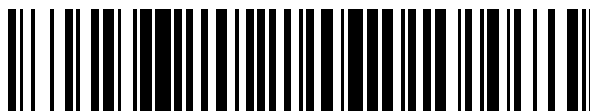


19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 600 129**

51 Int. Cl.:

G06F 11/14 (2006.01)

G06F 9/44 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **29.08.2012 PCT/US2012/052945**

87 Fecha y número de publicación internacional: **07.03.2013 WO13033272**

96 Fecha de presentación y número de la solicitud europea: **29.08.2012 E 12826825 (7)**

97 Fecha y número de publicación de la concesión europea: **27.07.2016 EP 2751662**

54 Título: **Procedimiento para una recuperación de desastres de aplicación eficiente**

30 Prioridad:

02.09.2011 US 201113224794

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

07.02.2017

73 Titular/es:

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

72 Inventor/es:

**VALIYAPARAMBIL, MANOJ K.;
SINGLA, AMIT;
SEN, VIJAY y
ALI, ABID**

74 Agente/Representante:

CARPINTERO LÓPEZ, Mario

ES 2 600 129 T3

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

DESCRIPCIÓN

Procedimiento para una recuperación de desastres de aplicación eficiente

Antecedentes

5 Los ordenadores han llegado a integrarse notablemente en el mundo laboral, en el hogar, en los dispositivos móviles y muchos otros lugares. Los ordenadores pueden procesar cantidades masivas de información de manera rápida y eficiente. Las aplicaciones de software diseñadas para ejecutarse en los sistemas informáticos permiten a los usuarios realizar una amplia diversidad de funciones, incluyendo aplicaciones de negocios, tareas escolares, entretenimiento y más. Las aplicaciones de software a menudo se diseñan para realizar tareas específicas, tales como las aplicaciones de procesador de texto para la redacción de documentos o programas de correo electrónico para enviar, recibir y organizar el correo electrónico. El documento US2010/0318759 A1 desvela un almacenamiento distribuido de fragmentos RDC, el documento US 7.552.358 B1 desvela una copia de seguridad y un restablecimiento eficientes usando un mapeo de metadatos.

15 Los datos producidos por estas aplicaciones son a menudo muy valiosos y, por lo tanto, habitualmente se hacen copias de seguridad de los mismos de alguna forma. Las aplicaciones de copias de seguridad de datos pueden adoptar muchas formas diferentes. Algunas aplicaciones de copias de seguridad copian los datos a nivel local en una unidad de cinta u otros medios. Otras aplicaciones de copias de seguridad copian los datos en localizaciones remotas, incluyendo en la nube. Además de las copias de seguridad de datos habituales, las empresas pueden tener planes de protección contra desastres en su lugar que se aprueban en caso de emergencia. Estos planes de recuperación de datos, sin embargo, usan habitualmente una gran cantidad de ancho de banda de red, ya que la implementación de estos planes tiende a ser todo o nada.

Breve resumen

25 Las realizaciones descritas en el presente documento están dirigidas a hacer de manera eficiente copias de seguridad de una o más partes de datos y a realizar una recuperación de datos restringida. En una realización, un sistema informático precarga unas imágenes de datos con los datos correspondientes a diversas aplicaciones de software o sistemas operativos diferentes. El sistema informático fragmenta las imágenes de datos precargadas, de tal manera que cada imagen de datos se divide en múltiples fragmentos de datos, y en el que cada fragmento de datos está representado por un valor de comprobación aleatoria. A continuación, el sistema informático recibe de un usuario partes de datos delta que representan las diferencias de datos entre los datos de usuario recibidos y los datos de las imágenes de datos precargadas. El sistema informático también genera una representación lógica de copias de seguridad que incluye los valores de comprobación aleatoria de fragmentos de datos para las imágenes de datos precargadas, así como los datos delta recibidos del usuario. Esta representación lógica permite el restablecimiento de los datos del usuario usando solo los valores de comprobación aleatoria y los datos delta.

35 En otra realización, un sistema informático define una política de recuperación de desastres que especifica qué aplicaciones de software de entre múltiples aplicaciones de software diferentes van a restablecerse después de que se haya producido un suceso desastroso. El sistema informático recibe, desde un disco duro virtual generado, los datos de diferencia que comprenden las diferencias de datos entre los datos recibidos de un usuario y otras imágenes de datos precargadas, estando el disco duro virtual configurado para recibir los datos de diferencia del usuario. El sistema informático determina, basándose en la política de recuperación de desastres, qué datos de la aplicación de software van a restablecerse y restablece los datos delta de aplicación de software al usuario de acuerdo con la política.

40 La presente invención se refiere a un procedimiento de acuerdo con la reivindicación 1. Las reivindicaciones dependientes se refieren a las realizaciones preferidas de la presente invención.

45 Este resumen se proporciona para introducir una selección de conceptos de una forma simplificada que se describen con más detalle a continuación en la descripción detallada. Este resumen no está destinado a identificar características clave o características esenciales del objeto reivindicado, ni está destinado a usarse como una ayuda para determinar el ámbito del objeto reivindicado.

50 En la siguiente descripción, se expondrán características y ventajas adicionales, y que en parte serán evidentes a partir de la descripción, o pueden aprenderse mediante la puesta en práctica de las enseñanzas del presente documento. Las características y las ventajas de la invención pueden realizarse y obtenerse por medio de los instrumentos y las combinaciones especialmente indicadas en las reivindicaciones adjuntas. Las características de la presente invención se harán más evidentes a partir de la siguiente descripción y las reivindicaciones adjuntas, o pueden aprenderse mediante la puesta en práctica de la invención como se expone en lo sucesivo en el presente documento.

