(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 368 975**

(51) Int. CI.:
G06F 11/14 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **08864195 .6**
(96) Fecha de presentación: **04.12.2008**
(97) Número de publicación de la solicitud: **2229629**
(97) Fecha de publicación de la solicitud: **22.09.2010**

(54) Título: **PROCEDIMIENTO Y DISPOSITIVO DE COPIA AUTOMÁTICA DE SEGURIDAD DE DATOS DIGITALES, CONSERVADOS EN MEMORIA EN UNA INSTALACIÓN INFORMÁTICA, ASIMISMO SOPORTE DE DATOS LEGIBLE POR UN ORDENADOR QUE MEMORIZA LAS INSTRUCCIONES DE DICHO PROCEDIMIENTO.**

(30) Prioridad:
06.12.2007 FR 0708519

(45) Fecha de publicación de la mención BOPI:
24.11.2011

(45) Fecha de la publicación del folleto de la patente:
24.11.2011

(73) Titular/es:
F-Secure Corporation
Tammasaarenkatu 7
Helsinki, FI

(72) Inventor/es:
Camborde, Christophe

(74) Agente: **de Elzaburu Márquez, Alberto**

DESCRIPCIÓN

Procedimiento y dispositivo de copia automática de seguridad de datos digitales, conservados en memoria en una instalación informática, asimismo soporte de datos legible por un ordenador que memoriza las instrucciones de dicho procedimiento.

La presente invención se refiere a un procedimiento de copia automática de seguridad de datos digitales, conservados en memoria en una instalación informática, hacia un sistema de copia de seguridad remoto accesible por la instalación informática a través de una red de transmisión de datos. Se refiere asimismo a un soporte de datos legible por un ordenador, a una instalación informática y a un sistema para la puesta en práctica de este procedimiento.

Tales procedimientos de copia de seguridad son conocidos y permiten proteger el acceso a datos digitales conservados en memoria en una instalación informática. En efecto, este acceso puede verse contrariado por:

- una mera y simple pérdida de los datos digitales de la instalación informática con motivo de desastres tales como una inundación, un incendio o, más sencillamente, con motivo de accidentes tales como un daño inesperado de un disco duro o, incluso más corrientemente, con motivo de una manipulación indebida causada por un usuario, o
- una avería parcial o general, incluso momentánea, de la instalación informática que ya no permite acceder a los datos que almacena.

Por la creciente conservación de datos importantes, e incluso vitales, en forma electrónica, es esencial concebir procedimientos de copia de seguridad que ofrezcan una elevada garantía de dar con esos datos en la versión más reciente posible, en caso de problema en la instalación informática. Asimismo es importante que estos procedimientos sean automáticos para que un usuario no tenga que preocuparse de su uso ordinario de la instalación informática.

Estos procedimientos, por tanto, son puestos en práctica generalmente en forma de aplicaciones de copia de seguridad, previamente parametrizadas, que se ejecutan en la instalación informática.

La patente estadounidense publicada con el número US6.757.698 propone así un procedimiento puesto en práctica por una aplicación de copia de seguridad parametrizable por un usuario. El propio usuario determina cuáles son los datos digitales de los que desea realizar una copia de seguridad regularmente y define la frecuencia de las copias de seguridad. Para garantizar la seguridad de los datos guardados mediante copia de seguridad, se prevé definir varios destinos de copia de seguridad, uno de los cuales es un sistema de almacenamiento remoto, accesible por la instalación informática anfitriona a través de Internet. En cada copia de seguridad programada, la aplicación determina cuáles son los datos que han sido modificados desde la anterior copia de seguridad y no selecciona más que los datos que han sido modificados o adicionados para la nueva copia de seguridad.

Sin embargo, con ser automático, este procedimiento requiere del usuario una cierta pericia para definir el conjunto de los parámetros de ejecución de la aplicación de copia de seguridad. Para un óptimo funcionamiento de las copias de seguridad, estos pueden variar efectivamente de una instalación informática a otra. Más aún, ello implica que el usuario sabe determinar el conjunto de los datos importantes que merecen ser guardados mediante copia de seguridad. Si bien esto es efectivamente realista cuando el usuario es un profesional que opera en un servicio de soporte informático de una empresa, tal no es generalmente el caso cuando el usuario es un particular, o incluso administrador de una pequeña estructura profesional carente de los medios de dotarse de un servicio de soporte informático.

El documento US-A-2005/257085 constituye el estado de la técnica más cercano, pues da a conocer un procedimiento de copia automática de seguridad a distancia que permite el análisis de los datos, la clasificación de los datos, su ordenación según criterios de prioridad, así como la ejecución de la copia de seguridad, en su caso.

Así, se puede desear prever un procedimiento de copia automática de seguridad que sea simple de utilización y no precise de un particular conocimiento por parte de un usuario, en cuestión de copias de seguridad o, más generalmente, de sistemas informáticos.

La invención tiene pues por objeto un procedimiento de copia automática de seguridad de datos digitales conservados en memoria en una instalación informática hacia un sistema de copia de seguridad, que incluye la etapa consistente en analizar los datos digitales conservados en memoria y clasificar los datos digitales analizados en una pluralidad de clases de diferentes prioridades, caracterizándose el procedimiento porque el sistema de copia de seguridad es remoto y accesible por la instalación informática a través de una red de transmisión de datos y porque además incluye las etapas consistentes en:

- extraer y analizar información de funcionamiento de la instalación informática, incluyendo esta información de funcionamiento al menos uno de los elementos del conjunto constituido por una potencia y por una memoria disponibles, por la naturaleza y por la versión del sistema operativo de la instalación informática, por la naturaleza de las aplicaciones instaladas y ejecutables por la instalación informática, por la naturaleza y por la capacidad de una

conexión de la instalación informática con la red de transmisión, por una fecha de fabricación o puesta en servicio de la instalación informática, por una frecuencia de puesta en marcha, en espera o desconexión de la instalación informática y por una organización general de los directorios y por una clasificación de ficheros en esos directorios,

- determinar unos parámetros de una aplicación de copia de seguridad de datos hacia el sistema de copia de seguridad, en función del resultado de ese análisis, y

- ejecutar la aplicación de copia de seguridad sobre al menos una parte de los datos digitales, en función de los parámetros y de las clases de prioridades determinados.

El aprovechamiento de etapas previas de análisis combinados de los datos digitales y del funcionamiento general de la instalación informática que los aloja permite, en efecto, obviar la pericia del usuario final para parametrizar la aplicación de copia de seguridad y seleccionar los datos de los que se realizará una copia de seguridad.

Con carácter opcional, los parámetros de la aplicación de copia de seguridad incluyen al menos uno de los elementos del conjunto constituido por un límite de potencia consumida permitido para la aplicación de copia de seguridad, por una opción de ejecución de la aplicación de copia de seguridad en modo degradado y por criterios de selección de los datos digitales de los que se realizará una copia de seguridad.

Con carácter opcional, los criterios de selección y/o la clasificación de los datos digitales en clases de diferentes prioridades son referentes al menos a la naturaleza de los datos digitales.

