Infraestructura Extendida de Seguridad

IES

BANCO DE MÉXICO
Dirección General de Operaciones de Banca Central
Dirección de Sistemas Operativos y de Pagos

ÍNDICE

INFRAESTRUCTURA EXTENDIDA DE SEGURIDAD

1. INTRODUCCIÓN

Con el desarrollo de las nuevas tecnologías de telecomunicaciones y transmisión de datos por vía electrónica, se ha generalizado el uso de los sistemas de intercambio electrónico de información en virtud de que permiten mejorar la productividad y reducir costos, además de que brindan amplias posibilidades de nuevos servicios en línea.

Por ello, se hace necesario disponer de un entorno seguro en relación con la autenticación electrónica y en este contexto la firma electrónica es una herramienta esencial para dar seguridad y confianza a las redes de comunicación, ya que cumple con las dos principales características de las firmas autógrafas: atribuir el documento al signatario y verificar que el mensaje no ha sido manipulado después de su firma.

La Infraestructura Extendida de Seguridad (IES) es un sistema diseñado y administrado por Banco de México con el propósito de fortalecer la seguridad de la información que se transmite tanto en los sistemas de pago como entre el sistema financiero mexicano y el Banco Central.

La IES administra certificados digitales, los cuales son a su vez mensajes de datos firmados digitalmente por una entidad del sistema de administración. La seguridad está basada en el uso de firmas electrónicas mediante la aplicación de algoritmos criptográficos para garantizar la confidencialidad e integridad de la información que se transmite y a su vez acreditar la identidad del remitente.

El objetivo del presente documento es explicar brevemente en qué consiste la criptografía y la firma electrónica, cuál es la estructura y organización de la IES, así como divulgar el manual de uso del programa WebSecBM y su relación con dicha infraestructura. Con base en la información del citado manual los usuarios podrán enviar y recibir documentos firmados y/o cifrados electrónicamente, garantizando la autoría y confidencialidad de los mismos.

2. CRIPTOGRAFÍA

Los sistemas de seguridad se construyen aplicando técnicas basadas en el uso de algoritmos criptográficos, cuya función primordial es transformar un mensaje en un texto no inteligible excepto para el destinatario, ya que éste es el único que puede efectuar la transformación inversa y por lo tanto conocer el mensaje original. Al texto ininteligible se le conoce como documento cifrado o criptograma.

En la criptografía actual las transformaciones se efectúan por computadora mediante el uso de algún algoritmo y un conjunto de parámetros llamados claves, las cuales son palabras o secuencias de caracteres generados en forma aleatoria. De esta forma, un mensaje M se transforma en un criptograma C mediante un algoritmo de cifrado y, a partir de C se obtiene M

mediante un algoritmo de descifrado, utilizando las claves que correspondan en cada caso para realizar las transformaciones.

En la criptografía moderna la seguridad de un sistema no está basada en mantener los algoritmos de cifrado y descifrado en secreto, sino en el tiempo que tomaría descifrar un mensaje sin tener conocimiento de la clave correspondiente.

Existen dos tipos principales de algoritmos criptográficos cuya función la desarrollan utilizando una o dos claves:

- Criptografía simétrica (usa una clave privada)
- Criptografía asimétrica (usa dos claves, una pública y una privada)

2.1 CRIPTOGRAFÍA SIMÉTRICA

En la criptografía simétrica, el cifrado y descifrado de mensajes se basan en el uso de una clave privada, la cual es conocida tanto por el emisor del mensaje como por el destinatario del mismo.

En esta criptografía se requiere generar una clave privada para cada pareja de usuarios que deseen comunicarse confidencialmente entre sí. Esto significa que en un sistema donde participan n usuarios intercambiando información privada, se requiere que se generen y administren (n(n-1)/2) claves, y que cada usuario sea responsable de proteger y mantener en secreto (n-1) claves.

2.2 CRIPTOGRAFÍA ASIMÉTRICA

La criptografía asimétrica se basa en la posibilidad de usar una clave para cifrar un mensaje, y otra clave distinta, relacionada matemáticamente con la primera, para descifrar el mensaje.

