(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 762 905**

(51) Int. CI.:

G06F 16/11 (2009.01)
G06F 21/64 (2013.01)
H04L 29/06 (2006.01)
G06F 21/62 (2013.01)
G06F 21/60 (2013.01)
H04L 9/14 (2006.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **08.06.2016 PCT/IB2016/053357**

(87) Fecha y número de publicación internacional: **15.12.2016 WO16199034**

(96) Fecha de presentación y número de la solicitud europea: **08.06.2016 E 16733205 (5)**

(97) Fecha y número de publicación de la concesión europea: **07.08.2019 EP 3304409**

(54) Título: **Aseguramiento de datos digitales**

(30) Prioridad:

08.06.2015 FR 1501179

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
26.05.2020

(73) Titular/es:

RIETSCH, JEAN-MARC, MARIE-JOSEPH (100.0%)
1015 Boulevard du Maréchal Leclerc
06360 Eze, FR

(72) Inventor/es:

RIETSCH, JEAN-MARC, MARIE-JOSEPH

(74) Agente/Representante:

SUGRAÑES MOLINÉ, Pedro

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

Aseguramiento de datos digitales

La presente invención se refiere al campo del aseguramiento de los datos digitales durante su almacenamiento o archivo.

La invención concierne, de manera más particular, a un procedimiento que permite, por una parte, aumentar el aseguramiento del almacenamiento y archivo de datos digitales desde cualquier procedencia y, por otra parte, debido al diseño mismo de dicho procedimiento, modular el nivel de seguridad que se puede seleccionar en función de la naturaleza y del uso de dichos datos digitales.

Además de los dispositivos conocidos de cifrado de datos, existen hoy en día varias lógicas de almacenamiento asegurado de datos de la información digital, entre las cuales se pueden mencionar:

- las tecnologías RAID (por sus siglas en inglés de *Redundant Array of Independant Disks*, matriz redundante de discos independientes) que consiste en almacenar un fichero, cortado en trozos, en diferentes discos siguiendo varios niveles de corte y seguridad. De este modo, se conocen diferentes tipos de almacenamientos RAID y se distinguen en concreto por los sistemas de redundancia usados;
- el procedimiento de almacenamiento de la información, llamado CAS, (por sus siglas en inglés de *Content Addressed Storage*, almacenamiento direccionado de contenido) que permite el acceso a datos registrados en un espacio de almacenamiento usando una clave de identificación cuya conservación es necesaria para encontrar los datos conservados.

Paralelamente, en el sector de las telecomunicaciones, se conocen bien lógicas de transmisión por paquetes que consisten en cortar un fichero de datos que hay que transmitir en una pluralidad de paquetes de datos totalmente independientes y en reconstituir todo el fichero cuando todos los paquetes llegan a su destino. Por ejemplo, la red pública TRANSPAC operativa desde 1978.

En cambio, aun nunca se ha implementado el ensamblaje de los diferentes conceptos de la técnica anterior.

Asimismo, los procedimientos de la técnica anterior necesitan muchos recursos informáticos y requieren una organización o dispositivos complejo(s).

Además, no ofrecen la posibilidad de adaptar el nivel de seguridad a la naturaleza de los datos que hay que proteger.

Rick Copeland: "GridFS: The MongoDB File-system", https://web.archive.org/web/20150506020142/http://blog.pythonisito.com/2012/05/gridfs-mongodb-filesystem.html (XP055251683) revela un procedimiento del aseguramiento de datos digitales con fines de almacenamiento o archivo.

Resumen de la invención

Proponemos en el presente documento un dispositivo que permite explotar un fichero de datos digitales en diferentes elementos que a continuación podrán almacenarse cada uno en espacios distintos, preferentemente en diferentes ubicaciones físicas y geográficamente remotas. Este modo de almacenamiento se apoya en la lógica actual de la "nube". Realmente no se sabe dónde se almacena la información, pero podemos interrogarla y encontrarla sin problema. Sea lo que sea, en materia de "nube", la información se almacena en su conjunto en una ubicación determinada de modo que su confidencialidad no está en absoluto asegurada.

El dispositivo propuesto en el presente documento asegura una alta confidencialidad de los datos en la medida en que su acceso directo en las bahías de almacenamiento donde se conservan nunca permitirá tener la completitud de los datos porque se habrán cortado previamente en fragmentos o bloques. Asimismo, esta técnica se aplica sea el que sea el dispositivo de almacenamiento usado que podrá o no reforzar aun más la seguridad de los datos.

Solo, quien tenga los derechos de acceso podrá repatriar el conjunto de los fragmentos de manera coherente.

Un primer objeto de la invención es asociar según una nueva combinación varias técnicas, parcialmente conocidas per se, para mejorar el aseguramiento global del almacenamiento o archivo de datos digitales cuyos elementos binarios se agrupan en un fichero de origen, en concreto permitiendo mejorar cada uno de los criterios de seguridad que son la disponibilidad, la integridad, la confidencialidad y la trazabilidad de dichos datos.

En este marco, un primer aspecto de la invención concierne a la identificación, la autenticación del iniciador (persona física o material) de una petición ante el Centro de Gestión del procedimiento de la invención relativa al almacenamiento o archivo de un fichero inicial F0 de datos digitales, bajo condiciones que aseguran la garantía de su origen y de su integridad, por parte del Centro de Gestión.

Un segundo aspecto de la invención se refiere al procesamiento de dicho fichero inicial F0 de datos digitales para reestructurarlo en forma de un cierto número de bloques independientes e identificables y agrupados en el fichero de bloques FB.

Un tercer aspecto de la presente invención es relativo a la implementación de la distribución de los bloques identificados y formateados en el seno de una pluralidad de sitios de terceros de almacenamiento o archivo, pudiendo un sitio almacenar varios bloques y pudiendo un bloque estar presente en varios sitios.

Se señalará que los modos funcionales y los parámetros operativos del procedimiento de la invención se atribuyen a cada bloque y se indican en los campos específicos que constituyen el formato de dicho bloque.

Después de leer cada bloque, un dispositivo Emisor/Receptor transmite los bloques de datos a sus sitios de almacenamiento dedicados y, paralelamente, la Unidad Central de Procesamiento (UCT) construye una tabla llamada "Tabla cartográfica" que permite asociar esencialmente el código de identificación único de un bloque y el número y las direcciones de los sitios respectivos de almacenamiento de dicho bloque. La importancia de esta Tabla cartográfica es grande en la medida en que no contiene ninguna referencia a los elementos binarios de los datos atribuidos a cada bloque, sino en que, ella sola, permite recuperar el conjunto de los bloques completos distribuidos en una pluralidad de sitios, lo que constituirá un proceso previo a cualquier reconstitución del fichero de origen F0.

En consecuencia, el procedimiento de la invención debe implementar cualesquiera medios conocidos apropiados para asegurar el aseguramiento de esta Tabla cartográfica.

En línea con el objetivo de reforzar el aseguramiento de los datos digitales, un cuarto aspecto de la invención es relativo al cifrado facultativo de los datos atribuidos a los diferentes bloques con la ayuda de la aplicación de varios modos de cifrado que recurren a algoritmos y claves, pudiendo estos modos variar de un bloque al otro.

Obviamente, el conocimiento de dichos modos será necesario en el momento del descifrado de los datos. Sin embargo, con fines de seguridad, los algoritmos y claves usados no se integrarán en el seno de ningún campo del formato de bloque sino, en cambio, se memorizarán en la Tabla cartográfica correspondiente cuyas características ya se han mencionado.

Siempre en el mismo objetivo, un quinto aspecto de la invención se refiere al cálculo de la huella de cada bloque cuyo resultado se almacenará igualmente en la Tabla cartográfica y, de este modo, podrá permitir verificar la integridad de los datos atribuidos a cada bloque durante su vuelta con procedencia de los sitios dedicados con el fin de reconstruir el fichero de origen F0.

Un segundo objeto de la invención es permitir la selección del Nivel de Seguridad NS óptimo que se desea implementar en función de la naturaleza de los datos, de su importancia en los diversos campos a los que conciernen, o incluso, de su confidencialidad y de su durabilidad.

Un sexto aspecto de la invención describe los medios que conducen a una posible selección del Nivel de Seguridad NS. Entre estos medios, el elemento esencial se presenta en forma de una Tabla de Decisión que define,

para diferentes niveles de seguridad, del más bajo al más alto, los modos funcionales y los valores de los parámetros operativos que permiten alcanzar cada uno de los Niveles de Seguridad previstos en la Tabla de Decisión.

Dicho Nivel de Seguridad NS se selecciona durante la entrada del fichero de origen F0 y la Tabla de Decisión es interpretada y ejecutada por la UCT del Centro de Gestión hasta la obtención de la Tabla cartográfica correspondiente.

Un séptimo aspecto de la invención concierne a la reconstitución del fichero inicial F0 con la ayuda de las Tablas cartográficas conservadas en memoria y aseguradas, que no contienen ninguno de los datos para proteger, pero proporcionan la información necesaria para una reconstitución de este tipo.

