(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 744 841**

(51) Int. CI.:

G06Q 30/00 (2012.01)
H04M 7/12 (2006.01)
H04L 29/06 (2006.01)
G06F 21/60 (2013.01)
G06F 21/34 (2013.01)
G06F 21/62 (2013.01)
H04M 3/51 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **20.12.2012 PCT/GB2012/053206**

(87) Fecha y número de publicación internacional: **27.06.2013 WO13093474**

(96) Fecha de presentación y número de la solicitud europea: **20.12.2012 E 12813080 (4)**

(97) Fecha y número de publicación de la concesión europea: **19.06.2019 EP 2795556**

(54) Título: **Método y aparato para la mediación de comunicaciones**

(30) Prioridad:

21.12.2011 GB 201122107

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
26.02.2020

(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 y
BRIDEN, THOMAS EDWARD

(74) Agente/Representante:

RIZZO , Sergio

DESCRIPCIÓN

Método y aparato para la mediación de comunicaciones

Campo de la invención

[0001] La invención se refiere, por lo general, a la mediación de comunicaciones, especialmente comunicaciones en las que se transmita información personal, confidencial o sensible de cualquier otro tipo.

Estado de la técnica

[0002] A menudo, las empresas recogen, almacenan o procesan de otro modo información relativa a individuos con el fin de proporcionar servicios y productos. Muchos países han promulgado leyes que regulan cómo debe tratarse o cómo puede utilizarse dicha información. Además, algunos organismos industriales dictan códigos de conducta y normas que deben acatar sus miembros. Un organismo industrial de este tipo es el Consejo de Normas de Seguridad para la Industria de las Tarjetas de Pago (*Payment Card Industry Security Standards Council*, PCI SSC). Este administra el Estándar de Seguridad de Datos (DSS), un marco para la gestión segura de los datos del titular de la tarjeta. El cumplimiento del PCI DSS puede suponer una carga considerable para las empresas, especialmente aquellas que realicen transacciones comerciales en nombre de clientes utilizando operaciones de centro de llamadas. Esto se debe, por una parte, a que dichas operaciones de centro de llamadas pueden requerir el acceso a los datos del titular de la tarjeta y, por otra parte, a que los requisitos de cumplimiento del PCI DSS se aplican a todos los componentes del sistema que se incluyen en el entorno de datos del titular de la tarjeta (es decir, la parte de la red que almacena, procesa o transmite los datos del titular de la tarjeta), o que están conectados a este, incluyendo componentes de red, servidores y aplicaciones.

[0003] Además, existe una creciente demanda o expectación entre las personas de ser capaz de proteger su información personal o financiera a la hora de llevar a cabo transacciones comerciales digitales con bancos u otros proveedores de servicios.

[0004] Por consiguiente, se necesitan métodos y aparatos que mejoren la forma en la que se gestiona dicha información personal, confidencial o sensible.

[0005] Otra técnica anterior se muestra en la solicitud de patente internacional WO01/02935.

Sumario

[0006] La invención se define por medio de las reivindicaciones independientes.

[0007] Un aspecto de la invención da a conocer un método de mediación de comunicaciones entre un primer dispositivo informático y un segundo dispositivo informático, mediante un dispositivo informático intermediario, comprendiendo el método el establecimiento de un enlace de comunicaciones con cada uno del primer y el segundo dispositivo informático; la recepción de un primer mensaje desde el primer dispositivo informático, comprendiendo el contenido del primer mensaje información en un formato protegido; la conversión de al menos parte de la información en el formato protegido a un formato no protegido; y la transmisión de un segundo mensaje al segundo dispositivo informático, comprendiendo el contenido del segundo mensaje al menos parte de la información en el formato no protegido.

[0008] Al implementar un dispositivo informático intermediario, por ejemplo, en forma de un ordenador físicamente separado del primer y del segundo dispositivo informático, que convierta entre formatos protegido y no protegido, el método permite proteger la información, impidiendo de este modo el almacenamiento y el uso de números de tarjeta de crédito en texto plano en el primer dispositivo informático, por ejemplo, permitiendo aun así que el segundo dispositivo informático haga uso de la información no protegida, por ejemplo, para una transacción comercial.

[0009] En función de la ubicación del dispositivo informático intermediario, la información protegida y no protegida, o ambas, se puede(n) transmitir a través de una red de área amplia o local. Por lo tanto, a modo de ejemplo, el primer y el segundo dispositivo informático, y el dispositivo informático intermediario, se pueden situar en distintas ubicaciones, y se pueden comunicar a través de una red, tal como internet. De manera alternativa, el dispositivo informático intermediario se puede situar en la ubicación del primer dispositivo informático. Los dispositivos informáticos se pueden comunicar a través de enlaces con cables, inalámbricos, o una combinación de estos. Se puede transmitir de manera segura al menos la información en el formato no protegido.

[0010] El segundo mensaje puede ser una versión modificada del primer mensaje.

[0011] En una forma de realización, el establecimiento del enlace de comunicaciones con el primer dispositivo informático incluye la recepción de una solicitud de conexión dirigida a un nombre de dominio del segundo dispositivo informático. En otra forma de realización, el establecimiento del enlace de comunicaciones con el primer dispositivo informático incluye la recepción de una solicitud de conexión dirigida a un localizador uniforme de recursos del dispositivo informático intermediario. En este sentido, el dispositivo informático intermediario se puede incorporar en el proceso con un simple cambio a una tabla de consulta de IP. Por ejemplo, la dirección IP del segundo dispositivo informático se puede sustituir por la del dispositivo informático intermediario, para que

cualquier comunicación desde el primer dispositivo informático que normalmente se transmitiría al segundo dispositivo informático se transmita, en su lugar, a través del dispositivo informático intermediario.

[0012] En una forma de realización, el establecimiento del enlace de comunicaciones con el primer dispositivo informático incluye interceptar una solicitud de conexión desde el primer dispositivo informático hasta el segundo dispositivo informático, utilizando un conjunto de una o varias reglas de comunicación predefinidas. Por lo tanto, el dispositivo informático intermediario puede actuar como un filtro de paquetes, pasando cada paquete a través de un conjunto de reglas, por ejemplo, en función del contenido de los campos de IP y encabezado de transporte del paquete. El conjunto de reglas puede soportar uno o más de entre filtrado de puerto, filtrado de dirección IP, filtrado de nombre de dominio y filtrado de dirección MAC.

[0013] En una forma de realización, el establecimiento del enlace de comunicaciones con el primer dispositivo informático incluye la identificación de una solicitud de conexión desde el primer dispositivo informático hasta el segundo dispositivo informático, entre una pluralidad de solicitudes de conexión hasta una pluralidad de dispositivos informáticos que incluyen el segundo dispositivo informático. Por lo tanto, cuando prácticamente todas las solicitudes de conexión se transmitan al dispositivo informático intermediario, las solicitudes de conexión a dispositivos informáticos que no sean el segundo dispositivo informático se pueden remitir simplemente a esos dispositivos informáticos.

[0014] En una forma de realización, el método comprende, además, la recepción de un mensaje de solicitud de información desde el segundo dispositivo informático, comprendiendo el mensaje de solicitud de información un documento electrónico que permite la entrada de información en un formato no protegido; la modificación del mensaje de solicitud de información para permitir que el documento electrónico acepte la entrada de información en un formato protegido; y la transmisión del mensaje de solicitud de información modificado al primer dispositivo informático; donde el contenido de la información del primer mensaje comprende el documento electrónico con la información en el formato protegido. Al modificar el mensaje de solicitud de información, el dispositivo informático intermediario puede asegurar que es adecuado para el primer dispositivo informático. El término documento electrónico incluye formas electrónicas editables, como una página web con uno o varios campos editables.

[0015] En una forma de realización, la modificación del mensaje de solicitud de información comprende la modificación de uno o varios campos de entrada de datos para aceptar la entrada de la información en el formato protegido. Así, se puede modificar el modo en que se muestran datos en una página web o en que esta acepta datos. Por ejemplo, la información en el formato no protegido (p. ej., el número de cuenta primario, o PAN, de 16 dígitos de la tarjeta de crédito) puede presentar una primera longitud de datos y la información en el formato protegido (p. ej., la versión cifrada del PAN de 16 dígitos de la tarjeta de crédito) puede presentar una segunda longitud de datos distinta de la primera longitud de datos. Entre otros ejemplos, se incluye la introducción de la información como al menos uno de entre un token electrónico, información cifrada e información oculta. La información se puede introducir de manera automática o manual, o mediante una combinación de ambas.

[0016] En una forma de realización, el método comprende, además, la transmisión de un mensaje de evento que comprende código legible por ordenador que, cuando lo ejecuta el primer dispositivo informático, provoca que una interfaz de usuario asociada al primer dispositivo informático muestre un dispositivo de entrada virtual. El uso de un dispositivo de entrada virtual puede impedir que los registradores de pulsaciones de teclas y otros tipos de *spyware* o *malware* registren la información si se introduce manualmente mediante el primer dispositivo informático. El dispositivo de entrada virtual puede cifrar o proteger de otro modo la información conforme se introduce.

[0017] En una forma de realización, el método comprende, además, la recepción de eventos de entrada desde el dispositivo de entrada virtual, representando los eventos de entrada información en un formato no protegido, donde el contenido del primer mensaje comprende información ficticia, y donde la conversión de al menos parte de la información en el formato protegido a un formato no protegido comprende la sustitución de al menos parte de la información ficticia por la información correspondiente recibida a través del dispositivo de entrada virtual.

[0018] En una forma de realización, el método comprende, además, bloquear la transmisión de al menos parte de la información al segundo dispositivo informático. Así, únicamente se traspasa a este información autorizada por la política de seguridad de una empresa como aceptable para su transmisión al segundo dispositivo informático. En una forma de realización, el bloqueo de la transmisión comprende determinar si el segundo dispositivo informático ha sido aprobado para recibir la información o no. Esto proporciona una «lista blanca» de dispositivos informáticos, impidiendo de este modo que un usuario del primer dispositivo informático obtenga la información en el formato protegido y simulando una transacción con un proveedor de servicios utilizando esa información en el formato protegido.

[0019] En una forma de realización, el método comprende, además, seleccionar el segundo dispositivo informático de entre una pluralidad de dispositivos informáticos. En una forma de realización, el método comprende, además, transmitir al menos parte de la información en el formato no protegido a un tercer dispositivo informático. En este sentido, cuando exista más de un dispositivo informático que sea adecuado (p. ej., que esté autorizado) para aceptar la información sensible, el dispositivo intermediario puede efectuar una

selección. Esta selección se puede basar en una lista predeterminada, que puede indicar un orden en el que se ha de realizar la selección.

[0020] En una forma de realización, el método comprende, además, la recepción de una pluralidad de primeros mensajes desde uno o varios primeros dispositivos informáticos; para cada uno de la pluralidad de primeros mensajes, la conversión de al menos parte de la información en el formato protegido a un formato no protegido; y la transmisión de uno o varios segundos mensajes al segundo dispositivo informático, comprendiendo el contenido de cada segundo mensaje al menos una parte de la información en el formato no protegido desde cada uno de dicha pluralidad de primeros mensajes. Así, la información que se origina en varios primeros dispositivos informáticos se puede agregar y transmitir al segundo dispositivo informático. Asimismo, se puede implementar también el procesamiento «por lotes» de información procedente del primer dispositivo informático.

[0021] El formato protegido puede adoptar distintas formas.

[0022] En una forma de realización, el formato protegido comprende un formato cifrado, y la conversión de al menos parte de la información del formato protegido al formato no protegido comprende el descifrado de la información. El cifrado/descifrado se puede basar en técnicas de cifrado simétrico o asimétrico. Por consiguiente, el primer dispositivo informático y el dispositivo informático intermediario pueden compartir una clave simétrica. De manera alternativa, el primer dispositivo informático puede utilizar una clave pública del dispositivo informático intermediario para cifrar la información, que puede descifrar el dispositivo informático intermediario utilizando su clave privada. De manera alternativa, el primer dispositivo informático y el dispositivo informático intermediario pueden utilizar una técnica de cifrado híbrido que haga uso de características tanto de técnicas simétricas como asimétricas. Estas restularán familiares para los expertos en la materia.

[0023] En otra forma de realización, el formato protegido comprende un token digital y la conversión de al menos parte de la información del formato protegido al formato no protegido comprende la destokenización de la información. En una forma de realización, la destokenización de la información comprende el establecimiento de un enlace de comunicaciones con un proveedor de token digital; la transmisión del token digital recibido al proveedor de token digital; y la recepción de la información en el formato no protegido desde el proveedor de token digital.

[0024] En una forma de realización, el formato protegido comprende un formato oculto, y la conversión de al menos parte de la información del formato protegido al formato no protegido comprende la no ocultación de la información.

[0025] Un aspecto de la invención da a conocer un método de mediación de comunicaciones entre un primer dispositivo informático y un segundo dispositivo informático, mediante un dispositivo informático intermediario, comprendiendo el método la recepción de un primer mensaje desde el segundo dispositivo informático, comprendiendo el contenido del primer mensaje información en un formato no protegido; la conversión de la información en el formato no protegido a un formato protegido; el establecimiento de un enlace de comunicaciones al primer dispositivo informático; y la transmisión de un segundo mensaje al primer dispositivo informático, comprendiendo el contenido del segundo mensaje al menos parte de la información en el formato protegido.

[0026] El método protege contra el hecho de que llegue información no deseada al primer dispositivo informático desde fuentes externas, incluyendo comunicaciones «planificadas» (p. ej., transacciones en sitios web que contengan información de la tarjeta de crédito) y comunicaciones «no planificadas» (p. ej., clientes que envíen correos electrónicos que contengan, por ejemplo, datos de la tarjeta de crédito, a pesar de que el correo electrónico no haya sido reconocido como un método de pago seguro).

[0027] En una forma de realización, el método comprende, además, bloquear la transmisión de al menos parte de la información al primer dispositivo informático. La información que se bloquea puede ser de un tipo que sea predeterminado.

[0028] En una forma de realización, la recepción del primer mensaje desde el segundo dispositivo informático comprende interceptar el primer mensaje utilizando un conjunto de una o varias reglas de comunicación predefinidas; y redireccionar el primer mensaje interceptado a un motor de procesamiento del dispositivo informático intermediario. En esta forma de realización, el dispositivo intermediario puede actuar como un «cortafuegos» de información, protegiendo frente al hecho de que la información sensible en un formato no protegido llegue al primer dispositivo informático.

[0029] La información no deseada podría comprender información financiera, como números de tarjeta de crédito o datos de la cuenta. A menudo, dichos números presentan un formato predeterminado (en cuyo caso, se pueden determinar mediante el uso de expresiones regulares (RegEx), comprobación del algoritmo de Luhn, etc.) y, sin embargo, en otros casos, la información sensible se puede identificar de manera heurística mediante el dispositivo informático intermediario.

[0030] En una forma de realización, el formato protegido comprende un formato cifrado, y la conversión de la información del formato no protegido al formato protegido comprende el cifrado de la información.

[0031] En una forma de realización, el formato protegido comprende un token digital, y la conversión de la información del formato no protegido al formato protegido comprende la tokenización de la información.

[0032] En una forma de realización, la tokenización de la información comprende transmitir de manera segura la información en el formato no protegido a un proveedor de token digital; y recibir un token electrónico digital como respuesta.

[0033] En una forma de realización, el formato protegido comprende un formato oculto, y la conversión de la información del formato no protegido al formato protegido comprende la ocultación de la información sensible.

[0034] En un aspecto de la invención, se da a conocer un método de procesamiento de información, comprendiendo el método la recepción, mediante un dispositivo periférico que se acopla a un terminal informático, de información en un formato no protegido, estando concebida al menos parte de la información para un dispositivo informático de destino; la conversión, por parte del dispositivo periférico, de la información a un formato protegido; la salida de la información, mediante el dispositivo periférico, en el formato protegido a una aplicación que se esté ejecutando en el terminal informático; el establecimiento, por parte del terminal informático, de un enlace de comunicaciones con un dispositivo informático intermediario; y la transmisión, mediante el terminal informático, de un mensaje al dispositivo informático intermediario, comprendiendo el mensaje al menos parte de la información en el formato protegido a un dispositivo informático intermediario, donde el dispositivo informático intermediario puede ser utilizado para convertir el formato protegido a un formato no protegido y para transmitir al menos parte de la información en el formato no protegido al dispositivo informático de destino.

[0035] Al utilizar un periférico, la información en un formato no protegido no se gestiona mediante el terminal informático.

[0036] En una forma de realización, el establecimiento del enlace de comunicaciones incluye la transmisión, al dispositivo informático intermediario, de una solicitud de conexión dirigida a un nombre de dominio del segundo dispositivo informático. En otra forma de realización, el establecimiento del enlace de comunicaciones incluye la transmisión, al dispositivo informático intermediario, de una solicitud de conexión dirigida a un localizador uniforme de recursos del dispositivo informático intermediario. En este sentido, la información en el formato protegido no se transmite directamente al segundo dispositivo informático previsto, que puede no estar configurado para procesarla en ese formato.

[0037] En una forma de realización, el método comprende, además, la recepción, mediante el terminal informático desde el dispositivo informático intermediario, de un mensaje de solicitud de información procedente del segundo dispositivo informático, comprendiendo el mensaje de solicitud de información un documento electrónico que permite la entrada de información en un formato protegido, donde la aplicación puede ser utilizada para procesar el documento electrónico.

[0038] En una forma de realización, el método comprende, además, la recepción, mediante el terminal informático desde el dispositivo informático intermediario, de un mensaje de evento que comprende un dispositivo de entrada virtual; y la visualización, en una pantalla acoplada al terminal informático, del dispositivo de entrada virtual.