En esta criptografía sólo es necesario generar un par de claves únicas para cada usuario, que se denominan clave pública y clave privada, con la garantía de que computacionalmente no es factible deducir la clave privada a partir de la clave pública durante un periodo razonable.

Los usuarios tienen la responsabilidad de proteger y mantener en secreto su clave privada, mientras que las claves públicas se almacenan en una base de datos a la que tienen acceso todos los usuarios.

2.3 CLAVE PÚBLICA Y CLAVE PRIVADA

Se entenderá por clave pública al componente público del sistema de criptografía de clave pública y privada utilizado en la IES, que es uno de los argumentos de la función de verificación de la firma electrónica avanzada de un documento firmado electrónicamente.

Se entenderá por clave privada al componente privado del sistema de criptografía de clave pública y privada utilizado en la IES, que es uno de los argumentos de la función de creación de la firma electrónica avanzada que se asocia lógicamente a un documento electrónico.

Para mayor detalle sobre los conceptos mencionados en el presente numeral, referirse a los ejemplos del cálculo de las claves y del proceso de cifrado y descifrado para el algoritmo RSA contenidos en el anexo 3 de este documento.

2.3.1 IMPORTANCIA DE LAS CLAVES

Para mantener la seguridad de un sistema criptográfico, es fundamental que las claves se generen tanto de manera aleatoria como confidencial y que su longitud esté relacionada con la importancia de la información que se va a resguardar, teniendo en cuenta que a mayor número de caracteres de la clave se logra mayor seguridad, pero la ejecución de los algoritmos de cifrado y descifrado se vuelve más lenta.

Asimismo, es indispensable que los usuarios protejan y mantengan en secreto sus claves privadas y dada la complejidad de su memorización, es conveniente prever su almacenamiento en un medio electrónico en forma cifrada mediante un algoritmo de criptografía simétrica. Los mecanismos necesarios para descifrar las referidas claves deberán estar incluidos en la aplicación que se use para firmar documentos. El programa de cómputo denominado "WebSecBM", creado por Banco de México provee dicha funcionalidad. En el ***Anexo 2*** del presente documento, se describe la versión 1.0 del referido programa.

2.4 CARACTERÍSTICAS DE SEGURIDAD DE LA CRIPTOGRAFÍA

Utilizando las principales funciones criptográficas de clave privada y clave pública es posible establecer varias operaciones básicas de seguridad, sobre las cuales se pueden construir sistemas de información confiables.

Las principales características de seguridad que brinda la criptografía, son:

- Confidencialidad
- Autenticidad
- Integridad
- Atribuible al signatario

2.4.1 CONFIDENCIALIDAD, AUTENTICIDAD E INTEGRIDAD

Un algoritmo criptográfico simétrico garantiza la privacidad de la información, en virtud de que sólo el destinatario puede descifrarla, ya que es el único que conoce la clave privada con la cual el emisor realizó el cifrado de la información. En este caso el destinatario sabe quién generó el mensaje, pero no tiene elementos para demostrar que tal mensaje le es al emisor.

En el caso de algoritmos criptográficos asimétricos cuando el cifrado y descifrado de un mensaje se realiza con base en el par de claves asociado al destinatario, esto es:

- el emisor cifra utilizando la clave pública del destinatario, y
- el destinatario descifra utilizando su clave privada;

se garantiza que únicamente el destinatario pueda leer el mensaje, ya que sólo el dueño de la clave privada puede descifrar el mensaje, sin embargo el destinatario no puede saber quién generó el mensaje.

2.4.2 ATRIBUIBLE AL SIGNATARIO

En adición a las características a que se refiere el numeral inmediato anterior, un algoritmo criptográfico asimétrico también permite que el cifrado y descifrado del mensaje se realice con base en el par de claves asociado al emisor del mensaje, esto es:

- el emisor cifra utilizando su clave privada, y
- el destinatario descifra utilizando la clave pública del emisor;

en este supuesto se garantiza que el destinatario o cualquier otra persona puede verificar que el mensaje proviene realmente de la persona que lo emitió y asegurar que no está alterada la información. Asimismo, el emisor estaría impedido a negar válidamente ser el autor del mensaje, toda vez que asume la responsabilidad por el uso de su clave privada al firmar de puño y letra el documento de aceptación de su certificado digital; en tal virtud, los mensajes así cifrados le son atribuibles.