Breve descripción de los dibujos

55 Para aclarar aún más las ventajas y las características anteriores, y otras, de las realizaciones de la presente invención, se hará una descripción más específica de las realizaciones de la presente invención por referencia a los dibujos adjuntos. Se aprecia que estos dibujos representan solo las realizaciones habituales de la invención y, por lo

tanto, no deben considerarse limitantes de su ámbito. La invención se describirá y se explicará con mayor especificidad y detalle a través del uso de los dibujos adjuntos, en los que:

La figura 1 ilustra una arquitectura informática en la que las realizaciones de la presente invención pueden operar incluyendo la copia de seguridad eficiente de una o más partes de datos.

5 La figura 2 ilustra un diagrama de flujo de un ejemplo de procedimiento para hacer de manera eficiente copias de seguridad de una o más partes de datos.

La figura 3 ilustra un diagrama de flujo de un ejemplo de procedimiento para realizar una recuperación de datos restringida.

La figura 4 ilustra una arquitectura informática en la que los datos se restablecen de manera priorizada.

10 **Descripción detallada**

Las realizaciones descritas en el presente documento están dirigidas a hacer de manera eficiente copias de seguridad de partes de datos y a realizar una recuperación de datos restringida. En una realización, un sistema informático precarga unas imágenes de datos con los datos correspondientes a diversas aplicaciones de software o sistemas operativos diferentes. El sistema informático fragmenta las imágenes de datos precargadas, de tal manera que cada imagen de datos se divide en múltiples fragmentos de datos, y en el que cada fragmento de datos está representado por un valor de comprobación aleatoria. A continuación, el sistema informático recibe de un usuario partes de datos delta que representan las diferencias de datos entre los datos de usuario recibidos y los datos de las imágenes de datos precargadas. El sistema informático también genera una representación lógica de copias de seguridad que incluye los valores de comprobación aleatoria de fragmentos de datos para las imágenes de datos precargadas, así como los datos delta recibidos del usuario. Esta representación lógica permite el restablecimiento de los datos del usuario usando los valores de comprobación aleatoria y los datos delta. Por ejemplo, una vez que el valor de comprobación aleatoria se ha mapeado con el fragmento de datos apropiado, los datos delta pueden usarse para representar una visión completa de los datos restablecidos.

En otra realización, un sistema informático define una política de recuperación de desastres que especifica qué aplicaciones de software de entre múltiples aplicaciones de software diferentes van a restablecerse después de que se haya producido un suceso desastroso. El sistema informático recibe, desde un disco duro virtual generado, datos de diferencia que comprenden las diferencias de datos entre los datos recibidos de un usuario y otras imágenes de datos precargadas. El sistema informático determina, basándose en la política de recuperación de desastres, qué datos de las aplicaciones de software van a restablecerse y restablece los datos delta de aplicación de software al usuario de acuerdo con la política.

El siguiente análisis se refiere ahora a una serie de procedimientos y acciones de procedimiento que pueden realizarse. Cabe señalar que aunque las acciones de procedimiento pueden tratarse en un determinado orden o ilustrarse en un diagrama de flujo que transcurre en un orden específico, no se requiere necesariamente un orden específico a menos que se indique específicamente, o se requiera debido a que una acción depende de que otra acción se complete antes de que se realice la acción.

Las realizaciones de la presente invención pueden comprender o utilizar un ordenador de propósito especial o de propósito general que incluye un hardware informático, tal como, por ejemplo, uno o más procesadores y memorias de sistema, como se trata en mayor detalle a continuación. Las realizaciones dentro del ámbito de la presente invención también incluyen medios físicos y otros medios legibles por ordenador para transportar o almacenar instrucciones ejecutables por ordenador y/o estructuras de datos. Tales medios legibles por ordenador pueden ser cualquier medio disponible al que pueda accederse por un sistema informático de propósito general o de propósito especial. Los medios legibles por ordenador que almacenan instrucciones ejecutables por ordenador en forma de datos son medios de almacenamiento informáticos. Los medios legibles por ordenador que transportan instrucciones ejecutables por ordenador son medios de transmisión. Por lo tanto, a modo de ejemplo, y no de limitación, las realizaciones de la invención pueden comprender al menos dos tipos claramente diferentes de medios legibles por ordenador: los medios de almacenamiento informáticos y los medios de transmisión.

Los medios de almacenamiento informáticos incluyen RAM, ROM, EEPROM, CD-ROM, unidades de estado sólido (SSD) que se basan en RAM, memoria flash, memoria de cambio de fase (PCM), u otros tipos de memoria, u otros dispositivos de almacenamiento de disco óptico, almacenamiento de disco magnético u otro almacenamiento magnético, o cualquier otro medio que pueda usarse para almacenar un medio de código de programa deseado en forma de instrucciones ejecutables por ordenador, datos o estructuras de datos y al que pueda accederse por un ordenador de propósito general o de propósito especial.

Una "red" se define como uno o más enlaces de datos y/o conmutadores de datos que permiten el transporte de datos electrónicos entre sistemas y/o módulos informáticos y/u otros dispositivos electrónicos. Cuando la información se transfiere o se proporciona a través de una red (cableada, inalámbrica, o una combinación de cableada o inalámbrica) a un ordenador, el ordenador considera correctamente la conexión como un medio de transmisión. Los medios de transmisión pueden incluir una red que puede usarse para transportar datos o un medio de código de programa deseado en forma de instrucciones ejecutables por ordenador o en forma de estructuras de datos y al que puede accederse por un ordenador de propósito general o de propósito especial. Las combinaciones de los

anteriores también deben incluirse dentro del ámbito de los medios legibles por ordenador.