Breve descripción de los Dibujos

La invención se comprenderá mejor con la ayuda de la descripción detallada más abajo y de las figuras adjuntas en las que:

La figura 1 representa un esquema funcional de la primera fase del procedimiento de la invención.
La figura 2 representa un esquema funcional de la segunda fase del procedimiento de la invención completada por la implementación del cálculo de huella facultativo de cada bloque.
La figura 3 representa un esquema funcional de la tercera fase del procedimiento de la invención.
La figura 4 representa un esquema funcional de la implementación del proceso facultativo de cifrado de los datos atribuidos a cada bloque.
La figura 5 representa un esquema funcional del procedimiento de la invención que implementa la selección del Nivel de Seguridad.

Las figuras 6a, 6b, 6c y 6d representan unos esquemas funcionales parciales del proceso de reconstitución del fichero inicial F0.

Descripción de algunos modos de realización

En la continuación, se usarán indistintamente los términos almacenar y archivar, o almacenamiento y archivo.

La **Figura 1** representa el esquema funcional del primer aspecto de la presente invención.

Una petición R_q es dirigida por un Solicitante al Centro de Gestión (G) encargado del almacenamiento o archivo de datos digitales y, de manera más particular, de asegurar el aseguramiento de dichos datos que se presentan en forma de un fichero de origen F0 registrado en cualquier soporte.

El Centro de gestión (G) 1 dispone de medios apropiados:

- para identificar y autenticar el Solicitante, y para aportar la evidencia de la existencia de dichos datos en la fecha de la petición;
- para aportar la garantía del origen y de la integridad del fichero de datos que el Centro de Gestión 1 se compromete a almacenar o archivar, asegurando que mantengan su integridad, su confidencialidad y su durabilidad.

Para hacer esto, una base de datos de clientes 3 asociada con un reloj 4 permite alcanzar el primer objetivo mencionado anteriormente, pero, para las otras garantías, la Unidad Central de Procesamiento (UCT) 2, asociada con unos medios de cálculo de huella 6 del fichero F0 son necesarios, que puede conducir de este modo a una firma electrónica 7, en el caso de que el firmante sea una persona física, o a un sello electrónico 7 si el firmante es una persona jurídica o una máquina.

Igualmente, se puede calcular, por ejemplo, dicha huella y enviarla a un servicio de estampación de fecha y hora electrónico que asocia con esta huella un número de orden, una fecha y una hora y sella el conjunto.

Un modo preferente de realización de la presente invención contempla, además, la realización de las firmas electrónicas apoyándose en un algoritmo de cifrado asimétrico basado en el uso de un par de claves. El principio consiste, después del cálculo de la huella del fichero, en cifrar esta última con la clave privada cuyo el firmante solo tiene el control.

Habiendo tomado todas estas precauciones, los datos digitales del fichero de origen F0, así como la huella E (F0) del fichero F0 se transfieren a la memoria sistema 5 del Centro de Gestión 1.

El segundo aspecto de la presente invención está ilustrado por la representación del esquema funcional de la **figura 2** que concierne a un modo de realización de la segunda fase del procedimiento de la invención y destinado a reestructurar el fichero de origen F0 8 en forma de una pluralidad de bloques de datos independientes e identificables.

Por "bloque" se designa una secuencia de elementos binarios extraídos, en su orden inicial, a partir de los datos digitales del fichero F0 8 y que se presentan en un formato de varios campos entre los cuales:

- un primer campo reservado para el código de identificación único CI 9 de dicho bloque constituido por una etiqueta F0* específica del fichero F0 y por el Número de Orden NO asignado de manera definitiva a dicho bloque durante su formación;
- un segundo campo, llamado Campo de Datos 10, que agrupa los elementos binarios de los datos atribuidos a dicho bloque;
- varios otros campos destinados a indicadores operativos y cuyos contenidos respectivos evolucionarán durante el proceso, como se describirá ulteriormente.

Los bloques están construidos de tal manera que el conjunto de elementos binarios, tomados en su orden inicial, de los datos del fichero de origen F0 verifica una relación de identidad biunívoca con el conjunto de los elementos binarios de los datos contenidos en la totalidad de los bloques considerados sucesivamente según su Número de Orden NO.

Para la formación de un bloque, la UCT 2 asociada, con un contador 11, que ejecuta las instrucciones de una primera ley de programación extrae 12, a partir del fichero F0 8, un cierto número "l" de elementos binarios "eb" en su orden inicial para llenar el campo "Datos" 10 del bloque en formación y atribuye simultáneamente a este último, en el campo dedicado, el código de identificación único CI 9 constituido por la etiqueta F0* específica del fichero F0 y por el Número de Orden NO indicador de la posición de los l_i elementos binarios extraídos en el fichero F0 8 y atribuidos a dicho bloque "i". El número "l" representa el tamaño del bloque.

Dicha primera ley de programación asociada con la formación de los bloques 13 define el primer parámetro operativo que constituye el número total de bloques "k", sabiendo que la confidencialidad de los datos será tanto mejor en cuanto que el número de bloques "k" sea grande.

Dicha primera ley igualmente determina un segundo parámetro operativo al imponer que el tamaño "l" de los bloques sea constante para el conjunto de los bloques (con la unidad de precisión) o sea variable de un bloque al otro, contribuyendo el hecho de hacer los bloques de tamaño variable, como el aumento del número 'k', a la mejora de la confidencialidad de los datos.

Según un modo de realización, el procesador de la UCT 2 que ejecuta las instrucciones de la primera ley de programación puede usar un proceso de conteo de los elementos binarios, bloque por bloque, de tal modo que el tamaño de los bloques sea constante y, por ejemplo, igual a EB/k = 1, donde EB representa el número total de elementos binarios "eb" contenidos en el fichero F0 8, calculado automáticamente, por ejemplo, durante la entrada de dicho fichero F0 8 después de examen de la petición R_q inicial.

Todos los bloques harán aparecer entonces en el campo Tamaño de bloque 14, indicador del tamaño del bloque, un valor "l". El último bloque puede estar eventualmente incompleto según el valor de la relación EB/k y el tamaño "l'" de este bloque será inferior a "l".

Según otra opción, el proceso de conteo de los elementos binarios "eb" atribuidos a cada uno de los "k" bloques puede ser aleatorio y los indicadores l_i que intervienen en los campos Tamaño de bloque 14 respectivos serán, en consecuencia, variables.

Si aparecieran problemas de gestión de bloque relacionados con el tamaño físico del conjunto del bloque, unos caracteres de relleno pueden usarse para que su tamaño se vuelva igual.

Los bloques formados y formateados de este modo se registran unos tras otros en un fichero de bloques FB 15 que puede almacenarse en la memoria del sistema 5 o, preferentemente, en una memoria caché auxiliar 5' de acceso más rápido, estando dicho fichero de bloques FB 15, en un modo preferente de realización, constituido por una simple cola, por ejemplo, de tipo FIFO.

La **figura 2** representa en su parte izquierda (sin cálculo de huella de los bloques), el contenido de los bloques 9, 10, 14 del fichero de bloques FB 15 en este punto del procedimiento, que ilustra el código de identificación 9 (etiqueta del fichero FO* y Número de Orden NO del bloque), el indicador de tamaño de bloque l_i y los elementos binarios eb_i atribuidos a este bloque.

En un modo preferente de realización, ilustrado en la parte derecha de la figura 2 (con cálculo de huella de los bloques), un procesamiento adicional de los bloques destinado, en particular a asegurarse, en cualquier momento, de la integridad de los elementos binarios "eb" atribuidos a cada bloque, consiste en calcular la huella de cada bloque a partir de su formación por los medios tradicionales de cálculo 6 que disponen de varios algoritmos posibles almacenados en 6', y, preferentemente, usando dos algoritmos de huellas diferentes. Los resultados E_i de los cálculos de huellas de bloque se agrupan en una primera tabla, llamada "Tabla de huella" TE 16 constituida esencialmente por dos columnas que permiten asociar con cada código de identificación de bloque CI_i el valor de huella correspondiente E_i asociado con su algoritmo de cálculo aei.

Dicha Tabla de huella TE 16 está dispuesta de tal manera que se pueda combinar sin dificultad con otras tablas, como se describirá ulteriormente. Igualmente es posible prever registrar directamente la información de la Tabla de huella en la Tabla cartográfica final. Esta posibilidad igualmente existe para los otros modos estudiados con posterioridad.

Tan pronto como el fichero de bloques FB 15 esté completo y conservado en memoria 5 o 5', el procedimiento activa las instrucciones de la segunda ley de programación implementada según la Figura 3.

La **Figura 3** representa un esquema funcional de un modo de realización del tercer aspecto de la invención.

Esta etapa consiste en implementar una segunda ley de programación cuya ejecución por el Procesador de la UCT 2 incluye las etapas siguientes:

- atribuir 17 a cada uno de los diferentes bloques del fichero de bloques FB 15 una o varias dirección(direcciones) de sitio(s) de terceros disponible(s) registrada(s) en 18 para el almacenamiento o el archivo, pudiendo ser los sitios de terceros locales, deslocalizados, o incluso, resultar de la lógica actual "nube";
- indicar, paralelamente, en el campo "Sitio" apropiado 19 del formato de cada bloque, el número j_i y las direcciones si_k respectivas de los sitios dedicados. El conjunto de los bloques formateados de este modo constituye el nuevo fichero de bloques FBS 23 conservado, por ejemplo, en memoria 5';
- luego transmitir, por unos medios de comunicación tradicionales y apropiados 20, cada bloque hacia el o los sitio(s) de almacenamiento dedicado(s) 21.

