(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 760 627**

(51) Int. CI.:

***G06F 21/60*** (2013.01)
***G06F 21/62*** (2013.01)
***H04L 29/06*** (2006.01)
***H04L 29/08*** (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **10.04.2015 PCT/US2015/025419**

(87) Fecha y número de publicación internacional: **15.10.2015 WO15157699**

(96) Fecha de presentación y número de la solicitud europea: **10.04.2015 E 15777161 (9)**

(97) Fecha y número de publicación de la concesión europea: **11.09.2019 EP 3129912**

(54) Título: **Procedimiento y sistema para asegurar los datos**

(30) Prioridad:

**10.04.2014 US 201461977830 P**
**12.01.2015 US 201562102266 P**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**14.05.2020**

(73) Titular/es:

**ATOMIZER GROUP, LLC (100.0%)**
**250 West Old Wilson Bridge Road**
**Worthington, OH 43085, US**

(72) Inventor/es:

**PARKER, ERIC y**
**YOUNGEN, RALPH**

(74) Agente/Representante:

**PADIAL MARTÍNEZ, Ana Belén**

## DESCRIPCIÓN

Procedimiento y sistema para asegurar los datos

### I. Referencia cruzada a solicitudes relacionadas

Esta solicitud reivindica el beneficio de la solicitud provisional de Estados Unidos n.º 61/977.830, presentada el 10 de abril de 2014, y de la solicitud provisional de Estados Unidos n.º 62/102.266, presentada el 27 de enero de 2015.

### II. Antecedentes

La presente invención pertenece a la técnica de almacenar y recuperar datos de forma segura y confidencial en muchos tipos de medios de almacenamiento, incluidos los datos almacenados y recuperados mediante la Internet pública, también conocida como la "nube". Los medios de almacenamiento portátiles, como unidades USB, tarjetas SD y teléfonos celulares pueden almacenar grandes cantidades de datos, pero típicamente no tienen o tienen medios limitados para proteger los datos que contienen. El almacenamiento de datos en la nube los pone en riesgo de verse comprometidos, ya sea por intercepción durante la transmisión al proveedor de servicios en la nube o por pirateo del proveedor de servicios cuando se almacenan los datos. El cifrado de archivos típico usa HTTPS durante la transmisión y el cifrado de disco por parte del proveedor de servicios en la nube cuando se almacenan los datos; ambos ponen las claves bajo el control de los proveedores de servicios y requieren que el usuario confíe en que las claves de acceso de cifrado son seguras, no pirateadas, tomadas por empleados desleales u obligadas a entregarlas al gobierno. E incluso si las claves de cifrado se mantienen seguras, una vez que un pirata informático adquiere los archivos, los archivos están bajo el control del pirata informático. En ese punto, se pueden aplicar grandes recursos computacionales para descifrar los archivos, o los archivos se pueden conservar hasta que las tecnologías de descifrado mejoren.

Los procedimientos actuales de cifrado de clave privada y pública usan una pequeña cantidad de datos aleatorios (un vector de inicialización y una clave) junto con un algoritmo determinista para desordenar la información en datos seguros. La debilidad es el algoritmo determinista y el tamaño de la aleatoriedad para comenzar el proceso de cifrado.

Los algoritmos de dispersión de información (IDA) separan los datos confidenciales para su transmisión y almacenamiento para dificultar la recomposición de los datos confidenciales. Sin embargo, los paquetes dispersos pasan por "puntos de estrangulamiento" en la red a través de los cuales se encaminan todos los paquetes y, de este modo, se pueden recopilar (por ejemplo, mediante rastreadores o mediante el proveedor de servicios de Internet). Estos paquetes dispersos tienen encabezados que pueden usarse para reensamblar los datos confidenciales. Además, los servicios de almacenamiento en la nube pueden añadir sus propios encabezados a los paquetes dispersos de datos confidenciales almacenados por los servicios, donde los encabezados también pueden usarse para recopilar y reensamblar los datos confidenciales.

Las transformaciones de todo o nada (AONT) requieren la recopilación de todos los trozos de un secreto para descifrar el secreto. AONT depende de que un mal actor no pueda recopilar todos los trozos de un secreto (por ejemplo, todos los trozos fragmentados de datos confidenciales dispersos). Sin embargo, la transmisión de datos confidenciales protegidos por AONT en la nube requiere que los datos pasen por los mismos puntos de estrangulamiento como se ha analizado anteriormente, lo que hace probable que todos los trozos se puedan recopilar y, de este modo, descriptar o descifrar.

A partir del documento US 2008/0060085 A1, se sabe que un archivo electrónico puede descomponerse en un número de fragmentos. Los fragmentos pueden ensamblarse aleatoriamente en un número de archivos de fragmentos, que pueden almacenarse aleatoriamente en diferentes ubicaciones en uno o más dispositivos de almacenamiento y/o en una red. Uno o más de los fragmentos y/o archivos de fragmentos pueden cifrarse o protegerse de otra manera. Se pueden generar instrucciones (por ejemplo, ubicaciones de archivos de fragmentos, instrucciones de ensamblaje de fragmentos) para restaurar el archivo electrónico a partir de los fragmentos. Las instrucciones y otra información (claves de descifrado) para restaurar el archivo electrónico pueden residir en una aplicación protegida. La aplicación protegida puede dejarse inoperativa deliberadamente hasta que la aplicación protegida se vincule dinámicamente en tiempo de ejecución con un módulo de seguridad obtenido, por ejemplo, de un servicio de seguridad. Se pueden aplicar niveles variables de protección (por ejemplo, si se usa o no una aplicación protegida) a archivos electrónicos en base a atributos de archivo. A partir del documento US 2006/0045270 A1, se sabe que utiliza un sistema y un procedimiento para aleatorizar datos de acuerdo con un mapa, que puede ser definido por el usuario, de manera que el orden secuencial en el que deben leerse los datos está determinado por el mapa. En lugar de emplear una fórmula matemática para aleatorizar los datos, los datos pueden separarse en una pluralidad de fragmentos. Luego se selecciona un mapa para determinar el orden de los fragmentos, de manera que sin el mapa, los fragmentos no pueden ensamblarse en el orden correcto.

Los usuarios deberían poder compartir y almacenar archivos de forma segura, incluso a través de Internet, manteniendo el control de las claves e impidiendo el acceso a sus archivos. Con objeto de limitar el riesgo de compromiso, se divulgan este procedimiento y sistema.

**III. Sumario**

De acuerdo con un aspecto de la presente invención, un procedimiento para asegurar los datos de usuario como se define en la reivindicación 1 incluye las etapas de: a) establecer los datos de usuario como datos de entrada; b) fragmentar aleatoriamente los datos de entrada en una pluralidad de Átomos, donde un Átomo se define como al menos un bit de datos, y distribuir aleatoriamente los Átomos en una AgrupaciónDeÁtomos y una ClaveDeÁtomos, cada una de las cuales se define como un bloque de almacenamiento de datos o memoria diferente de, pero relacionada con, el otro; y c) registrar información sobre la fragmentación y la distribución de la etapa b) en instrucciones llamadas un MapaDeÁtomos; en el que: la AgrupaciónDeÁtomos y ClaveDeÁtomos preexisten la distribución de la etapa b); la AgrupaciónDeÁtomos de la etapa b) se divide en un número de zonas, el número que es Z-1, y con la ClaveDeÁtomos que es la zona Z; y la distribución de la etapa b) comprende las etapas de: d) seleccionar aleatoriamente la zona en la que se distribuye un Átomo, en el que la selección de zona se produce por separado para cada Átomo; e) copiar cada Átomo a la zona seleccionada para ese Átomo en la etapa d), empezando en un índice de zona para esa zona, sobrescribiendo cualquier dato que exista en la ubicación donde se copia cada Átomo; y f) mover el índice de zona de cada zona en la que se ha copiado cualquier Átomo en la etapa e) a una ubicación inmediatamente después de la ubicación donde se copia el Átomo. Otras características de este procedimiento se definen en las reivindicaciones del procedimiento dependiente adjuntas.

De acuerdo con otro aspecto de la presente invención, un medio no transitorio legible por ordenador incluye instrucciones para hacer que un ordenador realice el procedimiento anterior.

De acuerdo con otro aspecto más de la presente invención, un sistema para asegurar los datos de usuario incluye un primer ordenador y un segundo ordenador en comunicación con el primer ordenador; en el que el primer ordenador está programado para ejecutar algunas etapas del procedimiento anterior y comunicar la AgrupaciónDeÁtomos, la ClaveDeÁtomos y el MapaDeÁtomos final al segundo ordenador; y en el que el segundo ordenador está programado para ejecutar las otras etapas del procedimiento anterior.

Aún otros beneficios y ventajas de la invención serán evidentes para los expertos en la técnica a los que pertenece tras una lectura y comprensión de la siguiente memoria descriptiva detallada.

**IV. Breve descripción de los dibujos**

La invención puede tomar forma física en ciertas partes y disposición de partes, modos de realización de las cuales se describirán en detalle en esta memoria descriptiva y se ilustrarán en los dibujos adjuntos que forman parte de la misma y en la que:

La FIGURA 1 es un diagrama de un modo de realización del sistema.

La FIGURA 2 es una descripción general esquemática principal de un proceso de acuerdo con un modo de realización.

La FIGURA 3 es una descripción general esquemática del proceso de atomización de acuerdo con un modo de realización.

La FIGURA 4 es una descripción general esquemática del proceso de manejo de la ClaveDeÁtomos de acuerdo con un modo de realización.

La FIGURA 5 es una descripción general esquemática del proceso de desatomización de acuerdo con un modo de realización.

La FIGURA 6 muestra una leyenda para las FIGURAS 3-26.

La FIGURA 7 es un esquema de la función Autorizar Atomizar de acuerdo con un modo de realización.

La FIGURA 8 es un esquema de la función Atomizar de acuerdo con un modo de realización.

La FIGURA 9 es un esquema de la función AtomizarDatos de acuerdo con un modo de realización.

La FIGURA 10 es un esquema de la función DivisorÁtomo de acuerdo con un modo de realización.

La FIGURA 11 es un esquema de la función Construir Átomos de acuerdo con un modo de realización.

La FIGURA 12 es un esquema de la función Gestor CargaDeÁtomo de acuerdo con un modo de realización.

La FIGURA 13 es un esquema de la función Producir ClaveDeÁtomos de acuerdo con un modo de realización.

La FIGURA 14 es un esquema de la función Exportar ClaveDeÁtomos de acuerdo con un modo de realización.

La FIGURA 15 es un esquema de la función Importar ClaveDeÁtomos de acuerdo con un modo de realización.

La FIGURA 16 es un esquema de la función Revertir MapaDeUnMapaDeÁtomos de acuerdo con un modo de realización.

La FIGURA 17 es un esquema de la función Autorizar Reensamblar de acuerdo con un modo de realización.

La FIGURA 18 es un esquema de la función Reensamblar de acuerdo con un modo de realización.

La FIGURA 19 es un esquema de la función ReensamblarDatos de acuerdo con un modo de realización.

La FIGURA 20 es un esquema de la función Reconstruir de acuerdo con un modo de realización.

La FIGURA 21 es un esquema de la función Gestor DescargaDeÁtomo de acuerdo con un modo de realización.

La FIGURA 22a es un esquema de la función Transportar ClaveDeÁtomos de acuerdo con un modo de realización.

La FIGURA 22b es un esquema de la función Almacenamiento ClaveDeÁtomos de acuerdo con un modo de realización.

La FIGURA 23 es un esquema de la función Gestor CargaDeÁtomo de acuerdo con otro modo de realización.

La FIGURA 24 es un esquema de la función Gestor DescargaDeÁtomo de acuerdo con otro modo de realización.

La FIGURA 25 es una descripción general esquemática de un proceso de acuerdo con otro modo de realización.

La FIGURA 26 es una descripción general esquemática de un proceso de acuerdo con otro modo de realización más.

La FIGURA 27 es una descripción general esquemática principal de un proceso de acuerdo con otro modo de realización.

La FIGURA 28 es una descripción general esquemática del proceso de atomización de acuerdo con otro modo de realización.

La FIGURA 29 es un esquema de la función AtomizarDatos de acuerdo con un modo de realización.

La FIGURA 30 es un esquema de la función VectorizaciónAtómica de acuerdo con un modo de realización.

La FIGURA 31 es un esquema de la función Seleccionar Átomos de acuerdo con un modo de realización

La FIGURA 32 es un diagrama que muestra un Selector y un SelectorDeTabla de acuerdo con un modo de realización.

La FIGURA 33 es un esquema del proceso de transporte/almacenamiento de acuerdo con un modo de realización.

La FIGURA 34 es un esquema del proceso de transporte/almacenamiento de acuerdo con otro modo de realización.

La FIGURA 35 es un esquema del proceso de transporte/almacenamiento de acuerdo con otro modo de realización.

La FIGURA 36 es un esquema del proceso de transporte/almacenamiento de acuerdo con otro modo de realización.

La FIGURA 37 es un esquema del proceso de transporte/almacenamiento de acuerdo con otro modo de realización.

La FIGURA 38 es un diagrama del proceso de atomización de acuerdo con un modo de realización.

La FIGURA 39 es un diagrama de dos dispositivos que comparten datos atomizados de acuerdo con un modo de realización.

La FIGURA 40 es un diagrama de un dispositivo que obtiene una LibretaDeÁtomos de acuerdo con un modo de realización.

**V. Glosario**

En esta memoria descriptiva, los términos que se definen a continuación tienen los significados respectivos siguientes:

Átomo: al menos un bit de datos.

Atomizar: fragmentar y aleatorizar los datos.

ClaveDeÁtomos - un bloque de almacenamiento de datos o memoria diferente de, pero relacionado con, la AgrupaciónDeÁtomos.

MapaDeÁtomos - instrucciones sobre la atomización de datos; se usa para desatomizar datos atomizados.

AgrupaciónDeÁtomos - un bloque de almacenamiento de datos o memoria diferente de, pero relacionado con, la ClaveDeÁtomos.

Desatomizar - para desaleatorizar y reensamblar datos atomizados.

**VI. Descripción detallada**

Con referencia ahora a los dibujos en los que las presentaciones tienen el propósito de ilustrar modos de realización de la invención solamente y no el propósito de limitar los mismos, y en los que se entiende que los números de referencia similares se refieren a componentes similares, la FIGURA 1 muestra un diagrama de un modo de realización del sistema 100. El sistema 100 puede incluir un primer ordenador 102, que puede ser el ordenador del usuario que desea compartir archivos de datos 104 (o datos de usuario 104) con otra persona. El usuario también puede desear simplemente asegurar y almacenar los datos de usuario 104. El primer ordenador 102 puede incluir, pero no se limita a, un ordenador personal, un ordenador de mesa, un ordenador portátil, un teléfono móvil, un dispositivo móvil, un asistente personal digital y una tableta electrónica. Un ordenador puede incluir un procesador (incluida una CPU) y memoria. Un ordenador puede incluir al menos un dispositivo de entrada (que incluye un teclado, un teclado, una alfombrilla táctil, una pantalla táctil, un ratón, una palanca de mando y una bola de seguimiento) y al menos un dispositivo de salida (que incluye una pantalla y una impresora). Un ordenador puede incluir una interfaz de comunicación que le permita comunicarse con otros dispositivos, ordenadores o la nube 108. Un ordenador puede incluir un dispositivo de almacenamiento y puede incluir un puerto de conexión para la conexión de dispositivos de almacenamiento externo.

El primer ordenador 102 puede incluir una aplicación de software 106 para "atomizar" los archivos de datos 104, como se describirá más adelante. La aplicación 106 puede ser, en modos de realización alternativos, una aplicación nativa o puede ser un navegador de Internet que ejecuta una aplicación basada en Internet (o basada en la nube). El usuario puede usar la aplicación 106 para seleccionar los archivos de datos 104 a atomizar. Durante la atomización, la aplicación 106 puede cifrar los archivos de datos 104 (que pueden ser cifrado AES256 con claves aleatorias largas), separar aleatoriamente los archivos cifrados a nivel de bit en segmentos disociados (llamados "Átomos" 1102) de bits (donde a los Átomos 1102 se les puede dar nombres o identificaciones aleatorias largas), generar átomos (llamados "Átomos paja" o Átomos falsos que no se pueden distinguir de los Átomos 1102 reales) de datos aleatorios que no forman parte de los archivos de datos 104 y transmitir todos los Átomos 1102 (incluidos los Átomos paja) a la nube 108 en orden aleatorio para su almacenamiento en dispositivos, sitios o zonas de almacenamiento seleccionados al azar 110. La nube 108 puede albergar numerosos Átomos 1102 de diversos usuarios sin información sobre cómo reensamblarlos y descifrarlos 1102. La transmisión a y recepción desde la nube 108 puede realizarse a través de una conexión segura, como HTTPS.

La aplicación 106 puede crear una clave (llamada "ClaveDeÁtomos" 304) sobre cómo encontrar los Átomos 1102, reintegrarlos 1102, descifrar los datos y restaurar los archivos de datos 104. En un modo de realización, el sistema 100 también puede requerir una frase de paso junto con la clave para atomizar y desatomizar los archivos de datos 104. El usuario puede crear una frase de paso e introducirla en la aplicación 106 durante la atomización. La frase de paso puede ser una clave privada PKI donde la ClaveDeÁtomos 304 se puede cifrar con una clave pública PKI en un modo de realización.

En un modo de realización, el usuario puede escanear o tomar una fotografía de la ClaveDeÁtomos 304 desde la pantalla del primer ordenador 102 usando un primer teléfono móvil 112. Después de capturar la ClaveDeÁtomos 304 en el primer teléfono móvil 112, el usuario puede enviar la fotografía de la ClaveDeÁtomos 304 a un segundo teléfono móvil 114 propiedad del destinatario de los archivos de datos 104. La transmisión de la ClaveDeÁtomos 304 se puede realizar enviando un mensaje de texto, que incluye un mensaje de texto multimedia, MMS o SMS. En otro modo de realización, el usuario puede imprimir la ClaveDeÁtomos 304 y enviarla por correo o entregarla físicamente al destinatario. En otro modo de realización, cualquiera del primer teléfono móvil 112 y el segundo teléfono móvil 114 puede ser una tableta electrónica, un ordenador, un asistente personal digital (PDA), un reproductor multimedia u otro dispositivo móvil. En un modo de realización, el usuario también puede transferir la frase de paso al destinatario, que puede incluir, pero no se limita a, llamar y decirle al destinatario cuál es la frase de paso, enviar físicamente la frase de paso al destinatario, transferir electrónicamente la frase de paso al destinatario (por ejemplo, guardando la frase de paso en una unidad USB, CD o tarjeta de memoria, o enviando un mensaje de texto con la frase de paso), o visitando personalmente y diciéndole al destinatario cuál es la frase de paso. Un proceso fuera de banda para enviar la ClaveDeÁtomos 304 y la frase de paso puede mejorar la seguridad.

Al menos uno de entre el primer teléfono móvil 112 y el segundo teléfono móvil 114 puede incluir una aplicación de software que está diseñada para capturar la ClaveDeÁtomos 304, transmitirla a un destinatario y recibirla del usuario o emisor.

El destinatario puede usar un segundo ordenador 116 para ejecutar también la aplicación de software 106 y recuperar los archivos de datos atomizados 104. En un modo de realización, la aplicación 106 para atomizar los archivos de datos 104 y la aplicación 106 para desatomizar los archivos de datos 104 son iguales; la aplicación 106

incluye funcionalidad para hacer ambas cosas. En otro modo de realización, se pueden usar diferentes aplicaciones, una para atomizar archivos de datos 104 y otra para desatomizar archivos de datos 104.

El destinatario puede transferir la ClaveDeÁtomos 304 recibida (por ejemplo, desde el segundo teléfono móvil 114; desde una unidad USB, tarjeta de memoria o CD; o como sea que se reciba) al segundo ordenador 116 en la aplicación 106. En un modo de realización, el destinatario puede usar una cámara del segundo ordenador 116 para capturar una fotografía de la ClaveDeÁtomos 304 desde el segundo teléfono móvil 114. En un modo de realización, el destinatario también introduce la frase de paso recibida en la aplicación 106.

La aplicación 106 puede desatomizar los archivos de datos 104 usando la ClaveDeÁtomos 304 para reunir los Átomos 1102 (incluidos los Átomos paja 1102) de la nube 108 en orden aleatorio, descartar los Átomos paja 1102, reensamblar los Átomos 1102 en archivos cifrados y descifrar los archivos cifrados en los archivos de datos 104 que el usuario pretendía compartir con el destinatario. El destinatario puede usar los archivos de acuerdo con lo previsto.

La FIGURA 2 muestra una descripción general esquemática principal de un proceso 200 de acuerdo con un modo de realización. Este proceso puede incluir un proceso de atomización 202, un proceso de manejo de ClaveDeÁtomos 204 y un proceso de desatomización 206, cada uno de los cuales se analiza a continuación. El proceso de atomización 202 puede realizarse en un primer ordenador 102. El proceso de desatomización 206 puede realizarse en un segundo ordenador 116.

La FIGURA 3 muestra una descripción general esquemática del proceso de atomización 202 de acuerdo con un modo de realización. Una leyenda para los objetos que se muestran en las FIGURAS 3-26 se muestra en la FIGURA 6. Este proceso 202 puede incluir una función Autorizar Atomizar 300, que puede verificar con los servicios web antes de permitir la atomización y antes de proporcionar la información necesaria para atomizar los archivos de datos de usuario o los datos de usuario 104. Este 300 se analiza más adelante con respecto a la FIGURA 7. Las entradas a la función Autorizar Atomizar 300 pueden incluir los datos de usuario 104 y la información de usuario 302. Esta información de usuario 302 puede ser información que identifica de forma única al usuario con el sistema 100 y puede incluir un nombre, una dirección de correo electrónico, una identificación biométrica, una contraseña o cualquier otro medio de identificación o combinación de los mismos. La información de usuario 302 puede permitir que el sistema 100 le cobre al usuario por usar el sistema 100, realizar el seguimiento de las ClavesDeÁtomos 304 para su almacenamiento y reensamblaje, y matar ClavesDeÁtomos 304 para impedir su reensamblaje. La función Autorizar Atomizar 300 puede generar información de autorización 306, que puede ser información usada para prepararse para atomizar los datos de usuario 104. La información de autorización 306 puede incluir IDClaveDeÁtomos, IDÁtomo y AgrupaciónDeAlmacenamiento, y también cualquier instrucción para eliminar Átomos 1102 almacenados en el caso de una respuesta de la función Autorizar Reensamblar 502. En un modo de realización, la información de autorización 306 puede no ser secreta.

El proceso de atomización 202 puede incluir después una función Atomizar 308, que se describe más adelante con respecto a la FIGURA 8. Esta función 308 puede tomar datos de usuario 104, atomizarlos y devolver un MapaDeUnMapaDeÁtomos 310, que es un MapaDeÁtomos 806 que contiene información sobre un MapaDeÁtomos 806 atomizado. El MapaDeUnMapaDeÁtomos 310 puede ser el mapa de información completo y utilizable para reensamblar los datos de usuario 104.

El proceso de atomización 202 puede incluir después una función Producir ClaveDeÁtomos 312, que se describe más adelante con respecto a la FIGURA 13. Esta función 312 puede convertir un MapaDeUnMapaDeÁtomos 310 en una ClaveDeÁtomos 304, que puede ser un conjunto de bytes pequeño, conciso y bloqueado/cifrado que puede codificarse en formas fácilmente almacenadas y transmitidas que pueden usarse para invertir el proceso de atomización y reensamblar los datos de usuario 104 de dispositivos de almacenamiento de red o medios 110. La función Producir ClaveDeÁtomos 312 puede recibir como entrada un Bloqueo de Clave 314, que puede ser una clave privada o una clave pública. La función 312 también puede recibir como Información de Clave 316 de entrada, que puede ser información (que puede ser pública o no secreta) que puede estar incluida como parte de la ClaveDeÁtomos 304 exportada y mejorada; esta Información de Clave 316 puede incluir comentarios, notas, logotipos, información de marca e información de dirección (incluidos los campos "De" y "Para").

El proceso de atomización 202 puede incluir después una función Exportar ClaveDeÁtomos 318, que se describe más adelante con respecto a la FIGURA 14. Esta función 318 puede codificar la ClaveDeÁtomos 304 en una forma utilizable para su transmisión, almacenamiento o transporte.

La FIGURA 4 muestra una descripción general esquemática del proceso de manejo de ClaveDeÁtomos 204 de acuerdo con un modo de realización. El proceso de atomización 202 puede producir una ClaveDeÁtomos 304 que puede usarse para reensamblar los datos de usuario 104. El usuario puede transportar esta ClaveDeÁtomos 304 a un destinatario para compartir los datos de usuario 104, o el usuario puede almacenar la ClaveDeÁtomos 304 para permitir su reensamblaje futuro. Este proceso de manejo de ClaveDeÁtomos 204 puede realizarse en los dispositivos de origen o de destino (por ejemplo, el primer teléfono móvil 112 y el segundo teléfono móvil 114). El proceso de atomización 202 y la creación de la ClaveDeÁtomos 304 pueden producirse en el primer ordenador 102, la ClaveDeÁtomos 304 puede ser segura porque nunca ha entrado en la nube 108, y el control de cuándo y cómo transportar la ClaveDeÁtomos 304 puede estar solo con el usuario.

Este proceso de manejo de ClaveDeÁtomos 204 puede incluir una función Importar ClaveDeÁtomos 400, que se describe más adelante con respecto a la FIGURA 15. Esta función 400 puede recopilar y decodificar una ClaveDeÁtomos Renderizada 1404 mejorada y codificada, que se ha exportado en una forma utilizable para su transmisión, almacenamiento o transporte a la ClaveDeÁtomos 304 sencilla.

El proceso de manejo de ClaveDeÁtomos 204 puede incluir después una función Transportar/Almacenar ClaveDeÁtomos 402, que puede ser dos funciones separadas (Transportar ClaveDeÁtomos 2208 y Almacenar ClaveDeÁtomos 2210) que se describen más adelante con respecto a las FIGURAS 22a-b. La atomización de los datos de usuario 104 puede dar como resultado una ClaveDeÁtomos 304 altamente comprimida, cifrada y fácilmente compartida o almacenada. Gracias al pequeño tamaño y la seguridad intrínseca de la ClaveDeÁtomos 304, puede transportarse de manera fácil y eficaz en una amplia variedad de protocolos y medios de transmisión. Estos protocolos y medios de transmisión pueden proporcionar niveles adicionales de seguridad, ya que utilizan el transporte fuera de banda (mecanismo de transporte diferente al de los datos atomizados). Estos protocolos y medios pueden estar casi fuera de banda, como las tecnologías SMS o MMS, o más como fax u otros medios de modulación de audio, o incluso mensajeros o el Servicio Postal de los EE. UU. que entrega una ClaveDeÁtomos 304 física que se ha impreso. El almacenamiento de ClavesDeÁtomos 304 es eficaz (debido a un tamaño muy pequeño) y seguro puesto que las ClavesDeÁtomos 304 están cifradas y los datos de usuario reales 104 han sido atomizados. La ClaveDeÁtomos 304 y el Bloqueo de Clave 314 necesarios para desbloquear la ClaveDeÁtomos 304 pueden transmitirse cada uno en una banda diferente entre sí y fuera de banda con los datos almacenados para mejorar la seguridad.

El proceso de manejo de ClaveDeÁtomos 204 puede incluir después una función Exportar ClaveDeÁtomos 318, que puede operar como se ha analizado anteriormente con respecto a la FIGURA 3.

La FIGURA 5 muestra una descripción general esquemática del proceso de desatomización 206 de acuerdo con un modo de realización. Este proceso 206 puede incluir una función Importar ClaveDeÁtomos 400, que puede operar como se ha analizado anteriormente con respecto a la FIGURA 4.

El proceso de desatomización 206 puede incluir después una función Revertir MapaDeUnMapaDeÁtomos 500, que se describe más adelante con respecto a la FIGURA 16. Esta función 500 puede revertir una ClaveDeÁtomos 304, que contiene información mínima concisa y cifrada usada para iniciar el reensamblaje de datos de usuario 104, en el MapaDeUnMapaDeÁtomos 310 completo y uniforme mediante el Bloqueo de Clave 314.

El proceso de desatomización 206 puede incluir después una función de Autorizar Reensamblar 502, que se describe más adelante con respecto a la FIGURA 17. Esta función 502 puede verificar con el sistema 100 antes de permitir y proporcionar la información de autorización necesaria 306 para reensamblar los datos de usuario 104.

El proceso de desatomización 206 puede incluir después una función Reensamblar 504, que se describe más adelante con respecto a la FIGURA 18. Esta función 504 puede usar un MapaDeUnMapaDeÁtomos 310 para reconstruir los datos de usuario 104. La función 504 puede recomponer la cadena inversa de MapaDeÁtomos (el MapaDeUnMapaDeÁtomos 310 puede recomponer otro MapaDeÁtomos 806 muy grande) hasta que se reensamblan los datos de usuario 104 originales almacenados.

La FIGURA 7 muestra un esquema de la función Autorizar Atomizar 300 de acuerdo con un modo de realización. Esta función 300 puede incluir una función Calc Tamaño 700, que puede determinar el tamaño de los datos de usuario 104 a atomizar antes de la atomización para asegurar el cumplimiento y el coste.

La función Autorizar Atomizar 300 puede incluir después una función Solicitar Atomizar 702, que puede preparar y enviar adecuadamente la información de solicitud 704 de servicio formateada al servicio, que puede estar alojado en la nube 108, para autorizar la atomización especificada. Este servicio puede proporcionar un IDClaveDeÁtomos, un IDAtomización y una Lista AlmacenamientoÁtomos para realizar la atomización y la desatomización; sin embargo, dicho servicio puede no tener conocimiento de los datos de usuario 104, Átomos 1102, MapasDeÁtomos 806 o ClavesDeÁtomos 304. Este servicio puede vender servicios de atomización a otros u ofrecer servicios de atomización a sus empleados. Esta información de solicitud 704 puede incluir datos que definen el tamaño de los datos de usuario 104 a atomizar (que puede ser el agregado de todos los datos de usuario seleccionados 104) y puede incluir información de autentificación del usuario. La información de solicitud 704 puede incluir información relacionada con el coste. Esta función 702 puede, en un modo de realización, enviar una solicitud de servicio de descanso HTTPS con datos posteriores que incluyen la información de solicitud 704. En un modo de realización, la transmisión puede ser una transmisión TLS (HTTPS) para su protección. La información de solicitud 704 puede ser información que no es secreta cuando ninguna parte del contenido de los datos de usuario 104 a atomizar se incluye en la información de solicitud 704.

La función Autorizar Atomizar 300 puede incluir después una función Autorizar Autentificación 706, que puede ser una función especializada en los servicios web (que pueden estar basados en la nube) del sistema 100 para verificar que la información de usuario 302 muestra un usuario existente (autentificación) y que la acción solicitada para atomizar datos (basada en el tamaño) está permitida bajo la cuenta del usuario (autorización). Esta función 706 puede recibir información del AlmacénDeDatos Usuario 708, que puede contener datos persistentes sobre los

usuarios registrados para usar el sistema 100. El AlmacénDeDatos Usuario 708, que puede almacenarse en la nube 108, puede usarse la facturación y el seguimiento, y puede no contener información sobre los datos, su contenido, seguridad o ubicación.

La función Autorizar Atomizar 300 puede incluir después una función Generar IDAtomización 710, que puede generar una gran identificación aleatoria (por ejemplo, 128 bits) que puede usarse en una generación SHA-256 del IDÁtomo MapaDeÁtomos final, que puede ser una identificación larga y aleatoria (por ejemplo, 20 bytes) que identifica de forma exclusiva un Átomo 1102 pero no tiene información sobre de qué es parte, de dónde proviene, qué contiene, cómo está organizado o cualquier otro significado. Esta completa falta de información o relación entre los IDÁtomo y los Átomos 1102, el MapaDeÁtomos 806 o la ClaveDeÁtomos 304 se traduce en seguridad. El IDÁtomo puede almacenarse en el AlmacénDeDatos IDClaveDeÁtomos 712, que puede almacenarse en la nube 108. El AlmacénDeDatos IDClaveDeÁtomos 712 puede contener datos persistentes sobre los IDClaveDeÁtomos y los IDÁtomo, y puede usarse para la facturación y realizar el seguimiento de las atomizaciones y reensamblajes. El AlmacénDeDatos 712 puede no contener información sobre los datos, su contenido, seguridad o ubicación; en su lugar, 712 puede contener información sobre cuándo se ha generado una ClaveDeÁtomos 304, cuándo expira 304 y cuándo se ha usado 304 para reensamblar los datos de usuario 104. Los Átomos 1102 solo se pueden recuperar con un MapaDeÁtomos 806 usando los IDÁtomo de los Átomos 1102.

La función Autorizar Atomizar 300 puede incluir después una función Generar IDClaveDeÁtomos 714, que puede generar una identificación única aleatoria y larga (por ejemplo, 128 bits) que puede usarse para identificar la ClaveDeÁtomos 304 eventual producida por el proceso de atomización 202. Esta identificación puede no contener información sobre los datos 104 que se están atomizando o que podrían usarse para asociar los datos atomizados por ubicación, nombre o contenido. Esta identificación puede almacenarse en el AlmacénDeDatos IDClaveDeÁtomos 712.

La función Autorizar Atomizar 300 puede incluir después una función Crear AgrupaciónDeAlmacenamiento 716, que puede generar una lista de posibles ubicaciones de almacenamiento de datos para almacenar los Átomos 1102 producidos durante el proceso de atomización 202. Durante el proceso de atomización 202, se pueden seleccionar aleatoriamente ubicaciones de almacenamiento de datos de entre esta lista para cada Átomo 1102. Dichos datos aleatorios también pueden mantenerse en el MapaDeÁtomos 806 y no transmitirse a los servicios en la nube 108. El IDÁtomo, el IDClaveDeÁtomos y la lista de agrupación de almacenamiento (AgrupaciónDeAlmacenamiento) pueden comprender conjuntamente la información de autorización 306.

La función Autorizar Atomizar 300 puede incluir después una función Responder 718, que puede devolver datos de una solicitud. Esta función 718 puede transportar la información de autorización 306 de vuelta al primer ordenador 102 que ha enviado la información de solicitud 704 en la función 702. La función Responder 718 puede realizar el formateo de datos requerido y transmitir los datos a través de la conexión entre la nube 108 y el primer ordenador 102. Los datos transmitidos pueden ser la información solicitada o una negativa a autorizar. La función Autorizar Autentificación 706, la función Generar IDAtomización 710, la función Generar IDClaveDeÁtomos 714, la función Crear AgrupaciónDeAlmacenamiento 716 y la función Responder 718 pueden ser realizadas por ordenadores de servicio en la nube 108 en un modo de realización. En otro modo de realización, al menos una de dichas funciones puede realizarse en el primer ordenador 102.

La función Autorizar Atomizar 300 puede incluir después una función Responder Atomizar 720, que puede funcionar con la función Responder 718 para recibir una respuesta a la información de solicitud enviada 704 para su uso posterior en el proceso de atomización 202. Esta transmisión del servicio puede producirse a través de TLS/HTTPS. Esta información puede que no contenga nada que sea secreto o que contenga información sobre los datos 104 a atomizar.

La FIGURA 8 muestra un esquema de la función Atomizar 308 de acuerdo con un modo de realización. Esta función 308 puede incluir una función Comprimir 800, que puede comprimir los datos de usuario 104 usando técnicas de compresión de datos estándar de la industria. El MapaDeÁtomos 806 puede incluir información sobre el tipo de compresión usada con fines de descompresión al final de la función Reensamblar 504. Los datos de usuario 104 pueden convertirse en un estado de datos intermedio 802 durante el procesamiento, por ejemplo después de la función Comprimir 800.

La función Atomizar 308 puede incluir después una función AtomizarDatos 804, que se describe más adelante con respecto a la FIGURA 9. Esta función 804 puede tomar cualquier dato, como los datos 802, y atomizarlos para producir un MapaDeÁtomos 806 sobre cómo reensamblar los datos 802 más tarde. Un MapaDeÁtomos 806 puede contener información creada o recopilada durante el proceso de atomización 202 que puede usarse durante el proceso de desatomización 206 y recomponer los datos de usuario 104. El MapaDeÁtomos 806 puede incluir información sobre el propio MapaDeÁtomos 806, incluida la versión o el formato de definición del MapaDeÁtomos 806, el tipo de compresión, el tipo de cifrado, la clave de cifrado, el vector de inicialización del cifrado, la ListaDeBloqueo (que puede incluir cómo se separaron los archivos, incluidos el tamaño, la ubicación y las claves de DivisiónÁtomo), y la ListaDeÁtomos (que puede incluir los nombres de todos los Átomos 1102, incluidos los Átomos paja, y el índice en la lista AgrupaciónDeAlmacenamiento).

En un modo de realización, la función Atomizar 308 puede incluir después una función Suficientemente Pequeño 808, que puede evaluar un MapaDeÁtomos 806 producido por la función AtomizarDatos 804 para determinar si 806 debe reducirse aún más mediante la función AtomizarDatos 804 o si un MapaDeUnMapaDeÁtomos 310 es de tamaño apropiado y puede convertirse en ClaveDeÁtomos 304. Si se desea, el MapaDeÁtomos 806 se retroalimenta recursivamente en la función AtomizarDatos 804 para atomizar el MapaDeÁtomos 806 y reducir su tamaño. En dicho modo de realización, cada pasada adicional que atomiza un MapaDeÁtomos 806 realmente puede producir un MapaDeUnMapaDeÁtomos 310 como resultado; sin embargo, el procesamiento recursivo en la función AtomizarDatos 804 puede operar igual sin distinción de qué iteración se procesa. Este proceso iterativo puede producir finalmente una ClaveDeÁtomos 304 que se puede representar en menos de 100 bytes.

La FIGURA 9 muestra un esquema de la función AtomizarDatos 804 de acuerdo con un modo de realización. Esta función 804 puede incluir una función Preparar MapaDeÁtomos 900, que puede crear y establecer información en un MapaDeÁtomos 806, incluida la versión y el tamaño de los datos. Esta función 804 también puede crear una clave de cifrado aleatoria y larga para todos los datos y un vector de inicialización (IV) para iniciar la aleatorización, y puede anotar y validar el tipo de cifrado. La función 900 puede establecer el MapaDeÁtomos 806 en base a la información de autorización 306.

La función AtomizarDatos 804 puede incluir después una función Leer Bloque 902, que puede tomar los datos intermedios 802 y leer un trozo o Bloque 904 de los datos 802 a la vez para facilitar el procesamiento. El tamaño de un bloque 904 (la cantidad establecida de bytes de los datos 802) puede ser un parámetro que puede variar. En un modo de realización, este procesamiento basado en trozos no afecta a cómo se produce la atomización y la separación, sino que solo es útil para gestionar el tamaño de los datos procesados a la vez.

