(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 716 902**

(51) Int. CI.:

G06F 21/62 (2013.01)
H04L 9/08 (2006.01)
G06F 17/30 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **29.01.2015 PCT/US2015/013413**

(87) Fecha y número de publicación internacional: **13.08.2015 WO15119824**

(96) Fecha de presentación y número de la solicitud europea: **29.01.2015 E 15705151 (7)**

(97) Fecha y número de publicación de la concesión europea: **26.12.2018 EP 3103052**

(54) Título: **Métodos y sistemas para borrar información solicitada**

(30) Prioridad:

06.02.2014 US 201414173931

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
17.06.2019

(73) Titular/es:

GOOGLE LLC (100.0%)
1600 Amphitheatre Parkway
Mountain View, CA 94043, US

(72) Inventor/es:

SYBEN, JOANNE;
HARREN, MATTHEW THOMAS y
RUDYS, ALGIS PRANAS

(74) Agente/Representante:

ARIAS SANZ, Juan

DESCRIPCIÓN

Métodos y sistemas para borrar información solicitada

Solicitudes relacionadas y reivindicación de prioridad

La presente solicitud reivindica prioridad a la Solicitud de Patente de Estados Unidos con N.º de Serie 14/173.931, presentada el 6 de febrero de 2014, titulada “Methods and Systems for Deleting Requested Information.”

Antecedentes

El uso creciente de medios sociales, dispositivos móviles y servicios de tipo de asistente personal ha hecho más complejo conservar la anonimidad de usuario en datos registrados. A medida que se acumulan registros, se presenta una tubería de borrado con un conjunto de datos cada vez mayor. Puede ser necesario que se procesen y/o borren los datos dentro de un cierto periodo de tiempo conforme a un borrado solicitado del usuario u otra política que complica adicionalmente el proceso de borrado, la solicitud US2011/055559 describe un sistema relacionado para aplicación de políticas de retención asociadas con ficheros encriptados, que implica el borrado de claves de encriptación después del agotamiento de un periodo de retención de fichero.

Sumario

Como se usa en este documento, las formas singulares “un”, “una” y “el”, la” incluyen la referencia plural a menos que el contexto dicte claramente de otra manera. A menos que se defina de otra manera, todos los términos técnicos y científicos usados en el presente documento tienen los mismos significados que los entendidos comúnmente por un experto en la materia. Todas las publicaciones mencionadas en este documento se incorporan por referencia. Todos los tamaños indicados en este documento son a modo de ejemplo únicamente, y la invención no está limitada a estructuras que tienen los tamaños específicos o dimensión indicados a continuación. Como se usa en el presente documento, la expresión “que comprende” significa “que incluye, pero sin limitación”.

En una realización, un método de borrado de registros de anotación puede incluir identificar, por un dispositivo informático desde una base de datos de registros de anotación, una pluralidad de registros de anotación generados durante un periodo de tiempo. Cada registro de anotación puede corresponder a una actividad de usuario. El método puede incluir, para cada registro de anotación identificado, determinar, por el dispositivo informático, si se ha realizado una solicitud de borrado asociada con el registro de anotación, y, en respuesta a la determinación de que no se ha recibido una solicitud de borrado, identificar un identificador único asociado con el registro de anotación, buscar una tabla de actividad de usuario para una entrada que tiene un índice de tabla de claves asociado con el identificador único, donde la entrada está asociada con una indicación de tiempo, usando el índice de tabla de claves y la indicación de tiempo para identificar una clave asociada con el identificador único y la indicación de tiempo de una tabla de claves, encriptar, por el dispositivo informático, al menos una porción del registro de anotación con la clave identificada para generar un valor encriptado, y almacenar el valor encriptado como una entrada en la base de datos de registros de anotación que está asociada con el registro de anotación identificado.

En una realización, un sistema de borrado de registros de anotación puede incluir un dispositivo informático, y un medio de almacenamiento legible por ordenador en comunicación con el dispositivo informático. El medio de almacenamiento legible por ordenador puede incluir una o más instrucciones de programación que, cuando se ejecutan, provocan que el dispositivo informático identifique una pluralidad de registros de anotación generados durante un periodo de tiempo. Cada registro de anotación puede corresponder a una actividad de usuario. El medio de almacenamiento legible por ordenador puede incluir una o más instrucciones de programación que, cuando se ejecuta, provocan que el dispositivo informático, para cada registro de anotación identificado, determine si se ha realizado una solicitud de borrado asociada con el registro de anotación, en respuesta a la determinación de que no se ha recibido una solicitud de borrado, identificar un identificador único asociado con el registro de anotación, buscar una tabla de actividad de usuario para una entrada que tiene un índice de tabla de claves asociado con el identificador único, donde la entrada está asociada con una indicación de tiempo, usar el índice de tabla de claves e indicación de tiempo para identificar una clave asociada con el identificador único y la indicación de tiempo de una tabla de claves, encriptar, por el dispositivo informático, al menos una porción del registro de anotación con la clave identificada para generar un valor encriptado, y almacenar el valor encriptado como una entrada en la base de datos de registros de anotación que está asociada con el registro de anotación identificado.

Breve descripción de los dibujos

La Figura 1 ilustra una línea de tiempos de ejemplo de una solicitud de borrado de acuerdo con una realización.

La Figura 2 ilustra un diagrama de bloques de un sistema de borrado de ejemplo de acuerdo con una realización.

La Figura 3 ilustra un diagrama de flujo de un método de ejemplo de borrado de datos de usuario de acuerdo con una realización.

La Figura 4 ilustra un diagrama de flujo de un método de ejemplo de generación de una o más claves y creación de una lista de borrado de acuerdo con una realización.

La Figura 5 ilustra un diagrama de flujo de un método de ejemplo de borrado de registros de anotación de acuerdo con una realización.

La Figura 6 ilustra un diagrama de flujo de un método de ejemplo de depuración de uno o más registros de anotación de acuerdo con una realización.

La Figura 7 ilustra un diagrama de bloques de hardware de ejemplo que puede usarse para contener o implementar instrucciones de programa de acuerdo con una realización.

La Figura 8 ilustra una tabla de claves de ejemplo de acuerdo con una realización.

Descripción detallada

Los siguientes términos deberán tener, para los fines de esta solicitud, los respectivos significados que se exponen a continuación:

Un “dispositivo informático” hace referencia a un dispositivo que incluye un procesador y memoria legible por ordenador tangible. La memoria puede contener instrucciones de programación que, cuando se ejecutan por el procesador, provocan que el dispositivo informático realice una o más operaciones de acuerdo con las instrucciones de programación. Ejemplos de dispositivos informáticos incluyen ordenadores personales, servidores, ordenadores centrales, sistemas de juegos, televisiones, y dispositivos electrónicos portátiles tales como teléfonos inteligentes, asistentes digitales personales, cámaras, ordenadores de tableta, ordenadores portátiles, reproductores de medios y similares. Cuando se usa en las reivindicaciones, la referencia a “un dispositivo informático” puede incluir un único dispositivo, o puede hacer referencia a cualquier número de dispositivos que tienen uno o más procesadores que comunican entre sí y comparten datos y/o instrucciones para realizar las etapas reivindicadas.

Un “registro de anotación” hace referencia a información que pertenece a una o más actividades de usuario. Un registro de anotación puede ser un registro o fichero electrónico.

Un “proveedor de servicio” hace referencia a un proveedor de uno o más servicios electrónicos. Proveedores de servicio de ejemplo pueden incluir, sin limitación, proveedores de servicio de interconexión de red social, proveedores de servicio de correo electrónico, proveedor de servicio de motor de búsqueda y/o similares.

“Datos de usuario” hacen referencia a datos o información asociada con un usuario, una acción o actividad de un usuario en relación con un servicio, una cuenta de usuario y/o similares.

Un “identificador de usuario” puede ser un identificador único asociado con un usuario de un servicio.