Función Resumen

Dado que la ejecución de los algoritmos de criptografía asimétrica es lenta, existen algoritmos que combinan técnicas matemáticas de compresión de textos con técnicas de criptografía asimétrica, los cuales tienen los mismos efectos de seguridad.

Los algoritmos de compresión de texto, también conocidos como algoritmos hash, utilizan funciones matemáticas de no retorno, es decir, son procedimientos unidireccionales los cuales a partir de un texto dado de cualquier tamaño, generan un texto reducido de tamaño fijo entre 64 y 160 bits, el cual se denomina *resumen*. Es absolutamente claro que existe un número mayor de textos que de resúmenes posibles, lo cual significa dos cosas:

1. que existen con toda certeza mas de dos textos diferentes que tienen el mismo resumen, y
2. encontrar dos textos que tengan el mismo sentido, en el área a la que se refieren y que sean ligeramente diferentes(por ejemplo dos facturas electrónicas que tengan distinto valor) es prácticamente imposible.

Una función resumen tiene la particularidad de que el proceso de generación del *resumen* de un documento es rápido y sencillo, y no requiere de una clave para obtener el *resumen*, sin embargo el proceso a la inversa; esto es, obtener el documento original a partir del *resumen,* es imposible debido a que en el proceso que calcula el *resumen* se pierde información, por definición de la función de calculo del *resumen*. Además, se garantiza que el *resumen* cambia de manera drástica cuando cambia el documento origen, aunque sólo se modifique un bit, por ello, la probabilidad de que dos documentos ligeramente distintos tengan el mismo *resumen* es casi nula.

2.4.3 FIRMA ELECTRÓNICA

El método de criptografía esbozado en el numeral anterior se utiliza para generar firmas electrónicas, las cuales se añaden al documento como marca identificadora.

La firma electrónica se puede definir como el conjunto de datos que se agrega o adjunta a un documento electrónico y está asociado en forma lógica al propio documento y al signatario. Esta

firma se utiliza para identificar al autor del documento y asegurar que el documento no fue alterado.

La generación de una firma electrónica se realiza aplicando primero una función resumen sobre el documento que se desea firmar para así obtener el *resumen* correspondiente, después se cifra el *resumen* con la clave privada del signatario. Al texto cifrado resultante se le llama firma electrónica, el cual depende tanto del documento origen como de la clave privada del signatario. Al resultado de concatenar el documento origen y la firma electrónica se le denomina *documento firmado electrónica o digitalmente*.

La firma electrónica tiene las mismas funciones que la firma autógrafa, siendo más confiable la primera. Ambas sirven para garantizar que la persona que dice haber elaborado y/o enviado un documento, efectivamente lo elaboró y/o envió. La firma electrónica difiere de la firma autógrafa, en que la primera está vinculada al documento y al signatario, mientras que la segunda sólo depende del signatario y es invariable.

Dado que la firma electrónica de un documento es una función de la clave privada del signatario y a su vez del contenido del propio documento, las principales propiedades de una firma electrónica son:

- Es única por documento y signatario.
- Es atribuible al signatario.
- Es infalsificable.
- No puede transferirse a otro documento.

2.4.4 ENSOBRETADO

En ciertas situaciones, es deseable enviar documentos electrónicos asegurando su autenticidad, integridad y confidencialidad, lo cual se logra aplicando la técnica llamada "documento ensobretado" que consiste, primero en firmar el documento electrónicamente y luego cifrarlo mediante un algoritmo criptográfico simétrico. La firma garantiza la autenticidad e integridad del documento, mientras que el cifrado garantiza su confidencialidad.

A la acción de descifrar y verificar la firma electrónica de un documento ensobretado se le llama "abrir sobre".