La función AtomizarDatos 804 puede incluir después una función Cifrar 906, que puede cifrar cada Bloque 904 con el tipo de cifrado, la clave y IV definidos en el MapaDeÁtomos 806 para producir un Bloque de Cifrado 908, que es un bloque de bytes cifrados de los datos 802. El tipo y la solidez del cifrado usado puede ser un parámetro que se puede establecer por atomización en base a lo que se atomiza o en base a quién es el usuario. En cualquier caso, el sistema 100 puede maximizar la protección de cifrado puesto que la clave para cualquier tipo de cifrado puede ser larga y aleatoria. Otro beneficio del cifrado puede ser asegurar que los datos 802 no se han alterado o corrompido en la transmisión, de manera similar a una función de suma de comprobación o hashID.

La función AtomizarDatos 804 puede incluir después una función DivisorÁtomo 910, que se describe más adelante con respecto a la FIGURA 10. Esta función 910 puede dividir los datos (en cada Bloque de Cifrado 908) a nivel de bits en agrupaciones disociadas llamadas Átomos 1102 y proporcionar información de Átomo 912 que define un bloque 908 (por tamaño y dirección) y los Átomos que tienen los bits del bloque 908 y cómo recuperar los bits. Esta información de Átomo 912 puede almacenarse en el MapaDeÁtomos 806 en la ListaDeBloqueo y la ListaDeÁtomos.

La función AtomizarDatos 804 puede incluir después una función Terminar Bloque 914, que puede actualizar el MapaDeÁtomos 806 con la nueva información de ListaDeBloqueo y la ListaDeÁtomos. Si hay más de un bloque 904 para procesar, la función 914 puede devolver la función AtomizarDatos 804 de vuelta a la función Leer Bloque 902 para procesar el siguiente bloque 904. Si se han procesado todos los Bloques 904, la función 914 puede finalizar el MapaDeÁtomos 806.

La función AtomizarDatos 804 puede incluir después una función Terminar MapaDeÁtomos 916, que puede asegurar que el MapaDeÁtomos 806 esté terminado y tenga todos los datos de la ListaDeBloqueo y la ListaDeÁtomos.

La FIGURA 10 muestra un esquema de la función DivisorÁtomo 910 de acuerdo con un modo de realización. Esta función 910 puede incluir una función Preparar InformaciónDeÁtomo 1000, que puede establecer la información de Átomo 912 para el Bloque de Cifrado actual 908 que se está procesando, lo que puede asegurar que haya una ClaveDivisiónDeÁtomos y Átomos 1102 listos para recibir las agrupaciones de bits divididas 1008 a partir de la función Divisor 1006. Esta función 1000 también puede crear un IDÁtomo para este Átomo 1102.

La función DivisorÁtomo 910 puede incluir después una función Leer Palabra 1002, que puede tomar el Bloque Cifrado 908 y leer una Palabra 1004 (o un conjunto de bits) de él 908. El tamaño de Palabra (número de bits) puede ser un parámetro definido por la ClaveDivisiónDeÁtomos.

La función DivisorÁtomo 910 puede incluir después una función Divisor 1006, que puede dividir una Palabra 1004 en agrupaciones separadas 1008 de bits. Una clave aleatoria grande, la ClaveDivisiónDeÁtomos, puede definir cómo se dividen los bits de la Palabra 1004. La ClaveDivisiónDeÁtomos puede estar compuesta por *n* posiciones o ranuras (donde *n* es un parámetro que podría modificarse), donde cada posición cubre una Palabra 1004. Las posiciones pueden rotarse de modo que cada una se usa de acuerdo con la Palabra 1004 hasta la posición $^{n}$, momento en el cual la primera posición puede usarse nuevamente como si empezara otra vez desde el principio para cubrir todas las Palabras 1004. Cada posición puede incluir dos o más máscaras de bits. Cada máscara de bits puede definir los bits que irán a una agrupación de bits particular 1008 asociada con esa máscara de bits. El número de máscaras de bits por posición puede determinar cuántos Átomos concurrentes 1002 se usan para dividir una Palabra 1004. Si una máscara de bits contiene un "1" en la ubicación de un bit de una Palabra 1004, entonces ese

bit puede asignarse a la agrupación de bits 1008 asociada con esa máscara de bits. Si una máscara de bits contiene un "0" en la ubicación de un bit de Palabra 1004, ese bit no se asignará a la agrupación de bits 1008 asociada con esa máscara de bits. Cada máscara de bits puede incluir no más de la mitad de los bits de una Palabra 1004. Las máscaras de bits pueden coincidir con el tamaño de Palabra para capturar todos los bits de la Palabra 1004. Cada agrupación de bits 1008 puede añadirse a cualquier bit existente del Átomo 1102 asociado con esa agrupación de bits 1008. Los Átomos 1102 resultantes contendrán partes parciales y aleatorias de la Palabra 1004 y pueden almacenarse en ubicaciones aleatorias con identificaciones largas y aleatorias.

Un ejemplo simplificado puede ser ilustrativo. Supongamos una palabra de 10 "bits", W - ABCDEFGHIJ. Estos realmente no son bits puesto que no son un "1" o un "0"; sin embargo, ilustrarán más fácilmente el ejemplo. Supongamos tres máscaras de bits a partir de la ClaveDivisiónDeÁtomos para la posición de esta Palabra: M1 = 0100010010, M2 = 1011001000 y M3 = 0000100101. M1 está asociado con la agrupación de bits 1, M2 está asociado con la agrupación de bits 2 y M3 está asociado con la agrupación de bits 3. Por lo tanto, al aplicar estas máscaras de bits a la palabra produce las siguientes agrupaciones de tres bits: agrupación 1 = BFI, agrupación 2 = ACDG y agrupación 3 = EHJ. La agrupación 1 puede añadirse a los bits existentes del Átomo 1, la agrupación 2 puede añadirse a los bits existentes del Átomo 2 y la agrupación 3 puede añadirse a los bits existentes del Átomo 3.

La función DivisorÁtomo 910 puede incluir después una función Construir Átomos 1010, que se describe más adelante con respecto a la FIGURA 11. Esta función 1010 puede añadir agrupaciones de bits 1008 para separar los Átomos 1102. Cuando un Átomo 1102 está lleno, la función 1010 puede prepararlo 1102 para su transmisión y enviarlo 1102. Esta función 1010 puede preparar la información del Átomo 912 descrita previamente.

La función DivisorÁtomo 910 puede incluir después una función Terminar Palabra 1012, que puede añadir a la información de Átomo 912 cualquier información nueva creada durante la función Construir Átomos 1010. La función Terminar Palabra 1012 puede repetir la función 910 desde la función Leer Palabra 1002 si hay más Palabras 1004 para leer.

La función DivisorÁtomo 910 puede incluir después una función Terminar DivisiónÁtomo 1014, que puede finalizar la información de Átomo 912 a partir de la función DivisorÁtomo 910.

La FIGURA 11 muestra un esquema de la función Construir Átomos 1010 de acuerdo con un modo de realización. Esta función 1010 puede incluir una función Preparar Átomos 1100, que puede preparar Átomos 1102 y una ClaveDivisiónDeÁtomos para recibir las agrupaciones de bits divididos 1008. Esta función 1010 puede producir nuevos Átomos y ClavesDivisiónDeÁtomos según sea necesario. Las ClavesDivisiónDeÁtomos se pueden añadir a la información de Átomo 912 para su inclusión en el MapaDeÁtomos 806.

La función Construir Átomos 1010 puede incluir después una función Añadir Bits 1104, que puede añadir cada agrupación de bits 1008 a sus datos de Átomo 1102 respectivos. Un Átomo 1102 puede ser un pequeño conjunto de bits disociados divididos a partir de los datos de usuario cifrados 104. El Átomo 1102 puede no tener estructura o metadatos sobre su contenido, de dónde proviene el contenido o dónde pertenece el contenido. El Átomo 1102 puede identificarse con una identificación única aleatoria y larga (por ejemplo, 20 bytes) que no tiene información asociativa sobre de dónde procede el Átomo 1102 o de qué forma parte. Un Átomo 1102 puede incluir no más del 50% de los bits de cualquier Palabra 1004, y los bits incluidos se pueden determinar aleatoriamente con la ClaveDivisiónDeÁtomos.

La función Construir Átomos 1010 puede incluir después una función Terminar Átomo 1106, que puede finalizar un Átomo 1102 y su información de Átomo 912 si el Átomo 1102 está lleno. Esta función 1106 también puede seleccionar aleatoriamente el destino de almacenamiento para cada Átomo 1102 en base a la información de autorización 306, y puede determinar cuántos Átomos paja se enviarán con Átomos 1102 reales; dicha información puede almacenarse en la Información de Carga de Átomo 1108.

La función Construir Átomos 1010 puede incluir después una función Añadir Carga de Átomo 1110, que puede usar los Átomos 1102 y la Información de Carga de Átomo 1108 para hacer que un UÁtomo 1112 se envíe a la función Gestor CargaDeÁtomo 1114 para cargarse. Un UÁtomo 1112 puede incluir datos de Átomo 1102, así como metadatos sobre el Átomo 1102, incluida su identificación (IDÁtomo), identificación de Átomos paja (los IDPaja, que pueden ser los IDÁtomo de Átomos paja) y los destinos de almacenamiento para todos. Un UÁtomo 1112 puede destruirse una vez que la función Gestor CargaDeÁtomo 1114 ha enviado los Átomos 1102 definidos por el UÁtomo 1112.

La función Construir Átomos 1010 puede incluir después una función Gestor CargaDeÁtomo 1114, que puede gestionar el proceso (que puede ser síncrono) de enviar Átomos 1102 a través de una red a diversos servicios y dispositivos de almacenamiento específicos 110.

La FIGURA 12 muestra un esquema de la función Gestor CargaDeÁtomo 1114 de acuerdo con un modo de realización. Esta función 1114 puede incluir una función Recopilar UÁtomos 1200, que recopila los UÁtomos 1112 que están listos para almacenarse de forma remota o cargarse en la nube 108.

La función Gestor CargaDeÁtomo 1114 puede incluir después una función Aleatorizar Orden 1202, que puede seleccionar en orden aleatorio los UÁtomos 1112 que se han recopilado para transmitirlos al almacenamiento 110. El orden aleatorio de enviar los Átomos 1102 puede hacer que sea imposible comprender la relación entre los datos de usuario originales 104 y los Átomos enviados 1102. En un modo de realización, la función Aleatorizar Orden 1202 puede proceder solo si hay un número suficiente de UÁtomos 1112 para seleccionar. El número de UÁtomos 1112 recopilados antes de la aleatorización puede ser un parámetro que puede modificarse. Este número puede reflejar el equilibrio de seguridad, uso de memoria y latencia; un número más pequeño puede procesar más rápido, ocupar menos memoria, pero ser menos seguro; un número mayor puede procesar más lentamente, ocupar más memoria, pero ser más seguro. En un modo de realización, esta función 1202 puede proceder a aleatorizar solo si se recopilan todos los UÁtomos 1112.

La función Gestor CargaDeÁtomo 1114 puede incluir una función Producir Paja 1204, que puede usar la lista de IDPaja de los UÁtomos 1112 para crear Átomos Paja 1102, que son falsos Átomos 1102 llenos de datos aleatorios, que no se pueden distinguir de los Átomos 1102 reales, como se ha analizado previamente. Los Átomos Paja 1102 puede aumentar considerablemente el esfuerzo requerido para desatomizar los datos de usuario 104 sin el MapaDeÁtomos 806.

La función Gestor CargaDeÁtomo 1114 puede incluir una función Enviar Átomos 1206, que puede enviar aleatoriamente un Átomo 1102 real o un Átomo 1102 paja a un Servicio de Almacenamiento en Red definido. La transmisión puede ser una transferencia de datos por red típica (por ejemplo, publicación HTTP o flujo TCP), y esta función 1206 puede realizar los establecimientos de comunicación y la transferencia por red adecuados. El Átomo 1102 se envía como un Objeto Binario Grande (o BLOB 1208), que es un grupo de bits sin estructura interna o metadatos de identificación. Externo al primer ordenador 102, el BLOB no tendría significado ni asociación con otros Átomos 1102 o el MapaDeÁtomos 806. Esta función Enviar Átomos 1206 puede emitir eventos de progreso y eventos de éxito para mantener al usuario informado del progreso. Si falla una transferencia, esta función 1206 puede intentar enviar el Átomo 1102 nuevamente un número determinado de veces.

La función Gestor CargaDeÁtomo 1114 puede incluir un BLOB de Almacenamiento como la función IDÁtomo 1210, que puede almacenar el Átomo 1102 dentro del BLOB 1208 en un Servicio de Almacenamiento en Red definido basado en el IDÁtomo respectivo. Un Servicio de Almacenamiento en Red puede ser cualquier sistema de almacenamiento remoto. Puede incluir al menos un dispositivo de almacenamiento 110 que se almacena en la nube 108. Se pueden usar múltiples Servicios de Almacenamiento en Red para almacenar diferentes Átomos 1102, a los que se puede acceder desde cualquier ubicación con acceso a los Servicios de Almacenamiento en Red. Ejemplos de dichos Servicios de Almacenamiento en Red incluyen almacenamiento en la nube pública o privada (como Amazon S3, DropBox, Box, Rackspace, Google Drive), SAN o NAS privado (corporativo o individual), WebDAV (que es un estándar de servidor web para almacenar datos) y FTP. Un Servicio de Almacenamiento en Red puede ser igual o diferente del servicio que proporciona la atomización y desatomización, como se ha analizado anteriormente con respecto a la función Solicitar Atomizar 702. Se puede usar una pluralidad de Servicios de Almacenamiento en Red con dispositivos de almacenamiento 110 para mejorar la seguridad impidiendo un punto único de piratería o compulsión. La ubicación de estos Servicios de Almacenamiento en Red en diferentes jurisdicciones o naciones puede mejorar la seguridad.

La FIGURA 13 muestra un esquema de la función Producir ClaveDeÁtomos 312 de acuerdo con un modo de realización. Esta función 312 puede incluir una función Preparar ClaveDeÁtomos 1300, que puede reducir y simplificar el MapaDeUnMapaDeÁtomos 310 en un pequeño conjunto conciso de bytes llamado la PreClaveDeÁtomos 1302. En un modo de realización, la PreClaveDeÁtomos 1302 puede comprimir los bytes y minimizarse. La PreClaveDeÁtomos 1302 puede cifrarse y codificarse en formas fácilmente almacenadas y transmitidas que pueden usarse para desatomizar y reensamblar los datos de usuario 104 recuperados desde los dispositivos de almacenamiento 110. En un modo de realización, la ClaveDeÁtomos 304 solo puede necesitar identificar dos Átomos 1102 (que es el conjunto más pequeño necesario para el MapaDeUnMapaDeÁtomos 310 final), y no se requiere la ListaDeBloqueo ya que solo se usa un bloque.

La función Producir ClaveDeÁtomos 312 puede incluir después una función Cifrar 1304, que puede usar un Bloqueo de Clave 314 para cifrar la PreClaveDeÁtomos 1302 en un conjunto de bytes cifrados 1306. Esta función 1304 puede operar de manera similar a la función Cifrar 906. Un Bloqueo de Clave 314 puede ser cualquier técnica para bloquear la ClaveDeÁtomos 304 de modo que se requiera una "clave" para reensamblar los datos de usuario 104. El Bloqueo de Clave 314 puede variar dependiendo del uso y los mecanismos de transporte o almacenamiento. Los ejemplos de Bloqueo de Clave 314 incluyen cifrado de clave privada (clave simétrica), cifrado de clave pública (clave asimétrica) y cifrado biométrico.

La función Producir ClaveDeÁtomos 312 puede incluir después una función Terminar ClaveDeÁtomos 1308, que puede terminar la generación de una ClaveDeÁtomos 304, un conjunto de datos pequeño y bloqueado listo para codificar y usar, a partir de los bytes cifrados 1306. En un modo de realización, la ClaveDeÁtomos 304 incluye un byte para indicar el tipo de cifrado y el formato de la ClaveDeÁtomos.

La FIGURA 14 muestra un esquema de la función Exportar ClaveDeÁtomos 318 de acuerdo con un modo de realización. Esta función 318 puede incluir una función Codificar 1400, que puede convertir los bytes de una

ClaveDeÁtomos 304 en una forma más utilizable para su transmisión, almacenamiento o transporte. Los ejemplos incluyen Código QR visual o caracteres de base 64. Esta función 1400 también puede añadir Información de Clave 316 pública (no secreta) para mejorar la utilidad de la ClaveDeÁtomos 304. Por ejemplo, se puede añadir un logotipo o información legible por una persona a un Código QR.

La función Exportar ClaveDeÁtomos 318 puede incluir después una función Renderizar 1402, que puede producir la ClaveDeÁtomos Renderizada 1404 mejorada y codificada que puede transmitirse, almacenarse o transportarse. La ClaveDeÁtomos Renderizada 1404 puede ser un Código QR que se visualiza en una pantalla del primer ordenador 102 para ser capturada por una cámara o escaneada por una aplicación de un primer teléfono móvil 114 u otro dispositivo. La ClaveDeÁtomos Renderizada 1404 se puede imprimir en una hoja de papel física. La ClaveDeÁtomos Renderizada 1404 se puede renderizar en caracteres de base 64 para escribir o copiar en el portapapeles y pegar. En un modo de realización, la función Renderizar 1402 también puede añadir cualquier Información de Clave 316 pública adicional como se ha analizado previamente.

La FIGURA 15 muestra un esquema de la función Importar ClaveDeÁtomos 400 de acuerdo con un modo de realización. Esta función 400 puede incluir una función Recopilar 1500, que puede capturar la ClaveDeÁtomos Renderizada 1404 como datos electrónicos que pueden decodificarse. Por ejemplo, esta función 1500 puede incluir el uso de un segundo teléfono móvil 114 u otro dispositivo para escanear y capturar el Código QR de la ClaveDeÁtomos Renderizada 1404. En otro modo de realización, esta función 1500 puede incluir escribir los caracteres de base 64 de la ClaveDeÁtomos Renderizada 1404 en el segundo teléfono móvil 114 u otro dispositivo.

La función Importar ClaveDeÁtomos 400 puede incluir después una función Decodificar 1502, que puede convertir la ClaveDeÁtomos Renderizada 1404 codificada que se ha recopilado en los sencillos bytes de ClaveDeÁtomos 304.

La FIGURA 16 muestra un esquema de la función Revertir MapaDeUnMapaDeÁtomos 500 de acuerdo con un modo de realización. Esta función 500 puede incluir una función Descifrar 1600, que puede usar el Bloqueo de Clave 314 para descifrar la ClaveDeÁtomos 304 en bytes descifrados 1602. Esta función 1600 puede usar el tipo y la versión de cifrado en el proceso de descifrado.

La función Revertir MapaDeUnMapaDeÁtomos 500 puede incluir después una función Terminar MapaDeUnMapaDeÁtomos 1604, que puede revertir los bytes descifrados 1602 que contienen la ClaveDeÁtomos 304 descifrado en un MapaDeUnMapaDeÁtomos 310, que puede incluir ListaDeÁtomos, ListaDeBloqueo y la información de cifrado.

La FIGURA 17 muestra un esquema de la función Autorizar Reensamblar 502 de acuerdo con un modo de realización. Esta función 502 puede incluir una función Solicitar Reensamblar 1700, que puede usar el MapaDeUnMapaDeÁtomos 310 para enviar información de solicitud 1714 desde el segundo ordenador 116 al servicio, que puede estar alojado en la nube 108, para autorizar el reensamblaje especificado de datos de usuario 104. Esta función 1700 puede formatear y transmitir adecuadamente la información de solicitud 1714 como una solicitud de servicio de descanso HTTPS. La transmisión puede estar protegida por TLS (HTTPS). La función 1700 puede necesitar enviar solo el IDClaveDeÁtomos para solicitar la autorización de reensamblaje. La información de solicitud 1714 puede ser datos formateados apropiadamente con información de autentificación de usuario. El proceso de atomización 202 y el proceso de desatomización 206 pueden producirse sin pasar la ClaveDeÁtomos 304 o el MapaDeÁtomos 806 en la red.

La función Autorizar Reensamblar 502 puede incluir después una función Autorizar Autentificación 1702, que puede ser similar a la función Autorizar Autentificación 706 usada durante el proceso de atomización 202. Esta función 1702 puede ser una función especializada en los servicios web para verificar a partir de la información de solicitud 1714 que el IDClaveDeÁtomos existe (autentificación) y permite el reensamblaje (autorización).

La función Autorizar Reensamblar 502 puede incluir después una función Lógica de Reensamblaje 1704, que puede actualizar el AlmacénDeDatos IDClaveDeÁtomos 712 para reflejar la solicitud de reensamblaje. El sistema 100 puede incluir modos que desencadenan la limpieza de Átomos 1102 en base al número de solicitudes de reensamblaje; dichas instrucciones pueden añadirse a la información de autorización 306 y devolverse al solicitante.

La función Autorizar Reensamblar 502 puede incluir una función Recopilar IDAtomización 1706, que puede recopilar y devolver el IDAtomización asociado en la información de autorización 306 a partir del AlmacénDeDatos IDClaveDeÁtomos 712.

La función Autorizar Reensamblar 502 puede incluir después una función Recopilar AgrupaciónDeAlmacenamiento 1708, que puede recopilar y devolver la lista de AgrupaciónDeAlmacenamiento asociada en la información de autorización 306 a partir del AlmacénDeDatos IDClaveDeÁtomos 712. La función Reensamblar 504 puede usar el índice de destino de almacenamiento de la lista de AgrupaciónDeAlmacenamiento para saber dónde se ha almacenado cada Átomo 1102.

La función Autorizar Reensamblar 502 puede incluir después una función Responder 1710, que puede terminar de construir la información de autorización 306 y devolverla al segundo ordenador 116. Si se permite el reensamblaje, se puede devolver la información de autorización 306; de lo contrario, puede devolverse un código de fallo o un

mensaje que indique, por ejemplo, que la información de solicitud 1714 o el Átomo 1102 pueden haber expirado, pueden haberse eliminado o pueden ser inválidos. La respuesta puede transmitirse a través de la conexión establecida (TLS/HTTPS). Esta función Responder 1710 puede ser similar a la función Responder 718 usada durante el proceso de atomización 202.

La función Autorizar Reensamblar 502 puede incluir después una función Responder Reensamblar 1712, que puede recibir la información de autorización 306 en el segundo ordenador 116 del servicio de red.

La FIGURA 18 muestra un esquema de la función Reensamblar 504 de acuerdo con un modo de realización. Esta función 504 puede incluir una función Preparar Mapa 1800, que puede verificar el MapaDeUnMapaDeÁtomos 310 para asegurarse de que 310 cumple con el formato y la definición completos del MapaDeÁtomos.

La función Reensamblar 504 puede incluir después una función de reensamblaje de datos 1802, que puede recopilar y reensamblar datos originales que han producido el MapaDeÁtomos 806 durante el proceso de atomización 202. Esta función 1802 puede usar el MapaDeÁtomos 806 para reensamblar los datos atomizados que representa el MapaDeÁtomos 806. Los datos a reensamblar pueden ser datos de usuario 104 u otro MapaDeÁtomos 806. Esta función 1802 se describe más completamente en la FIGURA 19.

La función Reensamblar 504 puede incluir después una función Es MapaDeÁtomos 1804, que puede determinar el tipo de datos reensamblados 802. Si los datos 802 son un MapaDeÁtomos 806, esta función 1804 puede devolver los datos 802 para otra pasada de la función ReensamblarDatos 1802, que puede iterar hasta que los datos de usuario subyacentes 104 se reensamblen.

La función Reensamblar 504 puede incluir después una función de Descomprimir 1806, que puede descomprimir los datos 802 si los datos de usuario originales 104 se han comprimido. El tipo de compresión usado puede definirse en el MapaDeÁtomos 806. El resultado de esta función 1806 pueden ser los datos de usuario originales 104.

La FIGURA 19 muestra un esquema de la función Reensamblar Datos 1802 de acuerdo con un modo de realización. Esta función 1802 puede incluir una función Añadir ÁtomosdeDescarga 1900, que puede crear una definición, llamada DÁtomo 1902 (ÁtomoDeDescarga), para cada Átomo 1102 en la ListaDeÁtomos de un MapaDeÁtomos 806 usando la información de autorización 306 y la lista de AgrupaciónDeAlmacenamiento. El DÁtomo 1902 puede contener información sobre los Átomos 1102 a descargar, que puede incluir el IDÁtomo, la información de destino del almacenamiento y los IDPaja a incluir, de modo que los Átomos 1102 relacionados con un Bloque 904 pueden ubicarse y recuperarse. Una vez que la función Gestor DescargaDeÁtomo 1904 recupera todos los Átomos 1102 definidos, el DÁtomo 1902 puede destruirse.

La función ReensamblarDatos 1802 puede incluir después una función Esperar Datos de Átomo 1906, que puede permitir que la aplicación 106 realice otro trabajo (tal como proporcionar información de estado, por ejemplo) mientras los Átomos 1102 se descargan mediante la función Gestor DescargaDeÁtomo 1904. La descarga puede ser un proceso de E/S asíncrono que puede permitir que la aplicación 106 realice ese otro trabajo.

La función ReensamblarDatos 1802 puede incluir después una función Gestor DescargaDeÁtomo 1904, que puede gestionar el proceso (que puede ser asíncrono) de recuperar Átomos 1102 a través de una red desde diversos servicios y/o dispositivos de almacenamiento específicos 110.

La función ReensamblarDatos 1802 puede incluir después una función Reunir Datos de Átomo 1908, que puede recopilar los Átomos 1102 y reasociar los Átomos 1102 que forman parte de un Bloque 904 de datos en los Átomos asociados 1910. Esta función 1908 puede realizar el inverso de la función Divisor 1006, que puede separar los bits de un Bloque 904 en Átomos separados 1102. Ya que los Átomos 1102 en sí mismos no pueden contener información sobre sus datos, el MapaDeÁtomos 806 puede asociar los bits en los Átomos 1102 y los Bloques 904, que pueden usarse para reconstruir los datos de usuario 104. Los Átomos asociados 1910 pueden incluir los bytes reales de bits que se han dividido y añadido desde los bloques 904 a partir de los datos de usuario 104 cifrados.

La función ReensamblarDatos 1802 puede incluir después una función Reconstruir 1912, que puede tomar algunos Átomos asociados 1910, deshacer la división de los Átomos asociados 1910 en un Bloque Parcial 2006, reconstruir el Bloque completo 904, descifrar el Bloque 904 y poner el Bloque 904 en su ubicación apropiada en los datos de construcción intermedios 802.

La función ReensamblarDatos 1802 puede incluir después una función Terminar Reensamblar 1914, que puede asegurar que todos los datos 802 se han reensamblado y comprobado. Esta función 1914 puede realizar cualquier otra función para finalizar el reensamblaje.

La FIGURA 20 muestra un esquema de la función Reconstruir 1912 de acuerdo con un modo de realización. Esta función 1912 puede incluir una función Determinar Bloque 2000, que puede determinar usando un MapaDeÁtomos 806 si, cómo y dónde los Átomos asociados 1910 proporcionados pertenecen a un Bloque Parcial 2006 definido. Esta función 1912 puede extraer las agrupaciones de bits 1008 de datos de los Átomos asociados 1910. Un Bloque Parcial 2006 puede ser un Bloque Cifrado 908 que se está reconstruyendo a medida que los Átomos asociados 1910 se recuperan y se organizan con la función Gestor DescargaDeÁtomo 1904. Puesto que los Átomos 1102 se

pueden descargar en cualquier orden, los Bloques Cifrados 908 se pueden reconstruir en diversos órdenes y a diferentes velocidades. Por lo tanto, múltiples Bloques Parciales 2006 pueden definirse y reconstruirse concurrentemente.

La función Reconstruir 1912 puede incluir después una función Deshacer Divisor 2002, que puede tomar las agrupaciones de bits 1008 que corresponden al Bloque Parcial 2006 definido y recombinarlas 1008 en una Palabra 1004 usando la ClaveDivisiónDeÁtomos del MapaDeÁtomos 806 para el Bloque 904 especificado. Esta Palabra 1004 puede contener datos cuya división se ha deshecho que están listos para añadirse a un Bloque Parcial 2006. Esta función 2002 puede ser la inversa de la función Divisor 1006.

La función Reconstruir 1912 puede incluir después una función Construir Bloque 2004, que puede tomar una Palabra 1004 y añadirla al Bloque Parcial 2006 apropiado. Cuando un Bloque parcial 2006 se ha reconstruido completamente en un Bloque Cifrado 908, el Bloque Cifrado 908 puede descifrarse y añadirse a los datos de construcción 802.

La función Reconstruir 1912 puede incluir después una función Descifrar Bloque 2008, que puede descifrar el Bloque Cifrado 908 en un bloque 904 usando la información de criptografía en el MapaDeÁtomos 806 (que puede incluir el tipo de cifrado, la clave y el IV). El Bloque 904 ahora puede ser una porción descifrada de datos que se ha tomado inicialmente del MapaDeÁtomos 806 particular (que en sí mismo puede representar cualquiera de los datos de usuario 104 de otro MapaDeÁtomos 806 si es un MapaDeUnMapaDeÁtomos 310).

La función Reconstruir 1912 puede incluir después una función Añadir Bloque 2010, que puede añadir el Bloque 904 en la ubicación apropiada en los datos de construcción 802, que pueden ser datos de usuario comprimidos 104 o un MapaDeÁtomos 806).

La FIGURA 21 muestra un esquema de la función Gestor DescargaDeÁtomo 1904 de acuerdo con un modo de realización. Esta función 1904 puede usar DÁtomos 1902 para manejar y controlar la descarga de Átomos 1102 para su reensamblaje. Esta función 1904 puede incluir una función Recopilar DÁtomos 2100, que puede recopilar DÁtomos que están listos para descargar desde el dispositivo de almacenamiento de red remota 110.

La función Gestor DescargaDeÁtomo 1904 puede incluir una función Aleatorizar Orden 2102, que puede seleccionar los DÁtomos 1902 a recuperar (aparte de los 1902 que ya se han recopilado). Esta función 2012 puede aleatorizar el orden de recuperación/recopilación. En un modo de realización, esta función 2102 puede proceder a recuperar solo si hay una agrupación suficientemente grande de DÁtomos 1902 de la que elegir aleatoriamente. La recuperación aleatoria de Átomos 1102 puede mejorar la seguridad del sistema 100 al hacer imposible la comprensión de la relación de los Átomos 1102 con los datos de usuario 104 iniciales. El número de DÁtomos 1902 recopilados antes de la aleatorización puede ser un parámetro que puede modificarse. Este número puede reflejar el equilibrio de seguridad, uso de memoria y latencia; un número más pequeño puede procesar más rápido, ocupar menos memoria, pero ser menos seguro; un número mayor puede procesar más lentamente, ocupar más memoria, pero ser más seguro. En un modo de realización, esta función 2102 puede proceder a aleatorizar solo si se recopilan todos los DÁtomos 1902.

La función Gestor DescargaDeÁtomo 1904 puede incluir una función Obtener Átomos 2104, que puede recuperar aleatoriamente un Átomo 1102 (un Átomo 1102 real o un Átomo 1102 paja) del Servicio de Almacenamiento en Red definido. La comunicación entre el segundo ordenador 116 y el Servicio de almacenamiento en red puede ser similar a la existente entre el primer ordenador 102 y el Servicio de almacenamiento en red en la función Enviar Átomos 1206. La función Obtener Átomos 2104 puede emitir eventos de progreso y eventos de éxito para mantener al usuario informado del progreso. Si falla una transferencia, esta función 2104 puede intentar recuperar el Átomo 1102 nuevamente un número determinado de veces antes de indicar el fallo.

La función Gestor DescargaDeÁtomo 1904 puede incluir un Obtener BLOB como función IDÁtomo 2106, que puede recuperar el BLOB 1208 que es el Átomo 1102 con el IDÁtomo desde el dispositivo de almacenamiento 110 donde se ha guardado el BLOB 1208. El DÁtomo se puede usar para recuperar los Átomos 1102 de acuerdo con los IDÁtomo de un MapaDeÁtomos 806.

La función Gestor DescargaDeÁtomo 1904 puede incluir después una función Eliminar Paja 2108, que puede usar la lista de los IDPaja del DÁtomo 1902 para ignorar y desechar los Átomos paja 1102 de modo que solo los Átomos 1102 reales se conserven como resultado.

La FIGURA 22a muestra un esquema de la función Transportar ClaveDeÁtomos 2208 de acuerdo con un modo de realización. Esta función 2208 puede incluir una función Emitir 2200, que puede convertir y enviar los bytes cifrados y codificados de la ClaveDeÁtomos 304 desde un primer teléfono móvil 112 u otro dispositivo a través de un medio a un segundo teléfono móvil 114 u otro dispositivo usando un protocolo, como se ha analizado previamente. También se pueden usar otros dispositivos en esta función 2208 por seguridad o facilidad de uso.

La función Transportar ClaveDeÁtomos 2208 puede incluir después una función Recibir 2202, que puede recibir desde un primer teléfono móvil 112 u otros datos del dispositivo de acuerdo con un protocolo a través de un medio y convertir los datos en bytes de una ClaveDeÁtomos 304 en un segundo teléfono móvil 114 u otro dispositivo.

La FIGURA 22b muestra un esquema de la función Almacenamiento ClaveDeÁtomos 2210 de acuerdo con un modo de realización. Esta función 2210 puede incluir una función Almacenar/recuperar 2204, que puede almacenar una ClaveDeÁtomos 304 en un medio de almacenamiento 2206 y recuperarla 304 del medio 2206. El almacenamiento/recuperación puede incluir sistemas de archivos, bases de datos u otros sistemas de almacenamiento/recuperación indexados o con nombre. El medio de almacenamiento 2206 puede incluir cualquier medio conocido por un artesano experto e incluye, pero no se limita a, un teléfono inteligente, una unidad USB, una unidad de red, un disco duro y una tarjeta de memoria. El medio de almacenamiento 2206 puede ser local (en el primer ordenador 102) o remoto, ya sea controlado por el usuario (por ejemplo, en el primer teléfono móvil 112 u otro dispositivo, o impreso en una hoja de papel física) o no (por ejemplo, en el nube 108 o en otro dispositivo).

La FIGURA 23 muestra otro modo de realización de la función Gestor CargaDeÁtomo 1114. Esta función 1114 puede enviar UÁtomos 1112 a una Lista de Espera y esperar hasta que se haya recopilado un número suficiente de UÁtomos 1112 en la Lista de Espera para ser procesados y aleatorizados. Después de reunir un número suficiente de UÁtomos 1112, la función 1114 puede enviar los UÁtomos 1112 a un Trabajador y moverlos 1112 a una Lista de Trabajo. El Trabajador puede tomar un UÁtomo 1112, producir Átomos Paja 1102 apropiados y enviar todos los Átomos 1102 a los Servicios de Almacenamiento en Red. Un Trabajador puede ser un mecanismo concurrente para manejar múltiples cargas y descargas simultáneas (por ejemplo, hilo de ejecución o Eventlet). Cada Trabajador puede ser responsable de un UÁtomo 1112. Si un UÁtomo 1112 no se puede procesar, el 1112 puede añadirse nuevamente a la Lista de Espera y eliminarse de la Lista de Trabajo. Si un UÁtomo 1112 falla un número específico de veces, se puede añadir 1112 a una lista Fallida, lo que puede provocar que el proceso de atomización 202 se detenga y genere un mensaje de error. Si un UÁtomo 1112 se procesa satisfactoriamente (y el Átomo 1102 se envía satisfactoriamente), el UÁtomo 1112 se puede eliminar de la Lista de Trabajo y se puede generar un evento que notifique la compleción de ese UÁtomo 1112. Esta función Gestor CargaDeÁtomo 1114 puede monitorizar las varias listas de UÁtomos 1112 para asegurar que todos los Átomos 1102 se envíen satisfactoriamente. Esta función 1114 puede relacionar el estado (En espera, Trabajando, Hecho y Fallo) de los Átomos 1102 que se envían a través de eventos a funciones que pueden manejar errores y estado. La función 1114 puede usar y administrar una pluralidad de Trabajadores para formatear apropiadamente y enviar simultáneamente múltiples Átomos 1102 a Servicios de Almacenamiento en Red específicos.

La FIGURA 24 muestra otro modo de realización de la función Gestor DescargaDeÁtomo 1904, que puede ser similar pero inversa a la función 1114 de Gestor DescargaDeÁtomo descrita anteriormente con respecto a la FIGURA 23. Esta función 1904 puede enviar DÁtomos 1902 a una Lista de Espera y esperar hasta que se haya recopilado un número suficiente de DÁtomos 1902 en la Lista de Espera para ser procesados y aleatorizados. Después de reunir un número suficiente de DÁtomos 1902, la función 1904 puede enviar los DÁtomos 1902 a un Trabajador y moverlos 1902 a una Lista de Trabajo. El Trabajador puede tomar un DÁtomo 1902, recuperar todos los Átomos asociados 1102 (incluidos los Átomos paja 1102) de los Servicios de Almacenamiento en Red y descartar los Átomos paja 1102. Un Trabajador puede ser un mecanismo concurrente para manejar múltiples cargas y descargas simultáneas (por ejemplo, hilo de ejecución o Eventlet). Cada Trabajador puede ser responsable de un DÁtomo 1902. Si un DÁtomo 1902 no se puede procesar, el 1902 puede añadirse nuevamente a la Lista de Espera y eliminarse de la Lista de Trabajo. Si un DÁtomo 1902 falla un número específico de veces, se puede añadir 1902 a una lista Fallida, lo que puede provocar que el proceso de desatomización 206 se detenga y genere un mensaje de error. Si un DÁtomo 1902 se procesa satisfactoriamente (y el Átomo 1102 se recupera satisfactoriamente), el DÁtomo 1902 se puede eliminar de la Lista de Trabajo y se puede generar un evento que notifique la compleción de ese DÁtomo 1902. Esta función Gestor DescargaDeÁtomo 1904 puede monitorizar las varias listas de DÁtomos 1902 para asegurar que todos los Átomos 1102 se recuperen satisfactoriamente. Esta función 1904 puede relacionar el estado (En espera, Trabajando, Hecho y Fallo) de los Átomos 1102 que se recuperan a través de eventos con funciones que pueden manejar errores y estado. La función 1904 puede usar y administrar una pluralidad de Trabajadores para formatear apropiadamente y recuperar simultáneamente múltiples Átomos 1102 de los Servicios de Almacenamiento en Red especificados.

La FIGURA 25 muestra otra descripción general esquemática de un proceso de atomización 202, un proceso de desatomización 206 y un proceso de manejo de ClaveDeÁtomos 204. Las etapas individuales de estos procesos se han descrito previamente.

La FIGURA 26 muestra otra descripción general esquemática de un modo de realización de un proceso de atomización 202, un proceso de desatomización 206 y un proceso de manejo de ClaveDeÁtomos 204. Las etapas individuales de estos procesos se han descrito previamente.