Con carácter opcional, los criterios de selección y/o la clasificación de los datos digitales en clases de diferentes prioridades son referentes además a al menos uno de los elementos del conjunto constituido por su tamaño, por sus fechas de creación, de última modificación y/o de último acceso, por datos suplementarios de información que llevan asociada, por un directorio en el que aquellos están situados, por una relación entre esos datos y una base de registro de un sistema operativo de la instalación informática y por una pertenencia a una lista de datos bien excluidos *a priori*, o bien incluidos *a priori*.

Con carácter opcional, el procedimiento de copia automática de seguridad incluye una etapa consistente en definir al menos una parte de los parámetros de la aplicación de copia de seguridad desde un servidor de administración conectado a la red de transmisión de datos y en transmitir esa parte de parámetros a la instalación informática para la ejecución de la aplicación de copia de seguridad basándose en al menos esa parte de parámetros.

Con carácter opcional, el procedimiento de copia automática de seguridad incluye además una etapa consistente en detectar la creación en memoria o la modificación de un dato digital y, como respuesta a esta detección, en analizar ese dato digital para asignarle un coeficiente de prioridad y en ejecutar la aplicación de copia de seguridad sobre ese datos digital, en función de los parámetros y del coeficiente de prioridad que se le asigna.

La invención tiene asimismo por objeto un soporte de datos legible por un ordenador que incluye instrucciones para la puesta en práctica de un procedimiento según la invención.

La invención tiene asimismo por objeto una instalación informática para la copia automática de seguridad de datos digitales que incluye medios de almacenamiento de datos digitales, medios de análisis de los datos digitales almacenados por la instalación informática y medios de clasificación de los datos digitales analizados en una pluralidad de clases de diferentes prioridades, caracterizada por incluir además:

- una aplicación de copia de seguridad de al menos una parte de los datos digitales hacia un sistema de copia de seguridad remoto accesible por la instalación informática a través de una red de transmisión de datos,

- unos medios de extracción de información de funcionamiento de la instalación informática, incluyendo esta información de funcionamiento al menos uno de los elementos del conjunto constituido por una potencia y por una memoria disponibles, por la naturaleza y por la versión del sistema operativo de la instalación informática, por la naturaleza de las aplicaciones instaladas y ejecutables por la instalación informática, por la naturaleza y por la capacidad de una conexión de la instalación informática con la red de transmisión, por una fecha de fabricación o puesta en servicio de la instalación informática, por una frecuencia de puesta en marcha, en espera o desconexión de la instalación informática y por una organización general de directorios y por una clasificación de ficheros en esos directorios,

- unos medios de análisis de esa información, y

- unos medios de determinación de parámetros de la aplicación de copia de seguridad en función del resultado de ese análisis,

y porque la aplicación de copia de seguridad está configurada para ejecutarse sobre al menos una parte de los datos digitales, en función de los parámetros y de las clases de prioridades determinados.

Finalmente, la invención tiene asimismo por objeto un sistema informático para la copia automática de seguridad de datos digitales conservados en memoria en una instalación informática, que incluye una instalación informática

según la invención y un sistema de copia de seguridad remoto accesible por la instalación informática a través de una red de transmisión de datos.

Se comprenderá mejor la invención con la ayuda de la descripción subsiguiente, dada únicamente a título de ejemplo y hecha con referencia a los dibujos que se acompañan, en los que:

La figura 1 representa la estructura general de un sistema informático para la copia automática de seguridad de datos digitales, conforme a una forma de realización de la invención,

la figura 2 representa esquemáticamente una interfaz de una aplicación de copia de seguridad implementada en el sistema de la figura 1,

la figura 3 ilustra parcialmente el funcionamiento de la aplicación de copia de seguridad de la figura 2, para el acceso a los datos digitales, y

la figura 4 ilustra las sucesivas etapas de un procedimiento de copia automática de seguridad de datos digitales, según una forma de realización de la invención.

El sistema informático 10 representado en la figura 1 está configurado para la copia automática de seguridad de datos digitales conservados en memoria en una instalación informática 12 ó 14, hacia un sistema de copia de seguridad remoto 16.

Este sistema de copia de seguridad remoto 16 es accesible por la instalación informática 12 ó 14 a través de una red de transmisión de datos 18 tal como la red Internet.

La instalación informática 12 ó 14 puede ser de cualquier tipo, desde el simple ordenador portátil 14 a una instalación más compleja tal como la instalación 12. La instalación 12, presentada más precisamente a título de ejemplo, incluye un microordenador constituido por una unidad central de proceso 20 conectada a varios periféricos, entre ellos al menos un teclado 22, una pantalla 24 y un disco duro externo 26.

La unidad central de proceso 20 de la instalación informática 12 incluye convencionalmente (no representada) un microprocesador y espacios de almacenamiento de tipo disco duro interno, memoria RAM, ROM, y/o EEPROM, interconectados merced a un bus de comunicaciones. Estos elementos permiten constituir unos medios de almacenamiento interno 28 de datos digitales, un módulo programado 30 de extracción de información de funcionamiento de la instalación informática 12 y una aplicación de soporte lógico de análisis y de copia de seguridad 32.

La aplicación de soporte lógico 32 incluye una aplicación de copia de seguridad 34, hacia el sistema de copia de seguridad 16, de al menos una parte de los datos digitales almacenados en los medios de almacenamiento interno 28 y en el disco duro externo 26. Ésta incluye además un módulo programado 36 de análisis de esos datos digitales y de clasificación de los datos digitales analizados en una pluralidad de clases de diferentes prioridades. Finalmente, incluye un módulo programado 38 de análisis de la información de funcionamiento de la instalación informática 12 extraída por el módulo 30 y unos medios de determinación de parámetros de la aplicación de copia de seguridad 34 en función del resultado de este análisis.

El sistema de copia de seguridad remoto 16 incluye al menos un servidor de acceso 40 conectado a la red 18. Por simplicidad, en la figura 1 se representa un sólo servidor de acceso 40, pero, en realidad, resulta necesaria una pluralidad de servidores. Por otro lado, este servidor de acceso 40 se halla conectado localmente a una pluralidad de espacios de almacenamiento seguros 42, 44, 46, destinados a recibir los datos guardados mediante copia de seguridad de varias instalaciones conectadas a la red 18, tales como la instalación informática 12 ó 14.

Se va a detallar a continuación el funcionamiento de la aplicación de copia de seguridad 34, con referencia a las figuras 2 y 3.

Como está representado en la figura 2, una ejecución de la aplicación de copia de seguridad 34 puede ser seguida, e incluso gestionada, por un usuario con ayuda de una interfaz interactiva 50, visible en la pantalla 24. Esta interfaz 50 incluye varias ventanas de presentación de información, visualizables selectivamente mediante activación de pestañas 52. En el ejemplo de la figura 2, meramente ilustrativo, ésta incluye cuatro de ellas, visualizables con ayuda de pestañas tales como una pestaña de copia de seguridad de los datos, una pestaña de restauración de los datos, una pestaña de configuración de la aplicación y una pestaña de asistencia.

En el ejemplo de la figura 2, la pestaña de copia de seguridad de los datos está activada y lo que se presenta en la pantalla 24 es una ventana de presentación 54 de la copia de seguridad de los datos.