Además, tras alcanzar diversos componentes del sistema informático, el medio de código de programa en forma de instrucciones ejecutables por ordenador o estructuras de datos puede transferirse automáticamente desde los medios de transmisión a los medios de almacenamiento informáticos (o viceversa). Por ejemplo, las instrucciones ejecutables por ordenador o las estructuras de datos recibidas a través de una red o un enlace de datos pueden almacenarse temporalmente en una RAM dentro de un módulo de interfaz de red (por ejemplo, una tarjeta de interfaz de red o "NIC") y, a continuación, transferirse finalmente a la RAM del sistema informático y/o a un medio de almacenamiento informático menos volátil en un sistema informático. Por lo tanto, debe entenderse que pueden incluirse medios de almacenamiento informáticos en los componentes del sistema informático que también (o incluso principalmente) utilizan medios de transmisión.

Las instrucciones ejecutables por ordenador (o interpretables por ordenador) comprenden, por ejemplo, instrucciones que hacen que un ordenador de propósito general, un ordenador de propósito especial, o un dispositivo de procesamiento de propósito especial realicen una determinada función o grupo de funciones. Las instrucciones ejecutables por ordenador pueden ser, por ejemplo, instrucciones binarias de formato intermedio, tal como un lenguaje ensamblador, o incluso un código fuente. Aunque el objeto se ha descrito en un lenguaje específico para características estructurales y/o acciones metodológicas, debe entenderse que el objeto definido en las reivindicaciones adjuntas no se limita necesariamente a las características o las acciones descritas anteriormente. Por el contrario, las características y las acciones descritas se desvelan como ejemplos de formas de implementar las reivindicaciones.

Los expertos en la materia apreciarán que la invención puede ponerse en práctica en entornos informáticos de red con muchos tipos de configuraciones de sistemas informáticos, incluyendo ordenadores personales, ordenadores de sobremesa, ordenadores portátiles, procesadores de mensajes, dispositivos manuales, sistemas multiprocesador, componentes electrónicos de consumo basados en microprocesador o programables, PC de red, miniordenadores, ordenadores centrales, teléfonos móviles, PDA, buscapersonas, enrutadores, conmutadores y similares. La invención también puede ponerse en práctica en entornos de sistemas distribuidos en los que los sistemas informáticos locales y remotos que se enlazan (mediante enlaces de datos cableados, enlaces de datos inalámbricos, o mediante una combinación de enlaces de datos cableados e inalámbricos) a través de una red, realizan, cada uno de los mismos, tareas (por ejemplo, la computación en nube, servicios en la nube y similares). En un entorno de sistemas distribuidos, los módulos de programa pueden localizarse en ambos dispositivos de almacenamiento de memoria local y remota.

La figura 1 ilustra una arquitectura 100 informática en la que pueden emplearse los principios de la presente invención. La arquitectura 100 informática incluye un sistema 101 informático. El sistema informático puede ser cualquier tipo de sistema informático local o distribuido. El sistema 101 puede configurarse para realizar diversas realizaciones que incluyen 1) optimizar la utilización de recursos cuando se configura un sitio secundario para la protección contra los desastres y 2) realizar una protección y recuperación restringidas de desastres de aplicación consciente. Cada uno de estos aspectos se describirá a continuación de manera preliminar, y en más detalle con respecto a los procedimientos 200 y 300 de las figuras 2 y 3, respectivamente.

Con el fin de tener una localización secundaria (en la nube o de otro modo) capaz de albergar un sistema operativo (OS), las aplicaciones y los datos correspondientes, con un tiempo de recuperación razonable (en caso de desastre), los datos de OS y de aplicación están disponibles en la localización secundaria, que se mantiene en sincronía con una localización primaria. En algunos casos, los datos de aplicación/OS pueden almacenarse en un disco duro virtual (VHD). Pueden usarse muchos otros dispositivos de almacenamiento además de, o como alternativa a, un VHD. Además, el enfoque descrito a continuación está diseñado para funcionar a través de implementaciones físicas y virtuales.

En algunas realizaciones, pueden crearse "imágenes de oro" para los OS y/o las aplicaciones. Tal como se usa en el presente documento, la expresión "imágenes de oro" puede referirse a imágenes de datos que incluyen versiones pre-instaladas de un sistema operativo y uno o más programas de software. Las realizaciones pueden aprovechar estas imágenes de oro para configurar de manera óptima la recuperación de desastres. Como una etapa de configuración, la localización (copia de seguridad) secundaria se genera con una biblioteca de imágenes de oro. Estas imágenes pueden ser binarios de OS y de aplicación convencionales cargados directamente en la localización secundaria sin necesidad de generarse a través de la red. En un ejemplo, una imagen de oro actualizada puede incluir el conjunto de cambios que ayudan al sistema a sintetizar una imagen de oro diferente en comparación con una imagen de oro original. En el contexto de este ejemplo, la imagen de oro actualizada puede almacenarse en un VHD de diferenciación (diseñado para almacenar las diferencias entre imágenes) que puede combinarse con la imagen de oro original para proporcionar una nueva variante de la imagen de oro sin requerir el almacenamiento múltiples veces.

Las imágenes de oro pueden almacenarse en una biblioteca y, a continuación, fragmentarse en un nivel de bloques usando (al menos en algunos casos) una fragmentación variable. La fragmentación divide las imágenes en múltiples "fragmentos" diferentes, estando cada fragmento representado por un identificador único (por ejemplo, un valor de comprobación aleatoria). Las imágenes de oro pueden retenerse tras la fragmentación con el fin de facilitar una

recuperación más rápida en caso de desastre, si se desea, pero esto requerirá más espacio de almacenamiento. Si debe conservarse el almacenamiento, las imágenes de oro pueden descartarse tras la fragmentación y resintetizarse a partir de los fragmentos, junto con los metadatos almacenados con los fragmentos que indican cómo deben los fragmentos volver a formarse en una imagen.

5 Una vez que los fragmentos se generan a partir de las imágenes de oro (el procedimiento de fragmentación solo se requiere cuando se generan nuevas imágenes en la biblioteca), los datos de fuente se transfieren a un VHD y estos se comparan con los bloques generados previamente fragmentando todas las imágenes de oro. Debido a la similitud entre los archivos de imágenes de oro (por ejemplo, binarios de OS, binarios de aplicación), grandes fragmentos de datos estarán fácilmente disponibles en la localización secundaria y el tiempo empleado (y los recursos consumidos) para transmitir solo los nuevos bloques a la secundaria será más eficiente (y más rápido) que transmitir todo el VHD transferido de la fuente primaria a la secundaria.

