Manual de la herramienta de Administración de @firma 6.4

Documento nº:	@Firma-Administracion-MAN
Revisión:	043
Fecha:	09-12-2021
Período de retención:	Permanente durante su período de vigencia + 3 años después de su anulación

CONTROL DE MODIFICACIONES

Documento nº:	@Firma-Administracion-MAN
Revisión:	043
Fecha:	09-12-2021

Rev.	001
Fecha	04-03-2013
Descripción	Documentación inicial.

Rev.	002
Fecha	08-03-2013
Descripción	Revisión y adaptación de la documentación respecto al entregable generado el día 08/03/2013.

Rev.	003
Fecha	18-03-2013
Descripción	Incluida información asociada a la generación de informes de aplicaciones. Incluida paginación de certificados asignados a las aplicaciones. Revisión y adaptación de la documentación respecto al entregable generado el día 18/03/2013.

Rev.	004
Fecha	11-04-2013
Descripción	Se modifica el proceso de importación inicial de modo que se tiene en cuenta la posibilidad de no realizar la importación de las TSL y políticas de firma desde un esquema Oracle anterior.

Rev.	005
Fecha	28-05-2013
Descripción	Se incluye interfaz de generación de TSL desde el módulo de gestión de políticas de validación.

Rev.	006
Fecha	04-12-2013
Descripción	Se incluye una nota en el apartado 5.3.6.1.1 indicando un bug de Primefaces en IE10.

Rev.	007
Fecha	21-02-2014
Descripción	Se añade nota (punto 5.3.10.5) para indicar que, en el caso de importar la implementación XML de la política de firma de la AGE v 1.9, se debe usar el parseador XML en su versión 1.1. Igualmente, se indica que, en el caso de importar la implementación ASN.1 de la política de firma de la AGE v 1.9, se debe usar el parseador ASN.1 en su versión 1.1.

Rev.	008
Fecha	07-07-2014
Descripción	Se incluye en la Gestión de Aplicaciones una nueva sección (punto 5.3.4.5.4) para indicar las TSL que son habilitadas para la validación de la aplicación seleccionada. También se ha mejorado la forma de presentar los listados de certificados en los distintos apartados de la Gestión de Aplicaciones y en la Gestión de Keystores, incluyendo también un icono al lado de cada alias, para indicar el estado en el que se encuentra el certificado. Se han actualizado las imágenes donde se reflejan estos cambios.

Rev.	009
Fecha	23-10-2014
Descripción	Se incluye las descripciones y referencias necesarias para explicar el comportamiento de un nuevo atributo en la configuración de @firma que determina si un PSC puede ser exportable o no, así como en todas las cosas en las que afecta. Este cambio afecta a los apartados correspondientes de PSC, proceso de exportación de políticas de certificación y generación de TSL. Se elimina el campo “RequestorName Obligatorio” de los Métodos de Validación OCSP. Se elimina la funcionalidad de generación de TSL a partir de las políticas de certificación.

Rev.	010
Fecha	16-02-2015
Descripción	Repaso general de la aplicación, sustituyendo las capturas de pantalla por los nuevos diseño. Añadimos toda la funcionalidad del módulo de la gestión de TSL. Se añade el módulo de Gestión de TSAs. Se añaden las referencias a DIR3, tanto en la Gestión de aplicaciones como en la configuración de la plataforma.

Rev.	011

Fecha	26-02-2015
Descripción	Se elimina el apartado de comprobación y validación del documento. Se elimina cualquier referencia a autor y a empresa. Se añade información de nuevos almacenes de claves y certificados. Se modifica la visualización de los certificados y claves privadas. Se añade el concepto de archivado asociado a certificados en el Almacén de PSC, Almacén de Confianza OCSP y Almacén de Confianza CRL.
Rev.	012
Fecha	20-04-2015
Descripción	Se añade toda la información asociada a la funcionalidad para gestionar la localización de los almacenes de claves, software y hardware. Se corrigen los subtítulos de las ilustraciones del documento. Se elimina de la Gestión de Configuración el punto relativo a Almacenes de Claves.
Rev.	013
Fecha	29-04-2015
Descripción	Se añade la información asociada a la nueva funcionalidad para crear tareas de validación, esto es, de caducidad y revocación, tantas como se quieran, para asociar a cada una los planificadores que se deseen y los almacenes de claves sobre los que aplican.
Rev.	014
Fecha	04-05-2015
Descripción	Se añade el módulo de SQL y LOGs.
Rev.	015
Fecha	22-05-2015
Descripción	Se añaden la “Plataforma de Mensajería” y la gestión de “SMS” en el módulo de Configuración. Aparte se modifica el alta de destinatarios en las alarmas, permitiendo ahora elegir entre tres tipos: correo electrónico, teléfono y host. Para modificar o eliminar dichos destinatarios, debemos recurrir a la zona de administración de “Destinatarios” en el módulo de Configuración.
Rev.	016
Fecha	01-06-2015
Descripción	Se añade la “Gestión de Plataformas Federadas” en el módulo de Configuración.
Rev.	017

Fecha	16-06-2015
Descripción	Se añade los check de “Custodia” en los parámetros de la gestión de aplicaciones.

Rev.	018
Fecha	18-06-2015
Descripción	Se extrae la“Gestión de Plataformas Federadas” a un documento aparte.

Rev.	019
Fecha	29-09-2015
Descripción	Se elimina la posibilidad del alta automática de certificados desde la gestión de PSC. Se indica que la exportación de mapeos se realiza en archivo XML o archivo JSON, y que se importa desde un archivo JSON. Se añade una descripción para indicar cómo buscar aplicaciones y unidades organizativas desde la gestión de las mismas. Se eliminan las operaciones que permiten copiar, pegar y eliminar aplicaciones y unidades organizativas desde el menú contextual del árbol de aplicaciones y unidades organizativas. Se elimina cualquier reseña al proceso de importación inicial. Se actualiza la información relativa a los procesos de importación y exportación de políticas de certificación. En el apartado 5.3.1 se indica la necesidad de seleccionar el nodo correcto antes de dar de alta una CA/SubCA/Tipo de Certificado.

Rev.	020
Fecha	01-10-2015
Descripción	Se incluye un comentario en la definición de mapeos de tipo “concatenación” indicando que no deben asociarse campos del certificado si se plantea exportar la política de certificación hacia una plataforma @firma 5.5.0_004, ya que no es compatible con esta definición.

Rev.	021
Fecha	05-11-2015
Descripción	Se modifica la declaración de los métodos de validación tipo CRL y OCSP con un nuevo parámetro que sirve para indicar si debe hacerse uso de la configuración de autenticación cuando se establezca conexión con una URL extraída de los puntos de distribución del certificado a validar.

Rev.	022
Fecha	16-11-2015
Descripción	Se añade punto “Comprobación de nuevas TSL disponibles”.

Rev.	023

Fecha	17-11-2015
Descripción	Se incluye la comparación de una TSL con las Políticas en su consulta, dentro del módulo de “Gestión de TSL”. Añadimos también la exportación de dichos resultados a fichero Excel.
Rev.	024
Fecha	19-11-2015
Descripción	Se complementa el punto 5.3.8.1 en lo relativo al estado “Bloqueado” de la alarma.
Rev.	025
Fecha	26-11-2015
Descripción	Se añade un nuevo punto en el que se explica la nueva funcionalidad para recargar una aplicación desde la Base de Datos a la caché compartida del cluster.
Rev.	026
Fecha	02-12-2015
Descripción	Se especifica en la gestión de tareas la existencia por defecto de la tarea que actualiza las TSL. Se añade en la gestión de mapeos de TSL una nota con los mapeos “estáticos” que se obtienen siempre que se valide un certificado mediante una TSL. Se concretan las especificaciones (y versiones) de las que se dispone de una implementación en la plataforma para poder interpretar las TSL.
Rev.	027
Fecha	15/02/2016
Descripción	Repaso general de la plataforma, actualizando el manual con la última versión de @firma6 y teniendo en cuenta una serie de indicaciones por parte de Soporte. Se actualiza Figura 13. – Módulo de Gestión de PSC. Panel de alta, en el que desaparece la opción de Alta automática de certificados. Se actualiza la Figura 69 - Ventana de registro de Aplicación (III), donde aparece el campo “Política de resultados de verificación de firma.” En el punto 5.3.14.1.10 – Firma, se actualizan propiedades (se añade selección de algoritmo de resumen y se elimina indicador para afirmar que existe TSA configurada). En el punto 5.3.14.1.14 – TSL, se añade nueva propiedad.

Rev.	028
Fecha	06/06/2016
Descripción	Se realiza una revisión completa del documento adaptándolo y realizando los cambios necesarios respecto a la versión final 6.2.0_000 de @firma. Tras haber modificado la forma de funcionamiento de la caché compartida a una local en cada nodo del clúster, se añade un nuevo botón para solicitar la recarga de la configuración en todos los nodos del clúster. Se añade una nueva funcionalidad en la pestaña de PSC que comprueba la posibilidad que existan identificadores de tipos de certificados no válidos, y discriminadores repetidos para distintos tipos de certificados bajo una misma CA, notificándolo mediante una ventana modal al administrador de la plataforma. Se eliminan todas las referencias a la funcionalidad de recargar una aplicación en la caché compartida.

Rev.	029
Fecha	14/12/2016
Descripción	Se realizan ajustes en diseño de la plantilla. Se inserta una nueva propiedad de configuración (general) relativa a los protocolos SSL restringidos. Se explica adecuadamente las posibles contingencias de recarga de la caché del clúster tras la ejecución de las tareas de revocación y caducidad. Se elimina la configuración relativa a los servicios de sello de tiempo mediante RFC3161 + SSL.

Rev.	030
Fecha	20/01/2017
Descripción	Se actualiza el punto 5.3.4.8 para indicar que cuando se pulsa sobre el botón "Sincronizar Todas las Unidades Organizativas desde DIR3" se lleva a cabo el funcionamiento indicado como hasta ahora, pero además, aquellas unidades organizativas que tienen definido el identificador de tipo DIR3 pero dicho identificador no se encuentra registrado en DIR3, o lo que es lo mismo, en la petición a DIR3 con todas las unidades organizativas presentes no se encuentra ninguna cuyo identificador coincida, serán a su vez también eliminadas, ya que poseen un identificador de DIR3 que no se encuentra realmente en DIR3.

Rev.	031
Fecha	09/03/2017
Descripción	Se actualizan los apartados 5.3.7.2.6 y 5.3.4.8 para indicar explícitamente los costes y riesgos de la sincronización con DIR3, así como el comportamiento de la plataforma en función de la configuración establecida. Se actualiza el apartado 5.3.4.5.1 para indicar explícitamente el valor que puede adoptar el identificador de una aplicación, así como el valor recomendado durante su proceso de alta.

Rev.	032
Fecha	10/03/2017
Descripción	Se actualiza el apartado 5.3.1.2 detallando correctamente los campos a establecer a la hora de especificar un discriminador para un tipo de certificado.

Rev.	033
Fecha	09-10-2017

Descripción	Se actualizan las capturas de todos los módulos.
	Se incluye las descripciones de nuevas funcionalidades:
	• Módulo PSC. Se añade la posibilidad de archivar un certificado del listado para un PSC seleccionado.
	• Módulo de aplicaciones. Se añade una nueva funcionalidad que permite mover los elementos del árbol de unidades organizativas y aplicaciones.
	• Módulo de Configuración:
	  ○ Se añade el servidor secundario de validación.
	  ○ Nuevo apartado para la gestión de los responsables de las aplicaciones.

Rev.	034
Fecha	02-03-2018
Descripción	Se elimina la vinculación de las aplicaciones con listas TSL. Se actualiza el apartado 5.3.4.5.2 para incluir el nuevo check que posibilita la validación de la aplicación contra TSL. Se elimina el anterior apartado “5.3.4.5.4 TSLs disponibles” dado que ya no se permite la vinculación de listas TSL con las diferentes aplicaciones.

Rev.	035
Fecha	08-03-2018
Descripción	Se actualiza el apartado 5.3.7.2.6 Configuración de la tarea "Realizar copia de seguridad del esquema de configuración" para incluir una anotación para indicar que la tarea debe estar inactiva en el caso en que la tarea se realice de forma externa al sistema.

Rev.	036
Fecha	11-05-2018
Descripción	Se añade en el apartado "5.3.2.1.2 - Alta Método de Validación CRL" la descripción de los distintos tipos de acceso para los métodos de validación tipo CRL, añadiendo uno nuevo, HTTP Secuencial.

Rev.	037
Fecha	29/05/2018
Descripción	Se modifica el punto 10.3.1 para indicar las palabras que no pueden utilizarse como identificadores de variable.

Rev.	038
Fecha	04/06/2018
Descripción	Se modifican las pantallas del módulo de Gestor Documental eliminando el gestor de Alfresco incluido por defecto.

Rev.	039
Fecha	22/06/2018
Descripción	Se modifica el apartado 5.3.13.3.1 para ampliar la información relativa al certificado firmante en las respuestas OCSP.

Rev.	040
Fecha	20/09/2018
Descripción	Se actualiza el manual con los últimos cambios de la plataforma. • Se actualiza el módulo de aplicaciones para añadir los cambios de aplicación prioritaria y no prioritaria. • Se actualiza la pestaña de tareas para contemplar el caso en el que la plataforma esté en mono-nodo. • Se actualiza el módulo de alarmas para contemplar el caso en el que la plataforma esté en mono-nodo.

- Se añade la nueva funcionalidad de validación de firma del módulo de consultas.

Rev.	041
Fecha	23/10/2019
Descripción	Se actualiza el manual con los últimos cambios de la plataforma.

- Se cambia el traslado de datos a través del clúster por la generación de versiones de la base de datos de configuración.
- Eliminamos el módulo de TSLs, ya que ahora éstas serán tratadas desde la plataforma de valET.
- Se añade la configuración de conexión con la plataforma de valET en el módulo de "Configuración".
- Se añade la importación de PSCs del fichero obtenido de la aplicación externa CA_DeskTools en el módulo de "Importación/exportación de Configuraciones".

Rev.	042
Fecha	28/10/2021
Descripción	Se actualiza el manual con los últimos cambios de la plataforma.

- De la Gestión de Aplicaciones, se eliminan en el apartado de "Parámetros de la Aplicación" los campos: "Aplicación con prioridad" y "Mantener el nivel actual".
- En la Gestión de Usuarios, se añade en el alta de nuevo usuario administrador un nuevo campo para añadir el certificado del usuario.
- En el Gestión de Tareas, se elimina la tarea "Prioridad de aplicaciones."
- Se elimina el apartado "TSLs" en 5.3.13.1 Configuración propiedades de la plataforma de la Gestión de Configuración.

Rev.	043
Fecha	09/12/2021
Descripción	Se actualiza el manual eliminando referencias erróneas a la versión 6.3

Control de Distribución

Documento nº:	@Firma-Administracion-MAN
Revisión:	043
Fecha:	09-12-2021

Propiedad del documento:

Este documento pertenece al Gobierno de España y posee un carácter de público para uso y distribución en ámbitos autorizados por este mismo, según se recoge en la declaración de privacidad.

Declaración de privacidad:

El contenido de este documento está sujeto al protocolo de libre distribución dentro del entorno definido para el contexto.

Copias Electrónicas:

La distribución de este documento ha sido controlada a través del sistema de información.

Copias en Papel:

La vigencia de las copias impresas en papel está condicionada a la coincidencia de su estado de revisión con el que aparece en el sistema electrónico de distribución de documentos.

El control de distribución de copias en papel para su uso en proyectos u otras aplicaciones es responsabilidad de los usuarios del sistema electrónico de información.

Fecha de impresión 09 de diciembre de 2021

Índice

1 Objeto 14

2 Alcance 14

3 Siglas 15

4 Documentos de Referencia 16

5 Módulo de Administración de la Plataforma @Firma 17

5.1 Descripción General 17

5.2 Acceso al interfaz gráfico del módulo de Administración 20

5.2.1 Información del usuario logado en la plataforma. 26

5.2.2 Generar versión de la base de datos de configuración 27

5.3 Componentes 28

5.3.1  Gestión de PSCs 29

5.3.2  Gestión de Métodos de Validación 50

5.3.3  Gestión de Políticas de Certificación 66

5.3.4  Gestión de Aplicaciones y Unidades Organizativas 88

5.3.5  Gestión de Usuarios 116

5.3.6  Gestión de Keystores 121

5.3.7  Gestión de Tareas 138

5.3.8  Gestión de Alarmas 159

5.3.9  Gestión de Descargas de CRLs. Caché de nivel 2 167

5.3.10  Gestión de Políticas de Firma 171

5.3.11  Gestión de TSA 179

5.3.12  Gestión de Gestores Documentales 191

5.3.13  Gestión de Configuración 195

5.3.14  Módulo Importación y Exportación de Configuraciones 227

5.3.15  Módulo de Auditoría 240

5.3.16  Módulo de Consultas 252

6 Anexo I. Caso Práctico: Utilización de CRL particionadas y descarga en caché L2 261

6.1 Configuración del PSC 262

6.2 Adición del certificado emisor de las CRL en el almacén de confianza de CRL 263

6.3 Configuración de los métodos de validación 265

6.4 Asignación de los métodos de validación 268

6.5 Creación de las tareas de descarga de las CRL 268

7 Anexo II. Caso práctico. Definición de métodos de validación: Tipo Asociación "Expresión Regular" 272

7.1 Expresiones regulares estándar de Java 272

7.2 Referencias a otros campos lógicos 274

7.3 Ejemplos prácticos 274

7.3.1 Ejemplo utilización expresión de Java 274

8 Anexo III. Recomendaciones de uso seguro de la plataforma @Firma 6.4 278

9 Anexo IV. Tratamiento de datos de carácter personal: LOPD 279

10 Anexo V. Definición y uso de pseudocódigo en la plataforma 280

10.1 Introducción. 280

10.2 Proceso de ejecución del pseudocódigo. 280

10.3 Estructura del pseudocódigo. 281

10.3.1 Definición de variables. 281

10.3.2 Realización de asignaciones. 282

10.3.3 Retorno de valores. 286

10.3.4 Ejemplo usando atributos de certificado. 287

11 Anexo VI. Implementación propia de cliente TSA. 289

1 Objeto

Es objeto de este documento describir la herramienta de administración de la plataforma de Validación y Firma Electrónica, @firma v6.4.

2 Alcance

El presente documento recoge un manual de administración y casos prácticos para gestionar la plataforma de validación y firma electrónica, @firma 6.4.

Los objetivos globales de este proceso son:

- Describir la utilización del interfaz gráfico del módulo de Administración.
- Enumerar y describir los componentes que forman dicho módulo.
- Mostrar varios casos prácticos de uso del módulo de Administración.

3 Siglas

ASN.1	Abstract Syntax Notation One
CA	Autoridad de Confianza
CDP	CRL Distribution Point
CRL	Certificate Revocation List
DES	Data Encryption Standard
FTP	File Transfer Protocol
HSM	Hardware Security Module
HTTPS	HyperText Transport Protocol Secure
IP	Internet Protocol
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PSC	Prestador de Servicios de Certificación
SOAP	Simple Object Access Protocol
SSL	Secure Socket Layer
TSL	Trusted Service Status List
UO	Unidad Organizativa
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
XAdESBES	XML Advanced Electronic Signature – Basic Electronic Signature
XAdEST	XML Advanced Electronic Signature – Timestamping
XML	Extensible Markup Language
XMLDSignature	XML Advanced Electronic Signature

4 Documentos de Referencia

- Documento @Firma-InstalacionyDespliegue-MAN, Manual de Instalación y despliegue de la plataforma @Firma 6.4.

5 Módulo de Administración de la Plataforma @Firma

5.1 Descripción General

El módulo de Administración de la plataforma de @Firma v6.4 tiene como objetivo permitir la configuración de todos los elementos, susceptibles de ello, que conforman la plataforma.

Entre sus características principales se encuentran:

- **Centralización de la configuración**. Todos los parámetros de configuración de la plataforma @firma han sido agrupados en un único elemento de configuración, independientemente de los nodos del *clúster* que conforma la plataforma y de los servicios ofrecidos por la misma.

- **Administración remota de la plataforma @firma y Administración delegada**. La administración delegada permite que los propios organismos usuarios de la plataforma configuren sus aplicaciones y generen sus reportes de consultas y estadísticas de uso. Para mayor detalle, consulten el manual específico de Administración Delegada.

- **Securización**. El sistema de administración se encuentra protegido por un doble sistema de seguridad:

    - Sistema de logado para usuarios basado en usuario y contraseña. El nivel de acceso de los distintos usuarios se establecerá en base a unos roles que determinarán el campo de acción. Alternativamente se permite la identificación del usuario mediante certificado digital.

    - Securización de las comunicaciones mediante *https*.

- **Realización de copias de seguridad de la configuración del servidor**, dando la posibilidad de recuperar manualmente la configuración estable de una base de datos anterior.

Los elementos o componentes que permite gestionar mediante sus interfaces gráficos este módulo son:

- **Prestadores de servicios de certificación**. Este componente permite registrar y modificar los prestadores que van a ser considerados por la plataforma, así como aquellos tipos de

certificados que puede emitir cada uno de ellos y su información (información DPC, discriminador de tipo de certificado, etc.).

- **Métodos de validación**. Este componente registra los distintos mecanismos de validación de certificados, así como la configuración necesaria para el correcto funcionamiento de cada uno de ellos.

- **Políticas de certificación**. Este componente define las diferentes políticas de certificación que podrán aplicarse a las aplicaciones registradas en la plataforma. Se define como política de certificación, al conjunto constituido por un certificado patrón (con sus correspondientes campos lógicos) y a los diferentes mapeos de los tipos de certificados aplicados sobre dicho certificado patrón.

- **Unidades organizativas y aplicaciones**. Este componente realiza la administración de unidades organizativas y gestión de aplicaciones, permitiendo configurar diversos aspectos como la política de certificación que se aplicará, securización de los servicios web, firma de las respuestas, custodia de documentos, etc.

- **Usuarios**. Mediante este componente es posible definir los usuarios encargados de administrar, monitorizar y auditar la plataforma.

- **Almacenes de certificados**. Mediante este componente se pueden configurar los distintos almacenes de certificados registrados en la plataforma.

- **Tareas**. Este componente permite administrar procesos que serán ejecutados periódicamente por la plataforma en segundo plano.

- **Alarmas**. Mediante este componente los administradores de la plataforma podrán configurar los destinatarios que deben ser informados, mediante un e-mail, por el lanzamiento de cada uno de los tipos de alarmas existentes en el sistema. También permite configurar el servidor de correo a utilizar, además de una completa gestión de creación y modificación de resúmenes de alarmas.

- **Planificador de descargas de CRL**. Este componente es el encargado de gestionar las tareas que van a permitir la descarga/actualización periódica de las CRL de los prestadores reconocidos por la plataforma, así como los accesos a las mismas. Estas CRL conformarán una

caché de segundo nivel que permitirá una mayor eficiencia a la hora de consultar el estado de los certificados a validar.

- **Gestión de Políticas de Firma**. Este componente permite gestionar las diferentes políticas de firma y sus versiones que podrán utilizarse en procesos de generación y validación de firmas EPES.

- **Gestión de TSA.** Este componente permite la gestión de configuración de múltiples TSA que se pueden asociar a las distintas aplicaciones disponibles.

- **Gestión de Gestores Documentales.** Este componente aporta la funcionalidad para dar de alta, modificar y gestionar gestores documentales externos a la plataforma.

- **Gestión de la configuración.** Este módulo permite gestionar todas las propiedades involucradas en el correcto funcionamiento de la plataforma. También gestiona los servidores internos (OCSP, Servidor de Correo), destinatarios de correos de alarmas, caché nivel 1, y el control del modo de emergencia.

- **Gestión Importación / Exportación de configuración.** Este módulo permite realizar importaciones y exportaciones de políticas de certificación, importar PSCs obtenidos de la aplicación externa de gestión de PSCs o generar una copia local de la configuración actual en el servidor.

- **Módulo de auditoría.** En la versión @firma 6.4, el módulo de auditoría ha sido incluido dentro del módulo de administración de la plataforma. En este módulo el administrador puede consultar las trazas de mantenimiento, servicio y las alarmas ocurridas en la plataforma.

- **Módulo de Consultas.** Este módulo permite realizar consultas básicas sobre la base de datos del sistema que elijamos, así como poder consultar los diferentes logs de la aplicación y verlos directamente en pantalla o descargarlos si nos resulta necesario. Además, desde este módulo podremos gestionar y revisar los elementos propios de nuestra caché o las del resto de nodos de la plataforma.

5.2 Acceso al interfaz gráfico del módulo de Administración

Para acceder al interfaz gráfico del módulo de Administración es necesario dirigirse a alguna de las siguientes URL:

Modo Securizado	https://IP_MAQUINA/Administracion https://IP_MAQUINA/Administracion/login.seam
Modo normal	http://IP_MAQUINA/Administracion http://IP_MAQUINA/Administracion/login.seam

Donde IP_MAQUINA es la dirección IP de la plataforma @firma, y PUERTO es el puerto de escucha por el cual han sido configurado/s el/los servidor/es de aplicaciones que aloja/n la plataforma. Por defecto esto puertos son: 443 (Modo Securizado) y 8080 (Modo normal).

Una vez insertada la URL en el navegador debe aparecer la siguiente pantalla:

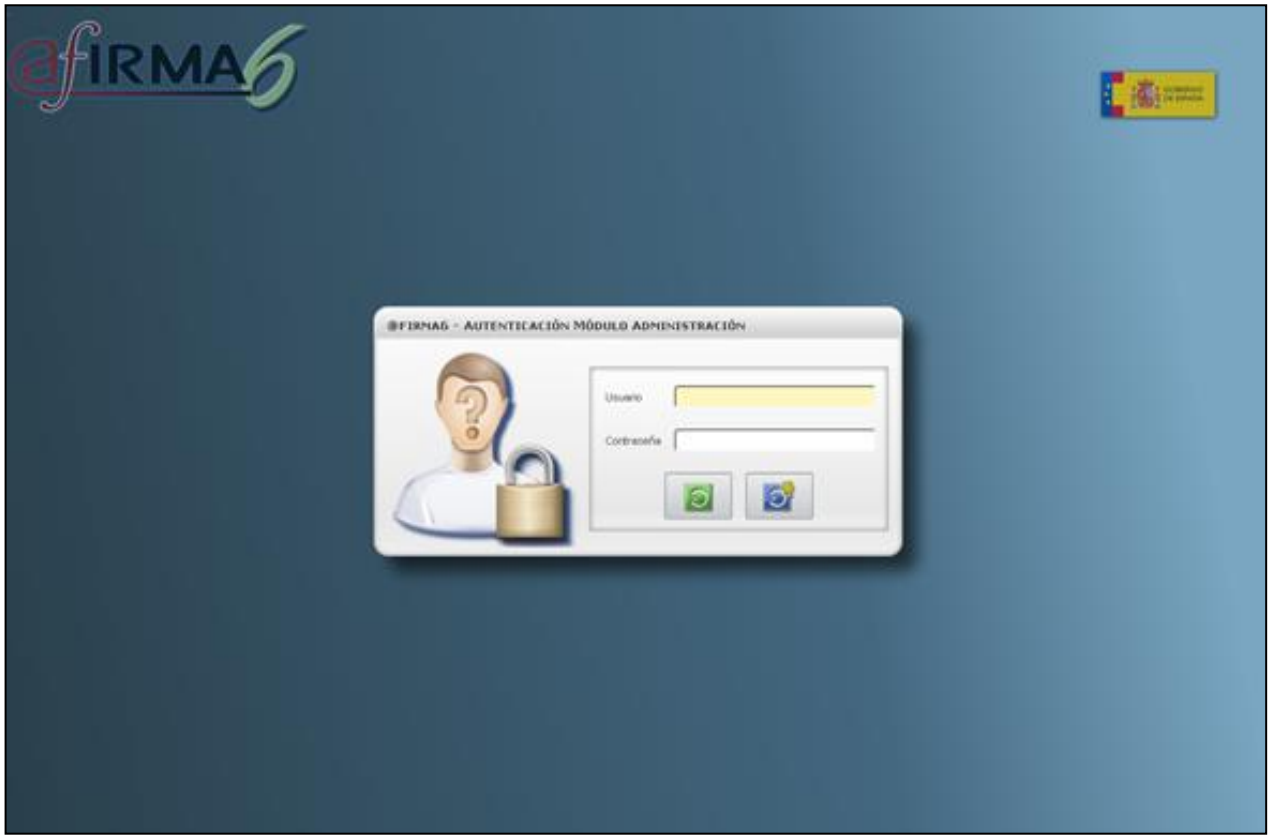


Figura 1 – Interfaz de acceso al módulo de Administración de @firma

Desde esta pantalla de *login* del módulo de administración, se puede acceder mediante usuario y contraseña, o mediante certificado electrónico.

- **Acceso mediante usuario y contraseña** 

Se debe introducir el usuario y contraseña de un usuario (con rol administrador) registrado en la plataforma para poder acceder a dicho módulo y realizar clic en el botón de "Logado mediante Usuario / Contraseña".

En caso de indicar un usuario y/o contraseña incorrectos nos aparecerá una pantalla de error que muestra el error que ha ocurrido:



Figura 2 – Ventana de Error en el proceso de Logado. Campos no especificados



Figura 3 – Ventana de Error en el proceso de Logado. Usuario / Contraseña incorrecta

Otra posibilidad de mensaje de error es el que se da si la plataforma tiene configurada el rol administrador como bloqueable, en el caso que el usuario no inserte correctamente su contraseña muestra el número de intentos restantes.



Figura 4 – Ventana de Error en el proceso de Logado con número de intentos

En el caso de sobrepasar el número de intentos el usuario será bloqueado mostrando el siguiente mensaje:



Figura 5 – Ventana de Error en el proceso de Logado con número de intentos sobrepasado

Si el usuario que intenta acceder se encuentra bloqueado se muestra el siguiente mensaje:



Figura 6 – Ventana de Error en el proceso de Logado, usuario bloqueado

- **Acceso mediante certificado** 

Para acceder mediante certificado electrónico se debe realizar clic en el botón de "Logado mediante certificado de usuario". La aplicación listará los certificados disponibles en el almacén de claves del navegador.

Seleccionaremos el certificado con el que realizar el acceso:

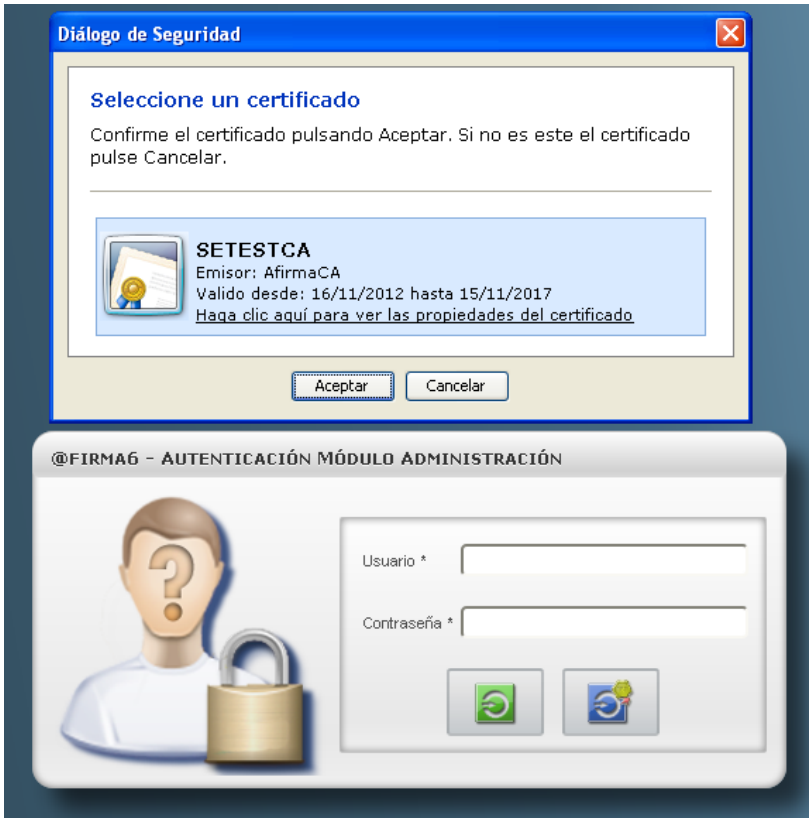


Figura 7 – Ventana de selección de certificado

Si se selecciona un certificado incorrecto se muestra un mensaje indicando que el certificado no es válido/reconocido o no hay ningún usuario dado de alta para el certificado seleccionado:



Figura 8 – Error en la validación de certificado

Si todo ha ido bien se accederá al escritorio principal del módulo de administración, el cual nos permite administrar todos los componentes (aplicaciones, PSC, alarmas, etc.) comentados anteriormente:

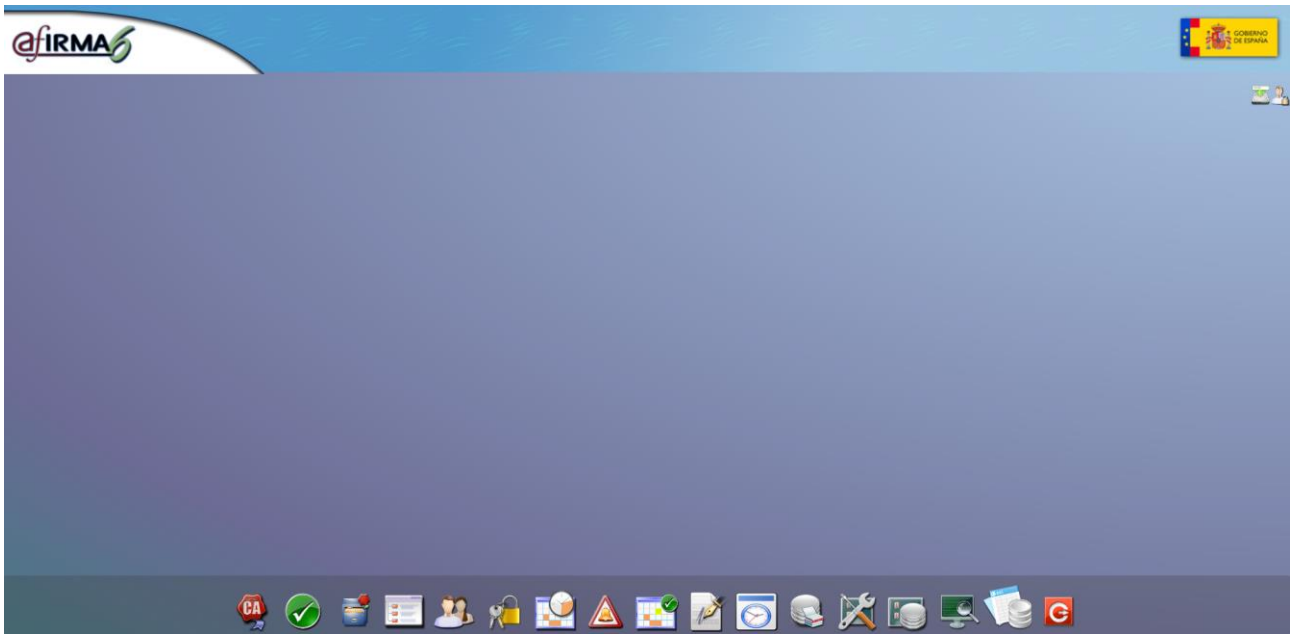


Figura 9 – Módulo de Administración de @firma

5.2.1 Información del usuario logado en la plataforma.

A partir de la versión 6.1.1 se añade en la parte superior del escritorio principal  un icono que permite obtener la información del usuario logado:

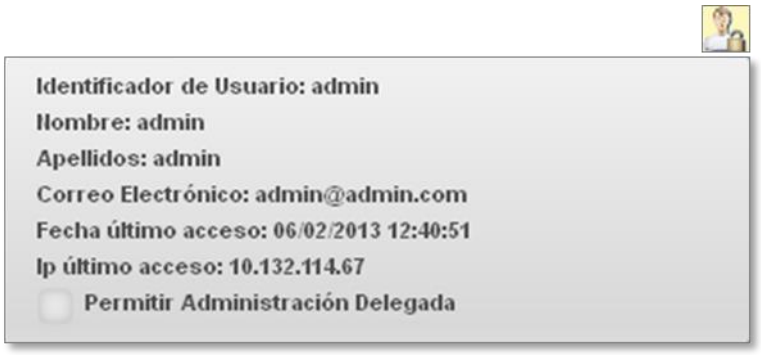


Figura 10 – Módulo de Administración de @firma. Información Usuario logado

- Identificador del usuario logado.

- Nombre.
- Apellidos.
- Email.
- IP de la máquina que accedió por última vez a la plataforma (la IP puede verse afectada debido al uso de proxy).
- Fecha de último acceso (será vacío en caso de que sea la primera vez que acceda a la plataforma).
- Permisos que tiene el usuario en la plataforma.

5.2.2 Generar versión de la base de datos de configuración

En esta versión, el concepto de configuración estable cambia con la nueva arquitectura. Ahora, cuando se hace click en la opción "generar configuración estable", o mejor dicho, "generar copia de la configuración en el servidor", reflejada con el botón .

Una vez se pulsa el botón, antes de continuar con el proceso, se solicita confirmación al administrador mediante el siguiente diálogo:



Figura 11 – Diálogo Confirmación Generar nueva versión de base de datos

En este sentido hay que tener en cuenta que puede darse el caso de que al intentar generar una nueva copia de la base de datos haya habido realmente cambios en la plataforma o no. Esto se indica con los siguientes mensajes:

- Se han realizado cambios en la Administración desde la última vez que se generó una copia de la base de datos.

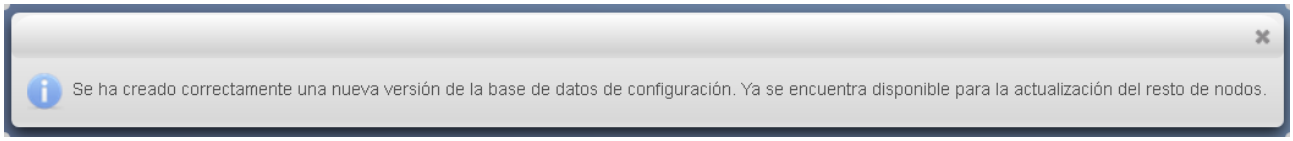


Figura 12 – Mensaje de confirmación de generación de nueva versión de la base de datos

- No se ha realizado ningún cambio en la plataforma desde la última vez que se generó la versión de la base de datos.

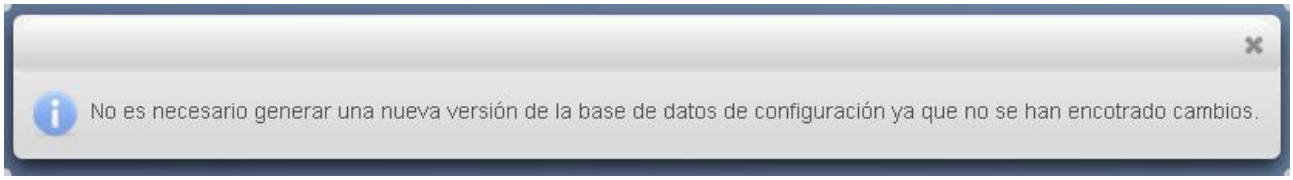


Figura 13 – Mensaje de "no" generación de nueva versión de la base de datos

5.3 Componentes

Mediante la botonera situada en la parte inferior del escritorio es posible gestionar varios aspectos de la plataforma @firma, los cuales están agrupados en componentes. El acceso a la configuración de estos componentes se realiza desde dicho interfaz, como muestra la siguiente figura:



Figura 14 – Módulo de Administración de @firma

Los iconos enmarcados en la parte superior de la imagen habilitan el acceso a las interfaces gráficas que permiten la gestión de los diferentes componentes contemplados en el módulo de administración de la plataforma. A continuación, se muestra relación de componentes e iconos:

- Gestión de PSC
- Gestión de Métodos de Validación.
- Gestión de Políticas de Certificación.
- Gestión de Aplicaciones y Unidades Organizativas.

-  Gestión de Usuarios.
-  Gestión de Keystores.
-  Gestión de Tareas.
-  Gestión de Alarmas.
-  Gestión de Descargas de CRLs. Caché de nivel 2.
-  Gestión de Políticas de Firma.
-  Gestión de TSA.
- Es importante indicar que, por motivos de seguridad, en las exportaciones no se incluye la información privada como contraseñas o partes privadas de certificados.
-  Gestión de Gestores Documentales.
-  Gestión de Configuración.
-  Módulo de Consultas.
-  Cerrar sesión.

En los siguientes apartados se describirán para cada componente los interfaces gráficos que lo conforman, funcionalidades que permiten realizar y la información que gestionan.

5.3.1  Gestión de PSCs

Los PSC (Prestadores de servicios de certificación), conforman la base sobre la que se asienta cualquier infraestructura de PKI. Acreditan la identidad de entidades externas mediante la emisión de certificados digitales x.509v3. Es por tanto primordial establecer un conjunto de PSC que acoten o definan el ámbito de confianza del sistema.

Por otro lado, cada PSC define en su correspondiente "Declaración de Prácticas de Certificación" (DPC) un conjunto de tipologías de certificados finales que puede emitir. Cada tipo de certificado tendrá un significado específico y será reconocido en un contexto determinado. Así, por ejemplo, podrán existir tipos de certificados de personas físicas, jurídicas, para componentes, etc.

Toda esta información debe ser registrada previamente en la plataforma con el fin de poder establecer un ámbito de confianza entre el sistema y los diferentes PSC, y de discriminar cada PSC y los tipos de certificados que emite. Para ello se proporciona el módulo de gestión de PSC que permitirá el registro de cada uno de los prestadores y tipos de certificados que van a ser reconocidos por el sistema. Este proceso conlleva por un lado la determinación de las dependencias existentes entre las distintas CA, y por otro la verificación de la cadena de confianza que garantiza que la identidad del propietario del certificado tiene validez en la fecha presente y cumple con los requisitos definidos en la RFC 3280.

Los PSC se darán de alta mediante el registro en el sistema de sus certificados X509 v3 y de la información necesaria para el tratamiento y gestión de los certificados que pueden emitir. Este mecanismo de gestión permitirá definir la manera de discriminar el tipo de cada certificado.

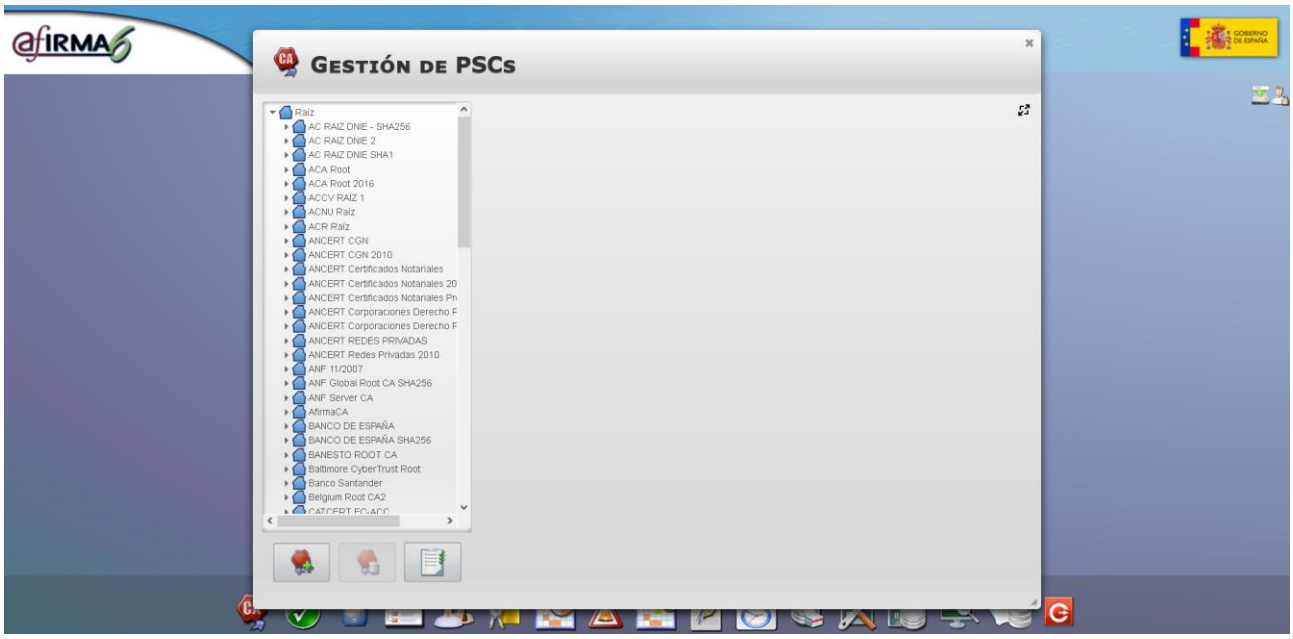
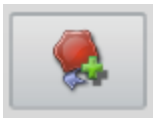


Figura 15 – Módulo de Gestión de PSC

5.3.1.1 Alta de Prestador de Servicios de Certificación



Para dar de alta la jerarquía de certificación es necesario disponer de los certificados X509 v3 asociados a todas y cada una de las entidades a registrar, es decir, el certificado de la CA raíz, de las CA intermedias, en caso de existir, y certificados de ejemplo de cada uno de los tipos de certificados que pueden emitir los PSC.

A tener en cuenta, previo a dar de alta una CA (o subCA), se debe seleccionar el nodo en el árbol sobre el que dicha CA se dará de alta. De este modo, para dar de alta una CA raíz, se debe seleccionar primero el nodo "Raíz", y si fuera a darse de alta una subCA, previamente debería existir y seleccionarse su emisora en el árbol.

Una vez en el módulo de Gestión de Prestadores, el botón de alta abre una ventana para indicar el tipo de alta a realizar:



Figura 16 – Módulo de Gestión de PSC. Panel de alta



Tras seleccionar el tipo de alta ***"Alta CA / subCA"*** se habilita el panel de alta de prestadores.

En esta pantalla, en función del nodo seleccionado en el árbol, los botones podrán estar activos y/o deshabilitados, en concreto:

- Si está seleccionado el nodo raíz: el botón de alta de CA estará habilitado.
- Si está seleccionada una CA o subCA: ambos botones se encontrarán habilitados.
- Si está seleccionado un tipo final: ninguno de los botones estará habilitado.



Figura 17 – Interfaz de alta de Prestador de Servicios de Certificación (I)

En la que se especificarán los siguientes datos:

- **Identificador Certificado:** Identificador de la CA con el que será mostrado el Prestador en el árbol de Prestadores.
- **URL DPC:** URL donde se encuentra publicada la última DPC del prestador.
- **Última Versión DPC:** Última versión de la DPC del prestador.
- **Domicilio Social:** Domicilio social del prestador.

- **Esta CA Será Incluida en las exportaciones de políticas de Certificación:** Marcador que indica si la información de esta CA (y de sus subCAs y tipos subordinados) se tendrá en cuenta a la hora de realizar una exportación de las políticas de certificación o no. En caso de no estar seleccionada, simplemente se ignorará. Esto no afecta a su comportamiento respecto al uso de los servicios que presta.

- **Estado:** Estado del certificado asociado al prestador. Se corresponde con un valor predefinido seleccionable entre una lista de posibles:
    - *Correcto*
    - *Sin Determinar*
    - *Caducado*
    - *Revocado*

- **Estado en el Bridge Europeo:** Estado asociado en el "bridge" europeo. Se corresponde con un valor predefinido seleccionable entre una lista de posibles:
    - *No Adherido*
    - *Adherido*
    - *En Pruebas*

- **Identificador de Partición:** Identificador de la partición de la CRL particionada. Este campo será necesario únicamente cuando el prestador emita CRLs particionadas y se pretenda validar contra ellas los certificados emitidos. Para más información se remite al lector a la gestión de métodos de validación y de tareas de descarga.

- **Certificado Padre:** Número de serie del certificado padre al que se va a asociar la CA que damos de alta. Este dato no aparece en la pantalla si la CA a dar de alta es una raíz, ya que no dependerá de ningún padre.

- **Fichero Adjunto:** Certificado X509 v3 asociado al prestador.

Para dar de alta el certificado en la plataforma y tras rellenar el formulario correspondiente y adjuntar el certificado, se habilita el botón de alta situado en la parte inferior derecha.



Figura 18 – Interfaz de alta de Prestador de Servicios de Certificación (II)

Tras pulsar el botón de alta, la plataforma realizará una validación del certificado (integridad y fechas de validez) procediendo a registrarlo en el sistema, ubicado en su nivel jerárquico correspondiente (En la raíz si es una CA o dentro de su jerarquía de emisor/es). El resultado de la operación se mostrará en una ventana emergente y se refrescará el árbol de prestadores reflejando el nuevo prestador.

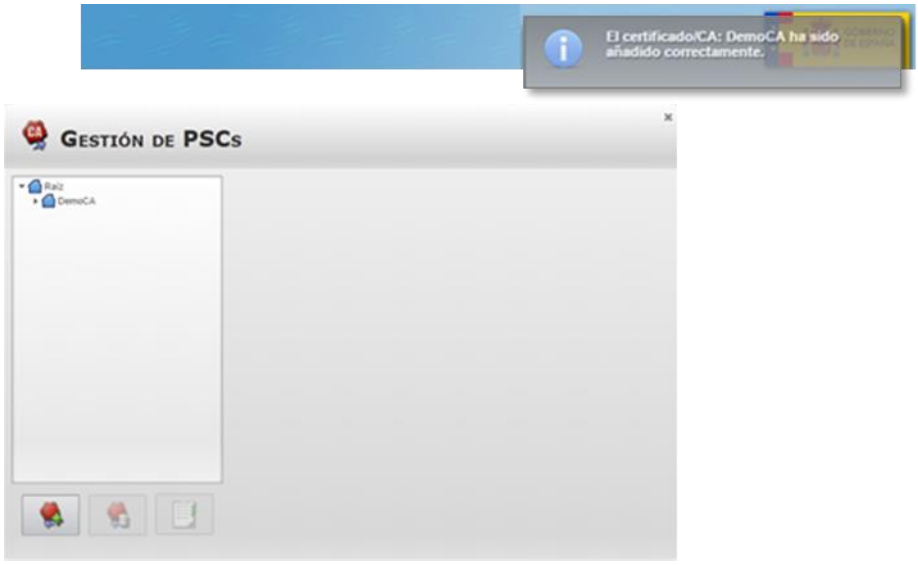


Figura 19 – Alta correcta de PSC / subPSC

Una vez dado de alta el prestador, si se pulsa sobre éste en el árbol de prestadores aparece toda la información que el administrador ha aportado en el alta del mismo.

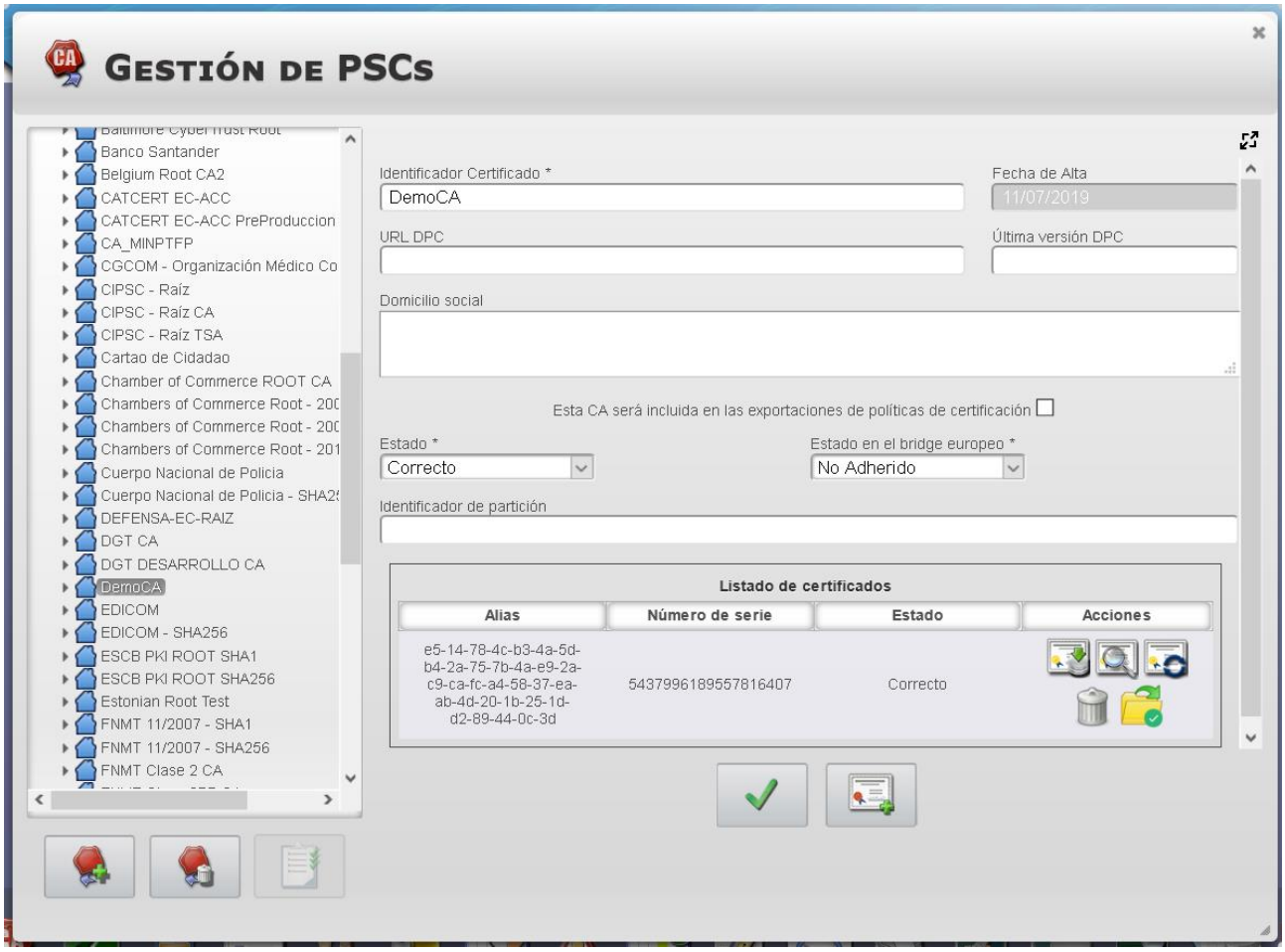


Figura 20 – Información PSC / subPSC

5.3.1.2 Alta de Tipo de Certificado



El proceso de alta de tipo de certificado es similar al de PSC / subPSC. Para ello primero debe seleccionarse un nodo tipo CA (o subCA) en el árbol, y luego pulsar sobre el botón de alta, el cual mostrará un panel con los tipos de altas que se pueden realizar.



Para dar de alta un tipo de certificado junto con su discriminador, sobre un PSC / subPSC existente en la plataforma se pulsará sobre el botón ***"Alta Tipo de Certificado"***.

Tras pulsar el botón ***"Alta Tipo de Certificado"*** aparecerá el formulario asociado al tipo de certificado que se desea dar de alta.



Figura 21 – Formulario Alta de tipo de Certificado (I)

Para dar de alta un tipo de certificado será necesario rellenar los siguientes campos:

- **Identificador:** Nombre identificativo del tipo de certificado a dar de alta. Los identificadores de tipo de certificado son únicos para cada prestador, pero pueden repetirse en diferentes prestadores.
- **Descripción:** Literal utilizado para especificar una descripción más detallada del tipo de certificado.
- **URL Perfil Certificado (opcional):** URL donde el PSC publica la información concreta acerca del tipo de certificado, bien sea una DPC o cualquier otro tipo de documento.
- **Última Versión (opcional):** Versión del tipo de certificado se está utilizando.
- **Priorizar ValET frente a la política de certificación para validar y obtener información de este tipo de certificado:** Este check indica, si está marcado, que se estarán tomando los datos del tipo de certificado seleccionado de la aplicación de ValET, en vez de sacarlos directamente de la política.

- **Estado:** Estado del tipo de certificado. Se corresponde con un valor predefinido seleccionable entre una lista de posibles:
    - *Habilitado*
    - *Deshabilitado*
- **Fichero Adjunto (opcional):** Certificado X509 v3 del tipo que se quiere dar de alta. Este certificado permitirá al administrador definir los criterios de discriminación del tipo de certificado de forma rápida e intuitiva dado que podrá navegar por los diferentes campos que lo componen y seleccionarlos con un simple clic de ratón.

Una vez rellenos los datos requeridos en la pantalla anterior se debe pulsar sobre el botón "Siguiente" que abrirá (si la información introducida es correcta) la pantalla de definición del discriminador de tipo de certificado.



Figura 22 – Definición del discriminador de un tipo de certificado

A la izquierda se muestra un árbol que muestra de forma jerárquica toda la información que contiene el certificado de ejemplo especificado en la pantalla anterior. Pulsando sobre cada elemento se irá

desplegando la estructura, hasta mostrar los campos finales que componen el certificado, y en la parte derecha aparecerá la ruta del elemento que se ha seleccionado, así como su valor correspondiente. En caso de que no exista un certificado de ejemplo para realizar este proceso, la ruta del campo a especificar tendría que ser introducida manualmente en el campo *Atributo del certificado*.

Los campos que aparecen en la pantalla se describen a continuación:

1. **Parte izquierda del discriminador (primer operando):**

   - **Aplicable a.** Mediante este combo podemos definir sobre qué elemento queremos aplicar el discriminador:

     - **Sobre un campo OID del certificado.** En caso de seleccionar esta opción, deberemos definir los siguientes campos:

       - **Atributo del certificado**. Especificará una ruta que especificará de forma inequívoca el atributo del certificado que será utilizado para realizar el proceso de discriminación. Esta ruta puede ser introducida a mano y tendrá el formato:

         {GENERAL || EXTENSION::NOMBRE_CAMPO[::NOMBRE_SUBCAMPO]}

         Algunos ejemplos de rutas válidas:

         {GENERAL::Subject::CommonName}

         {GENERAL::Issuer}

         {GENERAL::SerialNumber}

         {EXTENSION::CertificatePolicies::policyIdentifiers}

       - **Valor Atributo Certificado.** Mostrará el valor del campo del certificado que se haya seleccionado en el árbol de atributos. No mostrará nada si la ruta se especifica manualmente.

     - **Sobre una expresión definida mediante pseudocódigo**

- **Atributo del certificado.** Especificará una ruta que especificará de forma inequívoca el atributo del certificado seleccionado. Útil para hacer uso de esta ruta dentro del pseudocódigo.

- **Valor atributo certificado (Orientativo).** Indica el valor que posee la ruta seleccionada (informativo).

- **Pseudocódigo.** Campo donde se escribirá el pseudocódigo. Para más información consultar el anexo (Anexo V. Definición y uso de pseudocódigo en la plataforma).

2. **Operación a aplicar.** Indica el tipo de comparación que se realizará entre el valor del OID seleccionado / resultado del pseudocódigo con la cadena definida por el administrador de la plataforma. Los posibles valores son:

   - **MATCH:** Realiza una comparación en la que se pueden usar expresiones regulares para definir el segundo operando.

   - **EQUAL:** Realiza una comparación literal de cadenas.

   - **NOT EQUAL:** Evalúa si las cadenas son distintas de forma literal.

3. **Parte derecha del discriminador (segundo operando):** Almacenará el valor con el que será comparado el primer operando por medio del operador seleccionado. En caso que el operador sea “MATCH”, este campo se considerará una expresión regular que se usará para evaluar el primer operando.

Tras especificar el discriminador, se pulsará el botón “Dar de Alta”, y el sistema completará el alta del tipo de certificado asociado al prestador especificado.

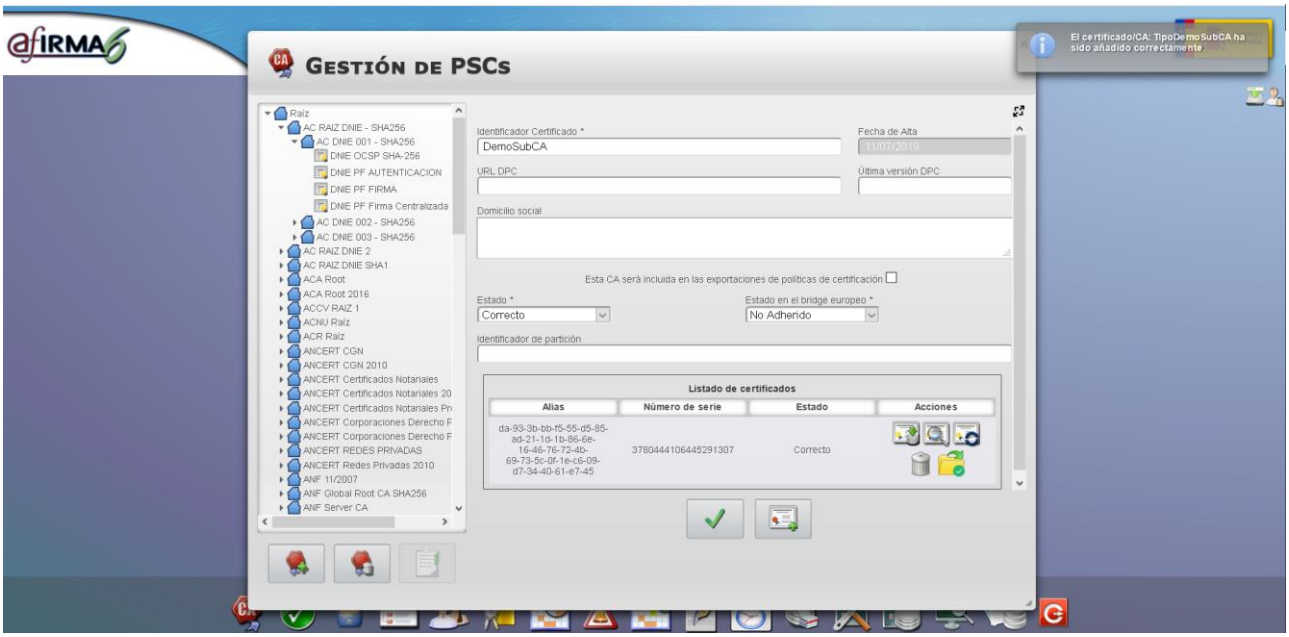


Figura 23 – Alta correcta de Tipo de Certificado



Figura 24 – Información Tipo de Certificado

5.3.1.3 Modificación de PSC / subPSC / Tipo de Certificado



El módulo de administración nos permite modificar los datos de los PSC / Tipos de Certificado, para ello, primero se tiene que seleccionar el elemento que se quiere modificar, en el árbol de prestadores. En la parte derecha de la pantalla se presentará una ventana con los datos del prestador, donde se podrán modificar los datos.

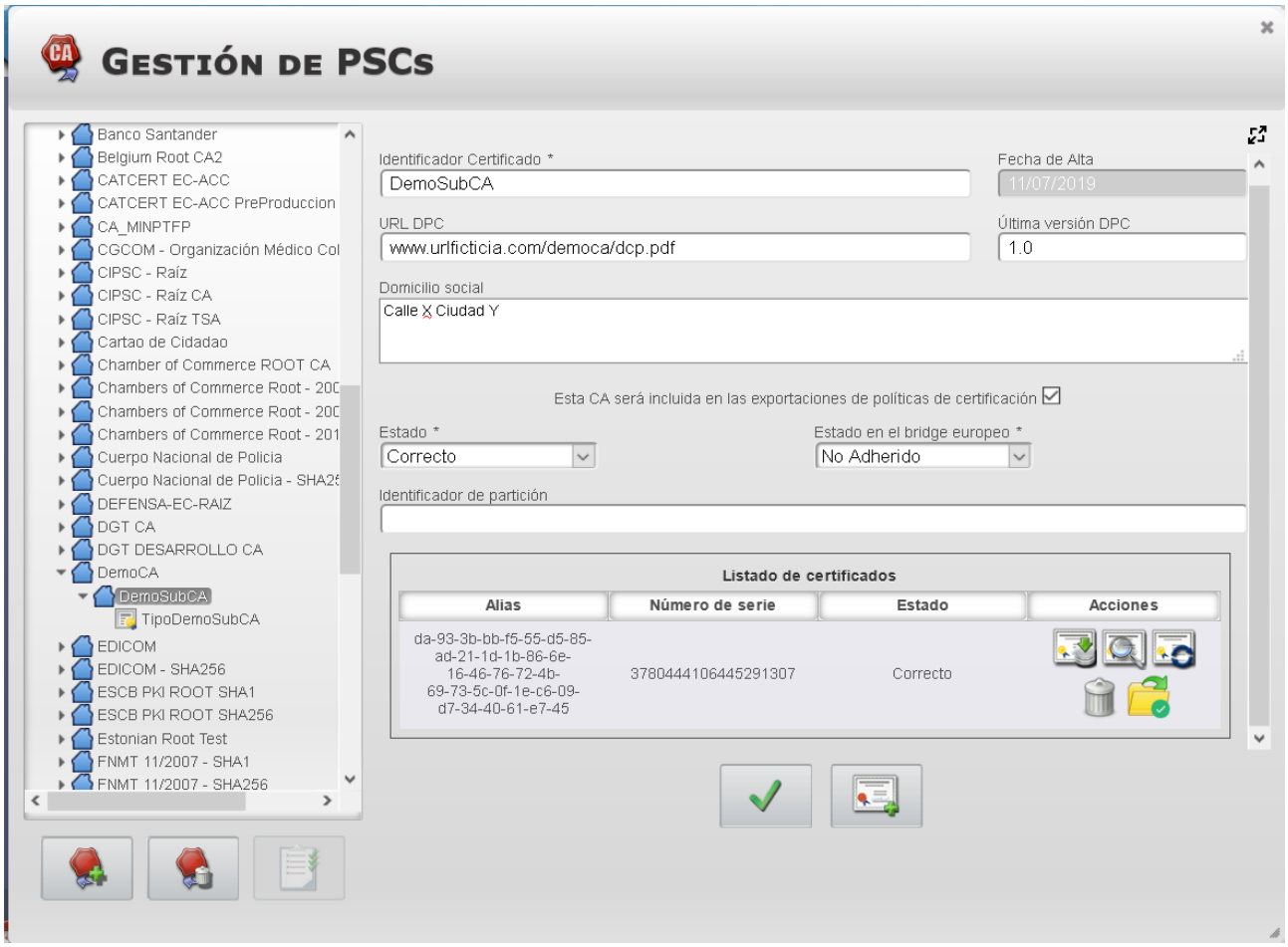


Figura 25 – Modificar datos PSC / subPSC

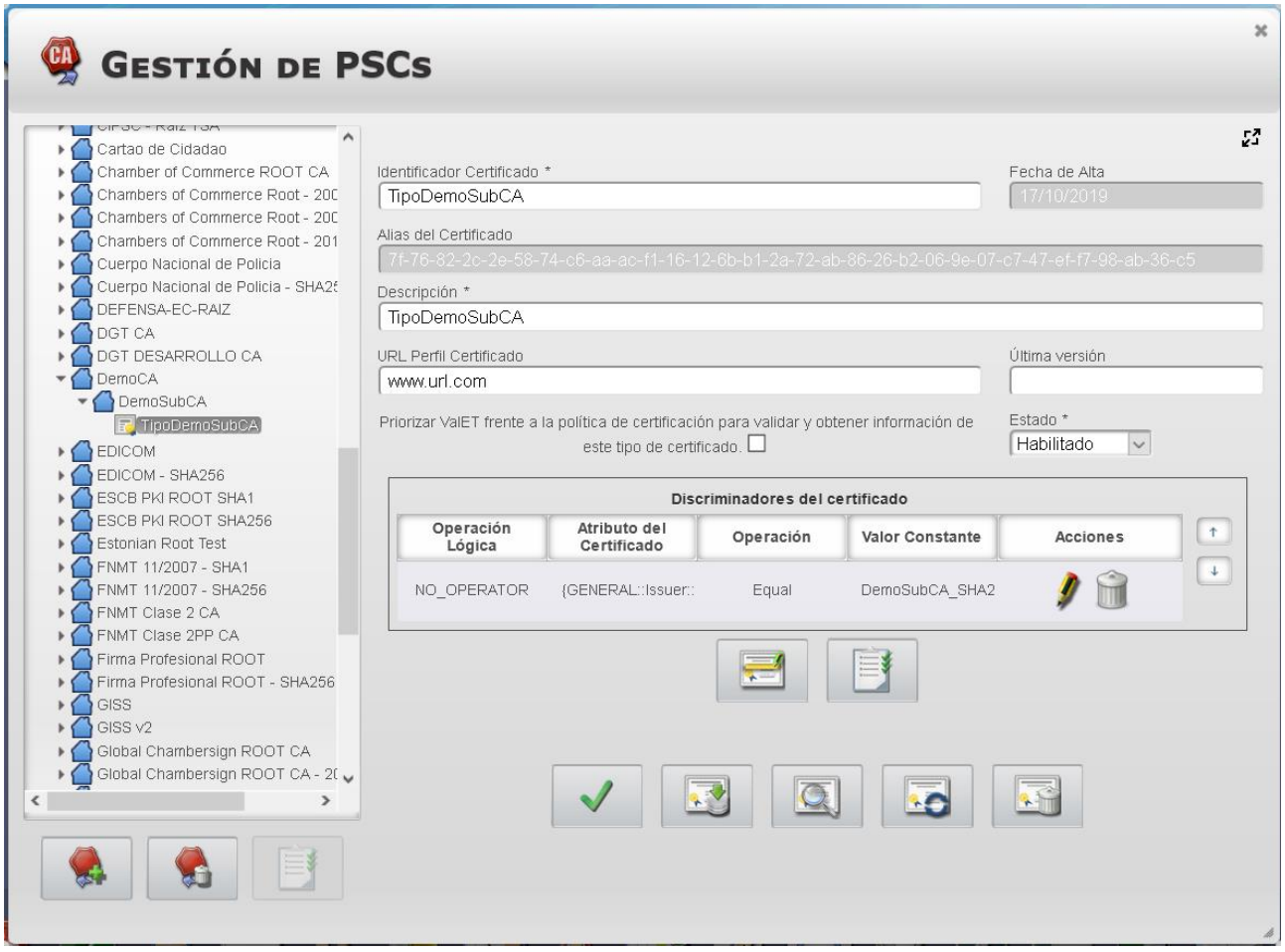


Figura 26 – Modificar datos Tipo de Certificado

Una vez modificada la información, tras pulsar el botón de aplicar cambios, aparece una ventana de pidiendo al usuario su confirmación.

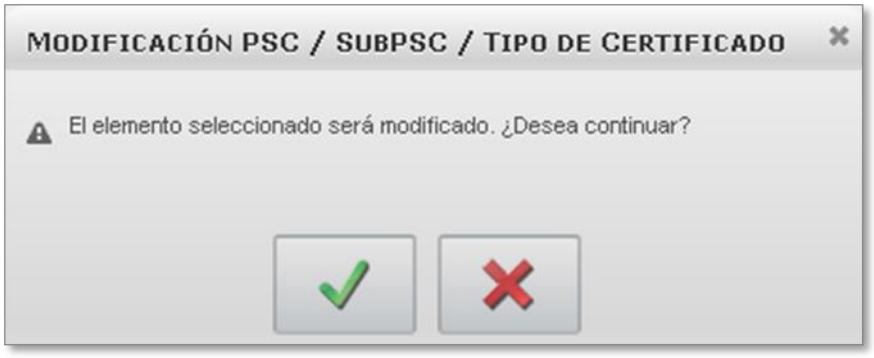


Figura 27 - Panel confirmación.

