



RAEDICOM Autoridad de registro de EDICOM  
Manual de Usuario

Título del documento:	Registration Authority EDICOM
Nombre del fichero:	ES RAEDICOM Manual Usuario.odt
Versión:	2.0
Estado:	VIGENTE
Fecha:	04/02/2011
Autor:	Oscar Albert Arcas

**Revisión, Aprobación**

Revisado por:	Francisco Belda Escamilla	Fecha: 28/02/2011
Aprobado por:	Oscar Albert Arcas	Fecha: 28/02/2011

**Historial de cambios**

Versión	Fecha	Descripción de la acción	Páginas
1.0	22/09/2010	Versión inicial de la aplicación	Todas
2.0	04/02/2011	Se añaden descripciones de nuevas funcionalidades.	
2.1	27/05/2013	Se añade referencia a la generación de certificados software en base a URL	3, 22, 28, 29

# Índice de Contenido

## RAEDICOM. EDICOM Registration Authority

1.1 Introducción.....	4
1.2 Acceso a RAedicom.....	4
1.3 Términos.....	5
<b>2 -Interfaz Web</b>	
2.1 Introducción.....	7
2.2 Menú principal de la Aplicación.....	8
2.3 Nodos Principales de la aplicación.....	8
2.4 Área principal de la aplicación.....	9
<b>3 -Opciones sobre Entidades/Certificados</b>	
3.1 Introducción.....	12
3.2 Filtro de búsqueda.....	12
<b>4 -Proceso de Alta y Validación de una Entidad</b>	
4.1 Introducción.....	14
4.2 Alta de nueva entidad.....	14
4.3 Proceso de Validación.....	18
4.4 Cancelar una Entidad.....	19
4.5 Proceso de Revocación.....	19
4.6 Gráfico de estados de una entidad/certificado.....	20
<b>5 -Proceso de generación de Certificados</b>	
5.1 Introducción.....	21
5.2 Certificados de navegador WEB.....	21
5.3 Certificados de Servidor.....	25
5.4 Generación múltiple (PKCS12).....	26
5.5 Certificados desde la parte pública.....	26
<b>6 -Gestión de Usuarios</b>	
6.1 Introducción.....	28
6.2 Opciones del gestor de usuario.....	29
<b>7 -Gestión de Clientes</b>	
7.1 Introducción.....	33
7.2 Opciones del gestor de paquetes de licencias.....	35
<b>8 -Estadísticas</b>	
8.1 Introducción.....	37
<b>9 -Utilidades</b>	
9.1 Carga masiva de entidades.....	39
9.2 Descarga de certificados pendientes.....	40
<b>10 -Navegadores y generación de claves.</b>	
10.1 Mozilla Firefox 3.....	41
10.2 Microsoft Internet Explorer.....	42

# RAEDICOM. EDICOM REGISTRATION AUTHORITY

## 1.1 INTRODUCCIÓN

---

**RAEDICOM** es la autoridad de registro de certificados de ACEDICOM la autoridad de certificación de EDICOM.

RAEDICOM es el servicio web que permite suscribir una solicitud de emisión de certificado vía Internet. Así como supervisar el proceso de validación y el estado de un certificado.

RAEDICOM permite a los usuarios habilitados, y según el rol asignado a cada usuario, a:

- Dar de alta de nuevas entidades asociadas a solicitudes de emisión de certificados.
- Cargar archivos digitalizados asociados a dichas entidades.
- La confirmación y aprobación de solicitudes de emisión de certificados.
- Validación de la identidad y autoridad del solicitante para la generación final del certificado.
- Revocación de certificados activos.

## 1.2 ACCESO A RAEDICOM

---

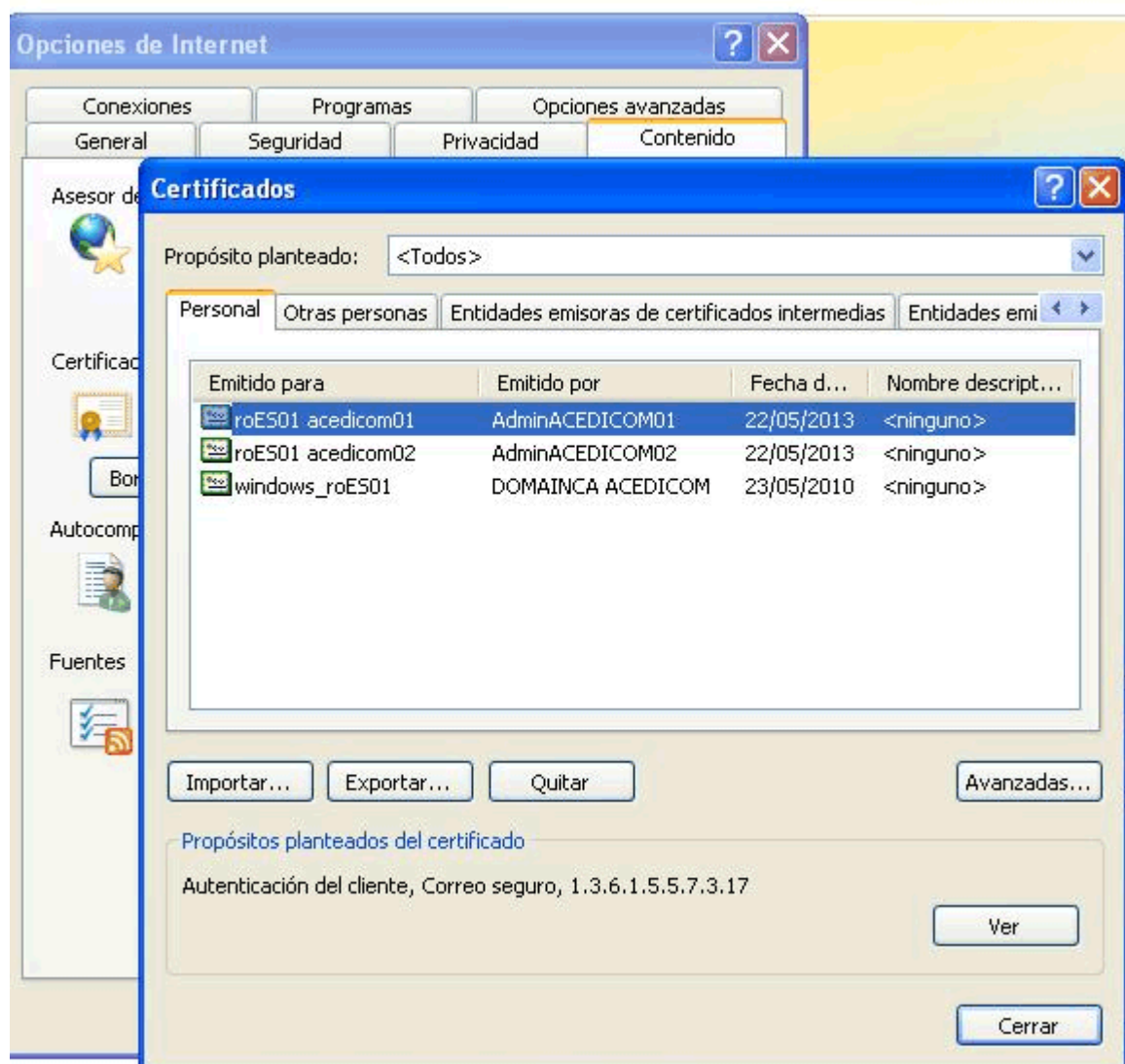
### Autenticación con Smart-Card

El acceso a la autoridad de registro de Edicom se realiza a través de la aplicación web RAEDICOM, ya sea directamente por internet desde el ordenador del operador de registro o a través de un escritorio remoto vía Terminal Server.

En cualquier caso el operador de registro que desee acceder a RAEDICOM debe estar en posesión de una Smart-Card proporcionada por EDICOM con los certificados autorizados para acceder al servicio de registro. La autenticación se realiza por validación directa de número de certificado alojado en la Smart-Card. (Para entrar en RAEDICOM no hay usuario ni contraseña).

Con los Drivers de la Smart-card correctamente instalados, al conectar la misma al equipo, el registrador podrá comprobar que dispone en el navegador de tres certificados personales nuevos.

- Dos de ellos, los correspondientes a "acedicom01" y "acedicom02" se utilizan para acceder al servicio RAEDICOM vía Internet.
- El tercero, correspondiente a "windows" se utiliza para validarse durante el acceso al servicio vía Terminal Server. (Necesario para la generación de certificados sobre dispositivo seguro centralizado).



Una vez seleccionado el certificado, para poder hacer uso de las claves asociadas, el Driver de la Smart Card pedirá el PIN del dispositivo.

**Nota:** Cada Smart-Card esta asociado en RAEDICOM a un usuario distinto y su rol correspondiente. Que debe estar dado de alta en la sección Usuarios antes de la primera entrada.

## 1.3 TÉRMINOS

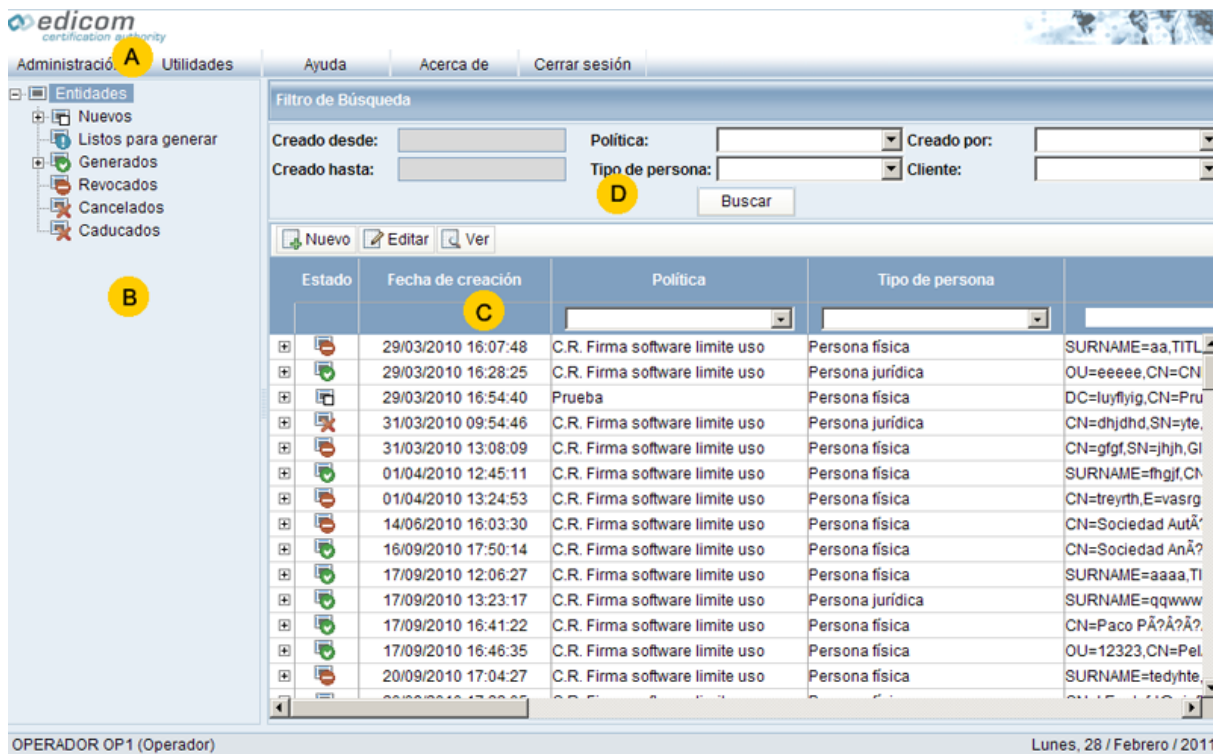
- **Entidad.** Hace referencia al conjunto de información personal y legal que identifica al futuro dueño del certificado (Cliente), así como la política de certificación que indica qué tipo de certificado es y para qué uso va a expedirse. La creación de una nueva entidad implica automáticamente la aparición de una nueva solicitud de emisión de certificado y el inicio de su proceso de validación. Mientras que la cancelación o revocación de una entidad es al mismo tiempo la cancelación o revocación del certificado correspondiente.

