CryptosecOpenKey
TSA

Manual de usuario
Rev. 2.0.2843

REALIA TECHNOLOGIES, SL 14 de enero de 2025

Version	Fecha	Componentes	Breve descripcion del cambio
1.0.0	04/07/2014	Todo	Versión inicial
1.0.1	12/12/2018	Documentación	Cambio a formato LaTeX
1.0.2	11/02/2020	RA	Interfaz de usuarios y aprobacion de certificados
1.0.3	23/11/2020	TSA	Informes XLS y autenticación de usuarios
1.0.4	08/07/2021	WS	Web Services de la RA
1.0.5	10/11/2021	Todo	Restauración
1.0.5-2762	02/02/2022	RA	TLSv.x en la configuración SMTP
2.0.2774	17/02/2022	Todo	Archivar datos

Cuadro 1: Control de versiones

Índice

1. Introducción

CryptosecOpenKey es un appliance que cuenta con Hardware y Software Criptográfico (HSM) integrados en un solo dispositivo para generar los Certificados Digitales en una estructura de clave única (PKI).

El servidor tiene dos puertos Ethernet y contiene en su interior un HSM Cryptosec 2048 (Certificación FIPS 140-2 level-3), que garantiza el almacenamiento seguro de las claves (Fig. 1).

El producto CryptosecOpenKey TSA ofrece un servicio de generación de sellos de tiempo a través del protocolo http según el estándar [RFC3161].

Figura 1: Vista frontal servidor CryptosecOpenKey

2. Administración

Antes de poner en marcha el sistema es necesario inicializar el servicio, para ello habría que crear los certificados internos, también hay que editar las políticas ya que vienen configuradas unas políticas por defecto. Finalizada la instalación, el sistema está preparado para dar el servicio de generación de sellos de tiempo conforme al estándar [RFC3161] mediante el servicio TSP (Ver sección 3), administrando los servicios de TSA a través de la interfaz de administración Web entre otras funcionalidades que se detallarán más adelante.

2.1. Asistente de instalación

Para acceder a la administración web se utilizará un navegador en un puesto cliente que esté conectado punto a punto al servidor. El proceso de instalación dependerá en algunos pasos en función del navegador seleccionado.

Antes de comenzar el proceso de instalación será necesario registrar en Java la URL del servidor como sitio de confianza. En Windows basta con acceder al panel de control de Java y seleccionar la pestaña Seguridad. En esta pestaña se activará el contenido de Java en el explorador y se añadirá a la lista de sitios de confianza la URL del servidor Fig. 2.

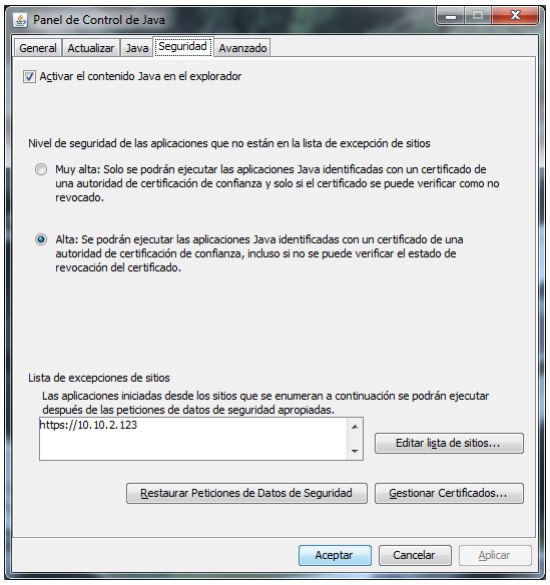


Figura 2: Pestaña de seguridad del panel de control de Java en Windows 7.

En el caso de que se utilice el navegador Internet Explorer será necesario añadir también a los sitios de confianza del navegador la URL del servidor. Para ello se accede a la ventana de Opciones de Internet y se selecciona la pestaña Seguridad. Pulsando en el botón Sitios se podrá modificar la lista de sitios de confianza del navegador (Fig. 3). Además será necesario configurar un nivel de seguridad para esta zona que permita la descarga de ActiveX no firmados.

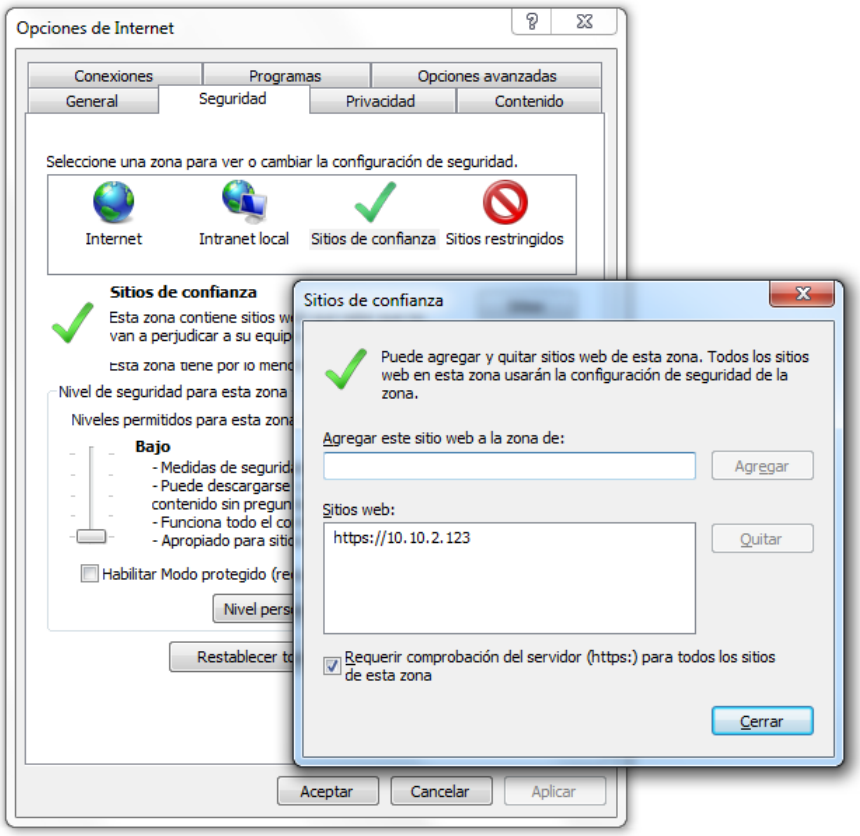


Figura 3: Configuración de sitios de confianza de Internet Explorer.

Una vez configurado el equipo cliente, se introduce en el navegador la URL `https://IP_servidor/CryptosecOpenKey/`, dónde IP _servidor es la dirección ip por defecto del equipo indicada por REALSEC.

Al acceder a la interfaz por primera vez, podemos apreciar la pantalla de creación de certificado de Mini CA (Fig. 4), además, la aplicación viene con unas autopolíticas configuradas por defecto, normalmente será necesario sustituir estas políticas, para ello se presiona el botón Editar Políticas, donde aparecerá la ventana de políticas y se deberá importar el fichero XML de las autopolíticas válidas.

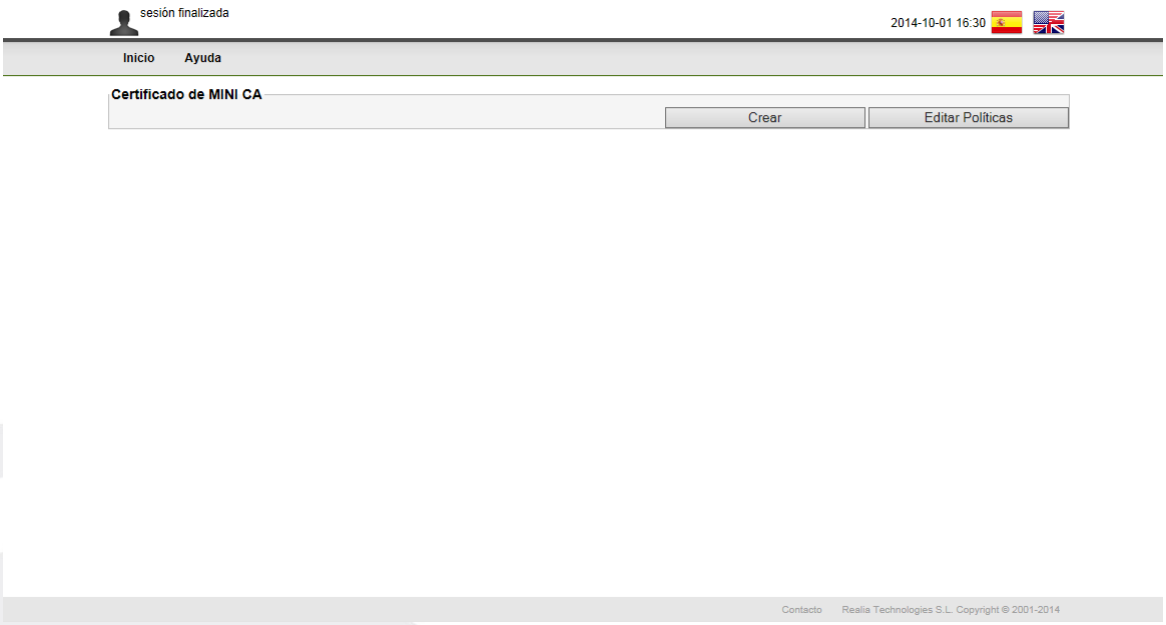


Figura 4: Pantalla para generar el certificado de MiniCA.

Una vez configuradas las autopolíticas, creamos el certificado de MiniCA, para ello, debemos presionar el botón Crear, y el sistema nos muestra la siguiente pantalla (Fig. 5), en la cual nos muestra la información previa al certificado de Mini CA.

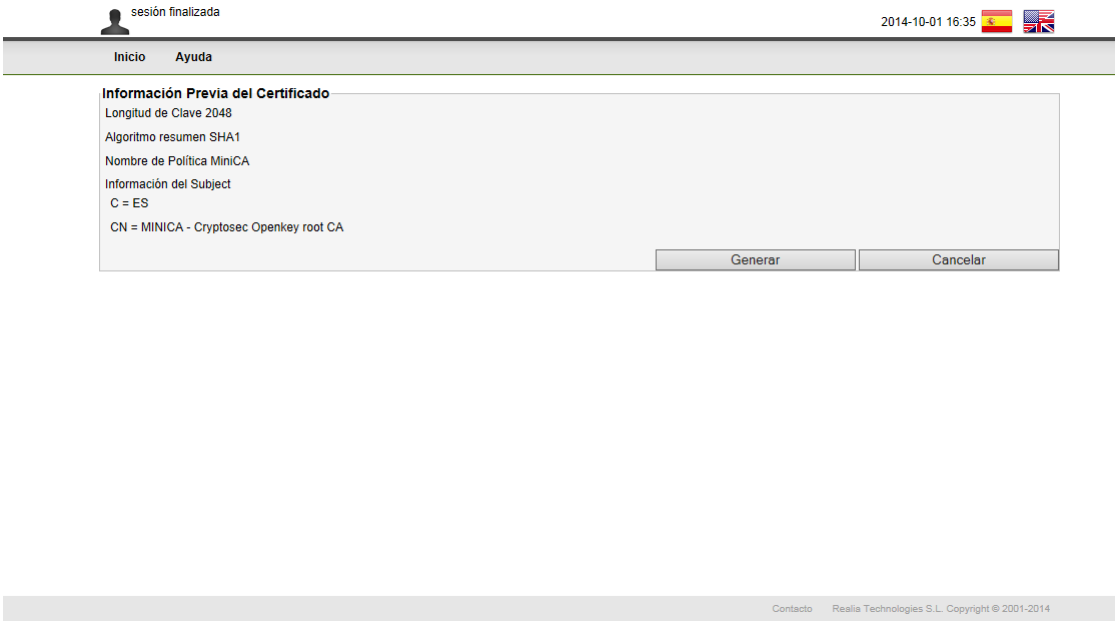


Figura 5: Pantalla de información previa del certificado de MiniCA.

Presionamos el botón Generar y el sistema nos muestra la pantalla a través de la cual podemos descargarnos y ver el certificado, el cual tenemos que instalárnoslo en el equipo, para ello se presiona sobre Bin o PEM (Fig. 6) y le damos a instalar certificado. Una vez que el certificado ha sido instalado, presionamos el botón continuar.

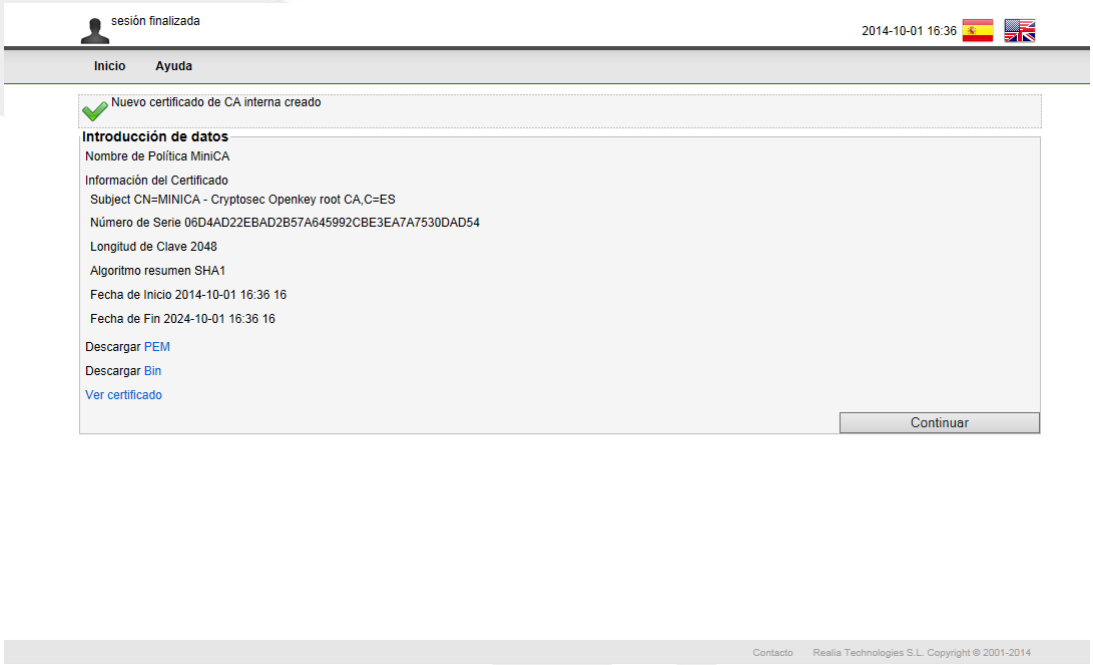


Figura 6: Pantalla de descarga y visualización del certificado.

A continuación, el sistema nos muestra la pantalla de creación de certificados de operador (Fig. 7), para ello hacemos click sobre el botón crear. Tras esto, el sistema nos muestra la pantalla con la información previa del certificado (Fig. 8) y presionamos sobre el botón Generar. En caso de tener configuradas variables en la política, antes de mostrarnos la información del certificado,

se nos mostraría un formulario con los campos correspondientes a las variables configuradas, el cual deberemos completar asignándole a cada una de ellas el valor deseado.

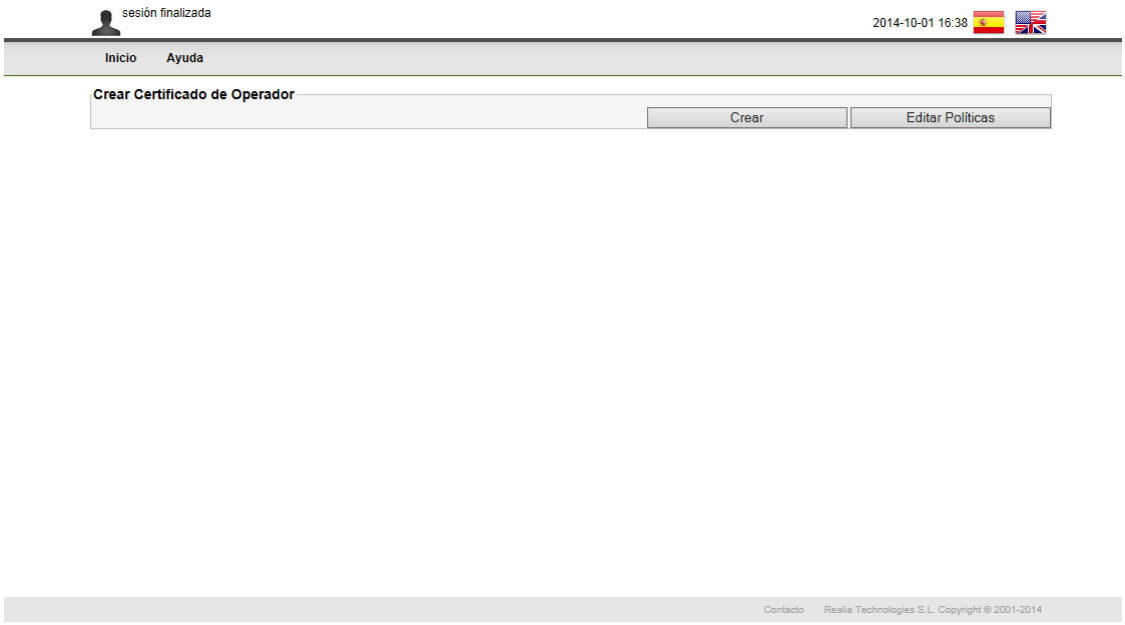


Figura 7: Pantalla para crear el certificado de Operador.

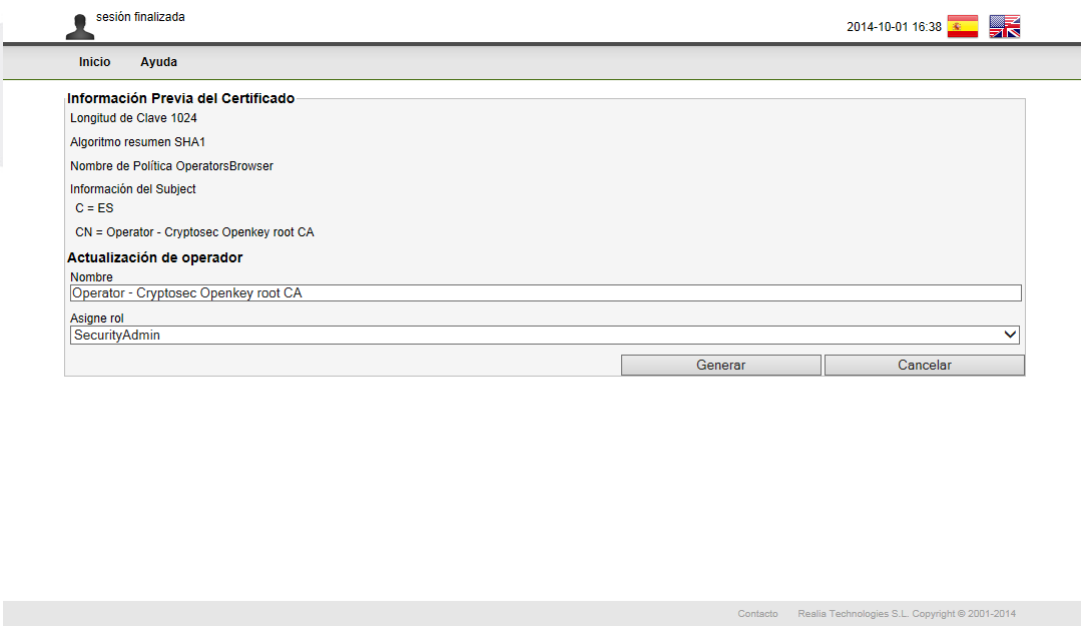


Figura 8: Información previa del certificado de Operador.

Una vez creado el certificado de operador (en caso de estar usando el navegador Firefox, el siguiente paso se omite), tenemos que seleccionar el proveedor de criptografía que mejor se adecue a nuestras necesidades (Fig. 9), para que nos aparezcan los proveedores de criptografía, debemos tener la ruta en sitios web de confianza, y una vez seleccionado el mismo, presionamos el botón Generar, tras esto, el sistema nos muestra una pantalla a través de la cual podemos descargarnos y ver el certificado de operador (Fig. 10).

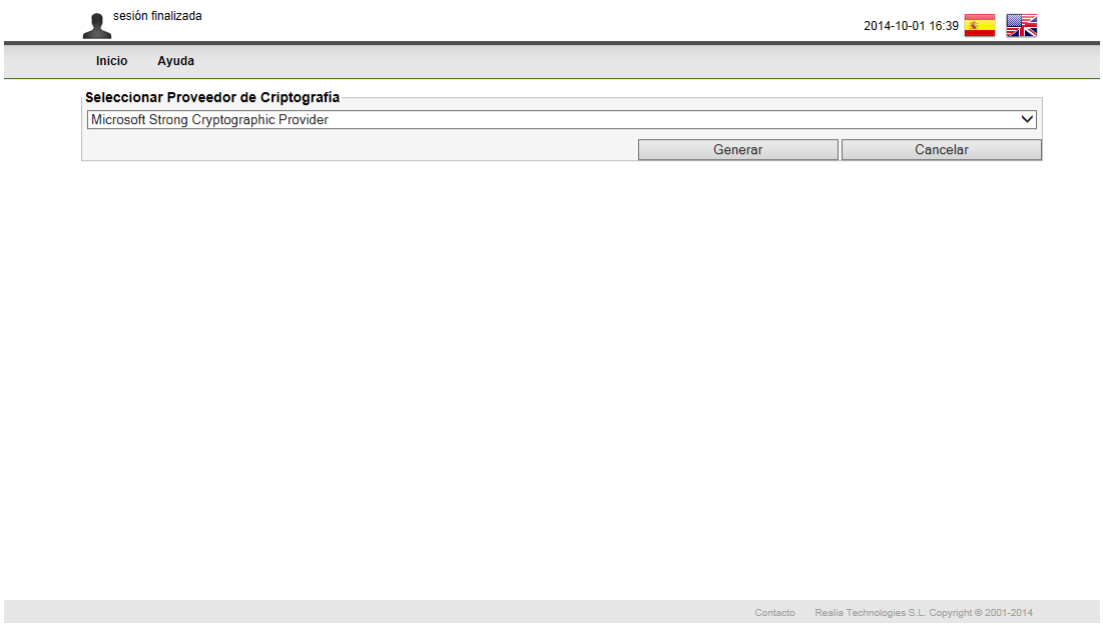


Figura 9: Pantalla para seleccionar el proveedor de criptografía (en caso de usar Firefox, esta pantalla no aparece).

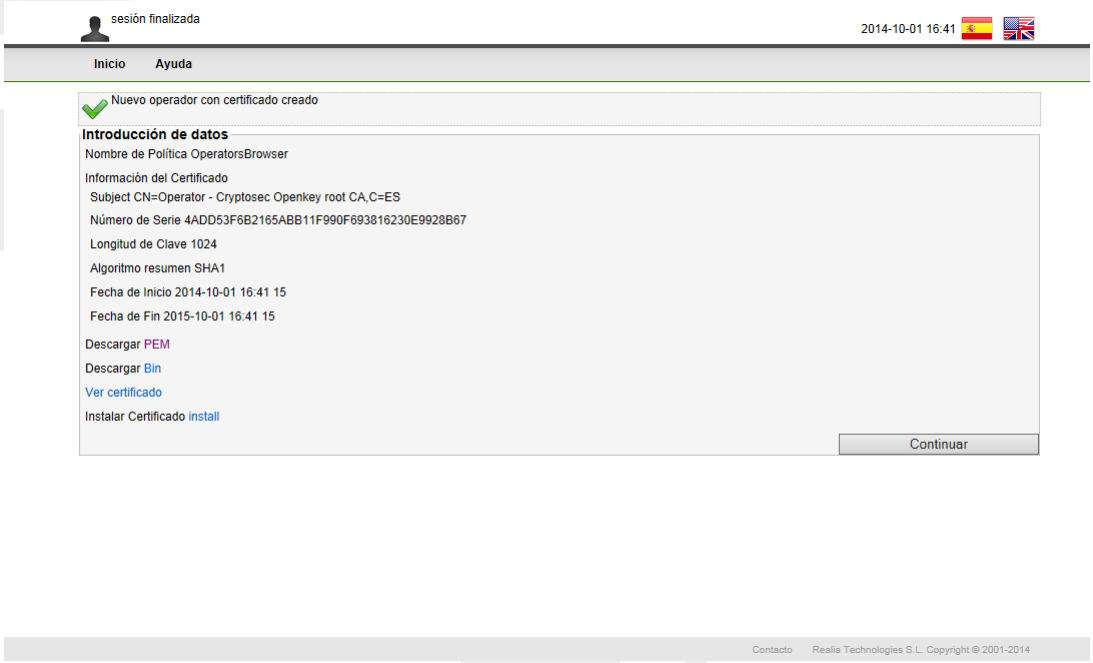


Figura 10: Pantalla para ver y descargar el certificado de operador.

Una vez creado e instalado el certificado de operador (se instala de forma automática), el sistema nos muestra la pantalla de creación de certificado de servidor web (Fig. 11) y presionamos el botón Crear, posteriormente el sistema nos muestra la información del certificado (Fig. 12), hacemos click sobre el botón Generar, en la pantalla siguiente, podemos descargarnos y ver el certificado, el cual se instala automáticamente y seleccionamos Continuar (Fig. 13).