Esta ventana 54 indica, por ejemplo, en la parte superior izquierda, información que permite un seguimiento de la copia de seguridad en curso: el número (por ejemplo, 5246) de elementos seleccionados por la aplicación de copia de seguridad 34 y el correspondiente tamaño total de los datos digitales de los que se realizará una copia de seguridad (10,70 Gigabytes), la progresión de la copia de seguridad («Avance: 21,5 %») y una estimación del tiempo necesario restante («Quedan: 3 d: 11 h: 12 min»). Como variante, en una forma de realización más simple en su

puesta en práctica, sólo se presenta visualmente una indicación en tiempo real del número y del tamaño de los documentos guardados mediante copia de seguridad por el sistema de copia de seguridad 16.

Con carácter opcional, en una zona representada en el presente caso en la parte superior derecha de la ventana 54, dos botones activos 56 y 58 permiten seleccionar bien un modo de funcionamiento por defecto de la aplicación de copia de seguridad, en el que la selección de los datos digitales para la copia de seguridad se realiza automáticamente en función de los parámetros y de las clases de prioridades determinados por los módulos programados 36 y 38 (botón activo 56 seleccionado), o bien un modo de funcionamiento avanzado de la aplicación de copia de seguridad, en el que la selección puede ser modificada e incluso completamente redefinida manualmente por el usuario (botón activo 58 seleccionado).

Con carácter opcional, en una zona representada en el presente caso en la parte derecha de la ventana 54, los elementos seleccionados se representan por categorías y la información que permite el seguimiento de la copia de seguridad se retoma al menos parcialmente en cada categoría. La pertenencia de un elemento, es decir, de un dato digital identificado mediante un fichero, a una categoría dada es determinada, por ejemplo automáticamente, por el módulo programado de análisis 36 con ayuda del tipo del dato digital identificado por la extensión del fichero correspondiente. También puede ser determinada automáticamente con ayuda de datos suplementarios asociados al fichero correspondiente, comúnmente conocidos como metadatos, o con ayuda de la localización del fichero en un árbol de directorios de la instalación informática 12. Así, una primera categoría, denominada «categoría 1», concierne a los documentos de ofimática procedentes de tratamientos de textos, hojas de cálculo u otros, reconocibles por extensiones tales como *.doc, *.xls, *.ppt, etc. Una segunda categoría, denominada «categoría 2», concierne a los documentos de tipo foto o vídeo reconocibles por extensiones tales como *.jpg, *.tiff, *.bmp, *.mpg, *.avi, etc. Una tercera categoría, denominada «categoría 3», concierne a los documentos de tipo audio reconocibles por extensiones tales como *.wav, *.au, etc. Una cuarta categoría, denominada «categoría 5», concierne a los documentos de mensajería, contactos y favoritos tales como el contenido de bandejas de entrada/salida de correos electrónicos. Finalmente, una quinta categoría, denominada «categoría 4», concierne a los demás documentos, aquellos que no corresponden a ninguna de las cuatro anteriores categorías.

Estas cinco categorías, de la categoría 1 a la categoría 5, están ordenadas, por ejemplo, de la más importante a la menos importante, propiedad ésta que debe ser tomada en cuenta por la aplicación de copia de seguridad 34 en su ejecución.

Por otro lado, los datos digitales en el seno de una misma categoría pueden hallarse jerarquizados por orden de importancia en varias clases de diferentes prioridades, según su tipo u otros criterios, en orden a afinar la clasificación de los datos y, en consecuencia, la estrategia de copia de seguridad.

Finalmente, con carácter opcional, un botón activo 60 situado, en el ejemplo de la figura 2, en la parte inferior derecha de la ventana 54, permite al usuario suspender temporalmente la ejecución de la aplicación de copia de seguridad 34.

La figura 3 ilustra una forma de realización en la que el funcionamiento de la aplicación de copia de seguridad 34 está concebido para precaverse de errores llamados «fatales». Un error fatal se produce, por ejemplo, cuando el acceso a un dato por parte de una aplicación entra en conflicto con la acción de otra aplicación sobre ese dato o se ve perturbado por un mal funcionamiento de la instalación informática. En tal caso, la aplicación que trata de acceder al dato es interrumpida bruscamente. Para evitar someter la aplicación de copia de seguridad 34 a esa clase de riesgo en esta forma de realización, ésta no accede directamente a los datos de los que se realizará una copia de seguridad. Ésta ejecuta otra aplicación 34', llamada aplicación de lectura, que accede en su lugar a los datos y se los transmite.

Así, en una primera etapa 100, la aplicación de copia de seguridad 34, que se ejecuta en la instalación informática 12, inicia la aplicación de lectura 34' para acceder a datos digitales de los que se realizará una copia de seguridad, almacenados indistintamente en el disco duro externo 26 o en los medios de almacenamiento interno 28.

En una siguiente etapa 102, se produce un error fatal Err en el acceso a un dato digital por parte de la aplicación de lectura 34'. La ejecución de la aplicación de lectura 34' queda entonces interrumpida bruscamente en una etapa 104.

Esta interrupción de ejecución es detectada por la aplicación de copia de seguridad 34 que, en una etapa 106, inicia nuevamente la aplicación de lectura 34' para acceder a datos digitales de los que se realizará una copia de seguridad, como en la etapa 100. Consecuentemente, el error fatal Err no ha perturbado la ejecución de la aplicación de copia de seguridad 34 que, con ello, queda protegida.

Además, la aplicación de copia de seguridad 34, cuando detecta la interrupción de ejecución debida al error fatal Err, puede excluir temporalmente el dato o el área de datos que ha causado esa interrupción, para reanudar la copia de seguridad en la etapa 106 sobre otros datos que los que se realizará una copia de seguridad. En el final de la ejecución, cuando ha realizado una copia de seguridad de todos los demás datos, la aplicación de copia de seguridad 34 puede ocuparse entonces de nuevo de los datos causantes del error fatal.

Con carácter opcional, la aplicación de copia de seguridad 34 genera, en su ejecución, un fichero de seguimiento de

las operaciones de copia de seguridad que se almacena, por ejemplo, en el disco duro interno de la instalación informática 12. Así, en caso de interrupción repentina de la aplicación por el problema que sea, ésta puede reanudar en el lugar donde ha quedado interrumpida en virtud de este fichero de seguimiento.

También con carácter opcional, la ejecución de la aplicación de análisis y de copia de seguridad 32, susceptible de consumir una parte importante del tiempo de cálculo de la instalación informática 12, está sometida a un regulador de tiempo de cálculo consumido que incluye las dos siguientes funciones:

- una función de observación de la potencia de cálculo consumida en cada instante por la aplicación 32, y

- una función de regulación de la cantidad de operaciones realizadas por la aplicación 32.

A continuación se va a detallar el funcionamiento de los módulos programados 30, 36 y 38.

Teniendo presente que los datos digitales de la instalación informática se almacenan en forma de ficheros, la misión del módulo de análisis y de clasificación 36 de los datos digitales susceptibles de ser guardados mediante copia de seguridad se desglosa como sigue:

- en primer lugar tiene que catalogar un conjunto de ficheros de la instalación informática susceptibles de ser guardados mediante copia de seguridad y extraer automáticamente información acerca de esos ficheros,

- a continuación tiene que analizar esa información extraída para asociar cada fichero con una clase de prioridad dada, para, eventualmente, excluir *a priori* determinados ficheros de la copia de seguridad o para, antes bien, considerar algunos de ellos como vitales.

