(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 525 527**

(51) Int. CI.:

H04L 12/24 (2006.01)
H04L 12/26 (2006.01)
H04L 29/08 (2006.01)
G06F 11/14 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **09.01.2005 E 05703070 (2)**

(97) Fecha y número de publicación de la concesión europea: **17.09.2014 EP 1706960**

(54) Título: **Aparato y procedimiento para controlar y auditar la actividad de un entorno heredado**

(30) Prioridad:

07.01.2004 US 534404 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
26.12.2014

(73) Titular/es:

INTELLINX LTD. (100.0%)
1C YONI NETANYAHU STREET P.O. BOX 1035
60200 OR YEHUDA, IL

(72) Inventor/es:

KRELBAUM, BOAZ y
MINTZ-DOV, ORNA

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Aparato y procedimiento para controlar y auditar la actividad de un entorno heredado

Campo de la invención

La presente invención se refiere al control y a la auditoría de la actividad de un entorno heredado.

Antecedentes de la invención

En el documento US 6,192,411 ("*Mapeo de control de flujo de sesión SNA para controlar el flujo TCP*", publicado en 2001) divulga un servidor TN3270 que reenvía un flujo de datos 3270 desde una conexión de una Arquitectura de Red de Sistema (SNA) a una conexión del Protocolo de Control de Transmisión (TCP) que controla la conexión TCP para segmentos que reconocen los bytes transmitidos por esta vía. El servidor TN3270 mantiene el seguimiento de los tamaños de ventana de los bytes no confirmados especificados por los segmentos de conexión TCP. Responde con una respuesta a una solicitud a ritmo constante que contiene el mensaje SNA solo cuando el reenvío de la información previamente recibida de la SNA puede ser completada sin que se traduzca en un número de bytes no confirmados que sobrepase el tamaño de la ventana específica.

El documento US 4,575,793 ("Ordenador personal respecto de aparato de disposición en interfaz de sistemas 3270", publicado en 1986) divulga un aparato para disponer en interfaz un ordenador personal con un controlador clúster compatible 3274/6 de un sistema tipo 3270, empleando el aparato un procesador especial a gran velocidad.

El documento WO 03,073,724 ("Sistema y procedimiento para detectar y eliminar la suplantación IP en una red de transmisión de datos", publicado en 2004) y el documento US 2003/110394 (*"Sistema y procedimiento para detectar y eliminar la suplantación de IP en una red de transmisión de datos"*, publicado en 2003) divulgan un sistema de gestión de tráfico que rastrea selectivamente datos que llegan de cualquier punto de un sistema. El rastreador selectivo opera para extraer determinados datos a partir de cualquier dirección. Estos datos de direcciones IP y los datos de direcciones físicas. Los datos extraídos son a continuación utilizados para acceder a bases de datos diferentes para determinar si se produce una correspondencia. Inserción de marcas temporales, secuenciación y otros parámetros de cada pieza de datos que entran en un sistema son utilizados para controlar el acceso a datos.

El documento WO 02/100,039 ("*Sistema y procedimiento para el control de gestión de tráfico en una red de transmisión de datos"*, publicada en 2002) divulga un sistema de gestión de tráfico que rastrea selectivamente datos que llegan a cualquier punto de un sistema. El rastreador selectivo opera para recordar determinados parámetros que pertenecen a los datos. Cuando la cantidad de datos que llegan al punto comienza a alcanzar un nivel crítico (generalmente dependiente de la capacidad de procesamiento de datos asociada con el punto), el sistema comienza a eliminar (y compartir) los datos posteriores que llegan en base, en parte, a los parámetros recordados de los datos recientemente recibidos. Los datos que son almacenados son devueltos al sistema cuando el umbral crítico retrocede.

El documento WO 02/087124 (*"Analizador / Rastreador selectivo de red con múltiples capacidades de protocolo"*, publicada en 2002) divulga unos sistemas y unos procedimientos para la comprobación automática de múltiples entornos de red en los que los datos que son formateados con una pluralidad de protocolos en secuencia son automáticamente identificados y comparados para determinar si los datos han sido correctamente transformados de cada protocolo al siguiente. Una indicación acerca de si los datos han sido correctamente transformados puede ser presentada a un usuario, junto con la información acerca de los propios datos, como por ejemplo comandos que pueden ser incluidos en ellos. La información presentada al usuario se ofrece en una forma legible por el usuario mejor que en datos brutos con el fin de facilitar el análisis de la información por parte del usuario.

El documento US 6,044,401 ("*Rastreador selectivo de red para controlar y dar cuenta de una información de red que no es privilegiada más allá de un nivel de privilegio del usuario"*, publicado en 2000) divulga un procedimiento y un sistema para localizar la información disponible en un entorno de red por un usuario de un nodo. En un aspecto del sistema, dentro de un nodo de la red, el sistema divulgado en el documento US 6,044,401 incluye un rastreador selectivo de red y un rastreador selectivo de acceso. El rastreador de acceso incluye un elemento de acceso y una interfaz de acceso. El elemento de acceso incluye, de modo preferente, una memoria y una base de datos. El elemento de acceso accede al rastreador selectivo de red y filtra la información no disponible utilizando informaciones tales como los números de la dirección y el puerto recogidos por el rastreador selectivo de red. La información no disponible incluye la información que no es pública o que está más allá del nivel de privilegio del usuario concreto. El elemento de acceso evalúa los flujos de datos que son información pública para determinar si los flujos de datos satisfacen criterios predeterminados. Si los flujos de datos satisfacen los criterios predeterminados, entonces los datos se guardan en la base de datos. El elemento de acceso transfiere solo la información disponible al usuario concreto hacia la interfaz de acceso. El elemento de acceso puede establecerse un tiempo durante una cantidad de tiempo destinada a la ejecución. Una vez que el periodo de tiempo predeterminado ha expirado, el elemento de acceso está completo y puede conservar y transferir la información apropiada a la interfaz de acceso.

El documento US 5,961,592 ("*Sistema de identificación por pantalla"*, publicado en 1999) divulga un procedimiento de identificación de pantallas de ordenador. El procedimiento es especialmente útil en la identificación de pantallas anfitrión de IBM en la creación de guiones y reproducción. De acuerdo con el procedimiento, se compone una firma para una pantalla determinada. La firma comprende características de una pantalla determinada que diferencian esa pantalla de representaciones en pantalla sustancialmente diferentes. Para una pantalla de anfitrión de IBM, la composición de firmas se basa en las pantallas de campos protegidos. Los campos protegidos son ulteriormente procesados mediante la retirada de información transitoria como por ejemplo la fecha y el tiempo.

El documento US 5,644,717 (*"Sistema para la generación de red de área local que opera estadísticas en base a un tráfico de red controlado y procedimiento al efecto"*, publicado en 1997) divulga un sistema para la generación de estadísticas operativas para una red que interconecta al menos dos estaciones en el que cada una de esas estaciones puede enviar y recibir mensajes durante una sesión que es implementada en software programado para controlar los mensajes existentes en la red, asignar una dirección a cada uno de los mensajes en base a la etapa de control, determinar el papel asumido por cada una de las estaciones en base a la etapa de asignación y calcular las estadísticas para una de las estaciones en base a la etapa de determinación.

El documento US 2003/0135612 divulga unos sistemas y unos procedimientos de registro del tráfico de red a tiempo completo.

Sumario de la invención

La invención se define en las reivindicaciones 1 y 11 independientes.

Breve descripción de los dibujos

Con el fin de comprender la invención y apreciar la forma en que puede ser desarrollada en la práctica, a continuación se describirá una forma de realización preferente, únicamente a modo de ejemplo no limitativo, con referencia a los dibujos que se acompañan, en los cuales:

La **Fig. 1** es un diagrama de bloques que ilustra un entorno heredado que incluye un aparato para controlar y auditar la actividad del mismo, de acuerdo con una forma de realización de la invención;

la **Fig. 2** es un diagrama de flujo que ilustra los procedimientos principales llevados a cabo por un aparato para controlar y auditar la actividad en un entorno heredado, de acuerdo con una forma de realización de la invención;

la **Fig. 3** es un diagrama de bloques que ilustra un aparato para controlar y auditar la actividad en un entorno heredado, de acuerdo con una forma de realización de la invención;

la **Fig. 4** es un diagrama de flujo que ilustra con detalle la forma en que los paquetes interceptados son analizados, de acuerdo con una forma de realización de la invención;

la **Fig. 5** es un diagrama de flujo que ilustra con detalle la generación de datos representativos de sesiones especulares, de acuerdo con una forma de realización de la invención;

la **Fig. 6A** ilustra una pantalla ejemplar mostrada en un terminal de un empleado de un banco, al abrir una nueva cuenta bancaria;

la **Fig. 6B** ilustra la misma pantalla de la Fig. **6A**, en la que los campos de entrada incluyen información;

la **Fig. 6C** ilustra al menos parte de los datos representativos del episodio de auditoría saliente de la **Fig. 6A**;

la **Fig. 6D** ilustra al menos parte de los datos representativos del episodio de auditoría entrante que incluyen los datos ilustrados en la **Fig. 6B**;

la **Fig. 6E** ilustra al menos parte de los datos representativos de la auditoría unida del episodio de la **Fig. 6B**;

la **Fig. 7** es un diagrama de flujo que ilustra con detalle la generación de datos representativos de episodios de auditoría, de acuerdo con una forma de realización de la invención;

la **Fig. 8** es un diagrama de flujo que ilustra con detalle la asociación de un episodio de auditoría saliente con un episodio de auditoría entrante, de acuerdo con una forma de realización de la invención;

la **Fig. 9** es un diagrama de flujo que ilustra la forma en que un episodio de negocio es definido, de acuerdo con una forma de realización de la invención; y

la **Fig. 10** es un diagrama de flujo que ilustra con detalle la generación de datos representativos de episodios de negocio, de acuerdo con una forma de realización de la invención.

Descripción detallada de la invención

En la siguiente descripción los componentes que son comunes a más de una figura serán referenciados con las mismas referencias numerales.

La **Fig. 1** es un diagrama de bloques que ilustra un sistema heredado **101** que incluye un aparato para controlar y auditar su actividad, de acuerdo con una forma de realización de la invención. El sistema heredado **101** incluye entidades tales como unos terminales **102** y unos anfitriones **103**. Para los versados en la técnica se comprende que los terminales **102** generalmente operan en los sistemas heredados como clientes, mientras que los anfitriones **103** operan como servidores. Estas entidades no limitativas y alternativas o adicionales pueden también ser incluidas en el sistema heredado. Por ejemplo, el sistema **101** heredado incluye también unas impresoras **104**.

El sistema incluye también al menos un rastreador selectivo **105** que intercepta el tráfico de red (esto es paquetes) transportados por las entidades de la red. El rastreador selectivo **105** puede conectar con la red por cualquier medio aplicable, como por ejemplo conectándose a un puerto especular de un conmutador **106** de red como se ilustra en la figura. Se debe apreciar que cada rastreador selectivo **105** puede ser preconfigurado para interceptar paquetes de red transportados por o hacia un determinado anfitrión **103** en el sistema **101** heredado. En una forma de realización diferente al menos algunos de los rastreadores selectivos **105** pueden ser preconfigurados para interceptar paquetes transportados por o hacia más de un anfitrión.

La conexión de al menos un rastreador selectivo **105** con un puerto especular es no limitativa y alternativa; también son aplicables procedimientos, como por ejemplo la aplicación de dispositivos TAP de red.

El al menos un rastreador selectivo **105** intercepta los paquetes anfitriones del sistema transportados por los paquetes TCP / IP y los paquetes de la Arquitectura de Red del Sistema (SNA) que son transportados por los terminales **102** y los anfitriones **103**. En general, los paquetes interceptados por los rastreadores selectivos son designados como “paquetes interceptados”.

Los paquetes del sistema anfitrión son paquetes que se refieren a sistemas heredados, incluyendo protocolos de pantalla heredados como por ejemplo el IBM Mainframe (protocolo 3270), IBM iSeries (protocolo 5250), Unisys (T27 y protocolos UTS), Hitachi Mainframes (protocolo 560), Fujitsu Mainframes (protocolo 6680), Tandem (protocolo 6530) etc.

El rastreador selectivo **105** está acoplado a un aparato **107** para controlar y auditar la propiedad del sistema heredado, o simplemente “auditor heredado” **107** que transporta hacia aquél los paquetes interceptados. Se debe advertir, no obstante, que con algunas formas de realización, el rastreador selectivo **105** está incluido, o es parte del auditor heredado **107**, en lugar de estar por fuera y acoplado al mismo, como se ilustra en la **Fig. 1**.

La **Fig. 2** es un diagrama de flujo que ilustra los procedimientos principales llevados a cabo por un auditor heredado, como por ejemplo el auditor heredado **107** de acuerdo con una forma de realización de la invención. El auditor heredado recibe **(201)** un paquete interceptado transportado por entidades del sistema heredado. Se debe entender que el auditor heredado puede recibir los paquetes interceptados de cualquier forma aplicable, como por ejemplo recibirlos directamente del rastreador selectivo **105**, leer los paquetes de un dispositivo de almacenamiento donde están almacenados o, por ejemplo, recibir paquetes de cualquier otro dispositivo conectado a red que pueda almacenar y / o procesar paquetes.

En la referencia numeral **202**, los paquetes interceptados recibidos son analizados y en la referencia **203** los datos analizados son generados en base a la información asociada con los paquetes interceptados. Durante el análisis **202** el auditor **107** heredado identifica si el paquete interceptado es parte de una sesión ya abierta mantenida en el sistema heredado y controlada por el auditor heredado o si el auditor heredado no es actualmente consciente de dicha sesión. Esta identificación se basa en las cabeceras de los paquetes interceptados. Si se encuentra que el paquete es parte de una sesión controlada, esta id de sesión se incluye en los datos analizados junto con los datos incluidos en el paquete interceptado (esto es, los datos incluidos en la cabecera y el contenido del paquete interceptado). Como alternativa, si no se encuentra dicha sesión controlada abierta, el auditor heredado asigna una nueva id de sesión y la incluye en los datos analizados. De esta manera, los datos analizados son indicativos de las sesiones. A parte de la id de sesión, los datos analizados pueden incluir también información adicional, como por ejemplo la categorización de sesiones (por ejemplo categorías de sesiones de representación y / o impresora).

En la referencia **204** al menos parte de los datos analizados es utilizada para generar datos relacionados con sesiones especulares, correspondiéndose cada sesión especular a una sesión mantenida en el sistema heredado.

Los datos relativos a una sesión especular incluyen los datos analizados que se corresponden con una sesión mantenida en el sistema heredado. Se analizó con anterioridad que los datos analizados consisten en datos incluidos en un paquete interceptado junto con datos adicionales tales como la id de sesión, etc. De esta manera, se aprecia que los datos relacionados con la sesión especular también consisten en datos incluidos en un paquete interceptado junto con datos adicionales. Sin embargo, como generalmente hay más de un paquete transportado en una sesión, se aprecia que los datos relacionados con una sesión especular consisten en datos incluidos en más de

un paquete interceptado, correspondiéndose todos estos paquetes interceptados con la misma sesión mantenida en el sistema heredado.

Debe destacarse que una sesión especular se corresponde con una sesión, sin embargo, puede haber sesiones que no ofrezcan una correspondiente sesión especular. Por ejemplo durante el análisis de los paquetes auditados, el auditor **107** heredado identifica dos sesiones; una entre un anfitrión H_0 y un terminal To (por tanto designada como sesión H_0 - To) y otra entre el mismo anfitrión H_0 y una impresora P_0 (por tanto designada como sesión H_0 - P_0). En la referencia **203** el auditor **107** heredado genera los datos analizados que se corresponden con las dos sesiones. En la referencia **204** el auditor **107** puede generar datos representativos de dos sesiones especulares (H_0 - T_0 y H_0 - P_0) o datos representativos de solo una de las sesiones (H_0 - T_0 o H_0 - P_0).

Esto es, los datos representativos de una sesión especular son generados en respuesta a los datos analizados heredados, correspondiendo cada sesión especular a una sesión.

De acuerdo con diversas formas de realización, el auditor **107** heredado puede almacenar **205** los datos analizados en un dispositivo de almacenamiento, además o en lugar de la generación de datos relacionados con sesiones especulares. Haciendo esto, el auditor **107** heredado hace posible la segmentación del proceso ilustrado en la **Fig. 12**, en cuanto es posible leer los datos a partir del dispositivo de almacenamiento algún tiempo después, por ejemplo, con el fin de generar datos representativos de sesiones especulares a partir de aquél. Se debe considerar que algunas veces solo parte de los datos analizados pueden ser almacenados en **205** en el dispositivo de almacenamiento.