Un proveedor de servicio puede recibir solicitudes de un usuario para borrar al menos una porción de los datos de usuario del usuario. El proveedor de servicio puede tener una política en lugar de cualesquiera solicitudes de borrado solicitadas por el usuario totalmente distinguidas dentro de un cierto periodo de tiempo (*t*) con relación a la solicitud de borrado del usuario (*dr*). Como tal, los registros de anotación relacionados con una solicitud de borrado deben borrarse dentro de *t* días de la solicitud. Además, para permitir que un intervalo de análisis (*i*) soporte por ejemplo, prevención de calidad y fraude, una política del proveedor de servicio puede especificar que el proceso de borrado no pueda borrar registros de anotación asociados con la actividad (*a*) hasta que sean al menos de *i* días de antigüedad. Como tal, el proceso de borrado debe asegurar que para cualquier actividad, a, los registros de anotación asociados se borrarán tan pronto como *dr*+*i* y no más tarde que *dr* + *t*. La Figura 1 ilustra una línea de tiempos de ejemplo de una solicitud de borrado de acuerdo con una realización.

La Figura 2 ilustra un diagrama de bloques de un sistema de borrado de ejemplo de acuerdo con una realización. Como se ilustra por la Figura 2, el sistema **200** puede incluir una tabla de claves **202**, una tabla de actividad de usuario **204**, una tubería de borrado **206** y uno o más registros de anotación **208**. Una tabla de claves **202** puede ser una estructura de datos configurada para almacenar una o más claves asociadas con uno o más identificadores de usuario.

En una realización, una tabla de claves **202** puede ser una tabla enlazada de manera sencilla plana que se indexa secuencialmente y contiene un campo de clave. Las claves pueden no ser únicas o enlazarse de manera consistente a un identificador de usuario particular, pero pueden generarse aleatoriamente. En una realización, una tabla de claves **202** puede incluir un número de generación que corresponde a una ejecución particular de la tubería de borrado. Aunque se denomina en esta divulgación como una tabla de claves, pueden usarse tipos de estructuras de datos alternativas tales como, por ejemplo, bases de datos, conjuntos y/o similares dentro del alcance de esta divulgación.

Una tabla de actividad de usuario **204** puede ser una estructura de datos configurada para almacenar una o más actividades de usuario codificadas por identificador de usuario. En una realización, una tabla de actividad de usuario **204** puede almacenar solicitudes de borrado realizadas por uno o más usuarios. En una realización, una o más entradas de una tabla de actividad de usuario **204** pueden asociarse con una indicación de tiempo, tal como, por ejemplo, un número de generación.

En una realización, una tubería de borrado **206** puede ser un proceso que recoge una o más solicitudes de borrado de la tabla de actividad de usuario **204** y las aplica a los registros de anotación **208**. Un registro de anotación puede ser una tabla, una base de datos, y serie y/o similares configuradas para almacenar información acerca de una o más actividades de usuario en relación con una cuenta de usuario o servicios de un proveedor de servicio. En una realización, un registro de anotación puede almacenar un identificador de usuario, una indicación de tiempo u otra indicación de cuándo tuvo lugar la actividad y/o similares.

En ciertas realizaciones, una tabla de claves, una tabla de actividad de usuario y uno o más registros de anotación pueden almacenarse en memoria asociada con uno o más dispositivos informáticos. En una realización, una tabla de claves, una tabla de actividad de usuario y registros de anotación pueden almacenarse en memoria asociada con el mismo dispositivo informático. Como alternativa, una tabla de claves, una tabla de actividad de usuario y registros de anotación pueden almacenarse en memoria asociada con diferentes dispositivos informáticos que comunican entre sí mediante una o más redes de comunicación. Una red de comunicación puede ser una red de área local (LAN), una red de área extensa (WAN), una red de comunicación móvil o celular, una extranet, una intranet, la Internet y/o similares.

De manera similar, una tubería de borrado puede ejecutarse por un dispositivo informático que está asociado con una tabla de claves, una tabla de actividad de usuario y/o registros de anotación. Como alternativa, una tubería de borrado puede ejecutarse con un dispositivo informático separado del dispositivo o dispositivos informáticos asociados con una tabla de claves, una tabla de actividad de usuario y/o registros de anotación.

La Figura 3 ilustra un diagrama de flujo de un método de ejemplo de borrado de datos de usuario de acuerdo con una realización. Como se ilustra por la Figura 3, puede recibirse **300** una solicitud de borrado. Puede recibirse **300** una solicitud de borrado de un usuario, y puede pertenecer a una o más actividades de usuario en relación con un servicio o proveedor de servicio. Por ejemplo, un usuario puede solicitar que se borre una consulta que realizó el usuario por un motor de búsqueda. Como otro ejemplo, un usuario puede solicitar que se borre el historial de búsqueda entero del usuario para el motor de búsqueda. Como otros ejemplos, una solicitud de borrado puede incluir una solicitud de que se borre la información asociada con una cuenta de usuario, o que se borre una cuenta de usuario completa. Si un proveedor de servicio es un proveedor de correo electrónico, una solicitud de borrado puede solicitar que se borren uno o más mensajes de correo electrónico. Pueden usarse también solicitudes de borrado adicionales y/o alternativas.

Una solicitud de borrado recibida puede almacenarse en una tabla de actividad de usuario junto con un identificador de usuario asociado con el usuario que realizó la solicitud. Una tabla de actividad de usuario puede estar asociada con una indicación de tiempo. Por ejemplo, haciendo referencia a la Figura **2**, la tabla de actividad de usuario incluye una entrada **210** asociada con el id de Usuario B para junio que corresponde a una solicitud de borrado que solicita el borrado de la actividad B.

Haciendo referencia de vuelta a la Figura 3, puede identificarse **302** un tiempo de finalización. Un tiempo de finalización, t, puede ser un periodo de tiempo dentro del cual un proveedor de servicio ha de cumplir una solicitud de borrado de un usuario. Por ejemplo, si t = 60 días, entonces los datos asociados con una solicitud de borrado deben borrarse dentro de no más de 60 días desde la fecha que se realizó la solicitud de borrado.

En una realización, un tiempo de intervalo de análisis, i, puede identificarse **304**. Un tiempo de intervalo de análisis puede indicar un periodo de tiempo durante el cual han de conservarse uno o más registros de anotación después de recibir una solicitud de borrado. Por ejemplo un proveedor de servicio puede tener una política de que uno o más registros de anotación asociados con una solicitud de borrado han de conservarse durante al menos 30 días después de que se reciba una solicitud de borrado. Como tal, un tiempo de intervalo de análisis puede ser 30 días después de que se reciba una solicitud de borrado.

Como un ejemplo, un intervalo de análisis puede ser 30 días, un tiempo de finalización puede ser 60 días, y una tubería de borrado puede ejecutarse el 1 de julio. Como tal, un registro de anotación para el que se realizó una solicitud de borrado el 1 de junio debe borrarse no más tarde del 1 de agosto. El intervalo de análisis puede distinguirse también, por lo que comenzar la tubería de borrado el 1 de julio permite 30 días de tiempo de recuperación de fallos para cada solicitud de borrado que afecta a registros con fecha de 30 de junio o más antiguos. En una realización, únicamente puede procesarse un día de registros por día del intervalo de análisis. Por ejemplo, el sistema puede procesar registros con fecha de 1 de junio el 1 de julio, puede procesar registros con fecha de 2 de junio el 2 de julio y así sucesivamente.

En una realización, si tiene lugar un error durante el proceso de borrado, el proceso puede poner al día registros de anotación procesando múltiples días de reserva de registros de anotación en un único día. Por ejemplo, pueden procesarse registros de anotación del 12, 13, 14 y 15 de junio el 15 de julio.

La Figura 4 ilustra un diagrama de flujo de un método de ejemplo de generación de una o más claves y creación de una lista de borrado de acuerdo con una realización. En una realización, puede generarse un índice para cada entrada en la tabla de actividad de usuario. Cada índice puede tener un valor único, y puede corresponder a una entrada en la tabla de claves. Un índice puede tener un valor numérico que puede generarse usando un contador incremental. La tabla de actividad de usuario **204** ilustrada en la Figura 2 muestra una captura de pantalla de dos filas de la tabla a través de un periodo de tres meses (junio, julio y agosto). Como se ilustra por la Figura 2, cada fila o entrada está asociada con un valor de índice y una indicación de tiempo correspondiente (por ejemplo, junio, julio o agosto). Por ejemplo, la entrada de tabla 210 asociada con el id de Usuario B para junio corresponde a un índice de '1', mientras que la entrada de tabla actualizada **212** asociada con el id de Usuario B para agosto corresponde a un índice de '3477'.