La información pertinente acerca de un fichero de dato digital y extraída por el módulo programado 36 incluye al menos uno de los elementos de la siguiente lista:

- información acerca de la naturaleza del fichero, que viene dada por la extensión del fichero y/o por sus atributos (por atributos de un fichero, se entiende fichero de sólo lectura o no, fichero oculto o no, fichero listo para archivar o no),

- el tamaño del fichero,

- las fechas de creación, de última modificación y/o de último acceso al fichero, que caracterizan la utilización del fichero y, por tanto, su importancia,

- los metadatos asociados al fichero, que pueden haber sido introducidos manualmente por el usuario o automáticamente por la aplicación que ha generado ese fichero (por ejemplo, datos de gestión digital de los derechos asociados al fichero),

- la naturaleza del directorio en el que se encuentra el fichero, pudiendo haberse definido una lista predeterminada de directorios para identificar la particular importancia de algunos directorios,

- la relación entre el fichero en cuestión y los demás ficheros del directorio en el que éste se encuentra, lo que permite decidir si un fichero *a priori* sin importancia pero almacenado en el mismo directorio que ficheros importantes pasa entonces a ser un fichero importante,

- la relación entre el fichero y la base de registro del sistema operativo de la instalación informática 12, dicho de otro modo, la existencia de una asociación entre el fichero y una aplicación de soporte lógico de la instalación para leerlo y/o ejecutarlo,

- la pertenencia del fichero a una lista de ficheros excluidos *a priori*, tales como los ficheros temporales o los ficheros del sistema.

El análisis de la información extraída para asociar cada fichero con una clase de prioridad dada se puede realizar con ayuda de un conjunto de reglas predeterminadas que permiten estimar un coeficiente para cada fichero, que determinará su pertenencia a una clase, o excluir *a priori* un fichero. Este conjunto incluye, por ejemplo, al menos una, o una combinación, de las siguientes reglas:

- las extensiones de los ficheros van clasificadas *a priori* según un orden de prioridad; por ejemplo, como anteriormente se ha visto, las extensiones de tipo ofimática (*.doc, *.xls, *.ppt, etc.) son prioritarias y llevan asignado un elevado coeficiente de prioridad, luego vienen las extensiones de tipo foto o vídeo (*.jpg, *.tiff, *.bmp, *.mpg, *.avi, etc.), luego las extensiones de tipo audio (*.wav, *.au), etc.,

- en lo que a los atributos se refiere, los ficheros ocultos, archivados o de sólo lectura quedan excluidos *a priori* de la copia de seguridad, o al menos su coeficiente de prioridad se ve considerablemente reducido,

- si el tamaño del fichero no queda situado entre un mínimo y un máximo predeterminados, el fichero queda excluido *a priori* de la copia de seguridad, o al menos su coeficiente de prioridad se ve considerablemente reducido,

- si el fichero ha sido creado o modificado recientemente, o es leído con frecuencia, su coeficiente de prioridad se ve incrementado,

- queda definida *a priori* como importante una lista predeterminada de directorios y/o algunos directorios son asociados con coeficientes de prioridad predeterminada,

- si el fichero no se considera como tal importante al primer análisis, pero se halla situado en un directorio en el que se encuentran ficheros importantes, su coeficiente de prioridad se ve incrementado,

- si el fichero no está asociado con ninguna aplicación, según la base de registro del sistema operativo de la instalación informática 12, su coeficiente de prioridad se ve reducido,

- los ficheros tales como los ficheros temporales de los navegadores por Internet o los ficheros del sistema operativo quedan excluidos.

La extracción de la información relativa a los ficheros susceptibles de ser guardados mediante copia de seguridad y su análisis permiten la clasificación de los ficheros en varias clases de diferentes prioridades. Esta jerarquía de clases, combinada eventualmente con la jerarquía de las antedichas categorías 1 a 5, es utilizada a continuación por la aplicación de copia de seguridad 34 para definir sus prioridades de copia de seguridad, o incluso efectuar una selección, según las circunstancias.

Las circunstancias en las que se ejecuta la aplicación de copia de seguridad y, en consecuencia, la elección de una estrategia de copia de seguridad y, por tanto, de parametrización de la aplicación de copia de seguridad 34 las determinan los módulos programados 30 y 38.

El módulo de extracción 30 de información de funcionamiento de la instalación informática 12 extrae, por ejemplo, al menos una de las siguientes informaciones:

- la edad de la instalación informática 12 (fecha de fabricación o de puesta en servicio),

- la naturaleza y la versión del sistema operativo,

- la naturaleza de las aplicaciones utilizadas por la instalación informática y su versión (soportes lógicos de mensajería, soporte lógico antivirus y cortafuegos, etc.),

- la potencia y la memoria disponibles,

- la naturaleza y la capacidad de la conexión de la instalación informática con la red 18,

- la frecuencia de puesta en marcha, en espera o desconexión de la instalación informática 12,

- la organización general de los directorios y la clasificación de los ficheros en esos directorios.

Basándose en la información extraída por el módulo programado 30, el módulo de análisis 38 efectúa un análisis, por ejemplo en función de reglas predefinidas, tales como:

- si la instalación informática 12 está obsoleta y reducidas sus capacidades, o si son escasas la potencia y la memoria disponibles, o si el ancho de banda de la conexión con la red 18 es reducido, elegir una estrategia de copia de seguridad degradada, en la que sólo se seleccionan las clases más importantes según un umbral por determinar y, eventualmente, avisar de ello al usuario de la instalación informática 12 por correo electrónico,

- si se trata de una primera copia de seguridad de los datos digitales de la instalación informática 12, elegir asimismo la estrategia de copia de seguridad degradada, eventualmente comprimiendo una parte de los datos guardados mediante copia de seguridad y, seguidamente, iniciar de nuevo la aplicación de copia de seguridad 34 una segunda vez, sustituyendo los datos guardados mediante copia de seguridad en forma comprimida por esos mismos datos en su formato y tamaño originales,

- adaptar la ejecución de la aplicación 34 a la frecuencia de puesta en marcha, en espera o desconexión de la instalación informática 12,

- ejecutar la aplicación de copia de seguridad 34 como tarea de fondo sin perturbar el funcionamiento de la instalación informática y detectar regularmente, e incluso en tiempo real, las modificaciones o creaciones de ficheros para realizar con prioridad una copia de seguridad de los mismos.

Basándose en este análisis, la aplicación de copia de seguridad 34 es parametrizada automáticamente por el módulo 38, en orden a definir una estrategia de copia de seguridad.

También se puede prever una matriz de potenciales problemas detectables y de soluciones predefinidas de parametrización para completar el análisis y afinar la estrategia de copia de seguridad.