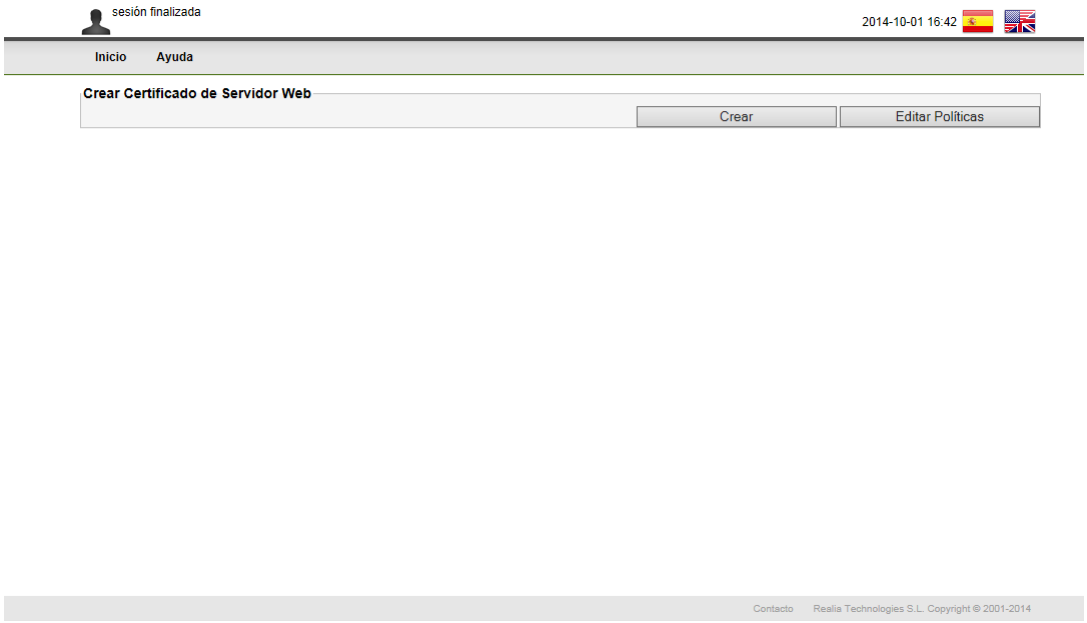


Figura 11: Pantalla para crear el certificado de Servidor web.

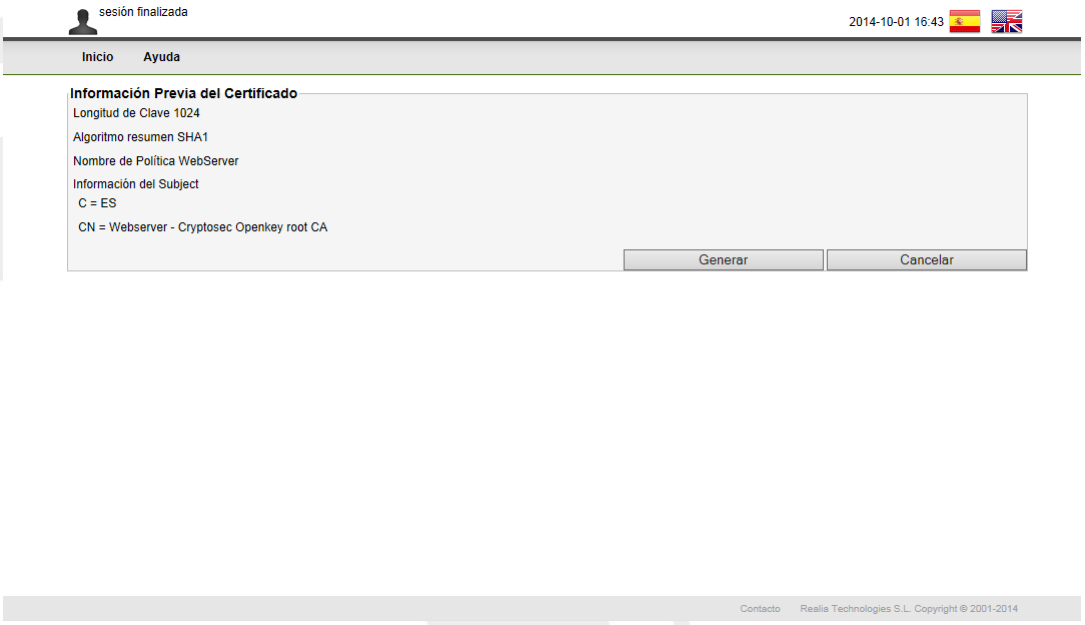


Figura 12: Información previa del certificado de Servidor Web.

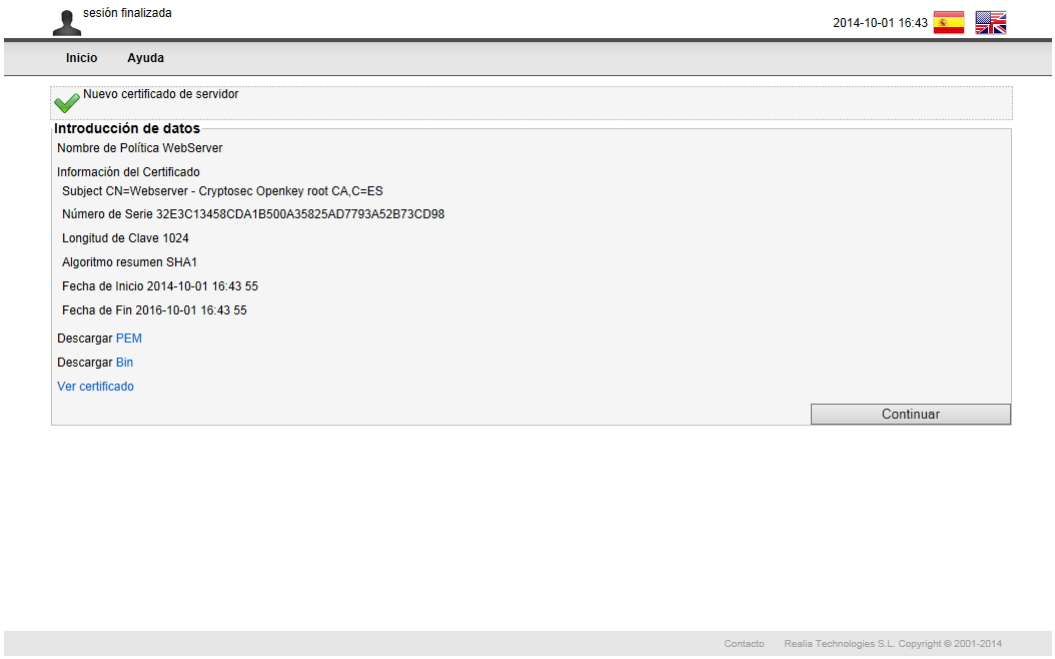


Figura 13: Pantalla para ver y descargar el certificado de servidor web.

Por último, será necesario reiniciar el servidor para completar el proceso de inicialización. Eston se consigue pulsando el botón continuar en la pantalla mostrada en la Fig. 14.

Figura 14: Pantalla de finalización del proceso de inicialización.

2.2. Administración web

Finalizada la fase de inicialización del servidor, en la pantalla que se nos muestra, aceptamos las advertencias y presionamos el botón Ver Certificados (Fig. 15), aceptamos la advertencia y si pulsamos sobre el desplegable, nos aparece una lista con los certificados de acceso que tenemos instalados, debiendo seleccionar el certificado que utilizaremos para autenticarnos, presionando posteriormente el botón Autenticar. En este punto el único certificado que tendremos disponible es el de operador, ya que acabamos de finalizar el proceso de inicialización.

Figura 15: Pantalla de selección de certificados de interfaz de administración.

En caso de tener asignado más de un rol para dicho usuario, el siguiente paso es la selección del rol con el que queremos acceder (Fig. 16), para ello presionamos el desplegable y nos aparecen los diferentes roles que tenemos disponibles para el certificado seleccionado (Fig. 17), seleccionamos aquel con el que queremos acceder y presionamos sobre el botón Continuar. En caso de tener asignado un único rol como es el caso de acabar de inicializar, se omite este paso.

Figura 16: Pantalla de selección de rol de interfaz de administración.

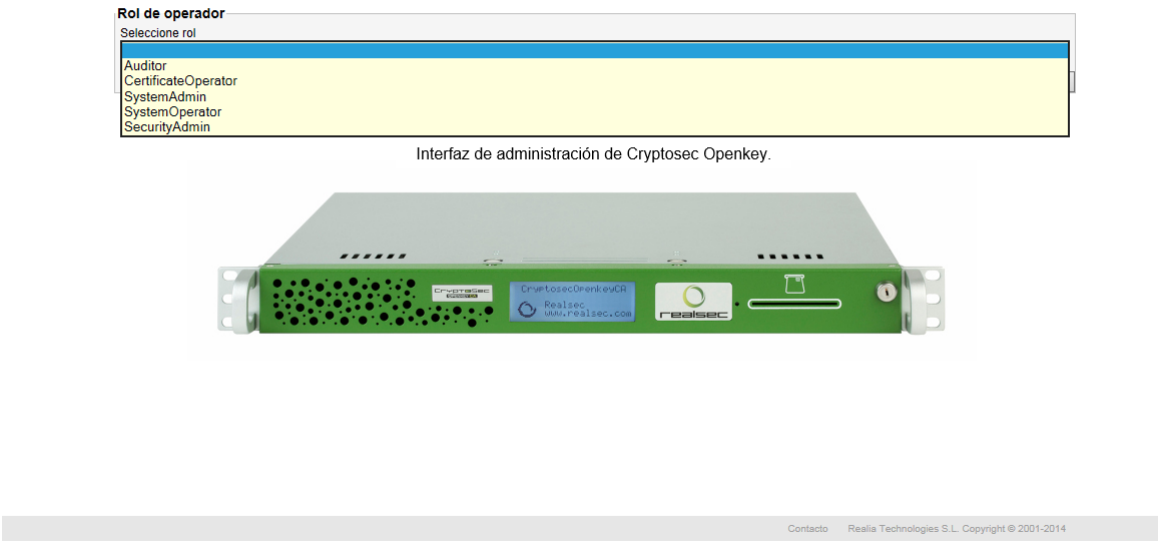


Figura 17: Pantalla con los roles disponibles para el certificado instalado.

Así podremos acceder con diferentes permisos según los certificados que tengamos instalados. Los roles disponibles que encapsulan las operaciones habilitadas son:

- Auditor: Autorizado para ver los datos generados por la TSA (certificados emitidos, sellos de tiempo, operadores) y las trazas de las operaciones realizadas (logs).
- Administrador de Sistema (SystemAdmin): Están autorizados para instalar, mantener y configurar el Software de los equipos de la TSA siempre y cuando no afecte a la seguridad del mismo.
- Administrador de Seguridad (SecurityAdmin): Tiene la responsabilidad general para la administración del Software de los equipos de la TSA siempre que afecten a la seguridad.
- Operador de sistema (SystemOperator): Tiene la responsabilidad de monitorizar los equipos de la TSA y realizar operaciones de mantenimientos.

Entre las operaciones principales que podemos encontrar en la interfaz de administración se enumeran las siguientes, que se detallarán más adelante en el punto que corresponda:

1. Consulta de sellos de tiempo emitidos.
2. Provisión de hora a los equipos de los otros componentes de Realsec.

2.2.1. Administración web para el rol Administrador de Seguridad

Mediante el rol administrador de seguridad, se pueden configurar los parámetros que condicionan el funcionamiento de los elementos software específicos de la TSA que afectan a la seguridad del sistema. Entre estas funcionalidades se encuentran la gestión de políticas de certificación, configuración de certificado de TSA, de restauración de claves, configuración de acceso al sistema operativo, copia de seguridad de datos, restauración de datos, consulta de certificados

internos, la gestión de acceso de los roles, la gestión de certificados de MiniCA, operadores o servidor.

2.2.1.1. Administración

Este menú proporciona distintas opciones relacionadas con la configuración de seguridad del componente TSA. Las operaciones permitidas en el menú administración son:

- Políticas de certificación.
- Certificado de TSA.
- Acceso S.O.
- Copia de seguridad de claves.
- Restauración.

Estas operaciones serán detalladas a continuación.

2.2.1.1.1. Políticas de certificación

- **Políticas de certificación (políticas internas)**

La opción Políticas de certificación permite editar las políticas internas correspondientes a la TSA. Al seleccionar la opción se accederá a una pantalla que mostrará el listado de las políticas (Fig. 18).

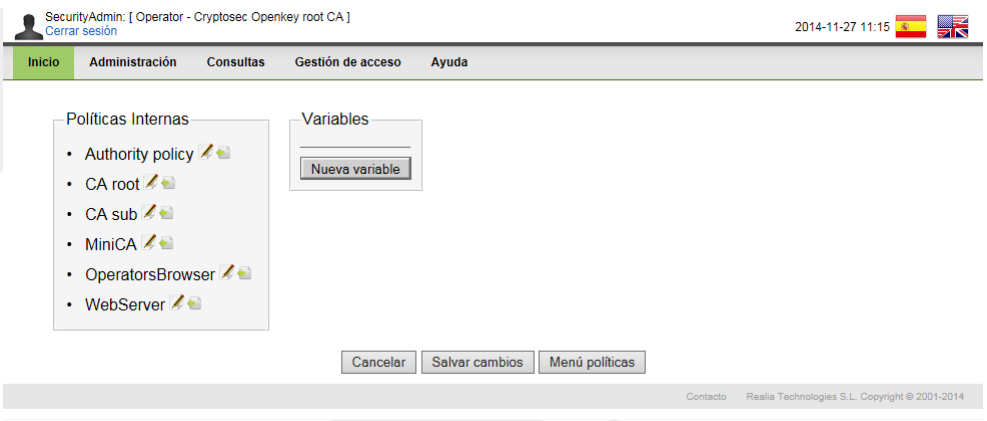


Figura 18: Pantalla de políticas de certificación y variables.

Mediante la opción 'Crear Política desde archivo XML', podemos importar políticas internas desde un archivo XML como muestra la (Fig. 19).

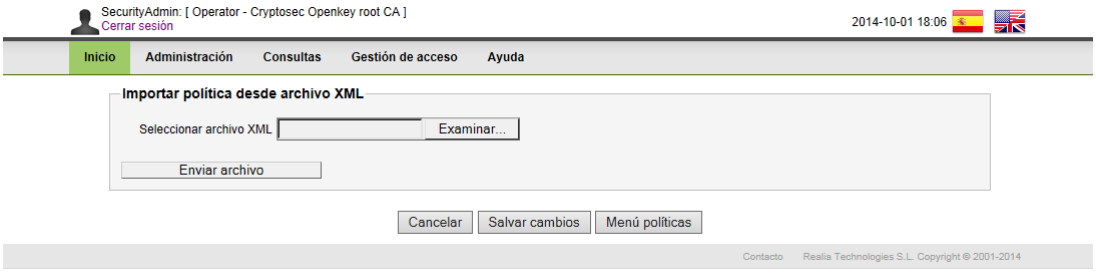


Figura 19: Pantalla para importar políticas internas desde XML.

Podemos también editar una política interna pulsando en el icono  a la derecha de cada política mostrada en (Fig. 18), una vez pulsado, aparece una pantalla como se muestra en la (Fig. 20).

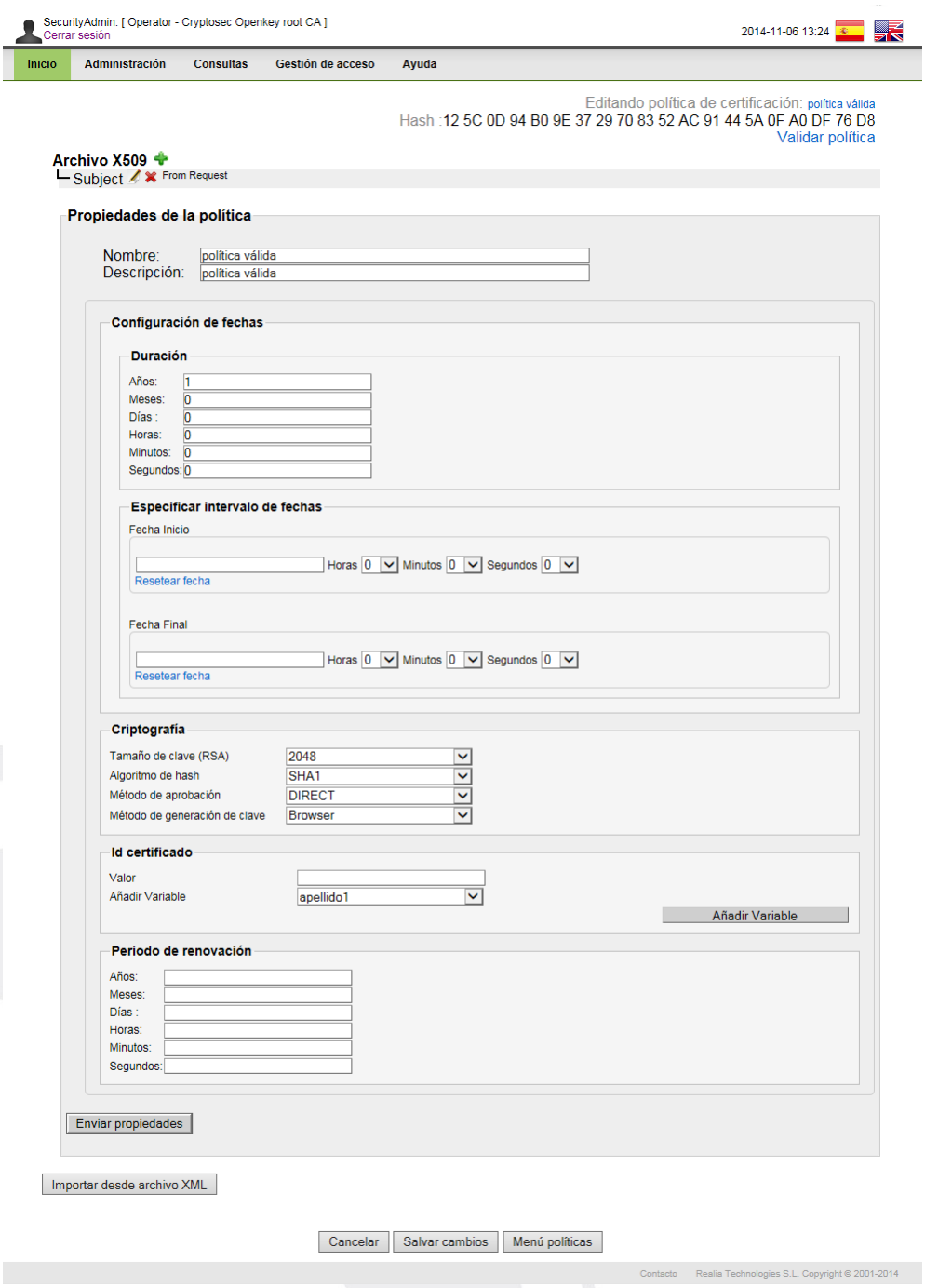


Figura 20: Pantalla con la información de la política.

Además, podemos ver si una autopolítica es válida o no, para ello seleccionamos editar una política , y nos muestra toda la información de la misma (Fig. 20), presionando sobre validar política podemos ver si es válida o no (Fig. 21 y Fig. 22 respectivamente). También se pueden exportar las autopolíticas como archivo XML, para ello pinchamos sobre el botón .

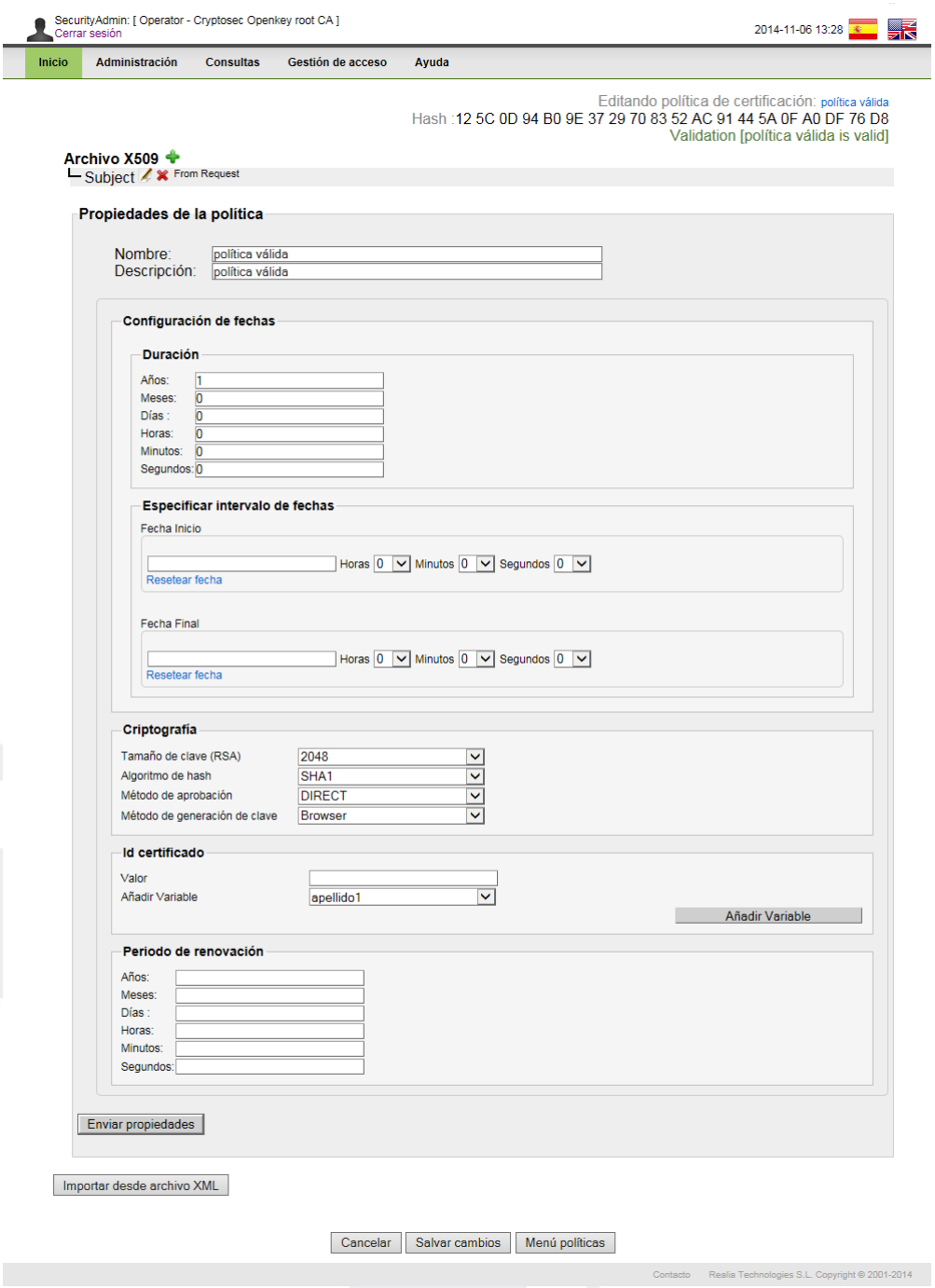


Figura 21: Pantalla con política válida.

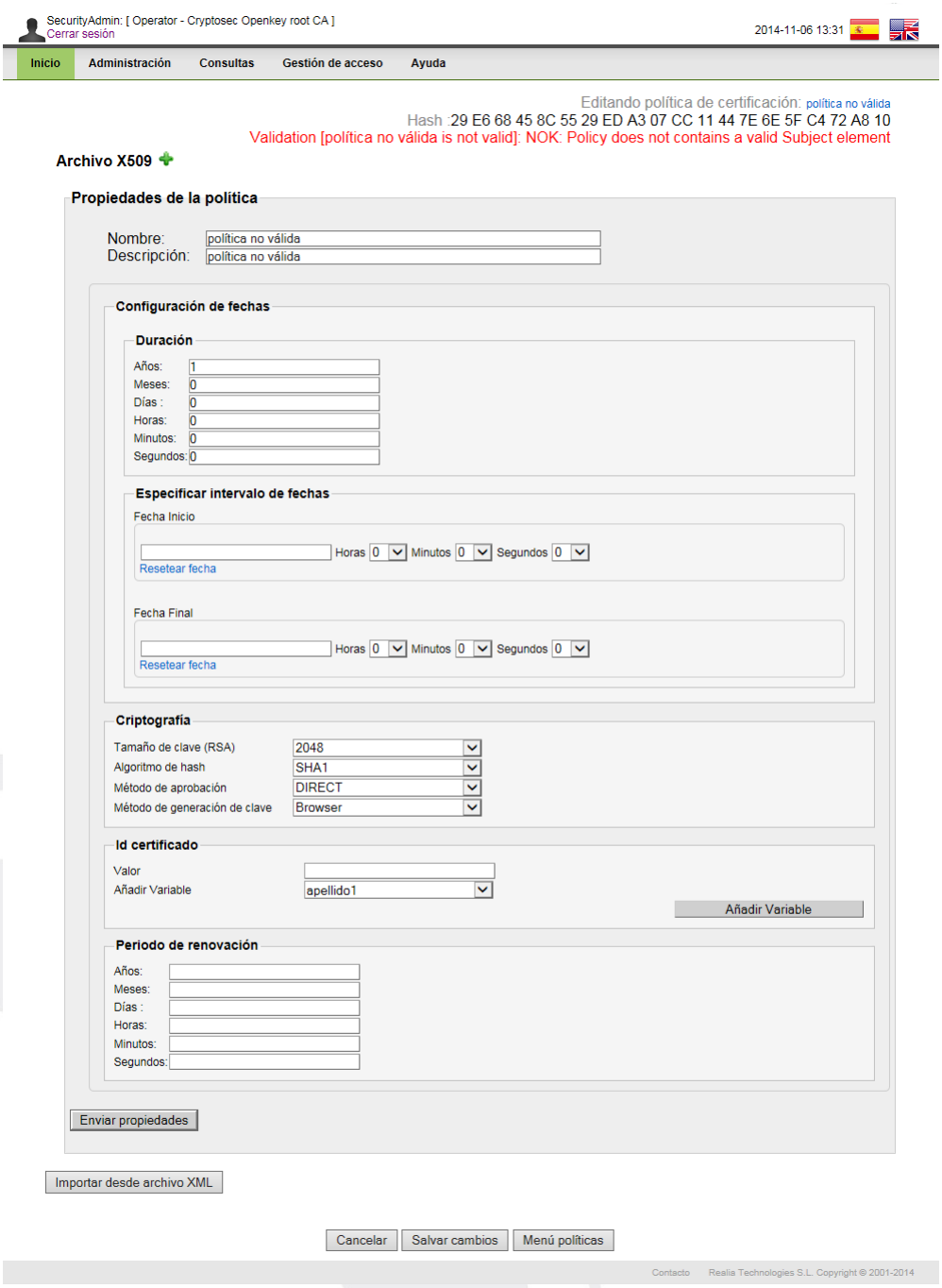


Figura 22: Pantalla con política no válida.