[0039] En una forma de realización, el método comprende, además, la transmisión, mediante el terminal informático al dispositivo informático intermediario, de eventos de entrada procedentes del dispositivo de entrada virtual, representando los eventos de entrada información en un formato no protegido, donde la información en el formato protegido comprende información ficticia. Por consiguiente, si el teclado virtual es realmente virtual, simplemente se mostrará como una imagen de un teclado. La conversión real (esto es, la protección) de la información se lleva a cabo mediante el dispositivo informático que se ocupa del dispositivo de entrada virtual. Por consiguiente, no fluye nada de información en el formato no protegido a través del terminal informático.

[0040] Un aspecto de la invención da a conocer un método para procesar señales de una comunicación telefónica mediante un modificador de audio, transportando las señales información sensible y no sensible, destinándose la información sensible para su uso en una transacción que tenga lugar entre un primer dispositivo informático y un segundo dispositivo informático a través de un dispositivo informático intermediario, comprendiendo el método la recepción de las señales; la monitorización de las señales recibidas para detectar, en las señales, una o varias instancias de una o varias características predeterminadas que representan la información sensible; la determinación de una representación alfanumérica para cada instancia identificada de las características predeterminadas, estando las representaciones alfanuméricas determinadas en un formato no protegido; el procesamiento de las representaciones alfanuméricas para obtener las representaciones alfanuméricas en un formato protegido; la salida de las representaciones alfanuméricas en el formato no protegido al dispositivo informático intermediario; y la salida de la representación alfanumérica en el formato protegido al primer dispositivo informático y al dispositivo informático intermediario.

[0041] La señal puede ser señales de audio o VoIP que transporten tonos/paquetes DTMF que representan la información sensible. Por lo tanto, cuando se detecten tonos/paquetes DTMF en la señal, el modificador de audio los modifica conforme lo atraviesan, y sustituye un tono DTMF de entrada o un paquete de señales de VoIP por

un tono/paquete de salida (posiblemente distinto). Por lo general, se puede considerar que esto protege la información, es decir, básicamente generando un «token» que comprende los tonos DTMF o paquetes de señales de VoIP sustituidos. Otros modos de proteger la información se han examinado y aplicado ya del mismo modo en el presente documento. En este sentido, la información en formato no protegido no se transmite en absoluto al primer dispositivo informático.

[0042] El modificador de audio puede generar información directamente para aplicaciones de terceros que se ejecuten en el primer dispositivo informático utilizando, por ejemplo, comunicación IP. De manera alternativa, el modificador de audio puede generar la información para las aplicaciones de terceros que se ejecuten en el primer dispositivo informático por medio de un dispositivo independiente acoplado al primer dispositivo informático. El modificador de audio puede enviar la información no protegida (pero de un modo seguro, como HTTPS) al dispositivo informático intermediario. Sin embargo, en una forma de realización, el modificador de audio se encuentra en el dispositivo informático intermediario.

[0043] Un aspecto de la invención da a conocer un aparato para mediar comunicaciones entre un primer dispositivo informático y un segundo dispositivo informático, comprendiendo el aparato medios para establecer un enlace de comunicaciones con cada uno del primer y el segundo dispositivo informático; medios para recibir un primer mensaje desde el primer dispositivo informático, comprendiendo el contenido del primer mensaje información en un formato protegido; medios para convertir al menos parte de la información en el formato protegido a un formato no protegido; y medios para transmitir un segundo mensaje al segundo dispositivo informático, comprendiendo el contenido del segundo mensaje al menos parte de la información en el formato no protegido.

[0044] En una forma de realización, los medios para establecer el enlace de comunicaciones pueden utilizarse para recibir una solicitud de conexión desde el primer dispositivo informático dirigida a un nombre de dominio del segundo dispositivo informático.

[0045] En una forma de realización, los medios para establecer el enlace de comunicaciones pueden utilizarse para recibir una solicitud de conexión desde el primer dispositivo informático dirigida a un localizador uniforme de recursos del dispositivo informático intermediario.

[0046] En una forma de realización, el aparato comprende, además, medios para interceptar una solicitud de conexión desde el primer dispositivo informático al segundo dispositivo informático, utilizando un conjunto de una o varias reglas de comunicación predefinidas.

[0047] En una forma de realización, los medios para establecer el enlace de comunicaciones con el primer dispositivo informático se pueden utilizar para identificar una solicitud de conexión desde el primer dispositivo informático al segundo dispositivo informático, entre una pluralidad de solicitudes de conexión hasta una pluralidad de dispositivos informáticos que incluyen el segundo dispositivo informático.

[0048] En una forma de realización, el aparato comprende, además, medios para recibir un mensaje de solicitud de información desde el segundo dispositivo informático, comprendiendo el mensaje de solicitud de información un documento electrónico que permite la entrada de información en un formato no protegido; medios para modificar el mensaje de solicitud de información para permitir que el documento electrónico acepte la entrada de información en un formato protegido; y medios para transmitir el mensaje de solicitud de información modificado al primer dispositivo informático; donde el contenido de la información del primer mensaje comprende el documento electrónico con la información en el formato protegido.

[0049] En una forma de realización, el documento electrónico permite la entrada de información de manera automática y/o asistida por el usuario.

[0050] En una forma de realización, los medios para modificar el mensaje de solicitud de información se pueden utilizar para modificar uno o varios campos de entrada de datos para aceptar la entrada de la información en el formato protegido.

[0051] En una forma de realización, el aparato comprende, además, medios para transmitir un mensaje de evento que comprende código legible por ordenador que, cuando lo ejecuta el primer dispositivo informático, provoca que una interfaz de usuario asociada al primer dispositivo informático muestre un dispositivo de entrada virtual.

[0052] En una forma de realización, el aparato comprende, además, medios para recibir eventos de entrada desde el dispositivo de entrada virtual, representando los eventos de entrada información en un formato no protegido, donde el contenido del primer mensaje comprende información ficticia, y donde los medios para convertir al menos parte de la información en el formato protegido a un formato no protegido se pueden utilizar para sustituir al menos parte de la información ficticia por la información correspondiente recibida a través del dispositivo de entrada virtual.

[0053] En una forma de realización, el aparato comprende, además, medios para bloquear la transmisión de al menos parte de la información al segundo dispositivo informático.

[0054] En una forma de realización, los medios para bloquear la transmisión se pueden utilizar para determinar si el segundo dispositivo informático ha sido aprobado para recibir la información o no.

[0055] En una forma de realización, el aparato comprende, además, medios para seleccionar el segundo dispositivo informático de entre una pluralidad de dispositivos informáticos.

[0056] En una forma de realización, el aparato comprende, además, medios para transmitir al menos parte de la información en el formato no protegido a un tercer dispositivo informático.

[0057] En una forma de realización, el aparato comprende, además, medios para recibir una pluralidad de primeros mensajes desde uno o varios primeros dispositivos informáticos; medios para convertir al menos parte de la información en el formato protegido a un formato no protegido para cada uno de la pluralidad de primeros mensajes; y medios para transmitir uno o varios segundos mensajes al segundo dispositivo informático, comprendiendo el contenido de cada segundo mensaje al menos una parte de la información en el formato no protegido desde cada uno de dicha pluralidad de primeros mensajes.

[0058] En una forma de realización, el formato protegido comprende un formato cifrado, y los medios para convertir al menos parte de la información del formato protegido al formato no protegido se pueden utilizar para descifrar la información.

[0059] En una forma de realización, el formato protegido comprende un token digital, y los medios para convertir al menos parte de la información del formato protegido al formato no protegido se pueden utilizar para destokenizar la información.

[0060] En una forma de realización, los medios para destokenizar la información se pueden utilizar para establecer un enlace de comunicaciones con un proveedor de token digital; transmitir el token digital recibido al proveedor de token digital; y recibir la información en el formato no protegido desde el proveedor de token digital.

[0061] En una forma de realización, el formato protegido comprende un formato oculto, y los medios para convertir al menos parte de la información del formato protegido al formato no protegido se pueden utilizar para no ocultar la información.

[0062] Un aspecto de la invención da a conocer un aparato para mediar comunicaciones entre un primer dispositivo informático y un segundo dispositivo informático, comprendiendo el aparato medios para recibir un primer mensaje desde el segundo dispositivo informático, comprendiendo el contenido del primer mensaje información en un formato no protegido; medios para convertir la información en el formato no protegido a un formato protegido; medios para establecer un enlace de comunicaciones con el primer dispositivo informático; y medios para transmitir un segundo mensaje al primer dispositivo informático, comprendiendo el contenido del segundo mensaje al menos parte de la información en el formato protegido.

[0063] En una forma de realización, el aparato comprende, además, medios para bloquear la transmisión de al menos parte de la información al primer dispositivo informático.

[0064] En una forma de realización, los medios para recibir el primer mensaje desde el segundo dispositivo informático se pueden utilizar para interceptar el primer mensaje utilizando un conjunto de una o varias reglas de comunicación predefinidas; y redireccionar el primer mensaje interceptado a un motor de procesamiento del dispositivo informático intermediario.

[0065] En una forma de realización, el formato protegido comprende un formato cifrado, y los medios para convertir la información del formato no protegido al formato protegido se pueden utilizar para cifrar la información.

[0066] En una forma de realización, el formato protegido comprende un token digital, y los medios para convertir la información del formato no protegido al formato protegido se pueden utilizar para tokenizar la información.

[0067] En una forma de realización, los medios para tokenizar la información se pueden utilizar para transmitir la información en el formato no protegido a un proveedor de token digital; y recibir un token electrónico digital como respuesta.

[0068] En una forma de realización, el formato protegido comprende un formato oculto, y los medios para convertir la información del formato no protegido al formato protegido se pueden utilizar para ocultar la información.

[0069] Un aspecto de la invención da a conocer un aparato para procesar información, comprendiendo el aparato un terminal informático; un dispositivo periférico acoplado al terminal informático; donde el dispositivo periférico comprende medios para recibir información en un formato no protegido, estando concebida al menos parte de la información para un dispositivo informático de destino; medios para convertir la información a un formato protegido, y medios para generar la información en el formato protegido para una aplicación que se esté ejecutando en el terminal informático; y donde el terminal informático comprende: medios para establecer un enlace de comunicaciones con un dispositivo informático intermediario, y medios para transmitir un mensaje al dispositivo informático intermediario, comprendiendo el mensaje al menos parte de la información en el formato protegido para un dispositivo informático intermediario; donde el dispositivo informático intermediario puede ser

utilizado para convertir el formato protegido a un formato no protegido y para transmitir al menos parte de la información en el formato no protegido al dispositivo informático de destino.

[0070] En una forma de realización, los medios para establecer un enlace de comunicaciones se pueden utilizar para establecer el enlace de comunicaciones con el dispositivo informático intermediario mediante la transmisión de una solicitud de conexión dirigida a un nombre de dominio del segundo dispositivo informático.

[0071] En una forma de realización, los medios para establecer un enlace de comunicaciones se pueden utilizar para establecer el enlace de comunicaciones con el dispositivo informático intermediario mediante la transmisión de una solicitud de conexión dirigida a un localizador uniforme de recursos del dispositivo informático intermediario.

[0072] En una forma de realización, el terminal informático comprende, además, medios para recibir, desde el dispositivo informático intermediario, un mensaje de solicitud de información procedente del segundo dispositivo informático, comprendiendo el mensaje de solicitud de información un documento electrónico que permite la entrada de información en un formato protegido, y donde la aplicación puede ser utilizada para procesar el documento electrónico.

[0073] En una forma de realización, el terminal informático comprende, además, medios para recibir, desde el dispositivo informático intermediario, un mensaje de evento que comprende un dispositivo de entrada virtual para su visualización en una pantalla asociada al terminal informático.

[0074] En una forma de realización, el terminal informático comprende, además, medios para transmitir, al dispositivo informático intermediario, eventos de entrada procedentes del dispositivo de entrada virtual, representando los eventos de entrada información en un formato no protegido, donde la información en el formato protegido comprende información ficticia.

[0075] Un aspecto de la invención da a conocer un modificador de audio para procesar señales de una comunicación telefónica, transportando las señales información sensible y no sensible, destinándose la información sensible para su uso en una transacción que tenga lugar entre un primer dispositivo informático y un segundo dispositivo informático a través de un dispositivo informático intermediario, comprendiendo el modificador de audio medios para recibir las señales; medios para monitorizar las señales recibidas para detectar, en las señales, una o varias instancias de una o varias características predeterminadas que representan la información sensible; medios para determinar una representación alfanumérica para cada instancia identificada de las características predeterminadas, encontrándose las representaciones alfanuméricas determinadas en un formato no protegido; medios para procesar las representaciones alfanuméricas con el fin de obtener las representaciones alfanuméricas en un formato protegido; medios para generar las representaciones alfanuméricas en el formato no protegido al dispositivo informático intermediario; y medios para generar la representación alfanumérica en el formato protegido al primer dispositivo informático y al dispositivo informático intermediario.

[0076] En una forma de realización, el modificador de audio se encuentra en el dispositivo informático intermediario.

[0077] Un aspecto de la invención da a conocer un sistema que comprende los aparatos mencionados anteriormente.

[0078] Un aspecto de la invención da a conocer un método para llevar a cabo una transacción comercial, comprendiendo el método la transmisión de una solicitud desde un dispositivo informático proveedor de servicios a un terminal de usuario a través de un dispositivo informático intermediario, siendo la solicitud de información de pago en relación con la transacción comercial; la transmisión de un mensaje desde el terminal de usuario al dispositivo informático intermediario, incluyendo el contenido del mensaje información de pago en un formato protegido; la conversión de la información de pago en el formato protegido a un formato no protegido en el dispositivo intermediario; la transmisión segura de al menos parte de la información de pago en el formato no protegido desde el dispositivo informático intermediario al dispositivo informático proveedor de servicios; y la autorización de la transacción comercial en el dispositivo informático proveedor de servicios utilizando la información de pago recibida.

[0079] En una forma de realización, el terminal de usuario comprende un terminal de centro de llamadas.

[0080] En una forma de realización, la información de pago comprende información de la tarjeta de crédito o de débito.

[0081] Las formas de realización se pueden encontrar en forma de una implementación de *hardware*, una implementación de *software*, o una mezcla de ambas. Por lo tanto, cualquier «medio», «parte» y «componente» definido en el presente documento se puede implementar como módulo de códigos en diferentes combinaciones en un ordenador. Así, las formas de realización abarcan un programa informático proporcionado como un producto de programa informático en un medio de transporte que puede incluir un medio de almacenamiento y una señal o medio transitorio. El programa informático se puede almacenar en un medio de almacenamiento, tal como una memoria de estado sólido, un disco óptico, un disco magnético, o dispositivo de cinta. El programa

informático se puede proporcionar en una señal o medio transitorio en forma de una señal óptica, señal acústica, señal magnética, señal de radiofrecuencia o señal eléctrica, tal como una señal TCP/IP que transporte código a través de internet. El producto de programa informático podría estar implicado en la implementación de una forma de realización, ya sea como un conjunto completo de instrucciones ejecutables por ordenador capaces de configurar, por sí solo, el rendimiento de una o varias de las formas de realización, o como un conjunto de instrucciones vinculadas a componentes de *software* operativos ya existentes en un ordenador, para producir la configuración del ordenador de la manera deseada. El producto de programa informático puede ser directamente ejecutable, o puede precisar procesamiento local, como decodificación, descompresión o compilación, antes de encontrarse en una condición ejecutable.

[0082] Los métodos y aparatos se pueden utilizar fácilmente en operaciones de centro de llamadas. Sin embargo, se podrá apreciar que la descripción se puede aplicar a otras aplicaciones que procesan información sensible.

Breve descripción de las figuras

[0083] Otros aspectos, características y ventajas de la invención resultarán evidentes para el lector de la siguiente descripción de formas de realización específicas de la invención, expuestas únicamente a modo de ejemplo, con referencia a los dibujos adjuntos, en los cuales:

la figura 1 muestra de manera esquemática componentes de un sistema en un entorno de transacción comercial;

las figuras 2a a 2d muestran de manera esquemática flujos de datos e interacciones entre componentes del sistema de la figura 1 durante una transacción por internet;

las figuras 3a y 3b muestran de manera esquemática flujos de datos e interacciones entre componentes del sistema de la figura 1 durante una transacción de planificación de recursos empresariales (ERP, por sus siglas en inglés);

la figura 4 muestra de manera esquemática componentes de un sistema, de acuerdo con una forma de realización en la que el tráfico de red se dirige de manera selectiva a un dispositivo informático intermediario;

la figura 5 muestra de manera esquemática componentes de un sistema, de acuerdo con una forma de realización en la que prácticamente todo el tráfico de red se dirige a un dispositivo informático intermediario;

la figura 6 muestra de manera esquemática componentes de un sistema, de acuerdo con una forma de realización en la que un dispositivo informático intermediario actúa como un filtro de tráfico de red;

la figura 7 es un diagrama secuencial que muestra flujos de datos e interacciones entre componentes de un sistema, de acuerdo con una forma de realización;

las figuras 8a a 8c muestran de manera esquemática flujos de datos e interacciones entre componentes de un sistema durante una transacción en internet, de acuerdo con una forma de realización;

las figuras 9a a 9c muestran de manera esquemática flujos de datos e interacciones entre componentes de un sistema durante una transacción de planificación de recursos empresariales (ERP, por sus siglas en inglés), de acuerdo con una forma de realización;

la figura 10 es un diagrama de flujo que muestra el procesamiento del mensaje, de acuerdo con una forma de realización;

la figura 11 muestra de manera esquemática un dispositivo periférico para procesar información, de acuerdo con una forma de realización;

la figura 12 muestra de manera esquemática un modificador de audio para procesar información, de acuerdo con una forma de realización;

la figura 13 es un diagrama de flujo que muestra el procesamiento mediante el modificador de audio, de acuerdo con una forma de realización;

la figura 14 muestra de manera esquemática un aparato de procesamiento de datos del cliente, de acuerdo con una forma de realización; y

la figura 15 muestra de manera esquemática un aparato de procesamiento de datos del servidor, de acuerdo con una forma de realización.

