y en los que se muestran, a modo de ilustración, realizaciones o ejemplos específicos. Con referencia ahora a los dibujos, en los que los números similares representan elementos similares en la totalidad de las varias figuras, se presentarán aspectos de un sistema informático, de un medio de almacenamiento legible por un ordenador y de metodología implementada por un ordenador para proteger el uso de datos.

Con referencia ahora a la FIGURA **1,** se describirán aspectos de un entorno operativo **100** para las diversas realizaciones presentadas en la presente memoria. El entorno operativo **100** mostrado en la FIGURA **1** incluye un dispositivo informático móvil **102,** tal como, sin limitación, un ordenador portátil, un ordenador superportátil de red, una tableta, un asistente personal digital, un sistema de videojuegos móvil, un lector electrónico o un teléfono móvil. Se ilustra que el dispositivo informático móvil **102** se encuentra en comunicación con una primera red **104** de acceso, tal como una red celular, una red WIFI, una red WIMAX u otra red incluyendo otras redes inalámbricas o redes alámbricas. La primera red **104** de acceso facilita el acceso a Internet **106** a través de la cual el dispositivo informático móvil **102** puede acceder a un ordenador servidor **108.** La primera red **104** de acceso puede proporcionar, adicionalmente, un acceso de voz al dispositivo informático móvil **102.** Por ejemplo, la primera red **104** de acceso puede proporcionar un acceso de voz celular o de voz sobre protocolo de Internet ("VoIP") al dispositivo informático móvil **102.**

El dispositivo informático móvil **102** puede establecer, adicional o alternativamente, una comunicación con una segunda red **110** de acceso, que también puede ser una red celular, una red WIFI, una red WIMAX u otra red incluyendo otras redes inalámbricas o redes alámbricas. La segunda red **110** de acceso puede proporcionar, adicionalmente, un acceso de voz al dispositivo informático móvil **102.**

En algunas realizaciones, las redes **104, 110** de acceso están disponibles simultáneamente al dispositivo informático móvil **102,** tal como cuando una de las redes **104, 110** de acceso es una red celular y la otra es una red WIFI o WIMAX. De forma alternativa, en algunas realizaciones, las redes **104, 110** de acceso son físicamente disparate de forma que el dispositivo informático móvil **102** sea incapaz de comunicarse simultáneamente con ambas redes **104, 110** de acceso. Por ejemplo, la primera red **104** de acceso puede ser una red WIFI u otra red en el hogar de un usuario y la segunda red **110** de acceso puede ser una red WIFI u otra red en el trabajo de un usuario. Se contempla que el dispositivo informático móvil **102** pueda estar configurado para mantener simultáneamente una conexión con ambas redes **104, 110** de acceso. Además, el dispositivo informático móvil **102** puede priorizar el acceso a datos mediante una de las redes **104, 110** de acceso con respecto a la otra mediante una o más configuraciones que están disponibles en el dispositivo informático móvil **102.**

En la realización ilustrada, la segunda red **110** de acceso facilita el acceso a una intranet **112** de la empresa, que, a su vez, se encuentra en comunicación con un ordenador servidor **114** de directrices de la empresa, con un ordenador servidor **116** de la empresa y con Internet **106** a través de un cortafuegos **118.** El ordenador servidor **114** de directrices de la empresa incluye un sistema operativo **120,** una aplicación **122** de creación de directrices, una aplicación **124** de gestión de directrices, y directrices **126.** El sistema operativo **120** es un programa de ordenador para controlar la operación del ordenador servidor **114** de directrices de la empresa. La aplicación **122** de creación de directrices y la aplicación **124** de gestión de directrices se ejecutan sobre el sistema operativo **120** para proporcionar diversas

funcionalidades descritas en la presente memoria. La aplicación **122** de creación de directrices es un programa de aplicación a través del cual un usuario (por ejemplo, un administrador) puede crear y configurar las directrices **126.** La aplicación **124** de gestión de directrices es un programa de aplicación a través del cual un usuario puede gestionar las directrices **126.** La aplicación **122** de creación de directrices y la aplicación **124** de gestión de directrices se ilustran como programas de aplicación diferenciados, sin embargo, se debería comprender que, en algunas realizaciones, se combina la funcionalidad de estas aplicaciones.

En algunas realizaciones, las directrices **126** son creadas por un administrador de una empresa asociada con la intranet **112** de la empresa mediante la aplicación **122** de creación de directrices del ordenador servidor **114** de directrices de la empresa. En otras realizaciones, las directrices **126** son creadas de forma remota y enviadas al ordenador servidor **114** de directrices de la empresa, o importados por el mismo, para su almacenamiento. En cualquier caso, el ordenador servidor **114** de directrices de la empresa está configurado para distribuir una o más de las directrices **126** al ordenador servidor **116** de la empresa, al ordenador servidor **108,** o a otra fuente de datos, tal como un repositorio de documentos, una compartición de ficheros, un servidor de página Web, un servidor de correo electrónico o alguna otra fuente de datos, de forma que la fuente de datos pueda controlar el acceso a los datos almacenados en la misma por el dispositivo informático móvil **102.** El ordenador servidor de directrices de la empresa también está configurado para distribuir una o más de las directrices **126** al dispositivo informático móvil **102,** de forma que se pueda controlar el acceso a los datos almacenados al menos temporalmente en el dispositivo informático móvil **102.**

Las directrices **126** incluyen, en general, instrucciones que definen bloqueos de acceso y/o controles de almacenamiento para datos que están asociados con la empresa y que son accesibles por el dispositivo informático móvil **102,** y/o almacenados en el mismo. Los datos pueden incluir, sin limitación, contactos, correos electrónicos, documentos, fotografías, vídeos, aplicaciones y/o contenido de páginas electrónicas. Las directrices que incluyen instrucciones que definen bloqueos de acceso son denominados, en la presente memoria, “directrices de bloqueo”. Las directrices que incluyen instrucciones que definen controles de almacenamiento son denominados, en la presente memoria, “directrices de control del almacenamiento”. Se debería comprender que cualquier dato puede estar asociado con uno o más directrices de bloqueo y/o con una o más directrices de control del almacenamiento y, por lo tanto, estar controlado por las mismas.

Las directrices de bloqueo incluyen instrucciones que especifican uno o más niveles de bloqueo, cada uno de los cuales permite un acceso a datos o a una porción de los mismos que ha sido definida como accesible a ese nivel de bloqueo particular. Se puede requerir que un usuario proporcione un mecanismo de autentificación, tal como una contraseña, un número de identificación personal (“PIN”), datos biométricos, una identificación de radiofrecuencia (“RFID”), su ubicación (por ejemplo, GPS, triangulación, o asistida por GPS), la red a la que está conectado u otra forma de autentificación, en cualquier combinación, para acceder a un nivel de bloqueo particular. En algunas realizaciones, una directriz de bloqueo podría especificar que un usuario necesite encontrarse en una cierta ubicación (por ejemplo, según se determina mediante GPS u otra técnica de determinación de la localización) para acceder a ciertos datos. En algunas realizaciones, una directriz de bloqueo especifica que el dispositivo de un usuario necesita estar conectado con una cierta red para acceder a ciertos datos. En algunas realizaciones, una directriz de bloqueo especifica que un usuario necesita autorizar el acceso utilizando un cierto mecanismo de autentificación para acceder a datos específicos. En algunas realizaciones, los bloqueos a un nivel mayor son suficientes para bloquear documentos a un nivel menor sin requerir una autentificación adicional mediante el mismo mecanismo de autentificación, o uno distinto. De forma alternativa, se puede requerir una autentificación en cada nivel de bloqueo o en un cierto número de niveles de bloqueo antes de desbloquear todos los niveles de bloqueo.

Las directrices de control del almacenamiento incluyen instrucciones que dictan el almacenamiento de datos en el dispositivo informático móvil **102.** En algunas realizaciones, una directriz de control del almacenamiento incluye instrucciones que indican si ciertos datos pueden ser mantenidos en memoria intermedia en el dispositivo informático móvil **102** y puede incluir, además, instrucciones que indican durante cuánto tiempo pueden ser mantenidos en memoria intermedia los datos en el dispositivo informático móvil **102.** En algunas realizaciones, una directriz de control del almacenamiento incluye instrucciones que indican durante cuánto tiempo pueden almacenarse ciertos datos en el dispositivo informático móvil **102.** En algunas realizaciones, una directriz de control del almacenamiento incluye instrucciones que indican una o más condiciones en las que han de borrarse ciertos datos o se ha de hacer que se vuelvan inaccesibles.

En algunas realizaciones, una o más de las directrices **126** están definidas en un certificado digital móvil. Por ejemplo, cuando un dispositivo, tal como el dispositivo informático móvil **102,** está dado de alta con la empresa, se le puede asignar al dispositivo un certificado digital móvil, que es utilizado entonces por el dispositivo para acceder a datos proporcionados a través de la intranet **112** de la empresa. Se puede facilitar un procedimiento de alta para dar de alta el dispositivo informático móvil **102** con la empresa mediante la aplicación **124** de gestión de directrices.

En algunas realizaciones, una o más de las directrices **126** son creadas como parte de un mecanismo de gestión de derechos de información (“IRM”) o de gestión de derechos digitales (“DRM”) que es aplicado por un servidor (por ejemplo, el ordenador servidor **116** de la empresa) a un lector de documentos, tal como una aplicación residente en

el dispositivo informático móvil **102** que está configurado para leer y, en algunos casos, modificar ciertos tipos de datos.