Tras pulsar en aceptar se realizará la modificación del elemento seleccionado.

5.3.1.4 Baja de PSC / subPSC / Tipo de Certificado



Para eliminar un PSC / subPSC / Tipo de Certificado, primero hay que seleccionar en el árbol el elemento en cuestión, y luego se deberá pulsar el botón de baja situado en la parte inferior del árbol de prestadores. Tras pulsar el botón aparecerá un cuadro de diálogo que pedirá al usuario su confirmación para realizar la operación. Una vez aceptada la plataforma dará de baja el elemento seleccionado del árbol de prestadores.

5.3.1.5 Comprobar Tipos de Certificados y Discriminadores



Desde el módulo de Gestión de PSC se puede realizar una comprobación sobre todos los tipos de certificados dados de alta en la plataforma, de modo que se comprueba si bajo el mismo emisor (CA) existen dos o más tipos de certificados con el mismo discriminador. En ese caso se muestra en una pantalla modal al administrador todos los conflictos encontrados. Es importante indicar que este botón tan solo se encuentra activo cuando se tiene seleccionado el nodo raíz en el árbol de prestadores.



Figura 28 - Panel de discriminadores NO compatibles.

Esta funcionalidad es esencial para la correcta generación de exportaciones de la configuración. En este sentido, antes de realizar la exportación de una política de certificación, siempre se realiza automáticamente esta comprobación.

5.3.1.6 Descargar Certificado (PSC / subPSC / Tipo de Certificado)



La administración permite descargar el certificado asociado al PSC / subPSC o Tipo de Certificado que el administrador ha incluido en el proceso de alta de los mismos. Dicha acción se realizará a través del botón de descargar certificado.

Este botón se encuentra tanto en la interfaz de modificación de PSC / subPSC como la de Tipo de Certificado. En el caso de Tipo de Certificado el botón de descargar aparecerá deshabilitado si el administrador ha eliminado el Certificado de ejemplo asociado.

5.3.1.7 Mostrar información del Certificado (PSC / subPSC / Tipo de Certificado)



Desde el módulo de Gestión de PSC se puede obtener un resumen con la información de los certificados asociados al elemento seleccionado, PSC / subPSC / Tipo de Certificado (siempre que el administrador no haya eliminado el Certificado de Ejemplo). Para ello, una vez hemos seleccionado el elemento en el árbol, debemos de pulsar en el icono que aparece debajo de cada certificado llamado “Mostrar información del certificado”.



Figura 29 - Panel información del Certificado.

5.3.1.8 Actualizar Certificado



Desde esta opción el administrador puede actualizar el certificado asociado al elemento seleccionado (PSC / subPSC / Tipo de Certificado), o incluir un certificado de ejemplo en caso de que el Tipo de Certificado no posea su certificado de ejemplo.



Figura 30 - Panel actualizar Certificado.

5.3.1.9 Eliminar Certificado (PSC)



Esta opción permite eliminar el certificado asociado a un PSC seleccionado. A diferencia de los tipos de certificados, la eliminación de un certificado de PSC solo se permite cuando hay más de uno en el listado de certificados. Si se intentase eliminar el único certificado de la lista se mostrará un mensaje de error que informará al usuario de la restricción.

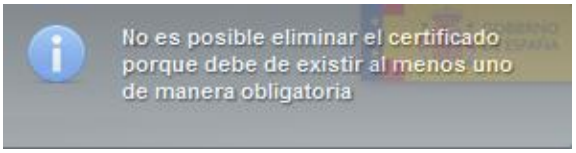


Figura 31 - Notificación imposible eliminar certificado PSC.

5.3.1.10 Archivar Certificado / Deshabilitar el archivado del Certificado (PSC)

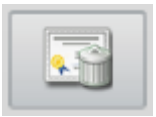


Pulsando en este icono indicamos a la plataforma que pase el estado del certificado seleccionado a archivado.



Con la siguiente opción deshabilitamos el estado de archivado del certificado, pasando su estado a uso normal.

5.3.1.11 Eliminar Certificado de Ejemplo (Tipo de Certificado)



Esta opción permite eliminar el Certificado de ejemplo asociado al Tipo de Certificado seleccionado. Estará disponible si el Tipo de Certificado posee certificado de ejemplo.

Una vez pulsada la opción de eliminar, aparecerá una ventana de confirmación de la operación a realizar.

5.3.1.12 Modificar Discriminador (Tipo de Certificado)

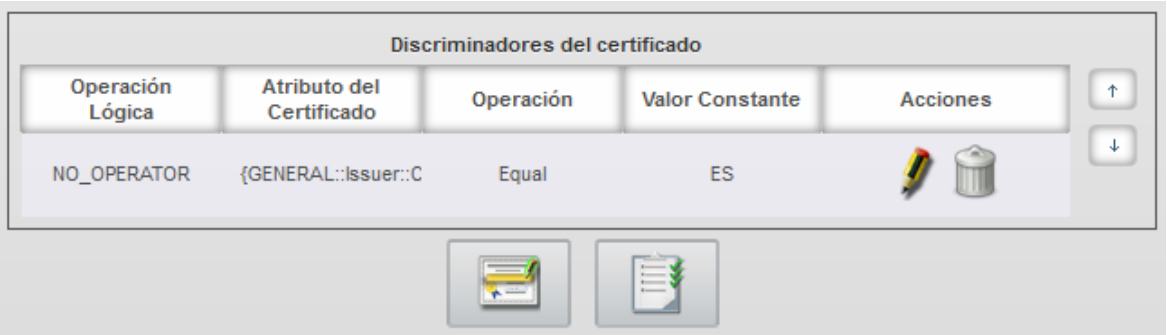


Figura 32 - Panel discriminadores.

 Tras pulsar la opción de modificación de discriminador aparecerá una nueva ventana con el discriminador definido por el administrador en el proceso de alta del Tipo de Certificado. A través de este panel el administrador podrá modificar tanto el OID o pseudocódigo, como el valor final sobre el que comparar el resultado del OID o ejecutar el pseudocódigo.



Figura 33 - Panel consulta / modificación Discriminador.

 Podemos eliminar un discriminador pulsando en la opción “Eliminar” del mismo.

 También podemos organizar los discriminadores del certificado para que sean evaluados por ese orden de prioridad. Para moverlos en la lista debemos hacer usar las flechas  que se encuentran en el lado derecho.

Una vez modificado todos los cambios, pulsamos sobre el botón “Guardar el orden de los discriminadores” para persistir los cambios.

5.3.1.13 Crear nuevo Discriminador (Tipo de Certificado)

 Podemos crear un nuevo discriminador pulsando sobre el botón “Añadir discriminador del tipo de certificado”. Se nos abrirá una nueva ventana donde podremos introducir los valores.



Figura 34 – Interfaz de gestión de Método de Validación

5.3.2 Gestión de Métodos de Validación

Los métodos de validación definirán cómo se llevará a cabo la obtención del estado de revocación de los certificados soportados por la plataforma, desde los certificados de prestador, hasta los certificados finales.

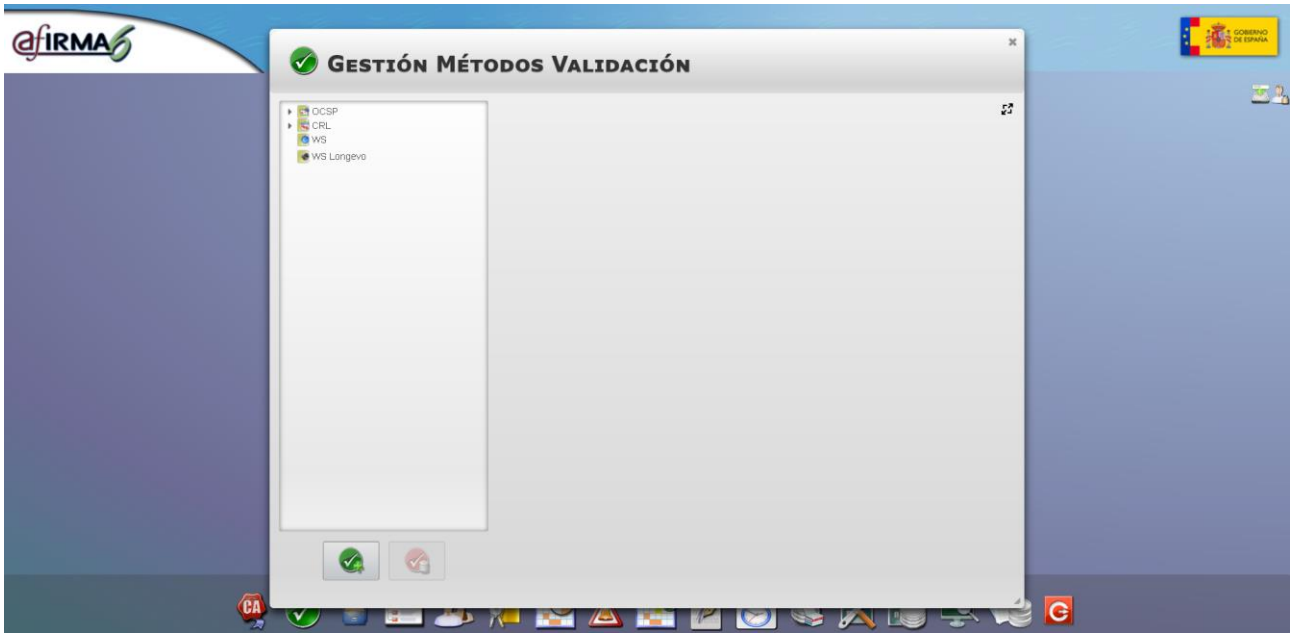


Figura 35 – Interfaz de gestión de Método de Validación

Los métodos de validación se dan de alta en la plataforma de manera independiente a los prestadores, pudiendo ser asignados a ellos posteriormente a través de las políticas de validación, definiendo también la prioridad en que serán utilizados. Esto permite utilizar un mismo método de validación para diferentes prestadores sin necesidad de duplicar la información.

Los métodos se agrupan dependiendo del protocolo utilizado para realizar la consulta, distinguiéndose así los siguientes: ***OCSP*** (*HTTP*), ***CRL*** (*HTTP, FTP, LDAP directo y segmentado*), ***SOAP*** (*HTTP y HTTPS*) y ***Validación Histórica/Longeva*** (*HTTPS con autenticación mutua*).

5.3.2.1 Alta de Métodos de Validación



El alta de un método de validación se realiza a través del botón definido para tal fin situado en la parte inferior del árbol de Métodos de Validación. Una vez pulsado, aparecerá una ventana en la que seleccionaremos el tipo de alta que queremos realizar: ***OCSP, CRL, SOAP y/o Validación Histórica/Longeva.***



Figura 36 – Interfaz de gestión de Método de Validación

Tras seleccionar el método a añadir se mostrará el panel de alta del método de validación seleccionado.

5.3.2.1.1 Alta Método de Validación OCSP.



Para dar de alta un método de validación de tipo OCSP, hay que pulsar el botón ***"Alta Método OCSP"***, el cual mostrará el panel con el formulario de alta de un método de validación OCSP.



Figura 37 – Panel Alta OCSP

El panel presenta los siguientes campos:

- **Identificador**: Identificador único en el sistema asignado al método de verificación.
- **Intervalo permitido**. Define en segundos el tiempo máximo aceptable entre la firma de la respuesta OCSP por parte del servidor OCSP, y la fecha de recepción del mensaje en la plataforma. La plataforma rechazará las respuestas que no se ajusten a dicho tiempo.
- **Usar *DistributionPoint***: habitualmente los certificados X.509 v3 suelen incluir unas extensiones donde se especifica una o varias URLs de acceso para la consulta de estado del propio certificado. Si se activa esta casilla la plataforma utilizará siempre como primer punto

de acceso la información contenida en el certificado y sólo en caso de no poder acceder a dicho origen se utilizaría el especificado en el método (si se ha definido uno).

- **En caso de error obteniendo las evidencias de revocación, lanzar alarma:** Check que, en caso de estar activado, lanzará una alarma si se produce un error obteniendo las evidencias de revocación de un certificado al usar este método de validación.

- **URL Servidor**: URL de acceso al recurso para la consulta de estado del certificado.

- **Este método de validación será incluido en las exportaciones de políticas de certificación**: Check que indica si esté método se incluirá o no en el fichero de exportaciones generado desde la plataforma.

- ***Timeout* conexión**: timeout en milisegundos definido para el establecimiento de conexión con la URL de destino.

- ***Timeout* lectura**: timeout en milisegundos definido para la lectura del recurso (CRL) o bien la respuesta del servidor (OCSP).

- **Firmar peticiones**: Indica si se firman las peticiones OCSP que envía la plataforma.

- **Usar también con DP**: Check que indica si se deben firmar las peticiones cuando se ataque a una URL extraída de alguno de los puntos de distribución del certificado a validar. Esta casilla tan solo se habilita en caso de tener marcada la de usar los puntos de distribución, y la de firmar la petición.

- **Certificados para firma OCSP**: Se seleccionará el certificado con el cual se firmarán las peticiones OCSP. Los certificados disponibles para esta operación deben haber sido dados de alta previamente en el keystore "*KeystoreClienteOCSP*" (véase la gestión de keystores).

- **Algoritmo de Firma:** Algoritmo usado para firmar las peticiones.

- **Identificador de la aplicación**: En el caso de que *RequestorName* sea obligatorio o bien que las peticiones deban ir firmadas, se debe especificar el identificador de cliente OCSP. Este identificador será acordado con el PSC correspondiente.

- **Tipo para el Requestor Name**: Desplegable que permite escoger el formato del tipo del Requestor Name a incluir en la petición OCSP. Se permite escoger entre los siguientes posibles formatos: *rfc822Name*, *dNSName*, *directoryName*, *uniformResourceIdentifier*, *iPAddress* y *registeredID*.

5.3.2.1.2 Alta Método de Validación CRL



Para dar de alta un método de validación de tipo CRL, hay que pulsar el botón ***"Alta Método CRL"***, el cual mostrará el panel con el formulario de alta de un método de validación CRL.

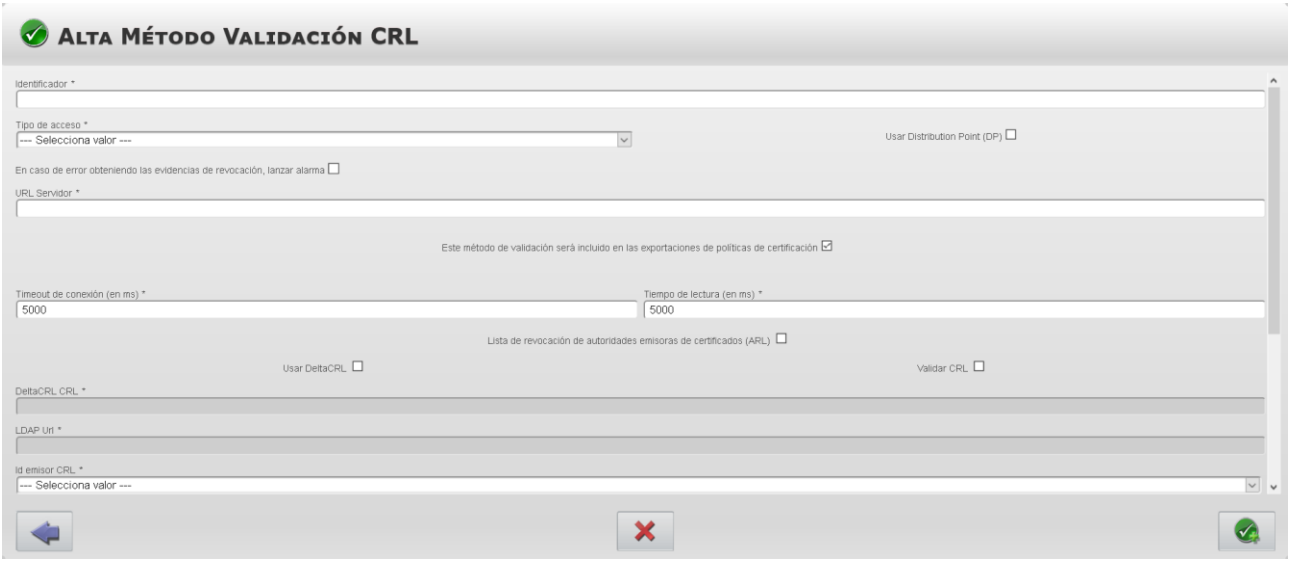


Figura 38 – Panel Alta CRL (I)

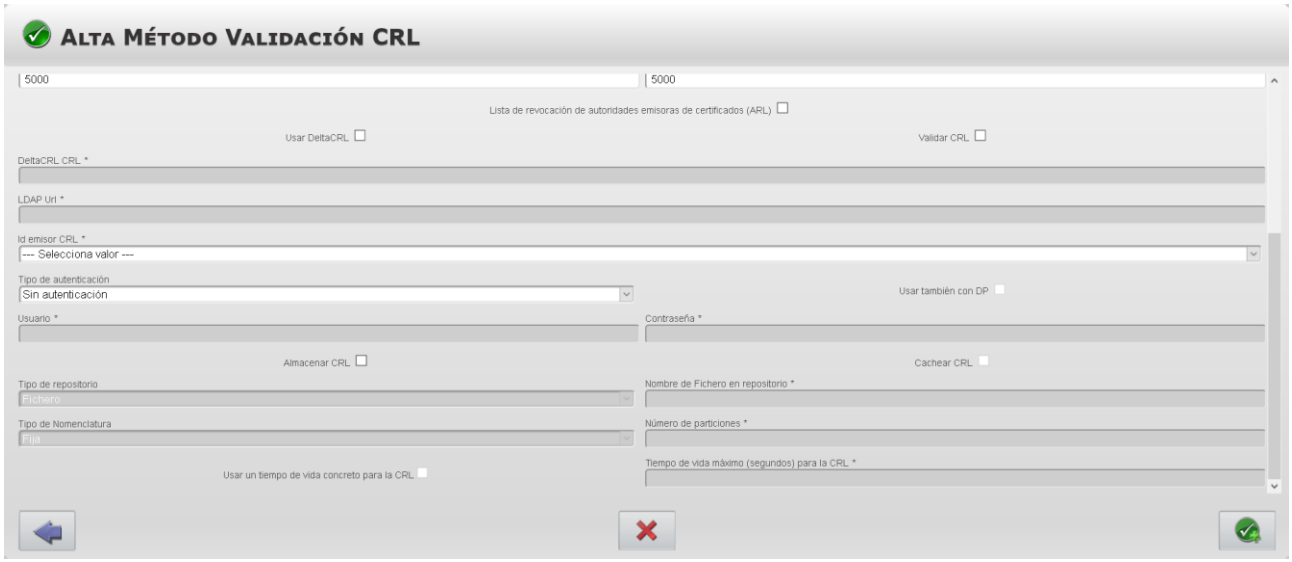


Figura 39 – Panel Alta CRL (II)

El panel presenta los siguientes campos:

- **Identificador**: Identificador único en el sistema asignado al método de verificación.
- **Tipo acceso**. Se identificará el protocolo que se va a utilizar para acceder al origen de la información de estado. Los tipos disponibles son: ***http, ftp, ldap directo***, ***ldap segmentado y HTTP Secuencial***:
    - **HTTP:** Representa un acceso directo al recurso mediante una URL que sigue el protocolo HTTP/S.
    - **FTP:** Representa un acceso directo al recurso mediante una URL que sigue el protocolo FTP.
    - **LDAP Directo:** Representa un acceso directo al recurso mediante una URL que sigue el protocolo LDAP.
    - **LDAP Segmentado:** Tipo de acceso exclusivo para el uso con los tipos de certificados de persona física de la FNMT (CA – Clase2CA), ya que la ruta dentro del LDAP se extrae de una forma particular de la información contenida en el punto de distribución del propio certificado a validar.
    - **HTTP Secuencial:** Tipo de acceso que construye la URL de destino del recurso a obtener uniendo lo definido en el campo "URL Servidor" (que debe definir la ruta

hasta el contexto), junto con el nombre del recurso, el cual se extrae de la información contenida en el punto de distribución del certificado, ya sea de una ruta HTTP o del CN de la ruta LDAP.

- **Usar Distribution Point**: habitualmente los certificados X.509 v3 suelen incluir unas extensiones donde se especifica una o varias URIs de acceso para la consulta de estado del propio certificado. Si se activa esta casilla la plataforma utilizará siempre como primer punto de acceso la información contenida en el certificado y sólo en caso de no poder acceder a dicho origen se utilizaría el especificado en el método (si se ha definido uno).

- **En caso de error obteniendo las evidencias de revocación, lanzar alarma:** Check que, en caso de estar activado, lanzará una alarma si se produce un error obteniendo las evidencias de revocación de un certificado al usar este método de validación.

- **URL Servidor**: URL de acceso al recurso para la consulta de estado del certificado.

- **Este método de validación será incluido en las exportaciones de políticas de certificación**: Check que indica si esté método se incluirá o no en el fichero de exportaciones generado desde la plataforma.

- **Timeout conexión**: timeout en milisegundos definido para el establecimiento de conexión con la URL de destino.

- **Timeout lectura**: timeout en milisegundos definido para la lectura del recurso (CRL) o bien la respuesta del servidor (OCSP).

- **Lista de revocación de autoridades emisoras de certificados (ARL).** Al habilitar esta opción (se trata de un checkbox) indicamos que el método de validación se utilizará para acceder a una ARL, y no a una CRL. Aquellos métodos de validación tipo CRL que tengan activa esta opción, tan solo se tendrán en cuenta cuando el certificado a validar se corresponda al de un prestador dado de alta en la configuración, en caso contrario, será ignorado.

- **Usar Delta-CRL.** Con este checkbox se puede indicar que se pretende realizar una configuración de acceso a CRLs mediante Delta-CRLs. Si marcamos esta opción se habilita automáticamente el campo donde se debe indicar la ruta absoluta hacia la Delta-CRL. La Base-CRL será la indicada en el campo anterior.

- **Validar CRL**. Indica a la plataforma si se debe validar la CRL cada vez que vaya a ser consultada para obtener el estado de un certificado. Esta opción se debe deshabilitar únicamente si la CRL a consultar se va a almacenar en la caché de segundo nivel y se desea que no se verifique cada vez que se vaya a consultar (el proceso de verificación sí se llevará a cabo siempre en el momento de la descarga).

- **Ruta Delta-CRL.** En caso de tratarse de un protocolo de acceso por CRLs y que además se utilicen en combinación las Base-CRLs con las Delta-CRLs, este es el campo donde se debe indicar la ruta hacia las segundas.

- **Ruta LDAP**. En caso de tratarse de un protocolo de acceso por LDAP, se indicará la ruta dentro del mismo donde se encuentra la CRL (por ejemplo: cn=*,cn=ARC DNIE 001,OU=DNIE,o=Direccion General de la Policia,c=ES). Siempre se introducirá la ruta LDAP especificando el acceso desde el nodo hoja hasta la raíz del árbol.

- **Id. Emisor CRL**: se especificará el identificador del certificado que emite la CRL. El emisor de la CRL debe encontrarse registrado en el Keystore de certificados de confianza para CRL correspondiente (consultar la gestión de Keystores). En caso contrario, la plataforma rechazará la CRL durante el proceso de validación de la misma.

- **Tipo Autenticación**: especifica el tipo de autenticación que requiere el acceso al origen de la información. Los métodos disponibles actualmente son: sin autenticación o bien mediante credenciales de tipo Usuario/Password.

- **Usar también con DP:** Check que indica que la autenticación establecida debe usarse también cuando la ruta de destino se haya obtenido de alguno de los puntos de distribución del certificado a validar. Esta casilla tan solo está habilitada cuando se ha indicado el uso de los puntos de distribución y la autenticación está establecida.

- **Usuario**: identificador del usuario en caso de especificarse el tipo de autenticación Usuario/Password.

- **Contraseña**: Contraseña necesaria para la autenticación de la petición.

- **Almacenar CRL:** indica si la CRL especificada por el método de validación debe ser almacenada en la caché de segundo nivel con el fin de optimizar los procesos de validación.

- **Cachear CRL:** indica si la CRL especificada por el método de validación debe ser almacenada en una caché intermedia por encima de la base de datos con el fin de optimizar los tiempos de acceso en aquellas CRLs de gran tamaño. Esta casilla tan solo se podrá activar si también está activada la de almacenar CRL.

- **Tipo de repositorio:** indica si la CRL debe ser almacenada en la plataforma como un fichero, o bien en la Base de Datos de CRL.

- **Nombre fichero repositorio:** especifica el nombre con el que será almacenada la CRL.

- **Tipo Nomenclatura:** puede ser Fija, el nombre de la CRL será el especificado en el campo anterior, o bien Secuencial, en cuyo caso el nombre de la CRL se conformará mediante un prefijo y un número secuencial en base al formato definido en el campo anterior (este formato tiene un tipo de nomenclatura especial). Este último tipo se utiliza para los accesos a CRL particionadas como por ejemplo las del DNI electrónico y únicamente podrá ser utilizado para la obtención de CRL por las tareas de descarga que conforman la caché de nivel 2. (En el Anexo I se muestra un ejemplo práctico)

  Cuando el tipo de nomenclatura es Secuencial, el formato del campo *Nombre fichero repositorio* debe contener una cadena literal, y dos caracteres especiales:

  - **'*'** las ocurrencias de este carácter serán sustituidas en tiempo de descarga de la CRL por un número generado de forma secuencial desde 0 hasta N-1, siendo N el número de particiones que conforman la CRL y que se define a continuación.

  - **'?'** las ocurrencias de este carácter serán sustituidas en tiempo de descarga de la CRL por un literal que debe haber sido definido en la tarea de que se encarga de la descarga periódica de la CRL. Este literal se denomina identificador de partición (para más información ir a la gestión de tareas de descarga de CRL o caché de segundo nivel).

    Un ejemplo de CRL particionada sería el siguiente:

    A6B4D3EEDDFF-55.crl

    donde:

A6B4D3EEDDFF es un identificador de partición.

55 es el número de partición.

Por tanto, para definir este identificador de CRL, debería utilizarse la expresión:

?-*.crl

- **Número Particiones:** en caso de especificar un tipo de nomenclatura secuencial, se debe especificar el número de particiones de las que constará la CRL. El sistema descargará una por una las CRL desde 0 hasta N-1

- El check **"Usar un tiempo de vida concreto para la CRL"** activará el campo "Tiempo de vida máximo para la CRL", con lo que podremos definir el valor concreto para dicho campo.

- **Tiempo de vida máximo (segundos) para la CRL:** aquí definimos el tiempo de validez máximo que se considerará para la CRL, a pesar que en su definición este tiempo sea mayor.

5.3.2.1.3 Alta Método de Validación WS



Para dar de alta un método de validación de tipo WS, hay que pulsar el botón ***"Alta Método Validación WebService"***, el cual mostrará el panel con el formulario de alta de un método de validación WS.



Figura 40 – Panel alta WS.

El panel presenta los siguientes campos:

- **Identificador**: Identificador único en el sistema asignado al método de verificación.
- **Tipo acceso**. Se identificará el protocolo que se va a utilizar para acceder al origen de la información de estado. Los tipos disponibles son: ***http, https***.
- **Tipo de WS:** Permite elegir el tipo de web service, nativo o DSS.

- **En caso de error obteniendo las evidencias de revocación, lanzar alarma:** Check que, en caso de estar activado, lanzará una alarma si se produce un error obteniendo las evidencias de revocación de un certificado al usar este método de validación.

- **URL Servidor**: URL de acceso al recurso para la consulta de estado del certificado.

- **Este método de validación será incluido en las exportaciones de políticas de certificación**: Check que indica si esté método se incluirá o no en el fichero de exportaciones generado desde la plataforma.

- **Timeout conexión**: límite en milisegundos definido para el establecimiento de conexión con la URL de destino.

- **Timeout lectura**: límite en milisegundos definido para la lectura del recurso o bien la respuesta del servidor.

- **Tipo de Acceso.** Especifica si para el acceso hará falta o no autenticación o la autenticación se realizará mediante certificado.

- **Id. Aplicación.** Especificará el identificador de la aplicación (incluyendo su unidad organizativa en caso de existir) que será utilizado en las consultas para obtener el estado de los certificados. El identificador especificado deberá encontrarse dado de alta por tanto en la plataforma que va a ser objeto de la consulta.

- **Autorización de Servicios Web.** En caso de se requiera securización de los mensajes SOAP enviados a la plataforma de destino (la securización a utilizar es configurada por dicha plataforma a nivel de aplicación) se deberá especificar el par Usuario/Password si la securización es por credenciales Usuario/Password, o bien seleccionar el certificado de la lista existente en caso de autenticación por certificado.

5.3.2.1.4 Alta Método de Validación WS Longevo



Para dar de alta un método de validación de tipo WS Longevo, hay que pulsar el botón ***"Alta Método Validación WebService Longevo"***, el cual mostrará el panel con el formulario de alta de un método de validación WS Longevo.



Figura 41 – Panel alta WS Longevo

El panel presenta los siguientes campos:

- **Identificador**: Identificador único en el sistema asignado al método de verificación.
- **En caso de error obteniendo las evidencias de revocación, lanzar alarma:** Check que, en caso de estar activado, lanzará una alarma si se produce un error obteniendo las evidencias de revocación de un certificado al usar este método de validación.
- **URL Servidor**: URL de acceso al recurso para la consulta de estado del certificado.
- **Este método de validación será incluido en las exportaciones de políticas de certificación**: Check que indica si esté método se incluirá o no en el fichero de exportaciones generado desde la plataforma.
- **Timeout conexión**: límite en milisegundos definido para el establecimiento de conexión con la URL de destino.
- **Timeout lectura**: límite en milisegundos definido para la lectura del recurso o bien la respuesta del servidor.

- **Usar solo con certificados caducados**. Mediante este checkbox, se puede restringir el uso de este método de validación que se está dando de alta, para poder aplicarse tan solo a los certificados ya caducados (principal objetivo del protocolo de validación longeva).

- **Certificado Cliente SSL.** Desplegable a través del cual se permite seleccionar el certificado deseado para realizar la identificación SSL, es decir, el certificado cliente en la autenticación mutua (los certificados que aquí aparezcan deben ser incluidos previamente en el almacén "KeyStore Cliente SSL").

5.3.2.2 Modificación de un Método de Validación



Para modificar cualquier parámetro especificado en un método de validación es necesario seleccionar en el árbol de métodos, ubicado en la parte izquierda de la pantalla de gestión, el método de validación que se quiere modificar. En la parte derecha de la pantalla se mostrará toda la información disponible de dicho método.

Como podemos ver, en la edición nos aparece una lista para definir las cabeceras específicas para HTTP/S. Por defecto, al crear un nuevo método de validación, se generarán dos cabeceras: "Accept-Encoding" y "User-Agent", esta última con valor "Apache-HttpClient". Desde aquí podremos modificarlas o borrarlas según nos convenga, así como dar de alta nuevas cabeceras para el método de validación seleccionado.

Para modificar la información simplemente especifique los nuevos valores y pulse el botón "Modificar".

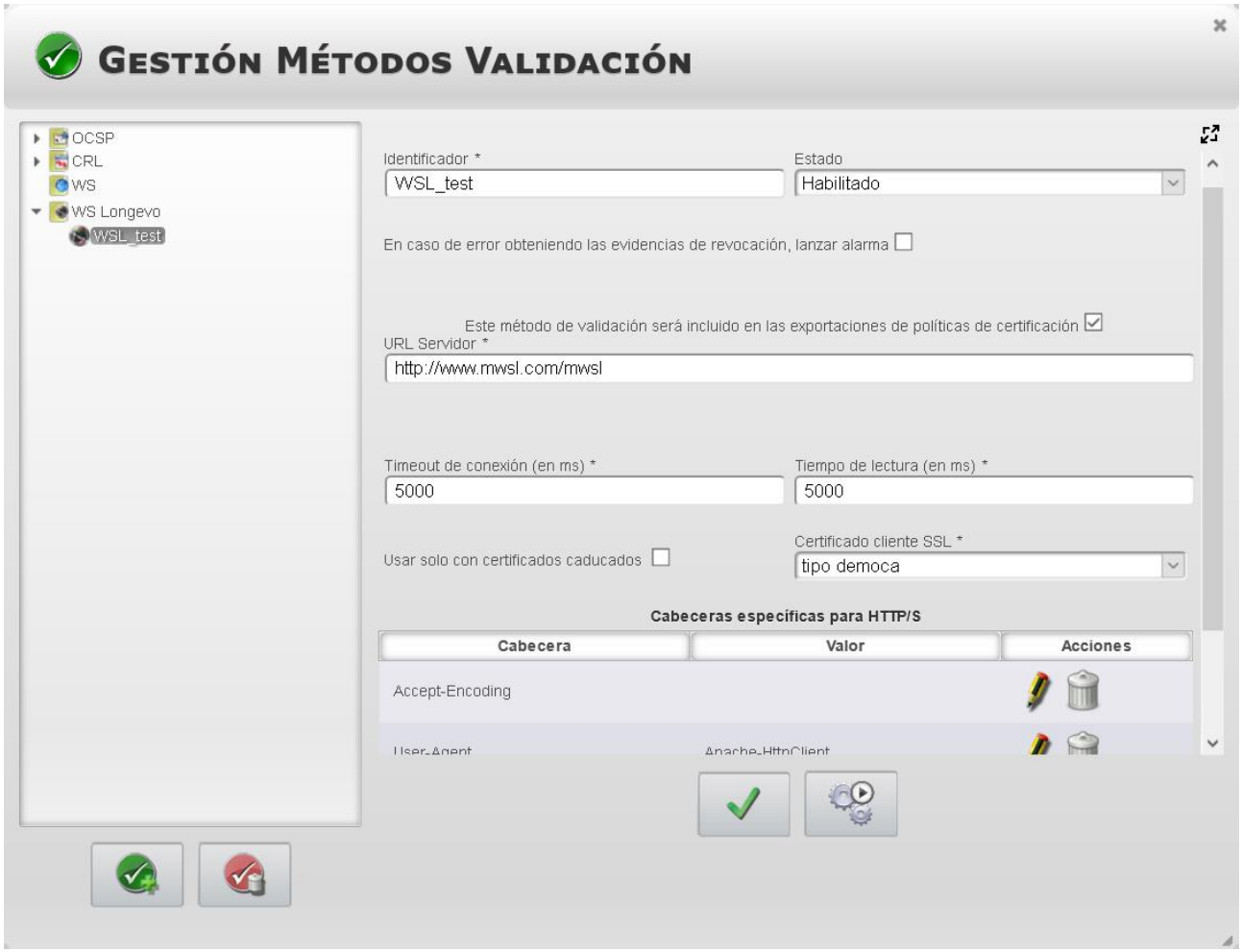


Figura 42 – Modificación método de validación

5.3.2.3 Baja de Métodos de Validación



Para eliminar un método de validación, deberá seleccionarlo mediante el árbol de métodos de validación. En la pantalla de consulta de datos que aparece en la parte derecha, pulse sobre el botón "Eliminar", posteriormente se le pedirá confirmación para realizar la operación. Una vez confirmada, el sistema procederá a dar de baja al método de validación seleccionado.

5.3.2.4 Test de Métodos de Validación



Para comprobar el funcionamiento de un método de validación, tan solo hay que pulsar sobre el botón "Test" situado en la parte inferior de la pantalla en la que se muestran los datos del método de validación. Esto provocará que se abra una pantalla de diálogo

en la que se solicitará que se seleccione un certificado para utilizarlo para la ejecución del test:



Figura 43 – Pantalla de diálogo de solicitud de un certificado para el Test

Tras seleccionar el certificado y continuar, la plataforma ejecutará el método de validación utilizando el certificado seleccionado. La conclusión del resultado de la prueba se mostrará en un mensaje. Para obtener una mayor información del proceso realizado, hay que consultar el log del sistema.

5.3.3 Gestión de Políticas de Certificación

Una política de validación o certificación especifica un conjunto de prestadores y tipos de certificados que van a conformar un ámbito de confianza. Además, las políticas permiten especificar de manera concreta cómo se va a llevar a cabo la validación de los certificados admitidos por dicha política (métodos de validación), la información que se debe extraer de los certificados (certificado patrón), y la manera de obtenerla (configuración de mapeos).

Cada una de las aplicaciones dadas de alta en la plataforma, tendrá asociada una política de validación que determinará los tipos de certificados que soportará, así como el modo en que se llevará a cabo la validación.

Cada política define la información genérica que se va a extraer de los certificados por medio de una estructura de información denominada *Certificado Patrón,* que no es más que un conjunto de campos lógicos que poseen asociados identificadores únicos.

Posteriormente, en la definición de los mapeos se especificará cómo se debe extraer cada campo lógico para cada tipo de certificado concreto.

El certificado patrón permite representar cualquier certificado X.509 v3 de manera homogénea por medio de una estructura de tipo Campo / Valor, lo que permite a las aplicaciones abstraerse de la tipología y estructura de los certificados.

Las políticas tienen asociadas una versión de política que permite conocer si se han realizado modificaciones sobre ella. Cada vez que se realiza una modificación sobre el certificado patrón la versión de la política aumenta.



Figura 44 – Módulo gestión de Políticas de Certificación

5.3.3.1 Alta de una Política de Certificación



Para realizar el alta de una política, se debe pulsar el botón “Alta Política” ubicado en la parte inferior del árbol de políticas situado en la parte izquierda de la pantalla. Tras ello se mostrará la pantalla de alta.



Figura 45 – Pantalla de alta de política de validación

Los campos a especificar son:

- **Identificador**. Identificador único en el sistema de la política a crear.
- **Descripción**. Descripción breve de la política.
- **Basada en la política**. Permite crear un duplicado de una política ya existente. Esta opción es muy útil si la política a crear es muy similar a otra ya registrada.

Tras pulsar el botón “Dar de Alta”, la política será registrada en el sistema.

5.3.3.2 Creación Campos Lógicos



Tras crear una política, el siguiente paso será definir los campos lógicos asociados a ella (o proceder a modificarlo en caso de haber creado la política a partir de otra ya existente). Para ello, se seleccionará pulsará el botón “Crear Campo Lógico”.

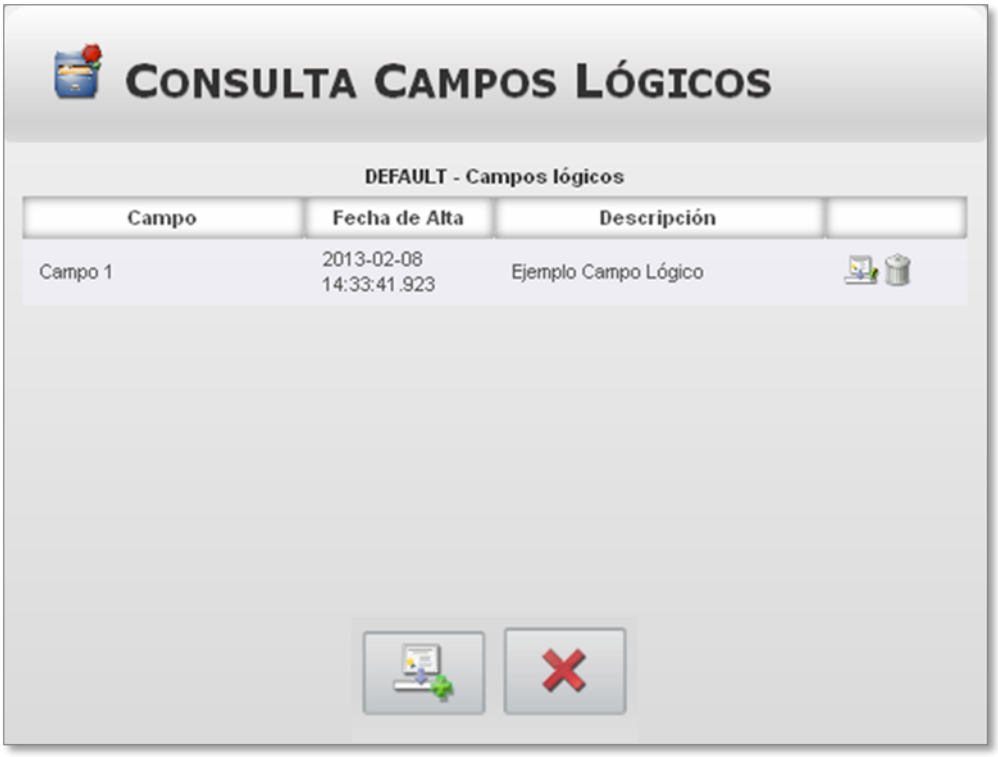


Figura 46 – Panel Consulta Campos lógicos



Los campos del certificado patrón se darán de alta uno a uno por medio del botón "Crear campo lógico". En la pantalla de alta del campo lógico se deberá especificar el identificador único del campo lógico, así como una descripción detallada de la información que albergará.

En caso de que queramos replicar los cambios en las otras políticas, seleccionaremos la opción "*Replicar los cambios en el resto de las políticas.*".

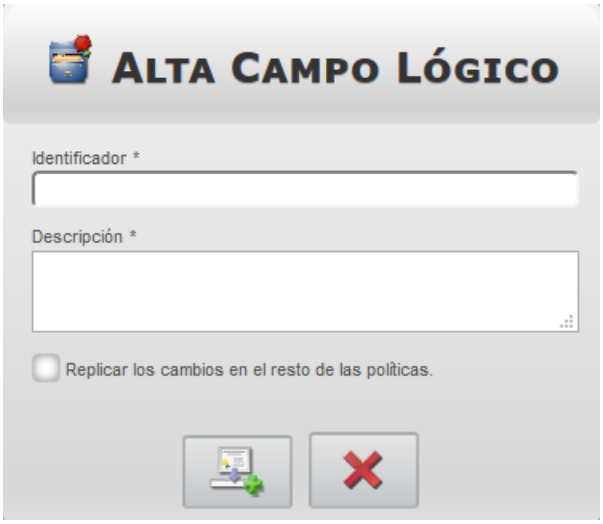


Figura 47 – Panel alta campo lógico



Una vez dado de alta el campo lógico, se mostrará en la parte derecha de la pantalla junto con todos sus datos y dos botones, que permitirán editar la información del mismo o eliminarlo de la configuración.

5.3.3.3 Asignación de tipos de certificados a una política



Una vez definidos los campos lógicos que se podrán mapear a campos del certificado, se procederá a asignar a la política los tipos de certificados que va a admitir. Para ello, se seleccionará la política en el árbol de políticas y en la pantalla derecha aparecerá la información general de la misma. En la parte inferior de dicha pantalla se debe pulsar el botón "Añadir PSC / Tipo Certificado" que desplegará una pantalla como la siguiente, donde aparecerán de manera jerárquica todos los **prestadores** que emiten tipos de certificados.



Figura 48 – Alta de tipo de certificado en política

Seleccionaremos del árbol los tipos de certificado que deseamos añadir a la política y pulsaremos el botón "Añadir PSC / Tipo de Certificado".

En caso de que queramos restringir el certificado en todas las aplicaciones que usen la política sobre la que añadir el tipo de certificado, seleccionaremos la opción "*Restringir Certificado en todas las aplicaciones*". Si quisiéramos añadir los tipos de certificados a todas de políticas, seleccionaremos la opción "Replicar los cambios en el resto de las políticas".

5.3.3.4 Configuración de los Métodos de Validación por Prestador

Tras el registro de los tipos de certificados en la política, se deberán definir qué métodos de validación van a ser usados por cada prestador, así como la prioridad asignada a cada uno para comprobar el estado de los certificados emitidos por él.

Los métodos de validación se asignarán de manera jerárquica, esto es, una configuración de métodos asignada a un determinado prestador define cómo se va a realizar la consulta de estado para todos

los certificados que se encuentran bajo su jerarquía, siempre y cuando sus nodos intermedios no redefinan dicha política, en cuyo caso se aplicará la misma filosofía.

Por ejemplo, dada la siguiente jerarquía:



Figura 49 – Jerarquía de certificación

Se puede asignar el método de validación *A* a la CA *AfirmaCA,* y el método *B* a la CA *AfirmaSubCA*. De este modo, al validar cualquiera de los tipos de certificados (firma o identidad) emitidos por la CA *AfirmaSubCA*, se utilizará el método *B*, mientras que, para validar la CA propiamente dicha, se utilizará el método *A*.

Por tanto, por regla general siempre se obtendrán los métodos de validación configurados para el emisor del certificado a validar.

Para realizar la asignación de métodos a un determinado prestador, debe seleccionarse del árbol de políticas ubicado a la izquierda de la pantalla, tras lo cual aparecerá en la parte derecha la configuración de métodos. Con dos campos, el primero de ellos, situado a la izquierda contendrá todos los métodos de validación dados de alta en la plataforma. A continuación 4 botones que permitirán añadir los métodos de validación a aplicar sobre la CA (flecha derecha), eliminar (flecha izquierda) y cambiar el orden de aplicación de los métodos de validación a aplicar (flecha arriba y flecha abajo).

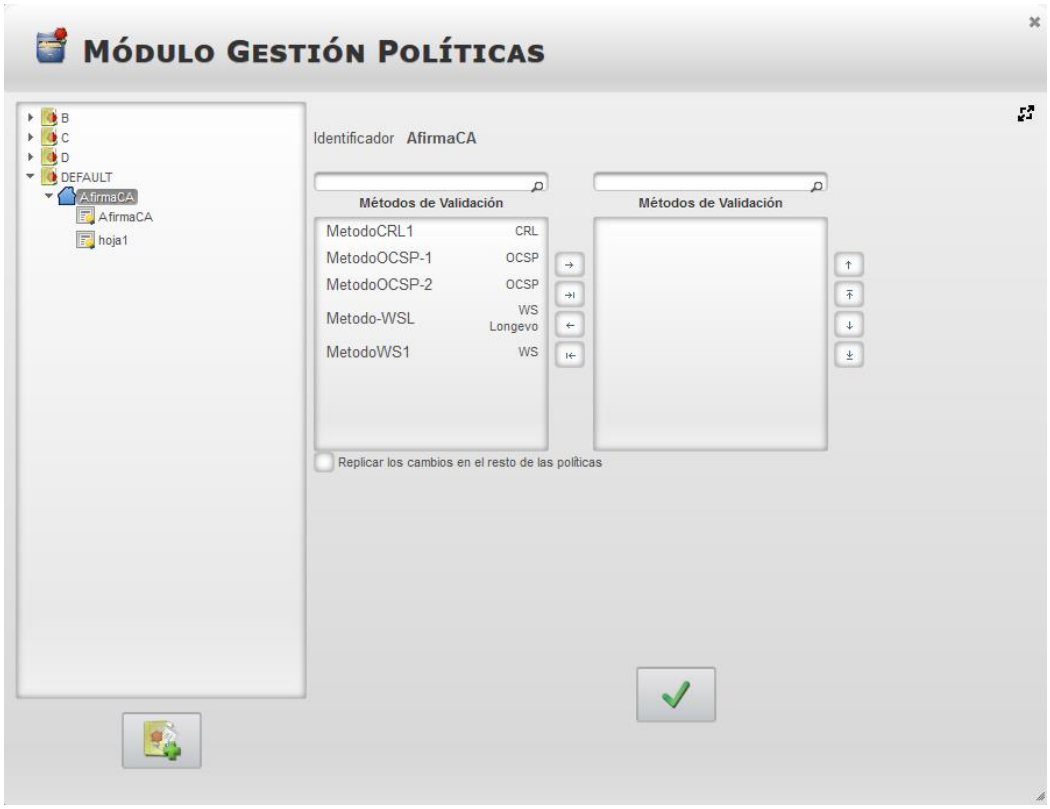


Figura 50 – Ventana de asignación de métodos de validación a un PSC (I)

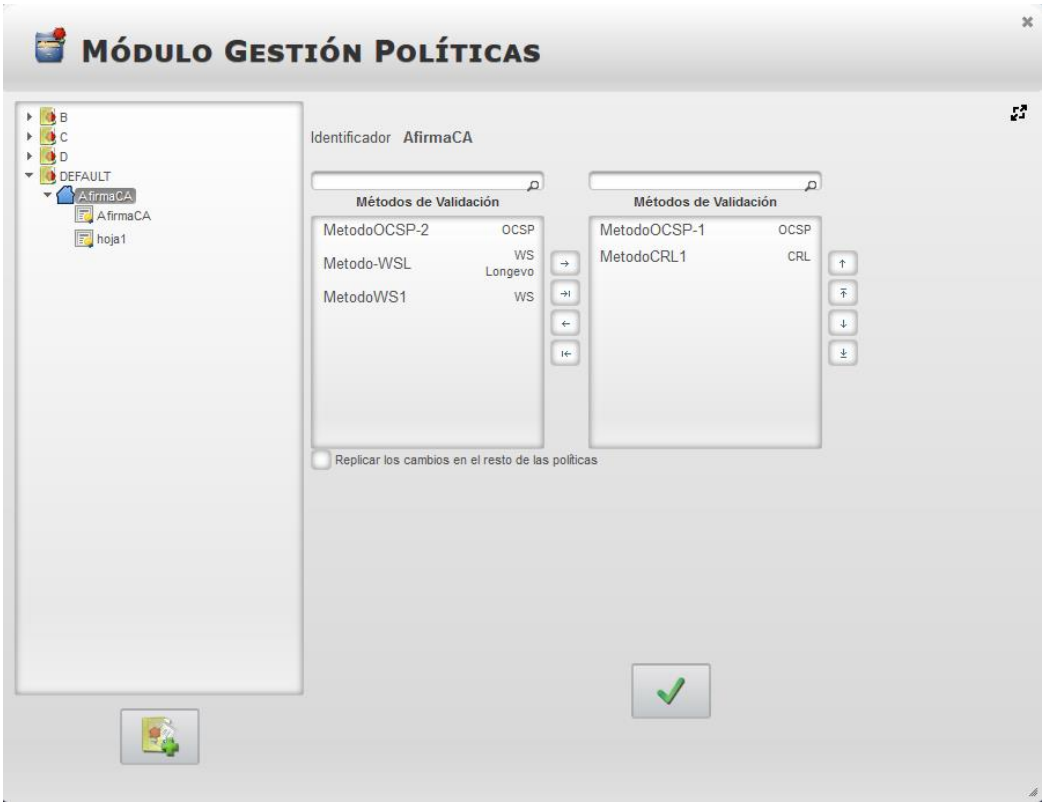


Figura 51 – Ventana de asignación de métodos de validación a un PSC (II)

El orden en que aparecen los métodos de validación en la lista será el orden en el que serán utilizados por la plataforma a la hora de consultar la información de un certificado, de manera que si no se puede obtener dicha información, se irá utilizando uno tras otro de forma secuencial. **Si quisiéramos que los cambios se apliquen a todas las políticas, seleccionaremos la opción "Replicar los cambios en el resto de las políticas".**

5.3.3.5 Definición de mapeos para tipos de certificados

El último paso para completar la configuración de la política es la definición de los mapeos por medio de los cuales se define cómo se extrae la información especificada por el certificado patrón para cada tipo de certificado definido en la política.

Para definir la configuración de mapeos, en la pantalla de gestión de políticas se debe seleccionar el tipo de certificado ubicado dentro de su jerarquía correspondiente en la política a modificar. En la parte derecha de la pantalla aparecerá la lista de campos lógicos definidos por el certificado patrón. A cada uno de estos campos lógicos puede asignársele un mapeo específico que determinará qué información va a contener, y cómo se extraerá del certificado correspondiente.



Figura 52 – Ventana de gestión de políticas. Definición de mapeos I

Cada campo lógico posee dos botones asociados mediante los cuales se podrá editar (o definir) el mapeo del campo, o bien eliminar la configuración del mapeo, lo que significa que no se extraerá información del certificado para completar dicho campo lógico.

5.3.3.5.1 Selección de mapeo de campo lógico

Tras pulsar el botón de edición de un mapeo, aparecerá la pantalla de selección de mapeos, donde en la parte izquierda se puede observar un árbol que agrupa toda la información existente en el certificado y mediante el cual se podrán seleccionar los campos que definirán la configuración del mapeo. En la parte derecha se muestra el nombre del campo lógico que estamos editando, el tipo de mapeo seleccionado y el tipo de dato. Dependiendo del tipo de asociación, los datos a especificar serán diferentes.

- **Auditar campo**. Mediante esta propiedad se establece si el campo lógico se va incluir en las trazas de auditoría del sistema y por tanto estarán accesible en las consultas del componente de Auditoría.

Los tipos de mapeos disponibles son los siguientes:

- **Libre**. Permite definir un literal constante para el campo lógico en cuestión. Un ejemplo de ello puede ser para definir el campo *tipo de certificado*, donde para cualquier certificado de un tipo determinado, el valor siempre va a ser el mismo.

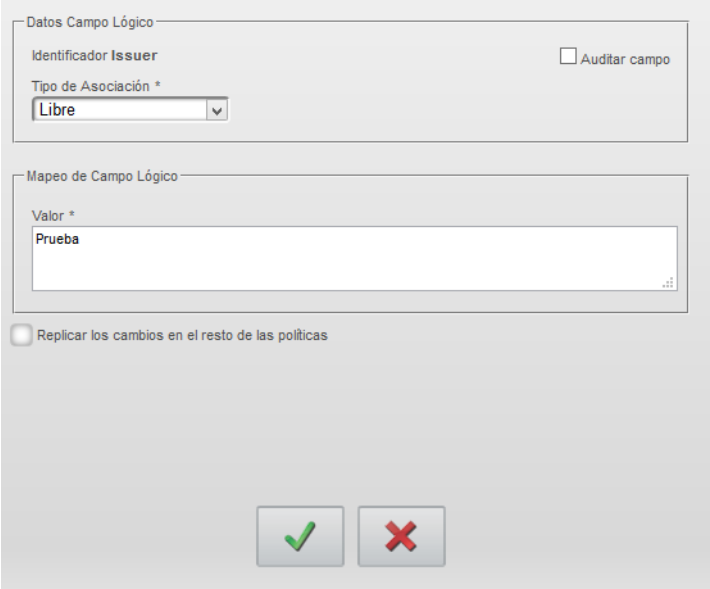


Figura 53 – Ventana de edición de mapeos. Mapeo Tipo Libre

- **Simple**. Permite asignar a un campo lógico el valor de un atributo específico del certificado. Dicho atributo se seleccionará haciendo clic sobre el campo deseado ubicado en el árbol de atributos de la parte izquierda de la pantalla, o bien estableciéndolo de forma manual (en caso de que el tipo de certificado no tenga asociado un certificado X509 de ejemplo). Su formato es:

  GENERAL || EXTENSION::NOMBRE_CAMPO[::NOMBRE_SUBCAMPO]

  Algunos ejemplos de rutas válidas:

  GENERAL::Subject::CommonName

  GENERAL::Issuer

  GENERAL::SerialNumber

  EXTENSION::CertificatePolicies::policyIdentifiers

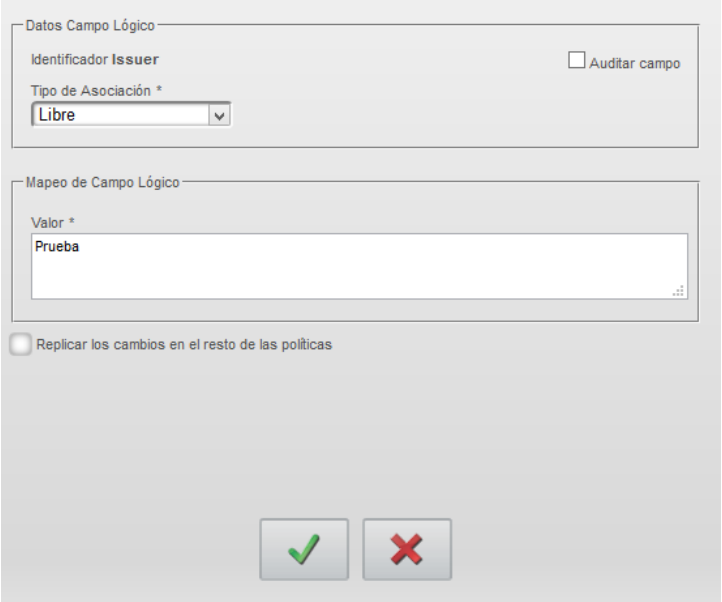


Figura 54 – Ventana de edición de mapeos. Mapeo Tipo Simple

Se debe definir también de forma obligatoria el "Tipo de dato" que se quiere definir, aunque en caso de no estar seguro se puede dejar marcado como "No definido" y la plataforma tratará de parsearlo automáticamente. Los diferentes tipos que podemos elegir son:

BOOLEAN	**IA5 STRING**	**UTF8 STRING**
INTEGER	**NUMERIC STRING**	**GENERALIZED TIME**
BIT STRING	**PRINTABLESTRING**	**VISIBLE STRING**
BMP STRING	**T61 STRING**	**UTC TIME**
GENERAL STRING	**UNI STRING**	

- **Compleja.** Permite extraer una subcadena del valor de un atributo del certificado por medio de la especificación de delimitadores. En primer lugar se debe seleccionar del árbol de atributos del certificado el campo donde se encuentra la información que queremos extraer. Una vez hecho esto, se mostrará en la parte derecha la ruta del campo así como su valor actual. El siguiente paso será especificar el delimitador, que puede estar conformado por uno o varios caracteres, y el número de token a obtener. Tras especificar toda esta información, si se pulsa el botón con refrescar/recargar, el sistema obtendrá el token especificado y lo mostrará en el campo "Resultado", pudiendo comprobar así si la configuración establecida es correcta o no.

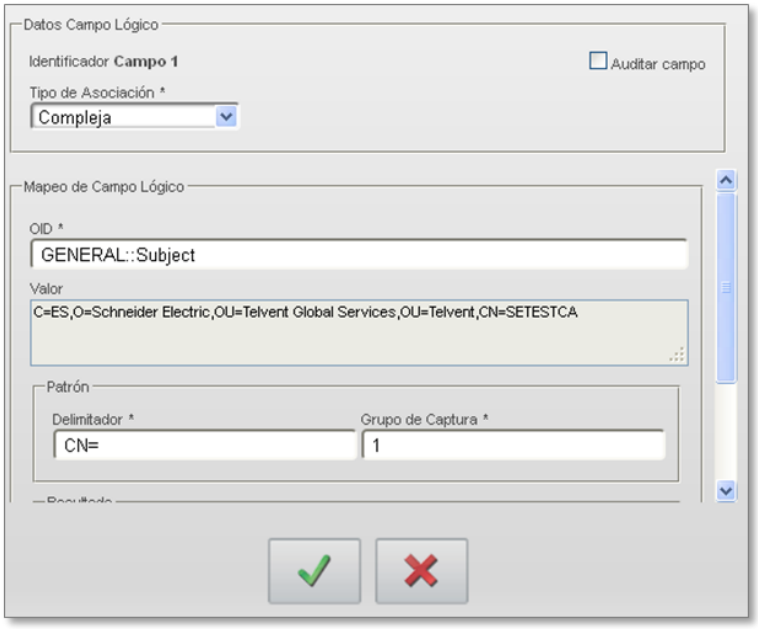


Figura 55 – Ventana de edición de mapeos. Mapeo tipo complejo, con delimitador "CN=" y selección del primer elemento.

El campo resultado permite calcular el resultado de aplicar el mapeo a realizar sobre el certificado de ejemplo.

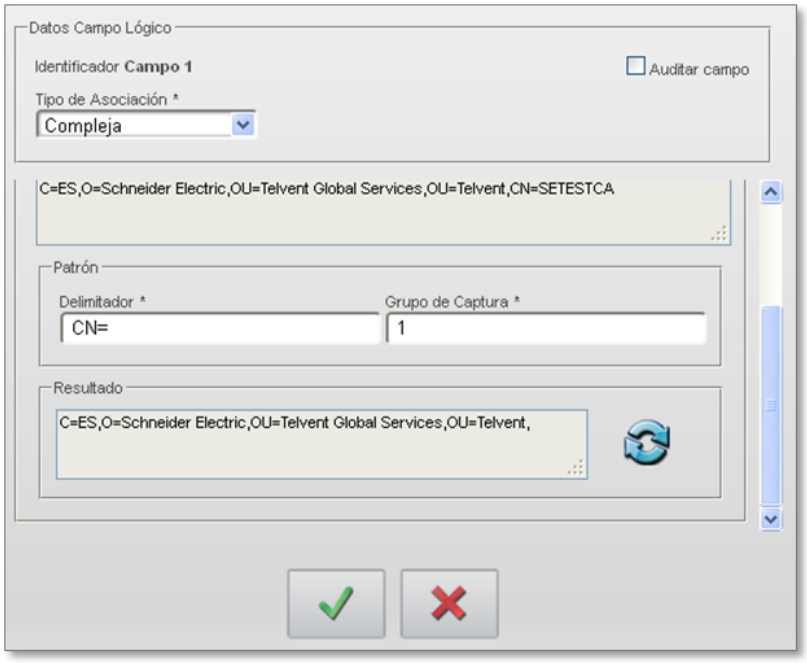


Figura 56 – Cálculo resultado asociación compleja.

- **Anagrama Fiscal.** El anagrama fiscal es una cadena de caracteres formada a partir del nombre, apellidos y NIF, que permite identificar unívocamente a una persona física. Para generar el anagrama fiscal, se debe especificar cada uno de los campos que lo conforman. Para ello, se selecciona del árbol de atributos del certificado y se arrastra hacia el campo correspondiente de la parte derecha de la pantalla. Una vez especificados todos los campos, si se pulsa sobre el botón refrescar/recargar, se generará el anagrama fiscal asociado a dichos datos.

  NOTA: Para rellenar los campos Nombre, Apellido 1, Apellido 2 y NIF el usuario debe seleccionar previamente el campo que desea rellenar y después el nodo del árbol que quiere asociar.

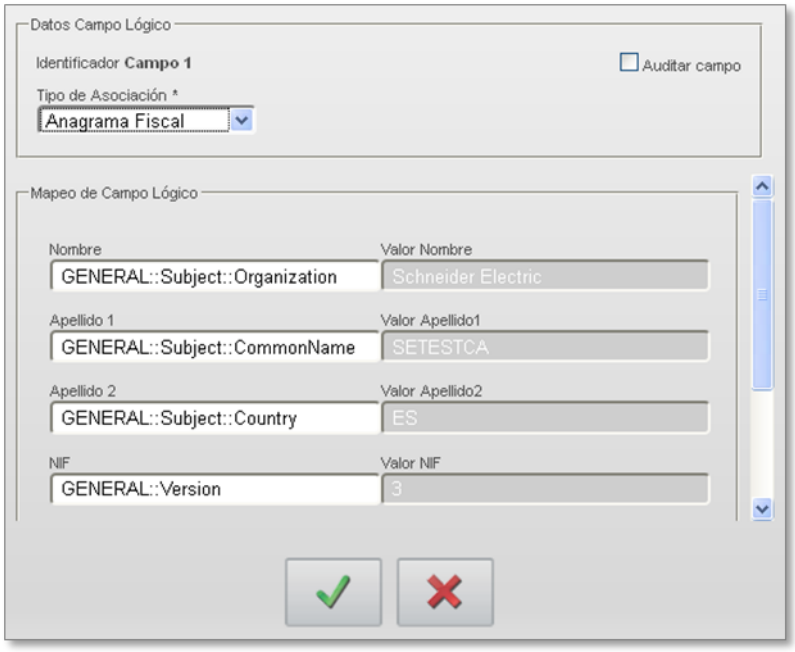


Figura 57 – Ventana de edición de mapeos. Mapeo tipo Anagrama Fiscal (I).

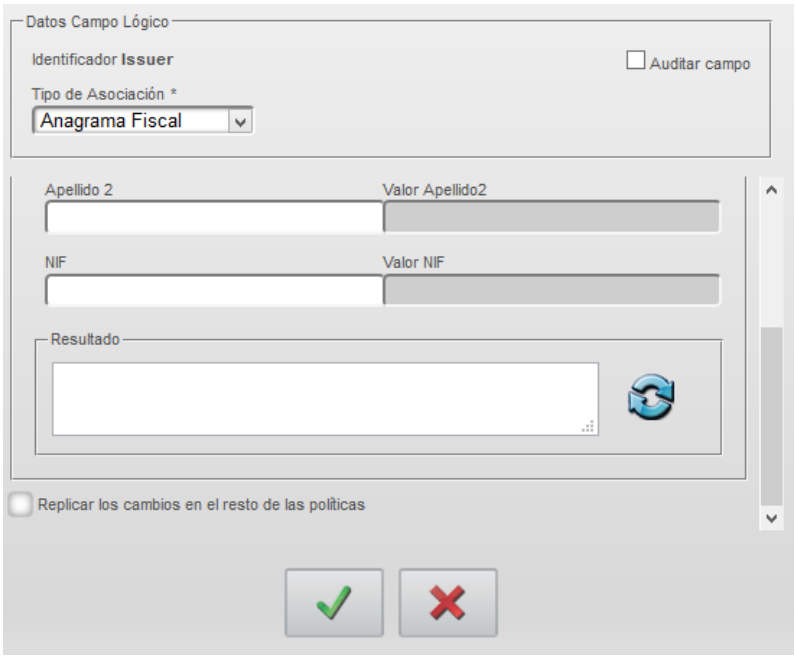


Figura 58 – Ventana de edición de mapeos. Mapeo tipo Anagrama Fiscal (II).

- **Apellidos.** Permite separar y extraer cada uno de los apellidos de una persona, cuando se encuentran especificados en un atributo del certificado y siempre y cuando los apellidos vayan separados por espacios en blanco (en caso contrario se recomienda utilizar el mapeo de tipo complejo). Para extraer un apellido, se seleccionará el atributo del certificado que contiene la información, apareciendo su ruta y valor en los campos correspondientes de la parte derecha de la pantalla. Seleccionaremos si se quiere extraer el primer o segundo apellido, y se pulsará sobre el botón refrescar/recargar para comprobar el resultado.

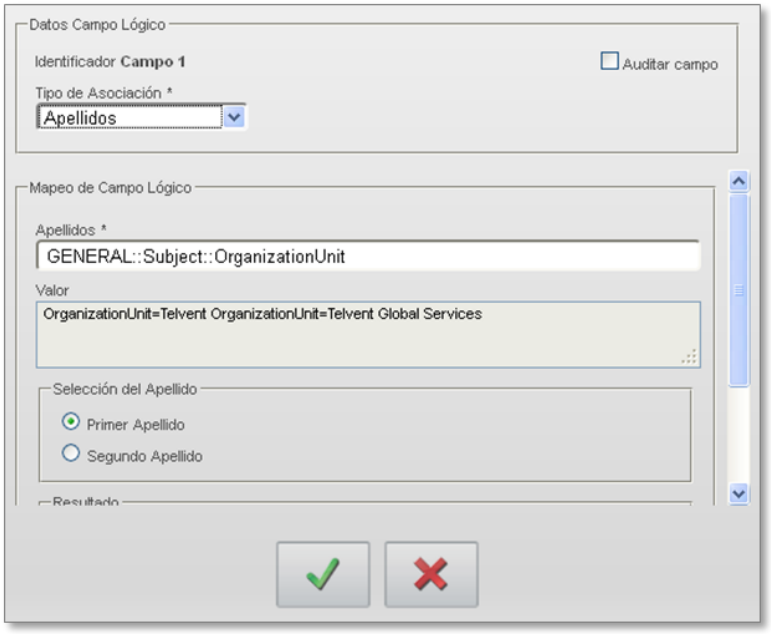


Figura 59 – Ventana de edición de mapeos. Mapeo tipo Apellidos (I)

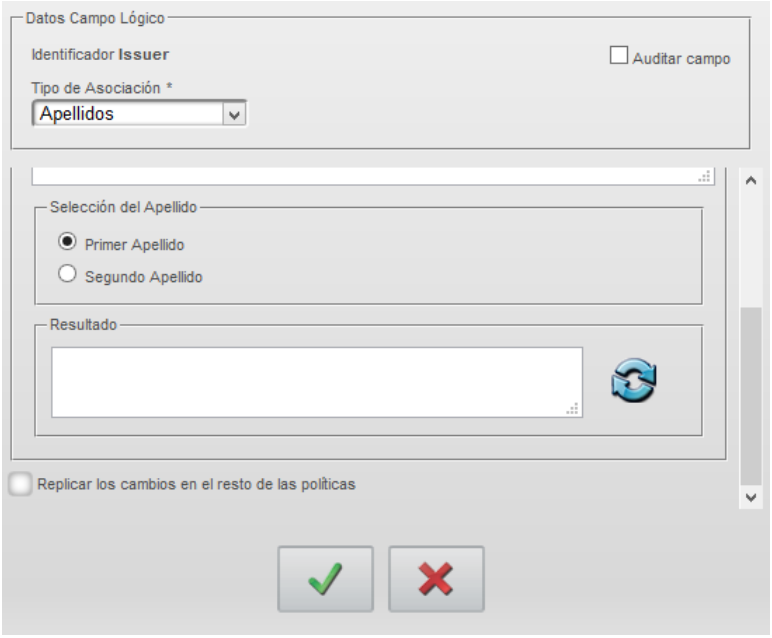


Figura 60 – Ventana de edición de mapeos. Mapeo tipo Apellidos (II)

- **Concatenación**. Permite asignar a un campo lógico el resultado de concatenar el valor de varios campos lógicos. Podemos concatenar hasta tres campos lógico seleccionándolos de las listas desplegables que aparecen.

  NOTA: Para rellenar los campos 1, 2 y 3, el usuario debe seleccionar previamente el campo que desea rellenar y después el nodo del árbol que quiere asociar.