Descripción detallada de formas de realización

[0084] La figura 1 muestra de manera esquemática componentes de un sistema 100 en un entorno de transacción comercial.

[0085] En el sistema 100, los terminales informáticos 102 de un centro de llamadas están conectados a una red interna 104, como una red Ethernet. El acceso a instalaciones informáticas externas, tales como el servidor web

106 de un proveedor de servicios (por ejemplo, bancos adquirientes («adquirientes») o proveedores de servicios de pago (PSP)), así como otros servidores 108, se proporciona a través de una red de área amplia 112, como internet, y por medio de dispositivos de enrutamiento 110.

[0086] En referencia ahora también a la figura 2, que muestra de manera esquemática ejemplos de flujos de datos e interacciones entre componentes del sistema 100 durante una transacción en internet, cuando un agente del centro de llamadas recibe una orden, ya sea por teléfono, fax, o en papel, el agente puede acceder a un sitio web del proveedor de servicios utilizando una aplicación de navegador web en uno de los terminales informáticos 102 (figura 2a). El servidor web 106 ofrece una página de pago 203 al terminal informático solicitante 102, como se muestra en la figura 2b. A continuación, el agente procede a introducir los datos de la tarjeta de crédito del cliente, por ejemplo, los números PAN y CV2 de la tarjeta de crédito (figura 2c), así como los detalles de la orden, como el nombre del cliente, la dirección, la cantidad de la orden, etc. (no representados). Posteriormente, el agente «envía» los datos (figura 2d), con el navegador enviando una solicitud «post» 205 al servidor web 106, que autoriza el pago y, en respuesta, envía detalles de confirmación al terminal informático en una nueva página web (no representada). El agente del centro de llamadas puede proporcionar entonces detalles de confirmación a la cuenta del cliente, o leer un número de confirmación al cliente a través del teléfono.

[0087] Además de transacciones en internet, el sistema 100 de la figura 1 puede incluir un sistema de planificación de recursos empresariales (ERP) o similar, que integra todos los datos y procesos en un sistema unificado. Resulta especialmente relevante para la presente descripción el hecho de que, en tales sistemas, los datos de la tarjeta se pueden encontrar en el sistema ERP desde su entrada hasta su envío. Las figuras 3a y 3b muestran de manera esquemática flujos de datos e interacciones habituales. En el presente documento, un agente recibe una orden a través del teléfono, fax o en papel, inicia el sistema ERP 105 y crea una nueva orden. (El sistema ERP 105 se puede situar en el interior o en el exterior, o una combinación de ambos, del centro de llamadas y no se muestra en la figura 1). El agente introduce los detalles de la orden (nombre, dirección, cantidad de la orden, etc.), y obtiene los datos de la tarjeta del cliente a través del teléfono (o desde una orden en fax/papel). Estos se introducen en una página de pago 303. El agente «envía» esta información al sistema ERP 105, como se muestra en la figura 3a. El sistema ERP 105 procesa la orden, enviando una solicitud de compilación/envío. Como se ha indicado anteriormente, los datos del titular de la tarjeta se pueden encontrar en el sistema ERP 105 hasta que se envía la orden. Durante el envío, el sistema ERP envía una solicitud «post» al proveedor de servicios 106 (figura 3b). Se trata de una transacción sin navegador, operando en el nivel API (o similar). El proveedor de servicios 106 autoriza el pago y envía los detalles de confirmación de vuelta al sistema ERP 105.

[0088] En el sistema 100 de la figura 1, el entorno de datos del titular de la tarjeta (las zonas en las que se almacenan, procesan o transmiten los datos del titular de la tarjeta) abarca un gran número de componentes del sistema 100. Con los requisitos PCI DSS actuales, los clientes necesitan implementar herramientas antivirus, monitorizar los puertos de acceso inalámbrico, implementar el análisis del archivo de registro y realizar pruebas de penetración externa para su entorno de datos del titular de la cuenta. Asimismo, a las empresas que procesan más de 6 millones de pagos con tarjeta al año se les solicita que contraten a un asesor de seguridad calificado (QSA, por sus siglas en inglés) para llevar a cabo una auditoría de seguridad de su entorno de datos del titular de la cuenta.

[0089] Dos métodos para proteger información sensible en los que esta se almacena o se transmite son la tokenización y el cifrado. Estos dos enfoques reducen el «ámbito» de almacenamiento (en este contexto, el «ámbito» es definido por el PCI DSS como sistemas que almacenan, procesan y transmiten datos del titular de la cuenta y sistemas conectados). También limitan el riesgo de pérdida de información sensible, y los costes de auditoría/cumplimiento por garantizar la seguridad de la información sensible almacenada. En la tokenización, por ejemplo, los proveedores de servicios emiten tokens, lo cual significa que una empresa puede enviar datos de la tarjeta una vez, y utilizar un token para cada transacción posterior. No obstante, este enfoque sigue necesitando el procesamiento de datos no protegidos de la tarjeta en el sitio de la empresa para la transacción inicial, haciendo así que la empresa quede incluida en el ámbito de aplicación de los requisitos PCI DSS. Además, el hecho de implementar la tokenización o el cifrado en sistemas ya existentes puede resultar complejo desde el punto de vista técnico. Esto se debe a que muchos proveedores de servicios no aceptan tokens ni números de tarjeta cifrados como un artículo de transacción válido; únicamente se acepta el número completo de la tarjeta de crédito (el PAN) y los datos de comprobación de seguridad CV2 durante una transacción.

[0090] El sistema 100 de la figura 1 tampoco limita la introducción involuntaria de información sensible en el sistema, es decir, no analiza los datos para detectar datos sensibles que se envíen (o se reciban) y que infrinjan las políticas de seguridad de una empresa. Los denominados sistemas de prevención de pérdida de datos (PPD, o DLP por sus siglas en inglés) registran que se ha enviado información sensible (sin detener la transmisión), o bien detienen por completo la transmisión. Este enfoque resulta inapropiado para los clientes que quieren permitir la transmisión, pero también proteger/asegurar los datos que se envían o reciben para que no constituya una violación de su política de seguridad. También resulta inapropiado para las empresas que desean permitir que continúe una transacción de entrada, pero también proteger los datos sensibles para que los puedan utilizar dentro del entorno las partes autorizadas (por ejemplo, en un entorno médico en el que los datos médicos personales necesiten ser almacenados, pero no utilizados, por parte del personal administrativo del hospital,

aunque sí necesiten ser utilizados por los médicos). Además, los sistemas DLP suelen ser complejos de implementar y monitorizar, y a menudo resultan muy costosos.

[0091] Además de la entrada involuntaria de información sensible, las empresas pueden obtener de manera activa información sensible de los clientes a partir de una fuente externa a su negocio, almacenarla internamente y transmitirla a continuación externamente en una fecha posterior. A modo de ejemplo, una empresa puede querer registrar los datos de la tarjeta de crédito de un cliente a través de un sitio web, llevar esa información de la tarjeta a su sistema de orden interno, y a continuación obtener un pago mensual de la tarjeta de crédito del cliente para un servicio de suscripción. Como se ha indicado anteriormente, este enfoque sigue necesitando el procesamiento de datos no protegidos de la tarjeta en el sitio de la empresa para la transacción inicial, haciendo así que el cliente quede incluido en el ámbito de aplicación de los requisitos PCI DSS.

[0092] La figura 4 muestra de manera esquemática componentes de un sistema, de acuerdo con una forma de realización en la que el tráfico de red se dirige de manera selectiva a un dispositivo informático intermediario.

[0093] El sistema 400 de la figura 4 incluye terminales informáticos 402 (únicamente se representa uno) de un centro de llamadas conectado a una red interna (no representada a efectos de claridad). El acceso a instalaciones informáticas externas, tales como el servidor web 406 de un proveedor de servicios, así como otros servidores web 408, se proporciona de nuevo a través de una red de área amplia 412, como internet, y por medio de dispositivos de enrutamiento 410. Sin embargo, el acceso al servidor web 406 del proveedor de servicios se facilita ahora mediante un servidor *proxy* 401. El servidor *proxy* se muestra de manera externa, aunque puede ser interno o externo, con direcciones IP de 192.168.1.99 o 10.0.0.1, por ejemplo, respectivamente. También se muestra en la figura 4 un servidor 403 para distribuir tokens digitales (y, en algunos casos, para convertir los tokens digitales), accesible tanto para el terminal informático 402 como para el servidor *proxy* 401 a través de la red de área amplia 412 (aunque, en aras de la claridad, la ruta de comunicación se muestra separada de esta).

[0094] Supongamos que el servidor web 406 con nombre de dominio «www.acquirer.com» está en la dirección IP 1.2.3.4 y que el servidor *proxy* 401 («www.proxy.com») está en la dirección IP 10.0.0.1. En este caso, cuando el agente del centro de llamadas accede a «www.acquirer.com» en un navegador, se establece una conexión desde el terminal informático 402 (como se describirá más adelante) al servidor *proxy* 401 en lugar de al servidor web 406, utilizando, por ejemplo, protocolo seguro de transferencia de hipertexto (HTTPS) para que las comunicaciones estén totalmente cifradas. En una forma de realización, el nombre de dominio «www.proxy.com» presenta un certificado de capa de puertos seguros (SSL) generado empleando el nombre de dominio «www.acquirer.com». Este podría ser un certificado SSL autofirmado X.509 (archivo .crt) en nombre de «www.acquirer.com» por ejemplo (X.509 es un estándar para una infraestructura de clave pública (PKI) y para una infraestructura de gestión de privilegios (PMI) del sector de normalización de las telecomunicaciones de la Unión Internacional de Telecomunicaciones (UIT)). El certificado .crt generado se registra en el servidor *proxy* 401 en la dirección IP 10.0.0.1.

[0095] Por lo tanto, cualquier conexión del navegador a «www.proxy.com» verá un certificado SSL válido, y determinará que el localizador uniforme de recursos (URL) solicitado, es decir, «www.proxy.com», coincide con el dominio del certificado. Sin embargo, debido a que el servidor *proxy* 401 puede ser un emisor de certificado que no sea de confianza, el centro de llamadas puede añadir el certificado proporcionado del servidor *proxy* 401 a una lista de confianza. Así, el centro de llamadas puede configurar todos los terminales informáticos 402 que normalmente se conectarían a «www.acquirer.com» para aceptar un certificado de confianza proporcionado por el servidor *proxy* 401, navegando individualmente a «www.acquirer.com» y aceptando posteriormente el certificado .crt como un certificado de confianza, o bien mediante la implementación masiva del certificado .crt en todos los terminales informáticos pertinentes 402 en el centro de llamadas. A continuación, el servidor DNS interno del centro de llamadas se modifica para que las comunicaciones dirigidas a «www.acquirer.com» se enruten a 10.0.0.1, o bien se implementa un archivo *host* local en terminales informáticos pertinentes 402 para que las comunicaciones dirigidas a «www.acquirer.com» (proveedor de servicios 406) se enruten en cambio al servidor *proxy* 401 en 10.0.0.1.

[0096] En este sentido, y con referencia también a la figura 7, cuando el terminal informático 402 solicita una conexión segura a «www.acquirer.com», la solicitud de conexión se enruta a 10.0.0.1 (es decir, al servidor *proxy* 401). El terminal informático 402 verifica el certificado SSL del servidor *proxy* 401. Dado que este certificado se ha marcado como «de confianza», la conexión SSL se establece entre el terminal informático 402 y el servidor *proxy* 401

[0097] (S702). Cuando el servidor *proxy* 401 recibe la solicitud de conexión, este comprueba la solicitud para el *host* al que el terminal informático 402 trata realmente de conectarse, es decir, «www.acquirer.com», recupera su dirección IP (1.2.3.4) desde un DNS externo e inicia una conexión con «www.acquirer.com» (S704). El sistema proveedor de servicios 406 proporciona esta conexión con su propio certificado HTTPS. A modo de ejemplo, el servidor *proxy* 401 solicita una conexión segura a «www.acquirer.com». El DNS local o externo enruta la solicitud a la dirección IP de «www.acquirer.com» (es decir, 1.2.3.4). Posteriormente, el servidor *proxy* 401 verifica el certificado SSL del proveedor de servicios. Si este certificado ha sido firmado por una autoridad de certificación (CA) de confianza y coincide con la URL del servidor, la conexión SSL se establece entre 10.0.0.1 y el adquiriente (S706). En este momento, todo lo que se recibe desde el terminal informático 402 en el servidor

proxy 401 se puede reflejar en el servidor proveedor de servicios 406, y viceversa. Por consiguiente, las «*cookies*» y los inicios de sesión funcionan como siempre, pero el servidor *proxy* 401 actúa como un «intermediario», y puede ver todo desde ambas conexiones en texto plano, para la manipulación necesaria.

[0098] Antes de proceder con una explicación del resto de procesos mostrados en la figura 7, se describirán otras formas de realización para implementar el sistema.

[0099] En la forma de realización que se acaba de describir, el DNS dirige algunas comunicaciones al servidor *proxy* 401. En otra forma de realización, las URL que utilizan los terminales informáticos 402 se modifican. Para todas las aplicaciones que utilizarían normalmente la URL «www.acquirer.com», el centro de llamadas configura en cambio la URL a «acquirer.proxy.com». Al igual que antes, se obtiene un certificado X.509 SSL (archivo .crt) en nombre de acquirer.proxy.com a partir de un CA de confianza y se registra en el servidor *proxy* 401. Para los terminales informáticos 402 que acceden a «www.acquirer.com», la URL se modifica a «acquirer.proxy.com». Así, cuando el terminal informático 402 solicita una conexión segura a «acquirer.proxy.com», este comprueba el certificado SSL del servidor *proxy* 401. Como este certificado ha sido emitido por una CA de confianza y coincide con la URL del servidor, se establece una conexión SSL entre terminales informáticos 402 y el servidor *proxy* 401 (S702), sin que se muestren avisos ni mensajes de error al usuario. En esta forma de realización, no existen cambios necesarios para los certificados aceptados por los terminales informáticos 402, ya que la URL «acquirer.proxy.com» con la que se comunican coinciden en realidad con la URL en el certificado. El servidor *proxy* 401 modifica ahora todas las solicitudes para «acquirer.proxy.com», por lo que el tráfico se envía a «www.acquirer.com» (S704). Para establecer una conexión segura con el servidor proveedor de servicios 406, el servidor *proxy* 401 solicita una conexión segura con «www.acquirer.com». Un DNS local o externo enruta esta solicitud a la dirección IP del servidor proveedor de servicios 406 (p. ej., 1.2.3.4). El servidor *proxy* 401 verifica el certificado SSL de «www.acquirer.com», y si este certificado ha sido firmado por un CA de confianza y coincide con la URL del servidor, se puede establecer una conexión SSL entre el servidor *proxy* 401 y el servidor 406 (S706). Los mensajes se pueden enviar de nuevo desde «www.acquirer.com» al terminal informático 402 a través del servidor *proxy* 401, pero, en esta ocasión, todas las repeticiones del texto «www.acquirer.com» contenidas en la comunicación desde «www.acquirer.com» se modifican a «acquirer.proxy.com» para que el navegador/sistema ERP no cambia entonces a «www.acquirer.com» y no utiliza el *proxy* para una futura comunicación (ya que, en esta forma de realización, los centros de llamada no han cambiado el DNS).

[0100] En una forma de realización, representada en la figura 5, prácticamente todas las solicitudes de conexión procedentes de los terminales informáticos 502 se enrutan a través del servidor *proxy* 501. En concreto, el acceso tanto al servidor web 508 como al servidor proveedor de servicios 506 se facilita a través del servidor *proxy* 501, mediante una red de área amplia 512, como internet y dispositivos de enrutamiento 510. El servidor *proxy* se muestra de manera externa o interna, con direcciones IP de 192.168.1.99 o 10.0.0.1, por ejemplo, respectivamente. El centro de llamadas configura todas las comunicaciones en internet que se enrutan a través del servidor *proxy* 501. En esta forma de realización, un certificado SSL autofirmado X.509 (archivo .crt) se genera en nombre de «www.acquirer.com», que se registra en el servidor *proxy* 501. El certificado .crt se añade como un certificado de confianza en los terminales informáticos pertinentes 502, navegando individualmente a «www.acquirer.com» y aceptando posteriormente el certificado .crt como un certificado de confianza, o bien mediante la implementación masiva del certificado .crt en todos los terminales informáticos pertinentes 502 en el centro de llamadas. Cuando el terminal informático 502 solicita una conexión segura a «www.acquirer.com», esta solicitud (junto con prácticamente todas las otras solicitudes de conexión) se enruta al servidor *proxy* 501. El servidor *proxy* 501 intercepta la solicitud de conexión HTTPS, «examinando» los paquetes que se dirigen a «www.acquirer.com», y esta se enruta a una dirección IP local del servidor *proxy* 501 (p. ej., 127.0.0.1). Por consiguiente, en esta forma de realización, la determinación del destino (S704) se puede llevar a cabo antes de que se establezca la conexión. El terminal informático 502 verifica el certificado SSL del servidor *proxy*. Este certificado se ha marcado como «de confianza» y se establece la conexión SSL entre el terminal informático 502 y el servidor *proxy* 501 (S702). Los paquetes interceptados se redirigen de manera interna a una dirección IP local, como 127.0.0.1, mientras que todo el resto del tráfico se envía a su destino previsto de la misma manera que un servidor *proxy* convencional. El servidor *proxy* 501 en 127.0.0.1 hospeda una aplicación de *proxy* que, a continuación, crea la conexión con el servidor proveedor de servicios 506. Por ejemplo, cuando el servidor *proxy* 501 solicita conexión segura con el servidor proveedor de servicios 506, un DNS local o externo enruta esta solicitud a la dirección IP del servidor proveedor de servicios 506 (p. ej., 1.2.3.4). El servidor *proxy* comprueba el certificado SSL en «www.acquirer.com». Este certificado ha sido firmado por una autoridad de certificación (CA) de confianza, coincide con la URL del servidor, y la conexión SSL se establece entre 10.0.0.1 y el servidor proveedor de servicios 506 (S706). En esta forma de realización, el cambio a la infraestructura de tecnología de la información del centro de llamadas comprende el enrutamiento de todo el tráfico de internet a través de la dirección IP del servidor *proxy* 192.168.1.99 o 10.0.0.1. En otras palabras, las direcciones web y los ajustes DNS se mantienen invariables. Si el servidor *proxy* 501 se aloja en el centro de llamadas, este enfoque no elimina necesariamente los datos del titular de la tarjeta del entorno del centro de llamadas. Sin embargo, reduce de manera significativa el entorno de datos del titular de la tarjeta sin introducir una parte remota en el proceso de procesamiento de la tarjeta.