Según un modo preferente de realización, el Procesador de la UCT 2 extrae los bloques del fichero FB 15, bloque por bloque, y a partir de una lista de direcciones de sitios 18 de almacenamiento disponibles, atribuye, de manera aleatoria o configurada, uno o varios sitio(s) a cada uno de los bloques escribiendo el número j_i y las direcciones si_k

correspondiente(s) en el campo "Sitio" 19 del formato de bloque reservado para este fin, luego transfiere el bloque al dispositivo emisor/receptor E/R 20 que, después de lectura de las direcciones, transmite el bloque hacia el o los sitio(s) de almacenamiento dedicado(s) 21.

La multiplicidad de dichos sitios de almacenamiento aumenta la complejidad de la agrupación de los bloques diseminados de este modo y, en consecuencia, refuerza la confidencialidad de los datos. Sin embargo, por unas razones de gestión, es posible moderar el carácter aleatorio de la atribución de dichos sitios fijando, previamente, un número máximo de sitios para un bloque dado y/o para el conjunto de los bloques.

La figura 3 igualmente muestra que, simultáneamente con la atribución de los sitios, el Procesador de la UCT 2 construye una tabla que llamaremos Tabla cartográfica TC 22. Esta última está constituida por dos columnas, la primera columna registra sucesivamente los códigos de identificación CI_i de todos los bloques y la segunda columna indica el número j_i y las direcciones de los sitios si_{i1}, si_{i2}, ..., si_{ij} de almacenamiento atribuidos a cada bloque identificado en dicha primera columna.

Se pueden considerar otros modos de realización para el experto en la técnica. Por ejemplo, es posible establecer, a partir del fichero de bloques FBS 23, previamente registrado en la memoria caché 5', que agrupa todos los bloques después de asignación de los sitios de terceros, una pluralidad de colas 24, una por sitio dedicado, igualmente registradas en la memoria caché auxiliar 5', y que agrupa, cada una, un conjunto de bloques destinados al mismo sitio dedicado, lo que permite efectuar su transferencia hacia los sitios respectivos en una sola operación de transmisión.

Después de cada emisión, el dispositivo Emisor/Receptor 20 del Centro de Gestión 1 recibe los acuses de recibo procedentes de los diferentes sitios. Si se produce un posible incidente, se efectúa una nueva emisión del o de los bloque(s) interesados, como sucede de manera tradicional.

Sin embargo, este proceso igualmente justifica la conservación en memoria 5' del fichero FBS 23, siendo al mismo tiempo susceptible de ser borrado ulteriormente.

Dicha Tabla cartográfica TC 22 presenta un gran interés en la medida en que no contiene ningún rastro de los elementos binarios atribuidos a cada bloque, pero en que ella sola, permite recuperar el conjunto de los bloques completos distribuidos en una pluralidad de sitios de almacenamiento, lo que es un proceso previo para cualquier reconstitución ulterior del fichero de origen F0 8.

Por lo tanto, la Tabla cartográfica TC 22 debe ser asegurada por unos medios tradicionales, por ejemplo, conservándose en memoria 5 y salvaguardándose en el sitio del Centro de Gestión 1, pero igualmente puede conservarse en uno o varios sitio(s) de terceros remoto(s), siempre que esté cifrada con el fin de respetar la confidencialidad buscada.

En el marco del modo de realización preferente que implementa la aplicación del cálculo de huella 6 de cada bloque y que conduce al establecimiento de la Tabla de huellas TE 16, esta última 16 se combinará con el primer tipo de Tabla cartográfica TC 22 para llegar a un segundo tipo de Tabla cartográfica final TCE 25 ahora constituida por tres columnas y que asocia con cada bloque identificado por su código CI_i, a la vez dicho resultado del cálculo de huella correspondiente y el número j_i y direcciones si_{il}, si_{ik}, ... de los sitios de almacenamiento dedicados a dicho bloque.

La Tabla cartográfica TCE 25, como la Tabla cartográfica TC 22 requiere, por las mismas razones ya mencionadas, que sean aseguradas según los mismos medios mencionados anteriormente.

Después del último acuse de recibo procedente del último sitio hacia el que se transmitió el último bloque, la Tabla cartográfica TC o la Tabla TCE completa de este modo se registra en la memoria del sistema 5. Esto puede desencadenar el borrado de los ficheros intermedios FB 15 y FBS 23 y el del fichero de origen F0 8 y, posiblemente, el de sus respectivas copias.

En efecto, la Tabla cartográfica TC o la Tabla TCE asociada con el contenido de todos los campos de cada bloque almacenado o archivado en los diferentes sitios de terceros, aportan toda la información necesaria para reconstituir, en el momento deseado, el fichero de origen F0 8, lo que incita, como ya se ha sugerido, a asegurar las Tablas TC y TCE, las únicas aptas para repatriar los bloques distribuidos entre los sitios de terceros.

La **Figura 4** representa un esquema funcional de otro modo preferente de realización que implementa un proceso opcional que permite reforzar el aseguramiento de los datos y, en concreto, su confidencialidad haciendo intervenir el cifrado de dichos datos.

Como se indica en la figura 4, se produce la aplicación del proceso de cifrado realizado en 26, en aras de la seguridad, como muy pronto después de la formación de un bloque.

De este modo, por ejemplo, tan pronto como se forme el i^o bloque, es decir, que se determina su código de identificación CI_i así como su tamaño l_i y los elementos binarios eb_i que se le atribuyen, el procesador de la UCT 2

selecciona, esencialmente de manera aleatoria entre varios modos (algoritmos y claves) de cifrado (simbolizados por "mcht") 28, un modo $mcht_i$, por ejemplo, para dicho primer bloque "i".

Es importante señalar que, del modo de cifrado "mcht" seleccionado en 28 se deduce igualmente la información necesaria para el descifrado de dichos datos. En consecuencia, por unas razones de seguridad, es fundamental no integrar el modo aplicado "mcht" en el seno de los bloques antes de su transferencia a una pluralidad de sitios de almacenamiento dedicados.

Después de aplicación de dicho modo "mcht", los datos iniciales "eb" son reemplazados por los datos cifrados "eb*" y el bloque correspondiente a estos datos cifrados se une al nuevo fichero de bloques cifrados FB* 29 que se memoriza en la memoria caché 5'.

Tan pronto como se atribuya un modo de cifrado "mcht" a un bloque, simultáneamente, el Procesador de la UCT 2 establece una tabla, llamada "Tabla de cifrado" Tcht 30 que posee dos columnas, listando la primera columna los códigos de identificación CI de los bloques y asociando la segunda columna con cada código de identificación CI_i el modo de cifrado $mcht_i$ usado para este bloque.

Al combinar la Tabla de cifrado Tcht 30 con el primer tipo de Tabla cartográfica TC 22 obtenida después de distribución de los bloques en sus respectivos sitios de almacenamiento, se establece un tercer tipo de Tabla cartográfica final TCH 31 de tres columnas, que unen códigos de identificación CI, modos de cifrado "mcht", números "j" y direcciones "si" de los sitios de almacenamiento dedicados.

De la misma forma, si igualmente se aplica la opción de cálculo de las huellas de bloques E, el cuarto tipo de Tabla cartográfica final TCHE 32, teniendo en cuenta la Tabla de huellas TE 16, estará constituido por cuatro columnas que unirán códigos de identificación CI, modos de cifrado "mcht", huellas E, números "j" y direcciones "si" de los sitios de almacenamiento dedicados.

Por unas razones idénticas, las Tablas TCH y TCHE están aseguradas, como se ha mencionado anteriormente.

La **Figura 5** representa un esquema funcional de los medios usados en los aspectos anteriores de la presente invención para implementarlos para cumplir los requisitos de un Nivel de Seguridad NS previamente seleccionado.

En función de la naturaleza, de la confidencialidad, de la criticidad u otro de los datos que hay que almacenar o archivar, el Nivel de Seguridad deseado puede variar y un Nivel de Seguridad óptimo se busca a menudo con respecto a la necesidad real de seguridad, pero igualmente con respecto al plazo de tratamiento, al coste y a la complejidad de los medios de aseguramiento implicados.

El elemento central que permite modular el Nivel de Seguridad consiste en establecer previamente una Tabla de Decisión TD 33 que defina los modos funcionales y los valores de parámetros operativos que corresponden a los diferentes Niveles de Seguridad seleccionables NS, en concreto, durante la entrada de la petición R_q de protección del fichero de origen F0 8.