En una realización, una entrada en la tabla de actividad de usuario puede identificarse **400**. Puede determinarse **402** si la entrada identificada ya está asociada con un valor de índice de tabla de claves. Si una entrada en la tabla de actividad de usuario ya está asociada con un valor de índice de tabla de claves, el valor de índice actual puede almacenarse **404** e identificarse como el valor del índice anterior. Por ejemplo, un valor de índice de tabla de claves puede almacenarse **404** en una variable temporal denominada "prev-index." Un nuevo valor de índice de tabla de claves puede generarse **406** para la entrada, y el nuevo valor de índice de tabla de claves puede almacenarse **408** en la tabla de actividad de usuario de modo que está asociado con la entrada. En una realización, el nuevo valor de índice de tabla de claves puede almacenarse **408** en la tabla de actividad de usuario en lugar del valor de índice anterior.

Si la entrada no está ya asociada con un valor de índice de tabla de claves, entonces un nuevo valor de índice de tabla de claves puede generarse **406** para la entrada, y el nuevo valor de índice de tabla de claves puede almacenarse **408** en la tabla de actividad de usuario de modo que está asociado con la entrada.

En una realización, una clave aleatoria puede generarse **410** para la entrada de la tabla de actividad de usuario y almacenarse **412** en la tabla de claves de manera que corresponde al índice de tabla de claves asociado de la tabla de actividad de usuario. Por ejemplo, la entrada de tabla de actividad de usuario **210** asociada con el id de Usuario B para junio corresponde a un índice de '1'. Como se ilustra en la Figura 2, puede generarse **410** la Clave B de clave aleatoria para esta entrada de tabla de actividad de usuario **210** y almacenarse **412** en la tabla de claves de manera que corresponda al índice '1'.

En una realización, la tabla de claves puede almacenar también una indicación de tiempo, tal como, por ejemplo, un número de generación, asociado con una o más entradas de tabla de actividad de usuario. Un número de generación puede hacer referencia a una indicación de tiempo asociada con una entrada en la tabla de actividad de usuario tal como, por ejemplo, un día, una semana, un mes y/o similares. En una realización, un número de generación puede corresponder a un periodo de tiempo durante el cual se realiza una solicitud de borrado correspondiente. Por ejemplo, los números de generación ilustrados en la Figura 2 representan meses, representando g0 junio, representando g1 julio y representando g2 agosto. Como tal, la solicitud de borrado asociada con el id de Usuario A y g0 es una solicitud de borrado realizada por el usuario asociado con el id de Usuario de identificador A en junio.

En una realización, una o más entradas en la tabla de claves pueden incluir un puntero a atrás. Un puntero a atrás puede ser una referencia a una o más otras entradas en la tabla de claves. Por ejemplo, un puntero puede ser un tipo de datos cuyo valor hace referencia al índice de otra entrada en la tabla de claves. Un puntero a atrás puede hacer referencia a una entrada en la tabla de claves. Cuando se borra una entrada en la tabla de claves, puede ajustarse un puntero a atrás correspondiente para apuntar a una entrada diferente. En una realización, el valor de índice anterior almacenado para una entrada puede almacenarse en la tabla de claves como un puntero a atrás para la clave de generación anterior para el usuario asociado.

En una realización, un puntero a atrás puede apuntar desde una cierta entrada en la tabla de claves a una entrada anterior en la tabla de claves que está asociada con el mismo identificador de usuario. En una realización, un puntero a atrás puede apuntar a la siguiente entrada más reciente en la tabla de claves que está asociada con el mismo identificador de usuario. Por ejemplo, haciendo referencia a la Figura 2, la entrada **214** en la tabla de claves asociada con un valor de índice de 543 puede incluir un puntero a atrás a la entrada **216** en la tabla de claves asociada con un valor de índice de 0 puesto que esta es la siguiente entrada más reciente en la tabla de claves que está asociada con el mismo identificador de usuario, id de Usuario A. Si no hay entrada anterior en la tabla de claves que corresponde al identificador de usuario, entonces la entrada puede no incluir un puntero a atrás ya que esta entrada puede considerarse la entrada más antigua asociada con el identificador de usuario.

Puede determinarse **414** si la entrada identificada incluye una solicitud de borrado que se ha realizado desde la generación anterior. Por ejemplo, la tubería de borrado puede determinar **414** si la entrada identificada incluye una

solicitud de borrado. Si lo hace, la tubería de borrado puede determinar **416** si una indicación de tiempo asociada con la solicitud de borrado publica la última generación o análisis de tubería de borrado. En caso afirmativo, la tubería de borrado puede almacenar **418** la solicitud de borrado y el índice de tabla de claves asociado con la entrada en una lista de borrado. Una lista de borrado puede ser una lista ordenada en el tiempo de solicitudes de borrado. En una realización, una lista de borrado puede ordenarse de las solicitudes más antiguas a las solicitudes más nuevas. En una realización, una lista de borrado puede ser cualquier estructura de datos adecuada tal como, por ejemplo, una tabla, un gráfico, una base de datos, una lista y/o similares.

En una realización, una o más de las etapas de la Figura 4 puede repetirse para una o más entradas de la tabla de actividad de usuario. Por ejemplo, cada una de las etapas de la Figura 4 puede repetirse en cada entrada de una tabla de actividad de usuario hasta que se hayan considerado todas las entradas.

La Figura 5 ilustra un diagrama de flujo de un método de ejemplo de borrado de uno o más registros de anotación de acuerdo con una realización. Como se ilustra por la Figura 5, un periodo de tiempo de finalización puede identificarse **500**. Un periodo de tiempo de finalización puede ser un cierto periodo de tiempo con relación a una solicitud de borrado de usuario dentro del cual ha de distinguirse una solicitud de borrado. Por ejemplo, haciendo referencia de vuelta a la Figura 1, el periodo de tiempo entre *dr* y *t* puede considerarse el periodo de tiempo de finalización.

En una realización, un intervalo de análisis puede identificarse **502**. Un intervalo de análisis puede ser un periodo de tiempo antes del cual no puede procesarse una solicitud de borrado. Por ejemplo, haciendo referencia a la Figura 1, el periodo de tiempo entre *dr* y *i* puede considerarse el intervalo de análisis.

La tubería de borrado puede identificar **504** una entrada en la lista de borrado. Puede determinarse **506** si un registro de anotación asociado con la entrada identificada es más antiguo que el periodo de tiempo de finalización identificado. Por ejemplo, si un periodo de tiempo de finalización es sesenta días, la tubería de borrado puede determinar si se creó un registro de anotación hace más de sesenta días.

Si se determina **506** que el registro de anotación es más antiguo que el periodo de tiempo de finalización, entonces la tubería de borrado puede usar el índice de tabla de claves asociado de la lista de borrado para identificar **508** un número de generación asociado con el registro de anotación. La tubería de borrado puede usar el índice de tabla de claves asociado para identificar **510** una correspondiente entrada de tabla de claves. La tubería de borrado puede determinar **512** si la entrada de tabla de claves identificada corresponde al número de generación identificado. En caso afirmativo, la tubería de borrado puede borrar **514** la entrada en la tabla de claves, y puede ajustar **516** los punteros a atrás según sea necesario.

En una realización, si la entrada de tabla de claves identificada no corresponde al número de generación identificado, la tubería de borrado puede atravesar **518** uno o más punteros a atrás hasta que localice la entrada en la tabla de claves que corresponde al número de generación identificado. La tubería de borrado puede borrar **514** la entrada en la tabla de claves, y puede ajustar **516** los punteros a atrás según sea necesario.

Por ejemplo, la actividad de usuario asociada con la entrada **218** de la tabla de actividad de usuario puede borrarse, y esta entrada puede ser más antigua que el tiempo de intervalo de análisis. La tubería de borrado puede buscar su índice, “544”, en la tabla de actividad de usuario, y puede usar este índice para localizar la clave correspondiente en la tabla de claves (es decir, la Clave B). La tubería de borrado puede borrar la Clave B asociada con la entrada en la tabla de claves, y puede ajustar los punteros a atrás de modo que la entrada posterior para el identificador de usuario **222** apunte a atrás a la entrada anterior para el identificador de usuario **224**. La Figura 8 ilustra una tabla de claves de ejemplo después de que la clave asociada con la entrada **220** se haya borrado de la tabla de claves de acuerdo con una realización.

