GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS
SUBSECRETARÍA
DIRECCIÓN GENERAL DE RELACIONES INSTITUCIONALES Y ORGANIZACIÓN
DIVISIÓN DE SISTEMAS DE LA INFORMACIÓN Y COMUNICACIONES

DSIC
DIVISION DE SISTEMAS DE INFORMACION Y COMUNICACIONES



Portafirmas v4

MANUAL DE INSTALACIÓN

Documento de Instalación
Sistemas Desarrollo
Versión
Rev001
Fecha de revisión
28/11/2014
Realizado por
Sistemas Desarrollo

ÍNDICE

1 Control de modificaciones del documento 3

2 Introducción 7

3 Información Técnica 8

4 Instalación nueva 9

5 Creación de base de datos de almacenamiento secundario 13

6 Despliegue en servidor de aplicaciones: 14

7 Configuración de Hibernate 15

8 Configuración de Quartz 16

9 Configuración de BBDD de histórico 16

10 Agregación del driver JDBC al WAR 16

11 Configuración desde Administración 16

12 Actualización de Port@firmas desde una versión anterior 32

13 Anexo I: Lista de parámetros de servidor 35

1 Control de modificaciones del documento

1.1 Versión actual del documento

Revisión Actual: 002
Fecha: 25/02/2015
Autor: Sistemas Desarrollo DSIC

Descripción de los cambios:

- Se modifica el apartado 13.5, 14.3 y 15 actualizando los parámetros de EEUTIL.
- Se modifica el apartado 14.1 generalizando como se debe actualizar de una versión a otra pasando por varias versiones.

1.2 Versiones anteriores del documento

Documento: Manual_Instalacion_Portafirmas_v4_rev001
Revisión Actual: 001
Fecha: 19/09/2014
Autor: Sistemas Desarrollo DSIC

Descripción de los cambios:

- Se modifica el apartado 6.1.1, indicando que debe crearse el directorio `conf`, en el que se guardarán los ficheros de propiedades de la aplicación.
- Se modifica el apartado 7, describiendo cómo ha de rellenarse el fichero de configuración de base de datos.
- Se modifica el apartado 8, describiendo cómo ha de rellenarse el fichero de quartz.
- Se modifica el apartado 9, describiendo cómo ha de rellenarse el fichero configuración de histórico.
- Se modifica el apartado 13.1, sustituyendo la imagen de la vieja interfaz por la de la nueva interfaz.
- Se modifica el apartado 13.2, sustituyendo la imagen de la vieja interfaz por la de la nueva interfaz.

Documento: Manual_Instalacion_Portafirmas_v3.2.6_rev008
Revisión Anterio: 008
Fecha: 19/09/2014
Autor: Sistemas Desarrollo DSIC

Descripción de los cambios:

- Se modifica el apartado 13.3.1. Se añaden los parámetros `NOTIFICACION.AVISAR.ADMIN` y `NOTIFICACION.CORREO.ADMIN`.

Revisión Anterior: 007

Fecha: 30/05/2014
Autor: Sistemas Desarrollo DSIC

Descripción de los cambios:

- Se modifica el apartado 3.1, en el que se indica que la librería correspondiente al drvier de conexión con BBDD no se distribuye por cuestiones de licenciamento, indicando el link de descarga en su lugar.
- Se modifica el apartado 3.2 indicando que se utiliza el Miniapplet 1.2
- Se crea el apartado 10, donde se explica cómo debe instalarse el driver de jdbc.

Revisión Anterior: 006
Fecha: 25/11/2013
Autor: Sistemas Desarrollo DSIC

Descripción de los cambios:

- Se modifica el apartado 3.2, indicando que la aplicación utiliza el Miniapplet 1.1 update 4.
- Se crea el apartado 5, donde se describen los pasos para crear la BBDD de almacenamiento de peticiones antiguas de Portafirmas.
- Se crea el apartado 9, donde se describe el fichero de configuración a rellenar para configurar la BBDD de almacenamiento de peticiones antiguas de Portafirmas.
- Se modifica el apartado 13.3.1, incluyendo parámetros de configuración de Interfaz Genérica de Portafirmas. Esta funcionalidad no se ha probado en un entorno de producción por lo que se recomienda no modificar estos parámetros.

Revisión Anterior: 005
Fecha: 04/11/2013
Autor: Sistemas Desarrollo DSIC

Descripción de los cambios:

- Se incluye la descripción del nuevo parámetro de configuración ‘AMBITO.DEFECTO’ al final del apartado 13.3.1

Revisión Anterior: 004
Fecha: 02/10/2013
Autor: Sistemas Desarrollo DSIC

Descripción de los cambios:

- Se modifica el índice, incluyendo también los apartados de nivel 3 y nivel 4.

- Se modifica la estructura del apartado 13.5, para una mejor comprensión de la configuración de la aplicación. Queda dividido en los subapartados:
  - 13.5.1 Configuración para validación de certificados, validación de firmas y sellado de tiempo de las firmas.
  - 13.5.2 Configuración para el tipo de firma.
  - 13.5.3 Configuración para generación de CSV y generación de justificante de firma.

- Se modifica el apartado 13.6, eliminando explicaciones que redundan con las del apartado 13.5.

- Se añade un Anexo (apartado 15) con todos los parámetros de servidor de la aplicación.

Revisión Anterior: 003
Fecha: 26/09/2013
Autor: Sistemas Desarrollo DSIC

Descripción de los cambios:

- Se modifica el apartado 13.5 . En la tabla de parámetros, estaban intercambiadas las descripciones y posibles valores de los parámetros FIRMA.MODO y FIRMA.SECURITY.MODE.
- Se añade al apartado 13.5 un subapartado donde se enumeran los pares de parámetros que son excluyentes entre sí (si uno toma valor 'S' el otro debe tomar necesariamente valor 'N').
- Se corrige el apartado 13.5, el parámetro FIRMA.SECURITY.FILE.NAME aparecía escrito como FIRMA.SECURITY.FILENAME.
- Se corrige el apartado 13.5, indicando la propiedad que no debe modificarse en el fichero de propiedades de la autenticación contra @firma por el método BinarySecurityToken.

Revisión Anterior: 002
Fecha: 09/09/2013
Autor: Sistemas Desarrollo DSIC

Descripción de los cambios:

- Se añade el apartado 14, donde se explican los pasos a seguir para la actualización de Portafirmas desde una versión anterior.
- Se elimina el punto 4.8, en el que se detallaban los scripts de BBDD a ejecutar para la actualización desde una versión anterior para que no haya redundancia con lo descrito en el apartado 14.1

Documento: Manual_Instalacion_Portafirmas_v3.2.6_05.pdf
Revisión: 001
Fecha: 31/07/2013
Autor: Sistemas Desarrollo DSIC

Descripción de los cambios:

- Modificación en los puntos 3.1 y 3.2, por la sustitución del Miniapplet por la versión más moderna (versión 1.1 update 3).
- Modificación del punto 3.2 por la eliminación del framework Axis.
- Se crea el punto 0 para definir el proceso de actualización de Portafirmas si se tenía la versión 3.2.5_14 instalada.

- Se modifica el punto 6.1, puesto que ya no es necesario el parámetro de arranque `javax.xml.soap.MessageFactory=org.apache.axis.soap.MessageFactoryImpl` al haber eliminado las dependencias del framework Axis.
- Se eliminan parámetros de configuración (`FIRMA.SECURITY.KEYSTORE`, `FIRMA.SECURITY.KEYSTORE.TYPE`, `FIRMA.SECURITY.PWD`) se añaden otros nuevos (`FIRMA.VALIDAR.CERTIFICADO`, `FIRMA.VALIDAR.FIRMA`, `FIRMA.SELLO` y `FIRMA.SECURITY.FILE.NAME`), por lo que se modifica el punto 13.5. Se crea también un apartado donde se explica cómo configurar el fichero para autenticación por método BinarySecurityToken.
- A partir de esta versión la implementación de los WS externos de EEUTIL sólo se necesitarán para la generación de CSV y la obtención del informe del justificante de firma. La validación de certificados y firmas y la obtención del timestamp de las firmas se podrá hacer a través de @firma. Se modifica el punto 13.6 al respecto.

Documento:	Manual_Instalacion_Portafirmas_v3.2.5_14_rev001.pdf
Fecha:	24/04/2013
Autor:	Sistemas Desarrollo DSIC
Descripción:	Versión inicial del documento.

2 Introducción

El objetivo del presente documento es servir de guía en la instalación de Portafirmas.

Todo el proceso de instalación está basada en scripts de base de datos que pueden ser ajustados por los Administradores de Base de Datos para revisar los parámetros de configuración a normas internas de implantación de aplicaciones en producción, o bien, a valores más reales a sus entornos de funcionamiento.

3 *Información Técnica*

A continuación vamos a ver los requisitos necesarios que hay que cumplir para el correcto funcionamiento de la aplicación, así como información sobre los componentes tecnológicos de los que hace uso.

3.1 Requisitos obligatorios

Hay que cumplir una serie de requisitos previos para iniciar la instalación de Portafirmas, a nivel de base de datos, servidor de aplicaciones, plataforma de firma así como el equipo con el que luego se vaya a acceder a la aplicación y firmar.