Según un modo preferente de realización, los modos funcionales y parámetros operativos seleccionados por la Tabla de Decisión TD 33 en función de un Nivel de Seguridad NS determinado, conciernen a:

- el número de bloques k, sabiendo que cuanto más alto es k, más tendencia tendrá el tamaño e de los bloques a disminuir y mejor será la confidencialidad,
- el número de sitios de almacenamiento que igualmente permiten mejorar la confidencialidad si el número de sitios aumenta,
- el número de ejemplares, es decir, el número de sitios que almacenan un mismo bloque, pudiendo dichos ejemplares intervenir en caso de defectos constatados relativos a la integridad de los bloques,
- la ejecución Sí/No del cálculo de huellas E para cada bloque que permite asegurar mejor, si la elección es positiva, la integridad de los bloques durante la reconstitución del fichero de origen F0,
- la ejecución Sí/No del cifrado de los datos que permite, si la elección es positiva, reforzar la confidencialidad de estos datos.

Una Tabla de Consulta 35 agrupa el conjunto de los modos funcionales y de los parámetros operativos disponibles cuyas múltiples combinaciones son susceptibles de determinar los diferentes Niveles de Seguridad NS.

La Tabla de Decisión TD 33 es implementada por el procesador de la UCT 2 después de la selección del Nivel de Seguridad NS.

Una vez que se determina el Nivel de Seguridad NS, se registran los modos funcionales y los parámetros operativos que corresponden a la elección de la Tabla de Decisión TD 33, por ejemplo, en una memoria caché auxiliar 34 reservada para dichos parámetros con fines de control en caso de posible fallo ulterior.

La UCT 2 implementa entonces todos los procesos descritos anteriormente por separado para resaltar las diferentes etapas básicas del procedimiento de la invención incluyendo las diferentes opciones susceptibles de ser tomadas en cuenta en la Tabla de Decisión 33.

Las Tablas cartográficas finales, sean cuales sean sus tipos, TC, TCE, TCH, TCHE, como ya se ha descrito anteriormente, se transfieren en la memoria del sistema 5 y se aseguran apropiadamente. Igualmente es posible usar solo una Tabla cartográfica actualizada directamente a medida que se constituyen los bloques.

Después de la vuelta del acuse de recibo de escritura del último bloque procedente del último sitio de almacenamiento dedicado y después de la implementación del aseguramiento de dichas Tablas cartográficas finales, en concreto, después de su registro en la memoria sistema 5, es posible considerar la supresión del fichero de origen F0 8, siempre que se conserve en memoria 5 su huella E (F0) calculada durante la entrada de la petición R_q, según un algoritmo determinado por el Centro de Gestión 1.

Las **Figuras 6a, 6b, 6e y 6d** representan varios esquemas y un organigrama funcionales relativos a la cuarta fase del procedimiento de la invención cuya implementación resulta de una petición concerniente a la reconstitución del fichero de origen F0 8.

Para hacer esto, una primera etapa, ejecutada por la UCT 2 (figura 6a), es emitir una señal "S" con destino a todos los sitios de almacenamiento dedicados cuyas direcciones se leen en la Tabla cartográfica final (TC, TCE, TCH, TCHE) 22, 25, 31, 32 conservada en memoria 5 y por cualesquiera medios de transmisión apropiados.

La señal "S" está diseñada para indicar que los bloques que hay que extraer se refieren únicamente a los que contienen en su campo "Identificación" (CI) la marca F0* específica del fichero de origen F0.

En una segunda etapa (figura 6b), el sistema de recepción 20 recoge todos los bloques que le lleguen de los diferentes sitios 21 en un fichero de bloques FR 36.

La UCT 2 entonces implementa, en los bloques del fichero FR 36, un proceso de clasificación según un algoritmo tradicional cuya clave de clasificación es el Número de Orden NO del bloque, sabiendo que a un Número de Orden NO corresponde solo un bloque y que este Número figura en el Código de Identificación CI del bloque, para conducir al establecimiento de dos ficheros FR1, 38 y FR2, 39.

El primer fichero FR1 38 contiene un conjunto de bloques, que difieren entre sí por al menos su Número de Orden NO, agrupando el segundo fichero FR2 39 todos los bloques que han sido objeto de un almacenamiento en varios sitios dedicados y que se presentan al menos como duplicados.

En este punto del procedimiento, una primera comprobación de su desarrollo correcto consiste en observar que el número de bloques del fichero FR1 38 es igual al número "k" de bloques del fichero de origen F0.

Además, una prueba relativa a la integridad de los datos atribuidos a cada bloque puede efectuarse a partir del fichero FR1 38. De este modo, la figura 6c presenta el organigrama funcional asociado con dicha prueba de integridad.

Para todos los bloques del fichero FR1 38, el proceso es el siguiente: en el bloque "i", se cuenta el número total de elementos binarios eb_i en el campo "Datos" y se compara con el valor l_i inscrito en el campo "Tamaño de bloque". En caso de igualdad, el proceso continúa para el siguiente bloque i+1, de lo contrario, en caso de desigualdad, es posible buscar si el bloque "i" figura en el fichero FR2 39 y se reanuda el ciclo análogo de la prueba.

Esto demuestra otro beneficio de almacenar un bloque dado en más de un sitio dedicado para asegurarse de la integridad de los datos que se le han atribuido.

Otra prueba de integridad es posible si el cálculo de huella de bloque es una opción seleccionada. De este modo, a partir del fichero FR1 38, para cada bloque "i", se emprende un cálculo de huella Ei', usando el mismo algoritmo ae_i indicado en la Tabla cartográfica final TCE 25 o TCHE 32 conservada en memoria 5, que igualmente da el resultado de huella E_i que corresponde al mismo bloque "i" que estaba presente en el fichero de origen F0.

La comparación entre las huellas Ei' y E_i permite verificar la integridad de los datos después de su almacenamiento.

La figura 6d representa la etapa final de la reconstitución del fichero de origen. Según un modo de realización, la UCT 2 extrae en 40 los elementos binarios presentes en el campo "Datos" de cada bloque del fichero FR1, 38 y los transfiere en una cola 41 según la misma consideración de los Números de Orden NO que durante la extracción efectuada en 12 durante la segunda fase del procedimiento de la invención (figura 2).

Una operación tradicional de concatenación 42 que trata sobre los registros de elementos binarios de la cola 41 conduce al fichero final $F0_{bis}$ 43 que debería ser idéntico al fichero de origen F0. Para verificar esta afirmación, es suficiente con comparar en 45 la huella E(F0) del fichero de origen F0 calculada por el Centro de Gestión 1 y

conservada en memoria 5, con la huella $E(F0_{bis})$ del fichero reconstituido $F0_{bis}$ calculada en 44 por el Centro de Gestión 1 según el mismo algoritmo de cálculo.

Durante la selección de las opciones para asegurar mejor la integridad y la confidencialidad de los datos que hay que almacenar por la mediación o no de la Tabla de Decisión 33, las Tablas cartográficas finales TC 22, TCE 25, TCH 31 y TCHE 32 intervienen de manera decisiva en el proceso de reconstitución del fichero de origen F0.

En efecto, aportan la información esencial necesaria para dicha reconstitución, en la medida en que, no solo permiten localizar los sitios de almacenamiento de los diferentes grupos de datos, sino igualmente establecer las relaciones:

- entre Código de Identificación CI, valor de Huella E y algoritmo usado "ae", y/o
- entre Código de Identificación CI y modo de cifrado "mcht" cuyo conocimiento es fundamental para el descifrado ulterior.

Se debe señalar igualmente que toda esta última información indispensable para la reconstitución del fichero de origen F0 no aparece en los bloques.

En consecuencia, es importante insistir en que dichas Tablas cartográficas finales TC 22, TCE 25, TCH 31 y TCHE 32 están conservadas en la memoria 5 del Centro de Gestión 1 y, además, salvaguardadas, así como aseguradas por cualesquiera medios como ya se ha mencionado.

Se pueden aportar diferentes modificaciones a lo que se ha descrito en el presente documento en los modos de realización y su implementación del procedimiento de la invención sin por ello apartarse del campo de la invención.

