(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 542 697**

(51) Int. CI.:

***H04L 9/32*** (2006.01)
***H04L 12/58*** (2006.01)
***H04L 29/06*** (2006.01)
***H04L 12/24*** (2006.01)
***G06F 17/30*** (2006.01)
***G06Q 10/00*** (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **10.12.2008 E 08863582 (6)**

(97) Fecha y número de publicación de la concesión europea: **29.04.2015 EP 2243248**

(54) Título: **Procedimiento de gestión de correo certificado por vía electrónica**

(30) Prioridad:

**10.12.2007 FR 0708584**
**10.01.2008 FR 0800147**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**10.08.2015**

(73) Titular/es:

**LOGIDOC SOLUTIONS (100.0%)**
**5 Rue Hubert Curien, Parc d'Activités de Romanet**
**87000 Limoges, FR**

(72) Inventor/es:

**PEAUDECERF, BERTRAND y**
**PREVEL, JEAN-CLAUDE**

(74) Agente/Representante:

**LAZCANO GAINZA, Jesús**

**DESCRIPCIÓN**

Procedimiento de gestión de correo certificado por vía electrónica

La presente invención se refiere a un procedimiento de gestión del correo certificado por vía electrónica.

La carta certificada existe desde hace más de dos siglos. Se trata hoy de un correo materializado en una hoja, fechada y firmada por su autor y colocada en un sobre en el que aparece la dirección del destinatario. El conjunto cerrado se presenta en una oficina de correo que lo enviará y lo entregará a su destinatario contra impresión de una fecha y de una firma. La cronología de la transacción se certifica por el sello que se presenta en el sobre y en el documento adjunto que materializa la integración del correo. Autenticación, confidencialidad y seguimiento caracterizan la carta certificada. Sin embargo, el papel certificado contiene varios inconvenientes. En particular, él aporta la prueba del continente pero no del contenido, él se limita al transporte de documentos reales, y él no puede aportar la prueba de la lectura del correo. Para remediar estos problemas, se ha propuesto enviar el correo certificado por vía electrónica. En efecto, contrariamente a su homólogo de papel, el certificado electrónico permite particularmente aportar la prueba del contenido y no solo del continente en la medida en que sea posible solicitarle a un tercero de confianza el conservar el original y entonces presentarlo en caso de litigio. Este permite también transportar ficheros informáticos, imágenes, vídeos, etc. Este permite igualmente establecer que el correo sea no solo aceptado sino leído igualmente, además de la firma electrónica que certifica la presentación del envío . El documento FR-2 900 013 describe un procedimiento de este tipo que utiliza dos memorias distintas, una accesible por el autor del correo y la otra por su destinatario, cada una de estas memorias que recibe un original de dicho correo. Este procedimiento es complejo, y la existencia de dos originales no es aconsejable, pues esto induce un riesgo potencial de litigio e impone una doble seguridad. Además, para que el proceso de certificado electrónico sea igual de válido que la carta certificada de papel, se debe apoyar en funciones esenciales de un proceso a valor probatorio o de prueba. Ahora bien, en los procedimientos existentes, este valor probatorio no es siempre una garantía. En particular, cada etapa entre el principio y el fin de la cadena debe asegurarse y garantizarse.

La presente invención tiene por objetivo proporcionar un procedimiento de gestión de correo certificado por vía electrónica que no reproduce los inconvenientes anteriormente mencionados.

La presente invención tiene en particular por objetivo proporcionar un procedimiento de gestión de correo certificado por vía electrónica que garantiza la integridad del documento que forma el correo del principio al fin del procedimiento, desde la creación del correo hasta la consultación por el destinatario y su archivo.

La presente invención tiene además por objetivo proporcionar un procedimiento de gestión de correo certificado por vía electrónica que es simple y poco costoso de realizar, de instalar y de utilizar.

La presente invención tiene entonces por objeto un procedimiento de gestión de correo certificado por vía electrónica tal como se describe en la reivindicación 1. Modos de realización favorables se describen en las reivindicaciones dependientes.

Estas características y ventajas y otros de la presente invención aparecerán con más claridad en la lectura de la descripción detallada siguiente, dada a título de ejemplo no limitativo, y que se refiere a la figura 1 adjunta, que es un esquema que ilustra las deferentes etapas del procedimiento según un modo de realización particular de la invención.