La Figura 6 ilustra un diagrama de flujo de un método de ejemplo de depuración de uno o más registros de anotación de acuerdo con una realización. Como se ilustra por la Figura 6, puede identificarse **600** una ventana de depuración. Una ventana de depuración puede ser un periodo de tiempo que tiene lugar después de la finalización de un intervalo de análisis pero antes del periodo de la finalización de un tiempo de finalización. Por ejemplo, si un periodo de tiempo de finalización es sesenta días desde una solicitud de borrado, y un intervalo de análisis es treinta días desde la solicitud de borrado, una ventana de depuración puede incluir uno o más registros que se ven afectados por la solicitud de borrado y tienen más de treinta días de antigüedad, pero menos que o igual a setenta días de antigüedad.

En una realización, puede identificarse **602** uno o más registros de anotación dentro de la ventana de depuración. Para cada registro de anotación identificado, puede determinarse **604** si ha de borrarse el registro de anotación. Por ejemplo, puede determinarse si un registro de anotación identificado está incluido en la lista de borrado. Si lo está, entonces puede determinarse **604** que el registro de anotación ha de borrarse. Si no lo está, entonces puede determinarse **604** que el registro de anotación no ha de borrarse.

Si ha de borrarse el registro de anotación, la tubería de borrado puede depurar **606** físicamente el registro de anotación. Si no ha de borrarse el registro de anotación, la tubería de borrado puede buscar **608** el identificador de usuario asociado con el registro de anotación en la tabla de actividad de usuario, y usar el índice almacenado para recuperar **610** la clave asociada de la tabla de claves. Por ejemplo, haciendo referencia a la Figura 2, el sistema puede determinar que el registro de anotación **208**a no ha de borrarse. La tubería de borrado puede usar el identificador de usuario (Usuario A) y el número de generación (g0) del registro de anotación para recuperar el índice correspondiente (es decir, "0") en la tabla de actividad de usuario.

La tubería de borrado puede usar el índice para recuperar **610** la correspondiente clave de la tabla de claves. Por ejemplo, usando el ejemplo anterior, la tubería de borrado puede usar el índice "0" para recuperar **610** la clave Clave A de la tabla de claves. La tubería de borrado puede encriptar **612** al menos una porción del registro de anotación usando la clave recuperada y puede escribir **614** el valor encriptado y el valor de índice al registro de anotación. En diversas realizaciones, otros datos que pueden almacenarse en un registro de anotación pueden encriptarse usando la clave recuperada tal como, por ejemplo, el identificador de usuario. En una realización, este contenido puede no incluir un índice o un número de generación, ya que estos datos pueden no estar incluidos en el proceso de encriptación. En una realización, la velocidad de procesamiento puede basarse en, al menos en parte, el contenido de cantidad del registro de anotación que se encripta.

En una realización, si la tubería de borrado procesa una solicitud para múltiples borrados entonces la tubería de borrado puede seguir punteros a atrás, volver a enlazar las entradas y borrar múltiples claves según sea necesario.

El método de borrado de datos de usuario como se describe en el presente documento proporciona varias salvaguardas con respecto a privacidad de usuario. En primer lugar, la tubería de borrado puede ser el único componente de sistema para tener acceso a la tabla de claves. Esto minimiza el acceso a claves y datos de usuario. En segundo lugar, en este sistema, el identificador de usuario no se almacena con su clave. En su lugar, se almacena un índice a la tabla de claves en registros de anotación, una tabla de actividad de usuario, y/o similares. En tercer lugar, una vez que se borra una clave de la tabla de claves, los datos de registro asociados con la correspondiente entrada de tabla de claves son desconocidos. Y finalmente, incluso si la tabla de claves se viera de alguna manera comprometida, el identificador de usuario de un registro borrado no podría inferirse debido a que la entrada de tabla de claves para un registro borrado no tiene punteros a atrás a otras claves para el identificador de usuario.

En situaciones en las que los sistemas analizados en este punto recopilan información personal acerca de usuarios, o pueden hacer uso de información personal, puede proporcionarse a los usuarios con una oportunidad para controlar si los programas o características recopilan información de usuario, o para controlar si y/o cómo recibir contenido que puede ser más relevante para el usuario. Además, ciertos datos pueden tratarse de una o más maneras antes de que se almacenen o usen de modo que se elimina información personalmente identificable. Por ejemplo, puede tratarse una identidad del usuario de modo que no pueda determinarse información personalmente identificable para el usuario, o puede generalizarse una localización geográfica del usuario donde se obtiene información de localización (tal como para una ciudad, código postal, o nivel de estado), de modo que no puede determinarse una localización particular de un usuario. Por lo tanto, el usuario puede tener control sobre cómo se recopila y/o almacena información acerca del usuario y se usa por el sistema.

La Figura 7 representa un diagrama de bloques de hardware que puede usarse para contener o implementar instrucciones de programa. Un bus **700** sirve como la autopista de información principal que interconecta los otros componentes del hardware ilustrados. La CPU **705** es la unidad de procesamiento central del sistema, que realiza cálculos y operaciones lógicas requeridas para ejecutar un programa. La CPU **705**, en solitario o en conjunto con uno o más de los otros elementos analizados en la Figura 7, es un ejemplo de un ordenador, dispositivo informático o procesador ya que tales términos se usan dentro de esta divulgación. La memoria de sólo lectura (ROM) **710** y la memoria de acceso aleatorio (RAM) **715** constituyen ejemplos de medio de almacenamiento legible por ordenador no transitorio.

Un controlador **720** interconecta con uno o más medios de almacenamiento legibles por ordenador no transitorios **725** opcionales al bus de sistema **700**. Estos medios de almacenamiento **725** pueden incluir, por ejemplo, una unidad de DVD externa o interna, una unidad de CD ROM, un disco duro, memoria flash, una unidad de USB o similares. Como se ha indicado previamente, estas diversas unidades y controladores son dispositivos opcionales.

Las instrucciones de programa, software o módulos interactivos para proporcionar la interfaz y realizar cualquier consulta o análisis asociados con uno o más conjuntos de datos pueden almacenarse en la ROM **710** y/o la RAM **715**. Opcionalmente, las instrucciones de programa pueden almacenarse en un medio legible por ordenador tangible no transitorio tal como un disco compacto, un disco digital, memoria flash, una tarjeta de memoria, una unidad de USB, un medio de almacenamiento de disco óptico y/u otro medio de grabación.

Una interfaz de visualización opcional **730** puede permitir que se visualice información del bus **700** en la pantalla **735** en formato de audio, visual, gráfico o alfanumérico. La comunicación con dispositivos externos, tales como un dispositivo de impresión, puede tener lugar usando diversos puertos de comunicaciones **740**. Un puerto de

comunicación **740** puede conectarse a una red de comunicación, tal como Internet o una intranet.

El hardware puede incluir también una interfaz **745** que permite la recepción de datos de dispositivos de entrada tales como un teclado **750** u otro dispositivo de entrada **755** tal como un ratón, una palanca de mandos, una pantalla táctil, un control remoto, un dispositivo apuntador, un dispositivo de entrada de vídeo y/o un dispositivo de entrada de audio.

Se apreciará que diversas de las características y funciones anteriormente desveladas y otras, o alternativas de las mismas, pueden combinarse de manera deseable en muchos otros diferentes sistemas o aplicaciones o combinaciones de sistemas y aplicaciones. También se pretende que diversas alternativas, modificaciones, variaciones o mejoras no previstas o no anticipadas en las mismas que pueden realizarse satisfactoriamente por los expertos en la materia estén abarcadas por las siguientes reivindicaciones.