En la referencia **206** el auditor **107** heredado procesa también los datos representativos de sesiones especulares con el fin de generar datos representativos de episodios de auditoría. Un episodio de auditoría es indicativo de una operación llevada a cabo por un usuario en el sistema **101** heredado, una operación reflejada en la pantalla del usuario. Debe destacarse que el usuario puede ser un operador individual o puede ser un operador automático, como por ejemplo un programa de ordenador o macro que opere un terminal. Ejemplos de episodios de auditoría son pantallas de representación sobre un terminal, el mecanografiado de datos en campos de datos, la pulsación de botones sobre una pantalla o de unas teclas sobre un teclado. Sin embargo, algunas veces la inicialización de una sesión especular y / o su terminación también son considerados como episodios de auditoría.

Debe destacarse que algunas veces el auditor **107** heredado genera datos representativos de episodios de auditoría correspondientes a parte de las sesiones especulares, a datos representativos de ellas y generadas en la referencia **204**.

Por ejemplo, en un sistema heredado que incluye un anfitrión H_0 dos terminales T_0 y T_1 y una impresora P_0 durante el análisis de los paquetes recibidos, el auditor **107** heredado identifica tres sesiones. H_0 - T_0, H_0 - T_1 y H_0 - P_0. Son generados los datos representativos de dos sesiones especulares H_0 - T_0 y H_0 - T_1. Sin embargo, los datos representativos de episodios de auditoría pueden ser generados en correspondencia con las dos sesiones especulares (H_0 - T_0 y H_0 - T_1) o en correspondencia solo con uno de ellas (H_0 - T_0 o H_0 - T_1).

Volviendo a la **Fig. 2** en la referencia **207** el auditor **107** heredado genera datos representativos de episodios de negocio. Con el fin de generar datos representativos de episodios de negocio, al menos parte de los datos representativos de sesiones especulares, y al menos parte de los datos representativos de episodios de auditoría son procesados. Se debe destacar que un episodio de negocio puede corresponder a una o más sesiones especulares y a una o más episodios de auditoría. Debe destacarse, sin embargo, que cada episodio de auditoría se corresponde con una sesión especular, por tanto, de acuerdo con algunas forma de realización, los datos representativos de un episodio de auditoría pueden incluir los datos representativos de la correspondiente sesión especular que son requeridos para la generación de datos representativos de episodios de negocio. En dichas formas de realización, el auditor **107** heredado puede generar datos representativos de episodio de negocio procesando solo datos representativos de episodios de auditoría.

En una forma de realización alternativa, también es posible almacenar datos representativos de sesiones **(208)** especulares, datos representativos de episodios **(209)** de auditoría y / o datos representativos de episodios **(210)** de negocios o partes de estos.

En formas de realización alternativas adicionales, antes, después o en paralelo con el almacenamiento **(208)** de datos representativos de datos especulares, es posible comprimir **(211)** y / o encriptar **(212)** y / o firmar **(213)** digitalmente los datos utilizando los datos conocidos *per se*.

La compresión **(211)** de al menos parte de los datos representativos de sesiones especulares se puede llevar a cabo en cualquier procedimiento conocido *per se*, como por ejemplo el procedimiento Lampel - Ziv. La encriptación **(212)** de al menos parte de los datos representativos de sesiones especulares se puede llevar a cabo en cualquier procedimiento conocido *per se*, por ejemplo en el procedimiento PGP. La firma digital **(213)** de al menos parte de los datos representativos de sesiones especulares se puede llevar a cabo en cualquier procedimiento conocido *per se*, por ejemplo el algoritmo DSA (Algoritmo de Firma Digital).

Otras formas de realización adicionales pueden generar alertas con respecto a al menos uno de los episodios de negocio, cuyos datos representativos fueron generados en la referencia **207**. Debe destacarse que la generación de al menos algunas de las alertas se pueden basar en umbrales predeterminados.

Un ejemplo de un episodio de negocio es la apertura de una nueva cuenta bancaria. Un empleado abre una pantalla denominada “información de nuevo cliente” donde teclea la información del cliente como por ejemplo su nombre, id y dirección. La información es tecleada en tres campos de datos dedicados. A continuación, el empleado presiona entrar y recibe una segunda pantalla denominada “información financiera” en la que teclea la información financiera inicial del cliente, como por ejemplo su crédito inicial y oprime entrar.

La sesión especular consiste en todos los datos incluidos en los paquetes transferidos entre el terminal del empleado y el anfitrión (en ambas direcciones), dado que el empleado ha comenzado la sesión, por ejemplo, por la mañana cuando encendió el terminal. Así, la sesión especular se compone solo de datos incluidos en esos paquetes relacionados con la pantalla de información de nuevos clientes y con la pantalla de información financiera. Los episodios de auditoría de acuerdo con este ejemplo se despliegan en la pantalla de información del nuevo cliente, transportando la información del cliente al anfitrión, mostrando la pantalla de información financiera y de nuevo transportando la información financiera hasta el anfitrión.

En un ejemplo más complicado después de transportar la información financiera al anfitrión, el empleado espera la recepción de la aprobación en línea de que la cuenta bancaria puede ser abierta, por ejemplo, por el gestor. Esto es, el gestor tiene que aprobar la apertura de una cuenta antes de que la operación se complete. Con este fin, después de que el empleado transporta la información financiera al anfitrión, aparece una pantalla de “aprobación de nueva cuenta” en el terminal del gerente, en el que puede apretar “aprobar” o “desaprobar”. Debe apreciarse que la representación de la pantalla de aprobación de la nueva cuenta y la respuesta del gerente es parte de la sesión del gerente con el anfitrión y no parte de la sesión del empleado. La representación de la pantalla de aprobación de la nueva cuenta y el transporte de la respuesta aprobada / desaprobada son nuevos episodios de auditoría en la sesión del gerente.

En este momento, se representa una pantalla de “cuenta aprobada” o de “cuenta desaprobada” en el terminal del empleado, que indica que la apertura de la nueva cuenta ha terminado con éxito o con fracaso. La representación de la pantalla es de nuevo un episodio de auditoría en la sesión del empleado. Cuando el empleado presiona la tecla entrar en el teclado la pantalla de la cuenta se considera abierta.

Este escenario global comprende un episodio de negocio, esto es, la apertura de una nueva cuenta bancaria. Este episodio de negocio combina dos sesiones y ocho sesiones de auditoría.

La **Fig. 3** es un diagrama de bloques que ilustra un auditor **107** heredado en un sistema heredado, como por ejemplo el sistema **101** heredado, de acuerdo con una forma de realización de la invención. De acuerdo con la forma de realización, los paquetes interceptados recibidos por el auditor **107** heredado son mantenidos en una cola de espera **301**, acoplada a y / o accesible por un inspector **302**. El inspector **302** algunas veces es designado como un “servidor analizador”. Se debe apreciar que los paquetes interceptados son, por ejemplo, paquetes interceptados transportados por al menos un rastreador selectivo **105**. Sin embargo, el inspector **302** no está necesariamente acoplado al rastreador selectivo **105**. También puede recibir los paquetes interceptados a partir de otras fuentes, por ejemplo leyéndolos en un dispositivo de almacenamiento.

Se debe apreciar que la cola de espera **301** puede llevarse a cabo de cualquier forma aplicable, como por ejemplo como una estructura de datos en cola de espera conocida *per se*, ejecutado en software. Sin embargo, también es posible utilizar la cola de espera del sistema de archivo, por ejemplo.

El inspector **302** incluye un analizador de paquetes o, en una palabra, un analizador **303**. El analizador accede a los paquetes interceptados (por ejemplo los paquetes3270) mantenidos en la cola de espera y analiza los datos incluidos en ella. El analizador **303** genera unos datos (designados como “datos analizados”) que son representativos de sesiones producidas en el sistema **101** heredado.

Un dispositivo de almacenamiento denominado “registrador de paquetes” **304** está acoplado al analizador **303**. De acuerdo con una forma de realización, el analizador **303** almacena los datos incluidos en los paquetes interceptados y / o en los datos analizados dispuestos en el registrador de paquetes **304**. Como alternativa, el registrador de paquetes **304** puede almacenar datos incluidos en paquetes interceptados mientras un dispositivo de almacenamiento diferente puede ser utilizado para almacenar (algunas veces designado como “archivar”) los datos analizados o *vice versa*. Se analizó con mayor detenimiento que los datos analizados consisten en datos incluidos en paquetes interceptados junto con información adicional, como por ejemplo la identificación de la sesión (id de sesión), la categorización de la sesión y / u otros tipos de información.

Volviendo a la **Fig. 3**, un gerente de sesiones especulares o abreviando un gerente **305** especular está acoplado al analizador **303** para recibir de aquél los datos analizados. El gerente **305** especular da respuesta a los datos analizados para generar los datos representativos de sesiones especulares, correspondiendo cada sesión especular a una sesión. Como alternativa, el gerente especular puede ser acoplado al registrador de paquetes **304**, leer los datos analizados a partir de este, en lugar de estar directamente acoplado al analizador **303**.

Se debe destacar que el gerente **305** especular no procesa necesariamente todos los datos analizados que están disponibles en aquél, esto es, el gerente **305** especular es sensible a al menos parte de los datos analizados.

El gestor especular puede estar acoplado a un "dispositivo de almacenamiento especular" **306** para almacenar los datos representativos de las sesiones especulares producidas en aquél. Se debe apreciar que el dispositivo de almacenamiento especular **306** puede ser un dispositivo de almacenamiento tangible, como por ejemplo un disco o RAID (Matriz Redundante de Discos Independientes o No Costosos), o una división de estos, con o sin una base de datos. También puede ser un dispositivo de almacenamiento virtual, como por ejemplo un dispositivo de almacenamiento al que se accede por medio de Internet, etc. Así mismo, el dispositivo de almacenamiento especular, puede ser un dispositivo de almacenamiento dedicado solo para sesiones representativas de datos de sesiones especulares o puede ser un dispositivo de almacenamiento generalmente utilizado para tipo de datos adicionales, como por ejemplo paquetes interceptados y / o datos representativos de sesiones (por ejemplo, el registrador de paquetes **304** puede ser utilizado como un dispositivo de almacenamiento especular **306**).

De acuerdo con una forma de realización, el gerente especular **305** almacena los archivos en el dispositivo de almacenamiento especular **306** cada archivo incluye datos representativos de una sesión especular. Sin embargo ello no es limitativo y los expertos en la materia apreciarán que existen modelos de almacenamiento alternativos, como por ejemplo el almacenamiento de datos en un dispositivo de almacenamiento que sea una base de datos, en la que exista una tabla para cada sesión especular.

Un analizador **307** de episodios de auditoría está acoplado al gerente especular **305** para procesar datos representativos de datos especulares generados a partir de aquél y la generación de datos representativos de episodios de auditoría. Esto es, el analizador **307** de episodios de auditoría está adaptado para recibir datos representativos de sesiones especulares, generar datos representativos de episodios de auditoría, esto es, de episodios que sean indicativos de operaciones llevadas a cabo por usuarios del sistema **101** heredado, operaciones reflejadas en las pantallas de los usuarios.

Lo mismo que anteriormente, en una forma de realización alternativa, el analizador **307** de episodios de auditoría puede ser acoplado al dispositivo de almacenamiento especular **306** para recibir los datos almacenados en su interior, en lugar de estar directamente acoplado al gerente especular **305**.

Se debe destacar que el analizador **307** de episodios de auditoría no procesa necesariamente todos los datos representativos de sesiones especulares que se encuentran a su disposición. Esto es, el analizador **307** de episodios de auditoría puede procesar al menos parte de los datos representativos de sesiones especulares.

El analizador **307** de episodios de auditoría puede ser acoplado a un "dispositivo de almacenamiento de episodios de auditoría" **308** para almacenar los datos representativos de episodios de auditoría situados en su interior. Se debe apreciar que el dispositivo de almacenamiento de episodios de auditoría **308** puede ser un dispositivo de almacenamiento tangible, como por ejemplo un disco o RAID (Matriz Redundante de Discos Independientes o No Costosos), o una división de éste, con o sin una base de datos. También se puede tratar de un dispositivo de almacenamiento virtual, como por ejemplo un dispositivo de almacenamiento al que se accede a través de Internet, etc. Así mismo, el dispositivo de almacenamiento de dispositivos de auditoría **308** puede ser un dispositivo de almacenamiento dedicado solo para datos representativos de episodios de auditoría, o puede ser un dispositivo de almacenamiento generalmente utilizado para otros tipos de datos, como por ejemplo paquetes interceptados o datos representativos de sesiones y / o datos representativos de sesiones especulares (por ejemplo, el registrador **304** de paquetes o el dispositivo de almacenamiento especular **306** pueden también ser utilizados como dispositivo de almacenamiento de episodios de auditoría **308**).

Un analizador **309** de episodios de negocio está acoplado al analizador **307** de episodios de auditoría y al gerente especular **305**. El analizador **309** de episodios de negocio es capaz de generar datos representativos de sesiones especulares y datos representativos de episodios de auditoría y de generar datos representativos de episodios de negocio. Esto es, el analizador **309** de episodios de negocio es capaz de recibir datos representativos de sesiones especulares y datos representativos de episodios de auditoría, procesar estos datos o parte de los mismos y generar datos representativos de episodios de negocio. Como se indicó ya anteriormente, en una forma de realización alternativa, el analizador **309** de episodios de negocio puede estar acoplado al dispositivo de almacenamiento especular **306** y / o al dispositivo de almacenamiento de episodios de auditoría **308** para recibir los datos almacenados en su interior, en lugar de estar directamente acoplado al gestor especular **305** y / o al analizador **307** de episodios de auditoría, respectivamente.

Se debe destacar que el analizador **309** de episodios de negocio no necesariamente procesa los datos de episodios especulares y / o todos los datos representativos de episodios de auditoría en el que se encuentran a su disposición. Esto es, el analizador **309** de episodios de negocio puede procesar al menos parte de los datos representativos de sesiones especulares y al menos parte de los datos representativos de episodios de auditoría.

Anteriormente se indicó, con referencia a la **Fig. 2** que algunas veces los datos representativos de episodios de auditoría pueden incluir datos representativos de la correspondiente sesión especular que son requeridos para la generación de datos representativos de episodios de negocio. En dichas formas de realización, el analizador **309** de

episodios de negocio puede generar datos representativos de episodios de negocios procesando solo datos representativos de episodios de auditoría. De esta manera, en dichas formas de realización, el analizador **309** de episodios de negocio puede estar acoplado solo al analizador de episodios de auditoría (a diferencia de la forma de realización de la **Fig. 3**, en la que el analizador **309** de episodios de negocio está acoplado a un analizador **307** de episodios de auditoría y al gerente especular **305**).

El analizador **309** de episodios de negocio puede estar acoplado a un "dispositivo de almacenamiento de episodios de negocio" **310** para almacenar en su interior los datos representativos de episodios de negocio. Se debe apreciar que el dispositivo de almacenamiento de episodios de negocio **310** puede ser un dispositivo de almacenamiento tangible, como por ejemplo un disco o RAID (Matriz Redundante de Discos Independientes o No Costosos), o una división de éste, con o sin una base de datos. También puede ser un dispositivo de almacenamiento virtual, como por ejemplo un dispositivo de almacenamiento al que se acceda a través de Internet, etc. Así mismo, el dispositivo de almacenamiento de episodios de negocio **310** puede ser un dispositivo de almacenamiento dedicado solo para datos representativos de episodios de negocio, o puede ser un dispositivo de almacenamiento generado utilizado para otros tipos de datos, como por ejemplo paquetes interceptados y / o datos representativos de sesiones y / o datos representativos de sesiones especulares y / o datos representativos de episodios de auditoría (por ejemplo, el registrador **304** de paquetes, el dispositivo de almacenamiento especular **306**, o el dispositivo de almacenamiento de episodios de auditoría **308** pueden también ser utilizados como dispositivo **310** de almacenamiento de episodios de negocio).

Así mismo, en algunas formas de realización, un gerente **312** de alertas puede estar acoplado al analizador **309** de episodios de negocio para generar o suscitar alertas cuando se producen determinados episodios de negocio.

Debe destacarse que algunas veces el inspector **302** puede estar acoplado a un dispositivo **311** de almacenamiento de datos además o en lugar de incluir el registrador **304** de paquetes y / o el dispositivo de almacenamiento especular **306**, y / o el dispositivo de almacenamiento de episodios de auditoría **308,** y / o el dispositivo de almacenamiento de episodios de negocio **310**. Este dispositivo **311** de almacenamiento de datos puede ser utilizado para el almacenamiento de los datos analizados y / o el almacenamiento de los datos representativos de sesiones especulares, y / o de los datos representativos de los episodios de auditoría, y / o de los datos representativos de episodios de negocio, respectivamente.