Las características de seguridad que tiene un documento ya sea que esté firmado, cifrado o ensobretado, se resumen en el cuadro siguiente:

CARACTERÍSTICAS DE SEGURIDAD	DOCUMENTO		
	FIRMADO	CIFRADO	ENSOBRETADO
AUTENTICIDAD	Π		Π
INTEGRIDAD	Π		Π
ATRIBUIBE AL SIGNATARIO	Π		Π
CONFIDENCIALIDAD		Π	Π

3. LA IES DISEÑADA POR BANCO DE MÉXICO

A fin de proveer una operación segura y eficiente tanto en los sistemas de pagos como en la comunicación a través de mensajes electrónicos protegidos mediante algoritmos de criptografía asimétrica (clave pública y privada), es necesario tener una infraestructura que permita administrar y distribuir las claves públicas en forma ágil y con la confianza de que cada correlación de clave pública y usuario implica necesariamente la corroboración de la identidad de los usuarios con base en la comparecencia física y presentación de documentación oficial.

3.1 CERTIFICADOS DIGITALES

El control y administración de las claves públicas de los usuarios se realiza a través de la expedición de "certificados digitales".

Un certificado digital es un documento electrónico que asegura que una clave pública determinada corresponde a un individuo en específico. Dicho certificado está firmado electrónicamente por la agencia que corroboró de manera razonable la identidad del individuo y la validez de su clave pública.

Un certificado digital usualmente contiene un número de identificación del certificado, una clave pública, los datos personales que identifican al propietario de la clave pública, las características propias de la clave, la vigencia del certificado y los datos particulares de la agencia certificadora, así como su firma electrónica.

3.2 FINALIDAD Y FUNCIONES

El objetivo principal de la IES es dar mayor seguridad y confianza a las operaciones financieras que se realizan a través de los medios electrónicos en los sistemas de pagos.

Para la consecución de tal objetivo, la IES tiene como función principal mantener el control sobre las claves públicas que se utilicen en la verificación de las firmas electrónicas, mediante la expedición y administración de certificados digitales.

3.3 ESTRUCTURA DE ORGANIZACIÓN

La estructura de organización de la IES establecida y administrada por Banco de México es flexible en el sentido de que es totalmente independiente del sistema criptográfico que se use. La estructura puede crecer gradualmente de acuerdo a las necesidades de los diferentes usuarios y permite que la administración de las claves quede distribuida entre diversos participantes, estableciendo para ello varios servidores de certificados digitales interconectados para satisfacer en forma ágil los requerimientos de los usuarios.

El modelo general de organización para la administración de las claves públicas y los certificados digitales se muestra en el ***Anexo 1***, en el que se aprecia que los participantes de la IES son:

- Agencia Registradora Central ARC
- Agencias Registradoras AR's

- Agencias Certificadoras AC's
- Agentes Certificadores AgC's
- Usuarios

3.4 PRINCIPALES FUNCIONES DE LOS PARTICIPANTES

Las principales funciones que desempeñan cada uno de los participantes de la IES se describen a continuación:

ARC – Agencia Registradora Central

- Normar y administrar la IES de acuerdo con las políticas que establezca el Banco de México.
- Crear su propio certificado digital y certificar a las AR's y AC's.
- Garantizar la unicidad de las claves públicas del sistema.
- Administrar la base de datos de las claves públicas correspondientes a los certificados digitales que las AR's tengan registradas en sus bases de datos y mantener una liga con las AC's que los expidieron.
- Difundir su clave pública y las claves públicas de las AR's y AC's a través de la página que el Banco de México tiene en la red mundial (Internet) que se identifica con el nombre de dominio www.banxico.org.mx.
- Establecer, administrar y mantener las medidas que garanticen la seguridad del sistema.

AR's – Agencias Registradoras

- Registrar certificados digitales siempre y cuando la ARC confirme la unicidad de las claves públicas.
- Administrar las bases de datos con los certificados digitales registrados, tanto vigentes como históricas.
- Proporcionar a los usuarios que lo soliciten a través de medios electrónicos, información respecto de certificados digitales.
- Revocar certificados digitales en los supuestos previstos en las disposiciones aplicables e informar de la revocación a la AC que los haya emitido, así como, divulgar dichas revocaciones de conformidad con las reglas emitidas por la ARC.