Para añadir un nuevo campo al certificado se pulsará el botón (). Aparecerá un menú desplegable con los tipos de campos disponibles (Fig. 23). Una vez seleccionado el tipo de campo que se desea añadir se accederá a una pantalla que permitirá añadir datos al nuevo campo (Fig. 24).

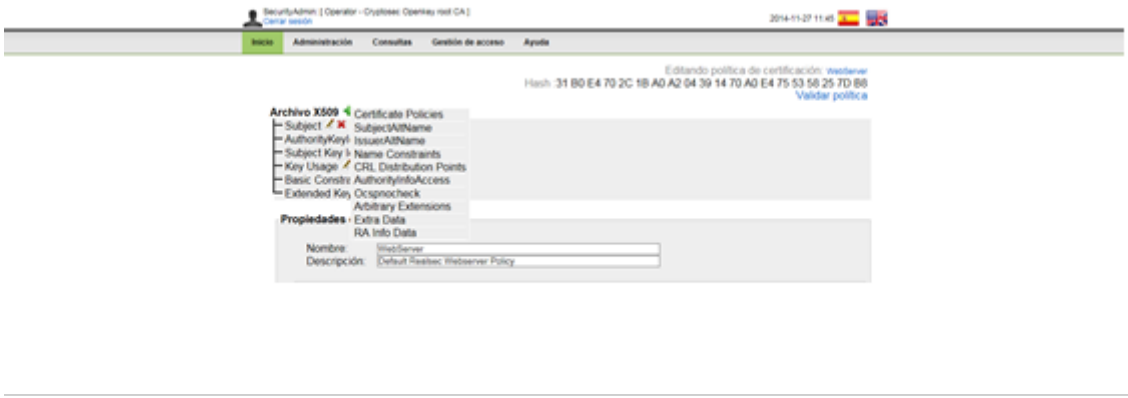


Figura 23: Selección de tipo de campo.

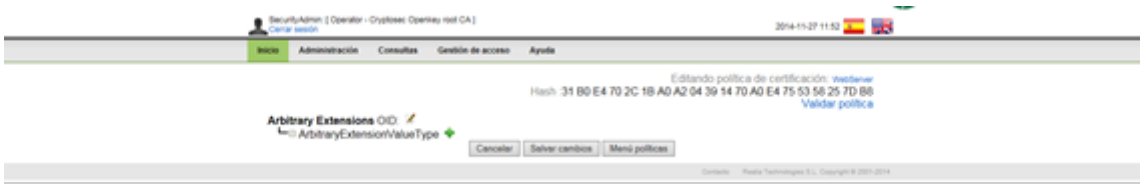


Figura 24: Pantalla de edición de campo.

- **Variables**

Mediante esta operación, se podrán crear nuevas variables, para ello debemos rellenar un formulario como el que se muestra en la siguiente figura (Fig. 25). Una vez completado, presionamos el botón Salvar variable y posteriormente el botón Salvar cambios.

La nueva variable aparecerá en el listado de variables que podemos apreciar en (Fig. 18).

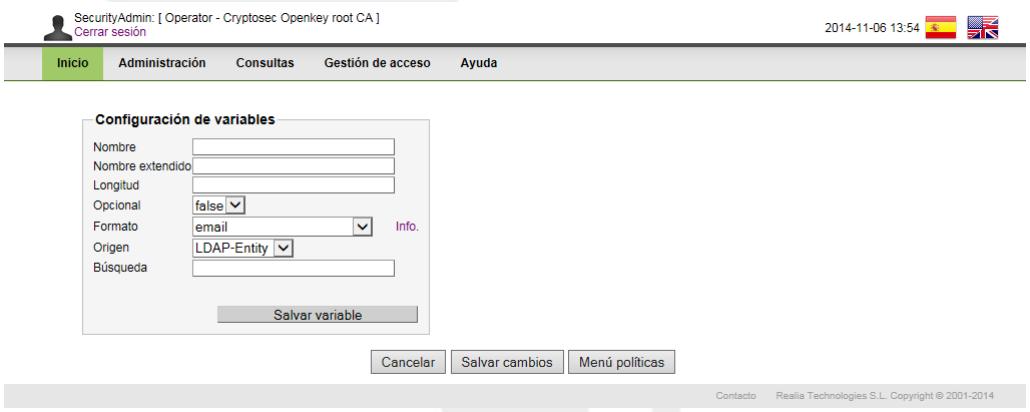


Figura 25: Pantalla para configurar nuevas variables.

También podemos editar variables, para ello presionamos el botón ( ), y nos aparece la siguiente pantalla, en la que además del formulario, nos muestra las políticas en las cuales se usa dicha variable. Una vez editado, se presiona el botón Salvar variable y nos muestra una pantalla con las políticas en las que se utiliza dicha variable en caso de que se use en alguna. En caso de que se use en algunas políticas, tenemos que seleccionarlas para que se actualice con la variable modificada. (Fig. 26).

Figura 26: Pantalla para editar las variables.

Además, podemos eliminar variables, para ello tenemos que presionar el botón ✖ y aceptar la advertencia mostrada (Fig. 27).

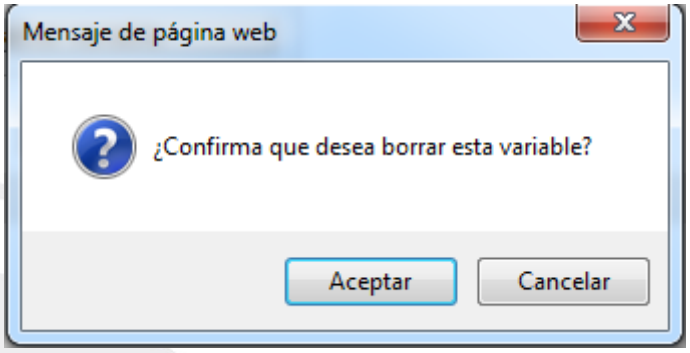


Figura 27: Pantalla de advertencia para eliminar variables.

2.2.1.1.2. Configuración de TSA

En este apartado, el administrador de seguridad puede configurar los datos de la TSA para la firma de sellos de tiempo (Fig. 28).

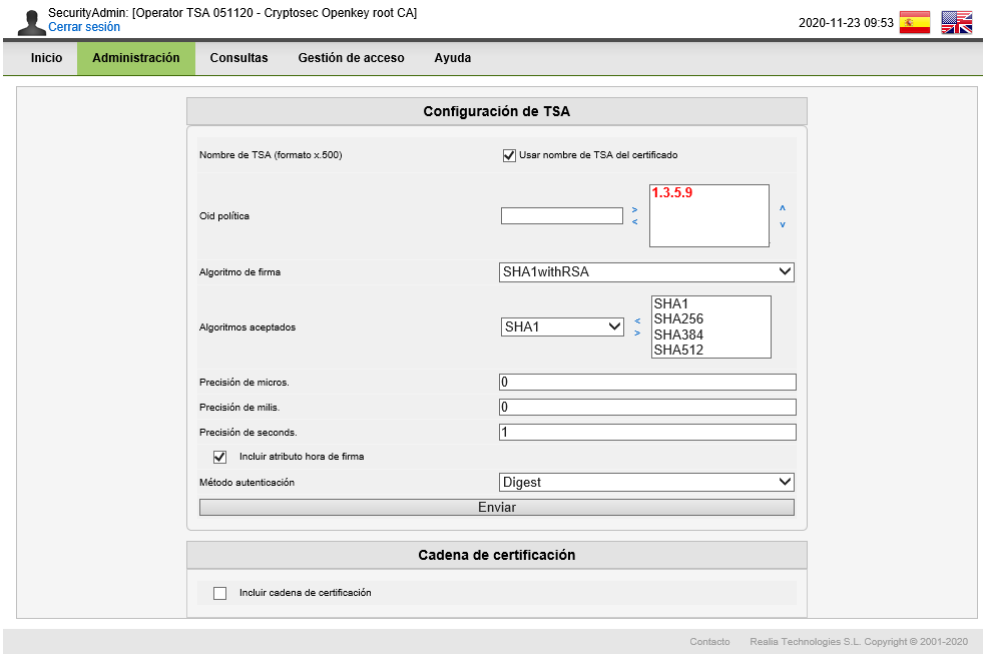
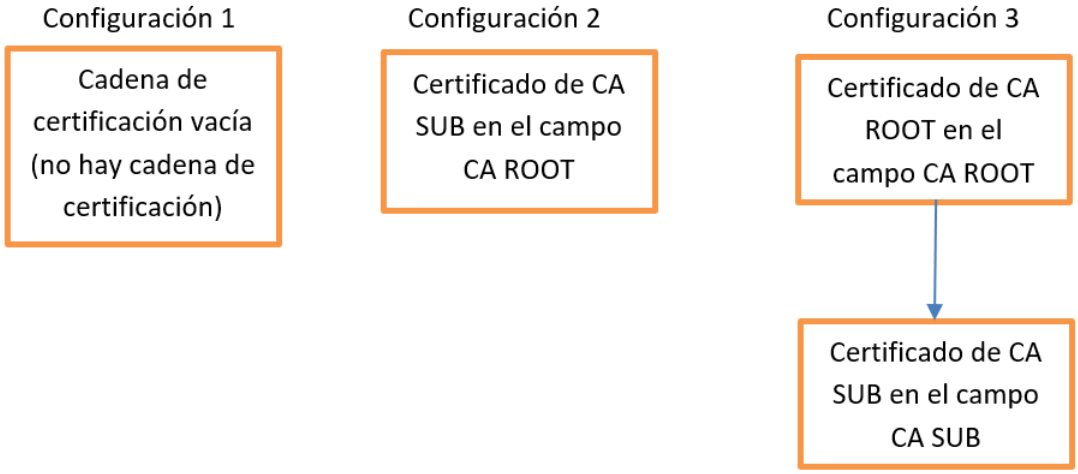


Figura 28: Pantalla de configuración de TSA.

Los parámetros que se pueden configurar son:

- **Nombre de TSA**: Se puede configurar que se use el atributo subject del certificado raíz en el sello de tiempo o bien se puede insertar un valor string en formato X500 (en caso de no cumplir este formato, se usará el valor del atributo subject del certificado). Si se configuran ambos valores, se dará preferencia al subject del certificado raíz.
- **OID de política**: Se refiere a los OID's de política admitidos en las peticiones de sellos de tiempo. En caso de no estar configurado este parámetro en la petición, el sello de tiempo en la respuesta será configurado con el primero de los OID's configurados.
- **Algoritmo de firma**: Algoritmo con el que se firma el sello de tiempo.
- **Algoritmos aceptados**: Algoritmos de hash soportados en las peticiones.
- **Incluir hora de la firma**: Define si se quiere o no incluir la hora de la firma en el sello de tiempo.
- **Método autenticación**: Permite establecer el tipo de autenticación HTTP (Basic o Digest) del servicio Timestamp cuando la autenticación de usuarios está activada.
- **Cadena de certificación**: Si se quiere o no incluir toda la cadena de certificación en el sello de tiempo. En caso afirmativo, se deberá configurar la cadena de certificación de los certificados de CA de los que hereda el certificado de TSA raíz, siendo obligatorio al menos el certificado de CA subordinada, que en caso de ir solo se configura en el campo CA ROOT del formulario. Dicho de otro modo, solamente una de estas configuraciones es válida:



2.2.1.1.3. Certificado TSA

Dentro de esta entrada del menú aparecerán las operaciones relativas a la configuración del certificado de TSA. Este es el certificado que firma los sellos de tiempo emitidos por el servicio TSP (sección 3).

El proceso requiere la generación de una solicitud de certificado PKCS10 que se utilizará para generar el certificado en la CA. Una vez obtenido el certificado se deberá importar en la TSA en la opción correspondiente.

- **Generación PKCS10**

El administrador de seguridad, genera un PKCS10 mediante el cual, se emitirá en la CA, el certificado de TSA. Para ello, debe seleccionar la longitud de clave privada y se presiona el botón Generar (Fig. 29).

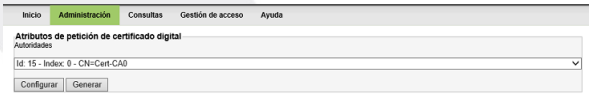


Figura 29: Pantalla para generar PKCS10.

- **Importar certificado**

En este apartado, debemos importar el certificado de TSA emitido a través de la CA Subordinada. (Fig. 30) mediante el pkcs10 generado en el punto anterior.

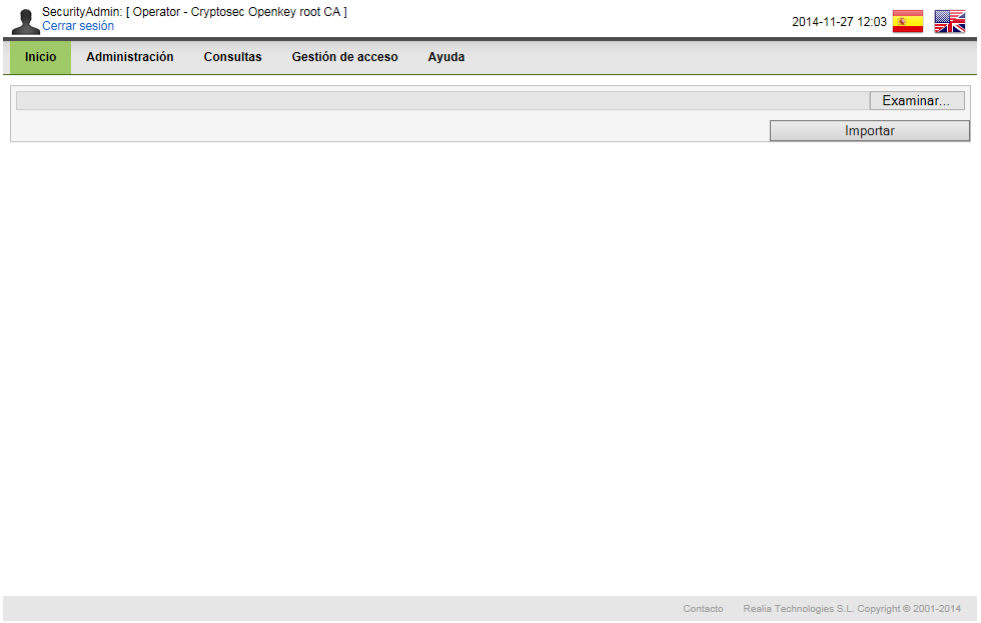


Figura 30: Pantalla de importación de certificado.

2.2.1.1.4. Acceso S.O.

La funcionalidad de esta operación es que el sistema nos permite proteger el sistema operativo mediante diversificación de contraseña del usuario administrador.

También se puede deshabilitar el SSH, para ello debemos presionar sobre . Una vez que se encuentre deshabilitado, debemos presionar para volver a habilitarlo. (Fig. 31)

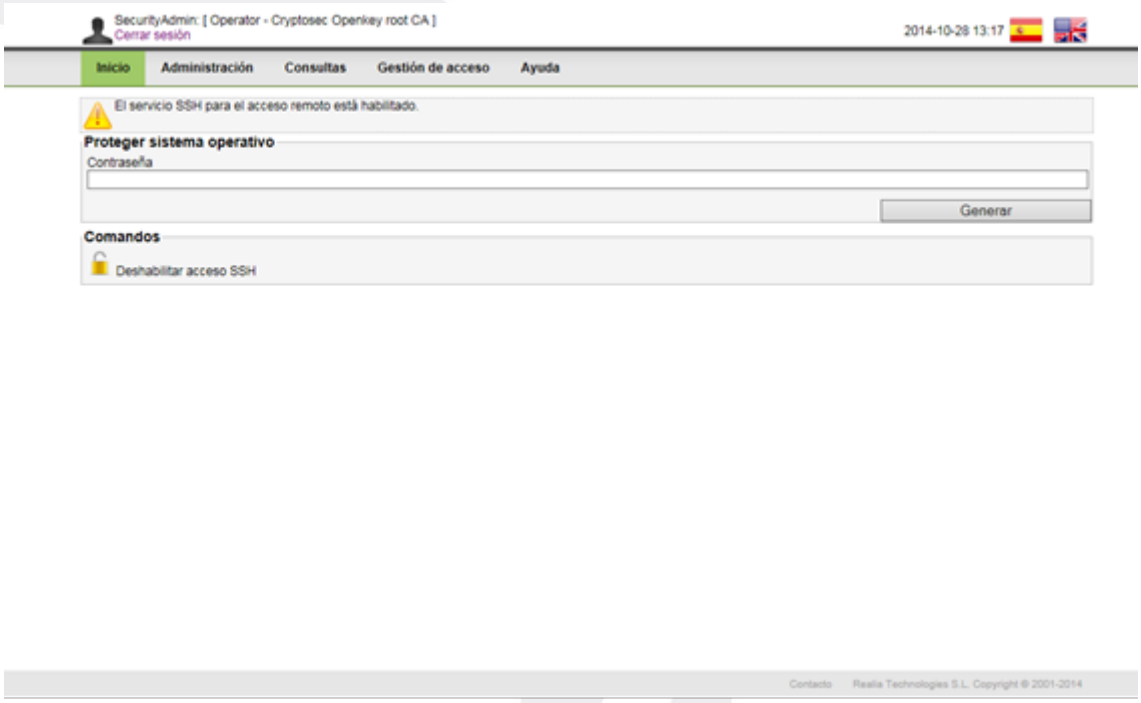


Figura 31: Pantalla de acceso al sistema operativo.

2.2.1.1.5. Copia de seguridad de claves

En esta sección, el administrador de seguridad puede generar y descargarse el fichero de backup de claves, para ello debe presionar el botón Generar para obtener el último backup de claves (Fig. 32) y posteriormente sobre Descargar (Fig. 33).

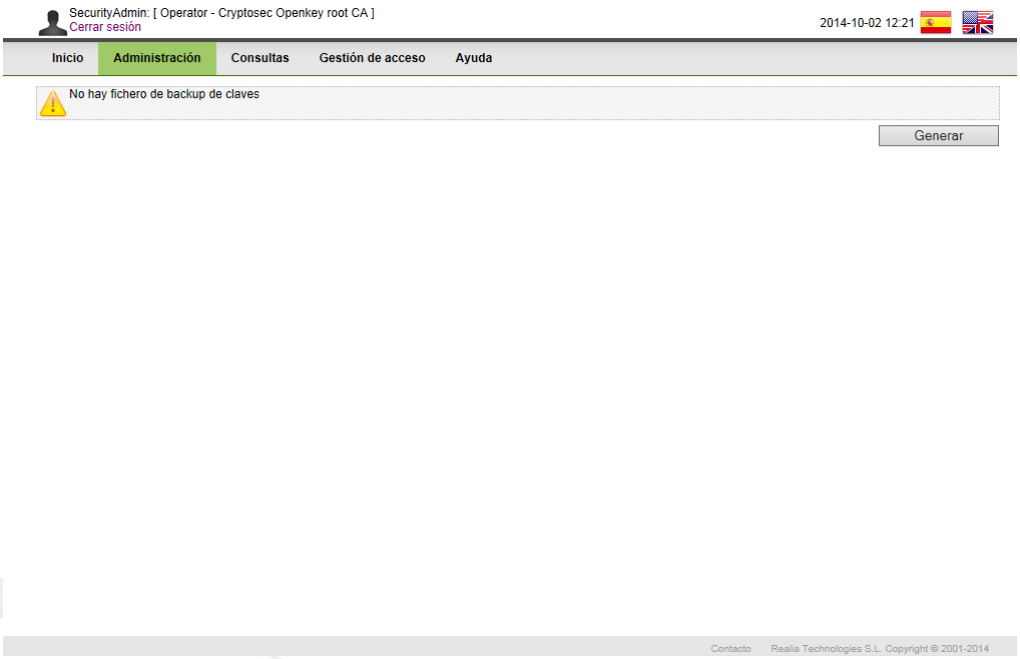


Figura 32: Pantalla para generar el backup de claves.

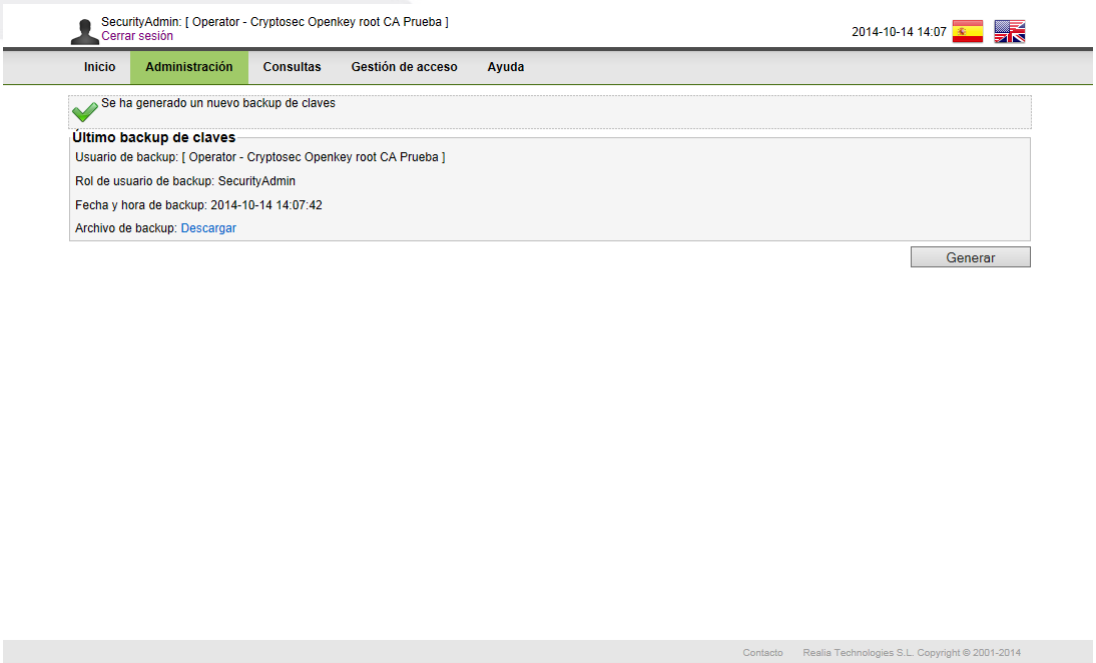


Figura 33: Pantalla para descargar backup de claves.

Cuando se procede a realizar una copia de seguridad de claves, las siguientes operaciones dejan de estar disponibles en la interfaz hasta que nuestra operación termine:

1. Otra copia de seguridad de claves.
2. Restauración.
3. Generación manual de un backup de datos.
4. Parar, iniciar o reiniciar los servicios de base de datos.

Hasta que nuestra operación de generación de backup haya terminado.

2.2.1.1.6. Restauración

El administrador de seguridad, en esta sección puede restaurar las claves, los datos o ambos (Fig. 34), para ello será necesario importar los backups que se desean restaurar. El backup de claves se puede descargar mediante la opción *Administración - Copia de seguridad de claves* explicada anteriormente y el backup de datos puede ser descargado por el Operador de Sistemas (opción Operaciones - Copia de seguridad de datos).

Figura 34: Pantalla de restauración.

Si se realiza una restauración SOLO de datos, presionamos sobre Examinar para buscar el .zip que contiene el backup y una vez adjuntado, presionar sobre Subir (Fig. 35).

