
Banco de México



**Aplicativo WEBSEC Banxico
(WEBSEC)
Manual de Usuario**

Versión A

WEBSEC	Versión: A
Manual de Usuario	Fecha: 26/08/2011
Manual de Usuario_Externos.docx	

Tabla de Contenido

1	Introducción	3
1.1	Alcance	3
1.2	Vista General	3
2	De la Aplicación	3
2.1	Descripción Funcional	3
2.2	Descripción de la Operación del Sistema	3
2.3	Requisitos Previos	3
2.3.1	De Instalación	3
2.3.2	Para el Acceso	4
3	Operación de la Aplicación	4
3.1	Funciones Principales	4
3.1.1	Autenticación de usuario	4
3.1.2	Firmar archivos	6
3.1.3	Cifrar archivo	8
3.1.4	Ensobretar	10
3.1.5	Verificar archivos	12
3.1.6	Descifrar archivo	15
3.1.7	Abrir sobre	17
3.2	Funciones Secundarias	19
3.2.1	Administrar Certificados	19
3.2.2	Configuración del Sistema	21
3.2.3	Detalle de Certificados	23
4	Información Adicional	25
4.1	Contactos	25

WEBSEC	Versión: A
Manual de Usuario	Fecha: 26/08/2011
Manual de Usuario_Externos.docx	

Manual de Usuario

1 Introducción

El presente documento representa una guía de apoyo al usuario para acceder y operar el aplicativo WEBSEC 2.0.0 de Banco de México.

WEBSEC 2.0.0 brinda herramientas de seguridad que permiten a los usuarios el intercambio de información por medios electrónicos, garantizando la integridad, autenticidad, no repudio y confidencialidad de los documentos electrónicos. El sistema es administrado por la Dirección de Sistemas de Pagos (DSP) de Banco de México.

1.1 Alcance

Este documento está dirigido tanto a las instituciones financieras como a usuario internos de Banco de México, principalmente funcionarios de la institución, que requieren realizar intercambio de información por medios electrónicos de una manera segura y confidencial.

1.2 Vista General

Este manual introduce al Usuario a la operación del WEBSEC 2.0.0, presentando los principales componentes, operación y contactos operativos que pueden brindar ayuda en caso de alguna observación o duda sobre el funcionamiento del sistema.

2 De la Aplicación

2.1 Descripción Funcional

WEBSEC 2.0.0 es una aplicación que aprovecha las características de seguridad de la Infraestructura de Seguridad Extendida (IES), desarrollada por el Banco de México, para el intercambio seguro de información a través de medios electrónicos.

WEBSEC 2.0.0 hace uso de un formato estándar en protección de datos y mantiene la compatibilidad de lectura con los formatos actuales.

2.2 Descripción de la Operación del Sistema

Las operaciones que se pueden realizar dentro de la aplicación son:

- Firmar documentos electrónicos.
- Cifrar documentos electrónicos.
- Ensobretar documentos electrónicos.
- Verificar firma digital.
- Descifrar documentos electrónicos.
- Abrir sobre.

2.3 Requisitos Previos

2.3.1 De Instalación

A continuación se listan los requerimientos mínimos para la instalación de la aplicación:

- 1 GB de memoria RAM.
- 640 MB reservados para el uso de la aplicación WEBSEC.
- Sistema Operativo Windows, Linux o MacOS.

WEBSEC	Versión: A
Manual de Usuario	Fecha: 26/08/2011
Manual de Usuario_Externos.docx	

- Versión del JRE 1.6 o superior.
- Resolución de pantalla recomendada 1280 x 1024; Mínima de 1220 x 800.
- Para la instalación se requieren permisos de administrador.

2.3.2 Para el Acceso

Para ingresar a la aplicación y poder hacer uso de todas las funciones es necesario que contar con un certificado digital válido compatible con la Infraestructura Extendida de Seguridad como los son los certificados emitidos por Banco de México, SAT y CECOBAN.

En caso de no contar con un certificado digital propio es posible ingresar a la aplicación con el certificado general, configurado por default durante la instalación, sin embargo, la funcionalidad de la aplicación es limitada y únicamente se tienen disponibles las opciones para Cifrar archivo y Verificar archivos.

3 Operación de la Aplicación

3.1 Funciones Principales

3.1.1 Autenticación de usuario

Esta opción permite que el usuario se identifique adecuadamente para realizar las operaciones que así lo requieran. La aplicación mostrará la siguiente pantalla:

Los campos que se deben llenar son:

(I) Certificado

Indicar la ubicación y el archivo que contiene el certificado del usuario.

Puede seleccionar el archivo si pulsa sobre el botón situado a la derecha de la caja de texto.

WEBSEC	Versión: A
Manual de Usuario	Fecha: 26/08/2011
Manual de Usuario_Externos.docx	

(II) Clave privada

Indicar la ubicación y el archivo que contiene la llave privada correspondiente al certificado indicado en el campo anterior.

Puede seleccionar el archivo si pulsa sobre el botón situado a la derecha de la caja de texto.


(III) Frase de seguridad

Introducir su frase de seguridad correspondiente a la clave privada. Este campo no muestra los caracteres tecleados.

(IV) Ingresar con certificado de uso general

En caso de no contar con un certificado digital personal que lo identifique en forma exclusiva, se puede ingresar a la aplicación con el certificado de uso general, sin embargo, la funcionalidad de la aplicación es limitada y únicamente se tienen disponibles las opciones para Cifrar archivo y Verificar archivos.



Si se pulsa el botón  y los datos proporcionados fueron correctos el usuario queda identificado a partir de este momento.