REIVINDICACIONES

1. Un método de borrado de registros de anotación, comprendiendo el método:
identificar, por un dispositivo informático a partir de una base de datos de registros de anotación, una pluralidad de registros de anotación generados durante un periodo de tiempo, en el que cada registro de anotación corresponde a una actividad de usuario; y
para cada registro de anotación identificado:
determinar, por el dispositivo informático, si se ha realizado una solicitud de borrado asociada con el registro de anotación, y
en respuesta a la determinación de que no se ha recibido una solicitud de borrado:
identificar un identificador único asociado con el registro de anotación, buscar en una tabla de actividad de usuario, configurada para almacenar una o más actividades de usuario codificadas por un respectivo identificador de usuario, para una entrada que tiene un índice de tabla de claves asociado con el identificador único, en el que la entrada está asociada con una indicación de tiempo,
después de la búsqueda de la tabla de actividad de usuario, usar el índice de tabla de claves y la indicación de tiempo para identificar una clave asociada con el identificador único y la indicación de tiempo de una tabla de claves,
después de la identificación de la clave, encriptar, por el dispositivo informático, al menos una porción del registro de anotación con la clave identificada para generar un valor encriptado, y
después de la generación del valor encriptado, almacenar el valor encriptado como una entrada en la base de datos de registros de anotación que está asociada con el registro de anotación identificado.

2. El método de la reivindicación 1, en el que identificar una pluralidad de registros de anotación generados durante un periodo de tiempo comprende identificar una pluralidad de registros de anotación que se generan después de una finalización de un intervalo de análisis pero antes de una finalización de un periodo de tiempo de finalización.

3. El método de la reivindicación 1, en el que encriptar al menos una porción del registro de anotación con la clave identificada para generar un valor encriptado, comprende encriptar uno o más de lo siguiente:
el identificador único, y
la actividad de usuario.

4. El método de la reivindicación 1, que comprende adicionalmente:
recibir una segunda solicitud de borrado, en el que la segunda solicitud de borrado indica que el registro de anotación ha de borrarse;
identificar un identificador único y una indicación de tiempo asociada con el registro de anotación;
buscar la tabla de actividad de usuario para un índice de tabla de claves asociado con el identificador único del registro a borrarse;
usar el índice de tabla de claves para identificar una entrada en la tabla de claves que corresponde a la indicación de tiempo del registro de anotación; y
borrar una clave asociada con la entrada identificada de la tabla de claves.

5. El método de la reivindicación 1, en el que borrar la clave comprende:
identificar un primer puntero a atrás de la entrada identificada a una entrada anterior en la tabla de claves;
identificar un segundo puntero a atrás de una entrada posterior en la tabla de claves a la entrada identificada;
borrar el primer puntero a atrás; y
ajustar el segundo puntero a atrás de modo que apunte a la entrada anterior en la tabla de claves.

6. El método de la reivindicación 1, en el que la segunda solicitud de borrado comprende uno o más de lo siguiente:
una solicitud para borrar una cierta acción de actividad web; y
una solicitud para borrar una cuenta de usuario.

7. El método de la reivindicación 1, que comprende adicionalmente:
recibir una tercera solicitud de borrado, en el que la tercera solicitud de borrado indica una pluralidad de registros de anotación a borrarse;
para cada uno de la pluralidad de registros de anotación a borrarse:
identificar un identificador único y una indicación de tiempo asociada con el registro de anotación a borrarse,
buscar la tabla de actividad de usuario para una entrada que tiene un índice de tabla de claves asociado con el identificador único del registro a borrarse,
usar el índice de tabla de claves asociado con la entrada para identificar una entrada en la tabla de claves que corresponde a la indicación de tiempo asociada con el registro de anotación, y
borrar una clave asociada con la entrada identificada de la tabla de claves.

8. El método de la reivindicación 7, en el que borrar la clave comprende:
identificar un primer puntero a atrás de la entrada identificada a una entrada anterior en la tabla de claves;
identificar un segundo puntero a atrás de una entrada posterior en la tabla de claves a la entrada identificada;
borrar el primer puntero a atrás; y
ajustar el segundo puntero a atrás de modo que apunte a la entrada anterior en la tabla de claves.

9. El método de la reivindicación 1, que comprende adicionalmente, para cada entrada en la tabla de actividad de usuario:
generar el índice de valor de clave asociado con la entrada, en el que el índice de tabla de claves corresponde a una entrada en una tabla de claves,
generar una clave aleatoria asociada con la entrada;
almacenar la clave aleatoria en la tabla de claves en el índice de tabla de claves;
determinar si la entrada incluye una solicitud de borrado; y
en respuesta a la determinación de que la entrada incluye una solicitud de borrado, añadir la solicitud de borrado y una indicación de tiempo de un registro de anotación asociado con la solicitud de borrado a una lista de borrado.

10. El método de la reivindicación 9, en el que determinar si se ha realizado una solicitud de borrado asociada con el registro de anotación comprende determinar si la solicitud de borrado está presente en la lista de borrado.

11. Un sistema de borrado de registros de anotación, comprendiendo el sistema:
un dispositivo informático; y
un medio de almacenamiento legible por ordenador en comunicación con el dispositivo informático, en el que el medio de almacenamiento legible por ordenador comprende una o más instrucciones de programación que, cuando se ejecuta, provocan al dispositivo informático:
identificar una pluralidad de registros de anotación generados durante un periodo de tiempo, en el que cada registro de anotación corresponde a una actividad de usuario, y
para cada registro de anotación identificado:
determinar si se ha realizado una solicitud de borrado asociada con el registro de anotación,
en respuesta a la determinación de que no se ha recibido una solicitud de borrado:
identificar un identificador único asociado con el registro de anotación,
buscar una tabla de actividad de usuario, configurada para almacenar una o más actividades de usuario codificadas por un respectivo identificador de usuario, para una entrada que tiene un índice de tabla de claves asociado con el identificador único, en el que la entrada está asociada con una indicación de tiempo,
después de la búsqueda de la tabla de actividad de usuario, usar el índice de tabla de claves y la indicación de tiempo para identificar una clave asociada con el identificador único y la indicación de tiempo de una tabla de claves,
después de la identificación de la clave, encriptar, por el dispositivo informático, al menos una porción del registro de anotación con la clave identificada para generar un valor encriptado, y
después de la generación del valor encriptado, almacenar el valor encriptado como una entrada en la base de datos de registros de anotación que está asociada con el registro de anotación identificado.

12. El sistema de la reivindicación 10 que está adaptado para llevar a cabo el método de acuerdo con una cualquiera de las reivindicaciones 2 a 10.