- **Certificado.** Hace referencia en distintos contextos al archivo físico o par de claves generadas para ser utilizado como certificado electrónico digital.
- **Operador/Usuario.** Hace referencia al usuario de la aplicación. Los usuarios disponen de distintas opciones según los roles asociados a dicho usuario. Para acceder a la aplicación el usuario debe estar dado de alta primero.
- **Cliente.** El cliente es la persona física o empresa para la cuál se genera una entidad y se expiden certificados. Durante el proceso de generación de una entidad se debe seleccionar un cliente de los ya creados o crear uno desde cero.
- **Perfiles.** El perfil está directamente relacionado con las políticas de certificación habilitadas por la Autoridad de Certificación de Edicom y las especificaciones para generar certificados bajo estas distintas Políticas.

## 2 - INTERFAZ WEB

### 2.1 INTRODUCCIÓN

La interfaz del panel principal de RAEDICOM se divide en varias zonas diferenciadas



- **Menú principal (A).** Dispuesto en la parte superior de la pantalla, contiene los menús asociados a las distintas opciones generales de administración y herramientas de la aplicación.
- **Árbol de estados de las entidades (B).** Dispuesto a la izquierda, donde se reflejan todos los posibles estados que atraviesa una entidad/certificado desde su propuesta de emisión hasta el término de su validez. Para más información ver [4.6. Gráfico de estados de una entidad/certificado](#).
- **Listado principal de entidades (C).** Dispuesto a la derecha, forma el cuerpo principal del panel de control. En este listado se muestran únicamente las entidades asociadas al usuario y desde él se puede acceder a la información de cada entidad así como gestionar la creación de nuevas entidades y certificados, (si el usuario está habilitado para ello). Para más información sobre el alta de nuevas entidades ver [4. Proceso de Alta y Validación de una Entidad](#)
- **Filtro de Búsqueda.** Dispuesto sobre las columnas del grid, permite ocultar las entidades que no correspondan con los parámetros de búsqueda. También sobre las columnas del listado principal existen listas de selección que permiten hacer filtros rápidos sobre los datos de las entidades mostradas.

## 2.2 MENÚ PRINCIPAL DE LA APLICACIÓN

El menú principal está situado en la parte superior de la pantalla. Las opciones del menú principal son:





- Menú principal **Administración**. Contiene las opciones de acceso a los paneles de control de **Usuarios, Perfiles, Clientes, Estadísticas y Configuración**. Estas opciones solo están disponibles para los Operadores autorizados.
- Menú principal **Utilidades**. Contiene las opciones de **Carga masiva de entidades y descarga de certificados pendientes**. Estas opciones solo están disponibles para los Operadores autorizados.
- Botón **Ayuda**. Permite acceder a la documentación de ayuda.
- Botón **Acerca de**. Permite acceder a la información de versión y copyright de la aplicación.
- Botón **Cerrar sesión**. Permite cerrar la sesión de usuario.

## 2.3 NODOS PRINCIPALES DE LA APLICACIÓN

El árbol de estados de las Entidades muestra todos los certificados/entidades que de alguna manera están asociados con el operador/usuario de la sesión. Podemos distinguir dos niveles distintos.

- **Estados principales de las entidades**. Son los estados que atraviesan las entidades en cada momento.
- **Estado de las entidades respecto del operador/usuario actual**. Son los estados relativos al usuario. Dependiendo de su intervención en el proceso de validación o revocación. Por ejemplo si el usuario ha dado su voto positivo la entidad aparecerá dentro del sub-nodo **Nuevos-Validados** (Validado por él), Mientras que si no ha dado su voto positivo, aparecerá en el subnodo **Nuevos-Pendientes de validar** (pendiente de validar por él).

### DESCRIPCIÓN ESTADOS

	<b>Nuevos.</b> Nuevas entidades pendientes de validar. El número de validaciones recibidas no iguala al número de validaciones necesarias para pasar la entidad y su certificado al estado <i>Listos para generar</i> .
	<b>Listos para generar.</b> Entidades que han concluido el proceso de validación . A partir de esta situación un operador habilitado puede generar el certificado correspondiente que inmediatamente pasa a <i>Generados</i> .
	<b>Generados.</b> Certificados generados a partir de una entidad validada y ya en uso.
	<b>Revocados.</b> Certificados revocados. Significa que la entidad correspondiente ha sido revocada y el certificado ha dejado de estar activo. La revocación puede producirse por un proceso de revocación o bien cuando el certificado supera el tiempo de vigencia para el que fue expedido.



	<b>Cancelados.</b> Entidades canceladas por el operador autorizado antes de que se generara el certificado correspondiente.
	<b>Caducados.</b> Certificados cuya fecha de caducidad ha sido superada en la actualidad.

## 2.4 ÁREA PRINCIPAL DE LA APLICACIÓN

En el listado principal aparecen las entidades cuya solicitud de emisión corresponde con el estado seleccionado en el árbol de nodos. Si se selecciona el nodo principal **Entidades** aparecen todas las entidades aunque puede identificarse el estado.

Nuevo

Editar

Ver

	Estado	Fecha de creación	Política	Tipo de persona	SubjectDN	Número de validaciones	Número rechaz
<input type="checkbox"/>		29/03/2010 16:07	C.R. Firma software limite uso	Persona física	SURNAME=aa,TITL	2/2	2/2
Revocado por			Fecha de revocación	Motivo de			
OPERADOR OP1			29/03/2010 16:19				
OPERADOR OP2			29/03/2010 16:20				
<input type="checkbox"/>		29/03/2010 16:28	C.R. Firma software limite uso	Persona jurídica	OU=eeeeee,CN=CN	2/2	0/2
<input type="checkbox"/>		29/03/2010 16:54	Prueba	Persona física	DC=luyflyig,CN=kujf	2/2	0/2
<input type="checkbox"/>		31/03/2010 09:54	C.R. Firma software limite uso	Persona jurídica	CN=dhjdhd,SN=yte,	1/2	0/2
<input type="checkbox"/>		31/03/2010 13:08	C.R. Firma software limite uso	Persona física	CN=gfgf,SN=jhjh,GI	2/2	0/2
<input type="checkbox"/>		01/04/2010 12:45	C.R. Firma software limite uso	Persona física	SURNAME=fhgjf,CN	1/2	1/2

**Nota:** la captura corresponde al nodo principal Entidades, donde aparecen todas las entidades independientemente de su estado.

Cada certificado se representa en forma de una línea seleccionable con información dividida en forma de columnas. Dentro de cada línea se puede desplegar una lista con la información de los usuarios asociados al proceso de validación/revocación del certificado.

### DESCRIPCIÓN DE LAS COLUMNAS

- **Estado.** Refleja con un icono el estado del certificado correspondiente.
- **Fecha de creación.** Fecha de creación de la entidad.
- **Política.** Política de certificación seleccionada en la entidad.
- **Tipo de persona.** Tipo de persona seleccionada para la entidad.
- **SubjectDN.** Resumen codificado de los atributos del certificado, atributos que deben estar presentes en el certificado de firma para que sea un certificado valido según la política de certificación seleccionada.
- **Número de validaciones.** Indica el número de validaciones conseguidas y el número total de validaciones necesarias para que el certificado pase de *Nuevo* a *Listo para generar*. Por ejemplo 1/3 significa que el certificado tiene una validación de tres necesarias.

- **Número de rechazos.** Indica el número de rechazos adjudicados y el número total de rechazos necesarios para que el certificado sea revocado. Con un solo rechazo adjudicado el certificado ya estaría en situación Pendientes de rechazo. (Aunque seguiría siendo valido hasta ser completamente rechazado)
- **Creado por.** Indica el usuario que ha creado la entidad.
- **Fecha de creación del certificado.** Indica la fecha de generación del certificado, fecha que marca el paso de *Listos para generar* a *Generado*.
- **Número de serie.** Indica el número de serie del certificado. Solo cuando el certificado ha sido generado se le aplica un número de serie.
- **Email.** Indica el email asociado al usuario del certificado, indicado en los datos de la entidad.
- **Cliente.** Indica el cliente al que se le ha asignado la entidad.
- **Fecha de caducidad.** Indica la fecha de caducidad de los certificados generados.
- **Tipo de generación.** Indica la forma en que se ha generado el certificado.





Si se despliega la información anidada dentro de cada línea se puede acceder a un registro de los usuarios implicado en el proceso de validación / revocación de la entidad. Solo aparecen los operadores que han suscrito su voto.



- **Validado por/ Revocado por.** Indica qué usuario ha dado su validación o revocación.
- **Fecha de validación/revocación.** Indica en qué fecha el operador dio su validación o revocación.
- **Motivo de revocación.** Indica el motivo por el cuál el usuario ha revocado el certificado.

## ICONOS ASOCIADOS A LAS ENTIDADES

### Iconos columna estado

Los iconos asociados a las entidades corresponden normalmente con el nodo de estado seleccionado.

	<b>Nuevo.</b> identifica a las entidades
	<b>Listo para generar.</b> Identifica entidades que han concluido el proceso de validación. A partir de esta entidad el operador autorizado puede generar un certificado con las opciones del menú contextual.
	<b>Generado.</b> Indica que sobre esta entidad ya hay un certificado generado y activo.
	<b>Revocado.</b> Indica que la entidad ha sido Revocada. Por tanto los certificados generados sobre ella también lo han sido.

	<b>Cancelado.</b> Indica que la entidad ha sido cancelada.
	<b>Caducado.</b> Indica que el certificado ha caducado.

## 3 - OPCIONES SOBRE ENTIDADES/CERTIFICADOS

### 3.1 INTRODUCCIÓN





Estas opciones afectan al elemento o elementos seleccionados en el listado principal. Aparecen al hacer clic con el botón derecho del ratón. Y los más utilizados también están disponibles en la barra de herramientas del Grid principal. Algunas de estas opciones pueden no estar disponibles según el nodo o entidad seleccionado.

Para realizar alguna acción sobre una entidad, primero se debe seleccionar y luego, pulsar la opción correspondiente de la barra de herramientas o del menú contextual

- Teniendo seleccionado una entidad, pulsar la tecla Shift y pulsar con el botón izquierdo del ratón otro documento del panel. De esta forma se seleccionan los documentos entre el primer documento seleccionado y el documento seleccionado con el botón izquierdo del ratón.
- Teniendo pulsada la tecla Ctrl, se puede seleccionar varias entidades pulsando con el botón izquierdo del ratón.

### MENÚ CONTEXTUAL Y BARRA DE HERRAMIENTAS

Las siguientes opciones están disponibles en la barra superior del listado principal y en el menú contextual cuando se hace clic con el botón derecho sobre el listado. En la mayoría de los casos afectan al certificado seleccionado en el listado.