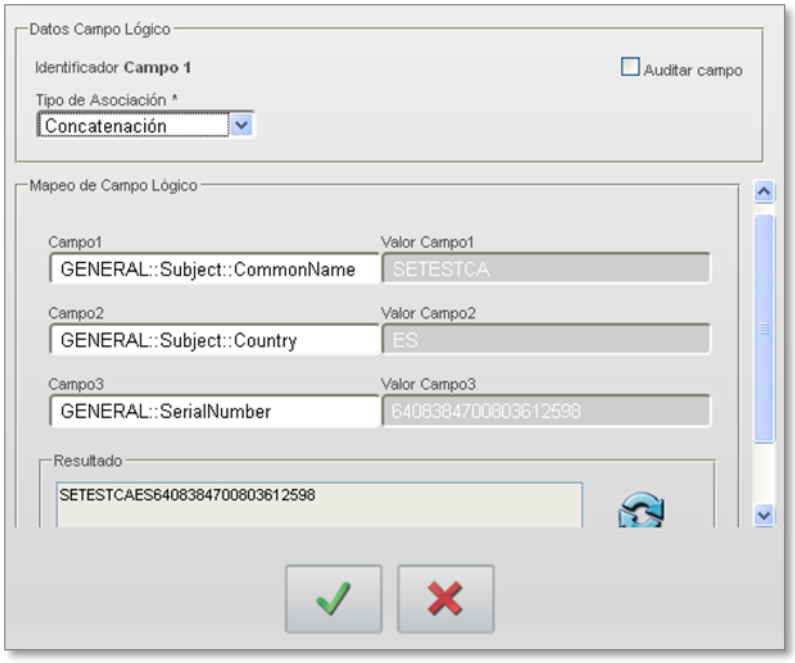


Figura 61 – Ventana de edición de mapeos. Mapeo tipo concatenación (I)

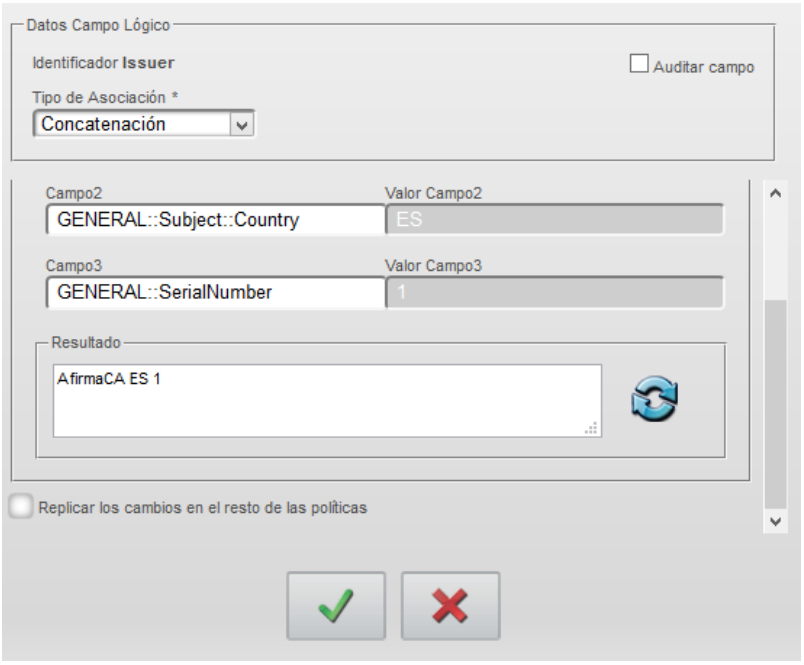


Figura 62 – Ventana de edición de mapeos. Mapeo tipo concatenación (II)

IMPORTANTE: Aunque se permite concatenar campos directamente del certificado en vez de campos lógicos, hay que tener en cuenta que la versión @firma 5.5.0_004 no tiene esta funcionalidad y tan solo puede concatenar campos lógicos, por lo que si existe la necesidad de

generar exportaciones de políticas de certificación a esta versión de la plataforma, se recomienda mantener configurados este tipo de mapeos mediante campos lógicos.

- **Expresión Regular:** Permite extraer una subcadena del valor de un atributo del certificado aplicando expresiones regulares de Java y/o haciendo referencia al valor de otro campo lógico del certificado. En primer lugar se debe seleccionar del árbol de atributos del certificado el campo donde se encuentra la información que queremos extraer. En siguiente paso es introducir una expresión regular de Java y/o el valor de un campo lógico ya definido (para indicar que queremos hacer referencia al valor de un campo lógico, se indicara ${NOMBRE_CAMPO_LOGICO}) al que se quiere hacer referencia, después se indicará el grupo de captura al que se asociará el campo lógico. Tras especificar dicha información, si se pulsa el botón con la refrescar/recargar, el sistema devolverá el valor del campo lógico y mostrará en el campo "Resultado", pudiendo comprobar si se han introducido correctamente los datos. (Para más información sobre expresiones de Java ver anexo)

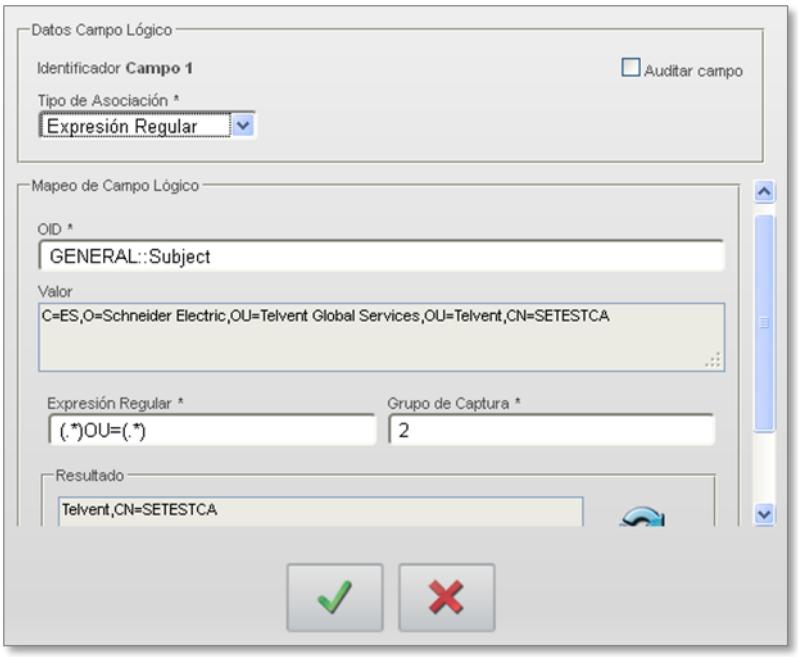


Figura 63 – Ventana de edición de mapeos. Mapeo tipo Expresión regular

Pseudocódigo: Mediante este tipo de operación podemos definir pseudocódigo para obtener el resultado que tendrá el campo lógico. Para más información consulta el anexo (Anexo V. Definición y uso de pseudocódigo en la plataforma).

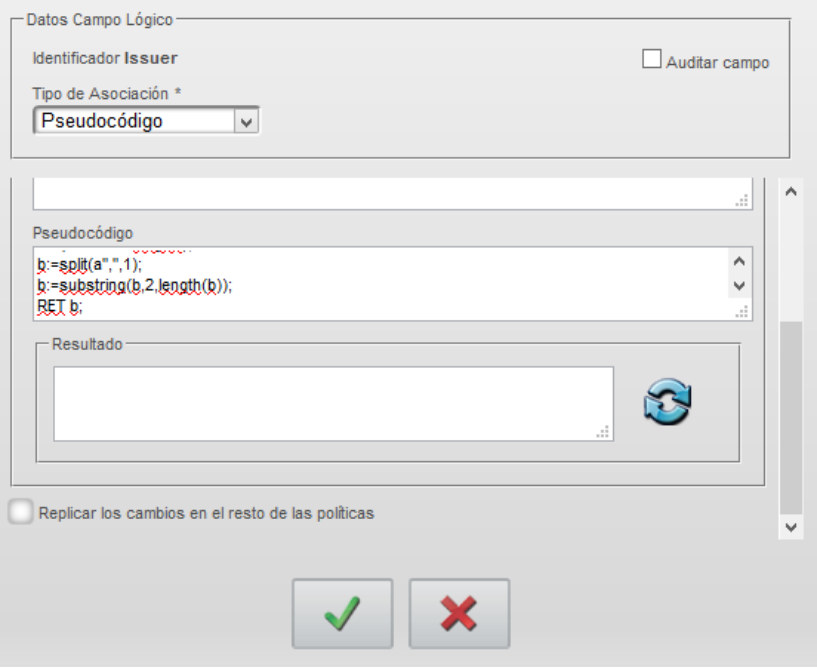


Figura 64– Ventana de edición de mapeos. Mapeo tipo Pseudocódigo

Tras finalizar la configuración del mapeo, se pulsará el botón "Modificar Mapeo", quedando dicha configuración asignada al campo lógico correspondiente. En todos los tipos de asociaciones existe la posibilidad de aplicar los cambios en todas las políticas seleccionando la opción ***"Replicar los cambios en el resto de las políticas."***.

5.3.3.5.2 Importación / Exportación de mapeos

Esta funcionalidad permite la generación de un fichero XML que contiene la información de los mapeos de un tipo de certificado concreto. Esta información podrá ser usada para importar los mapeos contenidos en dicho fichero en otros tipos de certificado, tanto de la misma plataforma como de otra distinta. También se ofrece la funcionalidad de importar los mapeos de un tipo de certificado existente en la plataforma.

Para acceder a la funcionalidad de importación / exportación, se debe navegar en el árbol de políticas hasta el tipo de certificado sobre el que se quiere realizar alguna de estas operaciones, apareciendo a

la derecha de dicho árbol la información referente al tipo de certificado seleccionado, además de los botones que nos permitirán acceder a estas funcionalidades.



Figura 65 – Ventana de gestión de políticas. Definición de mapeos II

5.3.3.5.2.1 Exportación de mapeos (XML)



Esta opción permite exportar los datos del mapeo para una versión 5.5 de @firma. Una vez se pulse sobre el botón se permitirá al usuario descargar un fichero XML denominado "mapping.xml" con los datos del mapeo.

5.3.3.5.2.2 Exportación de mapeos (JSON)



Esta opción permite exportar los datos del mapeo para una versión 6.2 o superior de @firma. Una vez se pulse sobre el botón se permitirá al usuario descargar un fichero JSON denominado "mapping.json" con los datos del mapeo.

5.3.3.5.2.3 Importación de mapeos

El proceso de importación obtendrá la información de los mapeos de un tipo de certificado, a través de un fichero JSON o a través de otro tipo de certificado existente en la plataforma, y tras su verificación, procederá a añadir la información en el sistema.

5.3.3.5.2.3.1 Importación de mapeos desde JSON



Al pulsar el botón "Importar Mapeo desde JSON" en la ventana del tipo de certificado al que se quiera importar, se nos muestra la siguiente ventana:



Figura 66 – Ventana de selección de fichero XML

Para importar un fichero, en la pantalla de importación se debe introducir el fichero de Mapeos (en formato JSON) que contenga a todos los mapeos a importar.

Tras especificar el fichero desde el que se quiere importar, se pulsará el botón "Importar Mapeo desde JSON". Tras lo cual comenzará el proceso de importación.

NOTA: El proceso de importación sobrescribe todos los mapeos existentes con los nuevos indicados en el fichero JSON.

5.3.3.5.2.3.2 Importación de mapeos desde otro tipo de certificados



Al pulsar el botón "Importar Mapeo" en la ventana del tipo de certificado al que se quiera importar, se nos muestra la siguiente ventana:

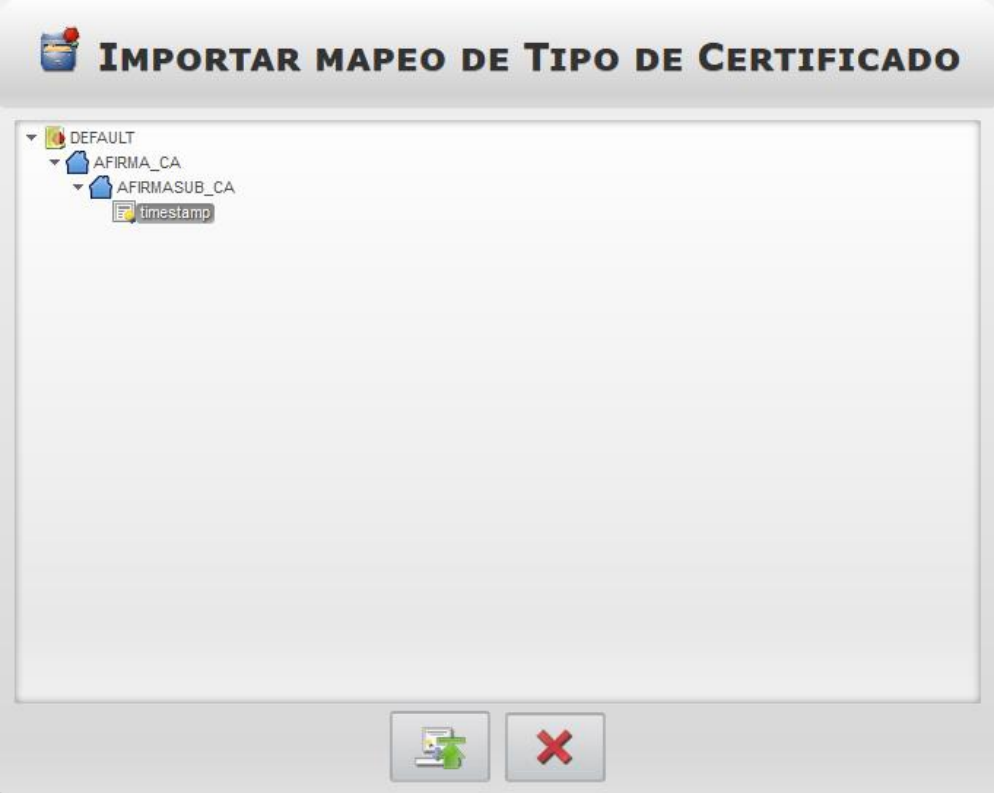


Figura 67 – Ventana de selección del tipo de certificado

Para importar un tipo de certificado, se debe navegar por el árbol y seleccionar el tipo de certificado que se quiere importar. Dicho certificado debe tener al menos un mapeo con su valor definido, y no debe ser el mismo tipo de certificado al que se quiere importar.

Tras especificar el tipo de certificado desde el que se quiere importar, se pulsará el botón "Continuar". Tras lo cual comenzará el proceso de importación.

NOTA: El proceso de importación sobrescribe todos los mapeos existentes con los que posee el Tipo de Certificado seleccionado.

5.3.3.5.2.3.3 _Sincronización de mapeos con TSL española



Al pulsar el botón "Sincronizar Mapeos" en la ventana del tipo de certificado cuyos mapeos se quieren sincronizar, se nos muestra el siguiente mensaje de confirmación:

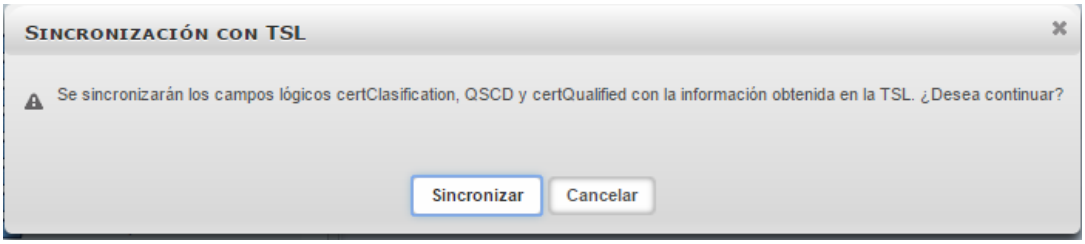


Figura 68 – Ventana de confirmación para sincronización de mapeos.

Si se confirma la acción, el sistema realiza la consulta de los valores de los campos lógicos contra la TSL española y los establece en el tipo de certificado seleccionado. Si no existe alguno de los campos lógicos para la política, se creará en este momento.

5.3.4 Gestión de Aplicaciones y Unidades Organizativas

La plataforma @firma publica sus servicios de cara a aplicaciones externas, convirtiéndose así en la base de la infraestructura de clave pública sobre la que se asienta todo el sistema. Con el fin de poder identificar y organizar cada una de estas aplicaciones y poder aplicarles configuraciones diferentes según sus necesidades, se definen las unidades organizativas (UO) y los identificadores de aplicación.

Las unidades organizativas permiten agrupar aplicaciones y otras unidades organizativas, formando de esta forma una estructura jerárquica. No obstante, no es necesario que las aplicaciones pertenezcan a alguna unidad organizativa.

La plataforma permite configurar a nivel de aplicación aspectos tales como la política de validación, de firma, de custodia, información acerca el responsable de la aplicación, etc. Toda esta información determinará las reglas aplicadas a los servicios ofrecidos por la plataforma.

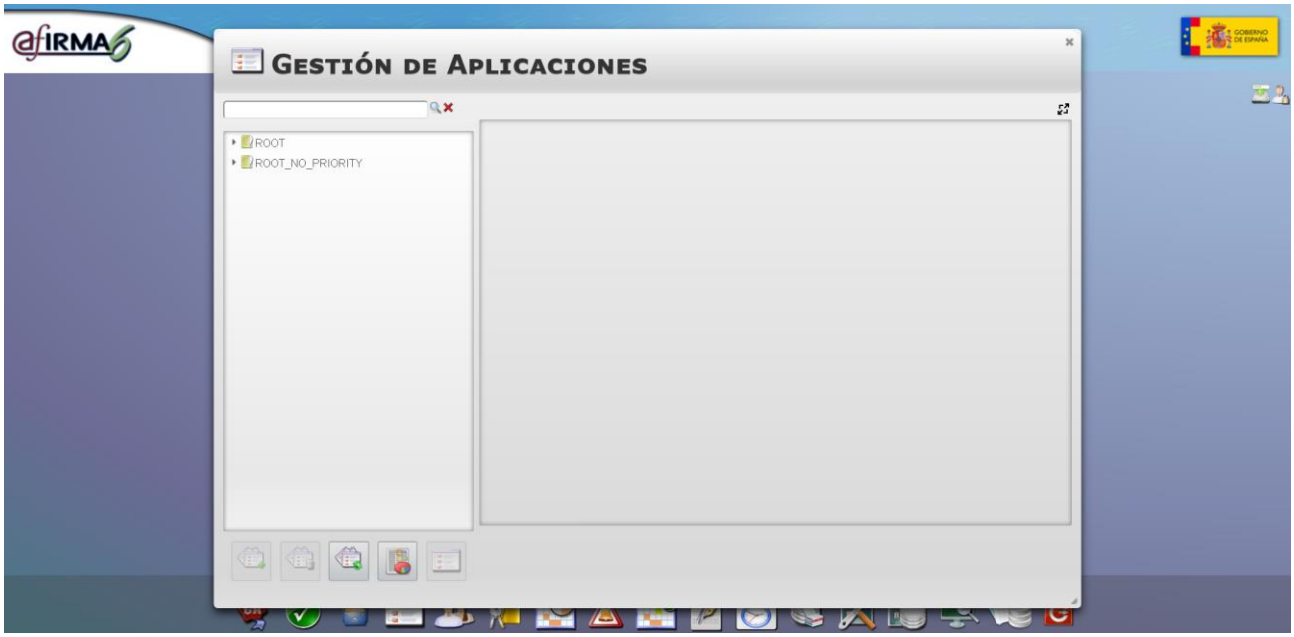


Figura 69 – Interfaz de gestión de UOs y Aplicaciones

En la parte izquierda de la interfaz se muestra un árbol que aloja las unidades organizativas y aplicaciones registradas en la plataforma. Existen dos nodos raíces, según si la aplicación es o no prioritaria. Una aplicación prioritaria (**ROOT**), es aquella que es usada con mucha frecuencia, y por lo tanto debe ser localizable con facilidad. Por el contrario, una aplicación NO prioritaria (**ROOT_NO_PRIORITY**) es aquella que rara vez es usada.

Como aplicaciones predefinidas se encuentran ***afirmaApp,*** aplicación para uso interno de la plataforma, por ejemplo, para validar la firma realizada por el usuario a logarse en caso de realizar el login mediante certificado. ***Ocspresponder*** es usada en las peticiones ***OCSP*** hacia el servidor de la plataforma en caso de que la petición no contenga la información asociada al ***requestorname.*** Sobre el árbol de unidades organizativas y aplicaciones se ubica un cuadro de entrada de texto que permite buscar aplicaciones por identificador y unidades organizativas por nombre. Así pues, una vez introducido el texto a usar como patrón de búsqueda, al pulsar sobre el botón  se procederá a mostrar en el árbol aquellas unidades organizativas cuyo nombre contenga el texto indicado, así como aquellas aplicaciones cuyo identificador contenga el texto indicado. Para eliminar el filtro indicado se deberá pulsar sobre el botón .

En la zona central se visualizará la información de configuración del elemento seleccionado, que podrá ser una unidad organizativa o bien una aplicación. Mediante este gestor es posible realizar las siguientes operaciones:

- Sobre unidades organizativas
    - Alta de unidades organizativas.
    - Modificación de unidades organizativas.
    - Baja de unidades organizativas.
- Sobre las aplicaciones:
    - Alta de aplicaciones.
    - Modificación de aplicaciones.
    - Baja de aplicaciones.

A continuación, se verán las diferentes operaciones, así como los datos que intervienen en cada una de ellas.

5.3.4.1 Generación de Informe de Aplicaciones



Mediante esta opción se genera un informe Excel con las propiedades establecidas para las aplicaciones registradas en la plataforma.

5.3.4.2 Alta de una Unidad Organizativa



Para registrar una nueva UO en la plataforma es necesario posicionarse sobre el nodo del árbol de UO y aplicaciones sobre el cual se desea crear la nueva UO. Este nodo debe ser o el nodo raíz (ROOT o ROOT_NO_PRIORITY) o cualquier otro nodo que represente una unidad organizativa, ya que las aplicaciones no pueden tener nodos hijos. En caso de no seleccionar ninguna Unidad Organizativa, la nueva Unidad Organizativa se dará de alta como hija de la unidad organizativa principal, ***ROOT***.

Tras pulsar el botón de alta aparecerá un panel para seleccionar el tipo de alta a realizar.



Figura 70 – Panel selección alta aplicación / unidad organizativa.



Tras pulsar el botón ***"Alta Unidad Organizativa"***, aparecerá el formulario de alta asociado a una unidad organizativa. La apariencia del mismo dependerá del tipo de identificador asociado a la unidad organizativa, así, para un tipo de identificador *Libre* la apariencia será la siguiente:



Figura 71 – Ventana de registro de unidad organizativa con tipo de identificador Libre

Mientras que para un tipo de identificador *DIR3* la apariencia será la siguiente:

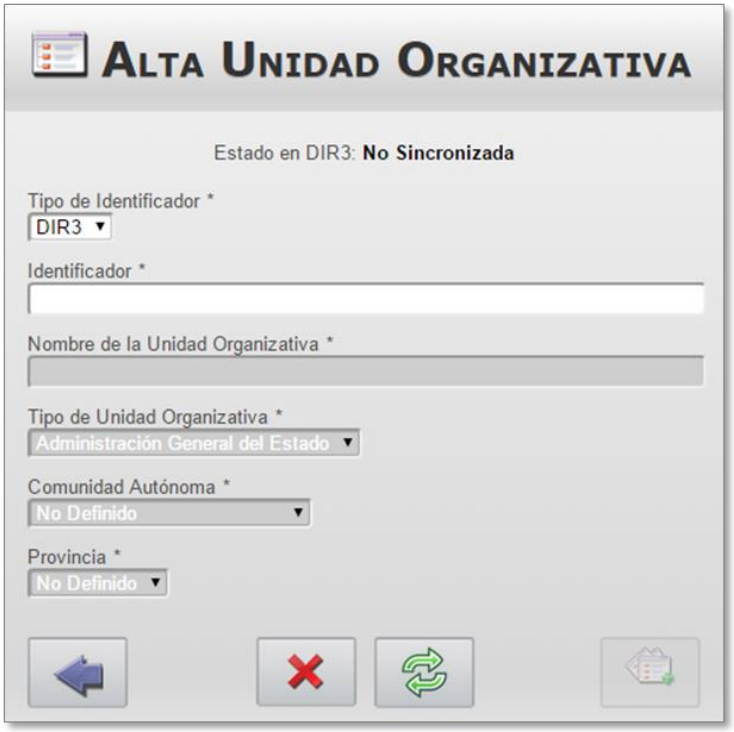


Figura 72 - Ventana de registro de unidad organizativa con tipo de identificador DIR3

Los datos asociados a la creación de una unidad organizativa son:

- **Estado en DIR3:** Texto que identifica el estado de la unidad organizativa respecto con DIR3. Sólo aplicable cuando el **Tipo de Identificador** es *DIR3*. El estado será uno de los siguientes:
    - *No Sincronizada:* La unidad organizativa no ha sido sincronizada con DIR3.
    - *Vigente:* La unidad organizativa se encuentra vigente desde el punto de vista oficial.
    - *Transitorio:* Se aplica este estado intermedio a toda unidad organizativa que se considere extinguida por disposición legal, pero continúe ejerciendo funciones de forma transitoria hasta la regularización completa de la estructura/competencias.
    - *Extinto:* Se aplica este estado a toda unidad organizativa que ha sido extinguida oficialmente y, en caso de que hubiera tenido una estructura de unidades dependientes orgánicamente de ella, todas ellas se encuentran regularizadas (extinguidas o dependiendo orgánicamente de una nueva unidad vigente).
    - *Anulado:* Se aplica este estado a toda unidad organizativa que se requiera dar de baja en el sistema, por motivos diferentes al fin de su vigencia o prestación de servicio. El

caso más común es el referido a altas erróneas por duplicidad (la misma unidad u oficina se da de alta con distinto código y descripción algo diferente, pero resto de atributos idénticos).

- **Tipo de Identificador:** Tipo de identificador asociado a la unidad organizativa. Se corresponde con un valor predefinido seleccionable entre una lista de posibles:
    - *Libre:* La unidad organizativa no se encontrará asociada a DIR3, ni llevará a cabo la sincronización con el mismo.
    - *DIR3:* La unidad organizativa se encontrará asociada a DIR3 y llevará a cabo la sincronización con el mismo.
- **Identificador:** Texto que identifica unívocamente a la unidad organizativa.
- **Nombre:** Texto descriptivo de la unidad organizativa.
- **Tipo de Unidad Organizativa:** Entidad donde ubicar la unidad organizativa. Se corresponde con un valor predefinido seleccionable entre una lista de posibles:
    - *Administración General del Estado*
    - *Administración Autonómica*
    - *Administración Local*
    - *Universidades*
    - *Otras Instituciones*
- **Comunidad Autónoma:** Nombre de la comunidad autónoma donde se ubica la unidad organizativa. Se corresponde con un valor predefinido seleccionable entre una lista de posibles, donde aparecen todas las comunidades autónomas definidas para España, así como el valor *No Definido*, para indicar que la unidad organizativa no posee comunidad autónoma asociada.
- **Provincia:** Nombre de la provincia donde se ubica la unidad organizativa. Se corresponde con un valor predefinido seleccionable entre una lista de posibles, donde aparecen todas las

provincias asociadas a la comunidad autónoma seleccionada. En el caso de que la comunidad autónoma tenga el valor *No Definido*, la provincia tomará el mismo valor para indicar que la unidad organizativa no posee comunidad autónoma ni provincia asociada.

Los campos indicados con un asterisco serán obligatorios. Para crear la unidad organizativa se debe pulsar sobre el botón , para sincronizar los datos de la unidad organizativa con DIR3 se debe pulsar sobre el botón , y para cancelar el proceso se debe pulsar sobre el botón . Una vez almacenada la nueva unidad organizativa se mostrarán los datos de la nueva unidad organizativa creada, que visualmente serán diferentes en función de si su tipo de identificador es *Libre* o *DIR3*. Tras pulsar el botón "Dar de Alta" la nueva unidad organizativa quedará registrada en la plataforma.

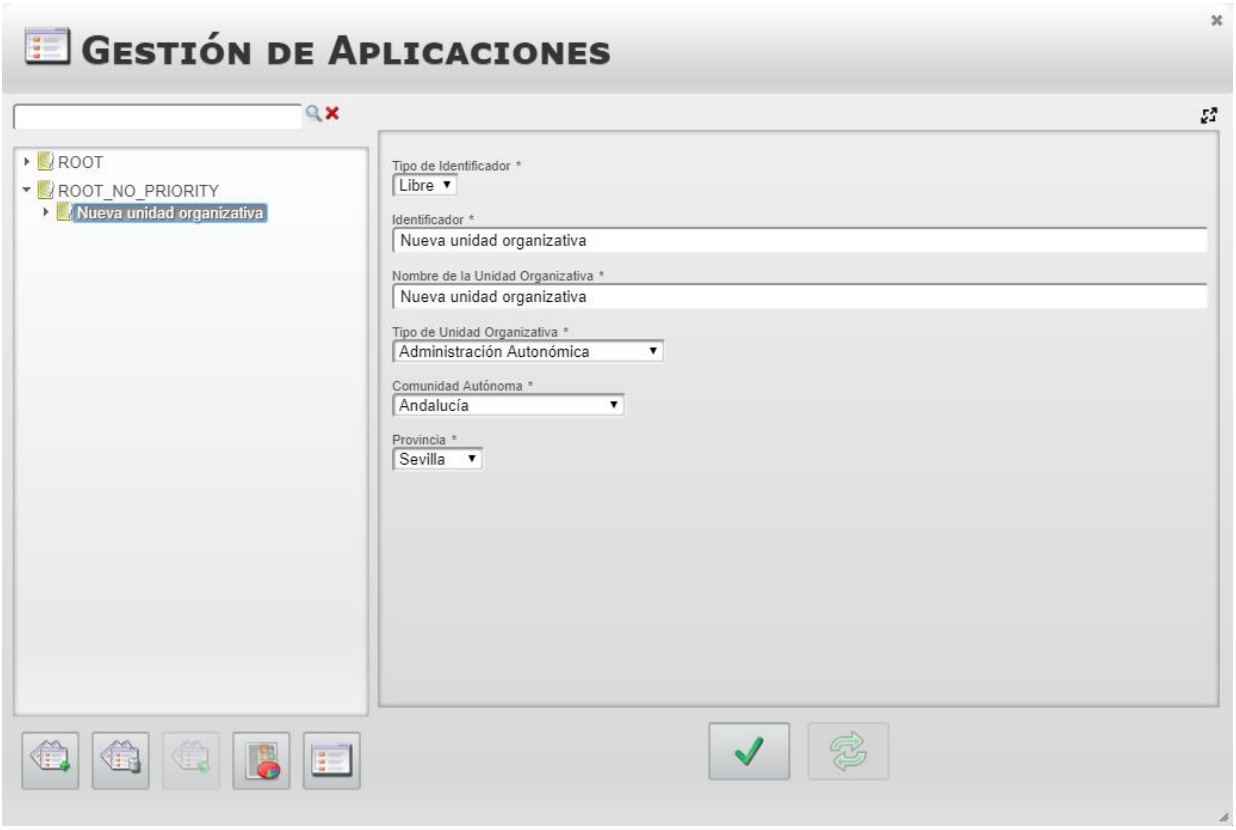


Figura 73 – Alta de unidad organizativa correcta

5.3.4.3 Modificación de una Unidad Organizativa



Para actualizar una UO registrada en la plataforma es necesario posicionarse sobre la unidad que se desea modificar en el árbol de UO y aplicaciones. En la parte derecha de

la pantalla aparecerá la información de la UO, que podrá ser modificada libremente.

Los datos susceptibles de ser actualizados para una unidad organizativa son:

- ***Identificador***.
- ***Tipo de Identificador***.
- ***Nombre de la Unidad Organizativa***.
- ***Tipo de Unidad Organizativa***.
- ***Comunidad Autónoma.***
- ***Provincia.***

Para guardar los cambios, pulse el botón “Guardar” ubicado en la parte inferior de la pantalla, y el sistema registrará la nueva información. Acto seguido aparecerá una ventana de confirmación. Tras la confirmación de la operación, se aplicarán los cambios en la unidad organizativa modificada.

5.3.4.4 Baja de una Unidad Organizativa



Para eliminar una UO registrada en la plataforma es necesario posicionarse sobre la unidad que se desea borrar en el árbol de UO y aplicaciones. Para eliminar la UO, se pulsará el botón “Eliminar Unidad Organizativa / Aplicación” ubicado en la parte inferior del árbol de políticas.

Acto seguido se pedirá confirmación al usuario para realizar la operación. Esta operación elimina tanto la unidad organizativa seleccionada como las unidades organizativas hijas y aplicaciones asociadas a dicha unidad organizativa. Tras confirmarse la operación, la plataforma eliminará definitivamente el elemento seleccionado.

5.3.4.5 Alta de una Aplicación



Para registrar una nueva aplicación en la plataforma es necesario posicionarse sobre el nodo del árbol de UO y aplicaciones sobre el cual se desea crear la nueva aplicación. Este nodo debe ser o el nodo raíz (ROOT o ROOT_NO_PRIORITY) o cualquier otro nodo

que represente una unidad organizativa, ya que las aplicaciones no pueden tener nodos hijos. Tras pulsar el botón de alta aparecerá un panel para seleccionar el tipo de alta a realizar.



Figura 74 – Panel selección alta aplicación / unidad organizativa.



Tras pulsar el botón ***"Alta Aplicación"***, aparecerá el formulario de alta asociado a la aplicación a dar de alta.

El formulario de Alta / Modificación de una aplicación contiene una gran cantidad de campos configurables, los cuales están agrupados según su contexto:

- Datos de la Aplicación.
- Parámetros de la Aplicación.
- Servicios disponibles.
- Usuarios de Administración Delegada.
- Certificados Permitidos para Firmar.
- Selección del Método de Acceso.
- Certificados Autenticación OCSP.
- Restricciones a la Política de Certificación.
- Gestores Documentales.

- Sellos de Tiempo



Figura 75 – Ventana de registro de Aplicación (I)

5.3.4.5.1 Datos de la aplicación

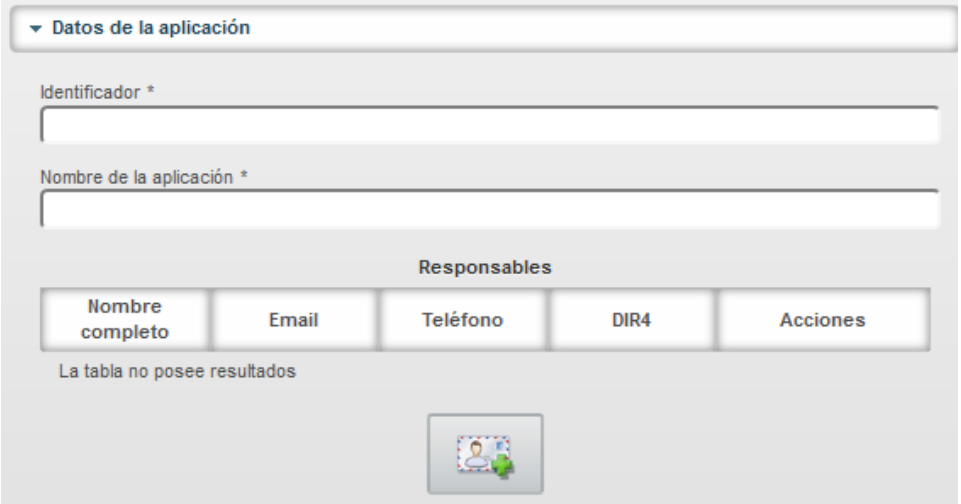


Figura 76 – Ventana de registro de Aplicación (II)

Los campos contenidos son:

- **Identificador.** Identificador que poseerá la aplicación dentro de la plataforma. Debe de ser único, independientemente de la Unidad Organizativa a la que pertenezca. Además, en este parámetro debe especificarse la "ruta" completa que se desee. Es decir, por ejemplo, suponiendo que se va a dar de alta la aplicación dentro de una unidad organizativa que a su vez está dentro de otra unidad organizativa, lo ideal es mantener un poco la estructura y establecer en este valor "identificadorUO1.identificadorUO2.identificadorAplicacion". En cualquier caso, no tiene por qué ser así. La única condición en este campo es que no coincida en el mismo valor con cualquier otra aplicación.

- **Nombre de la Aplicación.** Nombre descriptivo de la aplicación.

En la tabla de Responsables se insertarán los datos relativos a la persona de contacto asociada a la aplicación. Para gestionar los responsables se debe pulsar en el botón de la tabla de responsables . Se nos abrirá una nueva ventana donde podremos habilitar, deshabilitar o eliminar los responsables existentes, además de crear nuevos responsables.



Figura 77 – Ventana de gestión de responsables

Para añadir un nuevo responsable pulsaremos sobre el botón "Añadir Responsable" y rellenaremos los datos que se nos solicita.



Figura 78 – Insertar nuevo responsable

- **Nombre.** Nombre de la persona de contacto asociada a la aplicación.
- **Apellidos.** Apellidos de la persona de contacto asociada a la aplicación.

- **E-mail.** Dirección de correo electrónico asociado al responsable de la aplicación.
- **Teléfono.** Teléfono de contacto asociado al responsable de la aplicación.
- **DIR4.** Indica si el responsable tiene DIR4 habilitado o no.

5.3.4.5.2 Parámetros de la aplicación

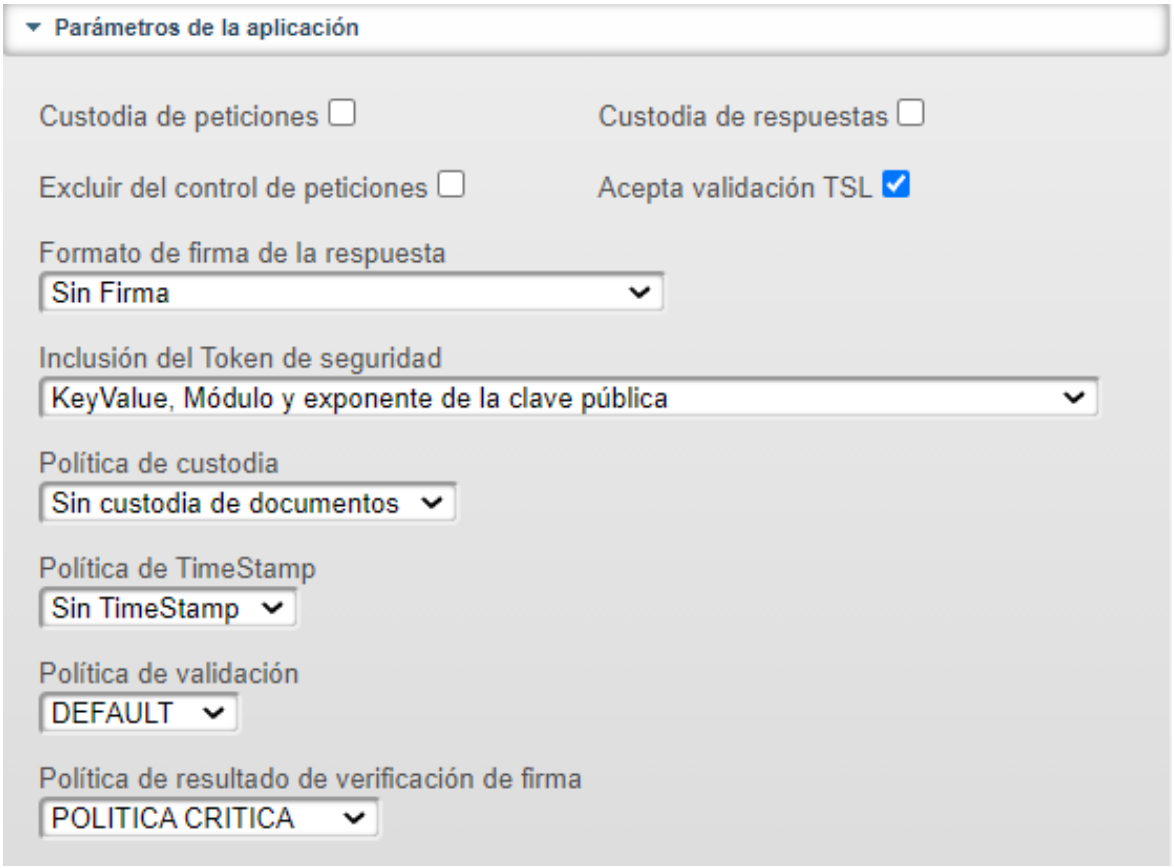


Figura 79 – Ventana de registro de Aplicación (III)

Los campos contenidos son:

- **Custodia de peticiones**: este indicador se marcará si queremos activar la custodia de peticiones. Por defecto, vendrá marcada a true.
- **Custodia de respuestas**: este indicador se marcará si queremos activar la custodia de respuestas. Por defecto, vendrá marcada a true.

- **Excluir del control de peticiones**: este indicador se marcará si queremos excluir a la aplicación del control de peticiones.

- **Acepta validación TSL**: este indicador se marcará si queremos que la aplicación permita ser validada contra TSL.

- **Formato de la firma de Respuesta**: formato de firma empleado por una aplicación para firmar los mensajes SOAP de respuesta ante una petición a un servicio Web publicado por la plataforma. Los posibles formatos son:

  - **Sin Firma**

  - **XMLDSignature (XML Básica)**

  - **XAdES-BES (XML Avanzada)**

  - **XAdES-T (XML Avanzada con Timestamping)**

- **Inclusión del Token de Seguridad**: formato del certificado introducido en la firma de Respuesta. Los posibles formatos son:

  - **KeyValue**, Módulo y exponente de la clave pública

  - **X509Data**, Certificado X.509 en base 64

  - **BinarySecurityToken**, Certificado X.509 referenciado por SecurityTokenReference

  Por defecto se recomienda utilizar la opción "***BinarySecurityToken***" para las aplicaciones desarrolladas sobre plataformas Microsoft en .NET.

- **Política de custodia de documentos**: determina que debe hacer la plataforma con los documentos que son firmados mediante esta aplicación. Los posibles valores son "***Sin custodia de documentos***" y "***Con custodia de documentos***".

- **Política de TimeStamp:** Indica si la plataforma aplicará un sellado temporal para las peticiones de firma. Sus posibles valores son "***Sin TimeStamp***" y "***Con TimeStamp***".

- **Política de validación:** política de certificación definida en la plataforma @firma y que definirá los prestadores y tipos de certificados soportados para la aplicación, los métodos de validación a utilizar, la configuración del mapeo de campos de certificado, etc.

- **Resultados de Verificación:** Este campo recoge la "Política de Resultados de Verificación de Firma" que tendrá la aplicación. Un proceso de validación de firma está formado por un conjunto de tareas de verificación (validación del "***CORE***", validación del certificado firmante…) el resultado de estas tareas determina el resultado final de proceso. Una "Política de Resultados de Verificación de Firma" contiene la prioridad y criticidad de todos los errores que pueden darse en un proceso de validación de firma, actualmente se define dos políticas:

    - "***POLITICA CRITICA***". Cualquier resultado no satisfactorio arrojado por una tarea de verificación de firma devuelve un resultado de "firma no válida". Este comportamiento es similar al que tenía la plataforma en la versión 5.3.

    - "***POLITICA AVANZADA***". Si no es posible determinar el estado de revocación de un certificado (firmante, TSA…) incluido en la firma se devuelve un resultado de "warning", en el caso de producirse cualquier otro resultado no satisfactorio el resultado será "firma no válida".

5.3.4.5.3 Servicios disponibles

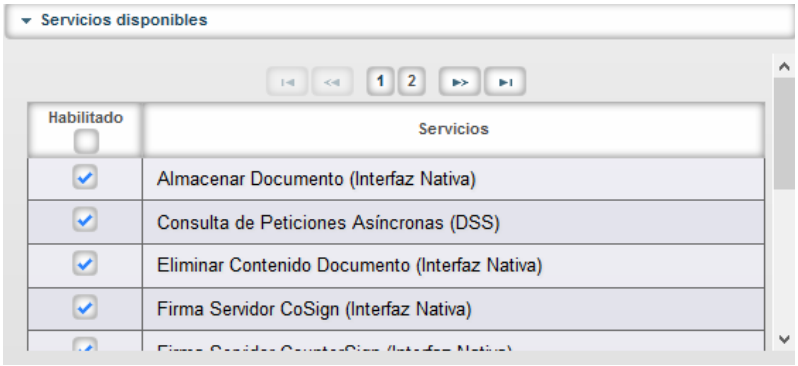


Figura 80 – Ventana de registro de Aplicación (IV)

Esta sección contiene una tabla con todos los servicios disponibles en la plataforma. El usuario habilitará/deshabilitará los servicios que la aplicación puede hacer uso.

5.3.4.5.4 Usuarios Administración Delegada

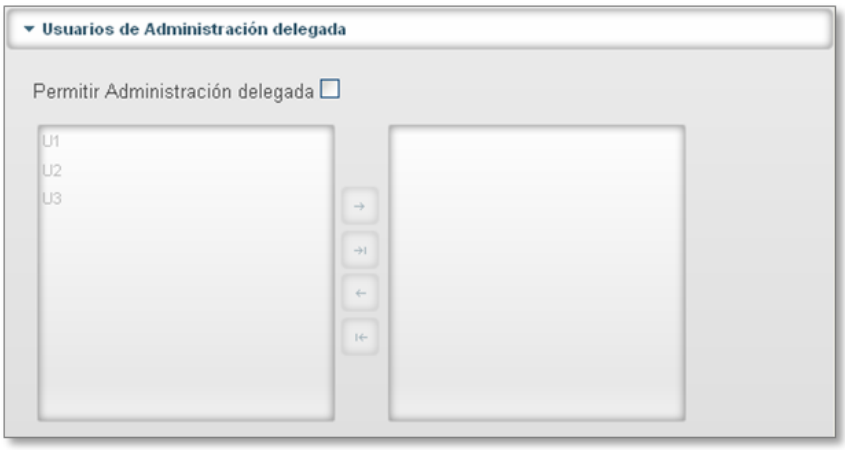


Figura 81 - Ventana de registro de Aplicación (VI)

Los campos contenidos son:

- **Permitir Administración Delegada.** En caso de seleccionarse esta opción, se permite hacer uso de la aplicación desde la administración delegada.

- **Usuarios Administradores.** En caso de permitir la administración delegada, se habilita la selección de los usuarios administradores para los que estará disponible la aplicación en la administración delegada.

5.3.4.5.5 Certificados permitidos para firmar

Si las respuestas producidas por la aplicación están configuradas para ser firmadas, este parámetro indica el certificado empleado para ello.



Figura 82 - Ventana de registro de Aplicación (VII)

En esta sección, la columna '**No permitidos'** contiene todos los certificados (clave) dados de alta en la plataforma en el Almacén de Par de Claves ***"Almacén de Claves Servidor"***. En esta sección el usuario puede habilitar los certificados permitidos para firmar las respuestas pasándolo a la columna '**Permitidos**'.

Junto al nombre del certificado (clave) aparecerá un icono, que dependiendo del estado en el que se encuentre dicho certificado, será de un color u otro.

Los distintos estados de los certificados (clave) se representarán con los siguientes colores:

Válido

Caducado

Revocado

Otro

No existe

Aún no válido

Esta forma de representación de los distintos estados en los que se puede encontrar un certificado (clave) será utilizada en distintos componentes de la administración.

5.3.4.5.6 Selección del método de acceso

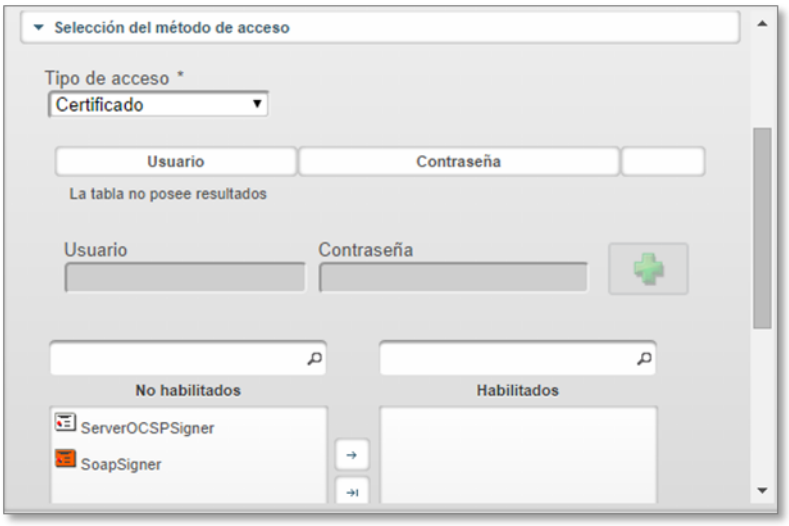


Figura 83 - Ventana de registro de Aplicación (VIII)

Lo primero, equivalente al estado de las claves de certificados, existen una serie de iconos que determinan el estado de los certificados (parte pública) que se muestran en esta sección (y en otras de la administración):

Válido

Caducado

Revocado

Otro

No existe

Aún no válido

En este apartado se le indica a la plataforma el método de seguridad empleado para la ejecución de servicios Web por una aplicación. Estos métodos siguen el estándar WS-Security.

Los métodos empleados son:

- **Tipo de Acceso.** Selecciona el tipo de acceso que poseerá la aplicación. Puede ser:
  - **Sin autenticación.** Se deshabilitan las opciones de inclusión / eliminación de usuarios. No se aplica ninguna medida de seguridad para ejecutar los servicios Web para una aplicación.
  - **Usuario/Password.** Se habilita la opción de inclusión / eliminación de usuarios. Mediante este método es necesario que las peticiones *SOAP* realizadas contengan el *tag* de seguridad "***UserNameToken***" y que el usuario y *password* alojados en dicho *tag* estén registrados para la aplicación que intenta ejecutar el servicio Web.
  - **Certificado.** Se habilita la tabla de selección de certificados procedentes del ***"Almacén de Autorización WS"***. Mediante este método es necesario que las peticiones *SOAP* realizadas contengan el *tag* de seguridad "***BinarySecurityToken***" y estén firmadas por alguno de los certificados registrados para la aplicación que intenta ejecutar el servicio Web.

5.3.4.5.7 Certificados Autenticación OCSP



Figura 84 - Ventana de registro de Aplicación (IX)

Permite configurar los parámetros de acceso al servicio *OCSP* de la plataforma para cada aplicación. Con el fin de poder aplicar esta configuración a las aplicaciones, es necesario que las peticiones *OCSP*

vengan firmadas, o bien que al menos se incluya el campo ***RequestorName***, con el fin de poder identificar a la aplicación llamante. En caso de no incluirse este campo, las aplicaciones utilizarán la configuración de la aplicación de sistema ***ocspresponder***. Los parámetros que se pueden configurar son:

- **Habilitar servicio OCSP:** Indica si la aplicación permite el uso del Servicio *OCSP*, es decir si permite la recepción de peticiones *OCSP*. En caso de no estar habilitado, el sistema devolverá un mensaje de error a la aplicación con el mensaje ***Unauthorized***.

- **Modo Firma Peticiones OCSP**. Únicamente puede configurarse si se encuentra habilitado el servicio OCSP para la aplicación correspondiente. Indica si las peticiones de cliente pueden o deben ser firmadas. Las configuraciones posibles son:

  - **Modo relajado**. La firma de la petición es opcional. Este modo tiene una problemática asociada y es que es posible que un cliente incluya un *RequestorName* que no esté asignado a él, suplantando así a dicho cliente. Para solventar esto, se recomienda activar el modo estricto, de forma que se pueda garantizar la identidad del cliente. Este modo únicamente debe utilizarse para aplicaciones en fase de adaptación a las firmas de mensajes *OCSP*.

  - **Modo estricto**: Se requiere que las peticiones *OCSP* enviadas a la plataforma estén firmadas. Cualquier petición no firmada será rechazada con un mensaje de error *sigRequired*.

- **Certificados para autenticación OCSP**. Se permite especificar qué certificados podrán ser utilizados por el cliente para realizar la firma de las peticiones *OCSP*. Si la firma se realiza con un certificado diferente, el sistema devolverá un mensaje *unauthorized*.

  En la lista de certificados '**No habilitado**' aparecen aquellos que han sido previamente incorporados al keystore "***Almacén Autorización WS"***.

Según la configuración seleccionada mediante los parámetros descritos, el comportamiento que adoptará la plataforma al recibir una petición por OCSP será el que se muestra en la siguiente tabla:

RequestorName	Modo de firma de peticiones	RequestorName incluido en la petición	Petición	Resultado procesamiento	Identificador de aplicación utilizado por la plataforma
NO Obligatorio	**Relajado**	No	No firmada	Petición procesada	***ocspresponder***
			Firmada	Petición procesada	***ocspresponder***
		Sí	No firmada	Petición procesada	***RequestorName***
			Firmada	Petición procesada	***RequestorName***
	Estricto	No	No firmada	Petición procesada	***ocspresponder***
			Firmada	Petición procesada	***ocspresponder***
		Sí	No firmada	***Sigrequired***	-
			Firmada	Petición procesada	***RequestorName***
Obligatorio	**Relajado**	No	No firmada	***Unauthorized***	-
			Firmada	***Unauthorized***	-
		Sí	No firmada	Petición procesada	***RequestorName***
			Firmada	Petición procesada	***RequestorName***
	Estricto	No	No firmada	***Unauthorized***	-
			Firmada	**Unauthorized**	-
		Sí	No firmada	**Sigrequired**	-
			Firmada	Petición procesada	***RequestorName***

En los casos en los que la petición va firmada, y el ***RequestorName*** no está definido o no es reconocido, la plataforma asociará la petición a aquella aplicación cuyo certificado de autenticación

OCSP habilitado coincida con el firmante de la petición. Si el certificado firmante está asociado en más de una aplicación como certificado de autenticación *OCSP*, se devolverá ***Unauthorized***.

5.3.4.5.8 Restricciones a la política de certificación



Figura 85 - Ventana de registro de Aplicación (X)

Permite configurar que tipos de certificados, de los incluidos en la política asignada, están operativos para la aplicación.

En la tabla "Restricciones a la Política de Certificación" se listan todos los certificados incluidos en la política elegida en el campo "Selección de política". La selección de un tipo de certificado indica que ese certificado está habilitado para la aplicación, en caso contrario el tipo de certificado estaría restringido.

- **Modo de restricción para OCSP:** Permite configurar el comportamiento del servicio OCSP respecto a las restricciones a la Política de Certificación.

  Las configuraciones que se permiten escoger son:

  - **Modo relajado:** si al menos un certificado de un determinado PSC aparece como NO restringido, el resto de certificados de dicho PSC se considerarán también NO restringidos.

  - **Modo total:** si al menos un certificado de un determinado PSC aparece como restringido, el resto de certificados de dicho PSC se considerarán también restringidos.

Si el servicio OCSP está deshabilitado, esta opción no estará disponible.

5.3.4.5.9 Gestores Documentales.



Figura 86 - Ventana de registro de Aplicación (XI)

Permite configurar qué gestores documentales podrá utilizar la aplicación para realizar operaciones de firma y validación sobre elementos alojados en él. Tras pulsar el botón "Dar de Alta" la nueva aplicación quedará registrada en la plataforma con los valores que han sido introducidos.

5.3.4.5.10 Sellos de tiempo.



Figura 87 - Ventana de registro de Aplicación (XI)

- **Plataformas TSA.**

  En la columna **'Seleccionables'** aparecerán todas las plataformas TSA disponibles para la obtención del sello de tiempo desde @Firma. En la lista **'Seleccionadas'** se incluirán, ordenadas por prioridad, aquellos servidores TSA que se podrán utilizar cuando se realice una petición de sellado de tiempo.

- **Sello de Tiempo Crítico.**

- **Seleccionado:** en el caso de agotar la lista de servidores TSA sin obtener una respuesta válida, @Firma emitirá un mensaje de error, informando del problema.

- **No seleccionado:** en el caso de agotar la lista de servidores TSA sin obtener una respuesta, @Firma devolverá la firma, pero indicando los motivos por los que no se ha obtenido una respuesta válida.

- **Formatos de Sello de Tiempo Admitidos**



Figura 88 - Formatos de Sello de Tiempo Admitidos

En esta sección se indica la prioridad a la hora de obtener tipo de sello de tiempo.

Casos posibles:

- Si es firma XML: Solo en el caso de marcar únicamente XML, se realizará un sello de tiempo tipo XML, en el resto de casos se realizará un sello de tiempo tipo RFC 3161.

- Si es firma CAdES: Independientemente de los seleccionados, siempre usa tipo de sello de tiempo RFC3161.

5.3.4.6 Modificación de una Aplicación

Para actualizar una aplicación registrada en la plataforma es necesario posicionarse sobre la aplicación que se desea modificar en el árbol de UO y aplicaciones. En este momento, la plataforma mostrará los datos de la aplicación seleccionada.

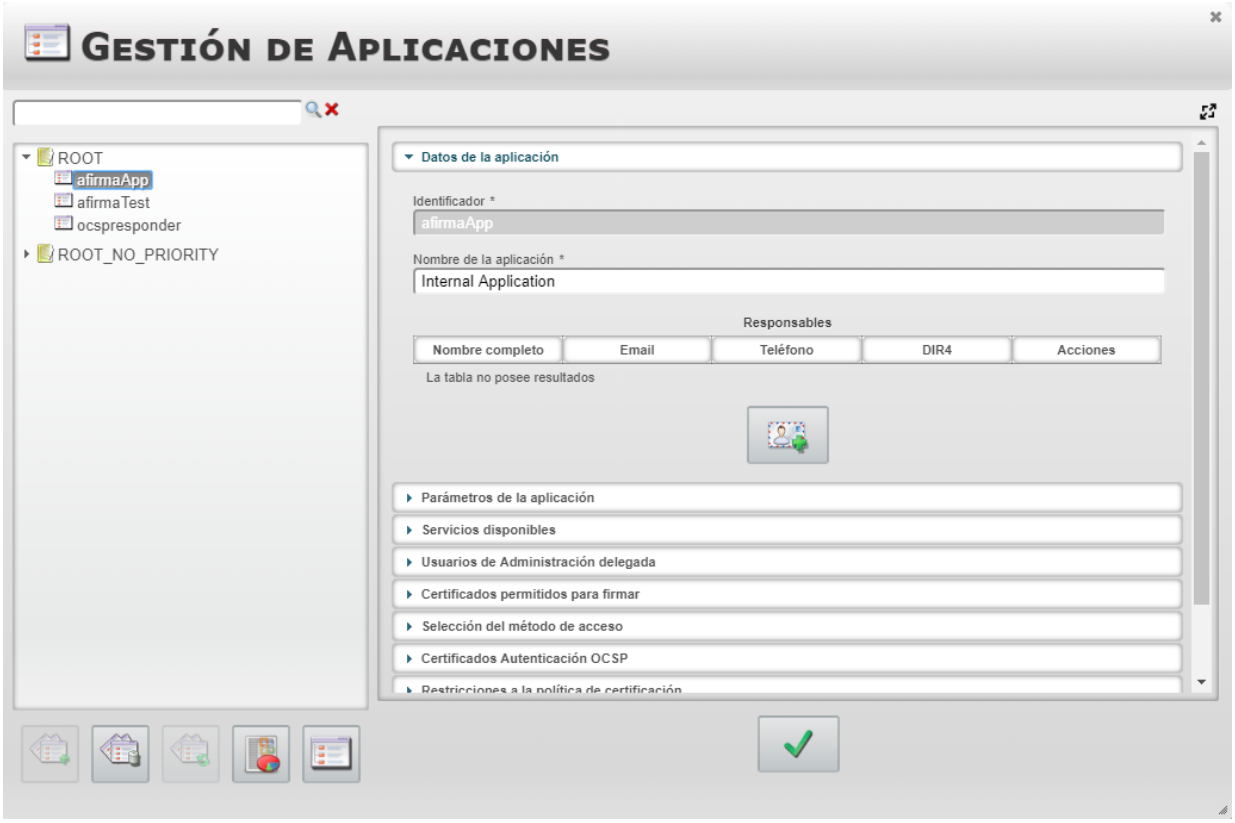


Figura 89 - Interfaz de gestión de UO y aplicaciones. Modificación de aplicación

Tras realizar algún cambio sobre los distintos parámetros, ahora, tan solo es necesario pulsar "Modificar". Tras realizar esto, la plataforma le solicitará confirmación.

Una vez confirmada la operación la plataforma registrará los cambios.

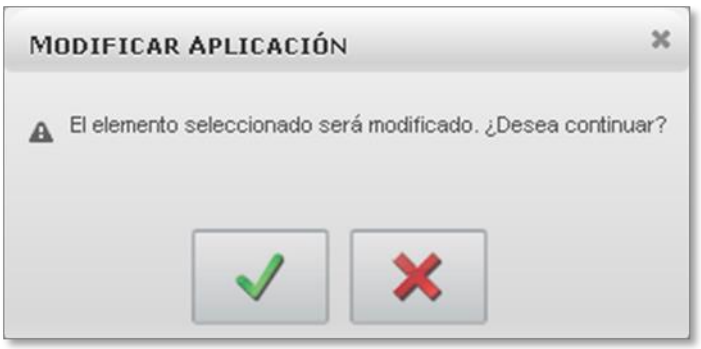


Figura 90 - Confirmación Modificación Aplicación

5.3.4.7 Baja de una Aplicación



Para eliminar una aplicación registrada en la plataforma es necesario posicionarse sobre la aplicación que se desea borrar en el árbol de UO y aplicaciones. Hay que tener en cuenta que al eliminar una aplicación no será posible recibir más peticiones de validación o firma con el identificador de la aplicación seleccionado.

Tras esto, se pulsa "Baja" y se mostrará una ventana de confirmación.

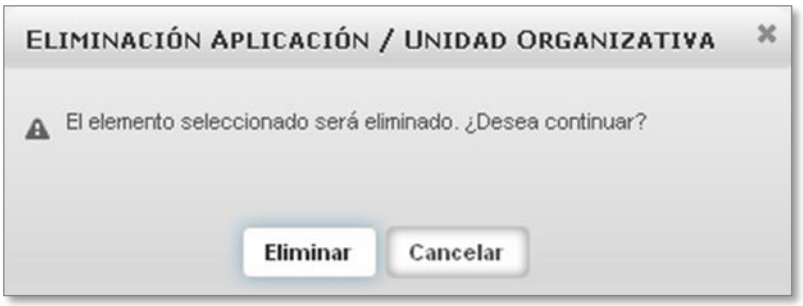


Figura 91 - Confirmación Eliminación Aplicación

Una vez confirmado, se eliminará la aplicación de la plataforma.

5.3.4.8 Sincronización del árbol de unidades organizativas y aplicaciones con DIR3

Para sincronizar todo el árbol de unidades organizativas y aplicaciones con DIR3, la plataforma debe tener definido el modo de integración con DIR3 como relajado o estricto, en las propiedades configurables definidas para ello en la Gestión de la Configuración. Este tipo de sincronización afecta a todas las unidades organizativas y aplicaciones almacenadas en el sistema, de manera que sus datos se actualizarán en base a los definidos en DIR3 en función del modo de integración seleccionado.

En cualquier caso, se actualizarán los datos de las unidades organizativas cuyo tipo de identificador sea *DIR3*, de modo que su identificador es/coincide con uno existente en *DIR3*, se actualiza su información asociada, e incluso se crea la jerarquía de unidades organizativas que debe contenerla, moviendo todas las subunidades organizativas y aplicaciones a la nueva estructura si fuera necesario. En el caso de estar establecido el modo de integración estricto, todas aquellas unidades organizativas con un tipo de identificador *LIBRE* serán eliminadas (así como toda la jerarquía por debajo de estas), ocurriendo lo mismo para aquellas unidades organizativas que tengan definido un identificador de tipo *DIR3* pero dicho identificador no se encuentre registrado en *DIR3*.

Para llevar a cabo el proceso se debe pulsar sobre el botón  ubicado en la ventana principal de la Gestión de Aplicaciones.

La primera vez que se realiza una sincronización con *DIR3* esta se hace de forma completa, por lo que debe obtener una gran cantidad de datos, pudiendo elevar el tiempo de respuesta del servicio web hacia DIR3 (configurable/modificable en las propiedades configurables definidas para ello en la Gestión de la Configuración) y el tiempo de procesamiento de toda la información. Además, si la plataforma está funcionando en clúster, al final del proceso siempre se realiza una recarga de la caché en todo el clúster. Una vez realizada la primera sincronización, las posteriores se realizan siempre de forma incremental, siendo mucho más rápido el proceso.

IMPORTANTE: La sincronización con DIR3 (ya sea en modo de integración relajado o estricto, aunque con mayores consecuencias en el segundo caso) implica cambios en la jerarquía de unidades organizativas y aplicaciones, por lo que se recomienda generar siempre de forma previa una configuración estable a modo de copia de seguridad (apartado 5.3.14.3).

5.3.4.9 Mover elementos del árbol



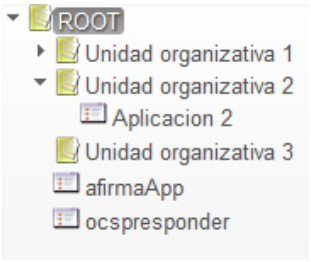
Para mover elementos del árbol de aplicaciones (unidades organizativas o aplicaciones) debemos seleccionar en el árbol aquel nodo que queramos mover y luego pulsar el botón “Mover elemento del árbol”. Nos aparecerá una nueva ventana que nos permite elegir el lugar al que queremos mover el elemento seleccionado.



Figura 92 - Interfaz mover elemento

- **Buscar por ruta**

  Debemos introducir manualmente la ruta destino completa, usando "." Como separador. Por ejemplo, dado el siguiente árbol:



  Si quisiésemos mover la *Aplicación 2* a la *Unidad Organizativa 1, d*eberíamos escribir "*ROOT.Unidad organizativa 1*" y pulsamos en el botón "Comprobar la ruta introducida" para verificar si la ruta es correcta o no. Una vez obtenemos el mensaje de confirmación de "Ruta válida", pulsamos sobre el botón de confirmar y los cambios se realizarían.

- **Buscar por Árbol**

  Para buscar por árbol debemos pulsar sobre el botón "Buscar por árbol". Nos aparecerá una pequeña ventana con el árbol de aplicaciones.

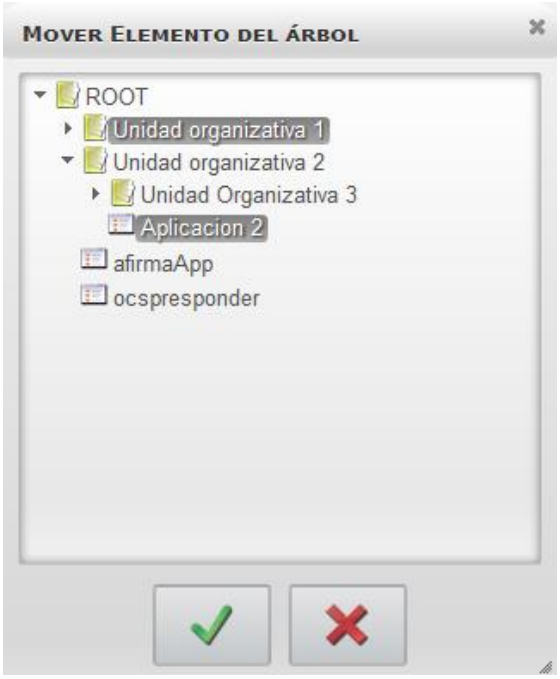


Figura 93 - Interfaz de Gestión de Usuarios (I)

Seleccionamos el elemento del árbol que deseemos y pulsamos en confirmar. Si el elemento es válido, la ventana se cerrará y nos aparecerá la nueva ruta en la ventana anterior.



Figura 94 - Interfaz de Gestión de Usuarios (II)

Para terminar el proceso, pulsamos en el botón de confirmar.

NOTA: El botón de mover elemento aparecerá deshabilitado en el nodo root, ya que éste jamás podrá moverse. Por otro lado, hay que tener en cuenta que no se pueden mover elementos a aplicaciones, por lo que, si elegimos una aplicación como destino, el sistema no permitirá la operación y se mostrará un mensaje de error.

5.3.5 Gestión de Usuarios

La gestión de usuarios consiste en administrar aquellos usuarios que participan en la administración, monitorización o auditoria de la plataforma. Esta gestión sólo podrá llevarse a cabo por los administradores de la plataforma.

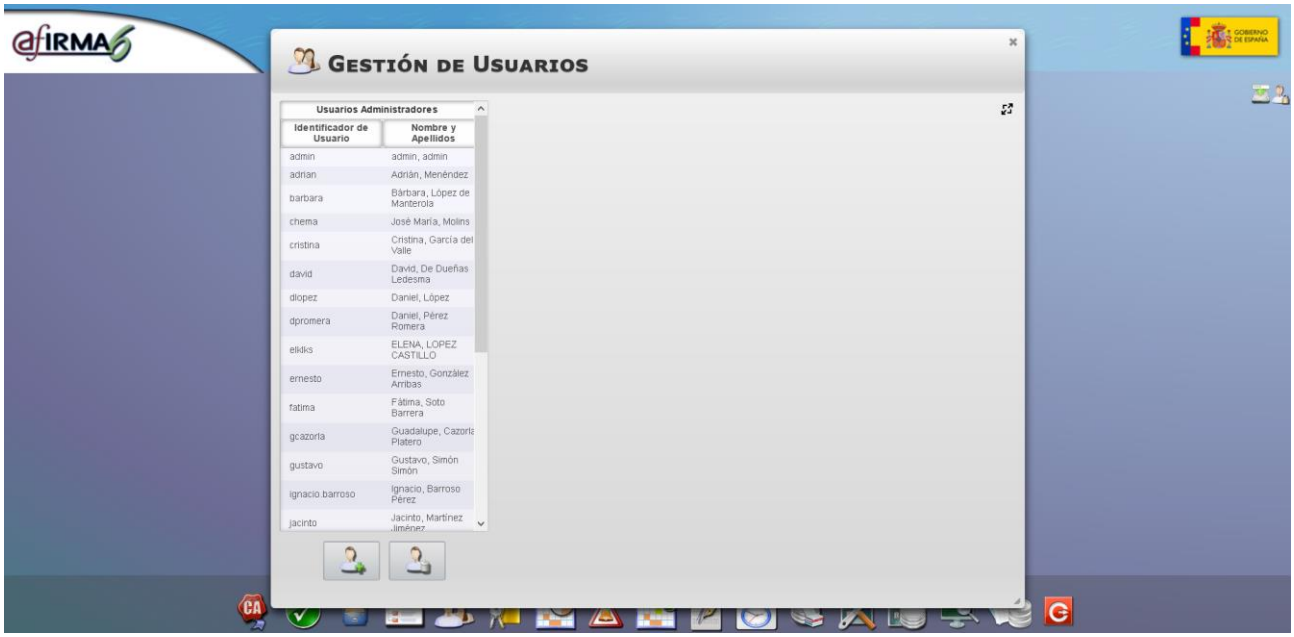


Figura 95 - Interfaz de Gestión de Usuarios

Cuando se da de alta un usuario en la plataforma, el usuario posee perfil de Administrador. Pudiendo asignarle también permisos para acceder a la aplicación de la administración delegada.

Las operaciones que puede realizar un administrador de la plataforma mediante este componente del módulo de administración son:

- Alta de usuario.
- Modificación de usuario.
- Baja de usuario.

5.3.5.1 Alta de Usuario



Mediante esta operación se añade un nuevo usuario a la plataforma @firma. Para ello, debemos acceder al interfaz de gestión de usuarios y pulsar el botón “Alta Usuario”.