En formas de realización alternativas, el dispositivo de almacenamiento especular, puede estar acoplado también a un agente **313** de compresión, y / o a un agente **314** de encriptación, y / o a un agente **315** de firma. Debe destacarse que el agente **313** de compresión puede comprimir al menos parte de los datos representativos de sesiones especulares en cualquier procedimiento conocido *per se*, por ejemplo el procedimiento Lampel - Ziv. Así mismo, el agente de compresión puede comprimir los datos representativos de las sesiones especulares antes, después o en paralelo con su almacenamiento (o al menos parte de ellos) en el dispositivo de almacenamiento especular **306**.

El agente **314** de encriptación puede encriptar al menos parte de los datos representativos de sesiones especulares en cualquier procedimiento conocido *per se*, como por ejemplo el procedimiento PGP. Así mismo, el agente de encriptación puede encriptar los datos representativos de sesiones especulares antes, después o en paralelo a su almacenamiento (o al menos parte de ellos) en el dispositivo de almacenamiento especular **306**.

El agente **315** de firma puede firmar al menos parte de los datos representativos de los datos especulares en cualquier procedimiento conocido *per se*, como por ejemplo el algoritmo DSA (Algoritmo de Firma Digital). Así mismo, el agente de firma puede firmar los datos representativos de sesiones especulares antes, después o en paralelo a su almacenamiento (o al menos parte de ellos) en el dispositivo de almacenamiento especular **306.**

Los expertos en la materia apreciarán, sin embargo, que el agente **313** de compresión, y / o el agente **314** de encriptación, y / o el agente **315** de firma pueden estar acoplados al gerente especular **305**, además o en lugar d estar acoplado al dispositivo de almacenamiento especular **306.**

Después de describir un diagrama de flujo ejemplar que ilustra los procedimientos principales llevados a cabo por un aparato para controlar y auditar la actividad en un entorno heredado (**Fig. 2**) y de un diagrama de bloques ejemplar que ilustra dicho aparato (**Fig. 3**), la **Fig. 4** proporciona así mismo una descripción detallada de un análisis de paquetes interceptados, llevado a cabo por el analizador **303** de acuerdo con una forma de realización de la invención.

El diagrama de flujo de la **Fig. 4** se refiere a los paquetes 3270 transportados por los paquetes SNA, sin embargo ello no es limitativo y los expertos en la materia apreciarán que pueden aplicarse procedimientos iguales o parecidos para otros protocolos, como por ejemplo los paquetes 3270 transportados por TCP / IP u otros protocolos de pantalla heredados. Se debe destacar que los paquetes heredados desde el anfitrión hasta una entidad de cliente, como por ejemplo un terminal o una impresora son designados como paquetes salientes, mientras que los paquetes enviados desde un cliente a un anfitrión son designados como paquetes entrantes.

En la referencia **401** el analizador recibe un paquete interceptado. Como ya se mencionó anteriormente, el analizador puede recibir los paquetes interceptados procedentes de una cola en espera (por ejemplo una cola en

espera **301**). En términos más generales, el analizador puede recibir paquetes interceptados procedentes de cualquier fuente disponible como por ejemplo un rastreador selectivo (por ejemplo **105** en la **Fig. 1**) o una base de datos.

En la referencia **402** se determina el protocolo de comunicación (TCP / IP o SNA) y en la referencia **403** el paquete es analizado con el fin de determinar su protocolo de pantalla heredado (3270, etc.).

La apreciación de que un paquete interceptado está siendo parte de una sesión y que la cabecera del paquete interceptado incluyen parámetros de identificación de sesión, en la referencia **404** los parámetros de identificación de sesión son extraídos de la cabecera del paquete interceptado, permitiendo la identificación de la sesión. Por ejemplo, en la SNA, la sesión que identifica los parámetros son la dirección MAC del cliente, la PU (Unidad Física) y LU (Unidad Lógica) conocidos *per se*, mientras en la sesión TCP / IP que identifican los parámetros son la dirección IP del servidor y el puerto, así como la dirección y el puerto IP de los clientes. Anteriormente se analizó que, en conexión con el auditor **107** heredado, cada rastreador **105** selectivo algunas veces está preconfigurado para interceptar paquetes de red transportados por o hacia un determinado anfitrión **103** de sistema **101** heredado. Por tanto, se debe apreciar por parte de los expertos en la materia que la identidad anfitrión hacia el cual se transporta el paquete interceptado o por medio del cual se puede determinar. Sin embargo, en aquellos casos en los que al menos uno de los rastreadores selectivos **105** está preconfigurado para interceptar paquetes transportados por o hacia más de un anfitrión **103**. La entidad del anfitrión de un paquete interceptado es transportada por o hacia o puede ser determinada de acuerdo con la dirección MAC del anfitrión, la PU y LU, como se indicó mediante la cabecera del paquete.

El analizador tiene acceso a una lista, o grupo, de sesiones abiertas que el auditor heredado actualmente controla. La lista puede ser almacenada en una estructura de datos de una memoria, puede ser almacenada en una base de datos, o puede ser gestionada de cualquier otra forma aplicable al supuesto. Para cada sesión abierta relacionada dentro de aquella, una identificación de sesión (id de sesión) es relacionada junto con la identificación de protocolo de pantalla heredado, la identificación del protocolo de identificación y los parámetros de identificación de la sesión. La id de sesión puede ser cualquier estructura de datos aplicable al caso, como por ejemplo un valor numérico, una ristra de caracteres, una estructura de cualquier tipo, etc.

En la referencia **405** el analizador busca la lista de sesiones abiertas controladas con el fin de determinar si los parámetros de identificación de sesión del paquete interceptado están relacionados en ella y, si es así, puede ser identificada la sesión respectiva del paquete interceptado. Si los parámetros de identificación de la sesión no se encuentra en la lista, en la referencias **406** el analizador asigna una nueva id de sesión a ella y en la referencia **407** añade esta id de sesión junto con los parámetros de identificación de sesión del paquete interceptado a la lista. La nueva id de sesión está ahora asociada con los parámetros de identificación de sesión, esto es, puede ser identificada la sesión del paquete interceptado.

En la referencia **408**, la id de sesión es añadida a los datos incluidos en el paquete interceptado (incluyendo la cabecera y el contenido) que constituyen conjuntamente los datos analizados.

Se debe destacar que el diagrama de flujo descrito no es vinculante y que pueden ser aplicados otros datos y procedimientos para generar los datos analizados. Por ejemplo, en una forma de realización diferente, los datos de categorización de sesión pueden ser asociados con los datos incluidos en el paquete interceptado (con o sin una id de sesión), constituyendo conjuntamente los datos analizados. Otras formas de realización pueden asociar la identificación de anfitrión y / o la indicación de si el paquete interceptado es un paquete saliente o un paquete entrante, etc. Sin embargo, una forma de realización diferente puede incluir en la lista de sesiones abiertas controladas una marca de tiempo, indicativa del tiempo en que la sesión fue detectada por primera vez (esto es, el tiempo en el que la id de sesión fue asignada), etc.

Después de considerar una forma de realización ejemplar de un analizador **303**, la **Fig. 5** es un diagrama de flujo que ilustra con detalle la representación de datos representativos de sesiones especulares en el gerente especular **305**, de acuerdo con una forma de realización de la invención.

Conociendo que una sesión tiene un principio y un final, se esperan conocer tipos de paquetes que comiencen y terminen una sesión, constituyendo un paquete de conexión y un paquete de desconexión. En el TCP / IP, por ejemplo, un paquete SYN es considerado como un paquete de conexión y un paquete FIN es considerado como un paquete de desconexión.

De esta manera, después de recibir los datos analizados en la referencia **501**, en la referencia **502** el gerente especular **305** determina si este es un paquete de conexión. Si lo es, identificando que ha comenzado una nueva sesión, en la referencia **503** el gerente especular extrae la sesión de la información especular procedente de los datos analizados, como por ejemplo la id de sesión y / o la entidad del anfitrión y del cliente que participa en la sesión, la marca de tiempo, etc. En la referencia **504** se abre una nueva sesión especular. Por ejemplo se abre un nuevo archivo en el dispositivo de almacenamiento especular **306** para incluir datos representativos de la sesión especular (en la que cada sesión especular se corresponde con una sesión). Como alternativa, se puede generar una tabla en una base de datos de esta sesión especular. Así mismo, la id de sesión junto con la información

adicional y la identificación del nuevo archivo (o tabla) son relacionadas (constituyendo conjuntamente la información de sesión especular) en una base de datos. Se debe destacar que el gerente especular puede asignar una id de sesión especular a cada nueva sesión especular recién abierta. Sin embargo, manteniendo la id de sesión especular igual a la id de sesión correspondiente de sesión especular, el análisis se simplifica de forma que los datos analizados puedan ser directamente situados en correspondencia con las ids de sesiones especulares.

Recordando que los datos analizados consisten también en datos incluidos en el paquete interceptado, se puede entender que el gerente especular tiene acceso a los datos incluidos en el paquete interceptado. Así, en la referencia **505** los datos incluidos en el paquete interceptado (incluyendo la cabecera y el contenido) son almacenados en asociación con la información de sesión especular, por ejemplo, en el archivo identificado en la información de sesión especular o en la tabla identificada en la información de sesión especular, etc.

Sin embargo, si en la referencia **502** el gerente especular encuentra que el paquete interceptado no es un paquete de conexión, puede ser un paquete de desconexión o un paquete de dentro de la sesión, por ejemplo, un paquete que es parte de una sesión ya abierta. En cualquier caso, en la mayoría de los supuestos el gerente especular espera encontrar una sesión especular ya abierta correspondiente a los datos analizados. Con el fin de identificar y localizar esta sesión especular ya abierta, en la referencia **506** el gerente especular extrae la id de sesión de los datos analizados.

Avanzando en el proceso, el gerente especular intenta hacer coincidir la id de sesión extraída (véase la referencia **506**) con las ids de sesiones especulares abiertas. Si en la referencia **507** el gerente especular encuentra una sesión especular abierta que presenta la misma id que la id de sesión extraída, en la referencia **508** verifica si el paquete interceptado es un paquete de desconexión. Si es así, en la referencia **509** la sesión especular se cierra, por ejemplo marcando en la base de datos que la sesión especular está cerrada, y / o dando instrucciones al sistema para cerrar el archivo de la sesión especular inmediatamente después de la siguiente escritura (los datos incluidos en la sesión especular necesitan todavía ser almacenados en el archivo) y / o dando instrucciones al analizador **303** para eliminar esta sesión de su lista de sesiones abiertas controladas. En la referencia **505** los datos incluidos en el paquete interceptado son almacenados.

Sin embargo, si en la referencia **508** el gestor especular encuentra que el paquete interceptado no es un paquete de desconexión (esto es, es un paquete de dentro de sesión) los datos incluidos en el paquete interceptado son almacenados (véase la referencia **505)** y el gerente especular puede recibir los datos analizados adicionales (**501**).

Volviendo a la referencia **507**, si el gerente especular encuentra que no hay ninguna sesión especular abierta con una id de sesión especular que sea igual a la id de sesión extraída, y recordando que este no es un paquete de conexión (véase la referencia **502**), se asume que el paquete interceptado pertenece a una sesión ya abierta, aunque por una u otra razón el auditor heredado no controla esta sesión (por ejemplo, es posible que el auditor heredado no operara cuando la sesión fue abierta). De esta manera, en la referencia **511** el gerente especular verifica si el paquete interceptado es un paquete de desconexión. Si se aprecia que en el caso de que el paquete interceptado es un paquete de desconexión, en la referencia **512** el gerente especular da instrucciones al analizador para retirar la sesión de su lista de sesiones abiertas controladas y después el gestor especular está listo para recibir datos analizados adicionales. Sin embargo, si el paquete interceptado resulta ser (en la referencia **511**) un paquete de dentro de la sesión, se aprecia que los paquetes de dentro de la sesión algunas veces incluyen información especular parcial (por ejemplo, la identidad del cliente y del anfitrión). Por tanto, en la referencia **513** el gerente especular extra la información especular de los datos analizados, en la referencia **504** abre una nueva sesión especular y en la referencia **505** almacena los datos incluidos en el paquete interceptado.

Antes de volver a describir la forma en que los datos representativos de episodios de auditoría son generados, se debe tener en cuenta que los episodios de auditoría están relacionados con las pantallas mostradas en los terminales. Debe apreciarse que los protocolos de pantallas heredadas se basan en la información de los caracteres.

Volviendo al ejemplo de la apertura de una nueva cuenta bancaria, una pantalla **6A01** de información de nuevo cliente ejemplar se ilustra en la **Fig. 6A**. Es sabido *per se* que en un protocolo de pantalla heredada con el fin de representar la pantalla sobre un terminal, el anfitrión transporta los datos representativos de la pantalla sobre el terminal. Los datos representativos de una pantalla incluyen, por ejemplo, los campos destinados a ser mostrados en el terminal, sus respectivos atributos (solo lectura o campo de entrada, si un campo de entrada permite la entrada de cualquier carácter, un conjunto limitado de caracteres o posiblemente un valor numérico) características adicionales, (por ejemplo la posición en la pantalla, la fuente y el color utilizados, la longitud del campo de los caracteres, etc.) y el texto que debe ser mostrado en ella. De esta manera, en la pantalla **6A01** ejemplar ilustrada en la **Fig. 6A** hay siete campos, uno de ellos (**6A02**) incluye e título de la pantalla; otro (**6A03**) incluye el texto “Nombre del Cliente:”; el campo **6A04** es un campo de entrada para recibir caracteres como entrada; **6A05** incluye el texto “id Cliente:”; **6A06** es un campo de entrada para recibir valores numéricos como entrada; **6A07** incluye el texto “Dirección cliente:” y **6A08** es un campo de entrada que recibe caracteres como entrada.

Los campos incluidos en una pantalla, junto con sus características y posiblemente también características adicionales de toda la pantalla (por ejemplo el color de fondo) son referenciados conjuntamente con las características de la pantalla.

De esta manera, mediante el reconocimiento de las características de pantalla es posible que la pantalla pueda ser reconocida. Si, de acuerdo con una forma de realización, cada pantalla soportada por un anfitrión **103** presenta una identificación (constituyendo una "id de pantalla"), en la que son almacenadas en el sistema una lista de ids de pantalla disponibles y sus características, como por ejemplo una tabla o una lista, entonces es posible solicitar la tabla, buscar las características de pantalla reconocidas, identificar la id de pantalla respectiva. Se debe apreciar, sin embargo, que otras formas de realización también son autorizadas. Por ejemplo, cuando no haya una tabla preconfigurada de ids de pantalla y sus respectivas características. Por el contrario, cuando se reconoce una pantalla, la tabla es escaneada. Si las características reconocidas no se encuentran en una tabla de ids de pantalla y sus respectivas características, una nueva id de pantalla es asignada para las características reconocidas, y ellas (las características reconocidas y la id de pantalla recién asignada) son insertadas en la tabla, esto es, la tabla está dinámicamente actualizada.

Así mismo, sabiendo el orden y / o la posición en la cual diferentes campos aparecen en la pantalla **6A01**, a cada campo se le puede otorgar una identificación. Por ejemplo, el campo **6A02** puede ser identificado como "cabecera de nuevo cliente"; **6A03** "título de nombre"; **6A04** "entrada de nuevo"; **6A05** "título de id"; **6A06** "entrada de id"; **6A07** "título de dirección"; y **6A08** "entrada de dirección". Debe apreciarse que, aunque esa identificación de campo (en lo sucesivo "id de campo") así como las ids de pantalla no deben ser necesariamente ristras de caracteres. También pueden ser utilizados valores numéricos o cualquier otra estructura de datos como ids de campo cuando sean aplicables.

Volviendo a la **Fig. 5**, se debe apreciar que los datos representativos de las sesiones especulares incluyen cabeceras y contenidos de paquetes interceptados. Un terminal en un sistema heredado es un terminal mudo, esto es, todas las pantallas mostradas en él son transportadas a él por un anfitrión. Por tanto, el análisis de las cabeceras y contenidos de los paquetes interceptados salientes puede revelar una información representativa de las pantallas mostradas en los terminales, incluyendo las características de pantalla y campo, en el que se aprecie que la cabecera del paquete indica si es un paquete saliente o un paquete entrante. La información representativa de una pantalla algunas veces es designada como "espacio de representación".

De modo similar, el análisis de los paquetes interceptados salientes puede revelar la información representativa de las operaciones llevadas a cabo por el usuario en una pantalla (como por ejemplo llenando el nombre del cliente, la id y la dirección) y transportadas al anfitrión.