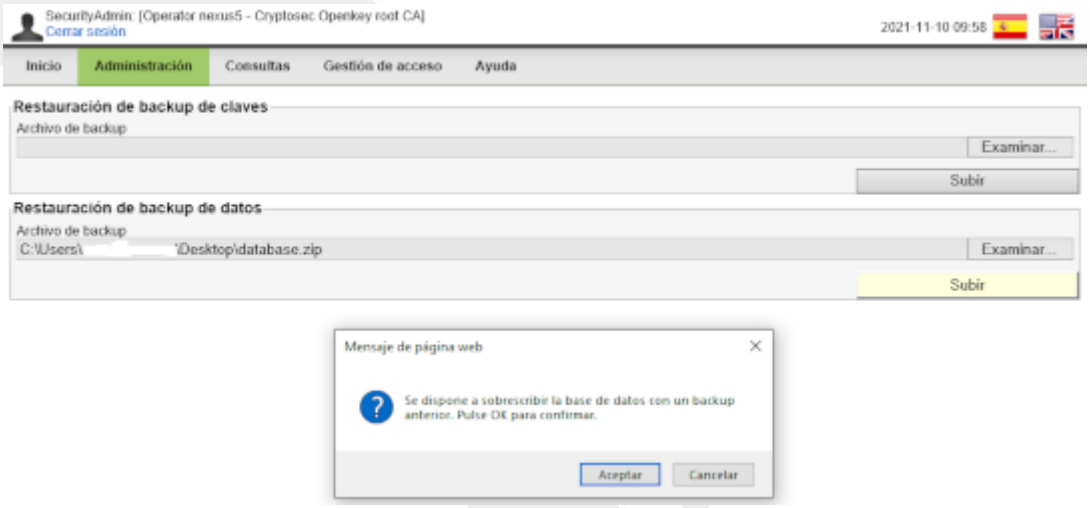


Figura 35: Restauración de datos.

Una vez subido el fichero zip de backup de datos, aparecerá la lista de archivos encriptados que componen los datos del backup (Fig. 36).

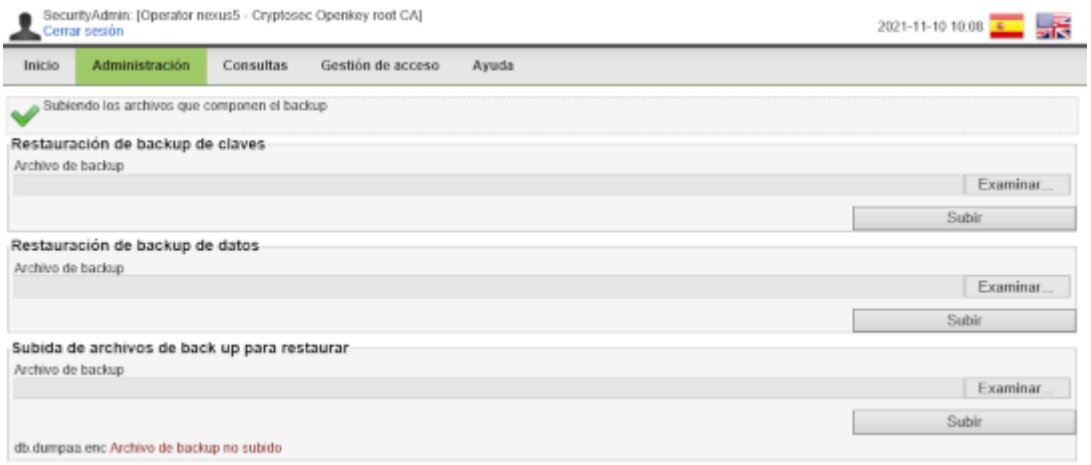


Figura 36: Subida de archivos del backup.

Vamos subiendo los archivos hasta que todos ellos tengan un mensaje en color verde informando que el archivo se ha subido, entonces nos aparecerá una nueva opción abajo diciendo restaurar (Fig. 37).

Figura 37: Subida de archivos del backup.

Si pulsamos el botón Restaurar, nos muestra una advertencia que debemos aceptar para que se proceda a la restauración y una vez realizada mostrará el resultado al terminar (Fig. 38).

Figura 38: Pantalla de éxito de restauración de datos.

En cambio, si se va a realizar una restauración INCLUYENDO las claves, al importar el fichero de claves el sistema informará que el servidor web será reiniciado tras el proceso (Fig. 39).

Figura 39: Restauración de claves.

Si pulsamos el botón Restaurar, tras finalizar la restauración el servidor web se reinicia automáticamente y se debe esperar varios minutos para asegurarnos que dicho reinicio ha terminado (Fig. 40).

Figura 40: Pantalla de éxito de restauración de claves.

Cuando se procede a una operación de restauración, las siguientes operaciones dejan de estar disponibles en la interfaz hasta que nuestra operación de restauración termine:

1. Otra restauración.
2. Generación de un backup de claves
3. Generación manual de un backup de datos
4. Parar, iniciar o reiniciar los servicios de base de datos.

Hasta que nuestra operación de restauración de backup haya terminado.

2.2.1.2. Consultas

2.2.1.2.1. Certificados internos

Mediante esta operación, el sistema muestra al administrador de seguridad una lista con los certificados internos (Fig. 41), presionando sobre ( ), podemos ver el cuerpo del certificado (Fig. 42), si presionamos sobre el ID, podemos ver el certificado y también podemos descargárnoslo, para ello debemos presionar (Fig. 43).

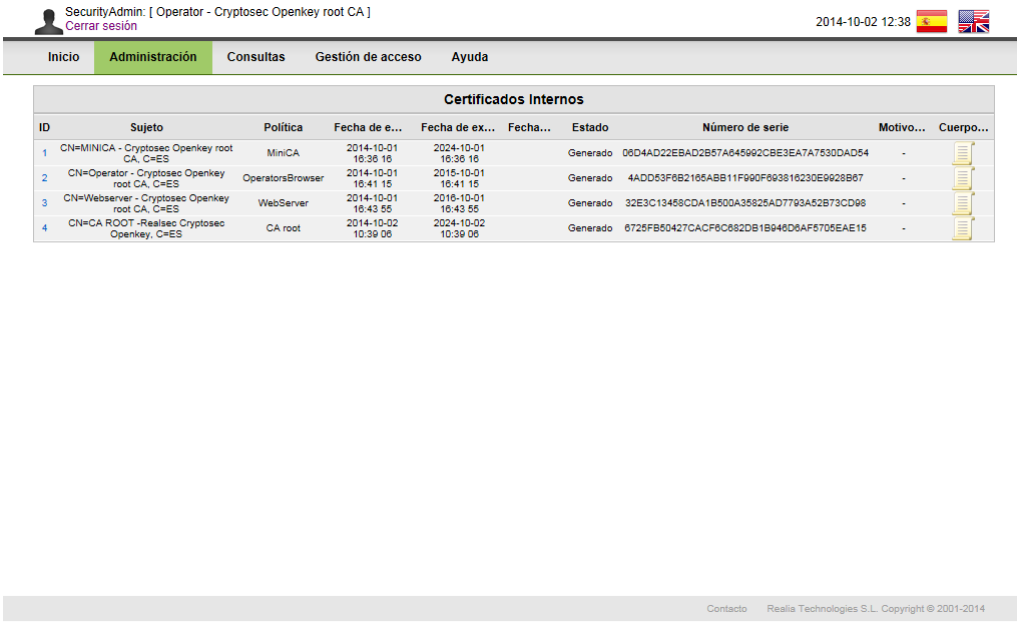


Figura 41: Pantalla de certificados internos.

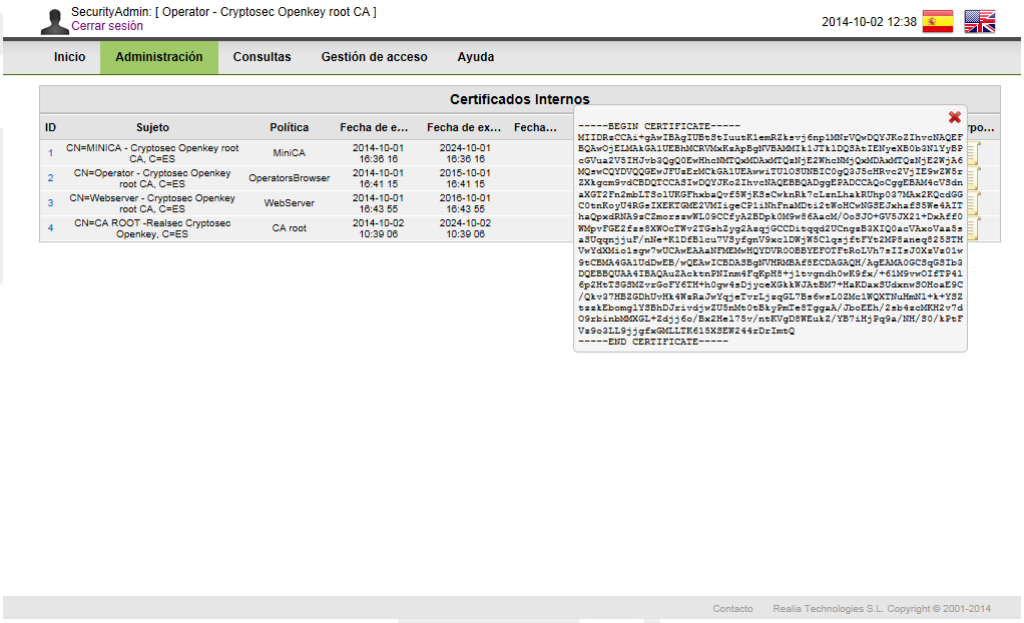
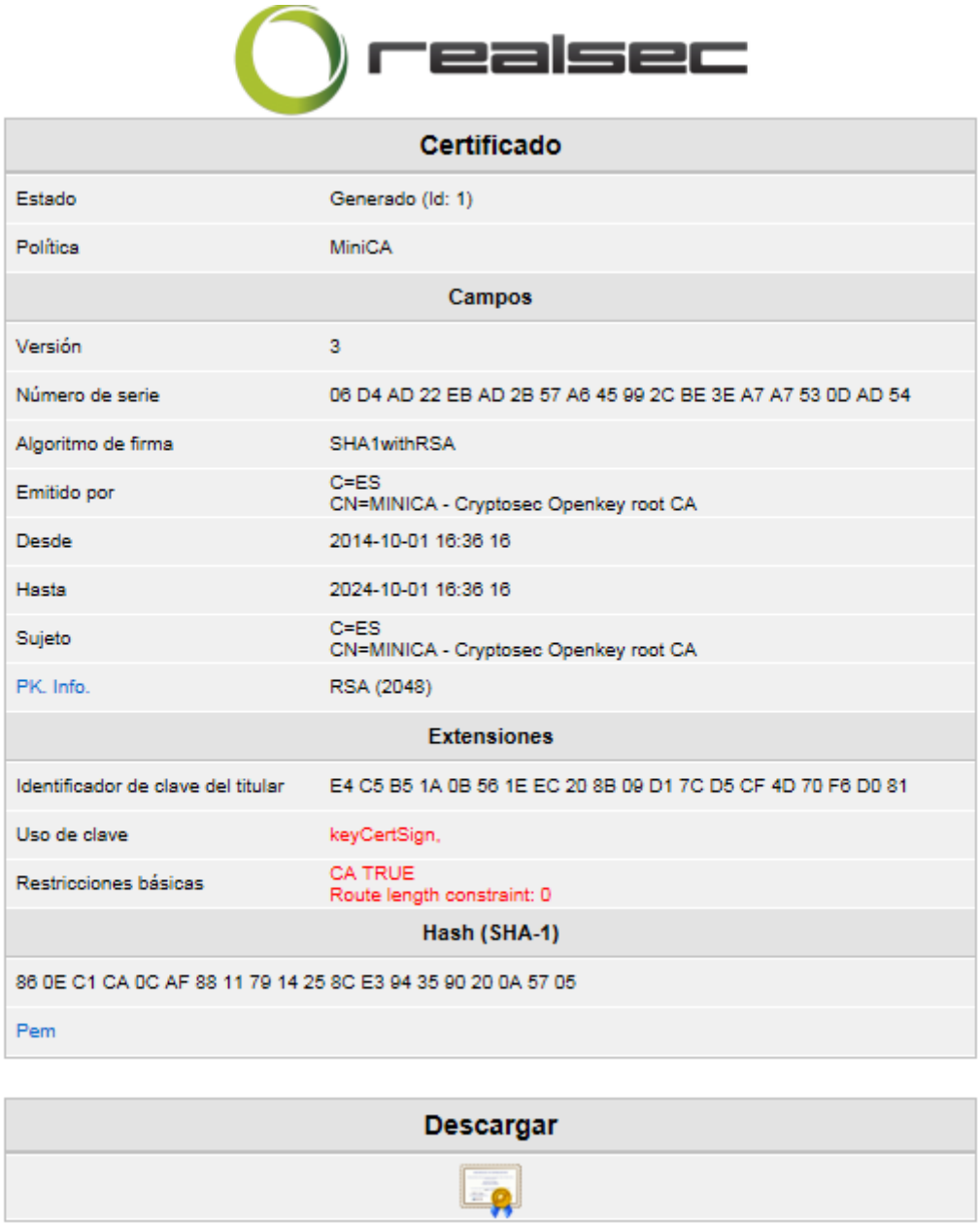


Figura 42: Pantalla con el cuerpo del certificado.



Certificado	
Estado	Generado (Id: 1)
Política	MiniCA
Campos	
Versión	3
Número de serie	06 D4 AD 22 EB AD 2B 57 A6 45 99 2C BE 3E A7 A7 53 0D AD 54
Algoritmo de firma	SHA1withRSA
Emitido por	C=ES CN=MINICA - Cryptosec Openkey root CA
Desde	2014-10-01 16:36 16
Hasta	2024-10-01 16:36 16
Sujeto	C=ES CN=MINICA - Cryptosec Openkey root CA
PK. Info.	RSA (2048)
Extensiones	
Identificador de clave del titular	E4 C5 B5 1A 0B 56 1E EC 20 8B 09 D1 7C D5 CF 4D 70 F6 D0 81
Uso de clave	keyCertSign,
Restricciones básicas	CA TRUE Route length constraint: 0
Hash (SHA-1)	
86 0E C1 CA 0C AF 88 11 79 14 25 8C E3 94 35 90 20 0A 57 05	
Pem	

Descargar

Figura 43: Pantalla con el certificado y la descarga del mismo.

2.2.1.2.2. Autoridades

Mediante esta operación, el sistema muestra al administrador de seguridad una lista con las autoridades disponibles para la emisisón de certificados, en el caso de la (Fig. 44) se muestran 3 autoridades una de ellas no materializadas aún.

Figura 44: Pantalla la lista de autoridades disponibles, en este caso hay 3.

2.2.1.3. Gestión de acceso

2.2.1.3.1. Roles

En esta sección, visualizamos los roles disponibles (Fig. 45), para poder acceder, así como una pequeña descripción de cada uno de ellos, el número de autenticaciones requeridas, y si está activo o no. Para editar su configuración debemos presionar sobre el icono correspondiente ( ) que nos llevará a una pantalla como la que se muestra en la Fig. 46, donde podremos seleccionar cuantas autenticaciones serán requeridas (multi-autenticación), así como activar/desactivar el rol, finalizando con el botón Actualizar.

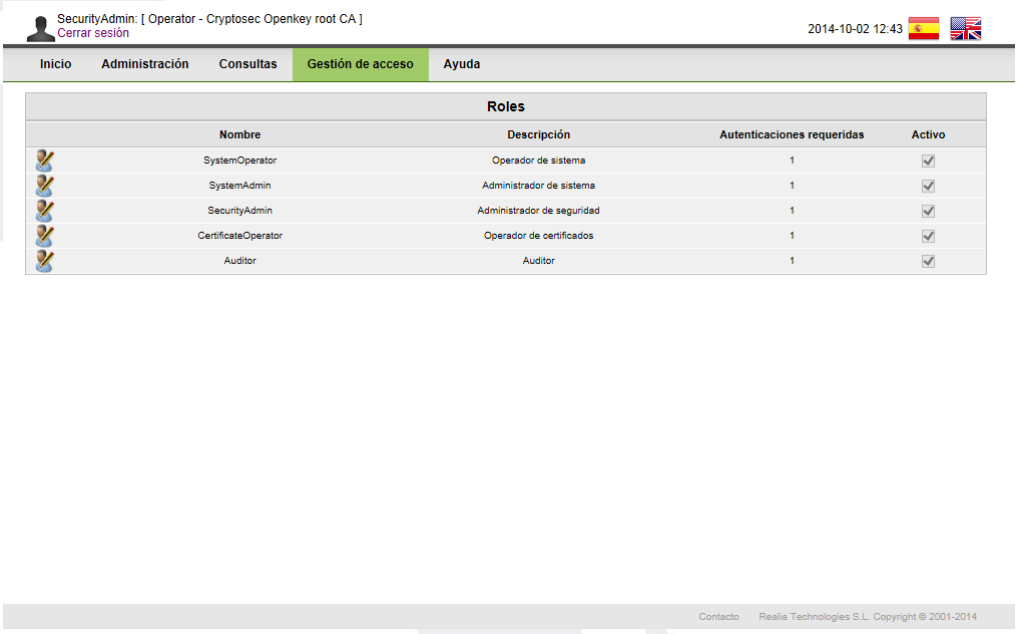


Figura 45: Pantalla de roles.

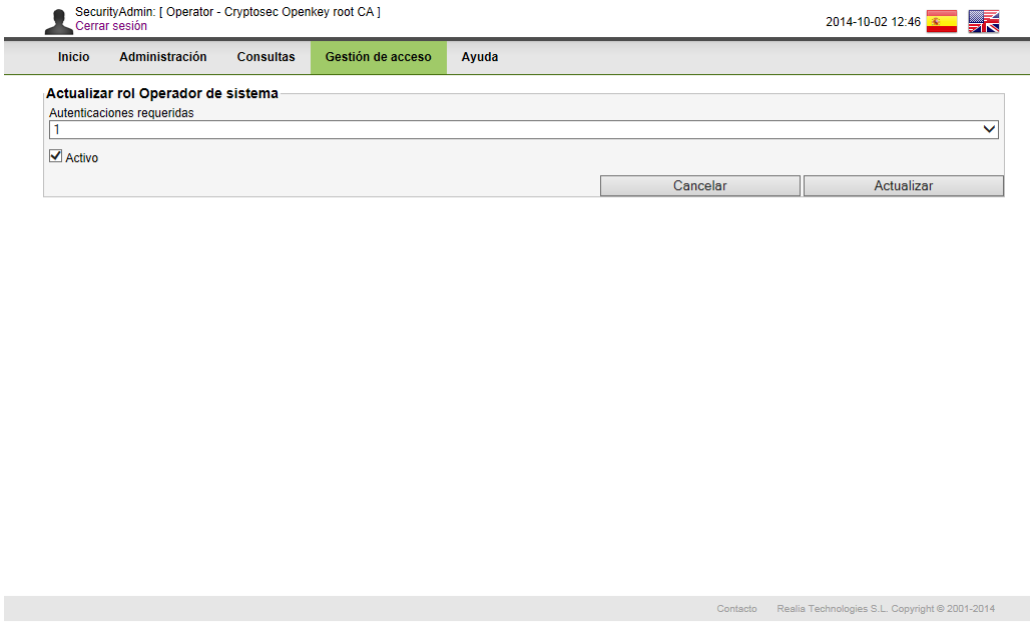


Figura 46: Pantalla de edición del rol.

2.2.1.3.2. Certificados de miniCA

- **Políticas de certificación**

En este apartado, igual que ocurre para Certificados de miniCA, certificado de servidor web y operadores, se podrán añadir, editar y eliminar los campos y extensiones de los certificados de miniCA, así como editar las propiedades de la política completando para ello el cuestionario de propiedades de la política. Una vez completado el mismo, presionamos Enviar propiedades y posteriormente en Salvar cambios (Fig. 47).

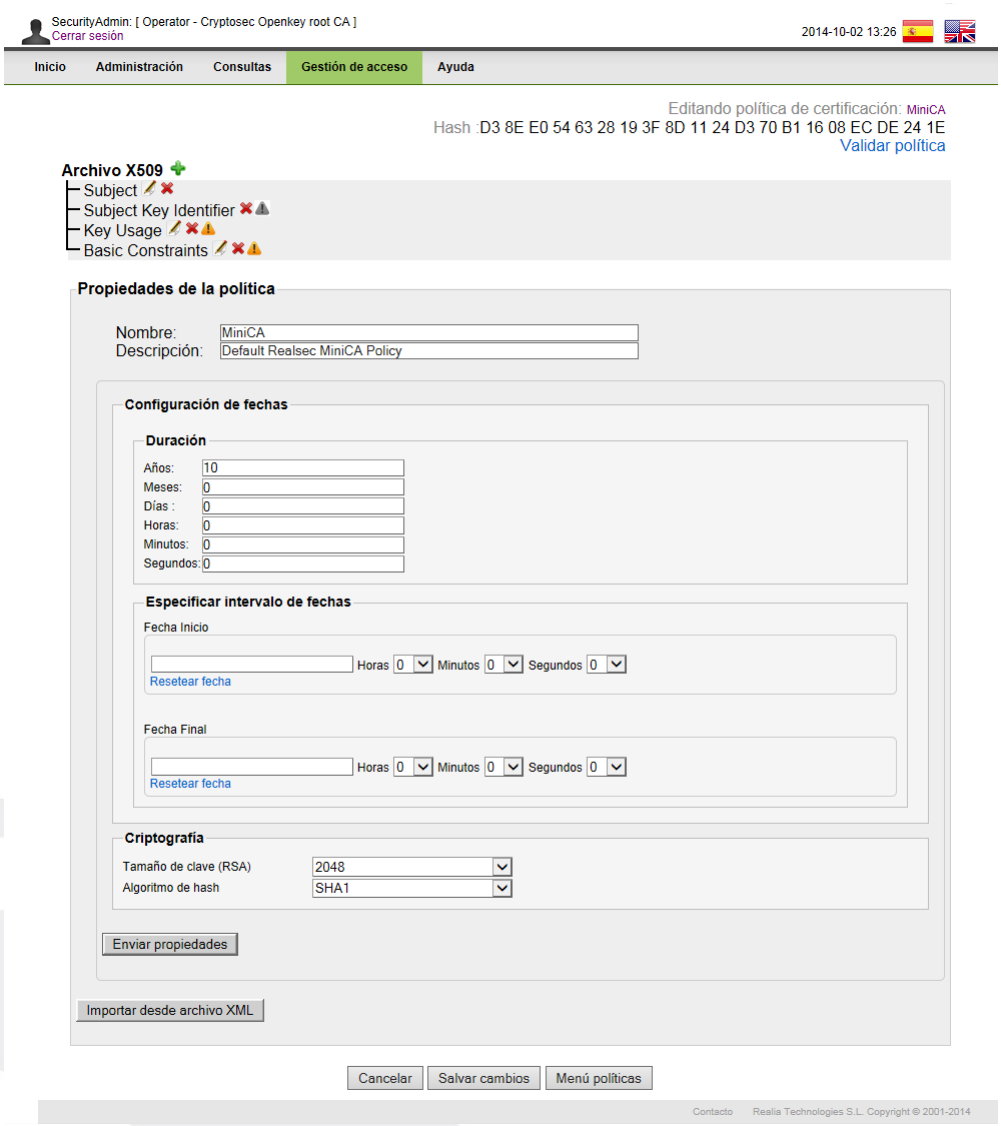


Figura 47: Pantalla para editar políticas de certificados miniCA.

Si presionamos el botón de añadir campos y extensiones de los certificados CA Raíz (), el sistema nos muestra los distintos campos y extensiones que podemos añadir (Fig. 48).

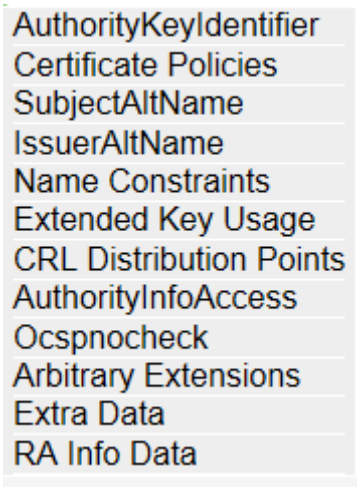


Figura 48: Listado de perfiles que podemos añadir al certificado.

Si presionamos el botón de editar campos y extensiones de los certificados CA Raíz ( ), el sistema nos muestra los campos del certificado seleccionado, pudiendo añadir, editar y eliminar propiedades del mismo modo, una vez realizados los cambios, presionar Salvar cambios (Fig. 49).

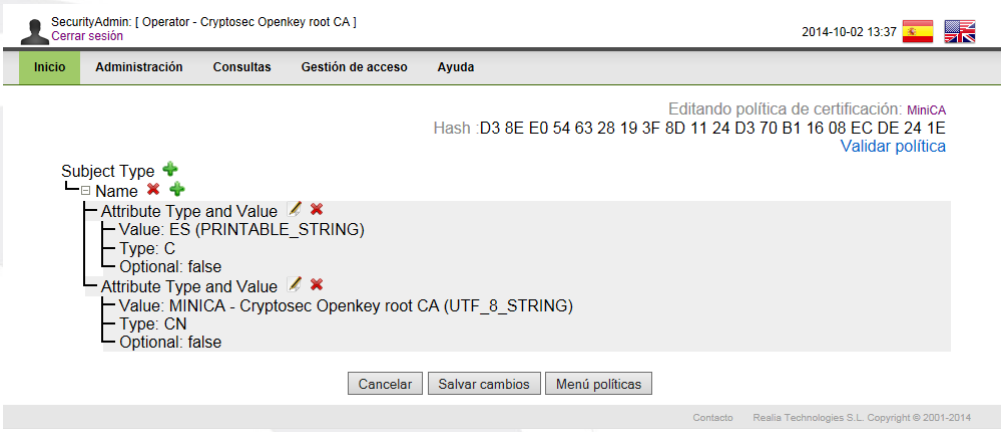


Figura 49: Listado de propiedades de perfil.