La FIGURA 27 muestra una descripción general esquemática principal de un proceso 2700 de acuerdo con otro modo de realización. Este proceso 2700 puede ser similar al proceso 200 divulgado en la FIGURA 2. Este proceso 2700 puede incluir un proceso de atomización 2702, un proceso de transporte/almacenamiento 2704 y un proceso de desatomización 2706, cada uno de los cuales se analiza a continuación.

La FIGURA 28 muestra una descripción general del proceso de atomización 2702 de acuerdo con un modo de realización. Este proceso 2702 puede tomar los datos de usuario 104 o los datos originales que se desean almacenar o transportar de manera confidencial y puede atomizarlos 104. Los datos de atomización pueden fragmentarse, aleatorizarse y/o cifrarse. El proceso 2702 puede incluir una función Producir AgrupaciónDeÁtomos

2800, que puede crear una AgrupaciónDeÁtomos 2802 usando un módulo generador aleatorio 2804. La función Producir AgrupaciónDeÁtomos 2800 puede ser similar a la función Crear AgrupaciónDeAlmacenamiento 716. La AgrupaciónDeÁtomos 2802 puede ser una agrupación, bloque o cantidad de almacenamiento o memoria. La AgrupaciónDeÁtomos 2802 puede ser una agrupación de datos aleatorios que es mayor en cierta cantidad que los datos de usuario 104. Este bloque previamente llenado de datos aleatorios (la AgrupaciónDeÁtomos 2802) puede recibir bits aleatoriamente seleccionados y distribuidos aleatoriamente de los datos de usuario 104. La AgrupaciónDeÁtomos 2802 también puede recibir bits seleccionados aleatoriamente y distribuidos aleatoriamente del MapaDeÁtomos 806, como se analiza a continuación, incluso de múltiples recursiones o iteraciones de los MapasDeÁtomos 806. Los datos aleatorios iniciales creados por esta función 2800 pueden actuar como paja para los fragmentos de datos que se añadirán a la AgrupaciónDeÁtomos 2802 mediante la función AtomizarDatos 2806 que se describe a continuación. La cantidad de inflado de la AgrupaciónDeÁtomos 2802 sobre los datos de usuario 104 (es decir, la diferencia en los tamaños entre los dos) puede aumentarse para una mayor protección o disminuirse para un procesamiento, transporte y almacenamiento más eficaces. La cantidad de inflado puede ser seleccionable por el usuario o puede variar automáticamente dependiendo del tamaño de los datos de usuario 104 o incluso aleatoriamente. En un modo de realización, la ClaveDeÁtomos 304 también se puede crear y llenar inicialmente con datos aleatorios mediante la función Producir AgrupaciónDeÁtomos 2800. El módulo generador aleatorio 2804 puede ser cualquier medio, dispositivo o proceso que pueda usarse para crear datos aleatorios. Una vez que finaliza este proceso 2702, la AgrupaciónDeÁtomos 2802 puede ser una agrupación de bits aleatoria y desordenada, con bits de los datos de usuario 104, los MapasDeÁtomos 806 y la paja inicial o datos aleatorios. El proceso de atomización 2702 puede aleatorizar los datos de usuario 104 y ocultarlos entre otros datos aleatorios.

El proceso de atomización 2702 puede incluir una función AtomizarDatos 2806, que puede ser similar a la función AtomizarDatos 804. La función 2806 puede atomizar los datos de entrada que recibe 2806 durante su iteración actual y enviar los datos atomizados o bien a la AgrupaciónDeÁtomos 2802 o bien a la ClaveDeÁtomos 304. En un modo de realización, la ClaveDeÁtomos 304 puede ser similar a la AgrupaciónDeÁtomos 2802, como se describirá más adelante. En un modo de realización, la AgrupaciónDeÁtomos 2802 y la ClaveDeÁtomos 304 pueden estar en el dispositivo que ejecuta el proceso de atomización 2702, que puede ser el primer ordenador 102 que ejecuta la aplicación 106 y que contiene, o tiene acceso a, los datos de usuario 104. La función AtomizarDatos 2806 puede usar el módulo generador aleatorio 2802 para seleccionar aleatoriamente bits de datos de entrada (que pueden ser los datos de usuario 104 o un MapaDeÁtomos 806), combinarlos en Átomos 1102 y distribuirlos o traducirlos aleatoriamente 1102 en la AgrupaciónDeÁtomos 2802 o la ClaveDeÁtomos 304. La función 2806 puede registrar toda la información requerida para reensamblar y descifrar los datos atomizados en el MapaDeÁtomos 806. El MapaDeÁtomos 806 puede incluir todas las instrucciones sobre dónde se han almacenado los diversos Átomos 1102 y de qué bits originales están hechos los Átomos 1102. La función AtomizarDatos 2806 se analiza a continuación con respecto a la FIGURA 29.

En un modo de realización, la primera pasada de la función AtomizarDatos 2806 atomiza los datos de usuario 104 y los distribuye entre la AgrupaciónDeÁtomos 2802 y la ClaveDeÁtomos 304, almacenando las instrucciones de descifrado en el MapaDeÁtomos 806. En un modo de realización, estas instrucciones de descifrado, el MapaDeÁtomos 806, son más pequeñas que los datos de usuario 104. En un modo de realización, la función AtomizarDatos 2806 puede ejecutarse a través de iteraciones recursivas adicionales con el MapaDeÁtomos 806 de la iteración anterior como sus datos de entrada, lo que puede dar como resultado otro MapaDeÁtomos 806 más pequeño. Por ejemplo, durante la pasada inicial, los datos originales 104 pueden ser los datos de entrada a la función 2806, y el $MapaDeÁtomos^0$ puede ser el resultado de la instrucción (además de los datos enviados a la AgrupaciónDeÁtomos 2802 y/o la ClaveDeÁtomos 304). Durante la segunda pasada, el $MapaDeÁtomos^0$ pueden ser los datos de entrada a la función 2806, y el $MapaDeÁtomos^1$ puede ser el resultado de la instrucción (además de los datos del $MapaDeÁtomos^0$ que se envían a la AgrupaciónDeÁtomos 2802 y/o ClaveDeÁtomos 304), donde el $MapaDeÁtomos^1$ puede ser de menor tamaño que el $MapaDeÁtomos^0$. Durante la tercera pasada, el $MapaDeÁtomos^1$ pueden ser los datos de entrada a la función 2806, y el $MapaDeÁtomos^2$ puede ser el resultado de la instrucción (además de los datos del $MapaDeÁtomos^1$ que se envían a la AgrupaciónDeÁtomos 2802 y/o la ClaveDeÁtomos 304), donde el $MapaDeÁtomos^2$ puede ser de menor tamaño que el $MapaDeÁtomos^1$. Estas iteraciones pueden continuar hasta que el MapaDeÁtomos 806 tenga el tamaño deseado. La función Reducir MapaDeÁtomos 2808 puede incluirse para realizar esta función de verificar si el tamaño de MapaDeÁtomos es lo suficientemente pequeño y llamar a las iteraciones de la función AtomizarDatos 2806 hasta que el tamaño de MapaDeÁtomos sea lo suficientemente pequeño. Cuando el MapaDeÁtomos 806 es lo suficientemente pequeño, la función Reducir MapaDeÁtomos 2808 puede devolver un final del proceso de atomización 2702. En un modo de realización, un tamaño deseado para el MapaDeÁtomos 806 final es de 5 KB o menos. En otro modo de realización, un tamaño deseado para el MapaDeÁtomos 806 final es aproximadamente del mismo tamaño que la ClaveDeÁtomos 304.

El MapaDeÁtomos 806 puede contener todos los números aleatorios que se usan para seleccionar y distribuir los Átomos 1102 en la AgrupaciónDeÁtomos 2802 y la ClaveDeÁtomos 304. Al fragmentar los datos de usuario 104 en pequeños bloques o grupos de bits (Átomos 1102), y proporcionar instrucciones donde se almacena cada uno de estos Átomos 1102 dentro de la AgrupaciónDeÁtomos 2802 o la ClaveDeÁtomos 304 puede producir un conjunto de instrucciones relativamente grande (MapaDeÁtomos 806) con información sobre cómo descifrar y reensamblar los datos atomizados. Puesto que el proceso de atomización usa datos aleatorios para fragmentar y dispersar los datos

de usuario 104 dentro de la AgrupaciónDeÁtomos 2802 y la ClaveDeÁtomos 304, el MapaDeÁtomos 806 puede contener una gran cantidad de datos aleatorios con fines de reensamblaje. Por ejemplo, un MapaDeÁtomos 806 inicial para un archivo de 1 MB puede ser de 100 KB, dependiendo de los parámetros usados durante el proceso de atomización 2702. Dichas instrucciones de descifrado de gran tamaño (MapaDeÁtomos 806) pueden ser demasiado grandes y difíciles de utilizar como una clave regular de la misma forma que en los esquemas de criptografía convencionales. Por ejemplo, los cifrados de 128 y 256 bits usan claves de 128 o 256 bits de longitud, respectivamente, mientras que un certificado o clave SSL de 2048 bits tiene una longitud de 2048 bits. Atomizar el MapaDeÁtomos 806 de forma recursiva y mezclarlo con la AgrupaciónDeÁtomos 2802 y la ClaveDeÁtomos 304 puede reducir el tamaño del MapaDeÁtomos 806 hasta que el 806 tenga un tamaño útil sin comprometer la seguridad. La ClaveDeÁtomos 304 se puede especificar para que sea de cualquier tamaño. En un modo de realización, la ClaveDeÁtomos 304 puede tener un tamaño de 1 kilobyte. En otro modo de realización, la ClaveDeÁtomos 304 puede tener un tamaño de 8 kilobytes, lo que equivale a 65536 bits (suponiendo la convención de que 1 KB = 1024 bytes; 1 KB también puede ser igual a 1000 bytes). En otro modo de realización, la ClaveDeÁtomos 304 puede tener un tamaño de 16 kilobytes. Por lo tanto, la ClaveDeÁtomos 304 puede ser una clave con una longitud de bits mucho más larga que las claves de cifrado convencionales y proporcionar una seguridad significativamente mayor frente al compromiso. En otro modo de realización, la ClaveDeÁtomos 304 puede ser mayor que 1 kilobyte pero lo suficientemente pequeña como para ser útil, lo que puede depender de la aplicación y la industria. En otro modo de realización, la ClaveDeÁtomos 304 puede ser mayor de 8 kilobytes. En un modo de realización, el tamaño de ClaveDeÁtomos 304 puede ser diferente para cada dato de usuario 104 que se atomiza.

La FIGURA 29 muestra un esquema de la función AtomizarDatos 2806 de acuerdo con un modo de realización. Esta función 2806 puede incluir una función Producir MapaDeÁtomos 2900, que puede crear e inicializar el MapaDeÁtomos 806 inicial para los datos de usuario 104 que se van a atomizar.

La función AtomizarDatos 2806 también puede incluir una función Comprimir 2902, que puede ser similar a la función Comprimir 800 analizada con respecto a la FIGURA 8. La función Comprimir 2902 puede comprimir los datos de entrada 2918 con cualquier tipo de mecanismo o esquema de compresión de datos y emitir datos comprimidos 2904. La compresión puede reducir el tamaño de los datos de entrada 2918, lo que puede mejorar el resultado cuando se atomizan 2918. El tipo de compresión puede registrarse en el MapaDeÁtomos 806. Como se ha analizado anteriormente, los datos de entrada 2918 pueden ser los datos de usuario 104 o el MapaDeÁtomos 806 que ha resultado de la iteración previa de la función AtomizarDatos 2806.

La función AtomizarDatos 2806 también puede incluir una función Aleatorizar 2906, que puede usar el módulo generador aleatorio 2804 para aleatorizar previamente los datos comprimidos 2904 que ayudará a desordenarlos 2904 antes de atomizarlos. En modos de realización alternativos, se pueden usar diferentes procedimientos o esquemas de pseudoaleatorización, que incluyen, pero no se limitan a, el cifrado AES. Las múltiples capas de desordenación de este proceso 2700 pueden mejorar la aleatorización de la AgrupaciónDeÁtomos 2802 y la ClaveDeÁtomos 304, lo que puede mejorar la seguridad del sistema 100. El resultado de esta función 2906 pueden ser datos aleatorios 2908. La forma en que los datos comprimidos 2904 se aleatorizan (por ejemplo, el esquema de cifrado, el vector de inicialización y la clave) pueden registrarse en el MapaDeÁtomos 806. El inflado de la AgrupaciónDeÁtomos 2802 descrito anteriormente puede, en un modo de realización, ser con respecto a los datos aleatorios 2908 en lugar de los datos de usuario 104.

La función AtomizarDatos 2806 también puede incluir una función Bloque Aleatorio 2910, que puede usar el módulo generador aleatorio 2804 para seleccionar un bloque de datos aleatorios 2912 o una porción de los datos aleatorizados 2908 para atomizar. El tamaño de los bloques de datos 2912 puede ser fijo o variable en modos de realización alternativos. En un modo de realización, el tamaño de los bloques de datos 2912 puede ser establecido por el usuario. En otro modo de realización, el tamaño de los bloques de datos 2912 puede variar automáticamente en base al tamaño de los datos de usuario 104. En otro modo de realización, el tamaño de los bloques de datos 2912 puede variar entre cada iteración de bloque. En un modo de realización, el tamaño de cada bloque de datos 2912 es un byte. Los bloques de datos de menor tamaño 2912 pueden aumentar la aleatoriedad y la seguridad de los datos atomizados y también pueden aumentar el tamaño resultante de los datos atomizados. La selección de bloque puede registrarse en el MapaDeÁtomos 806.

La función AtomizarDatos 2806 también puede incluir una función VectorizaciónAtómica 2914, que puede usar el módulo generador aleatorio 2804 para crear Átomos 1102 aleatorios a partir de cada bloque de datos 2912 y distribuir estos Átomos 1102 aleatoriamente en la AgrupaciónDeÁtomos 2802 y la ClaveDeÁtomos 304. Las instrucciones sobre la creación de Átomos 1102 y su distribución pueden registrarse en el MapaDeÁtomos 806. Esta función 2914 se analiza a continuación con respecto a la FIGURA 30.

La función AtomizarDatos 2806 también puede incluir una función Más Bloques 2916, que puede verificar si todos los datos aleatorios 2908 se han atomizado. De lo contrario, esta función 2916 puede llamar a otra iteración de la función Bloque Aleatorio 2910 para seleccionar otro bloque de datos 2912 para su procesamiento por la función VectorizaciónAtómica 2914. Si todos los datos aleatorizados 2908 se han atomizado, esta función 2916 señaliza o devuelve un final de la función AtomizarDatos 2806.

La FIGURA 30 muestra un esquema de la función VectorizaciónAtómica 2914 de acuerdo con un modo de realización. Esta función 2914 puede incluir una función Seleccionar Átomos 3000, que puede crear Átomos 1102 a partir del bloque de datos de entrada 2912 usando el módulo generador aleatorio 2804. Esta función 2914 puede guardar las instrucciones sobre cómo se han creado los Átomos 1102 en el MapaDeÁtomos 806. Esta función 3000 se analiza a continuación con respecto a las FIGURAS 31-32.

La función VectorizaciónAtómica 2914 también puede incluir una función Generar Vectores 3002, que puede generar un Vector 3004 para cada Átomo 1102 generado por la función Seleccionar Átomo 3000. El Vector 3004 puede determinar dónde se almacena el Átomo 1102 correspondiente en la AgrupaciónDeÁtomos 2802 o la ClaveDeÁtomos 304.

En modos de realización alternativos, durante la función Producir AgrupaciónDeÁtomos 2800 o durante la función AtomizarDatos 2806, la AgrupaciónDeÁtomos 2802 puede configurarse dividiéndolo 2802 en un número de zonas, de 0 a Z-1. El número de zonas puede ser mayor para una mayor aleatorización y seguridad. El número de zonas puede ser constante o puede ser variable en base a la selección del usuario o automáticamente en base al tamaño de los datos de usuario 104 o incluso aleatoriamente, en diferentes modos de realización. La ClaveDeÁtomos 304 puede considerarse zona Z. De este modo, los Átomos 1102 pueden distribuirse en Z zonas de la combinación de AgrupaciónDeÁtomos 2802 y ClaveDeÁtomos 304. Cada zona puede identificarse por un número de zona único, de 0 a Z. En un modo de realización, cada zona de la AgrupaciónDeÁtomos puede ser del mismo tamaño. En modos de realización alternativos, el tamaño de la ClaveDeÁtomos 304 puede ser menor, igual o mayor que el tamaño de cada zona en la AgrupaciónDeÁtomos 2802. En otro modo de realización, las zonas de la AgrupaciónDeÁtomos pueden ser de tamaños desiguales o variables. La información de zona puede registrarse en el MapaDeÁtomos 806.

El proceso de atomización 2702 también puede determinar el desplazamiento máximo (que puede estar en bits) por el cual los Átomos individuales 1102 pueden almacenarse uno al lado del otro dentro de la misma zona. Esta determinación de desplazamiento también puede realizarse durante la función Producir AgrupaciónDeÁtomos 2800 o durante la función AtomizarDatos 2806, en modos de realización alternativos. El desplazamiento máximo puede ser constante o puede ser variable en base a la selección del usuario o automáticamente en base al tamaño de los datos de usuario 104 o incluso aleatoriamente, en diferentes modos de realización. Un desplazamiento máximo mayor puede hacer que la AgrupaciónDeÁtomos 2802 y/o la ClaveDeÁtomos 304 resultantes sean más grandes.

El proceso de atomización 2702 también puede determinar la longitud, t, de cada Vector 3004. Cada Vector 3004 puede ser una concatenación del número de zona en el que se traducirá el Átomo 1102 respectivo de ese Vector, z, y el desplazamiento (que puede estar en bits) por el cual el Átomo 1102 de ese Vector se desplazará del Átomo anterior que fue traducido a esa zona, o. En otras palabras, cada Vector 3004 puede tener t bits de longitud, incluyendo una porción z y una porción o. El tamaño de z puede establecerse determinando cuántos bits se necesitan para representar el número de zonas, o Z. El tamaño de o puede establecerse determinando cuántos bits se necesitan para representar el desplazamiento máximo. La determinación de t puede realizarse durante la función Producir AgrupaciónDeÁtomos 2800 o durante la función AtomizarDatos 2806, en modos de realización alternativos.

La función Generar Vectores 3002 puede usar el módulo generador aleatorio 2804 para generar un GeneradorDeVector, que puede ser una cadena de bits larga y aleatoria. En un modo de realización, el GeneradorDeVector puede ser mayor que 64 bits. En otro modo de realización, el GeneradorDeVector puede ser de 640 bits. En otro modo de realización, el GeneradorDeVector puede ser de 1000 bits, o incluso más grande. La función Generar Vectores 3002 puede crear Vectores 3004 usando el GeneradorDeVector. La función Generar Vectores 3002 puede tomar t bits del punto inicial de GeneradorDeVector y hacer que esos bits t sean el Vector 3004. Después de que este vector se ha producido, el índice de GeneradorDeVector se puede mover en t bits para que el Vector 3004 siguiente o sucesivo se genere desde una porción diferente o sucesiva del GeneradorDeVector. En un modo de realización, el punto o índice inicial dentro del GeneradorDeVector puede empezar al principio del GeneradorDeVector. En otro modo de realización, el punto o índice inicial puede seleccionarse aleatoriamente dentro del GeneradorDeVector. En un modo de realización, si se requieren más Vectores 3004 después de que el GeneradorDeVector haya llegado a su fin, el GeneradorDeVector puede volver a empezar por el principio para crear los Vectores 3004 adicionales. En modos de realización alternativos, los Vectores 3004 pueden estar desplazados unos de otros por un cierto número de bits (que puede ser constante o variable, y pueden ser seleccionados por el usuario o seleccionados automáticamente) de manera que no sean contiguos a lo largo del GeneradorDeVector. El GeneradorDeVector puede guardarse en el MapaDeÁtomos 806. El tamaño de z, o, y t puede guardarse en el MapaDeÁtomos 806. Los Vectores 3004 pueden no guardarse en el MapaDeÁtomos 806.

En un modo de realización, z = (log Z)/(log 2). En un modo de realización, Z es una potencia de 2. En otro modo de realización, Z no es una potencia de 2. Una realización puede tener z de manera que no se puedan seleccionar todas las zonas Z. Otra realización puede tener z de manera que la función Generar Vectores 3002 pueda hacer selecciones mayores que Z, en cuyo caso los modos de realización alternativos pueden volver a empezar desde el principio por la selección de zona desde 0, pueden dividir la selección en módulos y usar el resto, o pueden llamar a la función Generar Vectores 3002 para generar un nuevo Vector 3004 donde z selecciona una de las zonas Z configuradas. Opciones similares están disponibles para el desplazamiento.

La función VectorizaciónAtómica 2914 también puede incluir una función Traducir Átomos 3006, que puede distribuir cada Átomo 1102 de acuerdo con las instrucciones de ese Vector de Átomo 3004. Esta función 3006 puede leer z (el número de identificación de zona) del Vector 3004 para determinar en qué zona traducir el Átomo 1102 de ese Vector 3004. Esta función 3006 también puede leer o (el desplazamiento) del Vector 3004 para determinar cuántos bits compensar o desplazar el Átomo 1102 actual del último Átomo 1102 que se ha guardado en esa zona.

Cada zona puede tener un ÍndiceDeZona, que indica el bit inicial en esa zona (ya sea en la AgrupaciónDeÁtomos 2802 o en la ClaveDeÁtomos 304) en el que se puede traducir un Átomo 1102. El ÍndiceDeZona puede empezar al principio de la zona o aleatoriamente dentro de la zona, en modos de realización alternativos. Antes de traducir un nuevo Átomo 1102 a una zona seleccionada, el ÍndiceDeZona de esa zona puede desplazarse por el número de bits indicados en el desplazamiento, o, del Vector 3004 correspondiente a ese nuevo Átomo 1102. Cuando el Átomo 1102 se traduce en la zona, el ÍndiceDeZona para esa zona puede desplazarse por el número de bits en ese Átomo 1102. Si el ÍndiceDeZona no empieza al principio de una zona, el ÍndiceDeZona puede volver al principio de esa zona cuando el ÍndiceDeZona llega al final de esa zona. La función Traducir Átomos 3006 puede averiguar si se ha recorrido toda una zona de manera que no queden bits en esa zona que no hayan sido sobrescritos por los Átomos 1102 o desplazados. Si una zona está llena, la función Traducir Átomos 3006 puede volver a la función Generar Vectores 3002 para generar otro Vector 3004 aleatorio para ese Átomo 1102. Si el ÍndiceDeZona no empieza al principio de una zona, pero vuelve al principio, la función Traducir Átomos 3006 puede recordar el punto inicial de cada ÍndiceDeZona de cada zona, de manera que cuando el ÍndiceDeZona vuelve al principio y llega a ese punto inicial, la zona puede ser designada como llena. Dicha indicación impide que los bits de Átomo en la AgrupaciónDeÁtomos 2802 sean sobrescritos por Átomos 1102 posteriores.

La función VectorizaciónAtómica 2914 también puede incluir una función Más Átomos 3008, que puede determinar si queda algún dato en el bloque de datos 2912 que aún no se ha atomizado y, de ser así, puede llamar a la función Seleccionar Átomos 3000 para otra iteración de la función VectorizaciónAtómica 2914.

Un ejemplo sencillo puede demostrar la función VectorizaciónAtómica 2914. En este ejemplo, la función Seleccionar Átomos 3000 ha creado tres Átomos 1102 a partir de un bloque de datos 2912: 010 (Átomo 1), 111 (Átomo 2) y 10 (Átomo 3). Como se analizará más adelante, los Átomos 1102 no necesitan ser del mismo tamaño.

Siguiendo con el ejemplo, el proceso de atomización 2702 ha configurado 2048 posibles zonas de almacenamiento, donde las zonas 0-2046 están en la AgrupaciónDeÁtomos 2802, y la ClaveDeÁtomos 304 es la zona 2047. Con Z = 2048, z requiere 11 bits para poder seleccionar cualquiera de las Z zonas ($2^{11}$= 2048). El proceso de atomización 2702 también ha configurado un desplazamiento máximo de 7 bits (en otras palabras, el desplazamiento puede ser uno de 8 valores, de 0 a 7), lo cual requiere que o sea 3 bits ($2^3$= 8). En este ejemplo, t, la longitud de cada Vector 3004, tiene 14 bits de longitud (o z concatenada con o).

Siguiendo con el ejemplo, la función Generar Vectores 3002 genera un GeneradorDeVector que en este ejemplo tiene una longitud de 80 bytes. Se muestra una porción de este GeneradorDeVector:

1110...***1***0001100011110***0***0000010010000***1***1101011001100***1***0011000101011010 1...

El índice de GeneradorDeVector para los nuevos Vectores 3004 está, en este ejemplo, en el bit después de la primera elipsis, o en el primer bit en negrita, subrayado y en cursiva. La función Generar Vectores 3002 puede crear el Vector 3004 para el Átomo 1 tomando los primeros 14 (o t) bits comenzando con el índice GeneradorDeVector actual en ese momento: 10001100011 110. Este Vector 3004 está escrito aquí con un espacio entre z y o. Este Vector 3004 indica que su Átomo 1 correspondiente se traducirá a la zona 1123 (binario 10001100011 convertido a decimal) con un desplazamiento de 6 (binario 110 convertido a decimal). El índice de GeneradorDeVector luego se mueve en 14 bits (en este ejemplo, no hay desplazamiento entre los bits de GeneradorDeVector usados para crear los Vectores 3004) al segundo bit en negrita, subrayado y en cursiva. La función Generar Vectores 3002 puede crear el Vector 3004 para el Átomo 2 tomando los siguientes 14 bits comenzando con el índice GeneradorDeVector actual en ese momento: 00000010010 000. Este Vector 3004 está escrito aquí con un espacio entre z y o. Este Vector 3004 indica que su Átomo 2 correspondiente se traducirá a la zona 18 (binario 00000010010 convertido a decimal) sin desplazamiento (binario 000 convertido a decimal). El índice de GeneradorDeVector se mueve 14 bits hasta el tercer bit en negrita, subrayado y en cursiva. La función Generar Vectores 3002 puede crear el Vector 3004 para el Átomo 3 tomando los siguientes 14 bits comenzando con el índice GeneradorDeVector actual en ese momento: 11101011001 100. Este Vector 3004 está escrito aquí con un espacio entre z y o. Este Vector 3004 indica que su Átomo 3 correspondiente se traducirá a la zona 1881 (binario 11101011001 convertido a decimal) con un desplazamiento de 4 (binario 100 convertido a decimal). El índice GeneradorDeVector se mueve 14 bits hasta el cuarto bit en negrita, subrayado y en cursiva.

Siguiendo con el ejemplo, la función Traducir Átomos 3006 toma estos tres Átomos 1102 con sus Vectores 3004 y traduce los Átomos 1102 en base a las instrucciones de los Vectores 3004. El Átomo 1 se traducirá a la zona 1123. Para este ejemplo, supongamos que a continuación se muestra una parte de la zona 1123, previamente llenada con bits aleatorios durante la función Producir AgrupaciónDeÁtomos 2800:

011010010000...101110111110***0***00001***0***00***0***1110010010100101000000...01110000

El ÍndiceDeZona actual en ese momento de la zona 1123 se encuentra en el primer bit en negrita, subrayado y en cursiva. Esta función 3006 desplaza el ÍndiceDeZona en 6 bits (el desplazamiento, o) al segundo bit en negrita, subrayado y en cursiva. Esta función 3006 sobrescribe los bits existentes por el Átomo 1. El número de bits sobrescritos puede ser igual al número de bits en ese Átomo 1102. En otras palabras, los bits 000 (comenzando desde el segundo bit en negrita, subrayado y en cursiva) pueden sobrescribirse a 010 (que son los bits del Átomo 1). El ÍndiceDeZona se puede mover al siguiente bit después del último sobrescrito por el Átomo 1, o al tercer bit en negrita, subrayado y en cursiva. Después de que Átomo 1 se traduzca en la AgrupaciónDeÁtomos 2802, esta porción de la zona 1123 se ve así:

011010010000...10111011111000000010***1***00111001001010010100000000...01110000

donde el Átomo 1 ha cambiado el bit en negrita, en cursiva y subrayado. Los Átomos 2 y 3 pueden traducirse de forma similar mediante la función Traducir Átomos 3006.

La FIGURA 31 muestra un esquema de la función Seleccionar Átomos 3000 de acuerdo con un modo de realización. Esta función 3000 puede tomar un segmento, P, del bloque de datos 2912 que se está atomizando y puede crear Átomos 1102 a partir de este segmento P. En los dibujos, i es el índice del bloque de datos 2912, y j es el índice del segmento P. Después de que se haya atomizado ese segmento, la función Seleccionar Átomos 3000 puede tomar el siguiente segmento y crear los Átomos 1102 a partir de él, continuando durante las iteraciones hasta que se haya atomizado todo el bloque de datos 2912. Cada segmento puede tener m bits de longitud. El índice j puede referirse a la posición del bit inicial de un segmento P dentro del bloque de datos 2912. Por ejemplo, un segmento puede identificarse como $P_j$, y el segmento siguiente puede identificarse como $P_{j+m}$.

Esta función 3000 puede incluir una función Inicializar SelectorDeTabla 3100. La función Inicializar SelectorDeTabla 3100 puede determinar la longitud de bits del segmento m que se usará durante esa iteración de la función Seleccionar Átomos 3000. La función Inicializar SelectorDeTabla 3100 puede inicializar un SelectorDeTabla 3200, que se muestra en la FIGURA 32, que puede usarse para atomizar el segmento. El SelectorDeTabla 3200 puede ser una tabla que tiene n columnas (de 0 a n-1) y x filas (de 1 a x). Cada celda del SelectorDeTabla 3200 puede contener una MáscaraDeÁtomo. Una MáscaraDeÁtomo puede ser una cadena binaria de longitud m. Al seleccionar una columna del SelectorDeTabla 3200, se puede seleccionar un conjunto de MáscarasDeÁtomo (de 1 a x). Las MáscarasDeÁtomo dentro de una columna del SelectorDeTabla 3200 pueden configurarse de manera que cada posición de bit de los m bits tenga un 1 binario en solo una MáscaraDeÁtomo (o fila del SelectorDeTabla 3200). Por ejemplo, para x MáscarasDeÁtomo, todas de m bits de longitud, si la MáscaraDeÁtomo 1 (o la fila 1 del SelectorDeTabla 3200) dentro de la columna 3 tiene un “1” para la posición de bit 5 (suponiendo que m sea al menos igual a 5), todas las otras MáscarasDeÁtomo 2-x dentro de la columna 3 tienen un “0” para la posición de bit 5. Cada MáscaraDeÁtomo puede tener cero, uno o más de un “1” en sus bits. Por ejemplo, una MáscaraDeÁtomo de 2 bits puede ser: 00, 01, 10 u 11. En este ejemplo, si la MáscaraDeÁtomo es 11, todas las demás MáscarasDeÁtomo dentro de esa fila pueden ser 00. Si una MáscaraDeÁtomo contiene todos “0”, esa MáscaraDeÁtomo puede no generar Átomos 1102 del segmento. En un modo de realización, cada MáscaraDeÁtomo contiene “1” en no más de la mitad de sus m bits. En otro modo de realización, cada MáscaraDeÁtomo contiene “1” en no más del 25% de sus m bits. En un modo de realización, cada MáscaraDeÁtomo contiene al menos un “1”. El tamaño del SelectorDeTabla 3200 (en bits) puede multiplicarse por x multiplicado por m.

Las columnas del SelectorDeTabla 3200 pueden configurarse de manera que sus MáscarasDeÁtomo sean patrones diferentes de los de otras columnas. Por ejemplo, si la columna 0 de un SelectorDeTabla 3200 de 2 filas contiene la MáscaraDeÁtomo 1 de “01” y la MáscaraDeÁtomo 2 de “10”, entonces la columna 1 de ese SelectorDeTabla 3200 puede contener la MáscaraDeÁtomo 1 de “10” y la MáscaraDeÁtomo 2 de “01”. El SelectorDeTabla 3200 puede almacenarse en el MapaDeÁtomos 806.

En un modo de realización, x puede ser igual a m. En otro modo de realización, x puede ser menor que m. En otro modo de realización, x puede ser mayor que m, lo que puede dar como resultado que las MáscarasDeÁtomo contengan todos “0”, lo que puede generar más datos para almacenar en el MapaDeÁtomos 806 pero un máximo de m Átomos 1102 puesto que el tamaño mínimo de un Átomo 1102 puede ser un bit. En un modo de realización, el número de columnas en el SelectorDeTabla 3200 puede ser igual al número de diferentes combinaciones de MáscarasDeÁtomo distribuidas entre las filas del SelectorDeTabla 3200. En modos de realización alternativos, el número de columnas en el SelectorDeTabla 3200 puede ser menor o mayor que el número de diferentes combinaciones de MáscarasDeÁtomo distribuidas entre las filas del SelectorDeTabla 3200. Si es mayor, entonces las columnas del SelectorDeTabla 3200 pueden repetirse. Los patrones de MáscaraDeÁtomo dentro de una columna de un SelectorDeTabla 3200 pueden determinarse en base a m y x.

Una vez que se configura el SelectorDeTabla 3200, la función Inicializar SelectorDeTabla 3100 puede determinar el número de bits necesarios para identificar el número de columnas en el SelectorDeTabla 3200. La función Inicializar SelectorDeTabla 3100 puede generar una cadena de bits aleatoria, el Selector 3202, usando el módulo generador aleatorio 2804. El Selector 3202 puede ser al menos tan largo como el número de bits necesarios para identificar el número de columnas en el SelectorDeTabla 3200 y puede ser 100 veces más largo que ese número en un modo de realización. El Selector 3202 puede almacenarse en el MapaDeÁtomos 806.

La función Seleccionar Átomos 3000 también puede incluir una función Seleccionar Segmento 3102, que puede seleccionar un segmento P del bloque de datos 2912 a atomizar, como se ha analizado anteriormente. La función 3102 puede seleccionar los m bits del bloque de datos 2912 a partir del bit de índice j. En un modo de realización, el índice inicial j puede ser 0. En otro modo de realización, el índice inicial j puede empezar desde una posición aleatoria y volver al principio del segmento cuando se alcanza el final de ese segmento. Después de que un segmento ha sido atomizado, el índice del segmento puede incrementarse en m de manera que el índice inicial para la siguiente iteración y segmento puede ser j+m. Si un segmento requiere más bits de los que quedan sin atomizar desde el bloque de datos 2912, pueden usarse bits aleatorios para rellenar el segmento.

La función Seleccionar Átomos 3000 también puede incluir una función Determinar SelectorDeÍndice 3104, que puede determinar qué columna de MáscarasDeÁtomo se aplicará al segmento. La función 3104 puede seleccionar del Selector 3202 un SelectorDeMarco que tiene una longitud de h bits que identifica un número de columna del SelectorDeTabla 3200 para ser usado en la atomización del segmento actual P. El número determinado por el SelectorDeMarco puede ser el SelectorDeÍndice, $S_k$, para ese segmento, $P_j$. El SelectorDeÍndice puede identificar el número de columna del SelectorDeTabla 3200 para usar en la atomización de ese segmento de datos. En un modo de realización, h puede ser igual al número de bits requerido para identificar el número de columnas en el SelectorDeTabla 3200. En un modo de realización, h = (log n)/(log 2). En modos de realización alternativos, h puede ser menor o mayor que el número de bits requerido para identificar el número de columnas en el SelectorDeTabla 3200. En un modo de realización, el número de columnas puede ser una potencia de 2. En otro modo de realización, el número de columnas no es una potencia de 2. Un modo de realización puede tener h de manera que no se puedan seleccionar todas las columnas. Otro modo de realización puede tener h de manera que sean posibles selecciones mayores que la columna más alta, en cuyo caso los modos de realización alternativos pueden volver al principio de la selección de columna desde 0, pueden dividir la selección en módulos y usar el resto, o pueden llamar a la función Determinar SelectorDeÍndice 3104 para generar un nuevo SelectorDeMarco que seleccione una de las columnas.

El punto o índice inicial, k, para el SelectorDeMarco puede ser el bit 0 del Selector 3202, en un modo de realización. En otro modo de realización, el índice inicial, k, puede seleccionarse aleatoriamente. Cuando el SelectorDeMarco determina un SelectorDeÍndice para un segmento, el índice inicial k puede incrementarse en h bits, de manera que el índice inicial para el SelectorDeMarco sucesivo del segmento siguiente o sucesivo puede ser k+h. Cuando el SelectorDeMarco llega al final del Selector 3202, el SelectorDeMarco puede volver al principio del Selector 3202, en un modo de realización.

Una vez que la función Determinar SelectorDeÍndice 3104 ha seleccionado una columna, la función Seleccionar Átomos 3000 puede operar las funciones AND 3106 digitales en el segmento P y cada MáscaraDeÁtomo dentro de la columna seleccionada.

La función Seleccionar Átomos 3000 puede incluir una función Normalizar, que puede tomar los resultados del segmento P aplicando una función AND con las MáscarasDeÁtomo y puede seleccionar los bits resultantes de las posiciones para las cuales cada MáscaraDeÁtomo usada tenía un “1”. Los resultados seleccionados pueden ser los Átomos 1102, uno para cada MáscaraDeÁtomo que tenga un “1” en al menos una posición.

En un modo de realización, m, n, x y h pueden fijarse por la aplicación 106. En otro modo de realización, m, n, x y h pueden variar, ya sea por selección del usuario o automáticamente (ya sea aleatoriamente o en base al tamaño de los datos de usuario). En un modo de realización, se puede usar el mismo SelectorDeTabla 3200 para todos los bloques de datos 2912. En otro modo de realización, el mismo SelectorDeTabla 3200 y el Selector 3202 pueden usarse para procesar todo un bloque de datos 2912 mediante la función Seleccionar Átomos 3000. En otro modo de realización, el SelectorDeTabla 3200 y el Selector 3202 pueden variar entre los bloques de datos de procesamiento 2912 mediante la función Seleccionar Átomos 3000. En diferentes modos de realización, el SelectorDeTabla 3200 se genera para cada nuevo dato de usuario 104 que se atomizará, o para cada nuevo bloque de datos 2912 que se atomizará, donde los patrones MáscaraDeÁtomo dentro del SelectorDeTabla 3200 se pueden generar aleatoriamente. En un modo de realización, h, m, n y x permanecen iguales durante el procesamiento mediante la función Seleccionar Átomos 3000 de todo un bloque de datos 2912. En otro modo de realización, h, m, n y x pueden variar entre el procesamiento por la función Seleccionar Átomos 3000 de diferentes bloques de datos 2912. En un modo de realización, h, m, n y x permanecen iguales durante el procesamiento mediante la función AtomizarDatos 2806 de los datos de entrada 2918. En otro modo de realización, h, m, n y x varían entre el procesamiento mediante la función AtomizarDatos 2806 de los diferentes datos de entrada 2918 (es decir, datos de usuario 104 o iteraciones de MapaDeÁtomos). En un modo de realización, h, m, n y x permanecen iguales durante el proceso de atomización 2702 de los datos de usuario 104.