De este modo, se pueden definir, a título de ejemplo, las siguientes situaciones características:

1- caso nominal de utilización: instalación informática 12 funcionando tres horas al día;

2- caso especial de utilización: instalación informática 12 funcionando todo el tiempo, es decir, nunca apagada en utilización corriente;

3- caso crítico de utilización: aplicación de copia de seguridad 34 ejecutada manualmente y raramente, o instalación informática 12 funcionando 2 horas al mes, o cuenta de copia de seguridad asociada a la instalación 12 en el sistema de copia de seguridad 16 vacía desde hace demasiado tiempo;

4- bloqueo o desconexión brusca de la aplicación de análisis y de copia de seguridad 32 durante la fase de análisis de los ficheros susceptibles de ser guardados mediante copia de seguridad o de transferencia de los ficheros que se van a descargar;

5- fase de análisis de los ficheros susceptibles de ser guardados mediante copia de seguridad demasiado larga;

6- copia de seguridad contrariada por otras aplicaciones (antivirus demasiado limitativo, derechos insuficientes);

7- conexión a la red 18 de mala calidad;

8- cuenta de copia de seguridad asociada a la instalación 12 en el sistema de copia de seguridad 16 vacía desde hace demasiado tiempo;

9- tiempo de transferencia de los ficheros de los que se realizará una copia de seguridad demasiado largo;

10- problema desconocido;

11- plan de emergencia: ningún fichero transferido a la cuenta de copia de seguridad asociada a la instalación 12 pasada una semana de la activación de la aplicación de copia de seguridad 34.

Ante estas situaciones características se pueden prever, a título de ejemplo, las siguientes reglas de parametrización:

A - si se detecta un problema durante la fase de análisis de los ficheros susceptibles de ser guardados mediante copia de seguridad o de transferencia de los ficheros que se van a descargar (demasiado largo, bloqueo o desconexión brusca), se excluye temporalmente la fuente de dato implicada para permitir la continuidad de la copia de seguridad de los demás datos;

B - parametrizar la aplicación de copia de seguridad 34 para que funcione de acuerdo con la forma de realización ilustrada por la figura 3;

C - guardar, en un fichero de seguimiento de copia de seguridad, el resultado de la anterior acción para poder reanudarlo como consecuencia de una ocasional desconexión brusca;

D - parametrizar la aplicación de copia de seguridad 34 para que funcione en un modo muy degradado en el que no se realiza ningún análisis de los ficheros susceptibles de ser guardados mediante copia de seguridad, sino que en él sólo se realiza una copia de seguridad de determinados directorios *a priori* considerados críticos;

E - prever una gestión de conectividad encaminada a avisar lo mejor posible a la aplicación de copia de seguridad 34 de ocasionales problemas de red;

F - optimizar la velocidad de la fase de análisis;

G - agrupar en lotes los ficheros pequeños de los que se realizará una copia de seguridad;

H - comprimir algunos tipos de ficheros, por ejemplo las imágenes;

I - clasificar los ficheros por orden de importancia;

J - prever un seguimiento de actividad claro y sintético, un seguimiento completo y un seguimiento del entorno en el transcurso de ejecución de la aplicación de copia de seguridad 34;

K - reanudación de la fase de análisis de los ficheros susceptibles de ser guardados mediante copia de seguridad o de transferencia de los ficheros que se van a descargar en la última posición;

L - definir una preselección y/o una exclusión de algunos elementos para la primera copia de seguridad;

M - realizar temporalmente una copia de seguridad de imágenes reducidas;

N - parametrizar la aplicación de copia de seguridad 34 para que funcione en un modo en el que quede limitado el

tiempo de la fase de análisis de los ficheros susceptibles de ser guardados mediante copia de seguridad, en orden a comenzar rápidamente una copia de seguridad, pudiendo ser reanudado en adelante el análisis para efectuar una copia de seguridad más completa.

La matriz puede tomar entonces la siguiente forma:

	A	B	C	d	E	F	G	H	I	J	K	L	M	N
1	X		X			X	X	X	X		X			X
2		X												
3				X			X	X	X			X	X	X
4	X	X	X								X			
5	X		X			X					X			X
6										X				
7					X								X	
8				X			X	X	X		X			X
9							X	X					X	
10										X				
11											X	X		

El funcionamiento del módulo de análisis 38 queda presentado anteriormente como basado en un conjunto de reglas y, por tanto, puede ser implementado en forma de un sistema experto. Pero, como variante, también cabe la posibilidad de contemplar una implementación en forma de una red de neuronas, del tipo perceptrón multicapa, en el que los datos de entrada son los datos extraídos por el módulo programado 30 y los datos de salida son los parámetros de la aplicación de copia de seguridad 34. En este último caso, no está predefinido necesariamente un conjunto de reglas, sino que se construye mediante parametrización automática de la red de neuronas en fases de aprendizaje.

Como complemento de la parametrización realizada por el módulo de análisis 38, se puede autorizar a distancia un acceso a los parámetros de la aplicación de copia de seguridad 34 y, más generalmente, a los de la aplicación de análisis y de copia de seguridad 32, desde el servidor de copia de seguridad 40 o cualquier otro servidor de administración. Se prevén entonces autorizaciones específicas de acceso, para permitir a un administrador del sistema de copia de seguridad 16 acceder a los parámetros de varias aplicaciones de análisis y de copia de seguridad implementadas en varias instalaciones informáticas tales como las instalaciones 12 y 14.

En virtud de estas autorizaciones específicas, el administrador se halla en disposición de regular el tráfico de datos digitales entrantes y de los que se realizará una copia de seguridad en la pluralidad de espacios de almacenamiento seguros 42, 44, 46. De este modo puede, para evitar cualquier sobrecarga del sistema de copia de seguridad 16, en particular en caso de conexiones simultáneas demasiado numerosas, controlar a distancia la estrategia de copia de seguridad de la aplicación 32 de la instalación informática 12 y de las demás aplicaciones. Dicho de otro modo, puede dictar una gestión de las prioridades que permite que se realice una copia de seguridad con prioridad de los ficheros más importantes en las instalaciones más importantes. Esta intervención autorizada del administrador es, obviamente, transparente para el usuario de la instalación informática 12. La intervención del administrador en la parametrización a distancia se puede hacer para el conjunto de las instalaciones gestionadas por el sistema de copia de seguridad, sólo para una parte de ellas, o para una sola instalación informática.

A continuación se van a describir, con referencia a la figura 4, las sucesivas etapas de un procedimiento de copia de seguridad, puesto en práctica por el sistema 10 ilustrado en la figura 1 según una forma de realización de la invención.

En una primera etapa de inicialización 200, la aplicación de análisis y de copia de seguridad 32 inicia la ejecución de los módulos programados 30, 36 y 38.

Esta primera etapa viene, pues, seguida, por una parte, por dos etapas 202 y 204 de extracción y de análisis de la información de funcionamiento de la instalación informática 12 para determinar los parámetros de la aplicación de copia de seguridad 34 en función del resultado de este análisis (función de los módulos 30 y 38) y, por otra parte, por dos etapas 206 y 208 de análisis de los datos digitales conservados en memoria y de clasificación de los datos

digitales analizados en una pluralidad de clases de diferentes prioridades (función del módulo 36).

En la etapa de extracción 202, el módulo programado 30 se ejecuta de acuerdo con cuanto se ha descrito anteriormente y suministra la información extraída al módulo programado 38.