El procedimiento de la invención utiliza principalmente un puesto de trabajo de un autor de un documento a enviar en forma de un correo electrónico certificado, un puesto de trabajo de un destinatario destinado a recibir este documento, un servidor para gestionar el documento entre el autor y el destinatario, y un tercero de confianza para garantizar y certificar todas las etapas del procedimiento. Por supuesto, el sistema de la presente invención puede incluir varios autores, varios puestos de trabajo por cada autor, varios destinatarios, varios puestos de trabajo por destinatario, varios servidores, y/o varios terceros de confianza.

Los terceros de confianza pueden ser organismos adaptados a almacenar de manera segura los datos electrónicos. Puede tratarse de autoridades de certificación aptas para garantizar las transmisiones seguras de documentos codificados entre personas autorizadas, identificadas y autentificadas. En particular, los terceros de confianza pueden incluir servidores de certificación adaptados a emitir certificados de garantía. Estos se adaptan además para emitir claves de codificación del tipo PKI (Public Key Infrastructure, o infraestructura de clave pública), cuyo funcionamiento se conoce bien.

La invención se describirá a continuación refiriéndose a una secuencia de etapas favorable, pero esta no debe considerarse como limitativa, algunas de las etapas descritas a continuación que pueden ser opcionales, otras etapas suplementarias que pueden agregarse a las descritas, y algunas etapas que pueden invertirse entre ellas.

La creación del documento

El documento puede crearse directamente en el puesto de trabajo del autor, por ejemplo al utilizar sus programas habituales (procesamiento de texto, hoja de cálculo, etc.).

En una primera variante, la persona que quiere utilizar el servicio de envío de un certificado electrónico puede conectarse a una plataforma WEB del servidor y conectarse a su cuenta de cliente (o crear una, llegado el caso), para descargar el documento previamente creado en su puesto de trabajo. Como variante, el autor puede además crear directamente su documento desde el espacio de cliente al conectarse y al crear su documento a través de un formulario o similar.

En una segunda variante, el autor del documento puede utilizar un controlador (también llamado driver) configurable instalado en su puesto de trabajo, y que crea en su puesto de trabajo una impresora virtual, adaptada a transferir el documento a dicho servidor.

La identificación y autentificación del Autor

El autor del documento debe identificarse y autentificarse de manera clara e indiscutible, de preferencia a través de la utilización de un sistema de clave pública / clave privada (cifrado asimétrico).

La codificación del documento

El documento no debe poderse consultar, ni modificar.

Para eso, antes de su envío, el documento se transforma favorablemente en un documento PDF asociado a un fichero XML (que contiene datos de información relativos al documento, tal como el número de página, el número de elementos adjuntos, el bloque de dirección extraído del documento, etc.) El documento puede entonces firmarse electrónicamente por el autor. La firma se efectúa de preferencia a través de un tercero de confianza. El documento final se envía sobre la plataforma de dicho tercero de confianza para la firma. El documento puede visualizarse particularmente por el autor para firmarse digitalmente a través de la aplicación del tercero de confianza. El fichero PDF se codifica entonces así como el fichero XML asociado.

Luego los dos ficheros (el fichero PDF y el fichero XML asociado) se comprimen en un fichero de archivo que se codifica.

La codificación se realiza de preferencia mediante el cifrado asimétrico proporcionado por un tercero de confianza.

Cuando el documento se ha transmitido al utilizar el controlador mencionado anteriormente instalado en el puesto de trabajo del autor, este controlador cuenta con una firma segura para garantizar que el documento sea íntegro.

El fichero de archivo codificado se recepciona por el servidor, de preferencia a través de un protocolo de transmisión seguro, del tipo HTPPS, FTPS o VPN.

Después de la recepción, este fichero es descodificado por el servidor, mediante claves de descodificación proporcionadas por dicho tercero de confianza.

Registro de fecha y hora y archivo a valor probatorio

Con el fin de establecer el valor probatorio del certificado electrónico, se registra favorablemente la fecha y hora de cada etapa del procedimiento y luego se archiva por y en las instalaciones de un tercero de confianza.