Sin embargo, antes de volver a describir la forma en que los datos representativos de episodios de auditoría son generados, se debe apreciar que una sesión normalmente comienza con la representación sobre un terminal de una pantalla predeterminada (designada como "pantalla de conexión predeterminada"), como por ejemplo una pantalla de registro. Esto significa que el anfitrión transporta paquetes hacia el terminal. Uno o más de estos paquetes incluye información de tentativa de la pantalla de conexión predeterminada. Ya se ha entendido que los datos correspondientes a una sesión especular pueden ser generados con relación a esta sesión, esto es, los datos representativos de esta sesión especular incluyen también la información representativa de la pantalla de conexión predeterminada.

En otras palabras, el primer episodio de auditoría en una sesión especular que comienza con un paquete de conexión es representar la pantalla de conexión predeterminada.

Aún más, se espera que el usuario se registre en el anfitrión tecleando su nombre y contraseña y pulsando en entrar, por ejemplo. De esta manera, el terminal transporta hacia el anfitrión paquetes con información representativa de las operaciones llevadas a cabo por el usuario, como por ejemplo el tecleo de información y la pulsación de entrar. Se debe entender que el segundo episodio de auditoría, de acuerdo con este ejemplo, se corresponde con estos paquetes.

El tercer episodio de auditoría puede ser un menú que incluya unas operaciones opcionales que el usuario puede llevar a cabo (en otras palabras: una lista de pantallas opcionales que ella pueda representar), y el cuarto episodio de auditoría incluirá la elección de la usuaria. Si su elección fuera la de abrir una nueva cuenta bancaria, la pantalla ilustrada en la **Fig. 6A** será transportada hasta su terminal. Esto es, la representación de la pantalla ilustrada en la **Fig. 6A** es un ejemplo de un episodio de auditoría.

A continuación, la usuaria tecleará en la información del cliente, como se ilustra, por ejemplo, en la **Fig. 6B**, en la que la información que incluye la información del cliente será transportada hasta el anfitrión. El transporte de la información representativa de la pantalla ilustrada en la **Fig. 6B** es, de acuerdo con el ejemplo, el episodio de auditoría entrante. La **Fig. 6C** ilustra al menos una parte **6C01** de los datos representativos del episodio de auditoría saliente de representación de la pantalla de información del nuevo cliente de la Fig**. 6A**. En la figura, 01 significa "cambio de pantalla", "C3-WCC" se refiere a DESBLOQUEAR **TECLADO** y Cada supuesto de "11 xx yy" significa que la posición del campo se calcula en base a xx e yy. Por ejemplo, 1140 40 significa la posición de la posición 1

columna 1 sobre la pantalla. Cada supuesto de “1d zz” significa un nuevo campo en esta localización y sus atributos descritos mediante zz. El resto son instrucciones respecto a la forma en que trazar la pantalla. El lado derecho contiene una traslación de un hex en caracteres visibles.

La **Fig. 6D** ilustra al menos una parte **6D01** de los datos representativos del episodio de auditoría entrante que incluye los datos ilustrados en la **Fig. 6B**. Esta parte representa los datos insertados del usuario, el Nombre de Cliente: John Doe; ID de Cliente: 123456; y Dirección de Cliente: TRUMPET 22 BANFF. En este ejemplo, “7D” significa “Entrar”; “C6 7B” es la posición el cursor; y el resto son instrucciones para situar datos específicos representativos de parte de la pantalla en localizaciones específicas.

Finalmente, la **Fig. 6E** ilustra al menos una parte **6E01** de los datos representativos de la auditoría unida de la **Fig. 6B**. Se debe apreciar que **6E01** es similar que **6C01,** pero incluyen los datos de **6D01**.

Siempre que el usuario no salga fuera del sistema, permitiendo el registro de otro usuario, es posible deducir que el usuario registrado está asociado con el terminal. Por tanto, es posible incluir una indicación de que el usuario (por ejemplo, el nombre del usuario o la id de usuario) en los datos representativos de los episodios de auditoría.

Sin embargo, en aquellos casos en que la sesión especular no se inicie con una sesión de conexión (véase, por ejemplo, las referencias **513, 504** y **505** en la **Fig. 5**), el primer episodio de auditoría puede ser diferente de la pantalla de conexión predeterminada. En este caso, el auditor heredado puede no ser capaz de asociar una indicación de usuario con los datos representativos del primero y posiblemente también de los episodios de auditoría entrantes.

Se debe destacar, sin embargo, que la pantalla de conexión predeterminada puede ser utilizada en otras oportunidades a parte del inicio de sesión. En el ejemplo, de que la pantalla de conexión predeterminada sea una pantalla de registro es conocido por parte de los expertos en la materia que un usuario puede salirse en la mitad de una sesión, permitiendo que un usuario diferente se registre.

La **Fig. 7** es un diagrama de flujo que ilustra con detalle la generación de datos representativos de episodios de auditoría, de acuerdo con una forma de realización de la invención. La generación de datos representativos de episodios de auditoría, se produce, por ejemplo, en el analizador **307** de episodios de auditoría. En la referencia **701** son recibidos los datos representativos de una sesión especular. Debe apreciarse que los datos representativos de una sesión especular consisten al menos en datos analizados que incluyen paquetes interceptados, esto es, los datos representativos de una sesión especular son también representativos de paquetes interceptados, correspondiendo todos los paquetes interceptados a una misma sesión. De esta manera, cuando los datos representativos de una sesión especular, el analizador de episodios de auditoría recibe de hecho los datos representativos de paquetes interceptados, recibiéndolos en el mismo orden en el que fueron transportados hacia / desde el anfitrión y el terminal.

En la referencia **702** el analizador de episodios de auditoría verifica si el paquete interceptado es un paquete saliente o entrante. Como se analizó con anterioridad, los paquetes salientes corresponden a una pantalla transportada por el anfitrión, para ser representada sobre el terminal, mientras que los paquetes entrantes corresponden a datos transportados por el terminal hacia el anfitrión.

Si en la referencia **702** se determina que el paquete es un paquete saliente, el paquete pertenece a un episodio de auditoría entrante. Sin embargo, el paquete interceptado puede indicar que el episodio de auditoría acaba de comenzar o, como alternativa, puede ser un paquete de episodio de auditoría interno. Con el fin de determinar cuál de las dos alternativas corresponde al paquete interceptado, el analizador de episodios de auditoría mantiene un estado variable que indica si actualmente el estado es saliente o entrante. Si en la referencia **703** se encuentra que el estado actual es distinto del saliente, eso significa que actualmente el paquete saliente analizado comienza con un episodio de auditoría saliente nuevo. Por tanto, en la referencia **704** el estado actual se establece como saliente y en la referencia **705** un episodio de auditoría nuevo es inicializado para almacenar datos representativos del episodio de auditoría. Por ejemplo, se abre un nuevo archivo y / o una tabla en una base de datos es inicializada, etc. El archivo puede incluir datos representativos de paquetes de datos interceptados, junto con datos adicionales tales como una indicación del episodio como un episodio de auditoría entrante o saliente y una marca de tiempo indicativa del tiempo en el que el episodio ha comenzado y / o terminado.

Si en la referencia **703** el analizador de episodios de auditoría encontró que el estado actual era de saliente o entrante, en la referencia **706** los datos representativos del paquete interceptado son adjuntados a los datos representativos del episodio de auditoría.

Así mismo, los expertos en la materia apreciarán que, con el fin de mostrar una pantalla sobre un terminal, el anfitrión transporta hacia ella los paquetes salientes. Con el fin de permitir que un usuario opere, actualice o inserte datos en la pantalla, el anfitrión transporta una indicación DESBLOQUEAR TECLADO hacia el terminal. De esta manera, la indicación DESBLOQUEAR TECLADO marca el final de un episodio de auditoría saliente.

Por tanto, en la referencia **707** el analizador de los episodios de auditoría verifica si los paquetes incluyen una indicación de DESBLOQUEAR TECLADO y, si es así, en la referencia **708** el episodio de auditoría se termina. Por ejemplo, añadiendo una marca de tiempo de terminación y cerrando el archivo.

Sin embargo, si en la referencia **702** el analizador de los episodios de auditoría encuentra que el paquete interceptado es un paquete entrante, esto significa que el paquete es parte de un episodio de auditoría entrante. En la referencia **709** el analizador verifica si el estado actual es otro distinto al de entrante. Si es así (el paquete entrante actualmente analizado inicia un nuevo episodio de auditoría entrante), en la referencia **710** el estado actual se fija como entrante y en la referencia **711** se inicializa un nuevo episodio de auditoría para almacenar los datos representativos del episodio de auditoría.

Si en la referencia **709** el analizador de los episodios de auditoría ha encontrado que el estado actual era de saliente o de entrante, en la referencia **712** los datos representativos del paquete interceptado son adjuntados a los datos representativos del episodio de auditoría.

Así mismo, los expertos en la materia apreciarán que cuando la información de pantalla es transportada por un terminal hacia un anfitrión, una indicación de “fin de mensaje” es incluida en los paquetes entrantes. Por ejemplo, en telnet la ristra hexadecimal “FF EF” es aceptada. Así, la indicación de final de mensaje marca el final de un episodio de auditoría entrante.

Por tanto, en la referencia **713** el analizador de episodios de auditoría verifica si los paquetes incluyen una indicación de fin de mensaje, y si es así, en la referencia **708** el episodio de auditoría se termina, por ejemplo, añadiendo una marca de tiempo de terminación y cerrando el archivo.

Se debe apreciar que es posible transportar los datos representativos de los paquetes interceptados almacenados en asociación con un episodio de auditoría saliente hacia un programa de emulación del terminal conocido *per se*, por ejemplo, con el fin de representar la pantalla como se representó con anterioridad sobre el terminal. Sin embargo, la representación de un episodio de auditoría entrante es más complicada, dado que el episodio de auditoría entrante se genera por el terminal y es transportado por el anfitrión. Esto es, el terminal genera el episodio de auditoría entrante y no lo representa. Con el fin de representar la información transportada en un episodio de auditoría entrante en el contexto de la pantalla en la que fue insertado por el usuario, se requiere analizar el episodio de auditoría; extraer la información transportada de dicho contexto; asociar el episodio de auditoría entrante con un episodio de auditoría saliente (esto es, con una pantalla mostrada); y a continuación asociar la información con uno o más campos de la pantalla mostrada.

La **Fig. 8** es un diagrama de flujo que ilustra con detalle la asociación de un episodio de auditoría entrante con un episodio de auditoría saliente, de acuerdo con una forma de realización de la invención. Se debe apreciar que los paquetes entrantes que incluyen información, generalmente proporcionan una indicación a la posición del cursor sobre la pantalla, en la que la información fue insertada. Así, mediante el análisis o el reconocimiento de los datos representativos del episodio de auditoría entrante en la referencia **801** es posible reconocer la información insertada por el usuario en los campos sobre la pantalla, la identidad de estos campos y posiblemente también la posición del cursor. Véase también la explicación suministrada anteriormente, con referencia a las **Figs. 6A** y **6B.**

Es importante también reconocer la tecla que el usuario pulsa antes de transportar la información al anfitrión. Algunas veces el usuario puede solo pulsar una tecla determinada, como por ejemplo “Entrar”. No obstante, en otras situaciones, el usuario puede pulsar una cualquiera de las diversas teclas opcionales, como el gerente que puede aprobar o desaprobar la apertura de una nueva cuenta en el ejemplo de nueva cuenta bancaria descrito con anterioridad. De esta manera, el reconocimiento de la clave en la referencia **802** también es valiosa. Por ejemplo, en la referencia **802** los Identificadores de Atención (AID) pulsados por el usuario son identificados, por ejemplo los botones Clear, Escape, PF1, PF2 sobre el teclado. El análisis puede también detectar la localización del cursor mientras se está pulsando la tecla.

Volviendo al ejemplo suministrado anteriormente que describe las **Figs. 6A** y **6B,** (en las que el primer episodio de auditoría es la pantalla de registro) el segundo episodio es el transporte de la información de registro hasta el anfitrión, etc.), y recordando que los protocolos de pantalla heredados son generalmente incrementales (esto es, cada paquete puede cambiar la información representativa de la pantalla creada por paquetes anteriores) se apreciará que muchas veces, al reconocer una identidad de un episodio de auditoría entrante, es posible identificar el correspondiente episodio de auditoría saliente. En el ejemplo, sabiendo que un episodio de auditoría entrante determinado está transportando la información de registro hacia el anfitrión, se puede deducir que la identidad del correspondiente episodio de auditoría saliente fue representar la pantalla de registro sobre un terminal. Así mismo, es bastante probable que un episodio de auditoría saliente que se corresponda con un episodio de auditoría entrante sea el episodio de auditoría saliente anterior en el tiempo al episodio de auditoría entrante.

De esta manera, en la referencia **803**, se identifica el correspondiente episodio de auditoría saliente, y en la referencia **804** se recuperan los datos representativos del episodio de auditoría saliente identificados. Si en la referencia de la **Fig. 7** los datos representativos del episodio de auditoría fueron almacenados en un disco (*disk*), por ejemplo, entonces en la referencia **804** son leídos a partir del disco. Sin embargo, ello por supuesto no es limitativo y

pueden ser aplicadas otras formas para almacenar los datos, por ejemplo su almacenamiento en la memoria, con lo que en la referencia **804** se accede a los datos de la memoria. Así mismo, también es posible una combinación. Por ejemplo, en la **Fig. 7** los datos pueden ser almacenados en un disco o en una base de datos y al mismo tiempo pueden ser almacenados (o una copia de los mismos) también en la memoria. En este caso, en la referencia **804** es posible acceder a los datos de la memoria, lo que generalmente se considera más rápido. En los procedimientos descritos en las referencias **803** y **804** de modo conjunto algunas veces constituyen un único procedimiento de recoger un correspondiente episodio de auditoría saliente.

En la referencia **805** el analizador de episodios de auditoría identifica los campos (título y / o campos de entrada) incluidos en el correspondiente episodio de auditoría saliente, y en la referencia **806** la información insertada en el episodio de auditoría entrante es correlacionada con los campos de entrada del episodio de auditoría saliente, por ejemplo de acuerdo con la posición del campo.

De acuerdo con algunas formas de realización, un nuevo episodio se genera en la referencia **807**, combinando los datos representativos del episodio de auditoría salientes y los datos representativos de la información insertada en el episodio de auditoría entrante. Estos episodios de auditoría recién generados constituyen un episodio de auditoría unido. Se debe apreciar que es posible transportar datos representativos de un episodio de auditoría unido hasta un programa de emulación de terminal, por ejemplo, para representar en él la pantalla correspondiente. Como alternativa, en lugar de generar un nuevo episodio de auditoría unido, es posible añadir datos a los datos representativos del episodio de auditoría saliente, por ejemplo los datos representativos de los campos de la pantalla.

Se debe destacar que algunas veces los datos representativos de un episodio de auditoría entrante incluyen datos que el usuario no modificó. Por ejemplo, un empleado puede visionar una pantalla de información de cliente que se refiera a uno de los clientes del banco. Si la pantalla incluye información acerca de la dirección y el número de teléfono del cliente, el empleado puede modificar la dirección y dejar el número de teléfono como apareció originalmente en la pantalla. En este caso, si el MDT indica que la dirección fue modificada, en la referencia **806** la información de la dirección recién insertada (según aparece en los datos representativos del episodio de auditoría entrante) sustituye la información de dirección original que aparecía en el correspondiente episodio de auditoría saliente, mientras la información del teléfono se deja intacta.

El procedimiento ilustrado en el diagrama de flujo de la **Fig. 8** puede ser adaptado para diferentes protocolos de pantalla heredada.

Se debe destacar que la división de los diferentes procedimientos entre el gerente especular **305** y el analizador **307** de episodios de auditoría ilustrados en las **Figs. 5, 7** y **8** no es limitativa. En diferentes formas de realización, el gerente especular **305** y el analizador **307** de episodios de auditoría pueden dividir las responsabilidades entre ellos de manera diferente. Por ejemplo, el gerente especular **305** puede generar datos representativos de sesiones especulares que incluyan también la identificación de pantallas y campos incluidos en ellas. En la forma de realización ilustrada en la **Fig. 8,** por ejemplo, la identificación de pantallas y campos se lleva a cabo en el analizador de episodios de auditoría y los datos representativos de los resultados de la identificación son incluidos en los datos representativos de los episodios de auditoría. La combinación también se autoriza por ejemplo, cuando los datos representativos de las sesiones especulares incluyan datos representativos de la identificación de pantalla y campo (esto es, los episodios de auditoría saliente) y cuando los datos representativos de los datos de identificación incluyan la identificación de datos representativos de la información insertada en episodios de auditoría entrantes, etc.