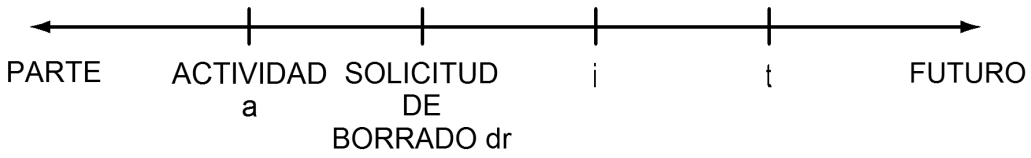

FIG. 1

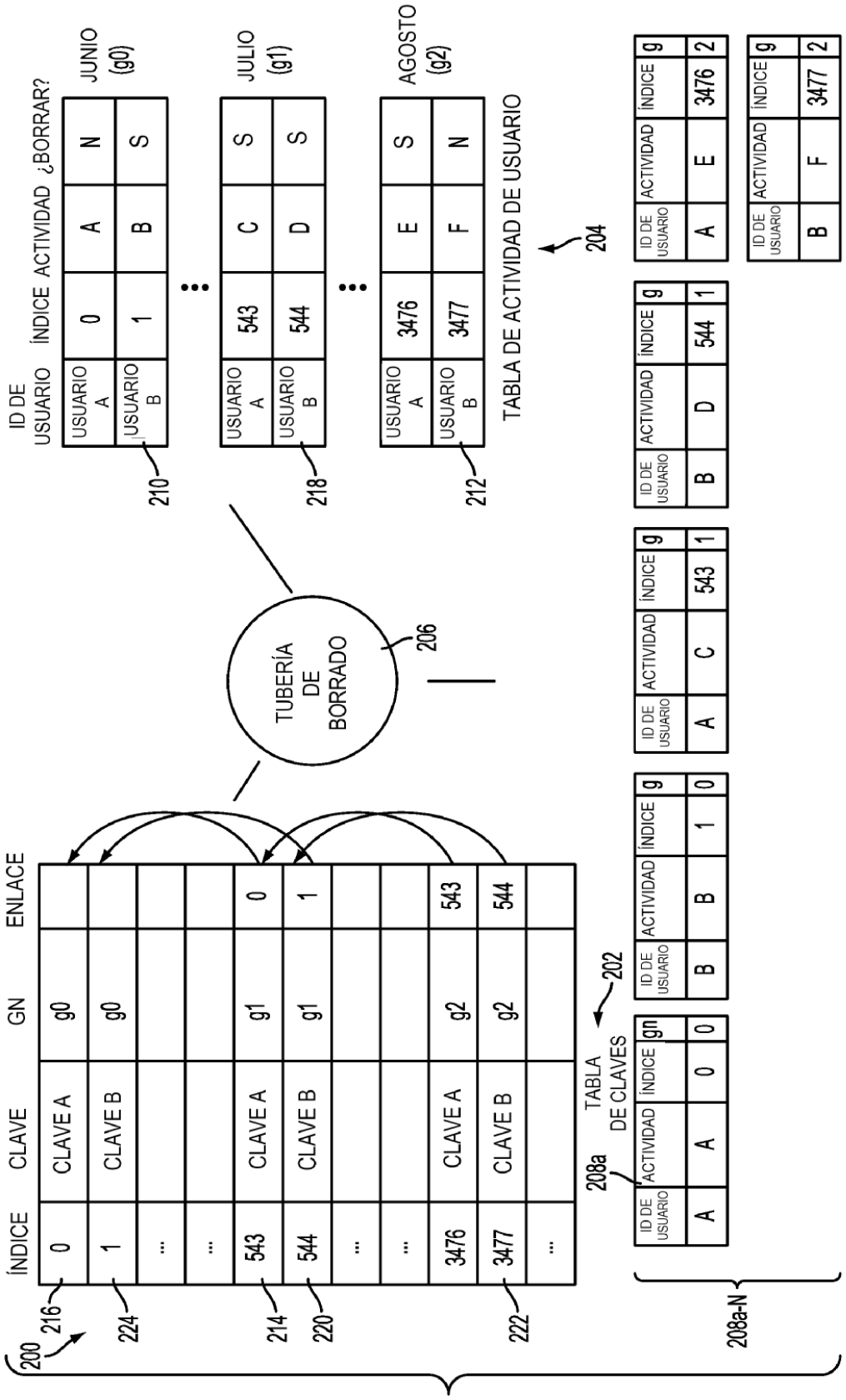
ÍNDICE
CLAVE
GN
ENLACE
CLAVE A
CLAVE B
g0
g1
g2
TUBERÍA DE BORRADO
206
TABLA DE CLAVES
202
208a
208a-N
200
216
224
214
220
222
ID DE USUARIO
ACTIVIDAD
¿BORRAR?
JUNIO (g0)
JULIO (g1)
AGOSTO (g2)
USUARIO A
USUARIO B
210
218
212
TABLA DE ACTIVIDAD DE USUARIO
204

FIG. 2

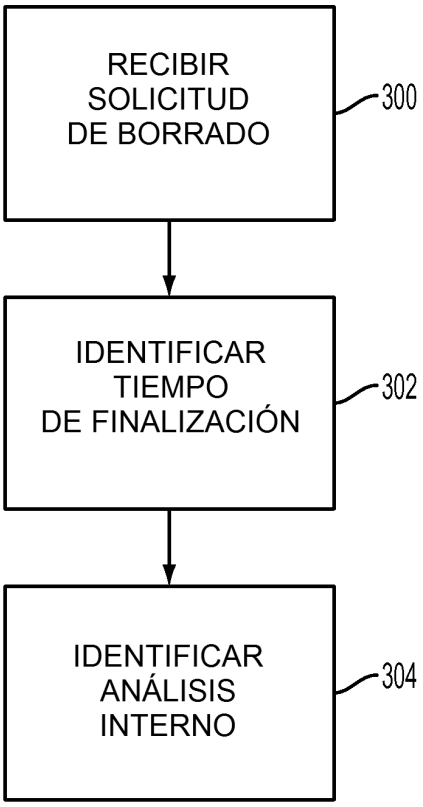
RECIBIR SOLICITUD DE BORRADO
300
IDENTIFICAR TIEMPO DE FINALIZACIÓN
302
IDENTIFICAR ANÁLISIS INTERNO
304

FIG. 3

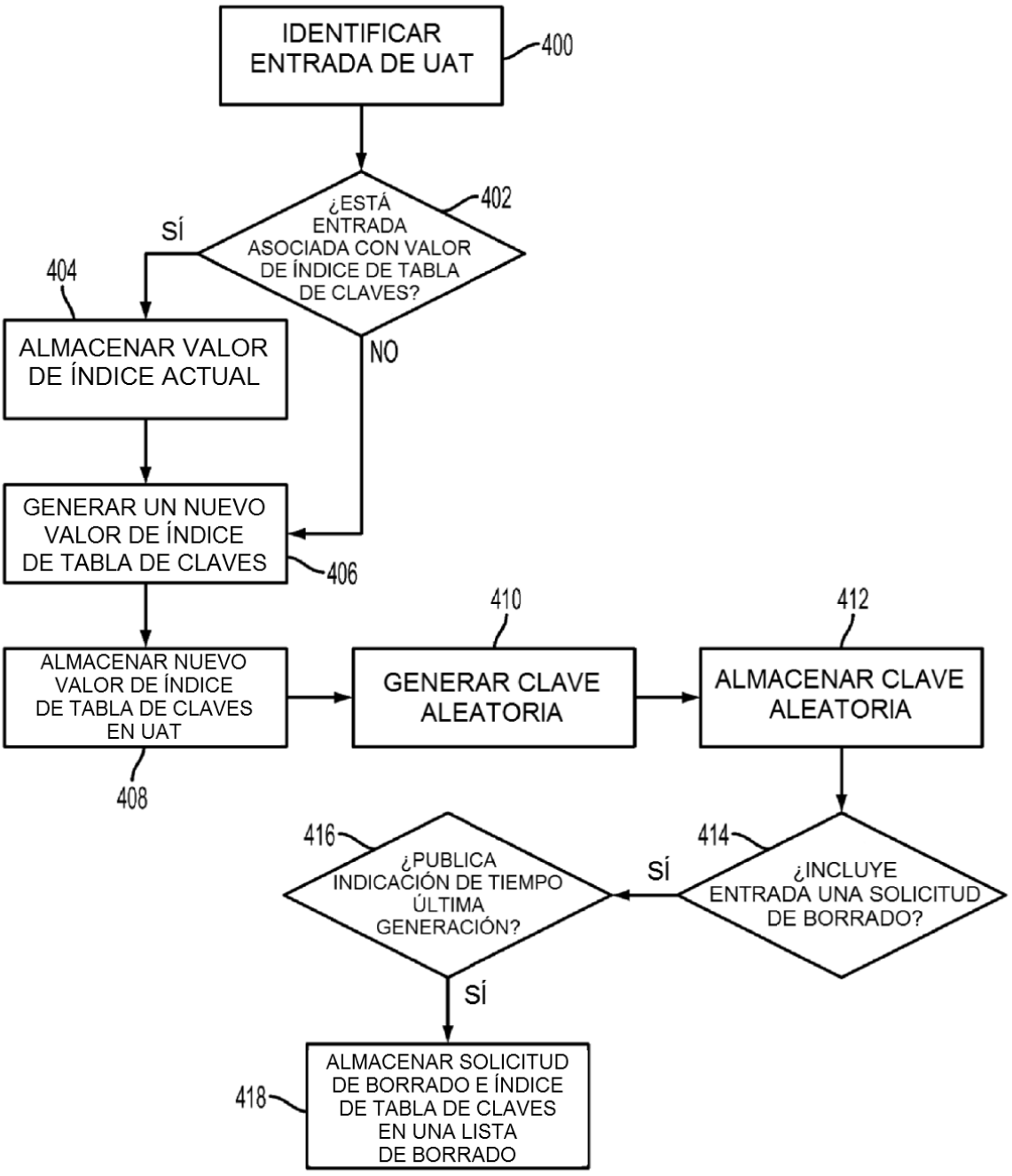
IDENTIFICAR ENTRADA DE UAT
400
¿ESTÁ ENTRADA ASOCIADA CON VALOR DE ÍNDICE DE TABLA DE CLAVES?
402
SÍ
NO
404
ALMACENAR VALOR DE ÍNDICE ACTUAL
GENERAR UN NUEVO VALOR DE ÍNDICE DE TABLA DE CLAVES
406
ALMACENAR NUEVO VALOR DE ÍNDICE DE TABLA DE CLAVES EN UAT
408
410
GENERAR CLAVE ALEATORIA
412
ALMACENAR CLAVE ALEATORIA
414
¿INCLUYE ENTRADA UNA SOLICITUD DE BORRADO?
SÍ
416
¿PUBLICA INDICACIÓN DE TIEMPO ÚLTIMA GENERACIÓN?
SÍ
418
ALMACENAR SOLICITUD DE BORRADO E ÍNDICE DE TABLA DE CLAVES EN UNA LISTA DE BORRADO