En algunas realizaciones, una o más de las directrices **126** se crean para permitir un borrado remoto de datos específicos del dispositivo informático móvil **102.** Se debería comprender que este borrado remoto permite que se mantengan los datos personales y otros datos de la empresa en el dispositivo informático móvil **102.**

En algunas realizaciones, se crean una o más directrices **126** para controlar cuándo pueden transmitirse y/o recibirse ciertos datos. Por ejemplo, una directriz puede especificar que datos sensibles de la empresa pueden ser enviados y/o recibidos únicamente desde una o más redes especificadas tales como únicamente la intranet **112** de la empresa y no en cualquier otra red, tal como una red celular o una red WIFI doméstica de acceso.

En algunas realizaciones, se crean una o más directrices **126** para especificar que no se debe acceder a ciertos datos en el dispositivo informático móvil **126** o, de forma más general, en cualquier dispositivo que pueda cambiar su ubicación.

En algunas realizaciones, se crean una o más directrices **126** para especificar que ciertos datos solo son válidos en la ubicación geográfica X durante el tiempo Y, después del cual los ciertos datos ya no son válidos.

Se contempla que las directrices de bloqueo y/o las directrices de control del almacenamiento puedan depender, al menos parcialmente, de uno o más componentes o características del dispositivo informático móvil **102** para su imposición. Por ejemplo, las directrices pueden ser impuestas, de forma selectiva, en función de la ubicación (por ejemplo, según se determina mediante un sistema de posicionamiento global y/o triangulación), de la hora y/o en función de un uso de una función o aplicación particular en el dispositivo informático móvil **102.**

Se pueden combinar cualesquiera de las realizaciones mencionadas anteriormente de diversas directrices en diversas configuraciones, de forma que haya implementados distintos niveles de protección para ciertos datos. Por ejemplo, una primera directriz puede especificar una o más ubicaciones en las que solo se concede el acceso a los datos cuando el usuario es capaz de proporcionar con éxito credenciales de autentificación tales como un código de acceso o PIN para acceder a los datos según una segunda directriz.

En algunas realizaciones, se envían una o más de las directrices **126** al ordenador servidor **116** de la empresa, al ordenador servidor **108** y/o al dispositivo informático móvil **102.** El ordenador servidor **116** de la empresa está configurado para almacenar un ejemplo de las directrices recibidas como directrices **128** del servidor de la empresa para su aplicación a datos **130** del servidor de la empresa. Los datos **130** del servidor de la empresa son datos almacenados y servidos por el ordenador servidor **116** de la empresa al dispositivo informático móvil **102** a través de la intranet **112** de la empresa y la red **110** de acceso. El ordenador servidor **108** está configurado para almacenar un ejemplo de las directrices recibidas como directrices **132** del servidor para su aplicación a datos **134** del servidor. Los datos **134** del servidor son datos almacenados y servidos por el ordenador servidor **108** al dispositivo informático móvil **102** a través de Internet **106** y de la red **104** de acceso. El dispositivo informático móvil **102** está configurado para almacenar un ejemplo de las directrices recibidos como directrices **136** del dispositivo móvil para su aplicación a datos **138** del dispositivo móvil. Los datos **138** del dispositivo móvil pueden incluir un ejemplo de los datos **130** del servidor de la empresa o una porción de los mismos, un ejemplo de los datos **134** del servidor o una porción de los mismos, y/o datos creados localmente en el dispositivo informático móvil **102** para los cuales son aplicables una o más de las directrices **126.**

Según diversas realizaciones, el ordenador servidor **114** de directrices de la empresa, el ordenador servidor **116** de la empresa y/o el ordenador servidor **108** son ordenadores personales (“PC”) tales como sistemas de ordenador de sobremesa, de tipo tableta o portátil. El ordenador servidor **114** de directrices de la empresa, el ordenador servidor **116** de la empresa y/o el ordenador servidor **108** pueden incluir otros tipos de sistemas informáticos incluyendo, sin limitación, ordenadores servidores, ordenadores de mano, ordenadores superportátiles de red, ordenadores de tipo tableta, sistemas de ordenador embebido, asistentes digitales personales, teléfonos móviles, teléfonos inteligentes u otros dispositivos informáticos.

Se debería comprender que algunas implementaciones del entorno operativo **100** incluyen múltiples ordenadores servidores **114** de directrices de la empresa, múltiples ordenadores servidores **116** de la empresa, múltiples ordenadores servidores **108,** múltiples dispositivos informáticos móviles **102,** más de dos redes **104, 110** de acceso, múltiples internets **106,** múltiples intranets **112** de la empresa y/o múltiples cortafuegos **118.** También se debería comprender que el ordenador servidor **114** de directrices de la empresa puede utilizar múltiples sistemas operativos **120,** múltiples aplicaciones **122** de creación de directrices, múltiples aplicaciones **124** de gestión de directrices y/o múltiples repositorios para almacenar las **126** de directrices usados por el ordenador 114 servidor de directrices de la empresa; y/o uno o más de estos componentes pueden ser proporcionados por otro ordenador servidor de la empresa (no mostrado). Además, aunque no se muestra en la FIGURA **1,** cada uno del ordenador servidor **116** de la empresa, del ordenador servidor **108** y del dispositivo móvil **102** puede estar configurado con un sistema operativo y con uno o más programas de aplicación que están configurados para ejecutarse sobre el sistema operativo para proporcionar diversas funcionalidades descritas en la presente memoria. De esta manera, se debería comprender que las realizaciones ilustradas son ejemplares, y no se debería entender que sean limitantes de ninguna forma.

Con referencia ahora a la FIGURA **2,** se describirá un diagrama que ilustra una jerarquía ejemplar **200** de almacenamiento de documentos de la empresa. La jerarquía **200** de almacenamiento de documentos de la empresa incluye un nivel raíz **202.** En algunas realizaciones, el nivel raíz **202** es un nivel de bloqueo para controlar el acceso a la intranet **112** de la empresa. Los usuarios que se autentifican con el nivel raíz **202** tienen acceso a la intranet **112** de la empresa, pero pueden tener o no acceso a recursos adicionales en la intranet **112** de la empresa dependiendo de la definición de la o de las directrices que dictan el acceso al nivel raíz **202.** En la realización ilustrada, estos recursos incluyen una plataforma **204** de correo electrónico, un nivel **206** de plataforma de colaboración y un nivel **208** de compartición de ficheros, cada uno de los cuales es un nivel de bloqueo para controlar el acceso a recursos específicos de la intranet **112** de la empresa. Se debería comprender que se puede proporcionar a cualquier plataforma, sistema de ordenador o dispositivo informático móvil asociado con una empresa un nivel de bloqueo y puede ser organizado jerárquicamente o no con una o más plataformas adicionales, sistemas de ordenador y/o dispositivos informáticos en función de niveles de bloqueo variables que dictan el acceso a los mismos.

El nivel **204** de plataforma de correo electrónico es un nivel de bloqueo para controlar el acceso a recursos relacionados con una plataforma de correo electrónico de la empresa. La plataforma de correo electrónico, en algunas realizaciones, es un programa de aplicación de correo electrónico de colaboración del lado del servidor tal como MICROSOFT EXCHANGE, disponible en Microsoft Corporation de Redmond, Washington, EE. UU., aunque se contemplan otras plataformas de correo electrónico. El nivel **204** de plataforma de correo electrónico incluye un nivel **210** de buzón de correo, uno o más documentos **212** del buzón de correo, un nivel **214** de folder público y uno o más documentos públicos **216.**

El nivel **210** de buzón de correo es un nivel de bloqueo para controlar el acceso a buzones de correo disponibles en la plataforma de correo electrónico. Los buzones de correo pueden ser particulares a un usuario o a un grupo de trabajo en la empresa. Los documentos **212** del buzón de correo incluyen documentos de correo electrónico u otros documentos asociados con un buzón de correo particular. Se puede limitar el acceso a los documentos **112** del buzón de correo bajo el nivel **210** de buzón de correo, individual o conjuntamente, mediante una o más directrices. El nivel **214** de folder público es un nivel de bloqueo para controlar el acceso a los uno o más documentos públicos **216.** Los documentos públicos **216** son documentos asociados con el nivel **214** de folder público.

Con referencia de nuevo al nivel **206** de plataforma de colaboración, este nivel es un nivel de bloqueo para controlar el acceso a los recursos relacionados con una plataforma de colaboración de la empresa. La plataforma de colaboración, en algunas realizaciones, es un programa de aplicación Web de colaboración, tal como MICROSOFT SHAREPOINT, disponible en Microsoft Corporation de Redmond, Washington, EE. UU., aunque se contemplan otros programas de aplicación Web de colaboración. El nivel **206** de plataforma de colaboración incluye un nivel **218** de sitio, un nivel **220** de biblioteca de documentos y uno o más documentos **222.** El nivel **218** de sitio es un nivel de bloqueo que controla el acceso a uno o más sitios disponibles en la plataforma de colaboración. Los sitios pueden estar configurados, por ejemplo, como sitios SHAREPOINT. Los sitios disponibles en el nivel **218** de sitio pueden incluir, a su vez, una o más bibliotecas de documentos en el nivel **220** de biblioteca de documentos. El nivel **220** de biblioteca de documentos es un nivel de bloqueo que controla el acceso a los uno o más documentos **222.**

Con referencia de nuevo al nivel **208** de compartición de ficheros, este nivel es un nivel de bloqueo para controlar el acceso a recursos relacionados con una plataforma de compartición de ficheros de la empresa. El nivel **208** de compartición de ficheros es un nivel de bloqueo que incluye uno o más directorios a un nivel **224** de directorio. El nivel **224** de directorio es un nivel de bloqueo para controlar el acceso a uno o más documentos **226.**

Se debería comprender que la jerarquía **200** de almacenamiento de documentos de la empresa descrita anteriormente ilustra dónde pueden aplicarse las directrices. Las directrices para un bloqueo de los datos móviles, de introducción en memoria intermedia, de transmisión de datos y de retención de datos pueden especificarse en cada nivel, al nivel de documentos y pueden ser heredadas o no heredadas de otro nivel (por ejemplo, un nivel anterior). En general, sin embargo, para un documento dado se puede aplicar la directriz más estricta combinando directrices de cualquiera de los documentos **216, 222, 226** hacia arriba, hacia el nivel raíz **202** en sus recorridos respectivos. Para las directrices de bloqueo, un nivel de bloqueo mayor puede ser suficiente para bloquear documentos a un nivel menor sin requerir la autentificación en cada nivel.