[0101] En una forma de realización, representada en la figura 6, el servidor *proxy* 601 comprende un filtro de paquetes, por ejemplo, insertado en las comunicaciones de internet de salida del centro de llamadas. En una forma de realización, el filtro de paquetes 601 presenta dos puertos LAN separados (representados por los círculos sólidos), que están puenteados internamente. Cuando el terminal informático 602 solicita una conexión segura a «www.acquirer.com», la solicitud de conexión es interceptada por el filtro de paquetes 601, examinando los paquetes que se dirigen a ese destino (S704). Estos paquetes se redirigen a 127.0.0.1, que hospeda una aplicación de *proxy*. A continuación, la aplicación de *proxy* suplanta la dirección IP del terminal informático 602 y solicita una conexión segura al servidor proveedor de servicios 606, que se enruta mediante un DNS local o externo a la dirección IP del servidor proveedor de servicios 606 (p. ej., 1.2.3.4) (S706). Todos los dispositivos que normalmente se conectarían al servidor proveedor de servicios 606 están configurados para aceptar un certificado generado por el filtro de paquetes. Al igual que antes, un certificado SSL autofirmado X.509 (archivo .crt) se puede generar en nombre de «www.acquirer.com». Este se registra en el filtro de paquetes. De nuevo, el certificado .crt se puede añadir como un certificado de confianza en los terminales informáticos pertinentes 602, navegando individualmente a «www.acquirer.com» y aceptando posteriormente el certificado .crt como un certificado de confianza, o bien mediante la implementación masiva del certificado .crt en todos los terminales informáticos pertinentes 602 en el centro de llamadas. (En otros casos, el certificado raíz del servidor *proxy* se puede añadir al almacenamiento de confianza para que cualquier certificado generado por el servidor *proxy* sea de confianza. Esto se debe a que el servidor *proxy* puede estar interceptando en realidad todas las conexiones HTTPS en lugar de únicamente las que van a «www.acquirer.com» y, por lo tanto, necesitaría generar certificados para esos otros sitios también). Por consiguiente, cuando el terminal informático 602 verifica el certificado SSL en el filtro de paquetes, debido a que este certificado se ha marcado como «de confianza», la conexión SSL se establece entre terminal informático 602 y filtro de paquetes 601. A continuación, el filtro de paquetes verifica el certificado SSL del servidor proveedor de servicios 606 y, si este certificado ha sido firmado por un CA de confianza y coincide con la URL del servidor, se puede establecer una conexión SSL entre el filtro de paquetes y el servidor proveedor de servicios 606. Al contrario que el servidor *proxy in situ* 501 de la forma de realización anterior, el filtro de paquetes no presenta una dirección IP *per se*, de manera que, si no se acoplan conectores de red adicionales, como cables LAN, al filtro de paquetes, no se puede dirigir mediante cualquier dispositivo en el interior o en el exterior del sitio del centro de llamadas. Esto impide la modificación, el control o el acceso al filtro de paquetes. No se necesitan cambios para el DNS del centro de llamadas ni para direcciones web.

[0102] La descripción expuesta anteriormente ha proporcionado ejemplos de cómo se puede establecer una conexión entre los terminales de cliente y el proveedor de servicios, a través de un dispositivo informático intermediario. A continuación, la descripción se centra en los tipos de mensajes e información que se puede transmitir entre el servidor proveedor de servicios y los terminales informáticos.

[0103] Volviendo a la figura 7, en respuesta al establecimiento de una solicitud de conexión procedente del terminal informático, el proveedor de servicios puede enviar un mensaje de respuesta (S708) al terminal informático a través del servidor *proxy*. En el bloque S710, el servidor *proxy* procesa el mensaje de respuesta. El procesamiento puede incluir la modificación del mensaje. Por ejemplo, como se ha descrito en referencia a la figura 4, el servidor *proxy* puede modificar todas las repeticiones del texto «www.acquirer.com» a «acquirer.proxy.com» para que el *proxy* no esté omitido para futuras solicitudes. De manera más general, el mensaje se puede modificar para cambiar la función y/o las propiedades del mensaje. Por ejemplo, cuando el mensaje de respuesta comprende un documento electrónico como una página web, el servidor *proxy* puede insertar, sustituir, eliminar y/o manipular de otro modo el mensaje para controlar qué contenido se muestra y/o cómo se muestra el contenido. Por consiguiente, se podría modificar una página de pago para aceptar el PAN de 16 dígitos en un formato cifrado más largo. El mensaje de respuesta modificado se envía posteriormente al terminal informático (S712). En el bloque S714, se introduce la información sensible y se convierte a un formato protegido. Tal y como se explicará en su momento, el terminal informático puede presentar un dispositivo de codificación independiente que se utiliza para proteger la información sensible. En otros casos, cuando se implementa un proveedor de token digital, el terminal informático puede solicitar un token digital e insertar el token digital recibido. La información sensible en el formato protegido se transmite a continuación al servidor *proxy* (S716). La información sensible en el formato protegido se puede transmitir de manera segura al servidor *proxy*. En otras palabras, la información sensible en el formato protegido puede estar cifrada en sí misma, por ejemplo, mediante HTTPS. En el bloque S718, el mensaje se procesa mediante el servidor *proxy*. Esto incluye la conversión de la información sensible en el formato protegido al formato no protegido. En caso de que se implemente un servidor de token digital, el servidor *proxy* puede enviar el token digital recibido al servidor de token digital para obtener la información sensible no protegida. Al menos una parte de la información sensible en el formato no protegido se transmite a continuación al servidor proveedor de servicios (S720). Al enviar dicha información a través de una red de área amplia, esta se puede transmitir de manera segura. En el bloque S722, la información sensible se procesa a continuación.

[0104] Las figuras 8a a 8c muestran de manera esquemática flujos de datos e interacciones entre componentes de un sistema durante una transacción en internet, de acuerdo con una forma de realización. Al igual que antes, se podría recibir una orden a través del teléfono, por fax o en papel. El agente abre un navegador y navega por «www.acquirer.com». Como se muestra en la figura 8a, se envía una solicitud de conexión para

«www.acquirer.com» desde el terminal del agente 802 al servidor *proxy* 801, debido a que la tabla de consulta de IP ha sido alterada (como se ha descrito anteriormente con referencia a la figura 4). El servidor *proxy* 801 examina la solicitud del agente. No se detectan palabras clave/frases/sustituciones, por lo que la solicitud se transmite sin modificar al servidor proveedor de servicios 806.

[0105] Como se muestra en la figura 8b, el servidor proveedor de servicios 806 proporciona una página de pago 803 al servidor *proxy* 801. Al observar que existe una definición html de un campo de entrada del número de tarjeta de crédito, el servidor *proxy* 801 modifica el código html para permitir una entrada de 128 caracteres (anteriormente se permitían únicamente 16 caracteres). El servidor *proxy* 801 modifica también el campo CV2 de 3 dígitos para permitir una entrada de 128 caracteres. (Los campos se pueden modificar también para ocultar los datos en la pantalla, para que se muestren asteriscos en lugar de los datos subyacentes). La página completa modificada 805 se transmite ahora al terminal informático 802. Si la orden se toma manualmente en papel, el agente puede introducir los datos de la tarjeta utilizando un teclado numérico cifrado. Si la orden se toma a través del teléfono, el cliente puede introducir los datos de su tarjeta en el teclado numérico de su teléfono, y utilizarse un decodificador para convertir tonos DTMF en pulsaciones de teclas cifradas.

[0106] Cuando el agente «envía» la información de la solicitud, el navegador del terminal informático 802 envía una solicitud «post» a «www.acquirer.com» (figura 8c). El servidor *proxy* 801 recibe la solicitud «post», y examina la solicitud. Al ver datos de la tarjeta cifrados, se descifra y se recompone la solicitud «post» con datos de la tarjeta no cifrados, antes de pasar al servidor 806 del proveedor de servicios, el cual, a su vez, autoriza el pago y envía detalles de confirmación de vuelta al terminal informático 802 en una nueva página web (no representada). El agente puede confirmar entonces los detalles con una cuenta de cliente, o dictar un número de confirmación al cliente a través del teléfono.

[0107] Las figuras 9a a 9c muestran de manera esquemática flujos de datos e interacciones entre componentes de un sistema durante una transacción de planificación de recursos empresariales (ERP), de acuerdo con una forma de realización. En esta forma de realización, el agente inicia el sistema CRM/ERP y crea una nueva orden escribiendo los detalles de la orden (nombre, dirección, cantidad solicitada, etc.) y, si la orden se toma a través del teléfono, pide que el cliente introduzca el PAN utilizando el teclado numérico de su teléfono. Se puede configurar un decodificador en el terminal informático del agente para detectar tonos DTMF, convertirlos en valores numéricos y cifrarlos. De manera alternativa, si la orden se toma manualmente en papel, el agente introduce el PAN utilizando un teclado numérico cifrado. Se da el mismo proceso para el CV2. Los datos de la tarjeta cifrados se envían posteriormente al servidor *proxy* o a otro servidor (no representado), que devuelve un token para el PAN (por ejemplo, «1111222233334444»). El token se introduce automáticamente en el campo PAN, y los datos de CV2 ficticios (por ejemplo, «000») se introducen en el campo CV2. El token y el CV2 ficticio (no datos del titular de la tarjeta) se pueden enviar al sistema ERP 907, donde se almacenan hasta que se expide la orden (figura 9a).

[0108] Durante el envío, el sistema ERP 907 envía una solicitud «post» al servidor *proxy* 901. Se trata de una transacción sin navegador, que opera en el nivel de API (o similar). El token y el CV2 ficticio se envían en lugar del número y el CV2 real de la tarjeta (aunque cabe destacar que no se requieren cambios en el sistema ERP, ya que el token puede presentar el mismo formato que un número de tarjeta de crédito). El servidor *proxy* destokeniza el PAN y recupera el CV2 de una tabla de consulta.

[0109] Como se muestra en la figura 9c, los números PAN y CV2 reales se sustituyen a continuación en la comunicación antes de enviarlos al servidor proveedor de servicios 906, que autoriza el pago y envía detalles de confirmación de vuelta a www.proxy.com para enviarlos de vuelta al cliente (no representado). A continuación, el servidor *proxy* elimina de manera segura su registro del CV2, ya que se ha completado la autorización. Opcionalmente, el PAN se puede conservar para una futura destokenización (p. ej., para un reembolso o para el pago periódico de una suscripción). El proceso de ERP continúa posteriormente de manera normal (facturación, envío, etc.).

[0110] La figura 10 es un diagrama de flujo que muestra el procesamiento del mensaje mediante el servidor *proxy*, de acuerdo con una forma de realización. Esta forma de realización se presenta en el contexto del protocolo de control de transmisión (TCP), aunque se podrá observar que los principios generales se pueden utilizar para otros protocolos, como el protocolo de datagramas de usuario (UDP) y el protocolo de transmisión para el control de flujo (SCTP). En aras de una mayor claridad, algunos procesos no aparecen representados.

[0111] Como resultará familiar para los expertos en la materia, el TCP acepta datos de una corriente de datos, los segmenta en grupos, y añade un encabezado TCP que crea un segmento TCP. El bloque S1002 implica recibir un segmento de datos. En el ejemplo de forma de realización, el segmento de datos comprende un «grupo» de segmento TCP. En el bloque S1004, los segmentos de datos recibidos se almacenan en búfer mediante el servidor *proxy*. En esta forma de realización, los grupos de datos se almacenan en búfer hasta que se recibe un segmento TCP completo. En el bloque S1006, las señales se revisan en busca de información predeterminada. Por ejemplo, los datos de TCP contienen cualquier cosa que se envía a través de TCP, y pueden incluir HTTP (página web convencional) (esta presenta encabezados de HTTP y datos de HTTP), HTTPS (página web cifrada) y VPN (tráfico de red privada virtual). Por lo tanto, esta etapa puede incluir la revisión de HTTP (p. ej., datos HTTP «post»), HTTPS o VPN. Si se encontró la información predeterminada

(bloque S1008), entonces en el bloque S1010 se modifican los datos. En una forma de realización, los datos pasan de un formato «protegido» a un formato «no protegido», como se describirá con más detalle más adelante. En el bloque S1012, los datos se modifican para reflejar el destino previsto. Para HTTP, esta puede incluir la modificación del encabezado HTTP, por ejemplo, para cambiar «acquirer.proxy.com» por «www.acquirer.com». En el bloque S1014, los datos se modifican para reflejar la longitud de datos modificados. Para HTTP, esto puede incluir la modificación del parámetro de longitud del encabezado HTTP para reflejar la nueva longitud de DATOS HTTP en función de todos los cambios anteriores. En la etapa S1016, el mensaje modificado se envía al destino previsto. Se podrá observar que puede no ser necesario «agrupar» los DATOS TCP para su envío, ni añadir un ENCABEZADO TCP a la información, ya que el protocolo de envío puede gestionar esto de manera automática.

[0112] A continuación se describirán formas de realización de aparatos para implementar aspectos de los métodos mencionados anteriormente.

[0113] La figura 11 muestra de manera esquemática un procesador de llamadas 1120 que puede estar implementado como un aparato periférico en el terminal informático 1102 del agente, donde la información se extrae de manera automática por medio del aparato periférico 1120, o bien la introduce manualmente el agente, es decir, se recibe en papel/fax, u oralmente, y la introduce manualmente utilizando un dispositivo de entrada de cifrado 1136. En la figura 11, se muestran dispositivos de entrada que cubren ambas opciones, aunque se podrá observar que este no es necesariamente el caso.

[0114] El procesador de llamadas 1120 comprende un módulo de interfaz de audio 1122 para recibir señales de datos, un módulo de decodificador de audio 1124 para reconocer información característica, y un módulo de interfaz de entrada de datos 1126 para introducir datos en aplicaciones en un terminal informático del agente.

[0115] Una llamada entrante 1104 procedente de un cliente se desvía al teléfono 1121 del agente 1134 mediante una central de conmutación (PBX) (no representada) del centro de llamadas. Las señales de datos recibidas pueden comprender señales de audio análogas mono o estéreo, señales de audio digitales mono o estéreo, señales de datos de voz sobre IP (VoIP), datos de audio por paquetes mono o estéreo, etc.

[0116] El módulo de interfaz de audio 1122 convierte las señales de datos recibidas en audio digital convencional para su análisis, aunque se podrá observar que dicha conversión no siempre es necesaria. Los métodos que puede utilizar el módulo de interfaz de audio 1122 para convertir las señales de datos incluyen los que resultan conocidos para los expertos en la materia del procesamiento de audio, por ejemplo, descomprimiendo 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.

[0117] El audio digital se genera para el módulo de interfaz de señal 1124, que detecta información característica en el audio digital. Esta información característica puede incluir, aunque sin carácter limitativo, tonos de audio concretos, como tonos de multifrecuencia de doble tono (DTMF), patrones de voz e identificadores de paquetes de datos, por ejemplo, de paquetes de VoIP.

[0118] La información característica establecida por el módulo de interfaz de señal 1124 se genera para el módulo de interfaz de entrada de datos 1126, que determina información relacionada con la información característica, por ejemplo, una letra o un número representado por un tono DTMF. Los métodos mediante los cuales el módulo de control de señal 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) 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 las medidas correspondientes para asegurar que se utiliza el método apropiado para cada tipo de patrón predeterminado. Dichos aspectos se pueden definir como ajustes de configuración para el módulo de interfaz de señal.

[0119] El módulo de interfaz de entrada de datos 1126 está configurado para proporcionar la información a una aplicación de terceros en el terminal informático 1102 del agente. A partir de la descripción anterior, se podrá observar que la aplicación de terceros puede estar ya configurada para aceptar datos protegidos, por ejemplo, porque el servidor *proxy* haya modificado la página web que se ofrece al terminal informático del agente. Esto puede incluir determinar cómo se muestra la información en la aplicación de terceros o el funcionamiento de la aplicación de terceros, de manera que la información se muestre en la aplicación de terceros en un formato adecuado, o de manera que la aplicación de terceros funcione de un modo deseado. Cuando la aplicación de terceros 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 puede ser igual que las señales recibidas desde el módulo de interfaz de señal. En este sentido, el módulo de interfaz de datos no necesita cambiar las señales ni su método de visualización en la aplicación de terceros, ni el funcionamiento de la aplicación de terceros, y simplemente puede transmitirlas directamente a la aplicación de terceros. Las señalas transmitidas por el módulo de interfaz de señal a la aplicación de terceros 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.