REIVINDICACIONES

1. Procedimiento de mejora del aseguramiento de datos digitales con fines de almacenamiento o archivo, temporal o duradero, **caracterizado por que** incluye una combinación de tres fases distintas, implementándose el procedimiento bajo control de un centro de gestión (G) (1),
consistiendo la primera fase en:

a) identificar y autenticar una petición (R_q) de un usuario que desea proteger sus propios datos digitales presentados en forma de un fichero de origen (FO) (8);
b) calcular (6) una huella (E(FO)) del fichero de origen (FO) (8) según un algoritmo de cálculo de huella con el fin de constituir una prueba de la existencia de dichos datos en la fecha de dicha petición (Rq), así como garantizar el origen y la integridad de dichos datos apoyándose en una firma electrónica (7) o un sello electrónico (7);
c) transferir dichos datos digitales y la huella (E(FO)) de dicho fichero de origen (FO) (8) en una memoria de un sistema (5) del centro de gestión, y
(d) entrar, en caso necesario, parámetros operativos requeridos para el funcionamiento de dicho procedimiento;
consistiendo la segunda fase en:
e) aplicar a una unidad central de procesamiento (UCT) (2) del centro de gestión una primera ley de programación que permite reestructurar el fichero de origen (FO) (8) en forma de una pluralidad de bloques independientes e identificables (13) cuyo número (K) y tamaño (I), constante o variable, están determinados en dicha primera ley, debiendo permitir la concatenación de dichos bloques reconstituir ulteriormente dicho fichero de origen (FO) (8),

estando dichos bloques estructurados según un formato que presenta un campo "Datos" (10) destinado a los elementos binarios (eb) de los datos respectivos atribuidos específicamente a cada uno de dichos bloques y varios campos reservados para información que indica cada una una característica útil relativa a dicho bloque, comprendiendo dicha información un código de identificación único del bloque (CI) (9), y posiblemente el tamaño (I) (14) de dicho bloque,
constituyendo el conjunto de los bloques formados y formateados de este modo un fichero de bloques (FB) (15), que se registra en memoria (5, 5'); y consistiendo la tercera fase en:

f) hacer aplicar por la unidad central de procesamiento (2) una segunda ley de programación que permite transferir (17, 20) los bloques del fichero de bloques (FB) (15) hacia al menos uno de una pluralidad de sitios de terceros de almacenamiento (21), correspondiendo cada bloque a al menos un sitio de almacenamiento,
pudiendo ser los sitios de almacenamiento locales, remotos o procesados en modo "nube" y pudiendo usar, además, internamente todos los medios tradicionales de aseguramiento;
g) insertar (17) en el formato de cada bloque un campo adicional (19) destinado a contener el número y las direcciones del al menos un sitio de terceros respectivo hacia los que debe transferirse dicho bloque, estando el conjunto de los bloques formateados de este modo agrupado en un segundo fichero de bloques (FBS) (23);
h) luego transferir en (20), por cualesquiera medios de transmisión apropiados (21), ya sea bloque por bloque, ya sea por sitio, el conjunto de los bloques de dicho segundo fichero de bloques (FBS) (23, 24) hacia los respectivos sitios de terceros;
i) a continuación, establecer, a partir de dicho segundo fichero de bloques (FBS) (23) un primer tipo de tabla cartográfica final (TC) (22) que se presenta en forma de una tabla de dos columnas, registrando la primera los códigos de identificación (CI) de los bloques y asociando la segunda con cada dicho código de identificación (CI) el número y las direcciones del al menos un sitio de terceros de almacenamiento; y
j) transferir la tabla cartográfica final (TC) (22) obtenida de este modo en la memoria del sistema (5) y asegurarla.

2. Procedimiento según la reivindicación 1, **caracterizado, además, por** el hecho de cifrar (26) los datos digitales contenidos en los bloques del fichero de bloques (FB) (15) según modos de cifrado (mcht) (28) apropiados, comprendiendo un modo de cifrado un algoritmo de cifrado y una clave de cifrado, y pudiendo variar de un bloque al otro y transformar de este modo el fichero de bloques (FB) (15) en un fichero de bloques (FB*) (29) que contiene los datos cifrados, y establecer con fines de seguridad, una tabla de cifrado (Tcht) (30) que permite asegurar la correspondencia entre un bloque determinado por su código de identificación único (CI) y los modos de cifrado (mcht) implementados para cifrar los datos de dicho bloque, estando dicha tabla de cifrado (Tcht) (30) destinada a combinarse con dicha tabla cartográfica (TC) (22) para establecer un segundo tipo de tabla cartográfica final (TCH) (31) que indica, para cada bloque, la correspondencia única entre código de identificación (CI), número (j) y direcciones de los sitios de terceros de almacenamiento (si) y modo de cifrado (mcht).

3. Procedimiento según la reivindicación 1 o la reivindicación 2, **caracterizado, además, por** el cálculo (6) según varios algoritmos posibles (ae) de cálculo de huella de una huella (E) de cada bloque formado y formateado en la etapa e) (13) y la operación de construir paralelamente una tabla de huellas (TE) (16) que establece el enlace único entre código de identificación de bloque (CI) y huella (E) de dicho bloque asociado con el algoritmo (ae) de cálculo de huella usado,
de combinar a continuación dicha tabla de huellas (TE) (16) con:

- sea la tabla cartográfica final (TC) (22) para formar un tercer tipo de tabla cartográfica final (TCE) (25), de tres columnas que unen de manera única para cada bloque, código de identificación (CI), número y direcciones de los

sitios de terceros de almacenamiento (j, si) y huella más algoritmo de cálculo de huella (E, ae),
- sea la tabla de cifrado (Tcht) (30) para formar un cuarto tipo de tabla cartográfica final (TCHE) (32) de cuatro columnas que unen, de manera única, para cada bloque, código de identificación (CI), número y direcciones de los sitios de terceros de almacenamiento (j, si), huella más algoritmo de cálculo de huella (E, ae), y modo de cifrado (mcht), y de transferir la tabla cartográfica final obtenida (TC, TCE, TCH, TCHE) (22, 25, 31, 32), en la memoria del sistema (5) y de asegurarla.

4. Procedimiento según las reivindicaciones 1, 2 y 3, **caracterizado, además, por que** permite una modulación de un nivel de seguridad (NS) del almacenamiento o archivo de un conjunto de datos digitales agrupados en un fichero de origen (FO) (8), una tabla de decisión (TD) (33) que define combinaciones de modos funcionales y de parámetros operativos que conducen a diferentes niveles de seguridad (NS) determinados, pudiendo seleccionarse un nivel de seguridad (NS) durante la entrada del fichero de origen (FO) (8),
definiendo los modos funcionales y los parámetros operativos un nivel de seguridad (NS) que se refiere:

- al número de bloques (k);
- al tamaño (l) fijo o variable de los bloques;
- al número total de sitios de terceros (j);
- al número de ejemplares, es decir, al número de diferentes sitios de terceros que almacenan el mismo bloque;
- a la ejecución o no del cálculo (6) de huellas de bloques (E);
- a la ejecución o no del proceso de cifrado de los datos;

la unidad central de procesamiento (UCT) (2), después de la selección de un nivel de seguridad (NS) dado, toma en cuenta los modos funcionales y los parámetros operativos definidos en la tabla de decisión (TD) (33) que corresponde al nivel de seguridad (NS) seleccionado y los transfiere en una memoria caché auxiliar adicional (34) conectada a la unidad central de procesamiento (UCT) (2) y reservada para los modos y parámetros usados para obtener dicho nivel de seguridad, luego ejecuta las instrucciones respectivas asociadas con dicha selección;
transfiriéndose las diferentes tablas cartográficas finales obtenidas (TC, TCE, TCH, TCHE) (22, 25, 31, 32) en la memoria del sistema (5) y asegurándose.

5. Procedimiento según la reivindicación 1, **caracterizado, además, por que** incluye una cuarta fase relativa a la reconstitución, a petición, del fichero de origen (FO) que incluye las siguientes etapas:

(k) emitir, a partir del centro de gestión (1), hacia todos los sitios de almacenamiento dedicados y listados en la tabla cartográfica (TC) conservada en la memoria del sistema (5), una señal de extracción (S(FO*)) fuera de los medios de almacenamiento presentes en dichos sitios dedicados, de todos los bloques identificados por la marca (FO*) específica del fichero de origen (FO) (8);
l) recibir todos los bloques identificados transmitidos de este modo por los sitios de almacenamiento dedicados en un fichero de bloques de reconstitución (FR) (36) conservado en una memoria caché (5');
m) a partir del fichero de bloques de reconstitución (FR), crear un primer fichero (FR1) (38) en el que todos los bloques identificados aparecen una sola vez, y un segundo fichero (FR2) (39) en el que solo aparecen los bloques almacenados en más de un sitio de terceros dedicado;
(n) con fines de verificación de integridad de los datos, comparar, en el primer fichero (FR1) (38), y para cada bloque (CI_i), el número de elementos binarios (eb_i) con el valor (l_i) indicado en el campo que indica el tamaño del bloque correspondiente;
o) extraer los elementos binarios (eb_i) de todos los bloques del primer fichero (FR1) (38) en un orden acordado de números de orden (NO) asignados a los bloques durante la formación inicial de los bloques (13) y aplicarles una operación de concatenación (42) para reconstituir el fichero de origen (FO_{bis}) (43);
p) con el fin de verificar la integridad del fichero de origen (FO) (8) y del fichero de origen reconstituido (FO_{bis}) (43), comparar la huella (E(FO)) del fichero de origen (FO) conservada con su algoritmo de cálculo de huella (ae) en la memoria (5) del centro de gestión (1) con una huella del fichero de origen reconstituido ($E(FO_{bis})$) (44) calculada según el mismo algoritmo (ae).

6. Procedimiento según las reivindicaciones 2 y 5, **caracterizado, además, por que** habiéndose seleccionado el cifrado para reforzar la confidencialidad de los datos almacenados, la implementación de las etapas k) y l) conduce a dicho fichero de bloques de reconstitución (FR) (36), que contiene entonces un conjunto de bloques en los que los datos están cifrados, usando los bloques que están descifrados el modo de cifrado (mcht) que corresponde a cada bloque (CI) contenido en la tabla cartográfica final (TCH) (31) conservada en la memoria (5),
permaneciendo las etapas de m) a p) funcionalmente inalteradas.