A medida que m disminuye, el proceso de atomización 2702 se acerca a una distribución aleatoria a nivel de bit de los datos de usuario 104. Donde m = 1, no se necesitarían más MáscarasDeÁtomo para aleatorizar los datos, pero se generaría un mayor número de Vectores 3004 (uno para cada bit), lo que distribuiría más aleatoriamente los bits de datos de usuario y generaría un MapaDeÁtomos 806 más grande. El aumento de m puede aumentar la posibilidad de que los bits cercanos de los datos de entrada 2918 se puedan almacenar cerca en la AgrupaciónDeÁtomos 2802 o la ClaveDeÁtomos 304 y disminuir el tamaño del MapaDeÁtomos 806. Los Átomos

1102 resultantes pueden incluir bits de los datos de entrada 2918 que no son contiguos. Los Átomos 1102 resultantes también pueden incluir bits de los datos de entrada 2918 que son contiguos.

Un ejemplo puede ilustrar la función Seleccionar Átomos 3000. En este ejemplo, una porción del bloque de datos 2912 es:

001...0***0***0110110***0***10100001110010110111001110000000100000000111111100...0

En este ejemplo, la función Inicializar SelectorDeTabla 3100 puede establecer la longitud del segmento, m, para que sea 8. La función 3100 puede Inicializar SelectorDeTabla 3200 para que tenga 3 filas (x = 3) y 64 columnas (de 0 a 63). Cada una de las 192 celdas (3x64) dentro del SelectorDeTabla 3200 tiene una MáscaraDeÁtomo de 8 bits de largo y se amolda a los patrones analizados anteriormente. En este ejemplo, ninguna MáscaraDeÁtomo en el SelectorDeTabla 3200 tendrá todos “0”, lo que significa que se generarán tres Átomos 1102 para cada segmento puesto que x = 3.

Siguiendo con el ejemplo, la función Inicializar SelectorDeTabla 3100 puede establecer la longitud del SelectorDeMarco h = 6 puesto que 6 bits serán suficientes para identificar cualquiera de las 64 columnas del SelectorDeTabla 3200 (es decir, $2^6$=64). La función 3100 puede generar un Selector 3202 de 75 bytes que se muestra parcialmente a continuación:

011110100...10100***0***111111***1***0000010101011100011111000010001111 1...1001110

Siguiendo con el ejemplo, la función Seleccionar Átomos 3000 puede proceder después a la función Seleccionar Segmento 3102, que selecciona un segmento P de m bits del bloque de datos 2912 mencionado anteriormente. En este ejemplo, el bit de índice actual es el primer bit en negrita, subrayado y en cursiva que se muestra en el bloque de datos 2912, puesto que los bits anteriores (a la izquierda del índice) se han procesado en pasadas anteriores de las funciones 3102-3108. P para este ejemplo es 00110110. Estos son los bits que se atomizarán en esta pasada de las funciones 3102-3108. El índice del segmento puede moverse 8 bits después de que este segmento actual se haya atomizado, de manera que el índice inicial para el siguiente segmento es el segundo bit en negrita, subrayado y en cursiva que se muestra en el bloque de datos 2912.

Siguiendo con el ejemplo, la función Seleccionar Átomos 3000 puede proceder después a la función Determinar SelectorDeÍndice 3104. Esta función 3104 usa el SelectorDeMarco, comenzando con el índice inicial que es el primer bit en negrita, subrayado y en cursiva en el Selector 3202 mostrado anteriormente, para determinar el SelectorDeÍndice para este segmento. El SelectorDeMarco de 6 bits de longitud para este segmento contiene 011111 (que es 31 en forma decimal), que es el SelectorDeÍndice para este segmento. Este SelectorDeÍndice significa que este segmento se atomizará usando la columna 31 del SelectorDeTabla 3200. El índice inicial o SelectorDeÍndice se incrementa en 6 bits hasta el segundo bit en negrita, en cursiva y subrayado.

Siguiendo con el ejemplo, la función Seleccionar Átomos 3000 puede proceder después a la función AND 3106, que puede realizar tres operaciones AND (puesto que x = 3), aplicando un AND del segmento P con cada una de las MáscarasDeÁtomo almacenadas en las tres filas de la columna 31 del SelectorDeTabla 3200. En este ejemplo, el SelectorDeTabla se ha inicializado en la función Inicializar SelectorDeTabla 3100 de manera que la columna 31 tiene las MáscarasDeÁtomo siguientes: La MáscaraDeÁtomo 1 en la fila 1 es 01001001, la MáscaraDeÁtomo 2 en la fila 2 es 10000100 y la MáscaraDeÁtomo 3 en la fila 3 es 00110010. En la primera operación AND, se aplica una función AND del segmento P con la MáscaraDeÁtomo 1:

00110110 AND 01001001 = 0***0***00***0***00***0*** (Producto 1)

En la segunda operación AND, se aplica una función AND del segmento P con la MáscaraDeÁtomo 2:

00110110 AND 10000100 = ***0***0000***1***00 (Producto 2)

En la tercera operación AND, se aplica una función AND del segmento P con la MáscaraDeÁtomo 3:

00110110 AND 00110010 = 00***11***00***1***0 (Producto 3)

Siguiendo con el ejemplo, la función Seleccionar Átomos 3000 puede proceder después a la función Normalizar 3108, que puede normalizar los Productos de la función AND 3106. La MáscaraDeÁtomo 1 tiene un "1" en las posiciones de bit 2, 5 y 8; la MáscaraDeÁtomo 2 tiene un "1" en las posiciones de bit 1 y 6; la MáscaraDeÁtomo 3 tiene un "1" en las posiciones de bit 3, 4 y 7. Ninguna posición de bit tiene un "1" en más de una MáscaraDeÁtomo, y cada posición de bit tiene un "1" en al menos una MáscaraDeÁtomo. Por lo tanto, la normalización del Producto 1 resulta en tomar los bits 2, 5 y 8 del Producto 1 y concatenarlos juntos como Átomo 1. El Átomo 1 es 000. La normalización del Producto 2 resulta en tomar los bits 1 y 6 del Producto 2 y concatenarlos juntos como Átomo 2. El Átomo 2 es 01. La normalización del Producto 3 resulta en tomar los bits 3, 4 y 7 del Producto 3 y concatenarlos juntos como Átomo 3. El Átomo 3 es 111. Los bits normalizados en los Productos están en negrita, subrayados y en cursiva arriba. Como se ve en los resultados, los Átomos 1102 pueden tener diferentes longitudes. Además, los Átomos 1102 resultantes pueden incluir bits no contiguos del segmento de datos original, y también 1102 pueden

incluir bits contiguos del segmento de datos original (por ejemplo, el "11" contiguo en los bits 3 y 4 del Producto 3). En este ejemplo, las funciones 3102-3108 se repetirían para atomizar todos los segmentos restantes del bloque de datos 2912 antes de traducir esos Átomos 1102 a la AgrupaciónDeÁtomos 2802 o ClaveDeÁtomos 304 como se ha descrito anteriormente.

Los diversos índices pueden ser índices de proceso que pueden no guardarse en los MapasDeÁtomos 806. La aplicación 106 puede programarse para realizar el proceso de atomización 2702 a partir de un valor establecido para cada índice (por ejemplo, 0 o cualquier otro valor), en un modo de realización, y por lo tanto puede realizar el proceso de desatomización 2706, como se analiza a continuación, trabajando en orden inverso al proceso de atomización 2702, conociendo el valor inicial de cada índice. En otro modo de realización, donde el valor inicial de un índice puede variar, como se ha analizado anteriormente, el valor inicial de ese índice puede incluirse en el MapaDeÁtomos 806 apropiado para que el proceso de desatomización 2706 pueda tener el valor inicial para ese índice en la desatomización.

Se proporciona otro ejemplo de un modo de realización. En este ejemplo, los datos de usuario 104 son 1,5 MB. Después de la función Comprimir 2902, los datos comprimidos 2904 son 0,96 MB. Después de la función Aleatorizar 2906, los datos aleatorizados 2908 son 1,0 MB (1.000.000 bytes). El inflado de la AgrupaciónDeÁtomos 2802 es de 200.000 bytes, lo que puede permitir el almacenamiento de MapasDeÁtomos 806 y el desplazamiento de Átomos 1102. El tamaño de AgrupaciónDeÁtomos es de 1.200.000 bytes. La AgrupaciónDeÁtomos 2802 tiene 255 zonas (0-254) y la ClaveDeÁtomos 304 es la zona 255. El tamaño de cada zona en la AgrupaciónDeÁtomos 2802 es de 4.686 bytes y el tamaño de la ClaveDeÁtomos 304 es de 5.000 bytes. La longitud del Vector, t, es de 10 bits, incluyendo z de 8 bits y o de 2 bits.

Siguiendo con el ejemplo, el GeneradorDeVector tiene 80 bytes (640 bits) y el Selector 3202 también tiene 80 bytes (640 bits). El SelectorDeTabla 3200 tiene 64 columnas (n = 64) y 3 filas (x = 3). El tamaño del SelectorDeMarco, h, es de 6 bits. El tamaño del bloque de datos es de 1000 bytes y el tamaño del segmento, m, es de 8 bits (o un byte). El tamaño de cada MáscaraDeÁtomo es de 8 bits y el tamaño del SelectorDeTabla 3200 es de 192 bytes.

Siguiendo con el ejemplo, la primera iteración de la función VectorizaciónAtómica 2914 tiene 1000 bloques de datos 2912 puesto que los datos aleatorios 2908 son 1.000.000 bytes y cada bloque de datos 2912 es de 1000 bytes. El $MapaDeÁtomos^0$ 806 tiene un encabezado de 4 bytes; 64 bytes de datos sobre cómo se han creado los datos comprimidos 2904 y los datos aleatorios 2908; y 1000 bloques, cada uno de 164 bytes, que contienen información sobre cómo se ha atomizado cada bloque de datos 2912; para un tamaño total de 164.068 bytes. El $MapaDeÁtomos^0$ 806 contiene información sobre la atomización de los datos de usuario 104.

Siguiendo con el ejemplo, la segunda iteración de la función VectorizaciónAtómica 2914 usa el $MapaDeÁtomos^0$ 806 de la primera iteración como datos de entrada 2918. La segunda iteración de esta función 2914 usa los mismos parámetros que en la primera iteración. La segunda iteración de la función 2914 tiene 164 bloques de datos 2912 puesto que los datos son 164.068 bytes y cada bloque de datos 2912 es de 1000 bytes. El $MapaDeÁtomos^1$ 806 tiene un encabezado de 4 bytes; 64 bytes de datos sobre cómo se han creado los datos comprimidos 2904 de esta iteración y los datos aleatorizados 2908 de esta iteración; y 164 bloques, cada uno de 164 bytes, que contiene información sobre cómo se ha atomizado cada bloque de datos 2912; para un tamaño total de 29.964 bytes. El $MapaDeÁtomos^1$ 806 contiene información sobre la atomización de $MapaDeÁtomos^0$ 806.

Siguiendo con el ejemplo, la tercera iteración de la función VectorizaciónAtómica 2914 usa el $MapaDeÁtomos^1$ 806 de la segunda iteración como datos de entrada 2918. La tercera iteración de esta función 2914 usa los mismos parámetros que en la primera iteración. La tercera iteración de la función 2914 tiene 27 bloques de datos 2912 porque los datos son 29.964 bytes y cada bloque de datos 2912 es de 1000 bytes. El $MapaDeÁtomos^2$ 806 tiene un encabezado de 4 bytes; 64 bytes de datos sobre cómo se han creado los datos comprimidos 2904 de esta iteración y los datos aleatorizados 2908 de esta iteración; y 27 bloques, cada uno de 164 bytes, que contienen información sobre cómo se ha atomizado cada bloque de datos 2912; para un tamaño total de 4.496 bytes. El $MapaDeÁtomos^2$ 806 contiene información sobre la atomización de $MapaDeÁtomos^1$ 806. La función ReducirMapaDeÁtomos 2808 detiene las iteraciones de la función AtomizarDatos 2806 puesto que el tamaño del $MapaDeÁtomos^2$ 806 final es lo suficientemente pequeño. El $MapaDeÁtomos^2$ 806 final resultante es de aproximadamente 5 KB, la ClaveDeÁtomos 304 es de 5 KB y la AgrupaciónDeÁtomos 2802 es de 1,2 MB.

Con referencia a la FIGURA 27, el proceso de transporte/almacenamiento 2704 puede almacenar o transportar la AgrupaciónDeÁtomos 2802, la ClaveDeÁtomos 304 y el MapaDeÁtomos 806 de forma segura una vez que finaliza el proceso de atomización 2702. Las FIGURAS 33-39 muestran modos de realización alternativos del proceso de transporte/almacenamiento 2704.

La FIGURA 33 muestra un modo de realización del proceso de transporte/almacenamiento 2704. El proceso 2704 puede incluir una función Almacenar AgrupaciónDeÁtomos 3300, que puede almacenar la AgrupaciónDeÁtomos 2802 en un medio de almacenamiento 2206. Esta función 3300 puede copiar la AgrupaciónDeÁtomos 2802 del ordenador que ha atomizado los datos de usuario 104 en el medio 2206 que no está en la nube 108. Las modos de realización alternativos de los medios de almacenamiento 2206 incluyen, pero no se limitan a, discos duros, discos

magnéticos, cintas, discos ópticos, CD, DVD, unidades de estado sólido o dispositivos de almacenamiento y unidades de memoria flash USB.

El proceso 2704 también puede incluir una función Almacenar Clave 3302, que puede almacenar la ClaveDeÁtomos 304 y el MapaDeÁtomos 806 en un medio de almacenamiento 2206 que es diferente del 2206 en el que se almacena la AgrupaciónDeÁtomos 2802, en un modo de realización. El medio 2206 que almacena la ClaveDeÁtomos 304 y el MapaDeÁtomos 806 puede ser un teléfono móvil, una unidad de memoria flash USB o una tarjeta de comunicaciones de campo cercano (NFC), en modos de realización alternativos. En otro modo de realización, la ClaveDeÁtomos 304, el MapaDeÁtomos 806 y la AgrupaciónDeÁtomos 2802 pueden almacenarse en el mismo medio 2206.

La FIGURA 34 muestra otro modo de realización del proceso de transporte/almacenamiento 2704. El proceso 2704 puede incluir una función Enviar AgrupaciónDeÁtomos 3400, que puede almacenar la AgrupaciónDeÁtomos 2802 en la nube 108 en un medio de almacenamiento en la nube 110, en un modo de realización. Esta función 3400 puede usar protocolos y servicios de comunicación típicos para la transmisión. En un modo de realización, la AgrupaciónDeÁtomos 2802 puede cifrarse usando un cifrado convencional antes de almacenarla 2802 en la nube 108. La función 3400 puede registrar la ubicación 3402 del almacenamiento AgrupaciónDeÁtomos, que puede incluir un localizador uniforme de recursos (URL) o un identificador universalmente único (UUID). El proceso 2704 puede incluir una función Almacenar Clave 3404, que puede ser similar a la función Almacenar Clave 3302. Esta función 3404 puede almacenar la ubicación del almacenamiento AgrupaciónDeÁtomos 3402, la ClaveDeÁtomos 304 y el MapaDeÁtomos 806 en un medio de almacenamiento 2206.

La FIGURA 35 muestra otro modo de realización del proceso de transporte/almacenamiento 2704, que puede ser similar al proceso 2704 que se muestra en la FIGURA 34, excepto que la función Enviar AgrupaciónDeÁtomos 3500 puede almacenar la AgrupaciónDeÁtomos 2802 en múltiples medios de almacenamiento, registrando la ubicación 3402 de cada uno. El almacenamiento en múltiples medios puede añadir redundancia y mejorar el resultado. En un modo de realización, la AgrupaciónDeÁtomos 2802 puede fragmentarse y dispersarse en múltiples medios de almacenamiento en la nube 110.

La FIGURA 36 muestra otro modo de realización del proceso de transporte/almacenamiento 2704, que puede ser similar al proceso 2704 que se muestra en la FIGURA 35. Después de la función Enviar AgrupaciónDeÁtomos 3500, el proceso 2704 puede incluir una función Enviar MetaClave 3600, que puede almacenar el MapaDeÁtomos 806 y las ubicaciones de almacenamiento 3402 de la AgrupaciónDeÁtomos 2802 en la nube. Esta función 3600 puede usar protocolos y servicios de comunicación típicos para la transmisión. Esta función 3600 puede usar cifrado convencional en el MapaDeÁtomos 806 y/o las ubicaciones 3402. El almacenamiento en la nube del MapaDeÁtomos 806 puede mejorar la conveniencia de este sistema 100. El MapaDeÁtomos 806 y las ubicaciones 3402 juntas pueden denominarse la MetaClave. El proceso 2704 también puede incluir una función Almacenar Clave 3602, que puede almacenar la ClaveDeÁtomos 304 en un medio de almacenamiento 2206 similar a cómo la función Almacenar Clave 3404 ha almacenado la ClaveDeÁtomos 304.

La FIGURA 37 muestra otro modo de realización del proceso de transporte/almacenamiento 2704, que puede ser similar al proceso 2704 que se muestra en la FIGURA 36. Después de la función Enviar MetaClave 3600, el proceso 2704 puede incluir una función BloquearLibreta ClaveDeÁtomos 3700, que puede combinar o procesar la ClaveDeÁtomos 304 con una LibretaDeÁtomos 3702 para obtener una LibretaDeÁtomosBloqueada 3704. En un modo de realización, una LibretaDeÁtomos 3702 puede ser un conjunto aleatorio de datos tan grande como la ClaveDeÁtomos 304. En otro modo de realización, una LibretaDeÁtomos 3702 puede ser un conjunto aleatorio de datos más grande que la ClaveDeÁtomos 304. En un modo de realización, la LibretaDeÁtomos 3702 puede generarse con un módulo generador aleatorio 2804. En un modo de realización, la LibretaDeÁtomos 3702 puede ser una libreta de un solo uso (OTP). En otro modo de realización, la LibretaDeÁtomos 3702 puede ser una libreta de uso múltiple. La LibretaDeÁtomos 3702 puede usarse para confundir la ClaveDeÁtomos 304 de modo que 304 pueda transmitirse y/o almacenarse en la nube 108. La LibretaDeÁtomos 3702 puede usarse para confundir de forma segura un número cualquiera de ClavesDeÁtomos 304 puesto que tanto la ClaveDeÁtomos 304 como la LibretaDeÁtomos 3702 son cadenas aleatorias. La LibretaDeÁtomos 3702 puede compartirse entre dispositivos o usuarios para permitir que la ClaveDeÁtomos 304 sea determinada y usada para acceder a los datos de usuario atomizados 104. En un modo de realización, la LibretaDeÁtomosBloqueada 3704 es el resultado de una ClaveDeÁtomos 304 aplicando una función XOR con la LibretaDeÁtomos 3702.

El proceso 2704 también puede incluir una función Enviar LibretaDeÁtomosBloqueada 3706, que puede transmitir la LibretaDeÁtomosBloqueada 3704 y almacenarla 3704 en la nube 108 en los medios de almacenamiento en la nube 110. Esta transmisión puede realizarse a través de protocolos y servicios de comunicación típicos. En un modo de realización, la LibretaDeÁtomosBloqueada 3704 puede cifrarse usando cifrado convencional antes de la transmisión. Si la LibretaDeÁtomosBloqueada 3704 está comprometida, el pirata informático aún no podrá usar la LibretaDeÁtomosBloqueada 3704 solo para descifrar fácilmente los datos de usuario atomizados 104 puesto que la LibretaDeÁtomosBloqueada 3704 es una cadena aleatoria; el pirata informático tendrá que adivinar todas las permutaciones posibles de la cadena que tiene la longitud de la LibretaDeÁtomosBloqueada 3704, cuya longitud puede, en un modo de realización analizado anteriormente, ser de 65536 bits para una ClaveDeÁtomos 304 de 8

KB, lo que representa una fuerza bruta o estrategia de adivinanza irrealizable incluso con el poder de computación disponible hoy o en el futuro.

La FIGURA 38 muestra un diagrama conceptual simplificado del proceso de atomización 2702. Los datos de usuario 104 originales que se van a cifrar se pueden aleatorizar en los datos aleatorizados 2908. Estos datos aleatorios 2908 pueden atomizarse aleatoriamente y distribuirse aleatoriamente en la ClaveDeÁtomos 304 y/o la AgrupaciónDeÁtomos 2802 con el mapa de distribución guardado en el MapaDeÁtomos$^0$ 806. El MapaDeÁtomos$^0$ 806 también se puede atomizar y distribuir aleatoriamente a la ClaveDeÁtomos 304 y/o a la AgrupaciónDeÁtomos 2802 con su mapa de distribución guardado en el MapaDeÁtomos$^1$ 806. Si bien el proceso de atomización 2702 puede continuar con iteraciones adicionales atomizando el MapaDeÁtomos$^1$ 806, solo se muestra una de esas iteraciones. El resultado puede ser una ClaveDeÁtomos 304 aleatoria, una AgrupaciónDeÁtomos 2802 aleatoria y un MapaDeÁtomos 806 que puede almacenarse o transportarse mediante el proceso de transporte/almacenamiento 2704.

El proceso de desatomización 2706 puede funcionar en orden inverso al proceso de atomización 2702. El proceso 2706 puede recopilar la AgrupaciónDeÁtomos 2802, la ClaveDeÁtomos 304 y el MapaDeÁtomos 806 (la última iteración del MapaDeÁtomos 806 que no se ha atomizado más), usar las instrucciones del MapaDeÁtomos para recuperar los Átomos 1102 mapeados a partir de la AgrupaciónDeÁtomos 2802 y la ClaveDeÁtomos 304, volver a llenar los segmentos y luego los bloques de datos 2912 a partir de los Átomos 1102, reensamblar los bloques de datos 2912 y desaleatorizar y descomprimir los datos 2918. Si los datos resultantes 2918 son otro MapaDeÁtomos 806, el proceso de desatomización 2706 puede repetir otra iteración, iterando recursivamente hasta que los datos 2918 sean los datos de usuario 104 en lugar de un MapaDeÁtomos 806. Si la AgrupaciónDeÁtomos 2802 se almacena en la nube 108, el proceso de desatomización 2702 puede recuperarla 2802 usando su ubicación de almacenamiento 3402. Si el MapaDeÁtomos 806, la ClaveDeÁtomos 304 y/o las ubicaciones 3402 también se almacenan en la nube 108, el proceso de desatomización 2702 puede recuperarlos (y descifrarlos si es necesario).

La FIGURA 39 muestra un diagrama de un modo de realización del sistema 100 donde los datos de usuario 104 son atomizados y compartidos por un primer ordenador o dispositivo 102 con un segundo ordenador o dispositivo 116. El primer dispositivo 102 puede atomizar los datos de usuario 104, generando una AgrupaciónDeÁtomos 2802, una ClaveDeÁtomos 304 y un MapaDeÁtomos 806. La AgrupaciónDeÁtomos 2802 y el MapaDeÁtomos 806 se pueden guardar en los medios de almacenamiento en la nube 110. Las ubicaciones de almacenamiento de la AgrupaciónDeÁtomos 3402 también pueden almacenarse en la nube 108. En modos de realización alternativos, se pueden usar los mismos o diferentes medios de almacenamiento 110 para guardar estos componentes. El primer dispositivo 102 puede usar la ClaveDeÁtomos 304 y la LibretaDeÁtomos 3702 para crear la LibretaDeÁtomosBloqueada 3704 y cargarla 3704 en los medios de almacenamiento en la nube 110.

El segundo dispositivo 116 puede ser notificado de la nueva MetaClave cargada (es decir, las ubicaciones 3402 y MapaDeÁtomos 806), por ejemplo, por el usuario del primer dispositivo 102 o por el servicio en la nube que aloja la MetaClave. El segundo dispositivo 116 puede descargar la MetaClave. Si la MetaClave está cifrada o requiere autentificación para su acceso, el usuario del primer dispositivo 102 puede proporcionar dicha información al usuario del segundo dispositivo 116 para dar acceso al segundo dispositivo 116 a la MetaClave. Usando la MetaClave, el segundo dispositivo 116 puede descargar la AgrupaciónDeÁtomos 2802 y la LibretaDeÁtomosBloqueada 3704. El segundo dispositivo 116 puede haber sido provisto previamente de forma segura con la LibretaDeÁtomos 3702. El segundo dispositivo 116 puede usar la LibretaDeÁtomos 3702 y la LibretaDeÁtomosBloqueada 3704 recuperada para obtener la ClaveDeÁtomos 304, que en un modo de realización puede realizarse mediante una función XOR. Con la AgrupaciónDeÁtomos 2802, la ClaveDeÁtomos 304 y el MapaDeÁtomos 806, el segundo dispositivo 116 puede desatomizar los datos de usuario 104 como se ha descrito anteriormente.

La FIGURA 40 muestra un diagrama de un modo de realización de cómo un dispositivo u ordenador (aquí, el tercer dispositivo 4000) puede obtener una LibretaDeÁtomos 3702 que puede usarse para obtener la ClaveDeÁtomos 304, como se ha analizado anteriormente. Una lista de datos aleatorios 4002 puede publicarse y estar disponible para descargarse desde los medios de almacenamiento en la nube 110. Esta lista 4002 puede ser de cualquier tamaño, por ejemplo, 1 MB, 10 MB, 100 MB o más. El tercer dispositivo 4000 puede descargar estos datos aleatorios 4002. Una Clave LibretaDeÁtomos 4004 puede entregarse de forma segura al usuario del tercer dispositivo 4000, por ejemplo, personalmente, por mensajería, por servicio postal, por teléfono (ya sea verbalmente o como transmisión de datos), o por otro procedimiento o medio de comunicación fuera de banda. La Clave LibretaDeÁtomos 4004 puede identificar ubicaciones aleatorias dentro de los datos aleatorios 4002 que se combinan para producir la LibretaDeÁtomos 3702. En modos de realización alternativos, la Clave LibretaDeÁtomos 4004 puede codificarse (por ejemplo, como un código QR o código de barras) antes de la entrega. La Clave LibretaDeÁtomos 4004 puede ser lo suficientemente grande para el tipo de datos que se protege. Una vez que se obtiene la LibretaDeÁtomos 3702, el tercer dispositivo 4000 puede recuperar y desatomizar los datos de usuario similares al segundo dispositivo 116 en el análisis con respecto a la FIGURA 39 anterior.

En un modo de realización, los datos aleatorios 4002 pueden estar dispuestos en una matriz. La Clave LibretaDeÁtomos 4004 pueden ser coordenadas de elementos en la matriz. Por ejemplo, los datos aleatorios 4002 pueden ser una matriz de 1000 KB x 1000 KB donde cada elemento contiene 2 KB de datos. Si la LibretaDeÁtomos 3702 tiene un tamaño de 8 KB, entonces se pueden usar cuatro tuplas para identificar los elementos en la matriz de

datos aleatorios 4002 que se combinan para producir la LibretaDeÁtomos 3702. Por ejemplo, la Clave LibretaDeÁtomos 4004 puede ser 793-134, 379-983, 037-328, 714-382.

En un modo de realización alternativa, la LibretaDeÁtomos 3702 puede codificarse en un dispositivo de hardware o dispositivo que se requiere que se conecte a un ordenador de desatomización para desatomizar los datos. En otro modo de realización, la LibretaDeÁtomos 3702 puede ser entregada fuera de banda por mensajería o por el servicio postal. En otro modo de realización, la LibretaDeÁtomos 3702 puede proporcionarse por teléfono, ya sea verbalmente o como una transmisión de datos. En modos de realización alternativos, la ClaveDeÁtomos 304 puede ser entregada personalmente (o por mensajería o servicio postal) al usuario del segundo dispositivo 116 fuera de banda, ya sea que la ClaveDeÁtomos 304 se guarde en el medio de almacenamiento 2206, directamente impresa en papel o algún otro objeto tangible, o codificado en papel u otro objeto tangible (por ejemplo, como un código QR o código de barras). En otro modo de realización, la persona que atomiza los datos de usuario 104 puede llamar al usuario destinado a desatomizar los datos 104 y puede proporcionar verbalmente la ClaveDeÁtomos 304 por teléfono. En otro modo de realización, la ClaveDeÁtomos 304 puede comunicarse mediante una transmisión de datos a través de un teléfono.

Las FIGURAS 33-37 y 39-40 divulgan la transferencia de información hacia y desde los medios de almacenamiento 2206 y los medios de almacenamiento en la nube 110. En modos de realización alternativos, cualquiera de dichos medios (ya sea divulgado en las figuras como medios de almacenamiento 2206 o medios de almacenamiento en la nube 110) puede ser local o remoto respecto al ordenador que realiza la atomización, puede ser un medio de almacenamiento en red, puede ser un medio de almacenamiento empresarial, pueden ser medios de almacenamiento distribuidos, o pueden ser medios de almacenamiento en la nube. Diversos modos de realización pueden incluir protección para datos almacenados en cualquier medio de almacenamiento físico (incluyendo unidad USB, disco duro, tarjeta NFC, teléfono inteligente o dispositivo móvil), así como almacenamiento en la nube o distribuido.

Los modos de realización divulgados pueden variarse alterando el orden de las funciones u operaciones divulgadas u omitiendo o duplicando funciones u operaciones. Se pueden combinar diversas características de los modos de realización con características de otros modos de realización. Los modos de realización y ejemplos divulgados no son limitativos.

**REIVINDICACIONES**

**1.** Un procedimiento para asegurar los datos de usuario (104), que comprende las etapas de:

a) establecer los datos de usuario (104) como datos de entrada;

b) fragmentar aleatoriamente los datos de entrada en una pluralidad de Átomos (1102), donde un Átomo (1102) se define como al menos un bit de datos, y distribuir aleatoriamente los Átomos (1102) en una AgrupaciónDeÁtomos (2802) y una ClaveDeÁtomos (304), cada una de los cuales se define como un bloque de almacenamiento de datos o memoria diferente pero relacionado con la otra; y

c) registrar información sobre la fragmentación y la distribución de la etapa b) en instrucciones llamadas un MapaDeÁtomos (806);

**caracterizado por que**:

la AgrupaciónDeÁtomos (2802) y ClaveDeÁtomos (304) preexisten la distribución de la etapa b); la AgrupaciónDeÁtomos (2802) de la etapa b) se divide en un número de zonas, el número que es Z-1, con la ClaveDeÁtomos (304) que es la zona Z; y

la distribución de la etapa b) comprende las etapas de:

d) seleccionar aleatoriamente la zona en la que se distribuye un Átomo (1102), en el que la selección de zona se produce por separado para cada Átomo (1102);

e) copiar cada Átomo (1102) en la zona seleccionada para ese Átomo (1102) en la etapa d), comenzar en un índice de zona para esa zona, que indica el bit inicial **en esa** zona, sobrescribir cualquier dato que exista en una ubicación donde cada Átomo (1102) se copia, donde la ubicación comienza desde el índice de zona y el número de bits sobrescritos puede ser igual al número de bits en el Átomo; y

f) mover el índice de zona de cada zona en la que se ha copiado cualquier Átomo (1102) en la etapa e) a una ubicación, al bit siguiente, inmediatamente después de la ubicación donde se copia el Átomo (1102).

**2.** El procedimiento de la reivindicación 1, en el que la etapa d) comprende, además, las etapas de:

g) determinar si la zona seleccionada está llena de Átomos (1102) previamente distribuidos en esa zona; y

h) seleccionar aleatoriamente otra zona si la determinación de la etapa g) es afirmativa;

el procedimiento que además comprende las etapas de:

i) seleccionar aleatoriamente un desplazamiento para cada Átomo (1102); y

j) mover el índice de zona de la zona seleccionada en la etapa d) para cada Átomo (1102) por el desplazamiento seleccionado en la etapa i) para ese Átomo (1102);

en el que:

las etapas i) - j) se realizan antes de la etapa e);

la distribución de la etapa b) además comprende las etapas de:

k) generar una cadena binaria aleatoria llamada GeneradorDeVector;

l) para cada Átomo (1102), la selección de t bits contiguos del GeneradorDeVector, en el que:

t incluye suficientes bits para seleccionar la zona en la etapa d) y para seleccionar el desplazamiento en la etapa h);

los bits t se denominan un Vector (3004);

z es una porción del Vector (3004) que selecciona la zona en la etapa d);

o es una porción del Vector (3004) que selecciona el desplazamiento en la etapa i); y

los grupos sucesivos de t bits del GeneradorDeVector se usan para generar Vectores (3004) para los Átomos sucesivos (1102);

m) usar z de cada Vector (3004) en la etapa d) para seleccionar la zona para el Átomo (1102) correspondiente a ese Vector (3004); y

n) usar o de cada Vector (3004) en la etapa i) para seleccionar el desplazamiento para el Átomo (1102) correspondiente a ese Vector (3004); y

la etapa c) comprende además la etapa de:

o) registrar el GeneradorDeVector en el MapaDeÁtomos (806).

**3.** El procedimiento de la reivindicación 1 o 2, que comprende además las etapas de:

p) establecer el MapaDeÁtomos (806) de la etapa c) como los datos de entrada; y

q) repetir al menos una iteración de las etapas b) - c), en el que el MapaDeÁtomos (806) de una iteración final de la etapa c) es un MapaDeÁtomos final (806).

**4.** El procedimiento de las reivindicaciones 1-3, en el que el tamaño del MapaDeÁtomos (806) después de cualquier iteración de las etapas b) - c) es menor que el tamaño de los datos de entrada fragmentados y distribuidos durante esa iteración; el procedimiento comprende además las etapas de:

r) comprimir los datos de entrada;

s) aleatorizar previamente los datos de entrada comprimidos de la etapa r);

t) registrar información sobre la compresión de la etapa r) e información sobre la aleatorización previa de la etapa s) en el MapaDeÁtomos (806); y

u) rellenar la AgrupaciónDeÁtomos (2802) y la ClaveDeÁtomos (304) con datos aleatorios;

en el que:

las etapas r) - s) se realizan antes de la etapa b);

la fragmentación y la distribución de los datos de entrada en la etapa b) son los datos de entrada previamente aleatorizados de la etapa s);

la AgrupaciónDeÁtomos (2802) de la etapa b) es más grande que los datos de entrada previamente aleatorizados de la etapa s);

la etapa u) se realiza antes de la distribución de la etapa b);

la fragmentación de la etapa b) comprende las etapas de:

v) seleccionar aleatoriamente un bloque de datos (2912) de los datos de entrada;

w) fragmentar el bloque de datos seleccionado (2912) en una pluralidad de Átomos (1102); y

x) repetir las etapas v) - w) hasta que cada bloque de datos (2912) de los datos de entrada se haya fragmentado; y

la etapa w) comprende las etapas de:

y) seleccionar un segmento contiguo de m bits del bloque de datos (2912);

z) fragmentar el segmento seleccionado en una pluralidad de Átomos (1102); y

aa) repetir las etapas y) - z) para un siguiente segmento hasta que todo el bloque de datos (2912) se haya fragmentado.

**5.** El procedimiento de la reivindicación 4, en el que la etapa z) comprende las etapas de:

bb) crear una pluralidad x de cadenas binarias llamadas MáscarasDeÁtomo, cada una con m bits, en el que cada una de las posiciones del bit m tiene un "1" en solo una de las MáscarasDeÁtomo;

cc) realizar operaciones AND entre el segmento seleccionado de la etapa y) y cada una de las MáscarasDeÁtomo de la etapa bb); y

dd) normalizar cada resultado de las operaciones AND de la etapa cc), cada resultado normalizado que es un Átomo (1102).

**6.** El procedimiento de las reivindicaciones 4 o 5, en el que la etapa z) comprende, además, las etapas de:

ee) crear una matriz, llamada un SelectorDeTabla (3200), que tiene x filas y n columnas;

ff) llenar cada celda del SelectorDeTabla (3200) con una cadena binaria llamada una MáscaraDeÁtomo de manera que cada columna del SelectorDeTabla (3200) contenga una pluralidad de MáscarasDeÁtomo de la etapa bb), en el que la pluralidad de MáscarasDeÁtomo de una columna difiere en el patrón de la pluralidad de MáscarasDeÁtomo de las columnas vecinas;

gg) generar una cadena binaria aleatoria llamada un Selector (3202);

hh) para cada segmento seleccionado de la etapa y), seleccionar h bits contiguos del Selector (3202), en el que:

h incluye suficientes bits para seleccionar n; y

los grupos sucesivos de h bits del Selector (3202) se usan para segmentos sucesivos; y

ii) usar los bits seleccionados de la etapa hh) para seleccionar una columna del SelectorDeTabla (3200), en la que las MáscarasDeÁtomo usadas en la etapa cc) son las contenidas en la columna seleccionada; y

la etapa c) comprende además la etapa de:

jj) registrar el Selector (3202) en el MapaDeÁtomos (806).

**7.** El procedimiento de las reivindicaciones 3 a 6, que comprende, además, las etapas de:

kk) establecer el MapaDeÁtomos (806) final de la etapa q) como un MapaDeÁtomos (806) de entrada;

ll) usar el MapaDeÁtomos (806) de entrada de la etapa kk) para recopilar y reensamblar la pluralidad de Átomos (1102) de la AgrupaciónDeÁtomos (2802) y la ClaveDeÁtomos (304) en los datos de salida; y

mm) si los datos de salida de una iteración de la etapa ll) son un MapaDeÁtomos (806), establecer esos datos de salida como el MapaDeÁtomos de entrada (806) y repetir las iteraciones de la etapa ll) hasta que los datos de salida no sean un MapaDeÁtomos (806);

en el que las etapas kk) - mm) se realizan después de la etapa q).

**8.** El procedimiento de las reivindicaciones 3 a 7, que comprende, además, las etapas de:

nn) almacenar la AgrupaciónDeÁtomos (2802) de la etapa b) en un primer medio de almacenamiento (2206); y

oo) almacenar la ClaveDeÁtomos (304) de la etapa b) y el MapaDeÁtomos (806) final de la etapa q) en un segundo medio de almacenamiento (2206);

en el que las etapas nn) - oo) se realizan después de la etapa q).

**9.** El procedimiento de las reivindicaciones 3 a 8, que comprende, además, las etapas de:

qq) almacenar la AgrupaciónDeÁtomos (2802) de la etapa b) en al menos un medio de almacenamiento (2206);

rr) registrar información de ubicación (3402) del almacenamiento de la etapa qq) en un segundo medio de almacenamiento (2206);

ss) almacenar el MapaDeÁtomos (806) final de la etapa q) en el segundo medio de almacenamiento (2206); y

tt) almacenar la ClaveDeÁtomos (304) de la etapa b) en un tercer medio de almacenamiento (2206);

en el que las etapas qq) - tt) se realizan después de la etapa q).

