(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 749 436**

(51) Int. CI.:

H04M 3/51 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **22.03.2011 PCT/GB2011/000406**

(87) Fecha y número de publicación internacional: **29.09.2011 WO11117573**

(96) Fecha de presentación y número de la solicitud europea: **22.03.2011 E 11720562 (5)**

(97) Fecha y número de publicación de la concesión europea: **24.07.2019 EP 2550795**

(54) Título: **Procedimiento y sistema para la seguridad de transacciones**

(30) Prioridad:

22.03.2010 GB 201004754

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
20.03.2020

(73) Titular/es:

ECKOH UK LIMITED (100.0%)
Telford House, Corner Hall, Hemel Hempstead
Hertfordshire HP3 9HN, GB

(72) Inventor/es:

ROSS, CAMERON, PETER, SUTHERLAND;
HEATH, JAMES;
BRIDEN, THOMAS, EDWARD y
BAMFORD, RYAN, PETER

(74) Agente/Representante:

RIZZO , Sergio

DESCRIPCIÓN

Procedimiento y sistema para la seguridad de transacciones

Campo de la invención

[0001] Por lo general, la invención se refiere al procesamiento de señales de datos que representan audio, en particular para evitar la grabación y la presentación de información confidencial durante transacciones telefónicas.

Estado de la técnica

[0002] Los centros de llamadas son ampliamente utilizados por proveedores de servicios para la prestación de servicios y la comunicación con los clientes. Los centros de llamadas suelen comprender un amplio grupo de miembros del personal que reciben llamadas telefónicas de los clientes o que hacen llamadas telefónicas a los clientes. Los centros de llamadas normalmente implementan dos piezas fundamentales de la tecnología para ayudar a la formación del personal, la gestión de reclamaciones de los clientes o la conservación de información. Estas son tecnologías de grabación de llamadas, en las que se guarda una grabación de audio de la conversación con el cliente, así como las tecnologías de grabación de pantalla, en las que se guarda un vídeo o instantánea estática del terminal informático del miembro de personal.

[0003] Cada año, millones de personas llaman a los centros de llamadas para realizar consultas de servicios o transacciones financieras o emitir instrucciones a empresas con las que tratan. En muchos casos, el cliente debe, bien confirmar su identidad al proporcionar una respuesta a preguntas de seguridad, bien proporcionar información relativa a su tarjeta de crédito para pagar una transacción. Como se puede observar, la naturaleza de la mayoría de esta información es muy confidencial. En particular, la información puede incluir contraseñas, información de identificación personal, tal como la fecha de nacimiento, un PIN, una frase fácil de memorizar, números de cuentas bancarias y códigos de seguridad de tarjeta de crédito, entre otros.

[0004] El robo de datos y de identidades, así como las transacciones financieras fraudulentas, están muy extendidos, por lo que es muy interesante para la persona que llama mantener en secreto la mayor cantidad de información posible. La revelación de información financiera de índole confidencial y personal u otro tipo de información de seguridad a un miembro del personal de un centro de llamadas puede, potencialmente, aumentar la pérdida de datos personales de diversas maneras. En primer lugar, el miembro del personal del centro de llamadas puede anotarse la información del cliente para una utilización posterior. En segundo lugar, cualquier persona que tenga acceso a una grabación de audio de la conversación del cliente puede escuchar la información del cliente y apuntarla. En tercer lugar, cualquier persona que tenga acceso a una grabación de pantalla tomada en el momento que la información del cliente apareció en una pantalla de ordenador del miembro del personal del centro de llamadas podría anotarla. En cuarto lugar, existe tecnología para “extraer” de forma automática grabaciones de audio y pantalla para obtener información del cliente, y la pérdida de datos a través de este modo puede, potencialmente, extenderse.

[0005] A consecuencia de estas preocupaciones en materia de seguridad que van en aumento, algunos gobiernos han consagrado normas de seguridad en relación con el almacenamiento de datos en su legislación, y algunos órganos de la industria han adoptado sus propias directrices sobre el almacenamiento de datos personales. Un ejemplo es el Consejo de Normas de Seguridad de la Industria de Tarjetas de Pago (PCI, por sus siglas en inglés), que publica directrices para el procesamiento y el almacenamiento de datos de tarjetas de crédito globalmente. Sus Normas de Seguridad de Datos (DSS, por sus siglas en inglés), que se actualizan periódicamente, imponen los procedimientos y los modos en los que las empresas que procesan datos de tarjetas de crédito (incluidas las transacciones con tarjetas de crédito por teléfono) pueden almacenar datos relativos a tarjetas y personales. Las regulaciones y directrices tales como las anteriores tienen un impacto directo en los centros de llamadas, que recogen los datos confidenciales de los clientes en las conversaciones telefónicas. Por ejemplo, las DSS estipulan que el valor de verificación de la tarjeta de 3 o 4 dígitos (CV2 - en ocasiones denominado CVN, CW2, CVC2 o CID) no se debe almacenar en cualquier formato, incluidas las grabaciones de audio cifradas.

[0006] En la figura 1, se muestra de forma esquemática el funcionamiento de un centro de llamadas del estado de la técnica 100. La llamada de un cliente 104 se enruta a través de una red 112 al centro de llamadas 102, donde se traslada a través de una central privada conectada a la red pública (PBX, por sus siglas en inglés) 108 a un teléfono 105 de uno entre una variedad de agentes del centro de llamadas 120 que manejan terminales informáticos 106. La llamada entrante también se desvía a un dispositivo de grabación de llamadas 110, que puede estar situado en el centro de llamadas o en un proveedor de servicios de telecomunicaciones de la red 112.

[0007] Un enfoque conocido para mejorar la seguridad de la interacción con los clientes en un centro de llamadas consiste en introducir la posibilidad de pausar la grabación, que puede aplicarse mientras se le

proporciona la información confidencial al agente. La pausa puede activarse manual o automáticamente, por ejemplo, cuando el agente hace clic en el campo CV2 del monitor para introducir el número de seguridad de la tarjeta de crédito de la persona que llama. Alternativamente, se puede saltar al agente al enrutar la llamada a una aplicación de respuesta de voz interactiva (IVR, por sus siglas en inglés) [no mostrada en la figura 1] cuando se solicita la información confidencial, lo que garantiza que esta parte de la llamada no se graba. No obstante, en este modo, el agente y la persona que llama están desconectados y no pueden hablar libremente durante la transacción de la tarjeta. Otro método alternativo, apagar la grabación, no siempre es práctico, puesto que la mayoría de las organizaciones que llevan a cabo transacciones con tarjetas de crédito necesitan grabar las llamadas para la formación del personal, la investigación de las reclamaciones de los clientes y, en algunas circunstancias, cumplir con la regulación del sector o la normativa jurídica, tal como las que establece la Financial Services Authority (FSA, por sus siglas en inglés).

[0008] Otro enfoque conocido consiste en que las personas que llamen utilicen señalización de multifrecuencia de doble tono (DTMF, por sus siglas en inglés). Los tonos DTMF suelen producirse al presionar las teclas de un teléfono estándar y se utilizan para la "marcación mediante contacto". Además de su utilización para la marcación, los tonos DTMF pueden transmitir diversos caracteres alfanuméricos claramente a través de un canal de audio de un teléfono durante una llamada de teléfono. La DTMF presenta la ventaja de seguridad de que es poco factible que un humano determine el equivalente alfanumérico del tono DTMF simplemente al escuchar el tono DTMF. Asimismo, permite que la llamada continúe con normalidad mientras la persona que llama introduce la información de su tarjeta de crédito mediante la utilización del teclado numérico de su teléfono. No obstante, los tonos DTMF son representativos de la información confidencial y, por lo tanto, no pueden grabarse si se debe cumplir con las DSS. Para abordar este asunto, se conoce la introducción de un procesador de llamadas 116 en el centro de llamadas 102 que bloquea los tonos DTMF.

[0009] Por ejemplo, en la solicitud de patente internacional WO 2009/136163 (Semafone Limited) se describe un procesador de llamadas telefónicas que puede cambiarse entre dos modos: "normal" y "seguro". El el modo normal, tanto los componentes de voz y de DTMF pueden pasar a la PBX. Esto es importante para el funcionamiento de los centros de llamadas, puesto que los tonos DTMF se utilizan frecuentemente para permitir que los clientes operen y naveguen a través de las selecciones de menú IVR, por ejemplo. En el modo seguro, el componente de voz de la llamada se le puede transmitir al agente mientras se bloquea o se oculta el componente de DTMF. Esto significa que ni el agente ni la grabación de llamdas "escuchan" los datos DTMF.

[0010] El proceso de cambiar entre un modo "normal" y "seguro", sin embargo, puede exigir una interacción compleja entre un sistema telefónico de un centro de llamadas, sus procesos de pago mediante tarjeta de crédito y los ordenadores de mesa de los agentes. Por lo tanto, se necesitan procedimientos y aparatos mejorados que no dependan de la aplicación de diversos estados operativos en diferentes momentos durante una llamada.

Sumario de la invención

[0011] En un aspecto de la invención, se proporciona un procedimiento de procesamiento de señales de una comunicación telefónica, transmitiendo las señales información confidencial y no confidencial, implementándose el procedimiento mediante un procesador de llamadas y comprendiendo: almacenar en búfer las señales, monitorizar las señales para detectar, en las señales, uno o más casos de una o más características predeterminadas que representan la información confidencial transmitida por las señales; modificar las señales almacenadas en búfer mediante la eliminación de las características predeterminadas identificadas de las señales almacenadas en búfer; generar las señales modificadas para la grabación; y determinar una representación alfanumérica correspondiente a cada caso identificado de las características predeterminadas, y generar datos indicativos de dicha representación alfanumérica para su uso por una aplicación de *software*; donde la modificación de las señales almacenadas en búfer comprende la eliminación de al menos una parte de las señales almacenadas en búfer previas a un punto de detección de cada caso identificado de las características predeterminadas.

[0012] Varios ejemplos de características predeterminadas incluyen, aunque sin carácter limitativo, patrones de onda, tales como patrones de tono de multifrecuencia de doble tono y patrones de voz, así como configuraciones de bits, tales como identificadores de paquetes de datos, por ejemplo, de paquetes de VoIP.

[0013] De esta manera, los datos que representan la información confidencial pueden extraerse de forma automática sin la intervención del agente y generarse para una aplicación de *software* informático. Los datos pueden formatearse a un formato adecuado para la aplicación de *software.* Algunos ejemplos de representación alfanumérica incluyen, pero sin carácter limitativo, frases, palabras, letras y números (por separado o juntos).

[0014] El procedimiento también puede comprender la grabación de dichas señales modificadas en el procesador de llamadas implementando dicha monitorización y dicha modificación.

[0015] La generación de las señales modificadas para la grabación puede comprender la generación de las señales modificadas para un dispositivo de grabación de llamadas.

[0016] El procedimiento también puede comprender la generación de una señal de dispositivo de entrada emulada para dicha representación alfanumérica, y donde la generación de datos comprende la generación de dicha señal de dispositivo de entrada emulada.

[0017] El procedimiento también puede comprender evitar que se muestre dicha representación alfanumérica a través de la aplicación de *software*.

[0018] El procedimiento también puede comprender determinar un dispositivo informático de destino de entre una pluralidad de dispositivos informáticos, comprendiendo la generación la transmisión de los datos a dicho dispositivo informático de destino.

[0019] La aplicación de *software* puede alojarse en un dispositivo informático en una ubicación remota del procesador de llamadas, comprendiendo el procedimiento, además, el cifrado de los datos.

[0020] El procedimiento también puede comprender el procesamiento de las señales para proporcionar una primera versión de las señales que se debe grabar y una segunda versión de las señales, donde dicha monitorización, modificación y generación se aplican a la primera versión de las señales.

[0021] La segunda versión de las señales puede generarse como audio.

[0022] Al menos dicha monitorización y dicha modificación puede aplicarse a dicha segunda versión de las señales, comprendiendo el procedimiento también la generación de la segunda versión modificada de las señales.

[0023] La información puede extraerse de la segunda versión de las señales.

[0024] El procedimiento también puede comprender monitorizar la segunda versión de las señales para detectar, en la segunda versión de las señales, uno o más casos de una o más características predeterminadas que representan la información confidencial transmitida por las señales; determinar una representación alfanumérica correspondiente a cada caso identificado de las características predeterminadas; y generar datos indicativos de la representación alfanumérica para su uso por una aplicación de *software*.

[0025] La monitorización, modificación y generación de la primera versión de las señales puede llevarse a cabo en una primera ubicación y donde la monitorización de la segunda versión de las señales, la determinación de la representación alfanumérica y la generación de los datos indicativos de la representación alfanumérica se llevan a cabo en una segunda ubicación.

[0026] El procedimiento también puede comprender la modificación de la segunda versión de las señales mediante la eliminación de las características predeterminadas identificadas de la segunda versión de las señales y la generación de la segunda versión de las señales para su escucha.

[0027] En otro aspecto de la invención, se proporciona un procesador de llamadas para procesar señales de una comunicación telefónica, transmitiendo las señales información confidencial y no confidencial, estando configurado el procesador de llamadas para implementar los procedimientos descritos en la presente memoria, que comprenden: medios configurados para almacenar en búfer las señales, medios configurados para monitorizar las señales almacenadas en búfer para detectar, en las señales almacenadas en búfer, uno o más casos de una o más características predeterminadas que representan la información confidencial transmitida por las señales; medios configurados para modificar las señales almacenadas en búfer mediante la eliminación de las características predeterminadas identificadas de las señales almacenadas en búfer; medios configurados para generar las señales modificadas para la grabación; medios configurados para determinar una representación alfanumérica correspondiente a cada caso identificado de las características predeterminadas, y generar datos indicativos de dicha representación alfanumérica para su uso por una aplicación de *software*; y donde los medios configurados para modificar las señales almacenadas en búfer comprenden la eliminación de al menos una parte de las señales almacenadas en búfer previas a un punto de detección de cada caso identificado de las características predeterminadas.

[0028] También se describe un procedimiento de procesamiento de señales de una comunicación telefónica, transmitiendo las señales información confidencial y no confidencial, comprendiendo el procedimiento almacenar en búfer las señales; monitorizar las señales para detectar, en las señales, uno o más casos de una o más características predeterminadas que representan la información confidencial transmitida por las señales; y modificar las señales almacenadas en búfer mediante la eliminación de las características predeterminadas identificadas.

[0029] Tal y como se ha descrito anteriormente, el almacenamiento en búfer de las señales permite que la modificación compense el periodo de tiempo corto asociado a la detección de las características predeterminadas. De esta manera, el procedimiento puede implementarse como un procedimiento autónomo; por ejemplo, en dispositivos de grabación ya existentes, tal como un servidor de grabación de llamadas. Por lo tanto, la modificación de las señales almacenadas en búfer puede comprender la eliminación de al menos una parte de

las señales almacenadas en búfer previas a un punto de detección de cada caso identificado de las características predeterminadas.

[0030] El procedimiento también puede comprender la grabación de las señales modificadas.

[0031] También se describe un procesador de llamadas para el procesamiento de señales de una comunicación telefónica, transmitiendo las señales información confidencial y no confidencial, comprendiendo el procesador de llamadas medios configurados para almacenar en búfer las señales; medios configurados para monitorizar las señales para detectar, en las señales, uno o más casos de una o más características predeterminadas que representan la información confidencial transmitida por las señales; y medios configurados para modificar las señales almacenadas en búfer mediante la eliminación de las características predeterminadas identificadas.

[0032] Los medios configurados para la modificación de las señales almacenadas en búfer pueden configurarse para modificar las señales almacenadas en búfer mediante la eliminación de al menos una parte de las señales almacenadas en búfer previas a un punto de detección de cada caso identificado de las características predeterminadas.

[0033] El procesador de llamadas puede comprender también medios configurados para la grabación de las señales modificadas.

[0034] También se describe un procedimiento para el procesamiento de señales de una comunicación telefónica, transmitiendo las señales información confidencial y no confidencial, comprendiendo el procedimiento el procesamiento de las señales para proporcionar una primera versión de las señales que se debe grabar y una segunda versión de las señales de la cual debe extraerse información; en una primera ubicación: monitorizar dicha primera versión de las señales para detectar, en la primera versión de las señales, uno o más casos de una o más características predeterminadas que representan la información confidencial transmitida por las señales; modificar dicha primera versión de las señales mediante la eliminación de las características predeterminadas identificadas de dicha primera versión de las señales; y generar la primera versión modificada de las señales para la grabación; y, en una o más segunda(s) ubicación(es): monitorizar dicha segunda versión de las señales para detectar, en la segunda versión de las señales, uno o más casos de una o más características predeterminadas que representan la información confidencial transmitida por las señales; determinar una representación alfanumérica correspondiente a cada caso identificado de las características predeterminadas; y generar datos indicativos de dicha representación alfanumérica para su uso por una aplicación de *software*.

[0035] Por lo tanto, este procedimiento facilita la grabación en una primera ubicación y la extracción de datos en una segunda ubicación; por ejemplo, en un servidor central y una estación de agentes de un centro de llamadas, respectivamente.

[0036] El procedimiento también puede comprender, en la primera ubicación, el almacenamiento en búfer de la primera versión de las señales, y donde la modificación de la primera versión de las señales comprende la eliminación de al menos una parte de la primera versión de las señales almacenada en búfer previas a un punto de detección de cada caso identificado de las características predeterminadas.

[0037] El procedimiento también puede comprender la grabación de la primera versión de las señales en la primera ubicación.

[0038] El procedimiento también puede comprender, en la una o más segunda(s) ubicación(es), evitar que se muestre dicha representación alfanumérica a través de la aplicación de *software.*

[0039] El procedimiento también puede comprender, en la una o más segunda(s) ubicación(es), la modificación de la segunda versión de las señales mediante la eliminación de las características predeterminadas identificadas de la segunda versión de las señales y la generación de la segunda versión de las señales para su escucha.

[0040] El procedimiento también puede comprender, en la una o más segunda(s) ubicación(es), la generación de una señal de dispositivo de entrada emulada para dicha representación alfanumérica, y donde la generación de datos comprende la generación de la señal de dispositivo de entrada emulada.

[0041] También se describe un procesador de llamadas para el procesamiento de señales de una comunicación telefónica, transmitiendo las señales información confidencial y no confidencial, comprendiendo el procesador de llamadas unos primeros medios en una primera ubicación, comprendiendo; medios de recepción configurados para recibir una primera versión de las señales; medios de monitorización configurados para monitorizar dicha primera versión de las señales para detectar, en la primera versión de las señales, uno o más casos de una o más características predeterminadas que representan la información confidencial transmitida por las señales; medios de modificación de dicha primera versión de las señales mediante la eliminación de las características predeterminadas identificadas de dicha primera versión de las señales; y medios de generación para generar la primera versión modificada de las señales para la grabación; y unos segundos medios en una o más segunda(s)

ubicación(es), comprendiendo: medios de recepción configurados para recibir una segunda versión de las señales; medios de monitorización configurados para monitorizar dicha segunda versión de las señales para detectar, en la segunda versión de las señales, uno o más casos de una o más características predeterminadas que representan la información confidencial transmitida por las señales; medios de determinación configurados para determinar una representación alfanumérica correspondiente a cada caso identificado de las características predeterminadas; y medios de generación configurados para generar datos indicativos de dicha representación alfanumérica para su uso por una aplicación de *software*.