Con referencia ahora a la FIGURA **3,** se describirá un diagrama que ilustra una jerarquía ejemplar **300** de almacenamiento del dispositivo informático móvil. La jerarquía **300** de almacenamiento del dispositivo informático móvil incluye un nivel **302** de dispositivo móvil que, a su vez, incluye un nivel **304** de contactos, un nivel **306** de correo electrónico y un nivel **308** de documentos. El nivel **304** de contactos, el nivel **306** de correo electrónico y el nivel **308** de documentos están asociados con datos personales **310** y con datos **312** de la empresa. Se pueden aplicar directrices al nivel **304** de contactos, al nivel **306** de correo electrónico, al nivel **308** de documentos y/o para los datos **312** de la empresa.

Aunque se pueden fusionar tipos de datos (por ejemplo, contactos, correo electrónico y documentos) de los datos personales **310** y de los datos **312** de la empresa en aplicaciones y en interfaces de usuario que están configuradas para utilizar los diversos tipos de datos, a los datos **312** de la empresa se les aplican directrices. Los datos personales

**310** pueden permanecer bajo el control del propietario y/o del usuario del dispositivo informático móvil **102** sin ser inhibidos por la imposición de las directrices.

Con referencia ahora a la FIGURA **4,** se describirán aspectos de un procedimiento **400** para crear y gestionar directrices. Se debería comprender que las operaciones de los procedimientos divulgados en la presente memoria no son presentadas necesariamente en ningún orden particular y que es posible y se contempla la realización de algunas de las operaciones, o de todas ellas, en uno o más órdenes alternativos. Las operaciones han sido presentadas en el orden demostrado para facilitar la descripción y la ilustración. Se pueden añadir, omitir y/o llevar acabo simultáneamente operaciones sin alejarse del alcance de las reivindicaciones adjuntas.

También se debería comprender que los procedimientos ilustrados pueden finalizar en cualquier momento y no necesitan ser llevados a cabo en su totalidad. Algunas de las operaciones, o todas ellas, de los procedimientos y/u operaciones sustancialmente equivalentes, pueden ser llevadas a cabo mediante la ejecución de instrucciones legibles por un ordenador incluidas en un medio de almacenamiento de ordenador, según se define a continuación. La expresión “instrucciones legibles por un ordenador”, y variantes de la misma, en la descripción y en las reivindicaciones, es utilizada de forma expansiva en la presente memoria de forma que incluya rutinas, aplicaciones, módulos de aplicación, módulos de programa, programas, componentes, estructuras de datos, algoritmos y similares. Se pueden implementar instrucciones legibles por un ordenador en diversas configuraciones del sistema, incluyendo sistemas de un único procesador o de múltiples procesadores, miniordenadores, ordenadores centrales, ordenadores personales, dispositivos informáticos de mano, electrónica de consumo programable basada en microprocesadores, combinaciones de los mismos, y similares.

Por lo tanto, se debería apreciar que las operaciones lógicas descritas en la presente memoria son implementadas (1) como una secuencia de acciones implementadas por un ordenador o de módulos de programa que se ejecutan en un sistema informático y/o (2) como circuitos lógicos de máquina interconectados o módulos de circuito en el sistema informático. La implementación es una cuestión de elección que depende del rendimiento y de otros requisitos del sistema informático. En consecuencia, las operaciones lógicas descritas en la presente memoria son denominadas de forma diversa como estados, operaciones, dispositivos estructurales, acciones o módulos. Estos dispositivos estructurales, operaciones, acciones y módulos pueden ser implementados en un soporte lógico, en un soporte físico inalterable, en lógica digital de uso especial y cualquier combinación de los mismos.

El procedimiento **400** comienza en la operación **402,** recibiendo el ordenador servidor **114** de directrices de la empresa una definición para una directriz para controlar el acceso a datos específicos. La definición de la directriz puede ser proporcionada por un administrador mediante la aplicación **122** de creación de directrices. Desde la operación **402,** el procedimiento **400** avanza a la operación **404,** en la que el ordenador servidor **114** de directrices de la empresa almacena la directriz en asociación con los datos específicos como una de las directrices **126.** El administrador puede desear proporcionar la directriz a uno o más servidores y puede designar a qué servidores se debe enviar la directriz utilizando la aplicación **124** de gestión de directrices. Por ejemplo, el administrador puede indicar al ordenador servidor **114** de directrices de la empresa que envíe la directriz al ordenador servidor **116** de la empresa y/o al ordenador servidor **108,** en la operación **406.** El procedimiento **400** termina en la operación **408.**

Con referencia ahora a la FIGURA **5,** se describirá un procedimiento **500** para imponer una directriz en un servidor de datos, tal como el ordenador servidor **116** de la empresa o el ordenador servidor **108.** Para facilitar la descripción de forma no limitante, se describirá que el ordenador servidor **116** de la empresa lleva a cabo las operaciones del procedimiento **500.**

El procedimiento **500** comienza en la operación **502,** en la que el ordenador servidor **116** de la empresa recibe la directriz procedente del ordenador servidor **114** de directrices de la empresa. Desde la operación **502,** el procedimiento **500** avanza a la operación **504,** en la que el ordenador servidor **116** de la empresa almacena la directriz en asociación con los datos específicos como una de las directrices **130** del servidor de la empresa. Entonces, el procedimiento **500** avanza a la operación **506,** en la que el ordenador servidor **116** de la empresa recibe una solicitud de datos específicos asociados con la directriz almacenada procedente del dispositivo informático móvil **102.** En respuesta a la recepción de la solicitud, en la operación **508,** el ordenador servidor **116** de la empresa permite o deniega el acceso del dispositivo informático móvil **102** a los datos específicos según la directriz. El procedimiento **500** termina en la operación **510.**

Con referencia ahora a la FIGURA **6,** se describirá un procedimiento **600** para proporcionar datos y una directriz asociada con el dispositivo informático móvil **102.** Para facilitar la descripción de forma no limitante, se describirá que el ordenador servidor **116** de la empresa lleva a cabo las operaciones del procedimiento **600.**

El procedimiento **600** comienza en la operación **602,** en la que el ordenador servidor **116** de la empresa recibe la directriz procedente del ordenador servidor **114** de directrices de la empresa. Desde la operación **602,** el procedimiento **600** avanza a la operación **604,** en la que el ordenador servidor **114** de directrices de la empresa almacena la directriz en asociación con datos específicos como una de las directrices **130** del servidor de la empresa. Entonces, el procedimiento **600** avanza a la operación **606,** en la que el ordenador servidor **116** de la empresa recibe una solicitud de datos específicos asociados con la directriz almacenada procedente del dispositivo informático móvil **102.** En respuesta a la recepción de la solicitud, en la operación **608,** el ordenador servidor **116** de la empresa envía los datos

específicos y la directriz asociada al dispositivo informático móvil **102,** en el cual se impone el acceso a los datos específicos según la directriz. El procedimiento **600** termina en la operación **610.**

Con referencia ahora a la FIGURA **7,** se describirá un procedimiento **700** para imponer una directriz en un dispositivo informático móvil **102.** El procedimiento **700** comienza en la operación **702,** en la que el dispositivo informático móvil **102** recibe una directriz. En algunas realizaciones, el dispositivo informático móvil **102** recibe la directriz procedente de un servidor, tal como el ordenador servidor **108,** el ordenador servidor **114** de directrices de la empresa o el ordenador servidor **116** de la empresa, en respuesta a una solicitud de datos o a una solicitud de directriz generada por el dispositivo informático móvil **102** y enviada al servidor. En algunas realizaciones, el dispositivo informático móvil **102** recibe la directriz procedente de un servidor en respuesta a un administrador que da la instrucción, a través de la aplicación **124** de gestión de directrices, de que el ordenador servidor **114** de directrices de la empresa envíe al dispositivo informático móvil **102** la directriz sin solicitud previa**.**