Si presionamos el botón de eliminar campos y extensiones de los certificados CA Raíz ( ), el sistema nos muestra una advertencia, la cual debemos aceptar para que sea eliminado y posteriormente presionar el botón Salvar cambios (Fig. 50).

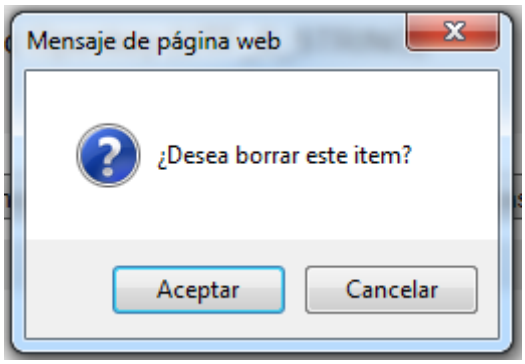


Figura 50: Advertencia para eliminar perfil.

Si presionamos el botón Importar desde archivo XML, el sistema nos muestra una nueva ventana, a través de la cual podemos importar la política mediante un fichero XML (Fig. 51).

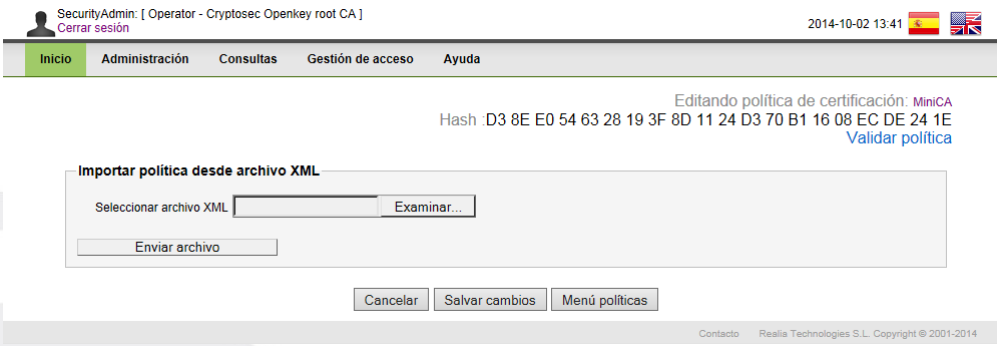


Figura 51: Pantalla para importar política mediante fichero XML.

- **Renovación**

En esta sección, se renueva el certificado de miniCA, para ello, en la primera pantalla debemos presionar el botón Crear (Fig. 52), para crear un nuevo certificado de miniCA, posteriormente, podemos observar la información del certificado (Fig. 53) y debemos presionar el botón Generar. Una vez generado, nos aparece el certificado (Fig. 54), el cual tiene que ser instalado para poder seguir haciendo uso de la aplicación y finalmente presionamos el botón continuar y volvemos a la página de inicio.

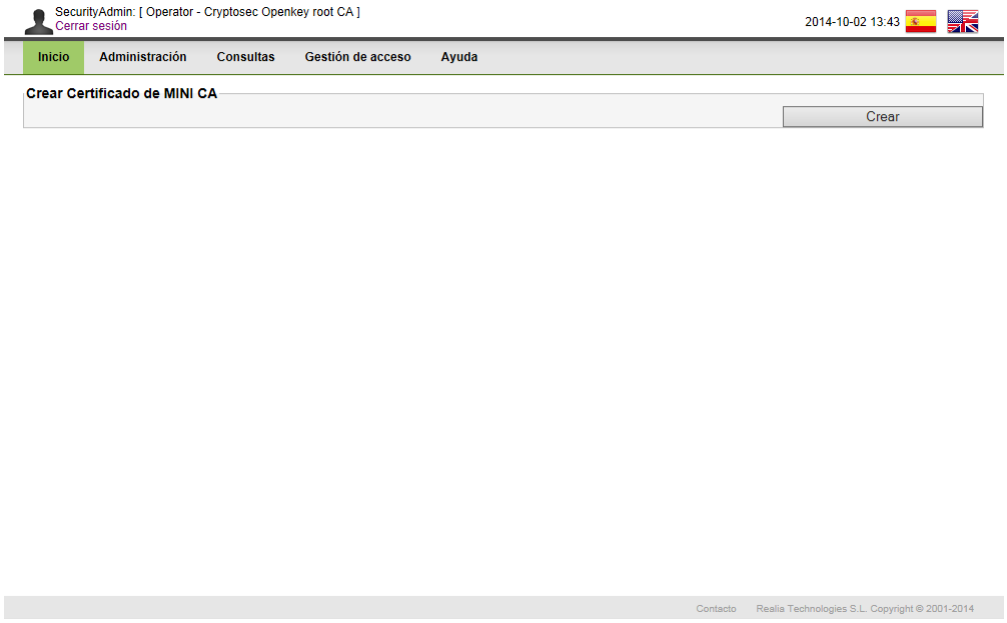


Figura 52: Pantalla para crear certificado de miniCA.

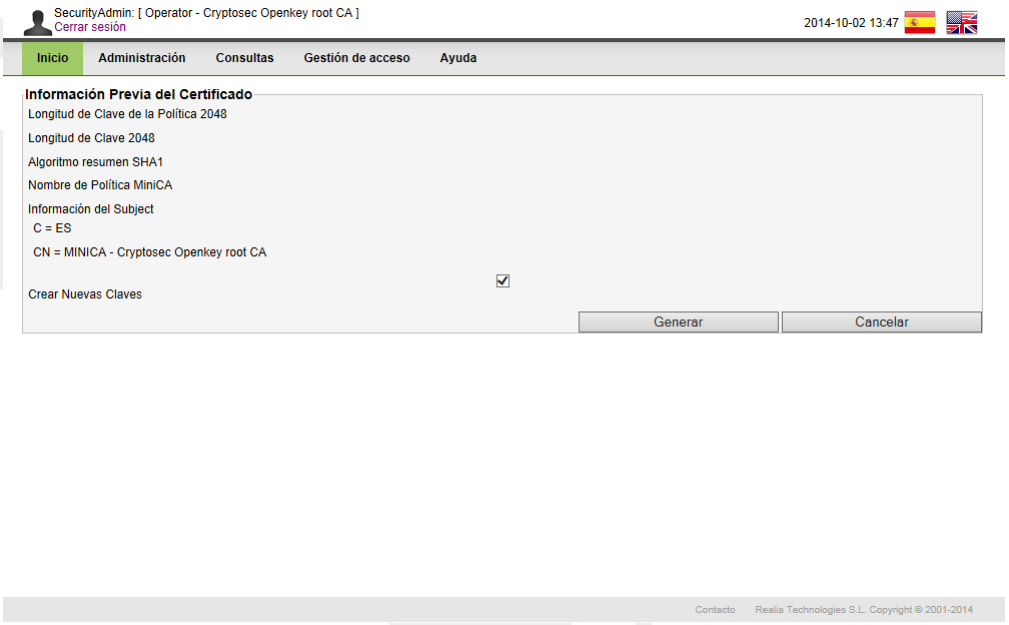


Figura 53: Pantalla con la información previa del certificado y nos permite generarlo.

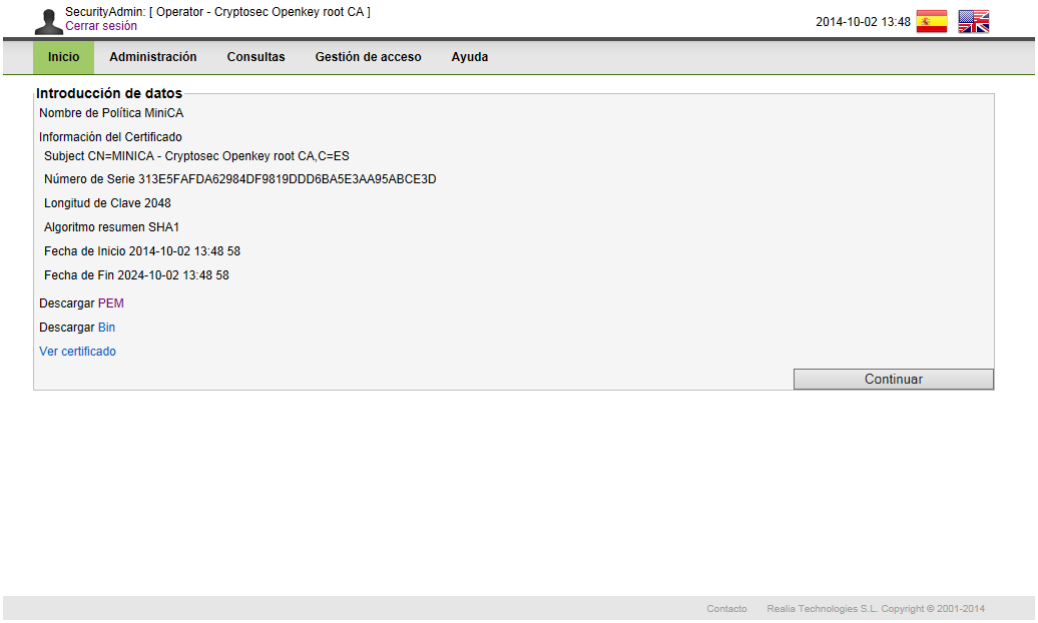


Figura 54: Pantalla con los datos del certificado y fichero de descarga del mismo para su instalación.

2.2.1.3.3. Certificado de Servidor Web

- **Renovación por miniCA**

En este apartado, podemos crearnos un certificado de Servidor Web, para ello en la pantalla que nos muestra el sistema (Fig. 55), presionamos el botón Crear; una vez realizado, el sistema nos muestra la información previa del certificado (Fig. 56) y presionamos sobre el botón Generar, en la pantalla siguiente podemos ver el certificado y descargárnoslo (Fig. 57), una vez que terminamos, presionamos continuar y volvemos a la página de inicio.

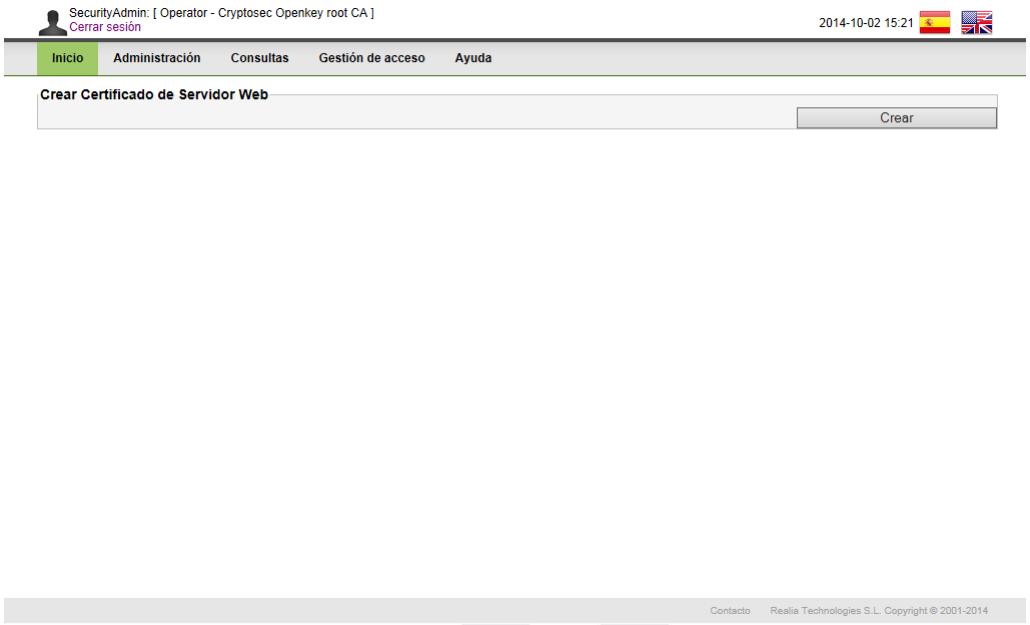


Figura 55: Pantalla para crear certificado de Servidor Web.

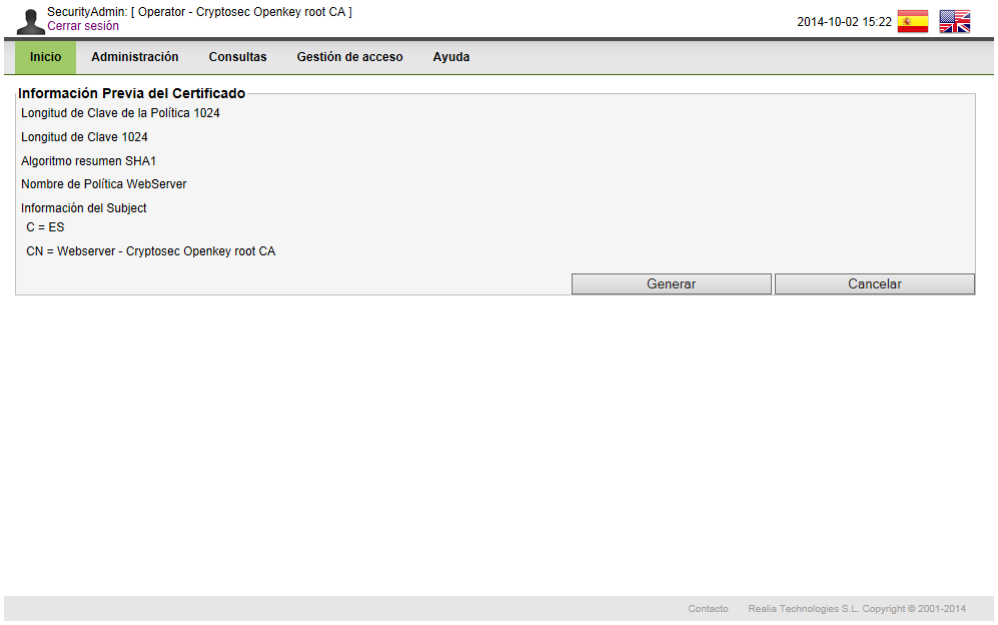


Figura 56: Pantalla con la información previa del certificado.

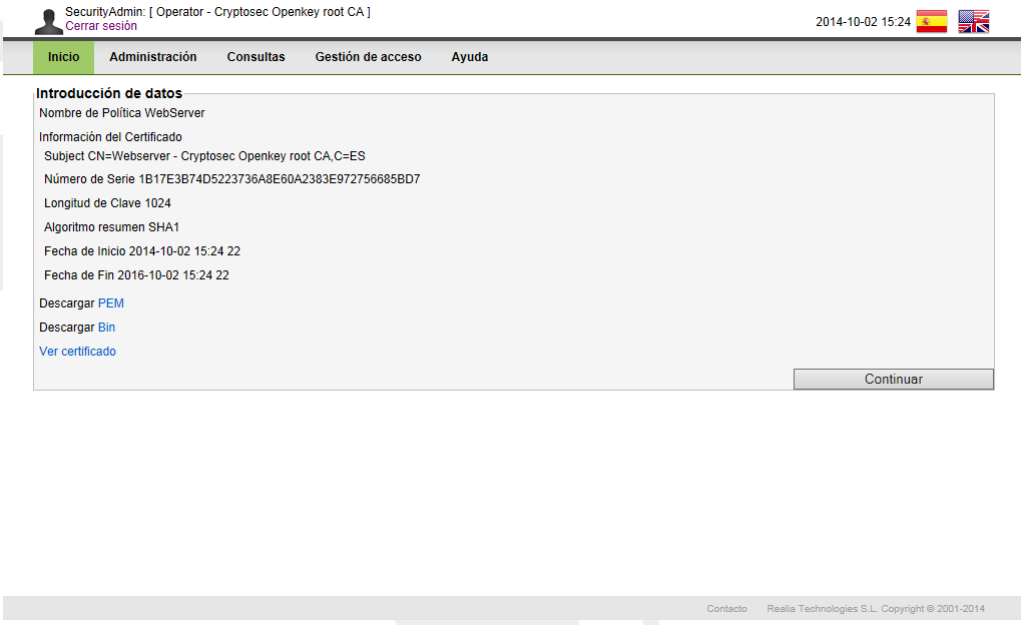


Figura 57: Pantalla para ver y descargar el certificado.

- **Renovación por CA Externa**

En este apartado, el administrador de seguridad, puede renovar un certificado, para ello, en la primera pantalla que nos aparece (Fig. 58) debemos presionar sobre el botón Generar, el sistema nos muestra la petición PKCS10 que puede ser descargada debiendo presionar para ello sobre PEM; con dicha petición, el usuario con el rol correspondiente debe emitir un certificado, y posteriormente el usuario con el rol administrador de seguridad importarlo para renovar el certificado de servidor web (Fig. 59).

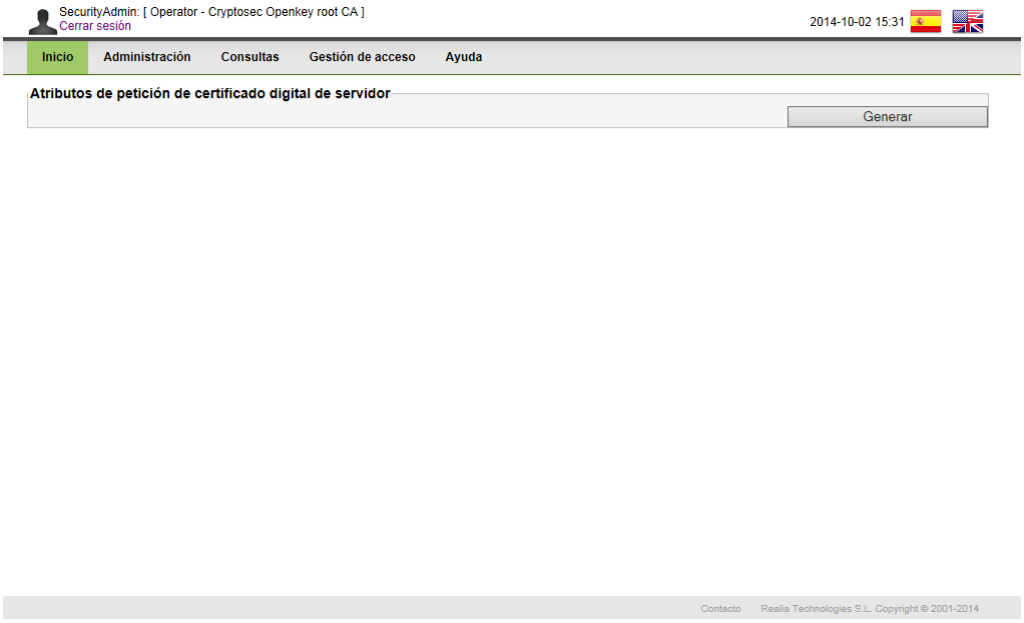


Figura 58: Pantalla inicial para renovar certificado mediante CA Raíz.

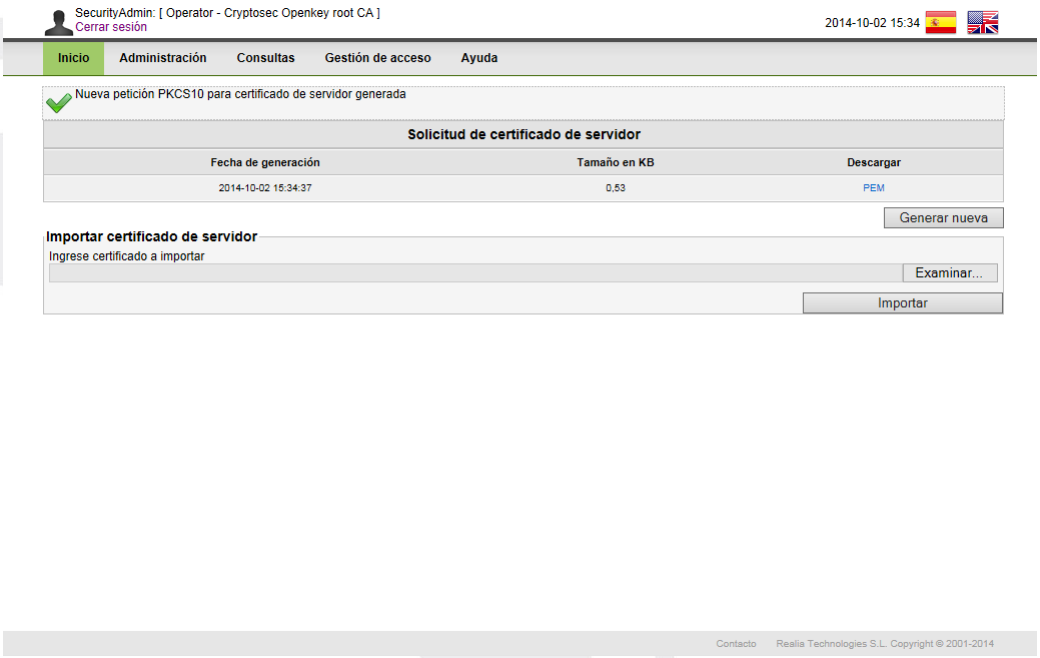


Figura 59: Pantalla de petición PKCS10 para generar certificado de servidor web mediante CA externa.

2.2.1.3.4. Operadores

En esta sección, podemos dar de alta un operador externo, un operador interno, también buscar operadores, y se puede ver un listado de operadores, los cuales pueden ser editados, eliminados y descargados (Fig. 60).

A continuación explicamos cada uno de ellos explícitamente.

En la opción Buscar operadores (Fig. 60), podemos completar los campos del formulario para filtrar por ellos.

En Operadores (Fig. 60), vemos el listado de operadores, si marcamos el campo Seleccionar y presionamos Eliminar, podemos eliminar dicho operados, debiendo para ello aceptar la advertencia que muestra el sistema. También podemos descargarnos el certificado para el cual se ha instalado.

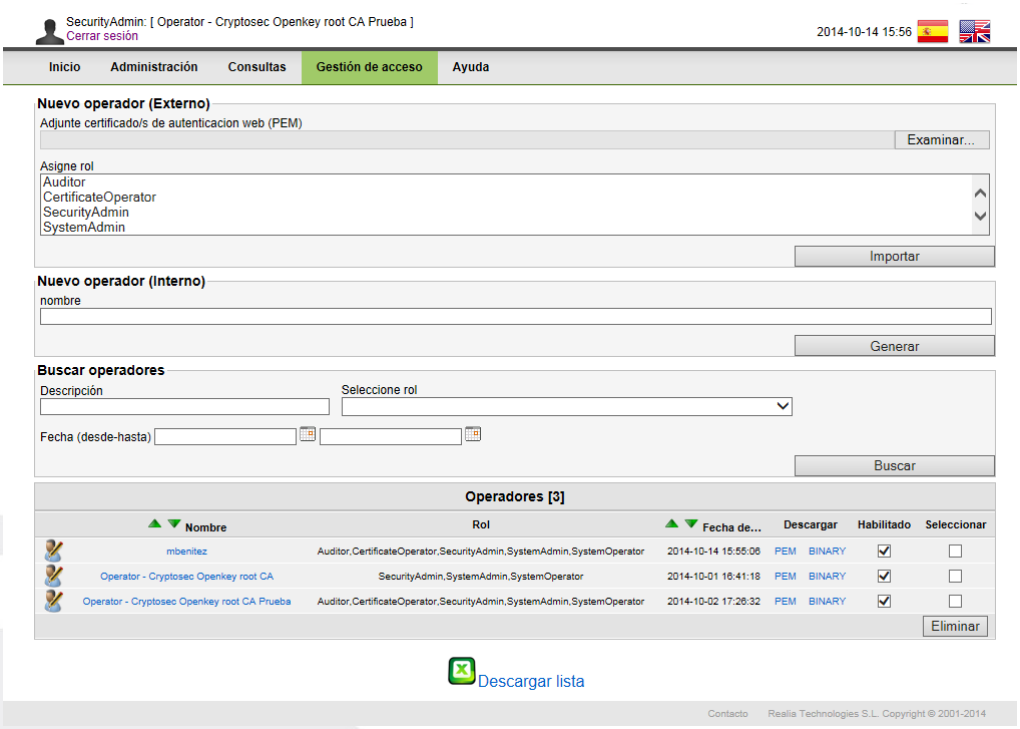


Figura 60: Pantalla principal de operadores.

Para dar de alta un operador externo, debemos adjuntar un certificado de operador web y asignarle los roles deseados para dicho operador (Fig. 61), y presionamos el botón Importar, devolviendo el sistema el siguiente mensaje (Fig. 62), apareciendo el nuevo operador en la lista de operadores. Para poder llevar a cabo esta función, debemos haber importado previamente un certificado de CA externo tal y como se indica en el siguiente apartado.