- Base de Datos: Oracle 10G o superior. El jar correspondiente al driver jdbc compatible con la BBDD no se distribuye por cuestiones de licenciamiento, pero se puede descargar de la página oficial de Oracle. Para la descarga del driver ha de tenerse en cuenta lo siguiente:
  - La aplicación está testeada para drivers *JDBC thin*.
  - El driver deberá ser compatible con JDK 1.6.
  - Descarga de driver para Oracle 10G:

http://www.oracle.com/technetwork/database/enterprise-edition/jdbc-10201-088211.html

  - Descarga de driver para Oracle 11G:

http://www.oracle.com/technetwork/database/enterprise-edition/jdbc-10201-088211.html

- Java Virtual Machine JDK 1.5.0 o superior.
- Servidor de Aplicaciones: Apache Tomcat 6.
- También ha de cumplir los requisitos necesarios para la ejecución del Miniapplet @firma v1.1 update 3.
- **Acceso a Plataforma @firma v5.3.1 o superiores. Es necesario disponer de conectividad con @firma, así como realizar el alta de la aplicación que usará** Port@firmas **para poder hacer uso de los servicios web. Para más información sobre la conexión con @firma se recomienda visitar los siguientes enlaces en el Pae-CTT http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_General&langPae=es&iniciativa=190** y http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=P30008362613063342540 91&langPae=es

http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=P30008362613063342540 91&langPae=es§

El procedimiento para rellenar correctamente la configuración de Port@firmas **se explica en apartados posteriores del presente manual.**

- Cuenta de Correo y acceso a servidor SMTP, si se quiere disponer de la funcionalidad de notificación a través de correo electrónico.
- La aplicación funciona correctamente en los siguientes navegadores:
  - Internet Explorer 11.x
  - Firefox 5.x en adelante.
- El usuario de la aplicación deberá tener instalada en su equipo una versión de JRE igual o superior a la versión 1.6.0_38. (Nota: Esta versión no tiene nada que ver con la versión instalada en el servidor de aplicaciones donde se despliegue la aplicación Port@firmas).

3.2 Tecnologías

- Miniapplet @firma v 1.2.
- Acceso a Base de Datos Hibernate-JPA 3.5.
- Modelo Vista Controlador: Spring-MVC
- Implementación: Thymeleaf
- Trazabilidad y monotización con log4j
- Gestión de procesos asíncronos con Quartz 1,6 con persistencia.
- Servicios Web Apache CXF 2.3 (WS V2).

4 *Instalación nueva*

En este apartado del documento se describe el proceso de instalación desde cero así como la carga inicial de parámetros de configuración.

4.1 Tablespaces

En nuestra instancia de base de datos tenemos que tener definidos los siguientes tablespaces:

- TS_PFIRMA_INDICES: El tamaño inicial 16MB.
- TS_PFIRMA_DATOS: El tamaño inicial 64MB.
- TS_PFIRMA_BLOB: El tamaño inicial 128MB.

Se recomienda activar la opción de crecimiento automático. El tamaño de chunk es algo complejo de definir a priori. Un tamaño pequeño repercute en un mejor aprovechamiento del espacio pero un mayor número de llamadas a disco, acceso por tanto más lento. Un tamaño mayor implica un mayor desaprovechamiento del espacio pero un acceso más rápido, al ser menor en numero de accesos al disco. Es por ello recomendable estudiar los valores obtenidos en el entorno de pruebas para poder extrapolar una configuración ajustada y equilibrada en producción.
Los valores iniciales indicados inicialmente son un buen punto de partida, pero cada DBA puede ajustar los mismos a los valores que estime oportuno.

Se proporciona un script aproximado de creación de los tablespaces, en la ruta:

bbdd/<version_actual>/creacion/1_script_creacion_tbsp.sql

4.2 Usuario propietario

Es necesario un usuario de base de datos para que sea el propietario de los objetos. Recomendamos que este sea el usuario “PFIRMAMG”, pues será el que empleemos como referencia en el resto del documento. El tablespace por defecto de este usuario sera “TS_PFIRMA_DATOS” y el temporal, “TEMP” o el definido en la instancia de base de datos como temporal.

```
create user PFIRMAMG identified by <clave>
default tablespace TS_PFIRMA_DATOS
temporary tablespace TEMP
quota unlimited on TS_PFIRMA_INDICES
quota unlimited on TS_PFIRMA_DATOS
quota unlimited on TS_PFIRMA_BLOB;
```

4.2.1 Permisos

Los permisos que necesita el usuario propietario del esquema son:

```
grant create session, alter session, alter user to PFIRMAMG;
grant create table, create sequence, create procedure to PFIRMAMG;
grant ″RESOURCE″ TO ″PFIRMAMG″;
grant “connect” to “PFIRMAMG” ;
grant CREATE TYPE to PFIRMAMG;
```

Estas sentencias (junto con las del apartado *3.3 Usuario de la aplicación*) se encuentran en el script situado en la ruta:

bbdd/<version_actual>/creacion/2_script_creacion_users.sql

Se deberá modificar en este script la clave escrita por la clave deseada.

4.3 Usuario de la aplicación

Será el que se configure a nivel de la aplicación y solo tendrá acceso a los objetos de base de datos, pero no será propietario de los mismos. Para crearlo:

```
create user PFIRMAWEB identified by <clave>

default tablespace TS_PFIRMA_DATOS

temporary tablespace temp;
```

Los permisos iniciales para este usuario serán:

```
grant create session, alter session, alter user to PFIRMAWEB;

grant create synonym to PFIRMAWEB;

grant "RESOURCE" TO "PFIRMAWEB";

grant "connect" to "PFIRMAWEB";
```

Estas sentencias (junto con las del apartado *3.2 Usuario propietario*) se encuentran en el script situado en la ruta:

bbdd/<version_actual>/creacion/2_script_creacion_users.sq

Se deberá modificar en este script la clave escrita por la clave deseada.

4.4 Creación del modelo de datos

Una vez creado el usuario propietario probaremos a conectarnos con el mediante un cliente SQL, como el SQLPLUS, SQLDeveloper, TOAD o Tora. Tomemos el ejemplo de usar el SQLDeveloper, programa que se puede descargar de la página de Oracle.

Introduciremos los datos de conexión a la base de datos y probaremos dicha conexión.

Si la conexión es correcta podemos continuar a crear todas las entidades necesarias para Portafirmas, osease tablas, índices, restricciones y secuencias. Para ello hay que lanzar el siguiente script de base de datos:

bbdd/<version_actual>/creacion/3_script_creacion_objs.sql

Lo cargamos en el SQLDeveloper y la damos a ejecutar.

Tras la ejecución se habrá creado el modelo de datos, podemos revisarlo rápidamente mirando los objetos básicos del usuario, tablas, secuencias, restricciones e índices.

4.5 Creación de permisos para el usuario de la aplicación

El usuario propietario debe concederle permisos de SELECT, INSERT, DELETE, UPDATE sobre todos los objetos tabla, así como SELECT sobre todos los objetos secuencia. Deberá de crear además un sinónimo privado por cada objeto del esquema del propietario. En principio no deben hacerse sinónimos públicos sobre los objetos de Portafirmas dado que esto puede dar la sensación de que se pueda acceder a los mismos, es mejor por motivos de seguridad solo hacer sinónimos privados a nivel de usuario web.

El script de base de datos es el siguiente:

bbdd/<version_actual>/creacion/4_script_perm_objs.sql

4.6 Carga inicial de datos

Para que la aplicación pueda funcionar es necesario una carga inicial de parámetros. Para ello hay que lanzar los siguientes scripts:

bbdd/<version_actual>/creacion/5_script_datos.sql

~~4.7 Alta usuario administrador~~

~~Para seguir con la configuración de la aplicación desde el interfaz de Portafirmas es necesario crear un primer usuario que será el que acceda mediante certificado usuario/clave para terminar de configurar el resto de elementos.~~

~~Primero crearemos el usuario:~~

```
Insert into PF_USUARIOS
(X_USUARIO, C_IDENTIFICADOR, D_NOMBRE, D_APELL1, D_APELL2, C_TIPO, L_VIGENTE)
Values
(PF_S_USU.NEXTVAL, :DNI, :NOMBRE, :APELL_1, :APELL_2, 'USUARIO', 'S');
```

~~Luego le asignaremos una clave:~~

```
Insert into PF_USUARIOS_PARAMETRO
(X_USUARIO_PARAMETRO, T_VALOR, PAR_X_PARAMETRO, USU_X_USUARIO)
Values
```

~~(PF_S_UPAR.NEXTVAL,~~

~~:CLAVE,~~

~~(select X_PARAMETRO from pf_parametros where C_PARAMETRO='USUARIO.PASSWORD'),~~

~~(select X_USUARIO from pf_usuarios where c_identificador=:DNI));~~

~~Le damos perfil de acceso:~~

~~Insert into PF_USUARIOS_PERFIL~~

~~(X_USUARIO_PERFIL, F_INICIO, USU_X_USUARIO, PER_X_PERFIL)~~

~~Values~~

~~(PF_S_UPER.NEXTVAL,~~

~~SYSDATE,~~

~~(select X_USUARIO from pf_usuarios where c_identificador=:DNI),~~

~~(select X_PERFIL from pf_perfiles where c_perfil='ACCESO'));~~

~~Le asignamos perfil de administrador:~~

~~Insert into PF_USUARIOS_PERFIL~~

~~(X_USUARIO_PERFIL, F_INICIO, USU_X_USUARIO, PER_X_PERFIL)~~

~~Values~~

~~(PF_S_UPER.NEXTVAL,~~

~~SYSDATE,~~

~~(select X_USUARIO from pf_usuarios where c_identificador=:DNI),~~

~~(select X_PERFIL from pf_perfiles where c_perfil='ADMIN'));~~

~~Después haríamos commit.~~

5 *Creación de base de datos de almacenamiento secundario*

En este apartado se describe el proceso para crear una segunda base de datos que puede utilizarse para mover peticiones antiguas y así aligerar el funcionamiento de la aplicación. Si no se desea disponer de un almacenamiento secundario, se puede ignorar el este apartado completo.