[0120] En una forma de realización, el módulo de interfaz de señal 1124 está adaptado para reconocer tonos DTMF, el módulo de interfaz de señal 1124 comprende un módulo de decodificador de multifrecuencia de doble tono (DTMF), y el módulo de interfaz de entrada de datos 1126 es un microcontrolador que comprende un procesador de datos 1128 para procesar las señales de datos (p. ej., determinar los números de la tarjeta de crédito mediante los tonos DTMF) y un emulador de teclado USB 1130 que imita las pulsaciones de teclas del ordenador. En este sentido, los tonos DTMF se pueden «insertar» directamente en las aplicaciones sin la introducción por parte del agente 1134.

[0121] Se podrá comprender que las funciones de los módulos se pueden llevar a cabo en distintas combinaciones. Por ejemplo, la determinación de la información relacionada con la información característica se podría llevar a cabo mediante el módulo de interfaz de señal 1124. De manera alternativa, todas las funciones se podrían combinar en un único módulo. Un experto en la materia podrá concebir otras combinaciones.

[0122] En el caso del procesador de llamadas 1120 descrito anteriormente, los datos se extraen automáticamente. No obstante, como se ha mencionado anteriormente, la información la puede introducir también manualmente el agente utilizando un dispositivo de entrada de cifrado físico 1136, por ejemplo, un teclado/teclado numérico de cifrado o un dispositivo de escaneado. Por lo tanto, los datos de la tarjeta de crédito o de débito están protegidos desde el momento en que se introducen, por ejemplo, se teclean manualmente o se reúnen mediante un lector de tarjetas magnético, un terminal del punto de venta u otro dispositivo.

[0123] La figura 12 muestra de manera esquemática una forma de realización en la que un autor de la llamada 1202 transmite información sensible y no sensible utilizando un teléfono 1204. La información sensible y no sensible pasan a través de un modificador de audio 1200.

[0124] El modificador de audio 1200 comprende un módulo de conversión de audio 1206, un búfer 1208, un módulo de modificación de señal 1210, un módulo de control de señal 1212, un módulo de requisitos de modificación 1214, un módulo de interfaz de señal 1216 y un módulo de salida de audio 1218.

[0125] En la figura 13 se muestra un diagrama de flujo que muestra el funcionamiento del módulo de control de señal 1212, el módulo de requisitos de modificación 1214, y el módulo de interfaz de señal 1216 y se hará referencia a estos en la siguiente descripción.

[0126] Se puede considerar que el modificador de audio 1200 está «siempre activado» y es autónomo, es decir, no necesita alternar entre modos y puede funcionar de manera independiente. Aquí, el módulo de modificador de audio se muestra conectado al teléfono 1221 del agente del centro de llamadas, aunque se podrá observar que el modificador de audio 1200 se puede situar en cualquier punto entre el autor de la llamada 1202 y el teléfono 1221 del agente del centro de llamadas, o en otros puntos no situados directamente entre el autor de la llamada 1202 y el teléfono 1221 del agente del centro de llamadas.

[0127] En la figura 12, el módulo de modificador de audio se muestra separado del servidor *proxy* 1201, aunque se podrá observar que el módulo de modificador de audio puede estar contenido en el servidor *proxy*.

[0128] El módulo de conversión de audio 1206 está configurado para convertir los datos de entrada que representan audio en audio digital convencional para su análisis. Los métodos utilizados por el módulo de conversión de audio 1206 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), la supresión del encabezado y otra información que no sea de audio de los datos en paquetes, etc.

[0129] El audio digital se genera para el búfer 1208 y para el módulo de control de señal 1212.

[0130] El módulo de control de señal 1212 está configurado para detectar información característica (patrones predeterminados) en el audio digital, por ejemplo, tonos de audio concretos, como tonos DTMF (bloque S1302). El módulo de control de señal 1212 también está configurado para determinar información relacionada con la información característica (bloque S1306), como una letra o un número representado 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.

[0131] Los métodos mediante los cuales el módulo de control de señal 1212 determina si se ha encontrado un patrón predeterminado en el audio digital (bloque S1304) incluyen aquellos que resultan conocidos para los expertos en la materia, como las transformaciones rápidas de Fourier (FET) 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 método apropiado para cada tipo de patrón predeterminado. Dichos aspectos se pueden definir como ajustes de configuración para el módulo de control de señal 1212.

[0132] La información sobre sincronización establecida por el módulo de control de señal 1212 se genera para un módulo de requisitos de modificación 1214 y para el módulo de interfaz de señal 1216. Por consiguiente, información como la posición detectada del patrón en el audio digital puede ser utilizada por el módulo de requisitos de modificación para determinar cómo o cuándo modificar la señal. 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.

[0133] Se genera también otra información de la naturaleza del patrón predeterminado detectado por el módulo de control de señal 1212 para el módulo de requisitos de modificación 1214 y para el módulo de interfaz de señal 1216. Por consiguiente, información como el patrón exacto detectado o el número de repeticiones del patrón detectado puede ser utilizada por el módulo de requisitos de modificación 1214 para determinar cómo o cuándo modificar la señal.

[0134] El módulo de requisitos de modificación 1214 puede hacer referencia también a otra información, como algoritmos, heurística, información estadística acerca de patrones predeterminados detectados previamente en la llamada actual o en otras llamadas, el estado de la llamada e información procedente de bases de datos o fuentes de datos externas (no representadas).

[0135] El módulo de requisitos de modificación 1214 genera comandos para el módulo de modificación de señal 1210, dictando las modificaciones que se deben realizar en la señal. También genera datos para el módulo de interfaz de señal 1216.

[0136] En una forma de realización, el módulo de modificación de señal 1210 sustituye los tonos DTMF por otros tonos DTMF, posiblemente distintos. De este modo, el modificador de audio puede actuar para convertir el número de la tarjeta de crédito del autor de una llamada en un token de la misma longitud. También puede actuar para convertir información sensible en información «ficticia», por ejemplo, convertir el CV2 de 3 dígitos del autor de una llamada en «000». También puede actuar para convertir información sensible en un formato de cifrado que conserve el formato, manteniendo la longitud del número de la tarjeta de crédito del autor de la llamada, pero cifrándolo. En otra forma de realización, el módulo de modificación de señal 1210 puede introducir tonos DTMF adicionales en la señal. De este modo, el modificador de audio puede actuar para convertir el número de la tarjeta de crédito de 16 dígitos del autor de una llamada en un formato cifrado con una longitud mayor de 16 dígitos. Por lo general, se puede hacer referencia a los métodos mencionados anteriormente como generadores de un formato protegido de la información (bloque S1308).

[0137] La salida de datos por parte del módulo de requisitos de modificación 1214 hacia el módulo de interfaz de señal 1216 puede incluir datos relacionados con los requisitos de modificación que pasan al módulo de modificación de señal 1210. En este sentido, el token, que actúa como un sustituto para el número de la tarjeta de crédito del autor de la llamada, puede pasar al módulo de interfaz de señal.

[0138] El módulo de interfaz de señal 1216, al que se le han proporcionado datos tanto del módulo de control de señal 1212 como del módulo de requisitos de modificación 1214, envía estos datos al servidor *proxy* 1201 y a cualquier otro dispositivo pertinente (bloque S1310).

[0139] En una forma de realización, el módulo de interfaz de señal 1216 envía el número de la tarjeta de crédito del autor de la llamada y el token que representa el número de la tarjeta de crédito (habiendo sido generado este por el módulo de requisitos de modificación) al servidor *proxy* 1201. En este sentido, cuando el pago del autor de la llamada lo procesa finalmente el centro de contacto y el token pasa desde el sistema de pago del agente al servidor *proxy* 1201, el servidor *proxy* puede sustituir el token por el número de la tarjeta de crédito del autor de la llamada antes de pasar la transacción al adquiriente. En este caso, la combinación del modificador de audio 1200 y el servidor *proxy* 1201 puede actuar para permitir que se procesen transacciones mediante el centro de llamadas, pero sin que ningún dato sensible de la tarjeta de crédito del autor de la llamada entre en el centro de llamadas.

[0140] En otra forma de realización, el módulo de interfaz de señal envía el token que representa el número de la tarjeta de crédito del autor de la llamada directamente al terminal informático del agente 1102 que se muestra en la figura 11. En este sentido, las aplicaciones de terceros del terminal informático 1102 pueden automatizar la tarea de introducción de datos del agente y suprimir el requisito de que el *hardware* procesador de llamadas 1120 se encuentre presente en el terminal informático del agente.

[0141] Tras cualquier modificación realizada por el módulo de modificación de señal 1210, el audio digital se convierte entonces para su posterior transmisión en el formato apropiado mediante el módulo de salida de audio 1218.

[0142] En una forma de realización, el módulo de salida de audio 1218 envía la señal de audio modificada hacia el teléfono 1221 del agente del centro de llamadas. La señal de audio modificada se decodifica según se muestra en la figura 11 para la entrada de datos automatizada en el terminal informático del agente del centro de llamadas 1102.

[0143] En otra forma de realización, el módulo de salida de audio envía la señal de audio modificada como datos de VoIP directamente al terminal informático 1102 del agente del centro de llamadas, donde una aplicación de terceros 1132 decodifica el audio modificado para la entrada automatizada de datos.

[0144] En las formas de realización descritas anteriormente, el autor de la llamada se mantiene en línea con el agente del centro de llamadas durante la transacción, aunque el agente del centro de llamadas no puede escuchar ni acceder de otro modo a la información sensible del autor de la llamada. La información que se muestra en el terminal informático del agente del centro de llamadas es una representación de los datos de la tarjeta de crédito del autor de la llamada, no los datos reales en sí. De este modo, la totalidad del centro de llamadas, incluyendo su sistema telefónico, dispositivos de grabación de llamadas, bases de datos, redes, ordenadores y agentes se puede considerar fuera del alcance de PCI DSS.

[0145] En formas de realización, se proporciona un dispositivo de entrada virtual 1404 al terminal informático 1402 mediante el servidor *proxy* 1401, tal y como se muestra de manera esquemática en la figura 14. El dispositivo de entrada virtual 1404 se puede enviar al terminal informático 1402 a través de una conexión segura 1406 modificando la página web que se le proporciona mediante el servidor *proxy* 1401. El usuario hace clic con su ratón 1405 en teclas virtuales para introducir el número de la tarjeta. La información puede estar protegida (p. ej., cifrada) en el terminal informático, o enviarse de manera segura en un formato no protegido al servidor 1401. En cualquier caso, la entrada se puede situar en la casilla de la tarjeta de crédito en el campo, por ejemplo, en el formato protegido (p. ej., cifrado) o como información ficticia, respectivamente. En este último caso, la información ficticia se sustituye por la información no protegida enviada mediante un canal de comunicación independiente 1406 desde el canal de comunicación 1407 en el que se envía la página web. Así, la entrada se logra sin pulsaciones de teclas. En algunas formas de realización, el dispositivo de entrada virtual 1404 puede estar incrustado en la página web del usuario o proporcionarse a través de una conexión remota segura desde un servidor independiente, es decir, no desde el servidor *proxy* 1401.

[0146] En algunas formas de realización, el terminal informático puede ser un ordenador personal de un individuo, tal como un teléfono móvil. Así, se contemplan dispositivos de entrada distintos de una entrada con ratón 1405, como pantallas táctiles.

[0147] La figura 15 muestra de manera esquemática un servidor *proxy* 1501, de acuerdo con una forma de realización. El servidor *proxy* 1501 comprende dos interfaces de red 1502 y 1503, conectadas mediante un puente interno 1504. Las tarjetas de interfaz de red 1502 y 1503 permiten que el servidor *proxy* interactúe con la red, y se asocian a un controlador 1505, una pila de protocolo de red 1506 (por ejemplo, TCP/IP), reglas de filtrado 1508 y un motor de procesamiento *proxy* 1510. En la figura 15, estos elementos se ilustran en una jerarquía lógica en la que las tarjetas de interfaz de red 1502 y 1503 se encuentran en el nivel lógico más bajo y el motor de procesamiento *proxy* 1510 se encuentra en el nivel lógico más alto. El controlador 1505 es un elemento de *software* ejecutado en interfaces de red 1502 y 1503 y el puente 1504, o en estrecha relación con interfaces de red 1502 y 1503 y el puente 1504, y es responsable de examinar cada paquete de información que llega desde la red para determinar su fuente, el destino y el tipo de solicitud u otro mensaje que contiene. La pila de protocolo 1506 administra qué formatos pueden asumir los mensajes de red, y define un conjunto de reglas para cómo interpretar su contenido. Las reglas de filtrado 1508 determinan cómo se gestionan los paquetes diferentes. Cuando el servidor *proxy* funciona como un filtro de paquetes, la interfaz de red 1502 recibe todos los paquetes desde la red interna prevista para la red externa (p. ej., internet), y la interfaz de red 1503 recibe todos los paquetes desde la red externa prevista para la red interna. Al utilizar reglas de filtrado 1508, los paquetes pensados para un sistema proveedor de servicios externo, por ejemplo, se redirigen al motor de procesamiento *proxy* 1510. El motor de procesamiento *proxy* 1510 comprende un módulo 1512 para proteger o no proteger información sensible y un módulo 1514 para ordenar la modificación del tráfico. El servidor *proxy* se puede implementar utilizando un procesador y memoria (indicada mediante la línea discontinua) que presente un conjunto de instrucciones para llevar a cabo los métodos mencionados anteriormente. Como se ha mencionado anteriormente, si no existen conectores de red adicionales, como cables LAN, acoplados al filtro de paquetes, no se puede abordar mediante ningún dispositivo. Esto impide la modificación, el control o el acceso al filtro de paquetes.

[0148] Se podrá observar que, en las formas de realización anteriormente expuestas, no se han mostrado todos los componentes de los dispositivos informáticos en aras de una mayor claridad. Los dispositivos informáticos de servidor pueden ser cualquier dispositivo informático que proporcione uno o varios servicios a los usuarios, aplicaciones y/u otros dispositivos informáticos, p. ej., a través de una red. Por ejemplo, el dispositivo informático de servidor puede incluir servidores de archivos, servidores de correo, servidores web, servidores públicos, etc. Los dispositivos informáticos de cliente pueden ser cualquier dispositivo informático que utilice, emplee o esté asociado de otro modo a un servicio proporcionado por un servidor. Por ejemplo, los dispositivos informáticos de cliente pueden ser o pueden incluir, por ejemplo, un ordenador portátil, un ordenador de sobremesa, o un dispositivo portátil, como un dispositivo de asistente digital personal (PDA), una tableta, o un teléfono móvil. Los dispositivos informáticos pueden incluir, aunque sin carácter limitativo, una unidad de procesamiento, una memoria y un bus que acople diversos componentes, incluyendo la memoria, a la unidad de procesamiento. El bus puede ser cualquiera de entre diversos tipos de estructuras de bus que incluyen un bus de memoria o controlador de memoria, un bus periférico y un bus local que utilice cualquiera de entre varias arquitecturas de

bus. La memoria puede incluir tanto medios volátiles como medios no volátiles, medios extraíbles y no extraíbles, implementados en cualquier método o técnica para el almacenamiento de información, como instrucciones legibles por ordenador, estructuras de datos, módulos de programas u otros datos. La memoria puede incluir, aunque sin carácter limitativo, memoria RAM, ROM, EEPROM, *flash* u otra tecnología de memoria, CD-ROM, discos versátiles digitales (DVD) u otro almacenamiento de disco óptico, casetes magnéticos, cinta magnética, almacenamiento de disco magnético u otro dispositivo de almacenamiento magnético, o cualquier otro medio que se pueda utilizar para almacenar la información deseada y que sea accesible con ordenador. Un usuario puede introducir comandos e información a través de dispositivos de entrada, tales como un teclado y un dispositivo señalador, al que normalmente se hace referencia como ratón, bola de seguimiento o panel táctil. También puede haber presente un monitor u otro tipo de dispositivo de visualización.

[0149] Aunque, en formas de realización anteriores, la información pertenece a información financiera, como información de la tarjeta de crédito, el experto en la materia podrá observar que la información que debe estar protegida y/o no protegida se puede definir de forma distinta en función del contexto en el que se utilice. Por ejemplo, puede incluir información que esté relacionada con una persona específica X, información personal que alguna parte crea que se debe mantener en privado, e información que identifique o que se pueda utilizar para identificar, contactar o localizar a la persona a la que pertenezca dicha información. Entre los ejemplos concretos se incluye información, como el número de identificación nacional de una persona (como el número de la Seguridad Social o el número de seguro social), el número de registro de la matrícula del vehículo, el número del carné de conducir, el número de la tarjeta de crédito, la fecha de nacimiento e información genética.

[0150] Aunque en las formas de realización anteriores se detectan y se modifican los tonos DTMF en señales de audio digitales, los datos de la 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).

[0151] A pesar de que, en las formas de realización anteriormente expuestas, 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).

[0152] Las señales comunicadas mediante el módulo de interfaz de señal pueden estar con el sistema operativo de un aparato de procesamiento de datos (un ordenador). Las señales comunicadas mediante la interfaz de señal pueden estar con el sistema operativo de un teléfono u otro dispositivo de comunicación portátil. Las señales comunicadas mediante 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 comunicar a través de la interfaz de señal, de acuerdo con las normas de formato de comunicaciones que resultan conocidas para los expertos en la materia.