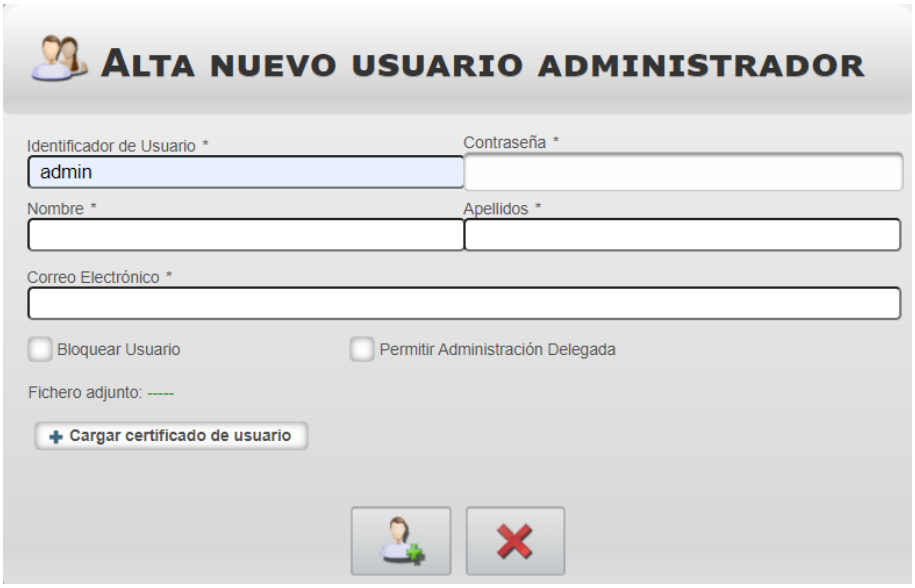


Figura 96 - Interfaz de Gestión de Usuarios: Alta de usuario

En la pantalla de alta de usuario se deben completar los siguientes datos:

- **Identificador de Usuario** (Login): nombre de usuario en la plataforma para el nuevo usuario.
- **Contraseña**: clave de acceso del nuevo usuario en la plataforma. La contraseña a establecer debe cumplir la expresión regular definida en el módulo de configuración – control del usuario (apartado 5.3.13.1.2).
- **Nombre**: nombre del nuevo usuario. Es necesario indicarlo correctamente para la autenticación por certificado del usuario.
- **Apellidos**: apellidos del nuevo usuario. Es necesario indicarlo correctamente para la autenticación por certificado del usuario.
- **Correo Electrónico**: dirección de correo electrónico del nuevo usuario.
- **Bloquear usuario:** Si se desea bloquear la entrada del usuario en la plataforma.
- **Permitir Administración Delegada:** Indica que el usuario puede ser Administrador de la aplicación de Administración Delegada.
- **Cargar certificado de usuario:** certificado digital mediante el cual podrá acceder a la plataforma.

5.3.5.2 Modificación de Usuario



Mediante esta operación se actualizan los datos de un usuario de la plataforma. Los datos susceptibles de ser actualizados son el nombre y apellidos del usuario, el e-mail y los roles que desempeña. Adicionalmente, se pude bloquear o desbloquear el usuario mediante el *check* correspondiente.

Para realizar una modificación de datos de usuario es necesario seleccionar un usuario de la lista de usuarios registrados que se muestra en la parte izquierda del interfaz. Al seleccionar el usuario se mostrarán sus datos, los cuales podrán ser actualizados.

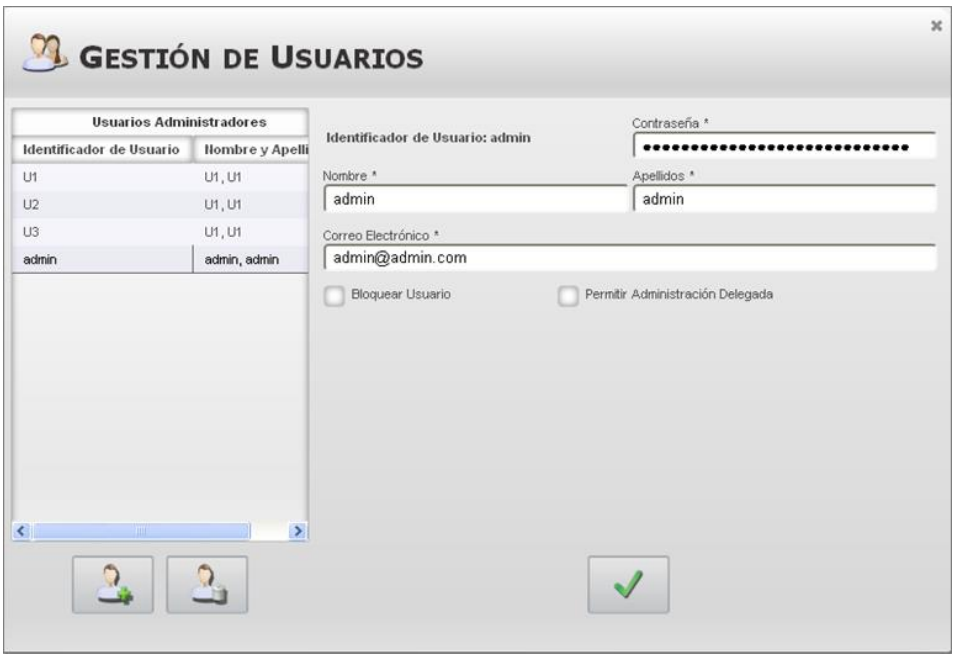


Figura 97 - Interfaz de Gestión de Usuarios. Modificación de Usuarios (I)

Una vez actualizados sus datos y tras pulsar “Modificar”, aparecerá una ventana de confirmación.



Figura 98 - Interfaz de Gestión de Usuarios. Modificación de Usuarios (II)

Tras confirmar, los cambios quedarán registrados.

5.3.5.3 Baja de Usuario



Para eliminar un usuario registrado de la plataforma es necesario posicionarse sobre el usuario que se desea borrar en la lista de usuarios. En este momento se mostrarán los datos del usuario en la zona central del interfaz.

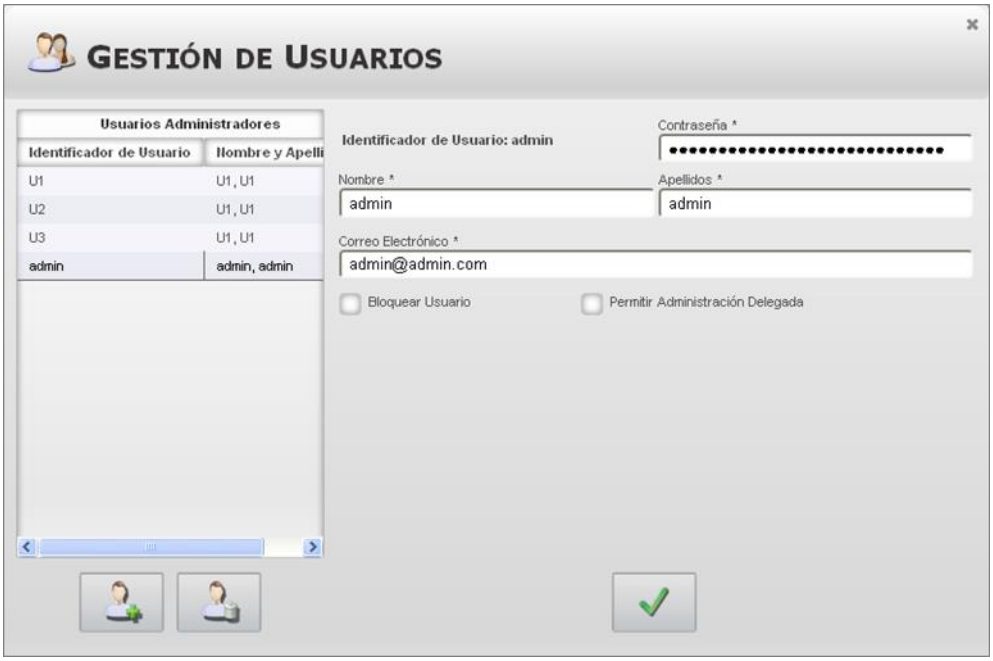


Figura 99 - Interfaz de Gestión de Usuarios: Baja de Usuario

Ahora es necesario pulsar el botón “Eliminar usuario”. Hecho esto, la plataforma solicita la confirmación por parte del usuario.

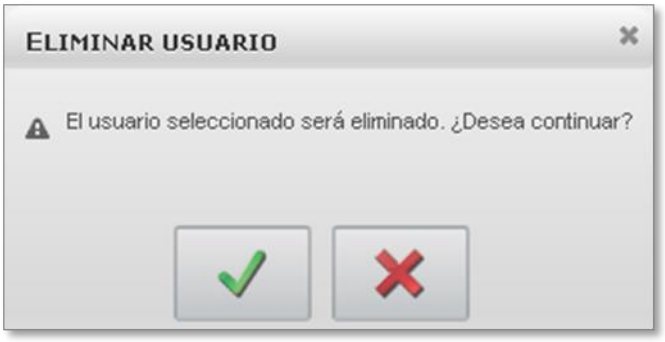


Figura 100 - Confirmación de Borrado de Usuario

Por último, la plataforma lo elimina y muestra un mensaje indicando que la operación se ha realizado correctamente.

5.3.6 Gestión de Keystores

Un keystore es, básicamente, un almacén que pueden contener claves privadas y certificados públicos X.509 v3. Los keystores se encuentran securizados por contraseñas que serán especificadas en la gestión de contraseñas.

En el árbol del módulo de gestión de keystores aparecen dos nodos principales: Almacén de Certificados y Almacén de Par de Claves. Estos dos nodos diferencian los keystores que contendrán únicamente certificados de los que contendrán el certificado y su clave privada asociada.

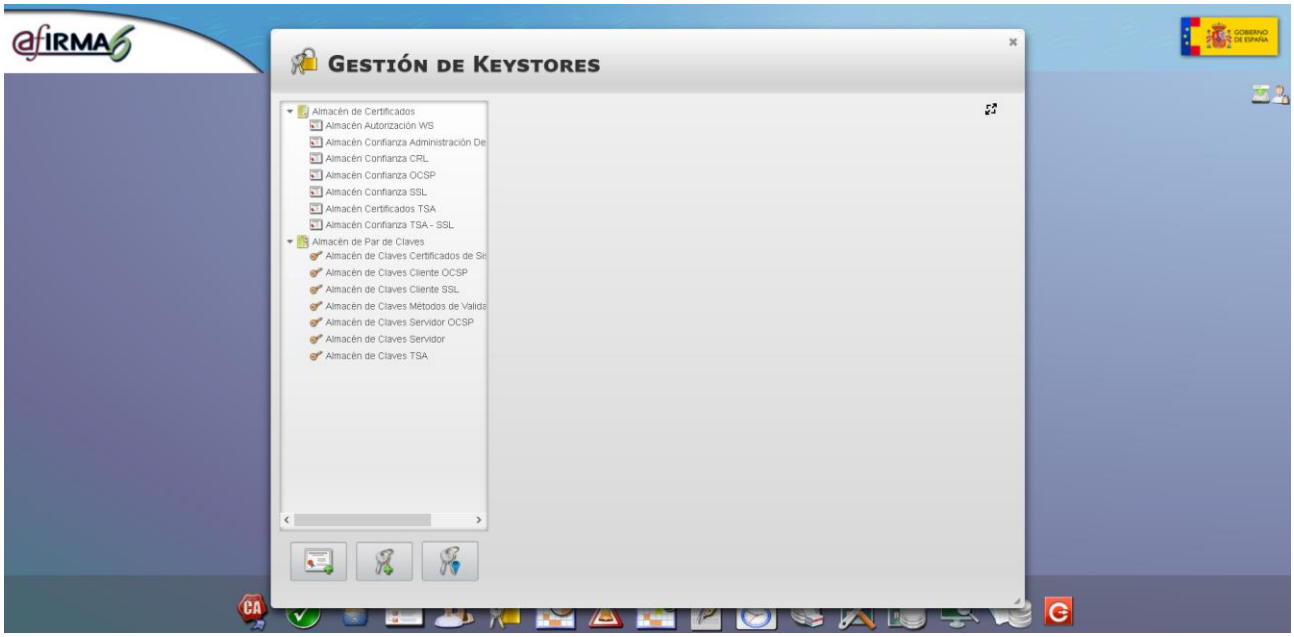


Figura 101 - Interfaz de Gestión de Keystores

La plataforma emplea estas claves criptográficas para proporcionar funciones de integridad, confidencialidad y autenticación, por lo que el uso no autorizado, la modificación o sustitución podría causar la pérdida de seguridad.

Las operaciones que pueden llevarse a cabo desde la interfaz podrían dividirse en dos grupos:

- Operaciones Críticas:
  - Importar certificado.
  - Importar par de claves.
  - Modificar la clave de acceso a un almacén.
  - Modificar la localización de un almacén.
- Operaciones No Críticas:
  - Modificar alias.
  - Eliminar certificado.
  - Eliminar par de claves.
  - Modificar situación de archivado.

Las operaciones críticas requerirán de las credenciales del usuario para su autorización.



Figura 102 - Interfaz de Autorización a Operación Crítica

5.3.6.1 Keystores

Los keystores no se pueden dar de alta o baja mediante la herramienta de administración, sino que ya se encuentran definidos por la plataforma previamente. Los keystores en la administración, aparecen divididos en dos grandes grupos:

- **Almacenes de Certificados:** Estos almacenes contendrán únicamente certificados (partes públicas). Los almacenes que componen este grupo son:

  - **Almacén Autorización WS.** Contiene los certificados en los que confiará el sistema cuando reciba una petición SOAP securizada por el método "BinarySecurityToken". Si una aplicación intenta realizar una petición a la plataforma y el certificado utilizado para securizar el mensaje no se encuentra presente en dicho almacén, se devolverá el error correspondiente. Así mismo, en este almacén se incluyen los certificados de confianza para las peticiones OCSP recibidas por la plataforma.

  - **Almacén Confianza Administración Delegada.** Contiene el/los certificado/s utilizado/s por la Administración Delegada para asegurar mediante WSS los mensajes que intercambiará con la plataforma central @Firma.

  - **Almacén Confianza CRL.** Contiene los certificados de CA en los que debe confiar la plataforma como emisores de CRL. Al validar cualquier CRL, el sistema verificará si el certificado del emisor de la misma se encuentra en el almacén de confianza. Si no es así, se rechazará la CRL por motivos de seguridad.

  - **Almacén Confianza OCSP.** Contiene los certificados de CA en los que debe confiar la plataforma como emisores (firmantes) de respuestas OCSP. Al validar una respuesta OCSP, el sistema verificará si el certificado del firmante de la misma se encuentra en el almacén de confianza. Si no es así, se rechazará la respuesta por motivos de seguridad.

  - **Almacén Confianza SSL.** Contiene los certificados en los que confiará la plataforma para las conexiones SSL contra servidores de terceros.

  - **Almacén Certificados TSA.** Contiene los certificados con los que validar las respuestas firmadas que proceden de las plataformas TSA dadas de alta.

  - **Almacén Confianza TSA-SSL.** Contiene los certificados utilizados para la comunicación mediante SSL y HTTPS con las plataformas TSA dadas de alta.

- **Almacén de Par de Claves:** Estos almacenes contendrán únicamente certificados junto con su clave privada. Los almacenes que componen este grupo son:

- **Almacén de Claves Certificados de Sistema.** Contiene las claves privadas que utilizará el sistema para realizar procesos internos como pueden ser el firmado de logs, comunicaciones con componentes internos, etc.

- **Almacén de Claves Cliente OCSP.** Contiene las claves privadas que utilizará la plataforma para realizar la firma de las peticiones OCSP al exterior.

- **Almacén de Claves Cliente SSL.** Contiene las claves privadas con las que se llevarán a cabo las operaciones de identificación como cliente en una conexión SSL mutua necesarias para el método de validación histórica. Dentro de la configuración de cada método se podrá seleccionar uno de los certificados contenidos en este almacén.

- **Almacén de Claves Métodos de Validación SOAP.** Contiene las claves privadas con las que se securizarán los mensajes SOAP (mediante WSS) realizadas a otras plataformas @Firma para consultar el estado de revocación de certificados. Las claves contenidas en este almacén aparecerán disponibles en la pantalla de Alta y Modificación de métodos de validación SOAP.

- **Almacén de Claves Servidor OCSP.** Contiene las claves privadas que utilizará el Servidor OCSP para firmar las respuestas. **Atención:** para poder utilizar los certificados contenidos en este keystore para la firma de respuestas OCSP es imprescindible que sus cadenas de certificación estén dadas de alta como Prestadores de confianza de la plataforma. Para más información sobre el proceso de alta véase el apartado Alta de PSC en este mismo documento.

- **Almacén de Claves Servidor.** Contiene las claves privadas con las que se van a llevar a cabo las operaciones de firma requeridas por las aplicaciones integradas. En la gestión de aplicaciones se pueden especificar los certificados que van a tener disponibles cada una de las aplicaciones dadas de alta en la plataforma.

- **Almacén de Claves TSA.** Contiene las claves privadas con las que se firmarán las peticiones SOAP a las plataformas TSA cuando la autenticación definida sea por certificado, así como las claves privadas utilizadas para la autenticación cliente para la comunicación HTTPS con las plataformas TSA cuando la autenticación cliente sea requerida.

NOTA: Desaparece de la administración (respecto a versiones anteriores a la 6.2 de la plataforma) el almacén de Tipos de Certificado desde el módulo de Gestión de Keystores, ya que las operaciones asociadas se pueden realizar desde el módulo de PSC / subPSC / Tipos de certificado. Del mismo modo también desaparece la gestión del almacén de plataformas federadas ya que en la versión 6 deja de existir el concepto de plataformas federadas. Por último, a partir de la versión 6.4 de la plataforma, desaparece el Almacén de PSCs ya que éste puede ser gestionado desde el módulo de PSC.

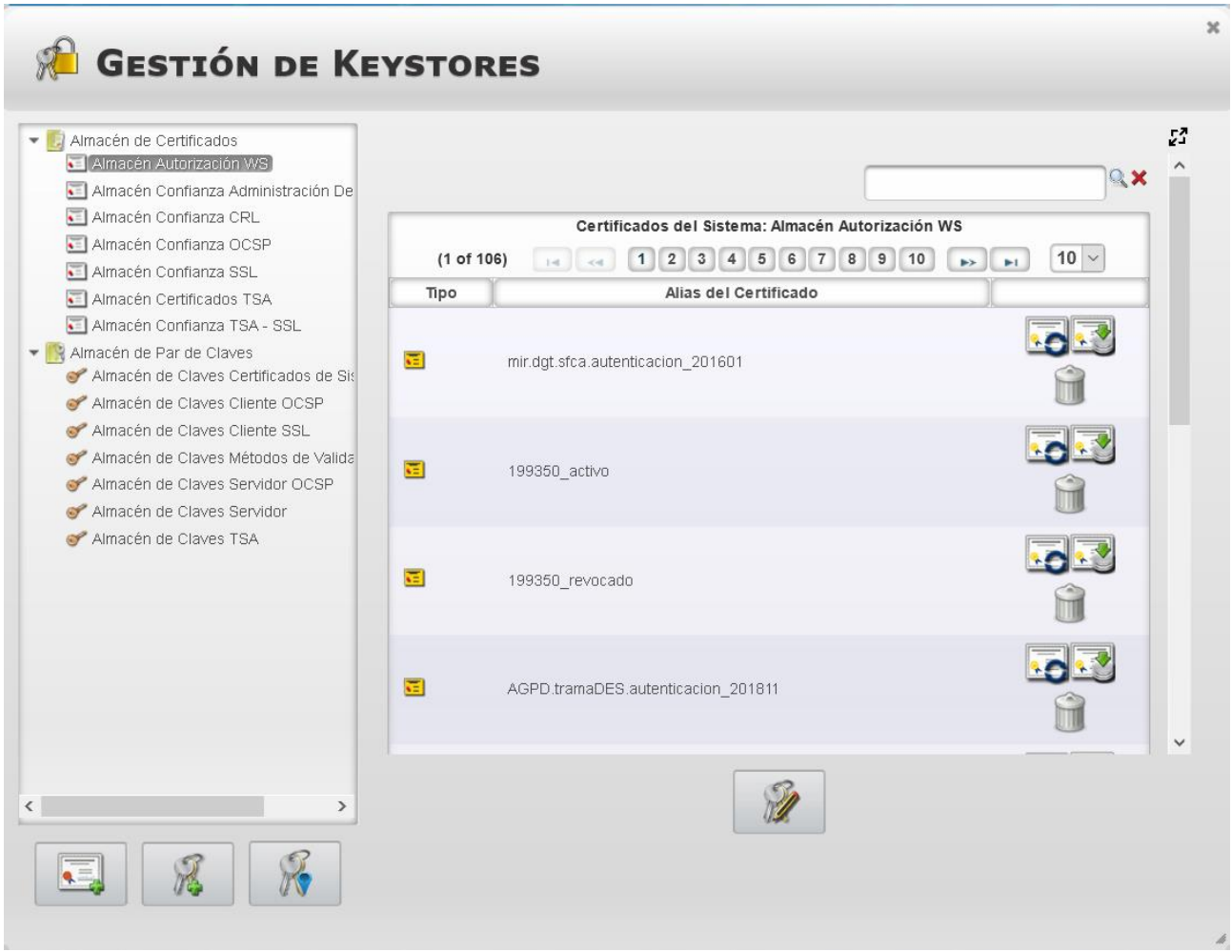


Figura 103 - Interfaz de Gestión de Keystores (Selección de un Almacén de Certificados)

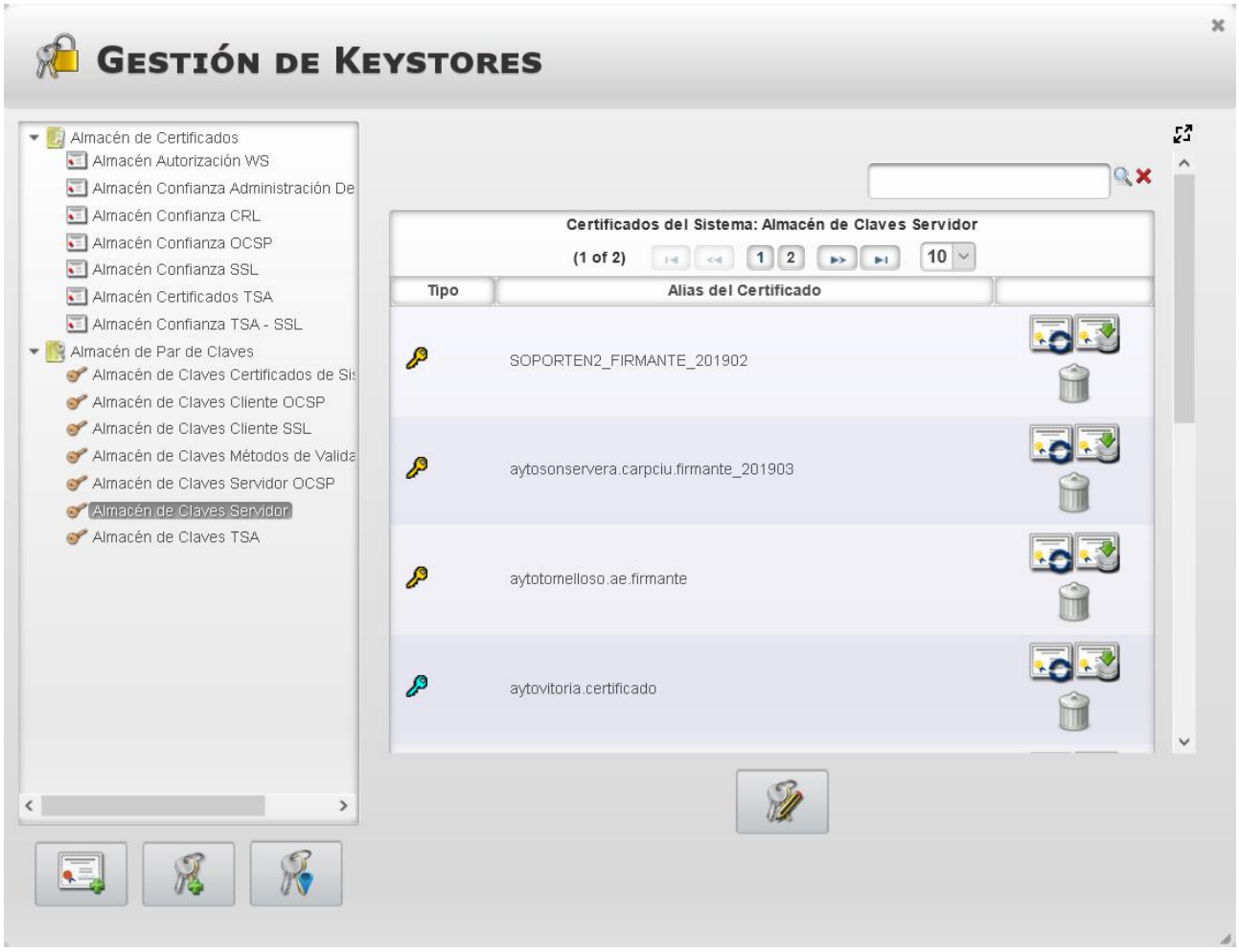


Figura 104 - Interfaz de Gestión de Keystores (Selección de un Almacén Par de Claves)

Al seleccionar un keystore, se muestra en la parte derecha de la pantalla su contenido distribuido en una tabla donde se indica:

- **Tipo**: Puede mostrar una o dos imágenes. La primera de ellas indica lo que está almacenado, así como su estado. La forma del icono identificará si se trata de una clave privada almacenada en un almacén de claves de tipo hardware (HSM), de una clave privada almacenada en un almacén de claves de tipo software, o de un certificado, y su color definirá su estado. Así para una clave privada almacenada en un almacén de claves de tipo hardware:



Válido



Caducado



Revocado


Otro


No existe


Aún no válido

En el caso de una clave privada almacenada en un almacén de claves de tipo software:


Válido


Caducado


Revocado


Otro


No existe


Aún no válido

En el caso de un certificado:


Válido


Caducado


Revocado


Otro


No existe


Aún no válido

La segunda imagen indicará si está archivado o no. Es decir, si la entrada posee el icono  indicará que se encuentra archivado. El concepto de archivado es sólo aplicable a los certificados almacenados en el Almacén de Confianza CRL y en el Almacén de Confianza OCSP. **Si un certificado se encuentra archivado no formará parte de los procesos (tareas) internos de validación de certificados**:

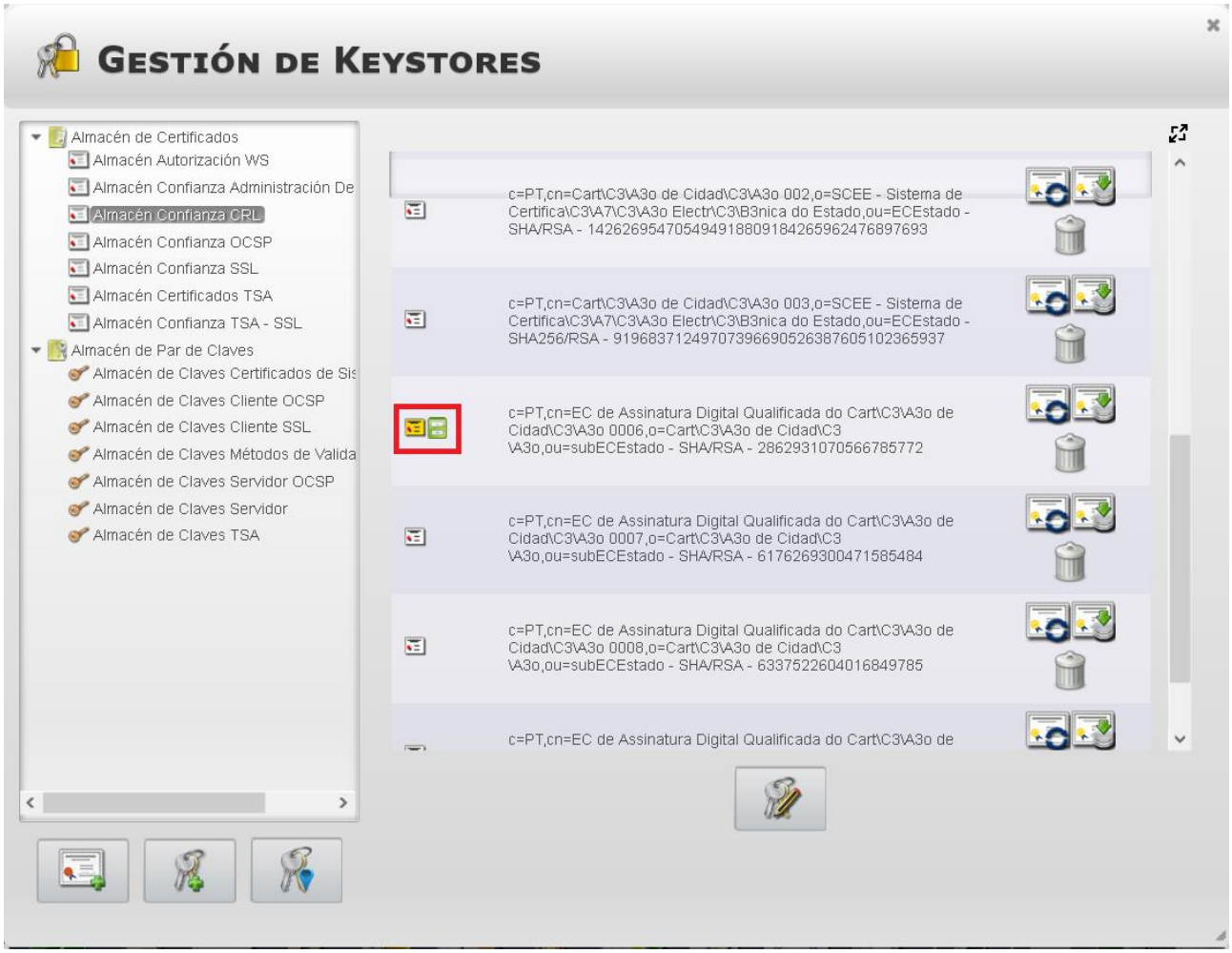


Figura 105 – Interfaz de Gestión de Keystores (Selección de un Almacén de Certificados con Certificado Archivado)

- **Alias**: Alias del certificado.

- **Editar**: En el caso de que el elemento (certificado o clave privada) pueda ser editado, se mostrará el botón . Al pulsar sobre él se accederá a la ventana de datos del elemento, donde se podrá editar su alias. Además, si el elemento, en este caso certificado, está almacenado en el Almacén de Confianza CRL o en el Almacén de Confianza OCSP, podrá establecerse como archivado o no.

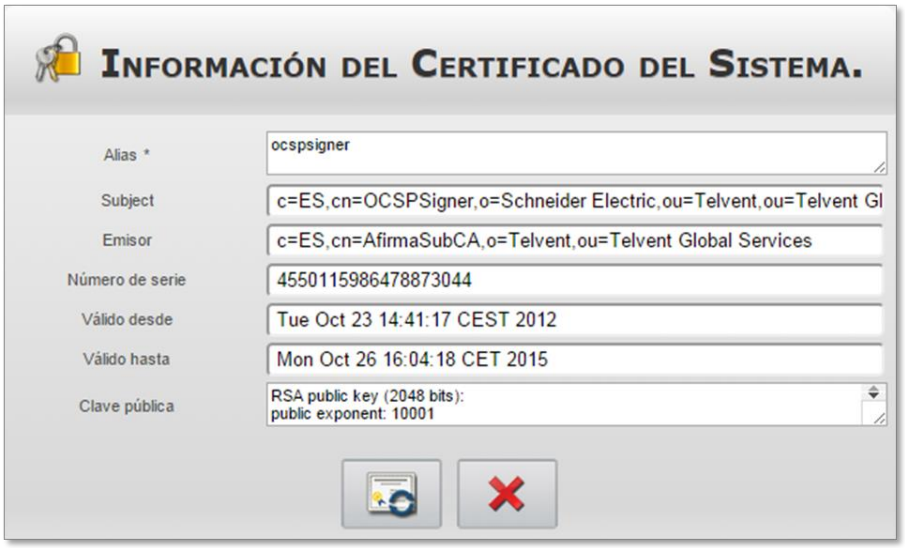


Figura 106 - Interfaz de Gestión de Keystores (Edición de Certificado sin Archivado)



Figura 107 - Interfaz de Gestión de Keystores (Edición de Certificado con Archivado)

Hay que tener en cuenta que los alias de los certificados constituyen una información sensible y puede afectar a la configuración de la plataforma. A continuación, se muestra el listado de almacenes, junto con una indicación sobre el hecho de editar su alias:

- **Almacén Autorización WS:** Se pueden modificar los alias de los certificados.
- **Almacén Confianza Administración Delegada:** Se pueden modificar los alias de los certificados.

- **Almacén Confianza CRL:** No se deben modificar los alias de los certificados ya que afecta directamente al funcionamiento del sistema. Se permite su modificación para aquellos que se desee mantener una copia sin que puedan ser usados funcionalmente.
- **Almacén Confianza OCSP:** Se pueden modificar los alias de los certificados.
- **Almacén Confianza SSL:** Se pueden modificar los alias de los certificados.
- **Almacén Certificados TSA:** Se pueden modificar los alias de los certificados.
- **Almacén Confianza TSA – SSL:** Se pueden modificar los alias de los certificados.
- **Almacén de claves Certificados de Sistema:** En caso de modificar el alias de alguna clave privada, hay que tener en cuenta que si se trata de uno de las especificados en "Configuración > Configuración de Propiedades > Alias de Certificados", hay que actualizar estas propiedades. Se aconseja no realizar modificaciones en los alias de este almacén.
- **Almacén de Claves Cliente OCSP:** Se pueden modificar los alias de las claves privadas.
- **Almacén de Claves Cliente SSL:** Se pueden modificar los alias de las claves privadas.
- **Almacén de Claves Métodos de validación SOAP:** Se pueden modificar los alias de las claves privadas.
- **Almacén de Claves Servidor OCSP:** Se pueden modificar los alias de las claves privadas.
- **Almacén de Claves Servidor:** Se pueden modificar los alias de las claves privadas.
- **Almacén de Claves TSA:** Se pueden modificar los alias de las claves privadas.

Sobre la tabla de resultados se ubica un cuadro de entrada de texto que permite buscar certificados por alias. Así pues, una vez introducido el texto a usar como patrón de búsqueda, al pulsar sobre el botón  se procederá a mostrar en la lista de resultados aquellos certificados cuyo alias contengan el texto indicado. Para eliminar el filtro indicado se deberá pulsar sobre el botón .

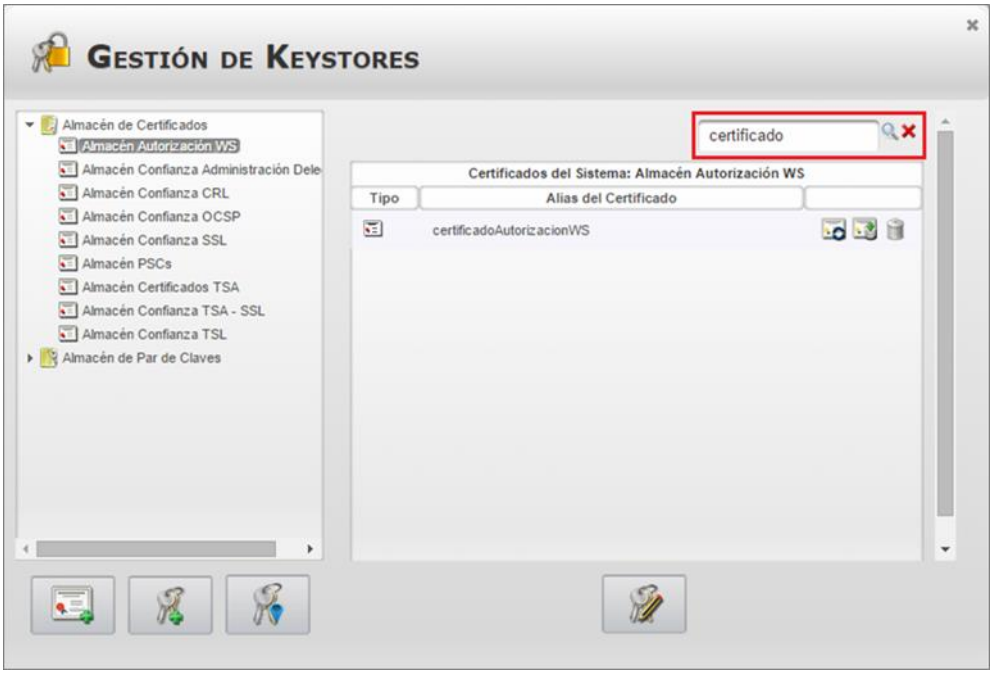


Figura 108 - Interfaz de Gestión de Keystores (Búsqueda de Elemento por Alias)

5.3.6.1.1 Importar Certificados



La opción de importar certificados permite importar un certificado X.509 v3 en un keystore. Para importar un certificado, se debe pulsar sobre el botón de añadir Certificado situado en la parte inferior del árbol de Almacenes. Tras pulsar el botón se pedirá al administrador que introduzca su contraseña como medida de seguridad.

Una vez validada la contraseña del usuario logado, y en caso de que sea correcta, se visualizará el panel de importación.



Figura 109 - Diálogo de Importación de Certificado en Keystore

Los campos que el usuario ha de introducir son:

- **Almacén.** Puesto que estamos dando de alta un certificado en el grupo de Almacenes de Certificados, deberemos de seleccionar del combo desplegable el almacén donde queremos darlo de alta.

- **Alias.** Alias que poseerá el certificado en el almacén (no definible para el caso de seleccionar el almacén de confianza de CRL).

- **Certificado a dar de alta.**

Para finalizar la importación, se debe pulsar el botón de alta.

NOTA: En el navegador Internet Explorer 10 la importación de certificados no funciona correctamente ya que existe un bug conocido en la librería de componentes PrimeFaces utilizada por la plataforma.

5.3.6.1.2 Importar Par de Claves



La opción de importar un par de claves permite importar una clave privada, así como su certificado X.509 v3 en un keystore. Para importar un par de claves, se debe pulsar sobre el botón de alta de par de claves situado en la parte inferior del árbol de almacenes. Tras pulsar el botón se pedirá al administrador que meta su contraseña como medida de

seguridad. Una vez validada la contraseña del usuario logado, y en caso de que sea correcta, se visualizará el panel de importación.



Figura 110 - Diálogo Importación Par de Claves (I)

- **Almacén.** Puesto que estamos dando de alta un par de claves en el grupo de Almacenes de Par de claves, deberemos de seleccionar del combo desplegable el almacén donde queremos darlo de alta.

- **Contenedor con el certificado y el par de claves asociado.**

- **Contraseña de acceso al contenedor**

Una vez introducida la información en el formulario, y tras pulsar el botón siguiente, aparecerá una lista con los pares de claves contenidos en el fichero adjuntado a dar de alta.

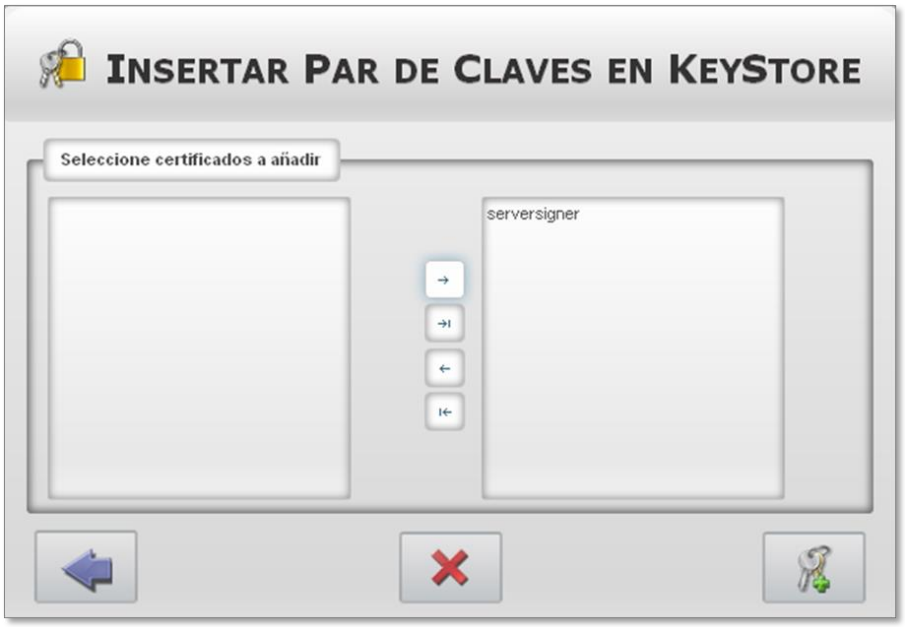


Figura 111 - Diálogo Importación Par de Claves (II)

En el lado izquierdo aparecerá el listado de pares de cables contenidas en el almacén cargado. Debe seleccionarse y pasar al lado derecho aquella que se desee dar de alta.

5.3.6.1.3 Gestionar Ubicación de Almacén de Claves



Gestionar la ubicación de un almacén de claves consiste en definir cuál será la localización del mismo. @firma permite definir la localización únicamente de los almacenes de pares de claves. Las localizaciones se dividen en:

- Software: Los pares de claves son almacenados en BBDD.
- Hardware Con Respaldo: Los pares de claves son almacenados en un HSM y en BBDD.
- Hardware Sin Respaldo: Los pares de claves son almacenados en un HSM.

El HSM es de uso común para todos los almacenes de pares de claves, es decir, todo almacén de claves definido como Hardware almacenará sus pares de claves en el mismo HSM.

Una vez pulsado sobre el botón arriba definido el sistema solicitará la contraseña del usuario logado. Tras comprobar su validez se mostrará la ventana con la ubicación de los almacenes de pares de claves:



Figura 112 - Gestión de Ubicación de Almacenes de Pares de Claves

Para cada almacén de pares de claves se mostrará su localización (Software o Hardware), si posee respaldo ( ) o si no posee respaldo ( ). El botón de la última columna ( ) permite cambiar los parámetros antes descritos, dando acceso a una nueva ventana:



Figura 113 - Definir Ubicación Almacén de Pares de Claves (Software)



Figura 114 - Definir Ubicación Almacén de Pares de Claves (Hardware)

En función del tipo seleccionado (Software o Hardware) se mostrará la opción de seleccionar Con Respaldo o no.

Si un almacén de tipo Software se define de tipo Hardware Con Respaldo, todos los pares de claves almacenados en BBDD serán importados al HSM (en caso de que no se encuentren importados previamente), y los futuros pares de claves que sean importados al HSM serán almacenados también en BBDD para que, en caso de que se produzca un problema de acceso al HSM y un par de claves no sea accesible, se utilizará el acceso a la BBDD para rescatarlo.

Si un almacén de tipo Software se define de tipo Hardware Sin Respaldo, todos los pares de claves almacenados en BBDD serán importados al HSM (en caso de que no se encuentren importados previamente), y los futuros pares de claves serán importados únicamente en el HSM. Debe tenerse en cuenta que, por la naturaleza del propio HSM, los pares de claves almacenados en el mismo no pueden ser exportados, por lo que un almacén de claves definido de tipo Hardware Sin Respaldo ya no podrá ser definido de tipo Software en el futuro.

Si un almacén de tipo Hardware Con Respaldo se define de tipo Software, todos los pares de claves serán almacenados en BBDD y dejará de hacerse uso del HSM.

Si un almacén de tipo Hardware Con Respaldo se define como Hardware Sin Respaldo, todos los pares de claves asociados almacenados en BBDD serán eliminados, de manera que no existirán como método de respaldo en caso de problema de acceso al HSM. Para llevar a cabo esta operación, será necesaria la confirmación por parte del usuario:



Figura 115 - Diálogo Confirmación para Almacén de Claves Hardware Sin Respaldo

Si un almacén de tipo Hardware Sin Respaldo se define como Hardware Con Respaldo, los futuros pares de claves que sean importados al HSM serán almacenados también en BBDD para que, en caso de que se produzca un problema de acceso al HSM y un par de claves no sea accesible, se utilizará el acceso a la BBDD para rescatarlo.

5.3.6.1.4 Modificar clave Almacén



Una novedad incluida en la versión @Firma 6.4 es la de modificar la clave del almacén de certificados / par de claves. Para ello se debe de seleccionar el Almacén cuya clave se desea modificar y pulsar sobre el botón de modificar.

Una vez pulsado el botón de modificar, el sistema pedirá la contraseña del usuario logado. Tras comprobar su validez, aparecerá la ventana de cambio de contraseña.

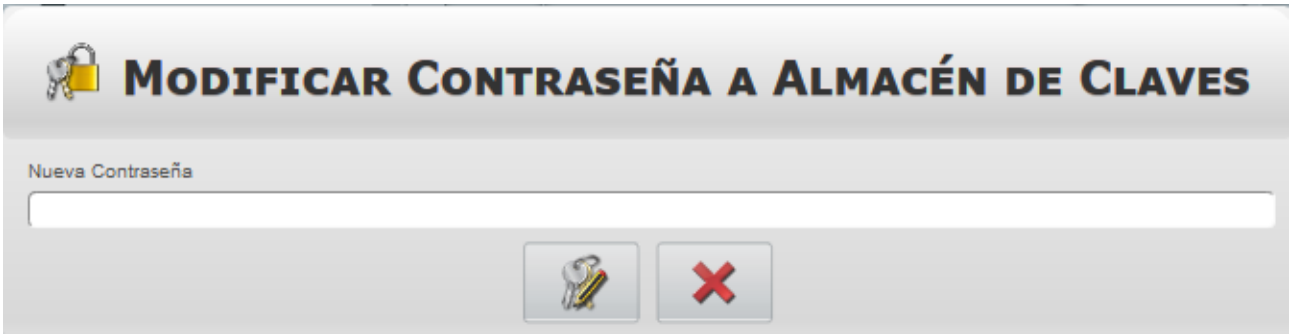


Figura 116 - Cambio de Contraseña de Almacén de Claves

5.3.7 Gestión de Tareas

Se entiende por tarea una operación que se ejecuta en un determinado instante de tiempo. En la plataforma existen dos tipos de tareas:

- **Tareas no críticas** (***Nodo Tareas***). Se entiende como aquellas que pueden ser eliminadas del gestor de tarea sin afectar al funcionamiento de la plataforma.
- **Tareas críticas** (***Nodo Tareas del sistema***). Se recogen aquellas tareas que no pueden ser eliminadas del gestor de tareas debido a su criticidad.

Cuando se selecciona la opción Gestión de Tareas, aparece una ventana dividida verticalmente en dos. En la parte izquierda puede verse la lista de tareas disponibles y, seleccionando cualquiera de las tareas, se pueden ver los datos de la misma en la parte derecha de la ventana.

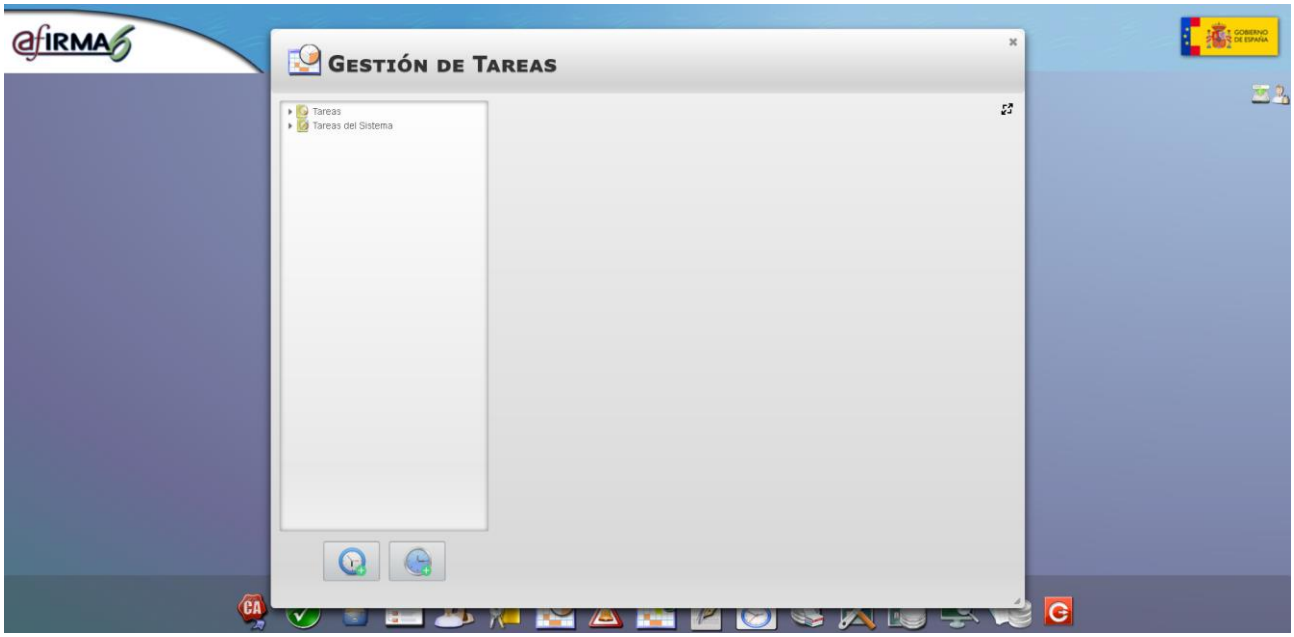


Figura 117 - Ventana de Gestión de Tareas

5.3.7.1 Tareas no críticas

Las tareas no críticas, en adelante, tareas, se pueden dividir en dos grupos:

- **Tareas de Validación:** Son aquellas que permiten validar el estado de caducidad y el estado de revocación de los certificados almacenados en los distintos almacenes de claves definidos en la plataforma.

- **Tareas Estándar:** Cualquier otra tarea ajena a la validación del estado de caducidad y del estado de revocación de los certificados almacenados en los distintos almacenes de claves definidos en la plataforma, como, por ejemplo, la tarea preconfigurada que comprueba si los certificados de los almacenes que elijamos están caducados o revocados.

Toda tarea, independientemente del tipo al que pertenezca, debe tener asociado al menos un planificador que defina el momento de ejecución de la misma. Una tarea puede tener tantos planificadores como se desee para así poder ejecutarse en diversos momentos, pero si carece de planificadores, dicha tarea no será ejecutada. Los planificadores se definen de tres tipos:

- **Periódico:** Planificador que permite la ejecución de una tarea repetidamente cada cierto tiempo, especificado como el periodo del mismo.

- **Diario:** Planificador que constituye la especialización de un planificador periódico. Permite la ejecución de una tarea una vez cada 24 horas a partir de la fecha definida para el mismo.

- **Por Fecha:** Planificador que permite la ejecución de una tarea únicamente en la fecha definida.

5.3.7.1.1 Alta de Tarea Estándar



Para crear una tarea estándar, el usuario debe pulsar el botón situado en la parte inferior a la izquierda y que está etiquetado como ***"Añadir Tarea"***. Una vez pulsado, se mostrará una ventana en la que se pueden establecer los datos de la tarea:



Figura 118 - Gestión de Tareas - Alta de Tarea Estándar

Los campos que componen una tarea estándar son:

- **Nombre:** Cadena de texto que identifica unívocamente a la tarea. Debe ser un nombre que no coincida con el de otra tarea existente previamente.

- **Clase de Implementación:** Nombre completa de la clase Java que constituye la implementación de la tarea. Dicha tarea debe extender la clase abstracta ***es.gob.afirma.mplanificacion.Task***.

- **Tipo Planificador:** Tipo de planificador asociado por defecto a la tarea. Constituye una lista en la que seleccionar el tipo, esto es, ***Periódico***, ***Diario*** o ***Por Fecha***.

- **Periodo:** Periodo de ejecución de la tarea asociado al planificador. Sólo aplicable para el planificador de tipo ***Periódico***.

- **Inicio:** Fecha de inicio para la ejecución de la tarea asociada al planificador.

Los campos indicados con un asterisco serán obligatorios. Para crear la tarea se debe pulsar sobre el botón ✓ y para cancelar el proceso se debe pulsar sobre el botón ✗. Una vez completado el proceso, en el árbol de tareas, aparecerá el nodo asociado a la nueva tarea.

5.3.7.1.2 Edición de Tarea Estándar

Para editar una tarea estándar se debe acceder a los datos de la misma pulsando sobre el nodo con su nombre en el árbol de tareas:



Figura 119 - Gestión de Tareas - Datos de Tarea Estándar

En la zona inferior de la ventana de datos de la tarea se indica un listado con los planificadores asociados. La lista de planificadores se compone de 4 columnas:

- **Tipo:** Tipo de planificador a utilizar en la ejecución de la tarea.

- **Inicio:** Fecha de inicio en la ejecución de la tarea.
- **Periodo:** Horas, minutos y segundos que componen el periodo respecto al cual se ejecutará la tarea.
- **Acciones:** La cuarta columna carece de descripción, pero ofrece tres acciones relacionadas con los planificadores en función del icono que presente. Dichas acciones serán descritas en el siguiente apartado.

Una vez editados los campos deseados, para almacenar los cambios se debe pulsar sobre el botón .

5.3.7.1.2.1 Alta de Planificador

Para asociar un nuevo planificador a una tarea se debe pulsar sobre el botón situado en la cabecera de la columna de acciones, de manera que aparecerá el formulario para la creación de un planificador:



Figura 120 - Gestión de Tareas - Alta de Planificador

Definidos los datos del planificador, para crearlo se debe pulsar sobre el botón y para cancelar el proceso se debe pulsar sobre el botón .

Una vez completado el proceso la ventana de datos de la tarea presentará en la lista de planificadores el nuevo planificador, si bien, no será almacenado en BBDD hasta que no se almacenen los datos de la tarea pulsando sobre el botón el botón  en la ventana de datos de la tarea.

5.3.7.1.2.2 Edición de Planificador

Para editar un planificador asociado a una tarea se debe pulsar sobre el botón  situado en la columna de acciones, en la misma fila del planificador a editar, de manera que aparecerá el formulario para la edición de un planificador:



Figura 121 - Gestión de Tareas - Edición de Planificador

Editados los datos del planificador, para almacenarlos se debe pulsar sobre el botón  y para cancelar el proceso se debe pulsar sobre el botón .

Una vez completado el proceso la ventana de datos de la tarea presentará en la lista de planificadores el planificador editado, si bien, no será actualizado en BBDD hasta que no se almacenen los datos de la tarea pulsando sobre el botón el botón  en la ventana de datos de la tarea.

5.3.7.1.2.3 Eliminación de Planificador

Para eliminar un planificador asociado a una tarea se debe pulsar sobre el botón  situado en la columna de acciones, en la misma fila del planificador a eliminar. De esta manera aparecerá un diálogo de confirmación para su eliminación. Aceptando dicho diálogo el planificador desaparecerá

de la lista de planificadores asociados a la tarea. Para que el planificador quede eliminado definitivamente de la BBDD se debe pulsar sobre el botón  en la ventana de datos de la tarea.

Si una tarea no dispone de ningún planificador, esta pasa a ser considerada deshabilitada.

5.3.7.1.3 Borrado de Tarea Estándar

Para eliminar una tarea estándar se debe acceder a los datos de la misma pulsando sobre su nombre en el árbol de tareas y pulsar sobre el botón .

5.3.7.1.4 Alta de Tarea de Validación



Para crear una tarea de validación, el usuario debe pulsar el botón situado en la parte inferior a la izquierda y que está etiquetado como ***"Añadir Tarea de Validación"***. Una vez pulsado, se mostrará una ventana en la que se pueden establecer los datos de la tarea:



Figura 122 - Gestión de Tareas - Alta de Tarea de Validación

Los campos que componen una tarea de validación son:

- **Nombre:** Cadena de texto que identifica unívocamente a la tarea. Debe ser un nombre que no coincida con el de otra tarea existente previamente.

- **Tipo:** Constituye una lista donde seleccionar el tipo de tarea de validación para indicar si llevará a cabo la validación del estado de caducidad de los certificados (***Caducidad***), o bien, el estado de revocación de los certificados (***Revocación***).

- **Tipo Planificador:** Tipo de planificador asociado por defecto a la tarea. Constituye una lista en la que seleccionar el tipo, esto es, ***Periódico***, ***Diario*** o ***Por Fecha***.

- **Periodo:** Periodo de ejecución de la tarea asociado al planificador. Sólo aplicable para el planificador de tipo ***Periódico***.

- **Inicio:** Fecha de inicio para la ejecución de la tarea asociada al planificador.

- **Almacenes de Claves:** Constituye una lista con los almacenes de claves sobre los que aplicará la tarea de validación.

Los campos indicados con un asterisco serán obligatorios. Para crear la tarea se debe pulsar sobre el botón  y para cancelar el proceso se debe pulsar sobre el botón . Una vez completado el proceso, en el árbol de tareas, aparecerá el nodo asociado a la nueva tarea.

5.3.7.1.5 Edición de Tarea de Validación

Para editar una tarea de validación se debe acceder a los datos de la misma pulsando sobre el nodo con su nombre en el árbol de tareas:



Figura 123 - Gestión de Tareas - Datos de Tarea de Validación

Una vez editados los campos deseados, para almacenar los cambios se debe pulsar sobre el botón ✓ .

5.3.7.1.6 Borrado de Tarea de Validación

Para eliminar una tarea de validación se debe acceder a los datos de la misma pulsando sobre su nombre en el árbol de tareas y pulsar sobre el botón 🗑 .

5.3.7.2 Tareas críticas

A diferencia de las tareas descritas anteriormente estas tareas no pueden ser eliminadas. Si la plataforma se está ejecutando en mono-nodo, las tareas de ejecución de procesos en lotes y las

tareas asíncronas estarán deshabilitadas, ya que no existe comunicación entre los nodos. en la plataforma se definen las siguientes tareas críticas.

- **Procesar Peticiones asíncronas de periodo de gracia**. Tarea que finaliza aquellas peticiones de Firma o Upgrade que están pendiente de la aplicación de un periodo de gracia. Esta tarea solo estará disponible cuando los nodos estén en clúster.

  El periodo de gracia es el intervalo de retención mínimo y necesario para asegurar que un certificado es válido según su PSC. Los PSC actualizan periódicamente sus servicios de validación de manera que, al revocar un certificado, éste continúa vigente de forma oficial hasta la nueva actualización. Así pues, por ejemplo, un PSC puede especificar que el periodo de gracia de verificación para sus certificados es 24 horas porque desde que se revoca un certificado hasta que lo publican en una CRL el periodo pasado es de 23 horas. Cuando llega una firma a la plataforma, se validan los certificados de la firma en el momento de la recepción. Si se ha solicitado que la validación se haga de acuerdo al periodo de gracia, tras la primera validación, si esta es correcta, se espera el tiempo establecido por el periodo de gracia para realizar una segunda validación que garantiza que en el momento de la petición de validación el certificado era correcto. Las peticiones que implican periodo de gracia sólo cambiarán su estado una vez transcurrido el tiempo especificado.

- **Procesar Peticiones asíncronas de Procesos en Lote**. Tarea que ejecuta las peticiones de Validación de Firmas o Certificados en Lote que se encuentran registrada en la plataforma. Mediante los servicios de “Validaciones en Lotes” se puede solicitar la verificación de múltiples firmas o certificados digitales al servidor en una única petición. Estas peticiones serán procesadas de forma asíncrona por el servidor. Esta tarea solo estará disponible cuando los nodos estén en clúster.

- **Eliminar Peticiones Caducadas**. Tarea que elimina las peticiones asíncronas caducadas. Para las peticiones asíncronas se debe definir un tiempo a partir del cual las peticiones no serán procesadas, esto se denomina Tiempo de caducidad. Esta tarea solo estará disponible cuando los nodos estén en clúster.

- **Eliminar Peticiones Consultadas**. Tarea que elimina aquellas peticiones asíncronas que han finalizado y han sido consultadas. Esta tarea solo estará disponible cuando los nodos estén en clúster.

- **Reactivar y reasignar procesos pendientes**. Tarea que recupera aquellos procesos asíncronos que han interrumpido su ejecución. Esta tarea solo estará disponible cuando los nodos estén en clúster.

- **Sincronización con DIR3**. Tarea encargada de realizar la sincronización periódica de aplicaciones y unidades organizativas respecto a DIR3.

Como veremos a continuación la configuración de estas tareas posee algunas diferencias con respecto a las tareas no críticas, pero se puede resumir en los siguientes puntos:

√ No pueden ser eliminadas del Gestor ni se pueden modificar sus clases de implementación.

√ Aunque no se puedan eliminar del Gestor sí se pueden activar o desactivar individualmente cada tarea.

√ Únicamente presentan un planificador.

√ Necesitan de cierta información adicional de configuración no contemplada en las tareas no críticas.

5.3.7.2.1 Configuración de la tarea "Procesado de Peticiones con periodo de gracia"

Esta tarea se ejecuta en cada uno de los nodos que forman el sistema, durante la ejecución cada nodo recuperará los procesos que tenga asignados y procederá a finalizar los mismos. **Únicamente disponible cuando se trabaja en clúster.**

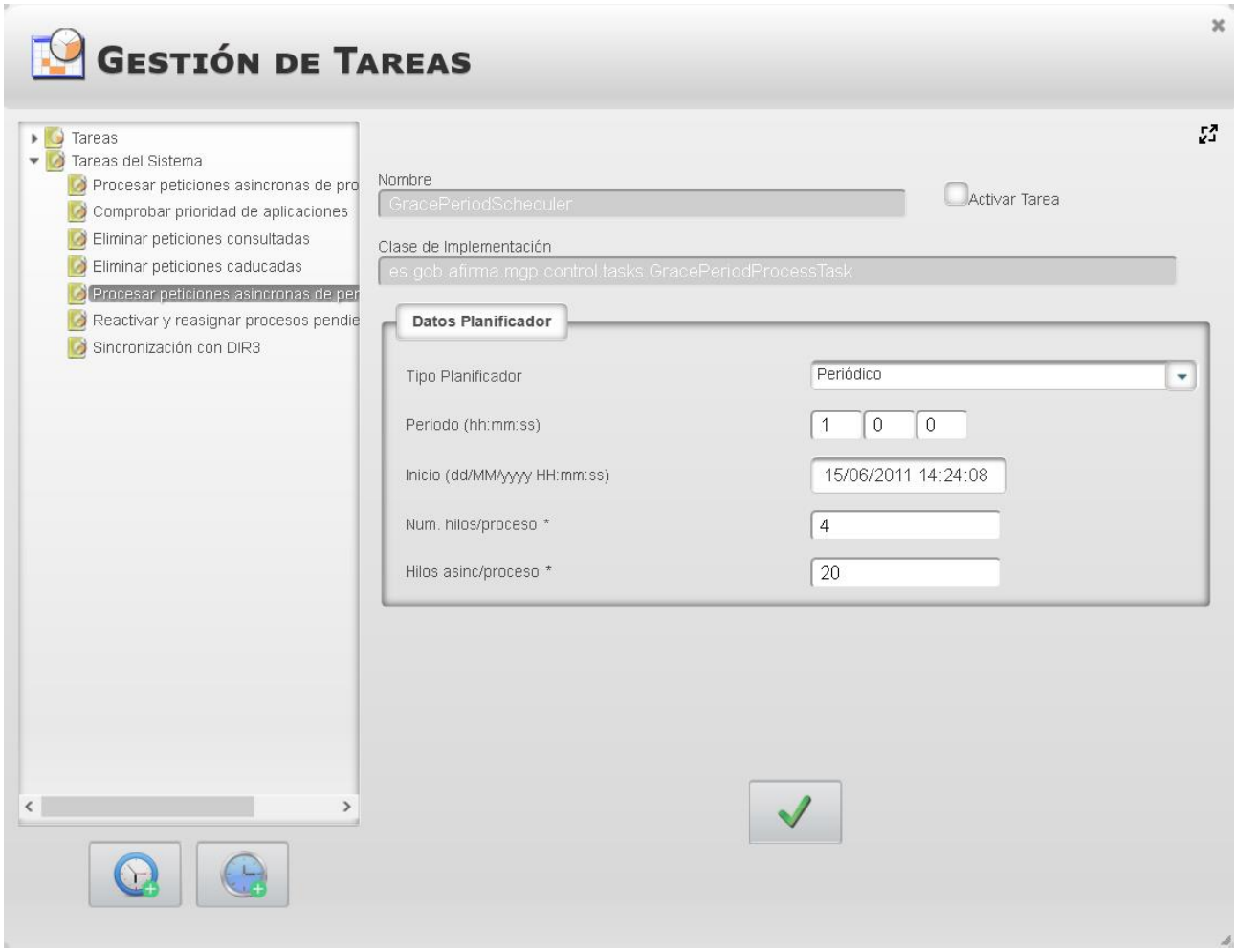


Figura 124 - Tarea: Procesado de Peticiones con Periodo de Gracia

Al ser una tarea crítica esta no puede ser eliminada del Gestor ni se puede modificar su clase de implementación ni su nombre asociado. La información manejada por la tarea es:

- **Tarea Activa**. Determina si la tarea se encuentra activa o no.
- **Tipo de Planificador**. Esta tarea admite planificador “DIARIO” y “PERIODICO”. Se puede obtener más información sobre este campo en el apartado 5.3.7.1.2.1.
- **Periodo**. Periodo de ejecución de la tarea.
- **Inicio**. Fecha de inicio de la tarea.
- **Número de hilos**. Esta tarea puede ser ejecutada de forma paralela en varios hilos, en este campo se indica el número de hilos que se activará en cada nodo.

- **Número máximo de procesos / hilos**. Campo que indica el número máximo de procesos asíncronos que se le asignará a cada hilo de ejecución. En el caso de no establecer valor en este campo repartirán todos los procesos pendientes entre los distintos hilos.

5.3.7.2.2 Configuración de la tarea "Procesado de Peticiones en Lote"

Tarea que ejecuta las peticiones de Validación de Firmas o Certificados en Lote que se encuentran registrada en la plataforma. **Únicamente disponible cuando se trabaja en clúster.**

En la siguiente figura se muestra la pantalla de configuración de esta tarea.

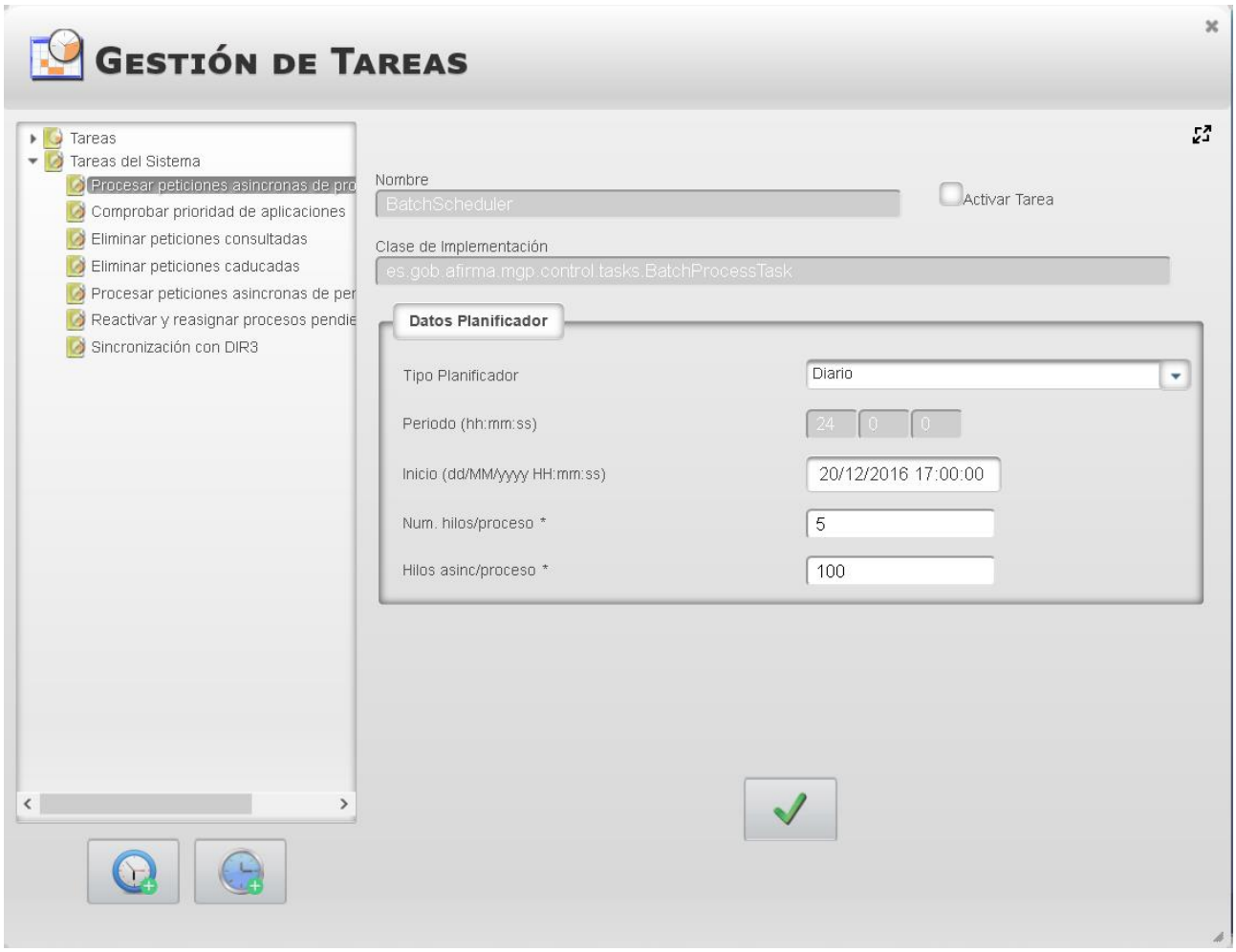


Figura 125 - Tarea: Procesado de Peticiones en Lote

La información manejada por esta tarea es similar a la desarrollada en la tarea anterior.

- **Tarea Activa**. Determina si la tarea se encuentra activa o no.

- **Tipo de Planificador**. Esta tarea admite planificador “DIARIO” y “PERIODICO”. Se puede obtener más información sobre este campo en el apartado 5.3.7.1.2.1.

- **Periodo**. Periodo de ejecución de la tarea.

- **Inicio**. Fecha de inicio de la tarea.

- **Número de hilos**. Esta tarea puede ser ejecutada de forma paralela en varios hilos, en este campo se indica el número de hilos que se activará en cada nodo.

- **Número máximo de procesos / hilos**. Campo que indica el número máximo de procesos asíncronos que se le asignará a cada hilo de ejecución. Se debe tener en cuenta que una Petición en Lote está formada por N peticiones individuales y por lo tanto por N procesos asíncronos. En el caso de no establecer valor en este campo repartirán todos los procesos pendientes entre los distintos hilos.