Después de comprender lo que son los episodios de auditoría y calibrar un ejemplo de la forma en que pueden ser generados los episodios de auditoría, se debe apreciar que, al controlar y auditar un sistema heredado, es ventajoso efectuar el seguimiento de los episodios de negocio que se producen en el sistema. Por ejemplo, se puede verificar cuántas nuevas cuentas bancarias fueron abiertas en el banco durante un periodo de tiempo determinado, y / o cuántas cuentas fueron abiertas por diferentes empleados. Con el fin de verificar esto, se define un episodio de negocio de “cuenta bancaria abierta”, como se analizó previamente en el ejemplo de un empleado de un banco, que abre una nueva cuenta bancaria.

Antes de volver a describir la forma en que los episodios de negocio se definen y la forma en que los datos representativos de episodios de negocio son generados, la descripción vuelve al ejemplo de empleado del banco. Anteriormente, este episodio de negocio (la apertura de una nueva cuenta bancaria) fue descrito como una combinación de seis episodios de auditoría entre el terminal empleado y el anfitrión (tres salientes y tres entrantes) y dos episodios de auditoría entre el terminal del gerente y auditoría (un saliente y un entrante). Se debe destacar que es posible describir este episodio de negocio también en términos de episodios de negocio unidos. Utilizando la terminología de los episodios de negocio unidos se debe apreciar que el episodio de negocio es una combinación de tres episodios de negocio unidos que implican el terminal del empleado y el anfitrión (la pantalla de información de nuevo cliente, la pantalla de información financiera, y la pantalla de cuenta aprobada / desaprobada) y un episodio de auditoría unido que implica el terminal del gerente y el anfitrión (la pantalla de aprobación de la nueva cuenta).

Al definir el episodio de auditoría saliente de la información de nuevo cliente, es el episodio de auditoría que inicializa el episodio de negocio. Es designado, por tanto, como un “desencadenante del inicio del episodio de negocio”. A continuación, viene el episodio de auditoría entrante de información de nuevo cliente, los episodios de auditoría saliente y entrante de información financiera, los episodios de auditoría saliente y entrante de aprobación de nueva cuenta y los episodios de auditoría salientes y entrantes de cuenta aprobada / desaprobada. Esto es, el episodio de auditoría entrante de cuenta aprobada / desaprobada completa el nuevo episodio de negocio de nueva cuenta bancaria abierta. Este episodio de auditoría es designado como “terminado del episodio de negocio”.

Sin embargo, el empleado (o el cliente) pueden arrepentirse en la mitad del proceso, terminando así antes de que la cuenta bancaria se abra completamente. En este caso, el desencadenante del episodio de negocio, es decir el episodio saliente de información de nuevo cliente será interceptado, pero solo parte de los episodios de auditoría esperados se producirán a continuación. El episodio de auditoría que será el último en este episodio de negocio parcial es designado como un “desencadenante de cancelación de episodio de negocio”.

Se ilustró en el ejemplo de la cuenta bancaria abierta que un episodio de negocio está compuesto por una cadena de episodios de auditoría, en la que la cadena termina con uno o más terminadores de episodios de negocio. En el ejemplo de la apertura de una nueva cuenta bancaria hay dos terminadores de episodio de negocio opcionales: los episodios de auditoría de cuenta aprobada y / o de cuenta desaprobada. Ejemplos más complicados hay también pocas opciones para los episodios de auditoría que estén en la mitad de la cadena. Por ejemplo, si un nuevo cliente es una mujer casada cuyo marido también tiene una cuenta en el banco, entonces, en lugar de abrir la pantalla de información financiera previamente introducida, abrirá otra pantalla, una pantalla de “información financiera familiar”, donde el crédito del marido aparece también.

Así, se debe apreciar por parte de los expertos en la materia que los episodios de auditoría opcionales que comprenden un episodio de negocio generan conjuntamente una estructura ramificada, en la que el desencadenante del episodio de negocio es el nodo de raíz y los terminadores del episodio de negocio son los nodos hoja. Otros nodos en el árbol algunas veces son designados como “desencadenantes agregados de episodios de negocio”.

La **Fig. 9** es un diagrama de flujo que ilustra la forma en que se define un episodio de negocio, de acuerdo con una forma de realización de la invención. En la referencia **901** se selecciona un desencadenante del inicio de un episodio de negocio, por ejemplo, entre un conjunto de episodios de auditoría disponibles. En la referencia **902** se seleccionan unos desencadenantes de episodios de negocio adicionales, en los que es posible marcar si el desencadenante es un terminador de episodios de negocio, un desencadenante de cancelación de episodios de negocio, o un desencadenante de agregados de episodios de negocio. Así mismo, es posible marcar lo que es el desencadenante que precede al desencadenante actual en el episodio de negocio.

Aún más, cuando hay parámetros que son parte de una definición desencadenante, estos parámetros (y su valor esperado, si es que existe) son suministrados en las referencias **901** y **902**.

Así mismo, algunas veces los desencadenantes incluyen parámetros. Por ejemplo, un episodio de auditoría de información de nuevo cliente es considerado como un desencadenante de inicio de un episodio de negocio solo si el nombre del cliente teclea en él “David Copperfield”. En un ejemplo alternativo, el episodio de auditoría de información de nuevo cliente es considerado solo como un desencadenante de inicio de episodio de negocio si su usuario asociado (esto es, el empleado en este caso, es “Huckleberry Finn”). Así mismo, es posible utilizar la posición del cursor como parámetro, así el episodio de auditoría de información de nuevo cliente es considerado como un desencadenante del inicio del episodio de negocio solo si, por ejemplo, la posición del cursor está entre la décima y la undécima líneas de la pantalla.

Volviendo ahora al analizador **309** de episodios de negocio, la **Fig. 10** es un diagrama de flujo que ilustra con detalle la generación de los datos representativos de los episodios de negocio, de acuerdo con una forma de realización de la invención. En la referencia **1001** los datos representativos de episodios de auditoría son recibidos. Los datos pueden ser limitados por diferentes criterios. Por ejemplo, pueden estar limitados por el tiempo, empezando a partir de un punto del tiempo y terminar en un segundo punto del tiempo. En el que los episodios de auditoría representados por los datos son asociados con uno o más asociados. En un ejemplo diferente, los datos representativos de los episodios de auditoría pueden ser asociados con solo un usuario predeterminado, etc. Los datos recibidos en la referencia **1001** son representativos de uno o más episodios de auditoría.

Los datos representativos de episodios de auditoría son procesados, un episodio cada vez. Cuando en la referencia **1002** se encuentra que no hay más episodios de auditoría cuyos datos representativos no estén procesados, el proceso ilustrado en la **Fig. 10** termina.

En la referencia **1003**, se accede a los datos representativos de un episodio de negocio a partir de los datos representativos de los episodios de negocio. Sin en la referencia **1004** se encuentra que este episodio de auditoría es un desencadenante del inicio de un episodio de negocio, se inicializa un nuevo episodio de negocio en la referencia **1005**, por ejemplo abriendo un nuevo archivo, abriendo una tabla en una base de datos o cualquier otra forma aplicable. En la referencia **1006**, los datos representativos del episodio de auditoría son adjuntados a los datos representativos del episodio de negocio. Debe destacarse, sin embargo, que esta etapa de los datos representativos

del episodio de negocio puede ser almacenada en la memoria o solo en un dispositivo de almacenamiento a largo plazo, como por ejemplo un disco o una base datos.

Sin embargo, en la referencia **1004** se encuentra que el episodio de auditoría no es un desencadenante del inicio de un episodio de negocio puede tratarse o bien de un terminado del episodio de negocio o un desencadenante de cancelación del episodio de negocio o un desencadenante de un agregado del episodio de negocio.

Si se buscan uno o más episodios de negocio específicos en los datos representativos de los episodio de negocio, en la referencia **1007** el episodio de auditoría representado por los datos representativos del episodio de auditoría son comparados con los nodos incluidos en estos árboles de los episodios de negocio, para ver si este episodio de auditoría puede ser parte de algún trayecto de estos árboles. Si no es así, este episodio de auditoría no es parte del episodio de negocio buscado y, por tanto, se puede acceder al siguiente episodio de auditoría (véanse las referencias **1002** y **1003**). Si se busca cualquier episodio de negocio para los datos representativos de episodios de negocio, la referencia **1007** el episodio de auditoría representado por los datos representativos del episodio de auditoría son comparados con los nodos incluidos en los árboles de cualquier episodio de negocio cuya raíz sea el desencadenante del inicio de episodio de negocio anteriormente detectado. Si el episodio de auditoría no puede ser parte de ningún trayecto en ninguno de estos árboles, este episodio de auditoría no es parte de un episodio de negocio y por tanto se puede acceder al siguiente episodio de auditoría (véanse las referencias **1002** y **1003**).

Si en la referencia **1007** se encuentra que el episodio de auditoría es parte de uno o más episodios de negocio, en la referencia **1008** se verifica si es un episodio de negocio terminador o un episodio de negocio de desencadenamiento de cancelación de cualquiera de estos episodios de negocio. Si es así, el episodio de negocio se termina en la referencia **1009**, y en la referencia **1010** los datos representativos del episodio de negocio son almacenados en un dispositivo de almacenamiento (si en la referencia **1006** los datos representativos del episodio de negocio son almacenados en un dispositivo de almacenamiento a largo plazo, entonces la referencia **1010** es redundante). Sin embargo, si en la referencia **1008** se encuentra que el episodio de auditoría es un desencadenante de agregados del episodio de negocio, en la referencia **1011** los episodios de negocio de los que es parte el episodio de auditoría se abren (o se accede a ellos), y en la referencia **1006** los datos representativos del episodio de auditoría se adjunta a aquellos.

Debe destacarse que un episodio de auditoría que indica que la sesión se ha terminado sirve como desencadenante de la cancelación del episodio de negocio para todos los episodios de negocio abierto en estas sesiones, esto es, para todos los episodios de negocio de la sesión que actualmente son objeto de seguimiento.

Así mismo, cuando los datos representativos de un episodio de negocio están almacenados, es posible generar una alerta o un mensaje de alerta (por ejemplo, enviando un correo electrónico, suscitando una alerta en una consola, iniciando un proceso en el sistema heredado o en cualquier otro sistema, o de cualquier otra forma aplicable) indicando que este episodio ha tenido lugar. Puede haber una lista (o un repositorio) de episodios de negocio que deberían suscitar alertas, y su respectiva gravedad. Se suscitan entonces alertas de acuerdo con este repositorio. Debe apreciarse que el repositorio y la generación de alertas pueden estar situadas en el gerente **312** de alertas.

A mayor abundamiento, el gerente de alertas puede generar al menos algunas de las alertas en base a umbrales predeterminados. Por ejemplo, si una alerta debe ser generada siempre que un determinado usuario intenta un inicio de sesión en el sistema, es posible contar con un umbral para esta alerta. Por ejemplo, una alerta debería ser generada solo si este determinado usuario intenta iniciar una sesión diez veces en el sistema (el umbral es “diez veces” en este caso).

Debe destacarse que el control de los episodios de negocio puede ser utilizado para detectar fraudes. Por ejemplo, los empleados del banco cuentan con unos niveles de franquía que les permite acceder a la información relacionada con determinadas cuentas, pero no a otra cuenta. Es posible buscar a esos empleados que intentan acceder a la cuenta a la cual no tienen derechos de acceso.

En un ejemplo diferente es posible buscar episodios de negocio en los que los empleados intentan acceder a cuentas utilizando nombres de los clientes en lugar de utilizar el número de cuenta. Normalmente se accede a la información relacionada con una cuenta bancaria tecleando el número de cuenta en el terminal del empleado. Sin embargo, es posible buscar cuentas pertenecientes a un determinado cliente, a continuación acceder a una de sus (de él o ella) cuentas. Un cliente que accede a muchas cuentas utilizando nombres de clientes puede suscitar la sospecha de fraude. En este caso, “buscar cuentas del cliente” puede ser el desencadenante del inicio de un episodio de negocio.

REIVINDICACIONES

1.- Un aparato (107) para controlar y auditar la actividad de un sistema heredado, comprendiendo el aparato:

un analizador (303) que está configurado para analizar paquetes interceptados, en el que dichos paquetes son transportados entre terminales y anfitriones (102, 103, 104) de dicho sistema heredado, en el que dichos anfitriones de dicho sistema heredado utilizan al menos un protocolo de pantalla heredado incremental para transportar campos asociados con una pantalla hacia un terminal y en el que dicho analizador está también configurado para generar datos analizados en base a la información asociada con al menos alguno de dichos paquetes, siendo los datos analizados indicativos de sesiones de dicho sistema heredado e indicativos de un protocolo de pantalla incremental utilizado en dichas sesiones;

un gerente especular (305) sensible a dichos datos analizados para generar datos representativos de sesiones especulares, correspondiendo cada sesión especular a una de dichas sesiones;

un analizador (307) de episodios de auditoría que es sensible a dichos datos especulares, estando dicho analizador de episodios de auditoría configurado para generar un episodio de auditoría saliente que comprende campos asociados con una pantalla dispuesta para ser mostrada en un terminal de dicho sistema heredado, comprendiendo dichos campos al menos un campo de entrada para permitir que un usuario inserte en su interior una información de entrada y un episodio de auditoría entrante que comprende una información de entrada insertada por un usuario de un terminal dentro de un campo de entrada asociado con una pantalla y una localización de pantalla que indica el lugar en el que dicha información de entrada fue insertada en dicha pantalla;

estando también configurado dicho analizador de episodio de auditoría para asociar un episodio de auditoría entrante con un episodio de auditoría saliente; para identificar datos representativos de la información de entrada insertados por un usuario en un episodio de auditoría entrante; y para formar datos representativos de un episodio de auditoría unido combinando datos representativos de un episodio de auditoría saliente con datos representativos de una información de entrada en un episodio de auditoría entrante asociado.

2.- El aparato de la reivindicación 1, que comprende además:

un terminal sensible a dichos datos representativos de un episodio de auditoría unido para representar dicho episodio de auditoría unido.

3.- El aparato de la reivindicación 1, que comprende además:

un analizador de episodios de negocio para procesar al menos parte de dichos datos representativos de episodios de auditoría salientes, entrantes y unidos y generar datos representativos de episodios de negocio.

4.- El aparato de la reivindicación 3, que comprende además:

un gerente (312) de alertas acoplado al analizador de episodios de negocio y que es sensible a dichos datos representativos de episodios de negocio para generar alertas.

5.- El aparato de la reivindicación 4, en el que los gerentes de alertas están configurados para generar al menos alguna de las alertas en base a umbrales predeterminados.

6.- El aparato de una cualquiera de las reivindicaciones precedentes, que comprende además:

un primer dispositivo (304) de almacenamiento a largo plazo para almacenar al menos parte de dichos datos analizados.

7.- El aparato de una cualquiera de las reivindicaciones precedentes, que comprende además:

un segundo dispositivo (306) de almacenamiento a largo plazo para almacenar al menos parte de dichos datos especulares representativos de sesiones especulares.

8.- El aparato de una cualquiera de las reivindicaciones precedentes, que comprende además:

un agente (313) de compresión para comprimir al menos parte de los datos especulares representativos de sesiones especulares.

9.- El aparato de una cualquiera de las reivindicaciones precedentes, que comprende además:

un agente de encriptación para encriptar al menos parte de los datos especulares representativos de una sesión especular.

10.- El aparato de una cualquiera de las reivindicaciones precedentes, que comprende además:

un agente de firma para firmar digitalmente al menos parte de los datos especulares representativos de sesiones especulares.

11.- Un procedimiento para controlar y auditar la actividad de un sistema heredado, comprendiendo el procedimiento:

el análisis de los paquetes interceptados, siendo dichos paquetes transportados por terminales y anfitriones (102, 103, 104) de dicho sistema heredado, en el que dichos anfitriones de dicho sistema heredado utilizan al menos un protocolo de pantalla heredado incremental para transportar los campos asociados con una pantalla hacia un terminal;

la generación de datos analizados en base a la información asociada con al menos alguno de dichos paquetes, siendo los datos analizados indicativos de sesiones de dicho sistema heredado e indicativos de un protocolo de pantalla incremental utilizado en cada una de dichas sesiones;

la generación de datos representativos de sesiones especulares en respuesta a dichos datos analizados, correspondiendo cada sesión especular a una de dichas sesiones;

la generación de un episodio de auditoría saliente que comprende campos asociados con una pantalla destinada a ser mostrada en un terminal de dicho sistema heredado, comprendiendo dichos campos al menos un campo de entrada para permitir que un usuario inserte en su interior una información de entrada y un episodio de auditoría entrante que comprende una información de entrada insertada por un usuario de un terminal dentro de un campo de entrada asociado con una pantalla y una localización de pantalla que indica el lugar en el que dicha información de entrada fue insertada en dicha pantalla;

la asociación de un episodio de auditoría entrante con un episodio de auditoría saliente;

la identificación de datos representativos de una información de entrada insertados por un usuario en un episodio de auditoría entrante; y

la información de un episodio de auditoría unido combinando datos representativos de dicha auditoría de episodios salientes y dichos datos representativos de dicha información de entrada insertados por dicho usuario en un episodio de auditoría entrante.

