



# Edicom Oftp2 Server Manual de Usuario



Título del documento:	EOS Edicom Odette Server
Nombre del fichero:	ES EOS Manual de usuario.odt
Versión:	1.0
Estado:	VIGENTE
Fecha:	01/07/2010
Autor:	Francisco Belda

**Revisión, Aprobación**

Revisado por:		Fecha:
Aprobado por:		Fecha:

**Historial de cambios**

Versión	Fecha	Descripción de la acción	Páginas
1.0	01/07/2010	Redacción inicial	Todas.

# Índice de contenido

<b>1 EDICOM Oftp2 Server.....</b>	<b>4</b>
1.1 Introducción.....	4
1.1.1 El EOS Viewer.....	4
1.2 El EOS Viewer.....	5
1.2.1 Menú principal.....	5
1.2.2 Barra de herramientas principal.....	6
1.2.3 Árbol de nodos.....	6
<b>2 Interlocutores.....</b>	<b>8</b>
2.1 Introducción.....	8
2.2 Crear un interlocutor.....	9
2.3 Datos de un interlocutor.....	10
2.3.1 Pestaña propiedades.....	10
2.3.2 Pestaña Identificadores.....	13
2.3.3 Pestaña Conexiones.....	14
2.3.4 Pestaña Planificación de conexiones.....	15
<b>3 Usuarios.....</b>	<b>17</b>
3.1 Introducción.....	17
3.2 Crear nuevo usuario.....	17
<b>4 Configuración de alarmas.....</b>	<b>19</b>
4.1 Introducción.....	19
4.2 Crear nueva alarma.....	19
<b>5 Certificados.....</b>	<b>20</b>
5.1 Introducción.....	20
5.2 Añadir un certificado.....	20
5.3 Niveles de seguridad.....	21
5.3.1 Firma electrónica del canal de conexión (TLS o SSL).....	21
5.3.2 Firma electrónica de la información de inicio de sesión (SSID).....	21
5.3.3 Firma electrónica de los mensajes (SFID y EERP).....	21
5.3.4 Encriptación.....	22
<b>6 Mensajes.....</b>	<b>23</b>
6.1 Introducción.....	23
6.1.1 Ciclo de un mensaje.....	23
6.2 Crear un nuevo mensaje.....	24
6.3 Características de un mensaje.....	25
6.4 Listado de mensajes.....	27
<b>7 Sesiones.....</b>	<b>30</b>
7.1 Introducción.....	30
7.2 Datos de la sesión.....	30
7.3 Ficheros de log.....	30

# 1 EDICOM OFTP2 SERVER

## 1.1 INTRODUCCIÓN

---

El **EOS** —EDICOM Oftp2 Server— es un servidor para el intercambio de ficheros a través del estándar *Odette File Transfer Protocol* (OFTP) incluyendo las especificaciones v1.2, v1.3, v1.4 y v2.0 con opciones de firma electrónica y encriptación.

1. El **EOS** gestiona sesiones OFTP entrantes y salientes ( modo *Responder* y modo *Initiator*) a través de conexión RDSI o TCPIP
2. El **EOS** gestiona sesiones salientes a través de **EBI**—EDICOM Business Integrator— para integrar los mensajes con **EDICOMNet**, la red de valor añadido de EDICOM.
3. El **EOS** ofrece un interfaz SOAP para la integración y la configuración a través de *Web Services*.

---

**Nota:** Para la instalación y configuración inicial del servidor EOS consultar el documento "ANEXO EOS Manual de Instalación"

### 1.1.1 EL EOS VIEWER

El **EOS Viewer** es el cliente *Web Services* que permite la configuración y la gestión del Servidor **EOS** a través de una interfaz de usuario intuitiva. Esta interfaz permite:

- La configuración del servidor (como usuario administrador).
- La creación de dominios y usuarios con configuraciones independientes.
- La monitorización gráfica del estado de los mensajes y comunicaciones realizadas a través del Servidor.
- La carga y almacenamiento de Certificados Digitales para las opciones de seguridad OFTP v 2.0

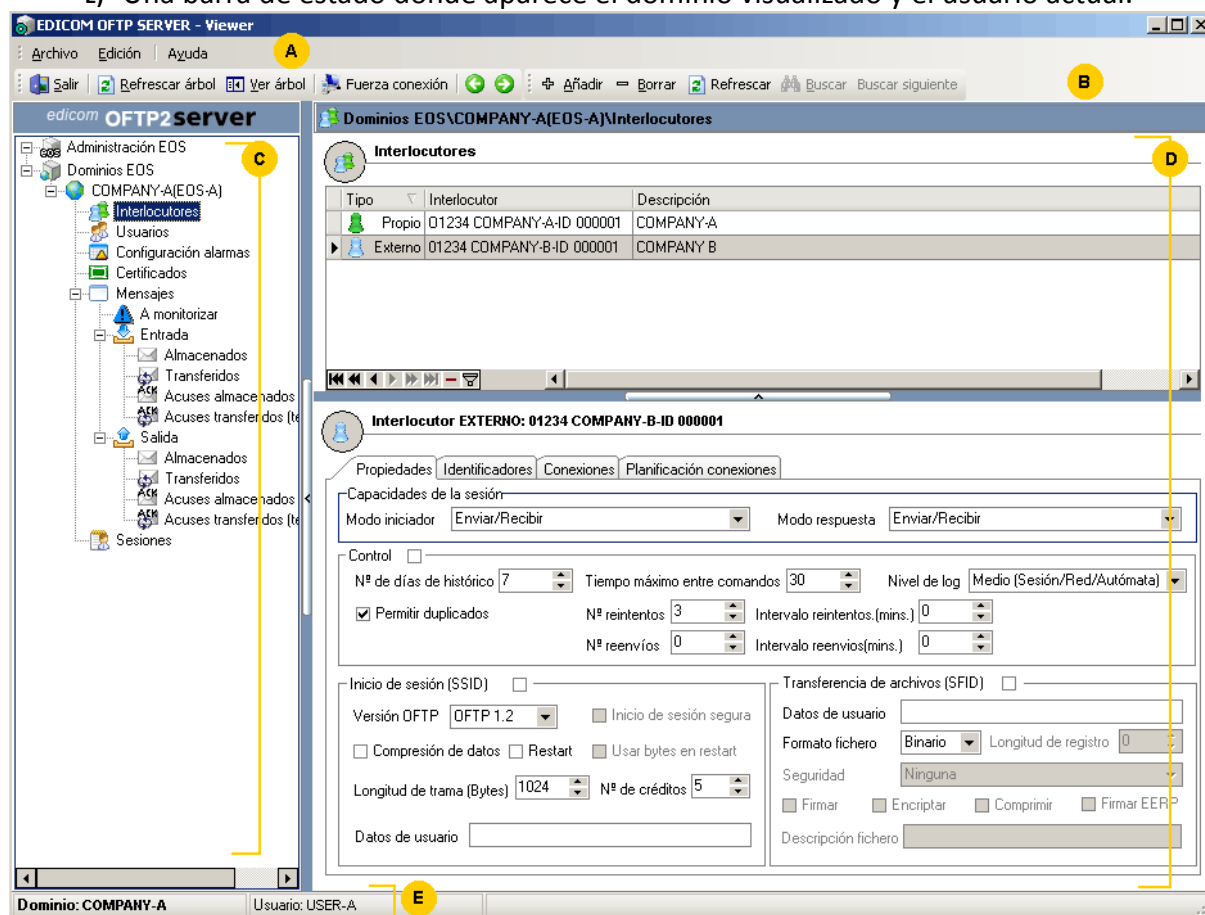
Para acceder al EOS Viewer.