5.3.7.2.3 Configuración de la tarea “Eliminar Peticiones Caducadas”

Esta tarea elimina las peticiones asíncronas que han superado el periodo de caducidad, su ejecución se realiza en un único nodo (nodo maestro) del sistema. **Únicamente disponible cuando se trabaja en clúster.**

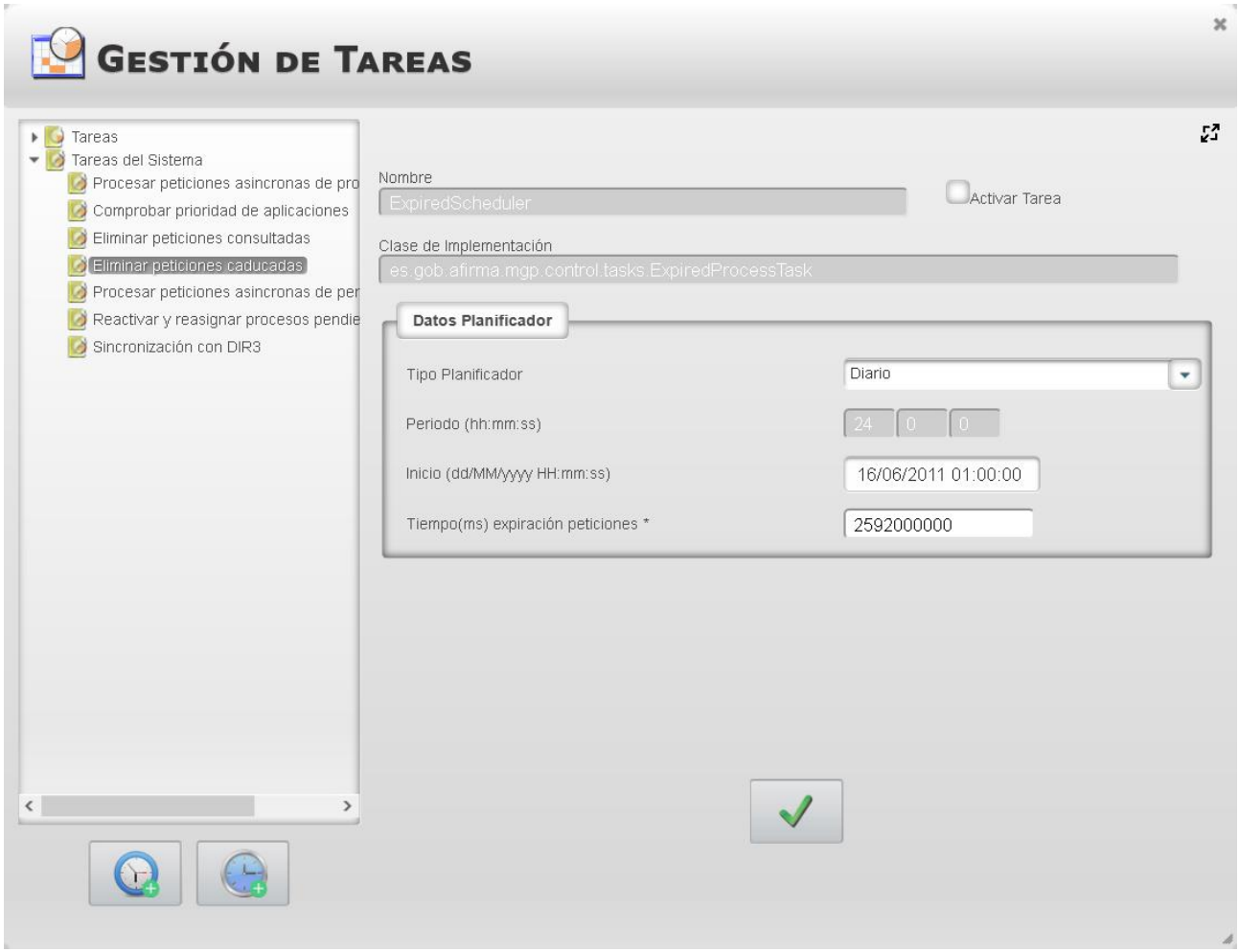


Figura 126 - Tarea: Borrado de Peticiones Caducadas

La información manejada por esta tarea es:

- **Tarea Activa**. Determina si la tarea se encuentra activa o no.
- **Tipo de Planificador**. Esta tarea admite planificador “DIARIO”, “PERIODICO”. Se puede obtener más información sobre este campo en el apartado 5.3.7.1.2.1.
- **Periodo**. Periodo de ejecución de la tarea.
- **Inicio**. Fecha de inicio de la tarea.
- **Tiempo de caducidad**. Tiempo de caducidad de una petición asíncrona.

5.3.7.2.4 Configuración de la tarea “Eliminar Peticiones Consultadas”

Esta tarea elimina del sistema aquellas peticiones asíncronas finalizadas y consultada (el cliente ya ha obtenido la respuesta asociada), su ejecución se realiza en un único nodo (nodo maestro) del sistema. **Únicamente disponible cuando se trabaja en clúster.**

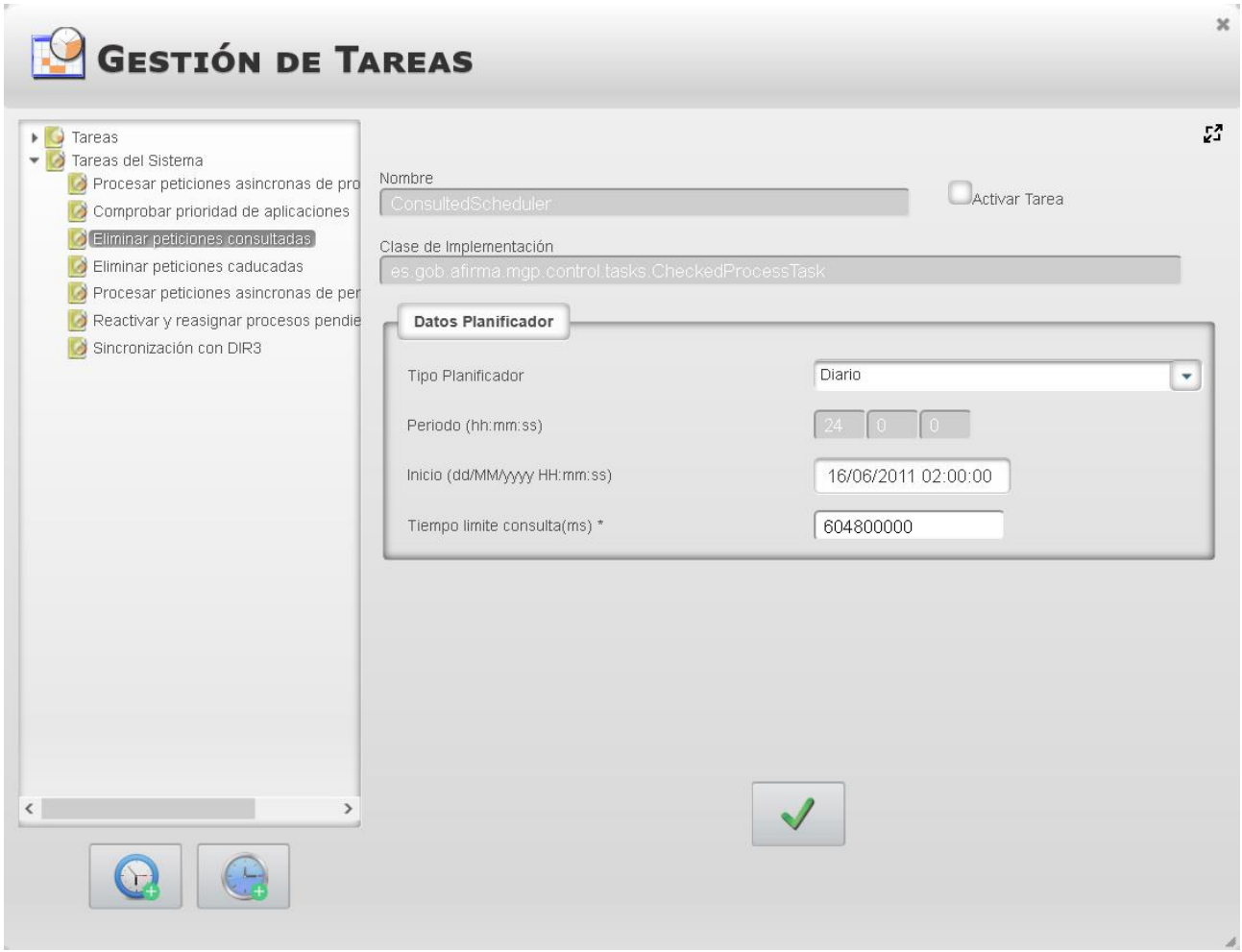


Figura 127 - Tarea: Borrado de Peticiones Consultadas

La información manejada por esta tarea es:

- **Tarea Activa**. Determina si la tarea se encuentra activa o no.
- **Tipo de Planificador**. Esta tarea admite planificador “DIARIO”, “PERIODICO” y “POR FECHA”. Se puede obtener más información sobre este campo en el apartado 5.3.7.1.2.1.
- **Periodo**. Periodo de ejecución de la tarea.

- **Inicio**. Fecha de inicio de la tarea.

- **Tiempo de consulta**. Tiempo que estará disponible la respuesta una vez se ha obtenido por primera vez. Pasado este tiempo la tarea eliminará esta petición.

5.3.7.2.5 Configuración de la tarea "Reactivar y reasignar peticiones pendientes"

Tarea de respaldo que realiza las siguientes acciones:

- Recupera aquellos procesos asíncronos que debido a un error del sistema han interrumpido su ejecución.

- Reasigna a nodos activos aquellos procesos asíncronos pendientes que están asignados a nodos no disponibles.

Esta tarea se ejecuta en un único nodo (nodo maestro) de la plataforma. **Únicamente disponible cuando se trabaja en clúster.**

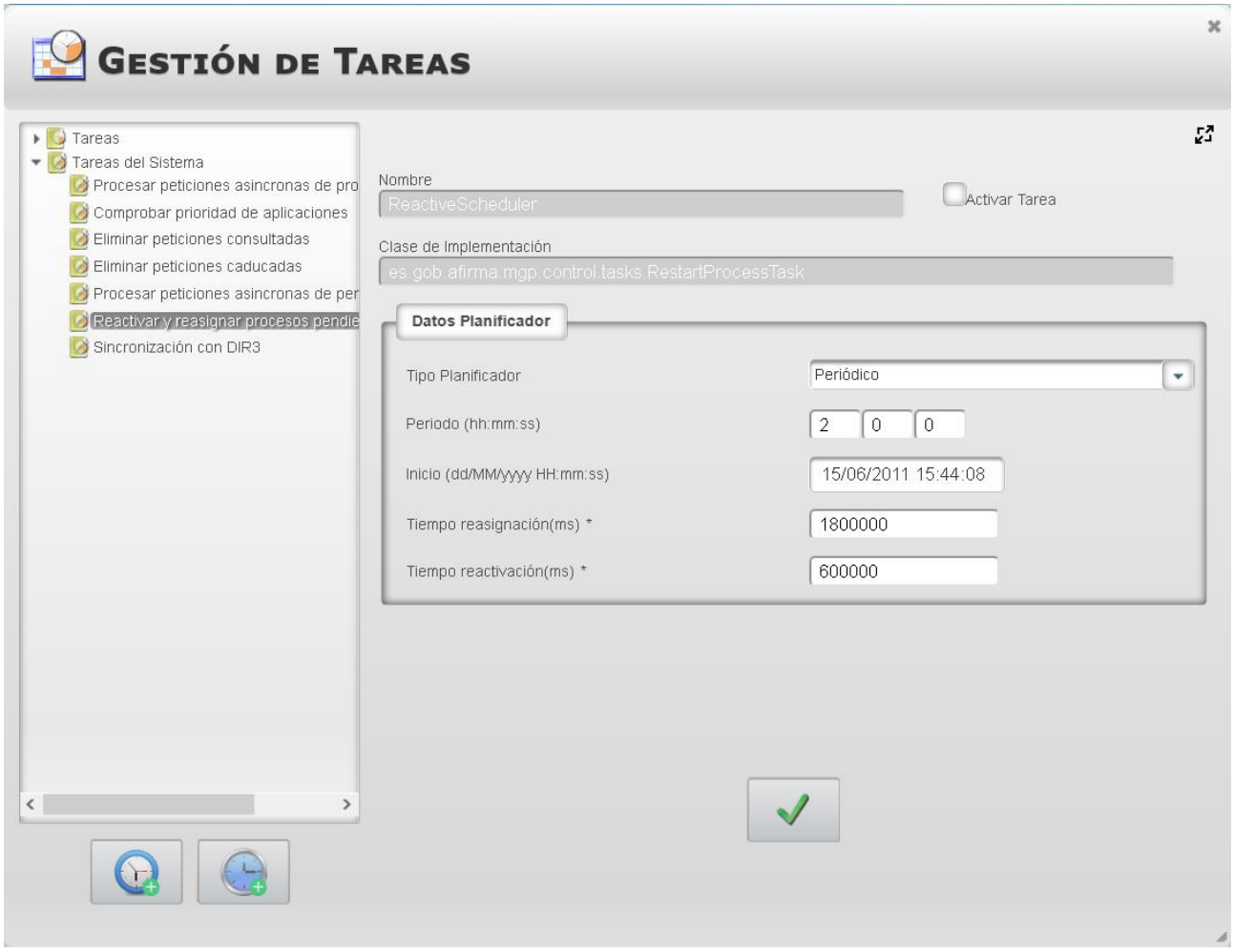


Figura 128 - Tarea: Reactivar Peticiones Pendientes

La información manejada por esta tarea es:

- **Tarea Activa**. Determina si la tarea se encuentra activa o no.
- **Tipo de Planificador**. Esta tarea admite planificador “DIARIO” y “PERIODICO”. Se puede obtener más información sobre este campo en el apartado 5.3.7.1.2.1.
- **Periodo**. Periodo de ejecución de la tarea.
- **Inicio**. Fecha de inicio de la tarea.
- **Tiempo de finalización**. Tiempo máximo estimado de finalización de un proceso asíncrono, si un proceso se encuentra en estado de “en ejecución” más del tiempo indicado en este campo se procederá a su reactivación.

- **Tiempo de reasignación**. Tiempo a partir del cual se considera que un nodo como no activo, una vez superado este tiempo se procede a reasignar los procesos pendientes de este nodo al resto de nodos activos.

5.3.7.2.6 Configuración de la tarea "Sincronización con DIR3"

Para sincronizar todo el árbol de unidades organizativas y aplicaciones con DIR3, la plataforma debe tener definido el modo de integración con DIR3 como relajado o estricto, en las propiedades configurables definidas para ello en la Gestión de la Configuración. Este tipo de sincronización afecta a todas las unidades organizativas y aplicaciones almacenadas en el sistema, de manera que sus datos se actualizarán en base a los definidos en DIR3 en función del modo de integración seleccionado.

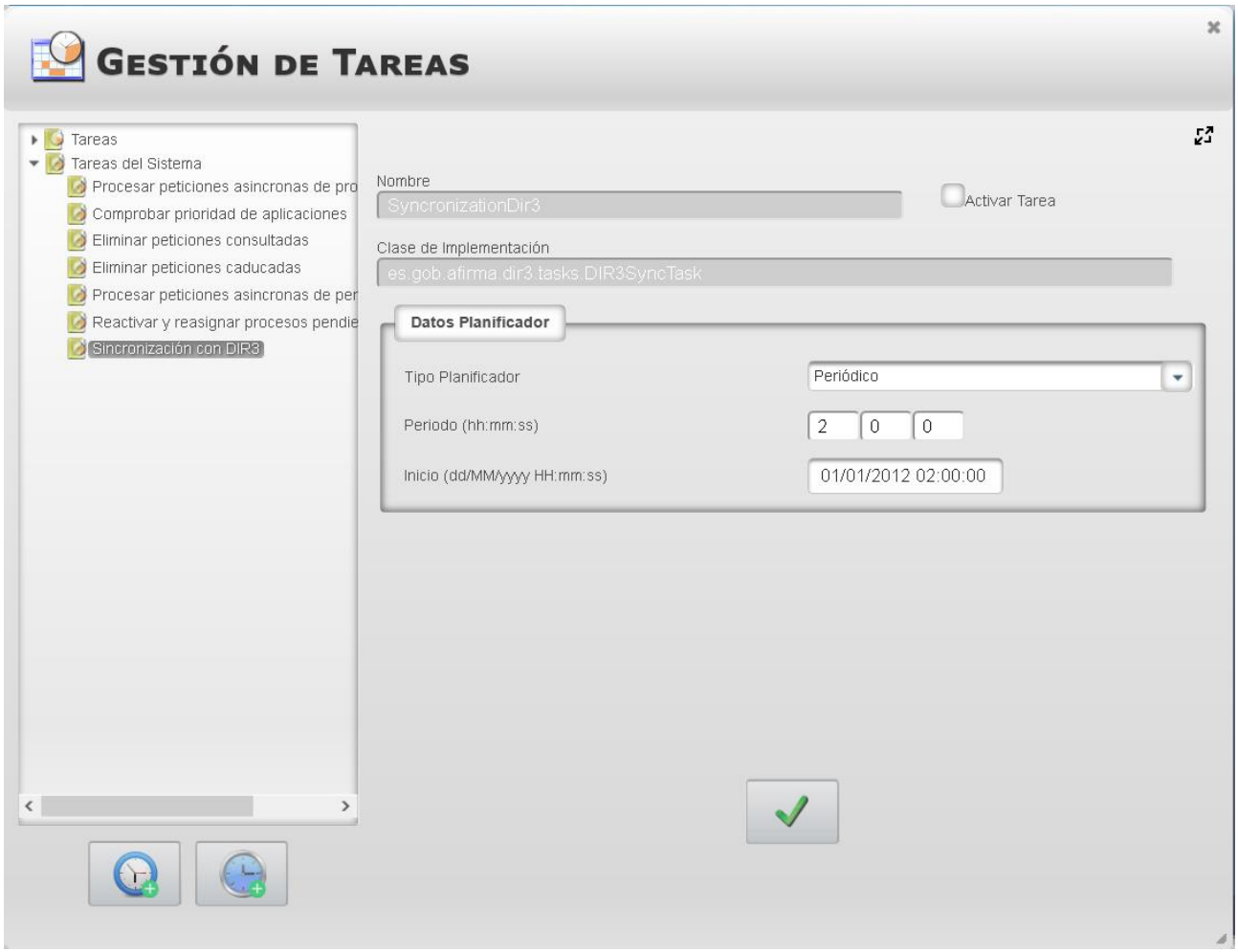


Figura 129 - Tarea: Sincronización con DIR3

En cualquier caso, se actualizarán los datos de las unidades organizativas cuyo tipo de identificador sea *DIR3*, de modo que si su identificador es/coincide con uno existente en *DIR3*, se actualiza su información asociada, e incluso se crea la jerarquía de unidades organizativas que debe contenerla, moviendo todas las subunidades organizativas y aplicaciones a la nueva estructura si fuera necesario. En el caso de estar establecido el modo de integración estricto, todas aquellas unidades organizativas con un tipo de identificador *LIBRE* serán eliminadas (así como toda la jerarquía por debajo de estas), ocurriendo lo mismo para aquellas unidades organizativas que tengan definido un identificador de tipo *DIR3* pero dicho identificador no se encuentre registrado en *DIR3*.

La primera vez que se realiza una sincronización con *DIR3* esta se hace de forma completa, por lo que debe obtener una gran cantidad de datos, pudiendo elevar el tiempo de respuesta del servicio web hacia DIR3 (configurable/modificable en las propiedades configurables definidas para ello en la Gestión de la Configuración) y el tiempo de procesamiento de toda la información. Además, al final del proceso siempre se realiza una recarga de la caché en todo el cluster. Una vez realizada la primera sincronización, las posteriores se realizan siempre de forma incremental, siendo mucho más rápido el proceso.

IMPORTANTE: La sincronización con DIR3 (ya sea en modo de integración relajado o estricto, aunque con mayores consecuencias en el segundo caso) implica cambios en la jerarquía de unidades organizativas y aplicaciones, por lo que se recomienda que antes de programar esta tarea, se realice al menos una primera sincronización manual (apartado 5.3.4.8), creando previamente una configuración estable (apartado 5.3.14.3) a modo de copia de seguridad.

La información manejada por esta tarea es:

- **Tipo de Planificador**. Esta tarea admite planificador “DIARIO” y “PERIODICO”. Se puede obtener más información sobre este campo en el apartado 5.3.7.1.2.1.
- **Periodo**. Periodo de ejecución de la tarea.
- **Inicio**. Fecha de inicio de la tarea.

5.3.8 Gestión de Alarmas

Una Alarma es una señal de que en el sistema ha ocurrido una anomalía. En el caso de la plataforma @firma, cada alarma tiene definida un protocolo de actuación y un determinado número de destinatarios a los que se debe avisar en caso de que dicha alarma se produzca. Las alarmas originadas en el sistema pueden consultarse haciendo uso de la herramienta de Monitorización y Auditoría (para consultar el histórico de alarmas por fecha y para ver en tiempo real las alarmas que se están generando).

Actualmente existen definidas las siguientes alarmas en la plataforma (tanto las alarmas como el procedimiento de actuación se encuentran definidos en el documento ***@Firma-MALARM-Alarmas-MAN***). Tras el rediseño del gestor de Alarmas, aparecen una nueva serie de datos y de conceptos, como el resumen de alarmas. Todo esto se irá explicando en los siguientes apartados, de los cuales, cada uno de ellos corresponderá con una de las pestañas dentro de la gestión de alarmas.

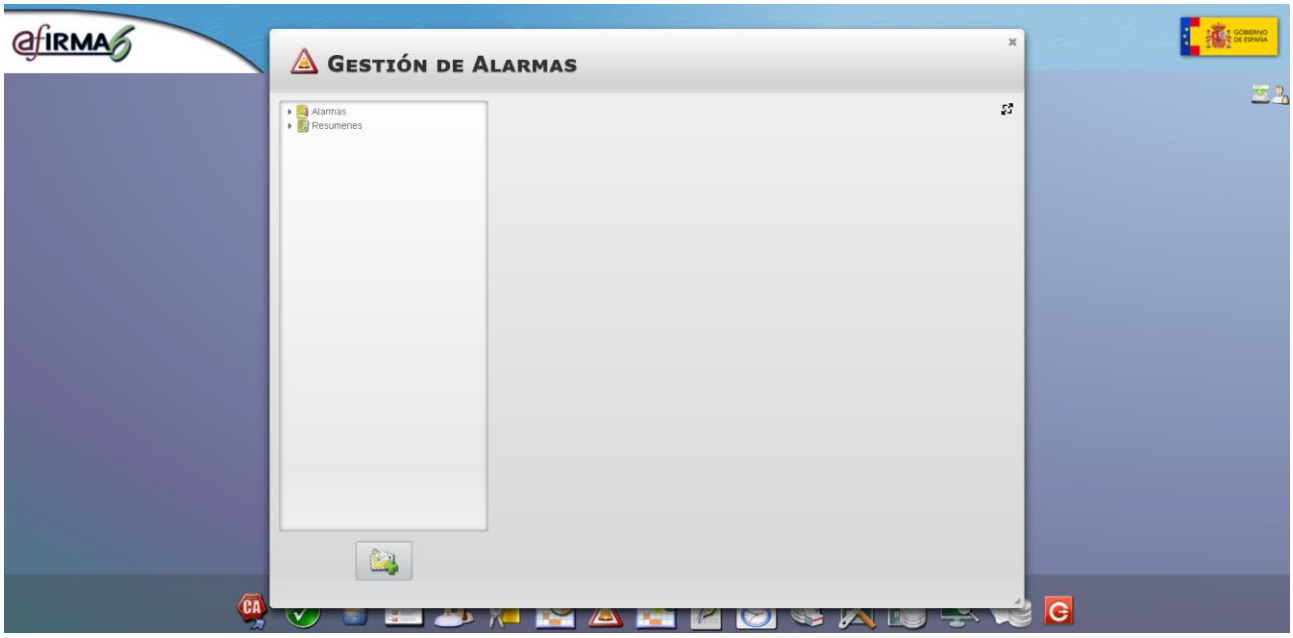


Figura 130 - Ventana Gestión de Alarmas

5.3.8.1 Modificación de los Datos de Configuración de una Alarma



Si se selecciona un nodo de tipo Alarma del árbol de alarmas y resúmenes situado a la izquierda de la interfaz, se puede modificar una serie de datos:

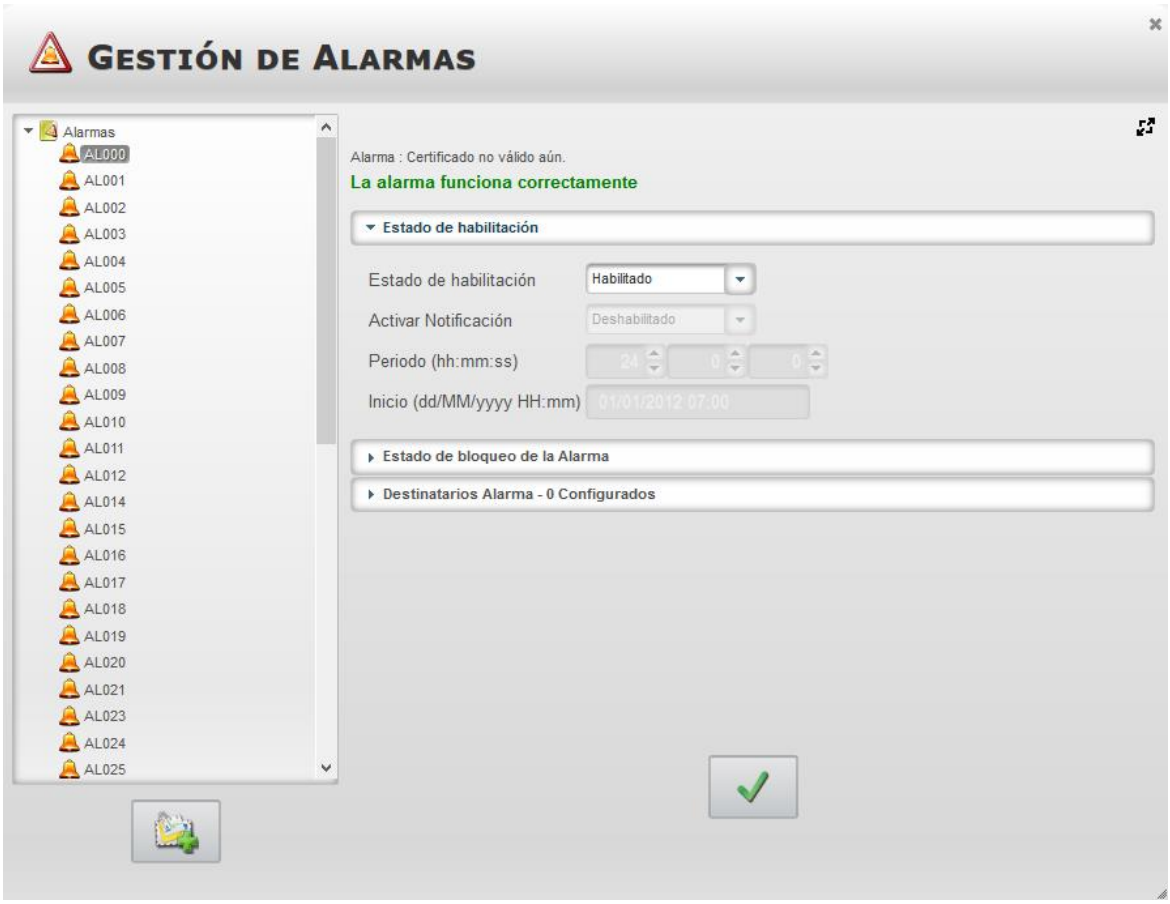


Figura 131 - Ventana de Gestión de Alarmas (I)

Para cada alarma, se puede dividir la pantalla en dos partes:

1) **Estado de la alarma:**

- **Estado de habilitación:** Una alarma puede ser configurada por el administrador en dos posibles estados: habilitada o deshabilitada. Al estar habilitada, su funcionamiento es funcionalmente completo, es decir, se registra el evento, se registra en auditoría y monitorización y finalmente se notifica a los destinatarios configurados por correo electrónico. En caso de estar deshabilitada, los eventos de dicha alarma, se ignorarán, será como si nunca hubieran ocurrido. El principal motivo de permitir esto, es el poder desactivar determinadas alarmas por petición propia del administrador, siendo útil por ejemplo en caso de necesidad de detener la base de datos y no estar recibiendo continuamente avisos de alarmas.

Se aporta la posibilidad de activar un sistema de notificaciones en caso que la alarma se encuentre deshabilitada. Así, a modo de recordatorio, los administradores configurados en la plataforma recibirán periódicamente un correo recordándoles el estado deshabilitado de la alarma. La configuración del periodo se hace mediante un planificador del tipo de las tareas programables.

2) Estado de bloqueo de la alarma:

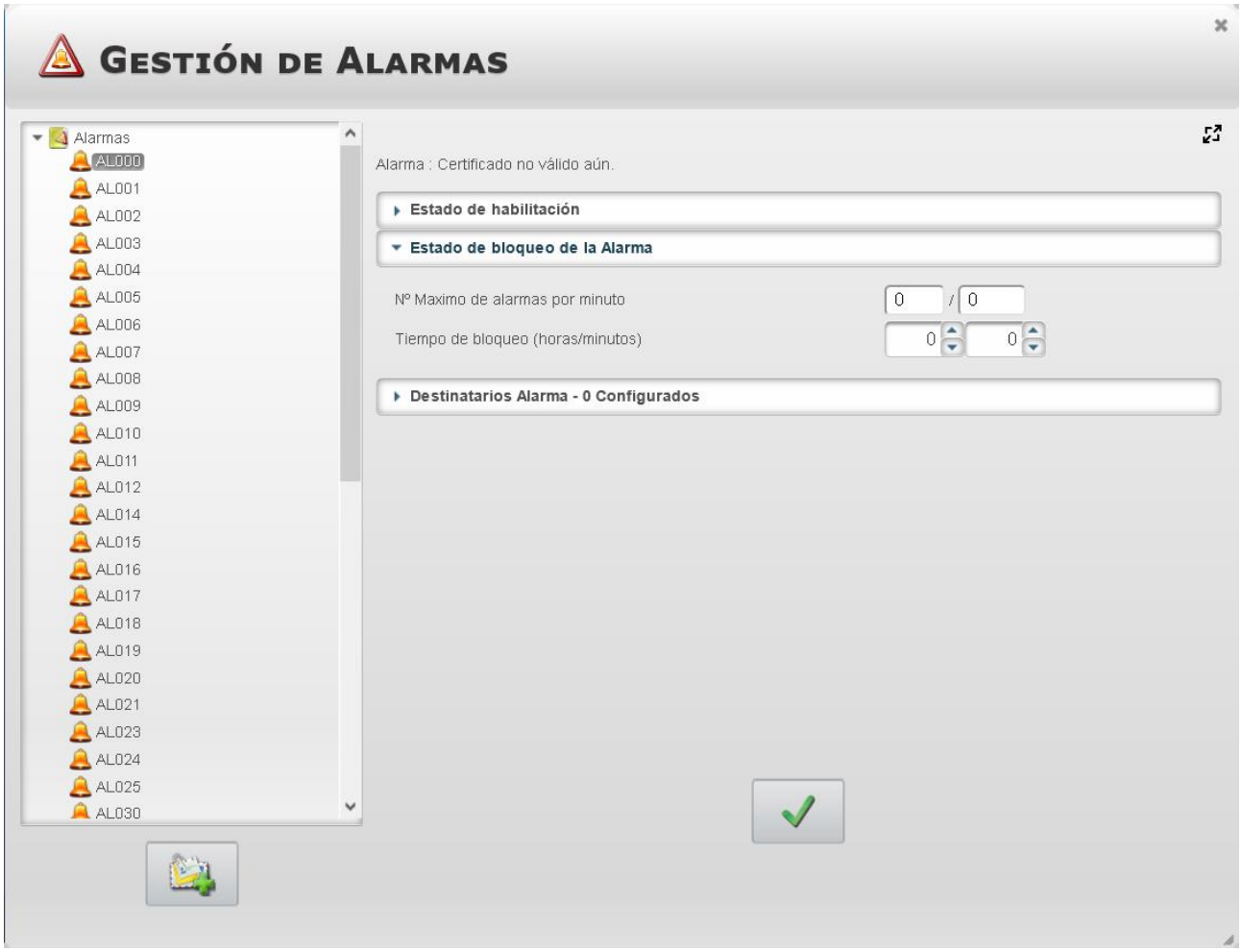


Figura 132 - Ventana de Gestión de Alarmas (II)

- **Bloqueo:** Existe un nuevo concepto, el de alarma bloqueada. Se asemeja a un tercer posible estado de la alarma. Ahora se puede configurar que si se sobrepasa un número determinado de alarmas durante un periodo de tiempo (también configurable), esta se bloqueará de forma automática, de modo que ya no se realizarán más envíos de correos electrónicos a los

destinatarios de las alarmas, pero sí que se registrará su evento y se registrará en base de datos (auditoría y monitorización).

En el caso que una alarma se encuentre bloqueada, aparecerá un mensaje en rojo indicándolo, además de un botón que aporta la posibilidad de desbloquearla. Evidentemente, esta acción tan solo es realizable por el administrador. Al ser desbloqueada, la alarma vuelve a un estado estable.

Si en el número máximo de alarmas por minuto se establece a 0/0, la alarma no será bloqueada en ningún caso.

Cuando una alarma se encuentra en estado bloqueado, se enviará un correo a los administradores de la plataforma indicando el estado bloqueado de la alarma. El correo se enviará haciendo uso del planificador existente en la zona “Estado de bloqueo de la Alarma” a la hora introducida en el campo “Inicio” y repitiéndose el envío según lo introducido en el campo “Periodo”.

Una vez bloqueada la alarma, esta solo podrá ser desbloqueada de forma manual con el botón habilitado a tal efecto.

En cualquier caso, para guardar los cambios que se realicen en la administración dentro del apartado correspondiente al estado de la alarma (considerando el bloqueo como un posible estado), tan solo hay que pulsar el botón “Guardar Cambios”.

IMPORTANTE: Si los nodos de la plataforma no están trabajando en clúster, la notificación vía email de que la alarma se encuentra bloqueada solo se producirá una vez, y no de forma periódica.

3) Configuración de destinatarios:



Figura 133 - Ventana de Gestión de Alarmas (III)

Los destinatarios se pueden configurar independientemente del estado de la alarma, este es el motivo por el que se consideran aparte.



La gestión de los destinatarios (alta, modificación y eliminación) se realiza a través del módulo de configuración de la plataforma. No obstante, se pueden dar de alta nuevos destinatarios desde este módulo, a través del botón alta **"Alta Nuevo destinatario"**.

5.3.8.2 Gestión de Resúmenes

En determinados momentos, resulta más útil tener un listado con todos los eventos de alarmas o con los eventos de determinadas alarmas que se han producido durante un periodo de tiempo, que la notificación en cada instante de cada evento de alarma que se produce.

Aquí nace el concepto de "Resumen de Alarmas". Los "Resúmenes de alarmas" no son más que una colección de eventos que se han producido sobre un listado configurable de alarmas, durante un periodo de tiempo especificado. Este resumen adopta forma de correo electrónico y es enviado a los

destinatarios configurados, evitando de esta forma, el cúmulo continuo de correos y además teniendo recolectada toda la información en uno solo.



Para dar de alta un nuevo resumen (inicialmente la plataforma no lleva ninguno definido), tan solo hay que pulsar sobre el botón ***"Nuevo Resumen"*** situado en la parte inferior del árbol de Alarmas y Resúmenes. Entonces aparecerá una nueva pantalla modal para insertar todos los datos necesarios:

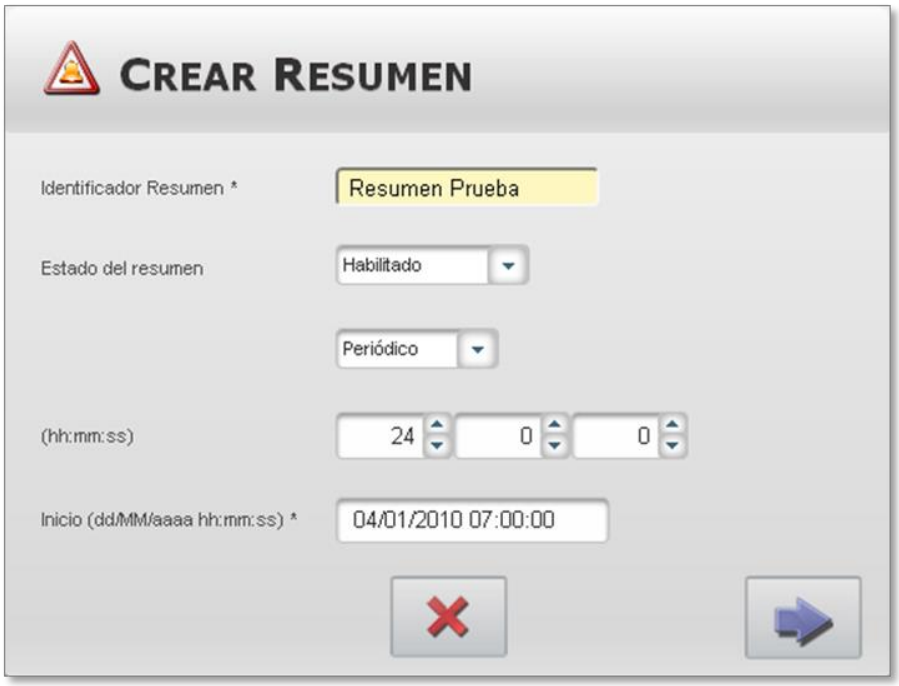


Figura 134 - Ventana de Alta de Resumen de Alarmas (I)

Los datos a completar son los siguientes:

- **Identificador Resumen:** Cadena alfanumérica que debe identificar de forma única el resumen. En caso de introducir una ya existente, el administrador será avisado mediante un mensaje y se cancelará la orden de alta del nuevo resumen.

- **Estado del Resumen:** Un resumen tiene dos posibles estados: habilitado o deshabilitado. Si un resumen se encuentra habilitado, y se produce un evento de alarma contenida en dicho resumen, se almacenará en base de datos un mensaje que asociará dicho evento con el resumen, para posteriormente recolectarlos todos y formar un único correo. Además, aquellos destinatarios incluidos en la alarma que también estén incluidos en el resumen, también recibirán el correo electrónico del evento de alarma, ya que se considera que el estar incluidos en el resumen no es

excluyente. En caso de encontrarse deshabilitado, el resumen puede ser configurable en cualquier momento, pero no se encontrará en funcionamiento, es decir, en caso de recibir un evento de alarma estando ésta incluida dentro del resumen deshabilitado, se ignorará el resumen y se continuará el procedimiento.

- **Datos Planificador:** Aquí se establecen los datos que determinan cada cuanto tiempo y a partir de cuándo se realizará el envío del resumen. Esto se gestiona como una tarea periódica mediante el Gestor de Tareas de Alarmas. Llegado el momento, se acudirá a base de datos, se recuperarán todos los eventos de alarmas asociados al resumen, se construirá un correo electrónico con todos ellos y se enviará dicho correo a los destinatarios configurados en el resumen. Después de esto, se eliminará de base de datos la asociación de dichos eventos con el resumen.

Una vez rellenada la información general. Tras pulsar siguiente aparecerá un panel donde añadir la información de las alarmas asociadas y destinatarios.

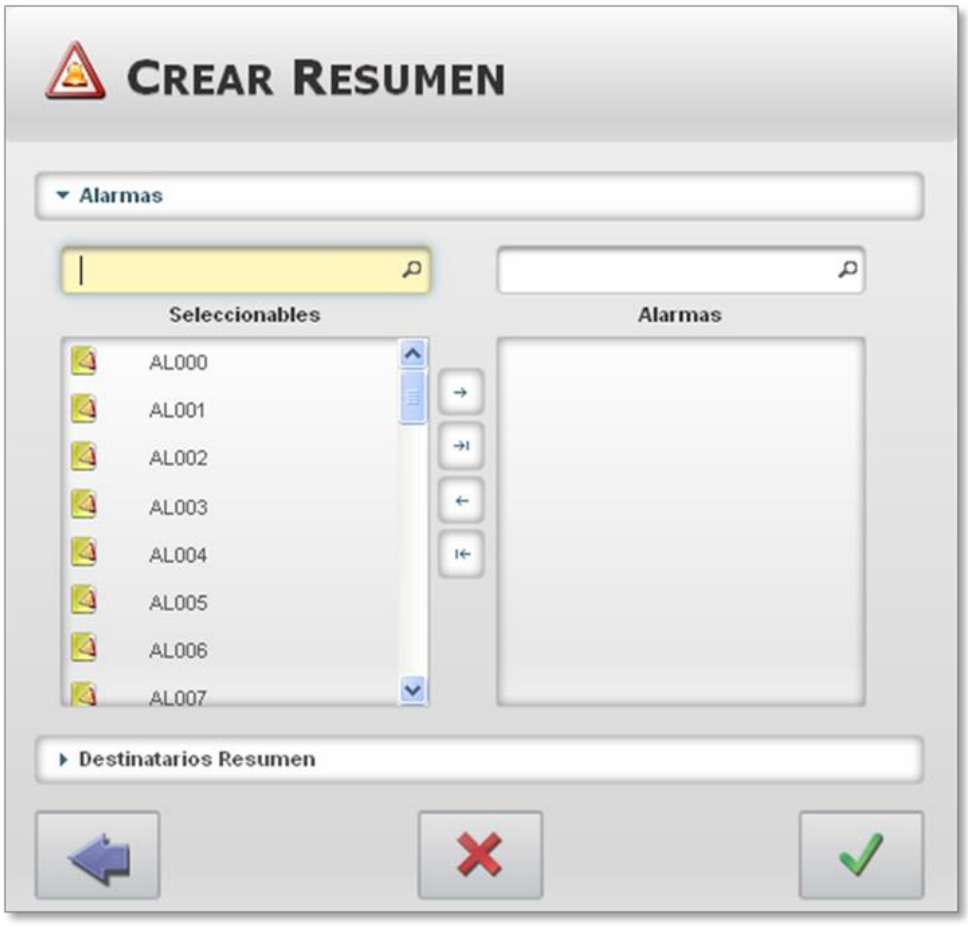


Figura 135 - Ventana de Alta de Resumen de Alarmas (II)

- **Alarmas:** Se trata de una doble pantalla en forma de árbol. En la izquierda se muestran todas las alarmas disponibles a incluir en el resumen (inicialmente todas), y a medida que vamos seleccionando y pulsando sobre el botón ">>", vamos creando el árbol de alarmas contenidas, que son aquellas que se considera que contendrá el resumen. Si en algún momento deseamos quitar alguna alarma de las contenidas, tan solo hay que seleccionarla y pulsar sobre el botón "<<".

- **Destinatarios:** Aquí se define la lista de destinatarios del resumen del mismo modo que se definen para las alarmas. El listado de posibles destinatarios se gestiona en la pantalla de configuración (apartado 5.3.13.4).

Una vez completados los campos deseados, se pulsa sobre el botón ***"Alta Nuevo Resumen"*** completando así el procedimiento de alta. En caso que faltase algún campo por completar, o se produjese un error, se le indicará al administrador mediante un mensaje en pantalla.

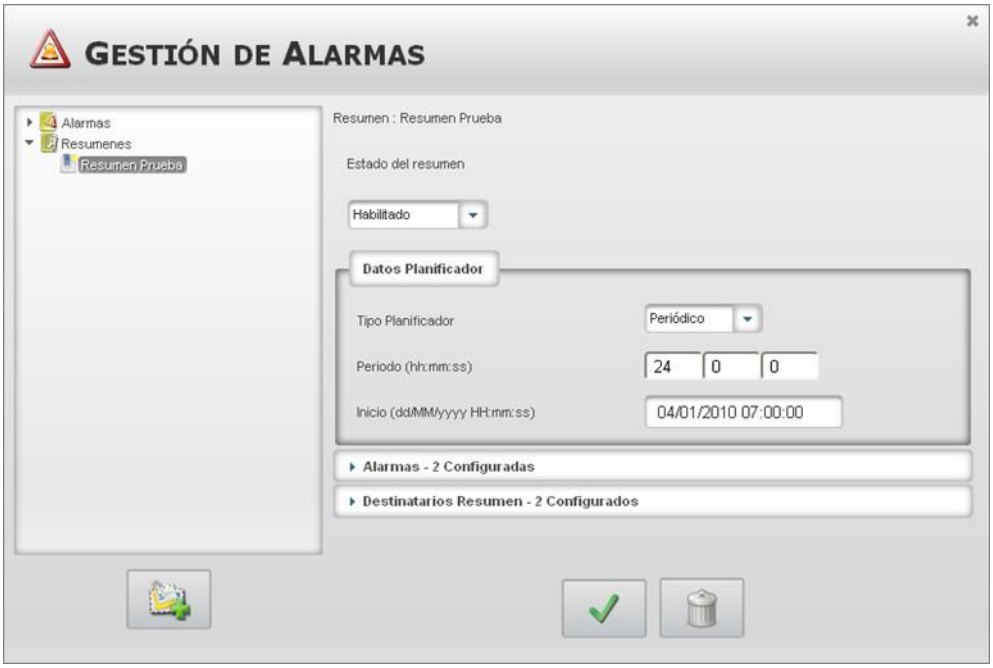


Figura 136 - Ventana de Datos de Resumen de Alarmas

En esta pantalla además aparece una opción más, la de eliminar el resumen mediante el botón ***"Eliminar Resumen"***. Hay que tener en cuenta, que, a diferencia de deshabilitar un resumen, al eliminarlo, se efectuará el envío con los datos acumulados en base de datos de las alarmas contenidas para este resumen, del correo a los destinatarios correspondientes, para posteriormente eliminar dichos datos de base de datos, para así eliminar de forma efectiva cualquier rastro del

resumen. Si lo que realmente se desea es que el resumen deje de estar activo, pero que no se realice el envío del correo ni se eliminen los datos de la base de datos, entonces hay que deshabilitarlo y no eliminarlo.

5.3.9 Gestión de Descargas de CRLs. Caché de nivel 2

El nivel 2 de la caché lo compone una base de datos de CRL que se actualizan automáticamente mediante una tarea configurable en la plataforma utilizando la opción de Gestión de Descargas de CRL. La mejora que se busca está clara: evitar accesos redundantes a los diferentes Prestadores obteniendo la CRL una única vez y almacenándola en un servidor (Base de Datos) para que sea recuperada oportunamente. Como la validez de la CRL obtenida no es indefinida, la base de datos de CRL debe actualizarse cada cierto tiempo que puede ser definido por el usuario.

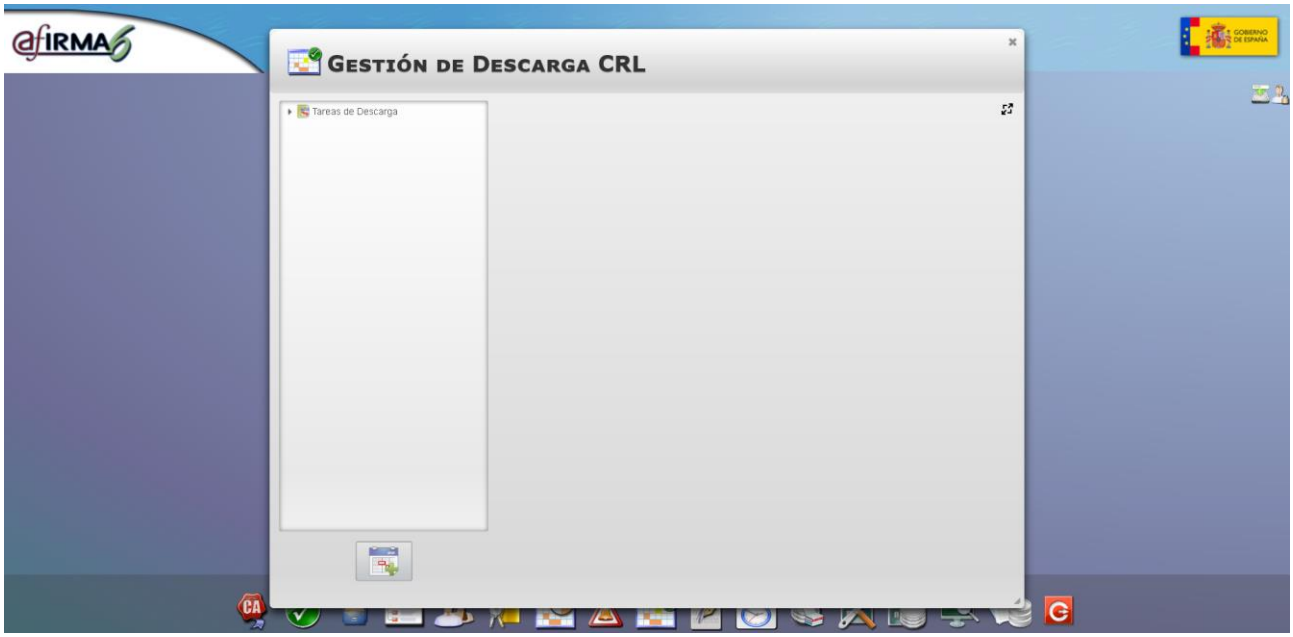


Figura 137 - Interfaz de Gestión de Tareas de Descarga de CRL

Para la descarga de cada CRL debe especificarse una tarea de descarga independiente (salvo en el caso de las CRL particionadas del EDNI, para lo cual se definirá una única tarea para la descarga de las N particiones). Las tareas de descarga se muestran en la parte izquierda de la pantalla, y su información en la parte derecha.

Las tareas realizarán la descarga de CRL haciendo uso de la información contenida en los métodos de validación especificados en la plataforma. Dicha información incluye el protocolo de comunicaciones, la ubicación de la CRL, su nombre, etc.

5.3.9.1 Dar de alta una nueva Tarea de descarga de CRLs



En la parte inferior del árbol de tareas de descarga, existe un botón ***"Añadir descarga de CRL"*** que permitirá crear una nueva tarea de descarga.



Figura 138 - Pantalla de Alta de Tarea de Descarga

Los datos a completar para el alta son los siguientes:

- **Identificador.** Identificador único de la tarea de descarga a crear.
- **Planificador de Refresco**. Intervalo de tiempo en minutos entre cada descarga de la CRL.
- **Tipo Descarga**. Puede ser *Simple* o *Múltiple*. Una tarea de descarga de tipo *Simple*, permite la descarga de una única CRL con un nombre específico. Las tareas de tipo *Múltiple* permiten la descarga de CRL particionadas del DNI Electrónico y su misión es la descarga de un número

bien definido de CRL con identificadoras variables que utilizan un patrón fijo en su composición.

- **Número de particiones**. Este parámetro únicamente está disponible para tareas de tipo Múltiple, y especifica el número de CRL que deben descargarse para cada partición especificada posteriormente.

Una vez completada esta información, se pulsa el botón ***"Guardar"***, creándose la tarea.

5.3.9.1.1 Modificación de grupo de descarga de CRL



Para completar el alta de la tarea, es necesario realizar otro paso adicional. Del menú de tareas se selecciona la tarea que se acaba de dar de alta, mostrándose su información en la parte derecha de la pantalla.

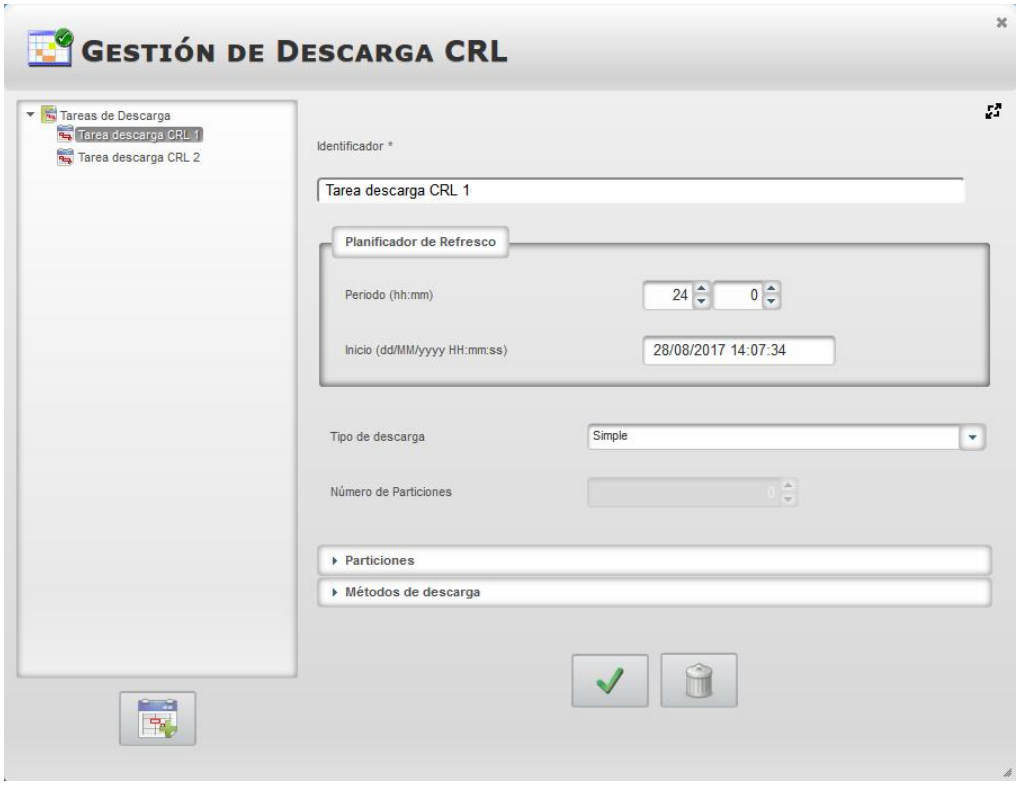


Figura 139 - Modificación de Tarea de Descarga (I)

En caso de haber especificado el tipo *Múltiple* en el alta de la tarea, es necesario definir cada una de las particiones que se deben descargar de la CRL. Como ya se ha comentado una CRL particionada es una CRL completa que se divide en un número determinado de archivos de CRL. Estos archivos tienen

un nombre diferente pero que se ajusta a un determinado patrón y que se compone de una cadena literal constante, un número de CRL y un identificador de partición. Los identificadores de partición se dan de alta por medio de la tabla “Particiones A Descargar” y de los botones “Añadir” y “Eliminar”.

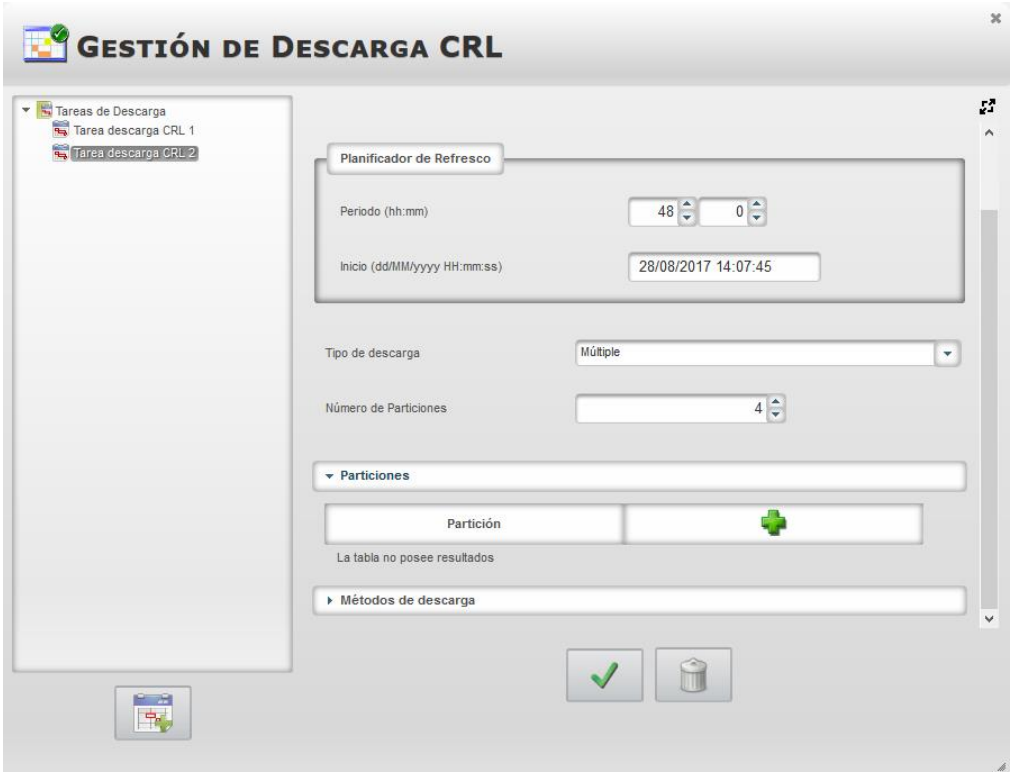


Figura 140 - Modificación de Tarea de Descarga (II)

Por último, y tras especificar las particiones (en caso de ser necesario), se deben especificar los métodos de descarga que se van a utilizar para obtener la información de las CRL a descargar. Estos métodos se corresponden con los métodos de validación previamente añadidos, además para que la descarga tenga efecto hemos debido marcar la casilla “Almacenar CRL” al dar de alta el método de validación. Al igual que en la configuración de métodos de validación para los Prestadores, en este caso se podrán especificar varios, definiendo la prioridad en que serán utilizados.

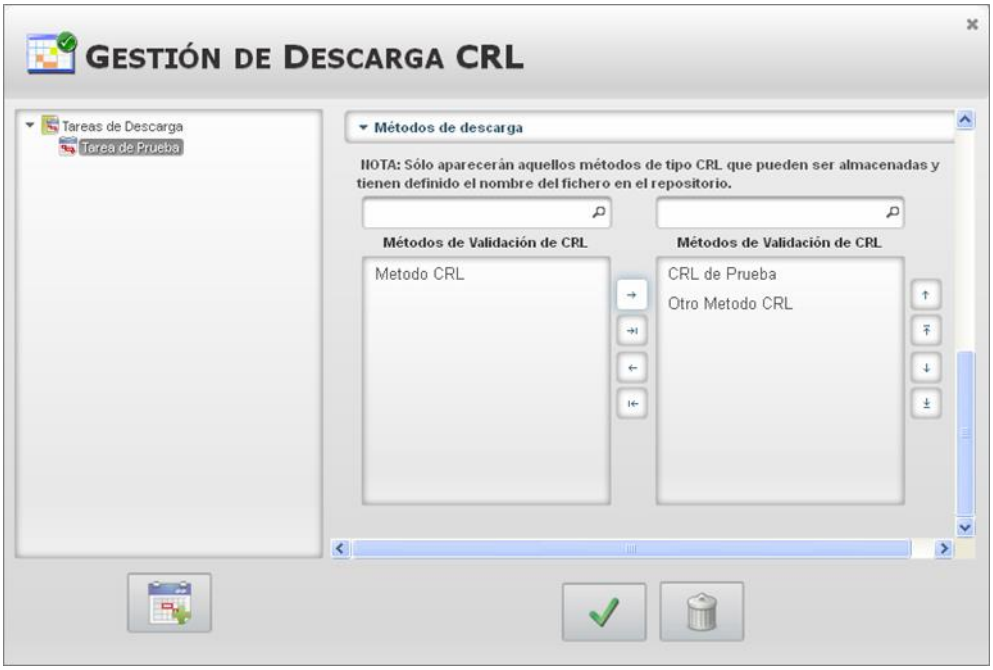


Figura 141 - Modificación de Métodos de Descarga

Tanto las particiones como los métodos de descargar se modifican directamente sobre la configuración, sin necesidad de tener que pulsar el botón ***"Modificar"*** para llevar a cabo este proceso.

5.3.10 Gestión de Políticas de Firma

La plataforma @firma incluye un gestor de políticas de firma desde el que dar de alta versiones de políticas, y sus implementaciones XML y/o ASN.1, a utilizar en los procesos en firma y validación.

Actualmente la plataforma sólo contempla las políticas de la AGE y FacturaE.

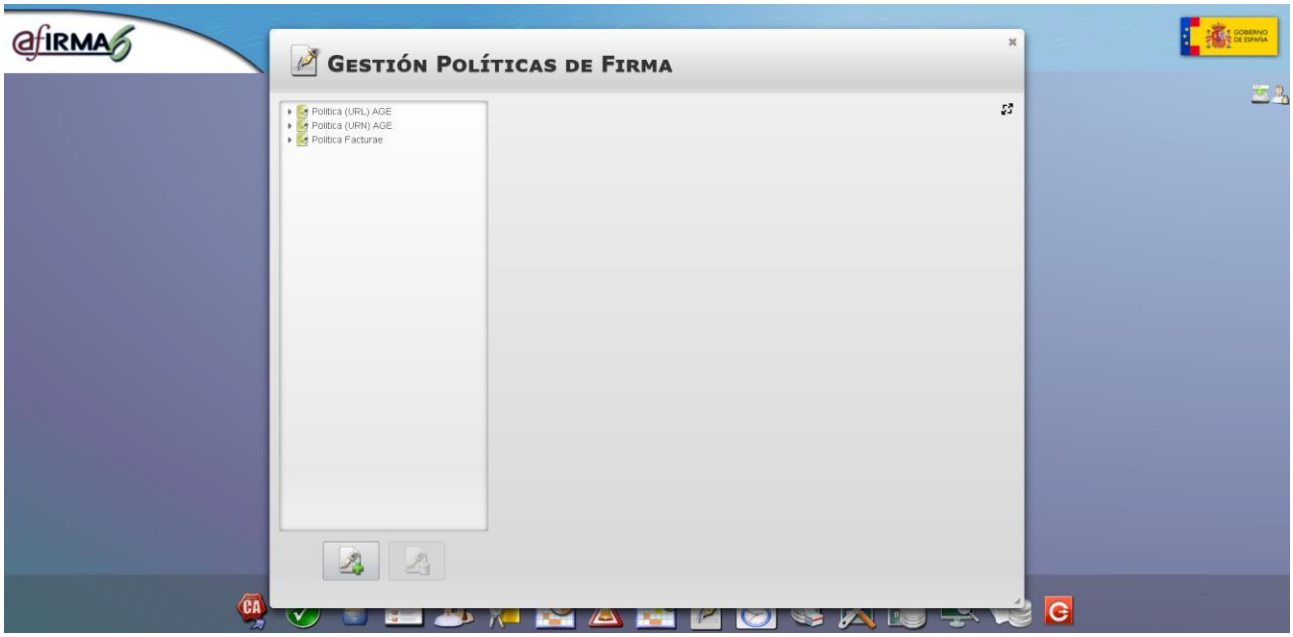


Figura 142 - Interfaz de Gestión de Políticas de Firma

En la parte izquierda de la interfaz se muestra un árbol que aloja las políticas de firma y las distintas versiones de las políticas registradas en la plataforma. En la zona central se visualizará la información de configuración de las Políticas de Firma y de sus implementaciones en XML y ASN.1.

Mediante este gestor es posible realizar las siguientes operaciones:

- Sobre Políticas de Firma no registradas
    - Alta de nueva versión de Políticas de Firma.
- Sobre las políticas registradas:
    - Modificación de los datos de gestión de la política.
    - Alta de documento legible correspondiente a la política de firma.
    - Eliminar Versión de Política de Firma.
    - Alta de implementación en XML
    - Alta de implementación en ASN.1

- Descarga de los documentos registrados con la política: documento legible, documento XML y estructura ASN.1

A continuación, se detallan las diferentes operaciones, así como los datos que intervienen en cada una de ellas.

5.3.10.1 Alta de una nueva versión de Política de Firma



Se permite registrar una versión de una política existente, o de una política de firma que aún no se encuentra registrada en el sistema. Para ello será necesario pulsar el botón ***"Añadir Política de Firma"*** situado en la zona inferior del árbol de políticas. Tras pulsar dicho botón aparecerá el formulario de alta.



Figura 143 - Ventana Alta Política de Firma

Los datos solicitados en la ventana de alta de política de firma son los siguientes:

- **Alias**: Campo obligatorio. Se puede indicar un alias nuevo o seleccionar uno ya existente.

- **Emisor**: Campo obligatorio con el nombre del emisor.
- **Fecha emisión**: Campo obligatorio con la fecha de emisión de la política.
- **Valido desde**: Campo obligatorio con la fecha inicial de validez para firma de la política.
- **Válido hasta**: Campo opcional con la fecha final del periodo de validez para firma.
- **Versión**. Campo obligatorio con el número/nombre de versión.
- **Estado**. Estado de la política de firma, los estados en lo que se puede encontrar es habilitado o deshabilitado para la firma.
- **Fichero con la política legible**: Campo obligatorio. Se ha de adjuntar el documento legible de la política.

5.3.10.2 Consulta de una versión de Política de Firma

Una vez dada de alta, la política registrada aparecerá en el árbol de "Políticas de Firma existentes". Al seleccionar una de las versiones registradas, de una determinada política, se mostrarán los datos de la política:



Figura 144 - Ventana Datos Política de Firma (I)



Figura 145 - Ventana Datos Política de Firma (II)

Desde esta consulta se permiten realizar distintas acciones sobre la versión de la política de Firma seleccionada:

- **Descargar documentos relacionados con la política**: documento legible, implementación en XML y/o implementación en ASN.1.
- Realizar el **alta del documento legible** de la política modificando el existente
- **Modificar los datos** de gestión de la Política de Firma
- **Eliminar la versión** de la Política de Firma
- Realizar el **alta** de una **implementación XML y/o ASN.1**.

En los siguientes apartados se detallan las operaciones que se pueden realizar sobre las versiones de Políticas de Firma registradas en el sistema.

5.3.10.3 Modificar datos de gestión de Política de Firma



Se pueden editar los datos de gestión directamente desde la consulta de la política de firma. Los datos de gestión que se pueden modificar son: Alias de la política, Emisor, Fecha de emisión, validez desde, validez hasta, versión y estado.

Una vez indicados los valores deseados es necesario hacer clic en el botón "Modificar Datos" para actualizar la información.

5.3.10.4 Eliminar versión de Política de Firma existente



Desde la consulta de una Política de Firma se permite realizar la baja de dicha versión realizando clic en el botón ***"Eliminar esta versión de la política"***.

La herramienta nos pedirá confirmación de la acción que se va a realizar:

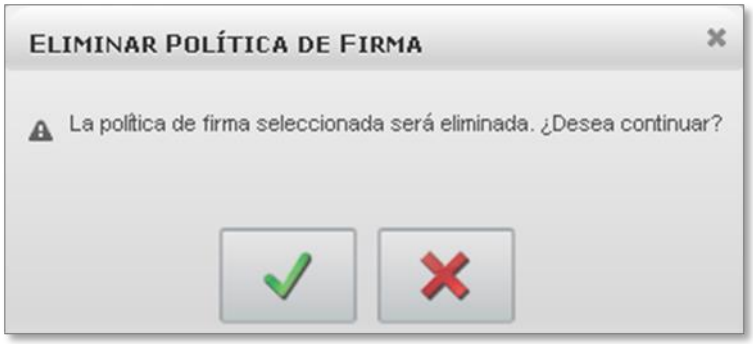


Figura 146 - Ventana Confirmación Eliminar Versión de Política de Firma

Una vez confirmada la acción, se eliminan los datos de gestión de la versión y sus implementaciones XML y ASN.1; así como los documentos asociados a la versión de la política: documento legible, implementación XML y/o fichero con estructura ASN.1

5.3.10.5 Alta de implementaciones XML y ASN.1 de Políticas de Firma





Al consultar los datos de la política de firma; además de los datos de gestión de la versión de política, se muestra la información de las implementaciones XML y ASN.1 asociadas a la versión de la política de firma consultada:

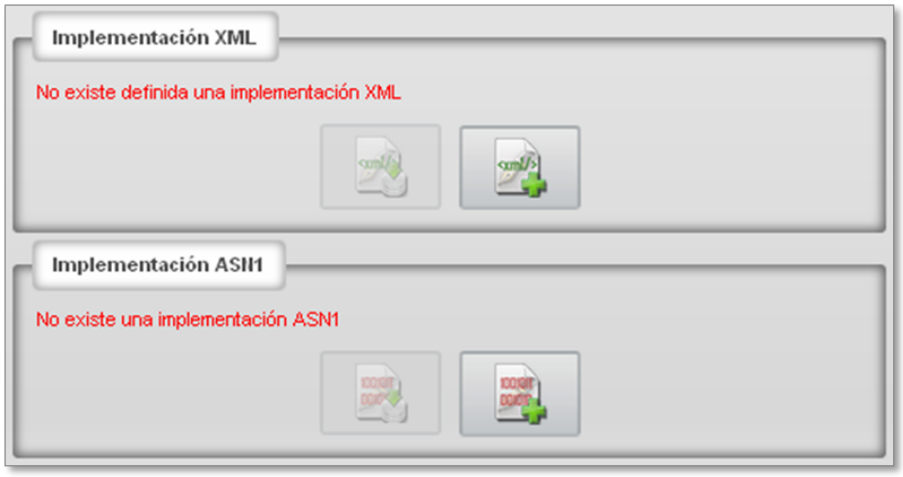


Figura 147 - Información Implementaciones de Política de Firma

Se puede dar de alta, o en su caso modificar la implementación existente, haciendo click en "Upload Implementación XML" o "Upload Implementación ASN.1"; dependiendo de la implementación a dar de alta. Esta acción nos mostrará una ventana donde se solicitan los datos de la implementación:



Figura 148 - Ventana Alta Implementación XML



Figura 149 - Ventana Alta Implementación ASN.1

La información solicitada para dar de alta una implementación es la siguiente:

- **Implementación en XML/ASN.1**: Fichero con la implementación XML o estructura ASN.1

- **Parseador**: Se habrá de seleccionar uno de los parseadores/versiones disponibles. El fichero indicado ha de poder ser interpretado por el parseador seleccionado para que se permita el alta.

Tras importar la/s implementación/es de la política ASN.1 y/o XML, aparecerá en el área de consulta de la política seleccionada la información obtenida de las implementaciones adjuntadas.

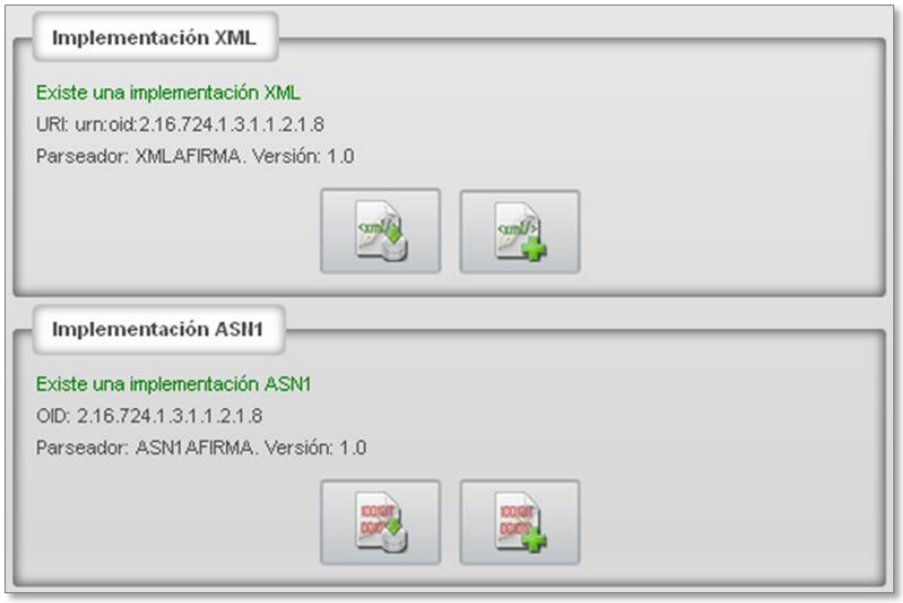


Figura 150 - Información Políticas ASN.1 y XML

NOTA: Para la política de firma de la AGE v 1.9, tanto para la implementación ASN.1, como para la implementación XML, se deberá seleccionar la versión 1.1 del parseador respectivo.

5.3.10.6 Descarga de documentos de Políticas de Firma



Al consultar la información de una versión de una Política de Firma, en cualquier caso se podrá descargar el documento legible de la política de firma haciendo clic en ***"Descargar documento legible"***.




En los casos que se encuentre disponible también se puede descargar el fichero con la implementación XML y/o estructura ASN.1 haciendo clic en ***"Descargar Implementación XML"*** y ***"Descargar Implementación ASN1"*** respectivamente.

5.3.11  Gestión de TSA

La gestión de los distintos servidores TSA se realizará desde la Herramienta de Administración. Mediante el componente de Gestión de TSA se podrá asignar servidores TSA a aplicaciones registradas en la plataforma, de manera que la plataforma pueda conectarse a los mismos en función de un orden de prioridad establecido para la generación de sellos de tiempo.

Dado que el MINHAFP dispone de su propia TSA, la plataforma @firma, por defecto, la tendrá configurada para permitir la interacción con la misma desde sus servicios web y RFC-3161.