Desde la operación **702,** el procedimiento **700** avanza a la operación **704,** en la que el dispositivo informático móvil **102** recibe una solicitud de datos específicos asociados con la directriz recibida. En respuesta a la recepción de la solicitud de datos, en la operación **706,** el dispositivo informático móvil **102** solicita a un usuario su autentificación según la directriz. Si las credenciales de autentificación proporcionados por el usuario en respuesta a la solicitud de autentificación son válidas, el procedimiento **700** avanza a la operación **710,** en la que un dispositivo informático móvil **102** permite al usuario acceder a datos específicos. Entonces, el procedimiento **700** avanza a la operación **712,** en la que termina el procedimiento **700.** Sin embargo, si las credenciales de autentificación proporcionadas por el usuario en respuesta a la solicitud de autentificación no son válidas, el procedimiento **700** avanza a la operación **714,** en la que el dispositivo informático móvil **102** deniega el acceso a los datos específicos. Entonces, el procedimiento **700** avanza a la operación **712,** en la que termina el procedimiento **700.**

La FIGURA **8** ilustra una arquitectura ejemplar **800** de ordenador para un dispositivo con capacidad para ejecutar los componentes de soporte lógico descritos en la presente memoria para proteger el uso de datos en dispositivos informáticos móviles. Por lo tanto, la arquitectura **800** de ordenador ilustrada en la FIGURA **8** ilustra una arquitectura para un ordenador servidor, un teléfono móvil, un PDA, un teléfono inteligente, un ordenador de sobremesa, un pequeño ordenador portátil, un ordenador de tipo tableta y/o un ordenador portátil. La arquitectura **800** de ordenador puede ser utilizada para ejecutar cualquier aspecto de los componentes de soporte lógico presentados en la presente memoria con respecto a cualquiera de los sistemas de ordenador descritos en la presente memoria, tales como el dispositivo informático móvil **102,** el ordenador servidor **114** de directrices de la empresa, el ordenador servidor **116** de la empresa y el ordenador servidor **108.**

La arquitectura **800** de ordenador ilustrada en la FIGURA **8** incluye una unidad central **802** de procesamiento (“CPU”), una memoria **804** del sistema, incluyendo una memoria **806** de acceso aleatorio (“RAM”) y una memoria **808** de solo lectura (“ROM”) y un *bus* **810** del sistema que acopla la memoria **804** con la CPU **802.** Un sistema básico de entrada/salida que contiene las rutinas básicas que ayudan a transferir información entre elementos en la arquitectura **800** de ordenador, tal como durante el arranque, se almacena en la ROM **808.** La arquitectura **800** de ordenador incluye, además, un dispositivo **812** de almacenamiento masivo para almacenar, cuando sea apropiado, el sistema operativo **120** (u otro/s sistema/s operativo/s), la aplicación **122** de configuración de directrices, la aplicación **124** de gestión de directrices, las directrices **126,** las directrices **128** del servidor de la empresa, las directrices **132** del servidor, las directrices **136** del dispositivo informático móvil, los datos **130** del servidor de la empresa, los datos **134** del servidor y los datos **138** del dispositivo informático móvil.

El dispositivo **812** de almacenamiento masivo está conectado con la CPU **802** a través de un controlador (no mostrado) de almacenamiento masivo conectado con el *bus* **810** del sistema. El dispositivo **812** de almacenamiento masivo y sus medios asociados legibles por un ordenador proporcionan un almacenamiento no volátil para la arquitectura **800** de ordenador. Aunque la descripción de los medios legibles por un ordenador contenidos en la presente memoria hace referencia a un dispositivo de almacenamiento masivo, tal como una unidad de disco duro o de CD-ROM, los expertos en la técnica deberían apreciar que los medios legibles por un ordenador pueden ser cualquier medio disponible de almacenamiento de ordenador o medio de comunicación al que puede accederse mediante la arquitectura **800** de ordenador.

El medio de comunicación incluye instrucciones legibles por un ordenador, estructuras de datos, módulos de programa u otros datos en una señal modulada de datos, tal como una onda portadora u otro mecanismo de transporte e incluye cualquier medio de suministro. La expresión “señal modulada de datos” significa una señal que tiene una o más de sus características cambiadas o establecidas de una forma que se codifique información en la señal. A modo de ejemplo, y no de limitación, el medio de comunicación incluye medios alámbricos tales como una red alámbrica o una conexión cableada directa, y medios inalámbricos tales como medios acústicos, de RF, infrarrojos y otros inalámbricos. Se deberían incluir las combinaciones de cualquiera de los anteriores en el alcance de los medios legibles por un ordenador.

A modo de ejemplo, y no de limitación, los medios de almacenamiento de ordenador pueden incluir medios volátiles y no volátiles, extraíbles y no extraíbles implementados en cualquier procedimiento o tecnología para el almacenamiento de información tal como instrucciones legibles por un ordenador, estructuras de datos, módulos de programa u otros

datos. Por ejemplo, los medios de ordenador incluyen, sin limitación, RAM, ROM, EPROM, EEPROM, memoria *flash* u otra tecnología de memoria de estado sólido, CD-ROM, discos versátiles digitales ("DVD"), HD-DVD, BLU-RAY u otro almacenamiento óptico, casetes magnéticos, cinta magnética, almacenamiento en disco magnético u otros dispositivos de almacenamiento magnético, o cualquier otro medio que pueda ser utilizado para almacenar la información deseada y que pueda ser objeto de acceso por la arquitectura **800** de ordenador. Para el fin de las reivindicaciones, la frase "medio de almacenamiento de ordenador", y variaciones de la misma, no incluye ondas, señales y/u otros medios transitorios y/o intangibles de comunicaciones, *per se*.

Según diversas realizaciones, la arquitectura **800** de ordenador puede operar en un entorno de red utilizando conexiones lógicas con ordenadores remotos a través de una red **814,** tal como la primera red **104** de acceso, la segunda red **110** de acceso, la intranet **112** de la empresa y/o Internet **106.** La arquitectura **800** de ordenador puede conectarse con la red **814** a través de una unidad **816** de interfaz de red conectada con el *bus* **810.** Se debería apreciar que la unidad **816** de interfaz de red también puede ser utilizada para conectarse a otros tipos de redes y de sistemas remotos de ordenador. La arquitectura **800** de ordenador también puede incluir un controlador **818** de entrada/salida para recibir y procesar una entrada procedente de un número de otros dispositivos, incluyendo un teclado, un ratón o un lápiz electrónico (no mostrado en la FIGURA **8**). De forma similar, el controlador **818** de entrada/salida puede proporcionar una salida a una pantalla de visualización, a una impresora o a otro tipo de dispositivo de salida (tampoco mostrado en la FIGURA **8**).

Se debería apreciar que los componentes de soporte lógico descritos en la presente memoria, cuando están cargados en la CPU **802** y son ejecutados, pueden transformar la CPU **802** y la arquitectura general **800** de ordenador de un sistema informático de uso general en un sistema informático de uso especial personalizado para facilitar la funcionalidad presentada en la presente memoria. La CPU **802** puede estar construida de cualquier número de transistores u otros elementos diferenciados de circuito, que pueden adoptar, individual o colectivamente, un número cualquiera de estados. Más específicamente, la CPU **802** puede operar como una máquina de estado finito, en respuesta a instrucciones ejecutables contenidas en los módulos de soporte lógico divulgados en la presente memoria. Estas instrucciones ejecutables por un ordenador pueden transformar la CPU **802** especificando cómo pasa la CPU **802** entre estados, transformando, de ese modo, los transistores u otros elementos diferenciados de soporte físico que constituyen la CPU **802.**

La codificación de los módulos de soporte lógico presentados en la presente memoria también puede transformar la estructura física de los medios legibles por un ordenador presentados en la presente memoria. La transformación específica de la estructura física puede depender de diversos factores, en distintas implementaciones de esta descripción. Ejemplos de tales factores pueden incluir, sin limitación, la tecnología utilizada para implementar los medios legibles por un ordenador, ya se caractericen los medios legibles por un ordenador como almacenamiento primario o secundario, y similares. Por ejemplo, si se implementan los medios legibles por un ordenador como memoria a base de semiconductores, el soporte lógico divulgado en la presente memoria puede ser codificado en los medios legibles por un ordenador transformando el estado físico de la memoria semiconductora. Por ejemplo, el soporte lógico puede transformar el estado de los transistores, de los condensadores o de otros elementos diferenciados de circuito que constituyan la memoria semiconductora. El soporte lógico también puede transformar el estado físico de tales componentes para almacenar datos en los mismos.

Como otro ejemplo, los medios legibles por un ordenador divulgados en la presente memoria pueden ser implementados utilizando tecnología magnética u óptica. En tales implementaciones, el soporte lógico presentado en la presente memoria puede transformar el estado físico de los medios magnéticos u ópticos, cuando el soporte lógico está codificado en los mismos. Estas transformaciones pueden incluir la alteración de las características magnéticas de ubicaciones particulares en los medios magnéticos dados. Estas transformaciones también pueden incluir la alteración de las características físicas o de las características de ubicaciones particulares en medios ópticos dados, para cambiar las características ópticas de esas ubicaciones. Son posibles otras transformaciones de medios físicos sin alejarse del alcance de la presente descripción, proporcionándose los anteriores ejemplos únicamente para facilitar esta exposición.