10 También cabe señalar que si la imagen de oro se retiene en la secundaria (para una recuperación de desastres rápida), la imagen de oro puede que no se actualice directamente por los cambios del sistema fuente. Por el contrario, puede usarse un VHD de diferenciación para capturar los cambios requeridos con el fin de sintetizar el sistema fuente de la imagen de oro. Puede crearse una agrupación lógica para mantener un seguimiento de esta relación.

15 Una vez que existe la agrupación lógica, una diversidad de opciones pueden estar disponibles para realizar una recuperación de datos (después de un desastre): 1) Una opción sería "recuperar" directamente una instancia del sistema fuente en la localización secundaria usando la relación de grupo lógico. En este caso, la recuperación podría realizarse activando directamente una instancia de los datos de OS y/o de aplicación contenidos dentro la agrupación lógica; o, como alternativa, copiando la agrupación lógica en otra área en la propia localización secundaria y, a continuación, crear instancias de la misma. 2) Una segunda opción sería usar la imagen de oro (cuando esté disponible en la localización primaria) para poner en funcionamiento el sistema fuente. Una vez hecho esto, solo se necesitará transferir la información de diferenciación (por ejemplo, desde el VHD de diferenciación) para corregir el sistema fuente. Este enfoque también puede usarse durante una conmutación por recuperación, una vez que los recursos primarios han llegado en línea después de un desastre.

20 Las realizaciones también pueden estar dirigidas a la protección y recuperación restringidas de desastres de aplicación consciente. En algunos casos, las empresas pueden tener un conjunto básico de aplicaciones que son más importantes para las mismas que otras aplicaciones (por ejemplo, programas de gestión de correo electrónico). Después de un desastre, tales empresas pueden querer usar sus recursos disponibles (por ejemplo, almacenamiento, ancho de banda de red, entre primarios y secundarios) para restablecer estas aplicaciones importantes antes de restablecer otras aplicaciones menos importantes. Por lo tanto, en algunas realizaciones, puede proporcionarse una copia de seguridad y/o un restablecimiento restringidos para cada aplicación.

25 Como una primera etapa en el flujo de trabajo, la política para determinar el ámbito de la aplicación y los datos necesarios a proporcionar (o detectarse automáticamente en función de la clasificación de metadatos). Basándose en el ámbito proporcionado, se genera y se corrige el VHD transferido restringido usando los fragmentos generados a partir de las imágenes de oro. Una vez que se ha completado la corrección, se determina la representación lógica para el sistema fuente restringido.

30 La determinación del ámbito puede hacerse a nivel de aplicaciones o a nivel de componentes (por ejemplo, restableciendo ciertas partes de las aplicaciones). Una manera de determinar los límites de las aplicaciones y los componentes sería usar un escritor de aplicaciones (o escritor de sistema para archivos de sistema). Una vez que se ha determinado el ámbito, puede configurarse un VHD de transferencia para el ámbito deseado y, a continuación, usarse para la copia de seguridad o la recuperación de desastres. Además, el VHD de copia de seguridad transferido puede restringirse aún más durante el procedimiento de recuperación de desastres para permitir la recuperación de desastres para un subconjunto de aplicaciones de las que originalmente se hizo una copia de seguridad. Puesto que la copia de seguridad tiene conocimiento de la aplicación y de los componentes, tiene la información requerida para permitir que solo se use un subconjunto de estos para la recuperación de desastres. De esta manera, las empresas u otros usuarios también pueden hacer copias de seguridad de todas sus aplicaciones y componentes, aunque realizando la recuperación de desastres solo para un subconjunto de la aplicación y de los componentes. Aprovechar las copias de seguridad activas para realizar la recuperación de desastres puede evitar el almacenamiento de datos duplicados. Estos aspectos se describirán con mayor detalle a continuación con respecto a los procedimientos 200 y 300 de las figuras 2 y 3, respectivamente.

35 En vista de los sistemas y las arquitecturas descritas anteriormente, las metodologías que pueden implementarse de acuerdo con el objeto desvelado se apreciarán mejor con referencia a los diagramas de flujo de las figuras 2 y 3. Con el fin de simplificar la explicación, las metodologías se muestran y se describen como una serie de bloques. Sin embargo, debe entenderse y apreciarse que el objeto reivindicado no está limitado por el orden de los bloques, ya que algunos bloques pueden sucederse en un orden diferente del que se representa y se describe en el presente documento, y/o simultáneamente con otros bloques. Además, puede que no se requieran todos los bloques ilustrados para implementar las metodologías descritas a continuación.

La figura 2 ilustra un diagrama de flujo de un procedimiento 200 para hacer de manera eficiente copias de seguridad de una o más partes de datos. El procedimiento 200 se describirá a continuación con referencia frecuente a los componentes y los datos del entorno 100.

5 El procedimiento 200 incluye una acción de precargar una o más imágenes de datos con los datos correspondientes a una o más aplicaciones de software (acción 210). Por ejemplo, el módulo 105 de precarga de imágenes puede precargar una imagen 106 (de oro) que incluye aplicaciones y/o sistemas operativos. Por ejemplo, la imagen de oro puede incluir una versión de un sistema operativo, una versión revisada o actualizada de un sistema operativo, un sistema operativo más una o más aplicaciones, o simplemente una aplicación o conjunto de aplicaciones (por ejemplo, un paquete de software de oficina) (cualquiera o todas estas combinaciones pueden representarse por el elemento 107). Estas imágenes, una vez precargadas, pueden fragmentarse por el módulo 110 de fragmentación de imágenes. Por lo tanto, cada imagen de datos se divide en múltiples fragmentos 111 de datos diferentes y cada uno de esos fragmentos de datos está representado por un valor 112 de comprobación aleatoria (acción 220). El valor de comprobación aleatoria puede generarse por MD5 o sustancialmente cualquier otro algoritmo de comprobación aleatoria. Los fragmentos de datos pueden almacenarse en un almacén 115 de datos. El almacén de datos puede incluir cualquier tipo de almacenamiento de datos local o distribuido. El almacén de datos también puede almacenar las imágenes 106 (de oro) de datos precargadas.