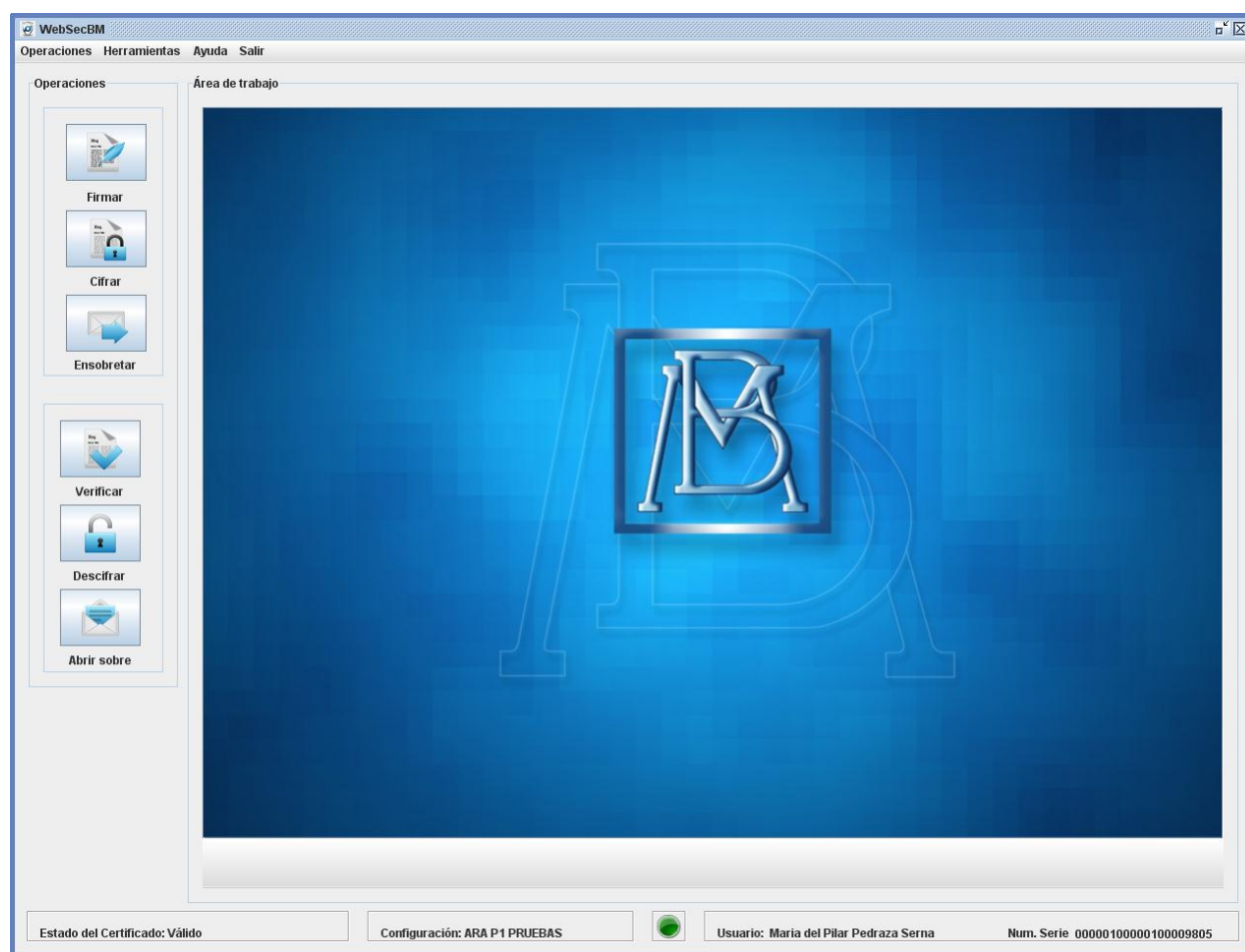
En caso de que los archivos proporcionados no existan o sean inválidos, o la frase de seguridad no corresponda a la clave privada se muestra un cuadro de diálogo con un mensaje de error y deberá repetir la operación.



Si se pulsa el botón  se terminará la ejecución del programa.

Una vez autenticado el usuario se activará el menú principal:

WEBSEC	Versión: A
Manual de Usuario	Fecha: 26/08/2011
Manual de Usuario_Externos.docx	



Si durante la ejecución del programa desea identificarse con otro certificado y clave privada, puede activar la pantalla de “Autenticación de Usuario” mediante la opción del menú Herramientas | Cambiar de usuario.

3.1.2 Firmar archivos

Con esta opción se puede agregar una firma digital a los documentos electrónicos seleccionados para que sea posible comprobar la integridad de los mismos y así garantizar su autenticidad. Al seleccionar esta opción se activará la siguiente pantalla:

WEBSEC	Versión: A
Manual de Usuario	Fecha: 26/08/2011
Manual de Usuario_Externos.docx	

Y los campos que se deben capturar son:


(I) DOCUMENTOS A FIRMAR ELECTRÓNICAMENTE

Para agregar los documentos electrónicos que requiere firmar se debe seleccionar la opción



, y proporcionar la ruta y nombre de cada archivo origen.




Adicionalmente, se tendrá la opción , para eliminar los documentos que ya no requiera firmar.

(II) ARCHIVOS DESTINO

Esta sección se llena automáticamente con la ruta y nombre por default para el archivo destino, la cual corresponde a la misma ruta y el mismo nombre del documento electrónico original, con la extensión “**fbm**”, correspondiente a los archivos firmados. Deberá existir un archivo destino por cada archivo a firmar.


Adicionalmente, si se requiere cambiar el nombre y/o ruta del archivo destino se debe pulsar el botón “Cambiar” ubicado a la derecha del cuadro de texto.




La opción  limpia los campos capturados tanto del documento a firmar como del

WEBSEC	Versión: A
Manual de Usuario	Fecha: 26/08/2011
Manual de Usuario_Externos.docx	

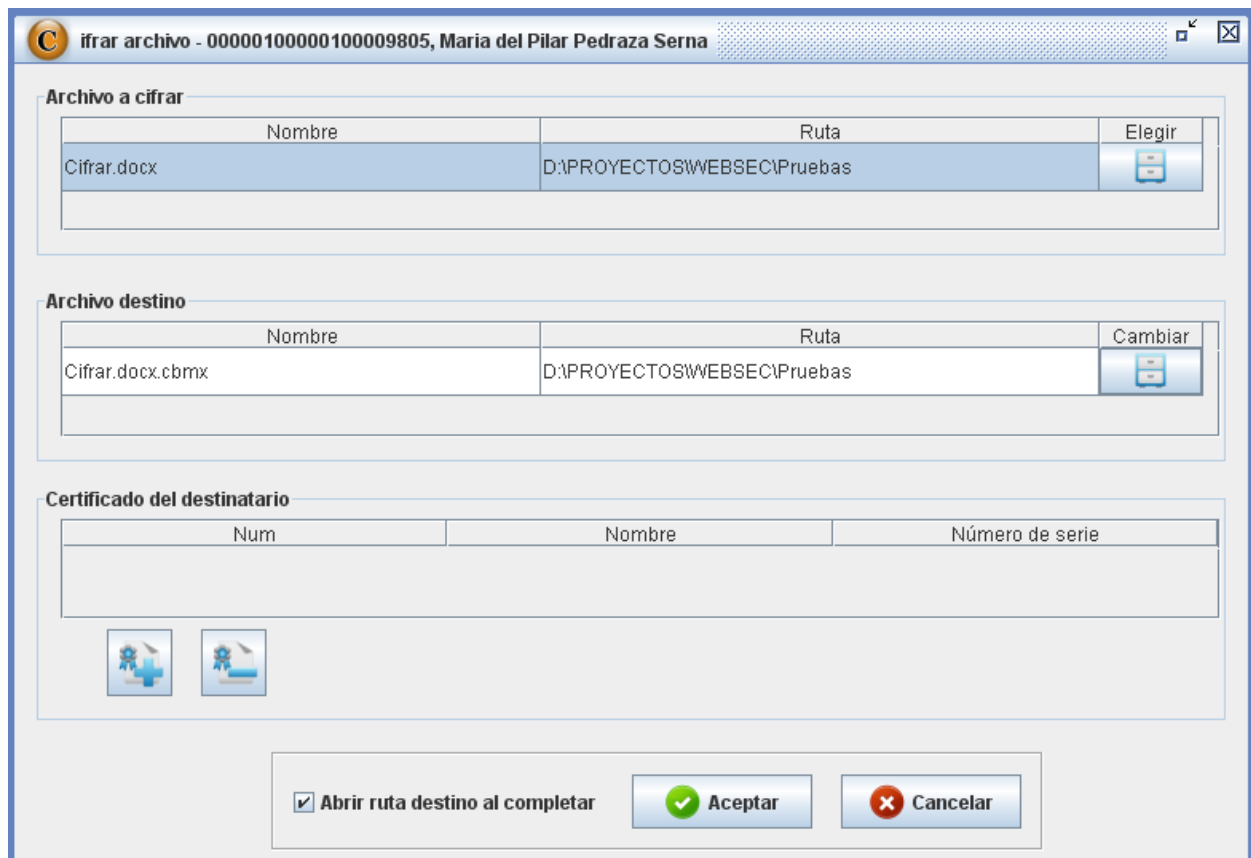
archivo destino, permitiendo iniciar una nueva captura.