En vista de lo anterior, se debería apreciar que muchos tipos de transformaciones físicas tienen lugar en la arquitectura **800** de ordenador para almacenar y ejecutar los componentes de soporte lógico presentados en la presente memoria. También se debería apreciar que la arquitectura **800** de ordenador puede incluir otros tipos de dispositivos informáticos, incluyendo ordenadores de mano, sistemas de ordenador embebido, asistentes digitales personales y otros tipos de dispositivos informáticos conocidos por los expertos en la técnica. También se contempla que la arquitectura **800** de ordenador pueda no incluir todos los componentes mostrados en la FIGURA **8,** puede incluir otros componentes que no se muestran explícitamente en la FIGURA **8** o puede utilizar una arquitectura completamente distinta de la mostrada en la FIGURA **8.**

En función de lo anterior, se debería apreciar que se han divulgado en la presente memoria conceptos y tecnologías para proteger el uso de datos. Aunque se ha descrito el contenido presentado en la presente memoria con un lenguaje específico a características estructurales de ordenador, acciones metodológicas y transformativas, maquinaria informática específica y medios legibles por un ordenador, se debe comprender que la invención definida en las reivindicaciones adjuntas no está limitada necesariamente a las características, a las acciones o a los medios

específicos descritos en la presente memoria. Más bien, se divulgan las características, las acciones y los medios específicos como formas ejemplares para implementar las reivindicaciones.

El contenido descrito anteriormente únicamente se proporciona a modo ilustrativo y no se debería interpretar como limitante. Se pueden realizar diversos cambios y modificaciones al contenido descrito en la presente memoria sin seguir las realizaciones y las aplicaciones ejemplares ilustradas y descritas, y sin alejarse del alcance de la presente invención, que se define en las siguientes reivindicaciones.

**REIVINDICACIONES**

**1.** Un medio de almacenamiento de ordenador que tiene instrucciones legibles por un ordenador almacenadas en el mismo que, cuando son ejecutadas por un ordenador, provocan que el ordenador:

reciba (602) una definición de una directriz configurada para controlar el acceso a datos en un dispositivo informático;
almacene (604) la directriz; y
envíe (608) la directriz al dispositivo informático, estando configurado el dispositivo informático para imponer el acceso a los datos según la directriz,
en el que la directriz una directriz de bloqueo comprende instrucciones que especifican una pluralidad de niveles de bloqueo, permitiendo cada uno de ellos el acceso a los datos o a una porción de los mismos en respuesta a la recepción de una credencial válida de autentificación,
en el que un bloqueo en un primer nivel de bloqueo bloquea los documentos a niveles de bloqueo menores que el primer nivel de bloqueo, comprendiendo la directriz, además, una directriz de control del almacenamiento que comprende instrucciones que dictan el almacenamiento de los datos en el dispositivo informático, y
en el que la directriz de control del almacenamiento comprende, además, instrucciones que indican durante cuánto tiempo pueden almacenarse los datos en el dispositivo informático.

**2.** El medio de almacenamiento de ordenador de la reivindicación 1, en el que la directriz comprende, además, una directriz de bloqueo que comprende instrucciones que especifican uno o más niveles de bloqueo cada uno de los cuales permite el acceso a los datos o a una porción de los mismos en respuesta a la localización del dispositivo informático en una cierta ubicación.

**3.** El medio de almacenamiento de ordenador de la reivindicación 1, en el que la directriz de control del almacenamiento comprende instrucciones que indican si los datos pueden ser mantenidos en memoria intermedia en el dispositivo informático.

**4.** El medio de almacenamiento de ordenador de la reivindicación 3, en el que la directriz de control del almacenamiento comprende, además, instrucciones que indican durante cuánto tiempo pueden ser mantenidos en memoria intermedia los datos en el dispositivo informático.

**5.** El medio de almacenamiento de ordenador de la reivindicación 1, en el que la directriz de control del almacenamiento comprende instrucciones que indican una o más condiciones en las que los datos han de ser borrados o se ha de hacer que se vuelvan inaccesibles.

**6.** El medio de almacenamiento de ordenador de la reivindicación 1, en el que la directriz está definida en un certificado digital móvil para el dispositivo informático.

**7.** Un medio de almacenamiento de ordenador que tiene instrucciones legibles por un ordenador almacenadas en el mismo que, cuando son ejecutadas por un dispositivo informático, provocan que el dispositivo:

reciba (702) una directriz;
reciba (704) una solicitud de datos específicos asociados con la directriz; y
permita (710) o deniegue (714) el acceso a los datos específicos según la directriz,
en el que la directriz una directriz de bloqueo comprende instrucciones que especifican una pluralidad de niveles de bloqueo cada uno de los cuales permite el acceso a los datos o a una porción de los mismos en respuesta a la recepción de una credencial válida de autentificación,
en el que un bloqueo en un primer nivel de bloqueo bloquea los documentos a niveles de bloqueo menores que el primer nivel de bloqueo, comprendiendo la directriz, además, una directriz de control del almacenamiento que comprende instrucciones que dictan el almacenamiento de los datos en el dispositivo informático, y
en el que la directriz de control del almacenamiento comprende, además, instrucciones que indican durante cuánto tiempo pueden almacenarse los datos en el dispositivo informático.

**8.** El medio de almacenamiento de ordenador de la reivindicación 7, en el que:

la directriz comprende, además, una directriz de bloqueo que comprende instrucciones que especifican uno o más niveles de bloqueo cada uno de los cuales permite el acceso a los datos o a una porción de los mismos en respuesta a la localización del dispositivo informático en una cierta ubicación; o
la directriz de control del almacenamiento comprende instrucciones que indican uno de los siguientes:

si los datos pueden ser mantenidos en memoria intermedia en el ordenador y, si los datos pueden ser mantenidos en memoria intermedia, durante cuánto tiempo pueden ser mantenidos en memoria intermedia los datos; o

una o más condiciones en las que han de borrarse o se ha de hacer que se vuelvan inaccesibles los datos, comprendiendo las una o más condiciones al menos una ubicación.

**9.** Un dispositivo informático móvil, que comprende:

un procesador (802); y
una memoria (812) en comunicación con el procesador, comprendiendo la memoria instrucciones almacenadas en la misma que, cuando son ejecutadas por el procesador, provocan que el procesador
almacene datos personales asociados con un usuario del dispositivo informático móvil,
almacene datos de empresa asociados con una empresa;
almacene una o más directrices, cada una de las cuales comprende instrucciones para al menos uno de controlar el acceso a los datos de empresa y de gestionar los datos de empresa;
reciba una solicitud de datos de al menos una porción de los datos de empresa; y
permita, de forma selectiva, el acceso a la porción de los datos de empresa según las una o más directrices sin inhibir el acceso a los datos personales,
en el que las una o más directrices una directriz de bloqueo comprende instrucciones que especifican una pluralidad de niveles de bloqueo cada uno de los cuales permite el acceso a los datos de empresa o a una porción de los mismos en respuesta a la recepción de una credencial válida de autentificación,
en el que un bloqueo en un primer nivel de bloqueo bloquea los documentos a niveles de bloqueo menores que el primer nivel de bloqueo, comprendiendo la directriz, además, una directriz de control del almacenamiento que comprende instrucciones que dictan el almacenamiento de los datos en el dispositivo informático, y
en el que la directriz de control del almacenamiento comprende, además, instrucciones que indican durante cuánto tiempo pueden almacenarse los datos en el dispositivo informático.

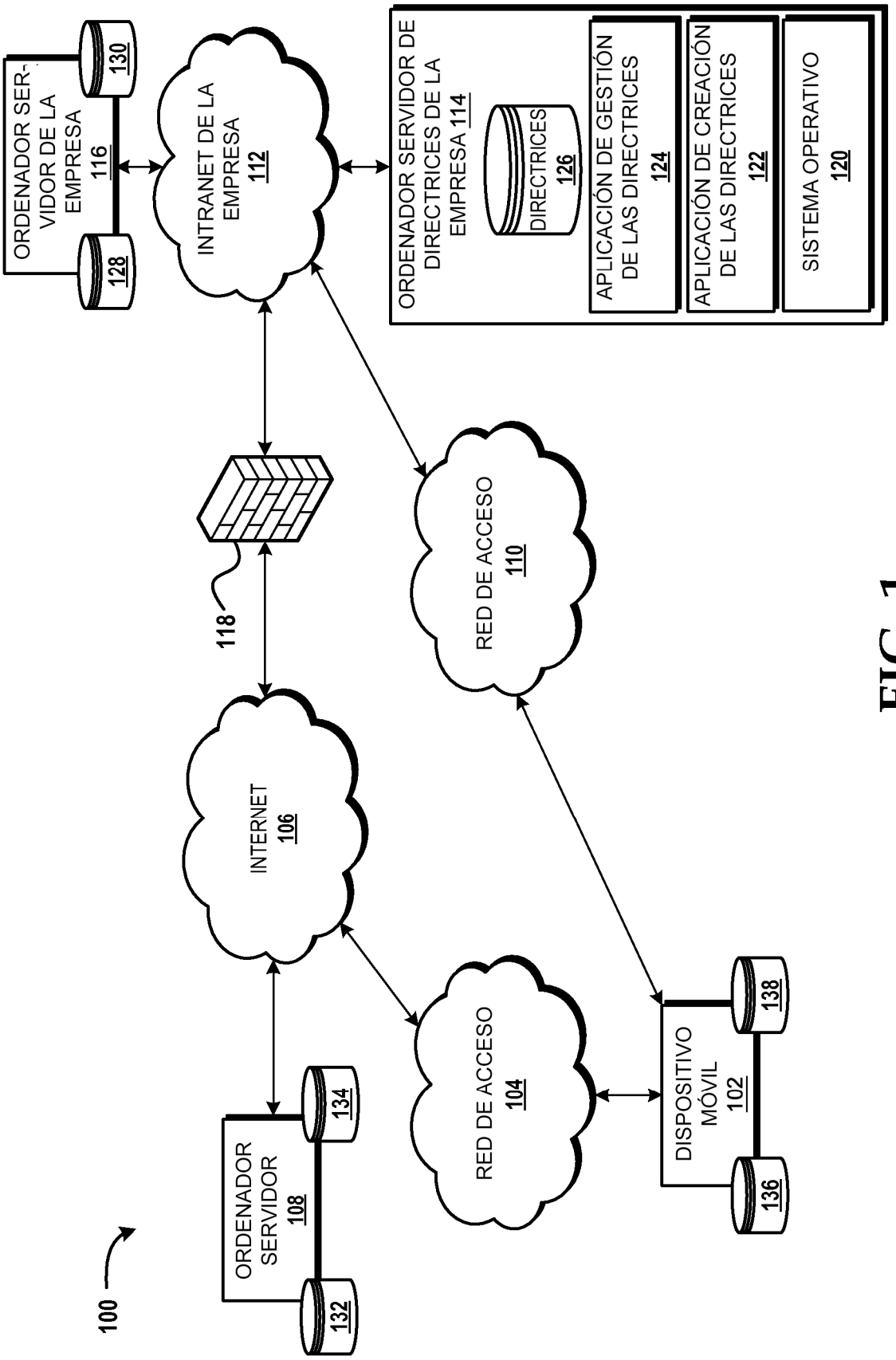
100
ORDENADOR SERVIDOR DE LA EMPRESA 116
130
128
INTRANET DE LA EMPRESA 112
ORDENADOR SERVIDOR DE DIRECTRICES DE LA EMPRESA 114
DIRECTRICES 126
APLICACIÓN DE GESTIÓN DE LAS DIRECTRICES 124
APLICACIÓN DE CREACIÓN DE LAS DIRECTRICES 122
SISTEMA OPERATIVO 120
118
RED DE ACCESO 110
INTERNET 106
ORDENADOR SERVIDOR 108
134
132
RED DE ACCESO 104
DISPOSITIVO MÓVIL 102
138
136