El documento final firmado con su clave de control se envía a través de un protocolo de transmisión seguro hacia las instalaciones de un tercero de confianza donde se registran con fecha y hora y después se archivan. Así los documentos archivados son infalsificables.

Igualmente, las etapas de identificación del autor, la codificación, la transmisión al servidor (llegado el caso) y la firma (llegado el caso), así como todos los otros eventos preferiblemente se registran con fecha y hora y se archivan.

Envío del correo electrónico de información

Después del archivo del documento, el servidor envía un correo electrónico de información al puesto de trabajo del destinatario, para informarle que un correo certificado está disponible. Este correo electrónico de información contiene un

vínculo de consulta, y se le informa al destinatario que él puede acceder al documento que forma dicho certificado al hacer clic sobre este vínculo en un tiempo de consulta predeterminado. Favorablemente, el envío de este correo electrónico de información se realiza también a través de un protocolo de transmisión seguro.

Registro de fecha y hora y archivo a valor probatorio

El correo electrónico de información enviado al destinatario se registra con fecha y hora en las instalaciones de un tercero de confianza.

Envío de un mensaje de texto

Para disminuir los riesgos de que el destinatario no esté al corriente de que un certificado lo espera en el servidor, se puede enviar un mensaje de texto del tipo SMS a un teléfono, particularmente un teléfono móvil, del destinatario para indicarle que recibió un certificado electrónico.

Registro de fecha y hora y archivo a valor probatorio

Este SMS enviado al destinatario se registra con fecha y hora y se archiva en las instalaciones de un tercero de confianza

Distribución del correo electrónico de información

Un acuse de recibo se envía al autor del documento para informarle que el correo electrónico de información se distribuyó bien al destinatario. Este acuse de recibo se envía favorablemente en forma de un correo electrónico.

Registro de fecha y hora y archivo a valor probatorio

Una vez más, esta etapa se registra con fecha y hora y después se archiva con el fin de probar la fecha de la puesta a disposición del certificado.

Activación del vínculo de consulta

Si el destinatario hace clic sobre el vínculo de consulta contenido en el correo electrónico de información antes de la expiración del tiempo de consulta, este va a conectarse al servidor.

Identificación y Autenticación del destinatario

Este debe conectarse entonces a su espacio de consulta al identificarse y autentificarse, preferiblemente al utilizar su certificado electrónico.

Registro de fecha y hora y archivo a valor probatorio

La activación del vínculo de consulta así como la identificación y la autenticación del destinatario se registrarán con fecha y hora y se archivarán.

Consulta del documento

Una vez el destinatario identificado y conectado en su espacio de consulta, este puede consultar su certificado electrónico. El documento puede descargarse entonces a través de un protocolo de transmisión seguro en el puesto de trabajo del destinatario, el cual puede entonces consultarlo, grabarlo y/o imprimirlo.

El autor del documento recibirá a su vez un mensaje, particularmente un correo electrónico, que indica que el destinatario examinó satisfactoriamente el certificado electrónico.

Registro de fecha y hora y archivo a valor probatorio

El evento de consulta a su vez se registrará con fecha y hora y se archivará luego en las instalaciones de un tercero de confianza con el fin de probar la fecha en la cual el mensaje se leyó.

Expiración del tiempo de consulta

En el caso en que el destinatario no consultó su certificado electrónico durante el tiempo de consulta seleccionado por el autor, es decir que el destinatario no hizo clic sobre el vínculo de consulta contenido en su correo electrónico de información, el espacio de consulta se desactiva. El destinatario no puede entonces consultar más su certificado por vía electrónica.

Un mensaje correspondiente se envía entonces al autor informándole que el destinatario no examinó el certificado electrónico durante el tiempo de consulta otorgado.

Registro de fecha y hora y archivo a valor probatorio

El evento de expiración del tiempo de consulta del correo electrónico de información se registra con fecha y hora y se archiva después en las instalaciones de un tercero de confianza.

Envío del documento por la vía del papel

A falta de activación del vínculo de consulta en el tiempo otorgado, el certificado electrónico se dirige entonces hacia un proceso de envío por vía postal.

El certificado electrónico se codifica y se envía después de manera segura hacia un centro de edición digital que se encargará de la impresión, de su plegado y del envío por vía postal.