20 El procedimiento 200 también incluye una acción de recibir, de un usuario, una o más partes de datos delta que representan las diferencias de datos entre los datos de usuario recibidos y los datos de las imágenes de datos precargadas (acción 230). Por ejemplo, el módulo 130 de recepción de datos delta puede recibir los datos 126 delta del usuario 125. Los datos delta representan las diferencias de datos entre los datos del usuario y los datos de las imágenes 106 precargadas. Por lo tanto, si un usuario ha creado un contenido, o complementos para diferentes aplicaciones, estas partes de los datos se incluirán en los datos delta. Además, cualquier cambio de configuración o de política se enviará en los datos delta. En general, los datos delta incluirán cualquier cambio de datos tras la aplicación de software inicial o la instalación del sistema operativo.

25 El procedimiento 200 incluye además una acción de generar una representación lógica de copias de seguridad que incluye los valores de comprobación aleatoria de fragmentos de datos para las imágenes de datos precargadas, así como los datos delta recibidos del usuario, permitiendo la representación lógica el restablecimiento de los datos del usuario usando los valores de comprobación aleatoria para hacer referencia a los fragmentos adecuados y los datos delta (acción 240). Por ejemplo, el módulo 135 de generación de representación de copias de seguridad puede generar una representación 136 lógica de copias de seguridad que incluye los valores 112 de comprobación aleatoria de las imágenes fragmentadas y los datos 126 delta recibidos del usuario 125. Después de un desastre, un usuario puede restablecer sus datos usando las imágenes precargadas (o simplemente instalando los propios datos de aplicación/OS) y los datos delta. Por lo tanto, la representación lógica de copias de seguridad puede incluir solo los valores de comprobación aleatoria y los datos delta.

35 En consecuencia, en una realización, el sistema 101 informático puede recibir una solicitud para restablecer los datos del usuario. La solicitud incluye una indicación de aquellos sistemas y programas operativos que ya están instalados en el sistema informático del usuario. A continuación, el sistema informático puede acceder a la representación 136 lógica de copias de seguridad para determinar qué datos van a devolverse para restablecer el sistema informático del usuario a su estado original. Adicionalmente, o como alternativa, los datos pueden devolverse para volver a crear el sistema informático copiado en un destino diferente, tal como otro sistema informático o en la nube. A continuación, tras determinar qué datos devolver, el sistema informático puede devolver esos datos al usuario.

45 En algunos casos, las representaciones lógicas de copias de seguridad se generan para aquellas aplicaciones de software especificadas por el usuario. De esta manera, se determina el ámbito de la recuperación de desastres para incluir solo aquellas aplicaciones deseadas por el usuario. Estas aplicaciones pueden incluir las aplicaciones consideradas como de alta prioridad por el usuario. Estas aplicaciones de alta prioridad pueden restaurarse antes que los datos de las aplicaciones de menor prioridad. La prioridad de las aplicaciones puede almacenarse en la política 127 de recuperación de desastres. El usuario podría, en algunos casos, solicitar que una o más imágenes precargadas se devuelvan además de los datos delta. En estos casos, las imágenes precargadas determinadas pueden enviarse además de los datos delta. Adicionalmente, o como alternativa, una o más de las aplicaciones del usuario pueden restablecerse de forma local en un sistema informático local, de tal manera que las aplicaciones se proporcionan a los usuarios de las aplicaciones desde el sistema informático local.

55 La figura 3 ilustra un diagrama de flujo de un procedimiento 300 para realizar una recuperación de datos restringida. A continuación, se describirá el procedimiento 300 con referencia frecuente a los componentes y los datos de los entornos 100 y 400 de las figuras 1 y 4, respectivamente.

60 El procedimiento 300 incluye una acción de definir una política de recuperación de desastres que especifica qué aplicaciones de software de entre una pluralidad de diferentes aplicaciones de software va a restaurarse después de que se haya producido el suceso desastroso (acción 310). Por ejemplo, un usuario en el sistema 401 informático cliente puede definir la política 403 de recuperación de desastres que especifica qué aplicaciones 404 de software van a restaurarse después de que se haya producido un suceso desastroso y los sistemas informáticos del usuario

ya no estén disponibles.

5 La política de recuperación de desastres puede especificar que se hagan copias de seguridad de la totalidad o de una parte de los datos del usuario (por ejemplo, en el almacén 410 de datos de servidor remoto). Después del desastre, puede restablecerse la totalidad o una parte de los datos 411/412 del usuario. En concreto, el usuario puede especificar que debe restablecerse la totalidad de sus aplicaciones con copia de seguridad, o puede especificar que deben restablecerse ciertas aplicaciones de entre su conjunto completo de aplicaciones con copia de seguridad. La política de recuperación de desastres puede especificar con mayor detalle una prioridad 405 para cada aplicación. En tales casos, las aplicaciones de mayor prioridad se restablecen antes que las aplicaciones de menor prioridad. En los casos en los que se restablecen partes de una sola aplicación, esas partes también pueden priorizarse, de manera que las partes de aplicación de alta prioridad se restablecen en primer lugar.