- **Paso 1.-** Lanzar el Ejecutable EOFTPS.exe que inicia el servidor **EOS**
- **Paso 2.-** Una vez arrancado el **EOS** utilizar una de estas dos opciones:
  - Desde el botón **Configuración** panel de motorización del **EOS**.
  - Desde el ejecutable **EOFTPV.exe** dentro de la carpeta de instalación.

## 1.2 EL EOS VIEWER

La interfaz del visor **EOS** esta dividida en las siguientes secciones

- Un menú principal de aplicación.
- Una barra de herramientas con botones de acceso rápido.
- Un menú en forma de árbol de nodos para acceder a los distintos paneles de gestión del dominio.
- La zona de gestión donde aparecerá un panel adecuado a cada opción (en el ejemplo interlocutores). En la parte superior aparece la ruta completa de la situación
- Una barra de estado donde aparece el dominio visualizado y el usuario actual.



### 1.2.1 MENÚ PRINCIPAL

**Salir.** Permite salir del **EOS Viewer**.

**Conexión remota.** Permite configurar el acceso al EOS vía *Web Services*.

<b>Refrescar árbol.</b> Permite refrescar todos los contenidos del <b>EOS Viewer</b> .
<b>Ver árbol.</b> Permite mostrar u ocultar el árbol de secciones.
<b>Fuerza conexión.</b> Permite forzar la conexión entre dos interlocutores del dominio seleccionado.

### 1.2.2 BARRA DE HERRAMIENTAS PRINCIPAL

<b>Salir.</b> Permite salir del EOS Viewer.
<b>Refrescar árbol.</b> Permite refrescar todos los contenidos del EOS Viewer.
<b>Ver árbol.</b> Permite mostrar u ocultar el árbol de secciones.
<b>Fuerza conexión.</b> Permite forzar la conexión entre dos interlocutores del dominio seleccionado.
(Anterior) Permite acceder a la anterior sección ya visitada.
(Siguiente) Permite acceder a la siguiente sección ya visitada.
<b>Añadir.</b> Permite acceder un nuevo elemento correspondiente a la sección actualmente visible, por ejemplo un Interlocutor, un usuario o un mensaje.
<b>Borrar.</b> Permite borrar el elemento seleccionado en la sección actualmente visible, por ejemplo un Interlocutor, un usuario o un mensaje.
<b>Refrescar.</b> Permite refrescar los contenidos de la sección actualmente visible.

### 1.2.3 ÁRBOL DE NODOS

El árbol de nodos permite acceder rápidamente a todas las secciones del dominio. Cada dominio posee los siguientes nodos.



- **Interlocutores.** Esta opción permite gestionar los interlocutores del dominio (crear, borrar, editar). En la sección de interlocutores se crean también los Identificadores OFTP adicionales y las comunicaciones.
- **Usuarios.** Esta opción permite gestionar usuarios (crear, borrar, editar) del dominio, establecer su contraseña de acceso y configurar sus permisos dentro del dominio.

- **Configuración de alarmas.** Esta opción permite añadir alarmas del dominio. Estas alarmas permiten la monitorización de los eventos que ocurren en el servidor desde una cuenta de correo e-mail.
- **Certificados.** Esta opción permite añadir al servidor los certificados electrónicos utilizados para las opciones de encriptación y firma electrónica (OFTP 2).
- **Mensajes.** Esta opción permite ver todos los mensajes y acuses de mensaje del dominio y monitorizar su estado.
- **Sesiones.** Esta opción permite monitorizar los registros de actividades (logs) asociados a cada sesión de comunicaciones OFTP

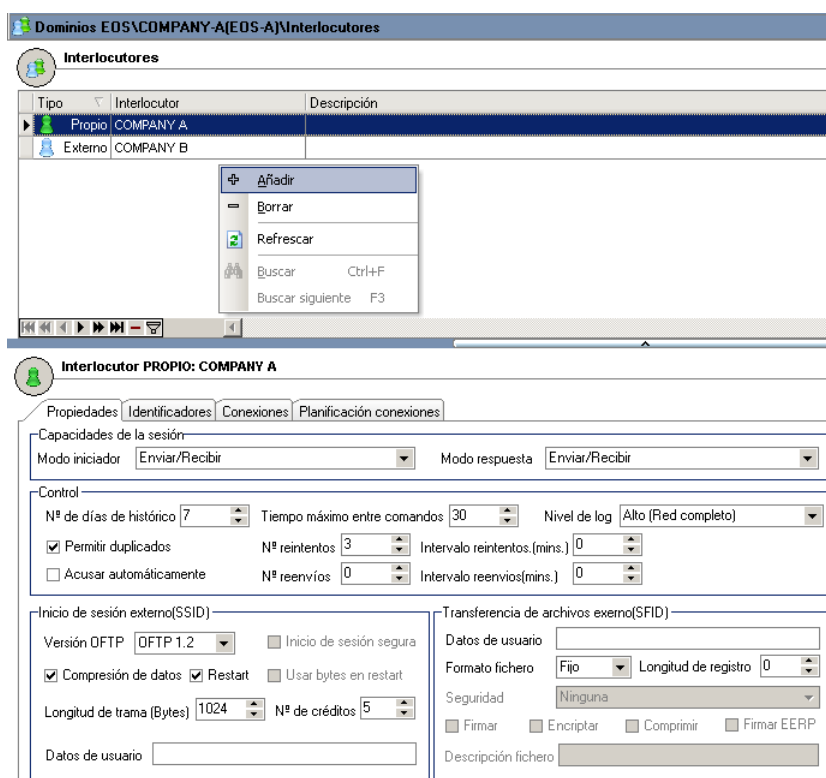
## 2 INTERLOCUTORES

### 2.1 INTRODUCCIÓN

Un dominio en el **EOS** es básicamente un conjunto de interlocutores que están de acuerdo en intercambiarse información a través del protocolo OFTP.



- **Interlocutor  Propio.** El interlocutor correspondiente a la empresa gestora del dominio.
- **Interlocutor  Externo.** Socios comerciales del gestor del dominio con los cuales quiere establecer comunicaciones.

Para que la comunicación a través del servidor sea posible es necesario que cada uno de los interlocutores intercambie con el otro previamente cierta información de identidad, relacionada con el Protocolo OFTP y sus especificaciones.



Una vez se conocen estos datos es posible dar de alta en la aplicación el perfil del interlocutor (tanto propio como externo). Si no se ha dado de alta o no se ha configurado correctamente el perfil de un interlocutor, el servidor será incapaz de establecer comunicación.