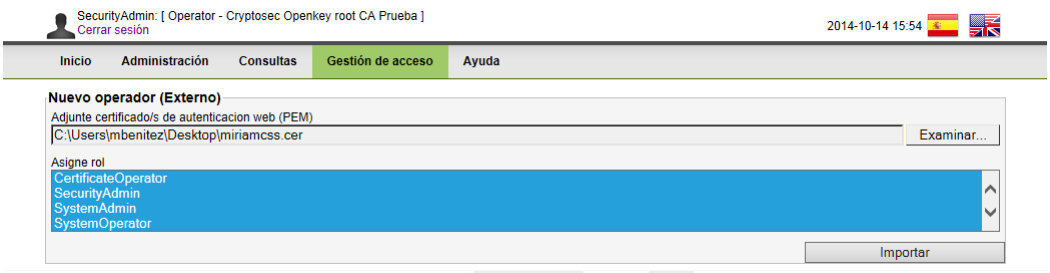


Figura 61: Pantalla para crear un operador externo.

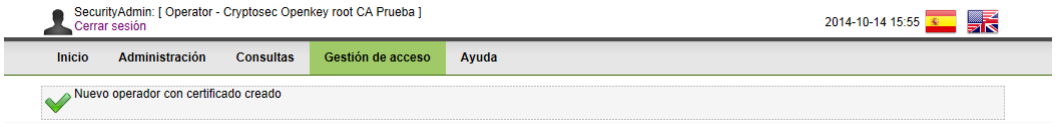


Figura 62: Pantalla de operador creado con éxito.

Para crear un nuevo operador interno, si la política de operador web tiene alguna variable, debemos completar el campo en el formulario y posteriormente presionar el botón *Generar*. El sistema nos muestra una ventana con la información previa del certificado, así como el nombre del mismo y debemos seleccionar los roles que queremos asignarle (Fig. 63), una vez seleccionado el/los rol/es, el sistema nos muestra una ventana en la cual debemos seleccionar un proveedor de Criptografía y presionar sobre *Generar* (si esta operación la realizamos con el navegador Firefox, este paso se omite) (Fig. 64). Si todo es correcto, nos mostrará la ventana con el mensaje de certificado instalado con éxito (Fig. 65). A continuación, nos muestra una pantalla con la confirmación de operador creado y los datos y la posibilidad de descargar el correspondiente certificado (Fig. 66).

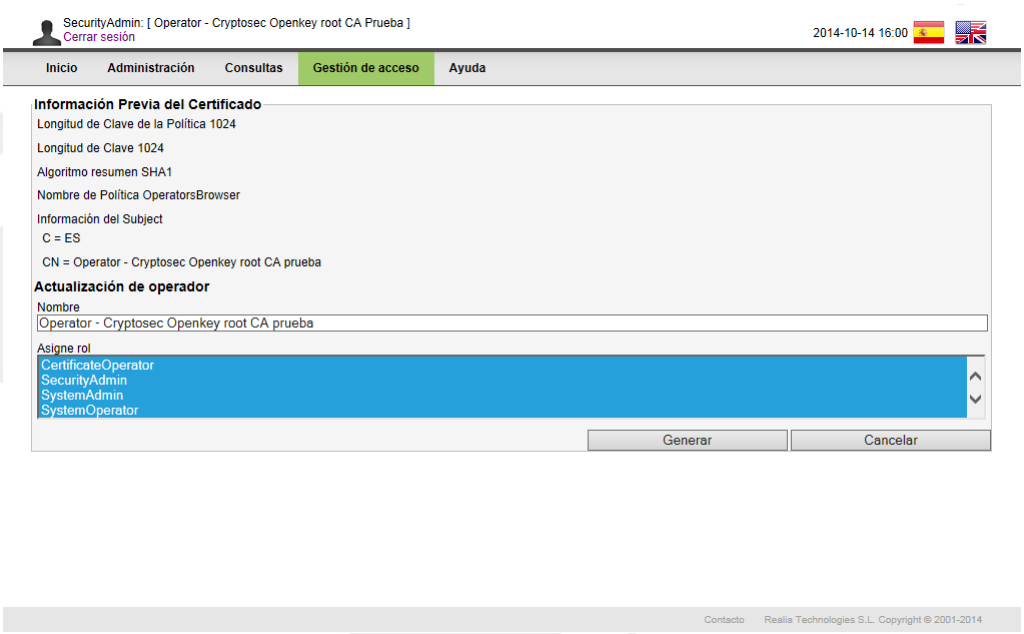


Figura 63: Pantalla para generar un operador interno.

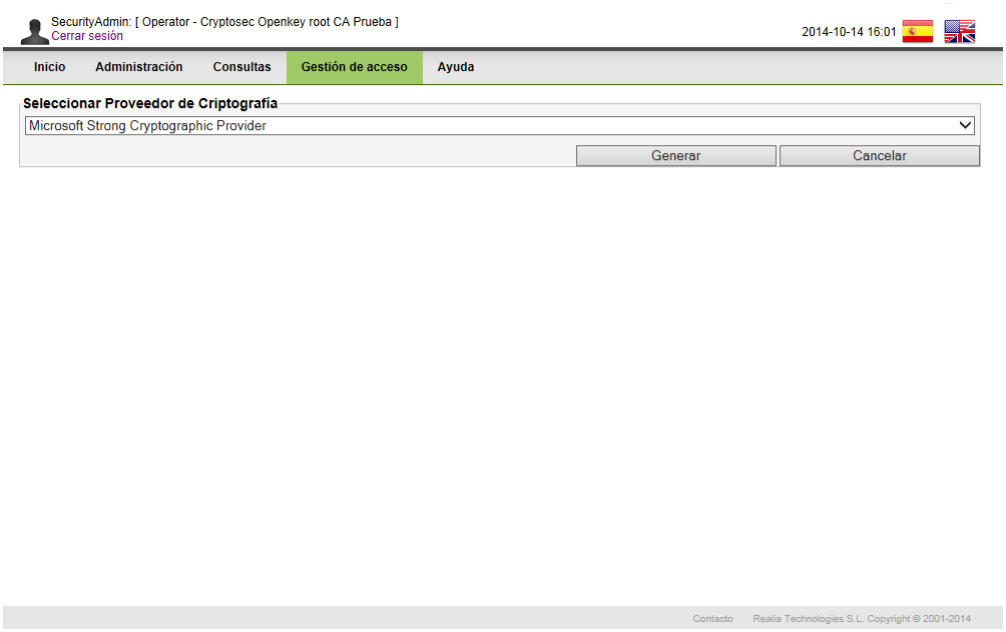


Figura 64: Pantalla para seleccionar un proveedor de criptografía.

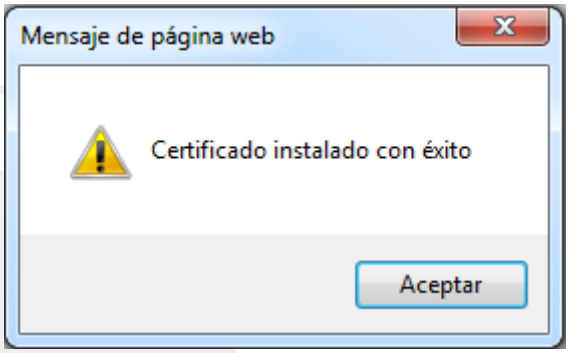


Figura 65: Mensaje de certificado instalado con éxito.

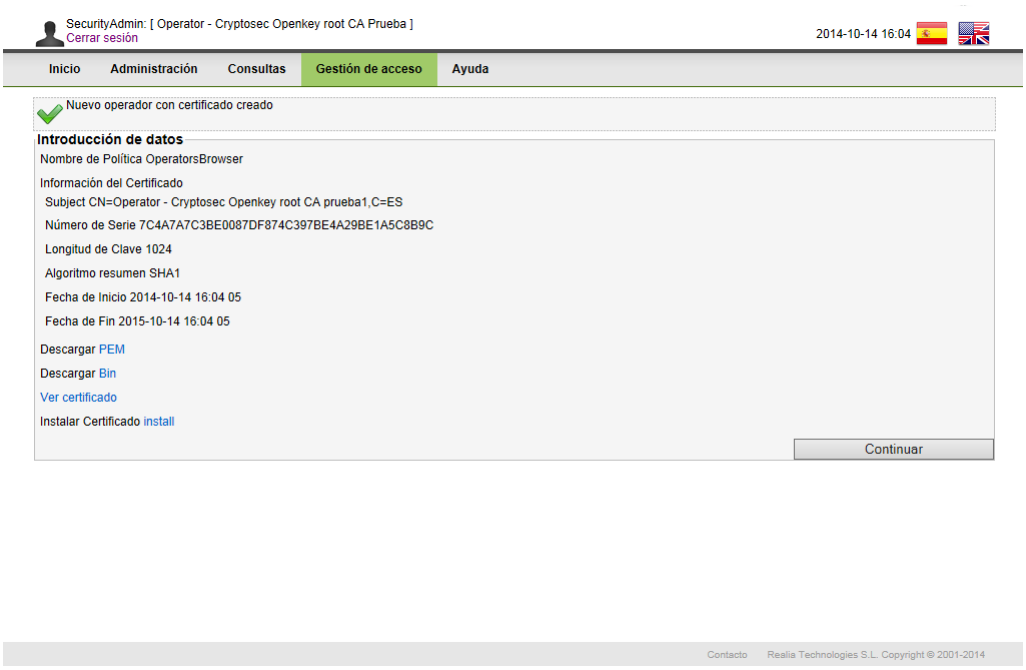


Figura 66: Pantalla de operador creado y descarga de certificado.

- **Certificados de CA externos**

Mediante esta operación, podemos importar certificados de CA emisora. Para ello mediante el botón *Examinar*, indicamos una descripción para el certificado, y posteriormente se presiona el botón *Importar*.

También podemos observar el listado con todos los certificados externos de los que disponemos, si marcamos el botón Seleccionar y presionamos el botón Eliminar, aceptando posteriormente la advertencia que aparece, eliminamos el certificado seleccionado, además se puede marcar/desmarcar Servidor, lo cual permite que todos los certificados de clientes firmados por dicho certificado tengan acceso a la aplicación (Fig. 67).

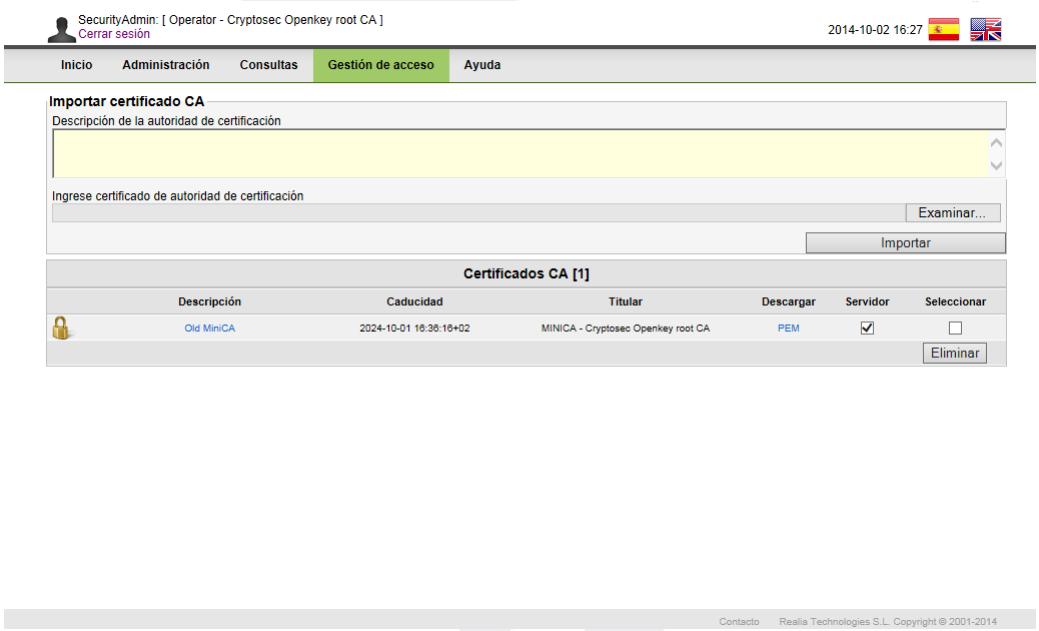


Figura 67: Pantalla de certificados de CA externos.

2.2.1.3.5. Usuarios

En esta sección, podemos dar de alta usuarios para el servicio de Timestamp, también se puede ver un listado de usuarios, los cuales pueden ser eliminados (Fig. 68).

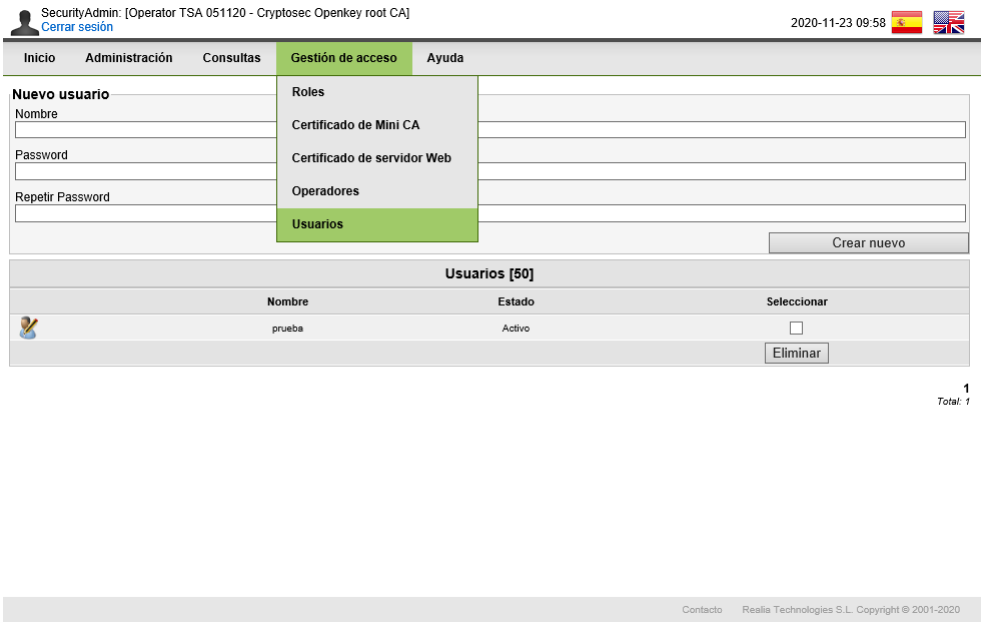


Figura 68: Sección de usuarios del servicio de Timestamp.

Mediante el botón *Crear Nuevo* se pueden crear usuarios indicando el nombre del mismo y su contraseña. En cambio, si se desea eliminar un usuario debe seleccionar el usuario en el listado y pinchar el botón *Eliminar*

2.2.2. Administración web para el rol Administrador de Sistemas

Mediante este rol, se autoriza para configurar los parámetros de red, actualizar software, actualizar firmware, así como el mantenimiento de la base de datos.

La pantalla de administración web para el rol administrador de sistema es (Fig. 69).

Figura 69: Pantalla de inicio de administración web para el rol administrador de sistema.

2.2.2.1. Configuración

2.2.2.1.1. Configuración de red

Podemos configurar el servicio NTP, para ello debemos escribir los servidores separados con comas en el hueco destinado para ello. También podemos hacer una prueba del servicio NTP. Vemos todo ello en la Fig. 70.

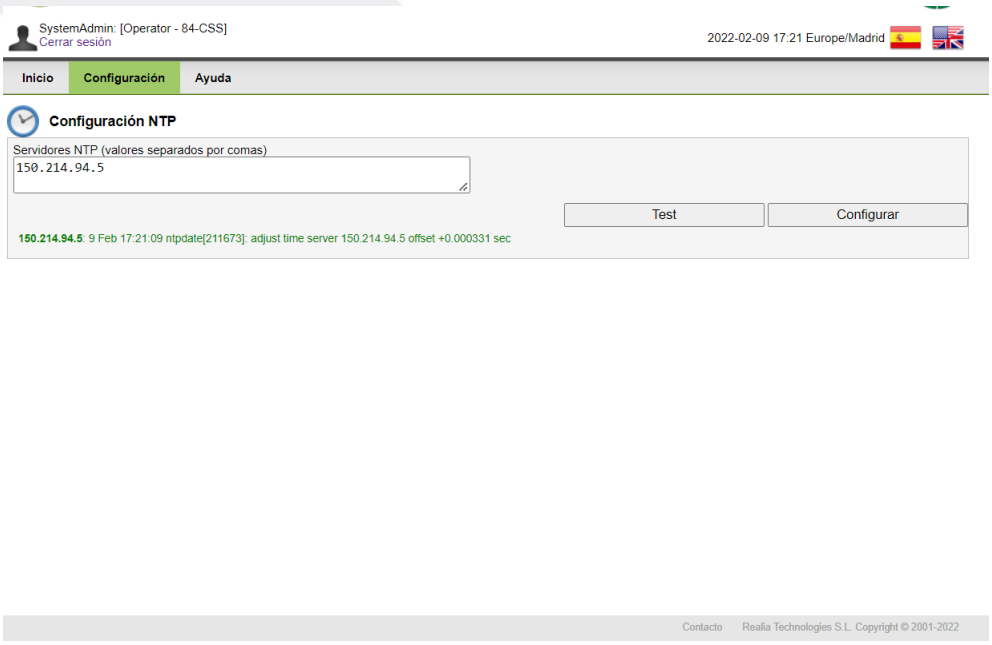


Figura 70: Pantalla configuración de red.

2.2.2.1.2. Actualización de Software

En esta sección, podemos actualizar la plataforma (Software y Firmware), debiendo para ello presionar el botón Examinar, seleccionar el certificado del operador que va a proporcionar la actualización (este será proporcionado por Realsec) y presionar el botón Actualizar. Posteriormente se presiona Examinar, y se selecciona el paquete correspondiente a la actualización, el cual va a estar cifrado y firmado, y presionar el botón Actualizar (Fig. 71).

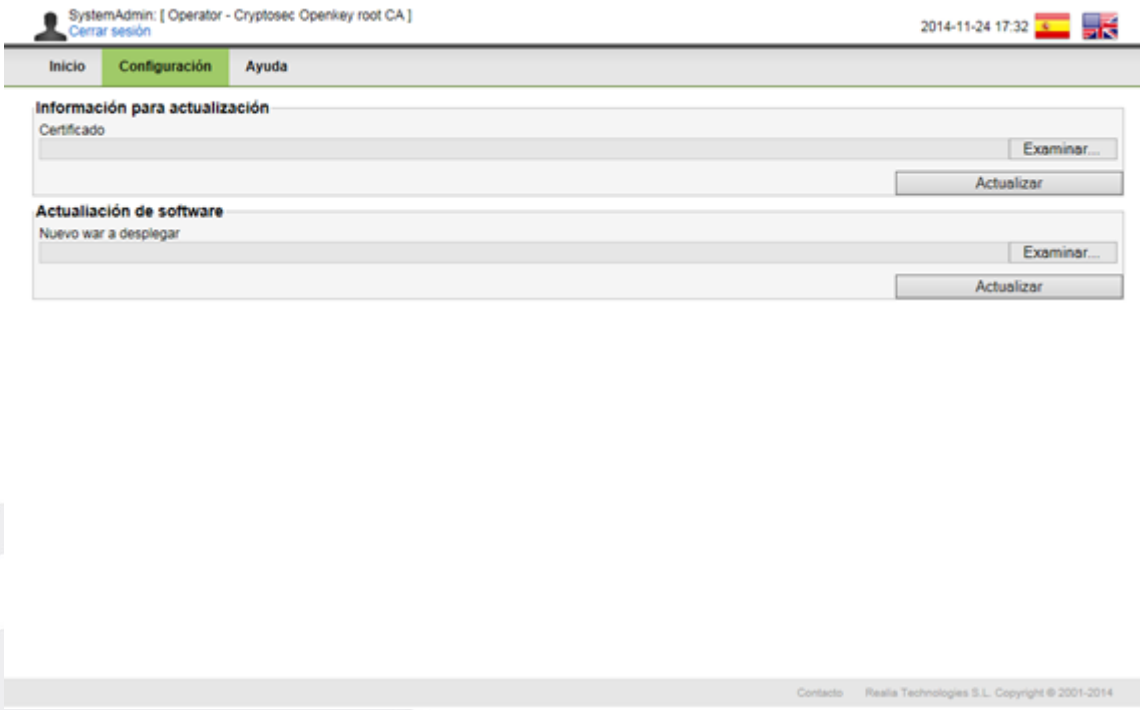


Figura 71: Pantalla para actualizar la plataforma.

2.2.2.1.3. Archivar datos

En esta sección, podemos archivar datos (Certificados, Logs y CRL) y moverlos a una base de datos diferente. Para realizar el proceso se debe proporcionar la siguiente información (Fig. 72):

- **Host**: Debe indicar la dirección IP del servidor de base de datos donde se almacenarán los datos a archivar.
- **Port**: Debe indicar el puerto del servidor de base de datos donde se almacenarán los datos a archivar.
- **Usuario**: Debe indicar el usuario del servidor de base de datos donde se almacenarán los datos a archivar.
- **Contraseña**: Debe indicar la contraseña del usuario del servidor de base de datos donde se almacenarán los datos a archivar.
- **Nombre BBDD**: Debe indicar el nombre de la base de datos en el servidor de base de datos donde se almacenarán los datos a archivar.
- **Datos a archivar**: Debe seleccionar los datos archivar.
- **Fecha desde-hasta**: Debe indicar el rango de fechas de los datos que desea archivar.

- **Incluir CREATE TABLE**: Debe marcar esta opción solo si la base de datos NO contiene todavía las tablas donde se almacenarán los datos.

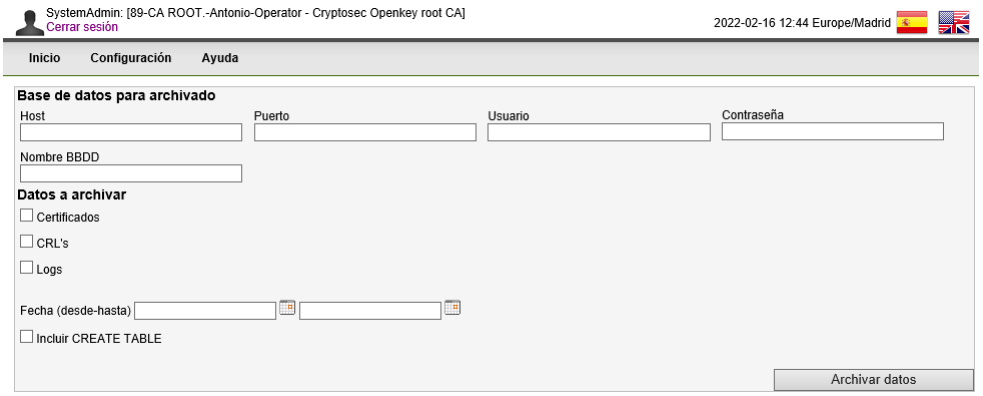


Figura 72: Pantalla para archivar datos.

Una vez introducidos los datos, al presionar el botón *Archivar datos* podremos ver el resultado de la operación (Fig. 73).

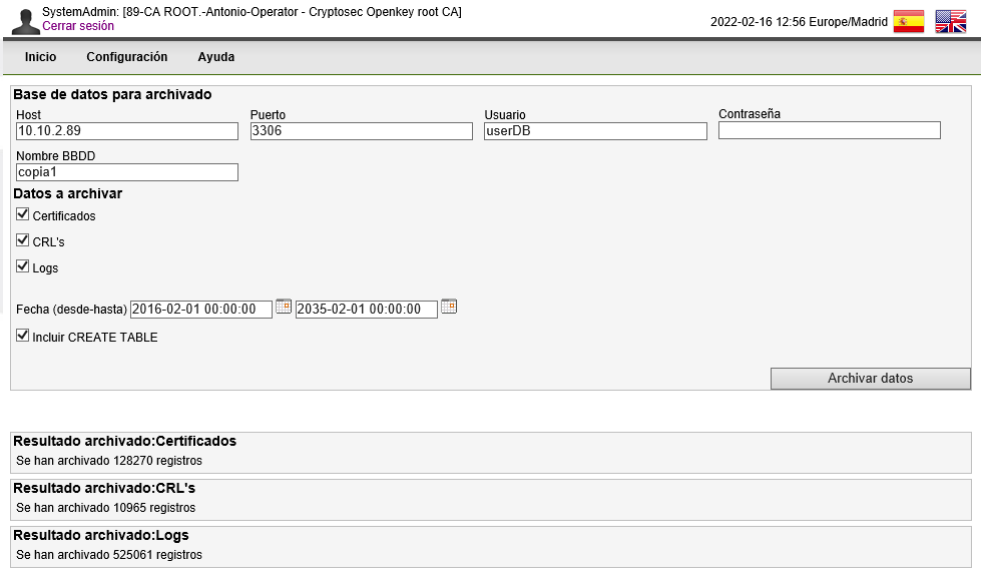


Figura 73: Pantalla con resultado de archivar datos.

2.2.2.1.4. Mantenimiento base de datos

Mediante esta tarea, podemos consultar el nivel de fragmentación de la base de datos, así como realizar una compactación ligera (la cual no bloquea la base de datos) y una compactación completa (la cual bloquea la base de datos). Además, podremos configurar un backup periódico, debiendo poner para ello cada cuantas horas queremos que éste sea generado o bien, poniendo a qué hora del día, queremos que se genere el mismo. (Fig. 74).