En la etapa de análisis y de parametrización 204, el módulo programado 38 se ejecuta de acuerdo con cuanto ha sido descrito anteriormente y determina los parámetros de funcionamiento de la aplicación de copia de seguridad 34. En esta etapa, pero también a lo largo de toda la puesta en práctica del procedimiento de copia de seguridad, como también se ha indicado, el administrador del sistema de copia de seguridad 16 puede intervenir en la definición de los parámetros, en orden a afinar la estrategia de copia de seguridad, en particular en función de exigencias exteriores a la instalación informática 12. También es en esta etapa cuando el módulo de análisis 38 puede decidir imponer una copia de seguridad en modo degradado. Finalmente, en la etapa 204, se puede descargar desde el servidor de copia de seguridad 40 un fichero, llamado fichero «cache», que retoma una estructura en árbol de los datos de la instalación 12 ya guardados mediante copia de seguridad en el sistema de copia de seguridad 16, que además incluye, eventualmente, también los atributos de los ficheros correspondientes, en particular si se han modificado datos en el sistema de copia de seguridad 16 sin intervención de la aplicación de análisis y de copia de seguridad 32. Este fichero cache permite limitar la utilización del ancho de banda de la instalación informática 12 ante la red 18 y, por tanto, acelerar el tratamiento de la copia de seguridad.

En la etapa de análisis 206, el módulo de análisis y de clasificación 36 de los datos cataloga el conjunto de los ficheros de la instalación informática 12 susceptibles de ser guardados mediante copia de seguridad y extrae automáticamente información acerca de esos ficheros de acuerdo con cuanto se ha descrito anteriormente.

En la etapa siguiente de clasificación 208, éste analiza esa información extraída para asociar cada fichero con una clase de prioridad dada para, eventualmente, excluir *a priori* determinados ficheros de la copia de seguridad o para, antes bien, considerar algunos de ellos como vitales, de acuerdo con cuanto se ha descrito anteriormente.

Las etapas 206 y 208 pueden llevar mucho tiempo. Así, según una forma de realización de la invención, estas etapas se realizan por franjas temporales. Dicho de otro modo, al cabo de un cierto tiempo predeterminado, si el análisis y la clasificación no han terminado, se pasa con todo a una etapa de activación 210 de la aplicación de copia de seguridad 34, a expensas de volver más tarde a las etapas 206 y 208 para proseguir el análisis y la clasificación de los datos restantes.

En la etapa 210, la ejecución de la aplicación de copia de seguridad 34 se activa sobre al menos una parte de los datos digitales de la instalación informática 12, en función de los parámetros y de las clases de prioridad determinados en las etapas 204 y 208.

En esta etapa, la aplicación de copia de seguridad 34 transmite cada dato digital del que se realizará una copia de seguridad, según las reglas de prioridades y/o de selección establecidas por los módulos programados 36 y 38.

En una forma de realización, ésta efectúa además una prueba de regulación de carga en función de la carga del sistema de copia de seguridad 16 antes de transmitir cada dato o grupo de datos. En tal caso, el servidor de copia de seguridad 40 transmite regularmente a la instalación 12 una información acerca de su carga corriente, que permite por ejemplo definir cinco niveles de carga: «tranquilo», «normal», «cargado», «máximo», «rechazo», asociados cada uno de ellos a una puntuación S1 predeterminada. El dato del que se realizará una copia de seguridad se asocia entonces a su vez a una puntuación S2 calculada en función del coeficiente de prioridad C1 de la clase en la que ha sido ubicado en la etapa 208, pero ponderada por otros coeficientes dictados por el administrador del sistema de copia de seguridad, tales como por ejemplo:

- un coeficiente de usuario C2, que toma un valor alto cuando se trata de una primera copia de seguridad para la instalación 12 y un valor bajo en caso contrario,

- un coeficiente de importancia del dato C3, que puede ser calculado según un procedimiento similar al utilizado por el módulo programado 36, pero por el administrador,

- un coeficiente de actualización C4 del dato, que toma un valor alto cuando se trata de una primera copia de seguridad para ese dato y un valor bajo en caso contrario.

En la práctica, S2 se puede obtener mediante la fórmula S2 = C1 . (C2 + C3 + C4) y compararse seguidamente con S1. Si S2 es mayor o igual que S1, el dato es transmitido al servidor de copia de seguridad o, en caso contrario, no es transmitido y se deja de lado para otra copia de seguridad.

En una forma de realización, la aplicación de copia de seguridad 34 efectúa otra prueba sobre el dato del que se realizará una copia de seguridad, antes de transmitirlo efectivamente al servidor de copia de seguridad 40. Ésta realiza un cálculo de firma convencional sobre ese dato y transmite esta firma al servidor de copia de seguridad 40. Este último compara esa firma con las de los datos que ya están almacenados en sus espacios de almacenamiento seguros 42, 44, 46, inclusive para otras instalaciones distintas a la instalación 12. Si un dato ya presente en el sistema de almacenamiento 16 tiene la misma firma que el dato del que se realizará una copia de seguridad para la

instalación 12, el servidor de copia de seguridad 40 sólo almacenará una referencia a ese dato para la instalación 12 y el dato no tiene necesidad de ser transmitido. En caso contrario, el dato del que se realizará una copia de seguridad es transmitido. Esta forma de realización permite aliviar la carga del sistema de copia de seguridad 16, evitando redundancias de ficheros en los espacios de almacenamiento seguros 42, 44 y 46.

Cuando termina la etapa 210, se pasa a una etapa de prueba 212 para comprobar si han sido tratados todos los datos susceptibles de ser guardados mediante copia de seguridad, o si aún quedan datos por analizar (cuando las etapas 206 y 208 se realizan por franjas, o cuando la copia de seguridad se ha realizado en un modo degradado, o como consecuencia de una primera copia de seguridad, o cuando unos datos han originado errores fatales, etc.). Si aún se tienen que analizar datos, se vuelve a la etapa 206 o, en caso contrario, se pasa a una etapa 214.

Cuando la copia de seguridad se realiza por franjas, es posible aplazar para más tarde la copia de seguridad de algunos datos, en particular presentes y no modificados desde un cierto tiempo en la instalación informática 12.

Cabe así la posibilidad de definir una prioridad decreciente de los datos en función de su antigüedad, ascendiendo progresivamente con el tiempo las sucesivas copias de seguridad.

La etapa 214 consiste en esperar un evento, por ejemplo una señal de reloj para una reinicialización de la aplicación de análisis y de copia de seguridad 32 (evento A) o la detección de la creación en memoria o de la modificación de un dato susceptible de ser guardado mediante copia de seguridad (evento B).

Cuando se detecta un evento, se pasa a una etapa de prueba 216 para identificar ese evento. El evento A provoca un retorno a la etapa 200, mientras que el evento B provoca el análisis del dato digital creado o modificado, para asignarle un coeficiente de prioridad, y luego un retorno a la etapa 210, para ejecutar la aplicación de copia de seguridad 34 sobre ese dato digital, en función de los parámetros y del coeficiente de prioridad que se le asigna.

En una forma de realización de la invención, cuando la instalación informática 12 realiza su primera copia de seguridad hacia el sistema de copia de seguridad 16, la etapa inicial 200 viene inmediatamente seguida por la etapa de ejecución de la aplicación de copia de seguridad 210 sin ejecución de los módulos programados 30, 36 y 38, como se indica mediante la flecha en punteado en la figura 4. La copia de seguridad se inicia en forma de una copia de seguridad rápida para transmitir tan sólo un cierto número limitado de datos digitales *a priori* considerados como vitales, tales como los datos relativos a una libreta de direcciones de una aplicación de mensajería electrónica, los favoritos y, por ejemplo, los diez últimos documentos leídos.