5.1 Tablespaces

Se propone la creación de tres tablespaces:

- IPFIRMAMGHIST: Tablespace para los índices.
- TPFIRMAMGHIST: Tablespace para datos.
- TPFIRMAMGHISTLOB: Tablespace para almacenar BLOBS.

El tamaño inicial y la opción de crecimiento automático se deja a criterio del instalador, pero se debe tener en consideración que esta base de datos servirá como “histórico”, por lo que debe poder almacenarse en ella un gran número de peticiones.

Se proporciona un script aproximado para la creación de los tablespaces:

bbdd/<version_actual>/creacion/6_script_creacion_tbsp_historico.sql

5.2 Creación del modelo de datos

El script de creación de objetos puede encontrarse en la siguiente ruta:

bbdd/<version_actual>/creacion/7_script_creacion_objs_historico.sql

5.3 Permisos sobre los objetos

Por último, habrá que crear los sinónimos y dar los permisos necesarios al usuario de la aplicación en esta base de datos. El script puede encontrarse en la siguiente ruta:

bbdd/<version_actual>/creacion/8_script_perm_objs_historico.sql

6 *Despliegue en servidor de aplicaciones:*

En este apartado se explicará cómo desplegar el WAR proporcionado en el servidor de aplicaciones.

6.1 *Apache Tomcat*

Bastará con copiar el WAR de la aplicación dentro del directorio webapps del servidor de aplicaciones, generalmente en:

$CATALINA_HOME/webapps/

6.1.1 Parámetros de arranque

El servidor ha de ser arrancado con algunos parámetros de configuración para que la aplicación funcione correctamente. Son los siguientes:

1. -Dsgtic.configpath=<ruta_configuracion> : En la ruta que se determine deberán existir los siguientes directorios:
   1. temp: La aplicación almacenará aquí temporalmente los ficheros a firmar.
   2. documentos: Se deben copiar los manuales de usuario y administrador en este directorio, con los nombres user_manual.pdf, admin_manual.pdf, admin_seat_manual.pdf y guia_rapida_manual.pdf respectivamente.
   3. properties: Directorio donde se almacenarán los ficheros de propiedades.
   4. Certificados: donde se encuentran los almacenes de claves y de confianza

6.1.2 Parámetros de configuración de server.xml

Por defecto, el servidor Tomcat está configurado para que el tamaño máximo de una petición POST sea de 2MB. Las firmas con los documentos implícitos son generalmente más grandes, puesto que contienen el documento, codificado en base 64, en el mismo fichero de firma.

El valor del tamaño máximo de las peticiones POST puede configurarse en el fichero *server.xml,* situado en la carpeta *conf* del tomcat. Para ello, es necesario incluir el parámetro *maxPostSize* en el nodo *Connector* correspondiente. A este parámetro se le puede asignar el valor “0”, y el efecto es que no habrá un máximo de tamaño para las Peticiones Post.

```
<Connector  connectionTimeout="20000"
                port="8080"
  protocol="HTTP/1.1"
  redirectPort="8443"
  maxPostSize="0"/>
```

7 Configuración de Hibernate

Se debe configurar el acceso a la base de datos de la aplicación, indicando el usuario (PFIRMAWEB, o el usuario de aplicación que se haya definido), el host y el puerto de ésta. El fichero donde configurar estos parámetros se encuentra el la carpeta de configuración conf, y debe llamarse jdbc.properties:

<ruta_configuracion>/properties/jdbc.properties

Se deberán modificar los parámetros de conexión a la BBDD, esto es, las siguientes líneas:

jdbc.url=jdbc:oracle:thin:@SERVIDOR:PUERTO:SID

```
jdbc.username=PFIRMAWEB
jdbc.password=CLAVE

bonecp.idleConnectionTestPeriodInMinutes=60
bonecp.idleMaxAgeInMinutes=30
bonecp.partitionCount=1
bonecp.maxConnectionsPerPartition=20
bonecp.minConnectionsPerPartition=5
bonecp.acquireIncrement=5
bonecp.statementsCacheSize=1000
bonecp.closeConnectionWatch=true


hibernate.generate_statistics=true
hibernate.show_sql=false
hibernate.format_sql=false

#Asignar este parámetro dependiendo del driver utilizado.
hibernate.dialect=org.hibernate.dialect.Oracle10gDialect

jpa.database=ORACLE
```

8 *Configuración de Quartz*

Deberemos configurar el fichero localizado en:

`<ruta_configuracion>/properties/quartz.properties`

Aquí también deberemos modificar los parámetros de conexión a la BBDD en las siguientes líneas:

```
org.quartz.dataSource.myDS.URL = jdbc:oracle:thin:@SERVIDOR:PUERTO:SID
org.quartz.dataSource.myDS.user = PFIRMAWEB
org.quartz.dataSource.myDS.password = CLAVE
```

9 Configuración de BBDD de histórico

Si se ha creado la BBDD para almacenar peticiones antiguas se deberá configurar en un fichero de propiedades los parámetros de la BBDD desde la que se van a mover las peticiones (BBDD de Port@firmas) y los parámetros de la BBDD a la que se van a mover las peticiones (BBDD de histórico). El fichero que hay que modificar se encuentra localizado en:

`<ruta_configuracion>/conf/storage.properties`

```
source_database=jdbc:oracle:thin:@SERVIDOR:PUERTO:SID
source_user=PFIRMAWEB (<USUARIO_BBDD_PORTAFIRMAS>)
source_password=CLAVE (<PASSWORD_BBDD_PORTAFIRMAS<)

storage_database=jdbc:oracle:thin:@SERVIDOR:PUERTO:SID
storage_user=<USUARIO_BBDD_HISTORICO>
storage_password=<PASSWORD_BBDD_HISTORICO>
```

10 Agregación del driver JDBC al WAR

El driver JDBC para la versión de Oracle correspondiente deberá meterse en la carpeta:

portafirma.war/WEB-INF/lib

11 Crear o añadir el certificado propio de la aplicación.

La aplicación debe tener un certificado propio cuya parte privada deberá encontrarse en `<ruta_configuracion>/certificados/almacen.jks`

12 Configurar Acceso por Certificado

El modo de acceso por defecto en Portafirmas es la autenticación mediante certificado.

Hay que solicitar el Alta de la aplicación en CLAVE, cuando se solicite hay que pasarles la parte pública de nuestro certificado (configurado en el paso anterior) para que en clave lo añadan.
Hay que configurar el fichero <ruta_configuracion>/properties/clave/clave.properties
Habrá que configurar las propiedades para que apunten a las urls donde tengan desplegado el protafirmas:
sp.url
sp.return
sp.logout.response.url
Hay que configurar el fichero <ruta_configuracion>/properties/clave/SignModule_SP.xml para que tenga la ruta donde se encuentra el almacén con nuestro certificado y las password para poder acceder al almacén y a nuestro certificado.

Hay que crear el usuario administrador que se corresponda con el certificado con el que vamos a acceder por primera vez, para ello se pueden lanzar los siguientes script:

```
INSERT INTO PF_PROVINCIA
(X_PROVINCIA, C_CODIGO_PROVINCIA, C_NOMBRE)
VALUES
(PF_S_PROV.NEXTVAL, 'ADM', 'ADMINISTRADOR');

INSERT INTO PF_USUARIOS
(X_USUARIO, C_IDENTIFICADOR, D_NOMBRE, D_APELL1, D_APELL2, L_VIGENTE, C_TIPO,
PROV_X_PROVINCIA, L_VISIBLE, L_ALERTA_NOTIF)
VALUES
(PF_S_USU.NEXTVAL, 'xxxxxxxxxxx', 'USUARIO', 'ADMINISTRADOR', 'PORTAFIRMAS', 'S',
'USUARIO', (SELECT X_PROVINCIA FROM PF_PROVINCIA WHERE C_NOMBRE =
'ADMINISTRADOR'), 'N', 'S');
```

```
INSERT INTO PF_USUARIOS_PERFIL
(X_USUARIO_PERFIL, F_INICIO, USU_X_USUARIO, PER_X_PERFIL)
VALUES
(PF_S_UPER.NEXTVAL, SYSDATE, (SELECT X_USUARIO FROM PF_USUARIOS WHERE
C_IDENTIFICADOR = 'xxxxxxxxxxx'), (SELECT X_PERFIL FROM PF_PERFILES WHERE
C_PERFIL = 'ACCESO'));

INSERT INTO PF_USUARIOS_PERFIL
(X_USUARIO_PERFIL, F_INICIO, USU_X_USUARIO, PER_X_PERFIL)
VALUES
(PF_S_UPER.NEXTVAL, SYSDATE, (SELECT X_USUARIO FROM PF_USUARIOS WHERE
C_IDENTIFICADOR = 'xxxxxxxxxxx'), (SELECT X_PERFIL FROM PF_PERFILES WHERE
C_PERFIL = 'FIRMA'));

INSERT INTO PF_USUARIOS_PERFIL
(X_USUARIO_PERFIL, F_INICIO, USU_X_USUARIO, PER_X_PERFIL)
VALUES
(PF_S_UPER.NEXTVAL, SYSDATE, (SELECT X_USUARIO FROM PF_USUARIOS WHERE
C_IDENTIFICADOR = 'xxxxxxxxxxx'), (SELECT X_PERFIL FROM PF_PERFILES WHERE
C_PERFIL = 'REDACCION'));

INSERT INTO PF_USUARIOS_PERFIL
(X_USUARIO_PERFIL, F_INICIO, USU_X_USUARIO, PER_X_PERFIL)
VALUES
(PF_S_UPER.NEXTVAL, SYSDATE, (SELECT X_USUARIO FROM PF_USUARIOS WHERE
C_IDENTIFICADOR = 'xxxxxxxxxxx'), (SELECT X_PERFIL FROM PF_PERFILES WHERE
C_PERFIL = 'ADMIN'));
```