[0153] En las formas de realización, la modificación de un mensaje puede incluir la alteración del contenido HTML de una página web o un modelo de objeto de documento, macros o secuencias de comandos, o cualquier comunicación similar o relacionada necesaria para interactuar con la aplicación de terceros. El mensaje modificado puede actuar para que la información protegida para la aplicación de terceros se realice de manera automática para únicamente una localización de entrada de datos prevista. Por ejemplo, el mensaje modificado puede incluir la función de localizar un campo de entrada de datos con una propiedad o característica concreta (por ejemplo, una que presente una etiqueta de texto «CVV» a su izquierda) y, a continuación, pasar el elemento CW de los datos de la tarjeta únicamente a este campo. En este sentido, se fuerza la entrada de datos de la tarjeta en su ubicación prevista.

[0154] La aplicación de terceros puede ser una página web que se visualice en el sistema operativo de un ordenador. También puede ser una aplicación que se ejecute en el sistema operativo de un ordenador. La aplicación de terceros puede ser una página web que se visualice en un dispositivo de telecomunicaciones, incluyendo un teléfono móvil. También puede ser una aplicación que se ejecute en un dispositivo de telecomunicaciones, incluyendo un teléfono móvil. También puede ser una base de datos u otro medio de almacenamiento de datos. Así, las interfaces de entrada de datos que se utilizan normalmente (como aplicaciones informáticas o sitios web) pueden presentar datos sensibles introducidos en un formato protegido.

[0155] A pesar de que los métodos y aparatos descritos pueden ofrecer ventajas concretas para operaciones de centro de llamadas, también se pueden aplicar a otras tecnologías de comunicación que procesen información sensible. En este sentido, aunque en las formas de realización expuestas anteriormente se hace referencia a servidores proveedores de servicios y a terminales informáticos de centros de llamadas, estas pueden comprender otros dispositivos informáticos.

[0156] En la descripción detallada de formas de realización indicada anteriormente, las referencias a «una forma de realización», «un ejemplo de forma de realización», etc., indican que la forma de realización descrita puede incluir una característica, función o estructura concreta, pero no es necesario que todas las formas de realización incluyan la característica, función o estructura concreta. Además, dichas expresiones no hacen referencia necesariamente a la misma forma de realización. Asimismo, cuando se describe una característica, función o

estructura concreta en relación con una forma de realización, se afirma que dentro del conocimiento de un experto en la materia se encuentra el hecho de llevar a cabo dicha característica, función o estructura en relación con otras formas de realización, hayan sido descritas de manera explícita o no.

[0157] Aunque la presente invención se ha descrito anteriormente con referencia a formas de realización concretas, un experto en la materia podrá observar que las modificaciones se incluyen en el alcance de las reivindicaciones adjuntas.

REIVINDICACIONES

1. Método para mediar comunicaciones entre un primer dispositivo informático y un segundo dispositivo informático, mediante un dispositivo informático intermediario, comprendiendo el método:

el establecimiento de un enlace de comunicaciones con cada uno del primer y el segundo dispositivo informático;

la recepción de un mensaje de solicitud de información desde el segundo dispositivo informático, comprendiendo el mensaje de solicitud de información un documento electrónico que permite la entrada de información en un formato no protegido;

la modificación del mensaje de solicitud de información para permitir que el documento electrónico acepte la entrada de información en un formato protegido;

la transmisión del mensaje de solicitud de información modificado al primer dispositivo informático;

la recepción de un primer mensaje desde el primer dispositivo informático, comprendiendo el contenido del primer mensaje el documento electrónico con información en el formato protegido;

la conversión de al menos parte de la información en el formato protegido al formato no protegido; y

la transmisión de un segundo mensaje al segundo dispositivo informático, comprendiendo el contenido del segundo mensaje al menos parte de la información en el formato no protegido.

2. Método según la reivindicación 1, donde el establecimiento del enlace de comunicaciones con el primer dispositivo informático incluye la recepción de una solicitud de conexión dirigida a un nombre de dominio del segundo dispositivo informático; o donde el establecimiento del enlace de comunicaciones con el primer dispositivo informático incluye la recepción de una solicitud de conexión dirigida a un localizador uniforme de recursos del dispositivo informático intermediario; o donde el establecimiento del enlace de comunicaciones con el primer dispositivo informático incluye interceptar una solicitud de conexión desde el primer dispositivo informático al segundo dispositivo informático, utilizando un conjunto de una o varias reglas predefinidas de comunicación; o donde el establecimiento del enlace de comunicaciones con el primer dispositivo informático incluye identificar una solicitud de conexión desde el primer dispositivo informático al segundo dispositivo informático, entre una pluralidad de solicitudes de conexión a una pluralidad de dispositivos informáticos que incluyen el segundo dispositivo informático.

3. Método según la reivindicación 1, donde el documento electrónico permite la entrada de información de manera automática y/o asistida por el usuario.

4. Método según la reivindicación 1 o la reivindicación 3, donde la modificación del mensaje de solicitud de información comprende la modificación de uno o varios campos de entrada de datos para aceptar la entrada de la información en el formato protegido.

5. Método según cualquiera de las reivindicaciones anteriores, comprendiendo, además, la selección del segundo dispositivo informático de entre una pluralidad de dispositivos informáticos.

6. Método según cualquiera de las reivindicaciones anteriores, comprendiendo, además, la transmisión de al menos parte de la información en el formato no protegido a un tercer dispositivo informático.

7. Método según cualquiera de las reivindicaciones anteriores, comprendiendo, además:

la recepción de una pluralidad de primeros mensajes desde uno o varios primeros dispositivos informáticos;

para cada uno de la pluralidad de primeros mensajes, la conversión de al menos parte de la información en el formato protegido a un formato no protegido; y

la transmisión de uno o varios segundos mensajes al segundo dispositivo informático, comprendiendo el contenido de cada segundo mensaje al menos una parte de la información en el formato no protegido desde cada uno de dicha pluralidad de primeros mensajes.

8. Método según cualquiera de las reivindicaciones anteriores, donde el formato protegido comprende un formato cifrado y la conversión de al menos parte de la información desde el formato protegido al formato no protegido comprende el descifrado de la información.

9. Método según cualquiera de las reivindicaciones 1 a 7, donde el formato protegido comprende un token digital y la conversión de al menos parte de la información desde el formato protegido al formato no protegido comprende la destokenización de la información.

10. Método según cualquier reivindicación anterior, comprendiendo, además:

la recepción de un tercer mensaje desde el segundo dispositivo informático, comprendiendo el contenido del tercer mensaje información en el formato no protegido;

la conversión de la información en el formato no protegido al formato protegido; y

la transmisión de un cuarto mensaje al primer dispositivo informático, comprendiendo el contenido del cuarto mensaje al menos parte de la información en el formato protegido.

11. Método según la reivindicación 10, comprendiendo, además, bloquear la transmisión de al menos parte de la información al primer dispositivo informático.

12. Método según la reivindicación 10 o la reivindicación 11, donde la recepción del primer mensaje desde el segundo dispositivo informático comprende:

interceptar el tercer mensaje utilizando un conjunto de una o varias reglas predefinidas de comunicación; y

redirigir el tercer mensaje interceptado a un motor de procesamiento del dispositivo informático intermediario.

13. Aparato para mediar comunicaciones entre un primer dispositivo informático y un segundo dispositivo informático, comprendiendo el aparato:

medios para establecer un enlace de comunicaciones con cada uno del primer y el segundo dispositivo informático;

medios para recibir un mensaje de solicitud de información desde el segundo dispositivo informático, comprendiendo el mensaje de solicitud de información un documento electrónico que permite la entrada de información en un formato no protegido;

medios para modificar el mensaje de solicitud de información para permitir que el documento electrónico acepte la entrada de información en un formato protegido;

medios para transmitir el mensaje de solicitud de información modificado al primer dispositivo informático;

medios para recibir un primer mensaje desde el primer dispositivo informático, comprendiendo el contenido del primer mensaje información en el formato protegido;

medios para convertir al menos parte de la información en el formato protegido al formato no protegido; y

medios para transmitir un segundo mensaje al segundo dispositivo informático, comprendiendo el contenido del segundo mensaje al menos parte de la información en el formato no protegido.

14. Aparato según la reivindicación 13, comprendiendo, además:

medios para recibir el tercer mensaje desde el segundo dispositivo informático, comprendiendo el contenido del tercer mensaje información en el formato no protegido;

medios para convertir la información en el formato no protegido al formato protegido;

medios para establecer un enlace de comunicaciones con el primer dispositivo informático; y

medios para transmitir el cuarto mensaje al primer dispositivo informático, comprendiendo el contenido del cuarto mensaje al menos parte de la información en el formato protegido.

15. Medio de transporte que transporta código legible por ordenador para controlar que un ordenador lleve a cabo el método según cualquiera de las reivindicaciones 1 a 12.