FIG. 4

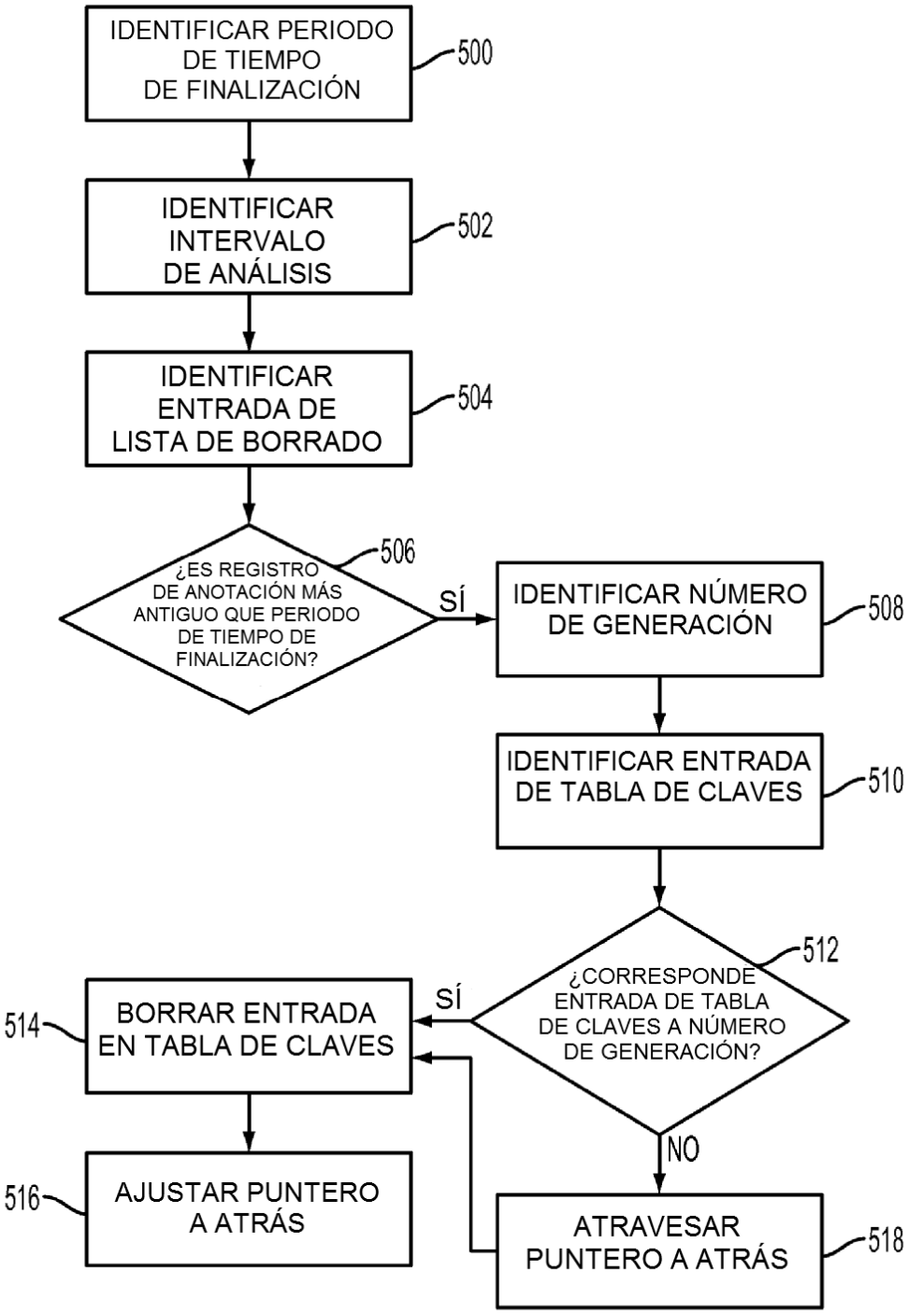
IDENTIFICAR PERIODO DE TIEMPO DE FINALIZACIÓN
500
IDENTIFICAR INTERVALO DE ANÁLISIS
502
IDENTIFICAR ENTRADA DE LISTA DE BORRADO
504
¿ES REGISTRO DE ANOTACIÓN MÁS ANTIGUO QUE PERIODO DE TIEMPO DE FINALIZACIÓN?
506
SÍ
IDENTIFICAR NÚMERO DE GENERACIÓN
508
IDENTIFICAR ENTRADA DE TABLA DE CLAVES
510
¿CORRESPONDE ENTRADA DE TABLA DE CLAVES A NÚMERO DE GENERACIÓN?
512
SÍ
NO
BORRAR ENTRADA EN TABLA DE CLAVES
514
AJUSTAR PUNTERO A ATRÁS
516
ATRAVESAR PUNTERO A ATRÁS
518

FIG. 5

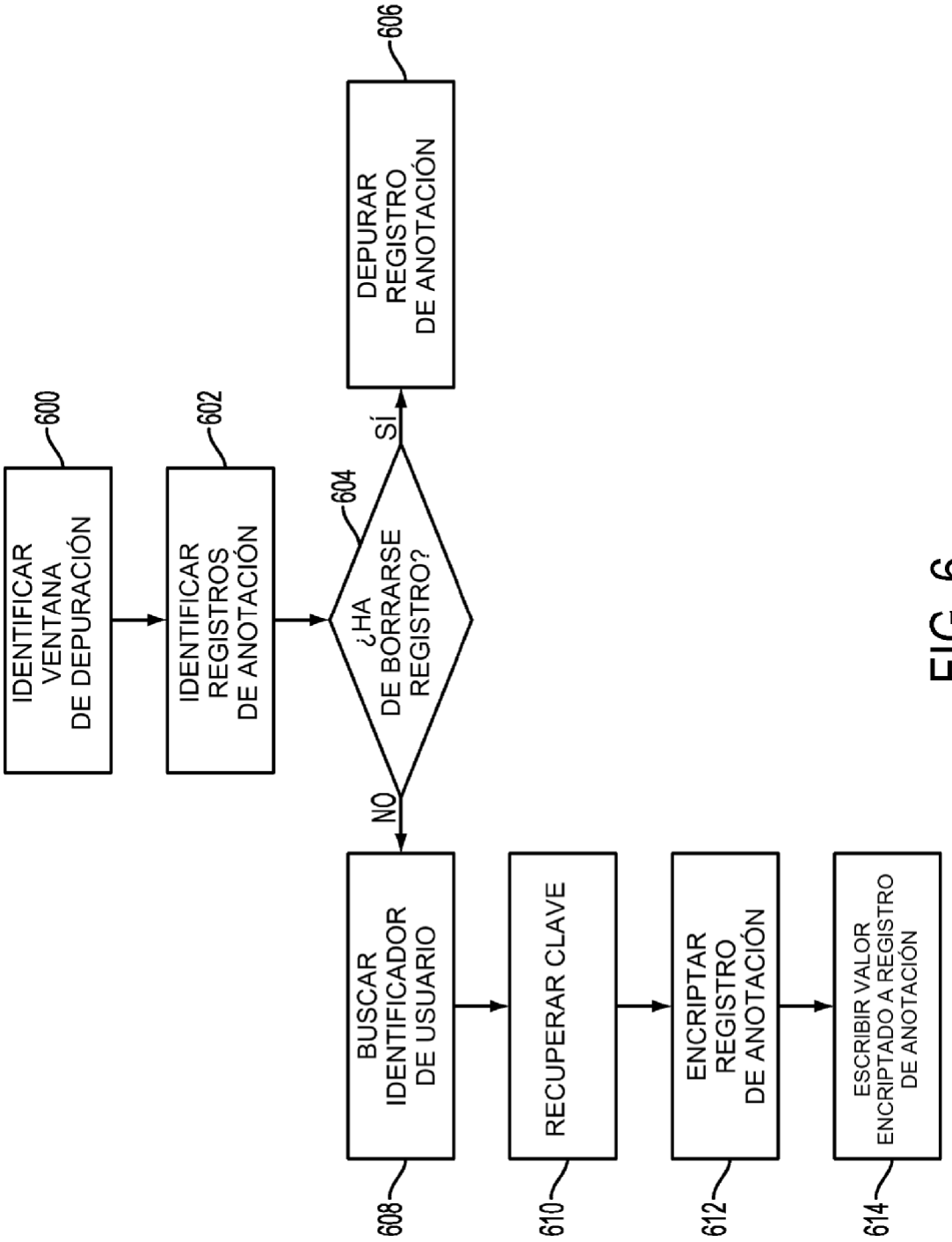
600
IDENTIFICAR VENTANA DE DEPURACIÓN
602
IDENTIFICAR REGISTROS DE ANOTACIÓN
604
¿HA DE BORRARSE REGISTRO?
SÍ
606
DEPURAR REGISTRO DE ANOTACIÓN
NO
608
BUSCAR IDENTIFICADOR DE USUARIO
610
RECUPERAR CLAVE
612
ENCRIPTAR REGISTRO DE ANOTACIÓN
614
ESCRIBIR VALOR ENCRIPTADO A REGISTRO DE ANOTACIÓN