	<b>Nuevo.</b> Permite dar de alta una nueva entidad, implica el inicio de una solicitud de certificado. Ver <a href="#">Proceso de Alta y Validación de un certificado</a> .
	<b>Editar.</b> Permite editar la entidad seleccionada mientras la entidad continúe dentro del proceso de validación. Es importante recordar que si se edita una entidad durante este estado todas las validaciones hasta el momento se cancelarán y volverá a iniciarse el proceso de validación. Ver <a href="#">Proceso de Alta y Validación de un certificado</a> .
	<b>Ver.</b> Permite ver los datos de una entidad en modo solo lectura.
	<b>Cambiar estado.</b> Permite cambiar de estado el certificado seleccionado en cada momento, incluyendo la posibilidad de que el usuario Valide o Revoque un certificado. Las opciones disponibles en este menú varían según el estado del certificado, siguiendo la lógica explicada en el punto <a href="#">3.5.Estados de una Entidad/Solicitud de Emisión</a> .
	<b>Ver certificado.</b> Permite ver la información del certificado, Siempre y cuando la entidad seleccionada tenga asociado un certificado ya generado.

### 3.2 FILTRO DE BÚSQUEDA

El área superior del listado de certificados es un formulario que permite parametrizar criterios de filtrado en el listado principal.

- **Creado desde.** Permite seleccionar la fecha de creación como parámetro de búsqueda.
- **Política.** Permite seleccionar la política de certificación como parámetro de búsqueda.
- **Creado por.** Permite seleccionar el usuario que generó la entidad como parámetro de búsqueda.
- **Creado hasta.** Permite seleccionar la fecha final de creación como parámetro de búsqueda.
- **Tipo de persona.** Permite seleccionar el tipo de persona asociado a los datos de la entidad (físico o jurídico) como parámetro de búsqueda.
- **Cliente.** Permite seleccionar el cliente al que se le ha asociado la entidad.

Solo aparecerán en el listado los certificados que cumplan con dichos parámetros. El resto estará oculto, pero podrán verse de nuevo cancelando el filtro activo.

Una vez establecidos los parámetros de búsqueda, apretar el botón **Buscar**.

## FILTROS DE COLUMNA

Además del filtro generales del listado principal, Se pueden utilizar filtros a nivel de columna. Un cuadro de texto o una lista seleccionable encima de cada columna permiten reducir aun más el ámbito de la búsqueda. Por otro lado haciendo clic sobre el nombre de una columna en concreto se organizan las entidades según ese valor.

## 4 - PROCESO DE ALTA Y VALIDACIÓN DE UNA ENTIDAD

### 4.1 INTRODUCCIÓN

---

Cuando en este manual se hace referencia a **Entidad**, se hace referencia al conjunto de información personal y legal que identifica al futuro dueño del certificado, así como la política de certificación que indica qué tipo de certificado es y para qué uso va a expedirse.



La creación de una nueva entidad implica automáticamente la aparición de una nueva solicitud de emisión de certificado y el inicio de su proceso de validación. Mientras que la cancelación o revocación de una entidad es al mismo tiempo la cancelación o revocación del certificado correspondiente.

### 4.2 ALTA DE NUEVA ENTIDAD

---

**Importante:** Solo los usuarios operadores de Registro con el rol **Crear entidades** asignado, pueden crear nuevas entidades.

Para crear una nueva entidad:

- Barra de herramientas: Opción  **Nuevo**.
- Menú contextual: botón  **Nuevo**.

Se accede así al formulario de datos de la entidad final (End Entity) que aparece parcialmente vacío.

**Autoridad de Registro ACEDICOM - Datos d Entity**

**End Entity**

\* **Política:** C.R. Firma software limite uso

\* **Tipo de persona:** Persona física

\* **Email:**

\* **Cliente:** Prueba 2 (11111112B) + Añadir Buscar

**Datos del usuario**

**Apellidos:**

**Título:**

**Unidad organizativa:**

\* **Nombre comun para la persona fisica:**

\* **Número de serie:**

\* **Nombre:**

\* **País:**

\* **Calificador DN:**

**Documentación del cliente**

Nuevo Borrar Descargar Actualizar


Nombre	Fecha de inserción	Usuario	Descripción
--------	--------------------	---------	-------------

Aceptar Cancelar

La aplicación todavía no puede indicar que datos son necesarios, ya que la lista de datos depende directamente de la política de certificación y del tipo de persona. Por eso es necesario seleccionar primero estos dos valores.

- **Política.** Permite seleccionar el perfil correspondiente a la política de certificación o tipo de certificado que se va a expedir. ACEDICOM puede emitir certificados bajo las siguientes políticas :
  - **Política de Certificados TLS para cliente y servidor.**
  - **Política de certificación para Certificados Reconocidos de firma sobre dispositivo seguro centralizado para factura electrónica y almacenamiento certificado.**
  - **Política de certificación para Certificados Reconocidos de firma sobre dispositivo seguro centralizado (con limitación de uso).**

- **Política de certificación para Certificado Reconocido de firma sobre dispositivo seguro "Smart Card" (con limitación de uso).**
- **Política de certificación para Certificado reconocido de firma con limitación de uso sobre soporte Software.**
- **Tipo de persona.** Permite seleccionar si se trata de una Persona física o una Persona jurídica. Los datos necesarios para cada política varían según el tipo de persona seleccionada.

**Importante:** Estos parámetros (los dos primeros) indican al formulario el resto de datos requeridos que aparecen automáticamente en pantalla. Los datos necesarios para cada tipo de política son distintos y se recomienda revisar la información contextual de la pantalla que hay junto a cada campo, a través del icono , para saber como se deben completar.

Además es obligatorio rellenar los campos **Email** y **Cliente**.

- **Email.** Permite indicar una cuenta de correo valida asociada a la entidad. Este campo es obligatorio por que permite a la ACEDICOM comunicarle al cliente las notificaciones necesarias para la gestión de sus certificados.
- **Cliente.** Permite indicar el cliente al que se le asignará la entidad y el nuevo certificado. Automáticamente se asignará el cliente por defecto asociado al usuario, pero puede cambiarse este valor por otro de los disponibles o crear uno nuevo desde esta pantalla, utilizando los botones asociados al campo.
  - Botón **Añadir.** Lanza desde esta pantalla el formulario de creación de clientes. Para más información ver creación de clientes.
  - Botón **Buscar.** Lanza desde esta pantalla el listado de clientes. Se puede seleccionar cualquiera de los disponibles.

Una vez terminada la introducción de los datos correspondientes a la Entidad aparecerá en el panel principal, asignado al estado *Nuevos* y se inicia automáticamente el proceso de validación con un voto, el correspondiente al operador que ha generado la entidad.

## AÑADIR DOCUMENTACIÓN DE UNA ENTIDAD

**Atención:** Solo los operadores con rol correspondiente a "**Subir documentación del cliente**", "**Borrar documentación del cliente**", "**Descargar documentación del cliente**" pueden realizar acciones relacionadas con la documentación de una entidad.

Además de la información asociada a la política y tipo de persona correspondiente a la entidad, Para validar una entidad puede ser necesaria la aportación de documentación adicionales. Por ejemplo una imagen del documento nacional de identidad del cliente para corroborar la veracidad de los datos.



RAEDICOM, a través del panel de edición de la entidad, permite adjuntar archivos en formato digital correspondientes a cualquier documento requerido por la política de certificación o por la propia ACEDICOM.

Según los permisos del usuario y el estado en que está la entidad las opciones asociadas a los archivos de documentación pueden variar.

- Si la entidad está en estado *Nuevo* todavía pueden editarse los archivos adjuntos (Opción **Nuevo**, Opción **Borrar**) siempre y cuando el usuario cuente con los permisos correspondientes.
- Si la entidad está ya en estado *Generado* la documentación anexa no se puede editar.

## AÑADIR NUEVA DOCUMENTACIÓN

Para añadir nueva documentación, desde la sección de documentación del panel de edición de entidades.

- Barra de herramientas: Opción **Nuevo**

Se accede así a un formulario de búsqueda de la información a adjuntar. Paralelamente a la selección del documento a importar se debe incluir una *Descripción* del mismo que se reflejará junto al usuario que lo adjunto y a la fecha en que lo hizo. Para que el proceso se complete se debe apretar el botón **Aceptar**.

## BORRAR DOCUMENTACIÓN

Para borrar documentos adjuntos a una entidad, se debe seleccionar el documento a borrar y desde el panel:


- Barra de herramientas: Opción **Borrar**.

## DESCARGAR DOCUMENTACIÓN

Para acceder a la documentación correspondiente y previsualizarla en pantalla, se debe seleccionar el archivo a visualizar y desde:

- Barra de herramientas: Opción  **Descargar**.

## ACTUALIZAR DOCUMENTACIÓN














Para refrescar la documentación de la entidad en pantalla, se debe pulsar el botón  **Actualizar** desde la barra de herramientas.

***Nota:** Si algunas de estas opciones no están disponibles. Puede deberse a que el usuario actual no tiene asignado los roles correspondientes o bien que la entidad se encuentre en un estado donde no es posible ejecutar estas funciones.*

## 4.3 PROCESO DE VALIDACIÓN

Cuando se da de alta una entidad en la RAEDICOM automáticamente se crea una solicitud de emisión de certificado comienza el proceso de validación.


Durante este proceso el operador de registro y los distintos operadores con permisos para validar una entidad se aseguran de la autenticidad de los datos asociados al solicitante y que la solicitud del certificado cumple con todos los requisitos indicados en la política de certificación para el certificado correspondiente.



	Estado	Fecha de creación	Política	Tipo de
+		17/09/2010 12:06	C.R. Firma software, limite uso	Persona física
+		17/09/2010 16:41	 Nuevo	Persona física
+		20/09/2010 17:04	 Editar	Persona física
+		20/09/2010 17:22	 Ver	Persona física
+		20/09/2010 17:23	 Cambiar estado	Persona física
+		20/09/2010 17:28	 Validar	Persona física
+		20/09/2010 17:47	Prueba  Cancelar	Persona física

El proceso de validación implica la obtención de un determinado **número de validaciones** otorgados por los distintos operadores implicados. El número de validaciones depende de la política del certificado. Un operador suscribe su validación con la opción del menú contextual:

- Menú contextual  **Cambio de estado**: Opción  **Validar**.

De ese modo la entidad pasa a tener un voto más y para el usuario que acaba de votar la entidad pasa de *Nuevos – Pendientes de validar* a *Nuevos – Validados*. Si este era el último voto requerido pasará a *Listos para generar*.

Estos son los estados que atraviesa una entidad respecto del usuario actual según su implicación en el proceso de Validación, Estos estados se visualizan al desplegar el nodo principal  **Nuevos** del Árbol de estados de los certificados.

	<b>Nuevos – Pendientes de validar.</b> Aparecen aquí las entidades de nueva creación que el usuario todavía no ha validado.
	<b>Nuevos – Validados.</b> Aparecen aquí los certificados que han recibido la validación del usuario.

*Nota: cuando todos los usuarios han validado la entidad, pasa automáticamente a "Listos para generar".*

## 4.4 CANCELAR UNA ENTIDAD

Si los datos de la solicitud o la identidad del suscriptor no fuesen correctas, el operador autorizado puede desestimar la petición de emisión indicando los motivos por los cuales la petición no puede ser procesada para que el suscriptor vuelva, si lo desea, a crear una nueva petición.