La interfaz del gestor de interlocutores está dividida en dos secciones.

- En la parte superior aparecen todos los interlocutores creados en el dominio, donde se pueden seleccionar, añadir o borrar. Cada uno identificado con su nombre y con un icono según sea externo  o propio .



- En la parte inferior aparece la información asociada al interlocutor seleccionado en ese momento dividida en varias pestañas.

## 2.2 CREAR UN INTERLOCUTOR

---

Para dar de alta un nuevo interlocutor, desde la sección superior del gestor de interlocutores:

- Menú contextual (botón derecho del ratón): Opción **Añadir**.

Aparece el formulario de configuración de un nuevo interlocutor. Este conjunto de datos permite indicar los datos de identificación del interlocutor, tanto dentro del dominio como para la comunicación OFTP

- **Interlocutor.**
  - **Tipo de interlocutor.** Permite indicar si es un interlocutor Propio o Externo. Este campo es obligatorio.
- **Datos de identificación.**
  - **Nombre.** Nombre del interlocutor en el EOS y en el inicio de las comunicaciones. Este campo es obligatorio.
  - **Identificador OFTP.** Identificador del interlocutor para comunicaciones OFTP. Este es el código identificador unívoco del interlocutor dentro del mundo OFTP. Este campo es obligatorio.
- **Propiedades para el inicio de sesión SSID (Start Session ID).**
  - **Contraseña.** Permite indicar la contraseña que se envía en el SSID y que, junto al **Nombre** verifica la identidad del interlocutor al inicio de la sesión. Esta contraseña tiene carácter restringido pero debe ser intercambiada entre los interlocutores que van a establecer comunicación.
  - **Certificado de la sesión.** Permite seleccionar un certificado para utilizar con las opciones opcionales OFTP v2.0 de sesión segura y firma electrónica del SSID.
- **Propiedades para la transferencia de ficheros SFID (Start File ID).**
  - **Certificado de firma.** Permite seleccionar un certificado para utilizar las opciones OFTP v2.0 de firma electrónica de los ficheros enviados.
  - **Certificado de cifrado.** Permite seleccionar un certificado para utilizar las opciones OFTP v2.0 de cifrado de los contenidos enviados.
  - **Certificado de firma de EERPs.** Permite seleccionar un certificado para utilizar las opciones OFTP v2.0 de firma electrónica de los acuses de recepción EERP (*End to End ResPonse*).

- **Script de almacenamiento.** Permite indicar una función de código **Ediwin Script** destinada a modificar el archivo original y así pre-tratar los ficheros al almacenarlos. El código Ediwin Script es un lenguaje de las aplicaciones EDICOM.
- **Propiedades adicionales (para la integración y acceso Web Services).**
  - **Contraseña de integración.** Permite indicar la contraseña de acceso a EOS a través del protocolo de acceso SOAP permitiendo descargar por WebServices los mensajes recibidos en este dominio y este interlocutor. Se trata de un parámetro habilitado únicamente para interlocutores propios. Esta contraseña es **totalmente privada**.

**Importante:** No se debe confundir la contraseña de integración con la contraseña de inicio de sesión SSID. La Contraseña de integración elegida NO DEBE SER COMUNICADA A UN INTERLOCUTOR EXTERNO BAJO NINGÚN CONCEPTO.

- **Identificador externo.** Permite indicar un identificador del interlocutor en un sistema informático externo para facilitar la integración de los datos.

**Nota:** Para más información sobre el uso de certificados y las opciones de seguridad OFTPv 2.0 ver [Certificados](#)

## 2.3 DATOS DE UN INTERLOCUTOR

### 2.3.1 PESTAÑA PROPIEDADES

Las propiedades de un interlocutor establecen tanto parámetros de la comunicación OFTP como parámetros propios de gestión del EOS. Algunas de estas propiedades son heredadas de la configuración por defecto del Servidor y se recomienda no hacer modificaciones.

Cuando se crea un nuevo interlocutor **externo**, los parámetros se obtienen del interlocutor propio del dominio, y algunos campos de la pestaña Propiedades no se pueden modificar. Para permitir la modificación de los parámetros de un interlocutor externo hay que habilitar la casilla que aparece al inicio del grupo de opciones.

**Interlocutor EXTERNO:**

Propiedades | Identificadores | Conexiones | Planificación conexiones

Capacidades de la sesión

Modo iniciador: Enviar/Recibir      Modo respuesta: Enviar/Recibir

**Control** ☐

Nº de días de histórico: 7      Tiempo máximo entre comandos: 30      Nivel de log: Alto (Red completo)

☒ Permitir duplicados      Nº reintentos: 3      Intervalo reintentos.(mins.): 0

Nº reenvíos: 0      Intervalo reenvios(mins.): 0

**Inicio de sesión (SSID)** ☐

Versión OFTP: OFTP 1.2      ☐ Inicio de sesión segura

☐ Compresión de datos      ☐ Restart      ☐ Usar bytes en restart

Longitud de trama (Bytes): 1024      Nº de créditos: 5

Datos de usuario:

**Transferencia de archivos (SFID)** ☐

Datos de usuario:

Formato fichero: Binario      Longitud de registro: 0

Seguridad: Ninguna

☐ Firmar      ☐ Encriptar      ☐ Comprimir      ☐ Firmar EERP

Descripción fichero:

## Capacidades de la sesión

Este grupo permite indicar qué capacidades se le permiten al interlocutor en el dominio, Enviar mensajes, Recibir mensajes o Ambas. Normalmente esto depende del modo en que este trabajando el EOS en cada comunicación con este interlocutor.

- **Modo iniciador.** Permite indicar si al interlocutor se le permite enviar, recibir o ambos cuando el EOS trabaja en modo Iniciador (*Initiator*).
- **Modo respuesta.** Permite indicar si al interlocutor se le permite enviar, recibir o ambos cuando el EOS trabaja en modo Respuesta (*Responder*).

## Control

En este grupo se configuran parámetros relacionados con el interlocutor dentro del EOS, no son datos propios del OFTP.

- **Nº de días de histórico.** Permite indicar el número de días de almacenamiento de los mensajes.
- **Tiempo máximo entre comandos.** Permite indicar el tiempo máximo entre la envío de un comando OFTP y ella recepción o envío del siguiente. Cuando vence este valor provoca un error en la sesión, y de esta forma evitamos un bloqueo.
- **Nivel de log.** Permite indicar el nivel de log a reportar en las comunicaciones con este interlocutor. Este log se reportará en el nodo *Sesiones* como una nueva entrada. Existen tres opciones que corresponden al nivel de detalle del reporte. Para más información ver [Sesiones](#).
- **Permitir duplicados.** Permite indicar cómo se comportará el servidor con los mensajes duplicados. Si permitimos duplicados significa que a la llegada en un mismo mensaje (mismo nombre de fichero virtual , fecha y hora) si el mensaje ya almacenado en eso está en situación terminal (mensaje transferido o acuse transferido), entonces se crea un nuevo mensaje. Por contra si no se permiten duplicados en mensaje se marcará como erróneo.
- **Nº reintentos.** Permite indicar el número de reintentos de envío que realizará el EOS con un mensaje dado de este antes de marcarlo como erróneo.
- **Nº reenvios.** Si transcurrido un tiempo no se recibe el acuse de un mensaje es se vuelve a reenviar tantas veces como indiquemos en este parámetro.
- **Intervalo reintentos.** Permite indicar en minutos el intervalo entre reintentos.
- **Intervalo reenvios.** Permite indicar en minutos el intervalo entre reenvios.