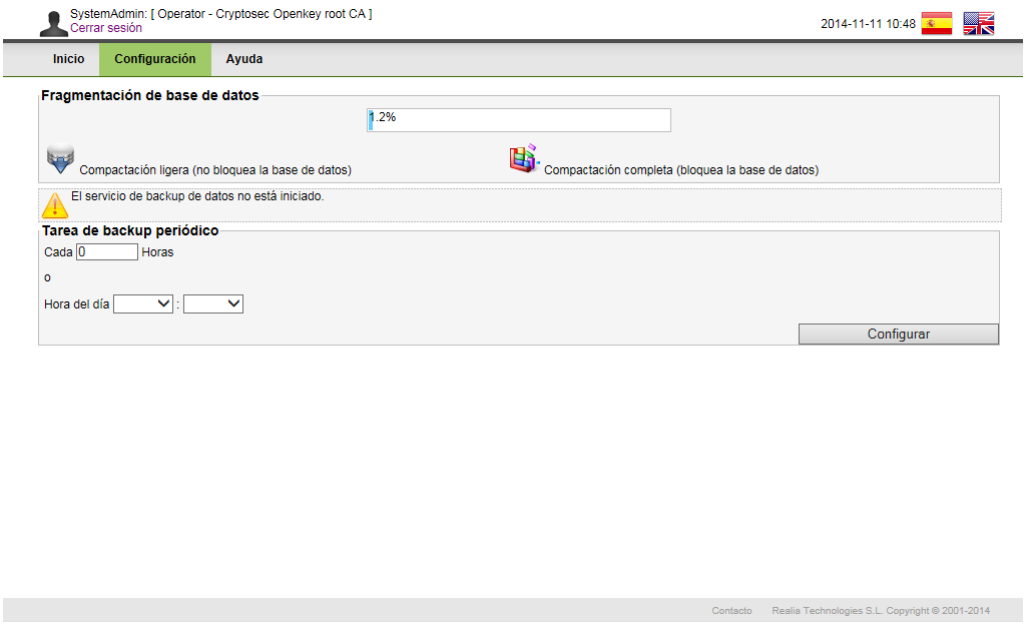


Figura 74: Pantalla para fragmentar la base de datos.

2.2.3. Administración web para el rol Auditor

Mediante el rol auditor, se autoriza al usuario a ver los datos generados por la TSA (sellos de tiempo emitidos) y las trazas de las operaciones realizadas (logs). Así como la visualización de las políticas de certificación y consulta de certificados internos.

La pantalla de administración web para el rol auditor es (Fig. 75).

Figura 75: Pantalla de inicio de administración web para el rol auditor.

2.2.3.1. Consultas

2.2.3.1.1. Sellos de tiempo

En esta funcionalidad, se realiza una búsqueda de los sellos de tiempo emitidos.

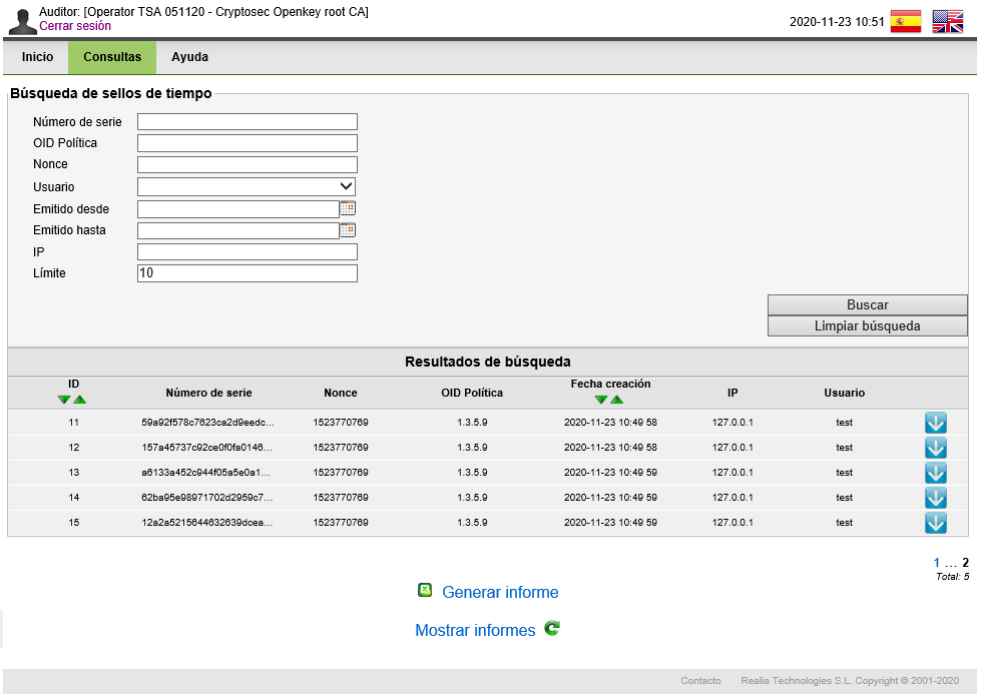


Figura 76: Pantalla de consultas de sellos de tiempo.

Para efectuar la búsqueda filtrando por los campos posibles debemos rellenar en el formulario los campos deseados, presionando el botón Buscar para llevar a cabo la búsqueda, según se puede observar en la (Fig. 77); si presionamos el botón Limpiar búsqueda, el formulario y la consulta se restablecen, de forma que queda tal y como estaba en la (Fig. 76). En caso de querer efectuar una búsqueda completa de los sellos de tiempo, no rellenaremos ningún campo, presionaremos sobre el botón Buscar y podremos observar el listado de todos los certificados como podemos observar en la (Fig. 76). Si presionamos en la última columna sobre el icono , podemos descargar el sello de tiempo codificado en base 64.

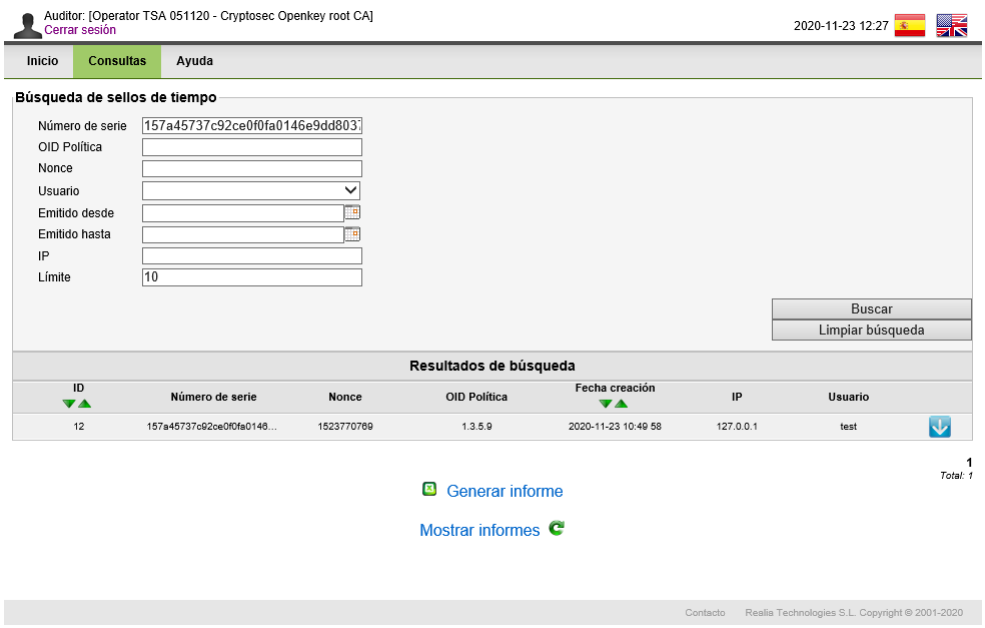


Figura 77: Pantalla de búsqueda de sellos de tiempo filtrando por campos, en este caso el número de serie.

Si se desea iniciar la generación de un informe XLS con los datos obtenidos en la consulta puede pinchar en el enlace *Generar Informe*. En cambio, si se desea abrir, descargar o borrar un informe ya generado hay que pinchar en el enlace *Mostrar informes* (Fig. 78).

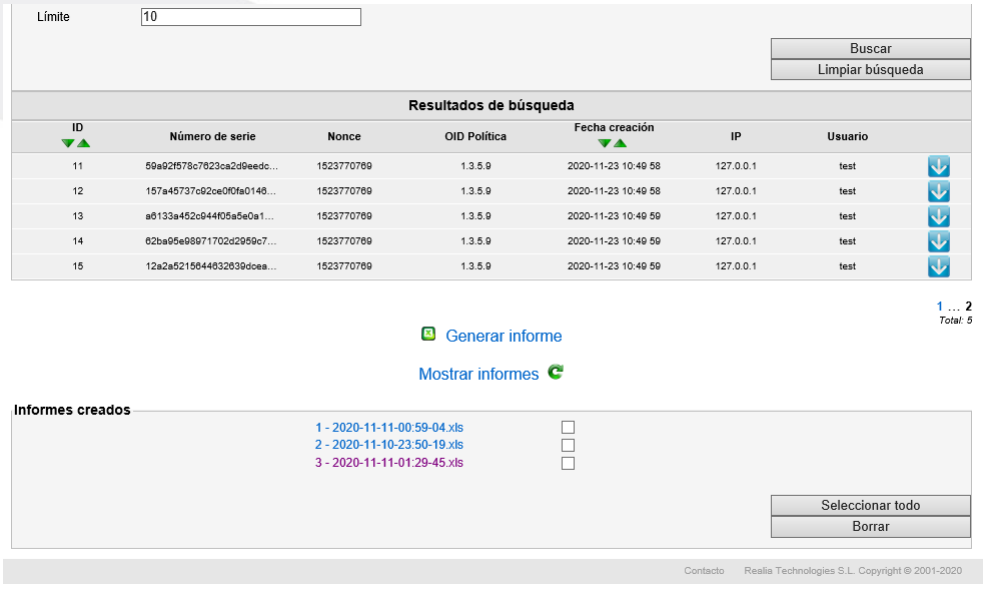


Figura 78: Pantalla de búsqueda de sellos de tiempo mostrando informes XLS generados.

2.2.3.1.2. Políticas de certificación

Figura 79: Pantalla de políticas de certificación.

- **Políticas**

Mediante esta operación, se podrán consultar las distintas autopolíticas y políticas, sin poder hacer cambios en ninguna de ellas ni crear nuevas (Fig. 80).

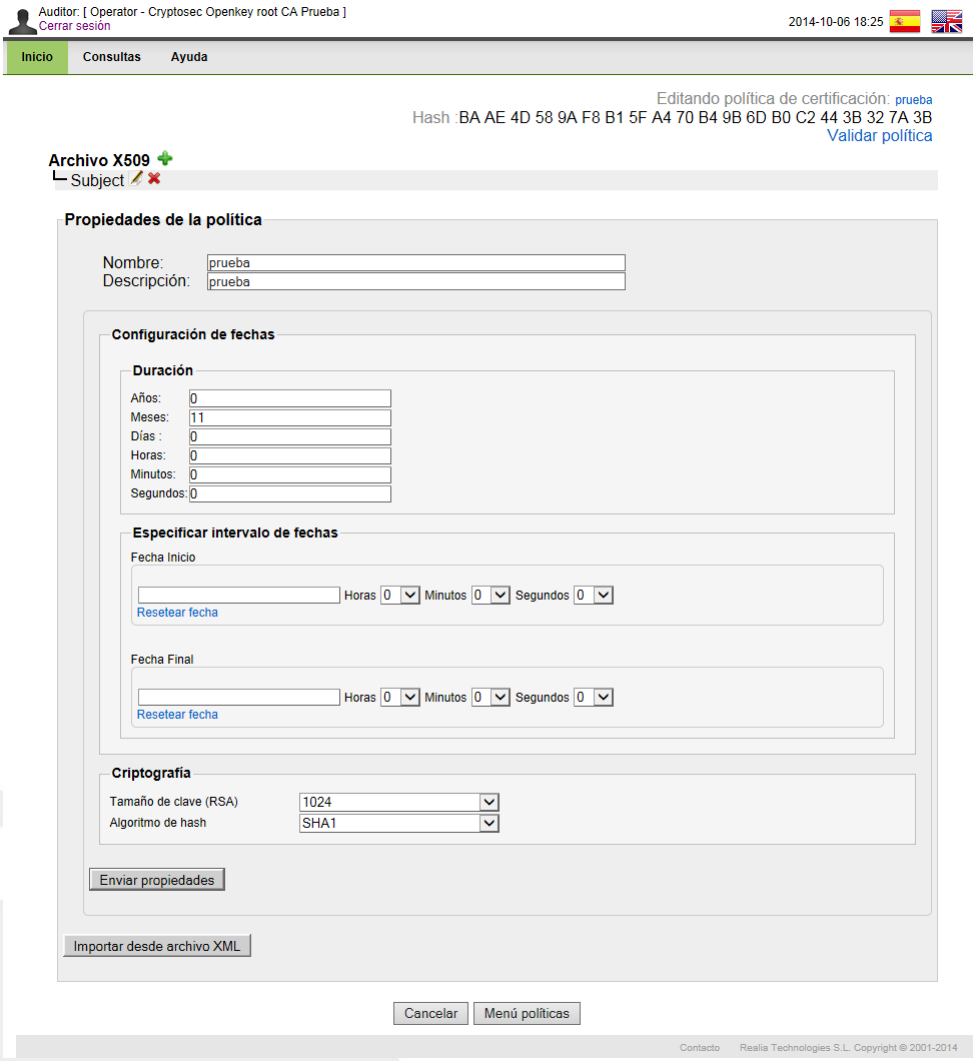


Figura 80: Pantalla para editar políticas internas.

Si presionamos sobre Validar política comprobamos si la política es válida (Fig. 81) o no (Fig. 82).

Figura 81: Pantalla para editar políticas internas.

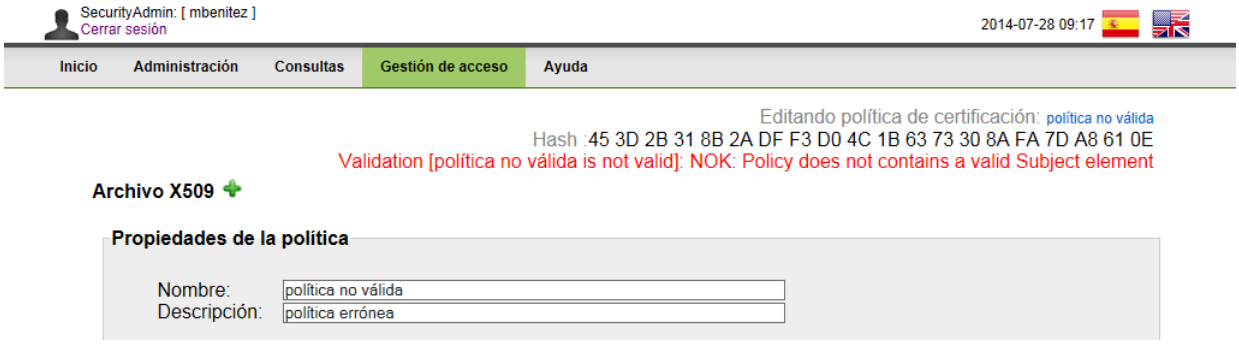


Figura 82: Pantalla de política no válida.

- **Variables**

En este apartado, se podrán consultar las variables, para ello presionamos el botón ( ), y nos aparece la siguiente pantalla (Fig. 83).

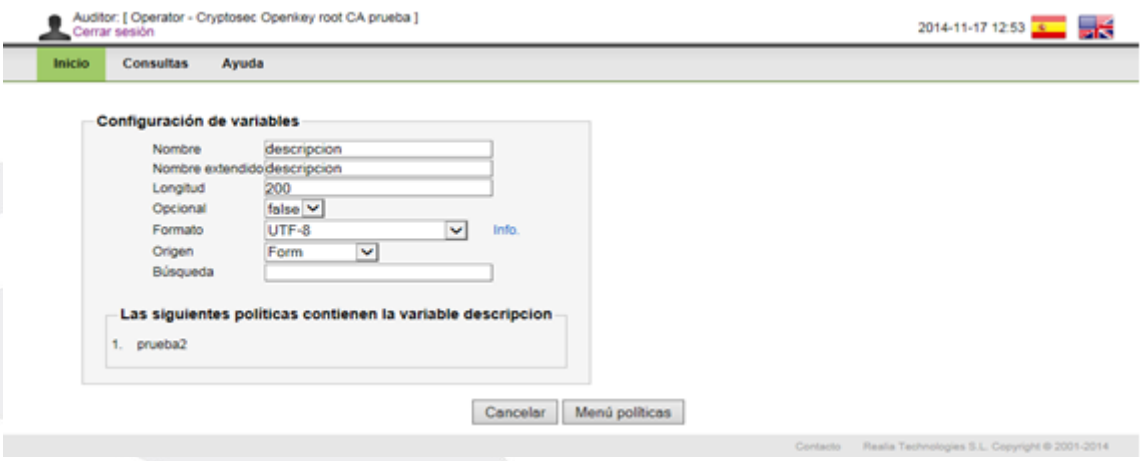


Figura 83: Pantalla para consultar la información de la variable.

2.2.3.1.3. Logs

- **Logs**

En este punto, se puede ver un listado con los logs de operación, también podemos hacer una búsqueda por campos y descargarnos el listado de logs de operaciones (Fig. 84).

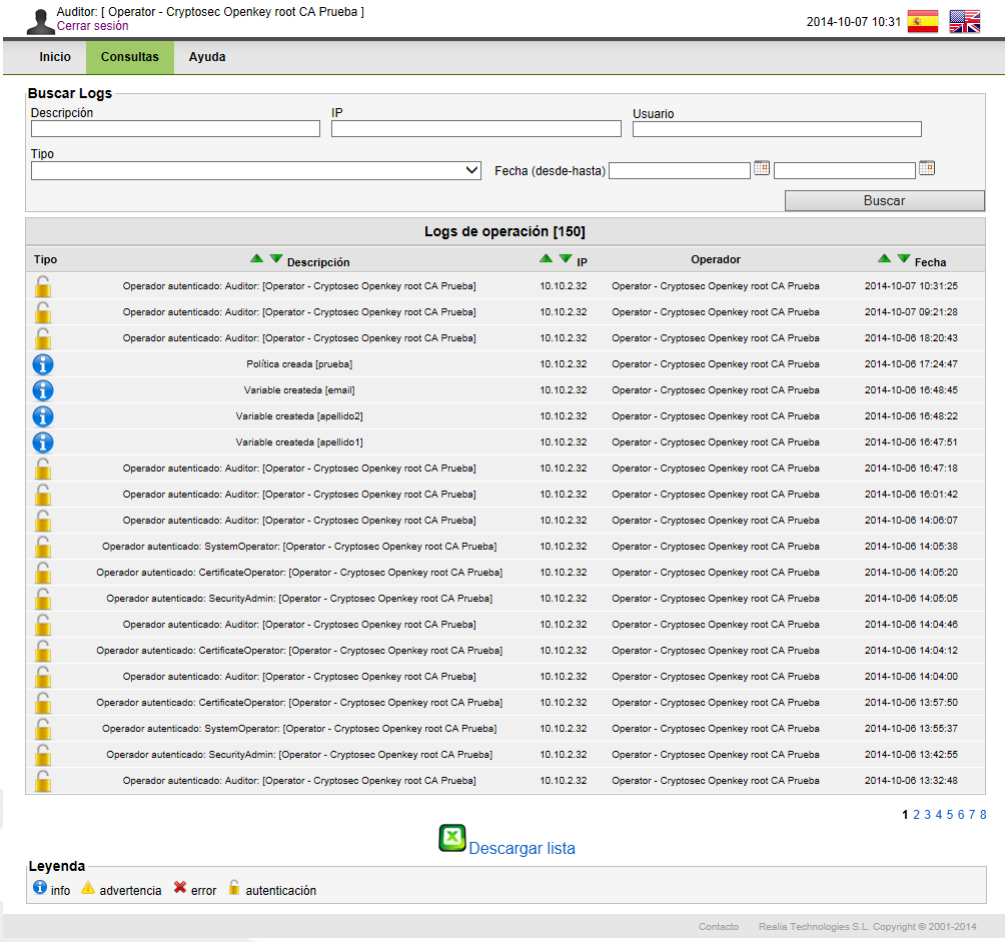


Figura 84: Pantalla de logs de operación.

- **Logs de sistema**

Mediante esta sección, podemos descargarnos los logs del sistema para poder ver los errores que se han presentado en el mismo, presionando para ello sobre cada uno de los logs. También podemos eliminar los logs, para ello, debemos marcar el campo seleccionar y posteriormente pulsar el botón *Eliminar*. (Fig. 85).

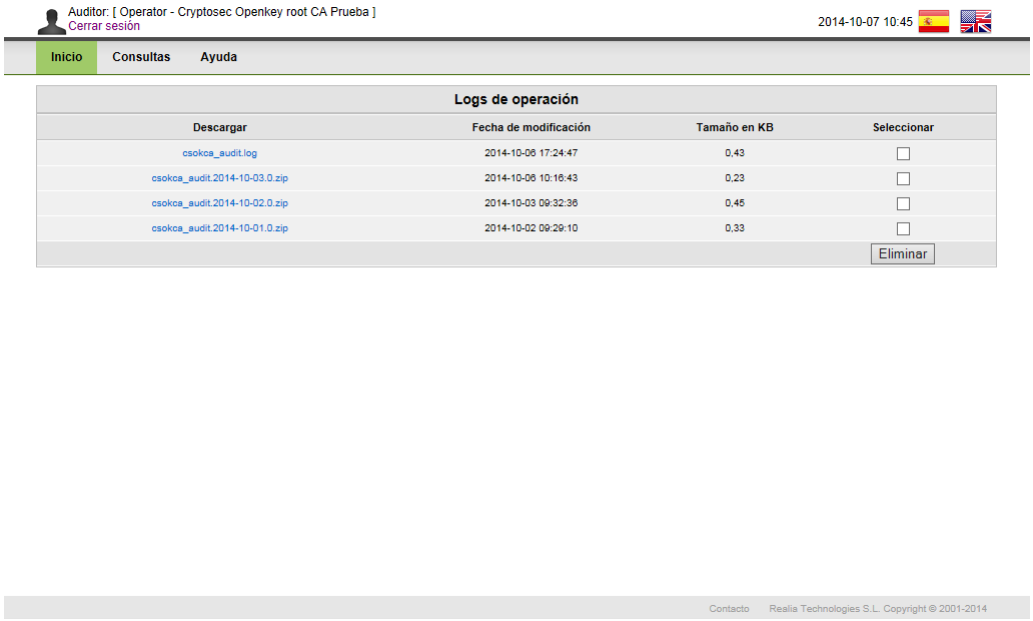


Figura 85: Pantalla de logs de operación.

2.2.3.1.4. Certificados internos

En esta sección, se nos muestra el listado de los certificados internos disponibles (Fig. 86), también podemos ver y descargarnos cada uno de ellos, ponemos como ejemplo uno (Fig. 87); para ello el sistema nos abre una nueva ventana con la información del certificado y la posibilidad de descargarnos el mismo, debiendo para ello presionar sobre el icono ( ).

Además, podemos visualizar el cuerpo de cada uno de estos certificados, debiendo hacer click sobre el icono ( ) Fig. 88.

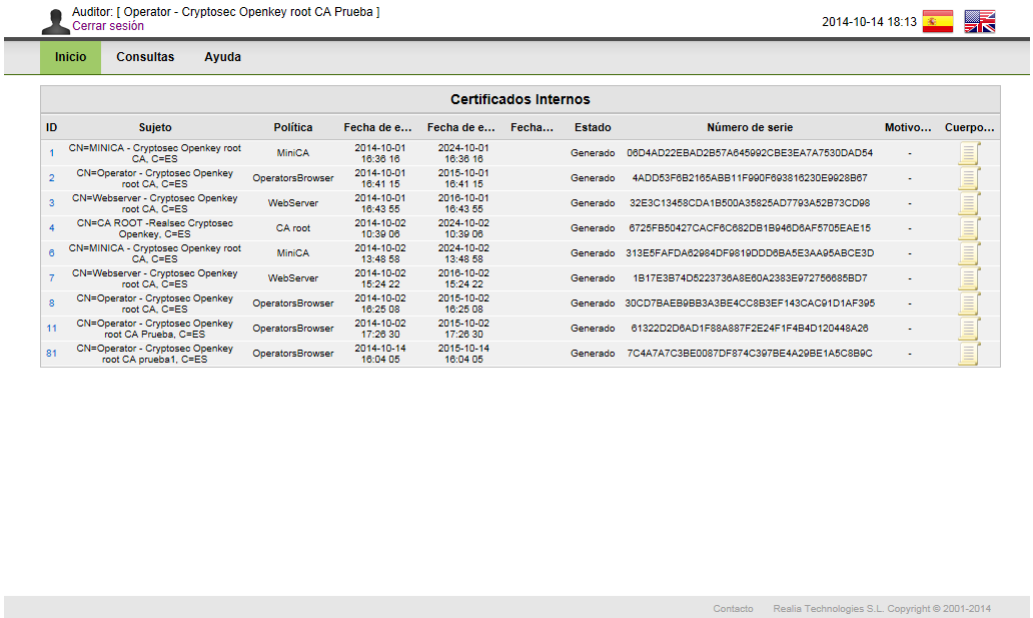


Figura 86: Pantalla de certificados internos.

realsec

Certificado	
Estado	Generado (Id: 6)
Política	MiniCA
Campos	
Versión	3
Número de serie	31 3E 5F AF DA 62 98 4D F9 81 9D DD 6B A5 E3 AA 95 AB CE 3D
Algoritmo de firma	SHA1withRSA
Emitido por	C=ES CN=MINICA - Cryptosec Openkey root CA
Desde	2014-10-02 13:48 58
Hasta	2024-10-02 13:48 58
Sujeto	C=ES CN=MINICA - Cryptosec Openkey root CA
PK. Info.	RSA (2048)
Extensiones	
Identificador de clave del titular	30 1A 90 06 B8 66 6C 17 80 67 C7 1B DF C4 C4 12 1A 4B 81 C3
Uso de clave	keyCertSign,
Restricciones básicas	CA TRUE Route length constraint: 0
Hash (SHA-1)	
29 58 4B FC 15 BA 6E 63 F2 A6 E4 F8 8C 55 E4 A4 3E 75 07 63	
Pem	

Descargar


Figura 87: Pantalla de visualización y descarga de certificado miniCA.