Archivo a valor probatorio

Todo el proceso del centro de edición electrónica garantiza la totalidad y la integridad del documento lo que permite asegurar el archivo y el seguimiento de los envíos (AR, NPAI).

Así, el procedimiento de la presente invención permite :

reducir significativamente los costos de fabricación, de envío postal y otros relativos a este,
optimizar y reducir los costos de la gestión de los correos certificados que salen de la Empresa sin cambiar los hábitos de trabajo,
recibir el correo certificado sin plazo,
desmaterializar los correos certificados,
personalizar los envíos,
conservar la integridad de los correos mediante firmas electrónicas seguras,
autentificar al autor y al destinatario (certificados electrónicos),
aportar la prueba del contenido y no solo del continente,
transportar ficheros de cualquier formato, y particularmente ficheros digitales, vídeos, imágenes,
realizar documentos constituidos de varios ficheros de formatos diferentes,
determinar si el certificado no solo se aceptó sino que también se leyó,
asegurar y mejorar la confidencialidad de los envíos (codificación),
garantizar la entrega del correo (impresión y envío por vía postal si no activación del vínculo de consulta),
garantizar su valor probatorio (identificación, autenticación, firma electrónica, registro de fecha y hora y archivo por y en las instalaciones de un tercero de confianza de cada etapa del proceso).

La importancia y la fiabilidad de un procedimiento tal se basan en su valor probatorio que se caracteriza por la confidencialidad de la identificación y de la autenticación del expedidor y del destinatario (certificado electrónico), por la integridad y la totalidad del mensaje y de los documentos adjuntos (firma electrónica, codificación), por la conservación (archivo en las instalaciones de un tercero de confianza) y por la garantía de las fechas de envío, de recepción y de lectura del correo electrónico certificado (registro de fecha y hora por un tercero de confianza).

La invención se describió en referencia a una variante de realización particular, y se entiende que un especialista en este campo puede aportarle cualquier modificación útil sin salirse del marco de la presente invención tal como se define en las reivindicaciones anexadas.

Reivindicaciones

**1.** Procedimiento de gestión de correo certificado por vía electrónica, en un sistema que comprende un puesto de trabajo de un autor, un servidor, un puesto de trabajo de un destinatario, al menos un tercero de confianza, y un centro de edición digital, **caracterizado en que** el procedimiento comprende varias etapas :

- creación del documento a enviar a un destinatario en forma de correo certificado;
- identificación y autenticación del autor;
- firma electrónica del documento a través de un tercero de confianza;
- codificación del documento;
- registro de fecha y hora de las etapas de identificación, d'autenticación y de codificación;
- transmisión del documento codificado hacia un servidor;
- descodificación del documento en el servidor;
- archivo en las instalaciones de un tercero de confianza de la identificación del autor, del documento y de las informaciones de registro de fecha y hora;
- envío de un mensaje de información al puesto de trabajo del destinatario del documento, dicho mensaje que es un correo electrónico que contiene un vínculo de consulta del documento;
- registro de fecha y hora de dicha etapa de envío;
- archivo en las instalaciones de un tercero de confianza del mensaje de información y de las informaciones del registro de fecha y hora;

dicho procedimiento, en caso de activación del vínculo de consulta por el destinatario en un tiempo de consulta predeterminado, que comprende las etapas siguientes :

- identificación y autenticación del destinatario;
- registro de fecha y hora de la etapa de identificación y de autenticación,
- archivo en las instalaciones de un tercero de confianza de la identificación, de l'autenticación y de las informaciones del registro de fecha y hora;
- consulta del documento por el destinatario, particularmente por el envío de una copia del documento al puesto de trabajo del destinatario;
- registro de fecha y hora de la etapa de consulta;
- archivo en las instalaciones de un tercero de confianza de la consulta y de las informaciones del registro de fecha y hora;

dicho procedimiento, en caso de no activación del vínculo de consulta por el destinatario en dicho tiempo de consulta predeterminado, que comprende las etapas siguientes :

- registro de fecha y hora de la expiración del tiempo de consulta;
- archivo en las instalaciones de un tercero de confianza de la expiración del tiempo de consulta y de las informaciones del registro de fecha y hora;
- envío del documento hacia el centro de edición digital para una transmisión al destinatario en forma de papel;
- archivo en las instalaciones de un tercero de confianza de la etapa de envío en forma de papel.