Para iniciar el proceso de firma se debe pulsar el botón . En caso de haber algún error en el proceso de validación de la información o del firmado, se muestra un cuadro de diálogo con el mensaje de error correspondiente.

Si se pulsa el botón  no se llevará a cabo la firma del documento electrónico.

3.1.3 Cifrar archivo

Esta opción permite cifrar un documento electrónico, para asegurar la confidencialidad del mismo, ya que sólo podrá ser descifrado por el propietario del certificado seleccionado como destinatario. Al seleccionar esta opción se activará la siguiente pantalla:



Y los campos que se deben capturar son:

(I) ARCHIVO A CIFRAR

Para agregar el documento electrónico que requiere cifrar se debe pulsar el botón “Elegir”, esto permitirá buscar la ruta y nombre del archivo mediante el explorador de Windows.

WEBSEC	Versión: A
Manual de Usuario	Fecha: 26/08/2011
Manual de Usuario_Externos.docx	


(II) ARCHIVO DESTINO

Al seleccionar el archivo a cifrar, se presenta automáticamente el nombre por default para el correspondiente archivo destino, en la misma ruta y con el mismo nombre del documento electrónico a cifrar, agregando la extensión “**cbmx**” correspondiente a los archivos cifrados.

Si requiere cambiar el nombre y/ ruta del archivo se puede pulsar el botón “Cambiar” ubicado a la derecha del cuadro de texto.

(III) CERTIFICADO DEL DESTINATARIO



Para seleccionar el certificado del destinatario del archivo cifrado, se debe pulsar el botón  y se mostrará la lista de certificados registrados localmente. Esta lista aparecerá vacía inicialmente:

Certificados registrados					
Búsqueda por nombre <input type="text"/>					
	Número de serie	Nombre común	Último estado	Fecha	Detalle
1	00000100000100009801	Pruebas UNO - Mena Angelito Pedro	Válido	23/05/2011 17:13...	
2	00000100000100009802	Pruebas DOS - Mena Angelito Pedro	Válido	23/05/2011 17:14...	
3	00000700000700000085	una pru0035	Sin verificar	23/05/2011 17:14...	
4	00000100000100009809	Certificado Alertado	No válido	23/05/2011 17:23...	

Para seleccionar el certificado del destinatario debe pulsar una vez sobre el renglón que contiene el



certificado deseado y . Una vez que ha sido seleccionado, se llenará el campo “Certificado del destinatario” con el nombre y número de serie correspondiente.

(IV) ABRIR RUTA DESTINO AL COMPLETAR CIFRAR

Esta opción permite abrir en el Explorador de Windows la ruta del documento cifrado, después de guardarlo en la ubicación especificada.



Para iniciar el proceso de cifrado se debe pulsar el botón . En caso de haber algún error en el proceso de validación de la información o del cifrado, se muestra un cuadro de diálogo con el mensaje de error correspondiente.



Si se pulsa el botón no se llevará a cabo el proceso de cifrado.

WEBSEC	Versión: A
Manual de Usuario	Fecha: 26/08/2011
Manual de Usuario_Externos.docx	

3.1.4 Ensobretar

Esta opción permite firmar y cifrar un documento electrónico, el cual puede estar dirigido a uno o más destinatarios, lo cual garantiza la confidencialidad y autenticidad del documento.

Al seleccionar esta opción se activará la siguiente pantalla:

The screenshot shows a software interface for document signing and encryption. The window title is "nsobretar documentos - 00000100000100009805, Maria del Pilar Pedraza Serna". The interface is divided into three main sections:

- Archivo a ensobretar:** A table with columns "Nombre" and "Ruta". The first row contains "Ensobretar.docx" and "D:\PROYECTOS\WEBSEC\Pruebas". To the right of the table is an "Elegir" button with a folder icon.
- Archivo destino:** A table with columns "Nombre" and "Ruta". The first row contains "Ensobretar.docx.sbm" and "D:\PROYECTOS\WEBSEC\Pruebas". To the right of the table is a "Cambiar" button with a folder icon.
- Destinatarios:** A table with columns "Num", "Nombre", and "Número de serie". Below the table are several icons: two document icons with a plus sign, two arrows (up and down), and a globe icon.

At the bottom of the window, there is a checkbox labeled "Abrir ruta destino al completar" which is checked. To its right are two buttons: "Aceptar" (with a green checkmark icon) and "Cancelar" (with a red X icon).

Y los campos que se deben capturar son:

(I) ARCHIVO A ENSOBRETAR

Para agregar el documento electrónico que requiere ensobretar se debe pulsar el botón "Elegir", permitirá buscar la ruta y nombre del archivo mediante el explorador de Windows.

(II) ARCHIVO DESTINO


Este campo se llena automáticamente con la ruta y nombre por default para el archivo destino, la cual corresponde a la misma ruta y el mismo nombre del documento electrónico original, con la extensión "sbm", correspondiente a los archivos ensobretados.

Si requiere cambiar el nombre y/o ruta del archivo se puede pulsar el botón "Cambiar" ubicado a la derecha del cuadro de texto.

WEBSEC	Versión: A
Manual de Usuario	Fecha: 26/08/2011
Manual de Usuario_Externos.docx	

(III) DESTINATARIOS




Para seleccionar el certificado del destinatario del archivo ensobretado, se debe pulsar el botón  y se mostrará la lista de certificados registrados localmente. Es posible agregar más de un destinatario del documento.

Esta lista aparecerá vacía inicialmente:

Certificados registrados					
Búsqueda por nombre <input type="text"/>					
	Número de serie	Nombre común	Último estado	Fecha	Detalle
1	00000100000100009801	Pruebas UNO - Mena Angelito Pedro	Válido	23/05/2011 17:13...	
2	00000100000100009802	Pruebas DOS - Mena Angelito Pedro	Válido	23/05/2011 17:14...	
3	00000700000700000085	una pru0035	Sin verificar	23/05/2011 17:14...	
4	00000100000100009809	Certificado Alertado	No válido	23/05/2011 17:23...	

 **Agregar**

 **Elegir**  **Regresar**

Para seleccionar el certificado del destinatario debe pulsar una vez sobre el renglón que contiene el certificado deseado y pulsar el botón .