AC's – Agencias Certificadoras

- Emitir certificados digitales.
- Emitir los certificados digitales de las personas que les presten los servicios de AgC's y acreditarlos como tales.
- Solicitar a la AR que corresponda, la revocación de los certificados digitales que haya emitido, en los supuestos previstos en las disposiciones aplicables o cuando los usuarios, directamente o a través de un AgC, lo soliciten.
- Auxiliarse de AgC's en la realización de sus funciones, de conformidad con las disposiciones aplicables.
- Responder por los daños y perjuicios que, con motivo de la realización de sus actividades, ocasione por negligencia en el proceso de certificación, de conformidad con las disposiciones aplicables.
- Responder por los actos que realicen sus AgC´s, así como de los daños y perjuicios que éstos generen en el cumplimiento de sus funciones, de conformidad con lo previsto en las disposiciones aplicables.

AgC's – Agentes Certificadores

- Auxiliar a la AC en la realización de sus funciones de conformidad con las disposiciones aplicables.
- Verificar la identidad de los solicitantes que desean obtener certificados digitales, con base en los documentos oficiales que éstos les presenten.
- Informar al solicitante de un certificado digital sus derechos y obligaciones.
- Recibir y verificar el requerimiento de certificado digital elaborado por el solicitante.
- Obtener una declaración con firma autógrafa del solicitante en la que manifieste su conformidad con las reglas sobre el uso de firma electrónica.
- Proporcionar al solicitante de un certificado digital los medios necesarios para la generación de datos de creación y verificación de su firma electrónica.
- Emitir el precertificado correspondiente y solicitar el respectivo certificado digital a la AC que corresponda.
- Entregar al titular su certificado digital registrado y obtener la carta de aceptación del referido certificado digital en la que conste su firma autógrafa.
- Informar, en su caso, al titular de la revocación de su certificado digital.

Usuarios

- Solicitar su certificado digital a una AC directamente o a través de un AgC, presentando su requerimiento digital y los documentos oficiales para su identificación, así como en su caso, la carta de solicitud correspondiente.
- Ser informado de sus derechos y obligaciones y manifestar su conformidad con las disposiciones aplicables a la firma electrónica.
- Establecer, en secreto y en forma individual, su frase de seguridad con la que podrá cifrar su clave privada para protegerla.
- Generar, en secreto y en forma individual, su par de claves (pública y privada) y su requerimiento, así como, los archivos correspondientes.
- Recibir la carta de aceptación de su certificado digital en la que conste su firma autógrafa y su certificado digital ya registrado.
- Mantener en un lugar seguro su clave privada.
- Recordar su frase de seguridad así como su Challenge Password y mantenerlos en secreto.
- Solicitar a la AR a través de medios electrónicos, la información de los certificados digitales de aquellos usuarios con los que tiene una relación operativa.
- Tener acceso a un servicio que le permita revocar, en línea, su certificado digital en cualquier momento.
- Ser informado por la AC o, en su caso, por un AgC, de las reglas, procedimientos y características generales de los servicios de certificación y de los certificados digitales.

3.5 ORGANIZACIÓN

La IES está organizada a través de las agencias siguientes:

- La ARC, bajo la responsabilidad exclusiva de Banco de México;
- Las AR y AC's, que están bajo la responsabilidad del propio Instituto Central, y
- La AR's y las AC's de aquellas instituciones y/o empresas que hayan sido autorizadas por Banco de México para actuar con tal carácter en la IES.

La operación de la IES fue iniciada con la generación del certificado raíz del sistema, es decir el de la ARC. Acto seguido, se expidieron los certificados de las AC's y de la AR operadas por Banco de México, los cuales fueron registrados en la ARC.