10 El procedimiento 300 incluye una acción de recibir, desde un disco duro virtual generado, los datos de diferencia que comprenden las diferencias de datos entre los datos recibidos de un usuario y una o más imágenes de datos precargadas, estando el disco duro virtual configurado para recibir los datos de diferencia del usuario (acción 320). Por ejemplo, el usuario 125 puede enviar sus datos delta a un disco 120 duro virtual. El disco duro virtual recibe y almacena estos datos delta. El usuario podría enviar una solicitud 406 de recuperación al servidor remoto para restablecer los datos del usuario de acuerdo con la política de recuperación de desastres. En algunos casos, puede generarse una representación lógica de copias de seguridad que incluye los valores de comprobación aleatoria de datos para las imágenes de datos precargadas, así como los datos de diferencia recibidos del usuario. La representación lógica permite el restablecimiento de los datos del usuario usando solo los valores de comprobación aleatoria para referenciar los fragmentos de datos apropiados y los datos de diferencia. El servidor remoto puede determinar, basándose en la política de recuperación de desastres, qué datos de la aplicación de software van a restaurarse (acción 330). A continuación, de acuerdo con la política, pueden restablecerse los datos del usuario (acción 340). Debido a que los datos se restablecen a partir de los datos con copia de seguridad almacenados previamente, se evita el almacenamiento de datos separados para la recuperación de desastres.

25 En consecuencia, se proporcionan procedimientos, sistemas y productos de programas informáticos que hacen de manera eficiente copias de seguridad de una o más partes de datos. Además, se proporcionan procedimientos, sistemas y productos de programas informáticos que realizan una recuperación de datos restringida.

30 La presente invención puede realizarse de otras formas específicas sin alejarse de las características esenciales. Las realizaciones descritas deben considerarse en todos los sentidos solo como ilustrativas y no restrictivas. Por lo tanto, el ámbito de la invención está indicado por las reivindicaciones adjuntas en lugar de por la descripción anterior.

REIVINDICACIONES

1. En un sistema (101) informático que incluye al menos un procesador y una memoria, en un entorno de red informática que incluye una pluralidad de sistemas informáticos, un procedimiento implementado por ordenador para hacer de manera eficiente copias de seguridad de una o más partes de datos, comprendiendo el procedimiento:
 - 5 una acción de precargar una o más imágenes de datos con los datos correspondientes a una o más aplicaciones (107) de software o sistemas operativos;
una acción de fragmentar las imágenes de datos, de tal manera que cada imagen de datos se divide en una pluralidad de fragmentos de datos, estando cada fragmento de datos representado por un valor de comprobación aleatoria;
 - 10 una acción de recibir, de un usuario, una o más partes de datos (126) delta que representan las diferencias de datos entre los datos de usuario recibidos y los datos en las imágenes de datos precargadas; y
una acción de generar una representación lógica de copias de seguridad que incluye los valores (112) de comprobación aleatoria de fragmentos de datos para las imágenes de datos precargadas, así como los datos (126) delta recibidos del usuario, en el que la representación lógica permite el restablecimiento de los datos del
 - 15 usuario usando los valores (112) de comprobación aleatoria y los datos (126) delta.
2. El procedimiento de la reivindicación 1, en el que solo los valores (112) de comprobación aleatoria y los datos (126) delta se almacenan como parte de la representación lógica de las copias de seguridad.
3. El procedimiento de la reivindicación 1, en el que la imagen de datos precargada comprende una imagen de sistema operativo.
- 20 4. El procedimiento de la reivindicación 1, que comprende además:
 - una acción de recibir una solicitud para restablecer los datos del usuario, en el que la solicitud incluye una indicación de aquellos sistemas operativos y programas que ya están instalados en el sistema informático del usuario;
 - 25 una acción de acceder a la representación lógica de las copias de seguridad para determinar qué datos van a devolverse para restablecer el sistema informático del usuario a su estado original; y
una acción de devolver los datos (126) delta al usuario.
5. El procedimiento de la reivindicación 4, en el que los datos (126) delta incluyen uno o más de los siguientes: programas de software, configuración de programas de software, datos generados por el usuario y configuración del sistema operativo.
- 30 6. El procedimiento de la reivindicación 1, en el que las representaciones lógicas de copias de seguridad se generan para aquellas aplicaciones de software especificadas por el usuario (125).
7. El procedimiento de la reivindicación 4, en el que los datos para las aplicaciones indicadas de alta prioridad se restablecen antes que los datos para las aplicaciones indicadas de menor prioridad.
8. El procedimiento de la reivindicación 4, que comprende además:
 - 35 una acción de determinar que una o más imágenes precargadas van a devolverse además de los datos (126) delta; y
una acción de enviar las imágenes precargadas determinadas además de los datos (126) delta.