7. Procedimiento según las reivindicaciones 3 y 5, **caracterizado, además, por que** habiéndose seleccionado el cálculo de huella de cada bloque para reforzar la integridad de los datos, la implementación de las etapas k) y l) conduce a dicho fichero de bloques reconstituido (FR) (36) a partir del que una huella de cada bloque se calcula con el algoritmo de cálculo de huella (ae_i) conservado en memoria en la tabla cartográfica final (TCE) (25) para cada bloque (CI_i), y comparada con la huella correspondiente (E_i) presente en dicha tabla cartográfica final (TCE) (25) para consolidar, en caso de igualdad, la calidad de integridad de los datos después de su almacenamiento.

8. Procedimiento según las reivindicaciones 4, 5, 6 y 7, **caracterizado, además, por que**, pudiendo conducir la implementación de la tabla de decisión (TD) (33), para garantizar un máximo aseguramiento de los datos, a la selección simultánea de las opciones del cifrado de los datos y del cálculo de huella de bloque, las etapas k) y l) conducen a dicho fichero de bloques de reconstitución (FR) (36), cuyos bloques se someten al proceso de descifrado descrito en la reivindicación 6 y a la prueba de comparación de los valores de huella de bloque descrita en la reivindicación 7 usando la información contenida en la tabla cartográfica final (TCHE) (32), conservada en la memoria (5), que asocia respectivamente el código de identificación (CI) del bloque, el modo de cifrado (mcht), el valor de huella y su algoritmo de cálculo (E, ae), permaneciendo las etapas de m) a p) funcionalmente inalteradas.

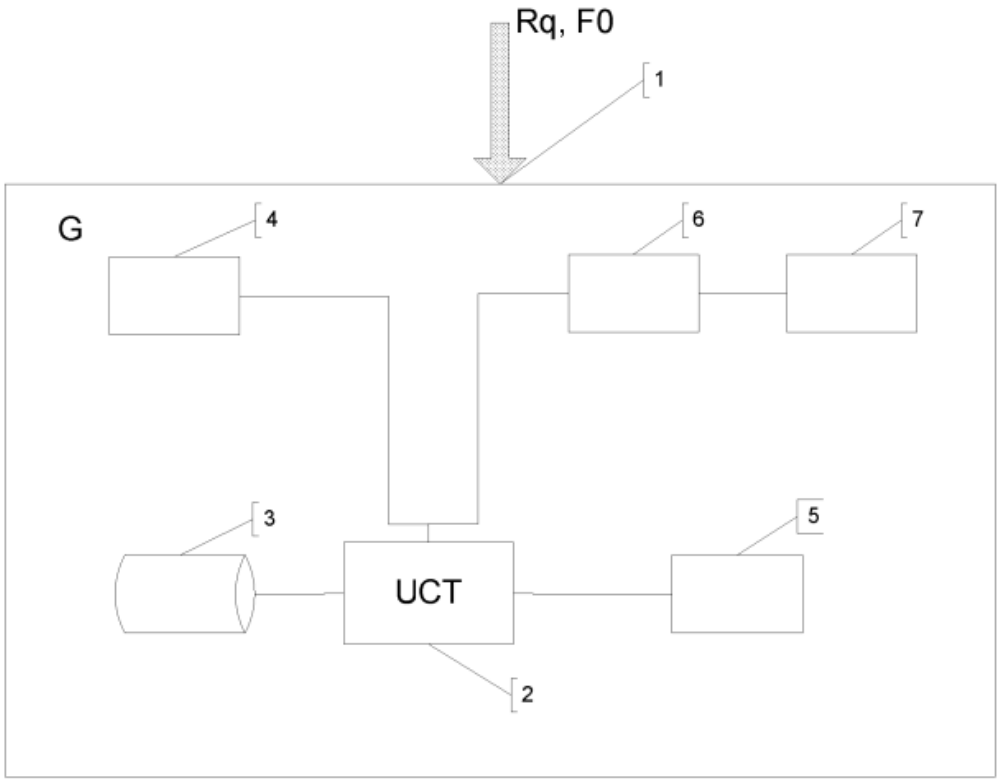

Figura 1

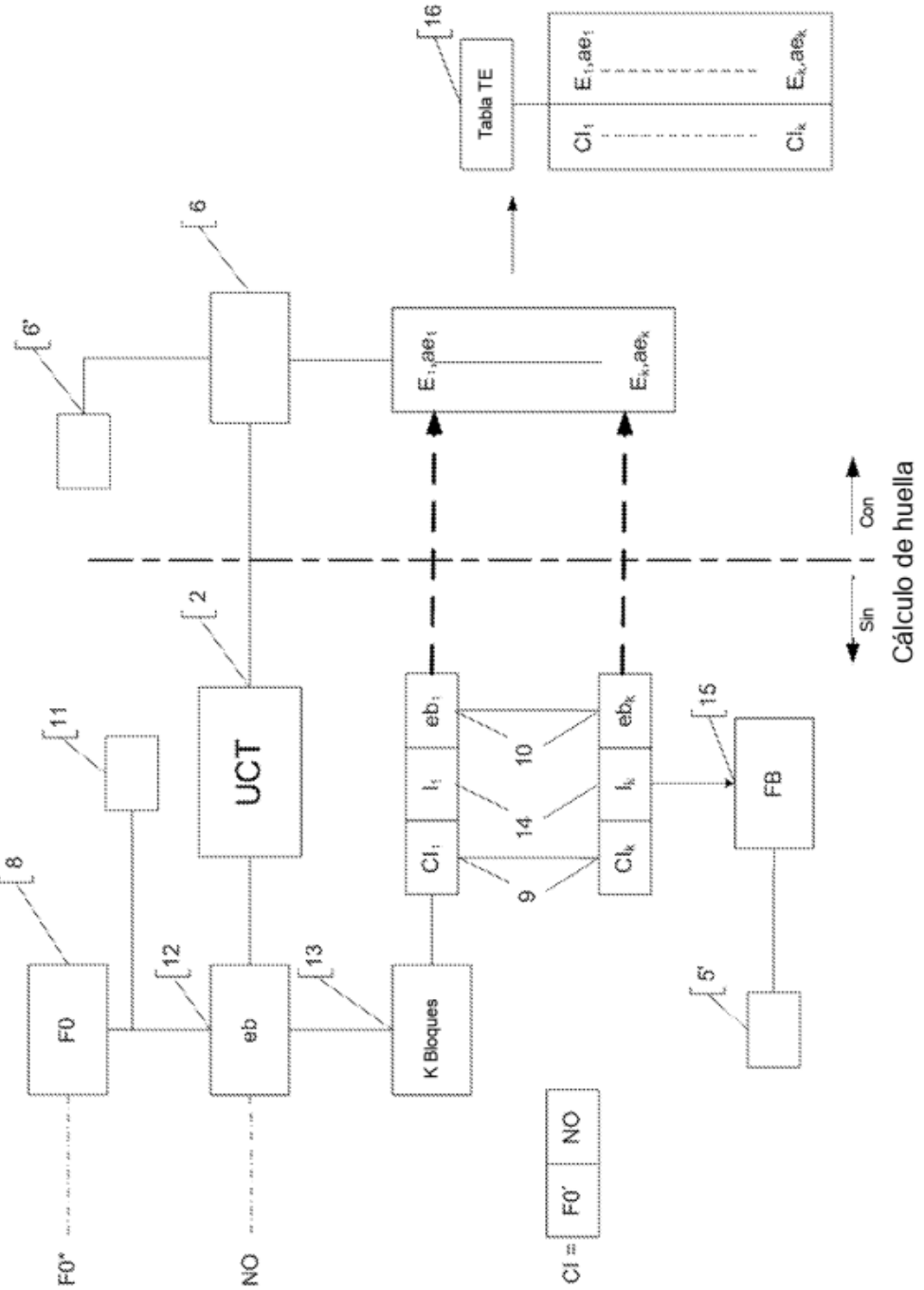
16
Tabla TE
E_1,ae_1
E_k,ae_k
CI_1
CI_k
6
6'
E_1,ae_1
E_k,ae_k
Con
Sin
Cálculo de huella
2
UCT
11
eb_1
I_1
CI_1
10
14
9
eb_k
I_k
CI_k
15
FB
8
F0
12
eb
13
K Bloques
5'
F0*
NO
CI =
F0'
NO