Un operador autorizado puede **Cancelar** una petición mientras no ha pasado el trámite de validación (en estado *Nuevo* o *Pendiente de generar*). Un operador indica su decisión de cancelar con la opción del menú contextual:

- Menú contextual  **Cambio de estado:** Opción  **Cancelar.**

De ese modo la entidad pasa al estado irreversible *Cancelado*. El proceso de cancelación no debe someterse a votación.

## 4.5 PROCESO DE REVOCACIÓN




Una vez un certificado ha sido generado pasa a estar *Activo* y su dueño puede comenzar a utilizarlo para los usos indicados en su política de certificación y según el proceso correspondiente al soporte del certificado.

Estando activo, un certificado puede ser revocado en cualquier momento posterior a su generación siguiendo un proceso de votos similar a la validación. El proceso de Revocación puede iniciarse por cualquier operador autorizado para ello a través de la opción:

- Menú contextual  **Cambio de estado:** opción  **Revocar.**

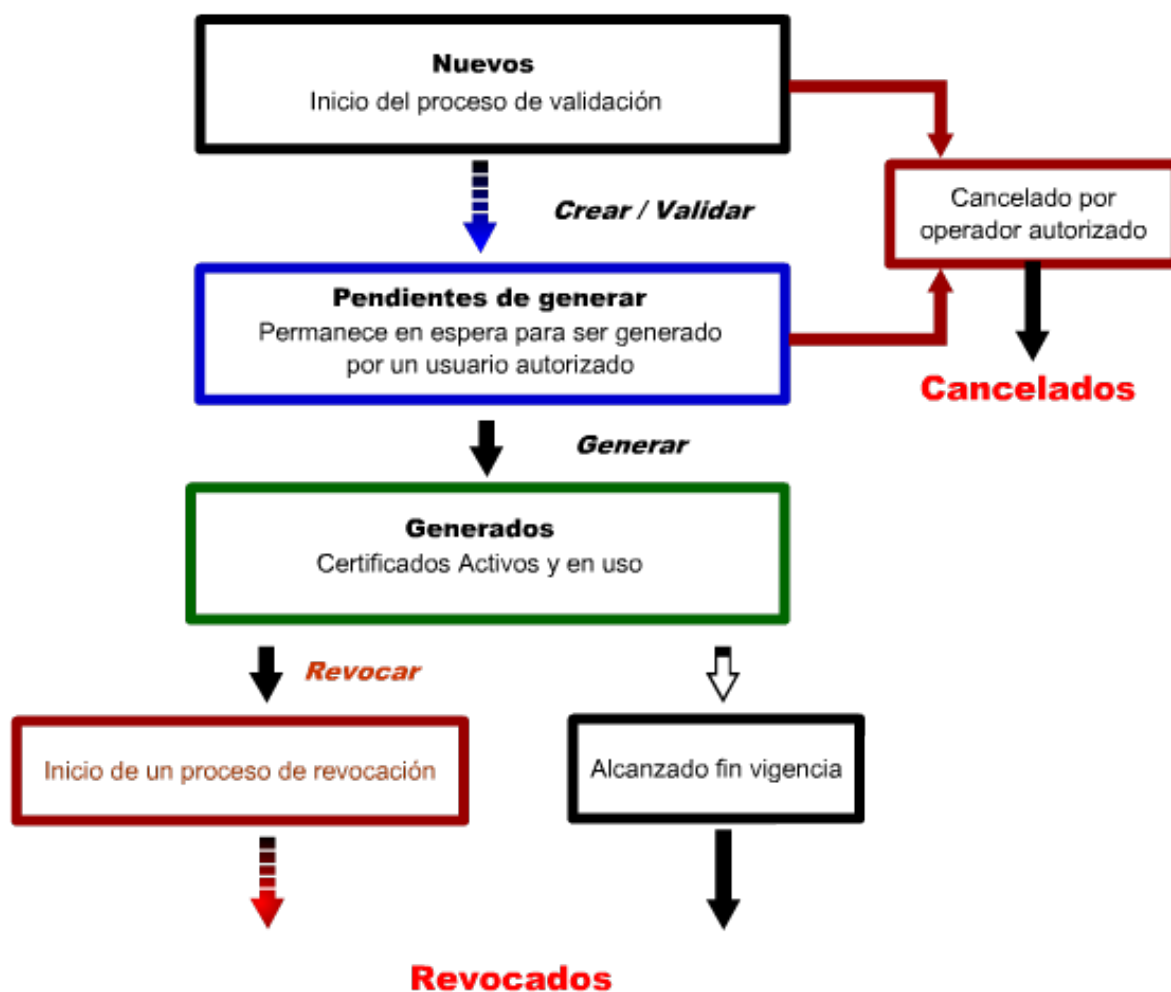
Como el proceso de validación, el de revocación implica alcanzar un determinado número de revocaciones. El certificado que ha comenzado un proceso de Revocación sigue estando activo hasta que el proceso de revocación ha sido completado en su totalidad con todos los votos necesarios. Una vez finalizada la revocación la entidad pasa a *Revocados*.

Estos son los estados que atraviesa un Certificado/Entidad respecto del usuario actual según su implicación en el proceso de revocación.

	<b>Generados – Activos.</b> Aparecen aquí los certificados generados para los cuales nadie ha iniciado un proceso de revocación.
	<b>Generados – Pendientes de revocar.</b> Aparecen aquí los certificados para los cuales algún operador distinto del usuario actual ha iniciado un proceso de revocación.
	<b>Generados – Revocados.</b> Aparecen aquí los certificados que han recibido la revocación del usuario actual.

*Nota: para suscribir un voto de revocación es obligatorio añadir un **motivo de revocación**.*

## 4.6 GRÁFICO DE ESTADOS DE UNA ENTIDAD/CERTIFICADO




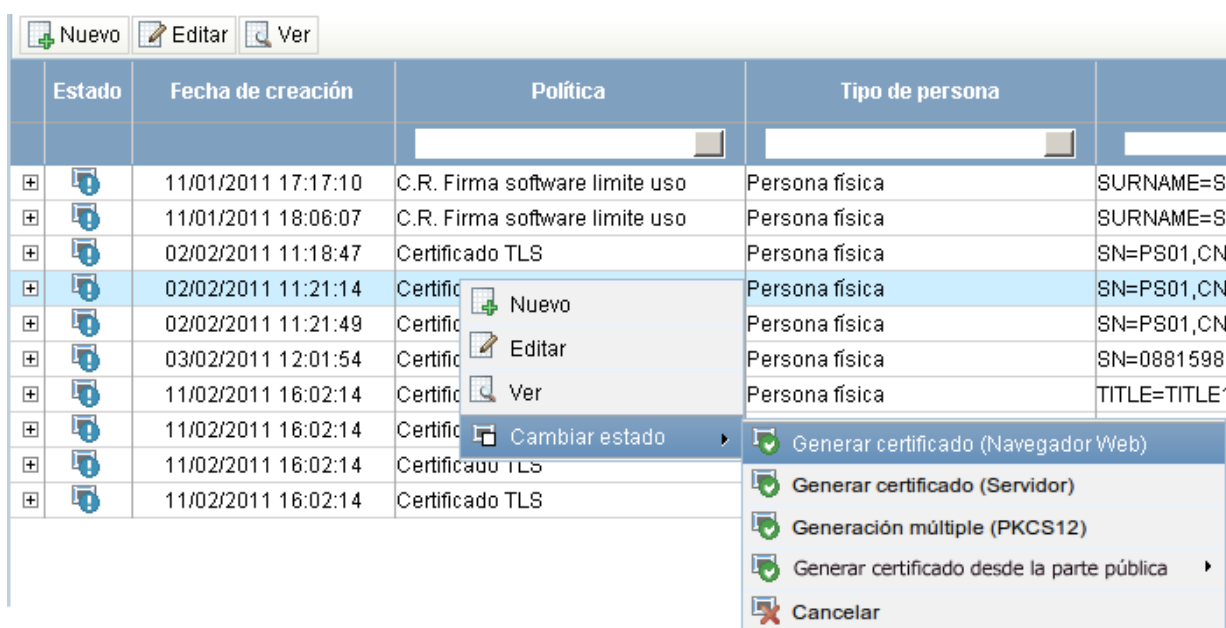
**Nota:** cuando todos los operadores habilitados para ello revocan el certificado, este pasa automáticamente a "Revocados" y deja de estar disponible para firma.

## 5 - PROCESO DE GENERACIÓN DE CERTIFICADOS

### 5.1 INTRODUCCIÓN

**Atención:** La generación de certificados solo se puede realizar si la entidad ha sido creada y validada previamente en RAEDICOM por un operador autorizado.

Una vez el proceso de validación ha sido terminado favorablemente el certificado pasa a estar *Listo para ser generado* y desde ese momento el certificado puede ser generado a través de las distintas opciones disponibles desde Menú contextual  **Cambiar estado**



The screenshot shows a web application interface with a table of certificates. At the top, there are buttons for 'Nuevo', 'Editar', and 'Ver'. The table has columns: 'Estado', 'Fecha de creación', 'Política', 'Tipo de persona', and an unlabeled column. A context menu is open over one of the rows, showing options: 'Nuevo', 'Editar', 'Ver', 'Cambiar estado', and a sub-menu for 'Cambiar estado' with options: 'Generar certificado (Navegador Web)', 'Generar certificado (Servidor)', 'Generación múltiple (PKCS12)', 'Generar certificado desde la parte pública', and 'Cancelar'.

Estado	Fecha de creación	Política	Tipo de persona	
	11/01/2011 17:17:10	C.R. Firma software limite uso	Persona física	SURNAME=SI
	11/01/2011 18:06:07	C.R. Firma software limite uso	Persona física	SURNAME=SI
	02/02/2011 11:18:47	Certificado TLS	Persona física	SN=PS01,CN:
	02/02/2011 11:21:14	Certificado	Persona física	SN=PS01,CN:
	02/02/2011 11:21:49	Certificado	Persona física	SN=PS01,CN:
	03/02/2011 12:01:54	Certificado	Persona física	SN=0881598
	11/02/2011 16:02:14	Certificado	Persona física	TITLE=TITLE1
	11/02/2011 16:02:14	Certificado	Persona física	
	11/02/2011 16:02:14	Certificado TLS	Persona física	
	11/02/2011 16:02:14	Certificado TLS	Persona física	



	<b>Generar certificado (Navegador Web)</b> Estos certificados electrónicos se generan sobre distintos soportes según la política de certificación seleccionada.
	<b>Generar certificado (Servidor)</b> Estos certificados se generan en formato PEM, conteniendo las claves públicas del certificado.
	<b>Generación múltiple (PKCS12).</b> Esta opción permite la generación de varios certificados al mismo tiempo, devolviéndolos en un archivo ZIP que contiene un lote de varios certificados.
	<b>Generar certificado desde la parte pública.</b> Esta opción permite la generación del certificado electrónico desde la parte pública por parte del propio usuario al que se le expide el certificado. Se puede crear cualquiera de los tipos de certificado anteriores desde la parte pública.

El paso de *Listo para generar* a *Generado* implica la generación de un par de claves y la petición a la Autoridad de Certificación de que a partir de ellas genere un Certificado Electrónico. Este proceso tiene ligeras diferencias dependiendo del tipo de certificado y la política de certificación seleccionada.