### ***Inicio de sesión (SSID)***

Este grupo contiene información sobre la negociación de la transmisión de archivos. Son datos propios de OFTP que se envían al inicio de la sesión con el comando SSID (*Start Session Identification*). Algunos de estos parámetros deben ser acordados previamente entre los interlocutores.

- **Versión OFTP.** Permite seleccionar la versión que este interlocutor va a utilizar tanto para el envío como para la recepción. Si dos interlocutores utilizan versiones distintas, se realiza una negociación a la baja para evitar incompatibilidades.
  - **Inicio de sesión segura.** Permite indicar que el interlocutor se comunica con inicio de sesión segura, utilizando un certificado electrónico para firmar electrónicamente el comando SSID y la información que contiene. Esta opción solo esta disponible para la versión OFTP v2.0. Ver [Certificados](#)
- **Compresión de datos.** Permite indicar que el interlocutor realiza una compresión de los ficheros enviados.
- **Restart.** Permite indicar si el servidor negociará el reinicio de una transmisión interrumpida. Si se activa esta opción permite que al volver a transmitir un mensaje parcialmente enviado solo se transmita a partir de la posición que indique el receptor.
  - **Usar bytes en restart.** Habitualmente la posición restar se indica en Kbytes. Existen softwares que por contra utilizan bytes. Con esta opción podemos indicar esta forma excepcional de trabajar con un interlocutor dado.
- **Longitud de trama (Bytes).** Permite indicar la longitud de cada trama de datos de la transmisión OFTP.
- **Nº de créditos.** Permite indicar el número de créditos (Buffer de datos) que este interlocutor otorga a sus interlocutores antes de pausar la comunicación momentáneamente. De este modo el receptor controla el flujo de la información que recibe.
- **Datos de usuario.** Permite indicar contenido adicional a declarar en el comando SSID.

### ***Transferencia de archivos (SFID).***

Este grupo contiene información que se declara en el comando SFID (*Start File Identification*), que identifica el inicio de la transmisión de un fichero virtual y contiene información importante para que el receptor lo procese correctamente.

- **Datos de usuario.** Permite indicar contenido adicional a incluir en el comando SFID
- **Formato fichero.** Permite seleccionar el formato del fichero virtual. Las opciones son:

- *Binario*: indica un formato de archivo binario no estructurado.
  - *Texto*: indica un formato de archivo de texto.
  - *Fijo*: indica un formato de archivo binario fijo.
  - *Variable*: indica un formato de archivo binario variable.
- **Longitud de registro.** Longitud en bytes del registro lógico más largo transferido del archivo. No es necesario definir este atributo para archivos de tipo *Texto* o *Binario* no estructurado.
  - **Seguridad.** Permite seleccionar el nivel de seguridad para la transmisión de archivos. No es necesario definir parámetros de seguridad si no se utiliza la versión OFTP 2.0. Las siguientes opciones también están asociadas a la seguridad.
    - **Firmar.** Indica que se aplica firma electrónica a los ficheros virtuales de este interlocutor.
    - **Encriptar.** Indica que se aplica encriptación a los ficheros virtuales de este interlocutor.
    - **Comprimir.** Indica que se aplica compresión estándar a los ficheros virtuales de este interlocutor.
    - **Firmar EERP.** Indica que se aplica firma digital a los acuses de recepción EERP (*End to End Response*) generados por este interlocutor al recibir correctamente el fichero.
  - **Descripción del fichero.** Permite indicar una descripción o nombre opcional acordado por los interlocutores para identificar el fichero.

---

**Nota:** Para las opciones de firma y encriptación asociadas a la versión OFTP v2.0 es necesario la utilización de Certificados digitales de firma electrónica. Ver [Certificados](#).

## 2.3.2 PESTAÑA IDENTIFICADORES

El concepto "identificador" OFTP se utiliza para definir de forma unívoca los diferentes actores que participan en la transferencia de los archivos.

En OFTP los identificadores se utilizan en varias de las fases del protocolo, que se resumen en dos. Por una parte los utilizados en el inicio de sesión (SSID) y por otra en la transferencia de archivos (SFID) y acuses (EERP). Normalmente los primeros identifican a la organización a nivel a nivel físico, y los segundos identifican a los diferentes partes de la organización.

Es posible que un interlocutor EOS (una empresa, por ejemplo) tenga asociados varios identificadores OFTP respondiendo a una organización interna u otros motivos, pero compartiendo la misma configuración de propiedades.

En ese caso, en lugar de crear un nuevo perfil de interlocutor, se le asocia un nuevo identificador OFTP distinto al principal pero que comparte toda su configuración como

interlocutor. Esto se conoce en EOS se conoce como identificadores lógicos. En contraposición al identificador central, el identificador parametrizado al crear el interlocutor.

Los identificadores lógicos no se reflejan en el listado principal de interlocutores, se gestionan desde la pestaña *Identificadores*. Donde se representan con iconos distintos los identificadores principales o centrales de los identificadores asociados posteriormente al interlocutor.

	Identificador (SSID/SFID)	Nombre
	01234 COMPANY-A-ID 000001	COMPANY-A
	01234 COMPANY-A-ID 000002	Company A02 (Lógico)
	01234 COMPANY-A-ID 000003	Company A03 (Lógico)

Para añadir un nuevo identificador lógico, desde:

- Menú contextual sobre el listado: opción **Añadir**.

Se accede así al formulario para configurar el nuevo identificador. El formulario es muy similar al que aparece al crear un interlocutor y **básicamente es necesario configurar el nuevo identificador OFTP y una descripción**.

***Nota:** Para un identificador lógico no es necesario indicar la contraseña para el Inicio de sesión ya que e toma la del identificador central.*

### 2.3.3 PESTAÑA CONEXIONES

Cada conexión se configura de manera independiente por interlocutor en la pestaña *Conexiones*. En este listado cada línea corresponde con una conexión distinta y cada columna refleja la siguiente información.

- Si la conexión esta activa o inactiva. Si el icono esta en verde la conexión está activa.
- Si la conexión es de entrada o de salida. Depende del tipo de interlocutor.
- El protocolo utilizado. RDSI (ISDN) o TCP/IP.
- Descripción de referencia de la comunicación.
- Un resumen de los parámetros de la configuración.

Para crear una nueva conexión, desde el listado de conexiones.