Para seleccionar más de un destinatario debe mantener pulsada la tecla CTRL y pulsar sobre cada uno de los certificados que desea agregar como destinatarios, posteriormente pulsar el botón



Una vez que ha sido seleccionado, se llenará el campo "Certificado del destinatario" con los nombres y números de serie correspondientes.

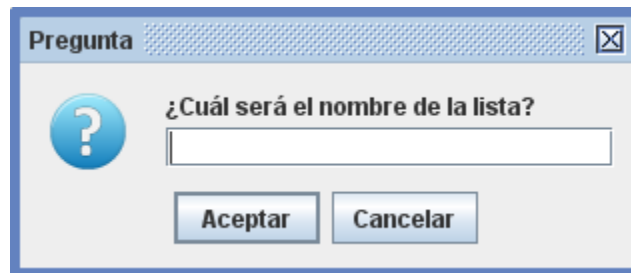
(IV) GUARDAR LISTA DE DESTINATARIOS


Es posible guardar la lista de los destinatarios en un archivo, para lo cual se debe pulsar sobre el botón




"Guardar Lista de Destinatarios". Se mostrará la siguiente pantalla, y deberá introducir el nombre de la lista a crear:

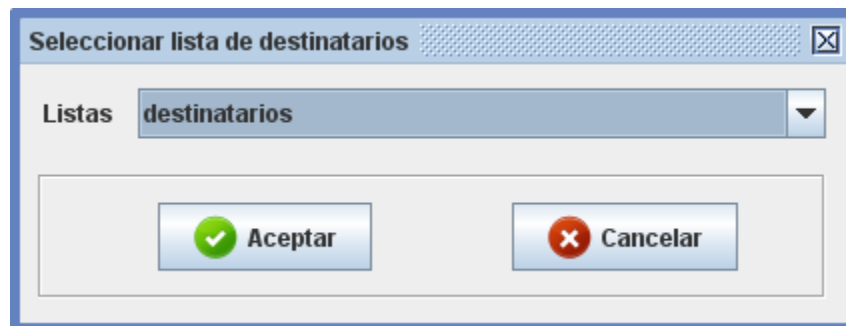
WEBSEC	Versión: A
Manual de Usuario	Fecha: 26/08/2011
Manual de Usuario_Externos.docx	




Para guardar la lista de destinatarios deberá pulsar sobre el botón .

(V) RECUPERAR DESTINATARIOS DESDE LISTA

Para hacer uso de esta función se debe pulsar sobre el botón “Recuperar Lista de Destinatarios” , se mostrarán las listas que han sido almacenadas de manera local tal como se muestra en la siguiente pantalla:





Seleccione la lista deseada y enseguida pulse el botón .

Los nombres y números de serie de los certificados contenidos en la lista aparecerán en el campo (III) Destinatarios.

(VI) ABRIR RUTA DESTINO AL FINALIZAR

Esta opción permite abrir en el Explorador de Windows la ruta del documento ensobretado, después de guardarlo en la ubicación especificada.

Para iniciar el proceso de ensobretado se debe pulsar el botón . En caso de haber algún error en el proceso de validación de la información o del ensobretado, se muestra un cuadro de diálogo con el mensaje de error correspondiente.

Si se pulsa el botón  no se llevará a cabo el proceso de ensobretado.

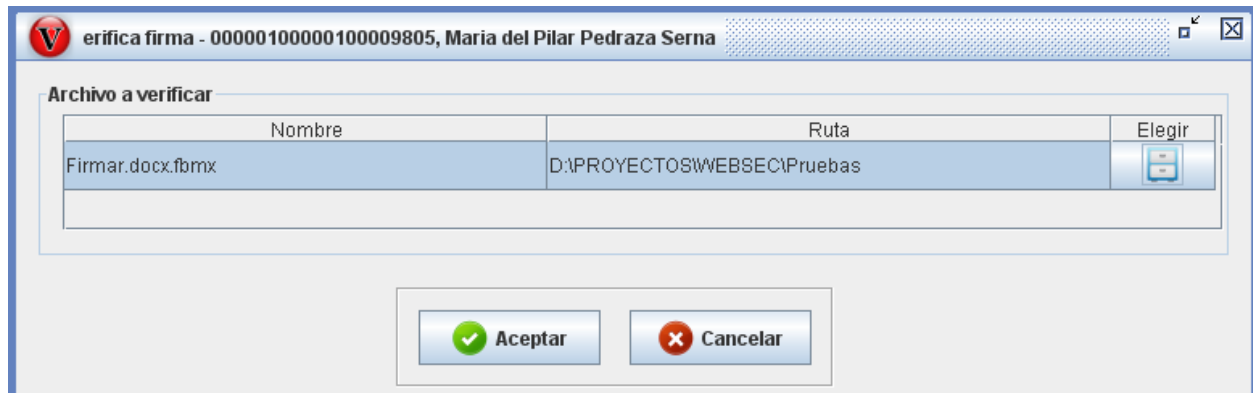
3.1.5 Verificar archivos

Esta opción permite verificar las firmas de un documento electrónico para poder confirmar la identidad de los firmantes y que el archivo original no fue alterado después de haber sido firmado.


WEBSEC	Versión: A
Manual de Usuario	Fecha: 26/08/2011
Manual de Usuario_Externos.docx	

WEBSEC 2.0.0 permite la verificación de archivos firmados con la versión anterior WEBSEC 1.2.0.3, los cuales cuentan con la extensión “fbm”.

Al seleccionar esta opción se activará la siguiente pantalla:

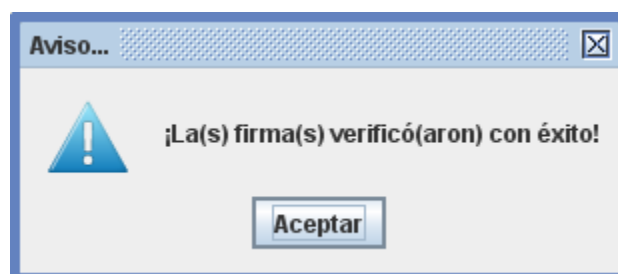



Para ingresar el documento electrónico cuya firma se requiere verificar, debe pulsar el botón “Elegir” situado a la derecha de la caja de texto, con lo que aparecerá una ventana estándar de Windows donde podrá seleccionar la ruta y nombre del archivo.

Al pulsar el botón  se llevan a cabo los procesos siguientes:

- Se verifica el formato del archivo.
- Se obtienen los certificados para verificar las firmas contenidas en el archivo.

Y se presentará un mensaje con el resultado de la verificación:



Para continuar debe pulsar el botón  y se activará la pantalla que muestra el detalle de las firmas verificadas:

WEBSEC	Versión: A
Manual de Usuario	Fecha: 26/08/2011
Manual de Usuario_Externos.docx	

Firmas verificadas para documento Firmar.docx.fbm

Archivo verificado

Nombre	Ruta	Resultado
Firmar.docx.fbm	D:\PROYECTOS\WEBSEC\Pruebas	Verificó

¡La(s) firma(s) verificó(aron) con éxito!