### 5.2 CERTIFICADOS DE NAVEGADOR WEB

Una vez llevadas a cabo las tareas descritas con anterioridad en **Alta de una entidad** y la petición de emisión cumpla todos los requisitos, se procede a la creación del certificado propiamente dicho, con la generación de un par de claves y la emisión de una solicitud de certificado al EJBCA, el software de generación de Certificados de la ACEDICOM.

Estos certificados se generan seleccionando el la entidad del panel de control y a través de la opción:

- Menú contextual  **Cambio de estado:** Opción  **Generar certificado (Navegador Web).**

ACEDICOM, la autoridad de Certificación de EDICOM, es capaz de emitir distintos tipos de certificados. La política de certificación y el tipo de certificado elegido dictan el proceso de registro que debe seguir el usuario de RAEDICOM. Para más información revisar el anexo [10.Navegadores y generación de claves.](#)

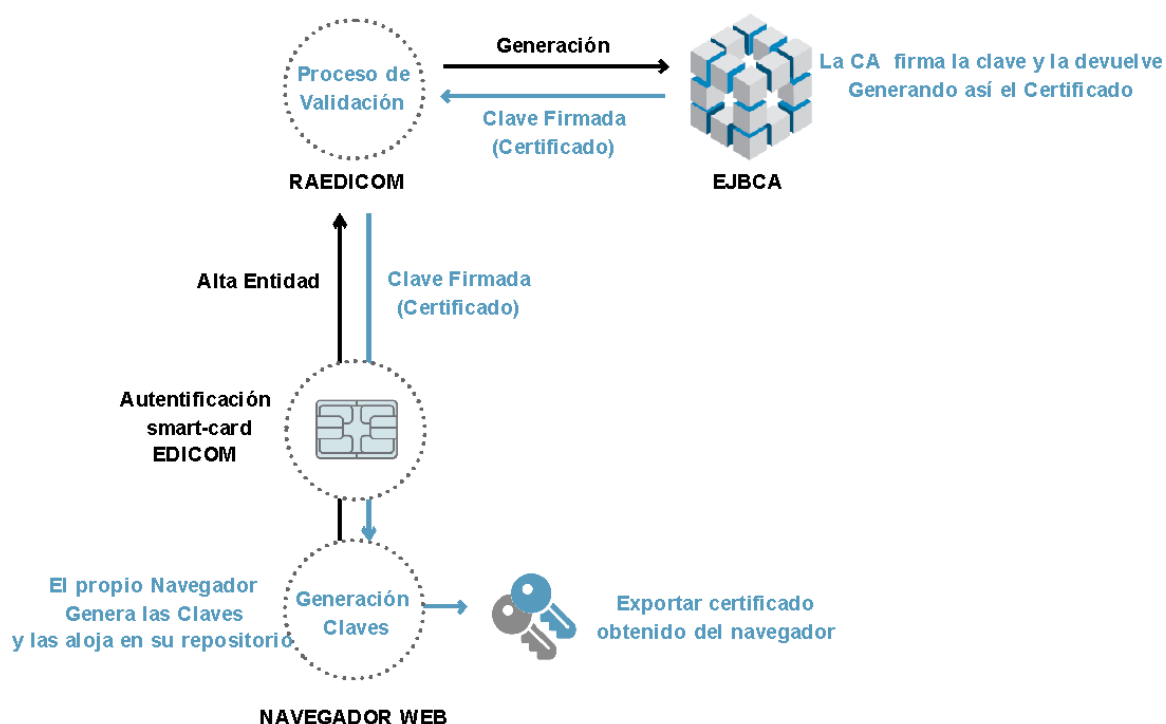
## PETICIÓN DE UN CERTIFICADO SOBRE SOPORTE SOFTWARE.

RAEDICOM permite el registro de certificados reconocidos sobre soporte software bajo su política de certificación correspondiente a:

- **Certificado Reconocido de firma con limitación de uso sobre soporte Software.**

Los pasos necesarios son:

- **Paso 1.** El Usuario, a través de la autenticación con Smart card se valida en la interfaz web de RAEDICOM. Para ello hay que seleccionar el certificado correspondiente al acceso web e introducir el PIN de la Smart card.
- **Paso 2.** Una vez dentro del interfaz web, El par de claves requerido para generar el certificado es generado en el propio navegador. Al generar un certificado se pedirá elegir los parámetros del futuro certificado a generar. Estos parámetros dependen del navegador utilizado y pueden llegar a ser muy distintos. Para más información revisar el anexo [10.Navegadores y generación de claves.](#)
- **Paso 3.** Una vez seleccionados los parámetros adecuados para la generación de las claves se envían al software de generación de certificados de Edicom (EJBCA). La CA da de alta el nuevo certificado y devuelve al usuario la clave firmada convirtiendo el par de claves en un certificado listo para usar.
- **Paso 4.** El certificado generado se deposita en el repositorio del propio navegador. Para su utilización en otros ordenadores o aplicaciones debe ser exportado del navegador según el proceso indicado en el manual de usuario del navegador.



## PETICIÓN DE UN CERTIFICADO SOBRE DISPOSITIVO SEGURO (SMART-CARD)

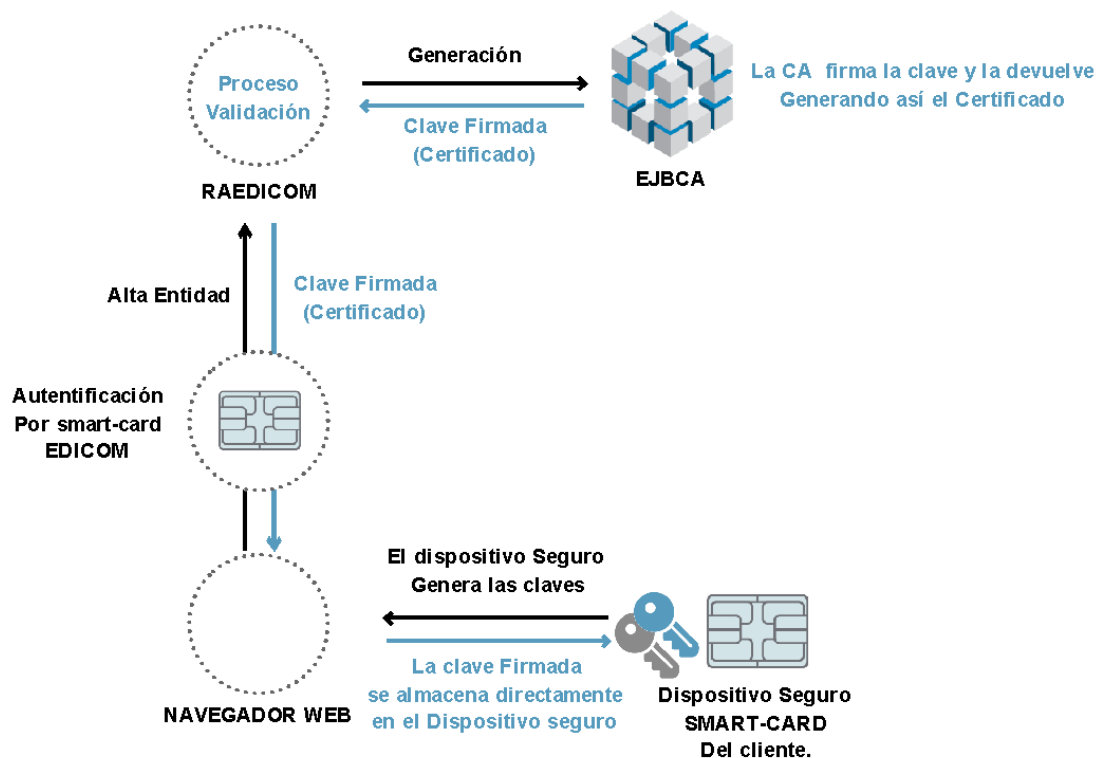
RAEDICOM permite el registro de certificados reconocidos sobre dispositivo seguro (Smart-card) bajo su política de certificación correspondiente a:

- **Certificado Reconocido de firma sobre dispositivo seguro "Smart Card".**

Los pasos necesarios son:

- **Paso 1.** El usuario, a través de la identificación con Smart Card se valida en la interfaz web de RAEDICOM. Para ello hay que seleccionar el certificado correspondiente al acceso web e introducir el PIN de la Smart Card.
- **Paso 2.** Para generar un certificado sobre soporte seguro o Smart Card, este debe ser conectado correctamente al ordenador del usuario. ACEDICOM solo permite el uso de ciertos Dispositivos seguros indicados en sus políticas de certificación para la expedición de este tipo de certificados sobre dispositivo Seguro.
- **Paso 3.** Una vez dentro del interfaz web, El par de claves requerido para generar el certificado es generado en el propio dispositivo seguro y enviado a través de RAEDICOM a el EJBCA. La CA firma la clave y la devuelve al usuario convirtiendo el par de claves en un certificado.

- **Paso 4.** El certificado generado se aloja directamente en el Dispositivo seguro. Siendo imposible extraerlo. A partir de ahora el uso del certificado debe estar asociado a que dicho dispositivo este accesible en el momento que se necesite.



## PETICIÓN DE UN CERTIFICADO SOBRE DISPOSITIVO SEGURO CENTRALIZADO

RAEDICOM permite el registro de certificados reconocidos sobre Dispositivo Seguro Centralizado (Hardware Security Modules) bajo sus política de certificación correspondiente a:

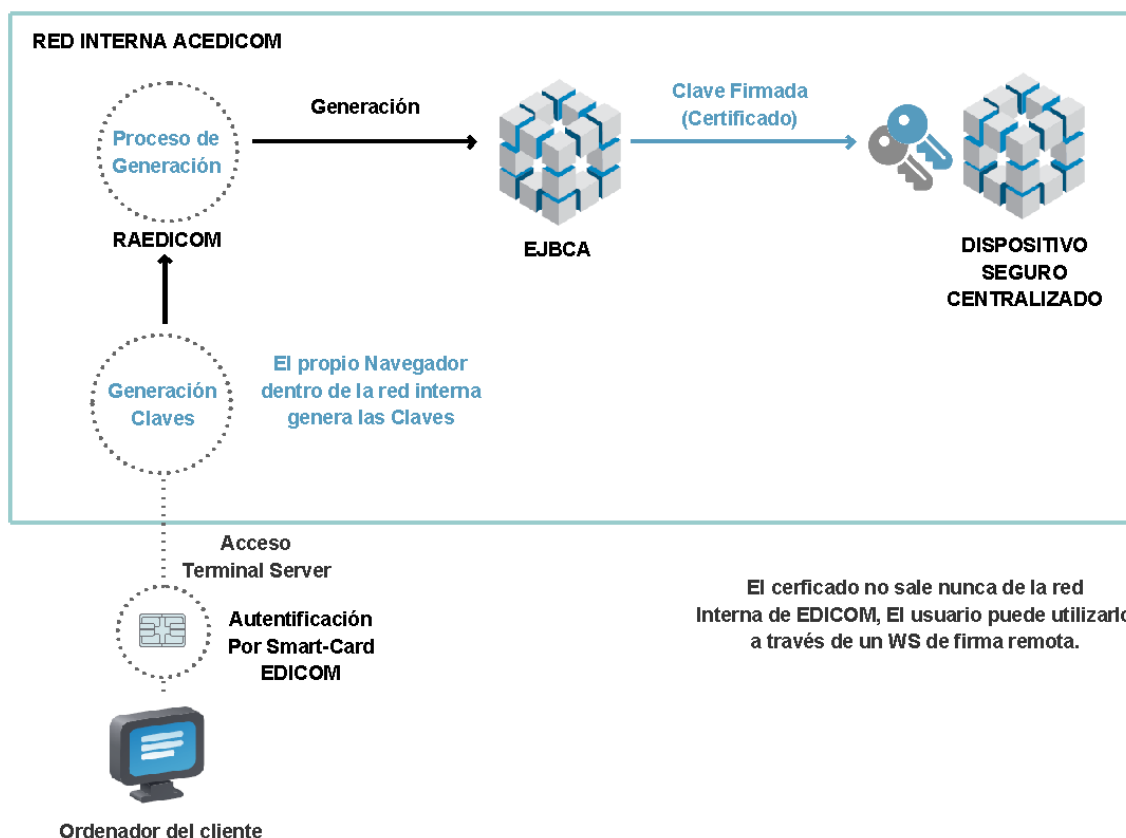
- **Certificado Reconocido de firma con limitación de uso sobre dispositivo seguro centralizado.**
- **Certificado Reconocido de firma sobre dispositivo seguro centralizado para factura electrónica y almacenamiento certificado.**

Los pasos necesarios son:

- **Paso 1.** El usuario, a través de la identificación con Smart Card, se valida en una conexión Terminal Server con una máquina remota preparada para el registro de certificados en el dispositivo seguro centralizado. Para ello hay que seleccionar el certificado correspondiente al acceso Terminal Server (Identificado como "Windows" e introducir el PIN de la Smart Card.