[0042] Los primeros medios también pueden comprender medios de almacenamiento en búfer configurados para el almacenamiento en búfer de la primera versión de las señales, y donde los medios de modificación están configurados para eliminar al menos una parte de la primera versión de las señales almacenada en búfer previas a un punto de detección de cada caso identificado de las características predeterminadas.

[0043] Los primeros medios pueden comprender también medios configurados para la grabación de la primera versión de las señales.

[0044] Los segundos medios también pueden comprender medios de prevención para evitar que se muestre dicha representación alfanumérica a través de la aplicación de *software.*

[0045] Los segundos medios también pueden comprender medios de modificación configurados para modificar la segunda versión de las señales mediante la eliminación de las características predeterminadas identificadas de la segunda versión de las señales y medios de generación configurados para generar la segunda versión de las señales para su escucha.

[0046] Los segundos medios también pueden comprender la generación de medios configurados para generar una señal de dispositivo de entrada emulada para la representación alfanumérica, y donde los medios de generación configurados para generar datos están configurados para generar la señal de dispositivo de entrada emulada.

[0047] También se describe un procedimiento de procesamiento de señales de una comunicación telefónica, transmitiendo las señales información confidencial y no confidencial, comprendiendo el procedimiento recibir las señales; monitorizar las señales recibidas para detectar, en dichas señales, uno o más casos de una o más características predeterminadas que representan la información confidencial; determinar una representación alfanumérica correspondiente a cada caso identificado de las características predeterminadas; generar una señal de dispositivo de entrada emulada para cada representación alfanumérica; y generar dicha señal de dispositivo de entrada emulada para su uso por una aplicación de *software*, comprendiendo la generación la realización de una comprobación de validación para garantizar que la señal de dispositivo de entrada emulada se introduce en un campo de entrada de datos validados de una aplicación de *software* validada.

[0048] La emulación de una señal de dispositivo de entrada significa que los datos extraídos pueden transmitirse a la aplicación de *software* en un formato que sea fácilmente reconocible. Al realizar una comprobación de validación para determinar que la señal de dispositivo de entrada emulada se introduce en la ubicación de entrada de datos esperada en la aplicación de *software* esperada, se puede rechazar la entrada de la señal de dispositivo de entrada emulada en ubicaciones de entrada de datos no esperadas. Esto puede incluir determinar el "título de ventana" actual de una aplicación de *software*, determinar el título de campo de entrada de datos actual, la inspección de unas propiedades de campo de entrada de datos, la determinación de cualquier otra propiedad específica de aplicación o la determinación de cualquier otra información en pantalla. Los procedimientos para llevar a cabo la comprobación de validación podrían incluir comunicación API, inspección del contenido html de una página web o de modelo de objeto de documento o cualquier comunicación similar o relacionada requerida para interactuar con la aplicación de *software*. De esta manera, las comprobaciones de validación pueden, por ejemplo, determinar si la propiedad de "visualizar como asteriscos" (*) de un campo de visualización en pantalla se ha habilitado o si el número de caracteres que puede introducirse en el campo de entrada de datos corresponde a la longitud de la representación alfanumérica. De este modo, puede evitarse que los agentes, por ejemplo, utilicen la señal de dispositivo de entrada emulada para introducir información de tarjeta confidencial en una ubicación separada de la que puede robarse.

[0049] El procedimiento también puede comprender la modificación de las señales recibidas mediante la eliminación de las características predeterminadas identificadas de dichas señales recibidas y la generación de las señales modificadas para su escucha.

[0050] El procedimiento también puede comprender evitar que se muestre la representación alfanumérica a través de la aplicación de *software.*

[0051] La generación de la señal de dispositivo de entrada emulada puede comprender la introducción de la señal de dispositivo de entrada emulada como datos en un campo de entrada de datos validados de la aplicación de *software*.

[0052] Se observará que la prevención de una visualización de la representación alfanumérica y la introducción de la señal de dispositivo de entrada emulada en un campo de entrada de datos validados son solamente dos de muchas interacciones o comandos que pueden implementarse con el fin de controlar el uso o la aplicación de los datos extraídos.

[0053] También se describe un procesador de llamadas para el procesamiento de señales de una comunicación telefónica, transmitiendo las señales información confidencial y no confidencial, comprendiendo el procesador de llamadas medios configurados para recibir las señales; medios configurados para monitorizar dichas señales para detectar, en dichas señales, uno o más casos de una o más características predeterminadas que representan la información confidencial; medios configurados para determinar una representación alfanumérica correspondiente a cada caso identificado de las características predeterminadas; medios configurados para generar una señal de dispositivo de entrada emulada para cada representación alfanumérica; medios configurados para generar dicha señal de dispositivo de entrada emulada para su uso por una aplicación de *software*; y medios configurados para llevar a cabo una comprobación de validación para garantizar que la señal de dispositivo de entrada emulada se introduce en un campo de entrada de datos validados de una aplicación de *software* validada.

[0054] Dicho procesador de llamadas puede introducirse fácilmente en infraestructuras existentes, por ejemplo, bien como *software* o *hardware* en un terminal informático. Por lo tanto, el procesador de llamadas puede generar señales a un terminal informático por medio de un USB u otra interfaz adecuada.

[0055] El procesador de llamadas también puede comprender medios configurados para la modificación de dichas señales recibidas mediante la eliminación de las características predeterminadas identificadas de dichas señales recibidas y medios configurados para la generación de las señales recibidas para su escucha.

[0056] El procesador de llamadas también puede comprender medios de prevención configurados para evitar que se muestre dicha representación alfanumérica a través de la aplicación de *software.*

[0057] También se describe un procedimiento de procesamiento de señales de una comunicación telefónica mediante un procesador de llamadas, transmitiendo las señales información confidencial y no confidencial, comprendiendo el procedimiento la recepción de las señales; la monitorización de las señales recibidas para detectar, en las señales, uno o más casos de una o más características predeterminadas que representan la información confidencial transmitida por las señales; la determinación de una representación alfanumérica correspondiente a cada caso identificado de las características predeterminadas; la generación de datos indicativos de la representación alfanumérica; la determinación de un dispositivo informático de destino de entre una pluralidad de dispositivos informáticos; y la generación de los datos para su uso por una aplicación de *software* ejecutable en el dispositivo informático de destino.

[0058] El procedimiento también puede comprender la modificación de las señales recibidas mediante la eliminación de las características predeterminadas identificadas de las señales recibidas y la generación de las señales modificadas para su grabación.

[0059] Los datos pueden comprender una señal de dispositivo de entrada emulada generada para cada representación alfanumérica.

[0060] El procedimiento también puede comprender la introducción de la señal de dispositivo de entrada emulada como datos en un campo de entrada de datos validados de la aplicación de *software*.

[0061] El procedimiento también puede comprender evitar que se muestre la representación alfanumérica a través de la aplicación de *software.*

[0062] El dispositivo informático de destino puede determinarse a partir de una dirección IP contenida en las señales.

[0063] También se describe un procesador de llamadas para el procesamiento de señales de una comunicación telefónica, transmitiendo las señales información confidencial y no confidencial, comprendiendo el procesador de llamadas medios configurados para recibir las señales; medios configurados para monitorizar las señales para detectar, en las señales, uno o más casos de una o más características predeterminadas que representan la información confidencial; medios configurados para determinar una representación alfanumérica correspondiente a cada caso identificado de las características predeterminadas; medios configurados para generar datos indicativos de la representación alfanumérica; medios configurados para determinar un dispositivo informático de destino de entre una pluralidad de dispositivos informáticos; y medios configurados para generar los datos para su uso por una aplicación de *software* que puede ejecutarse en el dispositivo informático de destino.

[0064] El procesador de llamadas también puede comprender medios configurados para modificar las señales recibidas mediante la eliminación de las características predeterminadas identificadas de las señales recibidas y medios configurados para generar las señales modificadas para su grabación.

[0065] Los datos pueden comprender una señal de dispositivo de entrada emulada generada para cada representación alfanumérica.

[0066] El procesador de llamadas también puede comprender medios configurados para la introducción de la señal de dispositivo de entrada emulada como datos en un campo de entrada de datos validados de la aplicación de *software*.

[0067] El procesador de llamadas también puede comprender medios configurados para evitar que se muestre la representación alfanumérica a través de la aplicación de *software.*

[0068] Los medios configurados para determinar un dispositivo informático de destino pueden configurarse para determinar el dispositivo informático de destino a partir de una dirección IP contenida en las señales.

[0069] También se describe un procedimiento de procesamiento de señales de una comunicación telefónica mediante un procesador de llamadas en una primera ubicación, transmitiendo las señales información confidencial y no confidencial, comprendiendo el procedimiento la recepción de las señales; la monitorización de las señales recibidas para detectar, en las señales, uno o más casos de una o más características predeterminadas que representan la información confidencial transmitida por las señales; la generación de datos indicativos de la representación alfanumérica; el cifrado de los datos; y la generación de los datos cifrados para su transmisión a través de una red a un dispositivo informático en una segunda ubicación.

[0070] El procedimiento también puede comprender la modificación de las señales recibidas mediante la eliminación de las características predeterminadas identificadas de las señales recibidas y la generación de las señales modificadas para su grabación.

[0071] Los datos cifrados pueden transmitirse a través de un dispositivo informático en la primera ubicación.

[0072] El procedimiento también puede comprender la recepción de un mensaje del dispositivo informático en la segunda ubicación que indique si los datos cifrados han sido procesados con éxito por la aplicación de *software*.

[0073] También se describe un procesador de llamadas para el procesamiento de señales de una comunicación telefónica, transmitiendo las señales información confidencial y no confidencial, estando el procesador de llamadas situado en una primera ubicación, comprendiendo el procesador de llamadas medios configurados para la recepción de las señales; medios configurados para la monitorización de las señales para detectar, en las señales, uno o más casos de una o más características predeterminadas que representan la información confidencial; medios configurados para la generación de datos indicativos de la representación alfanumérica; medios configurados para el cifrado de los datos; y medios configurados para la generación de los datos cifrados para su transmisión a través de una red a un dispositivo informático en una segunda ubicación.

[0074] El procesador de llamadas también puede comprender medios configurados para la modificación de dichas señales recibidas mediante la eliminación de las características predeterminadas identificadas de dichas señales recibidas y medios configurados para la generación de las señales modificadas para su grabación.

[0075] La transmisión puede llevarse a cabo a través de un dispositivo informático en la primera ubicación.

[0076] El procesador de llamadas también puede comprender medios configurados para la recepción de un mensaje del dispositivo informático en la segunda ubicación que indique si los datos cifrados han sido procesados con éxito por la aplicación de *software*.

[0077] También se describe un procedimiento para llevar a cabo una transacción, comprendiendo el procedimiento el establecimiento de una comunicación telefónica entre un cliente y un agente de un centros de llamadas, comprendiendo la comunicación telefónica señales que transmiten información confidencial y no confidencial del cliente; el procesamiento de las señales para proporcionar una primera versión de las señales que se debe grabar y una segunda versión de las señales que se debe generar como audio para el agente del centros de llamadas; la monitorización, por parte de un procesador de llamadas, de al menos la primera versión de las señales para detectar, en la al menos la primera versión de las señales, uno o más casos de una o más características predeterminadas que representan la información confidencial del cliente transmitida por las señales; la modificación, por parte del procesador de llamadas, de la al menos la primera versión de las señales mediante la eliminación de las características predeterminadas identificadas de la al menos la primera versión de las señales; y el procesamiento de la transacción por una aplicación de *software* que se ejecuta en un dispositivo informático, mediante la utlización de la información confidencial transmitida en las señales.

[0078] El procedimiento también puede comprender la determinación, por parte del procesador de llamadas, de una representación alfanumérica correspondiente a cada caso identificado de las características predeterminadas; la generación, por parte del procesador de llamadas, de datos indicativos de la representación alfanumérica; y la generación, por parte del procesador de llamadas, de los datos para su uso por la aplicación de *software* para procesar la transacción.

[0079] Los datos pueden comprender una señal de dispositivo de entrada emulada para cada representación alfanumérica.

[0080] El procedimiento también puede comprender la identificación, por parte del procesador de llamadas, del dispositivo informático de entre una pluralidad de dispositivos informáticos.

[0081] La determinación puede basarse en una dirección IP contenida en las señales.

[0082] El procedimiento también puede comprender el cifrado, por parte del procesador de llamadas, de los datos; y donde la generación comprende la generación de los datos cifrados para su transmisión a través de una red a un dispositivo informático en una ubicación remota del centro de llamadas.

[0083] La presente invención y cualquiera de sus modos de realización puede implementarse por *software* en un ordenador de propósito general o en una combinación de *software* y *hardware*. Por lo tanto, cualquiera de los "medios" definidos anteriormente se puede implementar como módulo de códigos en cualquier combinación en un ordenador.

[0084] También se describe un producto de programa informático que puede realizarse en un medio de almacenamiento pasivo y que configura un ordenador para llevar a cabo un procedimiento definido en cualquiera de los párrafos anteriores. En el presente documento, el término ordenador puede abarcar un ordenador con *hardware* especializado.

[0085] Algunos aspectos de la invención pueden proporcionarse en forma de producto de programa informático en un medio portador, que puede realizarse en un medio de almacenamiento pasivo, tal como un medio óptico o magnético, o un medio electrónico, tal como un dispositivo de almacenamiento masivo (p. ej., una memoria FLASH), o en un dispositivo de *hardware* implementado para conseguir la ejecución de instrucciones de acuerdo con la invención, tales como ASIC, un FPGA, un DSP, un microcontrolador RISC o similares. Alternativamente, el medio portador puede comprender una señal portadora del código de programa informático, tal como una señal óptica, una señal eléctrica, una señal electromagnética, una señal acústica o una señal magnética. Por ejemplo, la señal puede comprender una señal TCP/IP portadora del código a través de Internet.

[0086] Tal y como se utiliza en el presente documento, el término "comunicación telefónica", por lo general, se refiere a la transmisión de información a través de un canal de comunicación, que incluye canales de comunicaciones alámbricas e inalámbricas (o ambos) y abarca comunicaciones basadas en paquetes, tales como VoIP.

[0087] Tal y como se utiliza en el presente documento, el término "versión" es, por lo general, utilizado para describir un caso particular de las señales que transmiten considerablemente el mismo contenido de información que otros casos de las señales.

[0088] Los procedimientos y aparatos pueden utilizarse fácilmente en operaciones de centro de llamadas; por ejemplo, en una estación de agentes que comprende una organización de comunicación telefónica de audio de agentes (p. ej., teléfono y/o auriculares/auriculares con micrófono de teléfono) y un sistema informático de agentes, o en un servidor de grabación de llamadas, o una combinación de los mismos. Sin embargo, se observará que la descripción se puede aplicar a otras aplicaciones que llevan a cabo grabación y extracción de datos.

Breve descripción de los modos de realización

[0089] Otros aspectos, características y ventajas de la invención resultarán evidentes para el lector de la siguiente descripción de modos de realización específicos de la invención, expuestos únicamente a modo de ejemplo, con referencia a los dibujos adjuntos, en los que:

En la figura 1, se muestra de forma esquemática el funcionamiento de un centro de llamadas conocido;

En la figura 2, se muestra de forma esquemática el funcionamiento de un centro de llamadas que emplea procesadores de llamadas de acuerdo con modos de realización de la invención;

En la figura 3, se muestra de forma esquemática un procesador de llamadas de acuerdo con un modo de realización de la invención en el que se implementa la modificación de señales y la extracción de datos como *software* en un terminal informático;

En la figura 4, se muestra de forma esquemática un diagrama de flujo de un proceso de procesamiento de señales de datos de acuerdo con un modo de realización de la invención;

En la figura 5, se muestra de forma esquemática la detección y la modificación de señales de acuerdo con un modo de realización de la invención;

En la figura 6, se muestra de forma esquemática un procesador de llamadas de acuerdo con un modo de realización de la invención en el que se implementa la extracción de datos como *software*;

En la figura 7, se muestra de forma esquemática un procesador de llamadas de acuerdo con un modo de realización de la invención en el que se implementa la extracción de datos como *hardware*;

En la figura 8, se muestra de forma esquemática un procesador de llamadas de acuerdo con un modo de realización de la invención en el que se implementa la extracción de datos como *hardware*;

En la figura 9, se muestra de forma esquemática un procesador de llamadas de acuerdo con un modo de realización de la invención en el que se implementa la modificación de señales y la extracción de datos como *hardware*;

En la figura 10, se muestra de forma esquemática un procesador de llamadas de acuerdo con un modo de realización de la invención en el que se implementa la extracción de datos como *hardware*;

En la figura 11, se muestra de forma esquemática un procesador de llamadas de acuerdo con un modo de realización de la invención en el que se implementa la extracción de datos en un terminal informático;

En la figura 12, se muestra de forma esquemática un procesador de llamadas de acuerdo con un modo de realización de la invención en el que la modificación de señales se lleva a cabo en un dispositivo de grabación de llamadas o cerca de un dispositivo de grabación de llamadas.

En la figura 13, se muestra de forma esquemática un procesador de llamadas de acuerdo con un modo de realización de la invención en el que se implementa la extracción de datos como *hardware*.

En la figura 14, se muestra de forma esquemática un procesador de llamadas de acuerdo con un modo de realización de la invención en el que la modificación de señales se lleva a cabo en un dispositivo de grabación de llamadas o cerca de un dispositivo de grabación de llamadas y en el que la extracción de datos se lleva a cabo en la misma ubicación.

Descripción detallada de los modos de realización

[0090] En la figura 2, se muestra de forma esquemática el funcionamiento de un centro de llamadas de ejemplo 200 que implementa procedimientos y procesadores de llamadas de acuerdo con diversos modos de realización de la invención.

[0091] Una llamada entrante de un cliente 204 se enruta a través de una red 212 al centro de llamadas 202, donde se traslada a través de una central privada conectada a la red pública (PBX) 208, o similar, a un teléfono 205 de uno de entre una variedad de agentes 220 que manejan terminales informáticos 206. Cada teléfono 205 está acoplado al terminal informático correspondiente 206 mediante un adaptador 207, que también está conectado a unos auriculares o unos auriculares con micrófono (no se muestran) del agente 220.

[0092] En un modo de realización, que se describe a continuación con referencia a la figura 3, la modificación de señales, la extracción de datos y el enmascaramiento visual se llevan a cabo localmente en los terminales informáticos 206 por parte de procesadores de llamadas 216a, implementados como *software* en los terminales informáticos 206. En ese caso, el dispositivo de grabación de llamadas 210 no ha de utilizarse. En su lugar, las llamadas pueden grabarse temporalmente en los procesadores de llamadas 216a antes de enviarse al almacenamiento de grabación de llamadas 211 a través de una red local 214 o una red externa, en función de la ubicación del dispositivo de almacenamiento.