**2.** Procedimiento según la reivindicación 1, en el cual dichas etapas de autenticación de dicho autor y de dicho destinatario utilizan certificados electrónicos.

**3.** Procedimiento según cualquiera de las reivindicaciones precedentes, en el cual dichas etapas de codificación y descodificación utilizan un cifrado asimétrico.

**4.** Procedimiento según cualquiera de las reivindicaciones precedentes, en el cual dicho documento se transforma en el puesto de trabajo en un fichero PDF asociado a un fichero XML, después dicho fichero PDF se firma y después se codifica, después el fichero PDF codificado y el fichero XML se comprimen en un fichero de archivo, después dicho fichero de archivo se codifica para transmitirse al servidor.

**5.** Procedimiento según cualquiera de las reivindicaciones precedentes, en el cual todas las transmisiones y todos los envíos entre el puesto de trabajo, el servidor, el tercero de confianza y el puesto de trabajo del destinatario se realizan a través de un protocolo de transmisión seguro, particularmente del tipo HTPPS, FTPS o VPN.

**6.** Procedimiento según cualquiera de las reivindicaciones precedentes, en el cual el tercero de confianza comprende un servidor de certificación adaptado a emitir certificados electrónicos.

**7.** Procedimiento según cualquiera de las reivindicaciones precedentes, en el cual además del envío de un mensaje de información en forma de correo electrónico al puesto de trabajo del destinatario del documento, el servidor envía un mensaje de texto del tipo SMS a un aparato telefónico del destinatario.

**8.** Procedimiento según cualquiera de las reivindicaciones precedentes, en el cual después del envío de un mensaje de información al puesto de trabajo del destinatario, el servidor envía un acuse de recibo al puesto de trabajo del autor en forma de correo electrónico, para informarle al autor que el destinatario recibió el mensaje de información.

**9.** Procedimiento según cualquiera de las reivindicaciones precedentes, en el cual después de la consulta del documento por el destinatario, el servidor envía un acuse de lectura al puesto de trabajo del autor en forma de un correo electrónico, para informarle al autor que el correo certificado se consultó por el destinatario.

**10.** Procedimiento según cualquiera de las reivindicaciones precedentes, en el cual el envío del mensaje de información al puesto de trabajo del destinatario activa un espacio de consulta en el servidor, en el cual el destinatario puede venir a identificarse y autentificarse cuando hace clic sobre el vínculo de consulta dentro de dicho tiempo predeterminado.

**11.** Procedimiento según la reivindicación 10, en el cual, en caso de no activación del vínculo de consulta por el destinatario en el tiempo de consulta predeterminado, se desactiva dicho espacio de consulta

**12.** Procedimiento según cualquiera de las reivindicaciones precedentes, en el cual el documento objeto del correo certificado puede formarse por uno o varios ficheros de cualquier formato.

**13.** Procedimiento según cualquiera de las reivindicaciones precedentes, en el cual un controlador se instala en el puesto de trabajo del autor, lo que crea en dicho puesto de trabajo una impresora virtual configurable, a través de la cual el autor puede transmitir el documento que él creó a dicho servidor.