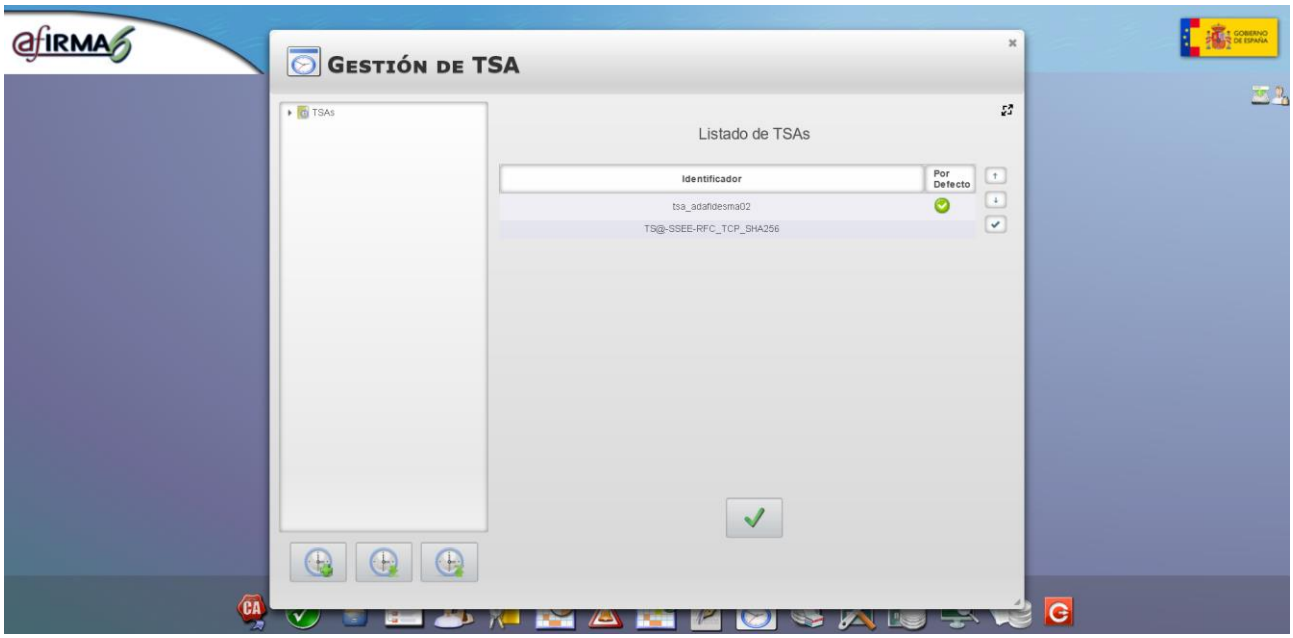


Figura 151 - Interfaz de Gestión de TSA

La ventana, en la zona central, dispone el listado de TSA existentes, ordenadas descendentemente por orden de prioridad de conexión, es decir, la primera en la lista será la primera a la que conectarse, y a medida que se bajen posiciones en la lista, se bajará en prioridad de conexión.

A la derecha de la lista se ubican 2 botones, el que está situado en la zona superior sirve para, una vez marcada una TSA de la lista, desplazarla hacia arriba en la misma, salvo que se encuentre en la primera posición, en cuyo caso no ascenderá más. El botón situado en la zona inferior sirve para, una vez marcada una TSA de la lista, desplazarla hacia abajo en la misma, salvo que se encuentre en la última posición, en cuyo caso no descenderá más.

En la zona inferior de la ventana se encuentran 2 grupos de botones.

A la izquierda hay un grupo de 3 botones:



El primero inicia el formulario para dar de alta una nueva TSA.



El segundo permite realizar la importación de configuración de una (o más) TSA mediante un fichero XML, que previamente fue exportado.



El tercero permite realizar la exportación de configuración de una (o más) TSA mediante un fichero XML.

En el centro de la zona inferior de la ventana se encuentra un único botón que sirve para almacenar el orden de prioridad de conexión definido para la lista de TSA tras haber sido modificado.

5.3.11.1 Gestión de TSA – Datos Generales

A continuación, se muestra cómo será la ventana de Datos de TSA dentro de la Gestión de TSA, en concreto, el grupo de propiedades que hacen referencia a los datos generales para una TSA:

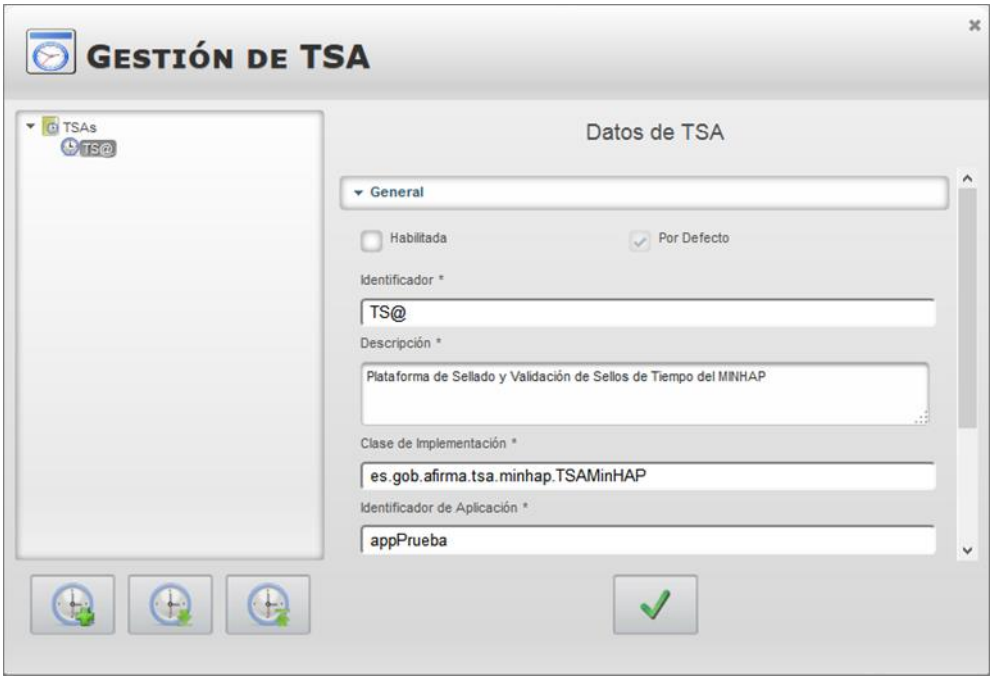


Figura 152 - Pantalla Edición de Datos Generales de TSA (I)

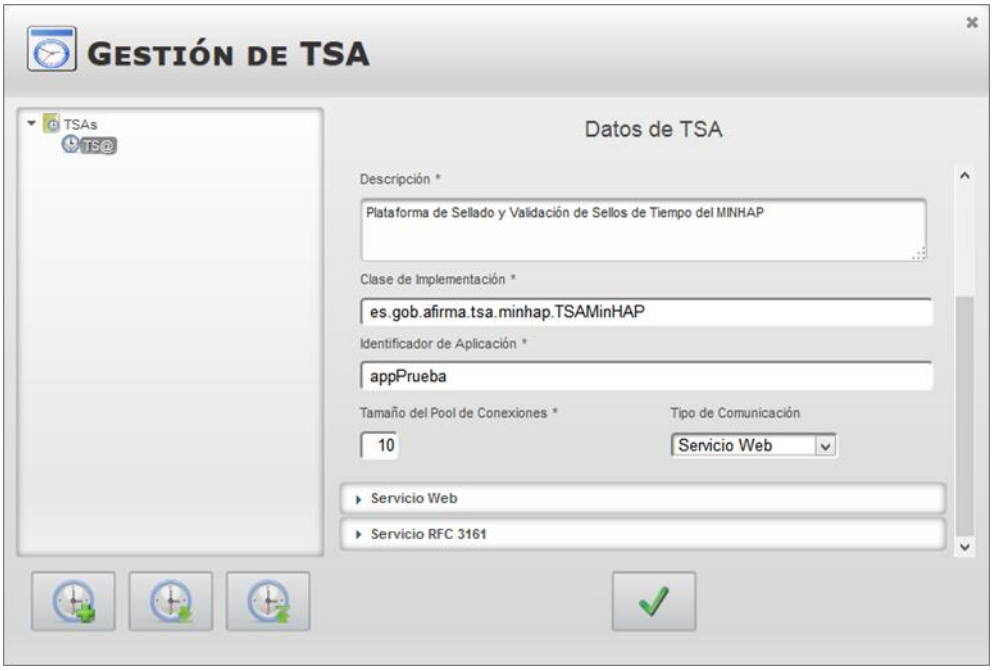


Figura 153 - Pantalla Edición de Datos Generales de TSA (II)

La ventana, en la zona superior izquierda tendrá un árbol con las TSA almacenadas en BBDD, listadas por su identificador de manera ascendente. Al pulsar sobre alguna de ellas se cargarán sus datos en la zona derecha de Datos de TSA.

Los datos generales de los que se compondrá una TSA son:

- **Identificador:** Cadena de texto que identifica unívocamente a la TSA. Es un campo obligatorio.
- **Habilitada:** Indicador que determina si la TSA está habilitada (se puede llevar a cabo comunicación con la misma) o deshabilitada (no se puede llevar a cabo comunicación con la misma).
- **Descripción:** Texto descriptivo que define la TSA. Es un campo obligatorio.
- **Clase de Implementación:** Nombre completo de la clase Java que gestiona la comunicación con la plataforma TSA. Es un campo obligatorio.
- **Tamaño del Pool de Conexiones:** Número de conexiones permitidas en el pool de conexiones contra dicha TSA. Sobrepasado dicho número no se permitirá llevar a cabo más conexiones. Es un campo obligatorio.

- **Identificador de Aplicación**: Identificador de aplicación para la plataforma @firma, registrada en la TSA para permitir la comunicación. Es un campo obligatorio.

- **Tipo de Comunicación**: Valor que describe el servicio a utilizar para realizar a cabo las operaciones de sellado y resellado con la TSA. Los valores posibles son: Servicio Web y Servicio RFC 3161. Es un campo obligatorio.

En la zona inferior central se localiza el botón para almacenar los datos de la TSA en la BBDD.

5.3.11.2 Gestión de TSA – Datos Servicio Web

A continuación, se muestra cómo será la ventana de Datos de TSA dentro de la Gestión de TSA, en concreto, el grupo de propiedades que hacen referencia a los datos de comunicación por servicio web para una TSA:

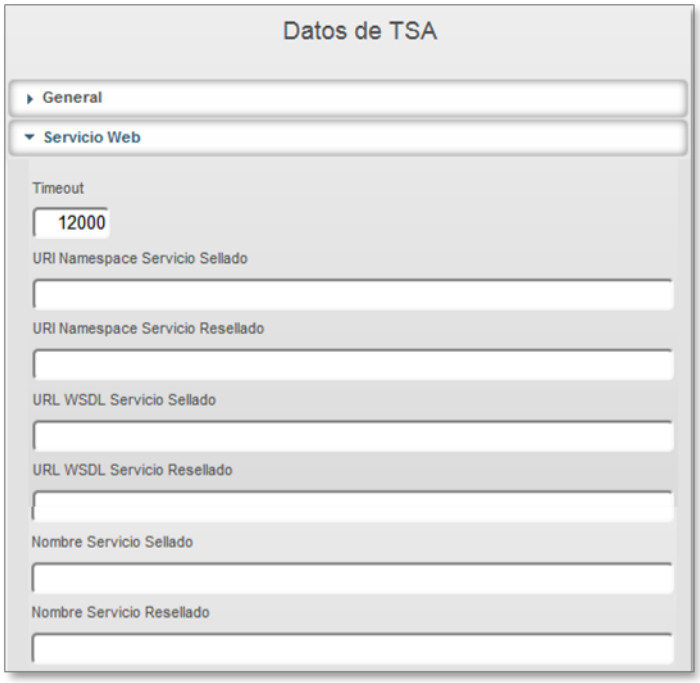


Figura 154 - Pantalla Edición de Datos Servicio Web de TSA (Datos y Endpoints)

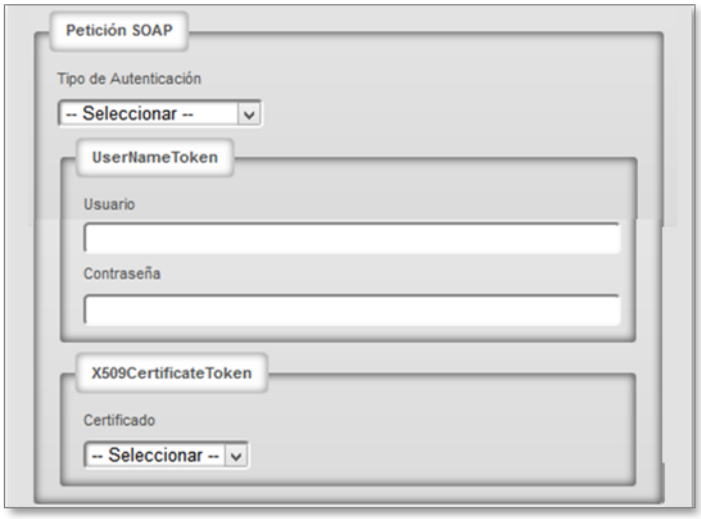


Figura 155 - Pantalla Edición de Datos Servicio Web de TSA (Petición)

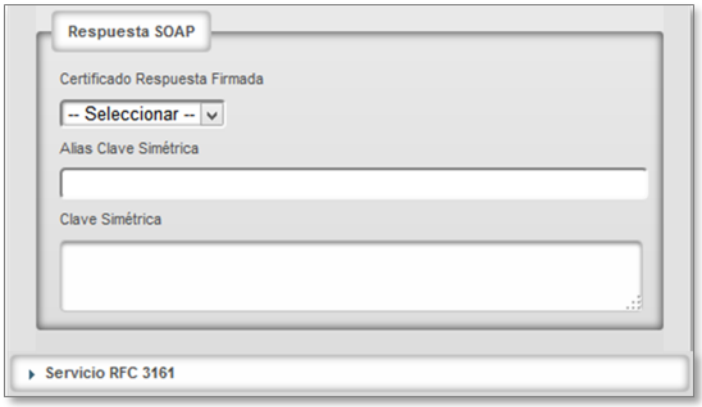


Figura 156 - Pantalla Edición de Datos Servicio Web de TSA (Respuesta)

Los datos de comunicación por servicio web de los que se compondrá una TSA son:

- **Timeout:** Tiempo de vida, en milisegundos, para las peticiones SOAP a la TSA.
- **URI Namespace Servicio Sellado:** URI del Namespace de acceso al servicio de sellado de la TSA.
- **URI Namespace Servicio Resellado:** URI del Namespace de acceso al servicio de resellado de la TSA.
- **URL WSDL Servicio Sellado:** URL de acceso al servicio de sellado de la TSA.
- **URL WSDL Servicio Resellado:** URL de acceso al servicio de resellado de la TSA.

- **Nombre Servicio Sellado:** Nombre del servicio de sellado de la TSA.
- **Nombre Servicio Resellado:** Nombre del servicio de resellado de la TSA.
- **Tipo de Autenticación:** Tipo de autenticación para las peticiones SOAP a la TSA. Los valores posibles son: UserNameToken y X509CertificateToken.
- **Usuario:** Nombre de usuario para el tipo de autenticación UserNameToken.
- **Contraseña:** Contraseña para el tipo de autenticación UserNameToken.
- **Certificado (X509CertificateToken):** Alias del certificado a usar para el tipo de autenticación X509CertificateToken.
- **Certificado Respuesta Firmada:** Alias del certificado a usar para validar las respuestas de la TSA que se encuentren firmadas.
- **Alias Clave Simétrica:** Alias de la clave simétrica usada para descifrar las respuestas SOAP que se encuentren cifradas.
- **Clave Simétrica:** Valor de la clave simétrica usada para descifrar las respuestas SOAP que se encuentren cifradas.

5.3.11.3 Gestión de TSA – Datos Servicio RFC 3161

A continuación, se muestra cómo será la ventana de Datos de TSA dentro de la Gestión de TSA, en concreto, el grupo de propiedades que hacen referencia a los datos de comunicación por servicio RFC 3161 para una TSA:

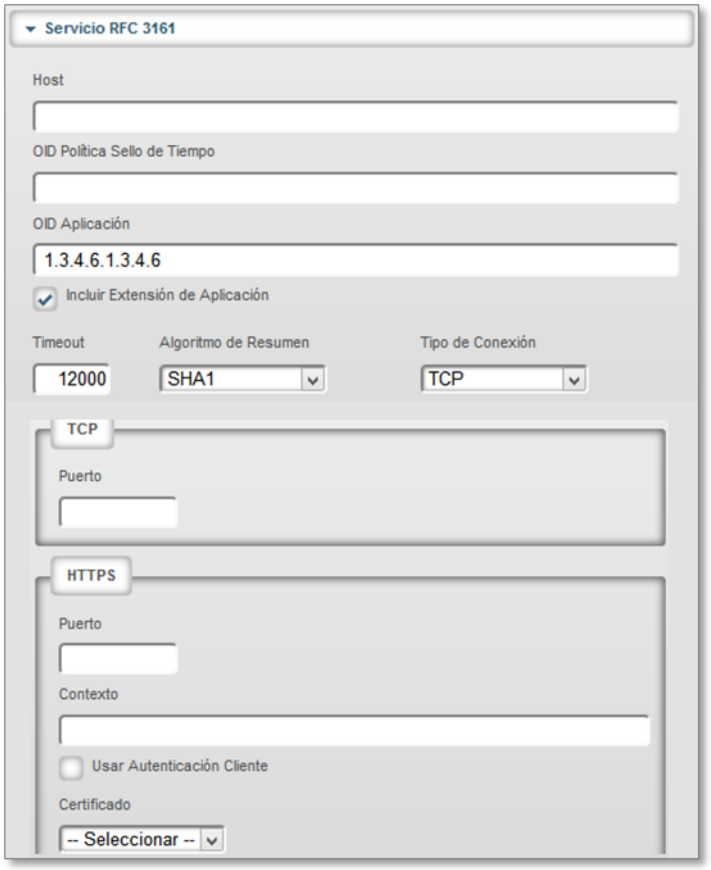


Figura 157 - Pantalla Edición de Datos Servicio RFC 3161 de TSA (I)

Los datos de comunicación por servicio RFC 3161 de los que se compondrá una TSA son:

- **Host:** Dirección host donde se encuentra desplegado el servicio RFC 3161.
- **OID Política Sello de Tiempo:** OID de la política de sello de tiempo a indicar en la petición.
- **OID Aplicación:** OID que identifica la extensión que alberga el identificador de aplicación en la petición.
- **Incluir extensión de Aplicación:** Si queremos guardar también la extensión de la aplicación marcamos este check.

- **Timeout:** Tiempo de vida para las peticiones al servicio RFC 3161, en milisegundos.
- **Algoritmo de Resumen:** Algoritmo de resumen que aplicar sobre los datos a sellar. Los valores posibles son: SHA, SHA-256, SHA-512, y RIPEMD-160.
- **Tipo de Conexión:** Tipo de conexión a utilizar para comunicarse con el servicio RFC 3161. Los valores posibles son: TCP, HTTPS, y SSL.
- **Puerto (TCP):** Número del puerto donde se encuentra desplegado el servicio RFC 3161.
- **Puerto (HTTPS):** Número del puerto donde se encuentra desplegado el servicio RFC 3161 por HTTPS.
- **Contexto**: Contexto para la conexión con el servicio RFC 3161 por HTTPS.
- **Certificado (HTTPS):** Alias del certificado a usar para la autenticación HTTPS del cliente.
- **Usar Autenticación Cliente:** Indicador para utilizar autenticación HTTPS mediante certificado cliente o no.

5.3.11.4 Gestión de TSA – Crear TSA



Para dar de alta una nueva TSA deberemos de pulsar el icono “Crear TSA” con lo que nos aparecerá la siguiente pantalla, rellenando los datos tal y como se ha indicado anteriormente, las pestañas “General”, “Servicio Web” y “Servicio RFC 3161”:

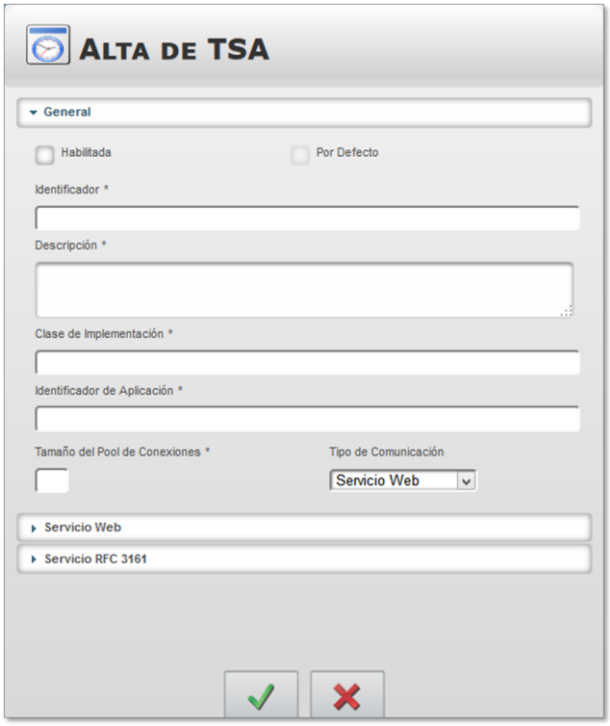


Figura 158 - Pantalla de Alta de TSA: Datos Generales

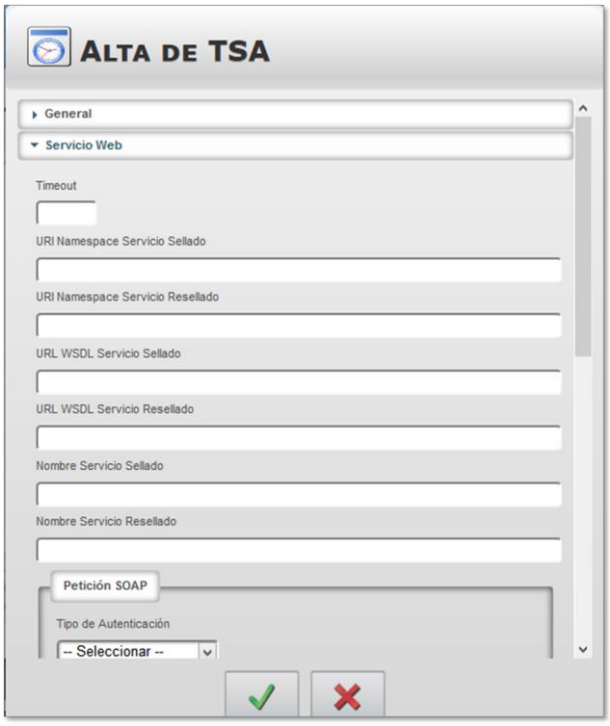


Figura 159 - Pantalla de Alta de TSA: Datos Servicio Web

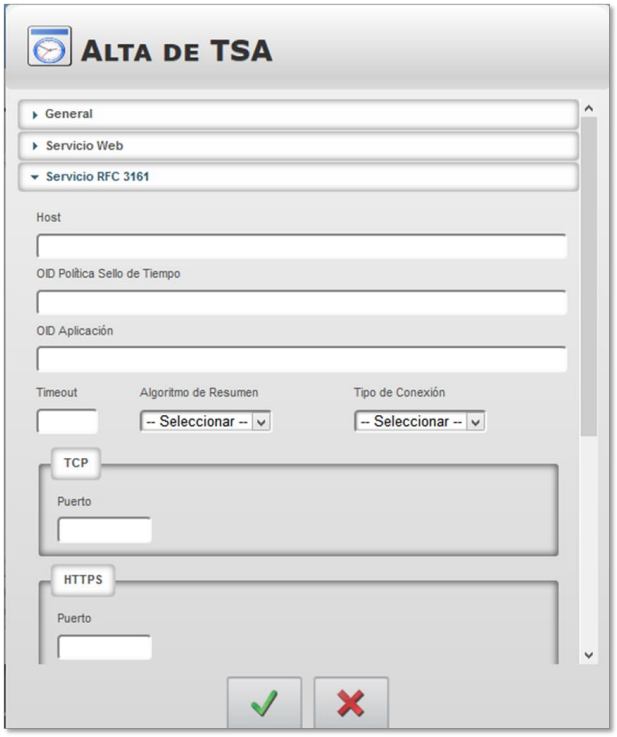


Figura 160 - Pantalla de Alta de TSA: Datos Servicio RFC 3161

5.3.11.5 Gestión de TSA – Importar TSA



Para importar a un fichero las diferentes TSA deberemos de pulsar el botón "Importar TSAs" apareciéndonos la pantalla siguiente:



Figura 161 - Pantalla de Importación de TSA

Aquí seleccionaremos el XML que contenga las TSA a importar y pulsaremos el botón "Importar TSAs". Si queremos salir de esta pantalla bastaría con pulsar en cancelar.

5.3.11.6 Gestión de TSA – Exportar TSA



Para exportar a un fichero las diferentes TSA deberemos de pulsar el icono “Exportar TSAs” apareciéndonos la pantalla siguiente donde elegiremos las TSA que queramos exportar, usando los botones centrales, y finalmente cuando nuestro conjunto de TSA esté completo pulsaremos en “Exportar TSAs”:



Figura 162 - Pantalla de Exportación de TSA

Esto nos generará un fichero que podremos guardar en nuestro equipo.

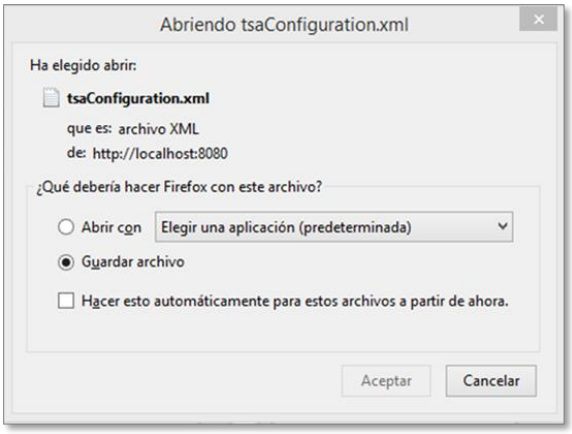


Figura 163 - Descarga de Fichero de Exportación de TSA

Es importante indicar que, por motivos de seguridad, en las exportaciones no se incluye la información privada como contraseñas o partes privadas de certificados.

5.3.12 Gestión de Gestores Documentales

La plataforma @firma incluye un componente para la configuración de los gestores documentales con los que interacciona la plataforma.



Figura 164 - Ventana de Gestión de Gestores Documentales

En la parte izquierda de la interfaz se muestra un árbol que aloja los distintos gestores documentales registrados en la plataforma. En la zona central se visualizará la información de configuración de establecida para un gestor documental concreto.

Mediante este gestor es posible realizar las siguientes operaciones asociadas a la configuración de un gestor documental:

- Alta de una nueva configuración.
- Consultar los gestores documentales configurados en la plataforma.
- Modificación de una configuración existente.
- Baja de una configuración establecida.

5.3.12.1 Alta de una nueva configuración de gestor documental



Se puede registrar una nueva configuración para un determinado gestor documental pulsando el botón ***"Alta Gestor Documental"***. Al pulsar el botón se muestra una ventana de "Alta" como la siguiente.



Figura 165 - Ventana de Alta Gestor Documental

Como observamos esta ventana se compone de tres campos:

- **Tipo de Gestor.** Nombre del Gestor documental.
- **Clase de Implementación.** Clase que implementa el controlador del gestor documental.
- **Parámetros Adicionales.** Conjunto de parámetros adicionales de configuración que deben establecerse para el gestor documental concreto. Mediante el botón  damos de alta parámetro nuevos

5.3.12.2 Alta Instancia Gestor Documental



Una vez dada de alta la configuración del gestor documental, podemos dar de alta una instancia de la configuración del mismo. Para ello pulsaremos el botón ***"Alta Instancia"***.



Figura 166 - Ventana de Alta Instancia Gestor Documental

Este formulario contiene los siguientes campos:

- **Identificador.** Identificador que poseerá la instancia del Gestor Documental.
- **Tipo de Gestor.** Configuración que poseerá la instancia.
- **URL Gestor.** URL donde se encuentra el Gestor documental.
- **Timeout (ms).** Tiempo máximo de espera de respuesta del gestor documental.
- **Tipo de autenticación.**
  - Sin autenticación
  - Mediante Usuario y Contraseña.
- **Datos que poseerán los parámetros adicionales.**

5.3.12.3 Consulta, Modificación o Baja de una configuración de gestor documental

Si seleccionamos un determinado gestor documental nos aparecerán los datos asociados en la parte derecha de la pantalla tal y como se observa en la siguiente figura.



Figura 167 - Ventana Mostrar Gestor Documental



Desde esta pantalla podemos consultar/modificar la información de configuración del gestor documental concreto.



De igual forma si pulsamos el botón “Baja” eliminaremos la configuración del gestor seleccionado.

5.3.13 Gestión de Configuración

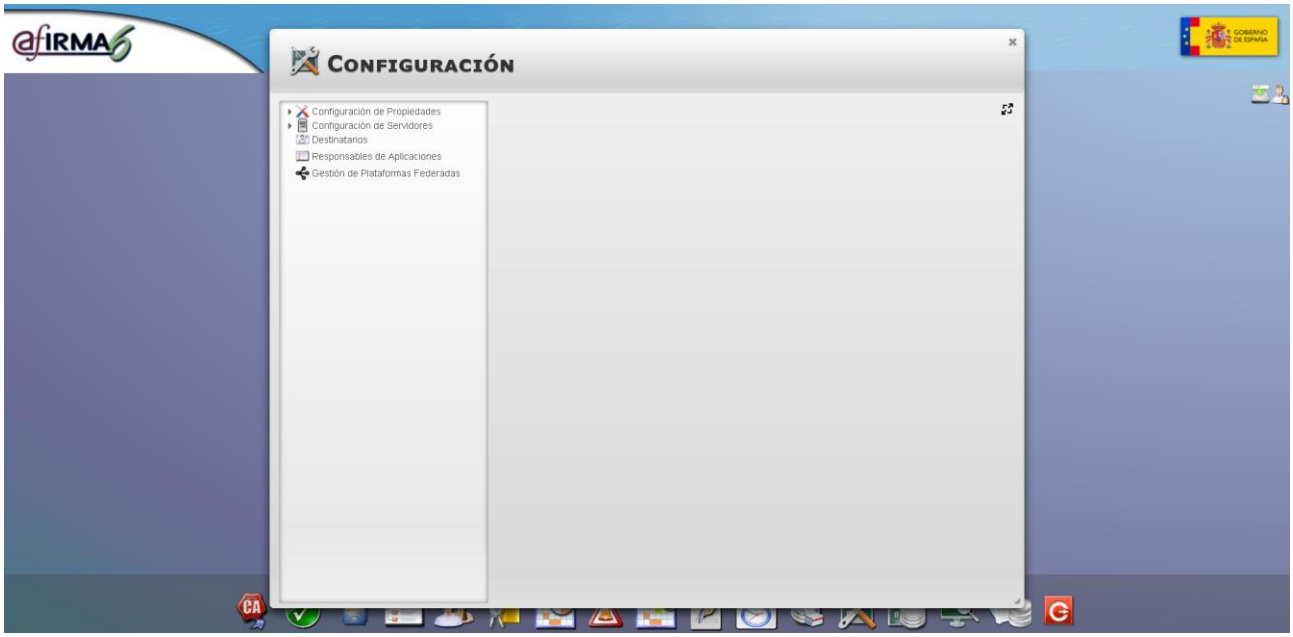


Figura 168 - Ventana Gestión de Configuración

El módulo de Gestión de Configuración permite al administrador:

- Configurar las propiedades de la plataforma.
- Configurar los servidores internos.
    - OCSP.
    - Correo.
    - SMS.
    - Gestión de caché.
    - Servidor Secundario de Validación.
    - valET
- Destinatarios.
- Responsables de Aplicaciones.
- Gestión de las plataformas federadas.

5.3.13.1 Configuración propiedades de la plataforma



Figura 169 - Ventana Gestión de Configuración (I)

Todas las propiedades del sistema están organizadas en grupos en función del área de la plataforma a la que afecta:

5.3.13.1.1 General

Las propiedades que se pueden modificar en este grupo son:

- Tamaño máximo (en bytes) permitido para los ficheros a importar desde la administración.
- Número máximo de transacciones de auditoría a mostrar en una administración delegada.
- Nombre del campo lógico que contendrá el nombre del usuario a logarse.

- Nombre del campo lógico que contendrá el apellido del usuario a logarse.

- Listado de protocolos restringidos para el cifrado SSL de conexiones externas (por ejemplo, al obtener una CRL de una ruta HTTPS): Por defecto se incluye SSLv2Hello por considerarse deprecado. Se deben incluir los nombres exactos de los protocolos a restringir separados por comas.

- Listado de algoritmos restringidos para el cifrado SSL de conexiones externas (por ejemplo, al obtener una CRL de una ruta HTTPS). Realmente se incluyen partículas contenidas dentro del nombre completo de los algoritmos (separadas por comas). Por defecto se incluyen _DHE_ y _DH_, que hacen referencia a los algoritmos de Diffie-Hellman, los cuales son problemáticos para certificados de más de 1024 bits.

- Tiempo de espera antes de detener la anterior caché local tras realizar una recarga de esta (al recargar se realiza sobre una nueva instancia de caché). De esta forma se da tiempo a que aquellas peticiones que están haciendo uso de objetos de la anterior caché, puedan finalizar correctamente.

- Activación de la restricción a la definición del CONTENT-LENGTH en la cabecera HTTP (error 411 de HTTP 1.1).

- Clave de cifrado AES para las contraseñas del sistema.

- Password de acceso al HSM. Esta propiedad puede estar vacía en caso de no ser necesario dicho Password.

5.3.13.1.2 Control del Usuario

Las propiedades que se pueden modificar en este grupo son:

- Expresión regular que controla las contraseñas de usuario que van a ser creadas. Por defecto: *"^.*(?=.{10,})(?=.*[0-9])(?=.*[a-z])(?=.*[A-Z])(?=.*[@#$%^&+=]).*$"*. *Concretamente esta expresión regular viene a indicar una contraseña con una longitud mínima de 10 caracteres en los que debe haber al menos una minúscula, una mayúscula, algún dígito (del 0 al 9) y alguno de los símbolos indicados (@#$%^&+=).*

- Número de intentos para insertar la contraseña antes de bloquear el usuario.

5.3.13.1.3 Mapeos

Las propiedades que se pueden modificar en este grupo son:

- Listado de partículas aplicables a los mapeos tanto del primer como del segundo apellido. Por defecto: “DEL, LOS, LAS, SOC, DE, LA, AL, SA, SL, SC, CB, EL, Y, I, DO, DOS, E, DA, DAS, SAN”.

5.3.13.1.4 Proxy

Las propiedades que se pueden modificar en este grupo son:

- Modo de operación a utilizar en el proxy: A escoger entre *NONE*, *NONE_AUTHENTICATION*, *BASIC_AUTHENTICATION* y *NTLM_AUTHENTICATION*.
- Modo de operación a utilizar en el proxy por el canal seguro (por ejemplo, HTTPS): A escoger entre *NONE*, *NONE_AUTHENTICATION*, *BASIC_AUTHENTICATION* y *NTLM_AUTHENTICATION*.
- Dirección IP del proxy.
- Dirección IP del proxy para el canal seguro.
- Puerto asignado al proxy.
- Puerto asignado al proxy para el canal seguro.
- Nombre de usuario en caso de necesitar autenticación.
- Nombre de usuario en caso de necesitar autenticación para el canal seguro.
- Contraseña asignada al usuario en caso de necesitar autenticación.
- Contraseña asignada al usuario en caso de necesitar autenticación para el canal seguro.
- Dominio del usuario en caso de autenticación NTLM.

- Dominio del usuario en caso de autenticación NTLM para el canal seguro.
- Listado de direcciones para las que no se utilizará el proxy.
- Indicador para utilizar el analizador de direcciones, de modo que si se trata de una dirección local, no sea utilizado el proxy para realizar la conexión.
- Workstation del usuario en caso de que el proxy necesite autenticación NTLM.
- Workstation del usuario en caso de que el proxy seguro necesite autenticación NTLM.

5.3.13.1.5 Fachada de servicios Web

Las propiedades que se pueden modificar en este grupo son:

- URL donde se publicarán los *SCHEMAS* asociados a las peticiones de entrada y salida a la plataforma.
- En el resto de propiedades se definen para los servicios web ofrecidos en la plataforma, los paquetes (a nivel de código) de los distintos traductores (estas propiedades no deben ser modificadas inicialmente), los espacios de nombres asignados y los esquemas asociados. **Estas propiedades no deben ser modificadas.**

5.3.13.1.6 Validación

Las propiedades que se pueden modificar en este grupo son:

- Indicador para validar los certificados a dar de alta de manera estricta, tal y como se especifica en la RFC 3280.
- Indicador para utilizar la librería de Jakarta para las conexiones HTTP, o la proporcionada por Sun en la JRE.
- Indicador para utilizar la librería de Novell para las conexiones LDAP, o la proporcionada por Sun en la JRE.

- Tamaño máximo permitido (en bytes) de descarga en las conexiones que se realicen. Por defecto 5242880 bytes.

- Indicador para comprobar el estado de revocación del certificado incluido en el token de seguridad *BinarySecurityToken* del mensaje SOAP.

- Fecha a partir de la cual todos los sellos de tiempo serán validados respecto a la RFC 5816.

5.3.13.1.7 Políticas de Custodia

Las propiedades que se pueden modificar en este grupo son:

- Indicador para almacenar las peticiones SOAP recibidas. En el caso de indicar “false” se realizará la custodia del hash de la petición.

- Indicador para almacenar las respuestas SOAP generadas por la plataforma. En el caso de indicar “false” se realizará la custodia del hash de la respuesta.

- Formato del hash que se almacena de la petición/respuesta SOAP, aplicará en el caso de indicar “false” en alguna de las propiedades anteriores. Se debe escoger entre “SHA1”, “SHA256” y “SHA512”.

- Modo de almacenamiento de las peticiones/respuestas SOAP o de sus respectivos hashes. Si el valor escogido es 0, las peticiones/respuestas se almacenarán en base de datos. Si el valor escogido es 1, las peticiones/respuesta se almacenarán en el sistema de ficheros.

- Número máximo de ficheros almacenados por directorio generado para el almacenamiento de las peticiones y las respuestas SOAP (modo 1).

- Número máximo de hilos permitidos en el pool para la creación de los ficheros (modo 1).

- Custodia de Aplicaciones: Indicador para forzar la custodia de peticiones a todas las aplicaciones.

- Custodia de Aplicaciones: Indicador para forzar la custodia de respuestas a todas las aplicaciones.

5.3.13.1.8 Alias de Certificados

Las propiedades que se pueden modificar en este grupo son:

- Alias del certificado de servidor utilizado para la firma de las respuestas SOAP. Por defecto *defaultFirma*.
- Alias del certificado de servidor utilizado para la firma de los ficheros de registro de eventos. Por defecto *defaultFirma*.

5.3.13.1.9 Firma

Las propiedades que se pueden modificar en este grupo son:

- Algoritmo de resumen utilizado para la generación de sellos de tiempo en firmas CAdES LTA-Level. Se debe escoger entre "SHA1", "SHA256", "SHA512" y "RIPEMD160".
- Algoritmo de firma utilizado para la firma del mensaje de respuesta SOAP fault. Se debe escoger entre *sha1WithRSAEncryption*, *sha256WithRSAEncryption*, *sha384WithRSAEncryption* y *sha512WithRSAEncryption*.
- Indicador para registrar la firma origen en procesos de actualización de firma.
- Indicador para registrar la firma actualizada tras un proceso de actualización de firma.
- Indicador para conservar las firmas originales registradas que hayan sido actualizadas.
- Formato de firma utilizado para la firma del mensaje de respuesta "SOAP fault". Se debe escoger entre *"NONE", "XMLDSIG", "XADES" y "XADES-T".*
- Indicador para comprobar la existencia de la extensión id-kp-timeStamping como crítica en los certificados firmantes de los sellos de tiempo.
- Algoritmo de generación de semilla a usar para las firmas, así como el origen de datos aleatorios. Se podrá elegir entre: *SHA1PRNG, NativePRNG, NativePRNGNonBlocking, PKCS11, Windows-PRNG*.

5.3.13.1.10 Atributo SigningTime

Las propiedades que se pueden modificar en este grupo son:

- Indicador para validar la propiedad firmada SigningTime.
- Ventana permitida de desviación temporal, en milisegundos, entre el momento de validación y el tiempo indicado por la propiedad firmada SigningTime.
- SigningTime para PAdES: Ventana permitida de desviación temporal, en milisegundos, entre el momento de validación y el tiempo indicado por la propiedad firmada SigningTime.

5.3.13.1.11 Módulo de Gestión de Aplicaciones

Las propiedades que se pueden modificar en este grupo son:

- Custodia de Peticiones.
- Custodia de Respuestas.
- Formato de firma de la respuesta. Se podrá elegir entre: *NONE_SIGN, XMLDSignature, XAdES_BES, XAdES_T*.
- Inclusión del Token de seguridad. Se podrá elegir entre: *KeyValue, X509Data, BinarySecurityToken*.
- Política de custodia. Deberemos decidir si lo queremos con custodia o sin ella.
- Política de Timestamp. Por defecto viene señalada sin Timestamp, pero podemos cambiarla y seleccionar que tenga Timestamp.
- Política de resultado de verificación de firma. Se podrá elegir entre *"Política Crítica" o "Política Avanzada"*.
- Política de validación. Debemos seleccionar una de las políticas de validación dadas de alta en la plataforma. Por defecto tendremos la política "DEFAULT".
- Excluir del control de peticiones.

- Indica si por defecto, al crear una aplicación, se le habilitará (o no) el uso de TSL.
- Indica si por defecto, al crear una aplicación, se le habilitará el check de "Mantener nivel actual".
- Indica si por defecto, al crear una aplicación, se le habilitará la opción de poder cambiar de nivel de aplicación.

5.3.13.1.12 Módulo de Custodia

Las propiedades que se pueden modificar en este grupo son:

- Modo de custodia de las firmas electrónicas: Custodia completa de la firma (valor 0) o custodia del hash de la firma (valor 1).
- Algoritmo de resumen utilizado para la custodia de firma. Se debe escoger entre “SHA1”, “SHA256”, “SHA384” y “SHA512” (modo 1).

5.3.13.1.13 TSL

Las propiedades que se pueden modificar en este grupo son:

- Fecha inicial (dd/MM/yyyy) a partir de la cual se tiene en consideración el uso de TSL para el reconocimiento y verificación de certificados.
- Lista de valores correspondientes al campo lógico 'clasificacion' que se mapean en el campo lógico 'certClassification' por NATURAL_PERSON: Números enteros separados por comas.
- Lista de valores correspondientes al campo lógico 'clasificacion' que se mapean en el campo lógico 'certClassification' por LEGAL_PERSON: Números enteros separados por comas.
- Lista de valores correspondientes al campo lógico 'clasificacion' que se mapean en el campo lógico 'certClassification' por ESIG: Números enteros separados por comas.
- Lista de valores correspondientes al campo lógico 'clasificacion' que se mapean en el campo lógico 'certClassification' por ESEAL: Números enteros separados por comas.

- Lista de valores correspondientes al campo lógico 'clasificacion' que se mapean en el campo lógico 'certClassification' por WSA: Números enteros separados por comas.
- TSL: Proceso Reconocimiento Certificados: AdditionalServiceInformationExtension obligatoria para los TSP-Service de tipo CA/QC.
- Lista de valores correspondientes al campo lógico “clasificacion” que se mapean en el campo lógico “certQualified” por YES.
- Lista de valores correspondientes al campo lógico “clasificacion” que se mapean en el campo lógico “certQualified” por NO.

5.3.13.1.14 Integración DIR3

Las propiedades que se pueden modificar en este grupo son:

- Modo de integración con DIR3: *WITHOUT INTEGRATION*, *RELAXED*, *STRICT*
- DIR3: Nombre de Usuario.
- DIR3: Contraseña de Usuario.
- DIR3: URL servicios.
- DIR3: Timeout de conexión en milisegundos: por defecto viene el valor 10000.

5.3.13.1.15 Plataforma de Mensajería

Las propiedades de este grupo hacen referencia a aspectos relacionados con la Plataforma de Mensajería que posee el Ministerio de Hacienda y Administraciones Públicas del Gobierno de España y que permite el envío de correos electrónicos y mensajes de texto desde la plataforma @firma.

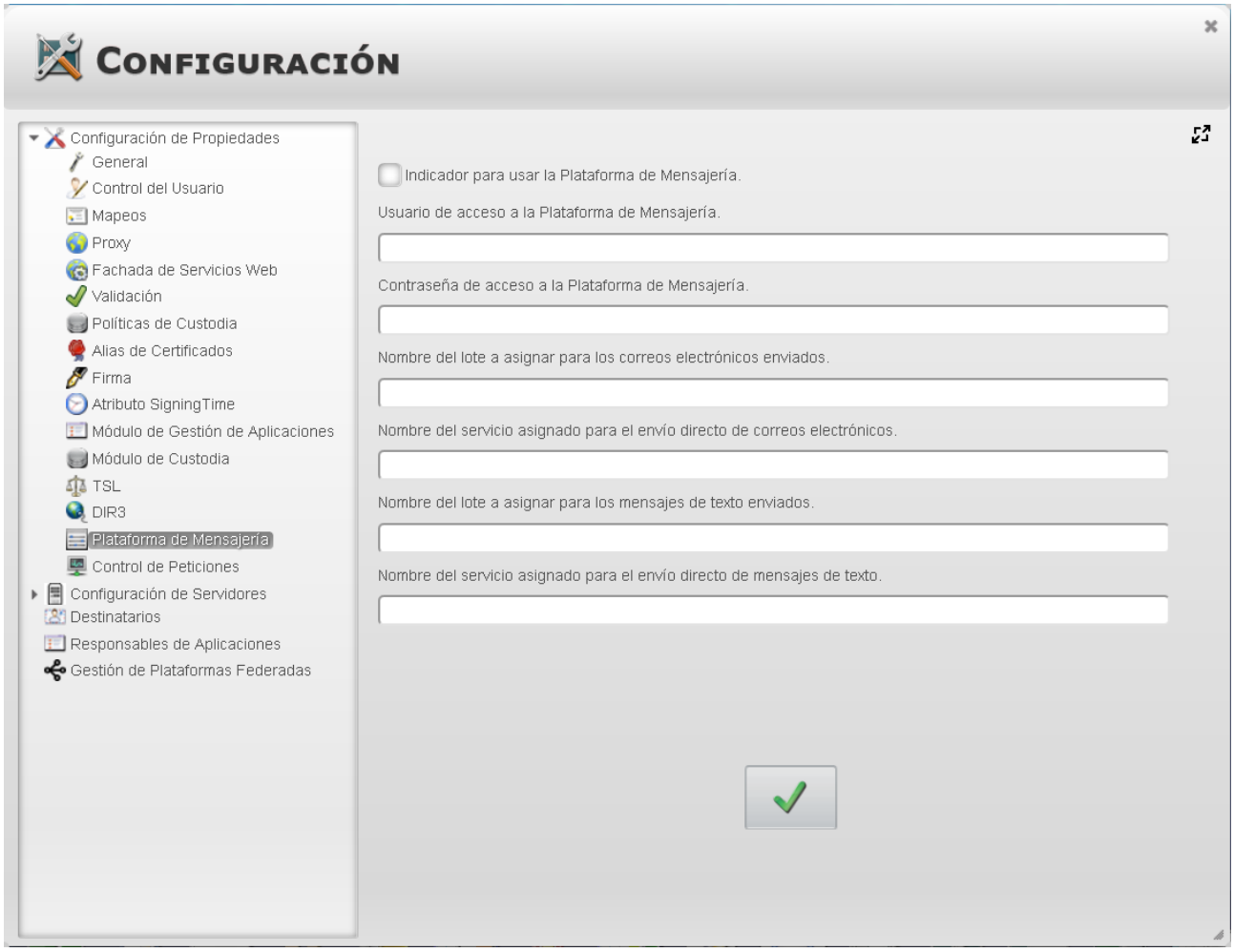


Figura 170 - Configuración: Datos de Configuración Plataforma de Mensajería

Existen siete propiedades dentro de este grupo:

- **Indicador para usar la Plataforma de Mensajería:** Marcador que indica si se hará uso de la Plataforma de Mensajería para el envío de mensajes de texto y correos electrónicos o no, en función de si se marca o no, respectivamente. Por defecto no se hará uso.

- **Usuario de acceso a la Plataforma de Mensajería:** Nombre del usuario de acceso a la Plataforma de Mensajería.

- **Contraseña de acceso a la Plataforma de Mensajería**: Contraseña de acceso a la Plataforma de Mensajería.

- **Nombre del lote a asignar para los correos electrónicos enviados:** Nombre para el lote que agrupe los correos electrónicos enviados.

- **Nombre del servicio asignado para el envío directo de correos electrónicos:** Nombre del servicio que permite el envío directo de correos electrónicos.

- **Nombre del lote a asignar para los mensajes de texto enviados:** Nombre para el lote que agrupe los mensajes de texto enviados.

- **Nombre del servicio asignado para el envío directo de mensajes de texto:** Nombre del servicio que permite el envío directo de mensajes de texto.

5.3.13.1.16 Control de Peticiones

Las propiedades que se pueden modificar en este grupo son:

- Ventana de tiempo a observar al controlar las peticiones iguales permitidas (en milisegundos). Se enviará alarma si se detectan N peticiones iguales por parte de una aplicación durante el tiempo configurado aquí.

- Ventana de tiempo a observar al controlar las peticiones por aplicación y servicio permitidas (en milisegundos). Se enviará alarma si se detectan N peticiones de la misma aplicación a un servicio durante el tiempo configurado aquí.

- Número N de peticiones iguales permitidas durante el tiempo configurado.

- Número N de peticiones de una aplicación a un servicio permitidas durante el tiempo configurado.

- Tiempo (en milisegundos) que se esperará antes de seguir comprobando si una petición se sigue repitiendo tras el envío de una alarma para informar que se ha superado el número N de peticiones iguales permitidas durante el tiempo configurado.

- Tiempo (en milisegundos) que se esperará antes de seguir comprobando si una aplicación sigue realizando peticiones a un servicio tras el envío de una alarma por superar el número N de peticiones permitidas durante el tiempo configurado.

- Indicador para activar el control de peticiones.

5.3.13.2 Modificación de propiedades del sistema



La modificación de las propiedades del sistema se realiza por grupos. Una vez seleccionado el grupo con la propiedad/propiedades del sistema a modificar, y tras realizar la modificación de la misma, se pulsará el botón ***"Modificar"***.

5.3.13.3 Configuración de los servidores internos

Dentro de este apartado, se podrá establecer la configuración de las siguientes propiedades (se adjunta una breve descripción de cada una de ellas):

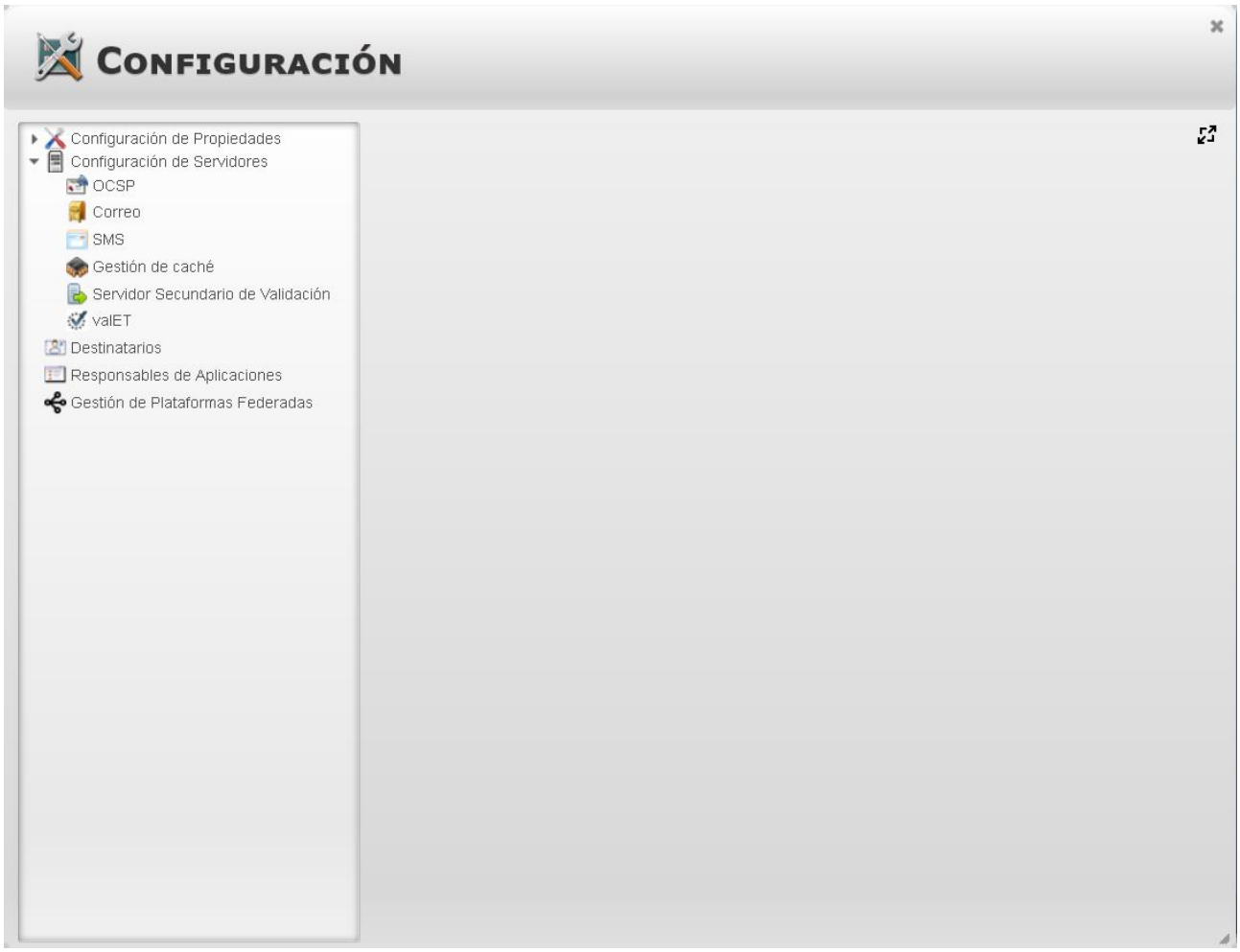


Figura 171 - Ventana Gestión de Configuración (II)

5.3.13.3.1 Servidor OCSP



Figura 172 - Configuración Servidor OCSP

Los campos que posee el formulario son:

- Algoritmo de resumen utilizado en la respuesta del servicio OCSP. Se debe escoger entre "SHA1", "SHA256" y "SHA384".

- Algoritmo de firma para la respuesta del servicio OCSP. Se deberá elegir entre "sha1WithRSAEncryption", "sha256WithRSAEncryption", "sha384WithRSAEncryption" y "sha512WithRSAEncryption".

- Selección del certificado por defecto a utilizar para la firma de las respuestas del servicio OCSP. Este certificado será utilizado para firmar las respuestas OCSP si en el "Almacén de claves servidor OCSP" no se encuentra ningún certificado emitido por el mismo emisor que

el certificado que se pretende validar en la petición, o bien, se encuentra, pero su cadena de certificación no está dada de alta en la configuración de la plataforma.

- Indicador de si es obligatorio el atributo *RequestorName* en las peticiones recibidas.



Una vez configurado el servidor OCSP se deberá pulsar sobre el botón de aplicar cambios.

5.3.13.3.2 Servidor de Correo



Figura 173 - Configuración Servidor de Correo

Los campos que posee el formulario son:

- Identificador del emisor de los correos emitidos por la plataforma.
- Host SMTP del servidor de correos.
- Puerto SMTP del servidor de correos.
- Usuario y contraseña de acceso para el uso del servidor de correos.



Una vez configurado el servidor de correo se deberá pulsar sobre el botón de aplicar cambios.

5.3.13.3.3 SMS

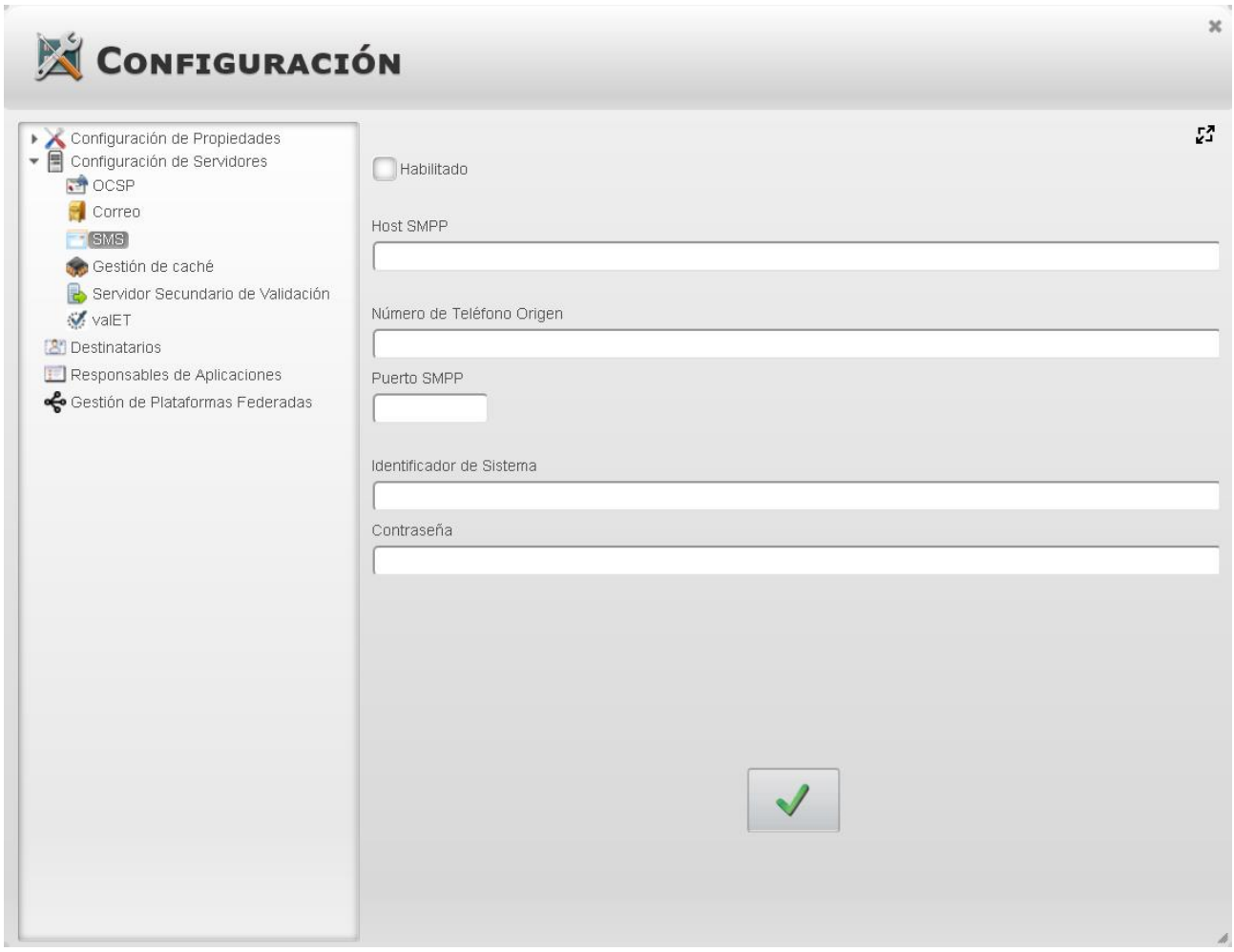


Figura 174 - Configuración SMS

Los campos que posee el formulario son:

- **Habilitado:** Marcador que indica si este servidor se encuentra habilitado o no, en función de si se marca o no, respectivamente. Si no se encontrara habilitado la plataforma no enviaría mensajes de texto.

- **Host:** Dirección IP donde se encuentra desplegado el servidor SMPP.

- **Número de Teléfono Origen:** Número de teléfono que aparecerá como emisor de los mensajes de texto enviados por la plataforma.
- **Puerto:** Número del puerto de conexión con el servidor SMPP.
- **Identificador de Sistema:** Identificador de sistema o nombre del usuario de acceso para el servidor SMPP.
- **Contraseña:** Contraseña de acceso para el servidor SMPP.



Una vez configurado el servidor SMS se deberá pulsar sobre el botón de aplicar cambios.

5.3.13.3.4 Gestión de Caché de Nivel 1

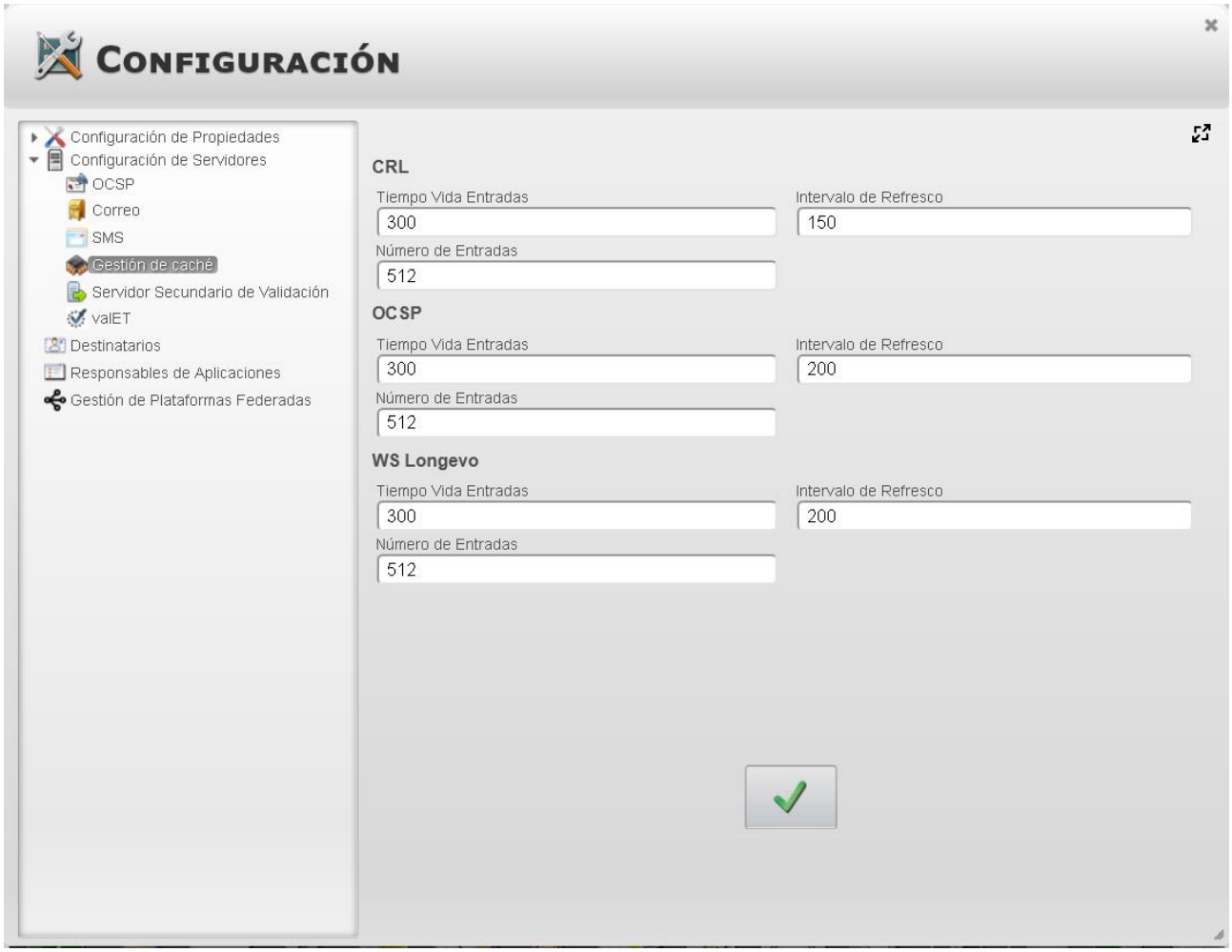


Figura 175 - Configuración Cache L1

El formulario de configuración de la caché posee tres áreas:

- **CRL.** Se define el tiempo de vida, intervalo de refresco y número de entradas para las respuestas de validación obtenidas mediante un método de validación tipo CRL almacenadas en la caché de nivel 1.
- **OCSP.** Se define el tiempo de vida, intervalo de refresco y número de entradas para las respuestas de validación obtenidas mediante un método de validación tipo OCSP almacenadas en la caché de nivel 1.
- **WS Longevo.** Se define el tiempo de vida, intervalo de refresco y número de entradas para las respuestas de validación obtenidas mediante un método de validación tipo WS-Longevo almacenadas en la caché de nivel 1.



Una vez configurada la cache L1 se deberá pulsar sobre el botón de aplicar cambios.

5.3.13.3.5 Servidor Secundario de Validación



Figura 176 - Configuración Servidor Secundario Validación

Esta configuración gestiona los parámetros necesarios para determinar cómo atacar a otro servidor @firma para ejecutar una validación de certificado. Dicha funcionalidad tan solo aplica cuando tras tratar de validar un certificado, la plataforma no es capaz de reconocer el tipo de certificado, en cuyo caso, se intenta hacer uso de esta configuración para validarlo.

El formulario para la configuración del servidor secundario de validación contempla los siguientes campos:

- **Habilitado.** Indicador para activar o desactivar el servidor.
- **Tipo de acceso.** Se define si el acceso se hará a través de HTTP o HTTPS.

- **URL: Puerto Servidor.** URL y puerto de acceso al servidor secundario.
- **Timeout de conexión.** Tiempo de vida, en milisegundos, para la conexión al servidor secundario de validación.
- **Identificador de aplicación.** Identificador de la aplicación existente, a la cual se va a atacar, en el servidor secundario.
- **Tipo de autenticación.** Los valores posibles que puede tomar son: *Sin autenticación*, *Usuario/Password* y *Certificado*.
- **Usuario.** Nombre de usuario para el tipo de autenticación "Usuario/Password".
- **Contraseña.** Contraseña para el tipo de autenticación "Usuario/Password".
- **Certificados disponibles.** Alias del certificado a usar para el tipo de autenticación "Certificado". Se muestra el listado de certificados disponibles en "Almacén de Claves Métodos de Validación SOAP".



Una vez configurado el servidor secundario se deberá pulsar sobre el botón de guardar cambios.

5.3.13.3.6 valET



Figura 177 - Configuración valET

Esta configuración gestiona los parámetros necesarios para determinar cómo atacar a la plataforma de valET si se van a hacer uso de las TSLs para la validación u obtención de información de certificados.

El formulario para la configuración de la plataforma de valET contempla los siguientes campos:

- **Habilitado.** Indicador para activar o desactivar la configuración de valET.
- **URL: Puerto Servidor.** URL y puerto de acceso a la plataforma de valET.
- **Timeout de conexión.** Tiempo de vida, en milisegundos, para la conexión a la plataforma de valET.

- **Identificador de aplicación.** Identificador de la aplicación existente, a la cual se va a atacar, en la plataforma de valET.



Una vez modificada la configuración de conexión a la plataforma de valET, se deberá pulsar sobre el botón de guardar cambios.

5.3.13.4 Destinatarios

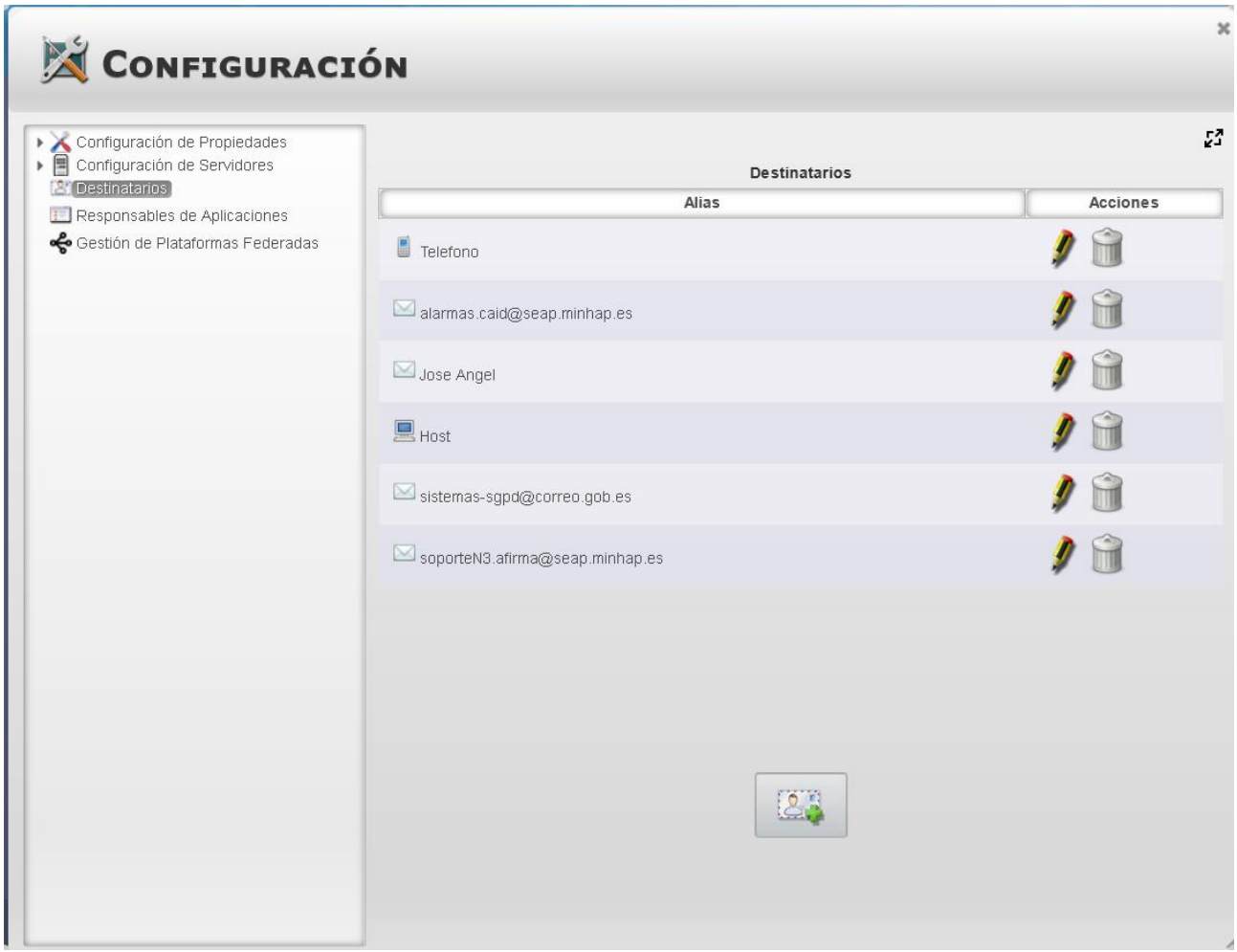
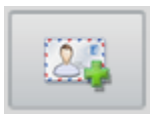


Figura 178 - Configuración Destinatarios



Para dar de alta un nuevo destinatario, se ha de pulsar el botón ***"Alta Destinatario".*** Una vez pulsado el sistema mostrará un panel para que el usuario introduzca el correo electrónico a dar de alta.