Resulta claramente manifiesto que un sistema de copia de seguridad de datos tal como el presentado con referencia a las figuras 1 a 4 permite facilitar la copia de seguridad de datos desde el punto de visto del usuario, puesto que aquél tan sólo requiere muy pocas intervenciones de su parte.

Adviértase también que la invención no queda limitada a las formas de realización anteriormente descritas.

En particular, la instalación informática no queda limitada a las dos estructuras ilustradas en la figura 1. Como variante, la instalación informática puede estar constituida por una pluralidad de ordenadores y/u otros dispositivos susceptibles de almacenar datos enlazados entre sí en red local.

Como variante, también, otras reglas distintas a las presentadas pueden afinar las etapas de parametrización de la aplicación de copia de seguridad y de análisis de los datos, con miras a su clasificación.

REIVINDICACIONES

1. Procedimiento de copia automática de seguridad de datos digitales conservados en memoria (26, 28) en una instalación informática (12, 14) hacia un sistema de copia de seguridad (16), que incluye la etapa consistente en analizar (206) los datos digitales conservados en memoria (26, 28) y clasificar (208) los datos digitales analizados en una pluralidad de clases de diferentes prioridades, **caracterizándose** el procedimiento **porque** el sistema de copia de seguridad (16) es remoto y accesible por la instalación informática (12, 14) a través de una red de transmisión de datos (18) y **porque** además incluye las etapas consistentes en:

- extraer y analizar (202) información de funcionamiento de la instalación informática (12, 14), incluyendo esta información de funcionamiento al menos uno de los elementos del conjunto constituido por una potencia y por una memoria disponibles, por la naturaleza y por la versión del sistema operativo de la instalación informática, por la naturaleza de las aplicaciones instaladas y ejecutables por la instalación informática, por la naturaleza y por la capacidad de una conexión de la instalación informática con la red de transmisión (18), por una fecha de fabricación o puesta en servicio de la instalación informática, por una frecuencia de puesta en marcha, en espera o desconexión de la instalación informática y por una organización general de los directorios y por una clasificación de ficheros en esos directorios,

- determinar (204) unos parámetros de una aplicación de copia de seguridad (34) de datos hacia el sistema de copia de seguridad (16), en función del resultado de ese análisis, y

- ejecutar (210) la aplicación de copia de seguridad (34) sobre al menos una parte de los datos digitales, en función de los parámetros y de las clases de prioridades determinados.

2. Procedimiento de copia automática de seguridad de datos digitales según la reivindicación 1, en el que los parámetros de la aplicación de copia de seguridad (34) incluyen al menos uno de los elementos del conjunto constituido por un límite de potencia consumida permitido para la aplicación de copia de seguridad, por una opción de ejecución de la aplicación de copia de seguridad en modo degradado y por criterios de selección de los datos digitales de los que se realizará una copia de seguridad.

3. Procedimiento de copia automática de seguridad de datos digitales según la reivindicación 1 ó 2, en el que los criterios de selección y/o la clasificación de los datos digitales en clases de diferentes prioridades son referentes al menos a la naturaleza de los datos digitales.

4. Procedimiento de copia automática de seguridad de datos digitales según la reivindicación 3, en el que los criterios de selección y/o la clasificación de los datos digitales en clases de diferentes prioridades son referentes además a al menos uno de los elementos del conjunto constituido por su tamaño, por sus fechas de creación, de última modificación y/o de último acceso, por datos suplementarios de información que llevan asociada, por un directorio en el que aquellos están situados, por una relación entre esos datos y una base de registro de un sistema operativo de la instalación informática (12, 14) y por una pertenencia a una lista de datos bien excluidos *a priori*, o bien incluidos *a priori*.

5. Procedimiento de copia automática de seguridad de datos digitales según una cualquiera de las reivindicaciones 1 a 4, que incluye una etapa consistente en definir al menos una parte de los parámetros de la aplicación de copia de seguridad (34) desde un servidor de administración (40) conectado a la red de transmisión de datos (18) y en transmitir esa parte de parámetros a la instalación informática (12, 14) para la ejecución de la aplicación de copia de seguridad (34) basándose en al menos esa parte de parámetros.

6. Procedimiento de copia automática de seguridad de datos digitales según una cualquiera de las reivindicaciones 1 a 4, que incluye además una etapa (214) consistente en detectar la creación en memoria (26, 28) o la modificación de un dato digital y, como respuesta a esta detección, en analizar ese dato digital para asignarle un coeficiente de prioridad y en ejecutar (210) la aplicación de copia de seguridad (34) sobre ese datos digital, en función de los parámetros y del coeficiente de prioridad que se le asigna.

7. Soporte de datos legible por un ordenador que incluye instrucciones para la puesta en práctica de un procedimiento según una cualquiera de las reivindicaciones 1 a 6.

8. Instalación informática (12, 14) para la copia automática de seguridad de datos digitales, que incluye unos medios de almacenamiento (26, 28) de datos digitales, unos medios de análisis (36) de los datos digitales almacenados por la instalación informática y unos medios de clasificación (36) de los datos digitales analizados en una pluralidad de clases de diferentes prioridades, **caracterizada por** incluir además:

- una aplicación de copia de seguridad (34) de al menos una parte de los datos digitales hacia un sistema de copia de seguridad remoto (16) accesible por la instalación informática (12, 14) a través de una red de transmisión de datos (18),

- medios de extracción (30) de información de funcionamiento de la instalación informática (12, 14), incluyendo esta información de funcionamiento al menos uno de los elementos del conjunto constituido por una potencia y por una

memoria disponibles, por la naturaleza y por la versión del sistema operativo de la instalación informática, por la naturaleza de las aplicaciones instaladas y ejecutables por la instalación informática, por la naturaleza y por la capacidad de una conexión de la instalación informática con la red de transmisión (18), por una fecha de fabricación o puesta en servicio de la instalación informática, por una frecuencia de puesta en marcha, en espera o desconexión de la instalación informática y por una organización general de directorios y por una clasificación de ficheros en esos directorios,

- medios de análisis (38) de esa información, y

- medios de determinación (38) de parámetros de la aplicación de copia de seguridad (34) en función del resultado de ese análisis,

y **porque** la aplicación de copia de seguridad (34) está configurada para ejecutarse sobre al menos una parte de los datos digitales, en función de los parámetros y de las clases de prioridades determinados.

9. Sistema informático (10) para la copia automática de seguridad de datos digitales conservados en memoria (26, 28) en una instalación informática (12, 14), que incluye una instalación informática (12, 14) según la reivindicación 8 y un sistema de copia de seguridad remoto (16) accesible por la instalación informática (12, 14) a través de una red de transmisión de datos (18).