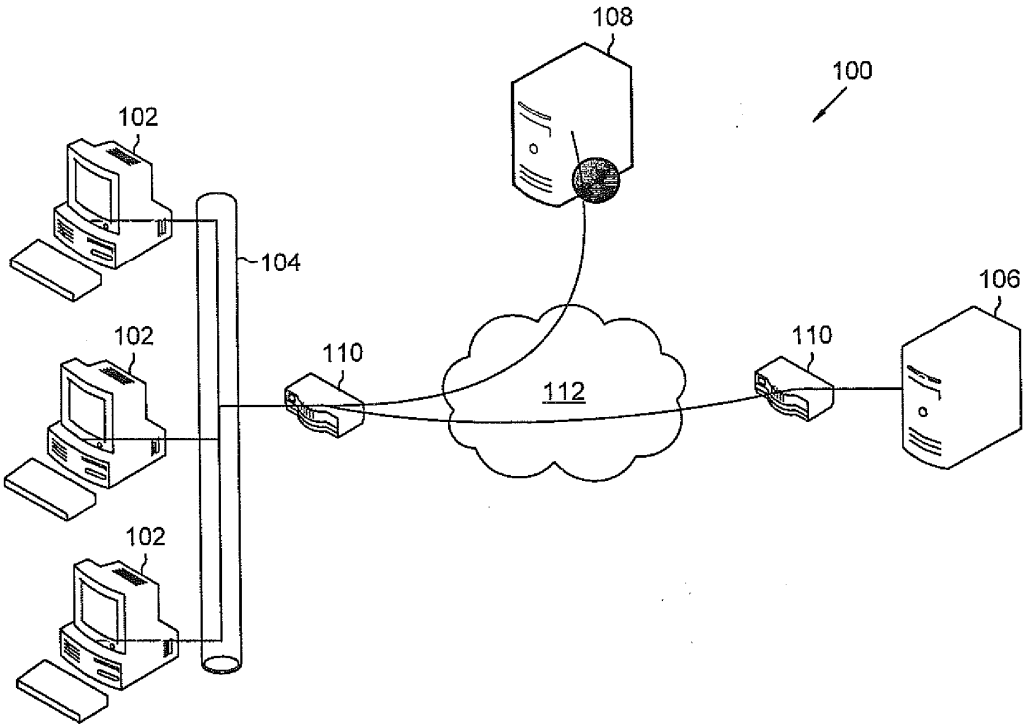

FIGURA 1

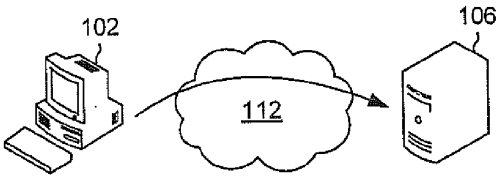

FIGURA 2a

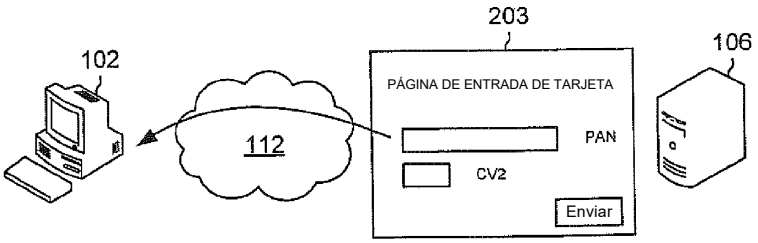

FIGURA 2b

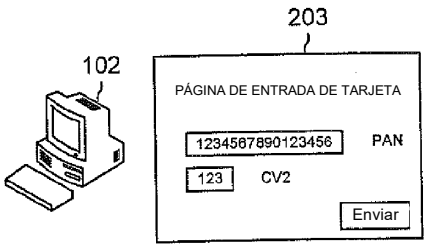

FIGURA 2c

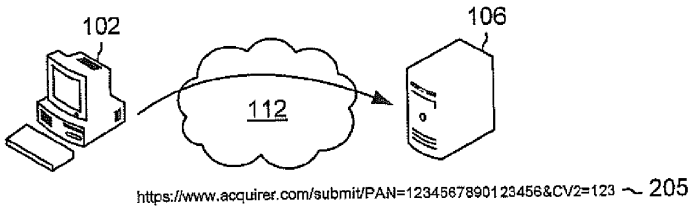

FIGURA 2d

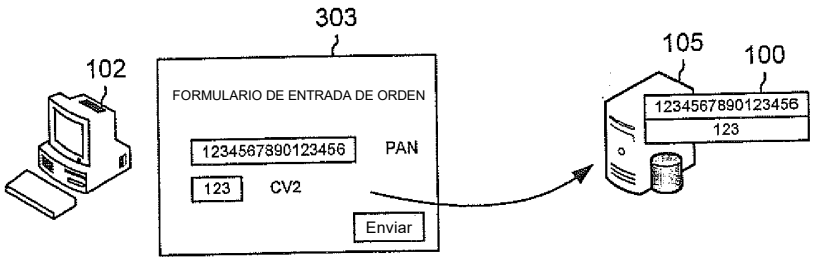

FIGURA 3a

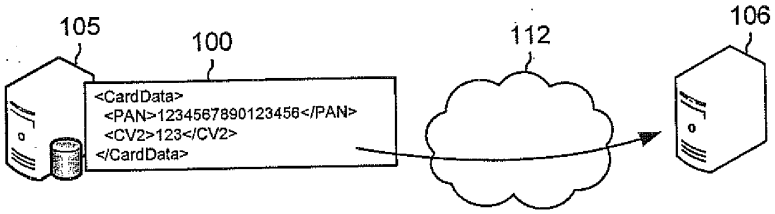

FIGURA 3b

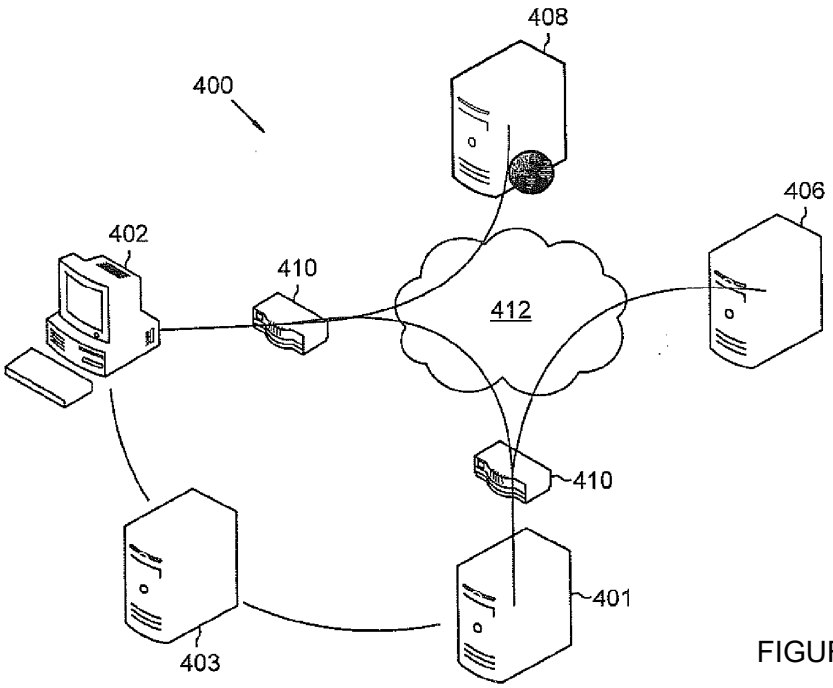

FIGURA 4

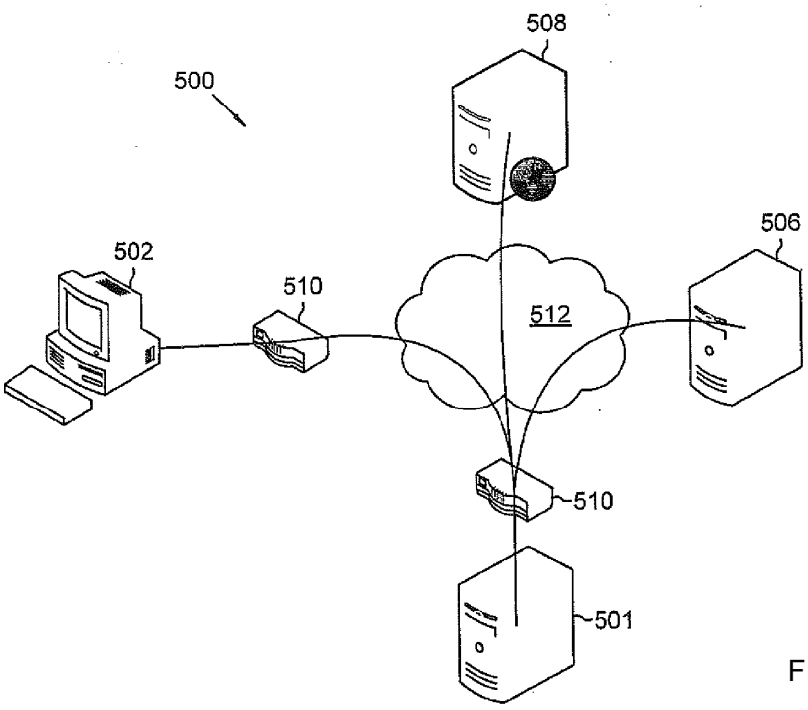

FIGURA 5

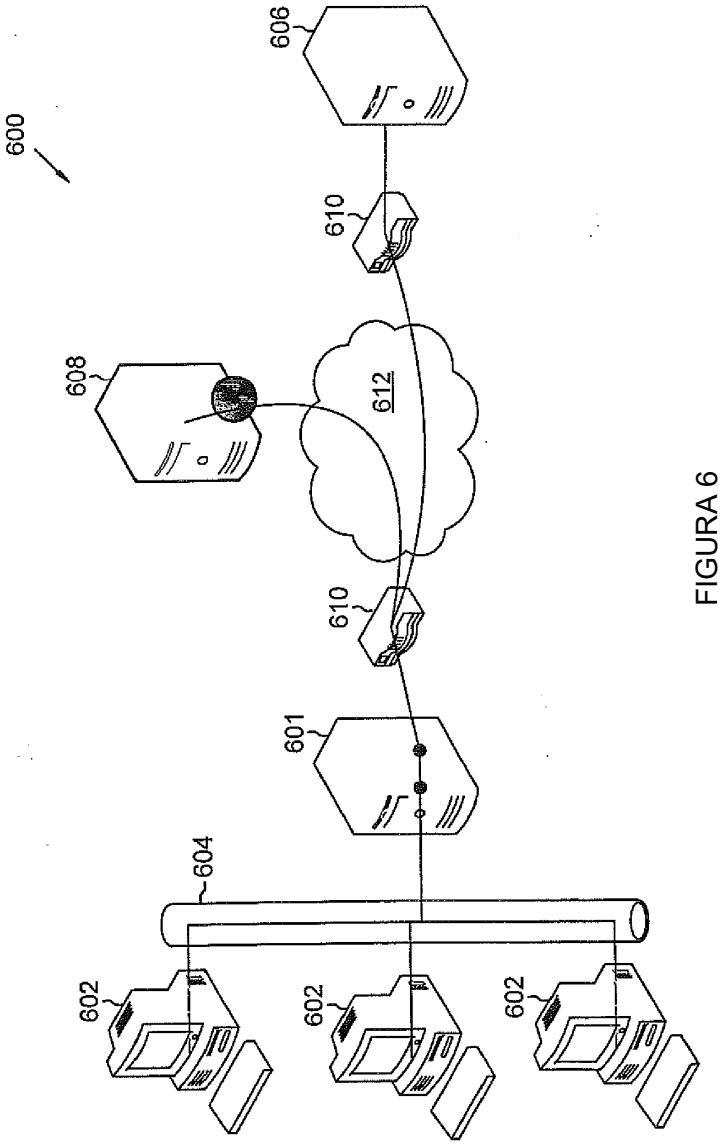

FIGURA 6

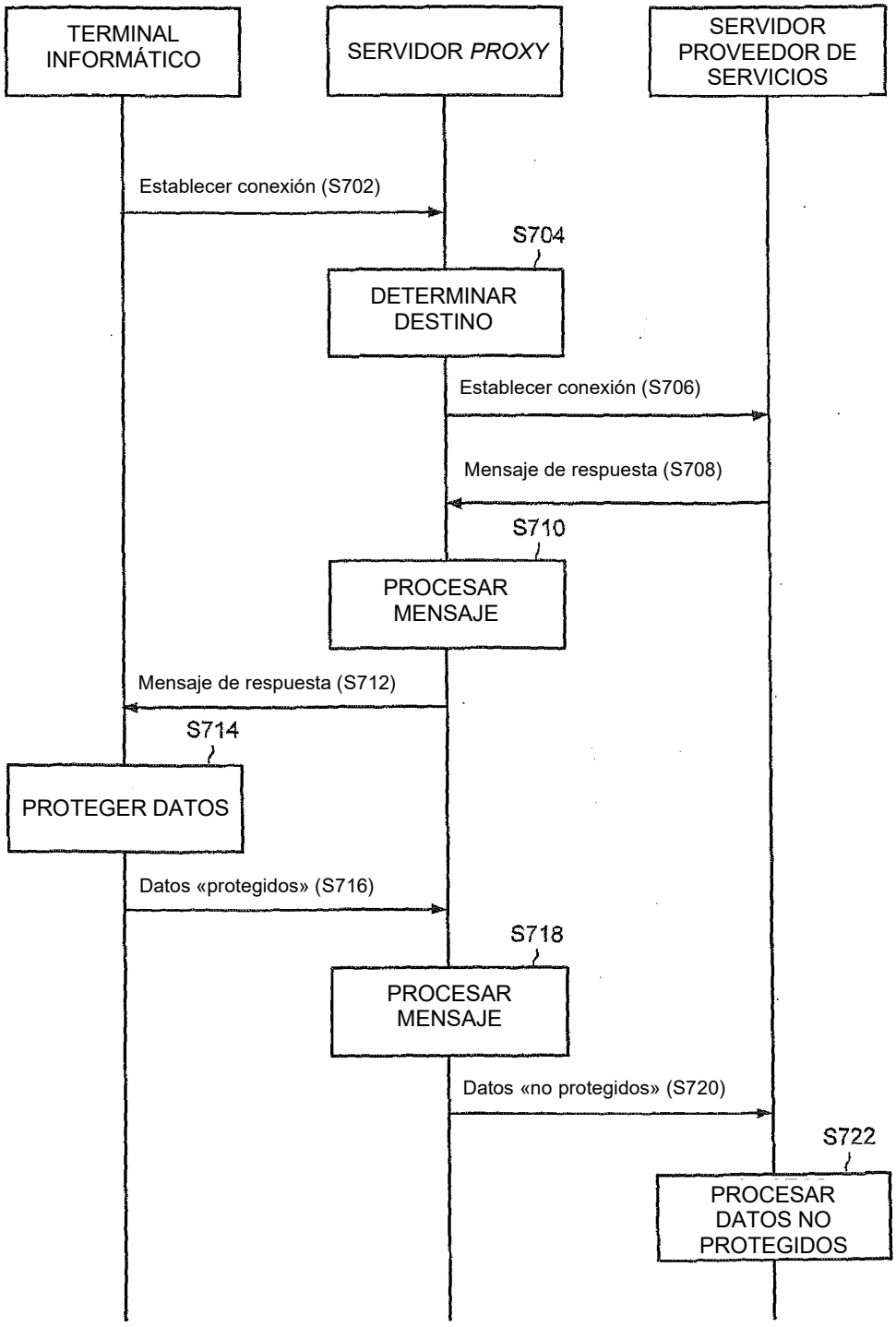
TERMINAL INFORMÁTICO
SERVIDOR *PROXY*
SERVIDOR PROVEEDOR DE SERVICIOS
Establecer conexión (S702)
S704
DETERMINAR DESTINO
Establecer conexión (S706)
Mensaje de respuesta (S708)
S710
PROCESAR MENSAJE
Mensaje de respuesta (S712)
S714
PROTEGER DATOS
Datos «protegidos» (S716)
S718
PROCESAR MENSAJE
Datos «no protegidos» (S720)
S722
PROCESAR DATOS NO PROTEGIDOS

FIGURA 7

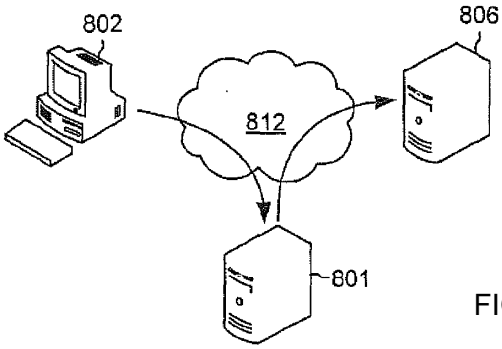

FIGURA 8a

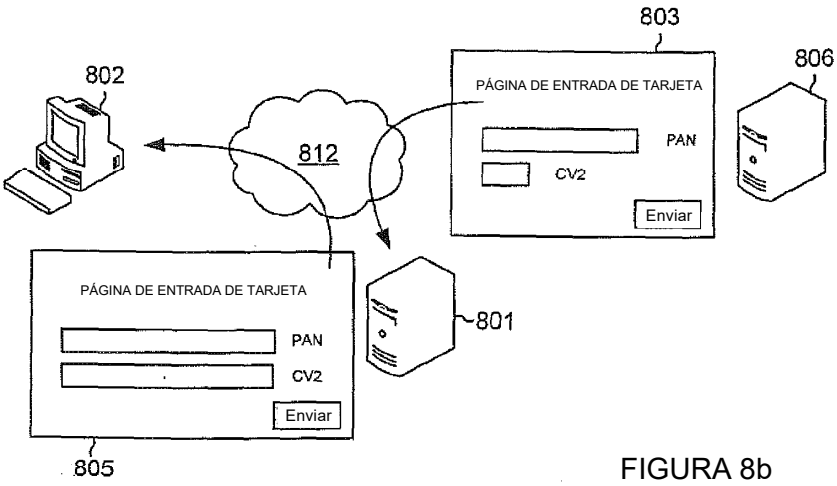

FIGURA 8b

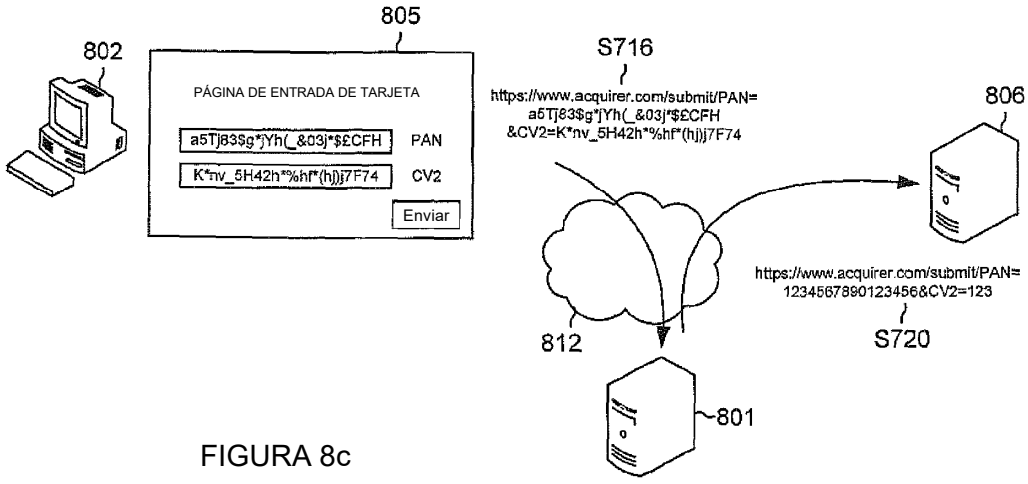

FIGURA 8c

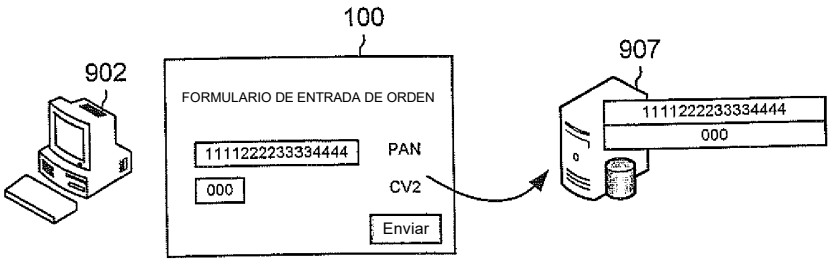

FIGURA 9a

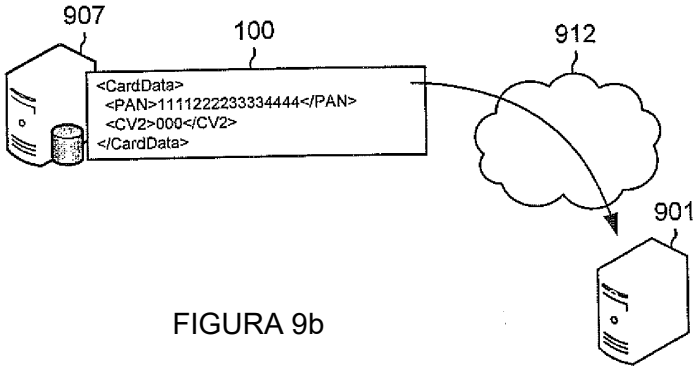

FIGURA 9b

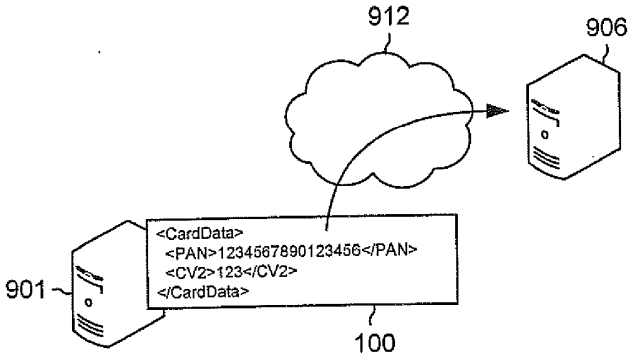

FIGURA 9c

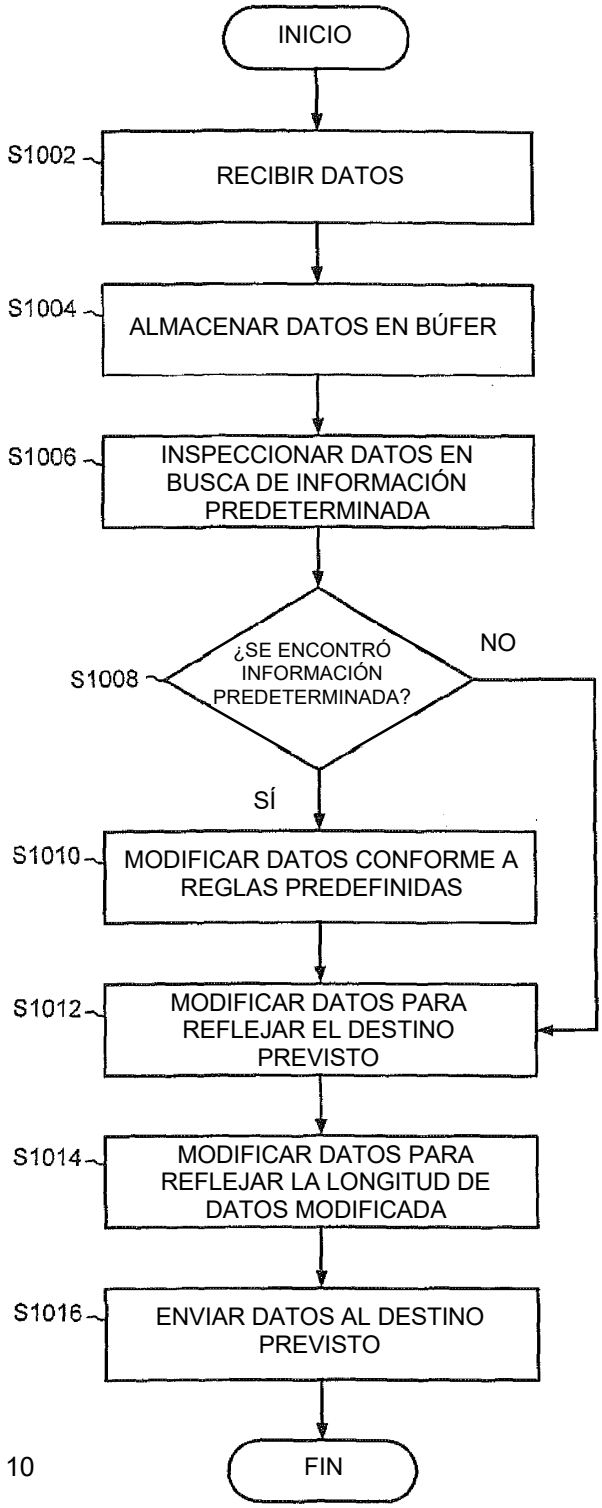
INICIO
S1002
RECIBIR DATOS
S1004
ALMACENAR DATOS EN BÚFER
S1006
INSPECCIONAR DATOS EN BUSCA DE INFORMACIÓN PREDETERMINADA
S1008
¿SE ENCONTRÓ INFORMACIÓN PREDETERMINADA?
NO
SÍ
S1010
MODIFICAR DATOS CONFORME A REGLAS PREDEFINIDAS
S1012
MODIFICAR DATOS PARA REFLEJAR EL DESTINO PREVISTO
S1014
MODIFICAR DATOS PARA REFLEJAR LA LONGITUD DE DATOS MODIFICADA
S1016
ENVIAR DATOS AL DESTINO PREVISTO
FIN