- **Paso 2.** Una vez dentro de la red interna de EDICOM se accede a un escritorio remoto desde donde acceder a RAEDICOM normalmente para emitir la solicitud de generación de certificado al EJBCA.
- **Paso 3.** El certificado generado se aloja directamente en el Dispositivo Seguro Centralizado. A partir de ahora el uso del certificado debe estar asociado al acceso remoto a dicho Dispositivo a través de las URL indicadas por ACEDICOM. La diferencia en este caso es que ni las claves originales ni el certificado salen nunca de la red Interna de EDICOM.



### 5.3 CERTIFICADOS DE SERVIDOR

Una vez llevadas a cabo las tareas descritas con anterioridad en **Alta de una entidad** y la petición de emisión cumpla todos los requisitos, se procede a la creación del certificado propiamente dicho.

En el caso de certificados de servidor se procede a la creación del certificado a partir del fichero de petición CSR (Certificate Signing Request) proporcionado por el cliente. Estos certificados se generan seleccionando la entidad del panel de control y a través de la opción:

- Menú contextual **Cambio de estado:** Opción **Generar certificado (Servidor).**

Aparece así el formulario de generación, donde se puede enviar la solicitud de generación CSR de dos formas distintas:

- A través del campo **Fichero CSR** que permite examinar el disco duro para cargar el fichero CSR.
- A través del campo de texto **Texto CSR** que permite pegar en un campo de texto La petición. Esta petición es la solicitud del certificado codificado en BASE64 siguiendo este esquema:

```
-----BEGIN CERTIFICATE REQUEST-----
Petición de certificado codificada en BASE64
-----END CERTIFICATE REQUEST-----
```

- Finalmente el certificado será devuelto en formato PEM (Privacy Enhanced Mail) con la información del certificado codificado en BASE64 siguiendo este esquema:

```
-----BEGIN CERTIFICATE-----
Certificado en formato PEM codificado en BASE64
-----END CERTIFICATE-----
```

## 5.4 GENERACIÓN MÚLTIPLE (PKCS12)

Esta opción permite generar múltiples certificados al mismo tiempo. Este proceso genera un fichero "zip" con los PKCS12 que estén seleccionados en ese momento en el panel de control. Estos certificados se generan seleccionando las entidades del panel de control y a través de la opción:

- Menú contextual  **Cambio de estado:** Opción  **Generación múltiple (PKCS12).**



La duración del proceso de generación múltiple de certificados aumenta en función del número de certificados que se quiere generar. Por ese motivo el proceso de generación de certificados se hace de forma asíncrona. De esta forma, el proceso se puede cambiar en cualquier momento para que se ejecute en background y posteriormente descargar los certificados creados desde el menú de Utilidades, a través de la opción

- Menú principal **Utilidades-Carga Masiva de Entidades:** Opción **Descarga de certificados pendientes.**

## 5.5 CERTIFICADOS DESDE LA PARTE PÚBLICA

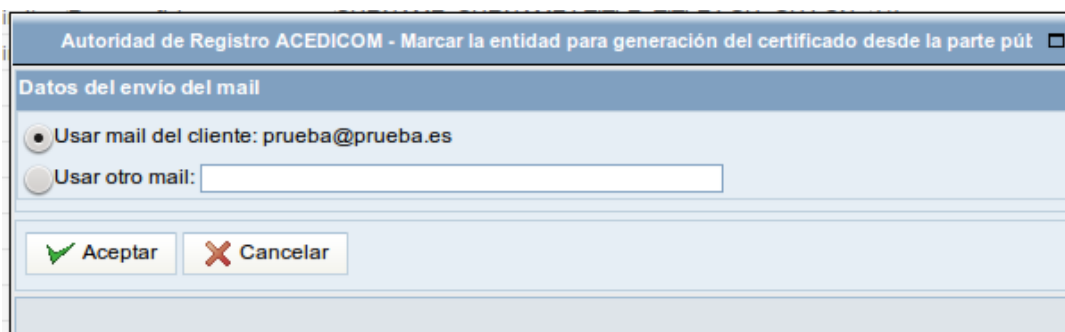
El operador puede marcar la entidad para que el cliente pueda generar él mismo su propio certificado desde la parte pública de la aplicación. Estos certificados no se generan automáticamente, sino que se marcan para permitir ser generados más tarde por el usuario desde la parte pública y por tanto son visibles desde la parte pública. De esta forma, el certificado puede ser generado directamente en su propio token o navegador web (según el caso), o para ser descargado directamente en caso de un PKCS12.

La única restricción que tiene esta alternativa de generación del certificado, es que en el momento de marcar el certificado como generable por el usuario de este modo, el operador debe determinar por adelantado el tipo de certificado que el usuario generará. El usuario solo puede generar desde la parte pública este tipo determinado de certificado de entre los tipos de certificados ya comentados.

- **Paso 1. Marcar y elegir el tipo de certificado a generar.** El operador puede marcar la entidad para generar el certificado desde la parte pública a través del panel de control, seleccionando la entidad y desde:
  - Menú contextual  **Cambio de estado:** Opción  **Generar certificado desde la parte pública.** Elegir uno de los tres tipos de certificado a generar.



- **Paso 2. Elegir la cuenta de correo de notificación.** En ese momento, el operador debe elegir a que cuenta de correo e-mail enviar los datos de acceso al certificado para que pueda generarlo desde la parte pública. Al la cuenta por defecto del usuario o cualquier otro e-mail que indique en ese momento el operador.



Una vez indicado se envía un e-mail a la dirección de correo indicada con los datos de acceso: la URL para acceder a la generación del certificado y el token autogenerado de referencia. A partir de esta información puede localizar la entidad y generar él mismo el certificado.



Filtro de Búsqueda	
Email:	prueba@prueba.es
Token:	E8B40179C351B38EE7FE7EA65BE46506
[Buscar]	
Estado de la generación del certificado	
Política:	Certificado TLS
Tipo de persona:	Persona física
Email:	prueba@prueba.es
Cliente:	Nombre 1 (11111111A)
Estado:	VALIDADO
Datos del usuario	
SubjectDN:	CN=Nombre
AltName:	
[Generar certificado]	

## 6 - GESTIÓN DE USUARIOS

### 6.1 INTRODUCCIÓN

---



**Atención:** La creación de usuarios es un privilegio reservado a los administradores y operadores de la RAEDICOM. Si el usuario no tiene permisos para acceder a estas opciones es posible que no pueda verlas en el interfaz.

En la **RAEDICOM** el usuario es un operador de registro cuya función principal puede variar según los roles de usuario que tenga asignados.

Para acceder al listado de usuarios, desde:

- Menú principal **Administración**: Opción  **Usuarios**.

Aparece así el listado de usuarios habilitados en la estación. Dentro del listado cada usuario viene representado como una línea con los siguientes datos.

- **Nombre.** Indica el nombre o la razón social detrás de este usuario.
- **Número de serie.** Indica el número de serie del certificado con el que se valida en la estación de manera directa.
- **Tipo.** Indica de manera gráfica el tipo de usuario, si se trata de un usuario operador o no.
- **Nombre del usuario.** Indica el nombre de usuario con que se representa en la aplicación.
- **Fecha de creación.** Indica la fecha de creación del usuario en la aplicación.
- **Habilitado.** Indica de manera gráfica si el usuario está  habilitado o  inhabilitado. Cuando un usuario esta inhabilitado no puede acceder a la aplicación. Es una manera de impedir temporalmente o de manera definitiva el acceso de dicho usuario a la aplicación. Esta situación es reversible. En realidad lo que se cancela es el acceso del nº de certificado asociado a dicho usuario.
- **Idioma.** Indica el idioma en que el usuario accede a la RAEDICOM.

	Nombre de usuario	Número de serie	Tipo	Nombre	Fecha de cr
		55555555555555		OPERADOR OP1	29/03/2010
	Rol				
	Subir documentación del cliente				
	Descargar documentación del cliente				
	Generar certificados				
	Revocar entidades				
	Crear entidades				
	Descargar certificados				
	Cancelar entidades				
	Usuario superadministrador				
	Borrar documentación del cliente				
	Validar entidades				
		55555555555555		OPERADOR OP2	29/03/2010

**Nota:** Si se despliega la línea del usuario se accede a una lista de los roles que tiene asociado dicho usuario.

## 6.2 OPCIONES DEL GESTOR DE USUARIO

El menú contextual del gestor de usuarios tiene las siguientes opciones

	<b>Nuevo.</b> Permite añadir un nuevo usuario.
	<b>Editar.</b> Permite editar los datos del usuario seleccionado.
	<b>Habilitar.</b> Permite cambiar de estado un usuario inhabilitado (visible solo si está inhabilitado).
	<b>Inhabilitar.</b> Permite cambiar de estado un usuario habilitado (visible solo si está habilitado).
	<b>Recargar.</b> Permite recargar la información de usuarios de la base de datos.

### CREAR NUEVO USUARIO

Para crear un nuevo usuario, una vez en el panel de configuración de usuarios.

- Menú contextual: Opción **Nuevo.**

Se accede así al formulario de datos de nuevo usuario donde se pueden definir los datos del usuario y los roles que desempeñará dentro de la RAEDICOM.