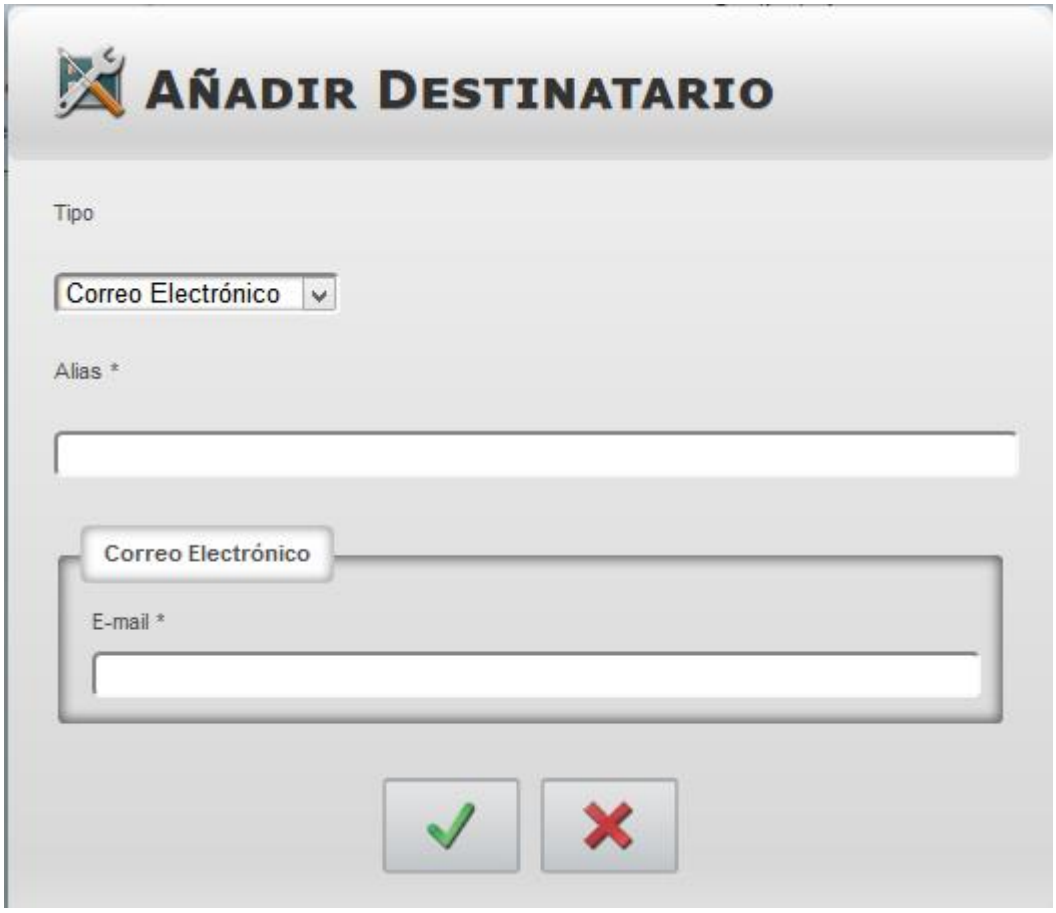


Figura 179 - Configuración Destinatarios de Correo

Debemos rellenar los diferentes campos antes de dar de alta al nuevo destinatario, eligiendo el tipo de destinatario entre: Correo electrónico, número de teléfono y host. Dependiendo de la elección que hagamos, los campos de la pantalla cambiarán adaptándose a dicha elección.



Figura 180 - Configuración Destinatarios de Host

Desde la interfaz de configuración de destinatarios se puede también eliminar un destinatario, o modificar uno ya existente. En caso de modificar uno existente, aparecerá tras pulsar el botón el mismo panel de Alta, pero con la información del destinatario a ser modificado.

5.3.13.5 Responsables de Aplicaciones



Figura 181 – Gestión de Responsables de Aplicaciones

En este apartado se tratará toda la gestión de los responsables asociados a las aplicaciones de la plataforma, desde su alta hasta su edición o eliminación.

Para dar de alta un nuevo responsable debemos pulsar en “Añadir Responsable”, con lo que se nos abrirá la pantalla de alta del responsable y debemos de ir rellenando los diferentes campos.



Figura 182 – Alta de Responsables

Los campos que posee el formulario de alta son:

- **Nombre:** Nombre del nuevo responsable.
- **Apellidos:** Apellidos del nuevo responsable.
- **Email:** Dirección de correo electrónico del nuevo responsable.
- **Teléfono:** Número de teléfono del nuevo responsable.
- **DIR4 habilitado:** Indicador para establecer si el nuevo responsable se encuentra recogido en el directorio común DIR4 (solo a nivel informativo, la plataforma no sincroniza estos datos).

Una vez configurada la Plataforma Federada se deberá pulsar sobre el botón de guardar cambios.

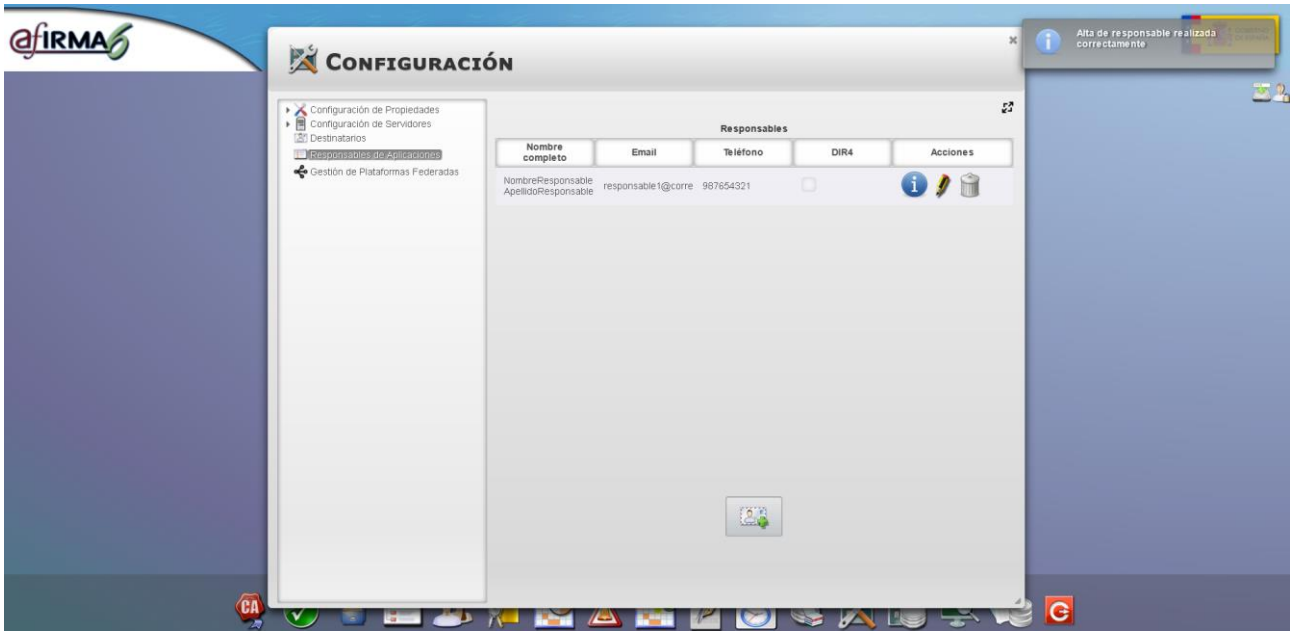


Figura 183 – Listado de Responsables

Desde la interfaz de "Responsables de Aplicaciones" se pueden también realizar las siguientes acciones:

- **Mostrar aplicaciones asociadas al responsable**: Pulsando en el icono de  podemos consultar todas las aplicaciones que tienen asociado al responsable seleccionado.

- **Editar**: Con el icono  se puede modificar el responsable indicado, editando todos sus campos y pulsando finalmente en el botón de "Guardar".

- **Eliminar**: Usaremos el icono  para eliminar de nuestra plataforma un responsable que esté en desuso. De todas formas, cuando pulsemos en dicho icono, nos aparecerá un listado con las aplicaciones a las que esté asociado el responsable, pudiendo cancelar la eliminación en ese momento.



Figura 184 – Modificación de Responsable

5.3.13.6 Gestión de Plataformas Federadas



Figura 185 – Gestión de Plataformas Federadas

En este apartado se darán de alta las diferentes Plataformas Federadas, que nos sirven para consultar las estadísticas de acceso a la plataforma.

Para dar de alta una nueva Plataforma Federada debemos pulsar en “Añadir Plataforma Federada”, con lo que se nos abrirá la pantalla de alta de la Plataforma y debemos de ir rellenando los diferentes campos.



Figura 186 – Alta de Plataformas Federadas

Los campos que posee el formulario de alta son:

- **Habilitado:** Marcador que indica si esta plataforma se encuentra habilitada o no, en función de si se marca o no, respectivamente. Si no se encontrara habilitada la plataforma no consultaría estadísticas de la plataforma seleccionada.
- **Identificador de la Plataforma:** Identificador que poseerá la Plataforma Federada.
- **Descripción:** Breve descripción de la Plataforma Federada.
- **URL de acceso a la Plataforma:** URL donde está publicada la Plataforma de la que queremos obtener las estadísticas.
- **Nombre del responsable (opcional):** Nombre de la persona responsable de la Plataforma.
- **Apellidos del responsable (opcional):** Apellidos de la persona responsable de la Plataforma.
- **Teléfono del responsable (opcional):** Número de teléfono de la persona responsable de la Plataforma.

- **Correo electrónico del responsable (opcional):** Dirección de correo electrónico de la persona responsable de la Plataforma
- **Timeout (msg):** Tiempo de vida, en milisegundos, para la conexión con la Plataforma Federada.
- **Número máximo de intentos:** Número de intentos para la conexión contra la Plataforma.
- **Rango de días:** Número de días de los que serán calculadas las estadísticas de la Plataforma Federada.



Una vez configurada la Plataforma Federada se deberá pulsar sobre el botón de guardar cambios.



Figura 187 – Listado de Plataformas Federadas

Desde la interfaz de "Gestión de Plataformas Federadas" se puede también eliminar una plataforma dada de alta , o modificar una ya existente . En caso de modificar una existente, sus datos aparecerán tras pulsar el botón con la información de la plataforma a ser modificada.



Figura 188 – Modificación de Plataformas Federadas

5.3.14 Módulo Importación y Exportación de Configuraciones

El módulo de Importación y Exportación de configuraciones permite al administrador realizar operaciones sobre la configuración general de la plataforma. Entre las operaciones aplicables a la configuración están:

- Importación y Exportación de políticas de certificación.
- Importación de configuración de PSCs.
- Generar copia de la configuración en el servidor.

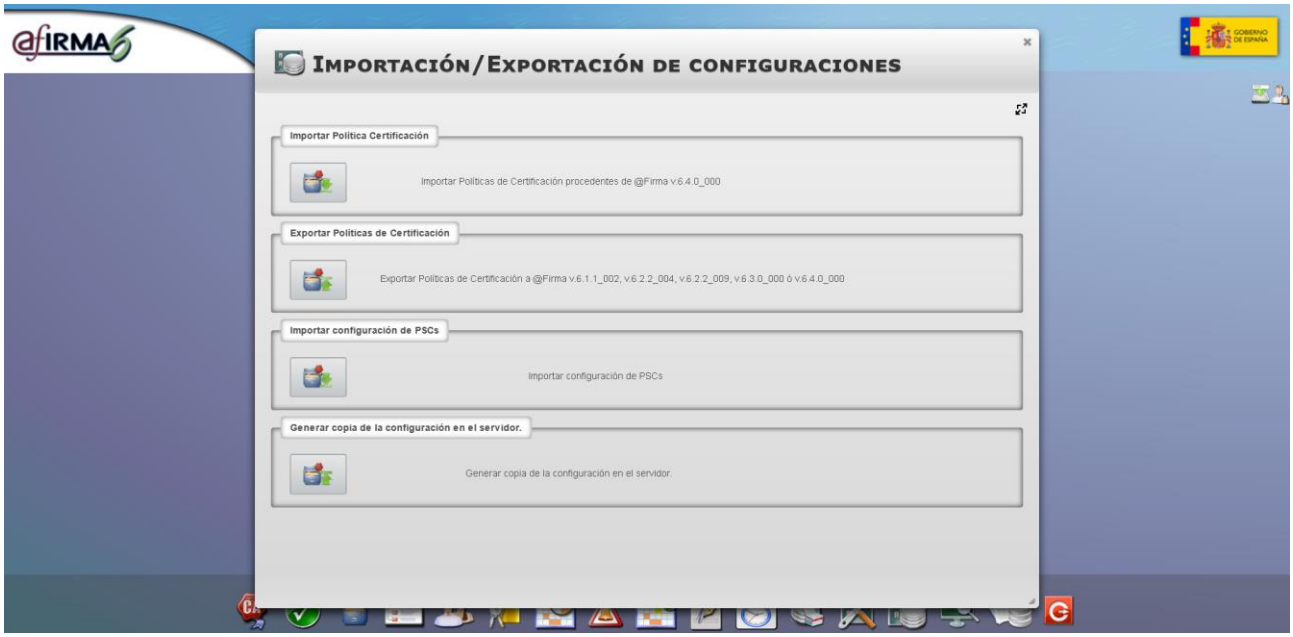


Figura 189 - Módulo Importación / Exportación de Configuraciones

5.3.14.1 Importación y Exportación de políticas de certificación

Desde el módulo de Importación / Exportación de configuraciones, el administrador también podrá realizar la importación / exportación de las políticas de certificación existentes en la plataforma (en caso de exportación) o procedentes de otra plataforma (en caso de importación), así como los certificados asociados a las mismas.

5.3.14.1.1 Importación de políticas de certificación



Para realizar la importación de políticas de certificación procedentes de otra plataforma de @Firma. El usuario deberá de pulsar el botón ***"Importar Política de Certificación"***

Un dato importante a tener en cuenta es que tan solo se permite realizar importaciones de políticas de certificación exportadas para la versión 6.4.0 de @firma.

Una vez pulsado dicho botón, el sistema mostrará el panel asociado al proceso de importación.



Figura 190 - Importar Políticas de Certificación (I)

Dicho panel contiene los siguientes campos:

- Fichero ZIP con la configuración de las políticas de certificación a importar (procedentes de @firma 6.4.0).
- Selector para sobrescribir la configuración existente. En el caso de que se marque este campo, todos los datos de configuración previos serán sobrescritos. En caso contrario, sólo se insertarán nuevos datos.
- Tabla con las políticas existentes en el fichero a importar. Esta tabla se completará en el momento en el que el usuario adjunte un fichero ZIP correcto con las políticas a importar.



Figura 191 - Importar Políticas de Certificación (II)

Tras adjuntar la configuración, la tabla mostrará todas las políticas existentes en la configuración, dando la posibilidad al administrador de renombrarlas durante el proceso de importación. Por último, una vez configurado todo el proceso, sólo hay que darle al botón ***"Importar"*** para comenzar el proceso de importación.

La estructura del fichero ZIP que representa la información de las políticas de certificación que importar será la siguiente:

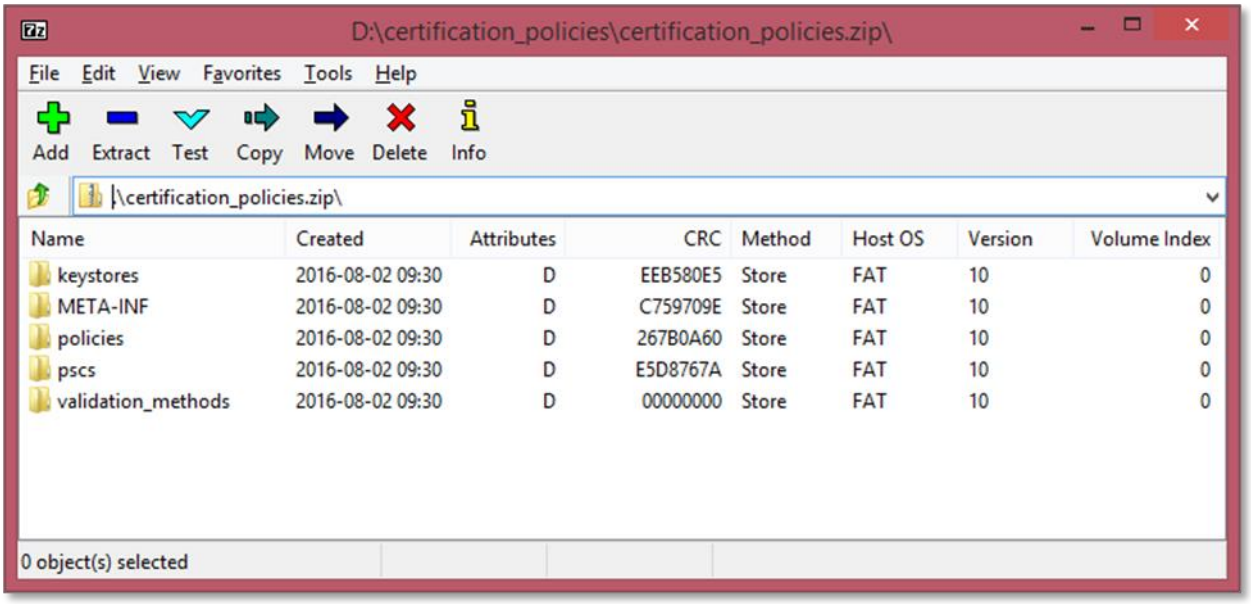


Figura 192 - Estructura fichero ZIP con políticas de certificación a importar

El fichero recibe el nombre "certification_policies.zip" y se compone de 5 carpetas:

- **keystores:** Contiene los ficheros JSON asociados a los datos de los almacenes de claves que importar. La nomenclatura de cada fichero será **keystore_NOMBRE_KEYSTORE.json**, donde **NOMBRE_KEYSTORE** es el nombre que identifica al almacén de claves. Por ejemplo, "keystore_AlmacenConfianzaCRL.json".

- **META-INF:** Contiene únicamente 2 archivos. El primero, **files_hash.properties**, está compuesto por una lista de pares clave/valor, donde cada clave es la ruta a cada uno de los archivos contenidos en el fichero ZIP, y su valor es el resumen calculado con el algoritmo SHA-256, y codificado en Base64, de dicho archivo. Por ejemplo, la entrada "/certification_policies/keystores/keystore_AlmacenConfianzaCRL.json=RZeL1+OoF8bLqmpQTVUtiB59WhsQSzsWXtjY6E2bVFk\=" asocia al fichero "/certification_policies/keystores/keystore_AlmacenConfianzaCRL.json" el valor de su resumen en SHA-256 y codificado en Base64 como "RZeL1+OoF8bLqmpQTVUtiB59WhsQSzsWXtjY6E2bVFk\=". El segundo archivo, **signature.p7s**, representa la firma en formato CAdES-BES del primer archivo.

- **policies:** Contiene los ficheros JSON asociados a los datos de las políticas de certificación que importar. La nomenclatura de cada fichero será **policy_IDENTIFICADOR_POLITICA.json**,

donde **IDENTIFICADOR_POLITICA** es el identificador de la política de certificación. Por ejemplo, "policy_DEFAULT.json".

- **PSC:** Contiene los ficheros JSON asociados a los datos de los PSC que importar. La nomenclatura de cada fichero será **psc_ALIAS_PSC.json**, donde **ALIAS_PSC** es la cadena en hexadecimal resultante de concatenar el resumen del valor del emisor y el resumen del valor del número de serie del certificado asociado al PSC, calculados con el algoritmo SHA-256. Por ejemplo, "PSC_e4-16-a0-e3-e2-3b-e4-81-8c-ee-7f-6a-ea-ed-f5-87-97-4a-32-85-7b-2b-6f-5e-e6-6f-c6-7e-e3-3c-29-77.json". Por otro lado, incluye un fichero de propiedades, **identifiers.properties**, con un conjunto de pares clave/valor, donde cada clave es la cadena en hexadecimal resultante de concatenar el resumen del valor del emisor y el resumen del valor del número de serie del certificado asociado al PSC, calculados con el algoritmo SHA-256, y su valor asociado es el identificador del PSC. Este fichero permite identificar más cómodamente cada PSC.

- **validation_methods:** Contiene los ficheros JSON asociados a los datos de los métodos de validación que importar. La nomenclatura de cada fichero será **validation_method_IDENTIFICADOR_METODO_VALIDACION.json**, donde **IDENTIFICADOR_METODO_VALIDACION** es el identificador del método de validación. Por ejemplo, "validation_method_CRL_ANF.json".

Durante el proceso de importación de las políticas de certificación, se mostrará una ventana que irá indicando el porcentaje realizado sobre el total, así como unas breves descripciones de los pasos realizados y/o problemas encontrados. Además, debido a la complejidad de este proceso, se genera un log exclusivo con todas las acciones realizadas. Este log es almacenado en el fichero "**JBOSS_HOME/standalone/log/importProcesses.log**".



Figura 193 – Importación de Políticas de Certificación – Ventana Descriptiva del Proceso

Una vez haya finalizado el proceso, puede observarse en la pantalla un resumen con los pasos ejecutados, y si la información asociada a aquellos que hayan fallado o tengan una notificación asociada.

En caso de producirse un error durante el proceso, se restablecerá la configuración a su estado inmediatamente anterior a la realización del proceso de importación de políticas de certificación.

5.3.14.1.2 Exportación de políticas de certificación

Para realizar la exportación de políticas de certificación a otra plataforma de @Firma, versiones 6.1.1_002, 6.2.2_004, 6.2.2_009, 6.2.2_011, 6.2.2_012 ó 6.4.0_000. El usuario deberá de pulsar el botón ***"Exportar Política de Certificación"***.

Hay que tener en cuenta, que **nunca se exportan las distintas contraseñas de autenticación** (por ejemplo, las establecidas en los métodos de validación tipo CRL cuando su autenticación es por usuario y contraseña). En concreto, al realizar una exportación hacia la versión 6.1.1, las contraseñas se pasan sin valor, y para las exportaciones al resto de versiones, se establece una contraseña falsa por defecto ("XXXXX"). Dependerá del administrador del sistema donde se realiza la importación, el repasar todos los métodos de validación y comprobar que tienen correctamente establecida su configuración de autenticación, y en su defecto, modificarla si fuera necesario.

Una vez pulsado dicho botón, el sistema mostrará el panel asociado al proceso de exportación.



Figura 194 - Exportar Políticas de Certificación

Este panel contiene la siguiente información:

- Tabla con las políticas existentes en la plataforma susceptibles de ser exportadas. El administrador seleccionará de esta tabla las políticas que quiere exportar.

- Si se desean incluir los certificados de ejemplo involucrados en dichas políticas. En ese caso, el administrador deberá seleccionar este campo, en caso contrario dejarlo sin seleccionar.

- Versión a la que se quiere exportar las políticas, 6.1.1_002, 6.2.2_004, 6.2.2_009, 6.2.2_011, 6.2.2_012 ó 6.4.0_000.

Una vez definidos dichos campos, la plataforma generará un fichero ZIP para el caso de las versiones 6.1.1_002, 6.2.2_004, 6.2.2_009, 6.2.2_011, 6.2.2_012 ó 6.4.0_000 con la configuración indicada por el administrador y se lo ofrecerá para descargar. Dicho fichero estará firmado por la plataforma usando el certificado definido en el Almacén de Claves Certificados de Sistema.

Una vez pulsado el botón, si la exportación se genera sin errores, se mostrará una pantalla que permitirá la descarga del fichero generado, o salir cancelando el proceso.



Figura 195 – Exportación políticas de certificación

5.3.14.2 Importación de configuración de PSCs

Desde el módulo de Importación / Exportación de configuraciones, el administrador también podrá realizar la importación de la configuración de los PSCs extraída de la aplicación externa CA_DeskTool (aplicación para la gestión de los PSCs y métodos de validación, así como de sus políticas asociadas).



Para realizar la importación de políticas de certificación procedentes de otra plataforma de @Firma. El usuario deberá de pulsar el botón ***"Importar configuración de PSCs"***

Un dato importante a tener en cuenta es que tan solo se permite realizar importaciones de PSCs exportados para la versión 6.4.0 de @firma.

Una vez pulsado dicho botón, el sistema mostrará el panel asociado al proceso de importación.



Figura 196 - Importar PSCs (I)

En dicho panel deberemos de seleccionar el fichero ZIP con la configuración de los PSCs a importar (procedentes de la aplicación CA_DeskTool).

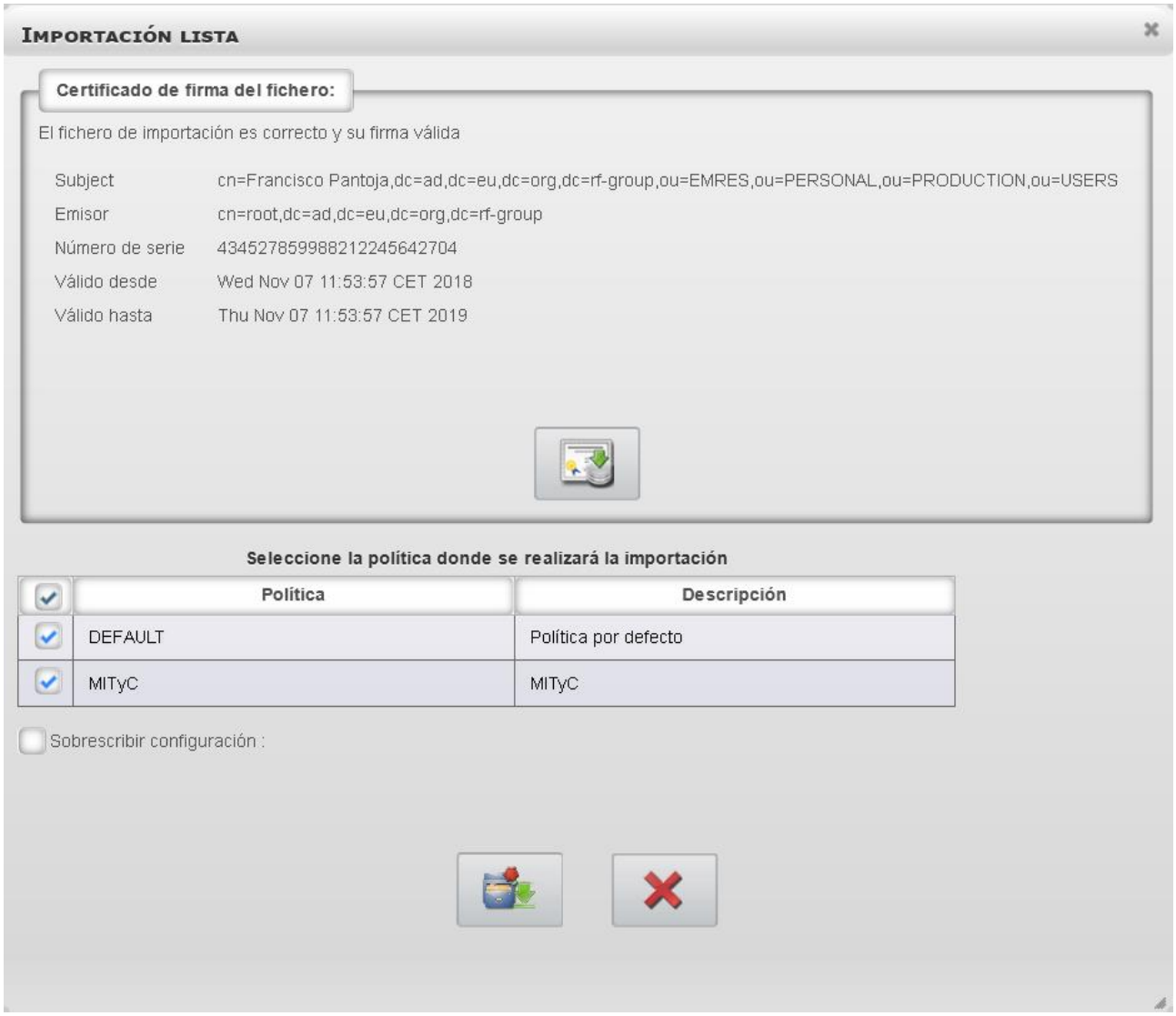


Figura 197 - Importar PSCs (II)

Tras adjuntar la configuración, la tabla mostrará la información asociada al certificado de firma del fichero, pudiendo descargar dicho certificado pulsando en el botón de .

A continuación, aparecerá un listado con las políticas dadas de alta en nuestra plataforma, pudiendo seleccionar aquellas a las que queramos realizar la importación de datos de las políticas exportadas (mapeos, métodos de validación…). Si no se seleccionase ninguna, se importarían solamente los PSCs y métodos de validación sin asociarlos a ninguna política.

Así mismo, aparece un check para "Sobrescribir configuración", con lo que conseguiremos, marcando este check, cambiar la configuración actual de una política por lo que importemos del fichero externo.

Por último, una vez configurado todo el proceso, sólo hay que darle al botón ***"Importar configuración de PSCs"*** para comenzar el proceso de importación.

La estructura del fichero ZIP que representa la información de las configuraciones de PSCs que importar será la siguiente:

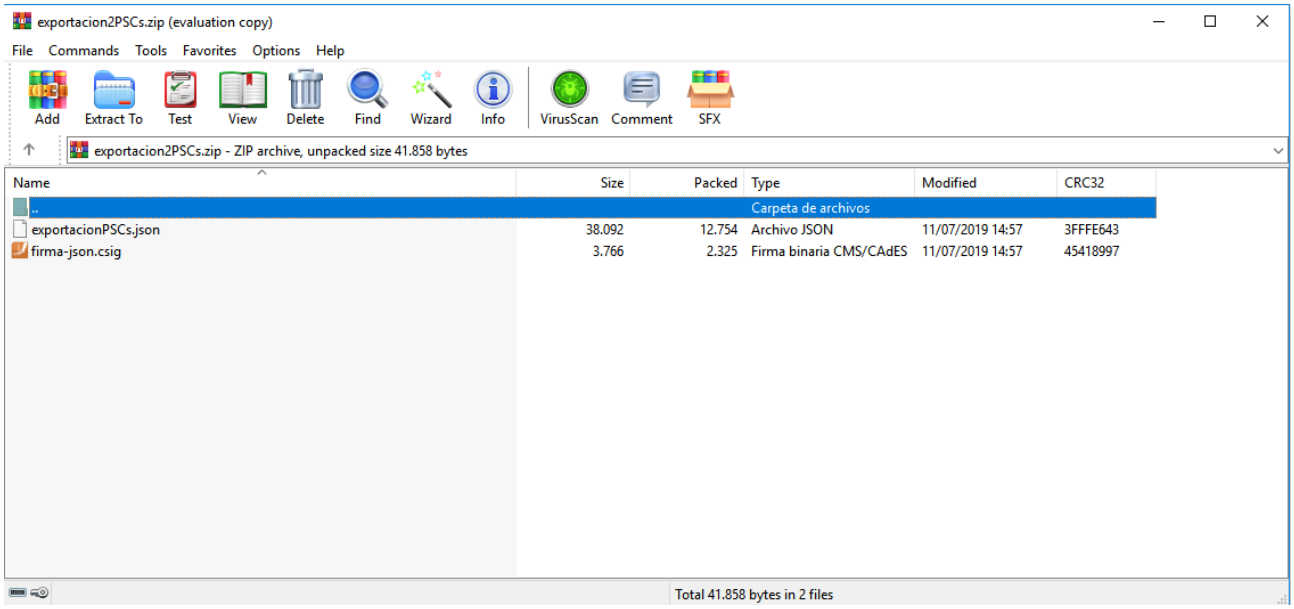


Figura 198 - Estructura fichero ZIP con PSCs a importar

El fichero recibe el nombre "exportacion.zip" y se compone de 2 ficheros:

- **exportacionPSCs.json:** Contiene los datos a importar de las CAs, tipos de certificado, métodos de validación y políticas.

- **firma-json.csig:** Firma del fichero json a importar.

Durante el proceso de importación de los PSCs, se mostrará una ventana que irá indicando el porcentaje realizado sobre el total, así como unas breves descripciones de los pasos realizados y/o problemas encontrados. Al igual que en el apartado anterior, este proceso genera un log exclusivo con las acciones realizadas, almacenándose en el fichero "**JBOSS_HOME/standalone/log/importProcesses.log**".

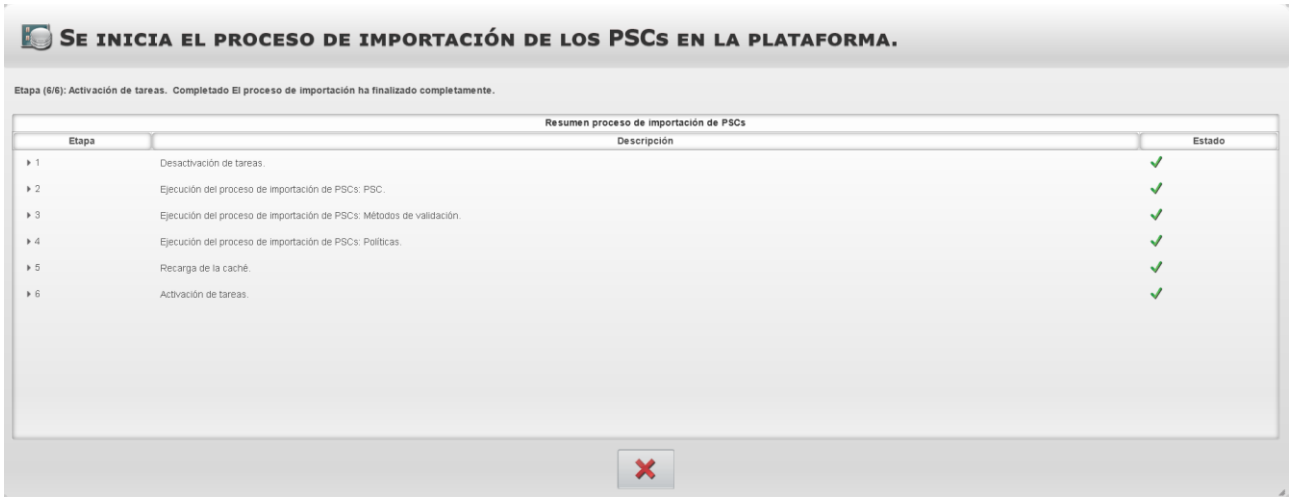


Figura 199 – Importación de PSCs – Ventana Descriptiva del Proceso

Una vez haya finalizado el proceso, puede observarse en la pantalla un resumen con los pasos ejecutados, y si la información asociada a aquellos que hayan fallado o tengan una notificación asociada.

En caso de producirse un error durante el proceso, se indicará en el listado de procesos pudiendo comprobar cuál ha sido exactamente el fallo acontecido.

5.3.14.3 Generar copia de la configuración en el servidor

Desde el módulo de Importación / Exportación de configuraciones, el administrador también podrá realizar una copia de la base de datos en un fichero local. Para poder ejecutar esta funcionalidad, el administrador deberá pulsar sobre el botón de ***"Generar copia de la configuración en el servidor".***



Figura 200 – Generar copia de la configuración en el servidor

Cuando se genere la copia, nos aparecerá un mensaje indicando la ruta donde se ha guardado en nuestro equipo local.



Figura 201 – Confirmación de la copia de la configuración en el servidor en fichero local

Como vemos, se creará un directorio dentro de "stableConf" cuyo nombre tendrá el formato YYYYMMDDHHMMSS y que contendrá a su vez los directorios database (con un backup de la base de datos) y blobs (con los blobs actuales de la base de datos.).

Para restablecer una configuración estable, en primer lugar, se realizarán los pasos indicados en el nodo de Administración, y no se continuará el proceso en el resto de nodos, hasta que **no haya finalizado el arranque del nodo de Administración**.

En el nodo de Administración:

1. Parada del servidor de aplicaciones WildFly del nodo de Administración.
2. Parada de la HSQLDB correspondiente (Configuración).
3. Eliminar por completo los directorios "blobs" y "database" de la BBDD (contenida en la ruta "[PATH_CONFIG]/configuration/LocalHSQLDBDataBase/configuration").
4. Copiar los directorios "blobs" y "database" contenidos en la configuración estable (ruta "[PATH_CONFIG]/configuration/LocalHSQLDBDataBase/configuration/stableConf/xxxxxxxxx/) o el backup correspondiente en la ruta "[PATH_CONFIG]/configuration/LocalHSQLDBDataBase/configuration") previamente eliminados.
5. En el fichero "staticAfirmaVersion.properties", contenido en la ruta "[PATH_CONFIG]/configuration", establecer el valor indicado a los siguientes parámetros:
    a. Eliminar el valor de fecha y hora del parámetro "last.database.version.date".
    b. Establecer el valor «true» al parámetro "update.database.on.startup".
6. Arrancar la HSQLDB de Configuración.
7. Arrancar el servidor de aplicaciones WildFly.

En el **resto de los nodos**, se seguirán los siguientes pasos:

1. Parada del servidor de aplicaciones WildFly del nodo en cuestión.
2. En el fichero “staticAfirmaVersion.properties”, establece el valor indicado a los siguientes parámetros:
    a. Eliminar el valor de fecha y hora del parámetro “last.database.version.date”.
    b. Establecer el valor <<true>> al parámetro “update.database.on.startup”.
3. Arrancar el servidor de aplicaciones Wildfly.

5.3.15 Módulo de Auditoría

A partir de la versión 6 de @Firma, el módulo de auditoría se encuentra definido dentro de la herramienta de administración web de la plataforma.

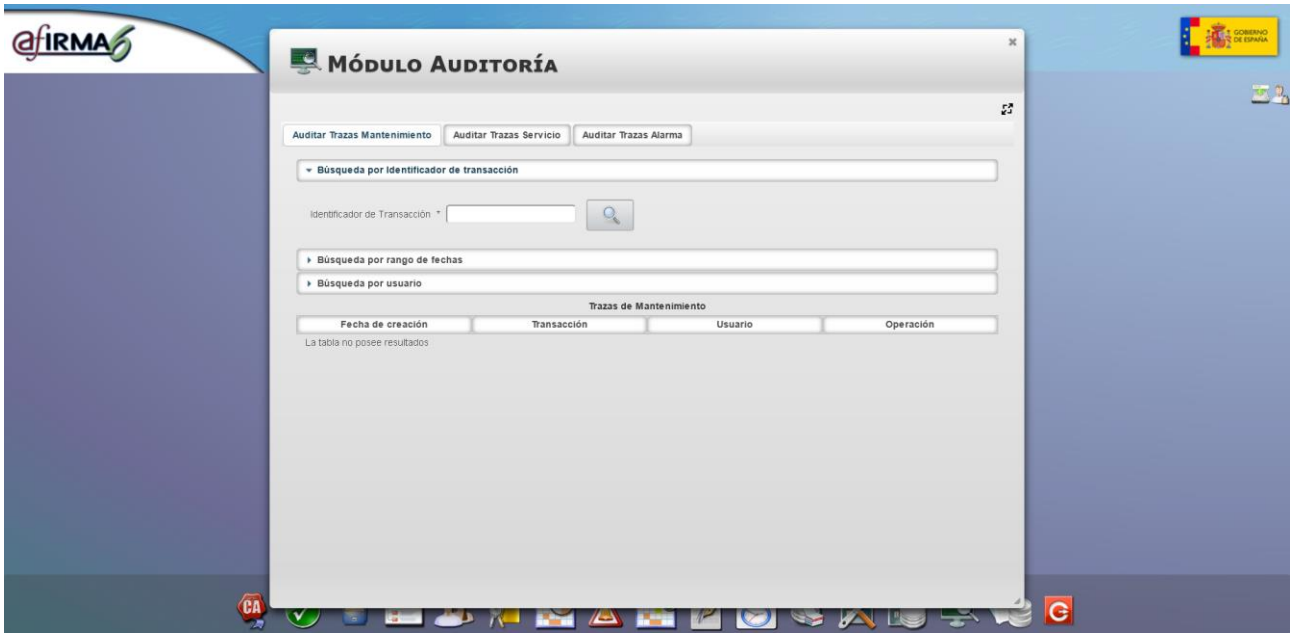


Figura 202 - Módulo de Auditoría

En dicho módulo, el usuario podrá consultar todas las trazas (u operaciones auditables) de mantenimiento y/o de servicio ocurridas en la plataforma en un momento determinado, o dentro de un periodo definido. También se podrán consultar todas las alarmas ocurridas en la plataforma.

5.3.15.1 Consulta trazas de mantenimiento.

Las trazas de mantenimiento son aquellas operaciones ocurridas en la administración de la plataforma. Actualmente las trazas de mantenimiento auditadas afectan a los módulos:

- Acceso a la plataforma

- Logado en el sistema

- Módulo de Política
  - Alta Campo Lógico en política
  - Alta Política
  - Inserción tipo de certificado en política
  - Baja Campo lógico
  - Baja mapeo
  - Baja política
  - Baja tipo de certificado
  - Modificar campo lógico
  - Modificar mapeo
  - Modificar política
  - Modificar método de validación en PSC
- Módulo de Aplicaciones. Operaciones:
  - Alta aplicación
  - Alta Unidad Organizativa
  - Baja aplicación
  - Baja Unidad Organizativa
  - Modificar aplicación
  - Modificar unidad organizativa
- Módulo de Keystores
  - Importar Certificado
  - Importar Par de claves
  - Modificar alias

- Módulo Gestión de Usuarios
  - Alta Usuario
  - Baja Usuario
  - Modificar usuario

Mediante la pestaña ***"Auditar Trazas de mantenimiento"*** el administrador puede consultar todas aquellas trazas de mantenimiento ocurridas en la plataforma en un instante de tiempo determinado.

Para facilitar la búsqueda de una traza en particular o un conjunto de trazas de mantenimiento, se han definido tres tipos de cuadros de búsqueda:

- ***Búsqueda por identificación de transacción***. Mediante este filtro de búsqueda, el administrador puede buscar una traza de mantenimiento concreta dada su identificador de transacción.



Figura 203 - Búsqueda Trazas de Mantenimiento por Identificador de Transacción

- ***Búsqueda por rango de fechas***. Este filtro permite al administrador buscar todas aquellas trazas que han ocurrido en un rango de tiempo definido. Permitiendo además discriminar por tipo de traza o mostrar todas las trazas ocurridas en dicho rango de tiempo.



Figura 204 - Búsqueda Trazas de Mantenimiento por Rango de Fechas

- ***Búsqueda por usuario***. Usando este filtro, podemos realizar la búsqueda de todas aquellas trazas de mantenimiento en las que un usuario ha estado involucrado.



Figura 205 - Búsqueda Trazas de Mantenimiento por Usuario



Tras definir el tipo de búsqueda y el contenido a aplicar en el filtro, el usuario deberá pulsar el botón ***"Buscar"***. En ese momento el sistema buscará todas aquellas trazas que cumplen con el filtro definido y mostrará el resultado final en la tabla de resultados situada en la parte inferior de los cuadros de búsquedas. Para facilitar la tarea de búsqueda al administrador en el caso de que existan muchos resultados, esta tabla ha sido paginada, mostrando en cada página un máximo de 10 resultados.

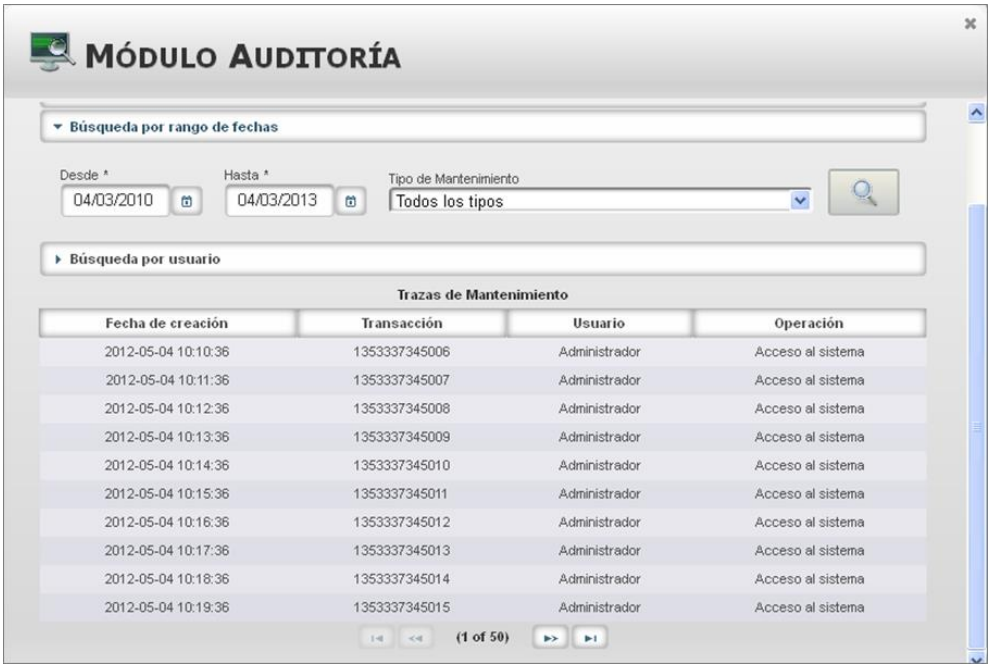


Figura 206 - Resultado Búsqueda de Trazas de Mantenimiento

Una vez el administrador haya localizado la traza a consultar, podrá pulsar sobre dicha traza para obtener una información más detallada.



Figura 207 - Panel Detalle Trazas de Mantenimiento



El panel de detalle mostrará la información asociada a la traza, así como todas las aquellas *subtrazas* dependientes de la traza principal. Este panel permite además al administrador generar un informe en formato PDF con la información completa asociada a la traza consultada.

5.3.15.2 Consulta trazas de servicio.

Aparte de las trazas de mantenimiento, asociadas a operaciones realizadas en las tareas de administración de la plataforma. Existen también las trazas de servicio, asociadas a todos los servicios ofrecidos por la plataforma:

- Validar certificado WebService
- Validar certificado WebService DSS
- Validar certificado OCSP
- Obtener información de certificado

- Validar firma
- Validar firma DSS
- Firma servidor
- Firma servidor DSS
- Firma servidor. CoSign (Co-Firma)
- Firma servidor. CoSign DSS (Co-Firma DSS)
- Firma servidor. CouterSign (Contra-Firma)
- Firma servidor. CounterSign DSS (Contra-Firma DSS)
- Actualizar firma
- Validar certificados en lote
- Validar firmas en lote
- Validación asíncrona de certificados
- Validación asíncrona de firmas
- Consulta de peticiones asíncronas
- Finalizar actualizar firma con periodo de gracia
- Finalizar firma servidor con periodo de gracia
- Finalizar firma. CoSign (Co-Firma) con periodo de gracia
- Finalizar firma. CounterSign (Contra-Firma) con periodo de gracia
- Almacenar documento
- Eliminar contenido de documento
- Obtener identificador de documento firmado
- Obtener firma transacción
- Obtener firma transacción DSS
- Obtener contenido de documento firmado

- Obtener contenido de documento

Mediante la pestaña ***"Auditar Trazas de servicio"*** el administrador puede consultar todas aquellas trazas de servicio ocurridas en la plataforma en un instante de tiempo determinado.

Para facilitar la búsqueda de una traza en particular o un conjunto de trazas de servicio, se han definido tres tipos de cuadros de búsqueda:

- ***Búsqueda por identificación de transacción***. Mediante este filtro de búsqueda, el administrador puede buscar una traza de servicio concreta dada su identificador de transacción.



Figura 208 - Búsqueda Trazas de servicio por Identificador de Transacción

- ***Búsqueda por rango de fechas***. Este filtro permite al administrador buscar todas aquellas trazas que han ocurrido en un rango de tiempo definido. Permitiendo además discriminar por tipo de servicio o mostrar todas las trazas de servicio ocurridas en dicho rango de tiempo.



Figura 209 - Búsqueda Trazas de Servicio por Rango de Fechas

- ***Búsqueda por aplicación***. Usando este filtro, podemos realizar la búsqueda de todas aquellas trazas de servicios dada la aplicación involucrada en el servicio ejecutado. El usuario puede indicar la ruta completa de la aplicación, o buscarla mediante en el árbol de aplicaciones que aparece cuando el usuario pulsa el botón.



Figura 210 - Búsqueda Trazas de Mantenimiento por Aplicación



Tras definir el tipo de búsqueda y el contenido a aplicar en el filtro, el usuario deberá pulsar el botón ***"Buscar"***. En ese momento el sistema buscará todas aquellas trazas que cumplen con el filtro definido y mostrará el resultado final en la tabla de resultados situada en la parte inferior de los cuadros de búsquedas. Para facilitar la tarea de búsqueda al

administrador en el caso de que existan muchos resultados, esta tabla ha sido paginada, mostrando en cada página un máximo de 10 resultados.

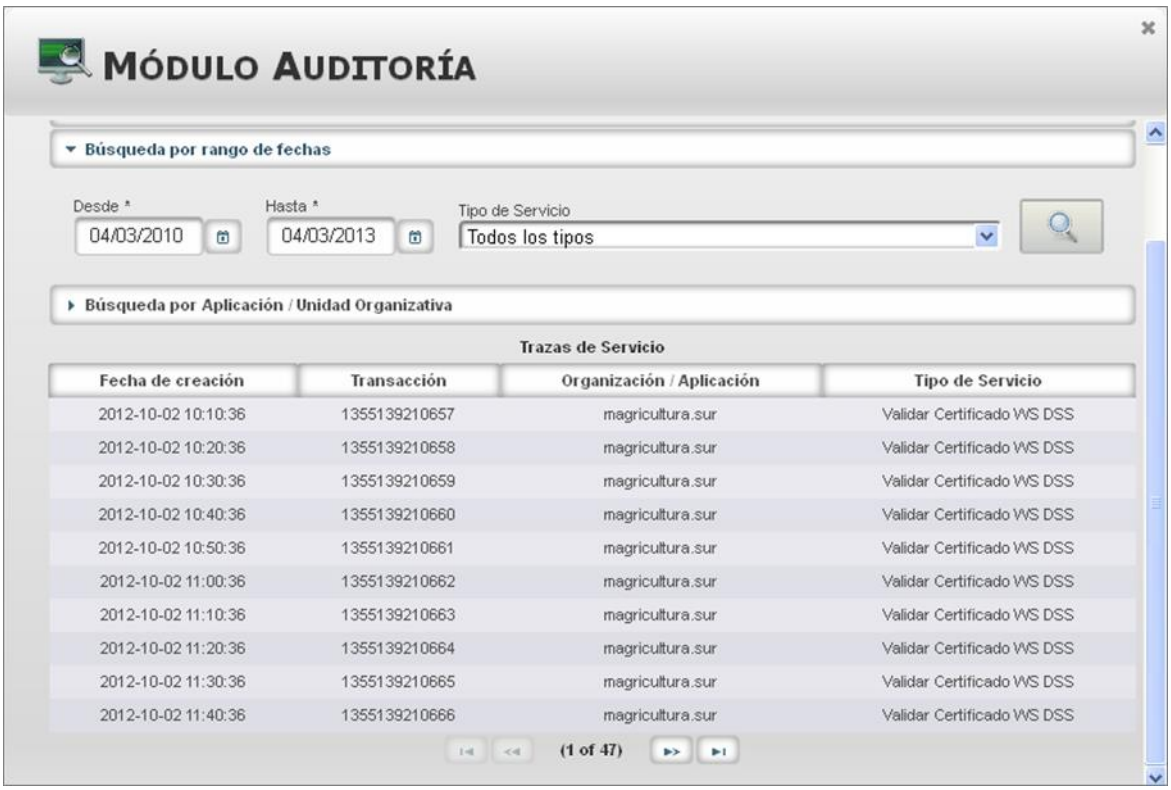


Figura 211 - Resultado Búsqueda de Trazas de Servicio

Una vez el administrador haya localizado la traza a consultar, podrá pulsar sobre dicha traza para obtener una información más detallada.

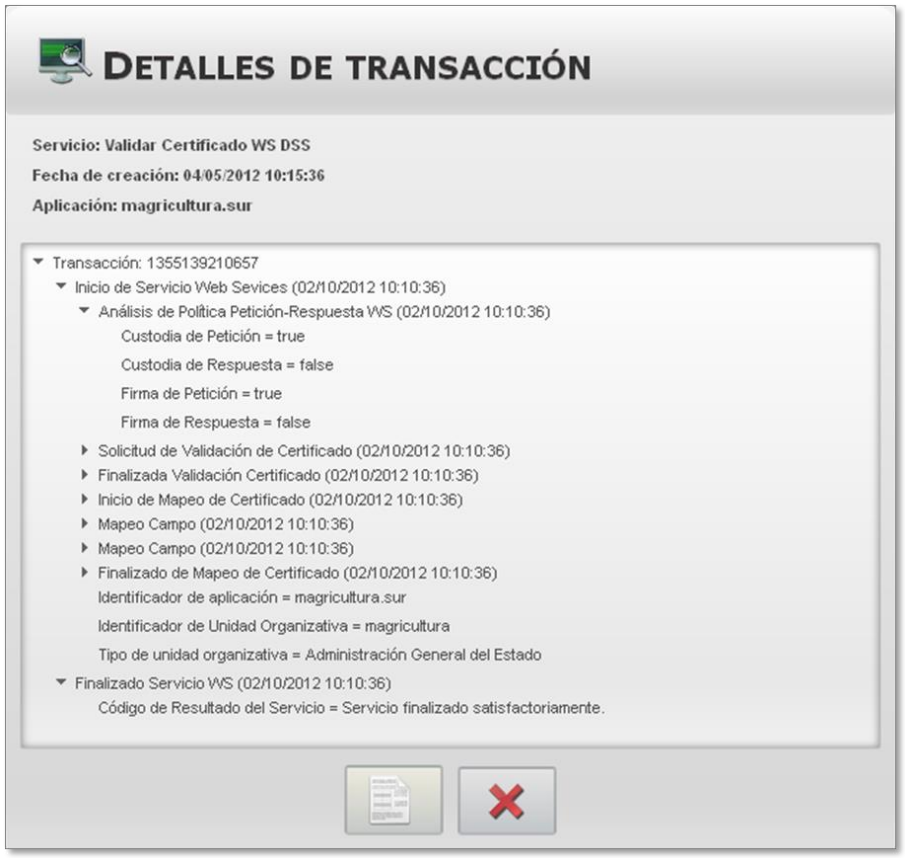


Figura 212 - Panel Detalle Trazas de Servicio



El panel de detalle mostrará la información asociada a la traza, así como todas las aquellas *subtrazas* dependientes de la traza principal. Este panel permite además al administrador generar un informe en formato PDF con la información completa asociada a la traza consultada.

5.3.15.3 Consulta de alarmas ocurridas en la plataforma

Por último, mediante el botón ***"Auditar trazas de alarma"*** el administrador puede consultar todas aquellas alarmas ocurridas en la plataforma en un rango de tiempo determinado. El filtro existente en esta pestaña permite además filtrar por un conjunto de alarmas.



Figura 213 - Búsqueda Trazas de Alarmas



Tras definir el filtro, y pulsar el botón ***"Buscar"***, los resultados aparecerán en la tabla situada en la parte inferior del filtro. Esta tabla, al igual que las anteriores se encontrará paginada en grupos de 10 resultados para facilitar al administrador la tarea de búsqueda en caso de que existan muchos resultados.

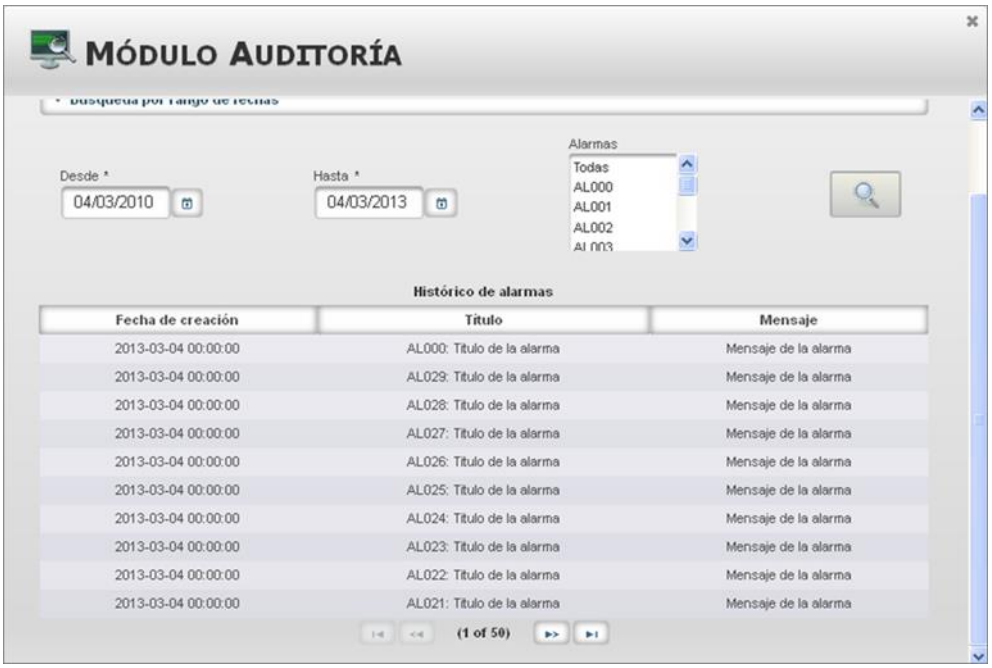


Figura 214 - Resultado Búsqueda Trazas de Alarmas

5.3.16 Módulo de Consultas

Este módulo permite la consulta de datos directamente en base de datos y también ofrece la posibilidad de validar una firma electrónica. La intención es facilitar el trabajo de los administradores de la plataforma.

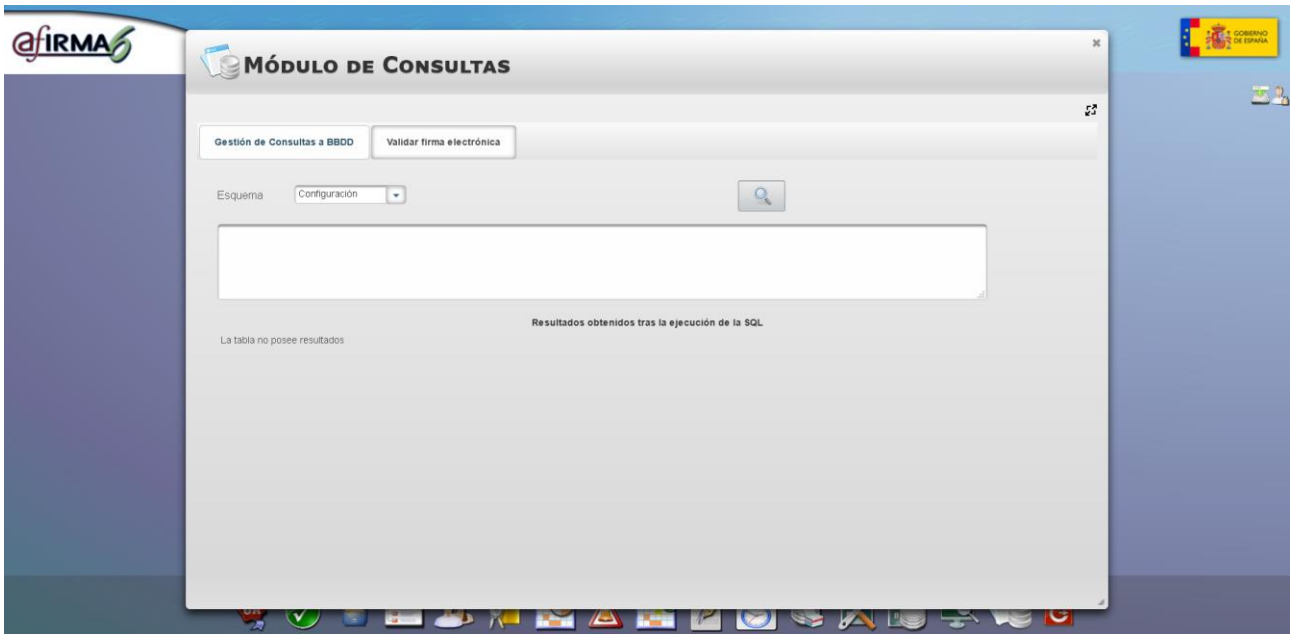


Figura 215 - Interfaz del módulo SQL/LOG

5.3.16.1 Gestión de Consultas a BBDD

La primera pestaña que tenemos muestra la funcionalidad para poder hacer consultas SQL directamente sobre el esquema de base de datos que seleccionemos (configuración o transaccional).



Tiene un uso sencillo puesto que sólo debemos de seleccionar el esquema correspondiente, escribir la sentencia a ejecutar y pulsar en el botón:



Figura 216 – Resultados de consulta SQL

Se han establecido una serie de restricciones en las consultas ya que puede darse una sobrecarga si se permiten realizar consultas muy pesadas:

- Todas las consultas deben de empezar por “SELECT”: con esto restringimos que no se puedan hacer inserciones, eliminaciones ni modificaciones en la BBDD, sólo consultar datos.

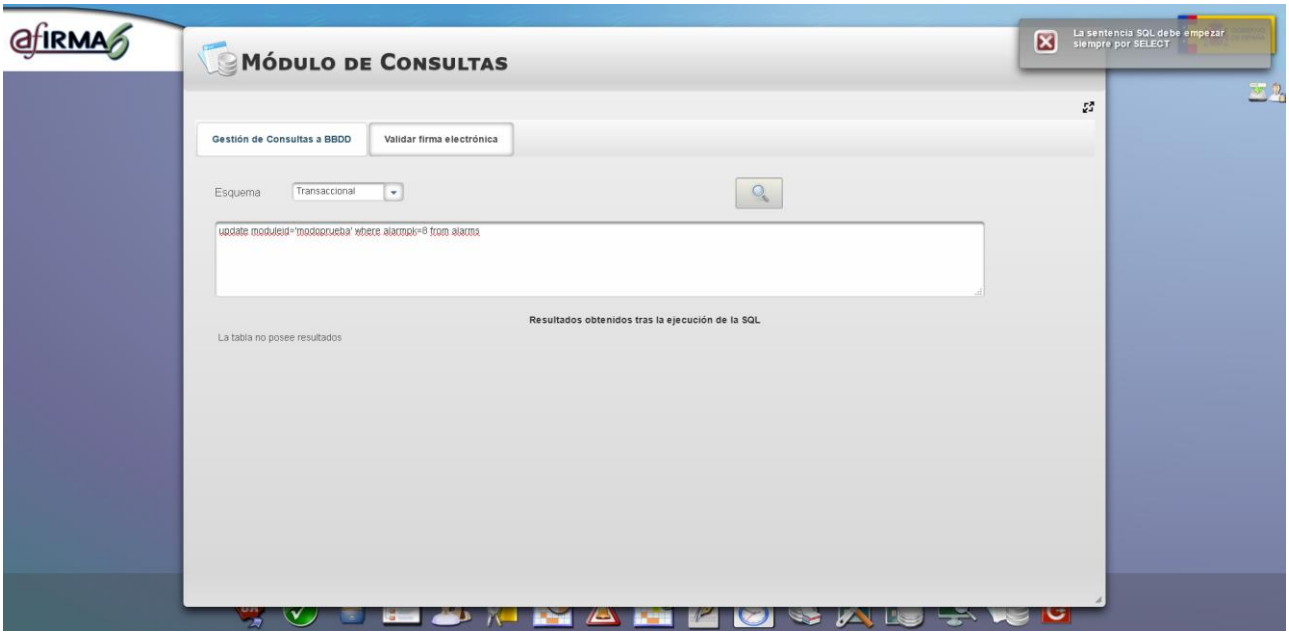


Figura 217 – Error al ejecutar "update" SQL

- No se permite el uso del operador "*", así consultamos sólo los campos que queramos comprobar y no todos los de la tabla, con lo que hacemos más ligeras las consultas.

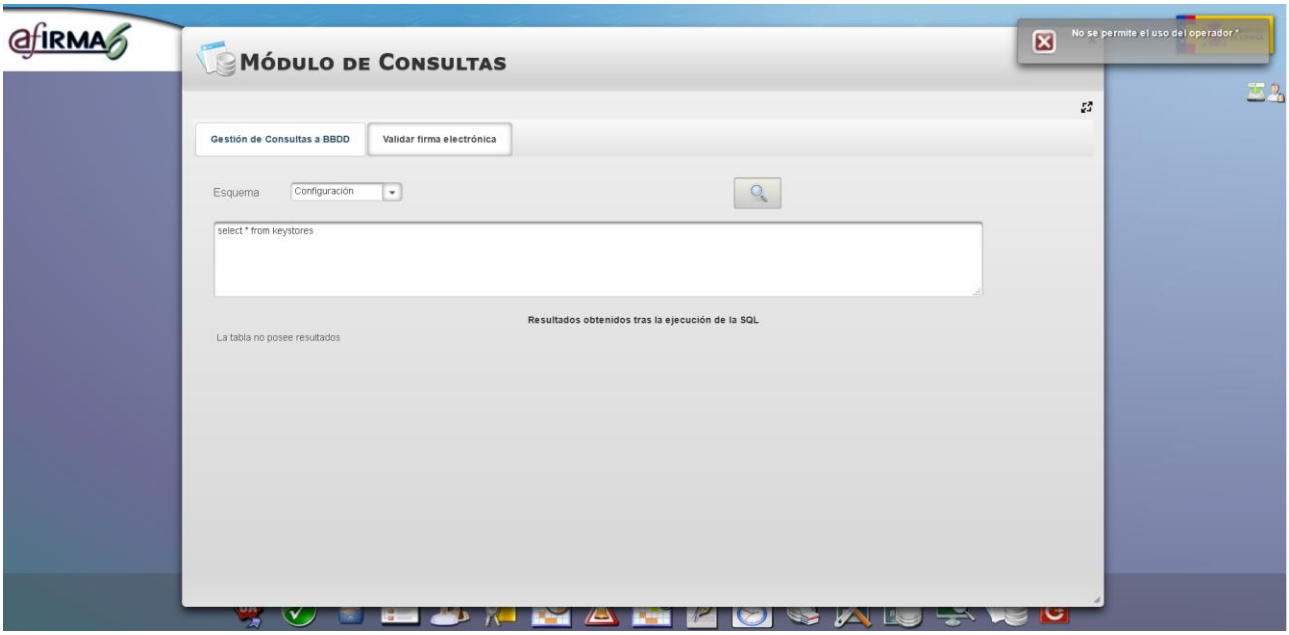


Figura 218 – Error usando operador "*" en consulta SQL

- No se permite el uso de "SELECT" anidados para hacer subconsultas, así como el uso del "JOIN". Por tanto, sólo podremos obtener datos de una tabla en concreto en cada consulta.

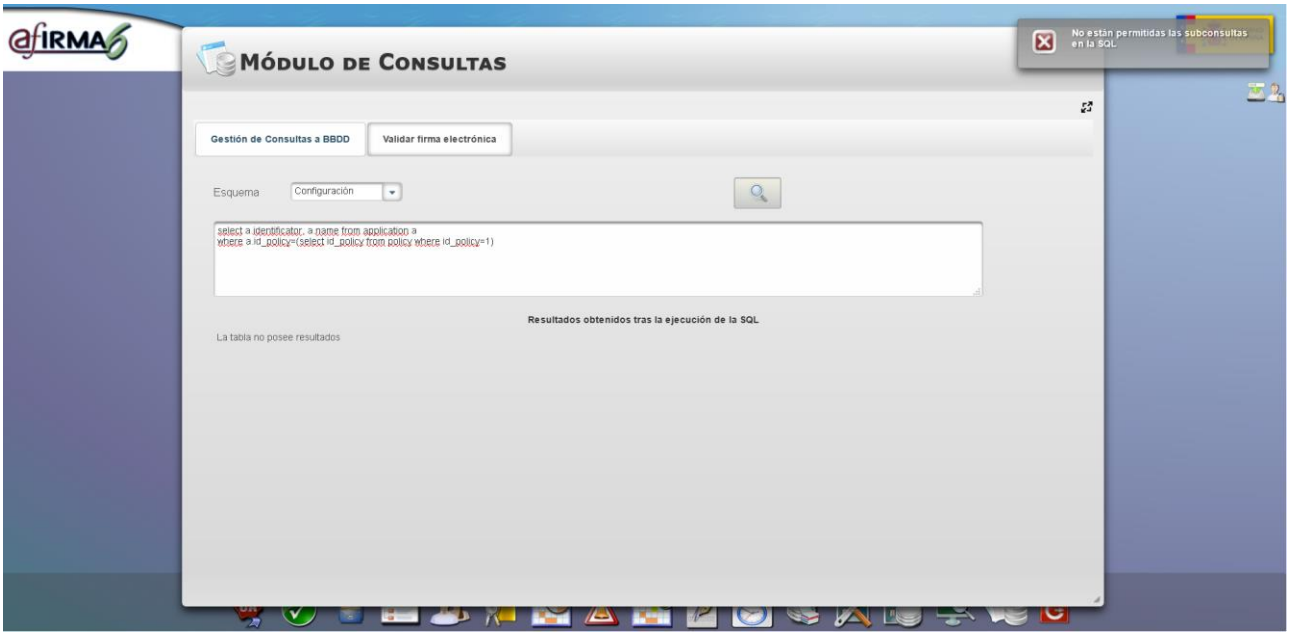


Figura 219 – Error utilizando subconsultas en la SQL



Figura 220 – Error utilizando "join" en la SQL

- Si decidimos consultar una columna que contenga datos binarios, podemos descargarlos directamente desde la pantalla de la aplicación, consiguiendo así el/los ficheros/s que queramos tener en nuestro equipo.