FIG. 1

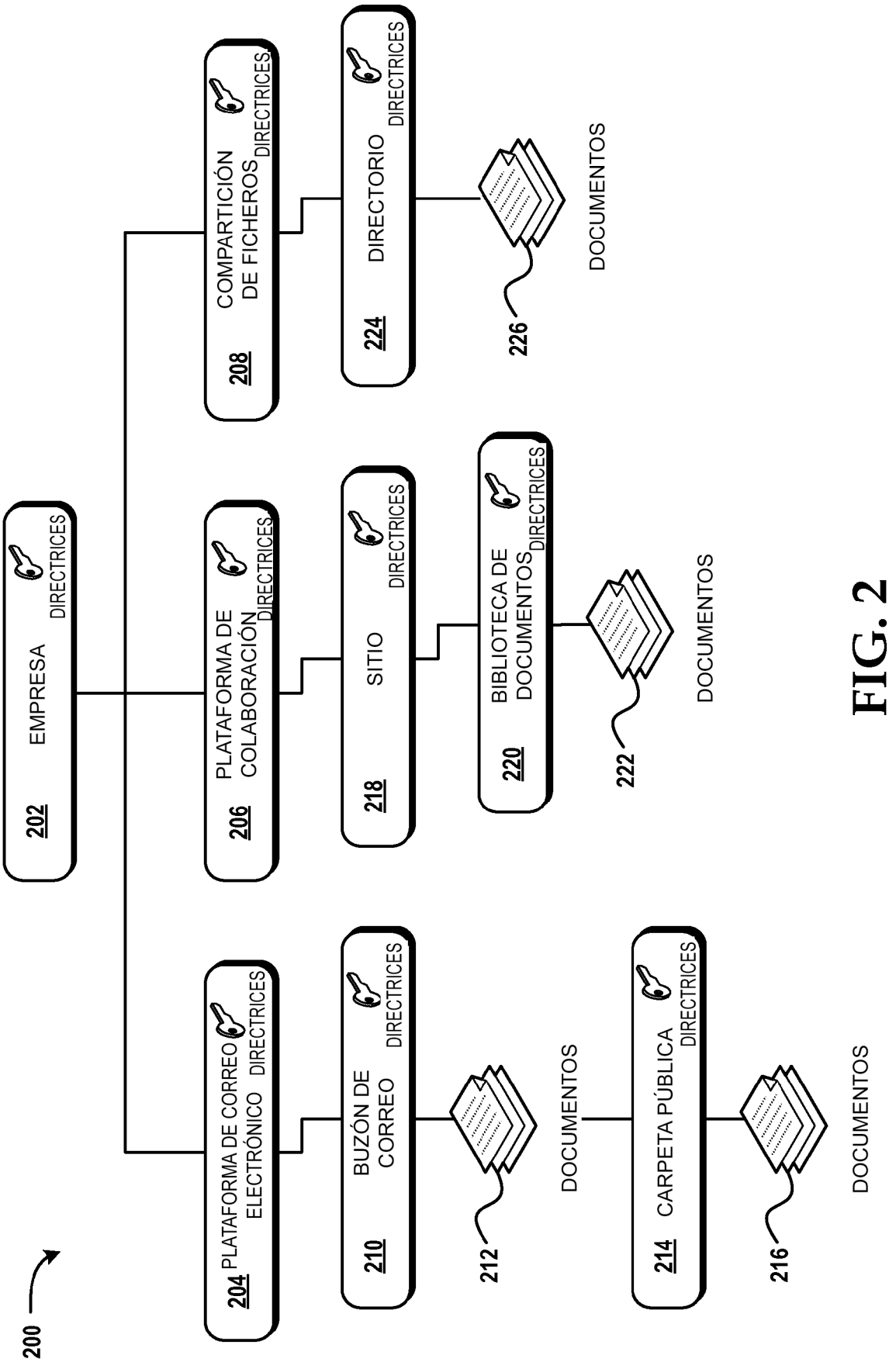
200
202 EMPRESA
DIRECTRICES
204 PLATAFORMA DE CORREO ELECTRÓNICO
DIRECTRICES
206 PLATAFORMA DE COLABORACIÓN
DIRECTRICES
208 COMPARTICIÓN DE FICHEROS
DIRECTRICES
210 BUZÓN DE CORREO
DIRECTRICES
212
DOCUMENTOS
214 CARPETA PÚBLICA
DIRECTRICES
216
DOCUMENTOS
218 SITIO
DIRECTRICES
220 BIBLIOTECA DE DOCUMENTOS
DIRECTRICES
222
DOCUMENTOS
224 DIRECTORIO
DIRECTRICES
226
DOCUMENTOS

FIG. 2

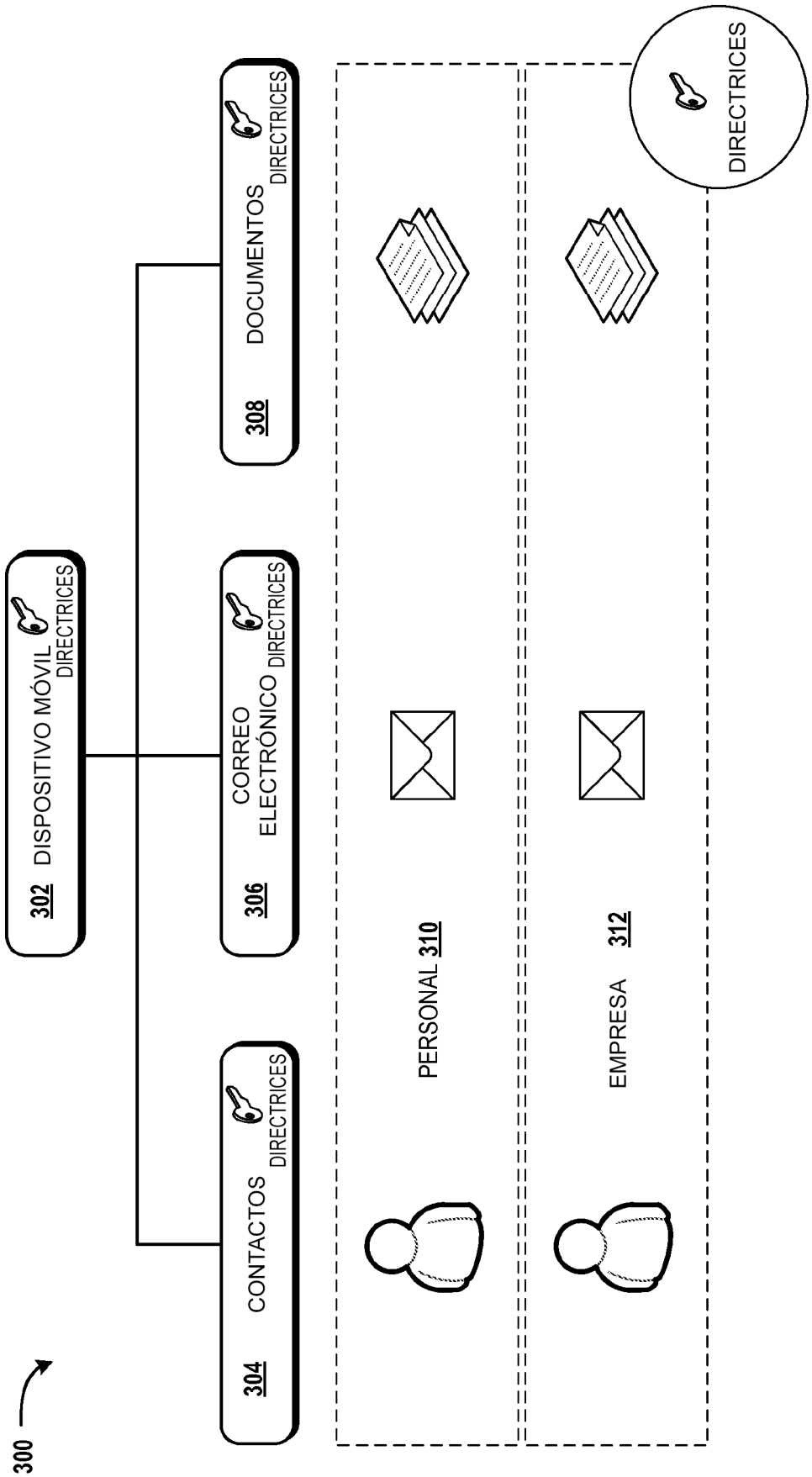
300
302 DISPOSITIVO MÓVIL DIRECTRICES
304 CONTACTOS DIRECTRICES
306 CORREO ELECTRÓNICO DIRECTRICES
308 DOCUMENTOS DIRECTRICES
DIRECTRICES
PERSONAL 310
EMPRESA 312