12.- El procedimiento de la reivindicación 11, que comprende además:

el procesamiento de al menos parte de dichos datos representativos de episodios de auditoría salientes, entrantes y unidos y la generación de datos representativos de episodio de negocio.

13.- El procedimiento de la reivindicación 12, que comprende además:

la generación, en respuesta a dichos datos representativos de episodios de negocio de alertas con respecto a al menos uno de dichos episodios de negocio.

14.- El procedimiento de la reivindicación 13, en el que la generación de al menos alguna de dichas alertas se basa en umbrales predeterminados.

15.- El procedimiento de una cualquiera de las reivindicaciones 11 a 14, que comprende además:

el almacenamiento de al menos parte de los datos analizados.

16.- El procedimiento de una cualquiera de las reivindicaciones 11 a 15, que comprende además:

el almacenamiento de al menos parte de los datos especulares representativos de sesiones especulares.

17.- El procedimiento de una cualquiera de las reivindicaciones 11 a 16, que comprende además:

la compresión de al menos parte de dichos datos especulares representativos de sesiones especulares.

18.- E procedimiento de una cualquiera de las reivindicaciones 11 a 17, que comprende además:

la encriptación de al menos parte de dichos datos especulares representativos de sesiones especulares.

19.- El procedimiento de una cualquiera de las reivindicaciones 11 a 18, que comprende además:

la firma digitalizada de al menos parte de dichos datos especulares representativos de una sesión especular.

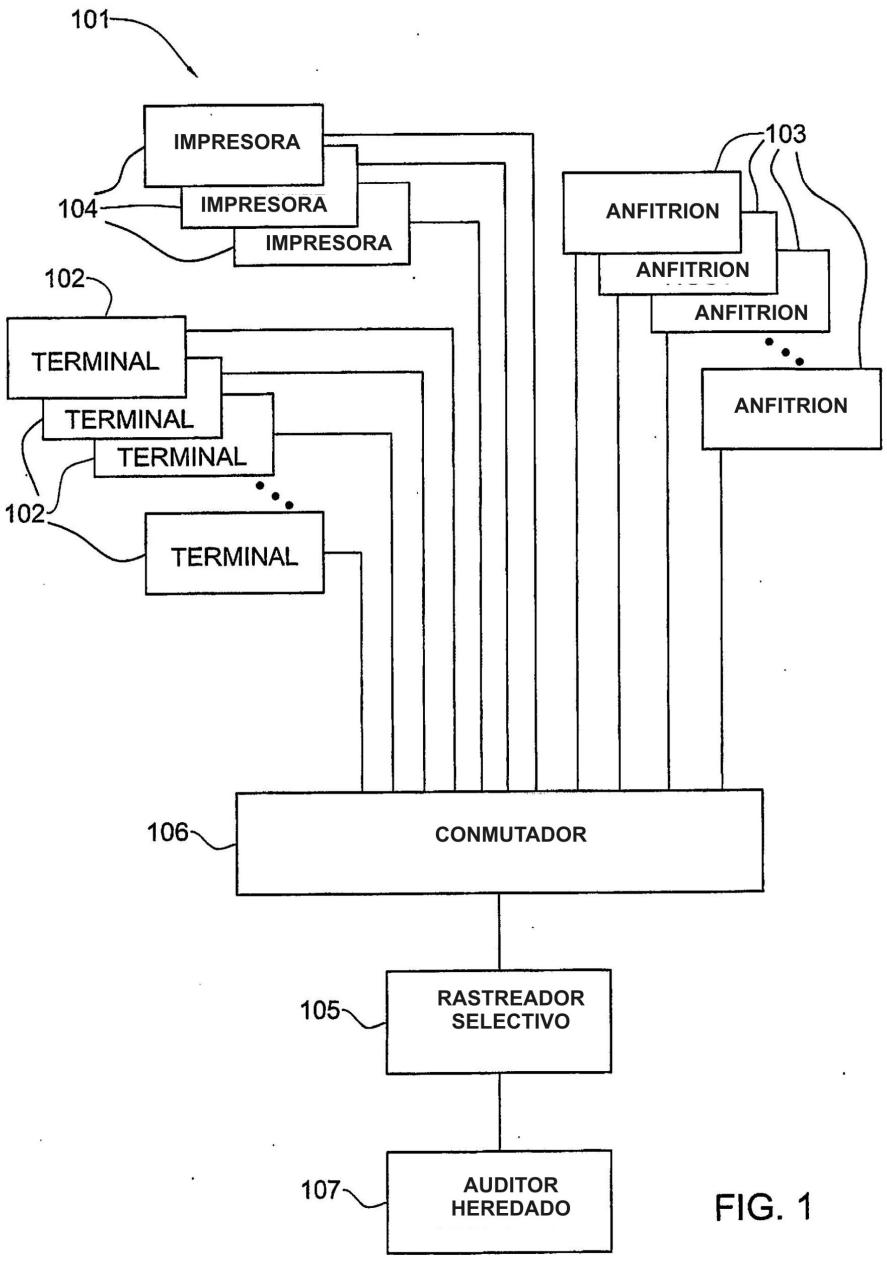
101
IMPRESORA
IMPRESORA
IMPRESORA
104
102
TERMINAL
TERMINAL
TERMINAL
102
TERMINAL
103
ANFITRION
ANFITRION
ANFITRION
ANFITRION
106
CONMUTADOR
105
RASTREADOR SELECTIVO
107
AUDITOR HEREDADO

FIG. 1

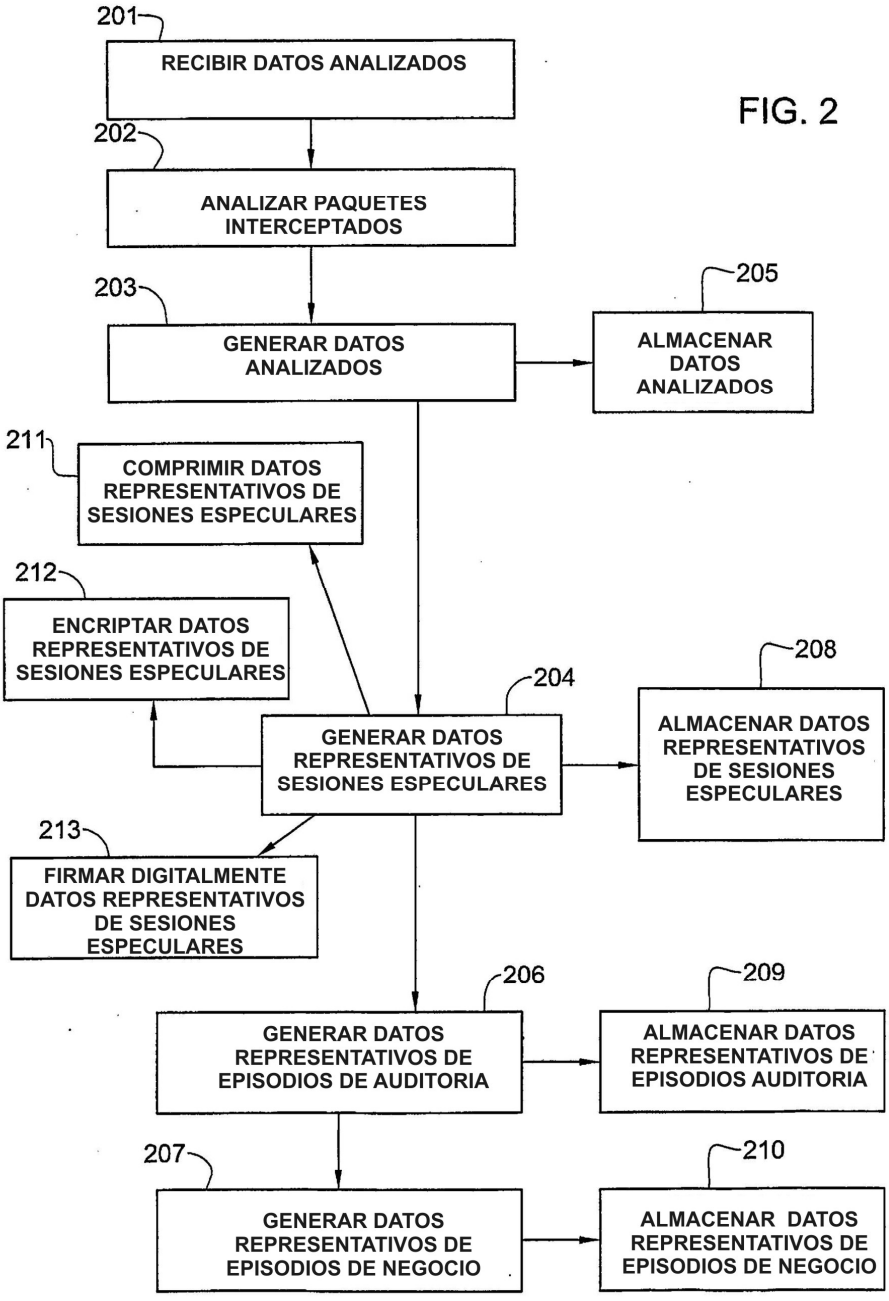
201
RECIBIR DATOS ANALIZADOS
202
ANALIZAR PAQUETES INTERCEPTADOS
203
GENERAR DATOS ANALIZADOS
205
ALMACENAR DATOS ANALIZADOS
211
COMPRIMIR DATOS REPRESENTATIVOS DE SESIONES ESPECULARES
212
ENCRIPTAR DATOS REPRESENTATIVOS DE SESIONES ESPECULARES
204
GENERAR DATOS REPRESENTATIVOS DE SESIONES ESPECULARES
208
ALMACENAR DATOS REPRESENTATIVOS DE SESIONES ESPECULARES
213
FIRMAR DIGITALMENTE DATOS REPRESENTATIVOS DE SESIONES ESPECULARES
206
GENERAR DATOS REPRESENTATIVOS DE EPISODIOS DE AUDITORIA
209
ALMACENAR DATOS REPRESENTATIVOS DE EPISODIOS AUDITORIA
207
GENERAR DATOS REPRESENTATIVOS DE EPISODIOS DE NEGOCIO
210
ALMACENAR DATOS REPRESENTATIVOS DE EPISODIOS DE NEGOCIO

FIG. 2

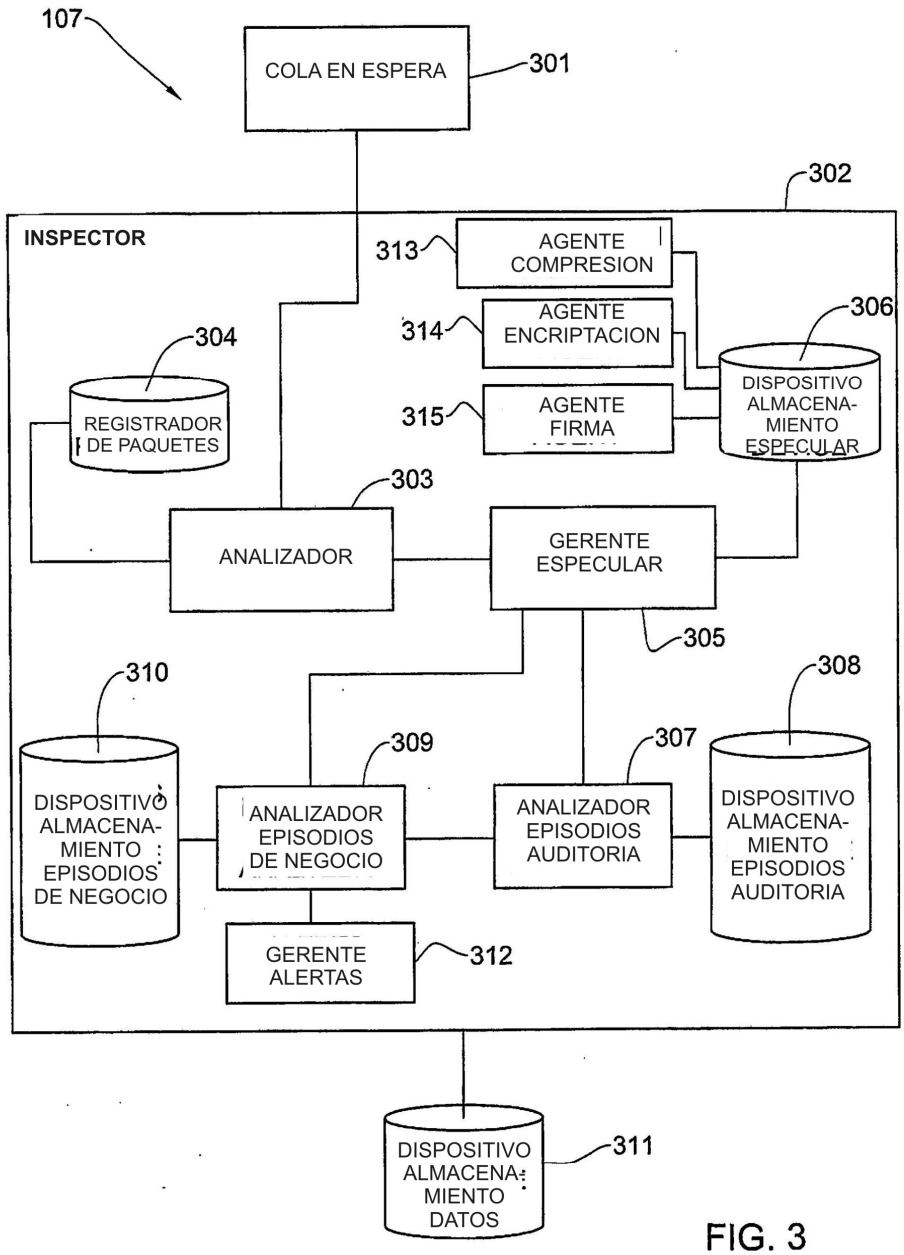
107
COLA EN ESPERA
301
302
INSPECTOR
313
AGENTE COMPRESION
314
AGENTE ENCRIPTACION
315
AGENTE FIRMA
306
DISPOSITIVO ALMACENA-MIENTO ESPECULAR
304
REGISTRADOR DE PAQUETES
303
ANALIZADOR
GERENTE ESPECULAR
305
310
DISPOSITIVO ALMACENA-MIENTO EPISODIOS DE NEGOCIO
309
ANALIZADOR EPISODIOS DE NEGOCIO
307
ANALIZADOR EPISODIOS AUDITORIA
308
DISPOSITIVO ALMACENA-MIENTO EPISODIOS AUDITORIA
GERENTE ALERTAS
312
DISPOSITIVO ALMACENA-MIENTO DATOS
311