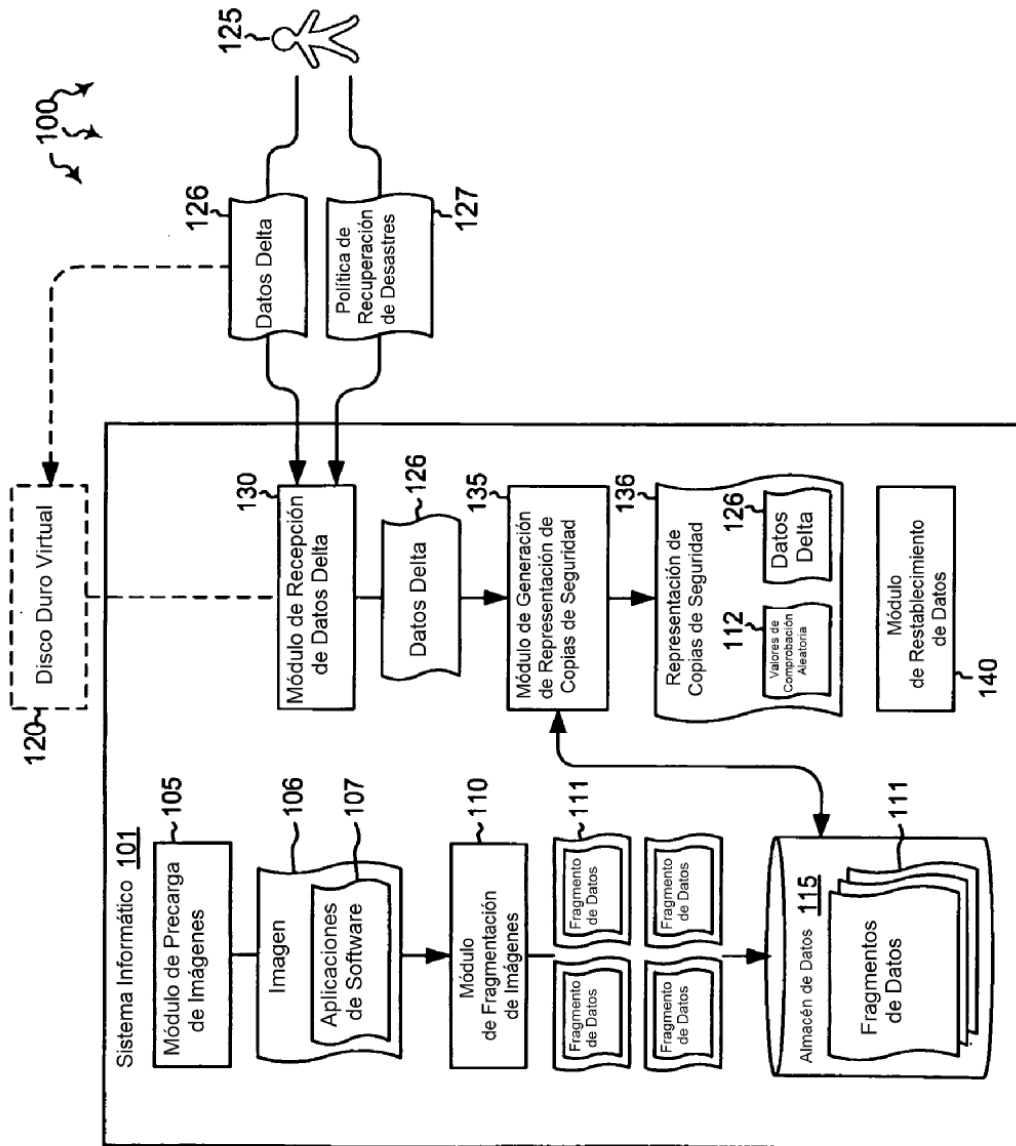


Figura 1

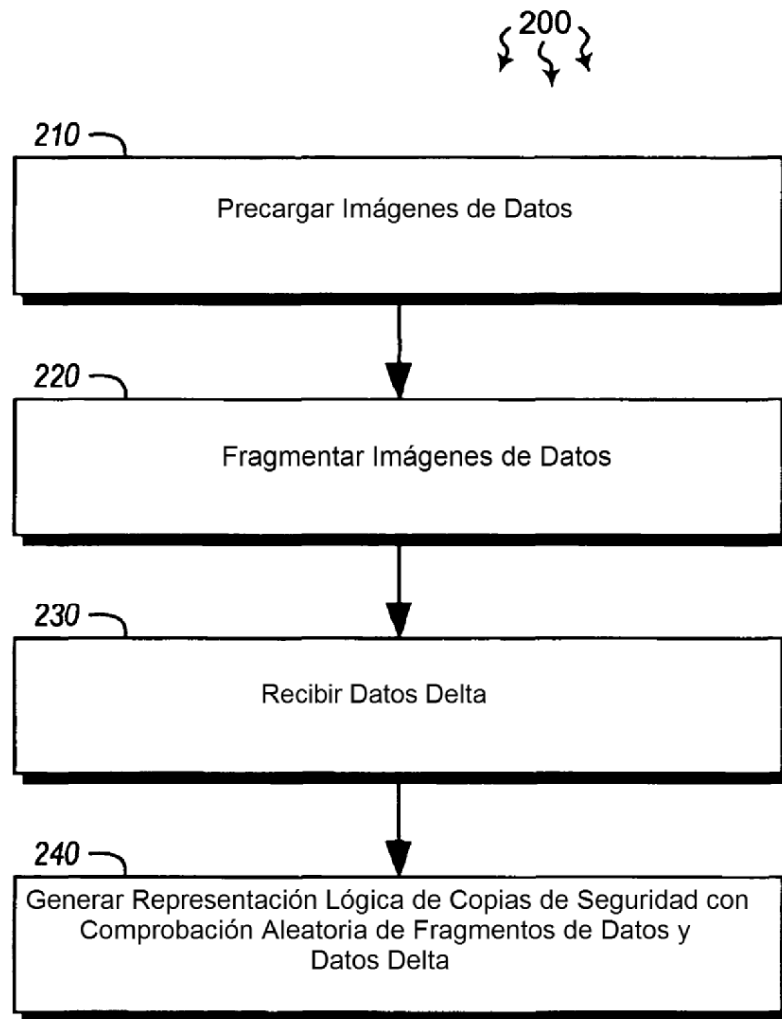


Figura 2