**10.** El procedimiento de las reivindicaciones 3 a 9, que comprende, además, las etapas de:

uu) almacenar la AgrupaciónDeÁtomos (2802) de la etapa b) en al menos un medio de almacenamiento (2206);

vv) registrar información de ubicación (3402) del almacenamiento de la etapa uu) en un segundo medio de almacenamiento (2206);

ww) almacenar el MapaDeÁtomos (806) final de la etapa q) en el segundo medio de almacenamiento (2206);

xx) combinar la ClaveDeÁtomos (304) con una cadena aleatoria llamada una LibretaDeÁtomos (3702) para producir otra cadena aleatoria llamada una LibretaDeÁtomosBloqueada (3704); y

yy) almacenar la LibretaDeÁtomosBloqueada (3704) de la etapa xx) en un tercer medio de almacenamiento (2206);

en el que las etapas uu) - yy) se realizan después de la etapa q).

**11.** El procedimiento de acuerdo con la reivindicación 10, que comprende, además, las etapas de:

zz) recuperar la AgrupaciónDeÁtomos (2802) almacenada en la etapa uu) del al menos un medio de almacenamiento (2206);

aaa) recuperar la información de ubicación (3402) registrada en la etapa vv) y el MapaDeÁtomos final (806) almacenado en la etapa ww) del segundo medio de almacenamiento (2206);

bbb) recuperar la LibretaDeÁtomosBloqueada (3704) almacenada en la etapa yy) del tercer medio de almacenamiento (2206);

ccc) aplicar la LibretaDeÁtomos (3702) a la LibretaDeÁtomosBloqueada (3704) recuperada en la etapa bbb) para producir la ClaveDeÁtomos (304);

ddd) establecer el MapaDeÁtomos final (806) recuperado en la etapa aaa) como un MapaDeÁtomos de entrada (806);

eee) usar el MapaDeÁtomos (806) de entrada de la etapa ddd) para recopilar y reensamblar la pluralidad de Átomos (1102) de la AgrupaciónDeÁtomos (2802) recuperada en la etapa zz) y la ClaveDeÁtomos (304) producida en la etapa ccc) en los datos de salida; y

fff) si los datos de salida de una iteración de la etapa eee) son un MapaDeÁtomos (806), establecer esos datos de salida como el MapaDeÁtomos (806) de entrada y repetir las iteraciones de la etapa

eee) hasta que los datos de salida no sean un MapaDeÁtomos (806);

en el que las etapas zz) - fff) se realizan después de la etapa yy).

**12.** El procedimiento de acuerdo con la reivindicación 11, que comprende, además, las etapas de:

ggg) obtener una lista de datos aleatorios; y

hhh) obtener la LibretaDeÁtomos (3702) usando la lista de datos aleatorios de la etapa ggg);

en el que:

las etapas ggg) - hhh) se realizan antes de la etapa ccc); y

la LibretaDeÁtomos (3702) obtenida en la etapa hhh) se aplica en la etapa ccc).

**13.** Un medio no transitorio legible por ordenador que comprende instrucciones para hacer que un ordenador (102) realice el procedimiento de la reivindicación 3.

**14.** Un sistema (100) para asegurar los datos de usuario (104), que comprende:

un primer ordenador (102); y

un segundo ordenador (116) en comunicación con el primer ordenador (102);

en el que el primer ordenador (102) está programado para:

ejecutar las etapas a) - j) y p) - q) del procedimiento de la reivindicación 7; y

comunicar la AgrupaciónDeÁtomos (2802), la ClaveDeÁtomos (304) y el MapaDeÁtomos final (806) al segundo ordenador (116); y

en el que el segundo ordenador (116) está programado para ejecutar las etapas kk) - mm) del procedimiento de la reivindicación 7.

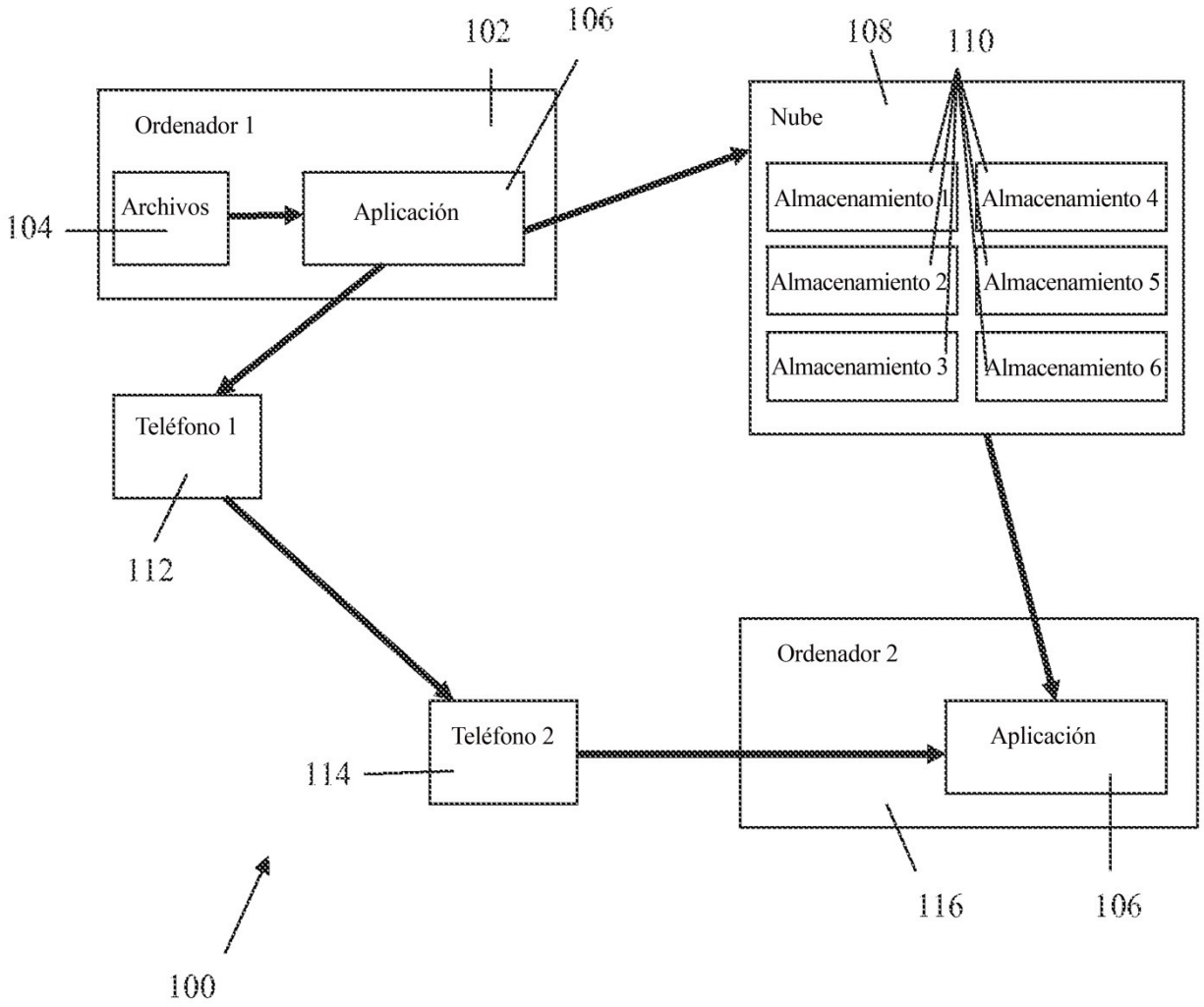
102
106
108
110
Ordenador 1
Archivos
Aplicación
104
Nube
Almacenamiento 1
Almacenamiento 4
Almacenamiento 2
Almacenamiento 5
Almacenamiento 3
Almacenamiento 6
Teléfono 1
112
Ordenador 2
Teléfono 2
Aplicación
114
116
106
100

Fig. 1

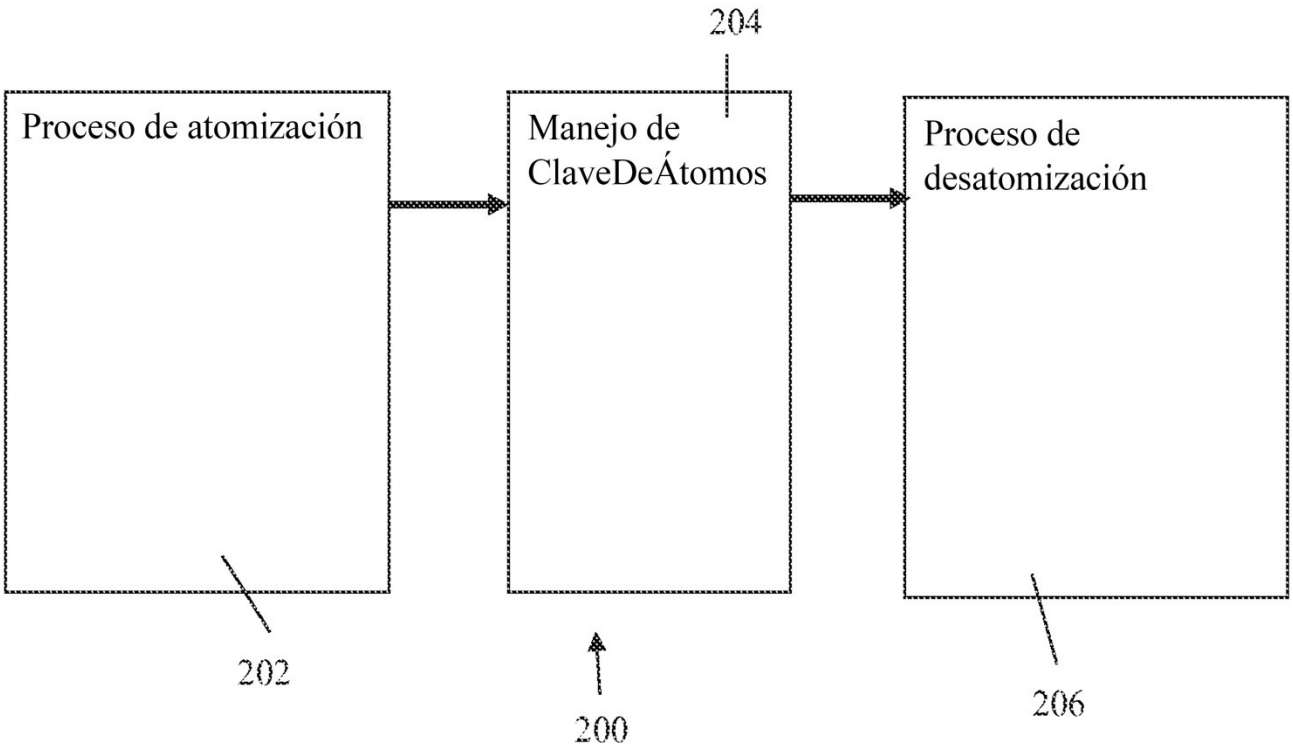
204
Proceso de atomización
Manejo de ClaveDeÁtomos
Proceso de desatomización
202
200
206

Fig. 2

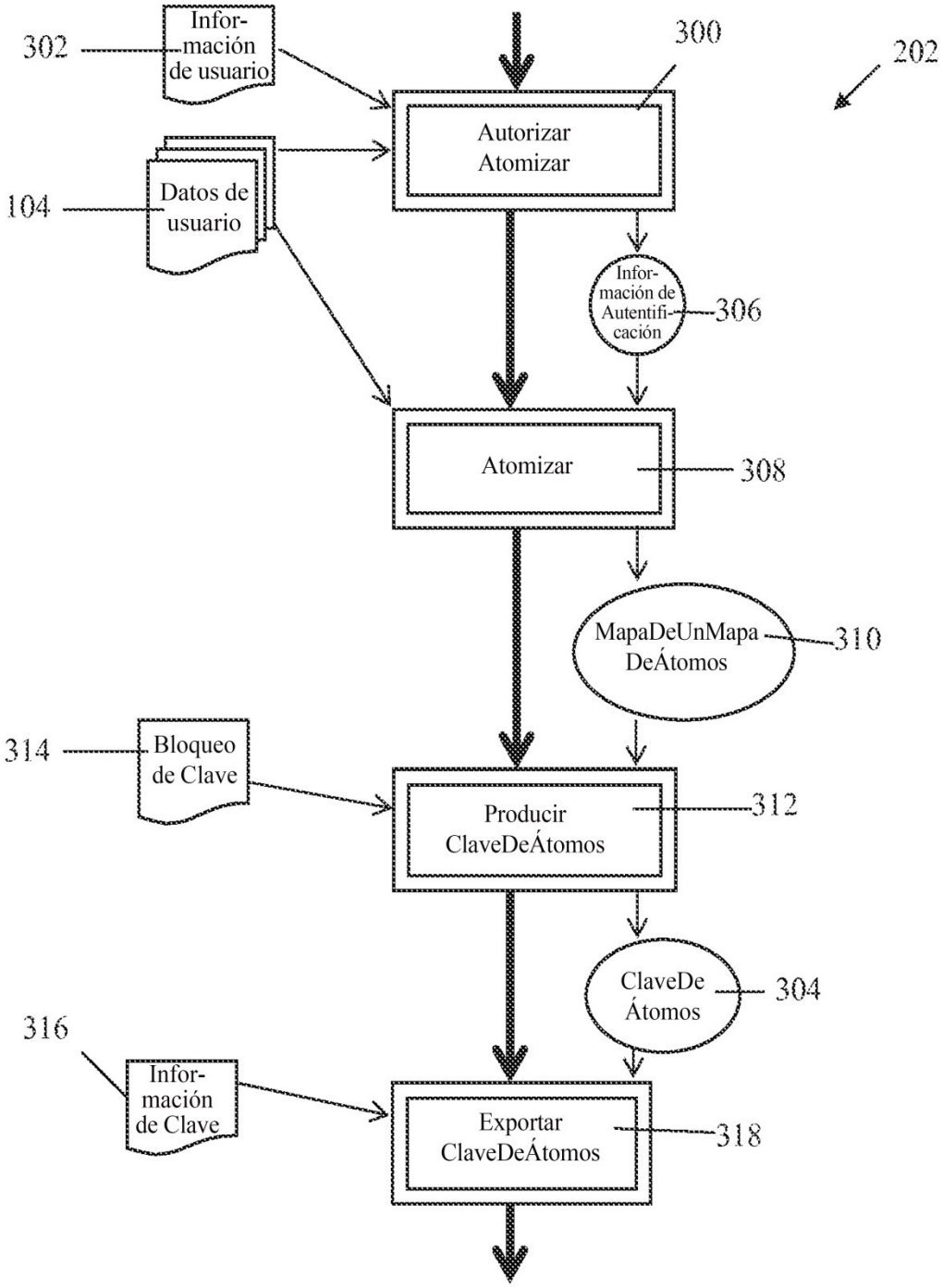
302
Infor-
mación
de usuario
300
202
Autorizar
Atomizar
104
Datos de
usuario
Infor-
mación de
Autentifi-
cación
306
Atomizar
308
MapaDeUnMapa
DeÁtomos
310
314
Bloqueo
de Clave
Producir
ClaveDeÁtomos
312
ClaveDe
Átomos
304
316
Infor-
mación
de Clave
Exportar
ClaveDeÁtomos
318

Fig. 3

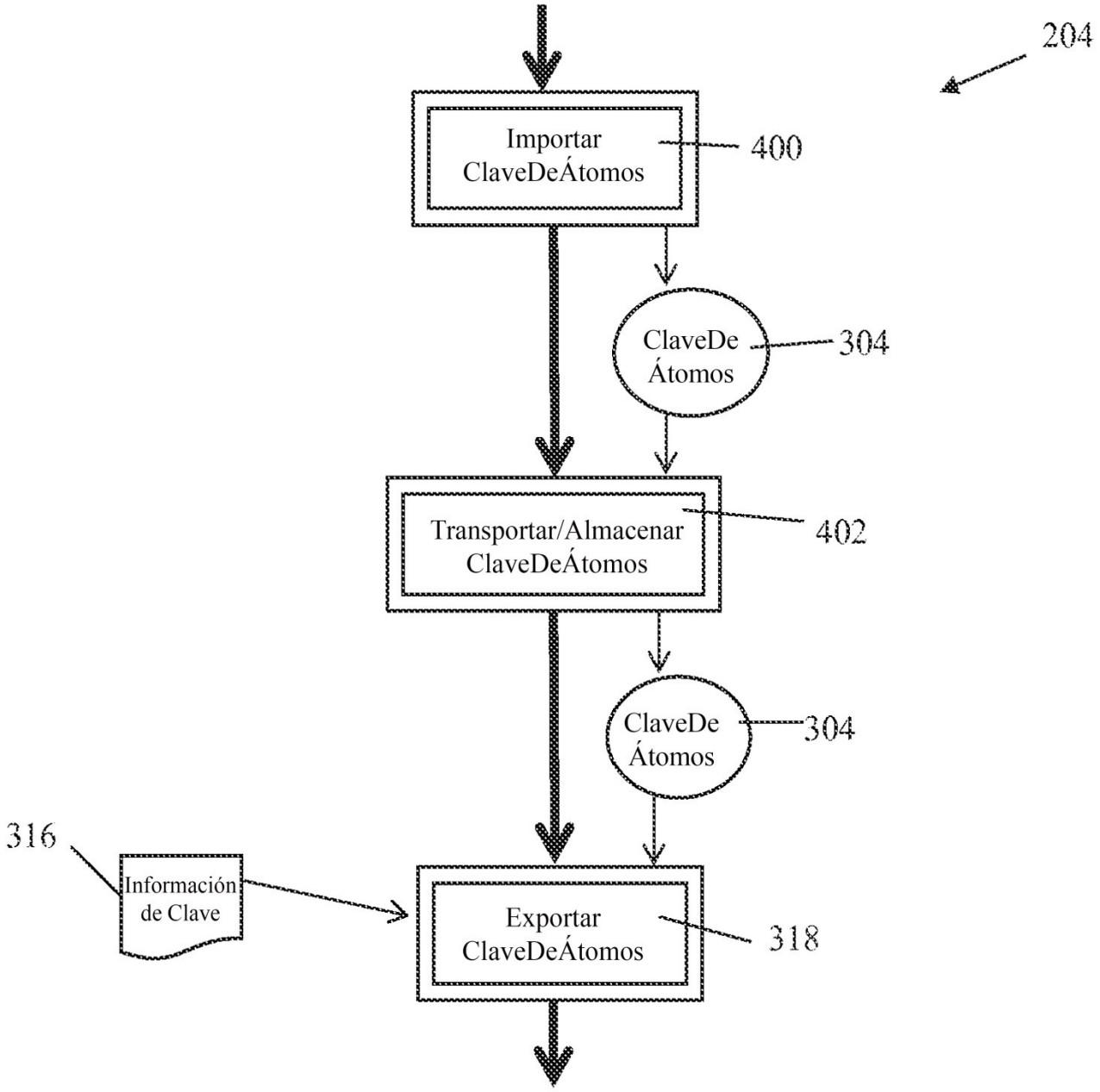
204
Importar ClaveDeÁtomos
400
ClaveDe Átomos
304
Transportar/Almacenar ClaveDeÁtomos
402
ClaveDe Átomos
304
316
Información de Clave
Exportar ClaveDeÁtomos
318

Fig. 4

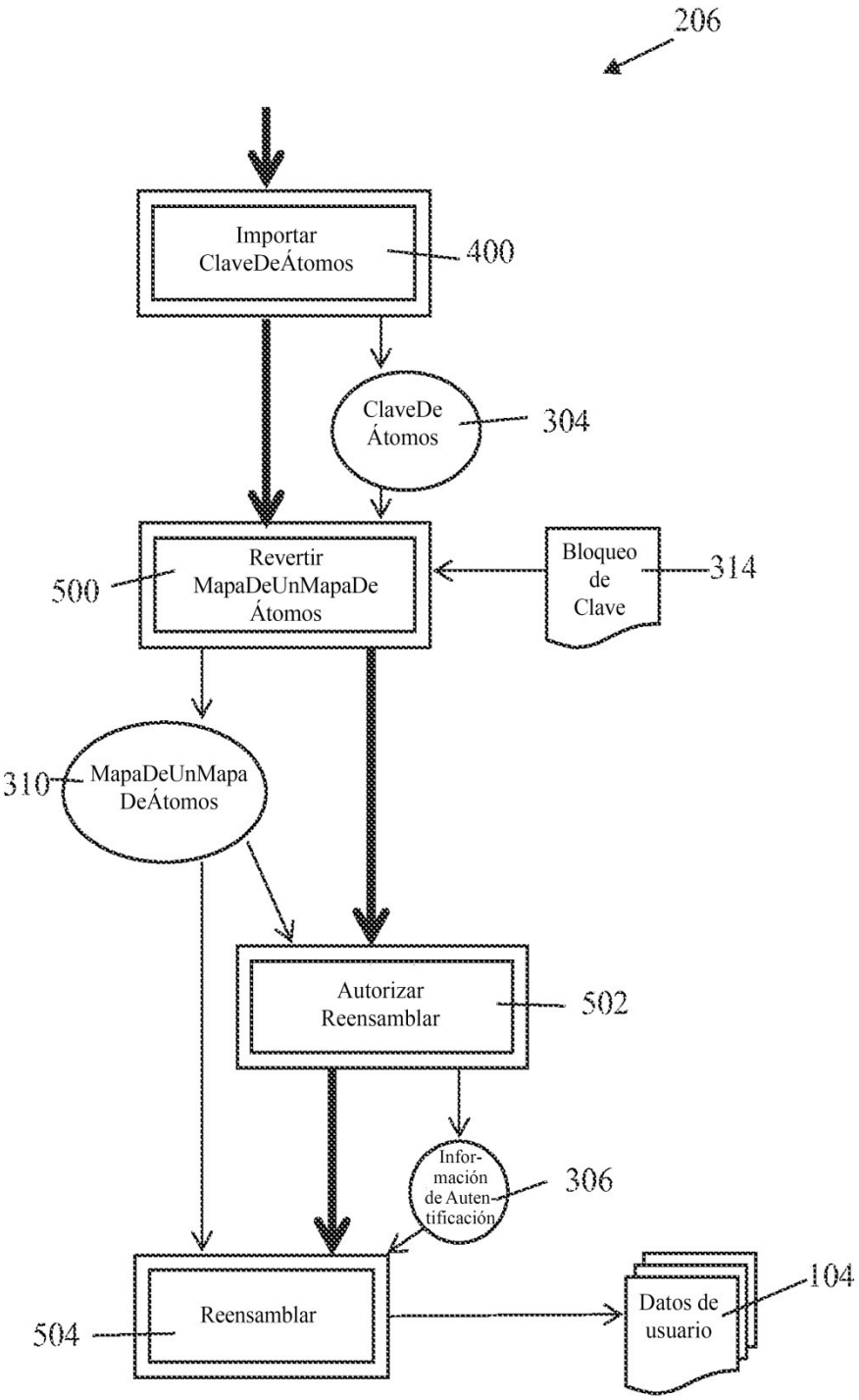
206
Importar ClaveDeÁtomos
400
ClaveDe Átomos
304
Revertir MapaDeUnMapaDe Átomos
500
Bloqueo de Clave
314
MapaDeUnMapa DeÁtomos
310
Autorizar Reensamblar
502
Infor-mación de Auten-tificación
306
Reensamblar
504
Datos de usuario
104

Fig. 5

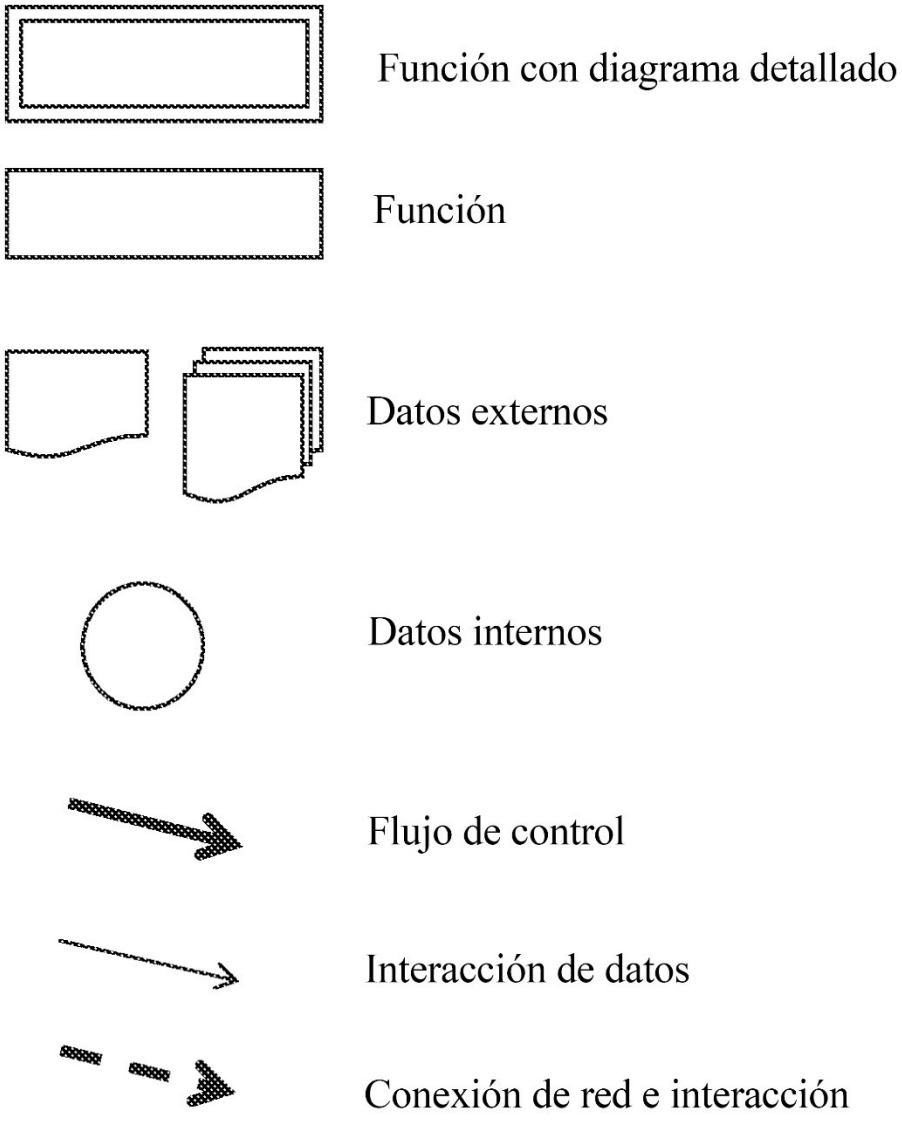
Función con diagrama detallado
Función
Datos externos
Datos internos
Flujo de control
Interacción de datos
Conexión de red e interacción

Fig. 6

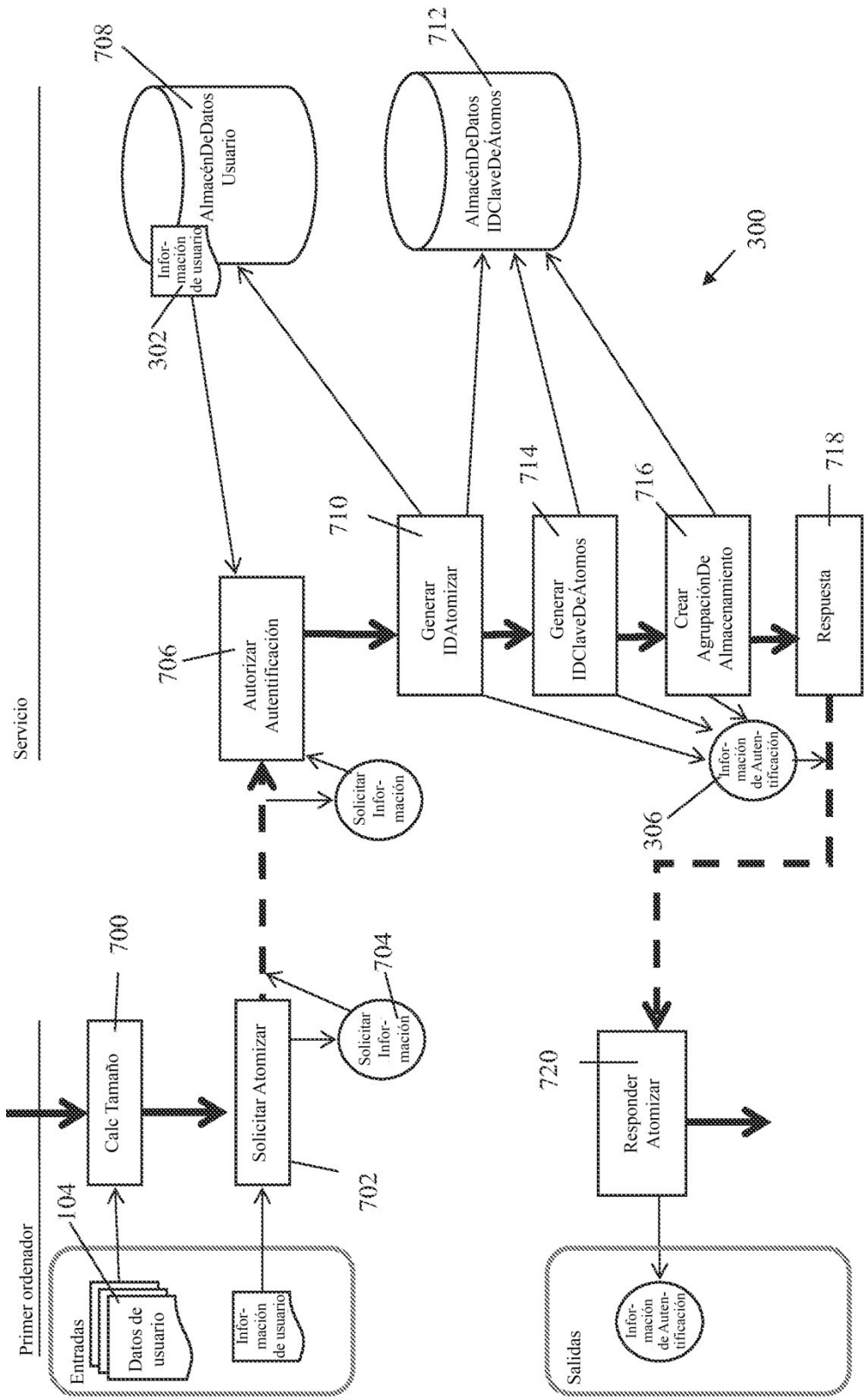
Primer ordenador
Servicio
Entradas
Datos de usuario
104
Información de usuario
Calc Tamaño
700
Solicitar Atomizar
702
Solicitar Información
704
Autorizar Autentificación
706
Solicitar Información
AlmacénDeDatos Usuario
708
Información de usuario
302
Generar IDAtomizar
710
Generar IDClaveDeÁtomos
714
Crear AgrupaciónDe Almacenamiento
716
Respuesta
718
AlmacénDeDatos IDClaveDeÁtomos
712
Información de Autentificación
306
300
Responder Atomizar
720
Salidas
Información de Autentificación

Fig. 7

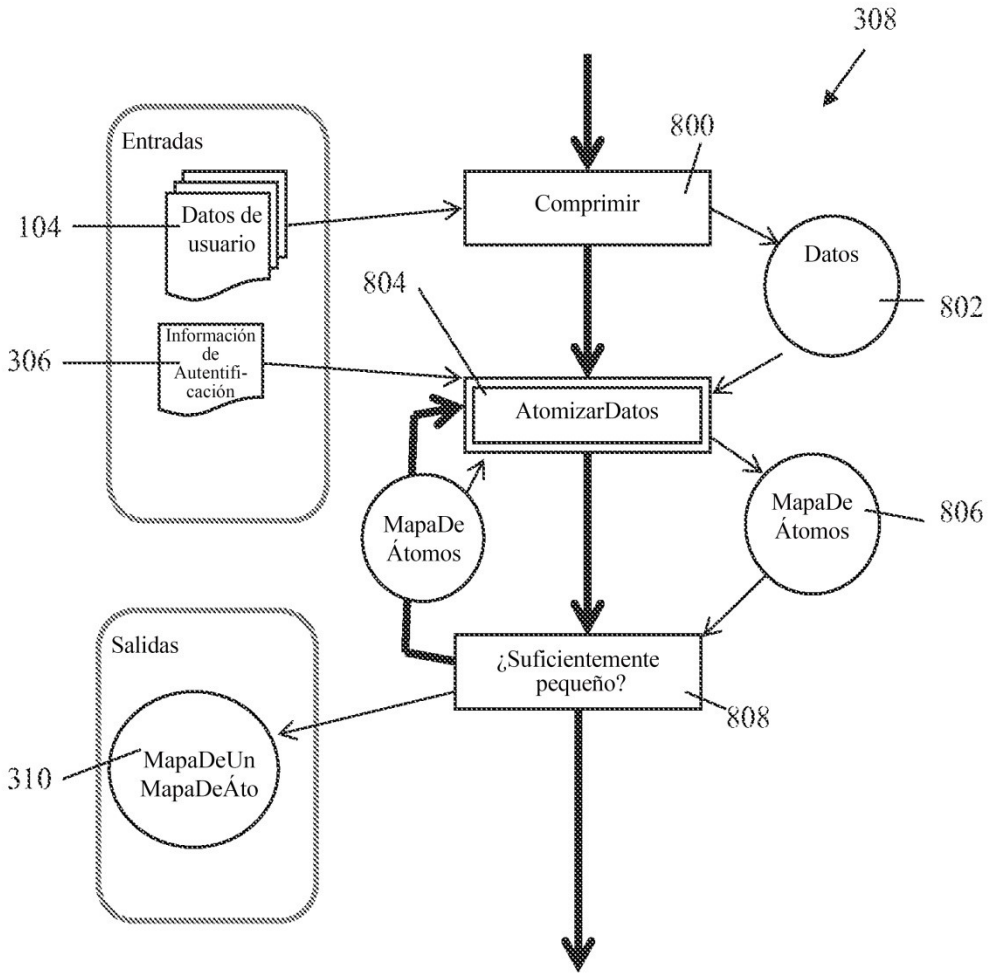
308
Entradas
800
Comprimir
104
Datos de usuario
Datos
802
804
306
Información de Autentifi-cación
AtomizarDatos
MapaDe Átomos
MapaDe Átomos
806
Salidas
¿Suficientemente pequeño?
808
310
MapaDeUn MapaDeÁto

Fig. 8

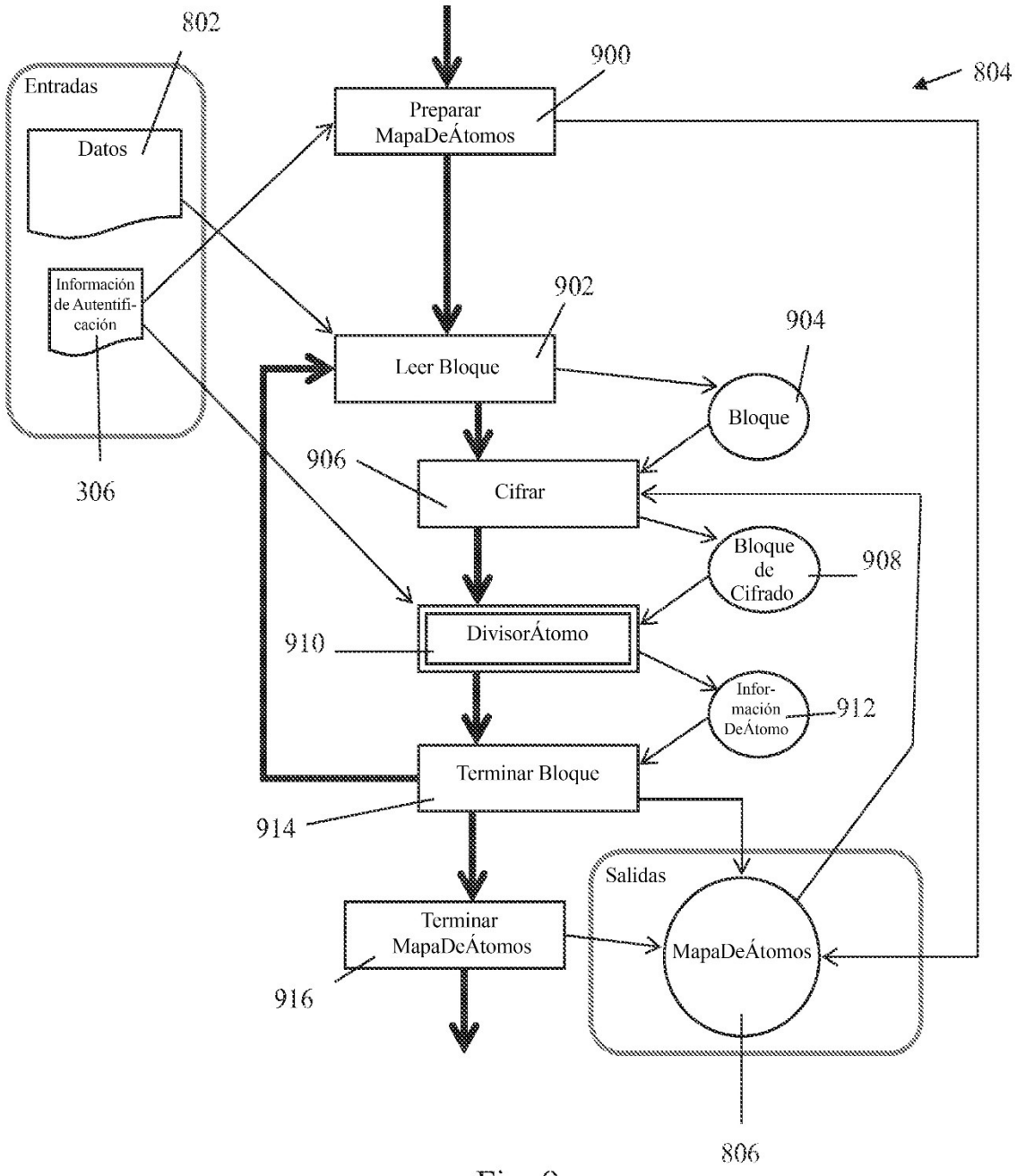
802
Entradas
Datos
Información de Autentifi-cación
306
900
Preparar MapaDeÁtomos
804
902
Leer Bloque
904
Bloque
906
Cifrar
Bloque de Cifrado
908
910
DivisorÁtomo
Infor-mación DeÁtomo
912
Terminar Bloque
914
Salidas
Terminar MapaDeÁtomos
MapaDeÁtomos
916
806