FIG. 3

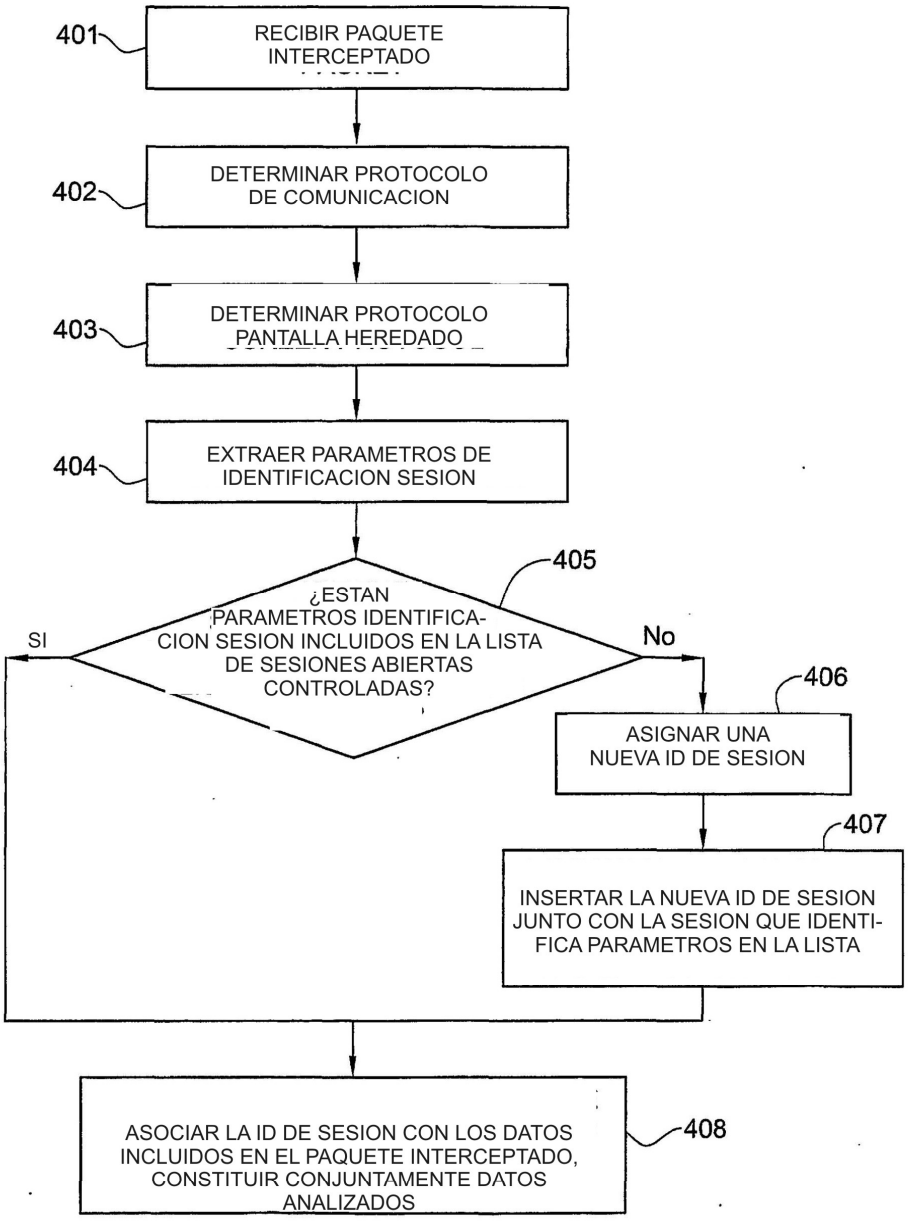
401
RECIBIR PAQUETE INTERCEPTADO
402
DETERMINAR PROTOCOLO DE COMUNICACION
403
DETERMINAR PROTOCOLO PANTALLA HEREDADO
404
EXTRAER PARAMETROS DE IDENTIFICACION SESION
405
¿ESTAN PARAMETROS IDENTIFICACION SESION INCLUIDOS EN LA LISTA DE SESIONES ABIERTAS CONTROLADAS?
SI
No
406
ASIGNAR UNA NUEVA ID DE SESION
407
INSERTAR LA NUEVA ID DE SESION JUNTO CON LA SESION QUE IDENTIFICA PARAMETROS EN LA LISTA
ASOCIAR LA ID DE SESION CON LOS DATOS INCLUIDOS EN EL PAQUETE INTERCEPTADO, CONSTITUIR CONJUNTAMENTE DATOS ANALIZADOS
408

FIG. 4

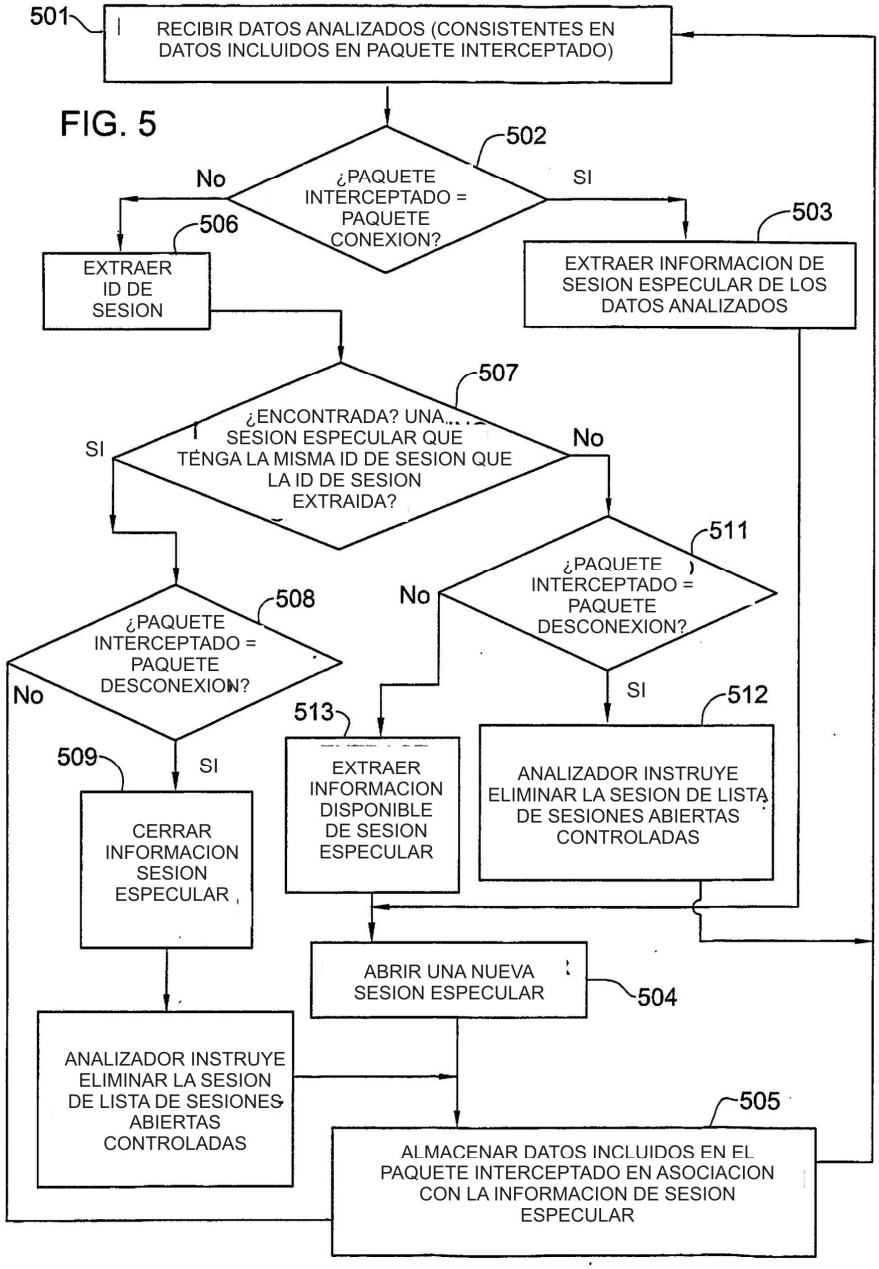
501
RECIBIR DATOS ANALIZADOS (CONSISTENTES EN DATOS INCLUIDOS EN PAQUETE INTERCEPTADO)
502
¿PAQUETE INTERCEPTADO = PAQUETE CONEXION?
No
SI
506
EXTRAER ID DE SESION
503
EXTRAER INFORMACION DE SESION ESPECULAR DE LOS DATOS ANALIZADOS
507
¿ENCONTRADA? UNA SESION ESPECULAR QUE TENGA LA MISMA ID DE SESION QUE LA ID DE SESION EXTRAIDA?
SI
No
508
¿PAQUETE INTERCEPTADO = PAQUETE DESCONEXION?
No
509
SI
CERRAR INFORMACION SESION ESPECULAR
511
¿PAQUETE INTERCEPTADO = PAQUETE DESCONEXION?
No
SI
512
ANALIZADOR INSTRUYE ELIMINAR LA SESION DE LISTA DE SESIONES ABIERTAS CONTROLADAS
513
EXTRAER INFORMACION DISPONIBLE DE SESION ESPECULAR
ABRIR UNA NUEVA SESION ESPECULAR
504
ANALIZADOR INSTRUYE ELIMINAR LA SESION DE LISTA DE SESIONES ABIERTAS CONTROLADAS
505
ALMACENAR DATOS INCLUIDOS EN EL PAQUETE INTERCEPTADO EN ASOCIACION CON LA INFORMACION DE SESION ESPECULAR

FIG. 5

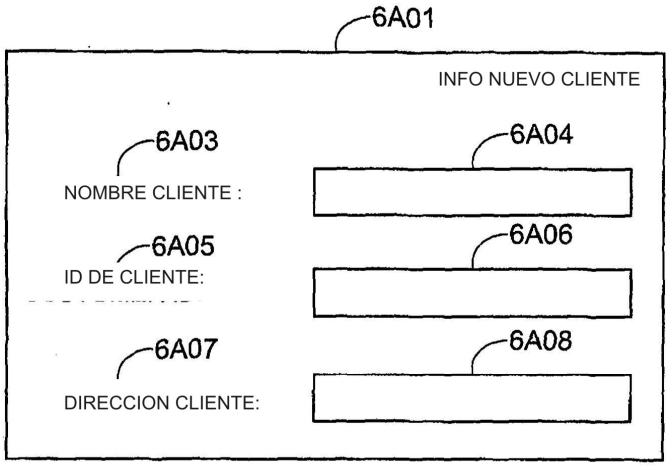
6A01
INFO NUEVO CLIENTE
6A03
NOMBRE CLIENTE :
6A04
6A05
ID DE CLIENTE:
6A06
6A07
DIRECCION CLIENTE:
6A08

FIG. 6A

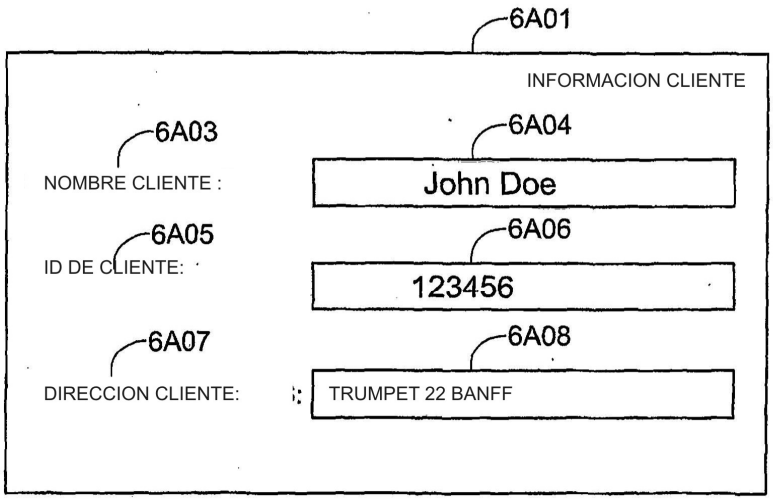
6A01
INFORMACION CLIENTE
6A03
NOMBRE CLIENTE :
6A04
John Doe
6A05
ID DE CLIENTE:
6A06
123456
6A07
DIRECCION CLIENTE:
6A08
TRUMPET 22 BANFF

FIG. 6B

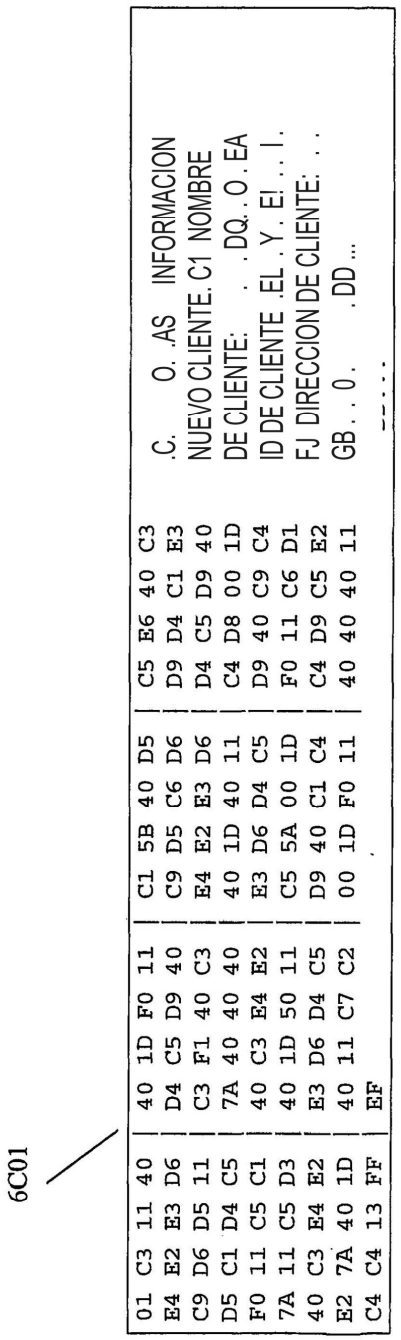
6C01
01 C3 11 40 | 40 1D F0 11 | C1 5B 40 D5 | C5 E6 40 C3 .C. O. .AS INFORMACION
E4 E2 E3 D6 | D4 C5 D9 40 | C9 D5 C6 D6 | D9 D4 C1 E3 NUEVO CLIENTE. C1 NOMBRE
C9 D6 D5 11 | C3 F1 40 C3 | E4 E2 E3 D6 | D4 C5 D9 40 DE CLIENTE: . . DQ. . O. EA
D5 C1 D4 C5 | 7A 40 40 40 | 40 1D 40 11 | C4 D8 00 1D ID DE CLIENTE .EL . Y. EI . . I.
F0 11 C5 C1 | 40 C3 E4 E2 | E3 D6 D4 C5 | D9 40 C9 C4 FJ DIRECCION DE CLIENTE: . .
7A 11 C5 D3 | 40 1D 50 11 | C5 5A 00 1D | F0 11 C6 D1 GB . . 0 . .DD ...
40 C3 E4 E2 | E3 D6 D4 C5 | D9 40 C1 C4 | C4 D9 C5 E2
E2 7A 40 1D | 40 11 C7 C2 | 00 1D F0 11 | 40 40 40 11
C4 C4 13 FF | EF
6D01
7D C6 7B 11 | C4 C4 D1 D6 | C8 D5 40 C4 | D6 C5 11 C5 .-F#. DDJOHN DOE. E
D4 F1 F2 F3 | F4 F5 F6 11 | C6 E4 E3 D9 | E4 D4 D7 C5 M123456 . FUTRUMPE
E3 40 F2 F2 | 40 C2 C1 D5 | C6 C6 40 40 | 40 40 40 40 T 2 BANFF
40 FF EF

FIG. 6C

FIG. 6D

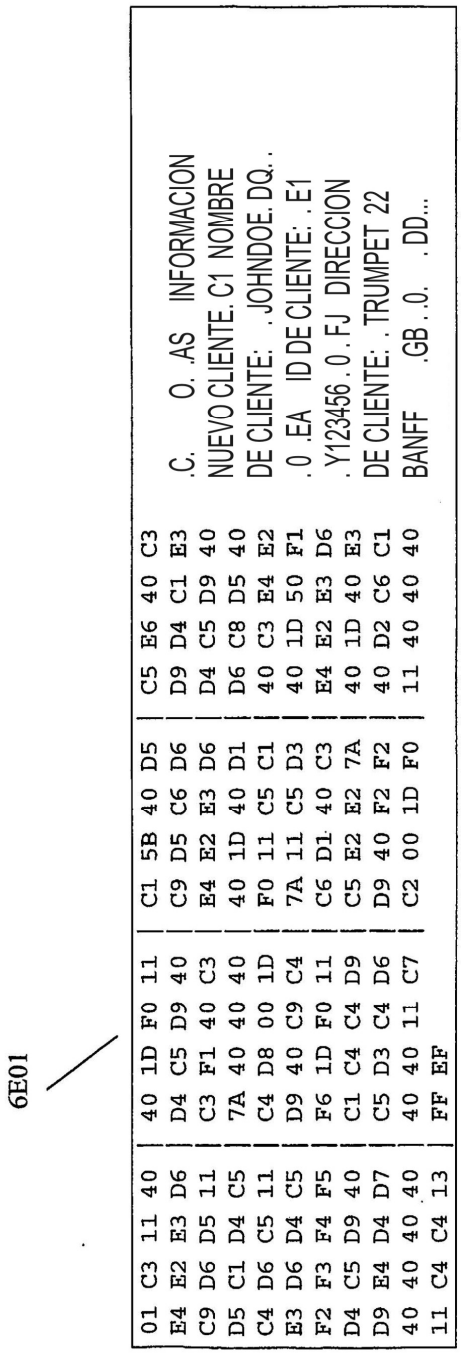
6E01
01 C3 11 40 | 40 1D F0 11 | C1 5B 40 D5 | C5 E6 40 C3
E4 E2 E3 D6 | D4 C5 D9 40 | C9 D5 C6 D6 | D9 D4 C1 E3
C9 D6 D5 11 | C3 F1 40 C3 | E4 E2 E3 D6 | D4 C5 D9 40
D5 C1 D4 C5 | 7A 40 40 40 | 40 1D 40 D1 | D6 C8 D5 40
C4 D6 C5 11 | C4 D8 00 1D | F0 11 C5 C1 | 40 C3 E4 E2
E3 D6 D4 C5 | D9 40 C9 C4 | 7A 11 C5 D3 | 40 1D 50 F1
F2 F3 F4 F5 | F6 1D F0 11 | C6 D1 40 C3 | E4 E2 E3 D6
D4 C5 D9 40 | C1 C4 C4 D9 | C5 E2 E2 7A | 40 1D 40 E3
D9 E4 D4 D7 | C5 D3 C4 D6 | D9 40 F2 F2 | 40 D2 C6 C1
40 40 40 40 | 40 40 11 C7 | C2 00 1D F0 | 11 40 40 40
11 C4 C4 13 | FF EF
.C. O. .AS INFORMACION
NUEVO CLIENTE. C1 NOMBRE
DE CLIENTE: . .JOHNDOE. DQ. .
.0 .EA ID DE CLIENTE: . E1
.Y123456 . 0 . FJ DIRECCION
DE CLIENTE: . .TRUMPET 22
BANFF .GB . .0. . .DD...