FIG. 6

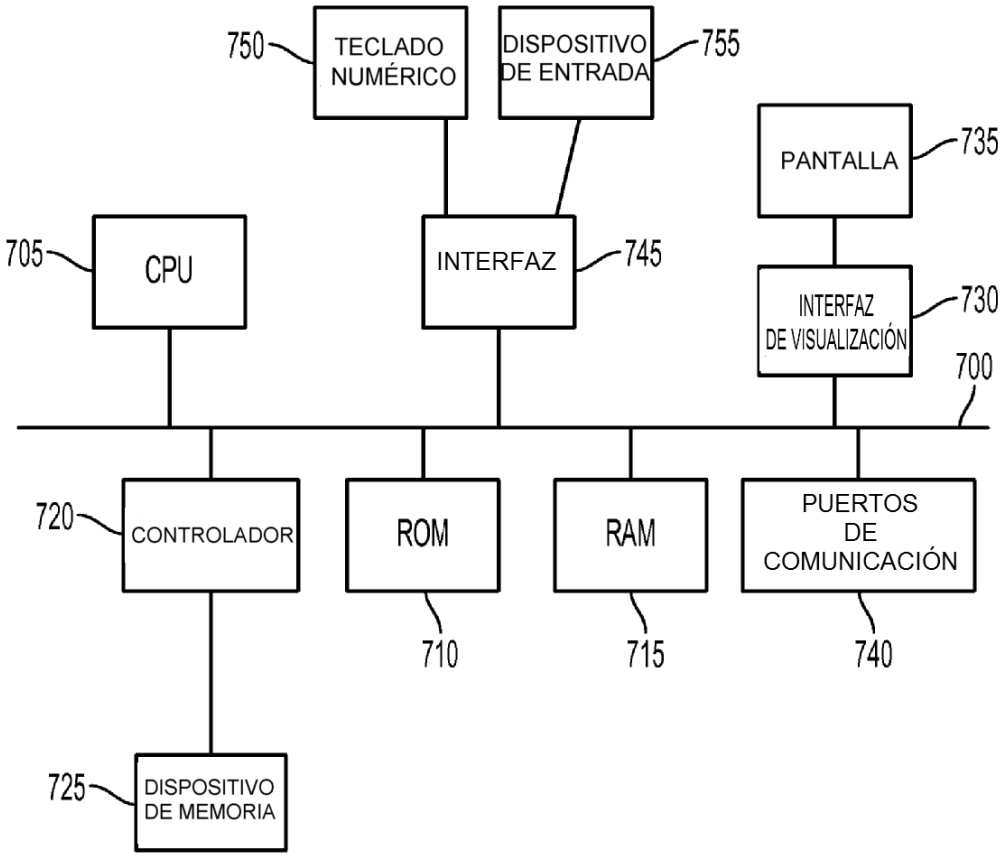
750
TECLADO NUMÉRICO
DISPOSITIVO DE ENTRADA
755
PANTALLA
735
705
CPU
INTERFAZ
745
INTERFAZ DE VISUALIZACIÓN
730
700
720
CONTROLADOR
ROM
RAM
PUERTOS DE COMUNICACIÓN
710
715
740
725
DISPOSITIVO DE MEMORIA

FIG. 7

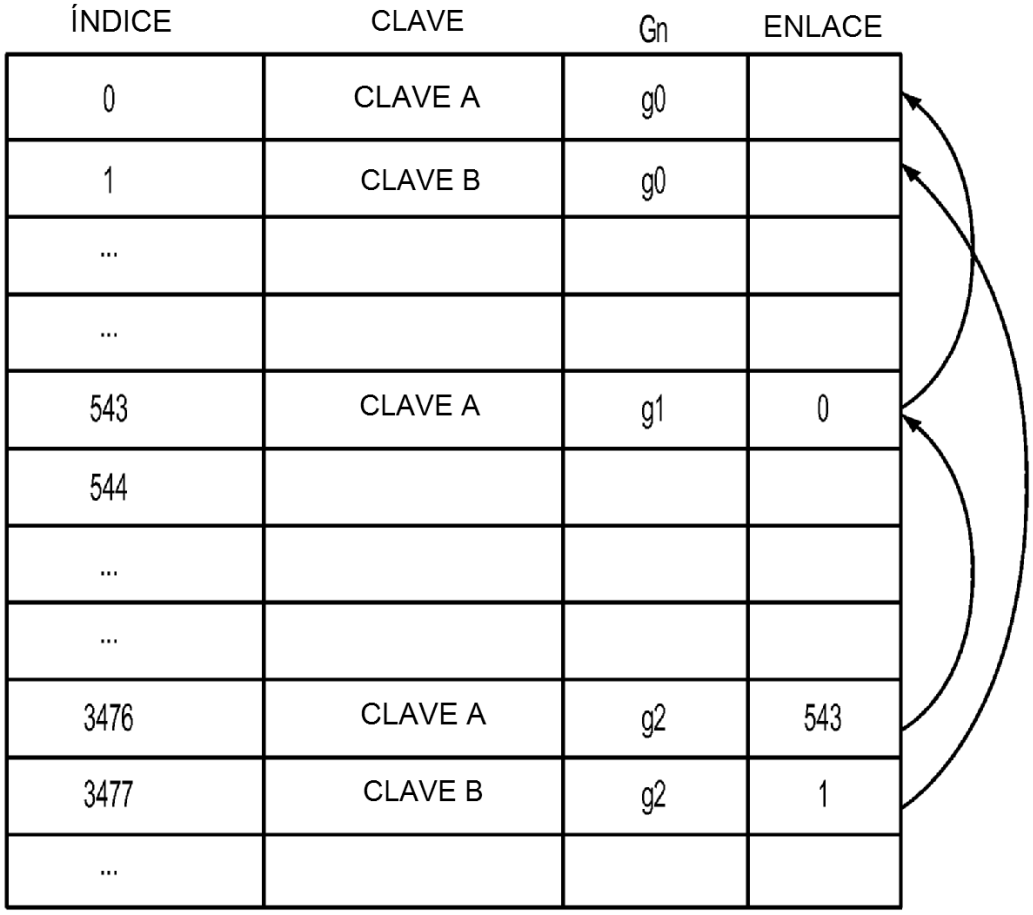
ÍNDICE
CLAVE
Gn
ENLACE
0
CLAVE A
g0
1
CLAVE B
g0
...
...
543
CLAVE A
g1
0
544
...
...
3476
CLAVE A
g2
543
3477
CLAVE B
g2
1
...
TABLA DE CLAVES

FIG. 8