[0093] En otros modos de realización, que se describen a continuación con referencia a la figura 6, los procesadores de llamadas 216a llevan a cabo la extracción de datos y el enmascaramiento visual, pero no llevan a cabo la grabación de llamadas. El enmascaramiento de llamadas al agente puede implementarse o no. En esos casos, pueden retenerse los dispositivos de grabación de llamadas ya existentes 210 (se observará que el dispositivo de grabación de llamadas puede “desviarse” antes o después de la PBX; por ejemplo, de cada una de las extensiones por debajo de la PBX. Sin embargo, en aras de la claridad, solamente se muestra una implementación). En los casos en los que los dispositivos de grabación de llamadas no tengan competencias de enmascaramiento de llamadas, el procesador de llamadas 216b o el procesador de llamadas 216c pueden implementarse para llevar a cabo la modificación de las señales; por ejemplo, bien en el centro de llamadas o en su proveedor de servicios de telecomunicaciones. Los procesadores de llamadas 216b, 216c pueden operar independientemente de los procesadores de llamadas 216a y se describen a continuación con referencia a la figura 12. En algunos modos de realización, el procesador de llamadas puede implementarse en otras ubicaciones, tal y como se muestra en las figuras 6 a 14 y tal y como se describe con referencia a dichas figuras.

[0094] En algunos modos de realización, los procesadores de llamadas 216b, 216c son independientes y funcionan sin la presencia del procesador de llamadas 216a. Como tales, los procesadores de llamadas 216b y 216c pueden, de forma alternativa, introducirse en centros de llamadas que cuenten con procedimientos de

extracción de datos existentes (es decir, sin la necesidad de implementar procesadores de llamadas 216a). Si bien en la figura 2, se muestran los procesadores de llamadas 216b, 216c como entidades distintas de los dispositivos de grabación de llamadas 210, en algunos modos de realización los procesadores de llamadas pueden integrarse en los dispositivos de grabación de llamadas; por ejemplo, como módulos de *software*.

[0095] En la figura 3, se muestra de forma esquemática un modo de realización de un procesador de llamadas 316 implementado como *software* en un terminal informático 306 de un agente de un centro de llamadas 320. El procesador de llamadas 316 está configurado para enmascarar los tonos DTMF de los datos grabados. Los tonos DTMF de los auriculares/auriculares con micrófono 309 del agente 320 no se enmascaran ni se graban.

[0096] Más específicamente, una llamada entrante de una persona que llama 304 se traslada al teléfono 305 del agente 320 a través de la PBX 308. Un adaptador 307 genera las señales de datos que representan el audio a los auriculares/auriculares con micrófono 309 del agente 320, así como el módulo de conversión de audio 326 del procesador de llamadas 316. Las señales de datos pueden comprender señales de audio análogas mono o estéreo, señales digitales mono o estéreo, señales de datos de voz sobre IP (VoIP) mono o estéreo, datos de audio por paquetes mono o estéreo, etc.

[0097] El módulo de conversión de audio 326 está configurado para convertir las diversas señales de datos en audio digital convencional para su análisis. Los procedimientos utilizados por el módulo de conversión de audio 326 para convertir las señales de datos incluyen los que resultan conocidos para los expertos en la materia del procesamiento de audio; por ejemplo, la descompresión de códecs de audio convencionales (p. ej., G.711 μ-Law, G.711 a-Law, G.729 y GSM), suprimiendo el encabezado y otra información que no sea de audio de los datos en paquetes, etc.

[0098] El audio digital se genera para el búfer 328 y para el módulo de monitorización de señal 330.

[0099] El módulo de monitorización de señal 330 está configurado para detectar información característica (patrones predeterminados) en el audio digital; por ejemplo, tonos de audio concretos, como tonos DTMF. El módulo de monitorización de señal 330 también está configurado para determinar información relacionada con la información característica, como un número o letra representados por un tono DTMF, un momento en el que se detecta el patrón en la señal de audio digital, la duración del tono (patrón), el número de tonos DTMF detectados, etc.

[0100] Los métodos mediante los cuales el módulo de monitorización de señal 330 determina si se ha encontrado un patrón predeterminado en el audio digital incluyen aquellos que resultan conocidos para los expertos en la materia, como las transformaciones rápidas de Fourier (FET, por sus siglas en inglés) y el procesamiento de señal digital, que incluye el análisis de Goertzel. Estos procesos suelen depender de la naturaleza del patrón predeterminado que se esté buscando en el audio digital, y puede ser necesario adoptar medidas correspondientes para asegurar que se utiliza el procesamiento adecuado para cada tipo de patrón predeterminado. Dichos aspectos se pueden definir como ajustes de configuración para el módulo de monitorización de señal 330.

[0101] La información sobre sincronización establecida por el módulo de monitorización de señal 330 se genera para un módulo de modificación de señal 332. Por consiguiente, se puede utilizar información como la posición del patrón detectado en el audio digital mediante el módulo de modificación de señal para determinar cómo o cuándo modificar las señales. En concreto, la señal de control de sincronización puede indicar un momento inicial y un momento final para cada tono, o tiempos iniciales y finales para un conjunto de tonos. De esta manera, las señales de tono DTMF detectadas que se grabarían, de lo contrario, mediante el módulo de grabación 334, se enmascaran mediante el módulo de modificación de señal 332.

[0102] Se observará que la detección de patrones predeterminados tardará normalmente una cantidad de tiempo finita. Por ejemplo, el reconocimiento de los tonos DTMF en el audio digital puede tardar aproximadamente entre 10 - 20 ms. El búfer 328 está configurado para almacenar temporalmente las señales de audio con el fin de permitir al módulo de modificación de señal 332 modificar una parte de la señal que precede al tiempo inicial detectado de cada tono; por ejemplo, mediante el enmascaramiento del audio digital. El módulo de modificación de señal 332 también puede modificar una parte de la señal que va después del tiempo final detectado de cada tono.

[0103] Con referencia a la figura 5, en la que se muestra de forma esquemática la detección y el enmascaramiento de dos tonos DTMF 515a, 515b, el módulo de monitorización de señal 330 detecta en el momento T_1 que el tono DTMF 515a ha empezado y detecta en el momento T_2 que el tono ha finalizado. Una parte del tono DTMF 515a existe antes del tiempo inicial T_1 detectado, como resulta evidente. Por consiguiente, el módulo de modificación de señal 332 puede aplicar una máscara 517a para incluir la parte del tono DTMF 515a que precede al tiempo inicial detectado a partir de la señal de tiempo T_1 (es decir, a partir del momento T_1 - δt_1). Con el fin de garantizar que se enmascara la totalidad del tono DTMF, el módulo de modificación de señal 332 también puede aplicar la máscara 517a a un periodo de tiempo posterior al tiempo final detectado T_2 del tono 515a (es decir, T_2 +δt_2). Los tonos DTMF 515a y 515b pueden tener una duración diferente. De la misma

manera, los valores de δt_1 y δt_2 pueden tener también una duración diferente. En un modo de realización, la modificación de señal (p. ej., enmascaramiento) se lleva a cabo para el audio en su totalidad; por ejemplo, hasta que se hayan introducido los 16 dígitos de una tarjeta de crédito. Si bien en la figura 5, se muestran dos tonos DTMF, el principio general de la modificación de señal, como la información de características de enmascaramiento, puede determinarse fácilmente.

[0104] Por lo tanto, la modificación de la señal aplicada por el módulo de modificación de señal hace que el patrón detectado sea inaccesible a partir de la grabación. En un modo de realización, el módulo de modificación de señal 332 enmascara la señal de audio digital mediante su sustitución por un tono audible; p. ej., a 1-2 kHz. De esta manera, de acuerdo con un aspecto de la invención, ninguna parte de los patrones predeterminados detectados por el módulo de monitorización de señal aparecerá en el audio digital enmascarado enviado para su almacenamiento. Esto garantiza que, por ejemplo, los tonos DTMF introducidos por una persona que llama, o un proceso de control de seguridad realizado por la persona que llama, no pasen a un módulo de grabación 334.

[0105] Con referencia de nuevo a la figura 3, la información establecida por el módulo de monitorización de señal 330 también se genera para el módulo de interfaz de señal 336. El módulo de interfaz de señal 336 puede determinar una representación alfanumérica del patrón DTMF detectado. De esta manera, los tonos DTMF detectados en el audio digital pueden automáticamente comunicarse a una aplicación de un tercero 342 y procesarse sin que el miembro del personal del centro de llamadas 320 tenga que introducir ningún dato en su terminal informático 306, de tal forma que se suprime la posibilidad de que el miembro del personal del centro de llamadas anote la información para un posible robo. Por lo tanto, se conserva el carácter secreto de los datos de seguridad, los números de tarjeta de crédito o cualesquiera otros datos similares de la persona que llama, que no estarán disponibles para una revisión posterior en una llamada grabada hecha a partir del audio digital.

[0106] Asimismo, puesto que el módulo de interfaz de señal 336 puede estar configurado para determinar y comunicar el número de veces que se ha detectado un patrón o varios patrones, es posible confirmar que, por ejemplo, los 16 dígitos de un número de tarjeta de crédito se han recibido correctamente a medida que el cliente teclea los datos de su tarjeta. Si no se ha recibido toda la información de seguridad, la aplicación de un tercero 342 puede hacer que el miembro del personal del centro de llamadas pida a la persona que llama que vuelva a introducir los datos de seguridad. Por lo tanto, las señales comunicadas por el módulo de interfaz de señal 336 pueden confirmar que los datos de seguridad se han introducido correctamente.

[0107] De esta manera, una transacción de tarjeta de crédito de un cliente podría procesarse con una mínima ayuda de un miembro del personal del centro de llamadas o sin ninguna ayuda y sin que el miembro del personal del centro de llamadas tenga que participar en la introducción de datos.

[0108] Las señalas transmitidas por el módulo de interfaz de señal 336 a la aplicación de terceros 342 se pueden comunicar mediante comunicación electrónica, como comunicación ActiveX, comunicación de protocolo de internet, comunicación de interfaz de programación de aplicaciones (API), señales con imitación de pulsaciones de teclas de ordenador, o cualquier otro método electrónico.

[0109] Un módulo de interfaz de entrada de datos 338 está configurado para adaptar la información, el procedimiento de su visualización en la aplicación de un tercero 342 o el funcionamiento de la aplicación de un tercero, de manera que la información se muestre en la aplicación de un tercero en un formato adecuado, o de manera que la aplicación de un tercero funcione de un modo deseado. Cuando la aplicación de un tercero esté ya configurada para mostrar la información en un formato adecuado, o para funcionar de la manera deseada, la salida de datos mediante el módulo de interfaz de entrada de datos 338 puede ser igual que las señales recibidas desde el módulo de interfaz de señal 336. De esta manera, el procesador de entrada de datos no necesita cambiar las señales ni su método de visualización en la aplicación de un tercero, ni el funcionamiento de la aplicación de un tercero, y simplemente puede transmitirlas directamente a la aplicación de un tercero 342.

[0110] En un modo de realización, el módulo de interfaz de entrada de datos 338 está configurado para aplicar comandos o métodos de enmascaramiento visual. De esta manera, la información de tarjeta de crédito segura de un cliente, comunicada a través de tonos DTMF (por ejemplo), no solamente puede eliminarse del audio digital y transmitirse la representación alfanumérica de los tonos DTMF a una aplicación de un tercero, sino que puede controlarse la presentación visual de la aplicación de un tercero para hacer que la representación alfanumérica de la información de DTMF sea invisible o se oculte de forma eficaz. De esta manera, no solamente se elimina del audio digital enviado para su almacenamiento la información segura del cliente, sino que, si alguna aplicación o algún proceso de grabación de pantalla están operativos en el ordenador del miembro del personal del centro de llamadas, las grabaciones de pantalla no contendrán una grabación de la información segura del cliente tampoco. Además, el miembro del personal del centro de llamadas nunca ve los datos de la tarjeta y, por lo tanto, no puede robarlos.

[0111] El módulo de gestión 340 está configurado para determinar la información sobre cada llamada, como la longitud de la llamada y los momentos en que se aplicó la modificación de señal y su duración. También permite que esta información esté asociada al cliente y a la aplicación de un tercero.

[0112] En el modo de realización que se muestra en la figura 3, la grabación de llamadas se lleva a cabo localmente en el terminal informático 306 del agente 320 mediante el módulo de grabación de llamadas 334. Cabe destacar que no hay ninguna "sobreescritura" de los tonos DTMF grabados. En su lugar, los tonos DTMF simplemente no se graban debido al almacenamiento en búfer. Las grabaciones pueden transmitirse a un servidor periódicamente o al final de la llamada. Por lo tanto, las llamadas pueden monitorizarse continuamente y, cuando proceda, modificarse sin tener que pausar o cambiar entre los modos "normal" y "seguro".

[0113] En la figura 4, se muestra un diagrama de flujo de las etapas realizadas por el aparato de la figura 3, en relación con la grabación de las señales modificadas. En la etapa S402, se reciben las señales. Estas pueden convertirse, por ejemplo, en audio digital. En la etapa S404, las señales se almacenan en búfer y, en la etapa S406, las señales se monitorizan para detectar características predeterminadas. Si se detectan (etapa S408, "SÍ"), se modifican las señales. De lo contrario (etapa S408, "NO") el procedimiento vuelve a la etapa S406. En la etapa S410, se aplica la modificación de señal a las señales almacenadas en búfer, antes de grabarse en la etapa S412. En la etapa S414, se extraen los datos.

[0114] Queda entendido que el orden específico de las etapas de los procedimientos expuestos son ejemplos de enfoques ilustrativos y que las etapas pueden reorganizarse u omitirse. Por ejemplo, algunos modos de realización no implementan el almacenamiento en búfer (etapa S404), tal y como se muestra en la figura 4. Asimismo, algunos modos de realización no llevan a cabo la grabación (etapa S412) o la extracción de datos (etapa S414). En otros modos de realización, las etapas pueden llevarse a cabo en diferentes ubicaciones. Por ejemplo, la monitorización y modificación de señal pueden llevarse a cabo en una primera ubicación, y la monitorización de señal y extracción de datos pueden llevarse a cabo en una segunda ubicación. Por lo tanto, algunas etapas o la totalidad de las etapas que se muestran en el diagrama de flujo de la figura 4 pueden llevarse a cabo mediante el aparato descrito a continuación con referencia a las figuras 6 a 12.

[0115] En la figura 6, se muestra de forma esquemática un procesador de llamadas 616 para la extracción de datos de los tonos DTMF de acuerdo con un modo de realización. El procesador de llamadas 616 se implementa como *software* en el terminal informático 606 del agente 620 que se comunica con la persona que llama 604. En este modo de realización en concreto, no se enmascaran los tonos DTMF. Los componentes del procesador de llamadas 616, a saber, el módulo de conversión de audio 626, el módulo de monitorización de señal 630, el módulo de interfaz de señal 636 y el módulo de interfaz de entrada de datos 638 están configurados, por lo general, como módulos correspondientes mostrados en la figura 3 y descritos con referencia a dicha figura 3. Sin embargo, una implementación alternativa, que se muestra en la figura 6, es un adaptador 623 para la conversión de un formato de audio digital propietario en audio. Otras alternativas (que se describirán a continuación) pueden incluir (para VoIP) la utilización de una segunda tarjeta LAN en el terminal informático y una conexión LAN puente al teléfono.

[0116] En la figura 7, se muestra de forma esquemática un procesador de llamadas 716 para la extracción de datos de los tonos DTMF de acuerdo con un modo de realización. El procesador de llamadas comprende un módulo de monitorización de señal 730, un módulo de interfaz de señal 736 y un módulo de interfaz de entrada de datos 738. A diferencia de la figura 6, el procesador de llamadas 716 de la figura 7 se implementa como *hardware* en el ordenador del agente 720, por ejemplo, como un adaptador entre el teléfono 705 y los auriculares/auriculares con micrófono 709. En este modo de realización en concreto, la modificación de señal al agente 720 no se lleva a cabo. En un modo de realización, el módulo de interfaz de entrada de datos 738 genera señales para aplicaciones de terceros 742 residentes en el terminal informático del agente 706 por medio de una interfaz USB que imita pulsaciones de teclas de un ordenador, u otra señalización. En la figura 8, se muestra de forma esquemática un ejemplo específico de una implementación de *hardware* del procesador de llamadas que se muestra en la figura 7. El procesador de llamadas 816 comprende una interfaz de audio 850 para la recepción de las señales de datos, un decodificador DTMF 852 para el reconocimiento de los tonos DTMF y un microcontrolador 854. El microcontrolador 854 comprende un procesador de datos 856 para el procesamiento de las señales de datos y un emulador de teclado USB 858 que imita las pulsaciones de teclas de un ordenador. De esta manera, los tonos DTMF se pueden "insertar" directamente en las aplicaciones de terceros residentes en el terminal informático del agente 806 sin la participación del agente 820.

[0117] En la figura 9, se muestra de forma esquemática un procesador de llamadas 916 para la extracción de datos de los tonos DTMF de acuerdo con un modo de realización. El procesador de llamadas 916 está implementado como *hardware* en el ordenador del agente 920. En este modo de realización en concreto, la modificación de señal para el agente 920 también se lleva a cabo mediante el módulo de modificación de señal 932. Por ejemplo, el módulo de modificación de señal puede poner el volumen a cero o aplicar una señal por encima de una señal existente. La utilización de un búfer (no se muestra) es opcional, puesto que las probabilidades de que el agente reconozca la parte inicial del tono DTMF antes del enmascaramiento son mínimas. Esto se debe a que la interpretación del DTMF es muy difícil para los humanos y, al combinarse con la duración muy corta del tono DTMF que escucha el agente antes del enmascaramiento (alrededor de 10 ms), resulta imposible. La monitorización de señal la lleva a cabo el módulo de monitorización de señal 930. En este modo de realización, la interfaz de entrada de datos 938 genera señales para aplicaciones de terceros 942

residentes en el terminal informático del agente 906 por medio de una interfaz USB que imita pulsaciones de teclas de un ordenador, u otra señalización.

[0118] En la figura 10, se muestra de forma esquemática un modo de realización de un procesador de llamadas 1016 en el que la señal de audio se toma del lado PBX 1008 del teléfono. El procesador de llamadas 1016 ahora comprende un módulo de decodificación de señal 1026 para convertir el audio digital propietario en audio antes de llevar a cabo la monitorización de señal en el módulo de monitorización de señal 1030. Por definición, el módulo de decodificación de señal 1026 puede considerarse comparable al módulo de conversión de audio. También se proporciona una interfaz de señal 1036 y una interfaz de entrada de datos 1038, similares a las descritas anteriormente.

[0119] En la figura 11, se muestra de forma esquemática un modo de realización de un procesador de llamadas 1116 que representa la versión VoIP de los procesadores de llamadas que se han descrito anteriormente, que opera en el *software* en el nivel de escritorio del agente. El módulo de monitorización de señal en este modo de realización comprende un módulo de monitorización de paquetes 1130. También se da a conocer una interfaz de señal 1136 y una interfaz de entrada de datos 1138. Para implementar la VoIP, el terminal informático 1106 incluye dos tarjetas LAN 1160 conectadas por un puente 1162, para la generación de la secuencia de paquetes para el teléfono VoIP 1122 del agente 1120. El terminal informático también incluye aplicaciones de terceros 1142.

[0120] En la figura 12, se muestra de forma esquemática un modo de realización de un procesador de llamadas 1216 configurado para bloquear los tonos DTMF de dispositivos de grabación de llamadas existentes. El procesador de llamadas 1216 comprende un módulo de monitorización de señal 1230, un búfer 1228 y un módulo de modificación de señal 1232. Se puede considerar que el procesador de llamadas 1216 está "siempre activado" y es autónomo, es decir, no necesita alternar entre modos y puede funcionar de manera independiente. En el presente documento, el procesador de llamadas 1216 se muestra como una unidad separada del dispositivo de grabación de llamadas 1210, aunque como se podrá apreciar, el procesador de llamadas 1216 puede ser parte integrante del dispositivo de grabación de llamadas 1210, bien como *hardware* o como *software*.