13 *Configuración desde Administración*

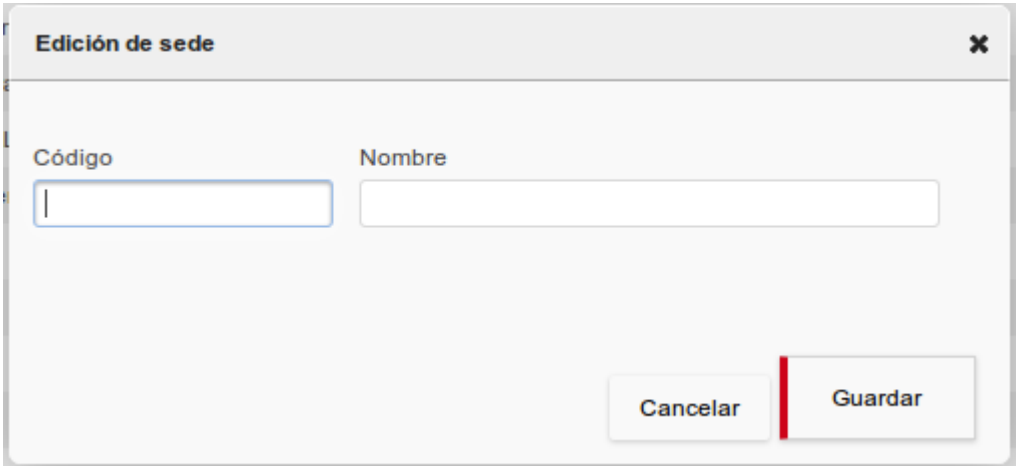
~~Para acceder a la administración en este primer acceso por defecto viene habilitado el modo DEBUG de la aplicación, y por tanto nos permitirá acceder por nuestro identificador y clave anteriormente introducidos al dar de alta el usuario con perfil administrador.~~

~~Para que la aplicación funcione correctamente, será necesario realizar las siguientes operaciones:~~

- ~~Crear al menos una sede.~~
- ~~Asignar al usuario administrador la sede creada.~~
- ~~Parametrizar la aplicación.~~

~~13.1 *Sedes*~~

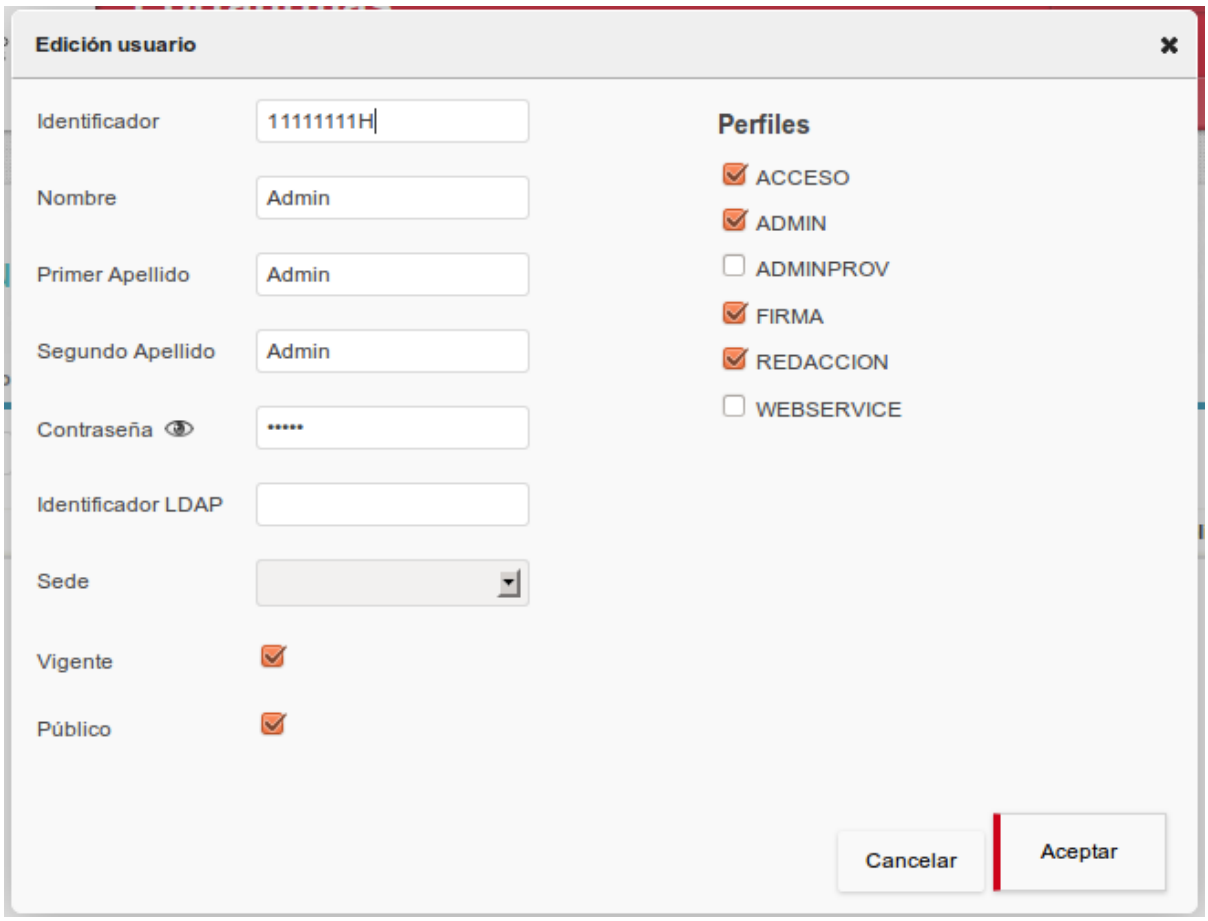
~~Para la creación de sedes accederemos al panel de Administración y nos situaremos en la pestaña *Sedes*. Una vez ahí, pulsaremos el botón *Nuevo*~~



~~Será necesario introducir el nombre de la sede y el código.~~

~~13.2 Modificar la sede del usuario administrador~~

~~Para ello, entraremos en la pestaña "Usuarios" y seleccionaremos el usuario administrador creado.~~



~~Será necesario seleccionar la sede creada y pulsar el botón *Aceptar.*~~

13.3 *General*

Desde aquí podemos revisar los valores globales a la aplicación, de acceso al servidor de correo, servicio de notificación, etc.

13.3.1 Parámetros

A continuación vamos a ver los parámetros de configuración susceptibles de ser personalizados. SÓLO modificar los aquí indicados y solo tras haber comprendido bien para qué sirven y qué valores pueden alojar.

Configuración de los modos de Acceso:

El modo de acceso por defecto en Portafirmas es la autenticación mediante certificado, sin embargo se pueden habilitar otro modo de acceso más, si se considera necesario:

- Acceso LDAP: autenticación de usuario mediante LDAP, el sistema solicita su usuario/clave de LDAP para realizar el proceso de autenticación.

Previamente a poder realizar el acceso del usuario por uno de estos medios, el administrador de Portafirmas debe establecer el valor de UID para ligar la autenticación LDAP con el usuario existente en Portafirmas.

Los valores a revisar son los siguientes:

- **LOGIN.LDAP** Indica si permite la autenticación mediante LDAP. Valores S o N.
- **LOGIN.LDAP.URL** Url de conexión al servidor LDAP, en caso de ser por SSL recordar importar el certificado al almacen de certificados.
- **USUARIO.LDAP.IDATRIBUTO**: Nombre del atributo del usuario en servidor LDAP que liga con el usuario de Portafirmas, generalmente será el propio UID pero puede ser cualquier otro que se desee de los existentes.
- **LOGIN.LDAP.IDENTIFICADOR** Expresión para buscar los datos del usuario. Ejemplo: (uid=$1).
- **LOGIN.LDAP.BASEDN**: Expresión para autenticar al usuario. Ejemplo: uid=$1,o=cice,o=empleados,o=minhap,c=es

Configuración de avisos por correo:

Portafirmas incorpora distintos puntos donde notifica por correo a los usuarios de los distintos eventos que suceden el sistema. Llegada de nuevas peticiones pendientes, lectura, firma, devolución de las mismas, o inclusión de nuevos comentarios a una petición.

La notificaciones solo llegarán a aquellas direcciones de correo que defina el usuario como susceptibles de recibir avisos, pudiendo por tanto desactivar la misma a conveniencia.