Figura 2

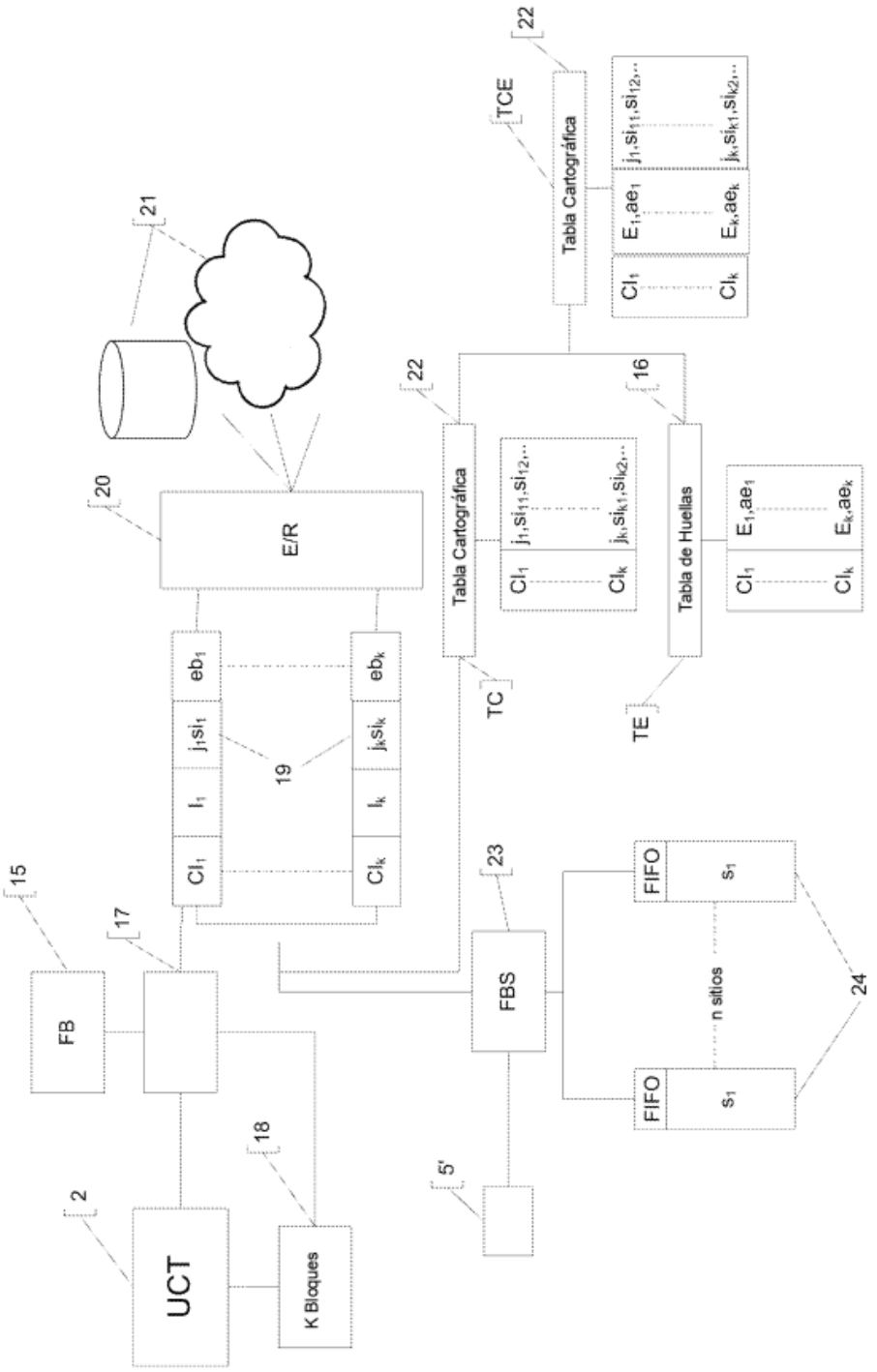
UCT
K Bloques
2
18
5'
FB
15
17
FBS
23
FIFO
s1
n sitios
24
19
ebk
jksik
Ik
Clk
eb1
j1si1
I1
Cl1
E/R
20
21
Tabla Cartográfica
22
TC
Tabla de Huellas
16
TE
TCE
Ek,aek
E1,ae1
jk,sik1,sik2,..
j1,si11,si12,..

Figura 3

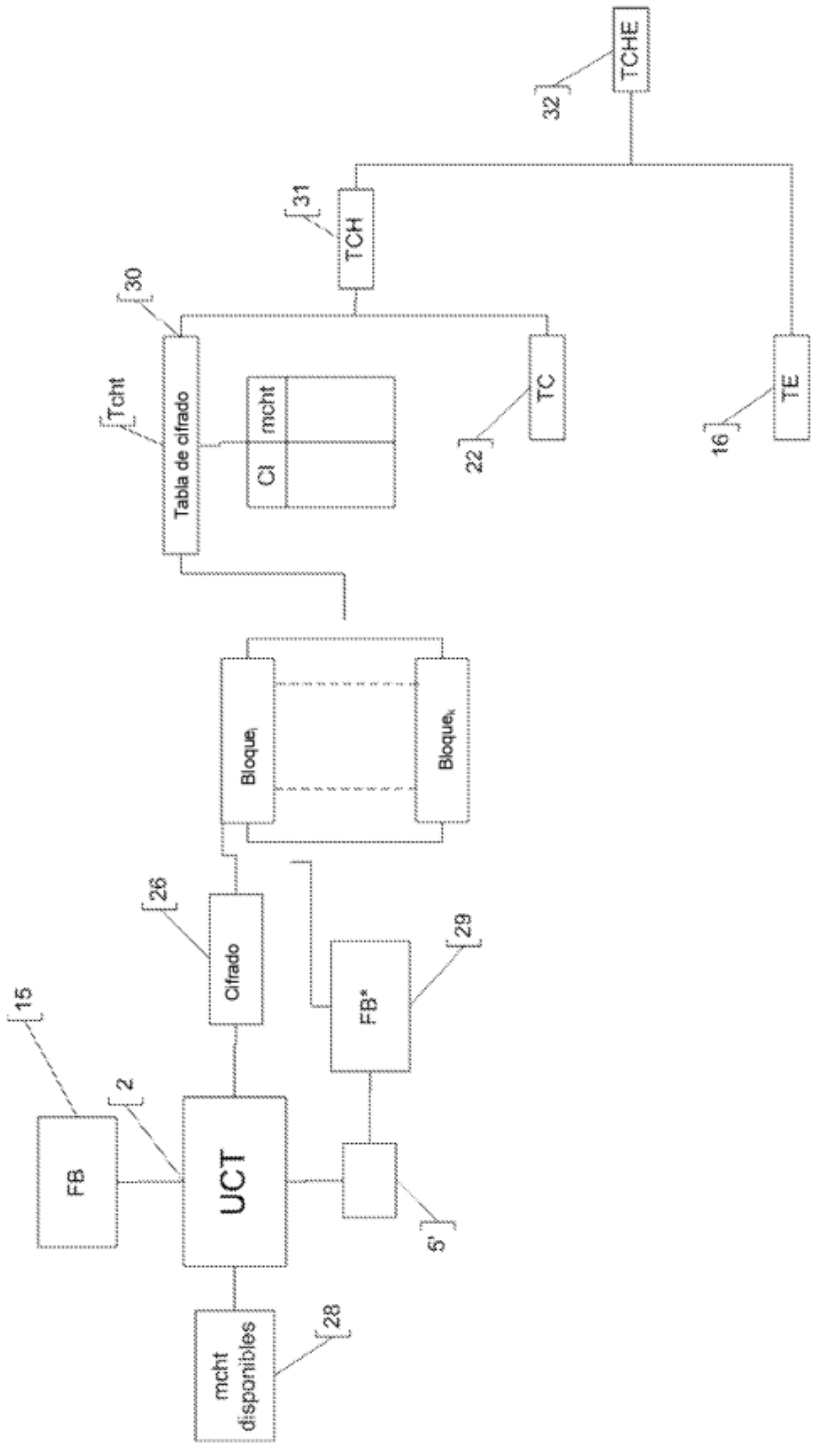
TCHE
32
TCH
31
30
Tcht
Tabla de cifrado
mcht
Cl
TC
22
TE
16
Bloque1
Bloquen
26
Cifrado
FB*
28
15
FB
2
UCT
5'
mcht disponibles
28

Figura 4

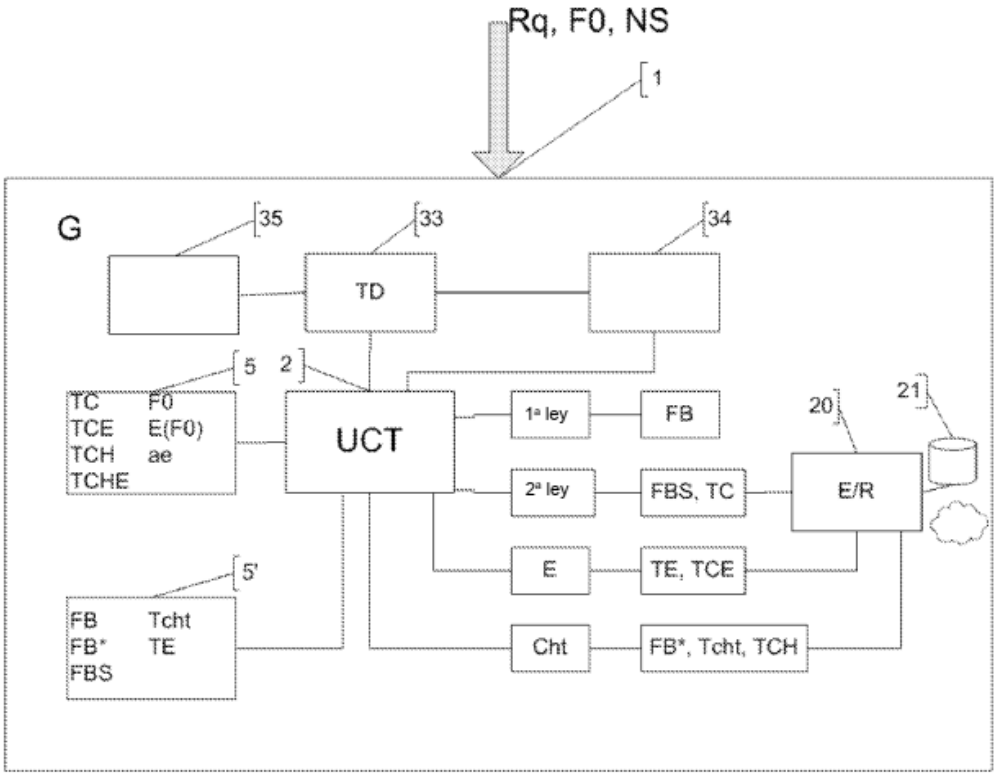
Rq, F0, NS
1
G
35
33
34
TD
5
2
TC F0
TCE E(F0)
TCH ae
TCHE
UCT
1ª ley
FB
20
21
2ª ley
FBS, TC
E/R
E
TE, TCE
5'
FB Tcht
FB* TE
FBS
Cht
FB*, Tcht, TCH