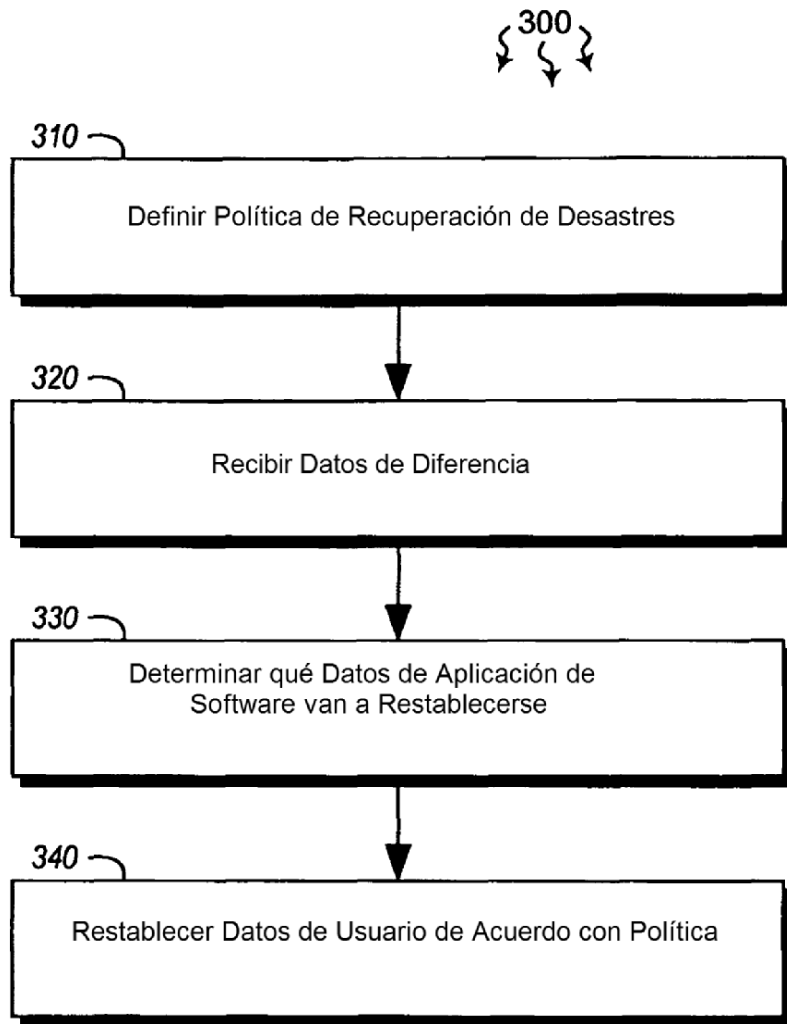


Figura 3

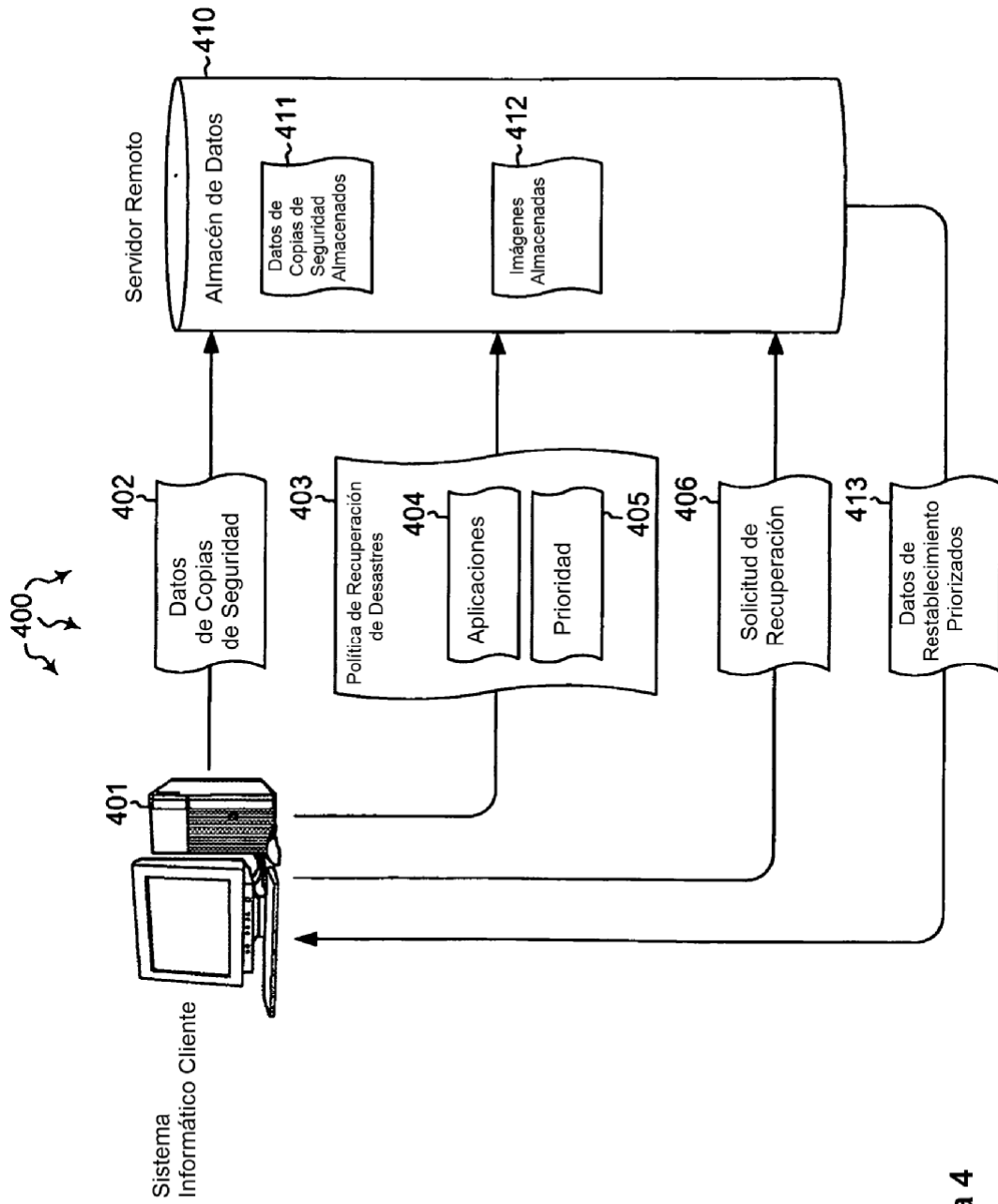


Figura 4