Los valores a revisar son los siguientes:

- **NOTIFICACION.CORREO** Permite habilitar o deshabilitar el envío de avisos por correo, tanto al receptor o al remitente. Valores S o N.
- **NOTIFICACION.CORREO.NOMBRE** Nombre a mostrar del remitente.
- **NOTIFICACION.CORREO.REMITENTE** Cuenta de correo que será remitente de todos los avisos por correo.
- **NOTIFICACION.CORREO.USUARIO** Usuario de correo.
- **NOTIFICACION.CORREO.CLAVE** Clave del usuario de correo.
- **NOTIFICACION.SMTP.SERVIDOR** Nombre del servicio SMTP de correo.
- **NOTIFICACION.SMTP.PUERTO** Puerto de escucha del servidor SMTP de correo. Generalmente es el 25.
- **NOTIFICACION.AVISAR.ADMIN** Indica si se envían correos al administrador cuando hay errores en la aplicación. De momento sólo está implementado para recibir correos cuando se producen errores en las llamadas a los WS de EEUTIL.
- **NOTIFICACION.CORREO.ADMIN** Correo del administrador para recibir avisos de errores en la aplicación.

La aplicación no soporta conexión a servidores de correo que requieren autenticación TLS/SSL.

Configuración de proxy:

Dado que Portafirmas puede acceder vía HTTP/HTTPS a otros servidores de aplicaciones para lanzar las acciones web que se le pasan las aplicaciones para ser avisadas de los distintos cambios de estado, en determinados entornos es necesario definir un servidor proxy.

Los valores a revisar son los siguientes:

- **PROXY** Utilización de proxy. Valores S o N.
- **PROXY.SERVIDOR** Máquina proxy conexiones http/https
- **PROXY.PUERTO** Puerto de escucha servidor proxy.
- **PROXY.USUARIO** Usuario servidor proxy. En caso de no haber, dejar en blanco.
- **PROXY.CLAVE** Clave del usuario del servidor proxy.

Cualquier conexión SSL requiere que se haya importado al almacén de certificados la clave pública del servidor al cual se conecta para que se autorice el acceso a dicha URL.

El uso de proxy sólo se efectúa para el acceso a las acciones web de terceras aplicaciones, no para el acceso a los servicios de firma. Esta comunicación debe ser directa por temas de rendimiento y seguridad de las informaciones.

Configuración de URLs de validación:

Se trata de configurar las URLs que se estamparán en los justificantes de firma (si está activada la opción EEUTIL.REPORT.ACTIVO), dependiendo del ámbito de los documentos:

Los valores a revisar son los siguientes:

- ~~**CVE.URL.VALIDACION.INTERNO**: Escribir la URL de acceso a Portafirmas~~ (OBSOLETO)
- **CVE.URL.VALIDACION.EXTERNO**: Escribir la URL de validación de documentos de ámbito externo.

Entorno:

Nombre del entorno donde se ejecuta la aplicación (por ejemplo, Preproducción, Producción). Se usa para configurar el texto que se enviará en los correos de notificación a los administradores:

Los valores a revisar son los siguientes:

- **ENTORNO**: Indica el entorno en el que está desplegada la aplicación.

Almacén de certificados de confianza:

En este apartado se configura la ruta de acceso al almacén de certificados de confianza. Tiene que estar dentro del directorio al que apunte la variable `sgtic.config`.

Los valores a revisar son:

- **TRUSTSTORE.FILE**: Nombre del almacén de certificados de confianza de la aplicación. Si se encuentra directamente dentro del directorio al que apunta `sgtic.configpath` escribiremos `/<nombre-almacen>`.
- **TRUSTSTORE.PASSWORD**: Password del almacén de certificados de confianza de la aplicación.
- **TRUSTSTORE.TYPE**: Tipo del almacén de certificados de confianza de la aplicación.

Extensiones aceptadas de ficheros a adjuntar:

En el siguiente parámetro se indican, separadas por comas, las extensiones de los ficheros aceptados a la hora de adjuntar documentos.

- **EXTENSIONES.ACEPTADAS**: Lista de extensiones de fichero aceptadas por la aplicación (deben ir separados por comas)

~~**Ámbito de documento por defecto**~~**(OBSOLETO)**

~~En el siguiente parámetro se indica el ámbito por defecto utilizado en la redacción de peticiones. Puede tomar los valores INTERNO o EXTERNO y determina la URL de validación de los justificantes de firma.~~

~~Durante la sesión de usuario el tipo de ámbito de documento toma inicialmente el valor por defecto que tenga configurada la aplicación, pero puede ser modificado manualmente en las opciones avanzadas de redacción para la sesión en curso.~~

- ~~**AMBITO.DEFECTO**: INTERNO o EXTERNO.~~

Parámetros de interfaz genérica de Portafirmas:

Esta funcionalidad de Portafirmas no está todavía probada en producción, por lo que no se recomienda de momento modificar los parámetros siguientes:

- **DOCEL.SMC.SECURITY.CERT.ALIAS**
- **DOCEL.SMC.SECURITY.CERT.PWD**
- **DOCEL.SMC.SECURITY.FILE.NAME**
- **DOCEL.SMC.SECURITY.MODE**
- **DOCEL.SMC.SECURITY.PASS.TYPE**
- **DOCEL.SMC.SECURITY.PASSWORD**
- **DOCEL.SMC.SECURITY.USER**
- **DOCEL.SMC.URL**
- **DOCEL.SPC.SECURITY.CERT.ALIAS**
- **DOCEL.SPC.SECURITY.CERT.PWD**
- **DOCEL.SPC.SECURITY.FILE.NAME**
- **DOCEL.SPC.SECURITY.MODE**
- **DOCEL.SPC.SECURITY.PASS.TYPE**
- **DOCEL.SPC.SECURITY.PASSWORD**
- **DOCEL.SPC.SECURITY.USER**
- **DOCEL.SPC.URL**

13.4 *Aplicaciones*

Desde aquí se pueden administrar las aplicaciones. Las aplicaciones que aparecen en un principio se corresponden con los tipos de firma que pueden configurarse a la hora de redactar una petición.

- **PFIRMA**: Se tomará esta configuración cuando en la ventana de Redacción se elija el modo de firma “defecto”. El comportamiento es el siguiente:
  - Si el documento es PDF se firmará en PadES.
  - Si el documento es de cualquier otro tipo se firmará en XadES Internally Detached implícito.
- **PFIRMA_XADES**: Es la configuración de firma que se tomará cuando en la ventana de Redacción se seleccione el modo de firma “XADES”. Se firmarán los documentos enviados en la petición en XadES Internally Detached Implícito.
- **PFIRMA_XADES_ENVELOPED**: Es la configuración de firma que se tomará cuando en la ventana de Redacción se seleccione el modo de firma “XADES ENVELOPED”. Se firmarán los documentos enviados en la petición en XadES Enveloped.
- **PFIRMA_CADES**: Configuración de firma que se tomará cuando en la ventana de Redacción se seleccione el modo de firma “CADES”. Se firmarán los documentos enviados en la petición en CadES Attached.

Adicionalmente se permite crear aplicaciones nuevas, que se corresponderán con las aplicaciones consumidoras de los WS de Port@firmas. Cada aplicación apuntará a una configuración, puede elegirse una de las ya creadas o se puede crear una configuración nueva. Los parámetros de estas configuraciones se explican en el apartado siguiente.

13.5 *Servidores*

En esta pestaña se pueden crear nuevos servidores, así como administrar las configuraciones que tiene un servidor.

Las configuraciones que se crean en un principio se corresponden con los tipos de firma señalados en el apartado *Aplicaciones*. Además, podrán crearse nuevas configuraciones con otros formatos de firma.

Los parámetros de configuración de las configuraciones se explican en los siguientes apartados:

13.5.1 Configuración para validación de certificados, validación de firmas y sellado de tiempo

La validación de certificados, de firmas, y generación de timestamp puede hacerse a través de la plataforma @firma o a través de otro servicio de libre implementación (EEUTIL). Se recomienda elegir o bien la plataforma @firma o bien el servicio de libre implementación (EEUTIL) para cada una de estas tres funcionalidades.

13.5.1.1 Validación de certificados

Para que se puedan realizar firmas en Portafirmas es necesario que esté activa esta funcionalidad, ya que aunque los usuarios no accedan a la aplicación con certificado y entren con identificador LDAP o con usuario/contraseña, el certificado con el que se firman las peticiones será validado a la hora de la firma para la obtención del NIF del firmante, y así poder comprobar que este NIF coincide con el del usuario autenticado.

Existen dos opciones para activar esta funcionalidad. Las dos opciones son excluyentes entre sí y son: validación de certificados contra la plataforma @firma y validación de certificados contra la plataforma EEUTIL.

Validación de certificados contra la plataforma @FIRMA

Habrá que dar valor al siguiente parámetro en la configuración por defecto para activar esta funcionalidad contra la plataforma @firma.

- **F**IRMA.VALIDAR.CERTIFICADO = 'S'

Además, habrá que desactivar la validación de certificados contra la plataforma EEUTIL, por lo que el siguiente parámetro deberá o eliminarse (para que no aparezcan parámetros innecesarios), o bien asginarle valor 'N'. La opción que se elija se tendrá que realizar en la configuración por defecto

- EEUTIL.VALIDAR.CERT.ACTIVO = 'N' (o eliminar el parámetro).