[Ver firmas identificadas >>>](#)

Agregar firma

[Firmar archivo](#) [Firma definitiva](#)

Extraer archivo

Nombre	Ruta	Cambiar
Firmar.docx	D:\PROYECTOS\WEBSEC\Pruebas	

Abrir la ruta destino al guardar [Guardar archivo](#)

[Regresar](#)

Firmas verificadas para documento Firmar.docx.fbm

Archivo verificado

Nombre	Ruta	Resultado
Firmar.docx.fbm	D:\PROYECTOS\WEBSEC\Pruebas	Verificó

¡La(s) firma(s) verificó(aron) con éxito!

[Ocultar firmas identificadas <<<](#)

Firmas identificadas

Firmante	Número de serie	Estado de firma	Estado certificado	Detalle
Maria del Pilar Pedraza Serna	00000100000100009805	Verificó	Válido	

Agregar firma

[Firmar archivo](#) [Firma definitiva](#)

Extraer archivo

Nombre	Ruta	Cambiar
Firmar.docx	D:\PROYECTOS\WEBSEC\Pruebas	

Abrir la ruta destino al guardar [Guardar archivo](#)

[Regresar](#)

WEBSEC	Versión: A
Manual de Usuario	Fecha: 26/08/2011
Manual de Usuario_Externos.docx	

Los campos que se muestran son:

(I) ARCHIVO VERIFICADO

Este campo muestra el nombre y la ruta del documento electrónico cuya firma se ha verificado, y el resultado de la verificación:

- Verificó (Verde) - Todas las firmas fueron verificadas y son válidas.
- Verificó (Amarillo) – Todas las firmas fueron verificadas, pero una o más firma tiene estado no válido.
- No Verificó (Rojo) – Una o más de las firmas no pudo ser verificada.

(II) FIRMAS IDENTIFICADAS

Esta opción permite mostrar cada una de las firmas identificadas en el archivo verificado, con la siguiente información:

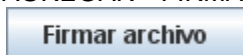
- Nombre asociado al certificado o Firmante.
- Número de serie del certificado.
- Estado de la firma: Verificó o No Verificó.
- Estado del certificado: Válido o No Válido
- Opción para consultar más información sobre el certificado, pulsando sobre la opción “Detalle”



(III) AGREGAR FIRMA

Esta opción permite realizar operaciones con firmas sobre el archivo verificado:

- **AGREGAR FIRMA:** Para agregar firma al archivo verificado debe pulsar el botón



Esta opción sólo estará disponible para archivos firmados con el formato nuevo, y no se permitirá agregar firmas duplicadas (que ya se encuentren en el archivo).

- **FIRMA DEFINITIVA:** Esta opción permite al usuario extraer el documento electrónico contenido en el archivo y generar un nuevo archivo con sólo la firma del usuario identificado, pulsando el



El archivo original es sustituido por el archivo con la firma definitiva en caso de encontrarse en el formato nuevo.

(IV) EXTRAER ARCHIVO

Esta opción presenta inicialmente el nombre y ruta por default del archivo destino donde se guardará el documento electrónico contenido en el archivo verificado.

Si requiere cambiar el nombre y/ ruta del archivo se puede pulsar el botón “Cambiar” ubicado a la derecha del cuadro de texto.

(V) GUARDAR ARCHIVO

Esta opción permite guardar el documento electrónico extraído del archivo verificado (sin la firma) en la ruta y con el nombre especificados.

(VI) ABRIR RUTA DESTINO AL GUARDAR

Esta opción permite abrir en el Explorador de Windows la ruta del documento extraído del archivo verificado, después de guardarlo en la ubicación especificada.

3.1.6 Descifrar archivo

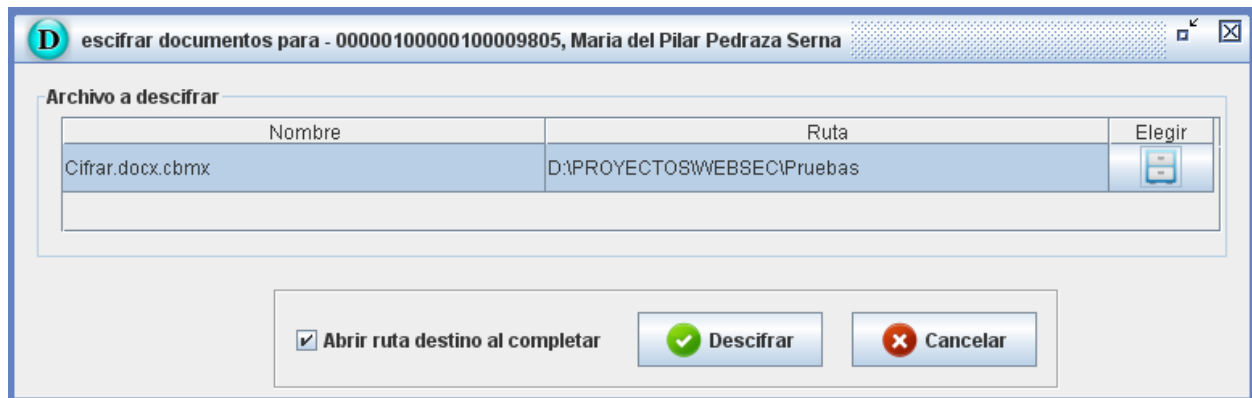
Esta opción permite ver el contenido de un archivo cifrado, mediante la operación de descifrado, siempre

WEBSEC	Versión: A
Manual de Usuario	Fecha: 26/08/2011
Manual de Usuario_Externos.docx	

que el usuario que intenta realizar la operación sea el destinatario del documento cifrado.

WEBSEC 2.0.0 permite descifrar un archivo que haya sido cifrado con la versión anterior WEBSEC 1.2.0.3, los cuales cuentan con la extensión "cbm".

Al seleccionar esta opción se activará la siguiente pantalla:




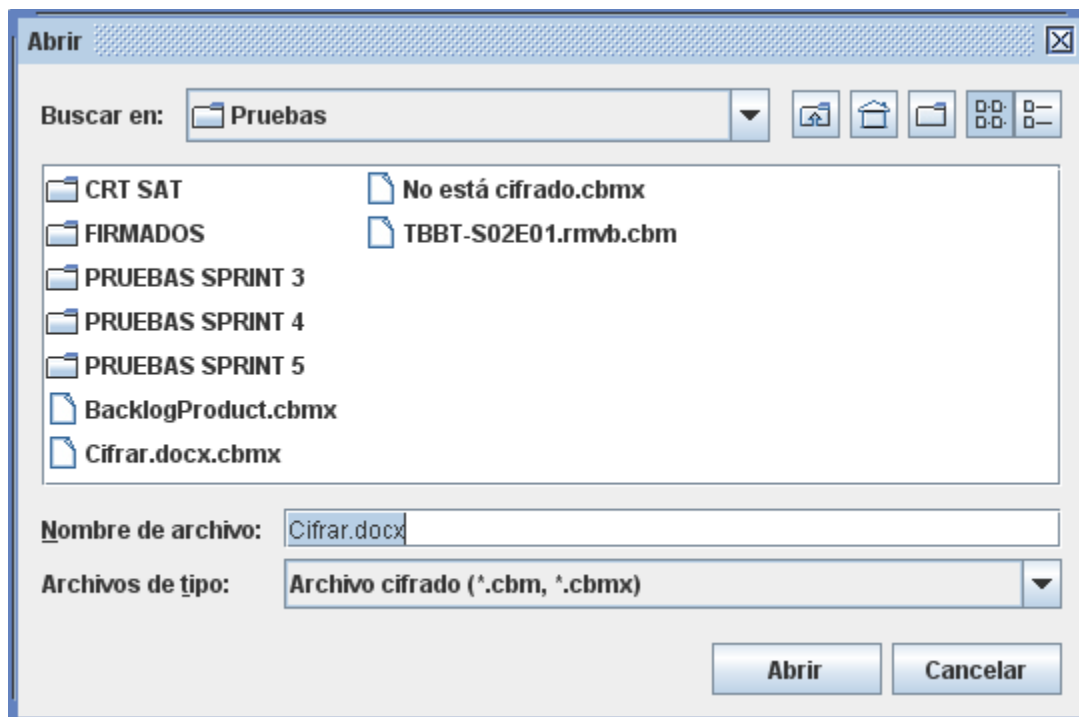
Los campos que se deben capturar:

(I) ARCHIVO A DESCIFRAR

Para ingresar el documento cifrado debe pulsar el botón "Elegir" situado a la derecha de la caja de texto, con lo que aparecerá una ventana estándar de Windows donde podrá seleccionar la ruta y nombre del archivo.



Al pulsar el botón  se llevará a cabo el proceso de descifrado, y se activará la pantalla que permita guardar el archivo descifrado:



WEBSEC	Versión: A
Manual de Usuario	Fecha: 26/08/2011
Manual de Usuario_Externos.docx	

El nombre del archivo destino sugerido es el del archivo original contenido en el archivo cifrado. Adicionalmente se sugiere guardar dentro de la misma ruta del archivo cifrado.

(II) ABRIR RUTA DESTINO AL COMPLETAR

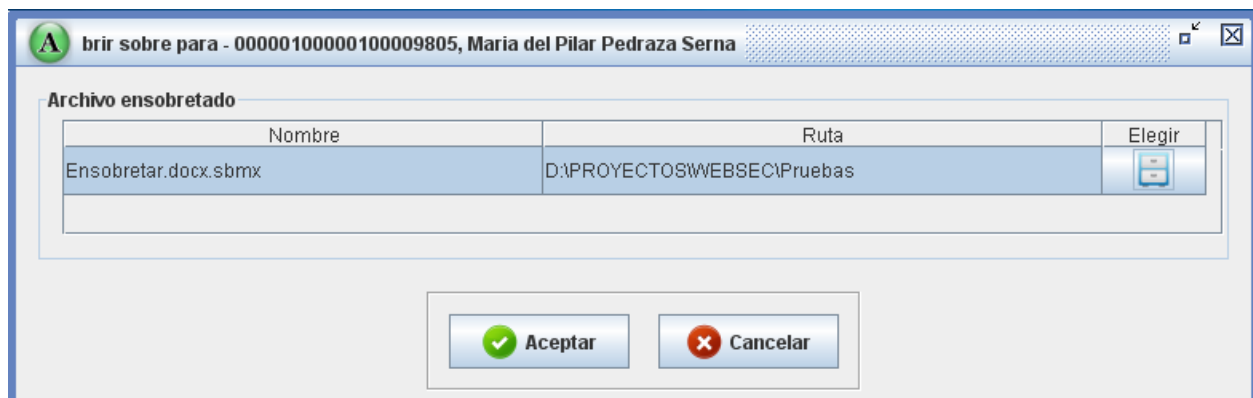
Al seleccionar esta opción, una vez que se haya completado el proceso de descifrar, la aplicación abrirá en el Explorador de Windows la ruta donde se haya guardado el documento descifrado.

3.1.7 Abrir sobre

Esta opción permite ver el contenido de un archivo que ha sido previamente ensobretado, siempre que el usuario que intenta abrir el sobre es destinatario del mismo.


WEBSEC 2.0.0 permite ver el contenido de un archivo que haya sido ensobretado con la versión anterior WEBSEC 1.2.0.3, los cuales cuentan con la extensión “sbm”.

Al seleccionar esta operación se activará la siguiente pantalla:



Para ingresar el documento ensobretado debe pulsar el botón “Elegir” situado a la derecha de la caja de texto, con lo que aparecerá una ventana estándar de Windows donde podrá seleccionar la ruta y nombre del archivo.