[0121] En la figura 13, se muestra un modo de realización de forma esquemática de un procesador de llamadas 1316 para la extracción de datos de los tonos DTMF. El procesador de llamadas comprende un módulo de monitorización de señal 1330, un módulo de interfaz de señal 1336 y una interfaz de entrada de datos 1338. A diferencia del modo de realización del procesador de llamadas que se muestra en la figura 7, el procesador de llamadas de la figura 13 genera señales para una o más aplicaciones de terceros 1342 que no residen en el terminal informático del agente 1306 sino en un ordenador situado de forma remota 1370, como un servidor o una estación de trabajo. En un modo de realización, el módulo de interfaz de señal 1336 cifra los datos extraídos de los tonos DTMF (u otras características predeterminadas) con un algoritmo de cifrado seguro y conocido, y el módulo de interfaz de entrada de datos 1338 transmite los datos cifrados a través de una red 1312 (p. ej., una red de área extensa, como Internet) a un ordenador 1370 directamente (es decir, desviándose del terminal informático del agente 1306). A continuación, las aplicaciones de terceros 1342 descifran los datos. En otro modo de realización, el terminal informático del agente 1306 se utiliza como pasarela para la comunicación entre la interfaz de entrada de datos y el ordenador 1370. Sin embargo, no se expondrá ningún dato confidencial como texto sin formato en el terminal informático del agente 1306, aunque sea de forma temporal. De esta manera, aunque una persona o aplicación maliciosas obtengan pleno control del terminal informático del agente 1306, no podrían determinarse los datos confidenciales de un cliente. A continuación, las aplicaciones de terceros 1342 en un ordenador situado de forma remota 1370 pueden descifrar y procesar la información confidencial del cliente, devolviendo un código de autorización, número de transacción o similar al procesador de llamadas 1316 o al terminal informático del agente 1306. La información confidencial del cliente no puede determinarse a partir del código de autorización o de cualquier otra información que se devuelva. De esta manera, un centro de llamadas puede, de forma eficaz, externalizar el procesamiento de los datos confidenciales de los clientes y suprimir algunos o la totalidad de los procesos requeridos para monitorizar los terminales informáticos de los agentes 1306 para detectar una intrusión u otra actividad maliciosa.

[0122] En la figura 14, se muestra de forma esquemática un modo de realización de un procesador de llamadas 1416 configurado para bloquear los tonos DTMF para un dispositivo de grabación de llamadas existente 1410 y, además, extraer datos de los tonos DTMF. Como se observará, este modo de realización es aplicable a otros tipos de características predeterminadas. A diferencia del procesador de llamadas de la figura 12, el procesador de llamadas de la figura 14 también incluye un módulo de interfaz de señal 1436. El módulo de interfaz de señal 1436 puede incluir componentes del procesador de llamadas que se han descrito con referencia a las figuras 7 y 8. En un modo de realización, cuando el módulo de monitorización de señal 1430 detecta los tonos DTMF en la señal de audio, el módulo de interfaz de señal 1436 pasa las señales que representan los tonos DTMF a uno o más terminales informáticos de agentes respectivos 1406 (solamente se muestra un terminal informático de agente por motivos de claridad). En un modo de realización, las señales que representan los tonos DTMF se reciben en los terminales informáticos de los agentes mediante una interfaz de entrada de datos 1438, que opera en el *software.* De esta manera, las señales que representan las señales DTMF pueden, directamente, "insertarse" en las aplicaciones de terceros 1442 que residen en el terminal informático del agente 1406 sin la

participación del agente 1420 y sin ninguna conexión entre el terminal informático del agente 1406 y la PBX 1408, el teléfono 1405 o los auriculares/auriculares con micrófono 1409. En otro modo de realización, puede no necesitarse la interfaz de entrada de datos 1438 que opera en el *software* del terminal informático del agente 1406, por ejemplo, si las aplicaciones de terceros 1442 pueden recibir y procesar las señales que representan los tonos DTMF directamente. En un modo de realización, las señales entre el módulo de interfaz de señal 1436 y el terminal informático de agente 1406 se envían a través de la red de datos del centro de llamadas (p. ej., red de área local).

[0123] Los medios para la identificación del terminal informático del agente adecuado al que deberían enviarse las señales puede variar en función del tipo de sistema de teléfono instalado en el centro de llamadas y de dónde esté situado el dispositivo de grabación existente 1410. Tales medios les resultarán evidentes a un experto en la materia. Por ejemplo, las llamadas entrantes pueden asignarse a un terminal informático de un agente por medio de identificación de línea. Otro ejemplo consiste en que, para una empresa con una PBX compatible con VoIP y un dispositivo de grabación de llamadas compatible con VoIP, los encabezados de paquete de los paquetes de VoIP que contienen información de audio que se debe grabar, también pueden incluir la dirección IP del terminal informático del agente 1406 o del teléfono 1405 en el que un agente recibe la llamada. Por lo tanto, cuando el módulo de monitorización de señal 1430 detecta tonos DTMF en la secuencia de audio, el módulo de interfaz de señal 1436 puede, asimismo, identificar la dirección IP del terminal informático pertinente y, a continuación, esto puede utilizarse cuando se enrutan las señales que representan tonos DTMF.

[0124] Como se observará, las referencias a "un modo de realización", "un modo de realización de ejemplo", etc., indican que el modo de realización descrito puede incluir una característica o estructura concretas, pero no todos los modos de realización deben incluir necesariamente la característica o estructura concretas. Además, dichas expresiones no hacen referencia necesariamente al mismo modo de realización. Asimismo, cuando se describe una característica o estructura concretas en relación con un modo de realización, se afirma que se encuentra dentro del conocimiento de un experto en la materia el hecho de llevar a cabo dicha característica o estructura en relación con otros modos de realización, hayan sido descritos explícitamente o no. Por ejemplo, es posible combinar un primer procesador de llamadas para la extracción de datos de tonos DTMF, de acuerdo con el procesador de llamadas que se muestra en la figura 7, con un segundo procesador de llamadas configurado para el bloqueo de tonos DTMF de dispositivos de grabación de llamadas existentes, de acuerdo con el procesador de llamadas que se muestra en la figura 12. Los dos procesadores de llamadas pueden funcionar en el mismo entorno; por ejemplo, en un centro de llamadas. De hecho, puede haber más de un procesador de llamadas de cada "tipo", es decir, más de un procesador de llamadas para la extracción de tonos DTMF y más de un procesador de llamadas para el bloqueo de los tonos DTMF. Por motivos de comodidad, puede hacerse referencia a estos dos tipos de procesador de llamadas como procesadores de llamadas de "decodificación" y de "filtrado". Si bien no se produce ninguna comunicación entre los procesadores de llamadas de decodificación y de filtrado, actúan conjuntamente para bloquear tonos DTMF a un dispositivo de grabación de llamadas existente y también extraen datos de los tonos DTMF y envían los datos extraídos directamente al terminal informático del agente, evitando posiblemente que se le muestren los datos extraídos al agente. Esto permite que el centro de llamadas pueda aislar su sistema de grabación de llamadas existente, su sistema de grabación de pantalla existente y también a sus agentes de los datos confidenciales de un cliente, sin tener que hacer ningún cambio en sus sistemas informáticos existentes en uso en el terminal informático del agente o en sus sistemas de grabación de llamadas o de pantalla. Otro ejemplo consiste en que el procesador de llamadas 1316, que se muestra en la figura 13, puede incluir un módulo de modificación de señal 932, tal y como se muestra en la figura 9.

[0125] Aunque en los modos de realización anteriores se detectan y se enmascaran los tonos DTMF en señales de audio digitales, los datos de señal pueden comprender paquetes de datos VoIP. En el caso de VoIP, los "tonos" DTMF se transmiten en paquetes específicos (paquetes de evento RTP RFC 2833). En ese caso, los datos correspondientes a los paquetes de voz pueden grabarse al tiempo que se descartan los paquetes DTMF, es decir, puede aplicarse el filtro de paquetes. No obstante, en el transmisor hay un retraso pequeño hasta que se reconoce el tono DTMF, antes de que el transmisor envíe un paquete de evento RTP RFC 2833. Por lo tanto, en este caso, puede utilizarse el almacenamiento en búfer para enmascarar toda la información de DTMF que precede a la recepción del paquete de evento RTP RFC 2833.

[0126] A pesar de que, en los modos de realización anteriormente expuestos, los patrones predeterminados se describen como comprendiendo tonos de audio tales como tonos DTMF, se pueden detectar también otros tipos de patrones predeterminados, por ejemplo, señales de voz que contengan información biométrica de voz, información que represente una palabra o frase hablada, o información hablada de seguridad (como una contraseña, una frase de contraseña u otra información de seguridad). Por lo tanto, cualquiera de los módulos de monitorización de señal mencionados anteriormente puede configurarse para establecer la información con referencia a fuentes externas; p. ej., una base de datos de contraseñas de clientes, y el empleo de técnicas de procesamiento de señales digitales, tales como las técnicas de reconocimiento del habla. Para el reconocimiento de voz en el que la persona que llama solamente debe proporcionar parte de la contraseña (p. ej., dos letras aleatorias de una palabra de diez letras), los patrones de voz detectados correspondientes a las letras solamente han de enmascararse para el módulo de grabación, puesto que el agente no puede formar la contraseña

completa. Es evidente que, para el reconocimiento de voz en el que se requiere una contraseña completa, puede enmascararse la generación para el agente. Asimismo, en el momento en que debe pronunciarse la contraseña, puede apagarse el audio del agente.

[0127] De por sí, el módulo de monitorización de señal puede hacer referencia a una fuente adicional con el fin de determinar la naturaleza de las señales comunicadas a una fuente externa. De esta manera, otra funcionalidad es posible (por ejemplo, hacer referencia a una base de datos que contiene contraseñas de clientes para comprobar si un cliente ha pasado un control de seguridad o comunicarse con un sistema de pago de tarjeta de crédito para autorizar una transacción de un cliente).

[0128] Aunque los modos de realización anteriores indican que el módulo de interfaz de señal está configurado para determinar y comunicar el número de veces que se han detectado los patrones, también se contemplan otras variaciones. Por ejemplo, las señales comunicadas por el módulo de interfaz de señal pueden configurarse para indicar la duración del patrón detectado y la proporción o la longitud del patrón detectado que se ha detectado en un periodo de tiempo determinado. De esta manera, es posible que la aplicación de un tercero determine qué cantidad de información de seguridad del cliente se ha recibido.

[0129] En un modo de realización, el módulo de interfaz de señal proporciona una confirmación de que se ha pasado un control de seguridad. De esta manera, es posible confirmar, a través de la aplicación de un tercero, al miembro del personal del centro de llamadas, que la persona que llama ha pasado un control de seguridad, sin que el miembro del personal del centro de llamadas tenga que llevar a cabo la operación de control de seguridad o ayudar a su realización.

[0130] En los modos de realización anteriores, el módulo de interfaz de señal se describe como comunicando señales que representan una o más de una representación alfanumérica del patrón detectado, el número de veces que se ha detectado un patrón o varios patrones, la duración del patrón detectado, la proporción o longitud del patrón detectado que se ha detectado en un periodo de tiempo determinado, la confirmación de que se ha pasado un control de seguridad y la confirmación de que se ha autorizado una transacción. Alternativa o adicionalmente, pueden comunicarse otros tipos de señales. Estas incluyen señales que representan el tipo de patrón que se ha detectado, metadatos relacionados con el patrón detectado y el audio digital, el valor de una función *hash* que opera en el patrón detectado, un identificador generado de manera única que representa los datos detectados, un valor verdadero/falso basado en si se ha detectado o no un patrón predeterminado, una probabilidad estadística de que el patrón predeterminado se ha detectado, una referencia a un registro en una base de datos que sea igual o probablemente igual que el patrón detectado o probablemente detectado, señales de "datos iniciales" o "datos finales" basadas en el patrón detectado, un valor o una secuencia de valores separados basados en el patrón detectado, y la no comunicación de ninguna señal.

[0131] Por ejemplo, a partir del tipo de patrón que se ha detectado, es posible que la aplicación de un tercero tenga conocimiento de si (por ejemplo) el cliente ha generado un tono DTMF mediante la utilización del teclado numérico de su teléfono.

[0132] Los metadatos relacionados con el patrón detectado y el audio digital permiten que la aplicación de un tercero tenga conocimiento de (por ejemplo) el momento en que se detectó el patrón, el número de repeticiones en el audio digital y la duración del patrón. Este uso también permite almacenar dichos datos con o junto al audio digital enmascarado, para su búsqueda o notificación posterior. De esta manera, es posible encontrar fácilmente todas las llamadas grabadas en las que se han enmascarado los tonos DTMF, simplemente mediante la búsqueda entre los metadatos asociados de estas llamadas.

[0133] El valor de una función *hash* que opera en el patrón detectado y del identificador generado de manera única que representa los datos detectados, permiten a las aplicaciones de terceros almacenar representaciones de números de tarjeta de crédito sin almacenar los propios números de tarjeta de crédito reales y sin almacenarse el número de tarjeta de crédito en la grabación de la llamada. Esta "tokenización" o "función *hash*" es conocida por los expertos en la materia de la seguridad o criptografía de tarjeta de crédito y sirve para mejorar la seguridad. Los valores "*token*" o "*hash*" no pueden utilizarse para realizar transacciones con tarjeta de crédito, pero son útiles para informar sobre datos de clientes, determinar en qué casos se ha utilizado la misma tarjeta de crédito para hacer compras en otra ocasión y para otros análisis de *marketing* o estadísticos.

[0134] Los valores verdaderos/falsos basados en si se ha detectado o no un patrón predeterminado, así como las señales que representan una probabilidad estadística de que se ha detectado el patrón predeterminado, permiten a las aplicaciones de terceros determinar la "seguridad" estadística de que un cliente ha (por ejemplo) pasado un control de seguridad.

[0135] Las señales que representan una referencia a un registro en una base de datos que es igual o probablemente igual al patrón detectado o probablemente detectado permiten que se le proporcione a una aplicación de un tercero (por ejemplo) el nombre del cliente que es igual o probablemente igual, un control de seguridad que acaba de realizar la persona que llama, pero sin que aparezca la información de seguridad real (como una contraseña) en la grabación de la llamada asociada.

[0136] Las señales que representan "datos iniciales" o "datos finales" basados en el patrón detectado permiten que una aplicación de un tercero (por ejemplo) esté preparada para recibir datos de tarjeta entrantes y, a continuación, detener la recepción de los datos, a partir de la detección de caracteres alfanuméricos DTMF concretos. Por ejemplo, si un cliente introdujera los datos de su tarjeta con un prefijo de tono de almohadilla *"#"*, el módulo de interfaz de señal avisaría de forma eficaz a la aplicación de un tercero de que a continuación se proporcionarían los datos de la tarjeta. Un tono de asterisco "*", por ejemplo, detendría la recepción de los datos de la tarjeta por parte de la aplicación de un tercero. De esta manera, asimismo, los clientes que cometan un error al introducir los datos de tarjeta pueden pulsar la almohadilla *"#"* para empezar de nuevo.

[0137] Un valor o una secuencia de valores distintos basados en el patrón detectado permiten que una aplicación de un tercero determine que está recibiendo una señal del procesador de llamadas y no de otra fuente. Por ejemplo, en un modo de realización, el procesador de llamadas genera señales para un terminal informático por medio de una interfaz USB que imita pulsaciones de teclas de ordenador. Al transmitir una secuencia de valores distintos (por ejemplo, una cadena semialeatoria predeterminada que es muy poco probable que jamás teclee un humano), la aplicación de un tercero puede determinar con exactitud que recibe una señal directamente del procesador de llamadas y no de un humano que escribe con un teclado.

[0138] El hecho de no transmitir ninguna señal basada en el patrón detectado permite que el procesador de llamadas (por ejemplo) corrija de forma automática algunos errores que pueden ser introducidos por un cliente que teclea los datos de tarjeta. Por ejemplo, los datos de tarjeta no contienen el carácter de almohadilla *"#"*, de tal forma que al no transmitir ninguna señal cuando un cliente teclea la almohadilla *"#"*, la aplicación de un tercero se aísla del error. Este mismo proceso es útil para eliminar la transmisión de secuencias de tono de "control" especiales (tales como "datos iniciales" y "datos finales" descritos anteriormente), que pueden utilizarse principalmente para comunicarse con el procesador de llamadas, pero que no están pensados para la comunicación posterior con una aplicación de un tercero.

[0139] Asimismo, las señales transmitidas por el módulo de interfaz de señal pueden enviarse tan pronto como se detecte el patrón. Por lo tanto, tan pronto como se detectan los tonos DTMF, las representaciones alfanuméricas de los mismos pueden transmitirse directamente a la aplicación de un tercero sin retraso. Además, las señales transmitidas por el módulo de interfaz de señal pueden almacenarse en búfer y, a continuación, enviarse más adelante. Por definición, puede detectarse toda la secuencia DTMF y, a continuación, enviarse de una sola vez sus representaciones alfanuméricas a la aplicación de un tercero. Asimismo, las señales transmitidas por el módulo de interfaz de señal pueden transmitirse bajo demanda desde otra fuente debidamente autorizada. De esta manera, una aplicación de un tercero debidamente autorizada podría solicitar al módulo de interfaz de señal el número de tonos DTMF que se han detectado durante la llamada actual.

[0140] Durante la comunicación con una aplicación de un tercero, resulta ventajoso que la identidad de la aplicación de un tercero se establezca como debidamente autorizada para recibir dichas comunicaciones. Las credenciales de autorización pueden presentarse en forma de certificado de seguridad u otro dispositivo de certificación similar conocido por los expertos en la materia de la seguridad de comunicaciones.

[0141] Las señales transmitidas por el módulo de interfaz de señal pueden encontrarse en el sistema operativo de un aparato de procesamiento de datos (un ordenador). Las señales transmitisdas por la interfaz de señal pueden encontrarse en el sistema operativo de un teléfono u otro dispositivo de comunicación portátil. Las señales transmitidas por la interfaz de señal se pueden transmitir por medio de un método intermedio (como a través de archivos de texto, archivos XML o *Really Simple Syndication* (RSS)). En este sentido, muchas aplicaciones distintas de terceros se pueden transmitir a través de la interfaz de señal, de acuerdo con las normas de formato de comunicaciones, que son conocidas por los expertos en la materia.

[0142] Las señales transmitidas por la interfaz de señal pueden representar comunicaciones sin cifrar de "texto sin formato". También pueden representar comunicaciones sin cifrar mediante la utilización de técnicas de cifrado de datos conocidas por los expertos en la materia. De esta manera, tanto las comunicaciones "abiertas" como las "cerradas" (o seguras) son posibles con las aplicaciones de terceros.

[0143] Si bien en los modos de realización anteriores, una máscara aplicada por el módulo de modificación de señal sustituye el patrón detectado por un tono de audio de un único tono, la modificación podría, alternativamente, comprender tonos de audio aleatorios o una señal de ruido blanco. Adicionalmente, la modificación aplicada por el módulo de modificación de señal puede servir para suprimir u ocultar parte del patrón detectado, de tal forma que las señales de datos iniciales que representan audio no pueden determinarse por completo a partir del audio digital enmascarado. De esta manera, la señal detectada se oculta de distintas formas en el audio digital, pero el audio digital todavía contendrá "marcadores de posición" audibles para indicar que se ha detectado un patrón.