Por último, habrá que rellenar los parámetros relativos a la conexión con @firma en la configuración por defecto:

- FIRMA.URL : Url de los servicios web de @firma (ejemplo: https://afirma.redsara.es/afirmaws/services/)
- FIRMA.APLICACION: Identificador de aplicación para la plataforma @firma.
- FIRMA.TRUSTEDSTORE: Ruta del almacén de certificados de confianza en que se incluye el certificado de @firma.
- FIRMA.TRUSTEDSTORE.PASSWORD: Password del almacén de certificados de confianza en que se incluye el certificado de @firma.
- FIRMA.SECURITY.MODE: Tipo de autenticación contra la plataforma @firma. Tres posibles valores: "None" (sin autenticación), "UsernameToken" (usuario/contraseña), "BinarySecurityToken" (con certificado)

Si el parámetro FIRMA.SECURITY.MODE tiene valor "UsernameToken" (autenticación por usuario/contraseña contra @firma), entonces habrá que dar valor a los parámetros:

- FIRMA.SECURITY.USER: Usuario
- FIRMA.SECURITY.PASSWORD: Contraseña
- FIRMA.SECURITY.PASSWORD.TYPE: Tipo de contraseña. Valores posibles: "PasswordDigest", "PasswordText".

Si el parámetro FIRMA.SECURITY.MODE tiene valor "BinarySecurityToken" (autenticación con certificado contra @firma), entonces habrá que dar valor a los parámetros:

- FIRMA.SECURITY.FILE.NAME: Nombre del fichero donde se configurará el almacén de claves (ruta, tipo de almacén y contraseña). Este fichero deberá alojarse obligatoriamente en la carpeta properties. La configuración de este fichero viene descrita en el apartado 13.5.1.4

  - FIRMA.SECURITY.CERT.ALIAS: Alias de la clave para la autenticación contra @firma.
  - FIRMA.SECURITY.CERT.PWD: Password de la clave para la autenticación contra @firma.

- FIRMA.TIPO: Obligatoriamente con valor “afirma5”.
- FIRMA.IMPL.AFIRMA5: Obligatoriamente con valor “es.guadaltel.framework.authenticator.impl.AfirmaAuthenticatorImpl".
- FIRMA.AFIRMA5.MAPPING: Obligatoriamente con valor “afirma5”.
- FIRMA.AFIRMA5.MAPPING.AFIRMA5: Obligatoriamente con valor "es.guadaltel.framework.authenticator.config.DefaultAfirmaMapping"

Validación de certificados contra la plataforma EEUTIL

Habrá que dar valor al siguiente parámetro en la configuración por defecto para activar la validación de certificados contra la plataforma EEUTIL:

- EEUTIL.VALIDAR.CERT.ACTIVO = 'S'.

Además, habrá que desactivar la validación de certificados contra la plataforma @FIRMA, por lo que el siguiente parámetro deberá o eliminarse (para que no aparezcan parámetros innecesarios), o bien asginarle valor 'N'. La opción que se elija se tendrá que realizar en la configuración por defecto.

- FIRMA.VALIDAR.CERTIFICADO = 'N' (o eliminar el parámetro).

Por último, habrá que configurar los siguientes parámetros relativos a la conexión con EEUTIL:

- EEUTIL.OPER.FIRMA.URL: URL del WSDL del web service EEUTIL-OPER-FIRMA
- EEUTIL.OPER.FIRMA.USER: Usuario de Port@firmas en el servicio EEUTIL-OPER-FIRMA.
- EEUTIL.OPER.FIRMA.PASSWORD: Password de Port@firmas en el servicio EEUTIL-OPER-FIRMA.

13.5.1.2 Validación de firmas

Para que las firmas sean validadas será necesaria la activación de esta funcionalidad. Existen dos opciones excluyentes entre sí: validación de firmas a través de la plataforma @afirma y validación de firmas a través de la plataforma EEUTIL.

Validación de firmas contra la plataforma @FIRMA

Habrá que dar valor al siguiente parámetro para cada una de las configuraciones para las que se quiera validar las firmas contra la plataforma @firma.

- FIRMA.VALIDAR.FIRMA = 'S'

Además, habrá que desactivar la validación de firmas contra la plataforma EEUTIL, por lo que el siguiente parámetro deberá o eliminarse (para que no aparezcan parámetros innecesarios), o bien

asginarle valor 'N'. La opción que se elija se tendrá que realizar para cada una de las configuraciones para las que se quiera validar las firmas contra la plataforma @firma.

- EEUTIL.VALIDAR.FIRMA = 'N' (o eliminar el parámetro).

Por último, habrá que rellenar los parámetros relativos a la conexión con @firma para cada una de las configuraciones para las que se quiera validar las firmas contra la plataforma @firma:

- FIRMA.URL : Url de los servicios web de @firma (ejemplo: https://afirma.redsara.es/afirmaws/services/)
- FIRMA.APLICACION: Identificador de aplicación para la plataforma @firma.
- FIRMA.TRUSTEDSTORE: Ruta del almacén de certificados de confianza en que se incluye el certificado de @firma.
- FIRMA.TRUSTEDSTORE.PASSWORD: Password del almacén de certificados de confianza en que se incluye el certificado de @firma.
- FIRMA.SECURITY.MODE: Tipo de autenticación contra la plataforma @firma. Tres posibles valores: "None" (sin autenticación), "UsernameToken" (usuario/contraseña), "BinarySecurityToken" (con certificado)

Si el parámetro FIRMA.SECURITY.MODE tiene valor "UsernameToken" (autenticación por usuario/contraseña contra @firma), entonces habrá que dar valor a los parámetros:

- FIRMA.SECURITY.USER: Usuario
- FIRMA.SECURITY.PASSWORD: Contraseña
- FIRMA.SECURITY.PASSWORD.TYPE: Tipo de contraseña. Valores posibles: "PasswordDigest", "PasswordText".

Si el parámetro FIRMA.SECURITY.MODE tiene valor "BinarySecurityToken" (autenticación con certificado contra @firma), entonces habrá que dar valor a los parámetros:

- FIRMA.SECURITY.FILE.NAME: Nombre del fichero donde se configurará el almacén de claves (ruta, tipo de almacén y contraseña). Este fichero deberá alojarse obligatoriamente en la carpeta properties. La configuración de este fichero viene descrita en el apartado 13.5.1.4
- FIRMA.SECURITY.CERT.ALIAS: Alias de la clave para la autenticación contra @firma.
- FIRMA.SECURITY.CERT.PWD: Password de la clave para la autenticación contra @firma.

- FIRMA.TIPO: Obligatoriamente con valor “afirma5”.
- FIRMA.IMPL.AFIRMA5: Obligatoriamente con valor “es.guadaltel.framework.authenticator.impl.AfirmaAuthenticatorImpl".
- FIRMA.AFIRMA5.MAPPING: Obligatoriamente con valor “afirma5”.
- FIRMA.AFIRMA5.MAPPING.AFIRMA5: Obligatoriamente con valor "es.guadaltel.framework.authenticator.config.DefaultAfirmaMapping.

Validación de firmas contra la plataforma EEUTIL

Habrá que dar valor al siguiente parámetro para cada una de las configuraciones para las que se quiera validar las firmas contra la plataforma EEUTIL:

- EEUTIL.VALIDAR.FIRMA.ACTIVO = 'S'.

Además, habrá que desactivar la validación de firmas contra la plataforma @FIRMA, por lo que el siguiente parámetro deberá o eliminarse (para que no aparezcan parámetros innecesarios), o bien asginarle valor 'N'. La opción que se elija se tendrá que realizar para cada una de las configuraciones para las que se quiera validar las firmas contra la plataforma EEUTIL.

- FIRMA.VALIDAR.FIRMA.ACTIVO = 'N' (o eliminar el parámetro).

Por último, habrá que configurar los siguientes parámetros relativos a la conexión con EEUTIL:

- EEUTIL.OPER.FIRMA.URL: URL del WSDL del web service EEUTIL-OPER-FIRMA
- EEUTIL.OPER.FIRMA.USER: Usuario de Port@firmas en el servicio EEUTIL-OPER-FIRMA.
- EEUTIL.OPER.FIRMA.PASSWORD: Password de Port@firmas en el servicio EEUTIL-OPER-FIRMA.

13.5.1.3 Sellado de tiempo de las firmas

El sellado o timestamping de las firmas se puede realizar a través de la plataforma @firma o a través del servicio externo de libre implementación (EEUTIL). Las dos opciones son excluyentes entre sí.

Sellado de tiempo de firmas contra la plataforma @FIRMA

Habrá que dar valor al siguiente parámetro para cada una de las configuraciones para las que se quiera añadir el sello de tiempo a las firmas contra la plataforma @firma.

- FIRMA.SELLO = 'S'

Además, habrá que desactivar el sellado de tiempo contra la plataforma EEUTIL, por lo que el siguiente parámetro deberá o eliminarse (para que no aparezcan parámetros innecesarios), o bien asginarle valor 'N'. La opción que se elija se tendrá que realizar para cada una de las configuraciones para las que se quiera validar las firmas contra la plataforma @firma.

- EEUTIL.SELLO.ACTIVO = 'N' (o eliminar el parámetro).

Por último, habrá que rellenar los parámetros relativos a la conexión con @firma para cada una de las configuraciones para las que se quiera añadir el sello de tiempo a las firmas contra la plataforma @firma:

- FIRMA.URL : Url de los servicios web de @firma (ejemplo: https://afirma.redsara.es/afirmaws/services/)
- FIRMA.APLICACION: Identificador de aplicación para la plataforma @firma.
- FIRMA.TRUSTEDSTORE: Ruta del almacén de certificados de confianza en que se incluye el certificado de @firma.
- FIRMA.TRUSTEDSTORE.PASSWORD: Password del almacén de certificados de confianza en que se incluye el certificado de @firma.
- FIRMA.SECURITY.MODE: Tipo de autenticación contra la plataforma @firma. Tres posibles valores: "None" (sin autenticación), "UsernameToken" (usuario/contraseña), "BinarySecurityToken" (con certificado)

Si el parámetro FIRMA.SECURITY.MODE tiene valor "UsernameToken" (autenticación por usuario/contraseña contra @firma), entonces habrá que dar valor a los parámetros:

- FIRMA.SECURITY.USER: Usuario
- FIRMA.SECURITY.PASSWORD: Contraseña
- FIRMA.SECURITY.PASSWORD.TYPE: Tipo de contraseña. Valores posibles: "PasswordDigest", "PasswordText".