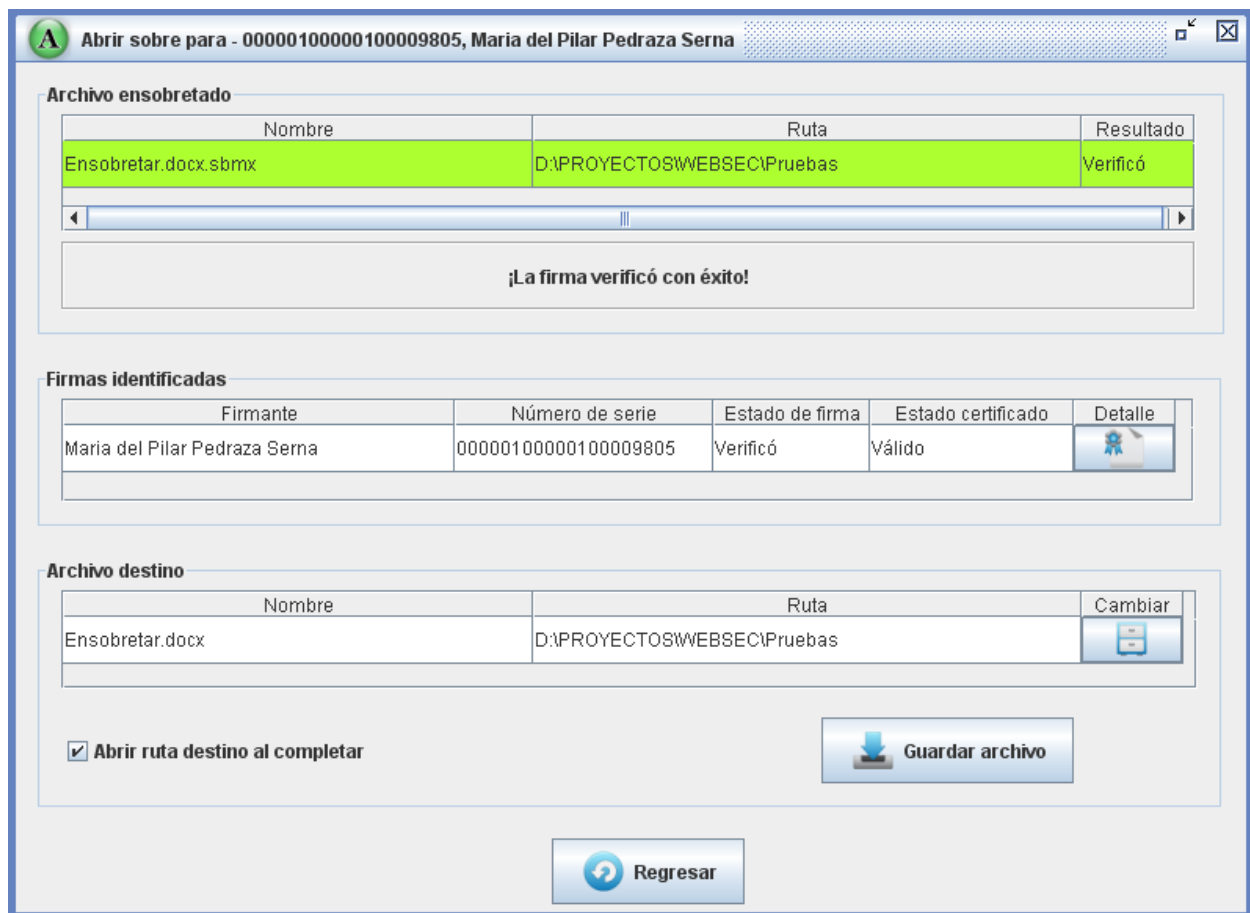


Al pulsar el botón  se llevará a cabo el proceso de verificación de firma y descifrado del archivo y se indicará el resultado mediante una advertencia:



Para continuar debe pulsar el botón , con lo que se activará la pantalla de resultado:

WEBSEC	Versión: A
Manual de Usuario	Fecha: 26/08/2011
Manual de Usuario_Externos.docx	



Los campos que se muestran son:

(I) ARCHIVO ENSOBRETADO

Se muestra el nombre y la ruta del documento electrónico que se abrió y el resultado de la verificación sobre el mismo:

- Verificó (Verde) - Todas las firmas fueron verificadas y son válidas.
- Verificó (Amarillo) – Todas las firmas fueron verificadas, pero una o más firma tiene estado no válido.
- No Verificó (Rojo) – Una o más de las firmas no pudo ser verificada.

(II) FIRMAS IDENTIFICADAS

En esta sección se muestra la información de cada certificado que ha firmado el documento con la siguiente información:

- Nombre asociado al certificado o Firmante.
- Número de serie del certificado.
- Estado de la firma: Verificó o No Verificó.
- Estado del certificado: Válido o No Válido
- Opción para consultar más información sobre el certificado, pulsando sobre la opción "Detalle"



WEBSEC	Versión: A
Manual de Usuario	Fecha: 26/08/2011
Manual de Usuario_Externos.docx	

(III) ARCHIVO DESTINO

Esta opción permite guardar el documento electrónico extraído del archivo ensobretado, el nombre y ruta sugerido inicialmente por la aplicación es el del archivo original. Sin embargo, se permite modificar estas especificaciones para generar un archivo destino diferente mediante la opción “Cambiar” ubicada a la derecha de la caja de texto.

Para guardar el archivo con el nombre y ruta indicados deberá pulsar el botón



(IV) ABRIR RUTA DESTINO AL COMPLETAR

Esta opción permite abrir en el Explorador de Windows la ruta del documento extraído del archivo ensobretado, después de haberlo guardarlo en la ubicación especificada.

3.2 Funciones Secundarias

3.2.1 Administrar Certificados

Esta opción permite mantener localmente los certificados que se hayan obtenido de la IES o bien que se hayan agregado a través de archivo:



A través de esta ventana se pueden administrar las referencias a los certificados, y es la misma que se utiliza cuando se seleccionan certificados en las operaciones de Cifrar un Archivo y Ensobretar un Archivo.

La información que se muestra en la pantalla corresponde a:

- Número de serie del certificado digital.
- Nombre común. Nombre del propietario del certificado digital.
- Último estado. Estado del certificado digital consultado en la IES
- Fecha. Última fecha y hora de actualización del estado del certificado consultado en la IES.
- Detalle. Esta opción permite consultar mayor detalle de cada uno de los certificados.

Es posible realizar la búsqueda de un certificado por nombre, tecleando los caracteres requeridos en el campo “Búsqueda por nombre”, de esta manera la aplicación presentará en pantalla únicamente los certificados cuyo nombre coincida con los datos proporcionados.

WEBSEC	Versión: A
Manual de Usuario	Fecha: 26/08/2011
Manual de Usuario_Externos.docx	

Adicionalmente se tienen tres opciones de funcionalidad:

- (I) **Agregar.** Esta opción permite agregar un nuevo certificado a la base local, ya sea mediante



archivo o por conexión a la IES. Al pulsar sobre el botón se activa la pantalla en la cual deberá capturar la información requerida para agregar el certificado:

- Para agregar un certificado desde archivo debe elegir la pestaña “Desde archivo” y pulsar sobre



el botón, ubicado a la derecha del cuadro de texto, esto permite ingresar la ruta y nombre del archivo que contiene el certificado digital.

- Para agregar un certificado desde la IES debe elegir la pestaña “Desde la IES” e ingresar el número de serie correspondiente al certificado digital que desea agregar.




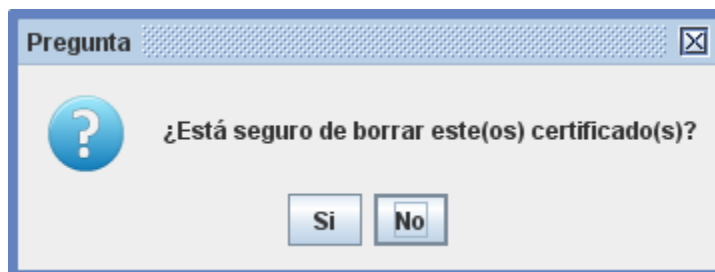
Una vez proporcionados los datos se debe pulsar el botón, y la aplicación guardará de manera local la información consultada en la IES.


WEBSEC	Versión: A
Manual de Usuario	Fecha: 26/08/2011
Manual de Usuario_Externos.docx	

(II) ELIMINAR

Para borrar un certificado almacenado localmente, basta con seleccionar el o los certificados que desea

eliminar y pulsar el botón , enseguida aparecerá un mensaje solicitando confirmar la operación:



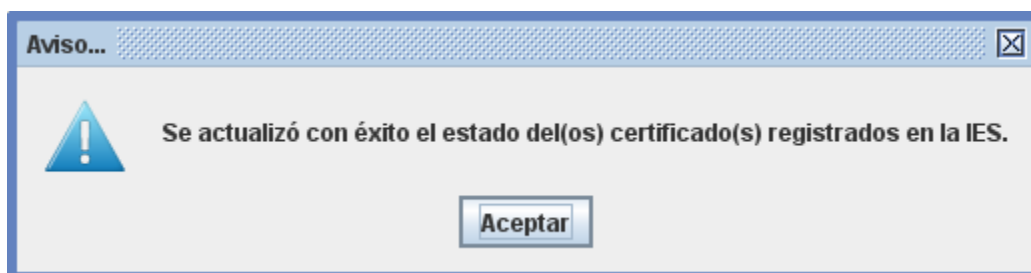
Para concluir el borrado del certificado debe pulsar sobre la opción .