[0144] La modificación aplicada por el módulo de modificación de señal puede servir para cifrar el patrón detectado. De esta forma, de acuerdo con un aspecto de la invención, pueden cifrarse los datos de seguridad personales de un cliente (preferiblemente, con un algoritmo de cifrado conocido por los expertos en la materia) para el descifrado posterior por parte de una aplicación o persona debidamente autorizadas. De esta manera, las

personas o aplicaciones que no estén debidamente autorizadas para descifrar el patrón no podrán determinar su naturaleza.

[0145] La modificación aplicada por el módulo de modificación de señal puede actuar en uno de los canales estéreo de las señales de audio digitales, en caso de que las señales de audio digitales estén en estéreo. De esta manera, de acuerdo con un aspecto de la invención, los datos de tarjeta de crédito de un cliente enviados a través de DTMF pueden eliminarse del audio digital, pero cualquier conversación o cualquier otra señal de audio del audio digital pronunciada, por ejemplo, por un miembro del personal del centro de llamadas, no se ven afectadas. Adicionalmente, la modificación aplicada por el módulo de modificación de señal puede actuar en ambos canales estéreo de las señales de audio digitales, en caso de que las señales de audio digitales estén en estéreo.

[0146] Los datos relacionados con las señales generados por el procesador de entrada de datos pueden representar un marcador de posición (tal como el carácter alfanumérico "*"). De esta manera, los datos de un cliente pueden representarse en el ordenador del miembro del personal del centro de llamadas como una serie de asteriscos, signos "X" o similares, para ocultar la información confidencial, al tiempo que siguen cumpliendo con el requisito de las aplicaciones informáticas del miembro del personal del centro de llamadas de que los datos pertinentes deben introducirse en la aplicación.

[0147] Asimismo, el marcador de posición puede ser un carácter alfanumérico aleatorio. Además, puede estar en el mismo formato que la información que se prevé recibir de la aplicación de un tercero. De esta manera, la aplicación informática del miembro del personal del centro de llamadas puede cumplir con el formato, la composición, la longitud u otras propiedades de cualquier requisito de entrada de datos.

[0148] Además, el marcador de posición puede no estar deliberadamente en el mismo formato que la información que se prevé recibir de la aplicación de un tercero. De esta manera, la aplicación de un tercero puede dotarse de información que interprete como deliberadamente errónea, con el fin de provocar una solicitud posterior de datos adicionales.

[0149] Las señales recibidas de la interfaz de señal pueden modificarse para adaptarse al formato que se prevé recibir de la aplicación de un tercero, antes de la generación de datos relacionados con señal para la aplicación de un tercero. De esta manera, por ejemplo, pueden cifrarse los datos de tarjeta para garantizar todavía más la seguridad.

[0150] Si bien en los modos de realización anteriores el procesador de llamadas está configurado para evitar que la aplicación de *software* muestre las representaciones alfanuméricas y/o que la señal de dispositivo de entrada emulada emulada las introduzca como datos en un campo de entrada de datos, también se contemplan otras interacciones o comandos.

[0151] Las interacciones o comandos pueden servir para determinar que las señales que estén a punto de transmitirse con una aplicación de un tercero se muestren en la ubicación de entrada de datos prevista de la aplicación de un tercero prevista. Por ejemplo, el comando o método pueden configurarse para determinar el "título de ventana" actual y el título de campo de entrada de datos actual de una aplicación de un tercero, y denegar la comunicación de señal a ubicaciones no previstas. De este modo, puede evitarse que los agentes, por ejemplo, vean datos de tarjeta confidenciales en una ubicación separada de la que pueden robarse.

[0152] Las interacciones o comandos pueden servir para que la visualización de representación alfanumérica en la aplicación de un tercero se realice de manera automática para solamente una ubicación de entrada de datos prevista. Por ejemplo, el comando o método pueden incluir la localización de un campo de entrada de datos con una propiedad o característica concretas (por ejemplo, una que presente una etiqueta de texto "CV2" a la izquierda) y, a continuación, pasar el elemento CV2 de los datos de tarjeta únicamente a este campo. De esta manera, los datos de tarjeta se dirigen de forma obligada a su ubicación prevista y, por lo tanto, los agentes no pueden robarlos de otras ubicaciones.

[0153] Las interacciones con la aplicación de un tercero o los comandos generados para la aplicación de un tercero pueden servir para restringir, limitar o denegar la entrada de datos manual en la aplicación de un tercero. Por ejemplo, se le denegaría al miembro del personal del centro de llamadas la competencia para introducir, corregir, sobrescribir o (críticamente) copiar los datos confidenciales del cliente de la pantalla de su ordenador.

[0154] Las interacciones con la aplicación de un tercero o los comandos generados para la aplicación de un tercero pueden servir para alterar la representación visual de la aplicación de un tercero. También pueden servir para cambiar la representación de la aplicación de un tercero con el fin de mostrar la información del marcador de posición (tal como el carácter alfanumérico "*"). De esta manera, aunque se puede preconfigurar una aplicación informática de un miembro del personal del centro de llamadas para que se muestre la información confidencial en la pantalla del ordenador, puede modificarse la visualización con el uso de comandos o métodos de enmascaramiento visual para ocultar los datos con asteriscos, signos "X" o similares.

[0155] Las interacciones con la aplicación de un tercero o los comandos generados para la aplicación de un tercero pueden servir para eliminar restricciones existentes en el formato de entrada de datos manual en la aplicación de un tercero. Por lo tanto, los datos transmitidos directamente a la aplicación de un tercero pueden tener un formato diferente al permitido para la entrada de datos manual.

[0156] Las interacciones con la aplicación de un tercero o los comandos generados para la aplicación de un tercero pueden servir para esconder u ocultar de cualquier otra forma partes de la aplicación de un tercero. En consecuencia, los datos de seguridad del cliente pueden esconderse de la pantalla del ordenador del miembro del personal del centro de llamadas con el fin de eliminar la competencia del miembro del personal de anotar la información.

[0157] Las interacciones con la aplicación de un tercero o los comandos generados para la aplicación de un tercero pueden servir para modificar el funcionamiento de la aplicación de un tercero. Asimismo, puede servir para insertar un proceso de "devolución de llamada" (que sirve para permitir que la aplicación de un tercero proporcione señales de vuelta al procesador de entrada de datos o solicite la transmisión de datos relacionados con señal desde el procesador de entrada de datos). Por ejemplo, una aplicación de un tercero puede pedir que se transmitan los datos de tarjeta de crédito confidenciales del cliente en el momento en que el miembro del personal del centro de llamadas intente autorizar los datos de tarjeta de crédito, de tal forma que se evita de antemano la visualización o la comunicación de la información de tarjeta de crédito en la pantalla del ordenador del miembro del personal del centro de llamadas.

[0158] Las interacciones con la aplicación de un tercero o los comandos generados para la aplicación de un tercero pueden servir para modificar el modelo de objeto de documento de una página web que se muestra en un navegador web. Por ejemplo, puede alterarse una página web para cambiar un campo de entrada de tarjeta de crédito específico por un campo de "visualización como asteriscos", de tal forma que se oculten los datos de tarjeta con caracteres de asterisco "*", y se restrinja todavía más la competencia del agente para copiar datos de tarjeta de ese campo.

[0159] Las interacciones con la aplicación de un tercero o los comandos generados para la aplicación de un tercero pueden servir para detectar cambios en aplicaciones de terceros, antes de transmitir las señales a la aplicación de un tercero. Por ejemplo, un comando o método se pueden configurar para detectar la activación de una función de "enviar" en la pantalla del ordenador del miembro del personal del centro de llamadas y transmitir los datos de tarjeta en el momento en que se activa la función de enviar. De esta manera, por ejemplo, un agente nunca ve los datos de tarjeta en la pantalla.

[0160] Las interacciones con la aplicación de un tercero o los comandos generados para la aplicación de un tercero pueden servir para descifrar información ya cifrada en otro lugar. De esta manera, por ejemplo, los datos pueden situarse a simple vista, pero de forma cifrada en una pantalla de ordenador del agente del centro de llamadas y, a continuación, descifrarse inmediatamente antes del procesamiento.

[0161] Las interacciones con la aplicación de un tercero o los comandos generados para la aplicación de un tercero pueden servir para emitir comandos reconocidos por la aplicación de un tercero. Asimismo, estos comandos o métodos pueden imitar comandos manuales que un operador de la aplicación de un tercero puede llevar a cabo. Si, por ejemplo, un cliente está confirmando datos de tarjeta de crédito para una transacción con tonos DTMF, puede ordenarse a la aplicación de un tercero que procese la transacción (por ejemplo, imitando la activación de una función de "enviar" en la pantalla del ordenador del miembro del personal del centro de llamadas) una vez que se ha recibido el número correcto de dígitos de la tarjeta de crédito.

[0162] Las interacciones con la aplicación de un tercero o los comandos pueden, asimismo, servir para reunir información de una aplicación de un tercero y combinarla con datos del módulo de interfaz de señal antes de emitir comandos reconocidos por la aplicación de un tercero. Por ejemplo, si un agente del centro de llamadas está tomando los datos de transacción de un cliente e introduciéndolos en una página web de pagos, el nombre del cliente, la dirección y los datos relativos al precio de la transacción pueden reunirse desde el lugar en el que ya los ha introducido en la página web el agente del centros de llamadas, combinados con los datos de tarjeta del cliente transmitidos a través de tonos DTMF y, a continuación, un comando HTTP "Post" ejecutado mediante la utilización de comandos o métodos de enmascaramiento visual, para transmitir todos los datos para la autorización del pago. De esta manera, el agente del centro de llamadas nunca ve los datos de tarjeta en pantalla.

[0163] Las interacciones con la aplicación de un tercero o los comandos generados para la aplicación de un tercero pueden servir para invertir o anular el efecto de cualquier interacción con la aplicación de un tercero o comandos previamente emitidos para la aplicación de un tercero. En consecuencia, cualquier cambio que se haya hecho con la actuación o la aparición de la aplicación de un tercero puede invertirse; por ejemplo, después de haberse procesado una transacción.

[0164] Las interacciones o comandos pueden incluir la comunicación de interfaz de programación de aplicaciones (API, por sus siglas en inglés) con una aplicación de un tercero, la alteración del contenido HTML de

una página web o un modelo de objeto de documento, macros o *scripts*, o cualquier comunicación similar o relacionada necesaria para interactuar con la aplicación de un tercero.

[0165] Los datos relacionados con señal pueden enviarse a la aplicación de un tercero alfanumérica carácter por carácter, a medida que el procesador de audio detecta el patrón. De esta manera, los datos de tarjeta de crédito de un cliente representados en tonos DTMF pueden enviarse un carácter a la vez a la aplicación de un tercero. Alternativamente, los datos relacionados con señal pueden enviarse a la aplicación de un tercero en uno o más bloques. Por ejemplo, los datos de tarjeta de crédito de un cliente pueden acumularse a medida que se reciben y, a continuación, transmitirse en un bloque a la aplicación de un tercero.

[0166] Los datos relacionados con señal pueden enviarse a la aplicación de un tercero en distintos momentos en función del modo o estado de la aplicación de un tercero. Por lo tanto, los caracteres del marcador de posición pueden transmitirse a la aplicación de un tercero hasta un momento después de la transacción, cuando se transmiten los datos confidenciales reales del cliente. Con esto se garantizaría que los datos confidenciales del cliente no aparecieran en la pantalla del ordenador de un miembro del personal del centro de llamadas hasta el momento en que se debiera autorizar una transacción, por ejemplo.

[0167] Los datos relacionados con señal pueden enviarse a la aplicación de un tercero tras recibir una solicitud adecuada por parte de la aplicación de un tercero. De esta manera, una aplicación de un tercero debidamente autorizada podría solicitar al procesador de entrada de datos (por ejemplo) que se transmitan los datos de tarjeta de crédito del cliente en el momento en que deba autorizarse la tarjeta de crédito, de tal forma que se garantice que los datos de tarjeta de crédito del cliente no aparezcan en la pantalla del ordenador del miembro del personal del centro de llamadas en absoluto antes de producirse ese momento.

[0168] Las interacciones con la aplicación de un tercero o los comandos generados para la aplicación de un tercero pueden enviarse a la aplicación de un tercero al mismo tiempo que los datos relacionados con señal. También pueden enviarse a la aplicación de un tercero en cualquier momento antes que los datos relacionados con señal. También pueden enviarse a la aplicación de un tercero en cualquier momento después de los datos relacionados con señal.

[0169] La aplicación de un tercero puede comprender un sistema operativo informático. También puede comprender un dispositivo de telecomunicaciones. Asimismo, el dispositivo de telecomunicaciones puede ser un teléfono móvil. Por lo tanto, los dispositivos de telecomunicaciones y ordenadores comunes utilizados en un entorno de centro de llamadas o en un entorno en el que las transacciones se llevan a cabo con datos confidenciales de clientes, pueden eliminar los datos confidenciales de clientes de sus representaciones visuales.

[0170] La aplicación de un tercero puede ser una página web que se visualice en el sistema operativo informático. También puede ser una aplicación que se ejecute en el sistema operativo informático. La aplicación de un tercero puede ser una página web que se visualice en un dispositivo de telecomunicaciones, incluido un teléfono móvil. También puede ser una aplicación que se ejecute en un dispositivo de telecomunicaciones, incluido un teléfono móvil. También puede ser una base de datos u otro medio de almacenamiento de datos. Por lo tanto, las interfaces de entrada de datos utilizadas habitualmente (tales como, aplicaciones informáticas o páginas web) pueden eliminar los datos confidenciales de clientes de sus representaciones visuales y los datos confidenciales de clientes también pueden transmitirse directamente a una base de datos, sin aparecer en la pantalla de ordenador de un miembro del personal del centro de llamadas.

[0171] Si bien los procedimientos y aparatos descritos pueden ofrecer ventajas concretas para operaciones de centro de llamadas, también se pueden aplicar a otras tecnologías de comunicación que implementen la grabación de llamadas de una u otra forma. En este sentido, si bien en los modos de realización anteriores el procesamiento de señales se describe como si se realizara para señales "entrantes", el procesamiento de señales también puede realizarse para señales "salientes"; p. ej., en el lado que origina la llamada.

[0172] Aunque la presente invención se ha descrito anteriormente con referencia a modos de realización específicos, un experto en la materia podrá observar que en el alcance de las reivindicaciones adjuntas caben modificaciones.

REIVINDICACIONES

1. Procedimiento de procesamiento de señales de una comunicación telefónica, transmitiendo las señales información confidencial y no confidencial, implementándose el procedimiento mediante un procesador de llamadas (316) y comprendiendo:

el almacenamiento en búfer de las señales (S404);
la monitorización de las señales (S406) para detectar, en las señales, uno o más casos de una o más características predeterminadas que representan la información confidencial transmitida por las señales;
la modificación de las señales almacenadas en búfer (S410) mediante la eliminación de las características predeterminadas identificadas de las señales almacenadas en búfer;
la generación de las señales modificadas para grabación; y
la determinación de una representación alfanumérica correspondiente a cada caso identificado de las características predeterminadas, y la generación de datos indicativos de dicha representación alfanumérica para su uso por una aplicación de *software*:
donde la modificación de las señales almacenadas en búfer comprende la eliminación de al menos una parte de las señales almacenadas en búfer previas a un punto de detección de cada caso identificado de las características predeterminadas.

2. Procedimiento de acuerdo con la reivindicación 1, que comprende además la grabación de dichas señales modificadas (S412) en el procesador de llamadas implementando dicha monitorización y dicha modificación.

3. Procedimiento de acuerdo con la reivindicación 1, donde la generación de las señales modificadas para la grabación comprende la generación de las señales modificadas para un dispositivo de grabación de llamadas.

4. Procedimiento de acuerdo con la reivindicación 3, que comprende además la generación de una señal de dispositivo de entrada emulada para dicha representación alfanumérica, y donde la generación de datos comprende la generación de dicha señal de dispositivo de entrada emulada.

5. Procedimiento de acuerdo con la reivindicación 3 o la reivindicación 4, que comprende además evitar que se muestre dicha representación alfanumérica a través de la aplicación de *software.*

6. Procedimiento de acuerdo con cualquiera de las reivindicaciones 3 a 5, que comprende además la determinación de un dispositivo informático de destino de entre una pluralidad de dispositivos informáticos, comprendiendo la generación la transmisión de los datos a dicho dispositivo informático de destino.

7. Procedimiento de acuerdo con cualquiera de las reivindicaciones 3 a 6, donde dicha aplicación de *software* se aloja en un dispositivo informático en una ubicación remota del procesador de llamadas, comprendiendo el procedimiento además el cifrado de los datos.

8. Procedimiento de acuerdo con cualquiera de las reivindicaciones anteriores, que comprende además el procesamiento de las señales para proporcionar una primera versión de las señales que se debe grabar y una segunda versión de las señales, donde dicha monitorización, modificación y generación se aplican a la primera versión de las señales.

9. Procedimiento de acuerdo con la reivindicación 8, donde la segunda versión de las señales se debe generar como audio.

10. Procedimiento de acuerdo con la reivindicación 8 o la reivindicación 9, donde al menos dicha monitorización y dicha modificación se aplican a dicha segunda versión de las señales, comprendiendo el procedimiento además la generación de la segunda versión modificada de las señales.

11. Procedimiento de acuerdo con la reivindicación 8, donde la información debe extraerse de la segunda versión de las señales.

12. Procedimiento de acuerdo con la reivindicación 11, que comprende además la monitorización de la segunda versión de las señales para detectar, en la segunda versión de las señales, uno o más casos de una o más características predeterminadas que representan la información confidencial transmitida por las señales; la determinación de una representación alfanumérica correspondiente a cada caso identificado de las características predeterminadas; y la generación de datos indicativos de la representación alfanumérica para su uso por una aplicación de *software*.

13. Procedimiento de acuerdo con la reivindicación 12, donde la monitorización, modificación y generación de la primera versión de las señales se llevan a cabo en una primera ubicación y donde la monitorización de la segunda versión de las señales, la determinación de la representación alfanumérica y la generación de los datos indicativos de la representación alfanumérica se llevan a cabo en una segunda ubicación.

14. Procedimiento de acuerdo con la reivindicación 12 o la reivindicación 13, que comprende además la modificación de la segunda versión de las señales mediante la eliminación de las características predeterminadas identificadas de la segunda versión de las señales y la generación de la segunda versión de las señales para su escucha.

15. Procesador de llamadas (316) para el procesamiento de señales de una comunicación telefónica, transmitiendo las señales información confidencial y no confidencial, estando configurado el procesador de llamadas para la implementación del procedimiento de cualquiera de las reivindicaciones anteriores, comprendiendo:

medios (328) configurados para el almacenamiento en búfer de las señales,
medios (330) configurados para la monitorización de las señales almacenadas en búfer para detectar, en las señales almacenadas en búfer, uno o más casos de una o más características predeterminadas que representan la información confidencial transmitida por las señales;
medios (332) configurados para la modificación de las señales almacenadas en búfer mediante la eliminación de las características predeterminadas identificadas de las señales almacenadas en búfer;
medios configurados para la generación de las señales modificadas para grabación:
medios (336) configurados para la determinación de una representación alfanumérica correspondiente a cada caso identificado de las características predeterminadas, y la generación de datos indicativos de dicha representación alfanumérica para su uso por una aplicación de *software* (342);
y
donde los medios configurados para la modificación de las señales almacenadas en búfer comprenden medios configurados para la eliminación de al menos una parte de las señales almacenadas en búfer previas a un punto de detección de cada caso identificado de las características predeterminadas.