Figura 5

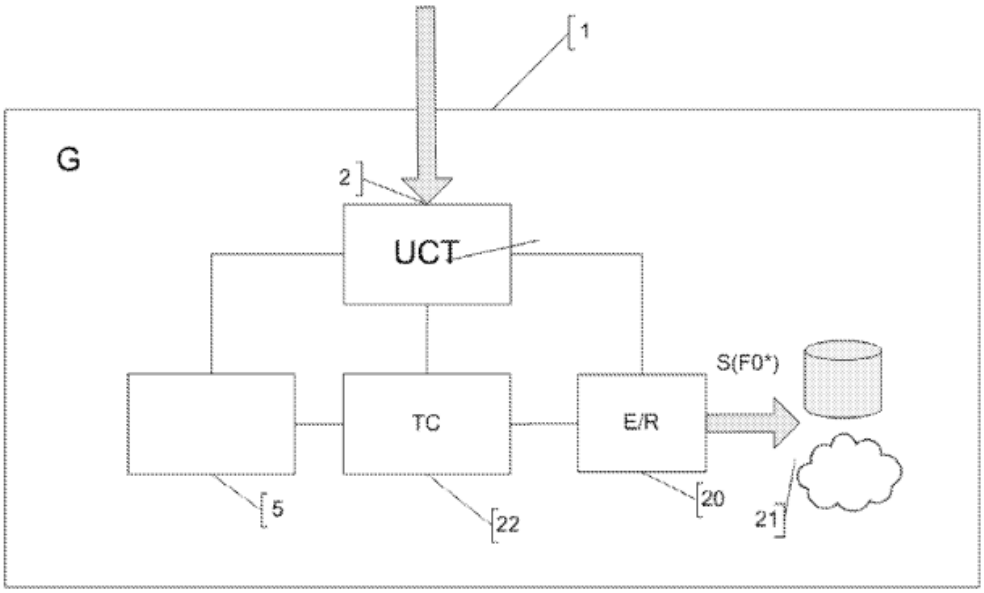

Figura 6a

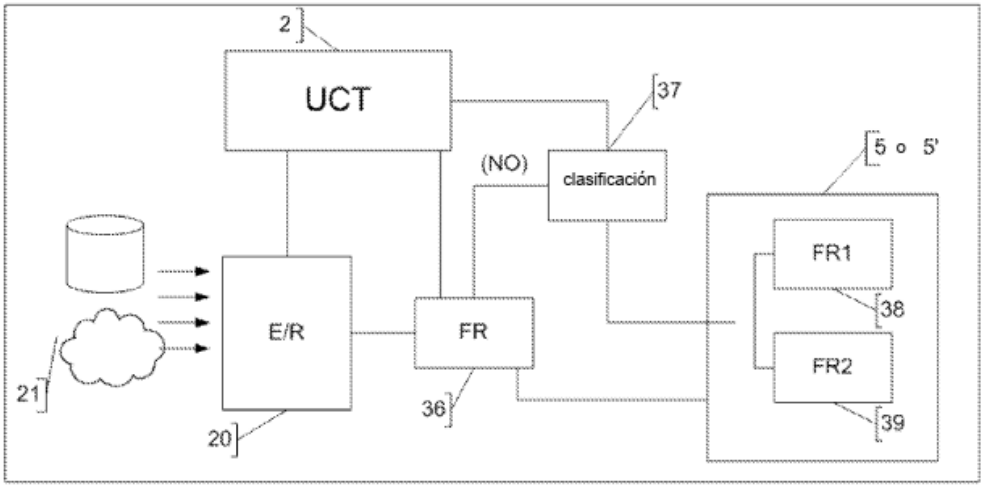

Figura 6b

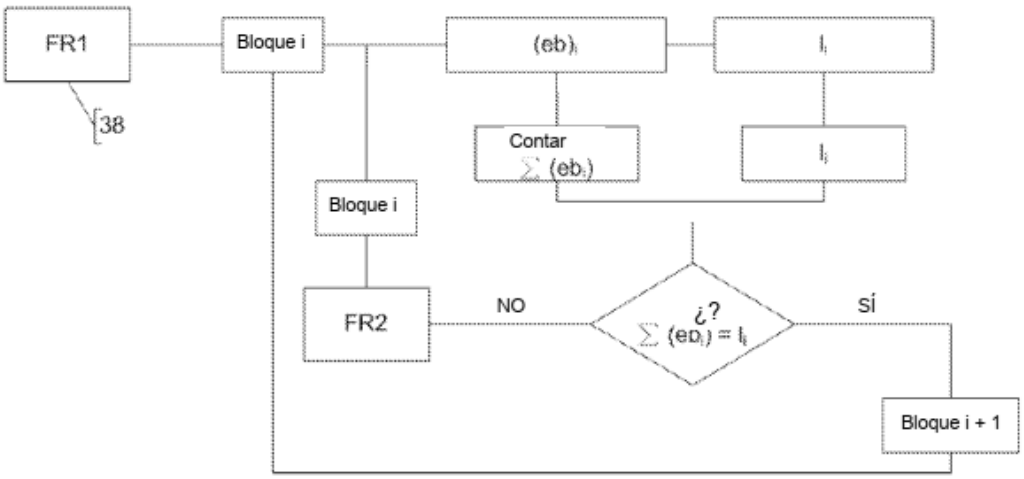

Figura 6c

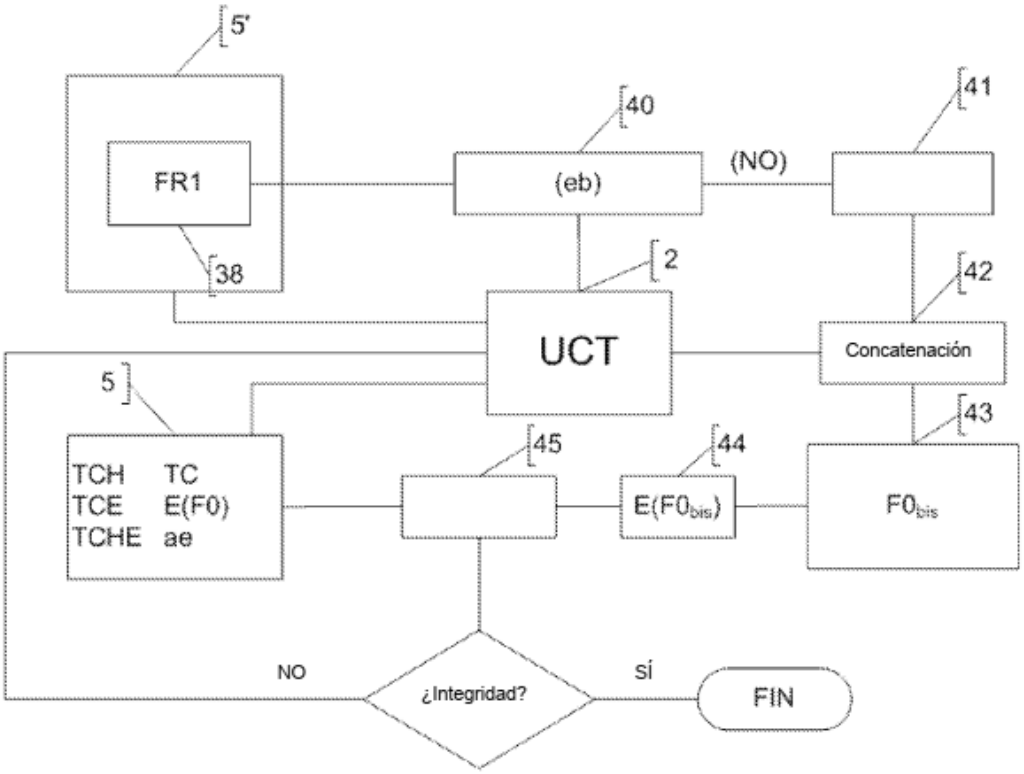

Figura 6d