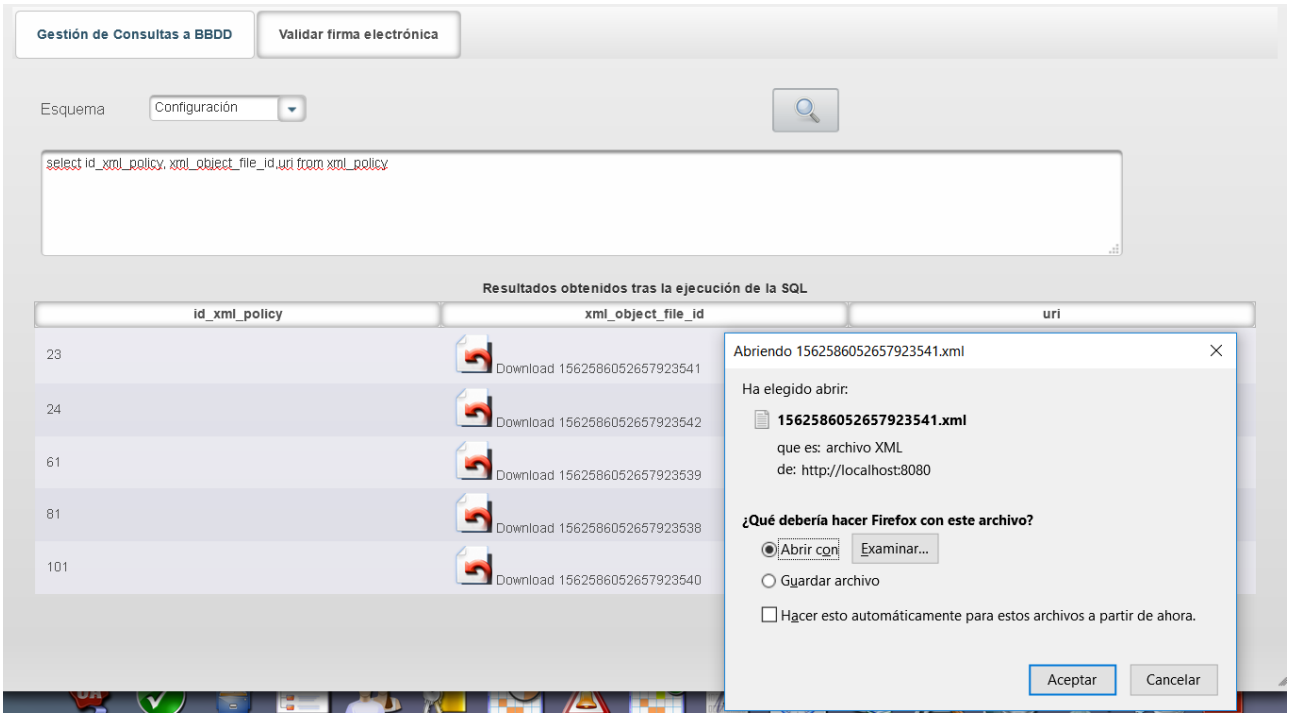


Figura 221 – Descarga de fichero usando sentencias SQL

- Finalmente, si escribimos mal la consulta SQL o si no existe la tabla indicada en el esquema seleccionado, nos saltará un error en pantalla indicando que "La sql ejecutada no es correcta".

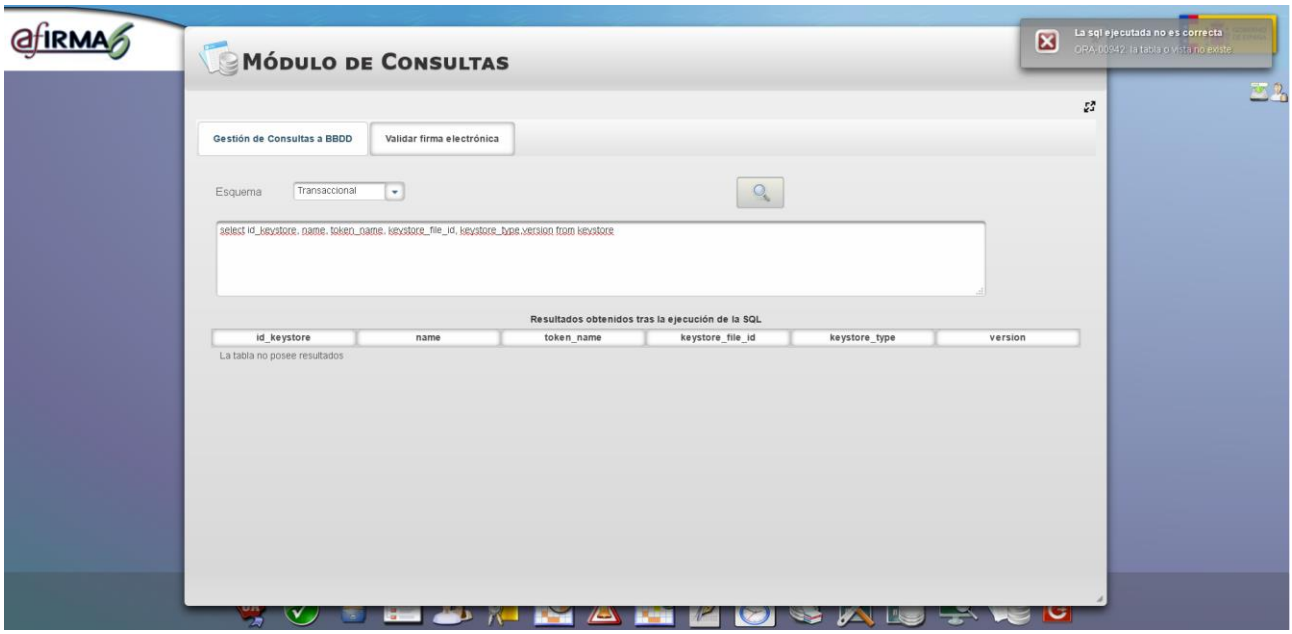


Figura 222 – Error de ejecución de consulta SQL

5.3.16.2 Validación firma electrónica

Esta pestaña permite al administrador validar una firma de forma rápida.

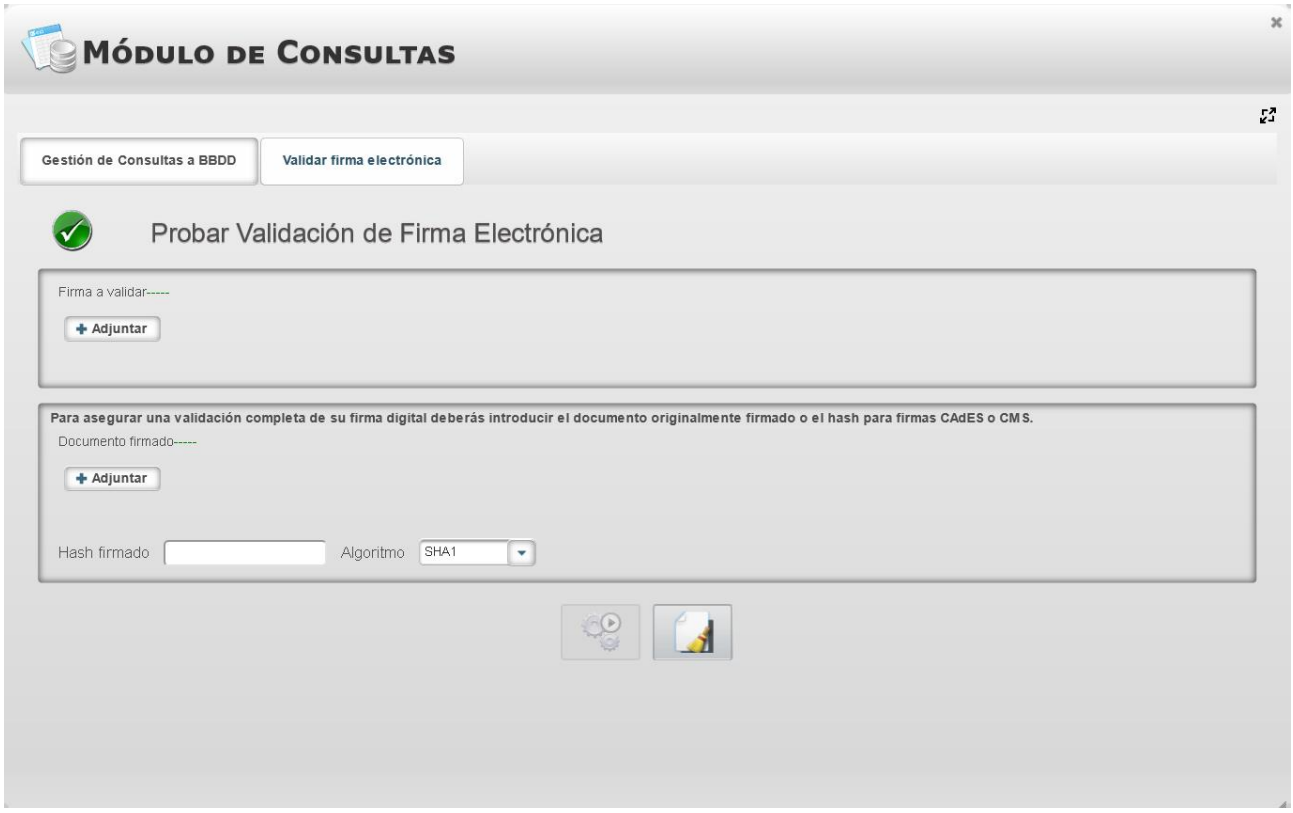


Figura 223 – Validación de firma electrónica

Existen 2 secciones:

- **Firma a validar:** Permite adjunta la firma que se desea validar contra la plataforma.
- **Documento firmado:** Para firmas CAdES o CMS es recomendable adjunta el fichero sin firmar, de este modo la validación será completa. También es posible introducir el resumen del fichero firmado, especificando el tipo de algoritmo de resumen utilizado.

Tras introducir los datos, pulsamos el botón "Validar Firma" para realizar la validación .

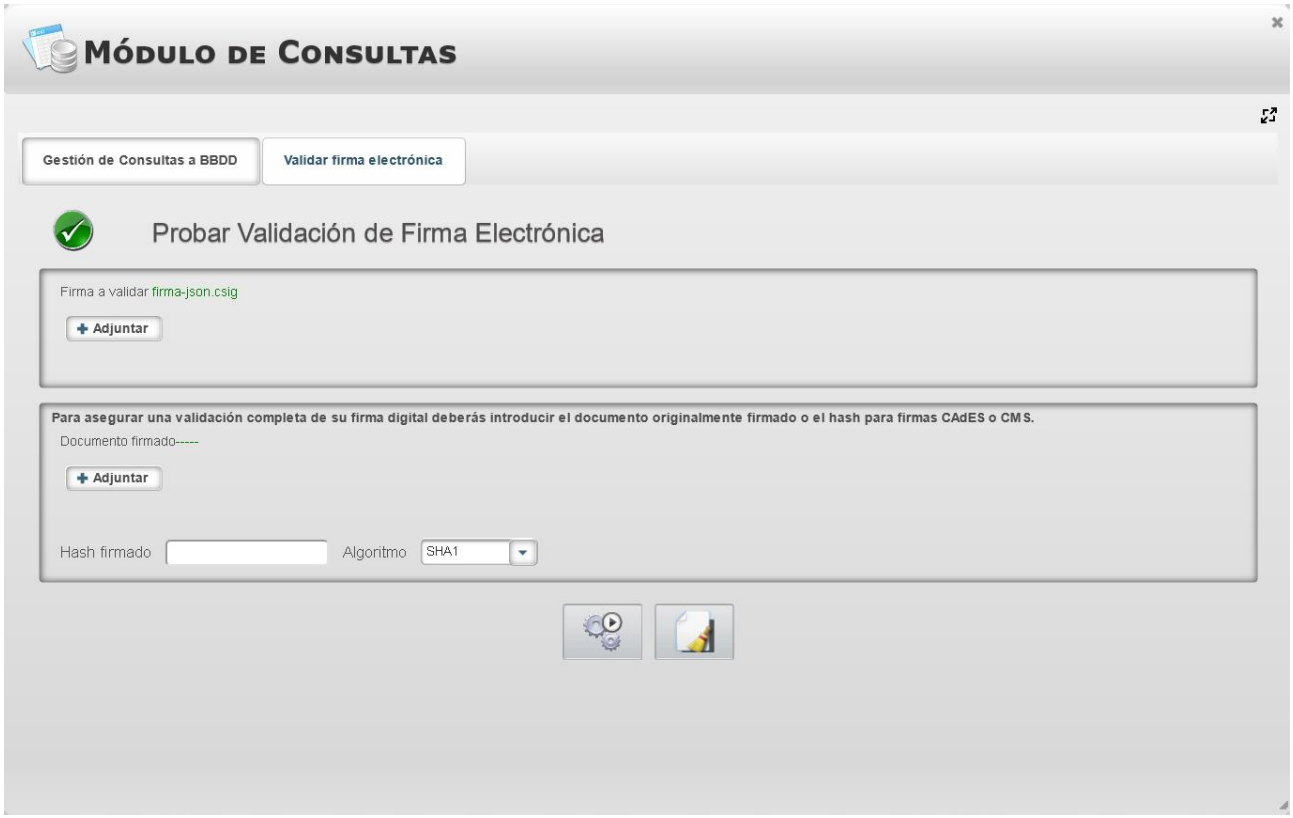


Figura 224 – Validar firma

Tras la validación, se mostrará una ventana con el resumen del resultado de la validación:



Figura 225 – Resultado de validación (I)

Desde esta ventana podemos descargarnos un informe del proceso de validación, ver información general sobre la validación, como por ejemplo si la firma es válida, si el certificado es válido, el tipo de

firma, el certificado usado para la firma e incluso podemos descargarnos el certificado firmante y los elementos de validación.



Figura 226 – Resultado de validación (II)

Teniendo en cuenta la segunda opción para realizar la validación completa, debemos incluir, aparte de la firma, el documento firmado o su hash firmado, seleccionando el algoritmo de hash usado. En caso de que el documento no corresponda con la firma a validar, nos lo indicará con un error en la ventana de información, aunque la firma sí sea correcta.



Figura 227 – Resultado de validación (II)

Por último, si queremos eliminar todos los datos introducidos para realizar alguna otra validación, podemos reiniciar los parámetros de la pestaña pulsando en “Limpiar formulario” .

Anexos

6 Anexo I. Caso Práctico: Utilización de CRL particionadas y descarga en caché L2

Se desea configurar los mecanismos de validación de los certificados de DNI Electrónico por medio de sus CRL particionadas. Las CRL deben ser almacenadas localmente en la caché de nivel 2 y deben ser actualizadas periódicamente cada hora.

El DNI Electrónico posee una jerarquía de certificación donde el nodo raíz (*AC RAIZ DNIE*) emite un número definido de CA intermedias con la nomenclatura AC DNIE XXX. Cada una de estas CA intermedias emitirán los mismos tipos de certificados que deberán ser validados por medio de las CRL emitidas por la CA específica *ARC DNIE 001*.

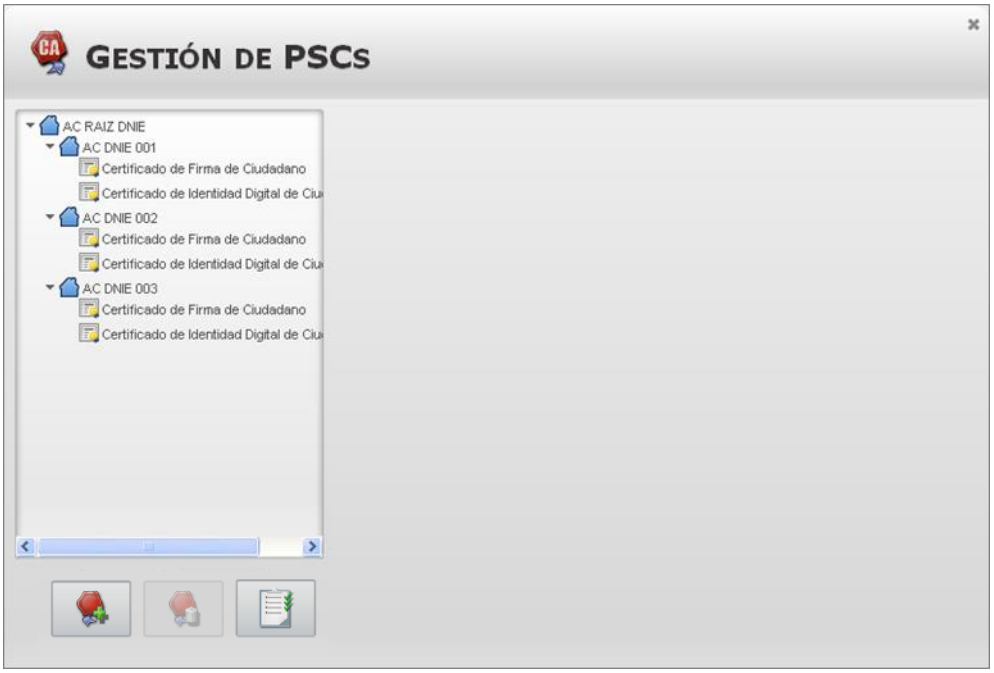


Figura 228 - Jerarquía de Certificación del EDNI

Dicha CA emite 1000 CRL para cada una de las CA intermedias del EDNI, por lo que se generarán 3000 CRL, donde para cada CA se utilizará un identificador distinto para discriminar las CRL. La nomenclatura que siguen los nombres de CRL es la siguiente:

XXXXXXXXXX-N.crl

Donde

XXXXXXXXXX, se denomina identificador de partición, y es un identificador que será único para cada CA y permitirá discriminar las CRL asociadas a cada una de ellas. Este identificador es proporcionado por la CA y sus valores para cada una de ellas son:

AC DNIE 001 SHA2: 1111111111

AC DNIE 002 SHA2: 2222222222

AC DNIE 003 SHA2: 3333333333

N es el número de la CRL que puede ir de 0 a 999.

A continuación, se detalla cómo se debe realizar la configuración para la descarga periódica y validación de certificados mediante estas CRL. Se parte del supuesto de que los Prestadores ya han sido dados de alta en la plataforma de la manera especificada en este mismo documento.

6.1 Configuración del PSC

En primer lugar, es necesario asignar el identificador de partición correspondiente a cada uno de las CA intermedias. Para ello, debemos ir a la pantalla de gestión de prestadores y seleccionar el Prestador deseado. En nuestro caso, la CA *AC DNIE 001.*

En el campo “Identificador de Partición” deberemos introducir el identificador asociado a la CA y pulsar el botón “Modificar”. En este caso, el identificador a especificar es “1111111111”.

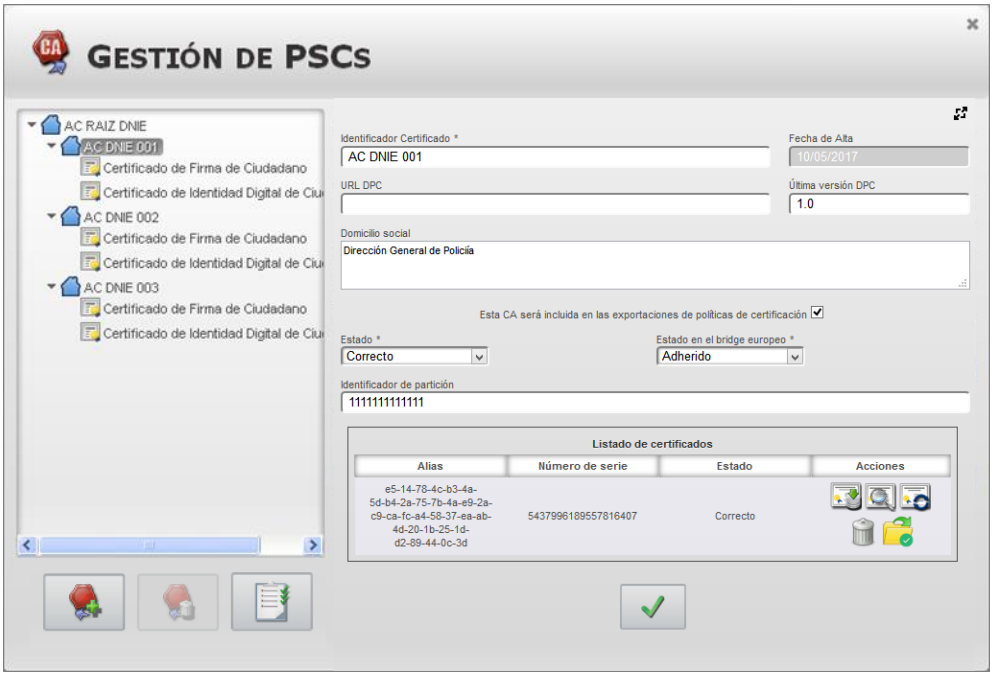


Figura 229 - Asignación de Identificadores de Partición

Se realizará el mismo proceso para las CA *AC DNIE 002 SHA2* y *AC DNIE 003 SHA2* con los identificadores de partición apropiados.

6.2 Adición del certificado emisor de las CRL en el almacén de confianza de CRL

Antes de proceder a crear los métodos de validación es necesario agregar los certificados de los emisores de las CRL que se van a utilizar en el almacén de confianza destinado a tal efecto. Para ello, deberemos ir a la gestión de Keystores, y pulsar sobre el keystore “AlmacenConfianzaCRL”.



Figura 230 - Adición de Certificados de Confianza de Emisores de CRL

Para añadir los certificados en el almacén, se debe pulsar el botón "Importar Certificado", y en la ventana que aparece deberemos especificar fichero local que contiene el certificado asociado al emisor de CRL que deseamos importar. En este caso se indicará el fichero que contiene el certificado de la CA *ARC DNIE 001* (CA intermedia cuya labor es firmar las CRL para toda la jerarquía de certificación del EDNI). En caso de no poseer el certificado, se puede exportar en la pantalla de consulta de datos de un prestador, en el módulo de gestión de prestadores.

Tras seleccionar el fichero y pulsar "Aceptar", el sistema mostrará el alias con el que será almacenado el certificado. Este alias no debe ser modificado, por lo que, para finalizar, se pulsará "Aceptar".



Figura 231 - Introducción del Alias del Certificado a Importar

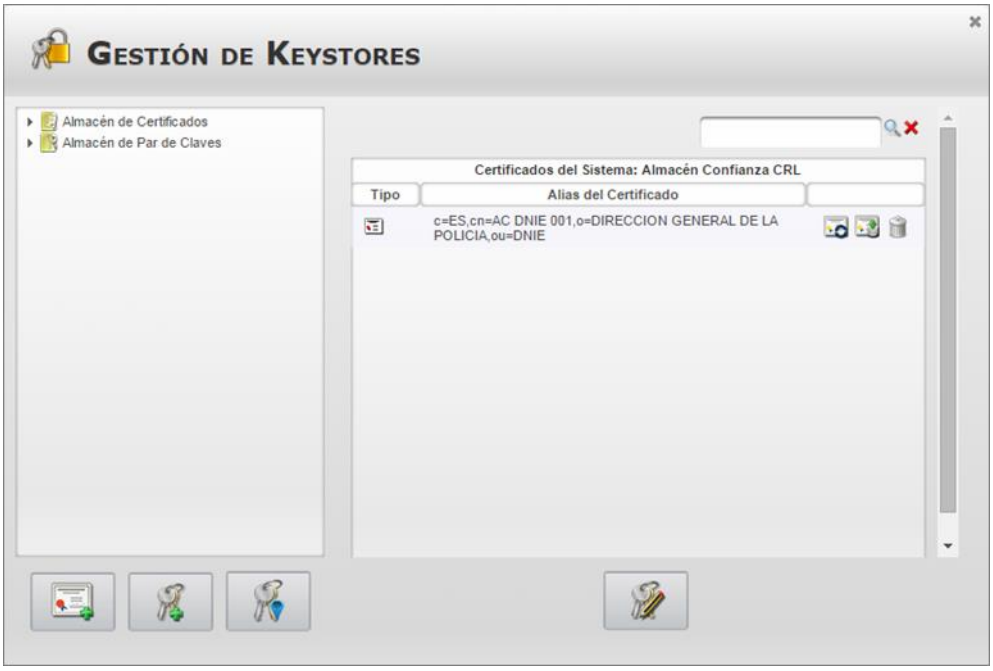


Figura 232 - Certificado DNI 001 en Almacén CRL

6.3 Configuración de los métodos de validación

A continuación, se crearán los métodos de validación apropiados para el acceso a las CRL de las CA emisoras de CRL. Dado que el emisor de las CRL siempre es el mismo, únicamente será necesario crear un método de validación que podrá ser asignado a todas las CA intermedias de la jerarquía del EDNI.

Tras acceder a la gestión de métodos de validación y pulsar “Alta Met. Val.”, se abrirá la pantalla de alta, donde lo único a destacar es que la URL del servidor debe especificar la URI donde cuelgan todas las CRL particionadas (por tanto, todas las CRL deberán estar publicadas bajo en la misma ubicación).

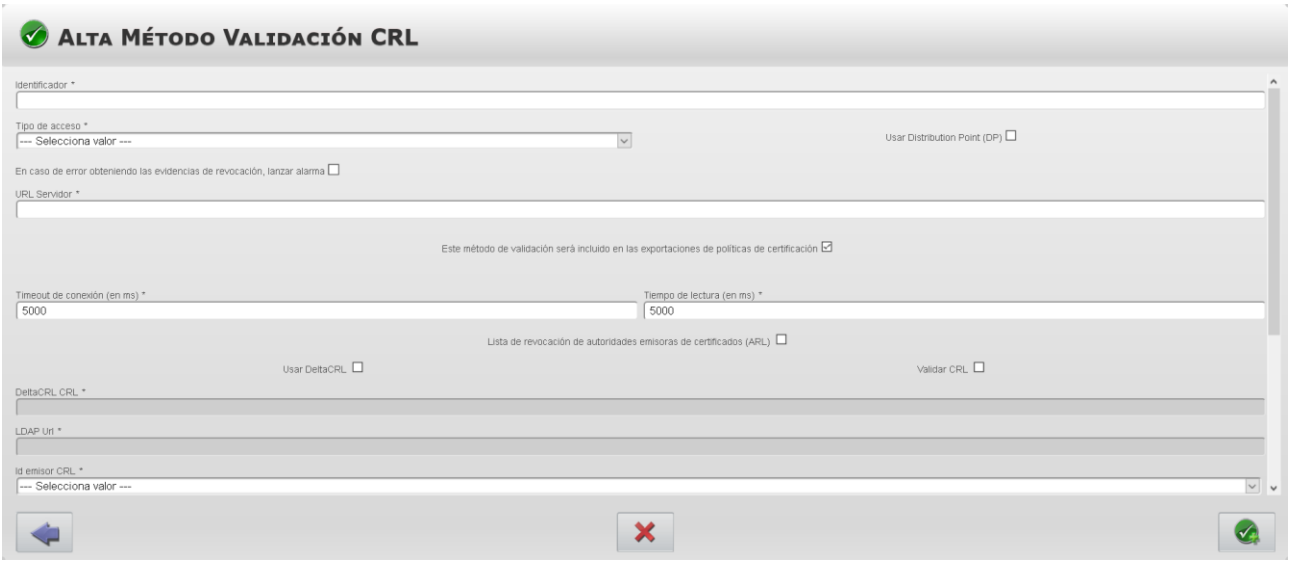


Figura 233 - Alta del Método de Validación (I)

Tras pulsar el botón “Continuar” se pasará a la segunda pantalla de alta, donde se deberán especificar los siguientes datos:

- **Tipo Acceso.** Según el tipo de método a utilizar para el acceso a la CRL. En este caso, será http.
- **Validar CRL.** Se desactivará el check para que las CRL únicamente se validen en la descarga y no cada vez que se consulten.
- **Id Emisor CRL.** Este dato es importante, ya que permitirá validar la CRL en el momento de la descarga. La lista de emisores que aparecen en el menú desplegable será la lista de certificados existentes en el keystore “AlmacenConfianzaCRL”, por lo que el emisor debe haberse dado de alta previamente.
- **Campos de autenticación.** Esta información es independiente de si las CRL son o no particionadas, por lo que se completarán según las necesidades específicas.
- **Almacenar CRL.** Se activará el check con el fin de especificar los parámetros de almacenamiento de las CRL en la caché de nivel 2 (incluido si se quiere cachear dicha CRL).

- **Tipo de Repositorio.** El repositorio utilizado en este caso será BBDD.

- **Nombre Fichero Repositorio.** Según la nomenclatura que seguirán las CRL, el formato del nombre de la CRL será el siguiente: ?-*.crl

  De esta forma, en tiempo de validación de un certificado, el carácter '?' será sustituido por el identificador de la partición especificado en la configuración del emisor de la CRL, mientras que el carácter '*' será sustituido por el número de la partición que posee la información del certificado a validar (este número es calculado de forma interna por el sistema, en base a las especificaciones proporcionadas por la DGP).

- **Número de particiones.** En nuestro caso, se emitirán 1000 particiones de la CRL para cada CA intermedia.

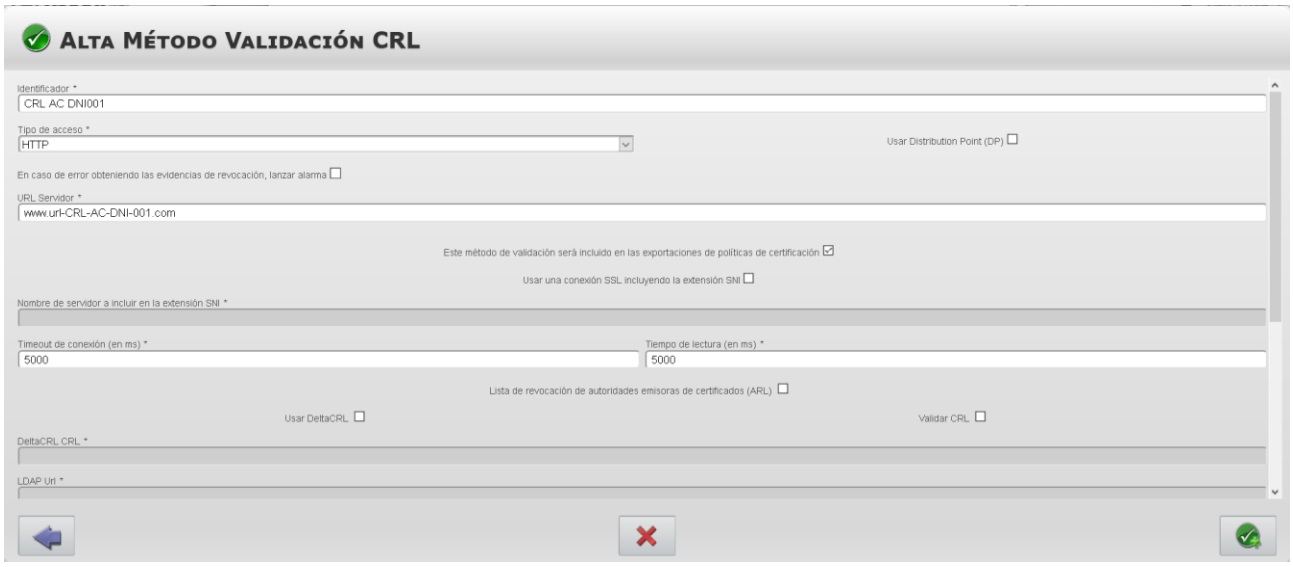


Figura 234 - Alta del Método de Validación (II)



Figura 235 - Alta del Método de Validación (III)

En este ejemplo únicamente se ha creado un método de validación, sin embargo, si existieran diversas maneras de acceder a la CRL (por LDAP, FTP, etc.), se deberían crear métodos de validación para contemplar estas posibilidades, lo que permitiría acceder a la CRL aun cuando alguno de ellos no estuviera activo.

6.4 Asignación de los métodos de validación

Tras crear el método de validación, se deberá asignar a cada una de las CA intermedias de la jerarquía del EDNI, esto es, a las CA *AC DNIE 001, AC DNIE 002 y AC DNIE 003.*

6.5 Creación de las tareas de descarga de las CRL

El último paso del proceso es la creación de la tarea que se encargará de descargar y almacenar las CRL en la caché de nivel 2.

En el caso que nos aborda, como el emisor de las CRL es el mismo, todas las CRL están ubicadas en el mismo lugar, y sus nombres poseen el mismo formato, únicamente será necesario definir una tarea, que llevará a cabo la descarga de todas las CRL.

En la pantalla de gestión de descargas de CRL, se debe pulsar el botón “Alta Tarea”. En la pantalla de Alta se deberán especificar los siguientes datos.



Figura 236 - Alta de la Tarea de Descarga

- **Identificador**. El identificador del grupo de descarga.
- **Tiempo Refresco**. Según las especificaciones deberá ser de 60 minutos.
- **Tipo Descarga**. Especificaremos la opción *Múltiple* que permitirá la descarga de CRL particionadas.
- **Número de particiones**. Se especificarán 1000 particiones, lo que significa que existirán 1000 CRL emitidas con cada identificador de partición.

Tras pulsar el botón "Aceptar", la tarea será dada de alta, debiéndose especificar en este momento las particiones y los métodos de validación a utilizar para descargar las CRL. Para modificar la tarea de descarga recién creada, se seleccionará la misma en el árbol de tareas, mostrándose su configuración en la parte derecha de la pantalla.

A continuación se añadirán los identificadores de partición definidos para cada una de las CA emisoras. Para ello, se especificará el identificador en el cuadro "Partición" y se pulsará el botón "Añadir". La tarea se modificará directamente sin necesidad de pulsar el botón "Modificar".



Figura 237 - Asignación de Identificadores de Partición a Una Tarea (I)

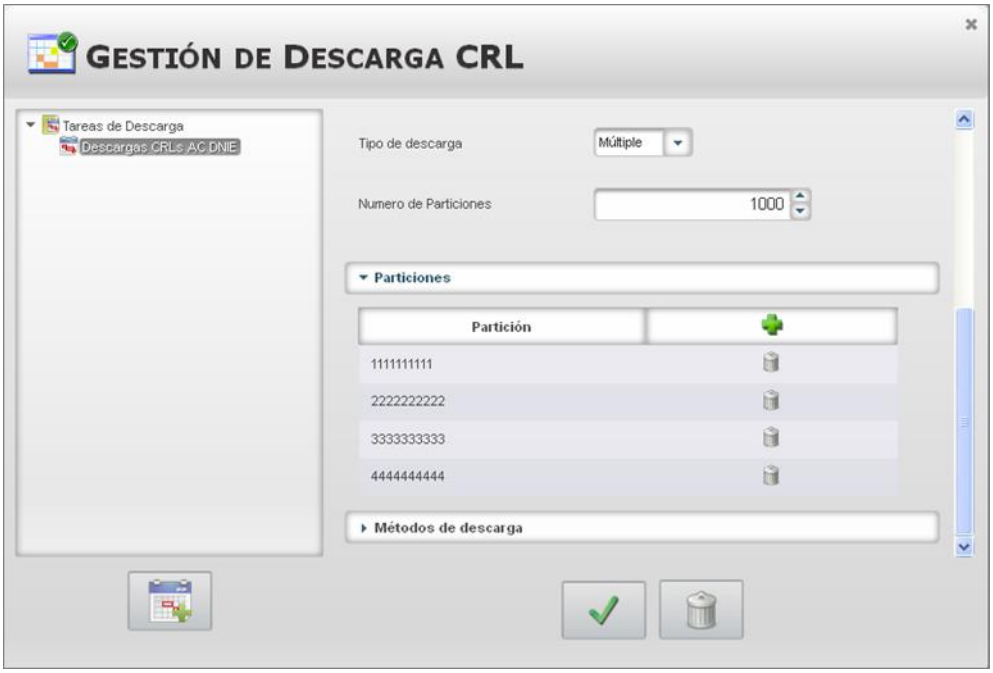


Figura 238 - Asignación de Identificadores de Partición a Una Tarea (II)

Para finalizar el proceso, se asignarán los métodos de validación a utilizar. En nuestro caso únicamente se añadirá el método que hemos creado anteriormente (CRL por http).

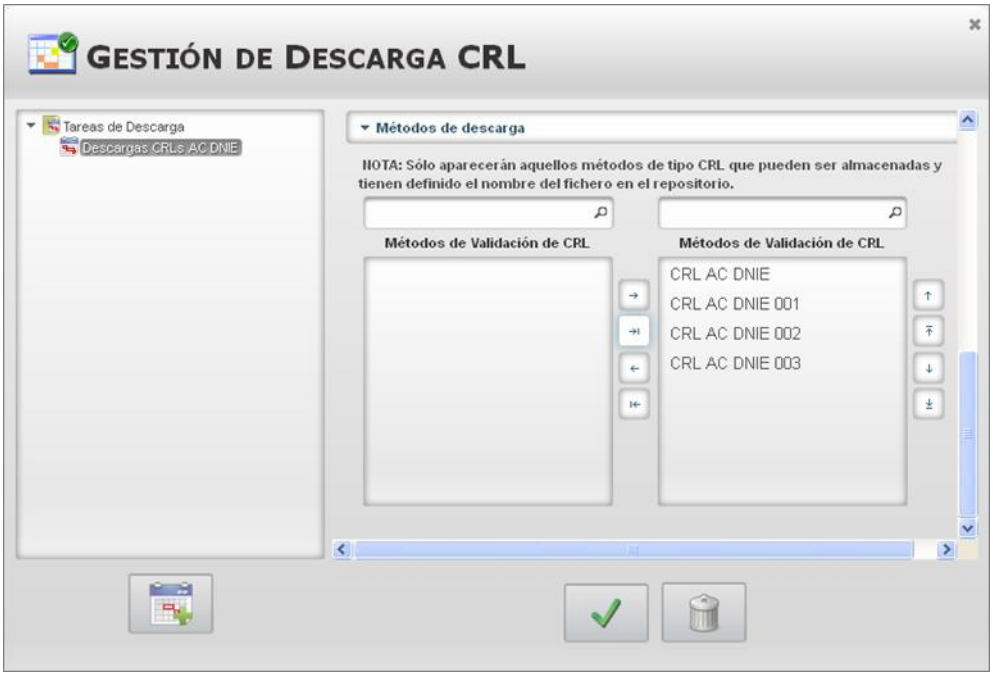


Figura 239 - Asignación de Métodos de Validación a una Tarea

Una vez dada de alta la tarea, el sistema iniciará automáticamente la descarga de las CRL de forma secuencial, obteniendo 1000 CRL por cada identificador de partición especificado, según la nomenclatura especificada en el método de validación utilizado.

7 Anexo II. Caso práctico. Definición de métodos de validación: Tipo Asociación “Expresión Regular”

7.1 Expresiones regulares estándar de Java

Una expresión regular es una manera de describir un conjunto de cadenas de texto a partir de unas características comunes compartidas por todas las cadenas del conjunto, es decir, una expresión regular nos permitirá buscar patrones en una cadena de texto. Por ejemplo: la expresión “a*” describe el conjunto de cadenas de texto que empiezan por “a”, es decir: “a*”. “aa”, “ab”, “ac”, … “aab”, “aac”, …, “antes”, “anterior”, etc, …

Las expresiones regulares pueden usarse para buscar, editar o manipular texto (o datos).

Par la definición de expresiones regulares en Java, se pueden usar:

- Literales (como por ejemplo “CN=”).
- Límites. Por ejemplo:

^	Comienzo de una línea
$	Fin de una línea
\b	Fin de palabra
\B	No es fin de palabra
\A	El principio de la cadena de entrada
\G	El final del ultimo patrón encajado
\Z	El final de la entrada pero el terminador final, si existe
\z	El final de la cadena de entrada

- Clases de caracteres (letras, números, etc…). Por ejemplo:

.	Cualquier carácter
X*	X, cero o ninguna vez
X+	X, una o más veces
X{n}	X, exactamente n veces
X{n,}	X, por lo menos n veces
X{n,m}	X, por lo menos n veces pero no más de m veces

- Cuantificadores (una vez una o varias veces, entre una y tres veces…).Por ejemplo:

?	X, una o ninguna vez
X*	X, cero o ninguna vez
X+	X, una o más veces
X{n}	X, exactamente n veces
X{n,}	X, por lo menos n veces
X{n,m}	X, por lo menos n veces pero no más de m veces

- Grupos de captura (subexpresiones que puede ser tratadas a posteriori, una vez reconocidas). Los grupos se numeran contando los paréntesis abiertos de izquierda a derecha (). El grupo de captura 0 siempre será la expresión completa.

- Operadores lógicos (éste literal o éste otro).

XY	X seguido de Y
X|Y	X o Y
(X)	X, como un grupo de captura

Por ejemplo, una expresión regular para describir el conjunto de cadenas de texto que puede contener el Subject del DNI electrónico de firma, podría ser de la siguiente: “CN=(.*), givenName=(.*),SN=(.*), serialNumber=(.*),C=ES”. Si la analizamos por partes vemos:

- CN=: es un literal
- (.*): Primer grupo de captura (primera “subexpresión”, definida entre paréntesis).
    - . (punto) Es una clase de caracteres (primera “subexpresión”, definida entre paréntesis).
    - *: (asterisco) Es un cuantificador, equivale a “cualquier número de veces” y se aplica al carácter, expresión, clase de caracteres, etc. Inmediatamente anterior.
- givenName=: Otro literal.
- (.*): Es el segundo grupo de captura…
- …

Una vez definida, podemos hacer referencia a los distintos grupos de captura de forma independiente. Así el primer grupo de captura se correspondería con el texto entre “CN=”y “,givenName=”, es decir, el CommonName.

Para más información, consultar http://docs.oracle.com/javase/6/docs/api/java/util/regex/Pattern.html

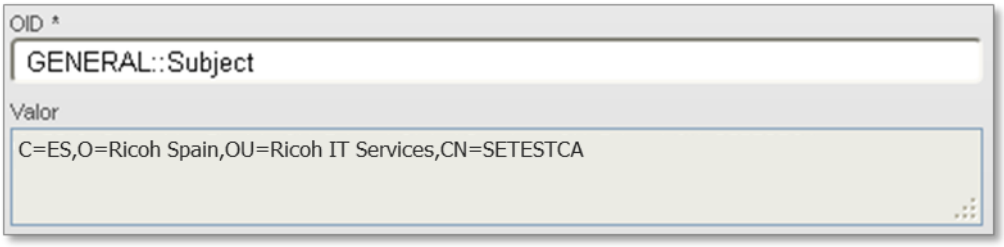
7.2 Referencias a otros campos lógicos

Las expresiones regulares permiten describir un conjunto de cadenas a partir de unas propiedades comunes conocidas ”a priori” y no admiten de manera estándar el uso de variables o referenciadas a otras cadenas distintas de las que se están tratando. Para poder incluir en las expresiones regulares el valor de un campo lógico se indicará con la siguiente notación: ${NOMBRE_CAMPO_LOGICO}.

7.3 Ejemplos prácticos

7.3.1 Ejemplo utilización expresión de Java

Queremos definir el valor del campo lógico “Campo1”, para ello seleccionamos el atributo del certificado “Subject” (que se carga en el campo de la página OID), cuyo valor se cargaría en el campo de la página “Valor”.



De esta cadena queremos extraer los apellidos del responsable, para ello podemos definir la siguiente expresión regular, por ejemplo:

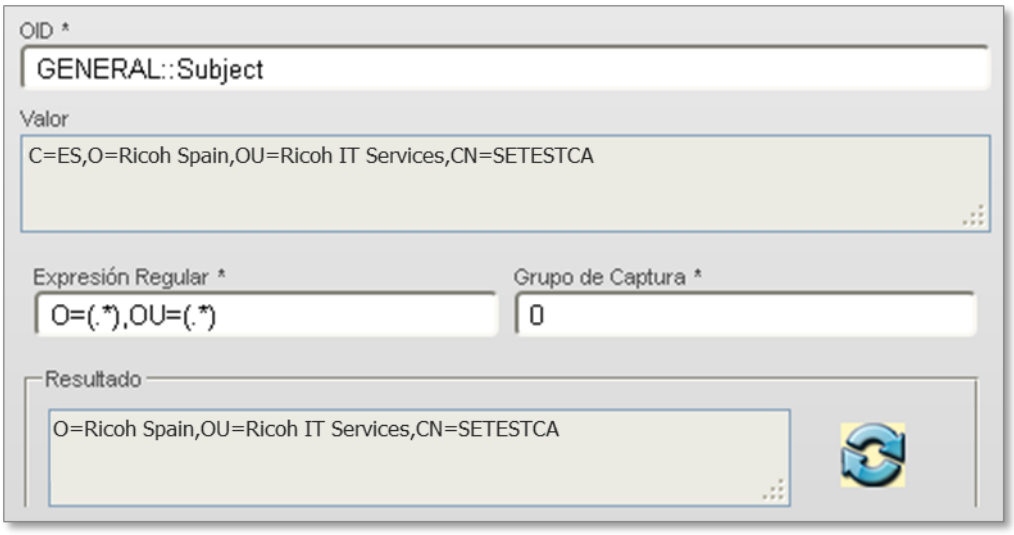


Si analizamos la expresión regular:

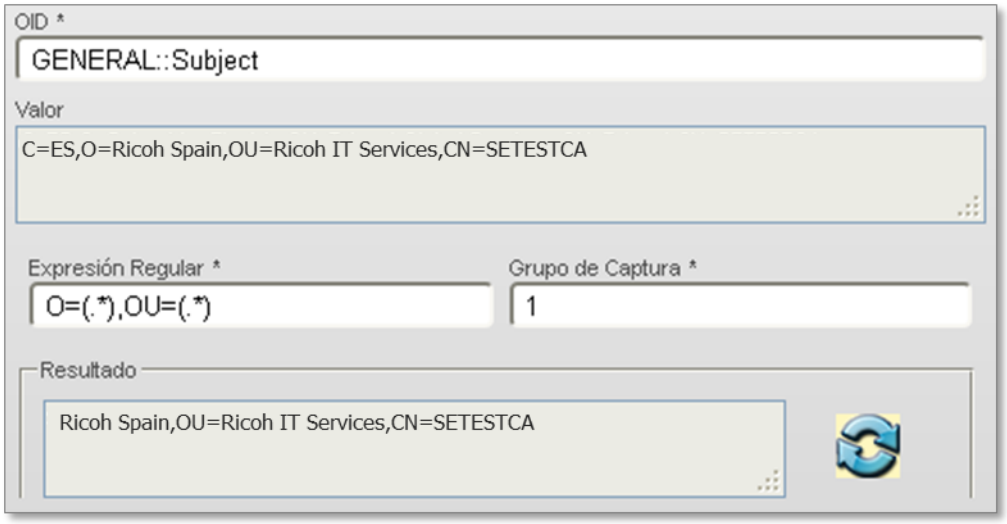
- O= es un literal.
- (.*) Es un grupo de captura, en que indicamos que sea cualquier carácter (con el punto) y repetido 0 o x veces (con el asterisco)
- ,OU= es otro literal.

Al definir dicha expresión regular, hemos definido tres grupos de captura:

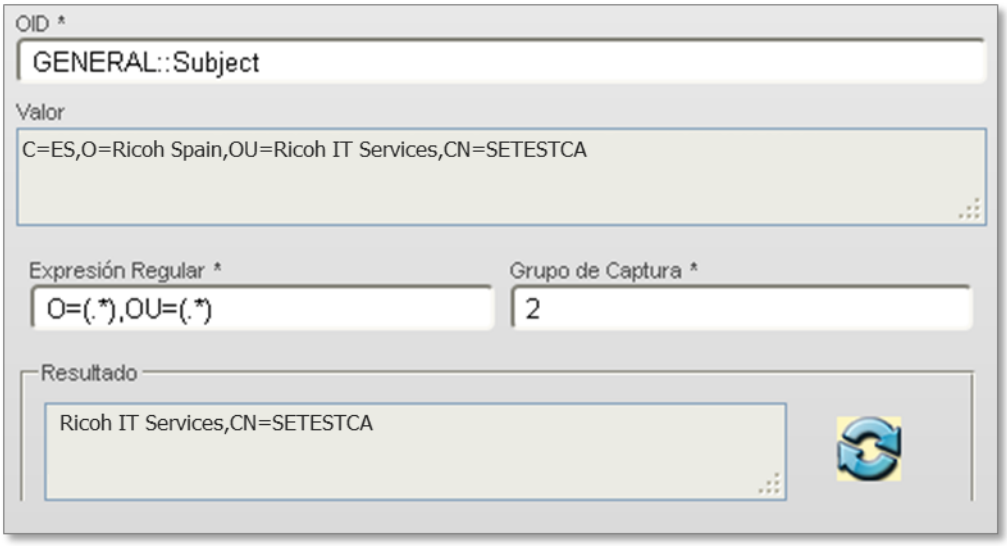
- El grupo de captura 0:



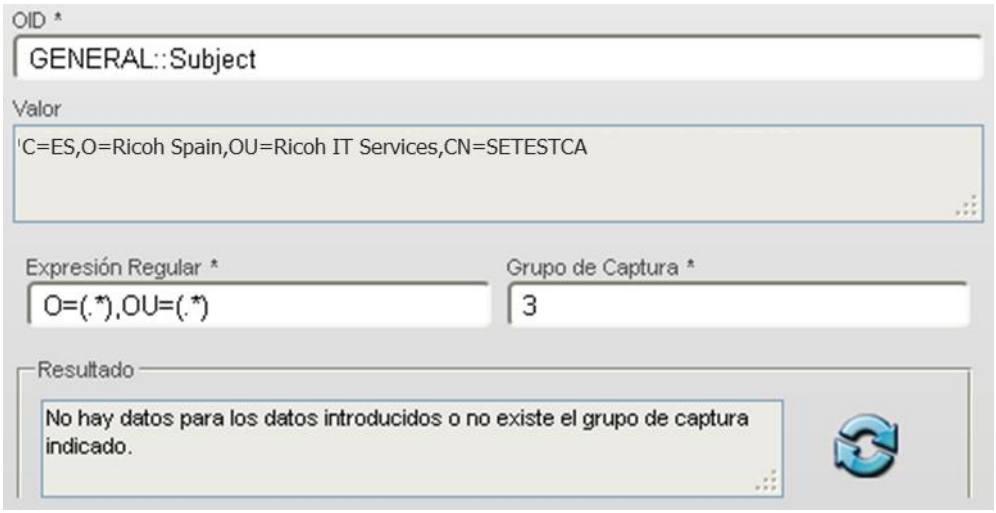
- Grupo de captura 1:



- Grupo de captura 2:



- Grupo de captura 3:


OID *
GENERAL::Subject
Valor
'C=ES,O=Ricoh Spain,OU=Ricoh IT Services,CN=SETESTCA
Expresión Regular *
O=(.*),OU=(.*)
Grupo de Captura *
3
Resultado
No hay datos para los datos introducidos o no existe el grupo de captura indicado.

8 Anexo III. Recomendaciones de uso seguro de la plataforma @Firma 6.4

A continuación, se ofrecen algunas recomendaciones para realizar un uso seguro de la plataforma desde el punto de vista del administrador:

- Mantener una política de contraseñas que evite la repetición de contraseñas.
- Se recomienda usar XAdES-T para la firma de respuestas SOAP de la plataforma. En caso de no estar disponible, realizar XAdES-BES.
- Se deberán firmar todas las respuestas de la plataforma.
- Se debe recomendar a los integradores la validación de las firmas electrónicas frente los datos firmados, no basando la validación solamente en los datos extraídos de la firma electrónica.
- Se recomienda no usar los algoritmos MD2, MD5, SHA1, MD2withRSA, MD5withRSA o SHA1withRSA mantenidos en la plataforma por motivos de compatibilidad hacia atrás.
- El acceso a la herramienta de administración deberá realizarse a través de HTTPS.
- No se debería permitir aplicaciones sin autenticación. El método de validación podrá ser por usuario y contraseña o por certificado, recomendando éste último. Tanto para uno como para otro se deberá especificar los parámetros necesarios para la autenticación.
- Si la aplicación va a permitir la validación de certificados mediante OCSP se impondrá modo estricto de peticiones OCSP.

9 Anexo IV. Tratamiento de datos de carácter personal: LOPD

La recogida de datos de carácter personal para el alta de nuevos usuarios y responsables de aplicación, así como la inclusión de nuevos certificados, susceptibles de contener información de carácter personal en los almacenes de la plataforma, se realizarán únicamente con la finalidad de agilizar los procedimientos o por necesidades de funcionalidad.

Los datos marcados como obligatorios en la gestión de usuarios y aplicaciones, serán imprescindibles para la realización de determinadas tareas en la administración, y a través de su cumplimentación el usuario final muestra su consentimiento para el tratamiento de sus datos, que se realizará de conformidad con lo dispuesto en *Decreto 1720/2007*, sobre protección de datos de carácter personal.

El órgano tramitador de las solicitudes de alta de esta información, y el mismo propietario de la plataforma, estará obligado a guardar secreto respecto a los mismos, así como a guardarlos, adoptando las medidas necesarias para evitar su alteración, pérdida, tratamiento, sustracción o acceso no autorizado.

Del mismo modo, al incluirse datos de carácter personal, se deberá informar a los dueños de los mismos sobre sus derechos de acceso, cancelación, rectificación, oposición y a ser informados previamente en caso de cesión de los datos, mediante solicitud dirigida al órgano gestor de los datos, que en caso de modelo no federados es el Ministerio de Hacienda y Administración Pública.

Sobre la información de carácter personal que puedan contener los distintos tipos de certificados que se den de alta, se ha de tener en cuenta la naturaleza de dicha información y las acciones a seguir en su tratamiento, según lo indicado por el Prestador de Servicios de Certificación, que como emisor de los certificados describa en su Declaración de Prácticas de Certificación y/o Políticas de Certificación.

Existe registrado un fichero automatizado de validación y firma electrónica (BOE 25 de marzo de 2008), correspondiente a la base de datos relacional de @firma5 del Ministerio con nivel de seguridad básico, cuya información de carácter personal se limita a datos de identificación personal: Nombre y apellidos o la razón o denominación social del interesado, el número del documento nacional de identidad o el código de identificación fiscal o cualquier otro equivalente, correo electrónico, certificado para firma electrónica. De tal modo que no se permite añadir información adicional (teléfonos, fax, etc.) en la gestión de usuarios/responsables de aplicaciones sin otro motivo que el de agilizar los futuros procedimientos que se realicen con el propietario de la información.

10 Anexo V. Definición y uso de pseudocódigo en la plataforma.

10.1 Introducción.

Una de las mejoras introducidas en la plataforma a partir de la versión 6 consiste en el uso de pseudocódigo para poder definir operaciones complejas tanto en los campos lógicos como en los discriminadores que poseen los certificados, de ésta manera se incrementa tanto la información que se puede obtener de un certificado a través de los campos lógicos como la capacidad de realizar una discriminación más fina de los certificados.

Se trata de un lenguaje sencillo y a la vez potente, que recoge el conjunto de operaciones necesarias para realizar potentes discriminadores como campos lógicos completos. El lenguaje permite:

- Definir variables.
- Realizar operaciones cuyo valor será asignado a las variables previamente definidas.
- Retornar un valor que será el que posea el campo lógico o el que se usará para aplicarle la operación seleccionada al discriminador.

10.2 Proceso de ejecución del pseudocódigo.

Antes de ejecutar el pseudocódigo, el sistema debe de realizar unos pasos previos para verificar que es correcto, al igual que es analizado de manera previa a ser almacenado en la plataforma, siendo el flujo el siguiente:

- Análisis del pseudocódigo para encontrar errores:
    - ***Léxicos***: En el que se detectarán tokens (palabras) del lenguaje que no son permitidas.
    - ***Sintácticos***: En el que se detectarán la correcta definición de cada una de las instrucciones.
    - ***Semántico***: En este caso se detecta que sean coherente las instrucciones (no se usen variables no definidas, los tipos devueltos por los métodos y pasados por parámetros sean correctos, …).

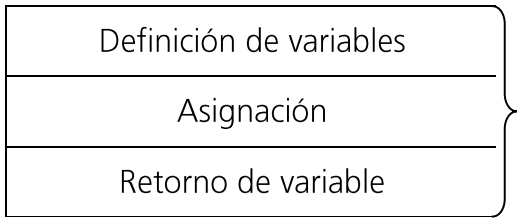
- Traducción del pseudocódigo a código ejecutable por la máquina.
- Ejecución del código traducido.

Durante todo el proceso se pueden lanzar distintas excepciones en función del punto donde se produjo el error (durante el análisis, traducción o ejecución). Un error detectado en alguno de los pasos impide la ejecución del código.

10.3 Estructura del pseudocódigo.

Todo pseudocódigo ha de poseer la siguiente estructura:

- Toda la definición de variables se deberá de realizar al principio.
- A continuación de la definición de las variables se deberán de realizar las asignaciones.
- Por último, se deberá de retornar una variable que contendrá el resultado que se desee devolver.



Pseudocódigo a

NOTA: Toda instrucción deberá terminar en "**;**"

10.3.1 Definición de variables.

El pseudocódigo es capaz de soportar dos tipos de variables:

- Variables de tipo entero (int)
- Variables de tipo cadena (string)

A continuación del tipo de variable deberemos indicar el identificador que poseerá dicha variable. El identificador solamente deberá poseer letras (mayúsculas o minúsculas), números o el carácter "_".

Dado que una vez creado, el pseudocódigo es traducido a código Java, no podrán usarse palabras reservadas de Java para el identificador de una variable. Las palabras reservadas de Java pueden consultarse en https://docs.oracle.com/javase/tutorial/java/nutsandbolts/_keywords.html.

Ejemplos:

- ***string*** a;
- ***int*** numero;
- ***String*** *miCadena;* ⍰ *Incorrecto ya que el tipo empieza en mayúsculas.*
- ***int*** *num_ID;*

10.3.2 Realización de asignaciones.

Una vez definidas las variables, podemos realizar asignaciones de valor sobre éstas. El token que indica que se va a realizar una asignación sobre una variable será "***:=***". En la parte izquierda del token de asignación se indicará el identificador de la variable cuyo valor se desea asignar y a la derecha el valor. Como valor podemos tener:

- Valor constante:
  - Si la variable es de tipo ***string*** el valor será una cadena de texto que podrá contener cualquier carácter y estando encerrada dicha cadena entre comillas dobles.

    a:=**"HOLA"**;
  - Si la variable es de tipo ***int*** el valor solamente podrá ser de tipo numérico

    numero:=**1**;
- OID procedente de un campo de un certificado. En este caso solamente podrá ser asignado a variables de tipo string. El OID deberá de ir encerrado entre llaves "**{OID}**"

  a := **{GENERAL::subject}**;
- Resultado de aplicar una operación. A continuación se describen las distintas operaciones a aplicar.

Nombre Operación	Tipo Argumento1	Tipo Argumento2	Tipo Argumento3	Tipo valor retorno
length	string / OID / variable tipo string	✖	✖	int
not	int / variable tipo int	✖	✖	int

Nombre Operación	Tipo Argumento1	Tipo Argumento2	Tipo Argumento3	Tipo valor retorno
lower	string / OID / variable tipo string	✖	✖	string
upper	string / OID / variable tipo string	✖	✖	string
normalize	OID	✖	✖	string
trim	string / OID / variable tipo string	✖	✖	string
matches	string / OID / variable tipo string	string (Reg. Expr.)	✖	int
contains	string / OID / variable tipo string	string / OID / variable tipo string	✖	int
concat	string / OID / variable tipo string	string / OID / variable tipo string	✖	string
substring	string / OID / variable tipo string	int / variable tipo int	int / variable tipo int	string
split	string / OID / variable tipo string	String (Reg. Expr)	int / variable tipo int	string

- **Función length:** Realiza el cálculo de la longitud de una cadena (en caso de que el parámetro pasado sea una cadena) o del valor que posee un campo (OID) de un certificado. Devuelve un valor entero con el número de caracteres que posee la cadena.

  Ejemplo: length("HOLA") → Devuelve 4

- **Función not:** Realiza la negación de un valor entero, devolviendo otro valor entero. En caso de que el valor sea 0 devuelve 1 en otro caso devuelve 0.

  Ejemplo: not(5). Devuelve 0 → not(0) devuelve 1

- **Función lower:** Convierte a minúsculas una cadena ó el valor que posee un OID. El resultado es otra cadena.

  Ejemplo: lower("HolA") → Devuelve hola

- **Función upper:** Similar a la anterior pero en este caso la transformación es a mayúsculas.

  Ejemplo: upper("HolA") → Devuelve HOLA

- **Función normalize:** Realiza la normalización (siguiendo el estandar RFC2253 de un campo de tipo OID DN (Distinguished Name). En caso de que el campo no sea de tipo DN devuelve el valor de dicho campo sin normalizar. El resultado es de tipo string.

  Ejemplo: Tenemos el certificado cuyo campo OID {GENERAL::Subject} posee el valor:
  "EMAIL=asd@ggg.com,CN=asdasdasd,OU=abcdç,O=Española,L=Cañada,ST=asd,C=SP"

  El resultado de aplicar normalize({GENERAL::Subject}); → "EMAIL=asd@ggg.com,CN=asdasdasd,OU=abcd\C3\A7,O=Espa\C3\B1ola,L=Ca\C3\B1ada,ST=asd,C=SP"

- **Función trim:** Elimina los espacios que aparecen al principio y al final de una cadena dada ó en el valor de un OID dado. El resultado es otra cadena.

  Ejemplo: trim(" HOLA "); → Devuelve "HOLA"

- **Función matches:** Comprueba que una cadena ó el valor de un campo OID cumpla una expresión regular. Devuelve un entero, 0 si no lo cumple ó 1 si lo cumple.

  Ejemplo: matches("HOLA",".*") → Devuelve 1 ya que coincide con la expresión regular

- **Función contains:** Comprueba si una cadena o el valor de un OID (argumento1) contiene a otra cadena u otro valor de campo OID. El resultado es de tipo entero, 0 si no la contiene y 1 si la contiene.

  Ejemplo: contains("HOLA","OHL") → Devuelve 0 ya que no contiene la cadena "HOLA" a la cadena "OHL".

- **Función concat:** Concatena a una cadena/valor de campo OID otra cadena/valor de campo OID. El resultado es de tipo string con la cadena concatenada.

  Ejemplo: concat("HOLA","ADIOS") → Devuelve la cadena HOLAADIOS

- **Función substring:** Obtiene la subcadena procedente de una cadena/valor de campo OID que se encuentra entre dos posiciones dadas.

  Ejemplo: substring("cadena",2,5) → Devuelve "den"

- **Función split:** Parte una cadena/valor de campo OID aplicando una expresión regular y obtiene la parte de la cadena que se indica en el tercer argumento. El resultado es de tipo cadena.

  Por ejemplo: split(“cadena1,cadena2,cadena3”,”,”,0) → Devuelve la cadena “cadena1”

  split(“cadena1,cadena2,cadena3”,”,”,1) → Devuelve la cadena “cadena2”

  split(“cadena1,cadena2,cadena3”,”,”,2) → Devuelve la cadena “cadena3”

NOTA: Está permitido realizar operaciones anidadas, por ejemplo podemos hacer:

length(substring(split(“cadena1,cadena2,cadena3”,”,”,1),2,5)) → Devolviendo 3.

Esto quiere decir que:

La manera de ejecutar esta sentencia sería desde dentro hacia afuera de la siguiente manera:

1. Se realiza la operación: split(“cadena1,cadena2,cadena3”,”,”,1) →Devuelve “cadena2”
2. Se realiza la operación: substring(split(“cadena1,cadena2,cadena3”,”,”,1),2,5) → Devuelve la cadena den, ya que sería lo mismo que aplicar: substring(“cadena2”,2,5)
3. Se realiza la operación: length(substring(split(“cadena1,cadena2,cadena3”,”,”,1),2,5)) → Devuelve 3 que sería lo mismo que realizar length(“den”);

Aunque se permitan anidar operaciones es aconsejable, sobre todo por legibilidad del código realizar las operaciones por separado apoyándonos en variables. En este caso sabemos que la operación length es una operación que devuelve un entero, por lo que la sentencia correcta sería:

```
int longitud;

longitud := length(substring(split(“cadena1,cadena2,cadena3”,”,”,1),2,5));
```

Que sería equivalente a:

```
int longitud;

string subcadena;

string parte;

parte := split(“cadena1,cadena2,cadena3”,”,”,1);
```

```
subcadena := substring(parte,2,5);

longitud := length(subcadena);
```

10.3.3 Retorno de valores.

El pseudocódigo no es más que una función que realiza una acción determinada y devuelve un valor. Solamente está permitido devolver variables (al fin y al cabo las variables poseen valores, si no están inicializadas poseerán el valor cadena vacía para las variables de tipo *string* ó 0 para variables de tipo *int).*

El valor a retornar será de tipo cadena, por lo que aunque se decida retornar un valor de tipo entero, ese valor se pasará a cadena, es decir, si retornamos una variable que posee el valor 3, lo que se retornará será la cadena 3.

La instrucción de retorno será la última instrucción que se colocará en el pseudocódigo siguiendo la siguiente estructura:

RET idVariable;

Aplicando el ejemplo (legible) anterior nos quedaría:

```
int longitud;

string subcadena;

string parte;

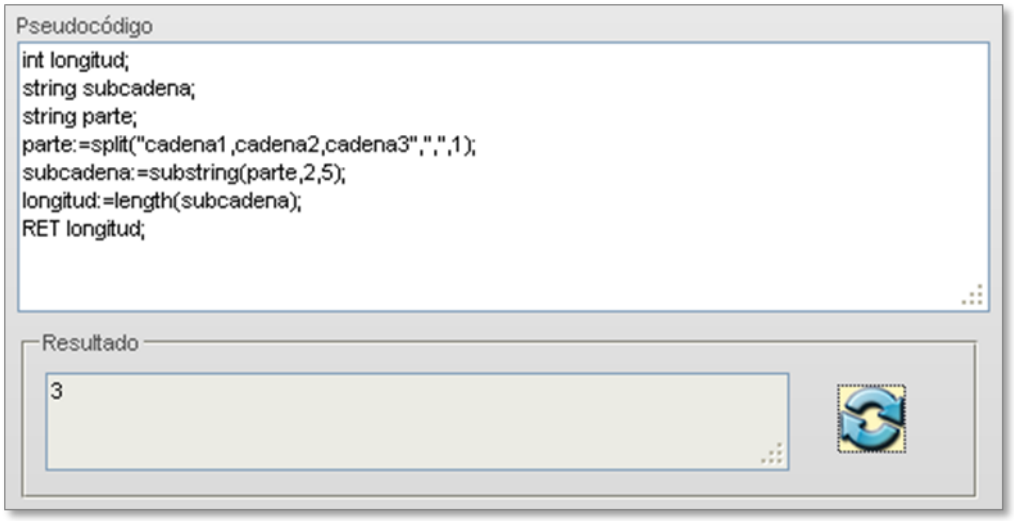
parte := split(“cadena1,cadena2,cadena3”,”,”,1);

subcadena := substring(parte,2,5);

longitud := length(subcadena);

RET parte;
```

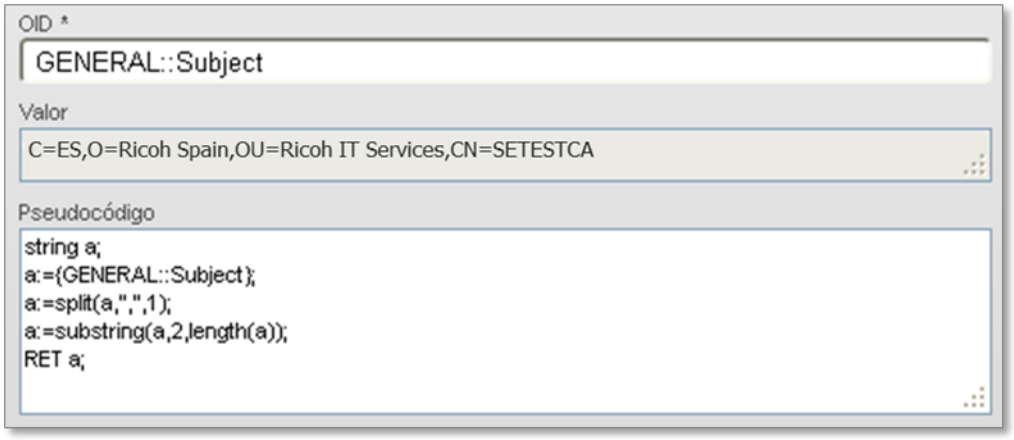
En este caso, tras ejecutar el pseudocódigo obtendremos como resultado la cadena 3.



10.3.4 Ejemplo usando atributos de certificado.

Vamos a definir el campo lógico que posee un certificado como tipo pseudocodigo:

El campo lógico poseerá el siguiente valor:



En este caso hemos usado el campo GENERAL:Subject. Para aplicarlo al pseudocódigo lo hemos seleccionado y copiado del campo OID seleccionado a la asignación de la variable a (a := ….), siempre entre las llaves.

En el campo valor OID (Orientativo) nos sirve para saber que posee el campo.

El siguiente código realiza lo siguiente:

- Se crea una variable (a) de tipo cadena (string)

- Esa variable (a) se carga con el valor del campo OID (GENERAL:Subject), cuyo valor es:

C=ES,O=Ricoh Spain,OU=Ricoh IT Services,CN=SETESTCA

- Acto seguido actualizamos el valor de la variable a (que contiene la cadena anterior) por el resultado de dividir dicha cadena entre "," y quedarnos con el elemento 1 (recuerde: el primer elemento empieza en 0). En este caso la división quedaría:
    - Posición0: ***C=ES***
    - Posición1: ***O=Ricoh Spain***
    - Posición2: ***OU=Ricoh IT Services***
    - Posición3: ***CN=SETESTCA***

    En este caso como se indicó, la variable se actualiza con la posición 1, quedando la variable a con el valor ***O=Ricoh Spain***

- A continuación se obtiene la subcadena de la variable a, comprendida entre la posición 2 y la longitud total de la cadena (length(***O= Ricoh Spain***) = 11), por tanto sería la longitud entre 2 y 11 de la cadena ***O= Ricoh Spain***, actualizándose la variable a al valor ***Ricoh Spain***.

- Por último, se retorna el valor de la variable a, en cuyo caso contendrá la variable ***Ricoh Spain***.

Por tanto, el valor de dicho campo lógico será ***Ricoh Spain***.

11 Anexo VI. Implementación propia de cliente TSA.

Para generar un cliente TSA propio, basta con generar una clase que implemente la interfaz:

es.gob.afirma.tsa.ITSAServices

Esta interfaz se encuentra declarada dentro de la librería que representa el core de la plataforma. Esta librería se encuentra dentro del CD de Instalación en la siguiente ruta:

CDInst/Instalacion/resources/1.7/ear/originalsToModify/ear/earBasicContent/afirma6-core.jar

IMPORTANTE: Para la nueva clase generada (o clases), si resultara necesario hacer uso de librerías de apoyo para su desarrollo, como por ejemplo las correspondientes al proveedor criptográfico IAIK, se debe hacer uso exactamente de la misma versión de la librería que ya exista dentro del desplegable (.ear) de @firma. Se puede obtener un listado completo de las librerías embebidas en el desplegable de @firma dentro del CD de Instalación en la siguiente ruta:

CDInst/Instalacion/resources/1.7/ear/originalsToModify/ear/earBasicContent/lib/.jar*

Así, de este modo, siguiendo el ejemplo anterior de IAIK, se debe usar (en caso que fuera necesario) las siguientes: “iaik_jce-5.2.4.jar” y “iaik_tsp-2.1.jar”.

En el caso en el que la librería usada no existiera actualmente dentro del desplegable de @firma, se puede usar sin ningún problema.

Es responsabilidad del desarrollador de esta implementación específica de un cliente TSA, seleccionar las librerías adecuadas.

Una vez realizada la implementación, se debe construir una librería (.jar) que incluya la clase (o clases) que la definen, e insertar en la ruta “lib/*.jar” dentro del desplegable de @firma situado en:

JBOSS_HOME/standalone/deployments/afirma6-ear.ear[lib/.jar]*

tanto la librería generada, como sus dependencias (otras librerías de apoyo utilizadas) que no estén ya incluidas.

Este cambio hay que realizarlo sobre todas las instancias del clúster, y por cada una de estas, para poder realizar esta modificación, primero hay que detener el servidor y luego volverlo a iniciar, por lo que se tiene que tener en cuenta las distintas necesidades de sistemas como por ejemplo sacar la instancia del balanceador previamente para volverla a incluir a posteriori, pérdida de servicio o capacidad de servicio momentánea… etc.

Una vez modificado el desplegable de @firma, y que las instancias hayan iniciado correctamente (revisión de los logs), ya se puede proceder mediante la administración de la plataforma, a hacer uso de la clase de implementación generada (apartado 5.3.11.1 -Gestión de TSA – Datos Generales).