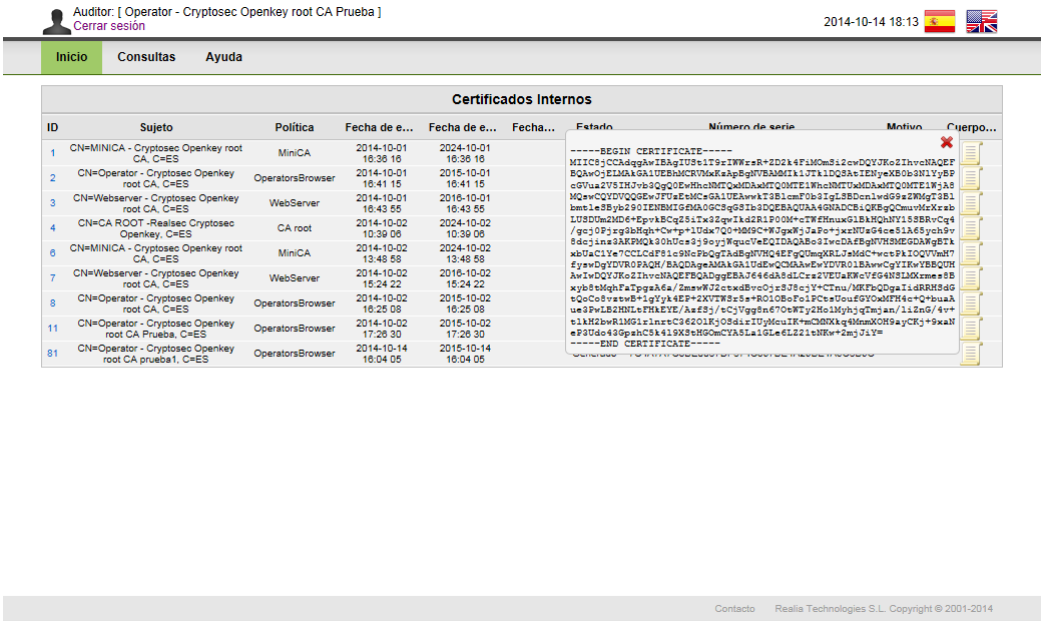


Figura 88: Pantalla con la visualización del cuerpo del certificado.

2.2.3.1.5. Autoridades

Se muestra en esta sección un listado con las autoridades disponibles para la emisión de certificados como mostrado en la (Fig. 89).

Figura 89: listado de autoridades disponibles.

2.2.4. Administración web para el rol Operador de Sistemas

Mediante el rol operador de sistema, se autoriza para generar y configurar CRLs, monitorizar el hardware y sistema operativo, administrar servicios, copia de seguridad de datos y ver los logs de software, sistema operativo y base de datos.

La pantalla de administración web para el rol operador de sistema es (Fig. 90).

Figura 90: Pantalla de inicio de administración web para el rol operador de sistema.

2.2.4.1. Operaciones

2.2.4.1.1. Monitorización

- **Hardware**

En este apartado, el sistema nos permite ver la monitorización del hardware actualizada (Fig. 91).

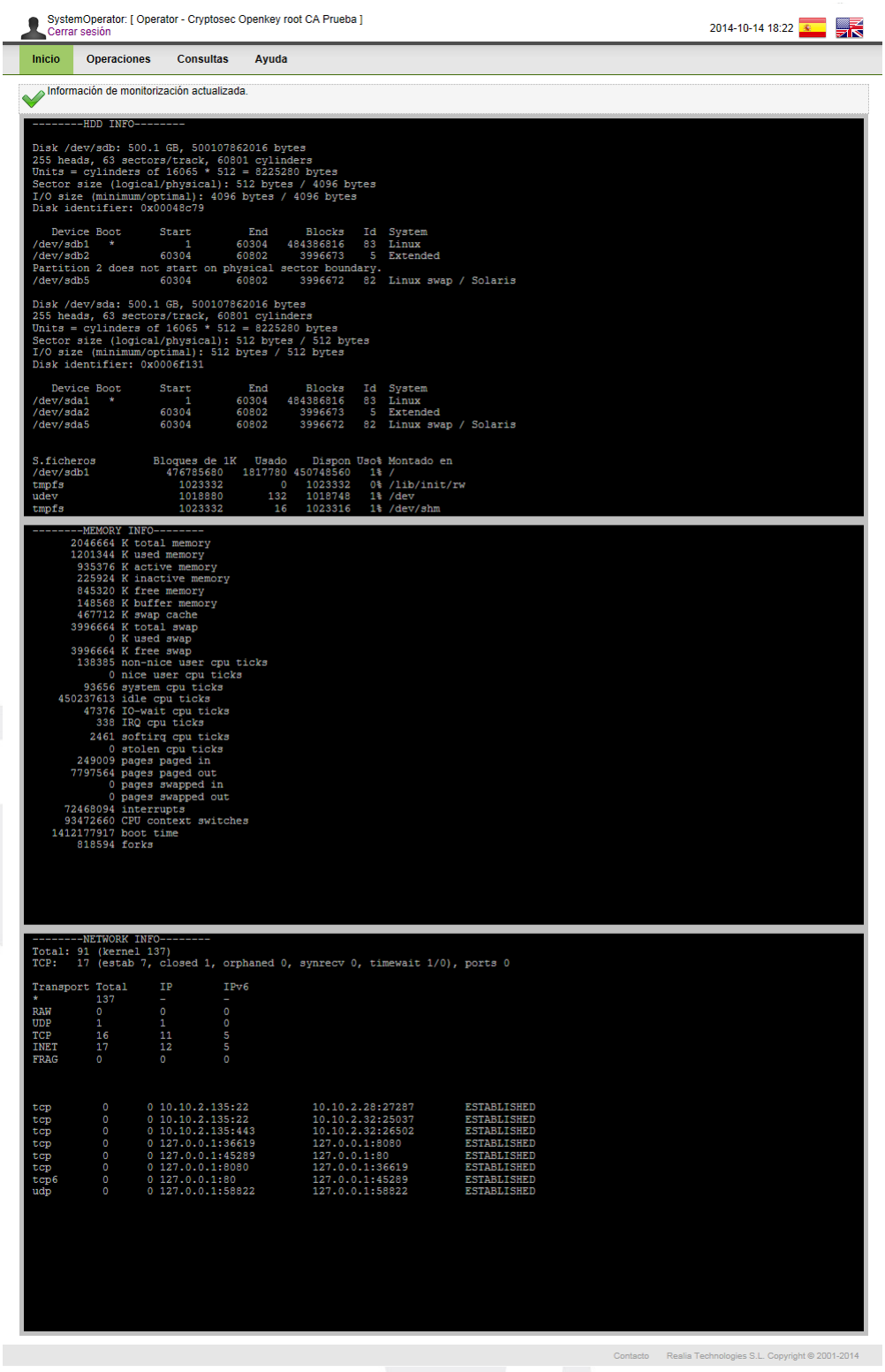


Figura 91: Pantalla con la monitorización del Hardware.

- **Sistema Operativo**

En esta sección, el sistema nos muestra la monitorización del sistema operativo, también podemos escribir el identificador de proceso y darle a terminar, para de este modo finalizar el proceso indicado (Fig. 92).

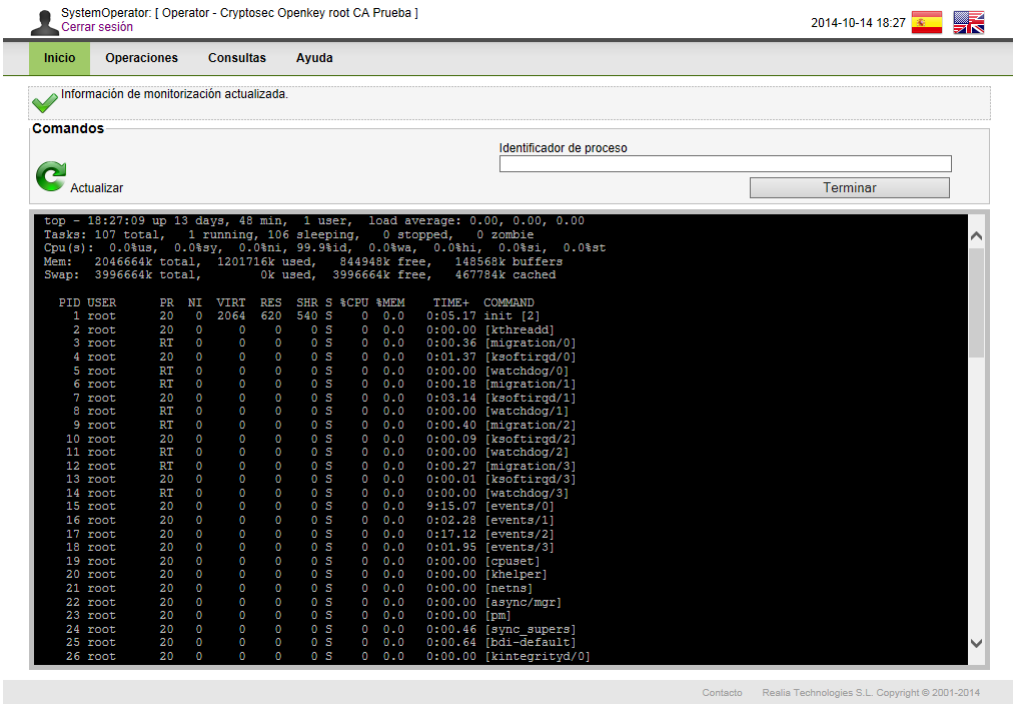


Figura 92: Pantalla con la monitorización del Sistema Operativo.

2.2.4.1.2. Administración de servicios

Mediante esta opción, el usuario puede realizar las siguientes acciones:

- Reiniciar el servidor web
- Parar el servicio de la base de datos
- Iniciar el servicio de la base de datos
- Reiniciar el servicio de la base de datos
- Reiniciar el servicio https.

Para ello, debemos presionar sobre el icono correspondiente a la acción que queramos llevar a cabo (Fig. 93).

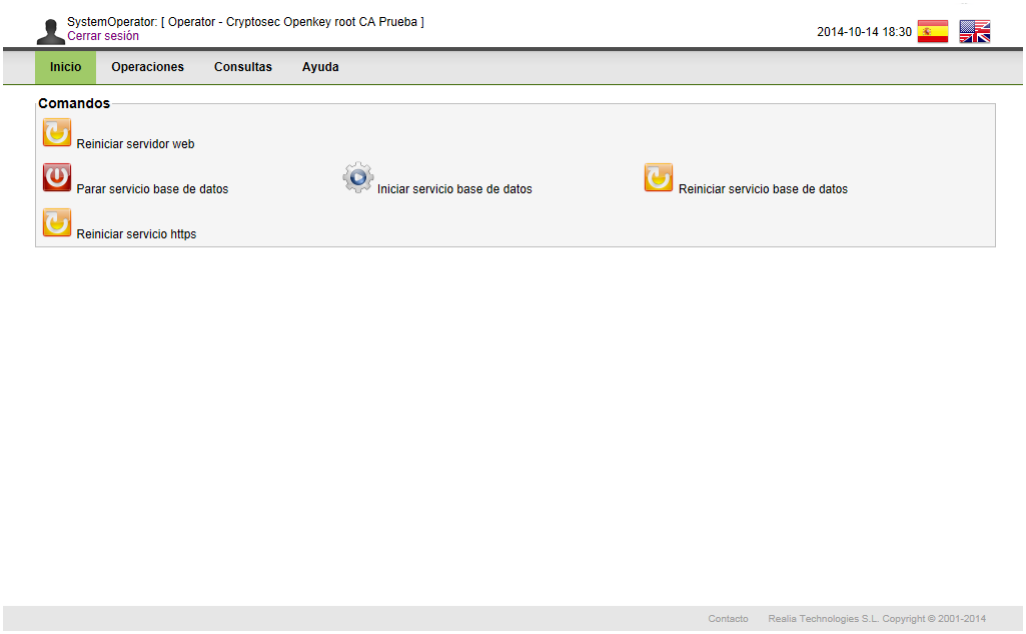


Figura 93: Pantalla con los servicios que podemos administrar.

2.2.4.1.3. Copia de seguridad de datos

La finalidad de esta funcionalidad es la de generar y descargar el fichero de backups de datos, para ello debemos presionar el botón *Generar*, de forma que se actualice el backup de datos y posteriormente presionamos sobre *Descargar* para guardarnos el backup de datos y poderlo importar posteriormente.

La primera vez que accedemos a este punto de la interfaz, si no hay un backup automático ya generado (ver apartado 2.2.2.1.4) , podemos apreciar la siguiente pantalla(Fig. 94).

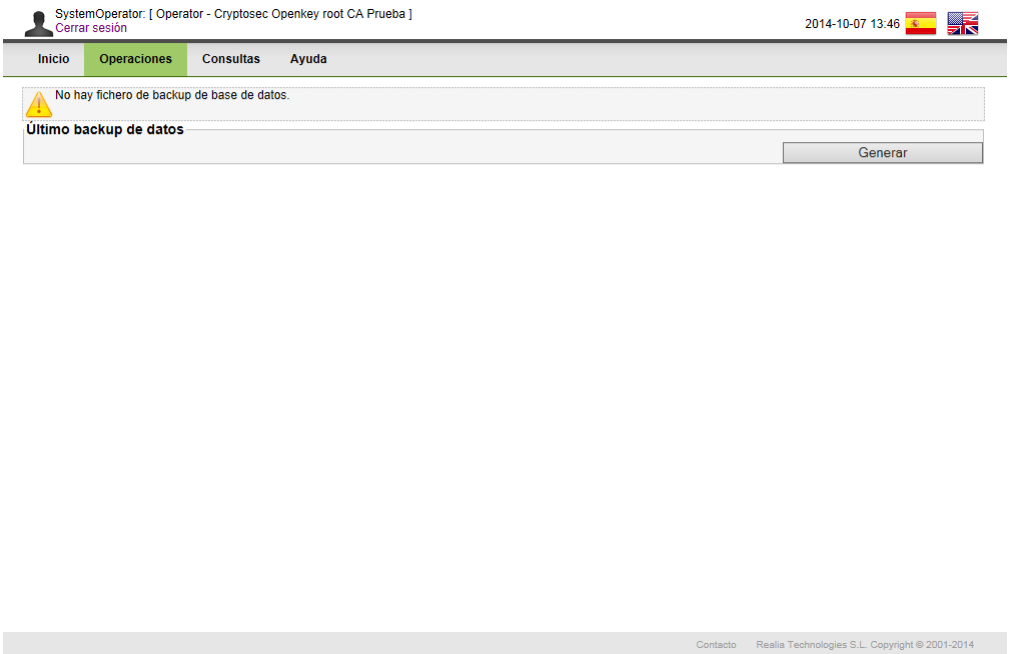


Figura 94: Pantalla de backup de datos.

En este caso, no hay ningún backup de datos generado.

Una vez pulsemos en 'Generar' se inicia el proceso de generación de backup. Cuando este proceso termine, nos mostrará en esta misma pantalla los archivos que componen el backup de datos para que podamos descargarlos (Fig. 95). Después podremos restaurar dicho backup con el usuario con el rol correspondiente (Ver apartado 2.2.1.1.6).

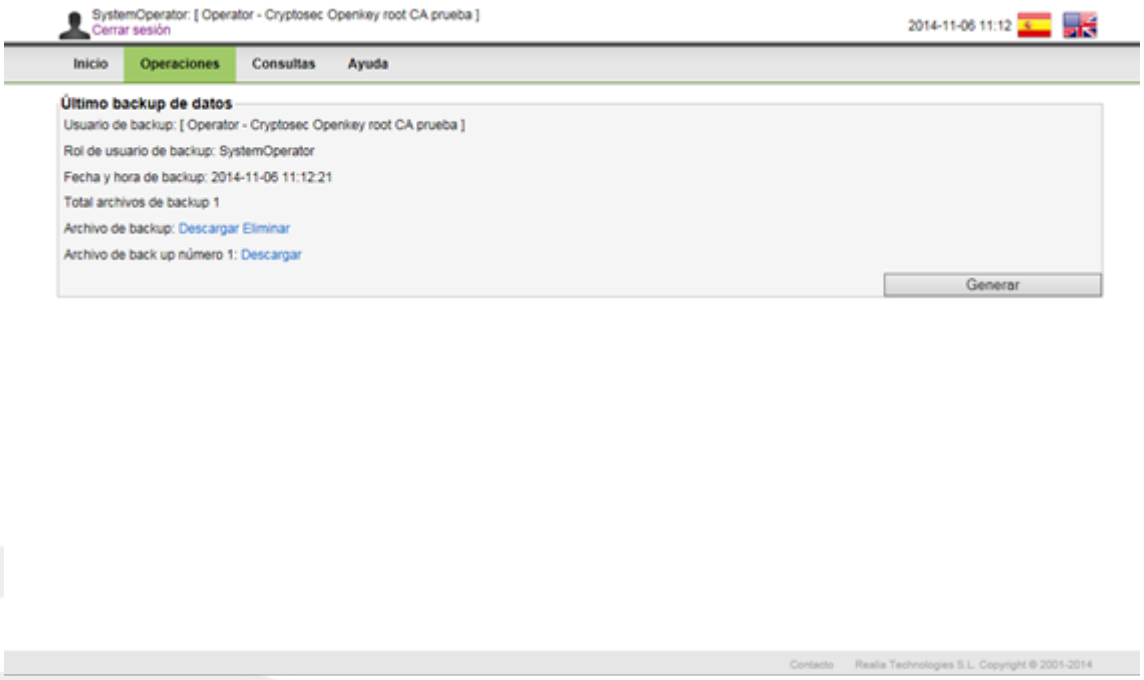


Figura 95: Pantalla para generar y descargar backup de datos.

Observar que el backup se compone de dos partes:

- Un archivo .zip descriptor del back up y de los archivos que lo componen.
- Uno o más archivos (el número depende del tamaño de nuestra base de datos) que componen los datos de la base de datos.

Cuando se procede a ejecutar un proceso de un backup manual de datos, las siguientes operaciones no están disponibles en la interfaz:

1. Otro backup manual de datos.
2. Restauración.
3. Backup manual de claves.
4. Parar, iniciar o reiniciar los servicios de base de datos.

Hasta que nuestra operación de generación de backup haya terminado.

2.2.4.2. Consultas

2.2.4.2.1. Logs

Mediante esta operación, podemos descargarnos los logs de software de la interfaz, los logs de servidor web y los logs de base de datos (Fig. 96). Si marcamos el campo *Seleccionar* y presionamos *Eliminar*, una vez aceptada la advertencia, se borra el log.

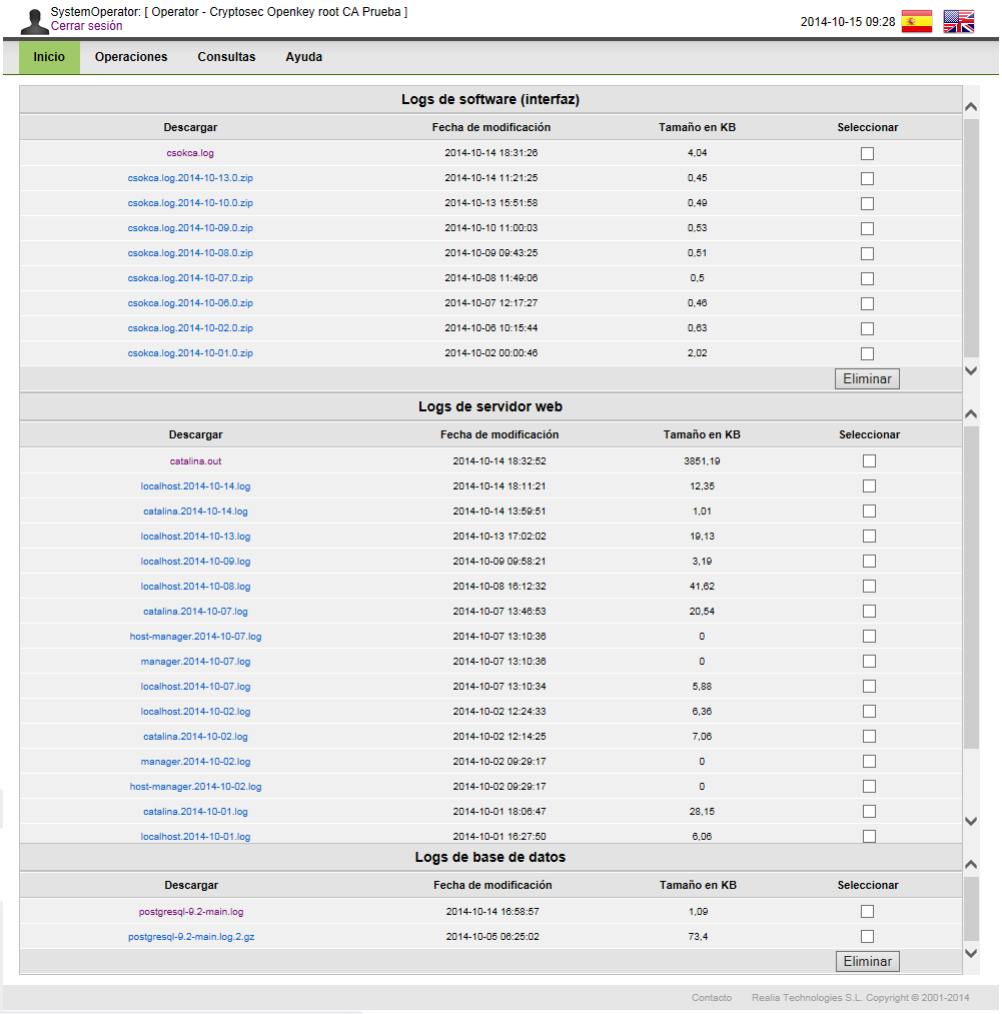


Figura 96: Pantalla de Logs.

3. Servicio TSP

El servicio TSP es el encargado de procesar las peticiones TSP enviadas sobre HTTP por las aplicaciones y servicios que solicitan sellos de tiempo a la TSA (por ejemplo para incorporarlos a firmas). Dicho servicio, envía las respuestas que contienen los sellos de tiempo emitidos conforme al estándar [RFC3161] y a la configuración introducida por el administrador de seguridad (ver sección 2.2.1.1.2).

La URL para acceder a dicho servicio es

`http://IP_servidor/CryptosecOpenKey/tsa_service`

Donde IP_servidor es, como hemos indicado antes, la dirección ip por defecto del equipo indicada por el equipo de REALSEC.

4. Preguntas frecuentes

1. **Si no nos permite ver el listado de certificados con los que podemos acceder a la interfaz y por lo cual tampoco acceder a ella:**

Si intenta acceder con Internet Explorer, compruebe que la URL se encuentra en sitios de confianza del navegador.

2. **La configuración de la seguridad de Java, depende de la versión del mismo.**
3. **Si intentamos acceder desde Google Chrome y el CN del certificado no coincide con IP_servidor, el navegador mostrará como que el certificado no es seguro, por lo que tendremos que presionar 'acceder de todas formas'.**
4. **Al intentar generar o restaurar un backup de datos aparece un error 504, o Timeout:**

   Puede ocurrir que al intentar generar un backup de datos, dependiendo del tamaño de la base de datos, la petición tarde tanto en ejecutarse que aparezca un error debido a la configuración servidor, de la red o del navegador cliente. Aunque aparezca este error, el servicio de backup seguirá ejecutándose hasta terminar de generar los archivos correspondientes. Esto no es ningún problema simplemente volvemos a acceder y pasado un tiempo suficiente para que finalice el proceso (tiempo a determinar dependiendo del tamaño de los datos) tendremos los archivos disponibles para descargar.

   En el caso de la restauración, la solución del problema es similar, con la particularidad de que puede ocurrir también en la subida de los archivos de datos, simplemente, volvemos a acceder para comprobar ha terminado el proceso de subida de archivos o en su caso, del proceso de ejecución de la restauración del backup.

5. **El servicio TSP no funciona. Al intentar firmar un documento, aparece un mensaje de error o la URL del TSP está inaccesible, a pesar de que la aplicación está accesible:**

   Compruebe con el administrador de seguridad que

   a) El certificado raíz de TSA ha sido generado y está firmado por la CA correspondiente (ver 2.2.1.1.3 en este documento).

   b) Compruebe que el certificado raíz tiene el uso extendido de clave 'timestamping'.

   c) Revise la configuración de TSA (ver 2.2.1.1.2).