Fig. 9

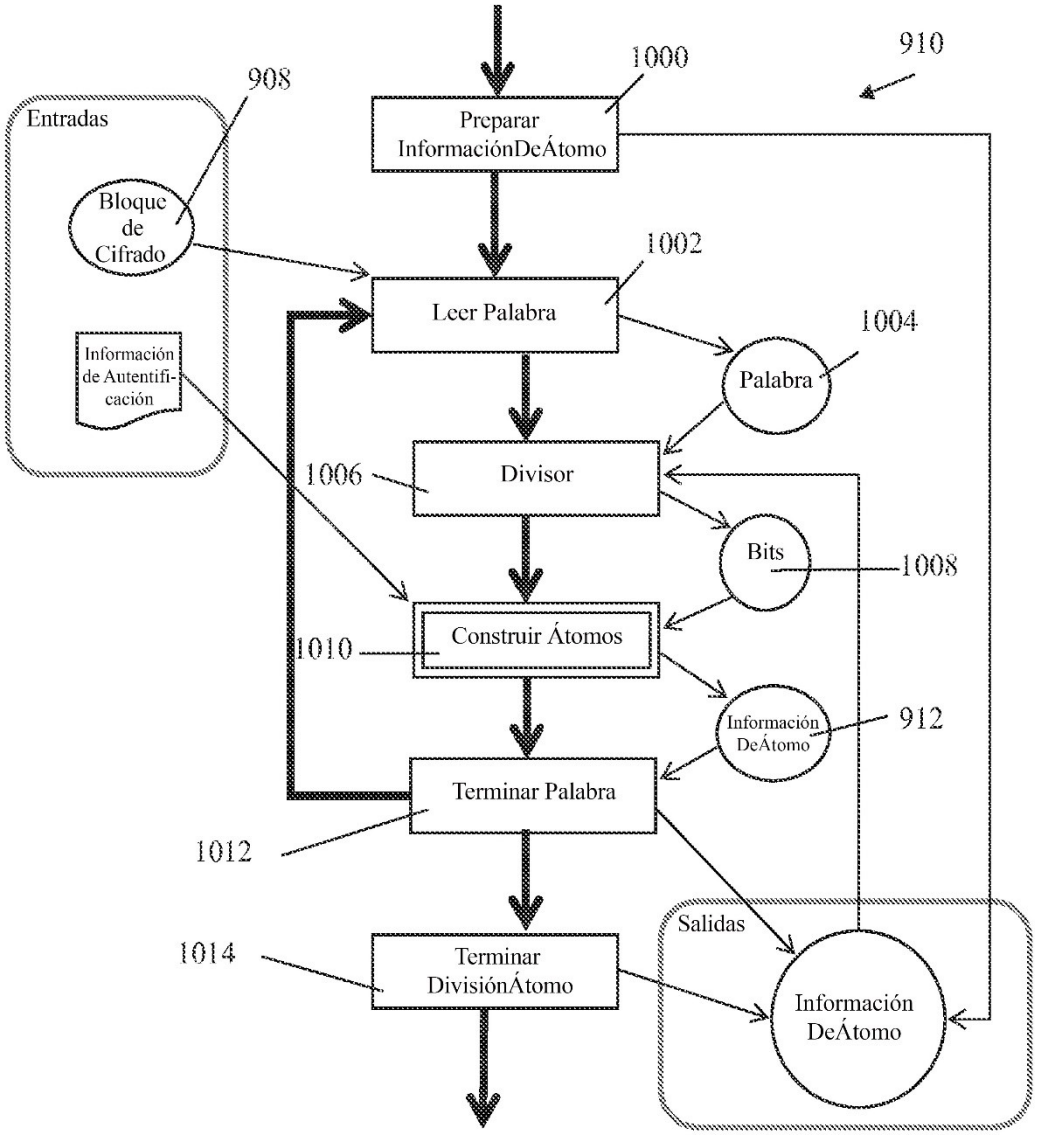
910
908
1000
Entradas
Preparar InformaciónDeÁtomo
Bloque de Cifrado
1002
Leer Palabra
1004
Información de Autentifi-cación
Palabra
1006
Divisor
Bits
1008
1010
Construir Átomos
Información DeÁtomo
912
Terminar Palabra
1012
Salidas
1014
Terminar DivisiónÁtomo
Información DeÁtomo

Fig. 10

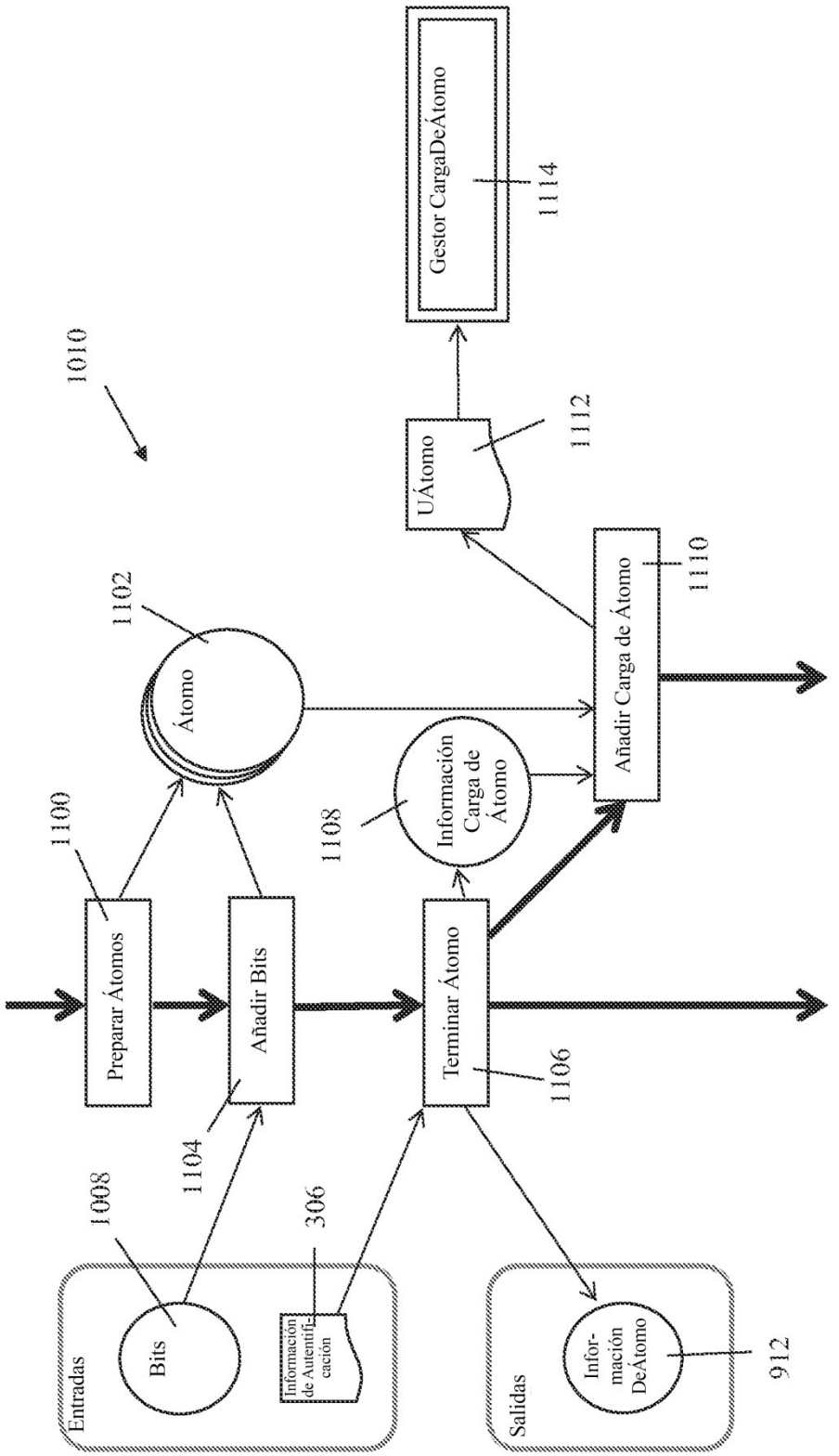
1010
Gestor CargaDeÁtomo
1114
UÁtomo
1112
Átomo
1102
Añadir Carga de Átomo
1110
Información Carga de Átomo
1108
Preparar Átomos
1100
Añadir Bits
Terminar Átomo
1106
1104
1008
306
Entradas
Bits
Información de Autentifi-cación
Salidas
Infor-mación DeAtomo
912

Fig. 11

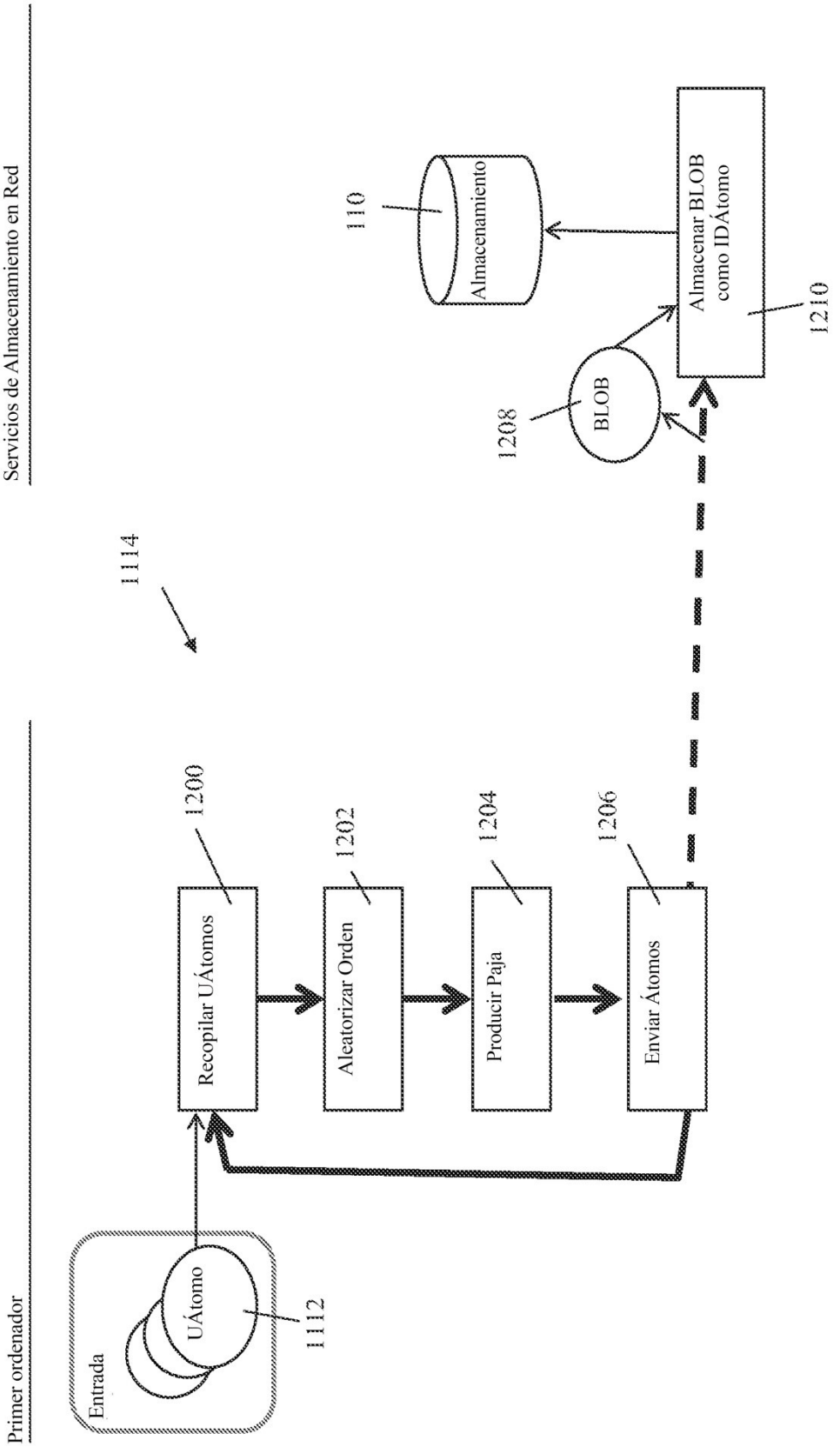
Servicios de Almacenamiento en Red
Primer ordenador
Entrada
UÁtomo
1112
1114
Recopilar UÁtomos
1200
Aleatorizar Orden
1202
Producir Paja
1204
Enviar Átomos
1206
BLOB
1208
Almacenar BLOB como IDÁtomo
1210
Almacenamiento
110

Fig. 12

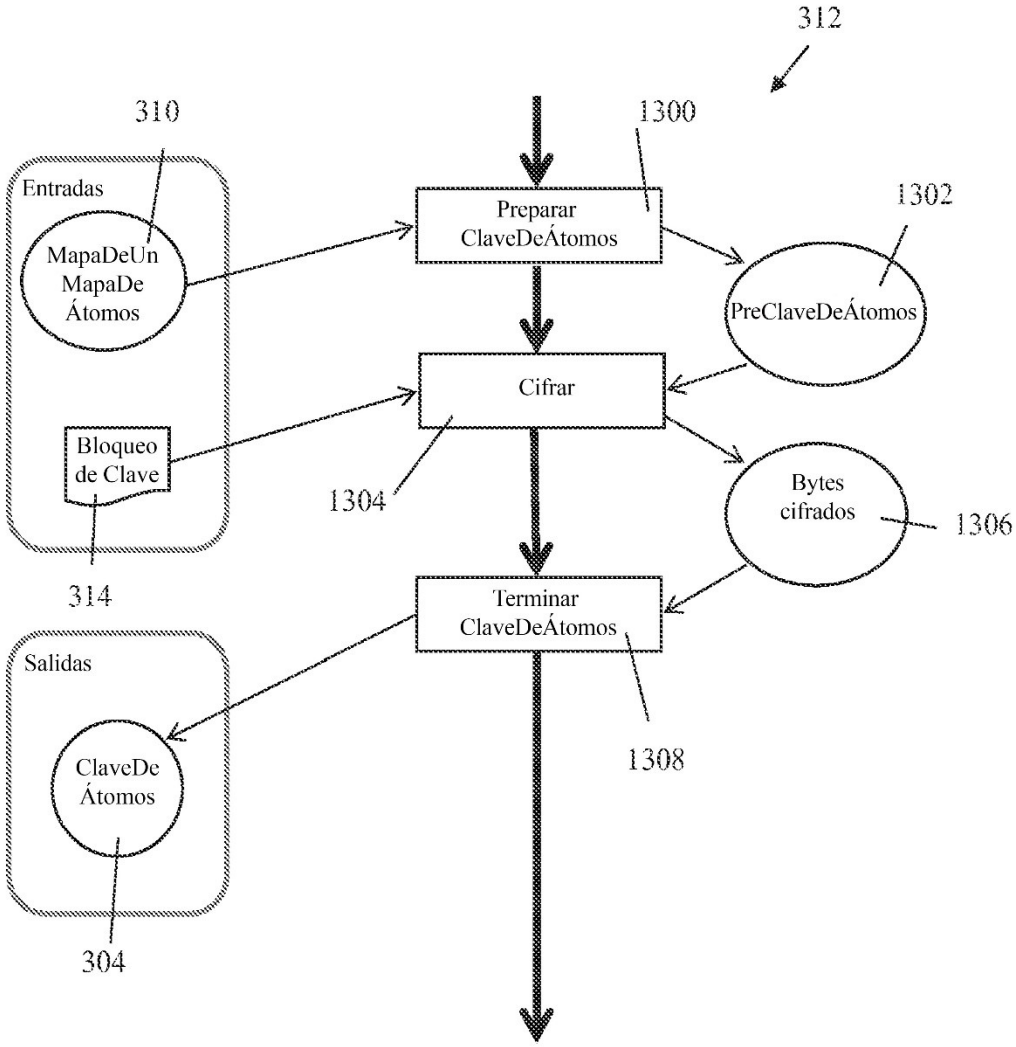
312
310
1300
Entradas
MapaDeUn MapaDe Átomos
Preparar ClaveDeÁtomos
1302
PreClaveDeÁtomos
Cifrar
Bloqueo de Clave
1304
Bytes cifrados
1306
314
Terminar ClaveDeÁtomos
Salidas
ClaveDe Átomos
1308
304

Fig. 13

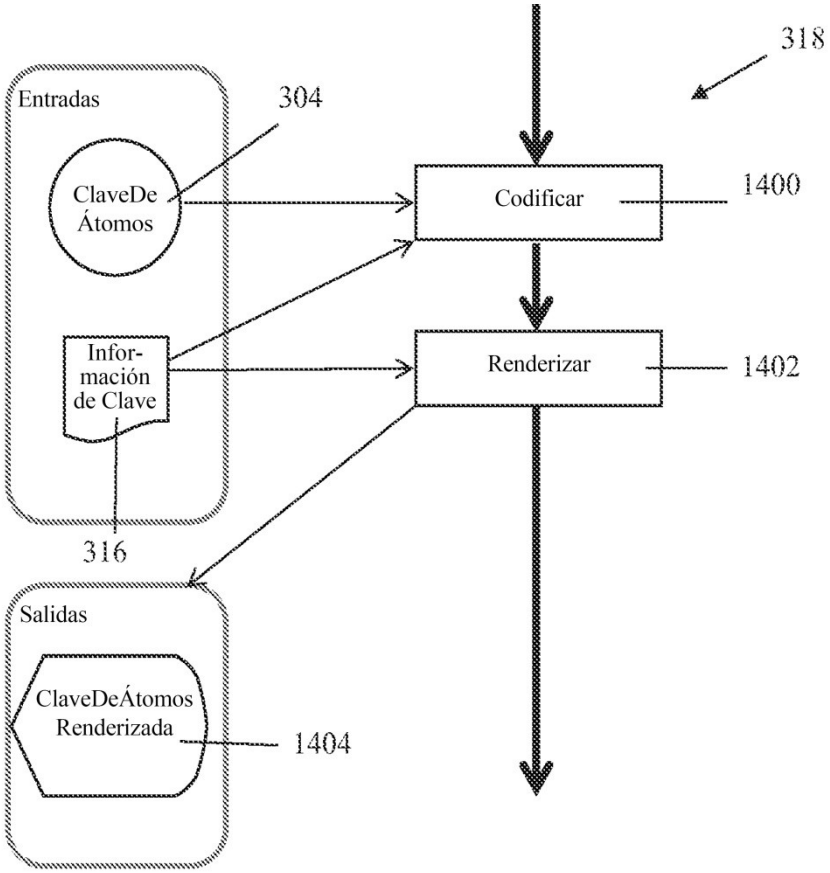
318
Entradas
304
ClaveDe
Átomos
Codificar
1400
Infor-
mación
de Clave
Renderizar
1402
316
Salidas
ClaveDeÁtomos
Renderizada
1404

Fig. 14

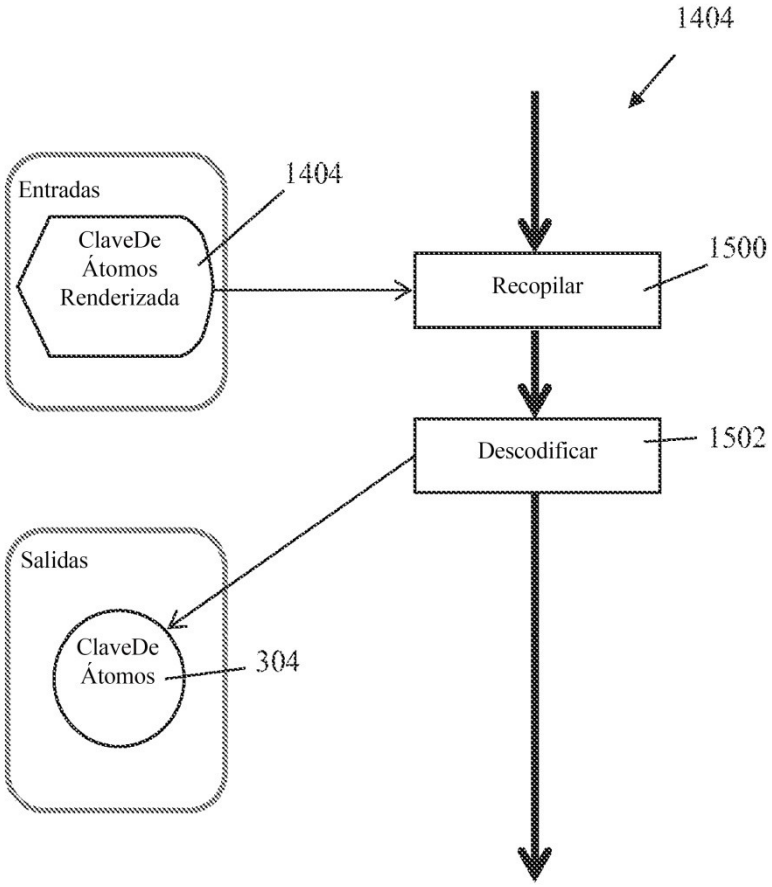
1404
Entradas
ClaveDe
Átomos
Renderizada
1404
Recopilar
1500
Descodificar
1502
Salidas
ClaveDe
Átomos
304

Fig. 15

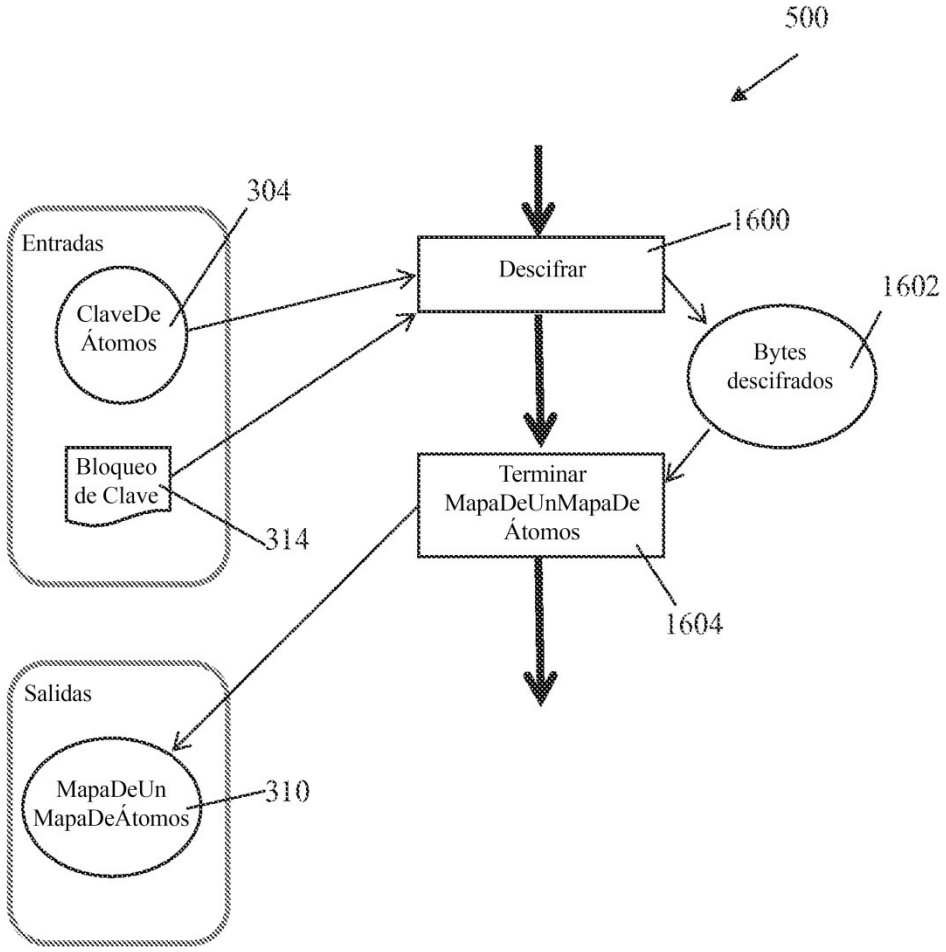
500
304
Entradas
ClaveDe
Átomos
Bloqueo
de Clave
314
Descifrar
1600
1602
Bytes
descifrados
Terminar
MapaDeUnMapaDe
Átomos
1604
Salidas
MapaDeUn
MapaDeÁtomos
310

Fig. 16

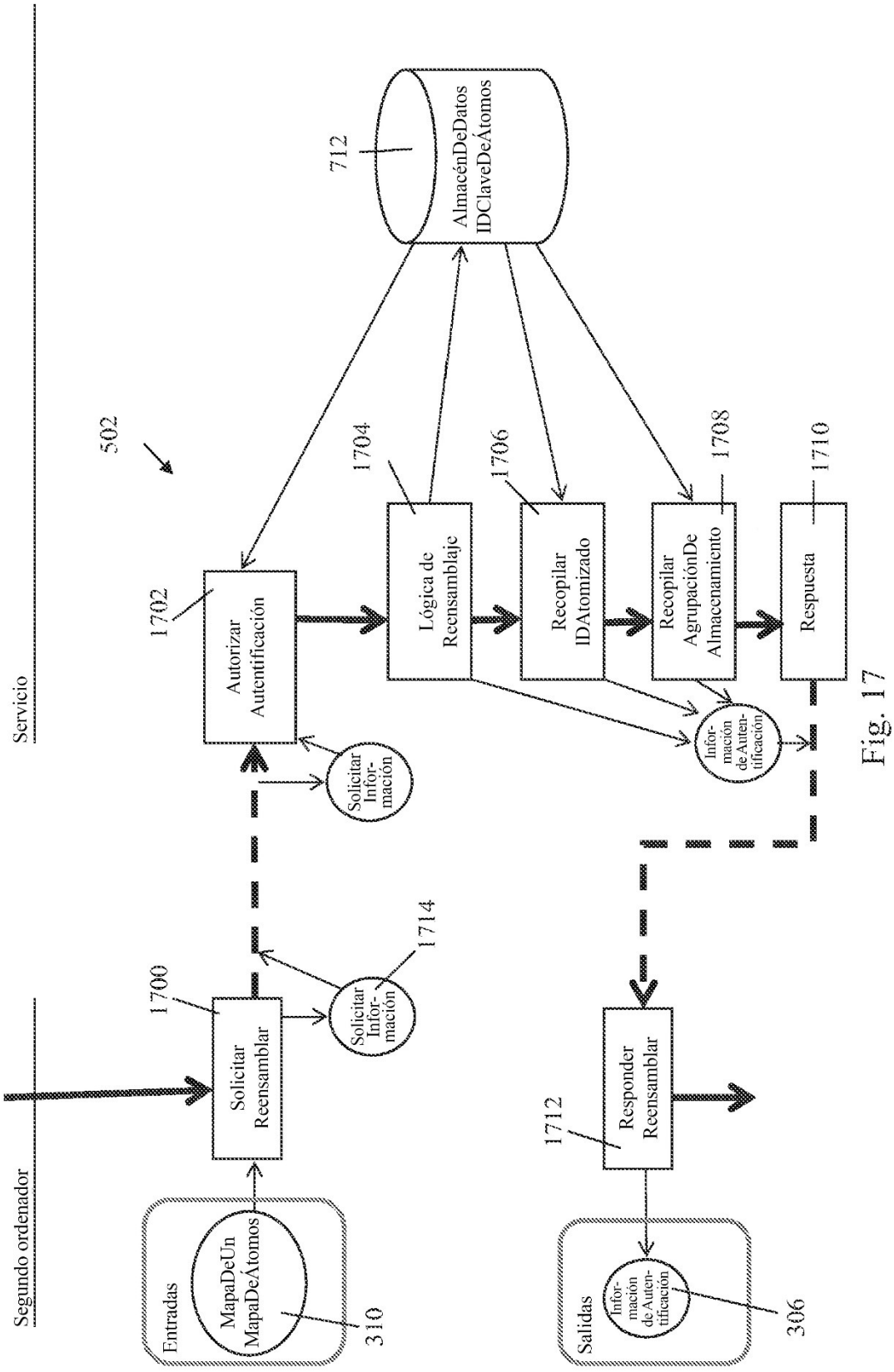
Servicio
Segundo ordenador
502
712
AlmacénDeDatos
IDClaveDeÁtomos
1702
Autorizar
Autentificación
1704
Lógica de
Reensamblaje
1706
Recopilar
IDAtomizado
1708
Recopilar
AgrupaciónDe
Almacenamiento
1710
Respuesta
Solicitar
Infor-
mación
Infor-
mación
de Auten-
tificación
1700
Solicitar
Reensamblar
1714
Solicitar
Infor-
mación
Entradas
MapaDeUn
MapaDeÁtomos
310
1712
Responder
Reensamblar
Salidas
Infor-
mación
de Auten-
tificación
306

Fig. 17

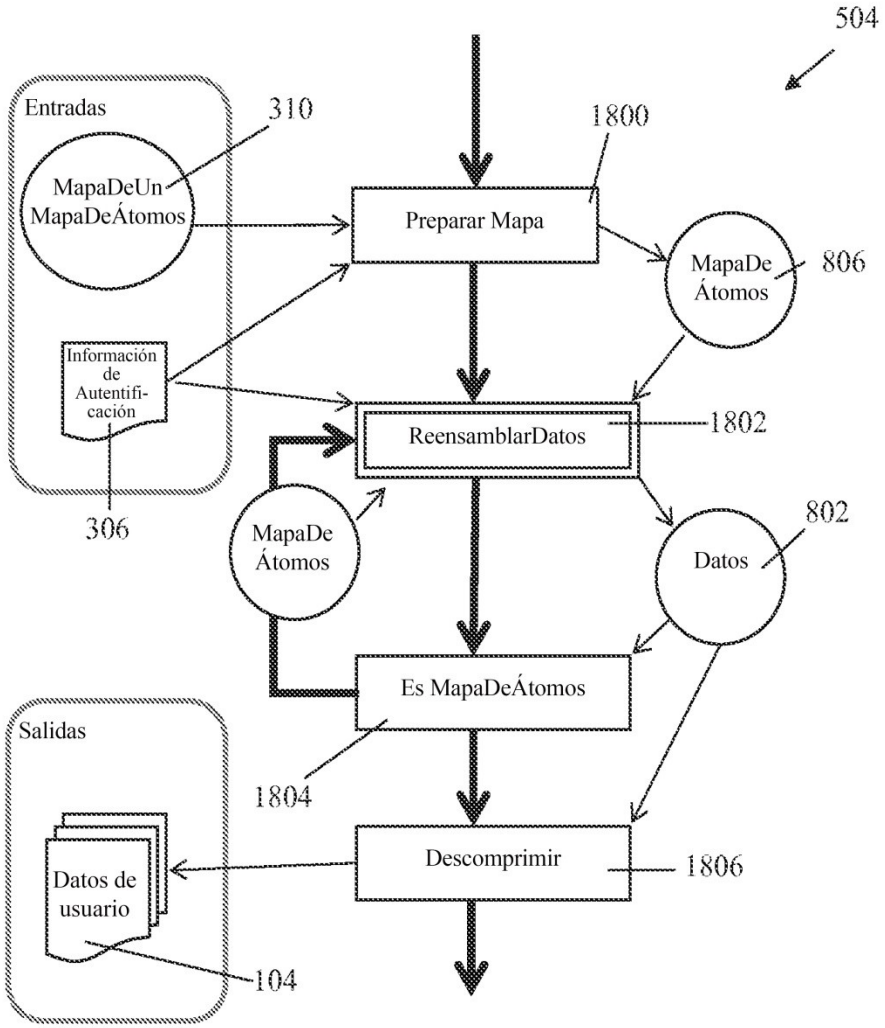
504
Entradas
310
MapaDeUn
MapaDeÁtomos
1800
Preparar Mapa
MapaDe
Átomos
806
Información
de
Autentifi-
cación
306
ReensamblarDatos
1802
MapaDe
Átomos
802
Datos
Es MapaDeÁtomos
1804
Salidas
Descomprimir
1806
Datos de
usuario
104

Fig. 18

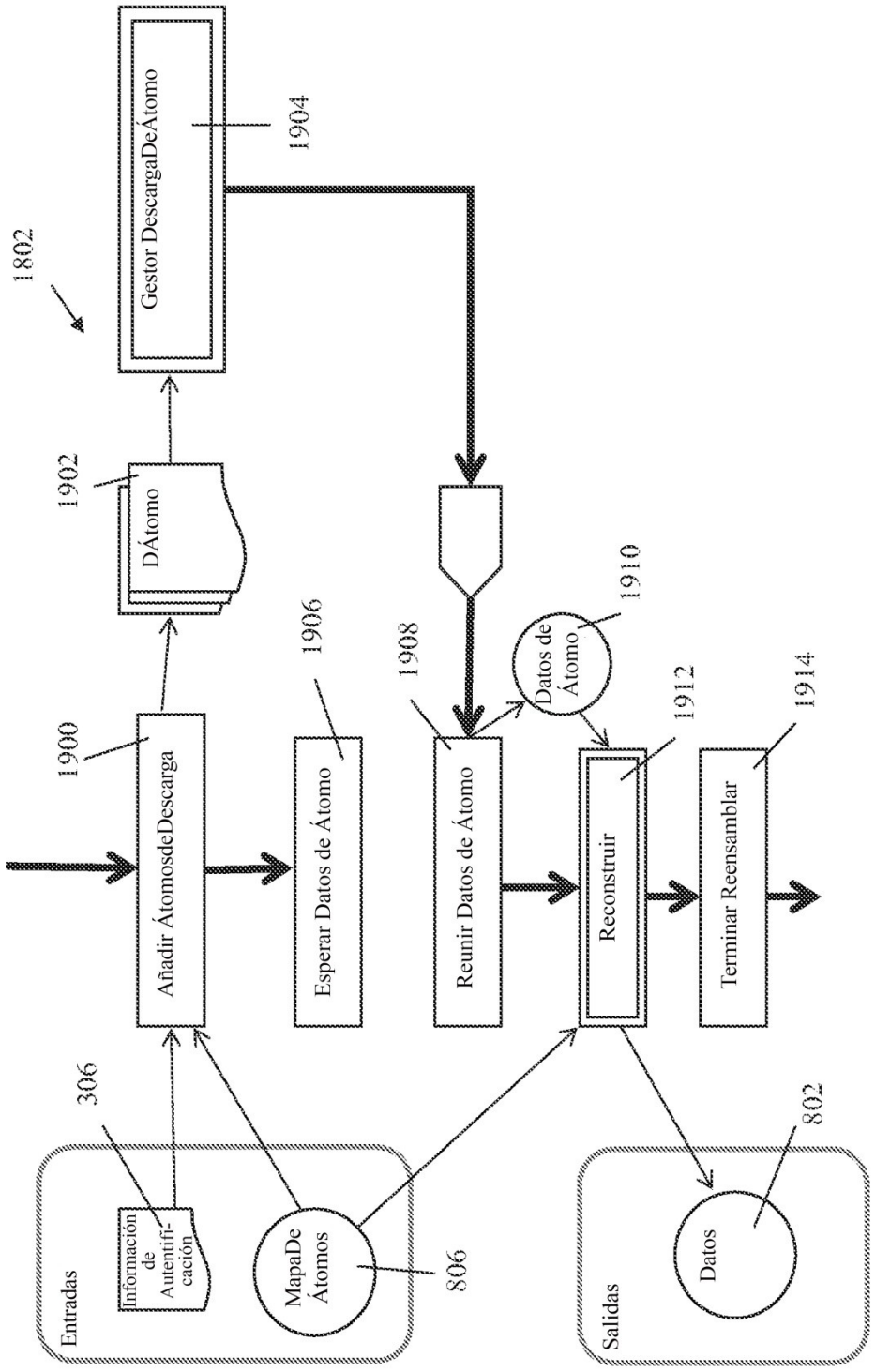
1802
Gestor DescargaDeÁtomo
1904
1902
DÁtomo
1900
Añadir ÁtomosdeDescarga
1906
Esperar Datos de Átomo
1908
Reunir Datos de Átomo
Datos de Átomo
1910
1912
Reconstruir
1914
Terminar Reensamblar
306
Información de Autentifi-cación
MapaDe Átomos
806
802
Datos
Entradas
Salidas

Fig. 19

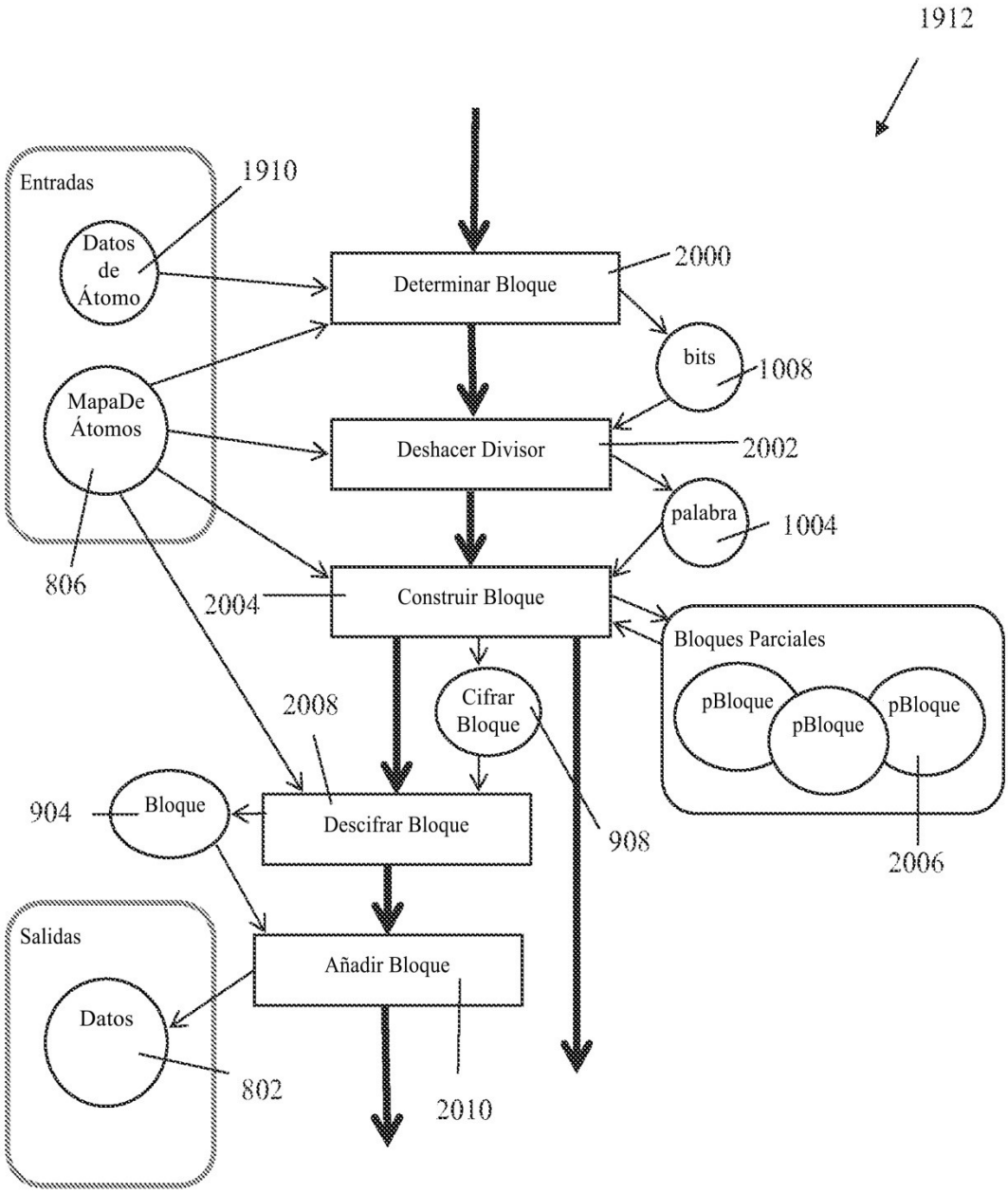
1912
Entradas
1910
Datos de Átomo
MapaDe Átomos
806
Determinar Bloque
2000
bits
1008
Deshacer Divisor
2002
palabra
1004
Construir Bloque
2004
Bloques Parciales
pBloque
pBloque
pBloque
2006
Cifrar Bloque
2008
904
Bloque
Descifrar Bloque
908
Salidas
Añadir Bloque
Datos
802
2010