FIG. 3

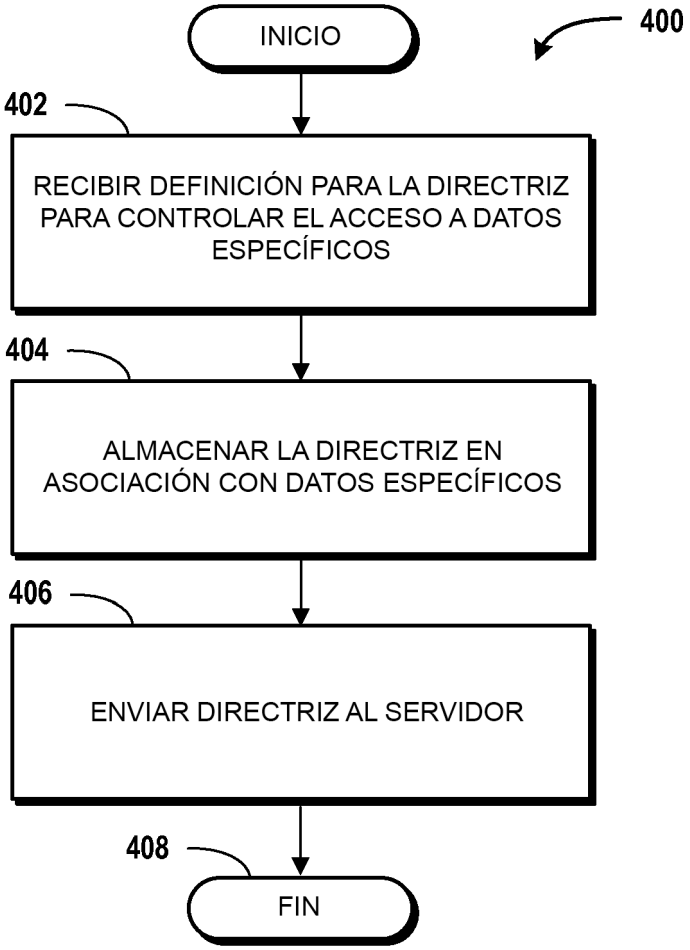
INICIO
400
402
RECIBIR DEFINICIÓN PARA LA DIRECTRIZ PARA CONTROLAR EL ACCESO A DATOS ESPECÍFICOS
404
ALMACENAR LA DIRECTRIZ EN ASOCIACIÓN CON DATOS ESPECÍFICOS
406
ENVIAR DIRECTRIZ AL SERVIDOR
408
FIN

FIG. 4

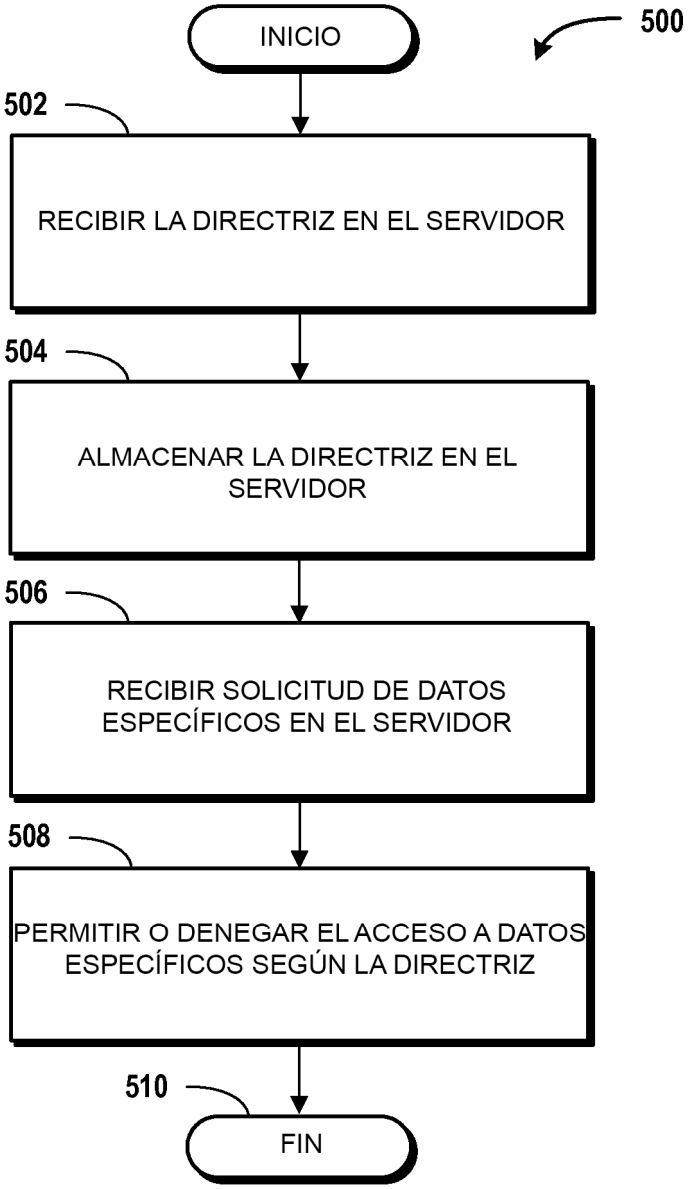
INICIO
500
502
RECIBIR LA DIRECTRIZ EN EL SERVIDOR
504
ALMACENAR LA DIRECTRIZ EN EL SERVIDOR
506
RECIBIR SOLICITUD DE DATOS ESPECÍFICOS EN EL SERVIDOR
508
PERMITIR O DENEGAR EL ACCESO A DATOS ESPECÍFICOS SEGÚN LA DIRECTRIZ
510
FIN

FIG. 5

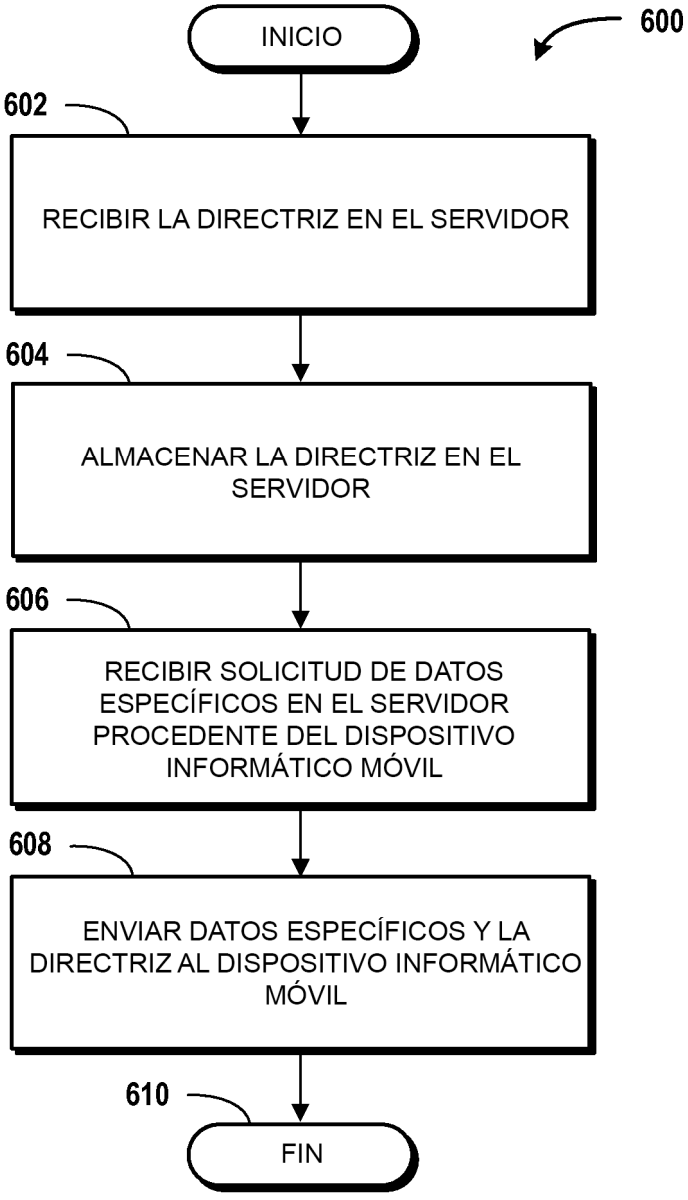
INICIO
600
602
RECIBIR LA DIRECTRIZ EN EL SERVIDOR
604
ALMACENAR LA DIRECTRIZ EN EL SERVIDOR
606
RECIBIR SOLICITUD DE DATOS ESPECÍFICOS EN EL SERVIDOR PROCEDENTE DEL DISPOSITIVO INFORMÁTICO MÓVIL
608
ENVIAR DATOS ESPECÍFICOS Y LA DIRECTRIZ AL DISPOSITIVO INFORMÁTICO MÓVIL
610
FIN