- Menú contextual: opción **Añadir**

Se accede así al formulario de configuración de la conexión. En el formulario se pueden parametrizar los siguientes datos

- **Tipo.** Indica si se trata de una conexión de entrada o salida. Normalmente este valor esta limitado según el tipo de interlocutor seleccionado.
  - Para un interlocutor Propio se puede configurar la conexión de entrada.
  - Para un interlocutor Externo se puede configurar la conexión de envío.
- **Protocolo.** Permite seleccionar el protocolo de conexión, Puede ser RDSI (ISDN) o TCP/IP. Según la selección estarán disponibles opciones adicionales de configuración.
- **Descripción.** Permite indicar una descripción opcional para identificar la conexión.
- **Activa.** Permite indicar si la conexión estará activa o inactiva. Esto se refleja en el listado de conexiones.

#### ***Configuración adicional para TCP/IP***

Estos parámetros son necesarios si el protocolo de conexión es TCP/IP

- **Dirección IP.** Permite indicar la dirección IP del Servidor.
- **Puerto IP.** Permite indicar el puerto IP para la transmisión de los mensajes OFTP.
- **Tipo SSL.** Permite indicar el tipo y versión del protocolo SSL o TLS a utilizar.
- **Certificado.** Permite indicar el certificado a utilizar para el protocolo SSL o TLS.

#### ***Configuración adicional para RDSI***

Estos parámetros son necesarios si el protocolo de conexión es RDSI

- **Nº RDSI local.** Permite indicar el Numero RDSI dentro de la red local.
- **Nº RDSI remoto.** Permite indicar el Número RDSI que se refleja externamente.
- **Controlador.** Permite especificar, si es necesario, el controlador RDSI a utilizar para la conexión.
- **Servidor.** Permite seleccionar, si es necesario, el servidor a través del cual se realiza la conexión.

### **2.3.4 PESTAÑA PLANIFICACIÓN DE CONEXIONES**

La pestaña de *planificación de conexiones* permite habilitar y configurar la transmisión automatizada de mensajes de este interlocutor.

Envío de mensaje y acuses.

- **Intervalo mínimo entre envíos (Segundos).** Permite indicar el intervalo mínimo entre envíos.
- **Forzar conexión temporizada.** Permite indicar un plan semanal para la transferencia de mensajes asociados a este interlocutor.
- **Frecuencia horaria.** Permite indicar un plan durante el día para la transferencia de mensajes asociados a este interlocutor.



## 3 USUARIOS

### 3.1 INTRODUCCIÓN

---

Para acceder al EOS Viewer un usuario debe identificarse al inicio de cada sesión, indicando su nombre de usuario y su contraseña. Los usuarios asociados a un determinado dominio solo pueden visualizar la información asociada a dicho dominio.

Toda la información de un usuario, incluido su nombre de usuario y contraseña se gestionan desde el nodo *Usuarios*, donde aparece un listado con todos los usuarios habilitados en el dominio.

### 3.2 CREAR NUEVO USUARIO

---

Para añadir un nuevo usuario, desde:

- Menú contextual (botón derecho) sobre el listado: opción **Añadir**.

Aparecerá un formulario para indicar el **Nombre de usuario** y su **descripción**. Al aceptar el nuevo usuario del dominio aparecerá en la lista superior. Este nuevo perfil de usuario todavía no está configurado. Los datos personales y permisos de acceso pueden verse y configurarse en la parte inferior del panel cuando el usuario está seleccionado.

Los datos de usuario son:

- **Descripción**. Permite indicar una descripción opcional del usuario.
- **Cargo**. Permite indicar una descripción opcional del cargo o función del usuario dentro del dominio.
- **Contraseña**. Permite indicar la contraseña que, asociada al Nombre de usuario, se utiliza para identificarse en el servidor. Es necesario repetir la contraseña para confirmar que es correcta.
- **E-mail**. Permite indicar una cuenta email de contacto.
- **Teléfono**. Permite indicar un teléfono de contacto.
- **Idioma**. Permite indicar el idioma del usuario.
- **Nº Máximo de mensajes a visualizar**. Permite indicar un número máximo de mensajes a visualizar. Esta opción permite limitar la cantidad de mensajes que el servidor muestra en el nodo *Mensajes* mejorando en algunos casos el rendimiento. Este límite solo estará activo para este usuario.

- **Nº Máximo de sesiones a visualizar.** Permite indicar un número máximo de sesiones a visualizar. Esta opción permite limitar la cantidad de sesiones que el servidor muestra en el nodo *Sesiones* mejorando en algunos casos el rendimiento. Este límite solo estará activo para este usuario.
- **Usuario para modo desasistido (Batch).** Permite indicar que este usuario y su configuración se ha creado para realizar procesos en modo desasistido.
- **Permisos.** Permite seleccionar a qué opciones y funciones tendrá acceso este usuario. El grupo de opciones representan todas las funciones posibles dentro del dominio. Esto permite establecer roles y niveles de acceso distintos para los usuarios del dominio.
  - **Configuración general.** Permite acceder a la configuración general del dominio.
  - **Configurar alarmas.** Permite acceder al nodo *Configuración de alarmas* del dominio.
  - **Configurar conexiones.** Permite acceder a la pestaña *Conexiones* dentro de *Interlocutores*.
  - **Configurar dominios.** Permite crear y modificar nuevos dominios.
  - **Configurar certificados.** Permite acceder al nodo *Certificados* del dominio.
  - **Ver mensajes.** Permite acceder al nodo *Mensajes*, donde se visualiza el histórico de los mensajes y acuses de recepción.
  - **Configurar usuarios.** Permite acceder al nodo *Usuarios* (esta misma sección).

**Importante.** Esta opción debería inhabilitarse para aquellos usuarios que no sean administradores ya que accediendo a esta misma sección podrían modificar sus permisos.

- **Configurar interlocutores.** Permite acceder al nodo *Interlocutores*.
- **Crear mensajes.** Permite generar mensajes desde el visor del EOS. Esto se realiza desde el nodo *Mensajes*.

## 4 CONFIGURACIÓN DE ALARMAS

### 4.1 INTRODUCCIÓN

---

El servidor puede generar notificaciones e-mail asociadas a determinados eventos que faciliten la monitorización de dichos eventos sin necesidad de estar conectado al servidor.

De manera genérica las alarmas son provocadas por tres eventos:

- **Sesión OFTP.** Permite notificar inicios de sesión OFTP realizadas en el servidor. Tanto en modo *Responder* como *Iniciator*.
- **Peticiones SOAP (WebServices).** Permite notificar peticiones de documentos a través de WebServices.
- **Sistema.** Permite notificar normalmente errores relacionados con el sistema.

Cada uno de estos eventos, o los tres al mismo tiempo, pueden generar una notificación que se recibirá en una cuenta de correo asociada a la alarma.

### 4.2 CREAR NUEVA ALARMA

---

Para añadir una nueva alarma, desde el panel de configuración de alarmas:

- Menú contextual: Opción **Añadir**.

Aparecerá un formulario de configuración de la nueva alarma, con los siguientes parámetros.