FIG. 6E

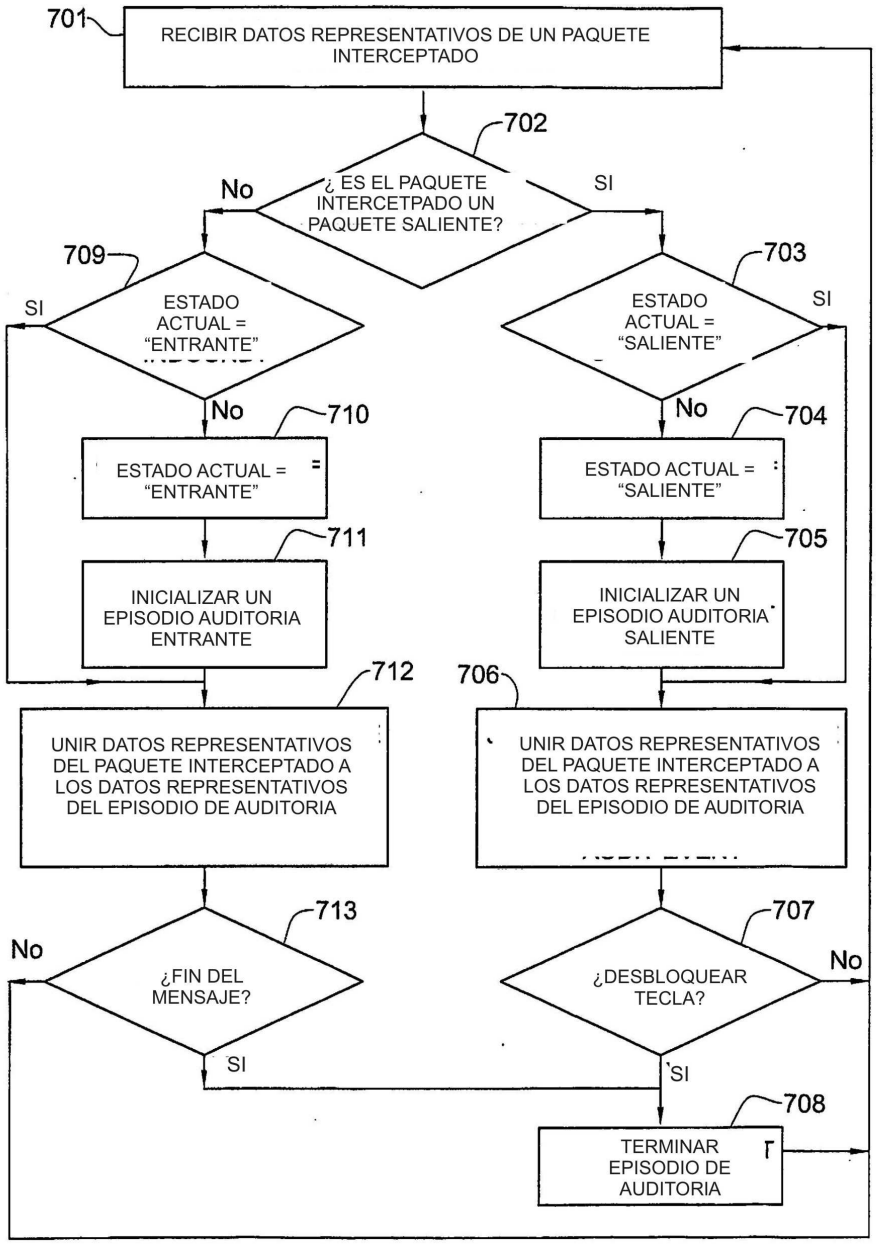
701
RECIBIR DATOS REPRESENTATIVOS DE UN PAQUETE INTERCEPTADO
702
¿ ES EL PAQUETE INTERCETPADO UN PAQUETE SALIENTE?
No
SI
709
ESTADO ACTUAL = "ENTRANTE"
SI
No
710
ESTADO ACTUAL = "ENTRANTE"
711
INICIALIZAR UN EPISODIO AUDITORIA ENTRANTE
712
UNIR DATOS REPRESENTATIVOS DEL PAQUETE INTERCEPTADO A LOS DATOS REPRESENTATIVOS DEL EPISODIO DE AUDITORIA
713
No
¿FIN DEL MENSAJE?
SI
703
ESTADO ACTUAL = "SALIENTE"
SI
No
704
ESTADO ACTUAL = "SALIENTE"
705
INICIALIZAR UN EPISODIO AUDITORIA SALIENTE
706
UNIR DATOS REPRESENTATIVOS DEL PAQUETE INTERCEPTADO A LOS DATOS REPRESENTATIVOS DEL EPISODIO DE AUDITORIA
707
¿DESBLOQUEAR TECLA?
No
SI
708
TERMINAR EPISODIO DE AUDITORIA

FIG. 7

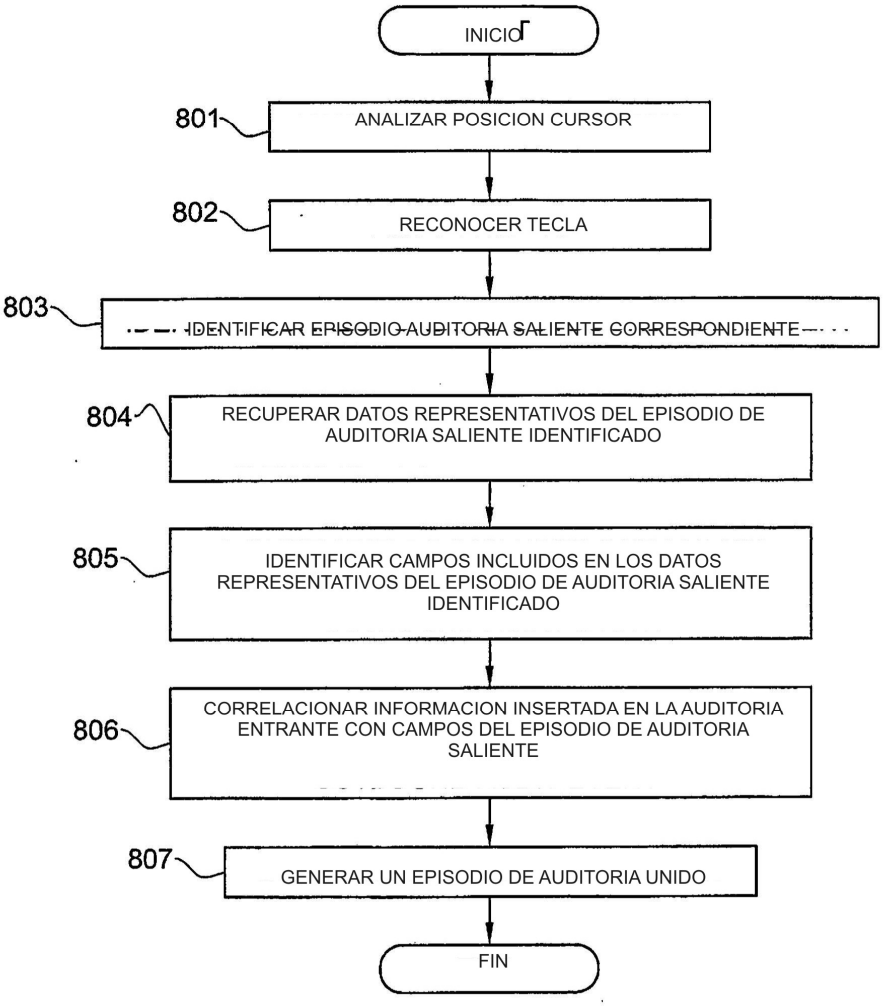
INICIO
801
ANALIZAR POSICION CURSOR
802
RECONOCER TECLA
803
IDENTIFICAR EPISODIO AUDITORIA SALIENTE CORRESPONDIENTE
804
RECUPERAR DATOS REPRESENTATIVOS DEL EPISODIO DE AUDITORIA SALIENTE IDENTIFICADO
805
IDENTIFICAR CAMPOS INCLUIDOS EN LOS DATOS REPRESENTATIVOS DEL EPISODIO DE AUDITORIA SALIENTE IDENTIFICADO
806
CORRELACIONAR INFORMACION INSERTADA EN LA AUDITORIA ENTRANTE CON CAMPOS DEL EPISODIO DE AUDITORIA SALIENTE
807
GENERAR UN EPISODIO DE AUDITORIA UNIDO
FIN

FIG. 8

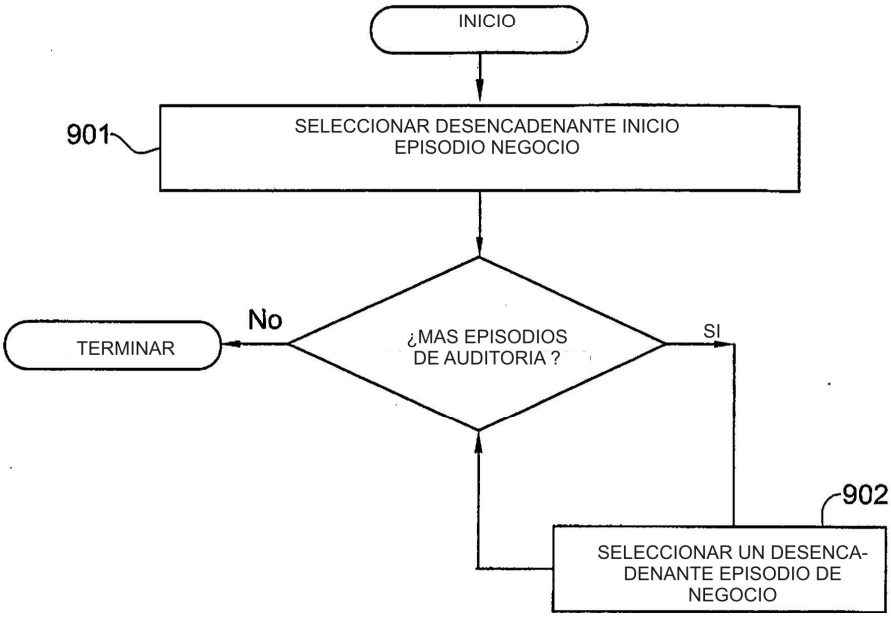
INICIO
901
SELECCIONAR DESENCADENANTE INICIO EPISODIO NEGOCIO
No
TERMINAR
¿MAS EPISODIOS DE AUDITORIA ?
SI
902
SELECCIONAR UN DESENCA-DENANTE EPISODIO DE NEGOCIO

FIG. 9

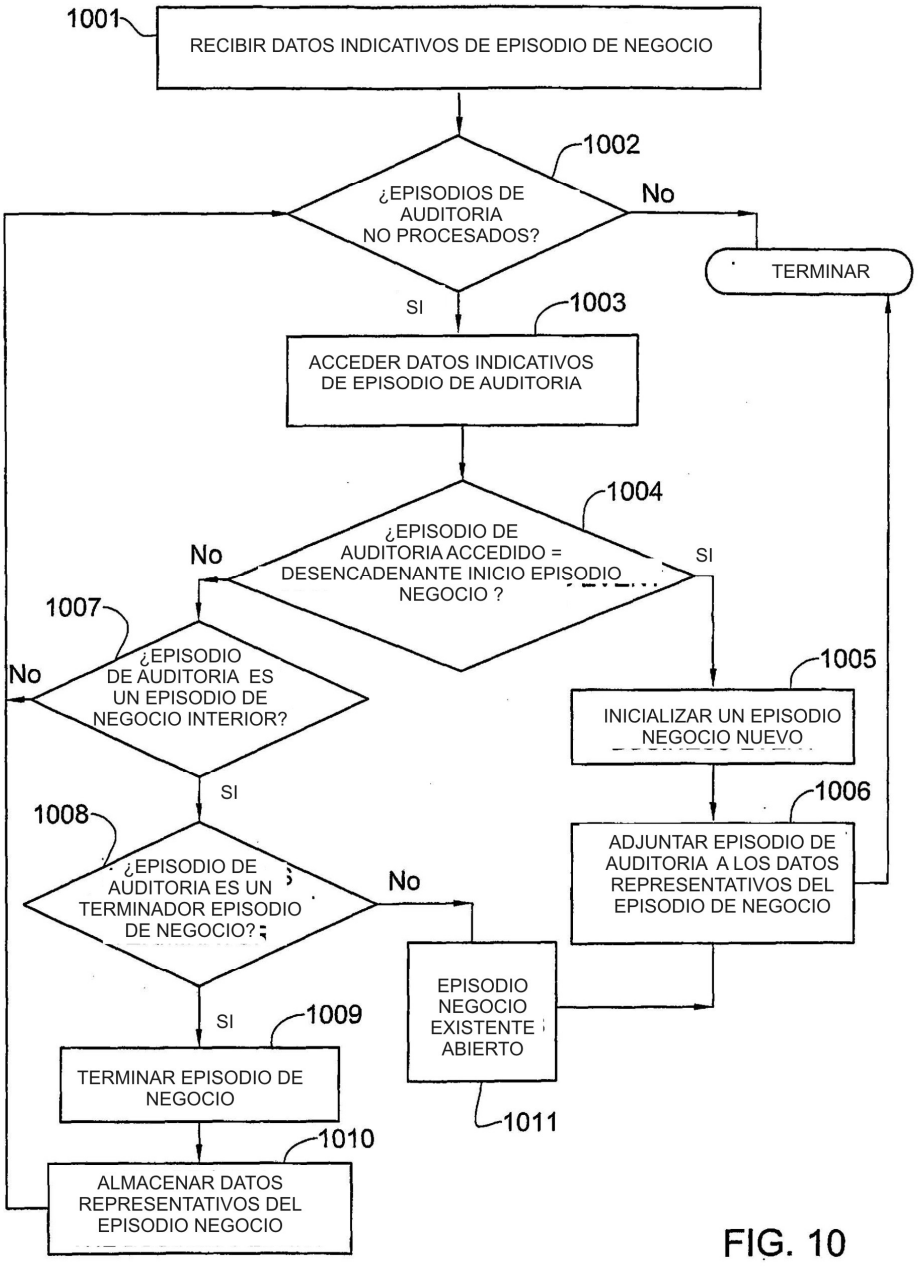
1001
RECIBIR DATOS INDICATIVOS DE EPISODIO DE NEGOCIO
1002
¿EPISODIOS DE AUDITORIA NO PROCESADOS?
No
TERMINAR
SI
1003
ACCEDER DATOS INDICATIVOS DE EPISODIO DE AUDITORIA
1004
¿EPISODIO DE AUDITORIA ACCEDIDO = DESENCADENANTE INICIO EPISODIO NEGOCIO ?
No
SI
1007
¿EPISODIO DE AUDITORIA ES UN EPISODIO DE NEGOCIO INTERIOR?
No
SI
1005
INICIALIZAR UN EPISODIO NEGOCIO NUEVO
1006
ADJUNTAR EPISODIO DE AUDITORIA A LOS DATOS REPRESENTATIVOS DEL EPISODIO DE NEGOCIO
1008
¿EPISODIO DE AUDITORIA ES UN TERMINADOR EPISODIO DE NEGOCIO?
No
SI
EPISODIO NEGOCIO EXISTENTE ABIERTO
1011
1009
TERMINAR EPISODIO DE NEGOCIO
1010
ALMACENAR DATOS REPRESENTATIVOS DEL EPISODIO NEGOCIO

FIG. 10