Autoridad de Registro ACEDICOM - Datos del usuario													
<b>Usuario</b>													
<b>Nombre de usuario:</b>	OPERADOR												
<b>Número de serie del certificado de usuario:</b>	55555555555555												
<b>Nombre:</b>	NOMBRE												
<b>Apellidos:</b>	APELLIDOS												
<b>Operador:</b>	<input checked="" type="checkbox"/>												
<b>Habilitado:</b>	<input checked="" type="checkbox"/>												
<b>Idioma:</b>	Español												
<b>Roles</b>	<b>Políticas</b>												
<table border="1"> <thead> <tr> <th>Roles</th> </tr> </thead> <tbody> <tr><td>Cancelar entidades</td></tr> <tr><td>Usuario superadministrador</td></tr> <tr><td>Subir documentación del cliente</td></tr> <tr><td>Borrar documentación del cliente</td></tr> </tbody> </table>	Roles	Cancelar entidades	Usuario superadministrador	Subir documentación del cliente	Borrar documentación del cliente	<table border="1"> <thead> <tr> <th>Roles del usuario</th> </tr> </thead> <tbody> <tr><td>Revocar entidades</td></tr> <tr><td>Descargar certificados</td></tr> <tr><td>Validar entidades</td></tr> <tr><td>Crear entidades</td></tr> <tr><td>Generar certificados</td></tr> <tr><td>Descargar documentación del cliente</td></tr> </tbody> </table>	Roles del usuario	Revocar entidades	Descargar certificados	Validar entidades	Crear entidades	Generar certificados	Descargar documentación del cliente
Roles													
Cancelar entidades													
Usuario superadministrador													
Subir documentación del cliente													
Borrar documentación del cliente													
Roles del usuario													
Revocar entidades													
Descargar certificados													
Validar entidades													
Crear entidades													
Generar certificados													
Descargar documentación del cliente													
<input checked="" type="checkbox"/> Aceptar <input type="checkbox"/> Cancelar													

### Datos de usuario

- **Nombre de usuario.** Permite indicar el nombre de usuario. Con que se identifica al usuario en la aplicación.
- **Número de serie del certificado de usuario.** Permite indicar el número de serie del certificado para validarse automáticamente en la aplicación. Este Nº de serie es el correspondiente al certificado alojado en la smart-card con que el usuario se valida en la RAEDICOM.
- **Nombre.** Permite indicar el nombre real del usuario.
- **Apellidos.** Permite indicar los apellidos del usuario.
- **Operador.** Permite indicar que se trata de un operador.
- **Habilitado.** Permite habilitar o inhabilitar un usuario.

- **Idioma.** Permite seleccionar el idioma con que el usuario entrará en la aplicación.

### ***Roles de usuario***

Los roles de usuario corresponden a los permisos que tiene el usuario en la aplicación y el papel que desempeñan en el proceso de registro de certificados.

Para **añadir** o **eliminar** permisos al usuario seleccionado se deben pasar los roles de la columna de la izquierda que refleja los roles todavía no asignados a la columna de la derecha, que representa los roles ya asignados al usuario. Para eliminar roles, hay que proceder de manera inversa.

La descripción de cada permiso es la siguiente.

- **Crear entidades.** Permite al usuario crear nuevas entidades: seleccionar la política de certificación y completar la información correspondiente a los datos de la entidad. Implica también una primera validación de dicha entidad recién creada.
- **Validar entidades.** Permite al usuario validar entidades que están en estado de nueva entidad.
- **Generar certificados.** Permite al usuario generar los certificados de las entidades que han alcanzado el estado "Listo para generar".
- **Descargar certificados.** Permite al usuario obtener el certificado en formato "\*.cer" directamente desde RAEDICOM y descargarlo a su disco duro.
- **Revocar entidades.** Permite al usuario revocar entidades.
- **Cancelar entidades.** Permite al usuario cancelar entidades, cuando están en estado "Nuevo" o "Listos para Generar".
- **Usuario superadministrador.** Habilita al usuario con todos los permisos disponibles para la administración de la aplicación.
- **Subir documentación del cliente.** Permite al usuario importar la documentación correspondiente al cliente en la pantalla de información de la entidad.
- **Descargar documentación del cliente.** Permite al usuario acceder a la documentación correspondiente al cliente incluida en la pantalla de información de la entidad.
- **Borrar documentación del cliente.** Permite al usuario borrar la documentación correspondiente al cliente incluida en la pantalla de información de la entidad.
- **Generación múltiple de certificados.** Permite al usuario la generación múltiple de certificados.
- **Acceso a través de webservice.** Permite al usuario acceder a Raedicom a través del Web Service

## **Políticas**

Las políticas de certificación se eligen al generar una nueva entidad. A nivel de usuario se puede limitar para qué políticas de certificación puede generar entidades el usuario. Esto afecta tanto al rol Generar Entidades como a la visibilidad en el listado principal de las entidades generadas bajo las políticas a las que el usuario no tiene acceso.

La pestaña **Políticas** permite seleccionar las políticas de certificación que serán accesibles por el usuario a la hora de Generar nuevas entidades. La lista de políticas disponible se muestra, como en el caso de los roles, a la izquierda, y la lista de políticas habilitadas a la derecha.



## 7 - GESTIÓN DE CLIENTES

### 7.1 INTRODUCCIÓN

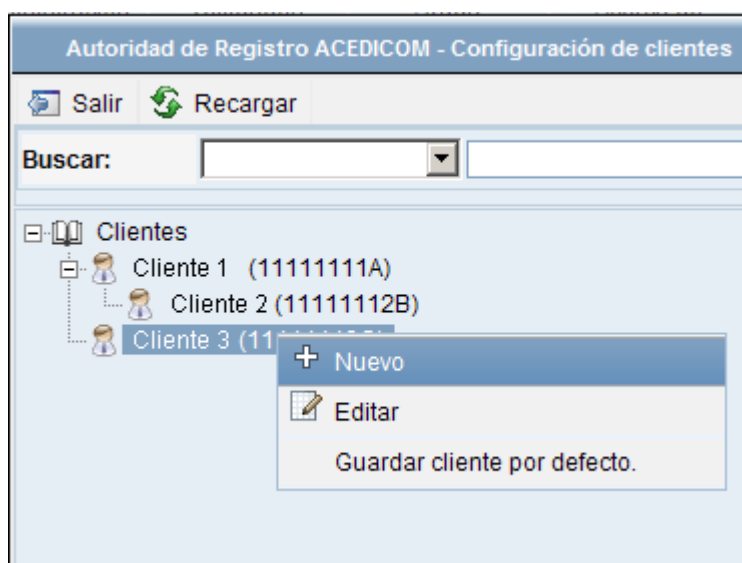
**Atención:** La creación de clientes es un privilegio reservado a los administradores y operadores de la RAEDICOM. Si el usuario no tiene permisos para acceder a estas opciones es posible que no pueda verlas en el interfaz.

En la **RAEDICOM** el cliente es el suscriptor del servicio, y la persona o empresa para la cual se va a generar la entidad y el certificado correspondiente. Cuando se genera una nueva entidad se debe seleccionar un Cliente. Esto carga automáticamente los datos de contacto del cliente en la entidad y también se comprueba la existencia de paquetes de licencias contratados por ese cliente.

El acceso al listado de clientes se puede hacer desde:


- Menú principal **Administración**: Opción  **Clientes**.


Aparece así el árbol de clientes de la estación.



Dentro del árbol de clientes, cada cliente puede tener ramas como si fueran nuevos clientes en función de sus necesidades de desglose de información o paquetes de licencias. Haciendo doble clic con el ratón sobre cada cliente es posible acceder a sus datos personales y al listado de paquetes de licencias solicitadas por cada uno.

Además, con el botón derecho del ratón, se accede al menú contextual con las siguientes opciones.

	<b>Añadir.</b> Permite añadir un nuevo cliente. Si se selecciona un nodo correspondiente a un cliente se asignará un subnodo.
---	---

	<b>Editar.</b> Permite editar los datos del paquete de licencias seleccionado.
	<b>Asignar cliente como cliente por defecto.</b> Asigna el cliente seleccionado como cliente por defecto en las nuevas entidades.

## DATOS PERSONALES DEL CLIENTE.

Autoridad de Registro ACEDICOM - Datos del cliente

**Cliente**

**Nombre:**  **NIF:**


**Dirección:**  **Código Postal:**

**Ciudad:**  **Provincia:**

**País:**

**Comentarios:**

**Paquetes de licencias**

+ Añadir  Editar

Nº de licencias	Licencias consumidas	Política	Fecha de creación	Operador	Fecha de finalización
10	10	C.R. Firma software limite u	12/01/2011 11:20:59	OPERADOR OP1	28/01/2011 11:03:42
1	1	Certificado TLS	11/01/2011 16:53:03	OPERADOR OP1	12/01/2011 11:38:50

- **Nombre.** Permite indicar el nombre asociado al cliente en el listado de clientes. Este dato es obligatorio.
- **N.I.F.** Permite indicar el NIF asociado al cliente. Este dato es obligatorio.
- **Dirección.** Permite indicar la dirección del cliente.
- **Código postal.** Permite indicar el código postal asociado al cliente
- **Provincia.** Permite indicar la provincia asociada al cliente.
- **País.** Permite seleccionar el país asociado al cliente.
- **Comentarios.** Permite incluir cualquier indicación asociada al cliente.

## PESTAÑA "PAQUETES DE LICENCIAS"

Los **paquetes de licencias** indican el número de licencias contratadas para una política determinada que ha solicitado el cliente. Mientras queden licencias disponibles, el cliente puede solicitar la emisión de nuevos certificados. Una vez las licencias para una política se



acaben, no se podrá generar un certificado para ese cliente con esa política hasta que contrate un nuevo paquete de licencias.

## PAQUETES DE LICENCIAS

- **Nº de licencias.** Indica el número de licencias que forman el paquete.
- **Licencias consumidas.** Indica indicar el número de licencias consumidas respecto al número de licencias total.
- **Política.** Indica la política de certificación bajo la que se han generado los certificados.
- **Fecha de creación.** Indica la fecha de creación de los certificados
- **Operador.** Indica el operador habilitado que genere el paquete de licencias.
- **Fecha de finalización.** Indica la fecha de fin de vigencia.


## 7.2 OPCIONES DEL GESTOR DE PAQUETES DE LICENCIAS

El menú contextual del gestor de licencias tiene las siguientes opciones.

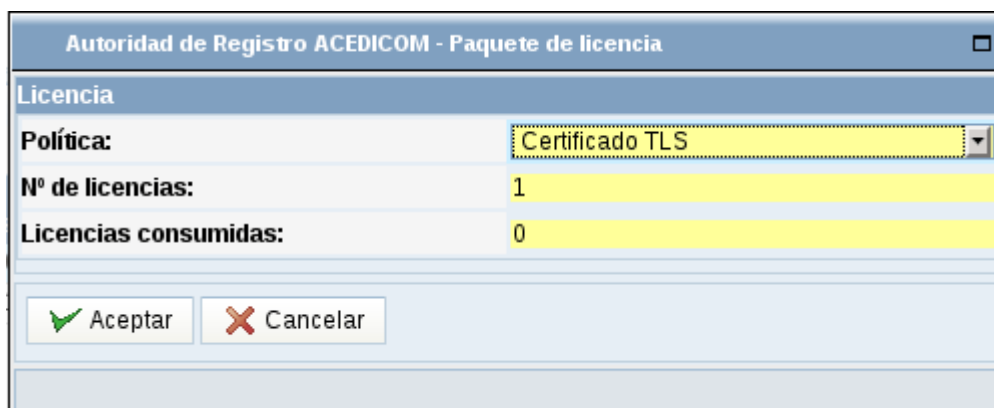
	<b>Añadir.</b> Permite añadir un nuevo paquete de licencias.
	<b>Editar.</b> Permite editar los datos del paquete de licencias seleccionado.

### CREAR NUEVO PAQUETE DE LICENCIAS.

Desde el menú contextual (botón derecho del ratón) sobre el área de *Paquetes de licencias*

- Menú contextual: Opción  **Añadir.**

Se accede así al formulario de datos de nuevo paquete de licencia donde se pueden definir la política de la licencia y el número de licencias que va a contener el paquete. El número máximo de licencias es de 32767 licencias.