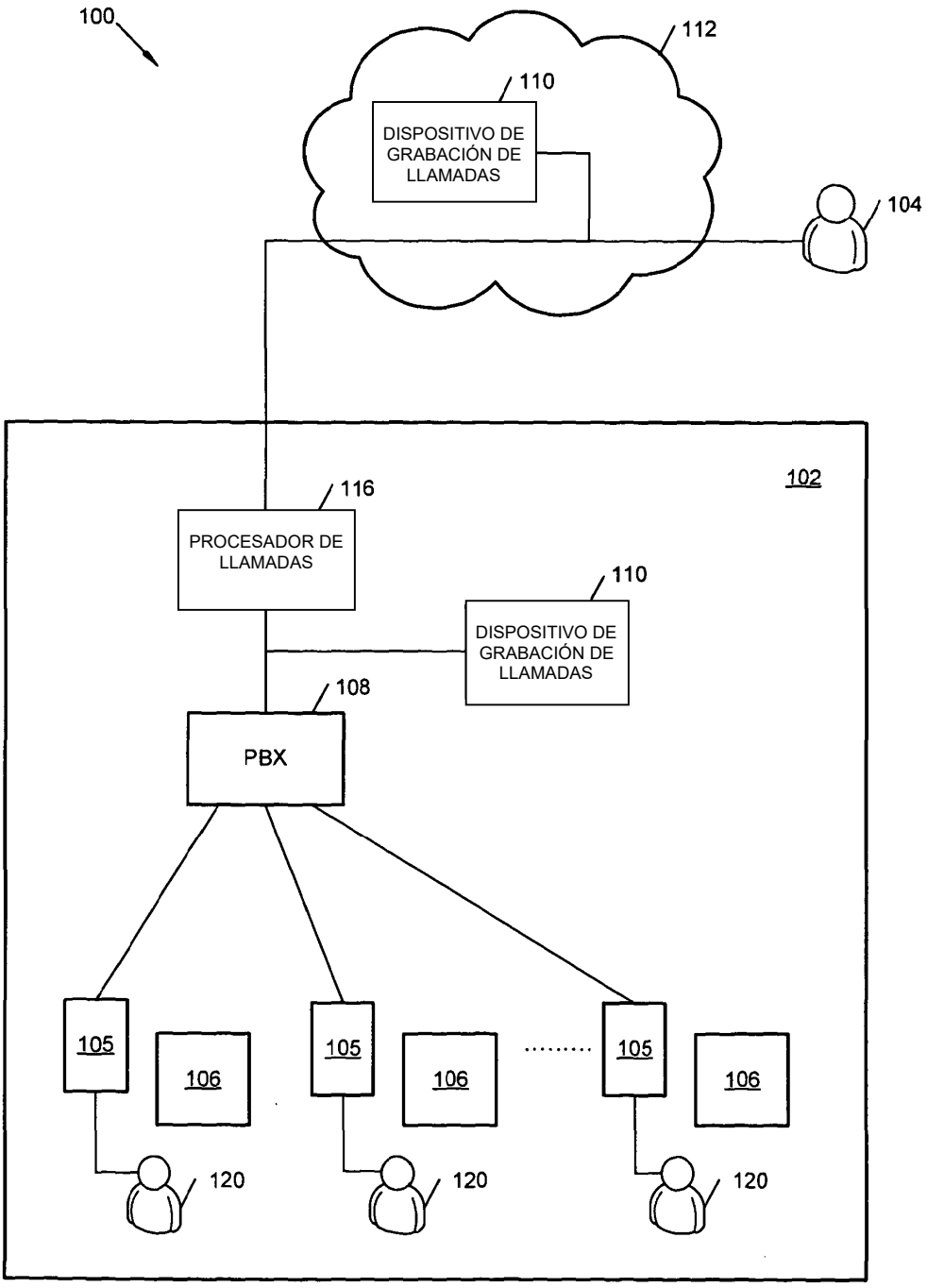

FIGURA 1 (TÉCNICA ANTERIOR)

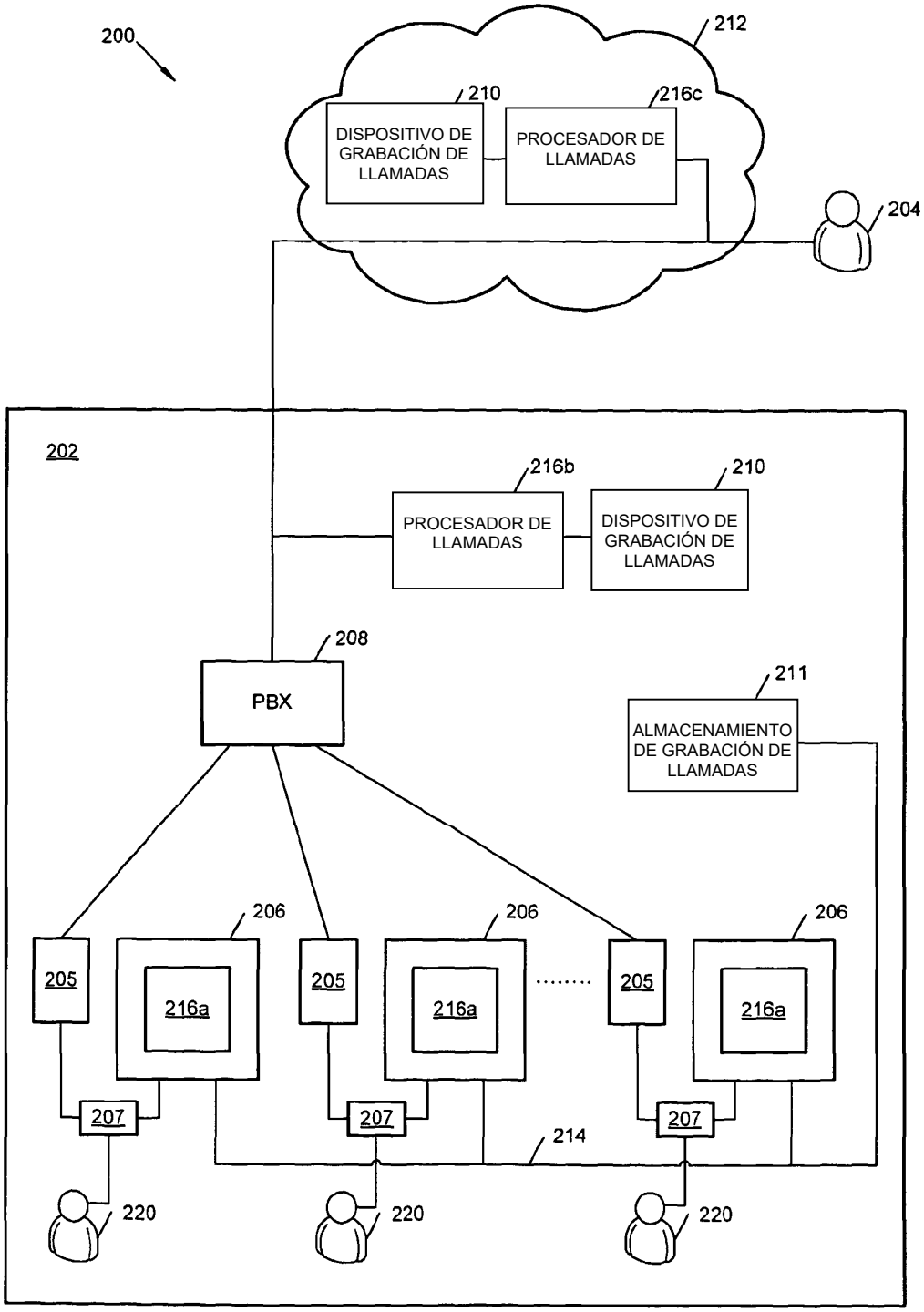
200
212
210
DISPOSITIVO DE GRABACIÓN DE LLAMADAS
216c
PROCESADOR DE LLAMADAS
204
202
216b
PROCESADOR DE LLAMADAS
210
DISPOSITIVO DE GRABACIÓN DE LLAMADAS
208
PBX
211
ALMACENAMIENTO DE GRABACIÓN DE LLAMADAS
206
205
216a
207
214
220

FIGURA 2

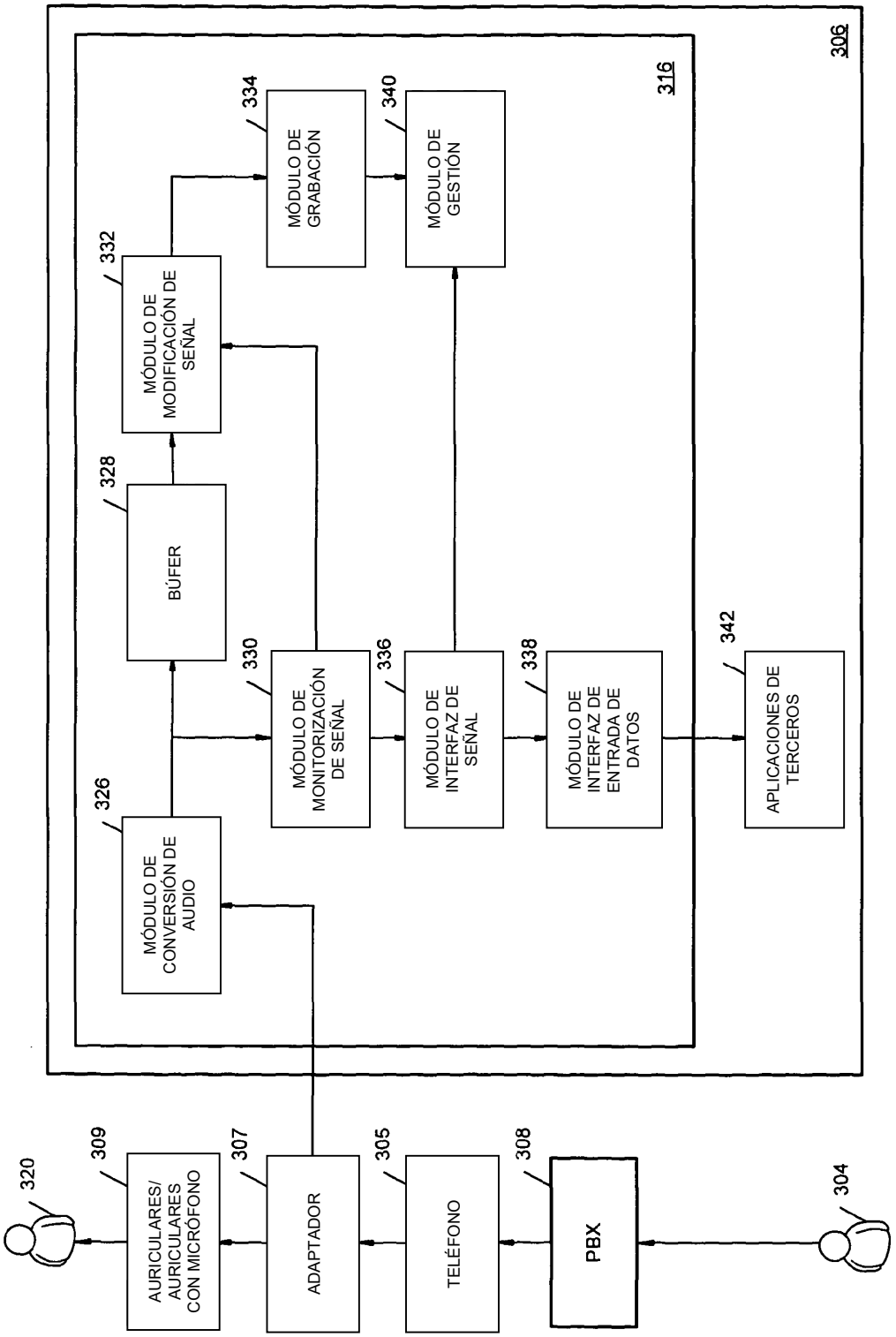
306
316
MÓDULO DE GRABACIÓN
334
MÓDULO DE GESTIÓN
340
MÓDULO DE MODIFICACIÓN DE SEÑAL
332
BÚFER
328
MÓDULO DE MONITORIZACIÓN DE SEÑAL
330
MÓDULO DE INTERFAZ DE SEÑAL
336
MÓDULO DE INTERFAZ DE ENTRADA DE DATOS
338
APLICACIONES DE TERCEROS
342
MÓDULO DE CONVERSIÓN DE AUDIO
326
320
309
AURICULARES/ AURICULARES CON MICRÓFONO
307
ADAPTADOR
305
TELÉFONO
308
PBX
304

FIGURA 3

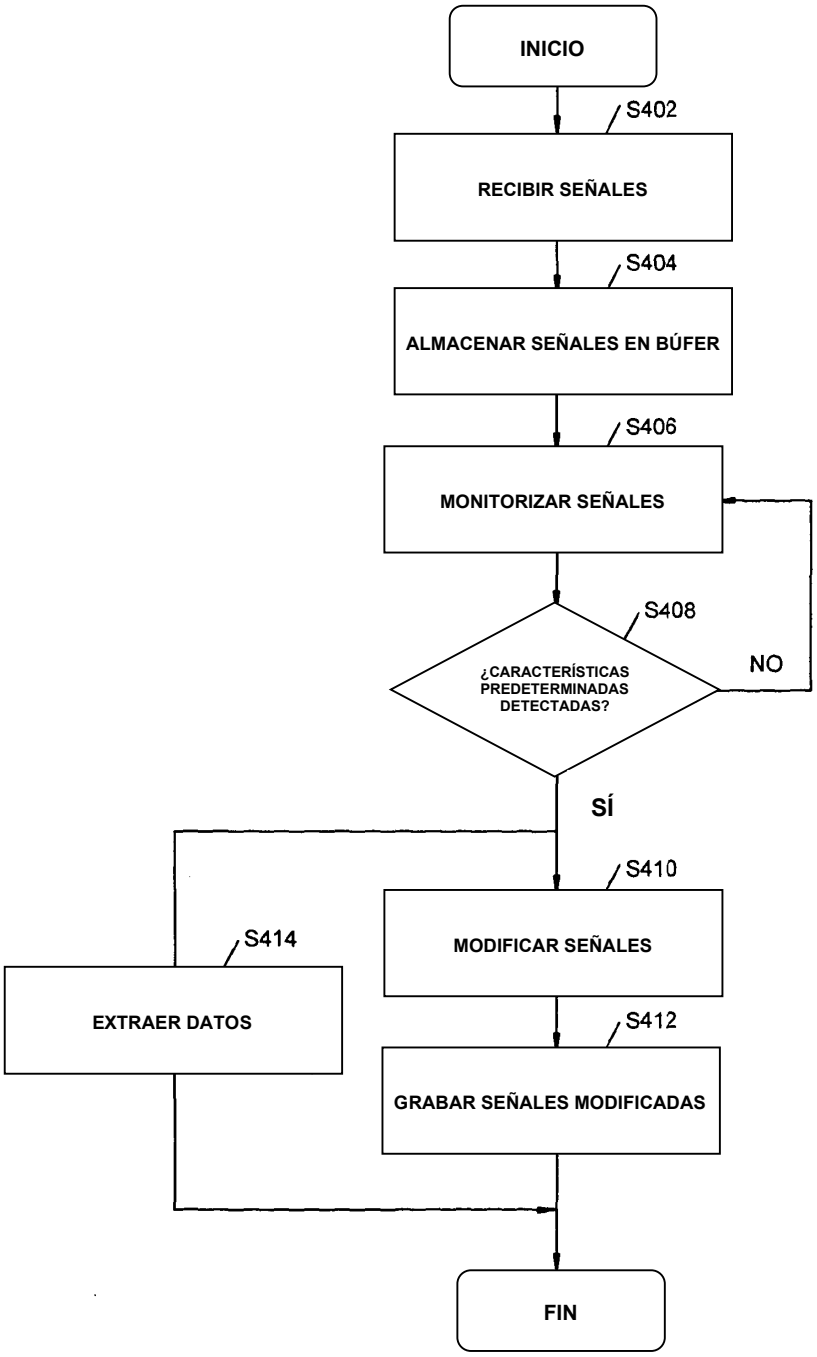
INICIO
S402
RECIBIR SEÑALES
S404
ALMACENAR SEÑALES EN BÚFER
S406
MONITORIZAR SEÑALES
S408
¿CARACTERÍSTICAS PREDETERMINADAS DETECTADAS?
NO
SÍ
S410
MODIFICAR SEÑALES
S412
GRABAR SEÑALES MODIFICADAS
S414
EXTRAER DATOS
FIN

FIGURA 4

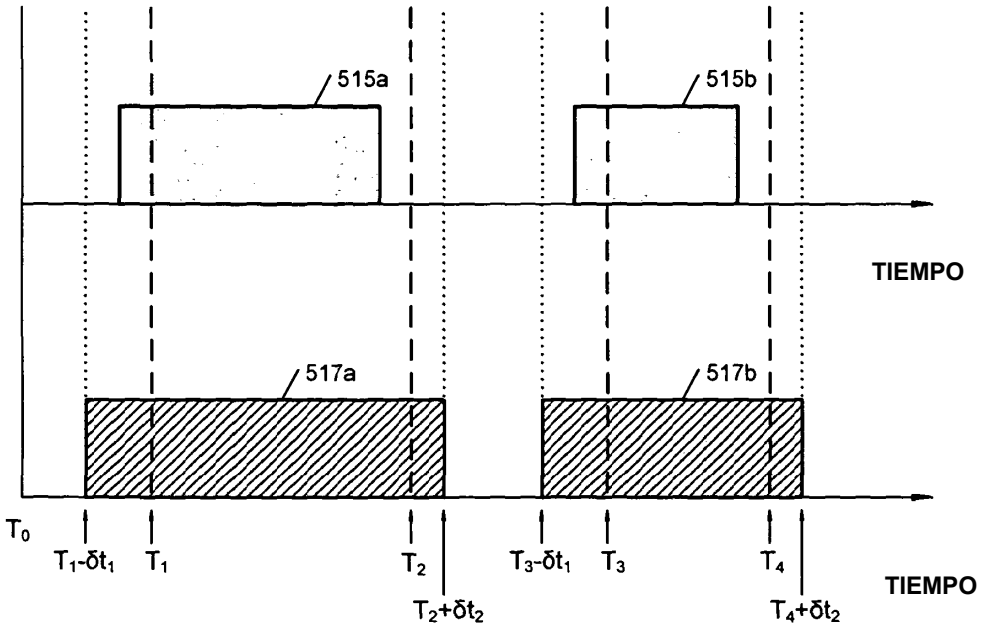
515a
515b
TIEMPO
517a
517b
T0
T1-δt1
T1
T2
T2+δt2
T3-δt1
T3
T4
T4+δt2
TIEMPO