Si el parámetro FIRMA.SECURITY.MODE tiene valor "BinarySecurityToken" (autenticación con certificado contra @firma), entonces habrá que dar valor a los parámetros:

- FIRMA.SECURITY.FILE.NAME: Nombre del fichero donde se configurará el almacén de claves (ruta, tipo de almacén y contraseña). Este fichero deberá alojarse obligatoriamente en la carpeta properties.La configuración de este fichero viene descrita en el apartado 13.5.1.4
- FIRMA.SECURITY.CERT.ALIAS: Alias de la clave para la autenticación contra @firma.
- FIRMA.SECURITY.CERT.PWD: Password de la clave para la autenticación contra @firma.
- FIRMA.TIPO: Obligatoriamente con valor “afirma5”.
- FIRMA.IMPL.AFIRMA5: Obligatoriamente con valor “es.guadaltel.framework.authenticator.impl.AfirmaAuthenticatorImpl".
- FIRMA.AFIRMA5.MAPPING: Obligatoriamente con valor “afirma5”.
- FIRMA.AFIRMA5.MAPPING.AFIRMA5: Obligatoriamente con valor "es.guadaltel.framework.authenticator.config.DefaultAfirmaMapping.

Sellado de tiempo de firmas contra la plataforma EEUTIL

Habrá que dar valor al siguiente parámetro para cada una de las configuraciones para las que se quiera añadir el sello de tiempo a las firmas contra la plataforma EEUTIL:

- EEUTIL.SELLO.ACTIVO = 'S'.

Además, habrá que desactivar el sellado de tiempo de firmas contra la plataforma @FIRMA, por lo que el siguiente parámetro deberá o eliminarse (para que no aparezcan parámetros innecesarios), o bien asginarle valor 'N'. La opción que se elija se tendrá que realizar para cada una de las configuraciones para las que se quiera añadir el sello de tiempo a las firmas contra la plataforma EEUTIL.

- FIRMA.SELLO.ACTIVO = 'N' (o eliminar el parámetro).

Por último, habrá que configurar los siguientes parámetros relativos a la conexión con EEUTIL:

- EEUTIL.OPER.FIRMA.URL: URL del WSDL del web service EEUTIL-OPER-FIRMA
- EEUTIL.OPER.FIRMA.USER: Usuario de Port@firmas en el servicio EEUTIL.
- EEUTIL.OPER.FIRMA.PASSWORD: Password de Port@firmas en el servicio EEUTIL.

13.5.1.4 Configuración de fichero de propiedades si se ha elegido autenticación con certificado (BinarySecurityToken) contra @firma

Siempre que se elija el método BinarySecurityToken como método de autenticación contra la plataforma @firma será necesario configurar los parámetros relativos al almacén donde se encuentra la clave privada en un fichero. Este fichero deberá encontrarse en la carpeta properties, y el nombre deberá indicarse en el parámetro FIRMA.SECURITY.FILE.NAME.

A continuación se copia un ejemplo del contenido que debe tener este fichero:

```
org.apache.ws.security.crypto.provider=org.apache.ws.security.components.crypto.Merlin
org.apache.ws.security.crypto.merlin.keystore.type=JKS
org.apache.ws.security.crypto.merlin.keystore.password=XXX
org.apache.ws.security.crypto.merlin.file=<ruta_absoluta_keystore>
```

La propiedad org.apache.ws.security.crypto.provider deberá dejarse tal cual. El resto de propiedades deberán configurarse adecuadamente. El alias del certificado de firma y la password de la clave privada deberán configurarse en los parámetros FIRMA.SECURITY.CERT.ALIAS y FIRMA.SECURITY.CERT.PASSWORD respectivamente.

13.5.2 Configuración de tipos de firma:

Para cada una de las configuraciones se tiene que dar valor a una serie de parámetros, donde se especifica el tipo de firma:

- FIRMA.MODO: Sólo puede tomar el valor "MASIVA".
- FIRMA.SIGNATURE.MODE: Puede tomar los valores "HASH" y "BINARIO".
- FIRMA.SIGNATURE.FORMAT: Puede tomar los valores: "PDF" (PAdES), "XADES ENVELOPED" (XAdES Enveloped Implícita), "XADES ENVELOPING" (XAdES Enveloping Implícita), "XADES IMPLICITO" (XAdES Detached Implícita), "CADES" (CAdES Implícita).
- FIRMA.SIGNATURE.ALGORITHM: Obligatoriamente valor "SHA1".

El comportamiento de la aplicación para las peticiones enviadas desde la configuración por defecto será el siguiente:

- Se firmarán en PadES si el documento es PDF.
- Se firmarán en XadES Detached Implícito, modo binario, si el documento no es PDF.

Las peticiones enviadas desde la configuración por defecto serán aquellas enviadas desde la propia aplicación Port@firmas, seleccionando en el tipo de firma la opción “Por defecto”, o aquellas enviadas desde otras aplicaciones que apunten a la configuración por defecto.

Además de la configuración por defecto, existen otras configuraciones creadas:

- CADES: Firma CAdES Implícita del binario del documento, sea cual sea la extensión del mismo. Se firmarán con esta configuración las peticiones enviadas desde la propia aplicación Port@firmas, seleccionando en el tipo de firma la opción “CADES”, o aquellas enviadas desde otras aplicaciones que apunten a la configuración CADES.

- XADES IMPLICITO: Firma XadES Detached implícita del binario del documento, sea cual sea la extensión de éste. Se firmarán con esta configuración las peticiones enviadas desde la propia aplicación Port@firmas, seleccionando en el tipo de firma la opción "XADES", o aquellas enviadas desde otras aplicaciones que apunten a la configuración XADES IMPLICITO.

- XADES ENVELOPED: Firma XadES Enveloped implícita. Se firmarán con esta configuración las peticiones enviadas desde la aplicación Port@firmas, seleccionando en el tipo de firma la opción XADES ENVELOPED, o aquellas enviadas desde otras aplicaciones que apunten a la configuración XADES ENVELOPED. Si el documento a firmar no es un XML la aplicación dará un error al intentar firmar la petición.

13.5.3 Configuración para generación de CSV y generación de justificante de firma

Para obtener estas dos funcionalidades es necesario implementar un servicio externo, EEUTIL (detallado en el documento *Guia_WebServices_EEUtil_Portafirmas_<version>_<revision>.pdf*) y configurar una serie de parámetros en la configuración por defecto:

13.5.3.1 Generación de CSV:

Los siguientes parámetros tendrán que ser asignados en la configuración por defecto:

- EEUTIL.CSV.ACTIVO = 'S'
- EEUTIL.UTIL.FIRMA.URL = <url_wsdl_eeutil-util-firma>
- EEUTIL.UTIL.FIRMA.USER = Usuario de Port@firmas en EEUTIL.
- EEUTIL.UTIL.FIRMA.PASSWORD = Password de Port@firmas en EEUTIL.

Si no se tiene implementado el servicio externo será necesario dar valor 'N' o bien eliminar el parámetro en la configuración por defecto.

- EEUTIL.CSV.ACTIVO = 'N' (o eliminar el parámetro).

13.5.3.2 Generación de justificante de firma:

Los siguientes parámetros tendrán que ser asignados en la configuración por defecto:

- EEUTIL.REPORT.ACTIVO = 'S'
- EEUTIL.UTIL.FIRMA.URL = <url_wsdl_eeutil-util-firma>
- EEUTIL.UTIL.FIRMA.USER = Usuario de Port@firmas en EEUTIL.
- EEUTIL.UTIL.FIRMA.PASSWORD = Password de Port@firmas en EEUTIL.

Si no se tiene implementado el servicio externo será necesario dar valor 'N' o bien eliminar el parámetro en la configuración por defecto.

- EEUTIL.REPORT.ACTIVO = 'N' (o eliminar el parámetro).

13.6 Servicio EEUTIL externo

Para poder generar CSV y justificantes de firma es necesario implementar un Web Service que cumpla con una especificación determinada. También se da la posibilidad de que la validación de las firmas, la validación de certificados y la generación de sellos de tiempo en las firmas se realice contra este Web Service, pero estas funcionalidades se pueden obtener también a través de la plataforma @firma.

En el documento *Guia_WebServices_EEUtil_Portafirmas_<version>_<revision>.pdf* se explica detalladamente el interfaz de estos servicios y qué operaciones deben ser implementadas para cada una de las funcionalidades que se desee obtener.

14 Actualización de Port@firmas desde una versión anterior

En este apartado se describen los pasos a seguir para actualizar la aplicación desde la instalación de la versión anterior.