El formulario, titulado "Autoridad de Registro ACEDICOM - Paquete de licencia", contiene los siguientes campos:

- Licencia:** Encabezado de la sección.
- Política:** Selector desplegable con la opción "Certificado TLS" seleccionada.
- Nº de licencias:** Campo de texto con el valor "1".
- Licencias consumidas:** Campo de texto con el valor "0".

En la parte inferior del formulario hay dos botones: "Aceptar" (con un icono de checkmark verde) y "Cancelar" (con un icono de X roja).

## EDITAR PAQUETE DE LICENCIAS

Para editar un paquete de licencias es necesario que el paquete de licencias no haya sido consumido totalmente. Para editar un paquete de licencias, una vez en el panel de configuración de paquetes de licencias.

- Menú contextual: Opción  **Editar**.

Se accede así al formulario de datos del paquete de licencia donde se puede modificar únicamente el número de licencias que va a contener el paquete. El número máximo de licencias es de 32767 licencias.

## 8 - ESTADÍSTICAS

### 8.1 INTRODUCCIÓN

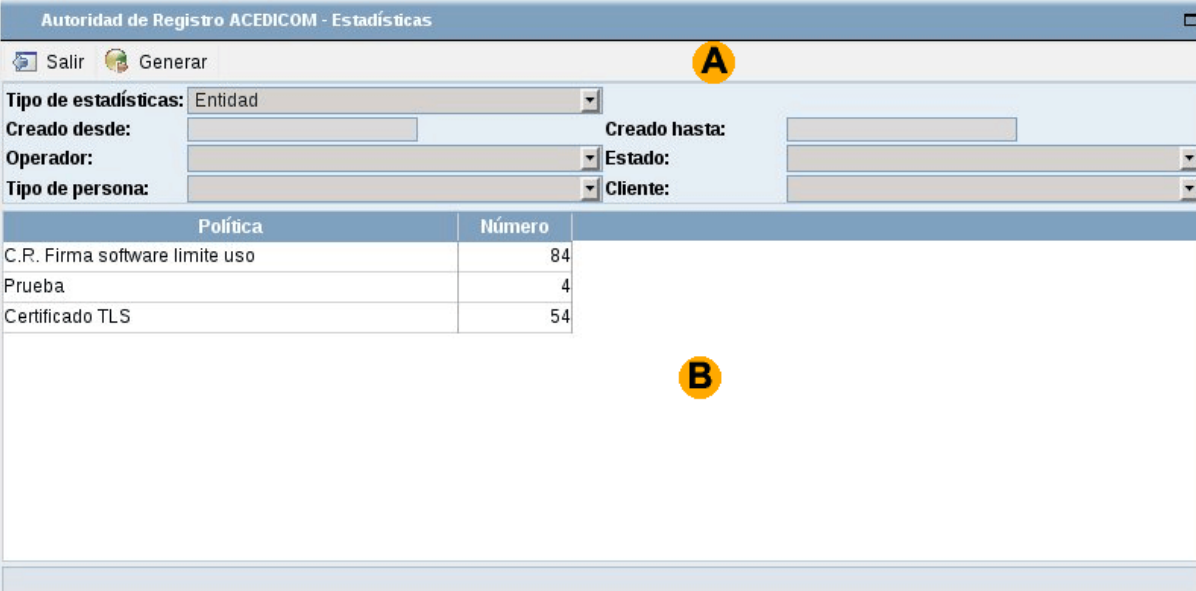
**Atención:** La visualización de estadísticas es un privilegio reservado a los administradores y operadores de la RAEDICOM. Si el usuario no tiene permisos para acceder a estas opciones es posible que no pueda verlas en el interfaz.

La **RAEDICOM** permite hacer un seguimiento de las entidades o certificados generados por política, a través de la opción Estadísticas.

El acceso al listado de clientes se puede hacer desde:

- Menú principal **Administración**: Opción  **Estadísticas**.

Aparece así la pantalla de generación de estadísticas.



Política	Número
C.R. Firma software limite uso	84
Prueba	4
Certificado TLS	54

La pantalla de estadísticas se divide en 2 zonas:

- a) **(A) Filtro de búsqueda.** Indica los parámetros de generación de las estadísticas.
- b) **(B) Resultados.** Indica las estadísticas por políticas.

Una vez seleccionado el filtro de búsqueda de estadísticas, hay que pulsar el botón **Generar** para obtener los datos de la consulta.

### FILTRAR ESTADÍSTICAS

El área superior de la pantalla permite parametrizar los criterios de filtrado de las estadísticas.

- **Tipo de estadísticas.** Permite seleccionar el tipo de datos buscados. Pueden ser Entidades o certificados (entidades con certificado generado).
- **Creado desde.** Permite seleccionar la fecha de creación como parámetro de búsqueda.
- **Creado hasta.** Permite seleccionar la fecha final de creación como parámetro de búsqueda.
- **Operador.** Permite seleccionar el usuario que generó la entidad como parámetro de búsqueda.
- **Estado.** Permite seleccionar el estado actual de la entidad.
- **Tipo de persona.** Permite seleccionar el tipo de persona asociado a los datos de la entidad (físico o jurídico) como parámetro de búsqueda.
- **Cliente.** Permite seleccionar el cliente al que está asignado la entidad.

## 9 - UTILIDADES

### 9.1 CARGA MASIVA DE ENTIDADES.

La carga masiva de entidades permite generar múltiples entidades a partir de un fichero con formato CSV. Una vez insertadas las entidades, si las entidades quedan en estado *Pendientes de generar* (solo tienen una validación), automáticamente comenzará el proceso de generación de los certificados de esas entidades.

El resultado será que se generarán los ficheros pfx de las entidades junto con un fichero de texto que indicará la clave de acceso del pfx. Todos los certificados se insertarán en un fichero zip que será el que se descargará al finalizar el proceso de generación de certificados.


- Desde la pantalla se selecciona la política de las entidades, el cliente al que se le asociarán las entidades y el fichero CSV.
- Según el formato del fichero CSV, se puede seleccionar también el carácter separador de los campos.
- Adicionalmente, y sabiendo el operador previamente los campos de la política a utilizar, se puede especificar el campo de los datos que servirá para poner el nombre de los pfx generados. En caso de no poner nada, se devolverán con el valor por defecto que asigna la aplicación.

El proceso de generación es costoso, por lo que se permite la ejecución en background del proceso. De esta forma, cuando termine la ejecución, el fichero zip estará disponible en la pantalla de descarga de certificados pendientes.

## 9.2 DESCARGA DE CERTIFICADOS PENDIENTES.

En esta pantalla aparecen los certificados generados que todavía no han sido descargados por el operador. Para descargar un paquete de certificados

- Menú principal de la pantalla : opción  **Descargar**.

Una vez descargado el fichero de certificados, automáticamente desaparece de la lista. Utilizar la opción  **Actualizar** para reflejar los cambios.

Autoridad de Registro ACEDICOM - Carga masiva de entidades			
 Descargar  Actualizar			
Nombre	Fecha de inserción	Usuario	Descripción
keyStores.zip	12/01/2011 11:21	OPERADOR OP1	Fichero de certificados.
keyStores.zip	07/01/2011 17:26	OPERADOR OP1	Fichero de certificados.
keyStores.zip	07/01/2011 17:21	OPERADOR OP1	Fichero de certificados.
keyStores.zip	20/12/2010 09:34	OPERADOR OP1	Fichero de certificados.
keyStores.zip	20/12/2010 09:34	OPERADOR OP1	Fichero de certificados.
 Salir			



## 10 - NAVEGADORES Y GENERACIÓN DE CLAVES.

### 10.1 MOZILLA FIREFOX 3


#### GENERACIÓN DE CLAVES



RAEDICOM bajo el Navegador **Mozilla Firefox** pedirá en dos pantallas distintas primero la longitud de la clave y seguidamente el protocolo de encriptación utilizado para generar las claves.

- **Longitud de la clave.** Este parámetro permite escoger la longitud de la clave a generar. Esta longitud debe coincidir con la Longitud especificada por la política de certificación.

*Nota: "High Grade" o "Grado Alto" corresponde a una clave de 2048 bits y "Medium Grade" o "Grado Medio" corresponde a 1024 bits*

Una vez especificado este parámetro se inicia el proceso de generación con el botón  **Generar**.

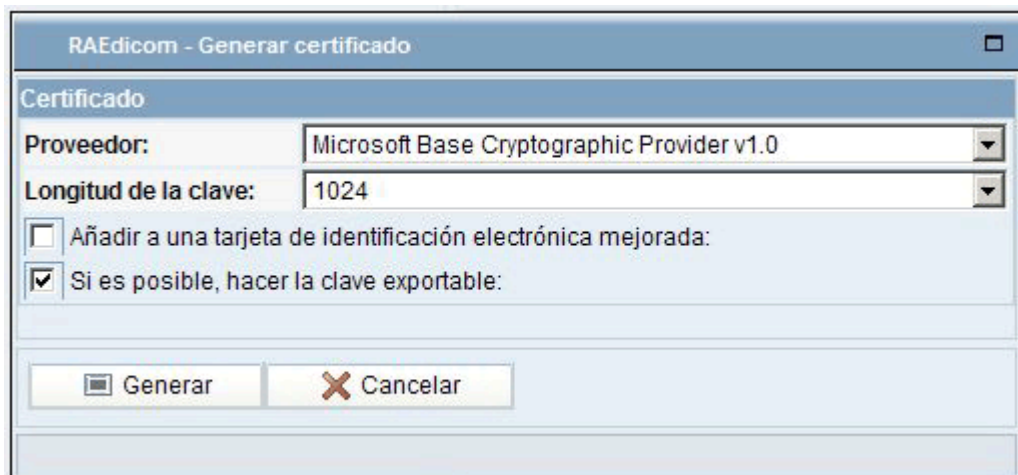
Y en este caso el propio navegador mostrará una segunda pantalla para elegir el tipo de encriptación a utilizar en la generación de las claves.

- En el caso de **certificados para dispositivo seguro**, el protocolo de encriptación corresponde con el driver del proveedor de la Smart Card.

Para saber más sobre lo especificado en las políticas de certificación, consultar la información actualizada en la web de ACEDICOM: [acedicom.edicomgroup.com](http://acedicom.edicomgroup.com)


## 10.2 MICROSOFT INTERNET EXPLORER

### GENERACIÓN DE CLAVES



RAEDICOM bajo el Navegador **Internet Explorer** pedirá que se especifique en una sola pantalla la longitud de la clave y el protocolo de encriptación utilizado para generar las claves.

- **Proveedor:** En el caso de *certificados para dispositivo seguro*, el protocolo de encriptación corresponde con el driver del proveedor de la Smart Card.
- **Longitud de Clave.** Este parámetro permite escoger la longitud de la clave a generar. Esta longitud debe coincidir con la Longitud especificada por la política de certificación.
- **Añadir a una tarjeta de identificación electrónica Mejorada.** Esta opción la proporciona Internet Explorer, pero no se debe seleccionar.
- **Si es posible, hacer la clave exportable.** Este parámetro es obligatorio para certificados en formato Software. En el resto de soportes (Smart card o dispositivo seguro centralizado) es indiferente si se marca o no, porque nunca será exportable.

Una vez especificado estos parámetros se inicia el proceso de generación con el botón  **Generar**.

Para saber más sobre lo especificado en las políticas de certificación, consultar la información actualizada en la web de ACEDICOM: [acedicom.edicomgroup.com](http://acedicom.edicomgroup.com)