Una vez registrados los certificados de la ARC y de las agencias de Banco de México, el área de operación tomó el control exclusivo de los equipos que albergan el sistema, previamente configurados por el Área de desarrollo, y sustituyó los passwords de las cuentas de usuario de dichas máquinas. A partir de ese momento el área de desarrollo no tiene acceso a las máquinas y el área de operación no tiene el control que se requiere para dar de alta certificados de AC's o AR's, por lo que es imposible dar de alta certificados de agencias sin la participación conjunta de las dos áreas.

Los certificados de los usuarios finales los puede dar de alta una AC de forma automática usando los programas informáticos de la IES correspondientes. La AR los registra de forma automática con la autorización electrónica de la AC y de la ARC, lo que agiliza la operación cotidiana de alta de certificados de usuario final.

3.6 MEDIDAS DE SEGURIDAD OPERATIVA

Es interés del Banco de México que la IES opere en un entorno confiable que permita asegurar que la asociación de claves públicas con los participantes del sistema sea fidedigna.

Considerando que la funcionalidad y seguridad de un sistema informático depende de todos y cada uno de sus componentes, se han incorporado a la IES diversos procedimientos de seguridad con el propósito de, entre otros aspectos, garantizar la seguridad física de los equipos de cómputo, proteger a los programas de modificaciones no autorizadas, asegurar la confidencialidad y, por ende la confiabilidad de las bases de datos y prever la continuidad de la operación de los sistemas de la IES, así como permitir el acceso a la red y programas de cómputo sólo a personal autorizado expresamente para ello.

Para tales efectos, la administración de la IES se realiza con base en ciertos principios de funcionamiento para el desarrollo, mantenimiento y operación de sus sistemas, los cuales se describen a continuación:

3.6.1 PRINCIPOS DE FUNCIONAMIENTO

- La implementación técnica del sistema de la IES (el diseño y control del código fuente así como la configuración inicial de las máquinas en las que se ejecuta dicho sistema), es responsabilidad de la Gerencia de Informática de la Dirección de Sistemas Operativos y de Pagos de Banco de México.

- La operación de los componentes de la IES está asignada a áreas distintas. Esto es, el personal encargado del desarrollo y mantenimiento del sistema de la IES tiene bajo su responsabilidad la administración de la ARC y el personal responsable de la operación de la IES, tiene a su cargo el control de los passwords de acceso a los servidores y a las cuentas de usuario de los equipos que albergan el sistema.

- Los equipos de cómputo que albergan los programas de la IES tienen habilitadas únicamente dos cuentas, una para el administrador del sistema y otra, sin privilegios, bajo la cual se ejecutan los programas de la IES.

- Los archivos de bitácora del sistema son revisados periódicamente para detectar intentos de acceso no autorizados y en su caso, tomar las medidas preventivas y/o correctivas necesarias.

- El área de desarrollo y mantenimiento de la IES, estableció la configuración inicial de las computadoras en las que se ejecutan los programas de la IES , con los servicios de red deshabilitados, a fin de evitar que persona alguna esté en posibilidad de tomar el control de los sistemas desde un lugar remoto de la red y de limitar los accesos no autorizados que pudieran dañar el sistema.

- Toda modificación a la configuración de los equipos de cómputo de la IES, cambio de versión del sistema IES o sistema operativo, debe ser supervisado y certificado conjuntamente por personal de las áreas competentes de Banco de México.

- El proceso de expedición y registro de certificados de AC's y AR's es realizado por el Área de desarrollo y mantenimiento de la IES y supervisado por el Área de operación para verificar que se den de alta sólo aquellas agencias que cumplan con los lineamientos establecidos en las disposiciones aplicables.

- Sólo se realizan conexiones a través de la red de telecomunicaciones con los servidores de la IES que estén debidamente documentadas, y se supervisa periódicamente que no existan conexiones no autorizadas.

- Los programas de la IES únicamente pueden crear, abrir o modificar archivos que estén claramente especificados, de los cuales se conozca su contenido y esté de acuerdo con la documentación del sistema. Dichos programas son verificados periódicamente para garantizar el cumplimiento de la condición antes referida.