14.1 Scripts de Base de Datos

Si ya se tenía una instalación de Portafirmas de una versión anterior será necesario ejecutar los scripts que se encuentran en la ruta:

bbdd/<version_actual>/actualizacion/.sql*

Tras ejecutar estos scripts será necesario dar permisos al usuario de la aplicación sobre los nuevos objetos creados, para lo cual se puede ejecutar el script:

bbdd/<version_actual>/creacion/4_script_perm_objs.sql

Si se desea disponer de la BBDD de histórico para mover peticiones, será necesario ejecutar los scripts:

bbdd/<version_actual>/actualizacion/3_act_script_creacion_tbsp_historico.sql
bbdd/<version_actual>/actualizacion/4_act_script_objs_historico.sql
bbdd/<version_actual>/actualizacion/5_act_script_perm_objs_historico.sql

Se recomienda leer el apartado 5.1 para tener una visión más detallada a la hora de crear los Tablespaces.

Nota: Para actualizarse a una versión determinada, habrá que ejecutar todos los scripts de actualización, empezando por la versión siguiente a la versión instalada y terminando en la versión actual:

bbdd/<version_instalada_+1>/actualizacion/.sql*
...
bbdd/<version_actual>/actualizacion/.sql*

14.2 Parámetros de arranque de la aplicación

Puesto que se ha sustituido el framework Apache Axis por Apache CXF será necesario eliminar de las opciones de arranque la opción

-Djavax.xml.soap.MessageFactory=org.apache.axis.soap.MessageFactoryImpl

14.3 Parámetros de configuración

Se han eliminado los siguientes parámetros de configuración por no resultar necesarios. Si se ha ejecutado el script `2_act_script_datos.sql`, no deberían aparecer en la tabla de parámetros de configuración:

- FIRMA.JAAS.USUARIO
- FIRMA.JAAS.CLAVE
- FIRMA.SECURITY.KEYSTORE
- FIRMA.SECURITY.KEYSTORE.TYPE
- FIRMA.SECURITY.KEYSTORE.PWD

Se han añadido los siguientes parámetros de configuración, cuyo valor deberá configurarse desde el panel de Administración para cada una de las configuraciones de firma que se vayan a utilizar:

- FIRMA.VALIDAR.CERTIFICADO: Indica si se quiere realizar la validación de certificados contra la plataforma @firma.
- FIRMA.VALIDAR.FIRMA: Indica si se quieren validar las firmas contra la plataforma @firma.
- FIRMA.SELLO: Indica si se quiere generar el sello de tiempo para las firmas desde la plataforma @firma.
- FIRMA.SECURITY.FILE.NAME: Nombre del fichero de configuración en caso de utilizar el método de autenticación `BinarySecurityToken` contra la plataforma @firma. En el apartado 13.5 se explica cómo se debe rellenar este fichero.

También se tendrán que revisar los parámetros relativos al almacén de certificados de confianza relativos a @firma para cada una de las configuraciones de firma:

- FIRMA.TRUSTEDSTORE: Ruta del almacén de certificados de confianza para la conexión https con la plataforma @firma. Se permite la referencia a la variable sgtic.configpath. Por ejemplo, si el almacén se encuentra en `<valor_sgtic.configpath>/conf/trustedstore.jks`, se podrá indicar dándole al parámetro el valor:

  `${sgtic.configpath}/conf/truststore.jks`

- FIRMA.TRUSTEDSTORE.PASS: Password del almacén de certificados de confianza para la conexión https con la plataforma @firma.

Se recomienda revisar el apartado 13.5 para saber qué parámetros se deben cambiar y en qué configuraciones.

Las acciones de validación de certificados, validación de firmas y generación de sello de tiempo también es posible realizarlas a través de la plataforma EEUTIL, por lo que si en una versión anterior se tenían seleccionadas las opciones contra la plataforma externa y en esta versión se desea utilizar la plataforma @firma habrá que desactivar (darles valor “N”) a las siguientes opciones:

- EEUTIL.VALIDAR.CERT.ACTIVO
- EEUTIL.VALIDAR.FIRMA.ACTIVO
- EEUTIL.SELLO.ACTIVO

Se recomienda revisar el apartado 13.5 para saber qué parámetros se deben cambiar y en qué configuraciones.

15 Anexo I: Lista de parámetros de servidor

En este apartado se incluye una tabla con todos los parámetros de servidor.

Parámetro	Descripción	Valores	Configurable
FIRMA.TIPO	Tipo de servidor de firma	afirma5	N
FIRMA.IMPL.AFIRMA5	Clase de implementación de @firma5	es.guadaltel.framework.authenticator.impl.AfirmaAuthenticatorImp	N
FIRMA.AFIRMA5.MAPPING	Nombre de la implementación que indica el mapeo de los datos devueltos en el retorno de @firma	afirma5	N
FIRMA.AFIRMA5.MAPPING.AFIRMA5	Clase que implementa la interfaz AfirmaMapping y devuelve un map en el método getMappingUserDetails con la correspondencia de los datos devueltos en el retorno de @firma y la clase AuthenticatedUserDetails	es.guadaltel.framework.authenticator.config.DefaultAfirmaMapping	N
FIRMA.MODO	Tipo de firma, especifica si los datos se firmarán en bloque o de forma masiva.	MASIVA	N
FIRMA.SIGNATURE.MODE	Indica el tipo de datos a firmar, si se firmará el contenido binario o el hash del fichero.	BINARIO/HASH	S
FIRMA.SIGNATURE.ALGORITHM	Algoritmo de la firma	SHA1	N
FIRMA.SIGNATURE.FORMAT	Formato de la firma	PDF, XADES ENVELOPED, XADES ENVELOPING, XADES IMPLICITO, CADES.	S
FIRMA.APLICACION	Nombre de aplicación dada de alta en el WS de @firma		S
FIRMA.URL	Url de acceso al servidor donde están los WS nativos de @firma		S
FIRMA.VALIDAR.CERTIFICADO	Indica si los certificados serán validados contra la plataforma @firma	S/N	S
FIRMA.VALIDAR.FIRMA	Indica si las firmas serán validadas contra la plataforma @firma	S/N	S
FIRMA.SELLO	Indica si se obtendrá el timepstamp de las firmas con la plataforma @firma	S/N	S
FIRMA.TRUSTEDSTORE	Ruta del almacén de certificados. Se deberá indicar este parámetro		S

	cuando la conexión con @firma se realice utilizando el protocolo HTTPS		
FIRMA.TRUSTEDSTORE.PASS	Password del almacén de certificados de confianza. Se deberá indicar este parámetro cuando la conexión con @firma se realice utilizando el protocolo HTTPS		S
FIRMA.SECURITY.MODE	Modo de seguridad	None, UsernameToken (seguridad con usuario y clave), BinarySecurityToken (seguridad con cerficado)	S
FIRMA.SECURITY.USER	Usuario usado para la encriptación de XML de comunicación con ws de @firma (para el modo UserToken).		S
FIRMA.SECURITY.PASSWORD	Contraseña usada para la encriptación de XML de comunicación con ws de @firma (para el modo UserToken).		S
FIRMA.SECURITY.PASSWORD.TYPE	Indica si la contraseña usada para la encriptación de XML de comunicación con ws de @firma va encriptada o no. Su valor por defecto es PasswordText (para el modo UsernameToken).	PasswordText/PasswordDigest	S
FIRMA.SECURITY.FILE.NAME	Indica el nombre del fichero de configuración para la autenticación mediante el método BinarySecurityToken		S
FIRMA.SECURITY.CERT.ALIAS	Alias del certificado dentro del almacén de claves (para el modo BinarySecurityToken)		S
FIRMA.SECURITY.CERT.PWD	Pwd del certificado dentro del almacén de claves (para el modo BinarySecurityToken)		S
EEUTIL.OPER.FIRMA.URL	Url del endpoint de los servicios que contienen las operaciones de validación de certificados y firmas y generación de sellos de tiempo	-	S
EEUTIL.OPER.FIRMA.USER	Usuario de autenticación en eeutil-oper-firma.	-	S
EEUTIL.OPER.FIRMA.PASSWORD	Password de autenticación en eeutil-oper-firma.	-	S
EEUTIL.VALIDAR.FIRMA.ACTIVO	Indica si se van a validar las firmas que se realicen	S/N	S
EEUTIL.VALIDAR.CE	Indica si el certificado se va a validar	S/N	S

RT.ACTIVO	contra eeutil en vez de contra @firma		
EEUTIL.SELLO.ACTIVO	Indica si se tiene activada la generación de sello de tiempo a través de eeutil-oper-firma	S/N	S
EEUTIL.UTIL.FIRMA.URL	Url del endpoint del servicio que contiene las operaciones de generación de CSVs y justificantes de firma		S
EEUTIL.UTIL.FIRMA.USER	Usuario de autenticación en eeutil-util-firma.		S
EEUTIL.UTIL.FIRMA.PASSWORD	Password de autenticación en eeutil-util-firma.		S
EEUTIL.CSV.ACTIVO	Indica si está activo el servicio de CSV de eeutil	S/N	S
EEUTIL.REPORT.ACTIVO	Indica si está activo el servicio de generar justificantes de firma a través de eeutil	S/N	S
EEUTIL.VIS.PREFIRMA.ACTIVO	Indica si se tiene activada la visualización de documentos prefirmados	S/N	S
EEUTIL.MISC.URL	Url del endpoint del servicio que contiene la operación de visualizar documentos TCN		S
EEUTIL.MISC.USER	Usuario de autenticación en eeutil-misc.		S
EEUTIL.MISC.PASSWORD	Password de autenticación en eeutil-misc.		S
EEUTIL.VISUALIZAR.TCN.ACTIVO	Indica si se tiene activada la visualización de documentos TCN	S/N	S