FIG. 6

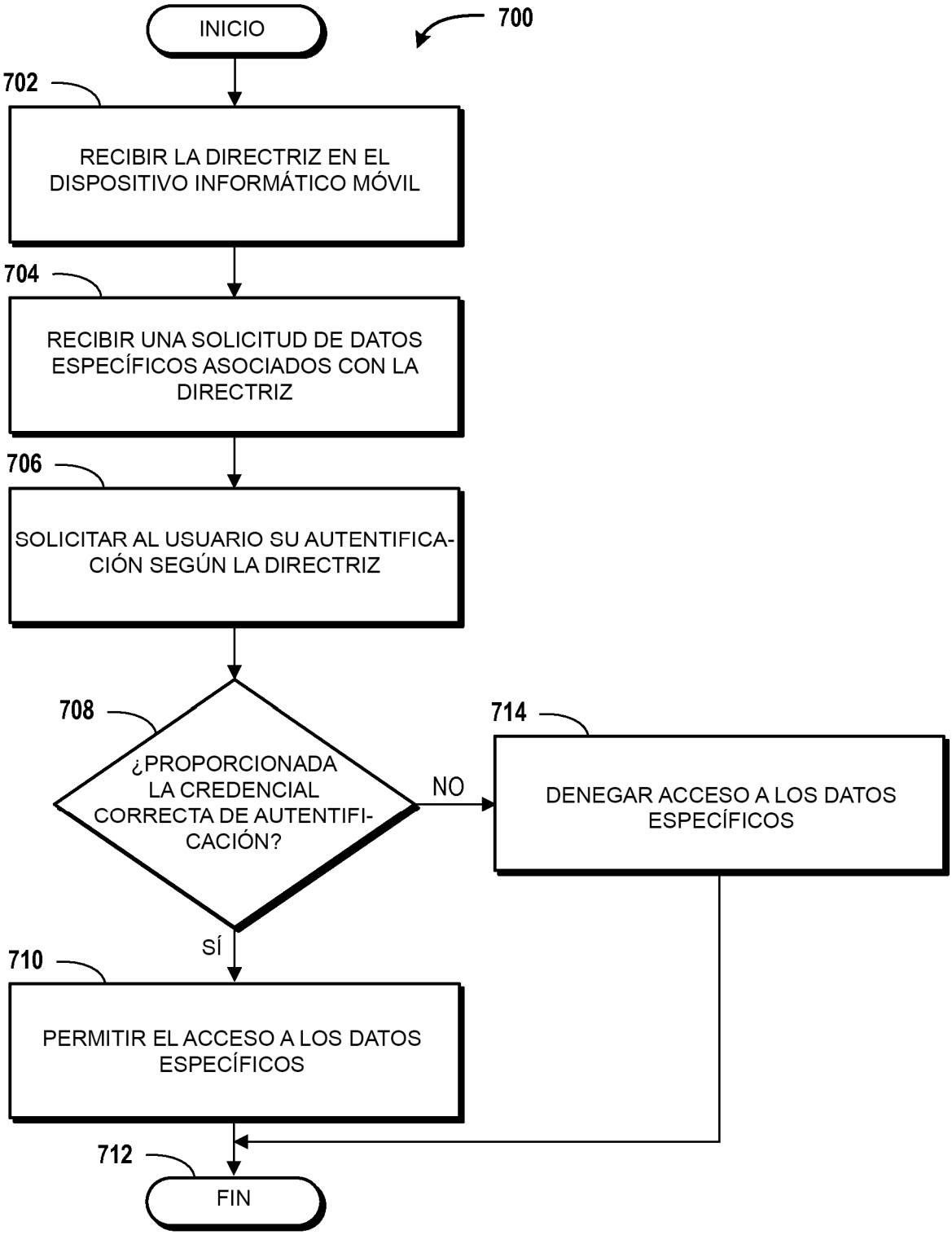
INICIO
700
702
RECIBIR LA DIRECTRIZ EN EL DISPOSITIVO INFORMÁTICO MÓVIL
704
RECIBIR UNA SOLICITUD DE DATOS ESPECÍFICOS ASOCIADOS CON LA DIRECTRIZ
706
SOLICITAR AL USUARIO SU AUTENTIFICACIÓN SEGÚN LA DIRECTRIZ
708
¿PROPORCIONADA LA CREDENCIAL CORRECTA DE AUTENTIFICACIÓN?
NO
714
DENEGAR ACCESO A LOS DATOS ESPECÍFICOS
SÍ
710
PERMITIR EL ACCESO A LOS DATOS ESPECÍFICOS
712
FIN

FIG. 7

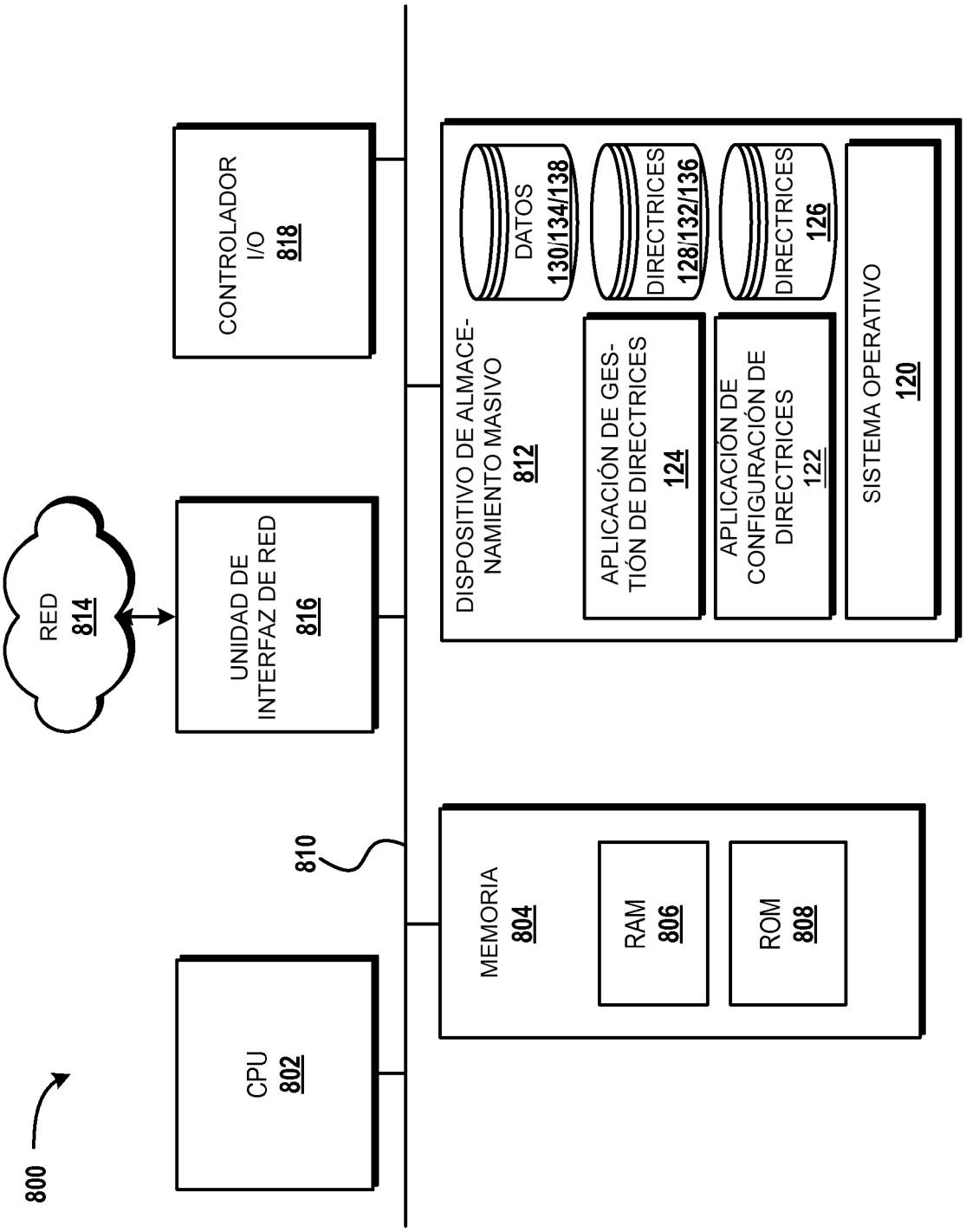
800
CPU
802
810
MEMORIA
804
RAM
806
ROM
808
UNIDAD DE INTERFAZ DE RED
816
RED
814
CONTROLADOR I/O
818
DISPOSITIVO DE ALMACE-NAMIENTO MASIVO
812
DATOS
130/134/138
DIRECTRICES
128/132/136
DIRECTRICES
126
APLICACIÓN DE GES-TIÓN DE DIRECTRICES
124
APLICACIÓN DE CONFIGURACIÓN DE DIRECTRICES
122
SISTEMA OPERATIVO
120

FIG. 8