- **Descripción.** Permite indicar una descripción única asociada a la alarma para identificarla en el listado.
- **Activa.** Permite activar o desactivar una alarma. Si una alarma esta inactiva no se recibirán notificaciones. Puede activarse más tarde reanudando las notificaciones.
- **Servidor de correo.** Este grupo de opciones permite configurar los parámetros para el envío de correos electrónicos al servidor de destino.
- **Alarmas a tratar.** Pueden seleccionarse los eventos que provocarán las notificaciones. Si ningún evento es señalado no se recibirán notificaciones.

## 5 CERTIFICADOS

### 5.1 INTRODUCCIÓN

---

El Servidor EOS permite el uso de certificados digitales para enviar y recibir transmisiones con opciones de encriptación y firma electrónica, Estas opciones son fundamentalmente implementadas por la especificación OFTP V 2.0.

Estas opciones de seguridad necesitan del uso de certificados digitales que permiten el uso de firma electrónica aplicada de manera independiente a los diversos elementos que forman parte de una transmisión OFTP. Todos estos niveles de seguridad se van añadiendo unos sobre otros para maximizar la confidencialidad de la comunicación entre el Emisor y el Receptor.

- Firma electrónica del canal de conexión (TLS o SSL).
- Firma electrónica de la información de inicio de sesión (SSID) y el identificador OFTP.
- Firma electrónica de los propios mensajes (Ficheros virtuales y EERP).
- Encriptación de los mensajes.

Para todos estos niveles de seguridad se puede usar el mismo certificado o distintos certificados.

### 5.2 AÑADIR UN CERTIFICADO

---

Si el propietario de un dominio tiene previsto establecer comunicaciones con opciones de seguridad, es necesario previamente añadir los ficheros de certificados digitales correspondientes a las claves privadas y públicas que se van a utilizar.

Los certificados digitales que se cargan en el servidor solo están disponibles para el dominio desde el cual se han cargado.

- El EOS es capaz de firmar electrónicamente los mensajes de salida utilizando para ello una clave Privada. Cuando se añade una clave privada al servidor se exige indicar la contraseña.
- El EOS es capaz de validar los mensajes de entrada, firmados electrónicamente por el emisor, utilizando para ello la clave pública del emisor. Cuando se añade una clave pública al servidor no es necesario indicar ninguna contraseña.

---

*Nota: Para más información sobre el uso de certificados digitales para la Firma electrónica consulte con el departamento técnico de EDICOM*

Para añadir un certificado al listado de certificados del dominio simplemente desde:

- Menú contextual: opción **Añadir**.

Aparecerá entonces un pequeño formulario para incluir el archivo físico de certificado

- **Fichero a importar.** Permite indicar o buscar en el disco el certificado digital. Archivos con extensión \*.p12, \*.key o \*.pfx
- **Password clave privada.** Permite indicar, si se trata de una clave privada, la contraseña que identifica al usuario como propietario del certificado.

## 5.3 NIVELES DE SEGURIDAD

---

Las opciones de seguridad y sus certificados correspondientes se configuran en distintos puntos del EOS, normalmente durante la configuración de interlocutores.

### 5.3.1 FIRMA ELECTRÓNICA DEL CANAL DE CONEXIÓN (TLS o SSL)

Esta opción se habilita dentro de la sección *Interlocutores*, al crear una nueva conexión en la pestaña "Conexiones". Solo esta disponible para comunicaciones a través del protocolo TCP/IP.

En este nivel de seguridad se firma y encripta el canal de conexión asegurando que ningún tercero puede acceder a la información enviada entre el receptor y el emisor del mensaje, evitando el acceso no autorizado de un tercero a la comunicación.

### 5.3.2 FIRMA ELECTRÓNICA DE LA INFORMACIÓN DE INICIO DE SESIÓN (SSID)

Esta opción se habilita dentro de la sección *Interlocutores*, al crear un nuevo interlocutor o, en la pestaña *Identificadores*, al añadir un nuevo identificador. En el grupo *Propiedades para el inicio de sesión (SSID)*, en el campo **Certificado de sesión**.

La firma electrónica del inicio de sesión permite asegurar a los interlocutores que tanto el *Iniciador* como el *Responder* son quienes afirman ser antes de aceptar la transmisión, evitando la suplantación de alguno de los dos.

### 5.3.3 FIRMA ELECTRÓNICA DE LOS MENSAJES (SFID Y EERP)

Esta opción se habilita dentro de la sección *Interlocutores*, al crear un nuevo interlocutor o, en la pestaña *Identificadores*, al añadir un nuevo identificador. En el grupo **Propiedades para la transferencia de ficheros (SFID)**, campos **Certificado de firma** y **Certificado de firma de EERPs**.

La firma electrónica en los ficheros virtuales permite asegurar que quien recibe o emite el mensaje es en realidad quien dice ser. Evitando la suplantación como emisor.

El Iniciador de la comunicación además puede exigir la firma electrónica de EERP. Asegurando al emisor del archivo que quien ha recibido el mensaje es en realidad quien dice ser, evitando la suplantación como receptor.

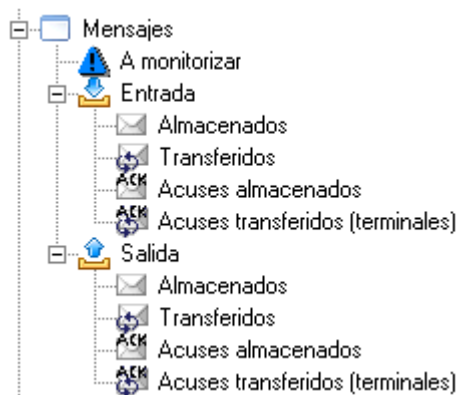
### 5.3.4 ENCRIPCIÓN

Esta opción se habilita dentro de la sección *Interlocutores*, al crear un nuevo interlocutor o, en la pestaña *Identificadores*, al añadir un nuevo identificador. En el grupo **Propiedades para la transferencia de ficheros (SFID)**, en el campo Certificado de cifrado.

La encriptación de los SSID, SFID y EERP es un paso más en la seguridad de la transmisión., evitando el acceso no autorizado de un tercero a la información.

## 6 MENSAJES

### 6.1 INTRODUCCIÓN



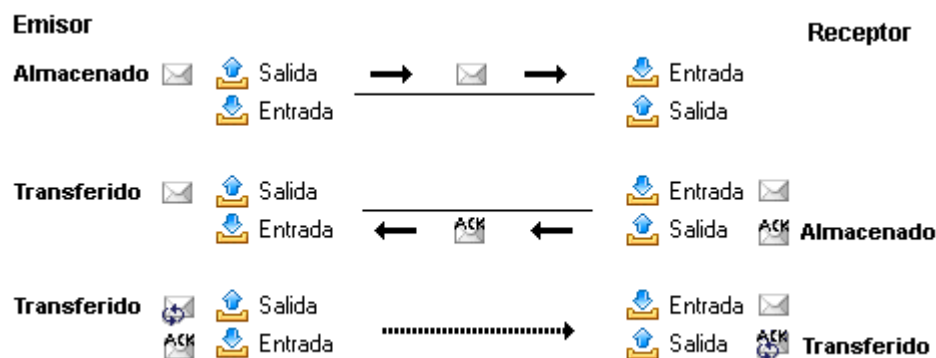
La sección **Mensajes** permite acceder a un histórico de los mensajes transmitidos a través del servidor. Los mensajes reflejados en esta sección son tanto los ficheros virtuales como los acuses de recepción asociados a la recepción de dichos ficheros.