FIGURA 10

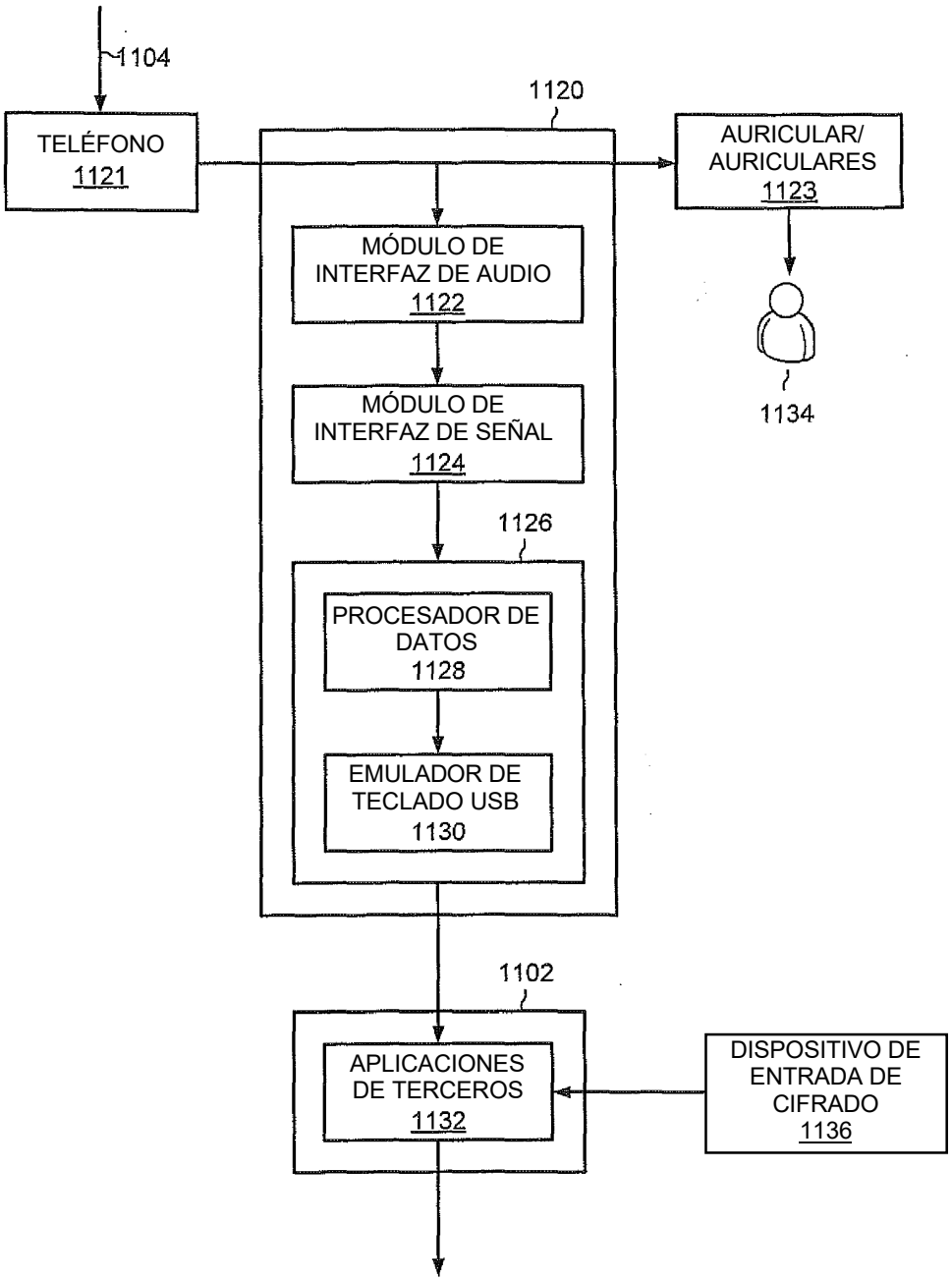
1104
1120
TELÉFONO
1121
AURICULAR/
AURICULARES
1123
MÓDULO DE
INTERFAZ DE AUDIO
1122
1134
MÓDULO DE
INTERFAZ DE SEÑAL
1124
1126
PROCESADOR DE
DATOS
1128
EMULADOR DE
TECLADO USB
1130
1102
APLICACIONES
DE TERCEROS
1132
DISPOSITIVO DE
ENTRADA DE
CIFRADO
1136

FIGURA 11

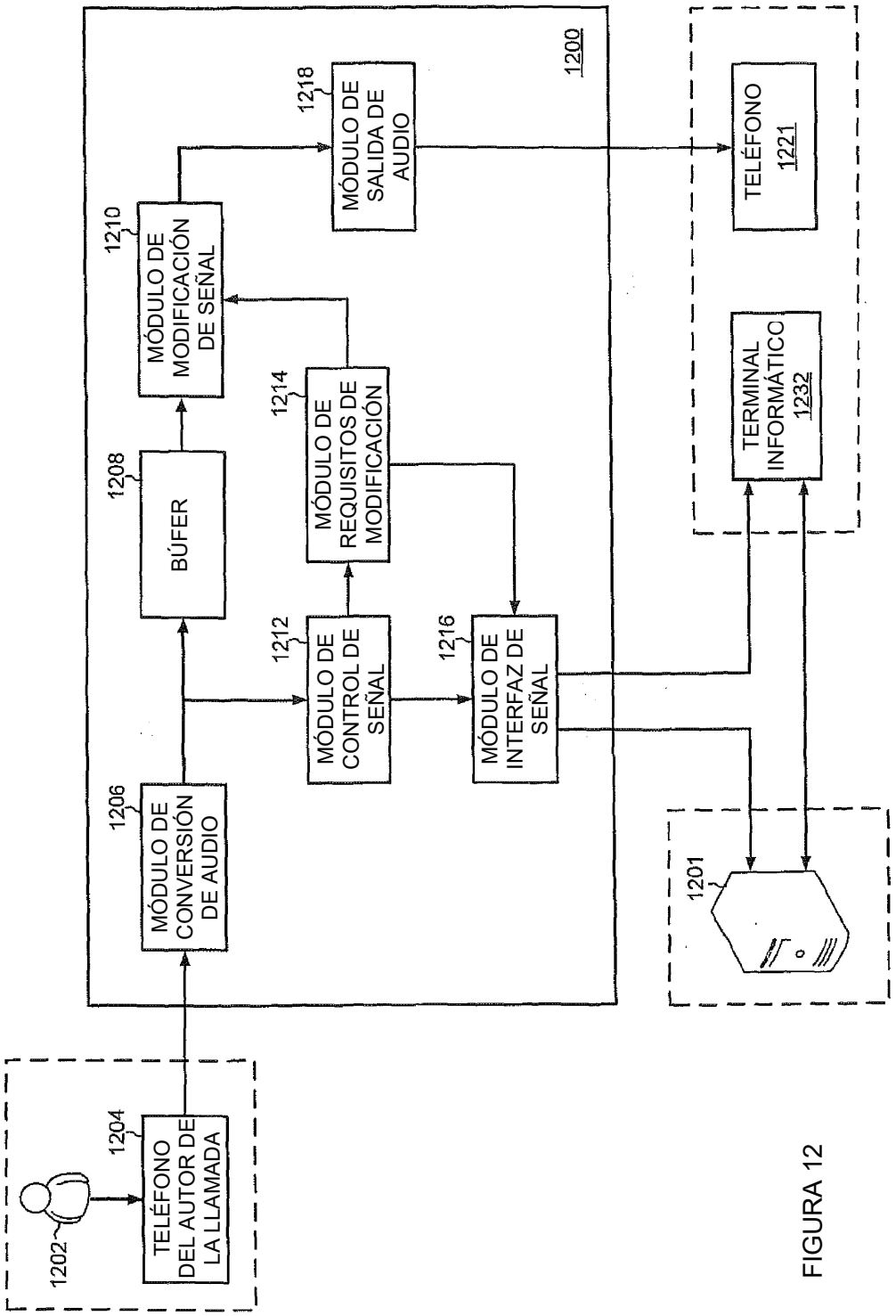
1200
1202
1204
TELÉFONO DEL AUTOR DE LA LLAMADA
1206
MÓDULO DE CONVERSIÓN DE AUDIO
1208
BÚFER
1210
MÓDULO DE MODIFICACIÓN DE SEÑAL
1212
MÓDULO DE CONTROL DE SEÑAL
1214
MÓDULO DE REQUISITOS DE MODIFICACIÓN
1216
MÓDULO DE INTERFAZ DE SEÑAL
1218
MÓDULO DE SALIDA DE AUDIO
1201
TELÉFONO 1221
TERMINAL INFORMÁTICO 1232

FIGURA 12

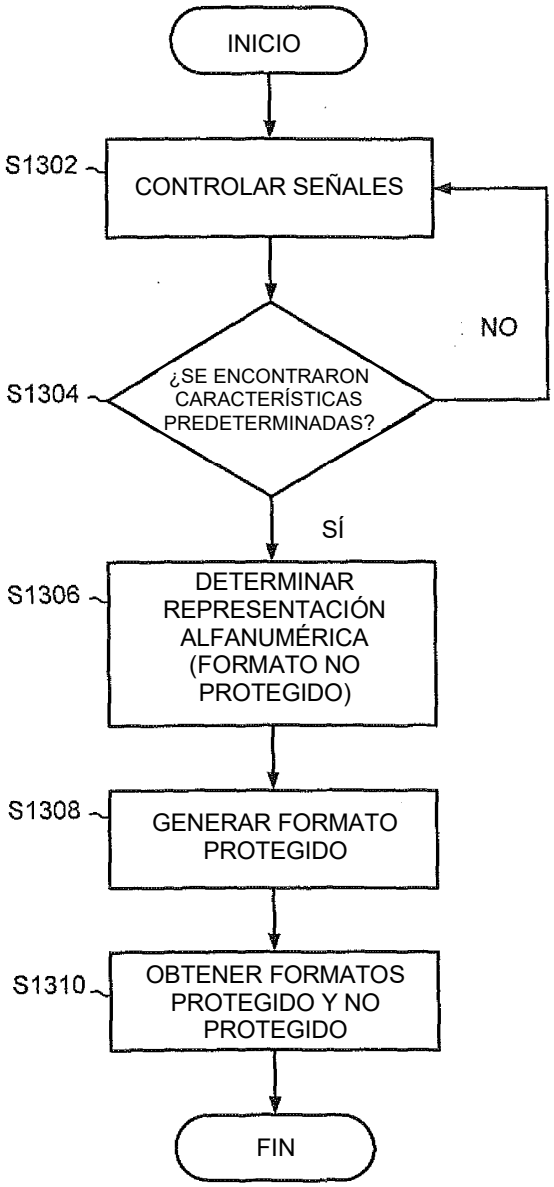
INICIO
S1302
CONTROLAR SEÑALES
NO
S1304
¿SE ENCONTRARON CARACTERÍSTICAS PREDETERMINADAS?
SÍ
S1306
DETERMINAR REPRESENTACIÓN ALFANUMÉRICA (FORMATO NO PROTEGIDO)
S1308
GENERAR FORMATO PROTEGIDO
S1310
OBTENER FORMATOS PROTEGIDO Y NO PROTEGIDO
FIN

FIGURA 13

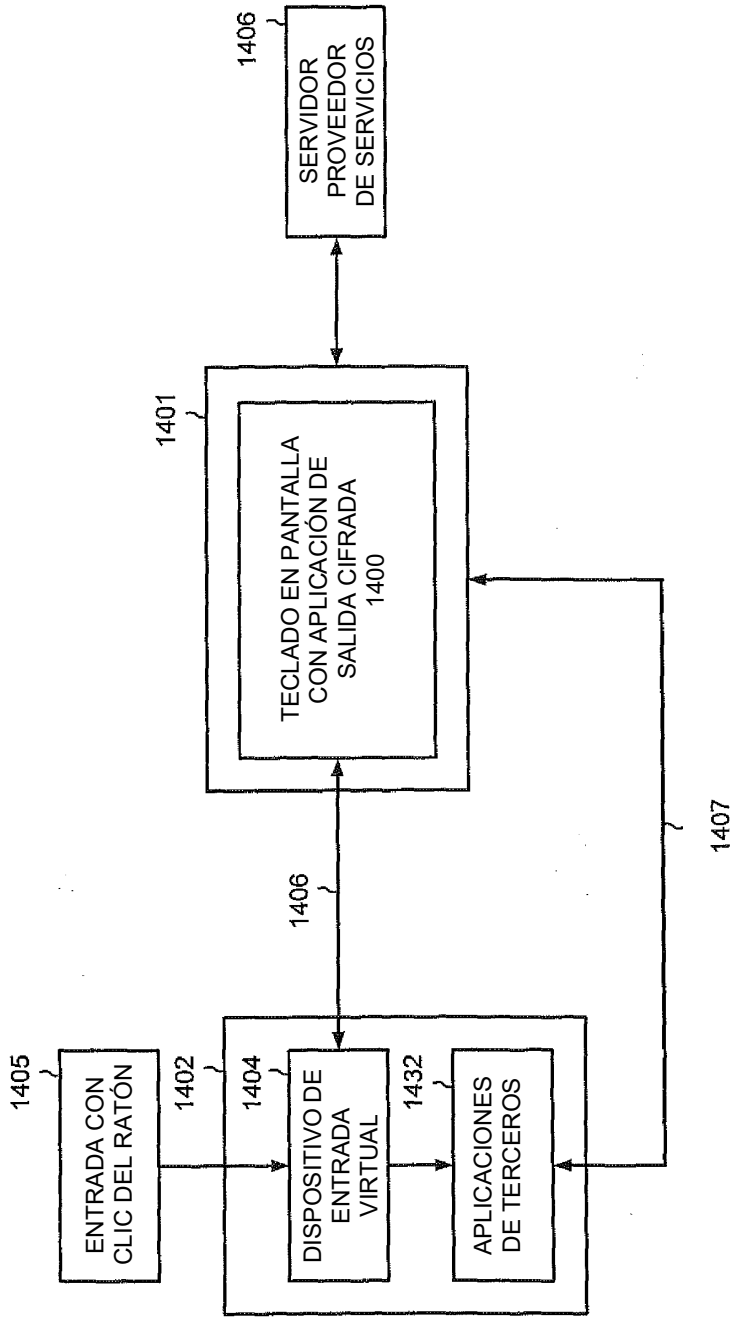
1406
SERVIDOR PROVEEDOR DE SERVICIOS
1401
TECLADO EN PANTALLA CON APLICACIÓN DE SALIDA CIFRADA 1400
1406
1407
1405
ENTRADA CON CLIC DEL RATÓN
1402
1404
DISPOSITIVO DE ENTRADA VIRTUAL
1432
APLICACIONES DE TERCEROS

FIGURA 14

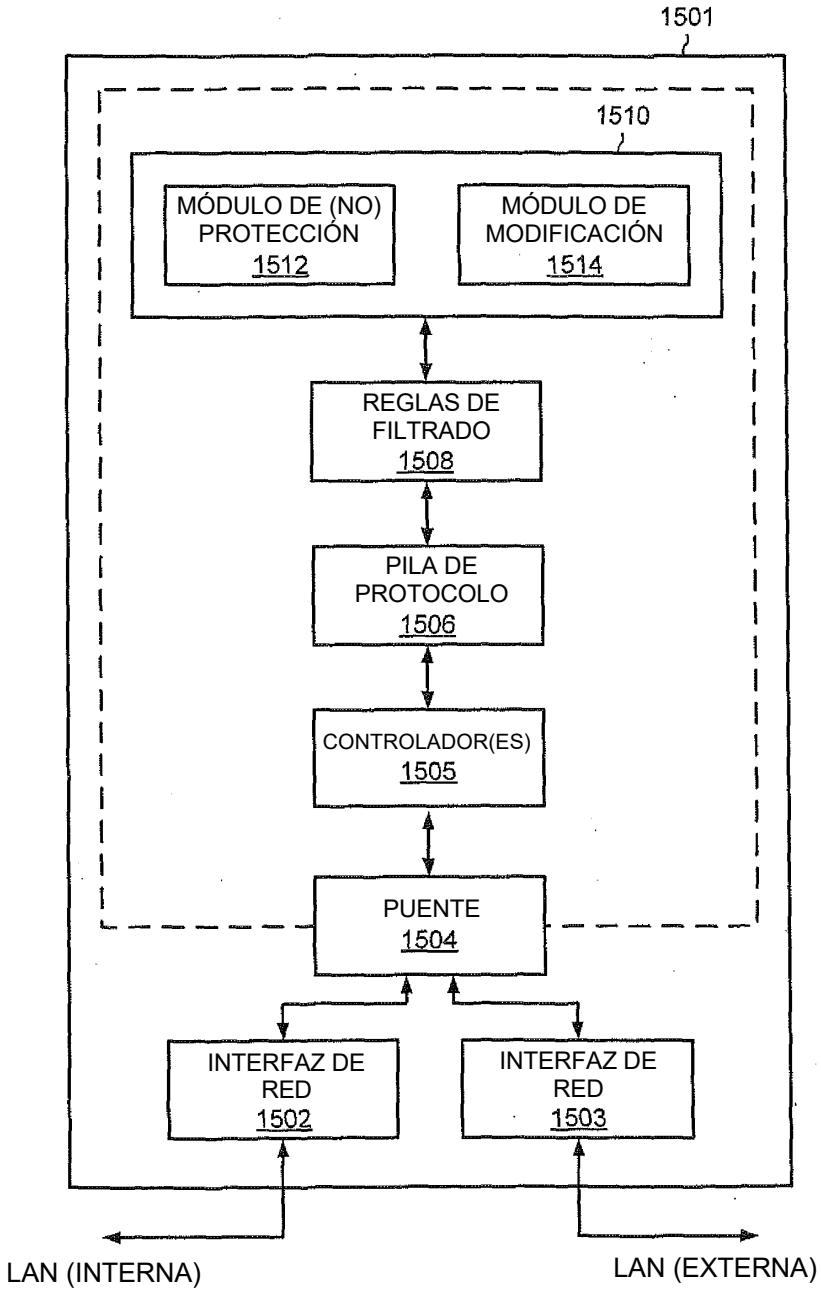
1501
1510
MÓDULO DE (NO) PROTECCIÓN
1512
MÓDULO DE MODIFICACIÓN
1514
REGLAS DE FILTRADO
1508
PILA DE PROTOCOLO
1506
CONTROLADOR(ES)
1505
PUENTE
1504
INTERFAZ DE RED
1502
INTERFAZ DE RED
1503
LAN (INTERNA)
LAN (EXTERNA)

FIGURA 15