Fig. 20

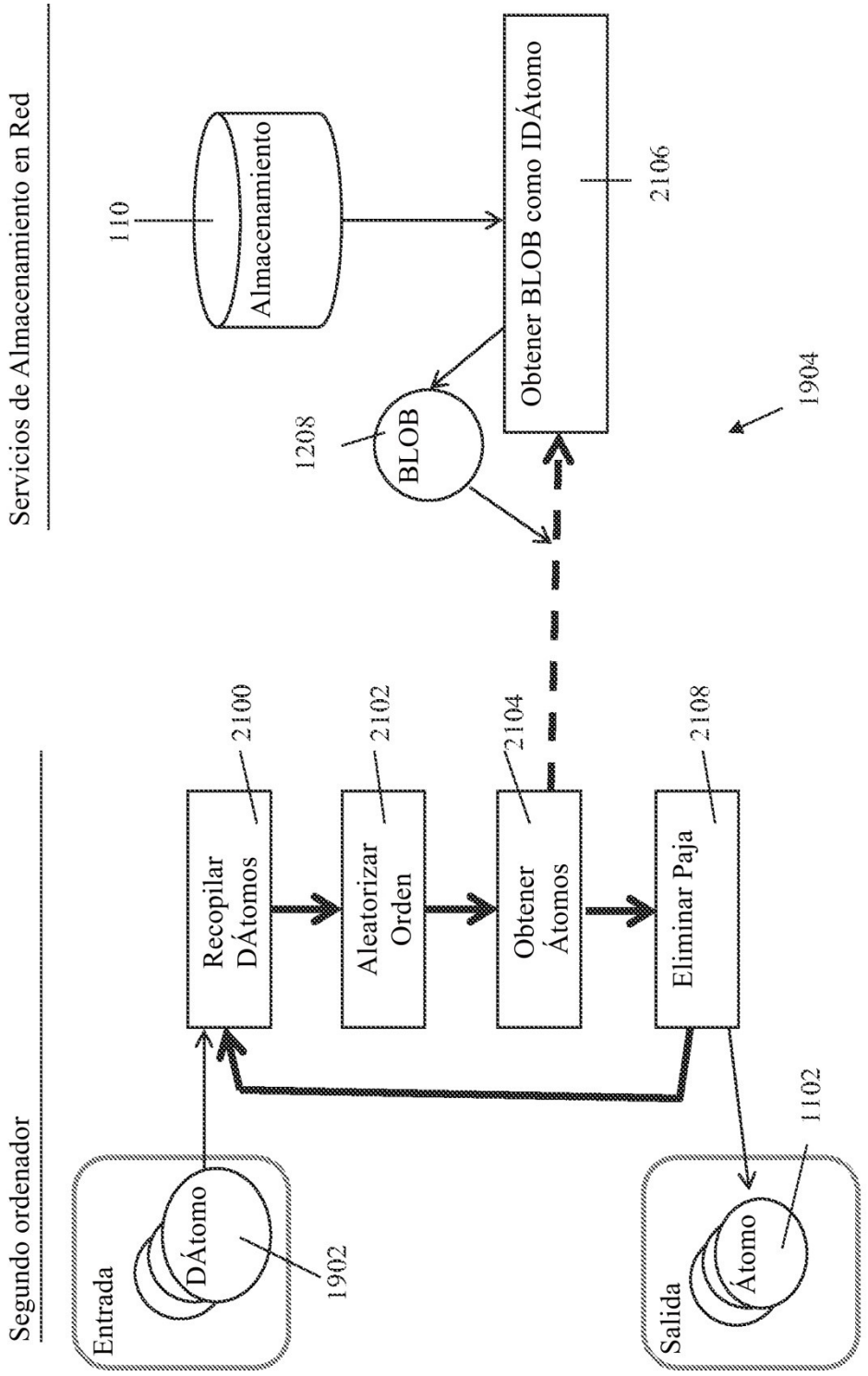
Servicios de Almacenamiento en Red
110
Almacenamiento
Obtener BLOB como IDÁtomo
2106
1208
BLOB
1904
Segundo ordenador
2100
Recopilar DÁtomos
2102
Aleatorizar Orden
2104
Obtener Átomos
2108
Eliminar Paja
Entrada
DÁtomo
1902
Salida
Átomo
1102

Fig. 21

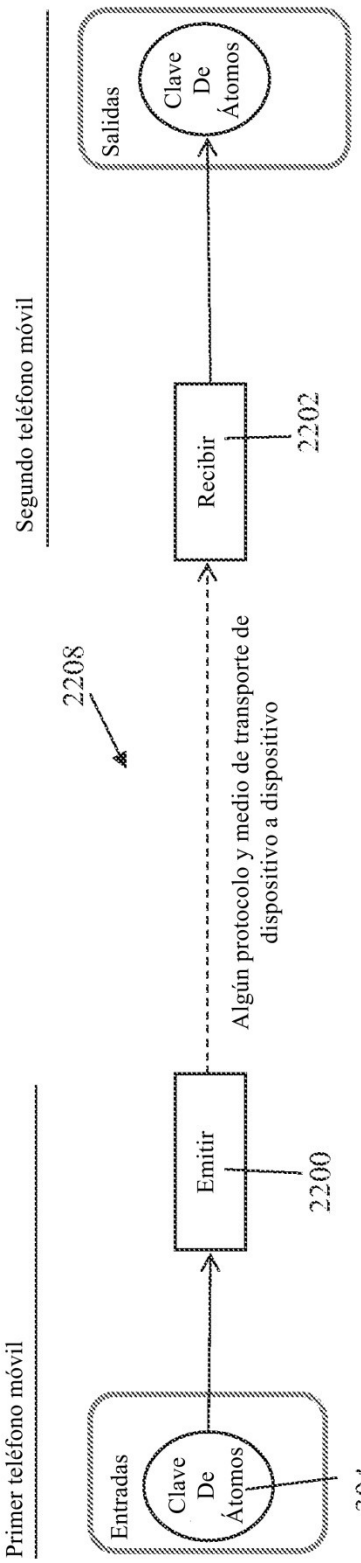


Fig. 22a

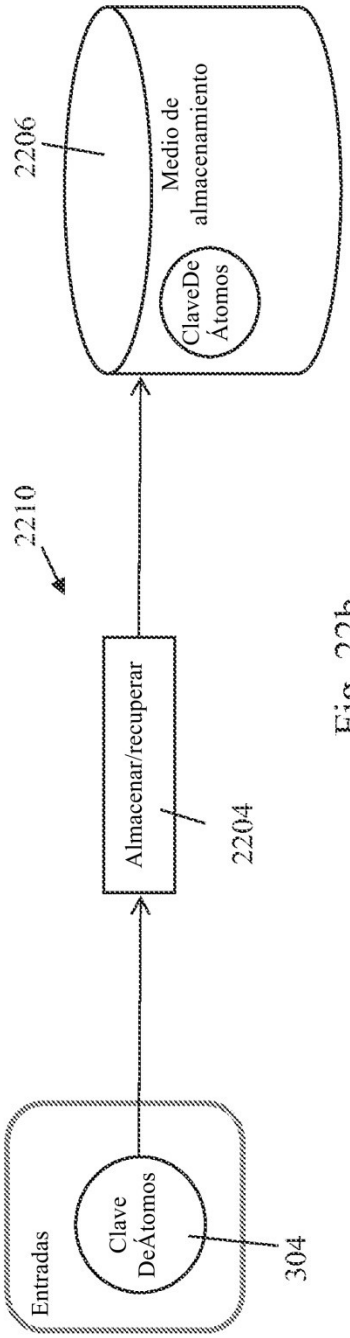


Fig. 22b

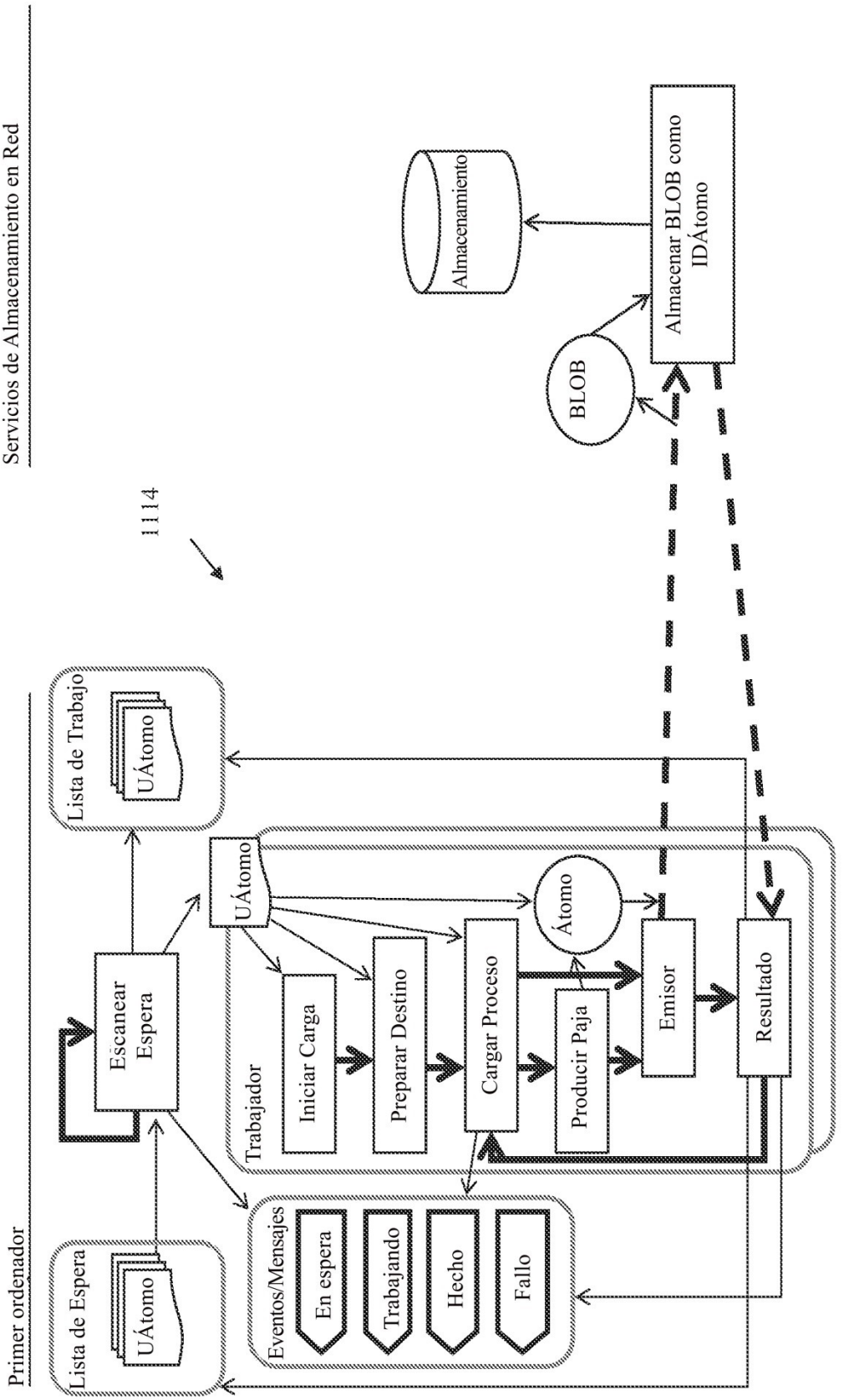
Servicios de Almacenamiento en Red
1114
Almacenamiento
Almacenar BLOB como IDÁtomo
BLOB
Primer ordenador
Lista de Trabajo
UÁtomo
Escanear Espera
UÁtomo
Átomo
Trabajador
Iniciar Carga
Preparar Destino
Cargar Proceso
Producir Paja
Emisor
Resultado
Lista de Espera
UÁtomo
Eventos/Mensajes
En espera
Trabajando
Hecho
Fallo

Fig. 23

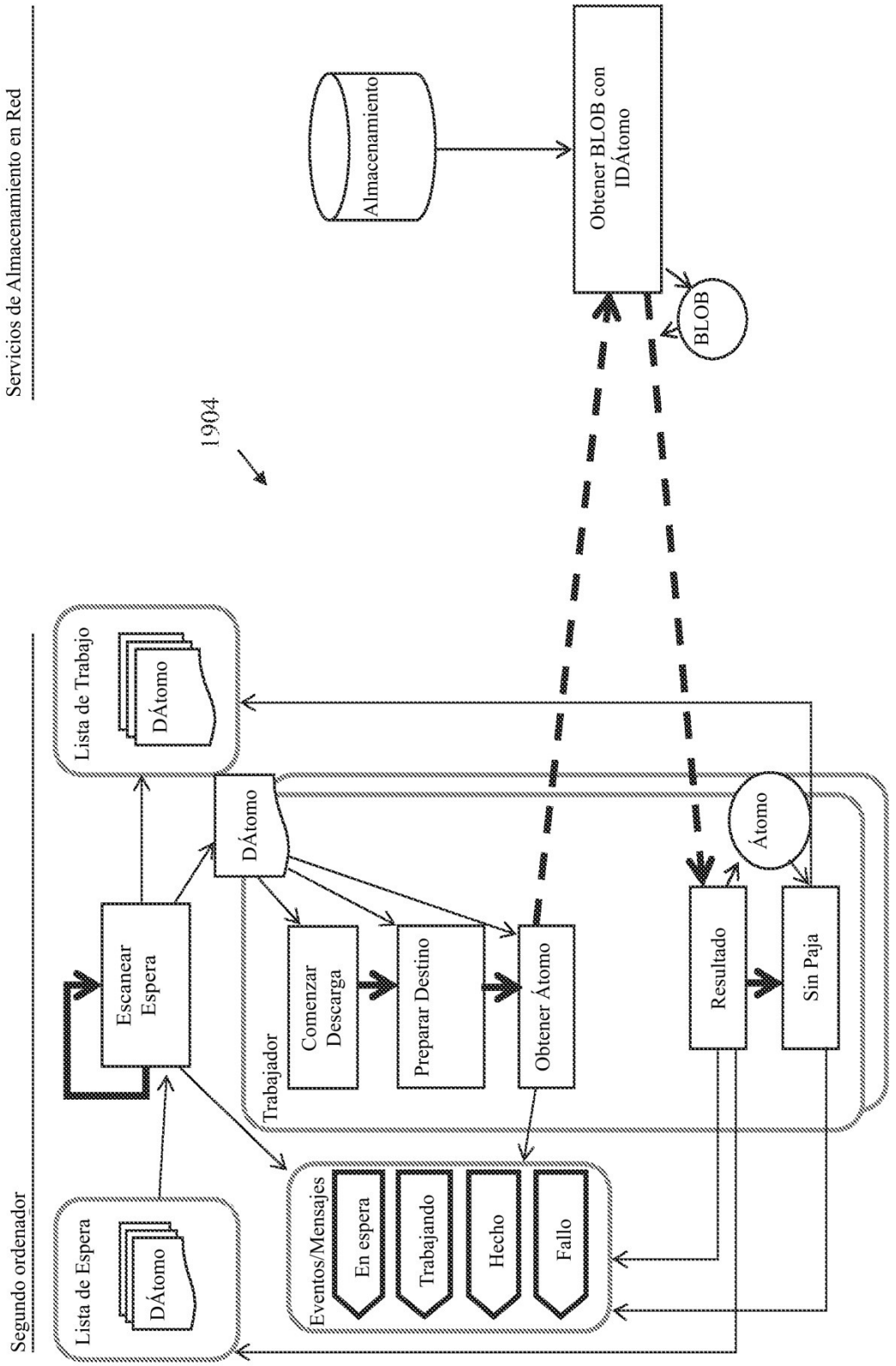
Servicios de Almacenamiento en Red
Almacenamiento
Obtener BLOB con IDÁtomo
BLOB
1904
Segundo ordenador
Lista de Trabajo
DÁtomo
DÁtomo
Escanear Espera
Trabajador
Comenzar Descarga
Preparar Destino
Obtener Átomo
Átomo
Resultado
Sin Paja
Lista de Espera
DÁtomo
Eventos/Mensajes
En espera
Trabajando
Hecho
Fallo

Fig. 24

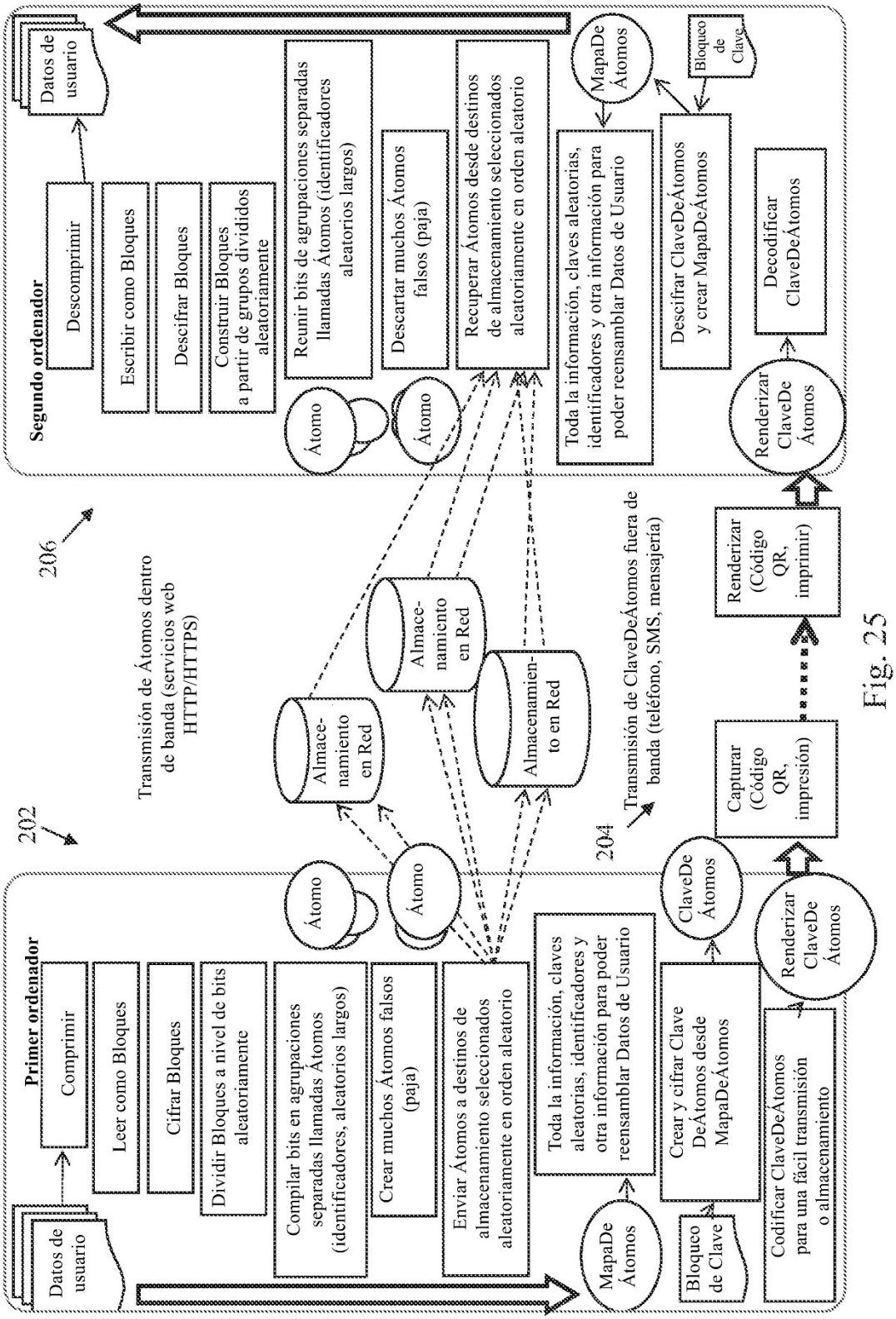
Primer ordenador
Datos de usuario
Comprimir
Leer como Bloques
Cifrar Bloques
Dividir Bloques a nivel de bits aleatoriamente
Compilar bits en agrupaciones separadas llamadas Átomos (identificadores, aleatorios largos)
Crear muchos Átomos falsos (paja)
Enviar Átomos a destinos de almacenamiento seleccionados aleatoriamente en orden aleatorio
Toda la información, claves aleatorias, identificadores y otra información para poder reensamblar Datos de Usuario
Crear y cifrar Clave DeÁtomos desde MapaDeÁtomos
Codificar ClaveDeÁtomos para una fácil transmisión o almacenamiento
MapaDe Átomos
Bloqueo de Clave
ClaveDe Átomos
Renderizar ClaveDe Átomos
Capturar (Código QR, impresión)
Renderizar (Código QR, imprimir)
202
204
206
Transmisión de Átomos dentro de banda (servicios web HTTP/HTTPS)
Transmisión de ClaveDeÁtomos fuera de banda (teléfono, SMS, mensajería)
Átomo
Átomo
Almace-namiento en Red
Almace-namiento en Red
Almacenamien-to en Red
Segundo ordenador
Descomprimir
Escribir como Bloques
Descifrar Bloques
Construir Bloques a partir de grupos divididos aleatoriamente
Reunir bits de agrupaciones separadas llamadas Átomos (identificadores aleatorios largos)
Descartar muchos Átomos falsos (paja)
Recuperar Átomos desde destinos de almacenamiento seleccionados aleatoriamente en orden aleatorio
Átomo
Átomo
Toda la información, claves aleatorias, identificadores y otra información para poder reensamblar Datos de Usuario
Descifrar ClaveDeÁtomos y crear MapaDeÁtomos
MapaDe Átomos
Bloqueo de Clave
Renderizar ClaveDe Átomos
Decodificar ClaveDeÁtomos
Datos de usuario

Fig. 25

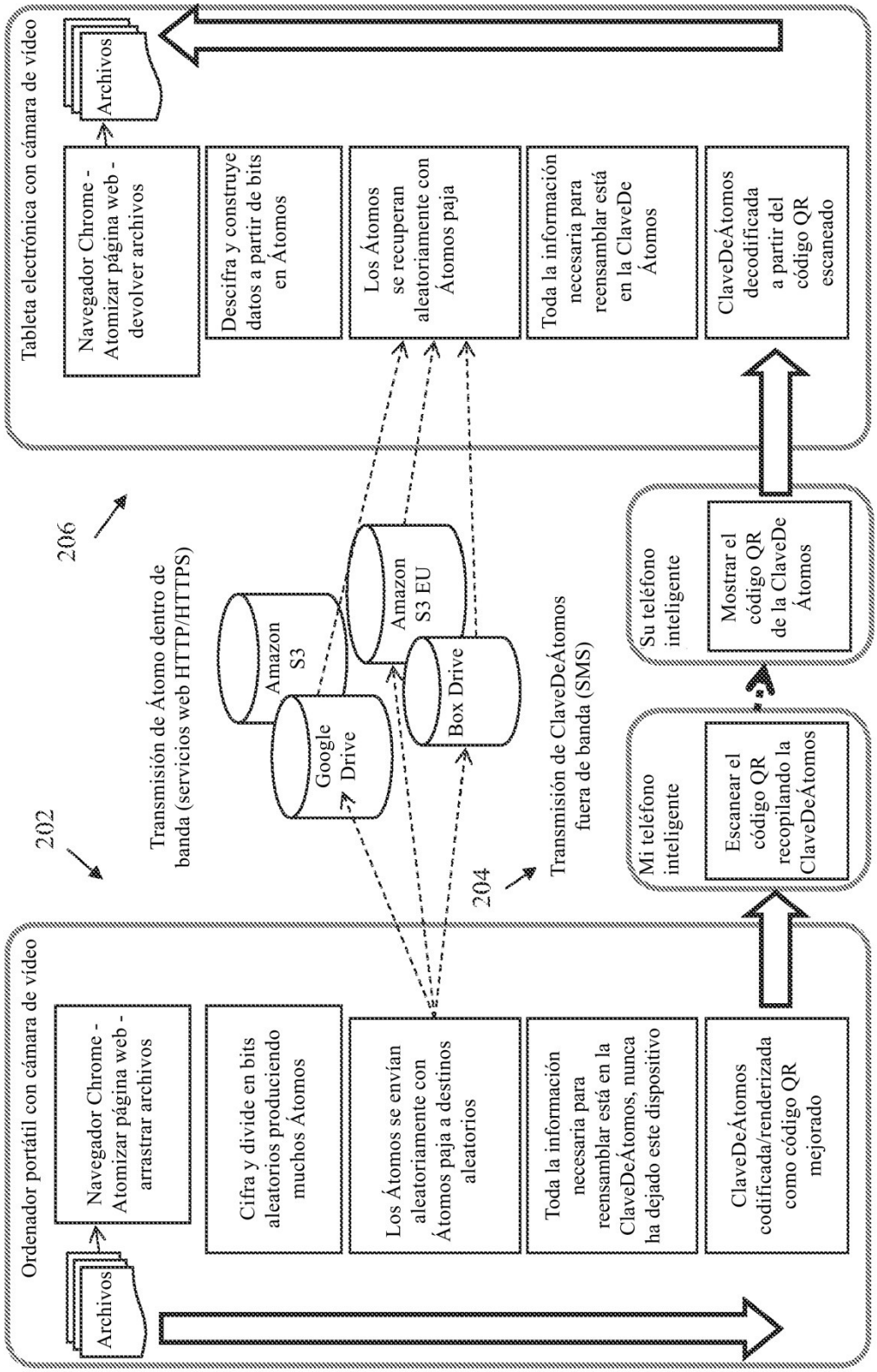
Ordenador portátil con cámara de vídeo
Archivos
Navegador Chrome - Atomizar página web - arrastrar archivos
Cifra y divide en bits aleatorios produciendo muchos Átomos
Los Átomos se envían aleatoriamente con Átomos paja a destinos aleatorios
Toda la información necesaria para reensamblar está en la ClaveDeÁtomos, nunca ha dejado este dispositivo
ClaveDeÁtomos codificada/renderizada como código QR mejorado
202
Transmisión de Átomo dentro de banda (servicios web HTTP/HTTPS)
206
Amazon S3
Amazon S3 EU
Google Drive
Box Drive
204
Transmisión de ClaveDeÁtomos fuera de banda (SMS)
Mi teléfono inteligente
Escanear el código QR recopilando la ClaveDeÁtomos
Su teléfono inteligente
Mostrar el código QR de la ClaveDe Átomos
Tableta electrónica con cámara de vídeo
Archivos
Navegador Chrome - Atomizar página web - devolver archivos
Descifra y construye datos a partir de bits en Átomos
Los Átomos se recuperan aleatoriamente con Átomos paja
Toda la información necesaria para reensamblar está en la ClaveDe Átomos
ClaveDeÁtomos decodificada a partir del código QR escaneado

Fig. 26

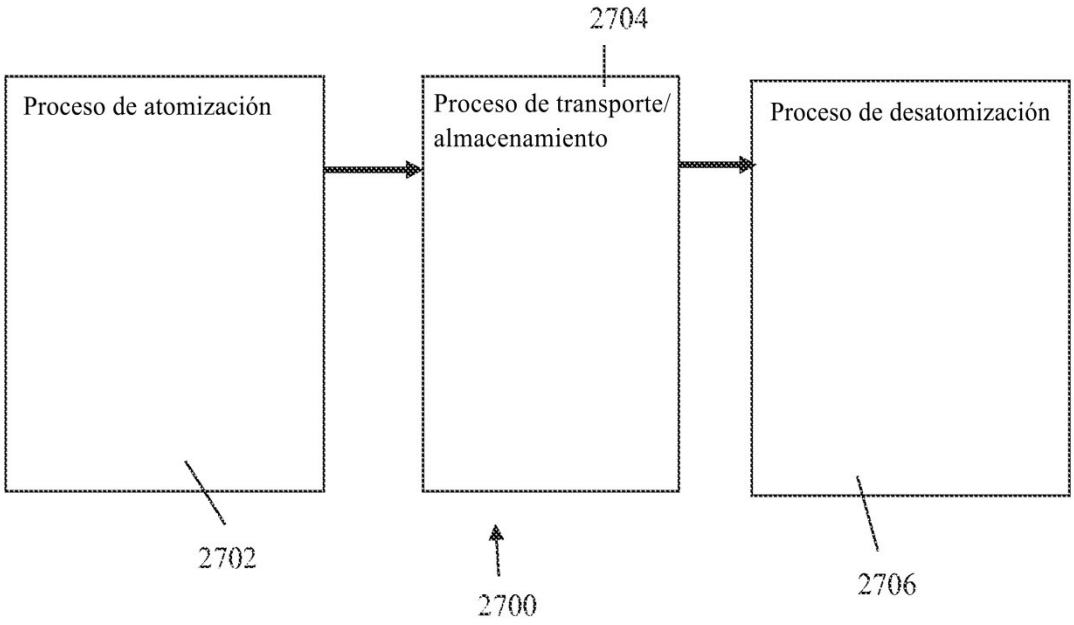
2704
Proceso de atomización
Proceso de transporte/ almacenamiento
Proceso de desatomización
2702
2700
2706

Fig. 27

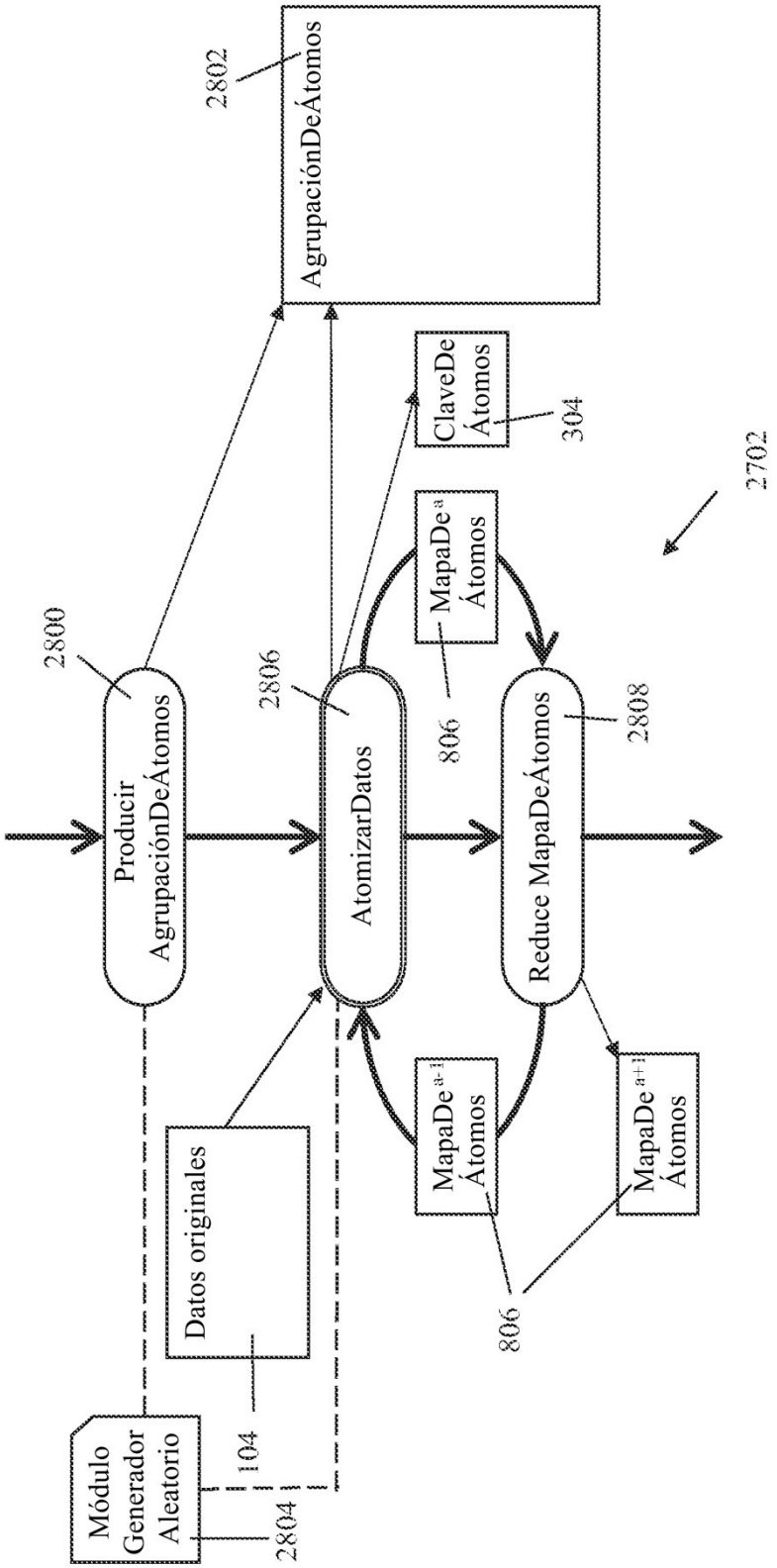
2802
AgrupaciónDeÁtomos
ClaveDe Átomos
304
2702
MapaDe$^{a}$ Átomos
2800
2806
806
2808
Producir AgrupaciónDeÁtomos
AtomizarDatos
Reduce MapaDeÁtomos
MapaDe$^{a-1}$ Átomos
MapaDe$^{a+1}$ Átomos
806
Datos originales
104
Módulo Generador Aleatorio
2804

Fig. 28

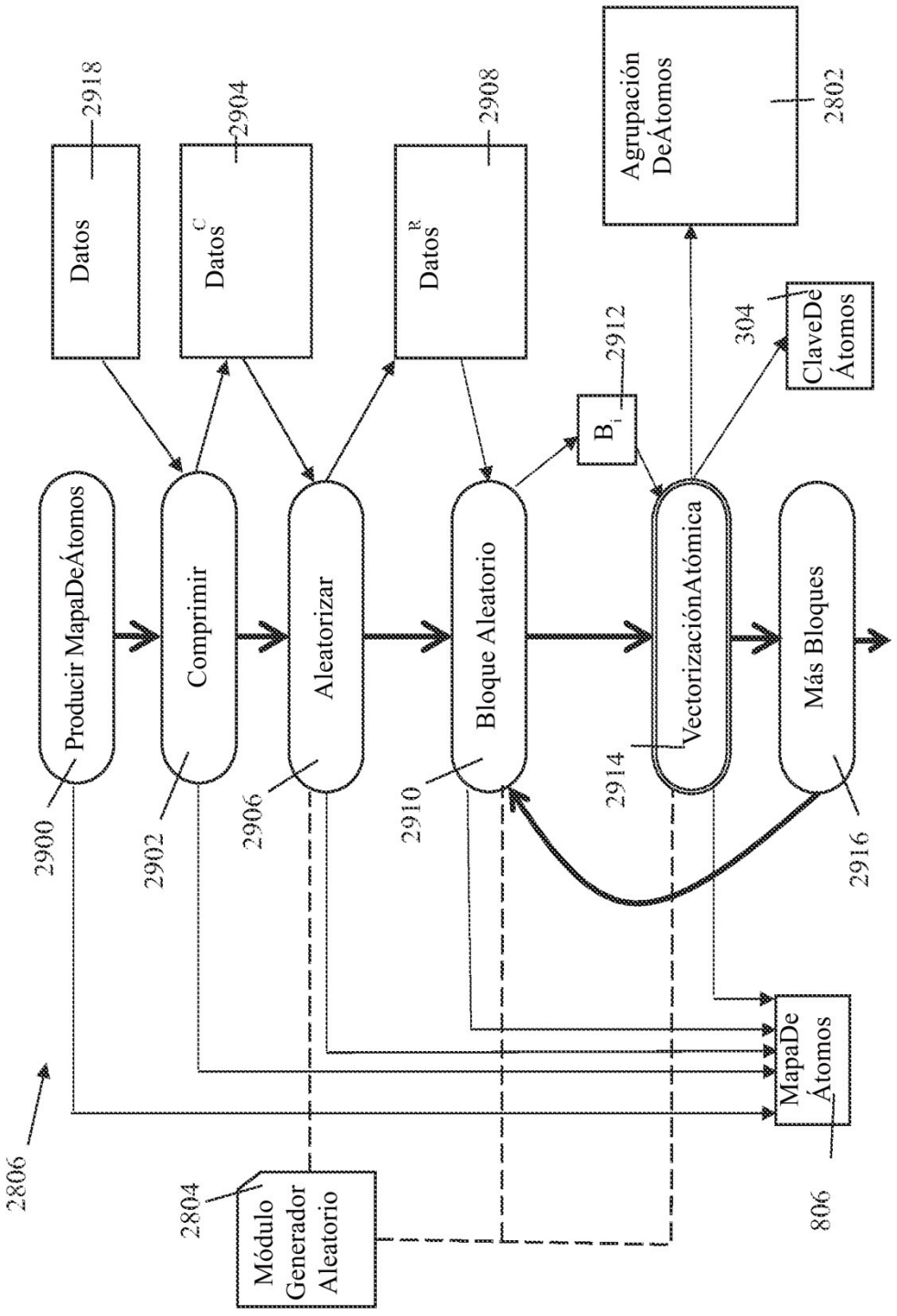
Producir MapaDeÁtomos
Comprimir
Aleatorizar
Bloque Aleatorio
VectorizaciónAtómica
Más Bloques
Datos
Datos C
Datos R
Agrupación DeÁtomos
ClaveDe Átomos
B i
MapaDe Átomos
Módulo Generador Aleatorio
2900
2902
2906
2910
2914
2916
2918
2904
2908
2912
304
2802
2806
2804
806