Para introducir el uso de esta sección se deben definir claramente los conceptos OFTP asociados al envío y recepción de mensajes y su representación equivalente dentro del EOS.

#### 6.1.1 CICLO DE UN MENSAJE

Cuando se inicia una comunicación con la intención de enviar un archivo virtual se inicia el ciclo del mensaje dentro del servidor. Sin tener en cuenta los procesos de transmisión y de una manera resumida el ciclo es este:

1. **Paso 1.-** El archivo virtual es enviado por el emisor hacia la bandeja de entrada del receptor. El documento aparece como "Almacenado" en la bandeja de salida del emisor.
2. **Paso 2.-** El archivo virtual es recibido en su bandeja de entrada por el receptor, en espera de ser procesado, una vez procesado se genera un acuse de recepción. Este acuse de recepción aparece en el dominio del receptor como "Almacenado" en la bandeja de salida.
3. **Paso 3.-** El acuse de recepción es recibido por el emisor del fichero confirmando así que su fichero ha sido debidamente integrado. Esto produce dos efectos. Primero, el archivo virtual que permanecía todavía como "Almacenado" en la bandeja de salida del emisor pasa a estado "Transferido". Segundo, automáticamente se emite una confirmación de recepción del propio acuse (no tiene representación porque no se trata de un comando OFTP sino una confirmación propia del EOS) pasando su estado también a "Transferido" en la carpeta de Salida del Receptor.



Cuando ambos mensajes, el Fichero y el Acuse de recepción están en estado "Transferidos" tanto para el receptor como en el emisor, se cierra el ciclo del envío de mensajes OFTP.

## 6.2 CREAR UN NUEVO MENSAJE

Es posible generar un nuevo mensaje partiendo de cero desde el propio servidor seleccionando el Origen, el Destino y el fichero que se quiere enviar como fichero virtual.

Para realizar el envío de un mensaje desde el propio servidor, desde el listado de mensajes:

- Menú contextual (botón derecho del ratón): opción **Añadir**

Aparece el formulario de nuevo mensaje, donde se parametrizan los siguientes datos.

- **Origen.** Permite seleccionar de los interlocutores propios el interlocutor de origen.
- **Destino.** Permite seleccionar de los interlocutores externos el interlocutor de destino
- **Fichero.** Permite seleccionar del disco duro el fichero que va a ser enviado como fichero virtual.
- **Datos opcionales.** Este grupo de opciones ya está definido en el SFID del interlocutor de origen, pero al generar un documento es posible configurar manualmente parámetros distintos
  - **Datos usuario.** Permite indicar información opcional que se envía con el mensaje.
  - **Formato.** Permite seleccionar el formato del fichero virtual.
  - **Longitud de registro.** Permite indicar la longitud máxima de registro del fichero virtual.
  - **Descripción.** Permite indicar una descripción adicional del fichero virtual.
  - **Seguridad.** Permite seleccionar una opción de seguridad para el envío de este mensaje en concreto.



- **Firmado. Comprimido, Encriptado y Acuse firmado** permite habilitar estas opciones para el envío de este mensaje en concreto.

Una vez configurado, al apretar la opción **Aceptar**, el mensaje aparece en la tabla de mensajes con el estado "Almacenado".

## 6.3 CARACTERÍSTICAS DE UN MENSAJE

---

### *Ficheros Virtuales y Acuses de recepción*

- Los **ficheros virtuales** son los archivos binarios enviados por el emisor al receptor a través de OFTP.
- Los **acuses de recepción** son los mensajes enviados por el receptor como respuesta al final de la recepción de un fichero virtual, se emiten cuando este fichero virtual ha sido integrado en su destino final (o si ha existido algún problema al integrarlo, en ese caso sería un acuse de recepción negativo).

La sección de mensajes se organiza en nodos distintos, que contienen los mensajes según su dirección (entrada y salida) y dentro de cada nodo si se trata de Ficheros virtuales o Acuses de recepción y si estos están en situación Almacenados o Transferidos.

### *Mensajes de Entrada y Salida*

- Los **mensajes de entrada** (ficheros virtuales o acuses) son aquellos que el interlocutor propio ha recibido de un interlocutor externo.
- Los **mensajes de salida** (ficheros virtuales o acuses) son aquellos que el interlocutor propio ha enviado hacia un interlocutor externo.

Es importante tener en cuenta que los mensajes almacenados en los subnodos Mensajes-Entrada y Mensajes-Salida no hacen referencia al rol del interlocutor en la comunicación (*Initiator* o *Responder*) sino a la dirección de la comunicación del mensaje en relación con el interlocutor Propio.

### *Mensajes Almacenados y Transferidos*

- Los mensajes **Almacenados** son aquellos que están listos para enviarse. Este concepto identifica la situación temporal de aquellos mensajes listos para ser enviados en la próxima comunicación del servidor (o aquellos cuya recepción no ha sido todavía confirmada).
- Los mensajes **Transferidos** son aquellos cuya recepción ha sido confirmada por su destinatario. Una vez la recepción de un mensaje ha sido confirmada, estos mensajes pasan de la situación Almacenado a Transferidos. Que es su situación final.

Se ha de aclarar que el protocolo OFTP contempla el envío de un acuse de recepción (EERP) de los archivos virtuales. Esto permite pasar de Almacenados a Transferidos los mensajes de tipo fichero Virtual.

Pero el EOS permite adicionalmente la confirmación de la recepción de los Acuses de recepción. Por tanto los acuses de recepción también pasan de la situación Almacenados a Transferidos cuando se confirma que se han recibido correctamente.

Si un mensaje permanece mucho tiempo en almacenados sin motivo aparente puede ser indicio de un problema en la configuración de la comunicación o del interlocutor.