Figura 1

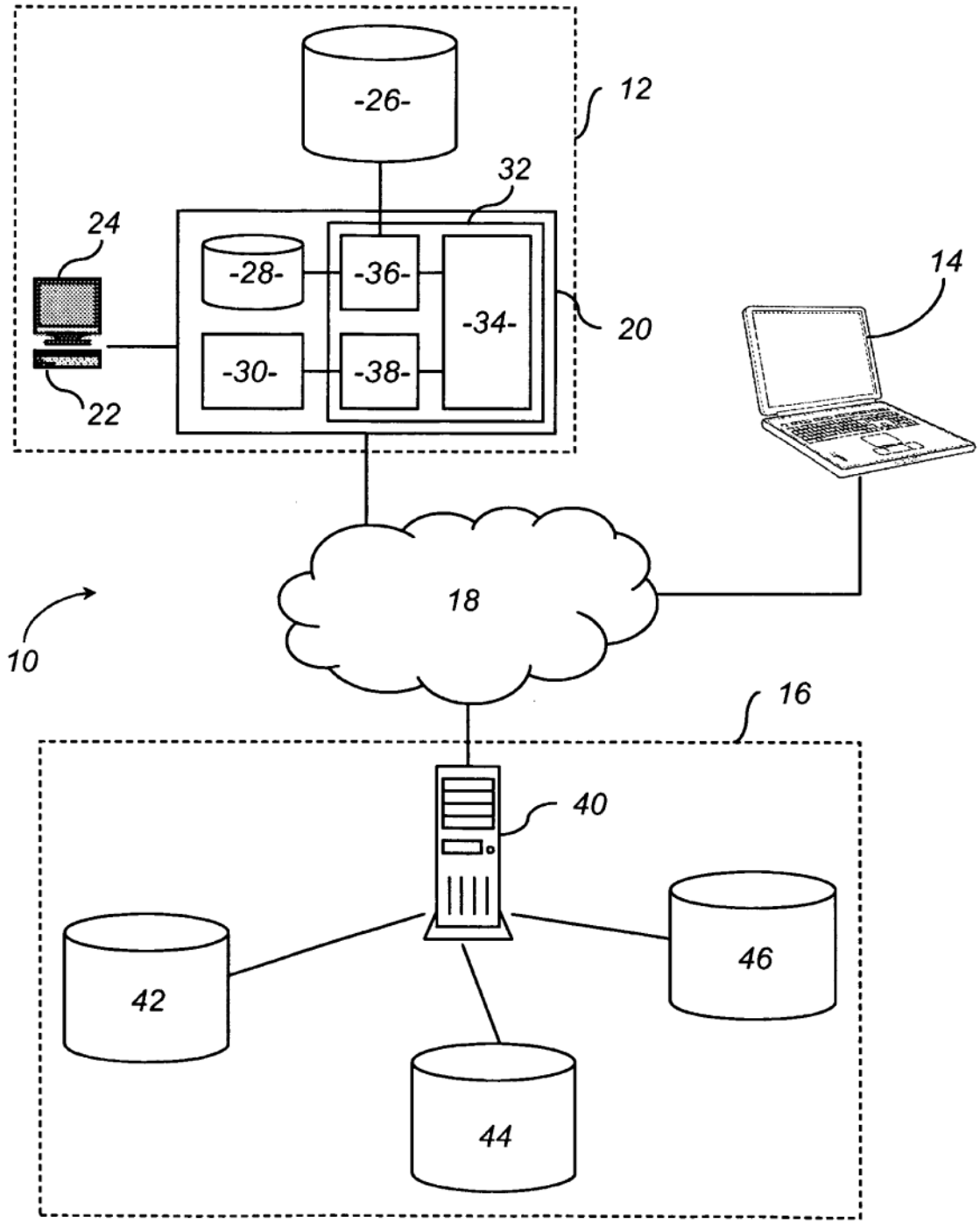

Figura 2

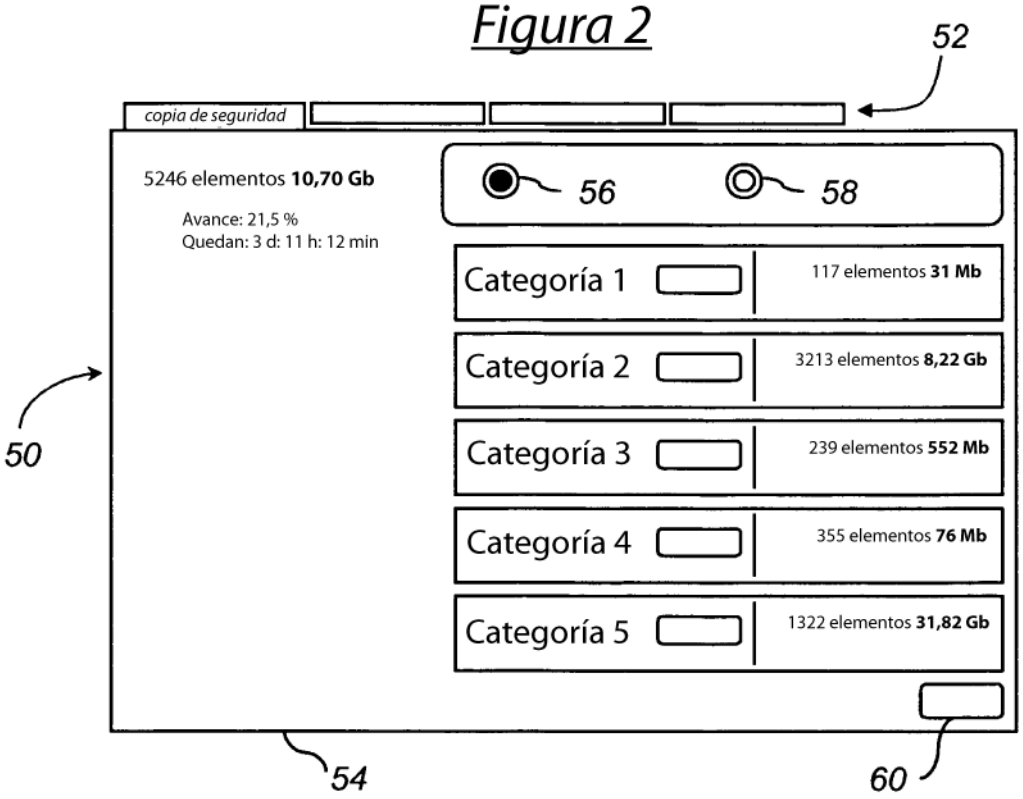

Figura 3

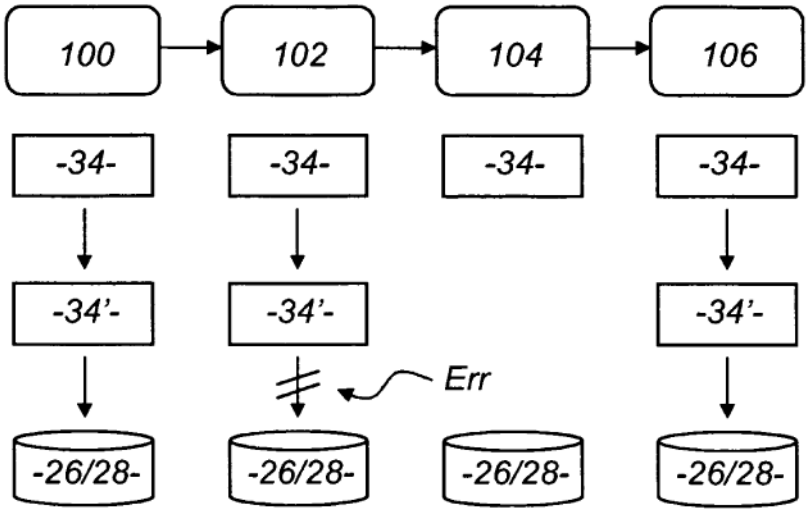

Figura 4