Fig. 29

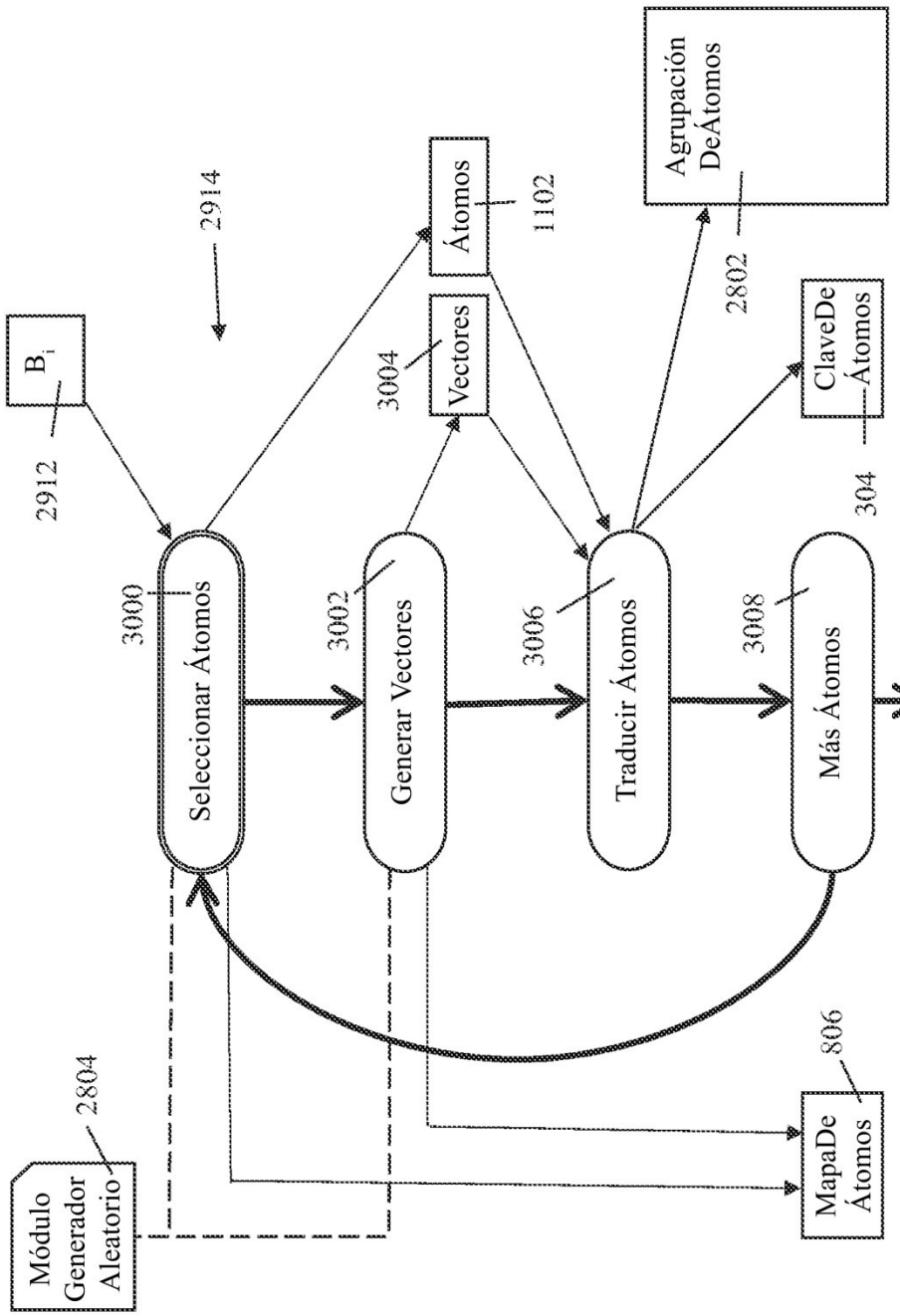
Módulo Generador Aleatorio
2804
$B_i$
2912
2914
Seleccionar Átomos
3000
Generar Vectores
3002
Traducir Átomos
3006
Más Átomos
3008
304
Vectores
3004
Átomos
1102
Agrupación DeÁtomos
2802
ClaveDe Átomos
MapaDe Átomos
806

Fig. 30

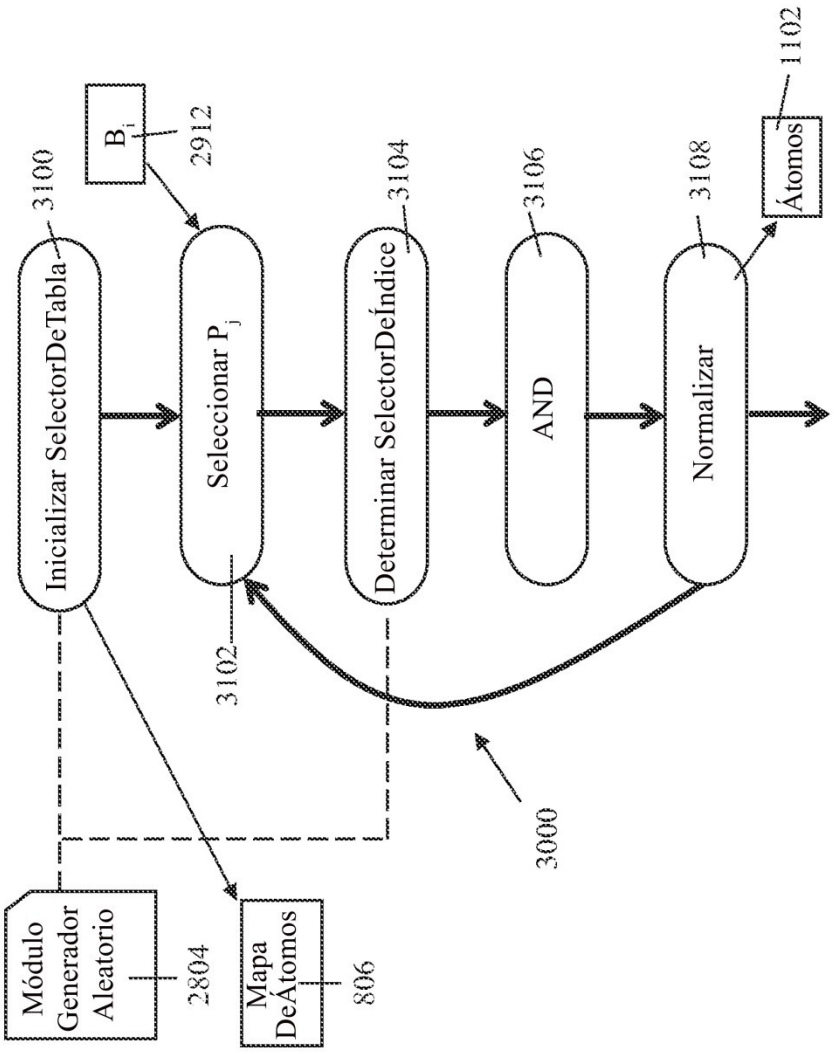
Inicializar SelectorDeTabla
3100
$B_i$
2912
Seleccionar $P_j$
3102
Determinar SelectorDeÍndice
3104
AND
3106
Normalizar
3108
Átomos
1102
Módulo Generador Aleatorio
2804
Mapa DeÁtomos
806
3000

Fig. 31

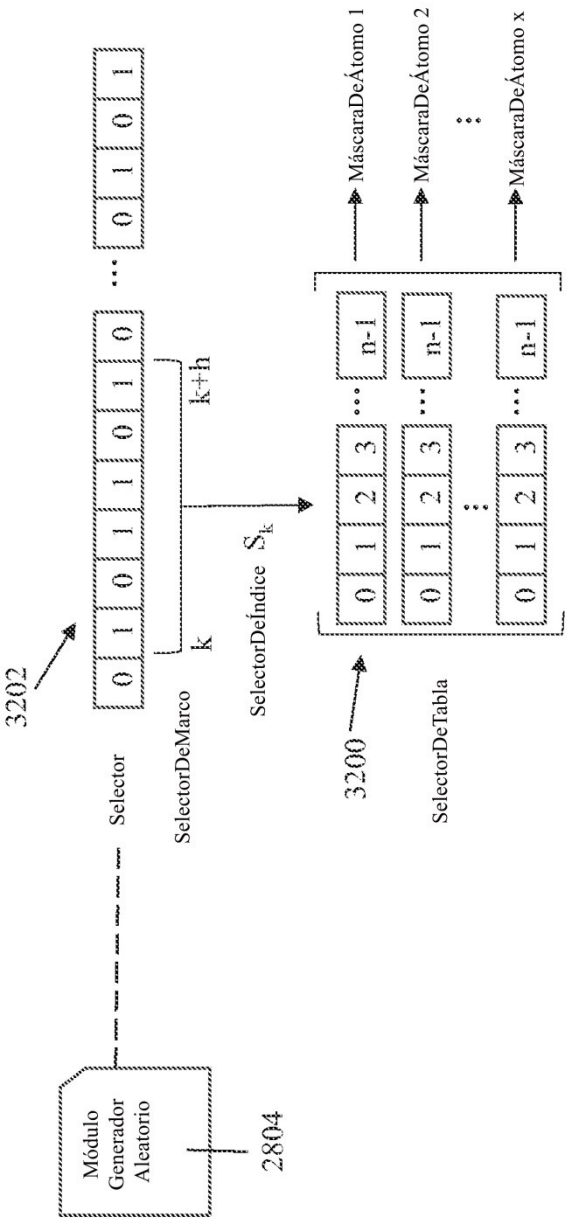
3202
Selector
SelectorDeMarco
k
k+h
SelectorDeÍndice $S_k$
3200
SelectorDeTabla
MáscaraDeÁtomo 1
MáscaraDeÁtomo 2
MáscaraDeÁtomo x
Módulo Generador Aleatorio
2804

Fig. 32

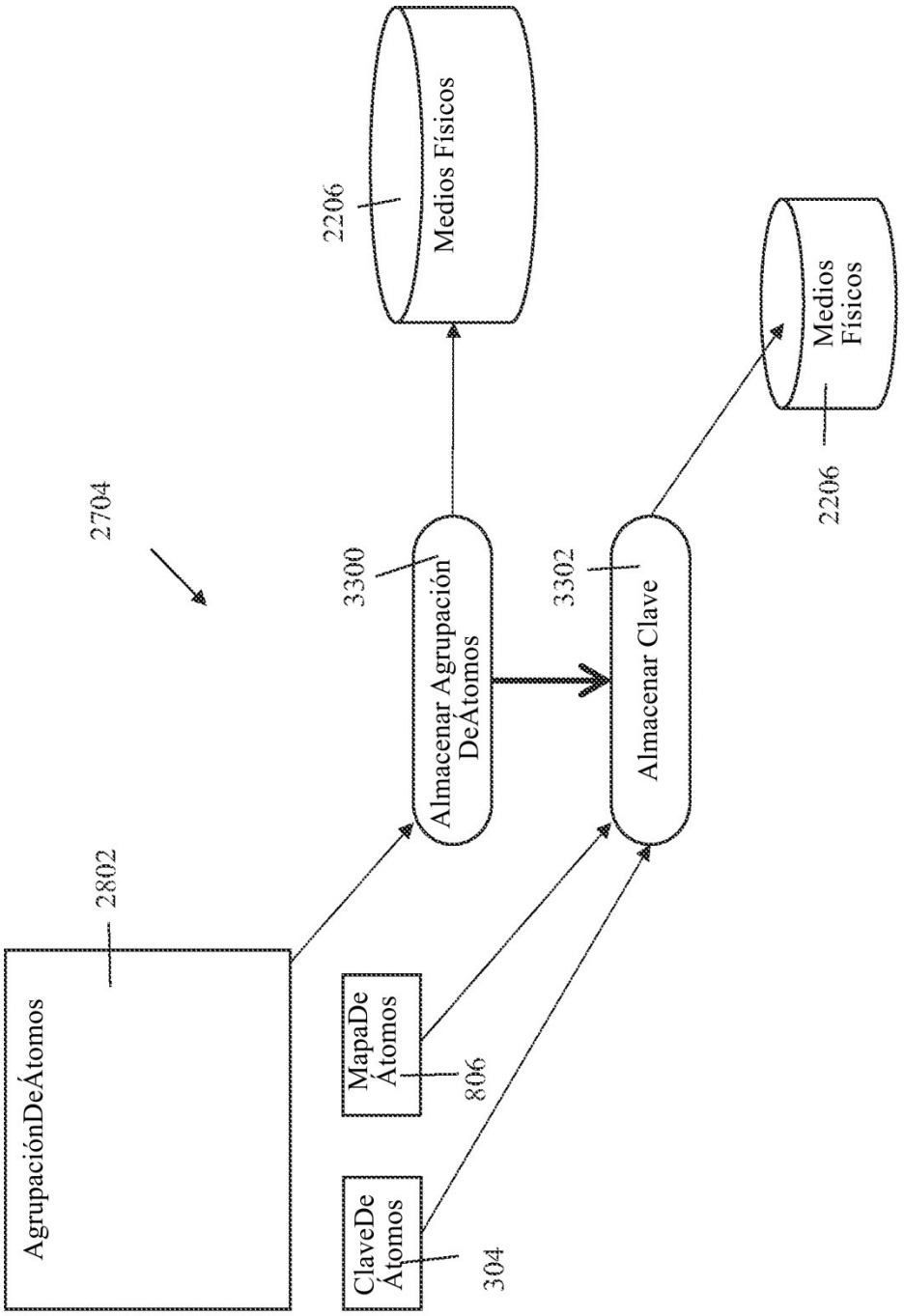
AgrupaciónDeÁtomos
2802
ClaveDe Átomos
304
MapaDe Átomos
806
2704
Almacenar Agrupación DeÁtomos
3300
Almacenar Clave
3302
Medios Físicos
2206
Medios Físicos
2206

Fig. 33

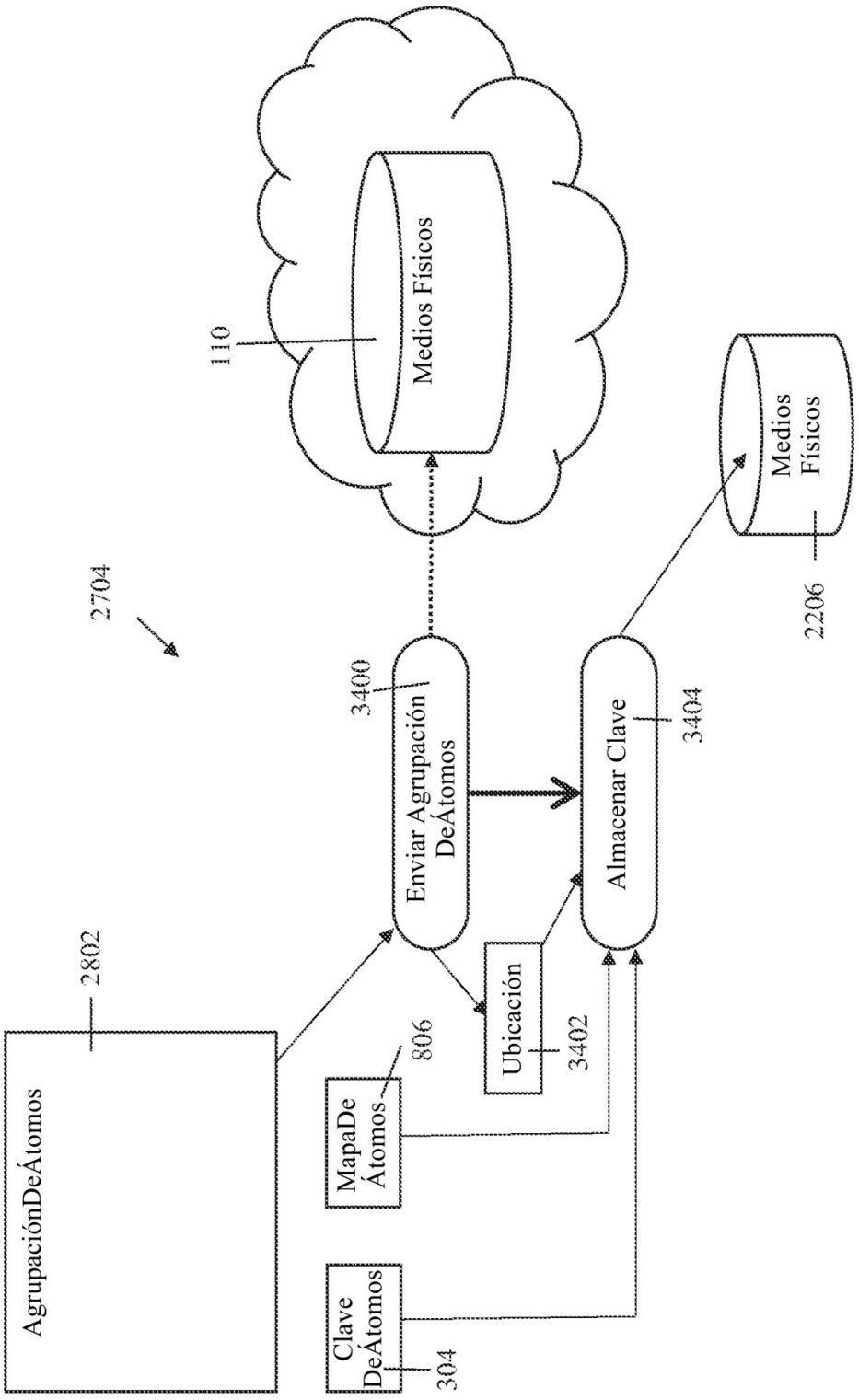
AgrupaciónDeÁtomos
2802
Clave DeÁtomos
304
MapaDe Átomos
806
Ubicación
3402
Enviar Agrupación DeÁtomos
3400
Almacenar Clave
3404
Medios Físicos
2206
Medios Físicos
110
2704

Fig. 34

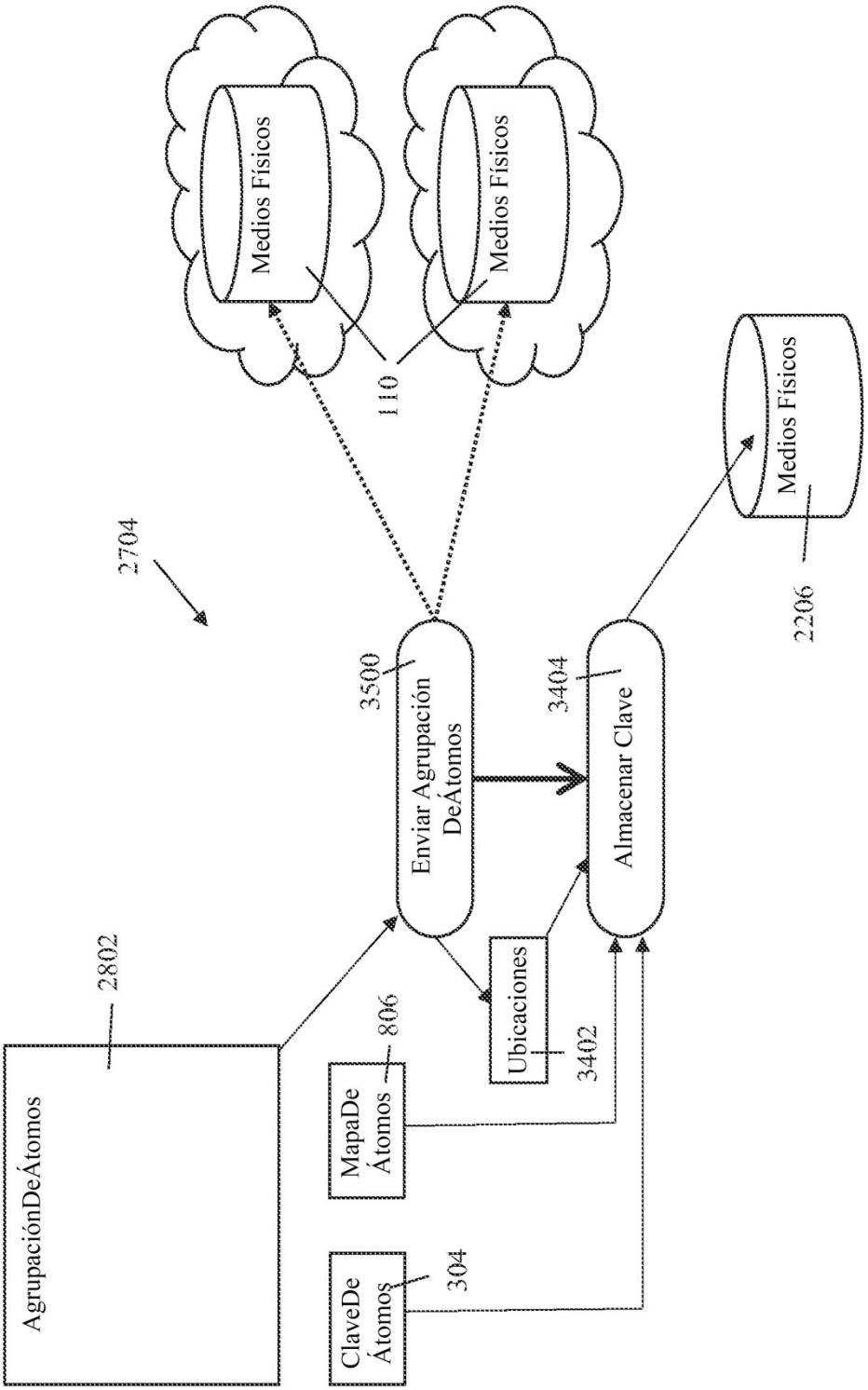
Medios Físicos
Medios Físicos
110
2704
Medios Físicos
2206
3500
Enviar Agrupación DeÁtomos
3404
Almacenar Clave
2802
AgrupaciónDeÁtomos
806
MapaDe Átomos
Ubicaciones
3402
ClaveDe Átomos
304

Fig. 35

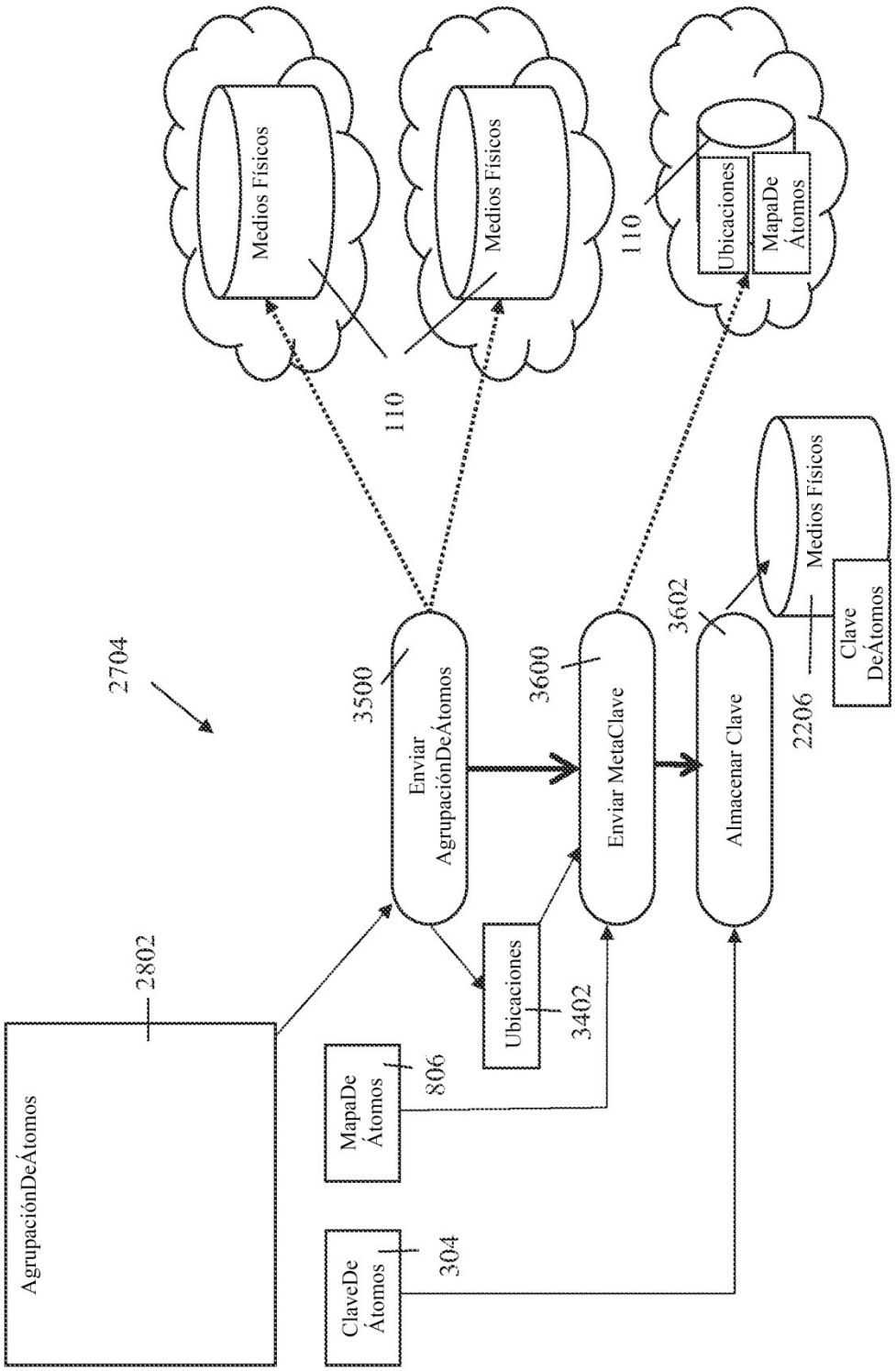
AgrupaciónDeÁtomos
2802
ClaveDe Átomos
304
MapaDe Átomos
806
Ubicaciones
3402
2704
3500
Enviar AgrupaciónDeÁtomos
3600
Enviar MetaClave
3602
Almacenar Clave
2206
Clave DeÁtomos
Medios Físicos
110
Medios Físicos
110
Medios Físicos
Ubicaciones
MapaDe Átomos
110

Fig. 36

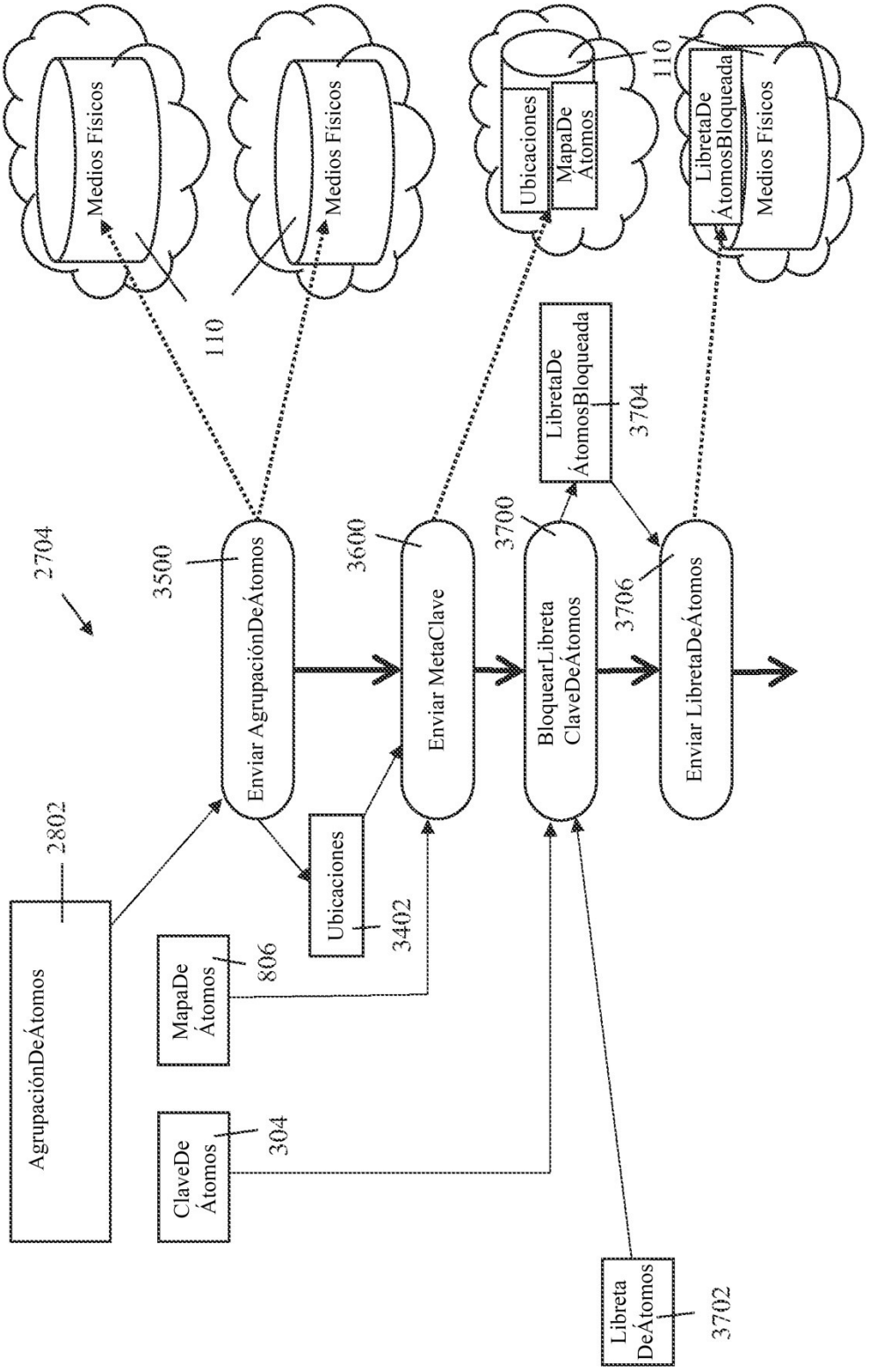
AgrupaciónDeÁtomos
2802
ClaveDe Átomos
304
MapaDe Átomos
806
Ubicaciones
3402
Libreta DeÁtomos
3702
2704
3500
Enviar AgrupaciónDeÁtomos
3600
Enviar MetaClave
3700
BloquearLibreta ClaveDeÁtomos
3706
Enviar LibretaDeÁtomos
LibretaDe ÁtomosBloqueada
3704
Medios Físicos
110
Medios Físicos
110
Ubicaciones
MapaDe Átomos
110
LibretaDe ÁtomosBloqueada
Medios Físicos

Fig. 37

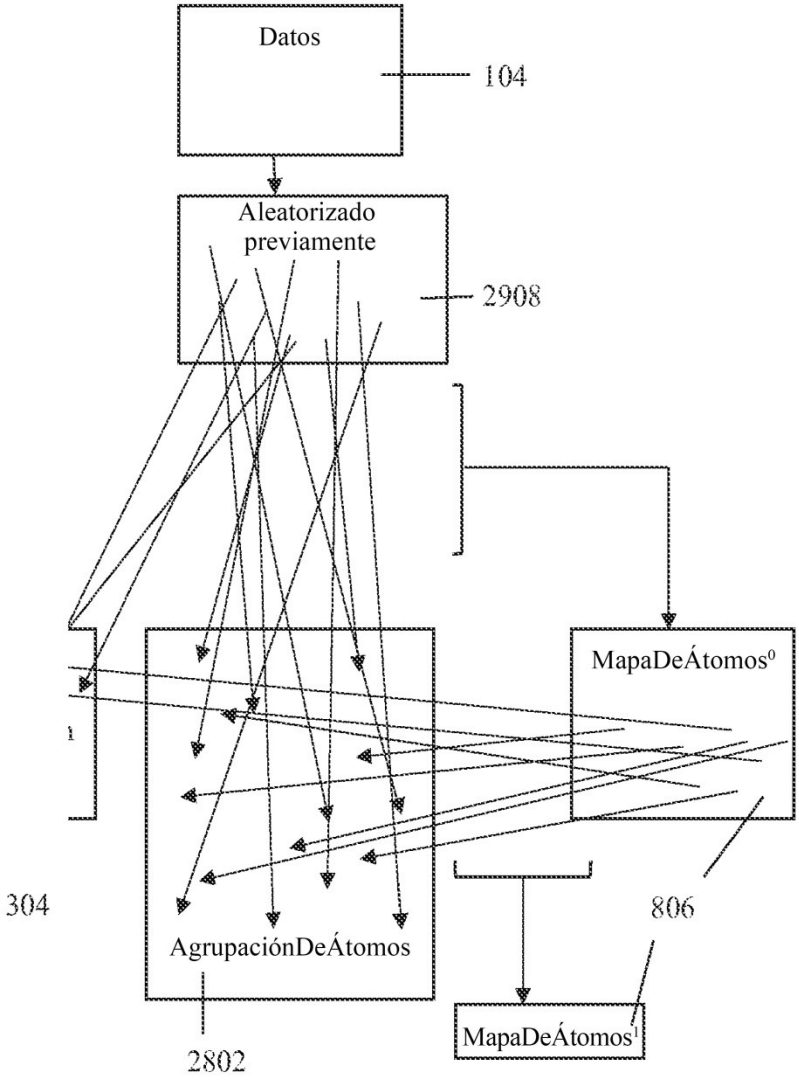
Datos
104
Aleatorizado previamente
2908
MapaDeÁtomos0
304
806
AgrupaciónDeÁtomos
2802
MapaDeÁtomos1

Fig. 38

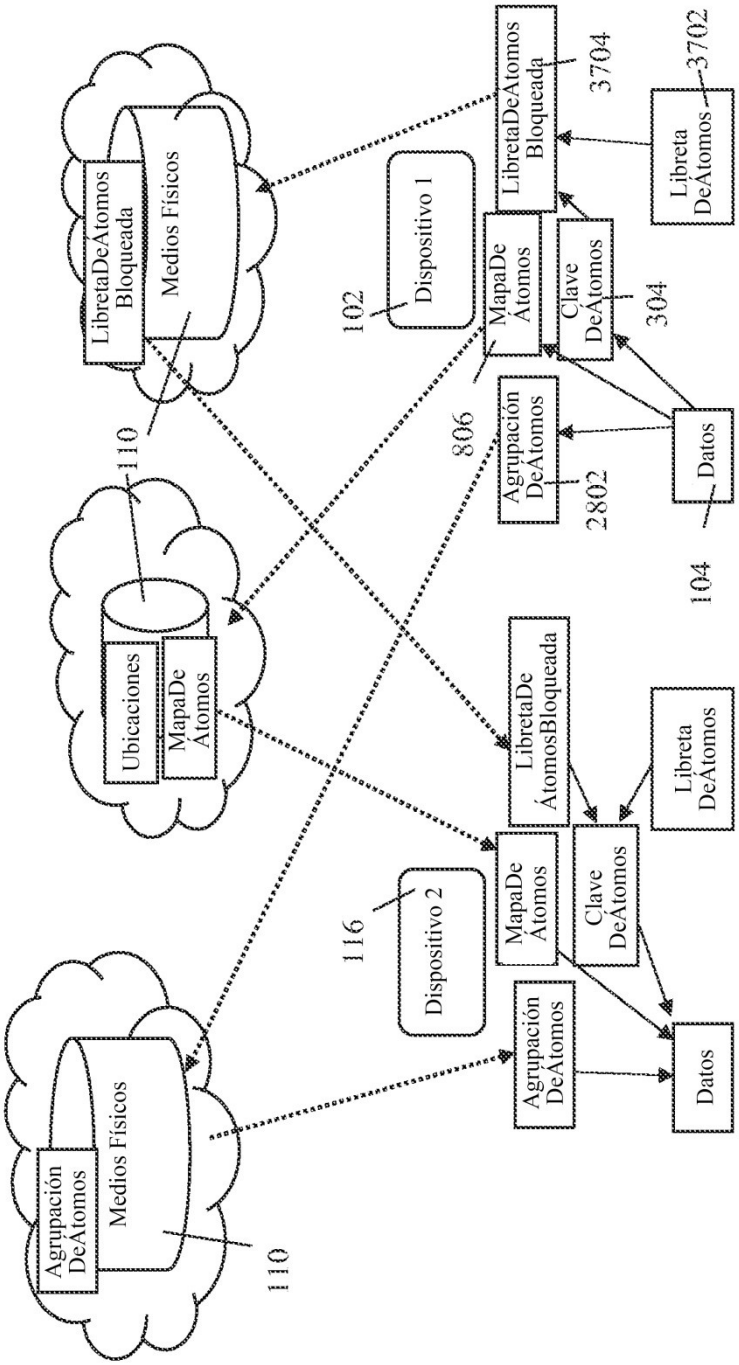
LibretaDeÁtomos Bloqueada
Medios Físicos
110
Ubicaciones
MapaDe Átomos
Agrupación DeÁtomos
Medios Físicos
110
102
Dispositivo 1
116
Dispositivo 2
806
LibretaDeÁtomos Bloqueada
3704
MapaDe Átomos
Clave DeÁtomos
304
Agrupación DeÁtomos
2802
Datos
104
Libreta DeÁtomos
3702
LibretaDe ÁtomosBloqueada
MapaDe Átomos
Clave DeÁtomos
Agrupación DeÁtomos
Datos
Libreta DeÁtomos

Fig. 39

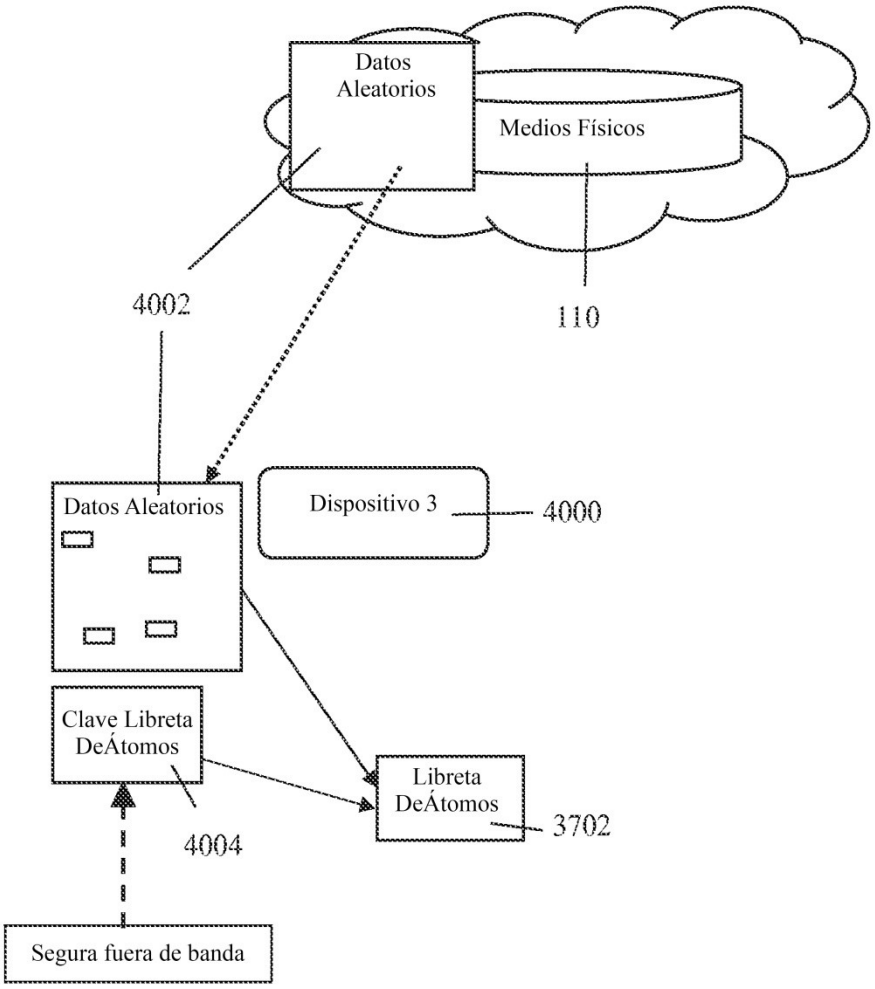
Datos
Aleatorios
Medios Físicos
4002
110
Datos Aleatorios
Dispositivo 3
4000
Clave Libreta
DeÁtomos
Libreta
DeÁtomos
3702
4004
Segura fuera de banda

Fig. 40