(III) ACTUALIZAR CRT

Esta opción actualiza a demanda el estado de los certificados de acuerdo a la información registrada en el IES, por lo que debe seleccionar el o los certificados de los cuales desea actualizar su estado y pulsar

el botón .

Una vez que la aplicación haya obtenido el estado de los certificados seleccionados, los actualiza de manera local y presenta el siguiente mensaje en pantalla:



3.2.2 Configuración del Sistema

Esta opción permite consultar los parámetros de conexión a la IES configurados por default.

Adicionalmente, se pueden realizar pruebas de conexión y consultar el detalle de los certificados de autoridad y general que permiten la autenticación con la IES.

WEBSEC	Versión: A
Manual de Usuario	Fecha: 26/08/2011
Manual de Usuario_Externos.docx	

Opciones del WebSecBM

Conexión a la IES | Elementos criptográficos

Nombre de la autoridad: ARA P1 PRUEBAS

Dirección IP del servidor: 170 . 70 . 91 . 27 : Puerto: 7090

Probar conexión

Ver certificados de conexión >>>

Remota [d255b35ffa658b95c578765b319cd92f7c3134391e49bb158cd0655cf3ef9de9]

Aceptar Cancelar

Opciones del WebSecBM

Conexión a la IES | Elementos criptográficos

Nombre de la autoridad: ARA P1 PRUEBAS

Dirección IP del servidor: 170 . 70 . 91 . 27 : Puerto: 7090

Probar conexión

Ocultar certificados de conexión <<<

Detalle de certificados de conexión

	Número de serie	Nombre	Fecha	Detalle
1	00000100000100009806	Certificado General(sin validez)	12/01/2015	
2	00000100000100009724	Agencia Registradora Aplicativa Financiera	7/06/2012	

Remota [d255b35ffa658b95c578765b319cd92f7c3134391e49bb158cd0655cf3ef9de9]

Aceptar Cancelar

WEBSEC	Versión: A
Manual de Usuario	Fecha: 26/08/2011
Manual de Usuario_Externos.docx	

Los campos mostrados son:

(I) NOMBRE DE LA AUTORIDAD

Este campo muestra el nombre de la autoridad a conectarse, el valor por default será el nombre correspondiente a la ARA externa. Sin embargo en caso de haber alguna otra autoridad disponible y si se requiere, el usuario puede cambiar la autoridad a conectarse, únicamente seleccionándola de la lista de este campo.

(II) DIRECCIÓN IP DEL SERVIDOR

Este campo muestra la dirección IP configurada por default del servidor con el cual se establecerá la conexión con la IES.

(III) PUERTO

Este campo muestra el puerto configurado por default a utilizar para realizar la conexión con la IES.

(III) PROBAR CONEXIÓN

Esta opción permite al usuario realizar una prueba de conexión con el servidor y puerto configurados. En caso de no ser exitosa, el sistema indicará el error detectado.

(IV) VER CERTIFICADOS DE CONEXIÓN

Esta opción permite consultar la información correspondiente a los certificados de autenticación: certificado general y certificado de autoridad. Los datos mostrados son:

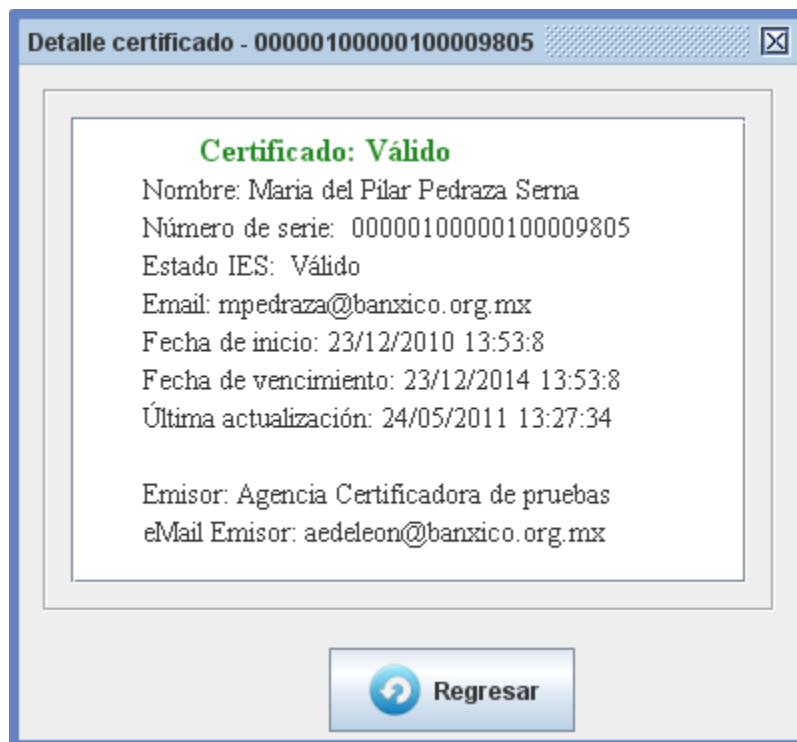
- Número de serie del certificado.
- Nombre del certificado.
- Fecha de actualización. Esta fecha corresponde a la última fecha en que fue actualizado el certificado.
- Detalle. Esta opción permite consultar el detalle de cada certificado de conexión.

El código en hexadecimal que aparece al final de la pantalla es la digestión del archivo de configuración, el algoritmo que se utiliza es SHA256.

3.2.3 Detalle de Certificados

Esta opción permite consultar el detalle del certificado seleccionado, en cualquier pantalla en la que aparezca la leyenda “Detalle” acompañada del ícono .

WEBSEC	Versión: A
Manual de Usuario	Fecha: 26/08/2011
Manual de Usuario_Externos.docx	



La información mostrada se describe a continuación:

- Presenta si el certificado es Válido (verde), No Válido (amarillo) o se encuentra Sin Verificar (rojo).
- Número de Serie: Número de serie del certificado.
- Nombre: Presenta el nombre del certificado.
- Estado IES: Válido, Caduco, Revocado o Alertado. En caso de que el certificado se encuentre sin verificar este campo estará vacío.
- Email: Correo electrónico del usuario al que corresponde el certificado digital.
- Fecha de inicio: Fecha de inicio de vigencia del certificado digital.
- Fecha de vencimiento: Fecha en la que pierde validez el certificado digital.
- Última actualización: Fecha y hora en la que la aplicación realizó la última consulta del estado del certificado en la IES.
- Emisor: Nombre del emisor del certificado.
- Email emisor. Correo electrónico del emisor del certificado.

WEBSEC	Versión: A
Manual de Usuario	Fecha: 26/08/2011
Manual de Usuario_Externos.docx	

4 Información Adicional

4.1 Contactos

Rol	Contacto
Centro de Atención de Sistemas de Pagos (CASP)	3333 opción 4
Grupo IES	ies@banxico.org.mx