FIGURA 5

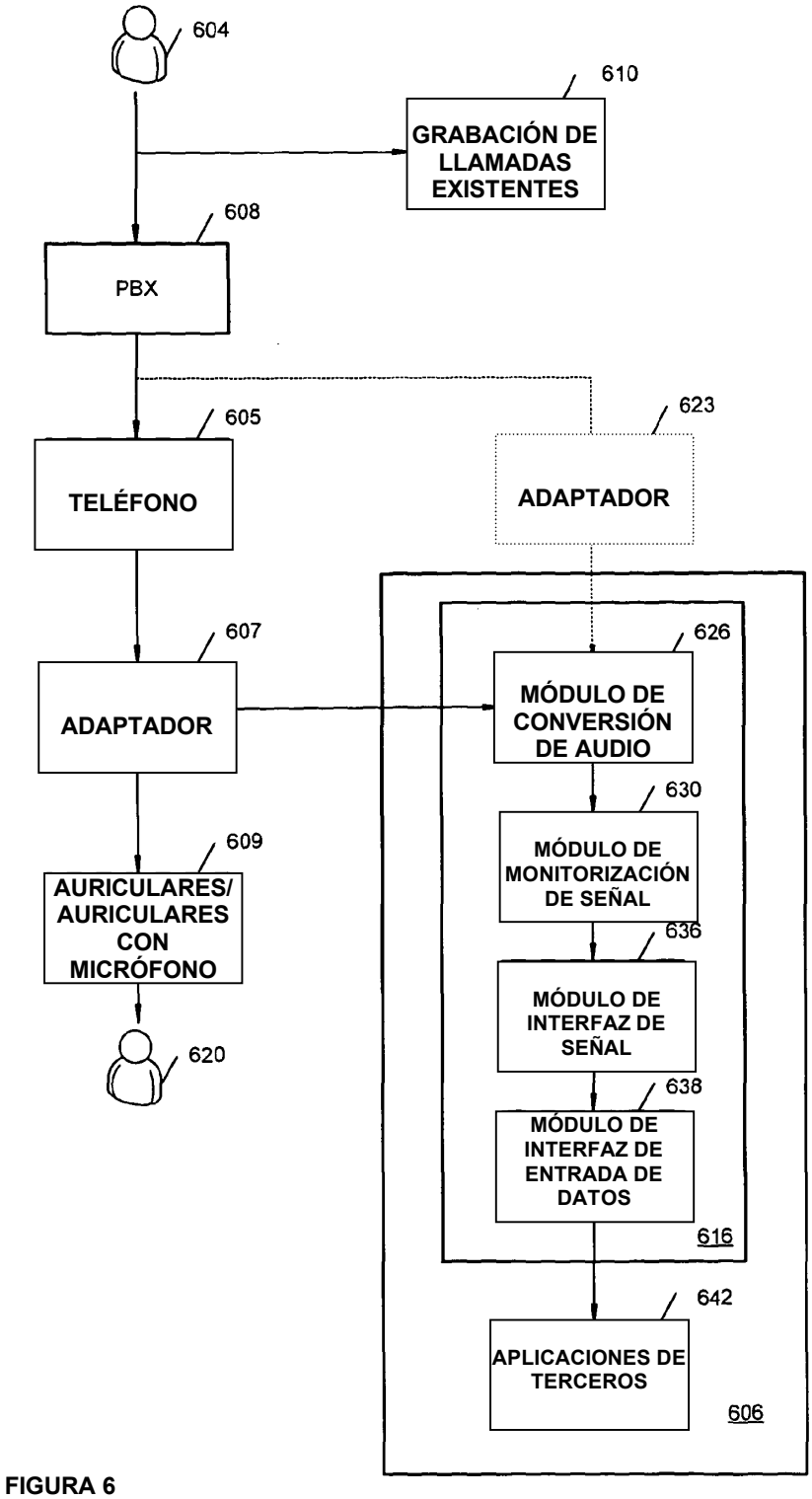
604
610
GRABACIÓN DE LLAMADAS EXISTENTES
608
PBX
605
TELÉFONO
623
ADAPTADOR
607
ADAPTADOR
626
MÓDULO DE CONVERSIÓN DE AUDIO
630
MÓDULO DE MONITORIZACIÓN DE SEÑAL
636
MÓDULO DE INTERFAZ DE SEÑAL
638
MÓDULO DE INTERFAZ DE ENTRADA DE DATOS
616
609
AURICULARES/ AURICULARES CON MICRÓFONO
620
642
APLICACIONES DE TERCEROS
606

FIGURA 6

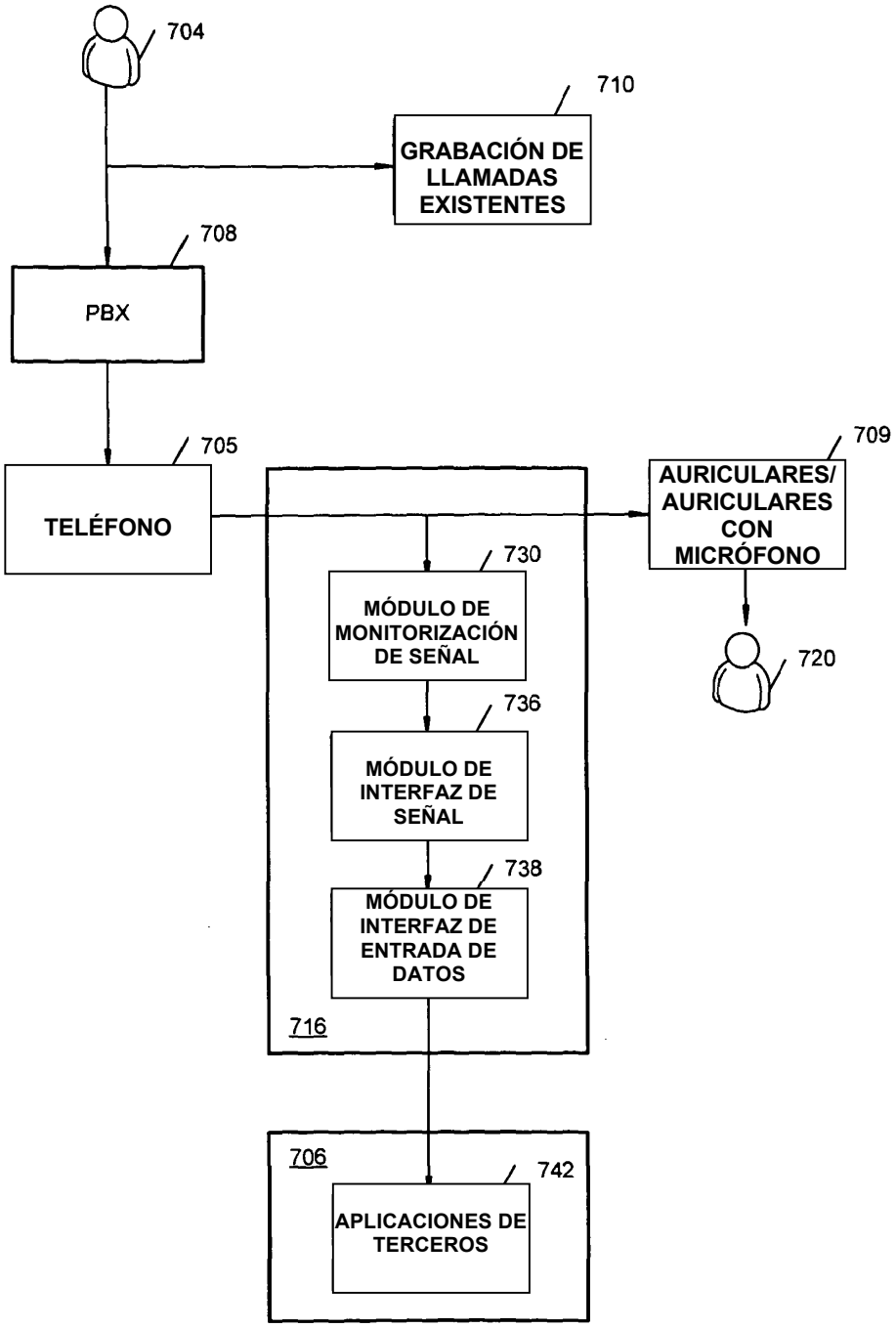
704
710
GRABACIÓN DE LLAMADAS EXISTENTES
708
PBX
705
TELÉFONO
709
AURICULARES/ AURICULARES CON MICRÓFONO
720
730
MÓDULO DE MONITORIZACIÓN DE SEÑAL
736
MÓDULO DE INTERFAZ DE SEÑAL
738
MÓDULO DE INTERFAZ DE ENTRADA DE DATOS
716
706
742
APLICACIONES DE TERCEROS

FIGURA 7

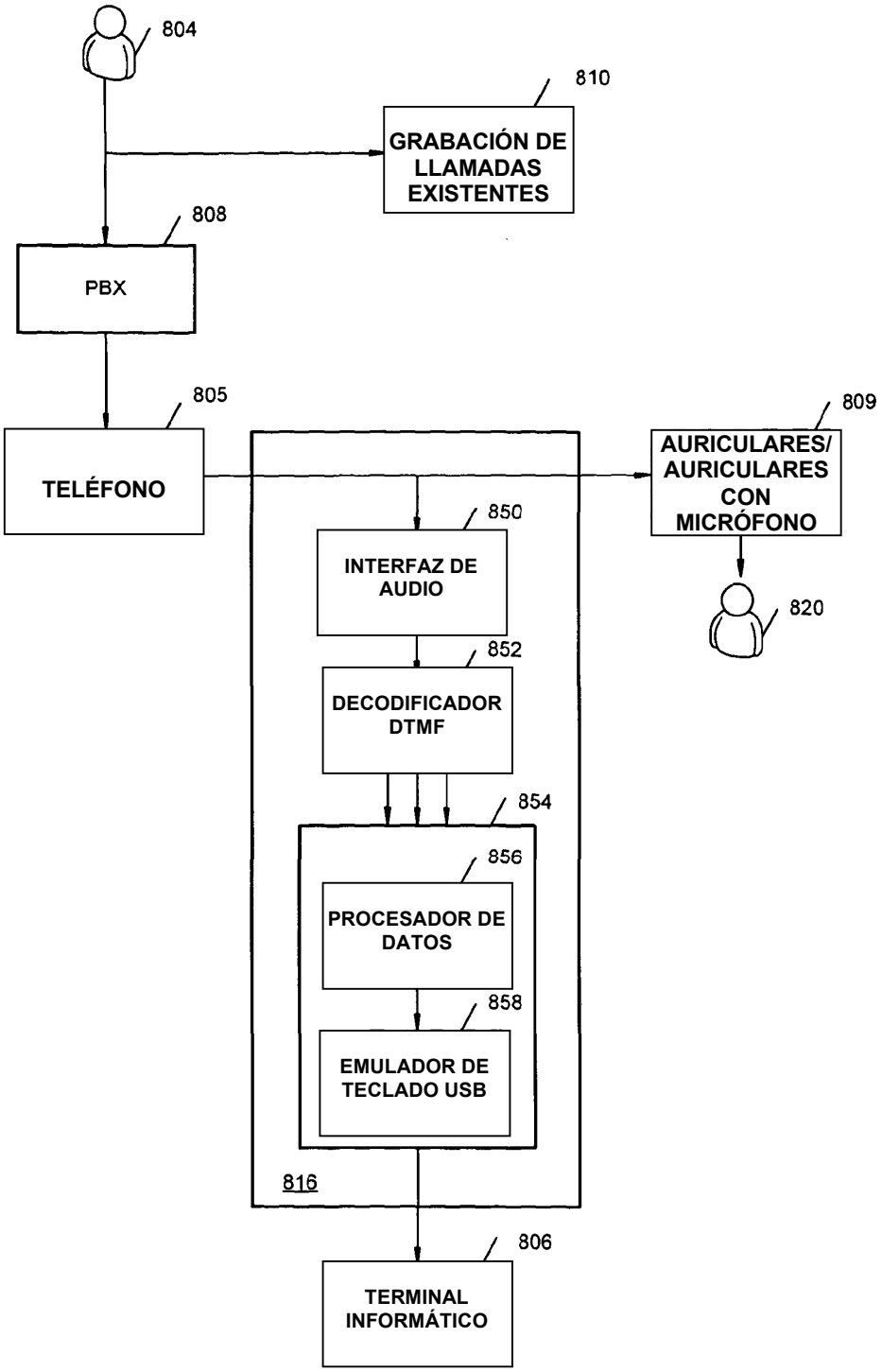
804
810
GRABACIÓN DE LLAMADAS EXISTENTES
808
PBX
805
TELÉFONO
809
AURICULARES/ AURICULARES CON MICRÓFONO
820
850
INTERFAZ DE AUDIO
852
DECODIFICADOR DTMF
854
856
PROCESADOR DE DATOS
858
EMULADOR DE TECLADO USB
816
806
TERMINAL INFORMÁTICO

FIGURA 8

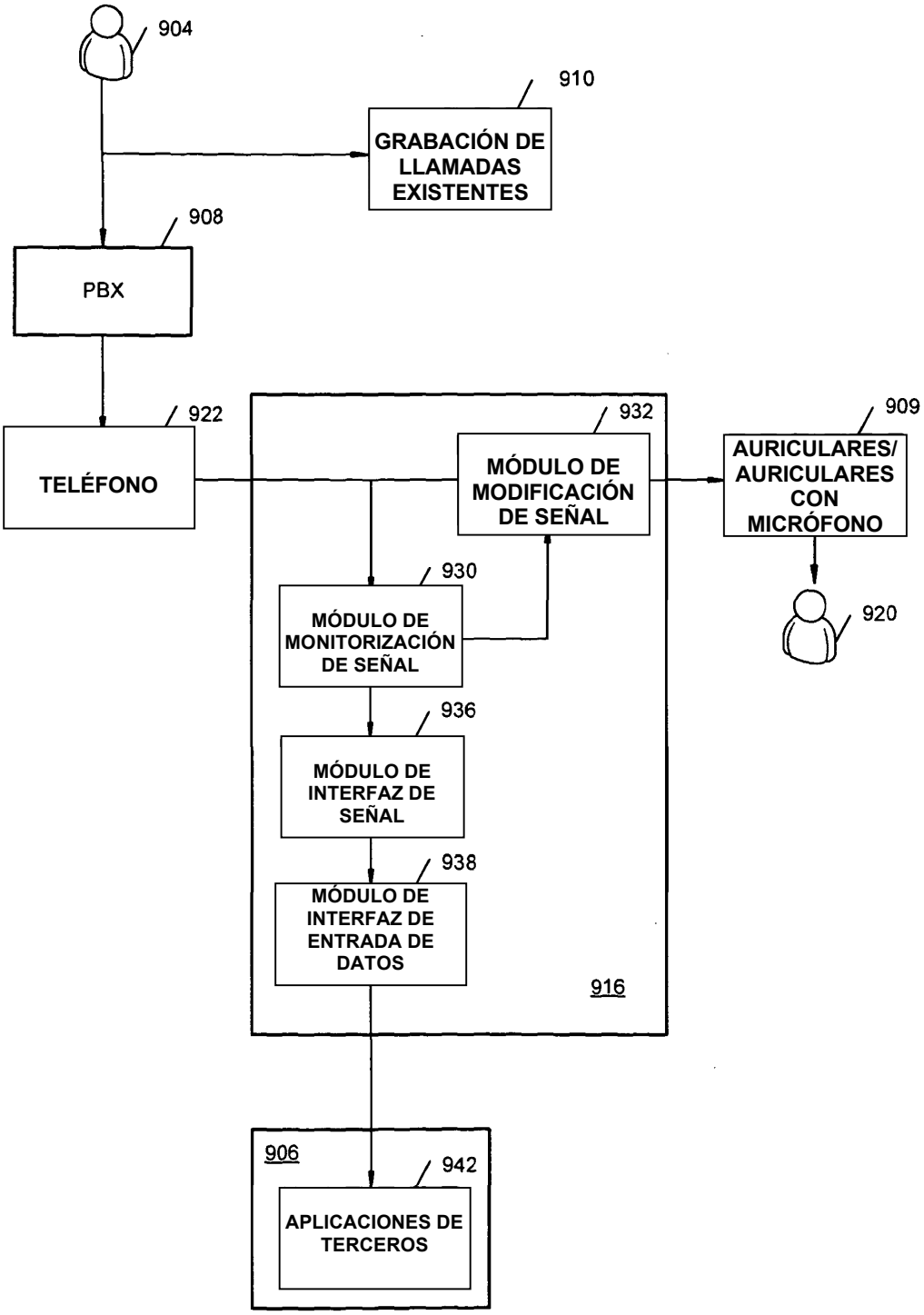
904
910
GRABACIÓN DE LLAMADAS EXISTENTES
908
PBX
922
TELÉFONO
932
MÓDULO DE MODIFICACIÓN DE SEÑAL
909
AURICULARES/ AURICULARES CON MICRÓFONO
920
930
MÓDULO DE MONITORIZACIÓN DE SEÑAL
936
MÓDULO DE INTERFAZ DE SEÑAL
938
MÓDULO DE INTERFAZ DE ENTRADA DE DATOS
916
906
942
APLICACIONES DE TERCEROS

FIGURA 9

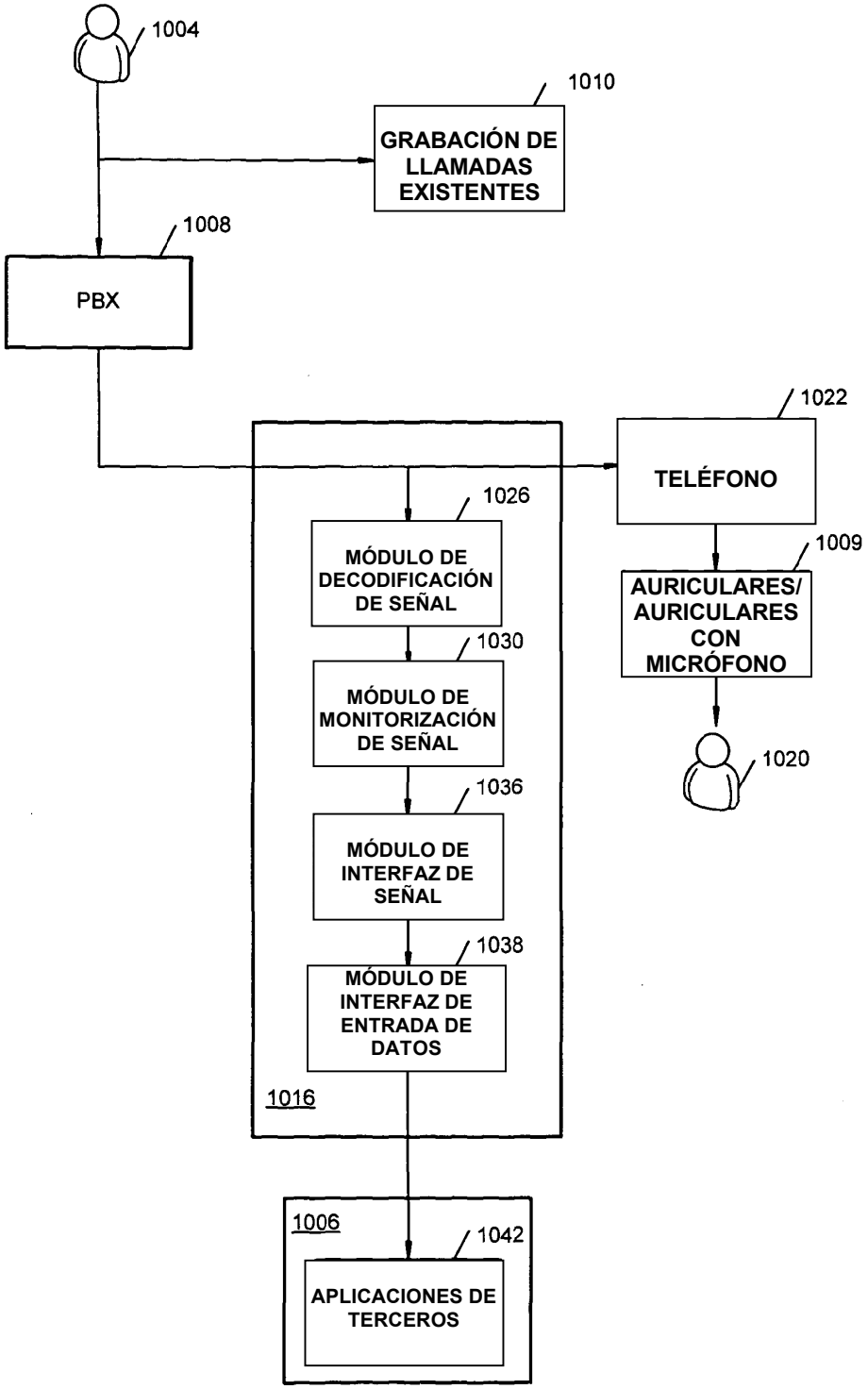
1004
1010
GRABACIÓN DE LLAMADAS EXISTENTES
1008
PBX
1022
TELÉFONO
1026
MÓDULO DE DECODIFICACIÓN DE SEÑAL
1009
AURICULARES/ AURICULARES CON MICRÓFONO
1030
MÓDULO DE MONITORIZACIÓN DE SEÑAL
1020
1036
MÓDULO DE INTERFAZ DE SEÑAL
1038
MÓDULO DE INTERFAZ DE ENTRADA DE DATOS
1016
1006
1042
APLICACIONES DE TERCEROS