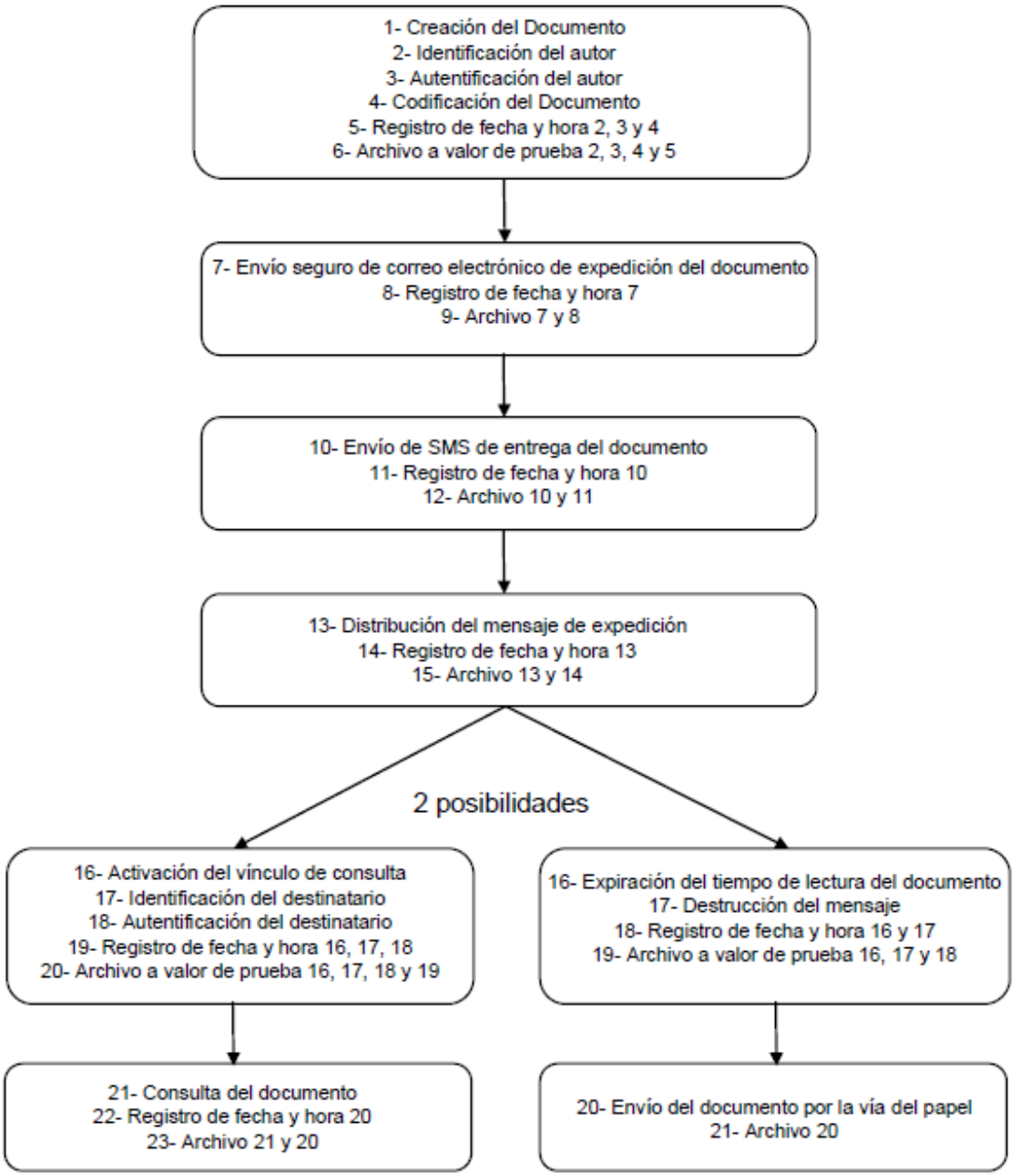
1- Creación del Documento
2- Identificación del autor
3- Autentificación del autor
4- Codificación del Documento
5- Registro de fecha y hora 2, 3 y 4
6- Archivo a valor de prueba 2, 3, 4 y 5
7- Envío seguro de correo electrónico de expedición del documento
8- Registro de fecha y hora 7
9- Archivo 7 y 8
10- Envío de SMS de entrega del documento
11- Registro de fecha y hora 10
12- Archivo 10 y 11
13- Distribución del mensaje de expedición
14- Registro de fecha y hora 13
15- Archivo 13 y 14
2 posibilidades
16- Activación del vínculo de consulta
17- Identificación del destinatario
18- Autentificación del destinatario
19- Registro de fecha y hora 16, 17, 18
20- Archivo a valor de prueba 16, 17, 18 y 19
16- Expiración del tiempo de lectura del documento
17- Destrucción del mensaje
18- Registro de fecha y hora 16 y 17
19- Archivo a valor de prueba 16, 17 y 18
21- Consulta del documento
22- Registro de fecha y hora 20
23- Archivo 21 y 20
20- Envío del documento por la vía del papel
21- Archivo 20

Fig.1