## 6.4 LISTADO DE MENSAJES

Drag a column header here to group by that column

	Identificador	SSID Propio	SSID Externo	Origen SFID	Destino SFID	Situación	Tipo acuse
	10042318032325625	COMPANY A	COMPANY B	COMPANY B1	COMPANY A1	Acuse transferido	Recuperado
	100423174822551542	COMPANY A	COMPANY B	COMPANY B1	COMPANY A1	Transferido	
	100423174621707790	COMPANY A	COMPANY B	COMPANY B1	COMPANY A1	Acuse transferido	Recuperado
	10042317462131638	COMPANY A	COMPANY B	COMPANY B1	COMPANY A1	Acuse transferido	Recuperado
	10042317460698891	COMPANY A	COMPANY B	COMPANY B1	COMPANY A1	Acuse transferido	Recuperado
	100423172437723468	COMPANY A	COMPANY B	COMPANY B1	COMPANY A1	Acuse transferido	Recuperado
	100423154200959955	COMPANY A	COMPANY B	COMPANY B1	COMPANY A1	Acuse transferido	Recuperado
	100423154200584218	COMPANY A	COMPANY B	COMPANY B1	COMPANY A1	Acuse transferido	Recuperado
	100423154004633794	COMPANY A	COMPANY B	COMPANY B1	COMPANY A1	Acuse transferido	Recuperado
	100423153916228967	COMPANY A	COMPANY B	COMPANY B1	COMPANY A1	Acuse transferido	Recuperado
	100423153638224633	COMPANY A	COMPANY B	COMPANY B1	COMPANY A1	Acuse transferido	Recuperado
	100423153607367509	COMPANY A	COMPANY B	COMPANY B1	COMPANY A1	Acuse transferido	Recuperado

Propiedades mensaje Fichero

Control: **Reprocesar mensaje**

Dirección: Entrada Situación: Acuse transferido Tipo acuse: Recuperado

Identificadores:

Origen: COMPANY A1 Propio: COMPANY A Identificador: 10042318032325625

Destino: COMPANY B1 Externo: COMPANY B Fic.Virtual: 100423175518673769/10042

Fechas:

Almacenado: Acuse almac: 23/04/2010 18:03:23 Creado: 23/04/2010 18:08:52

Transferido: Acuse trans: 23/04/2010 18:04:04 Modificado: 23/04/2010 18:09:06

Reintentos/Reenvíos:

Nº reintentos: 0 30/12/1899 Nº reenvíos: 0 30/12/1899

Propiedades mensaje:

Datos usuario: Formato: Binario 0 Longitud (bytes): 389

☐ Firmado ☐ Encriptado ☐ Comprimido ☐ Acuse firmado Descripción:

INF (18:03:23.428) -> STOR ()  
 INF (18:04:04.553) -> TRAN ()  
 INF (18:08:52.945) -> ACKS (RCP)  
 INF (18:09:06.742) -> ACKT (RCP)

1. En la parte superior de la sección mensajes se puede ver una lista de los mensajes correspondiente al nodo seleccionado, si se ha seleccionado el nodo principal de mensajes aparecen todos los mensajes.
2. En la parte inferior se visualizan los datos de cada mensaje de manera organizada, Así como un registro de los comandos de cambio de estado del mensaje. (Almacenado, transferido, acuse de recepción, etc).

<b>Fichero virtual Almacenado:</b> todavía no ha sido confirmada su recepción.
<b>Fichero virtual Transferido:</b> recepción del archivo confirmada.
<b>Acuse Almacenado:</b> todavía no ha sido confirmada su recepción.
<b>Acuse Transferido:</b> recepción del acuse confirmada.

Los datos de un mensaje aparecen tanto en el listado en forma de columnas como en el formulario cuando se selecciona el mensaje de la lista. Los datos asociados a un mensaje son los siguientes:

- **Estado.** Indica si existe algún problema con el mensaje en cuestión.
- **Tipo.** Permite indicar si se trata de un mensaje de Entrada o Salida, siempre en relación con el interlocutor propio.
- **Identificador.** Indica el Identificador del mensaje. Un código único generado automáticamente.
- **SSID Propio.** Indica el identificador OFTP del *Iniciator* del mensaje incluido en el comando SSID.
- **SSID Externo.** Indica el identificador OFTP del *Responder* de mensaje incluido en el comando SSID.
- **Origen SFID.** identificador del emisor del archivo virtual, incluido en el comando SFID.
- **Destino SFID.** identificador del receptor del archivo virtual, incluido en el comando SFID.
- **Situación.** indica la situación del mensaje. Existen dos situaciones principalmente Almacenado o Transferido
- Si estamos en mensajes el icono a continuación indica la dirección
- **Tipo de acuse.** Indica, para los mensajes de tipo Acuse, el tipo de acuse del cual se trata. Recuperado o rechazado, y en este último caso, el motivo del rechazo.
- **Creado.** Indica la fecha de creación original del mensaje.
- **Modificado.** Indica la fecha de modificación de su estado, por ejemplo tras un reenvío.
- Las columnas **Firmado**, **Encriptado**, **Comprimido** y **EERP firmado** indican si el mensaje se ha enviado o no con estas opciones.

- **Identificador Externo.** Incluye automáticamente un identificador externo al EOS para el mensaje, lo que puede permitir procesos de integración en otro sistema.
- **Fichero Virtual.** Indica el nombre del fichero virtual.
- **Fecha FV.** Indica la fecha de modificación del fichero virtual.
- **Hora FV.** Indica la hora de modificación del fichero virtual.

Cuando seleccionamos un mensaje la información de este se visualiza en el formulario inferior. Dividido en dos pestañas "Propiedades del mensaje" y "Fichero". En la parte inferior derecha aparece un log de información sobre las acciones realizadas para dicho mensaje. Normalmente el cambio de estado y los acuses asociados.

Desde la parte superior de la pestaña "Propiedades de mensaje" también se puede forzar el Reenvío del mensaje seleccionado (si es de salida) con el botón **Reenviar mensaje** y la descarga de los documentos de entrada con el botón **Conectar**.

## 7 SESIONES

### 7.1 INTRODUCCIÓN

---

Una **Sesión** es el registro de las actividades de una comunicación OFTP entre dos interlocutores. Cada vez que se inicia una sesión de conexión para el envío de archivos toda la información de esta sesión se almacena en forma de una nueva entrada en el nodo *sesiones*.

El panel de sesiones esta dividido en dos partes.

- En la parte superior aparece un listado con todas las sesiones registradas en el servidor para el dominio. Cada sesión viene identificada con sus datos mas importantes.
- En la parte inferior, cuando una sesión es seleccionada, aparecen hasta tres pestañas, según el nivel de Log indicado en las propiedades del interlocutor ( Log sesión, Log red y Log autómeta)

### 7.2 DATOS DE LA SESIÓN

---

Cada sesión tiene la siguiente información asociada que se refleja en el listado superior.

- El icono al principio de la tabla indica si la conexión ha sido establecida correctamente (Verde) o si ha existido algún error (Rojo)
- El icono de dirección indica si la conexión es de salida o de entrada. Siempre desde el punto de vista del servidor y el interlocutor propio.
- **Inicio.** Indica la fecha y hora de inicio de la conexión.
- **Segs.** Indica la duración en segundos de la conexión.
- **SSID sesión.** Indica la SSID del interlocutor externo relacionado con la sesión.
- **Información de sesión.** Indica que SSID actuá como *iniciator* y cual como *responder*.
- **Error.** Indica, si existe, el código y la descripción de los posibles errores.
- **Información de red.** Indica información a nivel de red de la conexión. (Protocolos, lps).
- **SSID propio.** Indica la SSID del interlocutor propio relacionado con la sesión.

## 7.3 FICHEROS DE LOG

---

Cada sesión, además, puede tener asociado hasta tres ficheros de log, donde se recogen a distintos niveles todas las actividades realizadas por el servidor. Los ficheros de log se visualizan al seleccionar una sesión del listado dentro de las pestañas de la parte inferior.