FIGURA 10

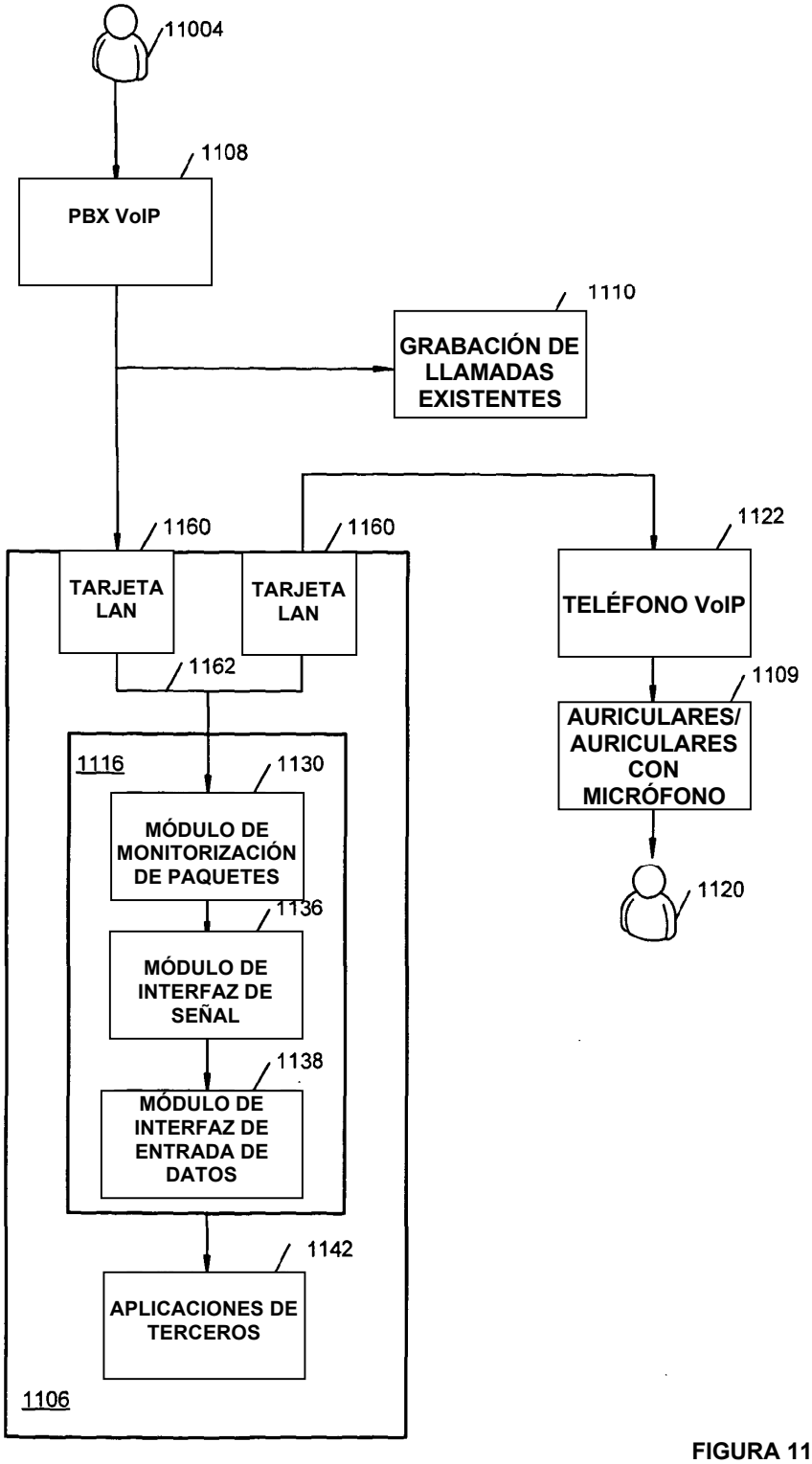
11004
1108
PBX VoIP
1110
GRABACIÓN DE LLAMADAS EXISTENTES
1160
1160
TARJETA LAN
TARJETA LAN
1162
1122
TELÉFONO VoIP
1109
AURICULARES/ AURICULARES CON MICRÓFONO
1120
1116
1130
MÓDULO DE MONITORIZACIÓN DE PAQUETES
1136
MÓDULO DE INTERFAZ DE SEÑAL
1138
MÓDULO DE INTERFAZ DE ENTRADA DE DATOS
1142
APLICACIONES DE TERCEROS
1106

FIGURA 11

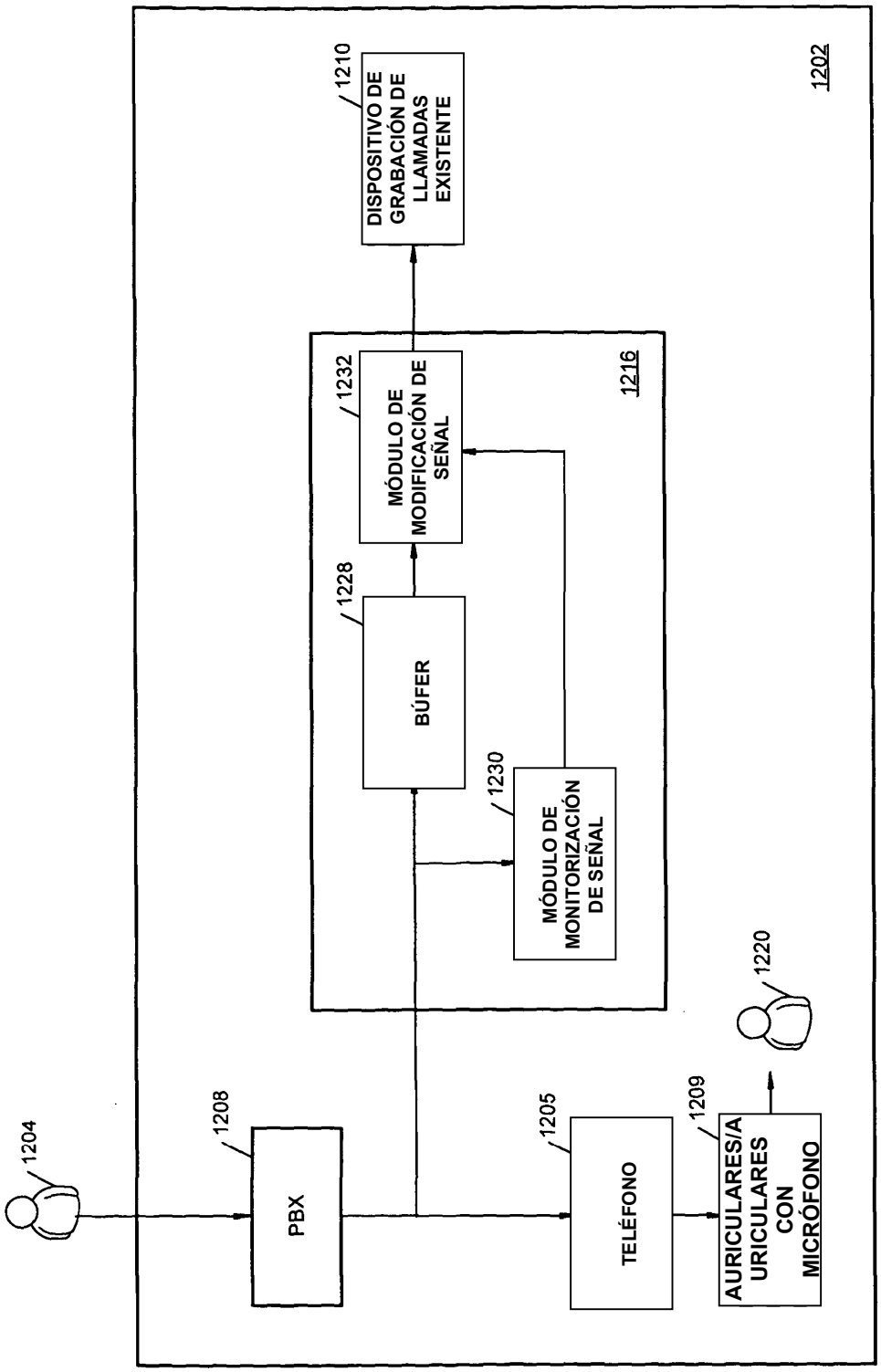
1202
1210
DISPOSITIVO DE GRABACIÓN DE LLAMADAS EXISTENTE
1216
1232
MÓDULO DE MODIFICACIÓN DE SEÑAL
1228
BÚFER
1230
MÓDULO DE MONITORIZACIÓN DE SEÑAL
1204
1208
PBX
1205
TELÉFONO
1209
AURICULARES/AURICULARES CON MICRÓFONO
1220

FIGURA 12

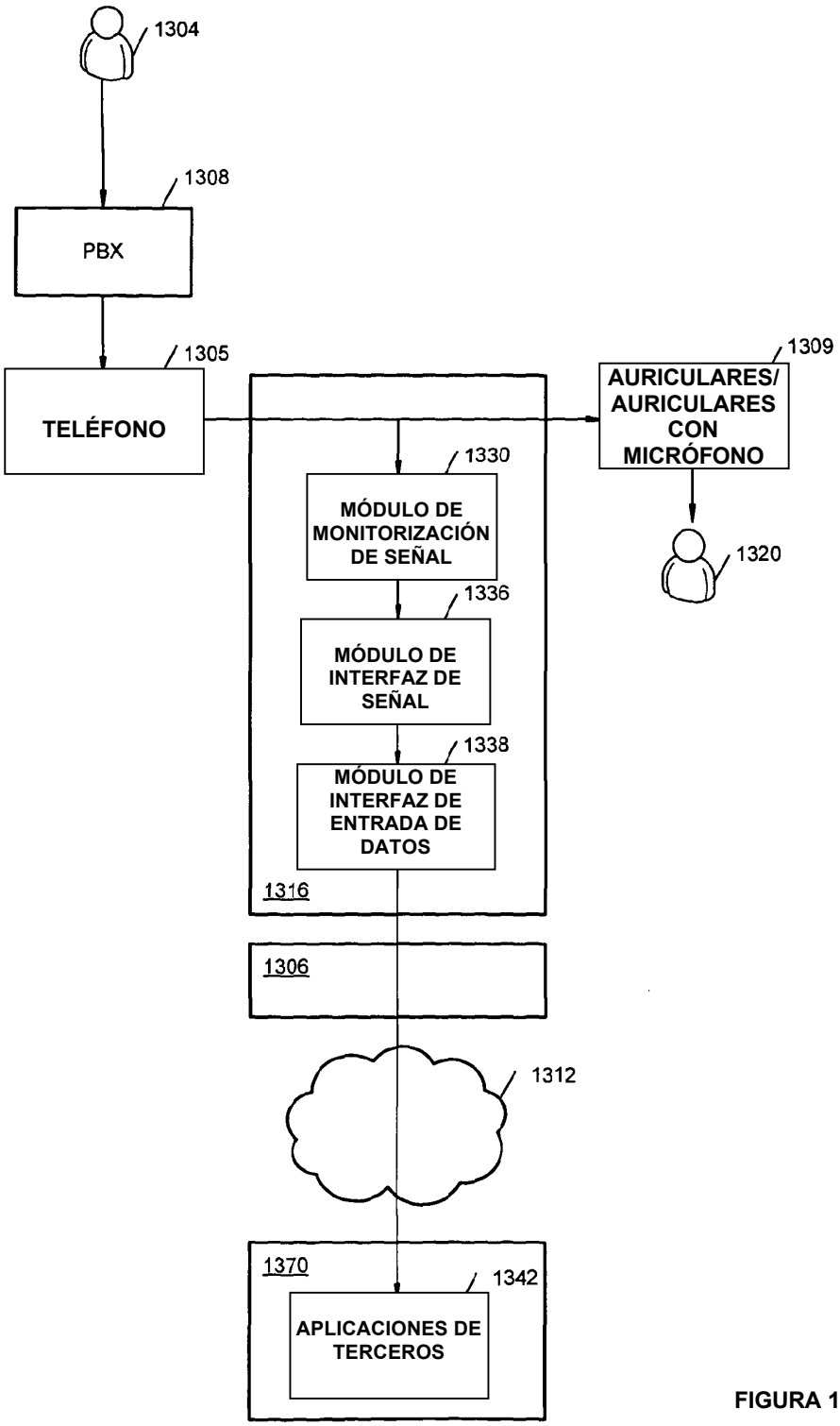
1304
1308
PBX
1305
TELÉFONO
1309
AURICULARES/ AURICULARES CON MICRÓFONO
1320
1330
MÓDULO DE MONITORIZACIÓN DE SEÑAL
1336
MÓDULO DE INTERFAZ DE SEÑAL
1338
MÓDULO DE INTERFAZ DE ENTRADA DE DATOS
1316
1306
1312
1370
1342
APLICACIONES DE TERCEROS

FIGURA 13

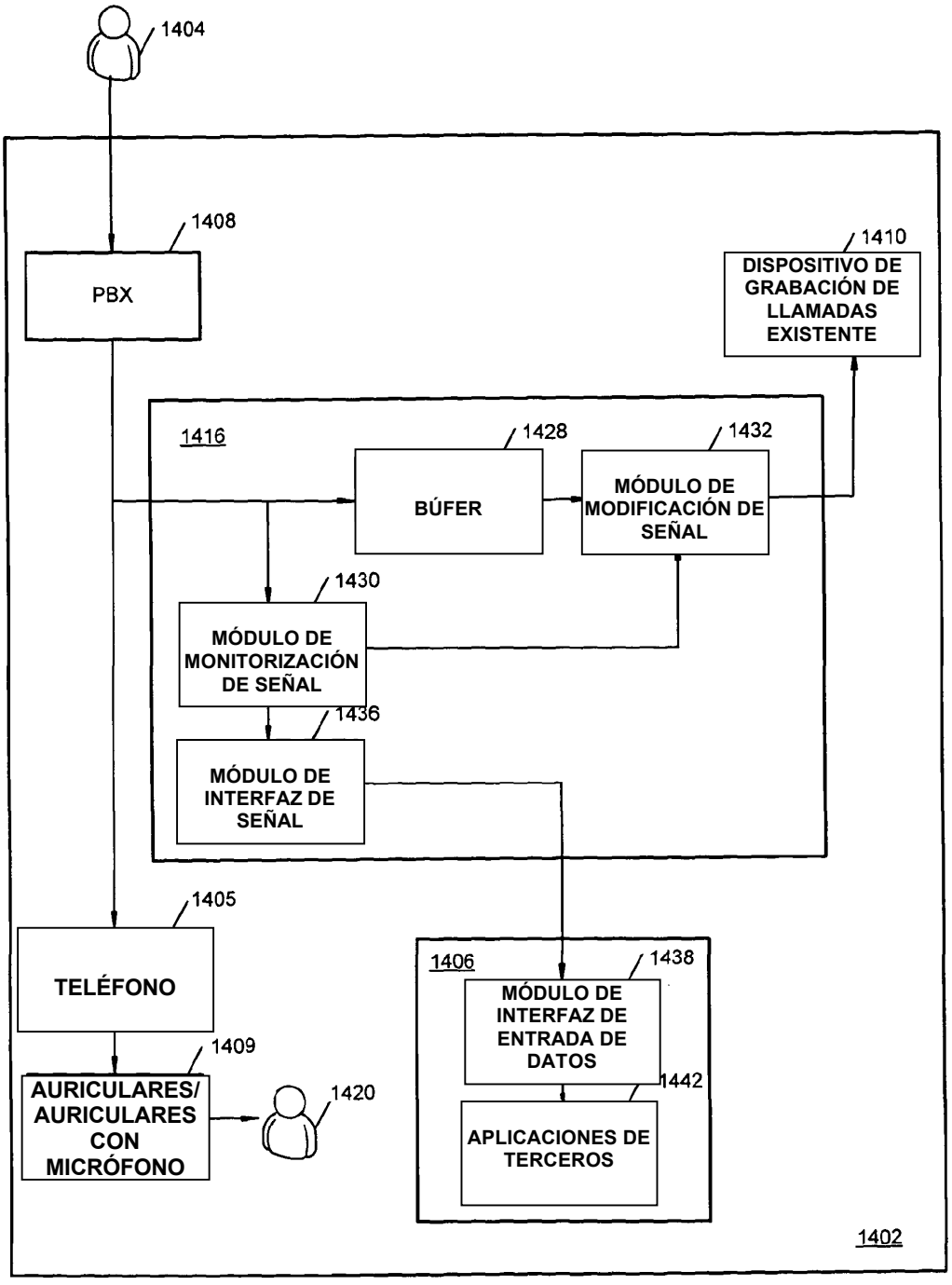
1404
1408
PBX
1410
DISPOSITIVO DE GRABACIÓN DE LLAMADAS EXISTENTE
1416
1428
BÚFER
1432
MÓDULO DE MODIFICACIÓN DE SEÑAL
1430
MÓDULO DE MONITORIZACIÓN DE SEÑAL
1436
MÓDULO DE INTERFAZ DE SEÑAL
1405
TELÉFONO
1406
1438
MÓDULO DE INTERFAZ DE ENTRADA DE DATOS
1442
APLICACIONES DE TERCEROS
1409
AURICULARES/ AURICULARES CON MICRÓFONO
1420
1402

FIGURA 14