- Se cuenta con una copia de los resúmenes digitales de los programas ejecutables de la IES, con el objeto de verificar en cualquier momento, que las versiones ejecutables en producción no han sido modificadas sin la autorización correspondiente.

- Existen planes de contingencia del sistema IES los cuales son probados periódicamente. Dichos planes consisten en mantener un respaldo diario de la información de la base de datos, copiándolo tanto a un servidor alterno, como en una cinta magnética. Asimismo, se mantiene un esquema de cluster de alta disponibilidad con dos nodos para la ARC, de manera que si se llegare a perder el nodo activo, inmediatamente entraría en operación el nodo alterno. Además todos los servidores de la IES cuentan con arreglos de discos en espejo y notificaciones para que, en caso de falla de alguna parte del equipo, se pueda actuar de manera pronta y expedita y no se pierda la información. Para mayor detalle, consultar el anexo 4.

- Personal de la Gerencia de Trámite de Operaciones Nacionales de la Dirección de Trámite Operativo; y de la Gerencia de Informática de la Dirección de Sistemas Operativos y de Pagos, revisa periódicamente los controles de funcionamiento implementados en la IES, descritos en el presente documento.

4. USO Y EXPLOTACIÓN DE LA IES

4.1 PROCEDIMIENTO PARA LA OBTENCIÓN DE UN CERTIFICADO DIGITAL

El procedimiento para la obtención de un certificado digital se deberá llevar a cabo conforme a las prácticas de certificación elaboradas por la AC que corresponda, previamente aprobadas por Banco de México, así como, por lo previsto en las disposiciones aplicables a la IES.

4.2 USO DE FIRMAS ELECTRÓNICAS

De acuerdo con la definición de firma electrónica, el signatario es una persona física que suscribe documentos utilizando un dispositivo y sus datos de creación de firma, y el destinatario del documento es la persona física que verifica la firma utilizando un dispositivo y los datos de verificación de firma del signatario

Los datos que el signatario utiliza para crear la firma electrónica son, como ya se mencionó, su clave privada, frase de seguridad y certificado digital**.** Los datos que el destinatario utiliza para verificar la firma electrónica son los del certificado digital del signatario, el cual lo obtiene de la IES a través de una AR.

De este modo el signatario y el destinatario deben contar, respectivamente, con dispositivos de creación y verificación de firmas electrónicas, los cuales deben ser sistemas de cómputo cuya función principal sea la aplicación de algoritmos criptográficos. A su vez, dichos sistemas deben mantener comunicación con la IES, en particular con una AR, para estar en posibilidad de solicitar y verificar la validez de los certificados digitales de los usuarios involucrados en los procesos de firma y cifrado de documentos.

Para tales efectos, Banco de México diseñó y desarrolló un sistema denominado WebSecBM, que permite a los usuarios de la IES, aplicar técnicas de criptografía en documentos electrónicos, ya sea para firmar documentos o verificar firmas, efectuar procesos de cifrado o descifrado de documentos, así como ensobretar documentos o abrir sobres, es decir, verificar las firmas y descifrar documentos ensobretados.

Como ***Anexo 2*** se adjunta a este documento el **Manual del Usuario** del sistema ***Uso de Firmas Electrónicas WebSecBM***.

5. ATENCIÓN DE CONSULTAS

Para consultas acerca de aspectos técnicos relacionados con la IES, los interesados podrán comunicarse con las personas que se señalan a continuación:

Nombre:	**Teléfono:**	**Dirección de correo electrónico:**
Angel Emilio De León Gutiérrez	5227-86-44	aedeleon@banxico.org.mx
Nury Laura Custodio López	5227-86-18	ncustodi@banxico.org.mx
José Antonio Hernández Ayuso	5227-87-75	ahernand@banxico.org.mx
Raymundo Peralta Herrera	5227-88-09	reperal@banxico.org.mx

Respecto de consultas sobre asuntos operativos relacionados con la IES, los interesados podrán comunicarse con las personas que se señalan a continuación:

Nombre:	**Teléfono:**	**Dirección de correo electrónico:**
Rogelio Domínguez Pacheco	5237-21-30	rdoming@banxico.org.mx

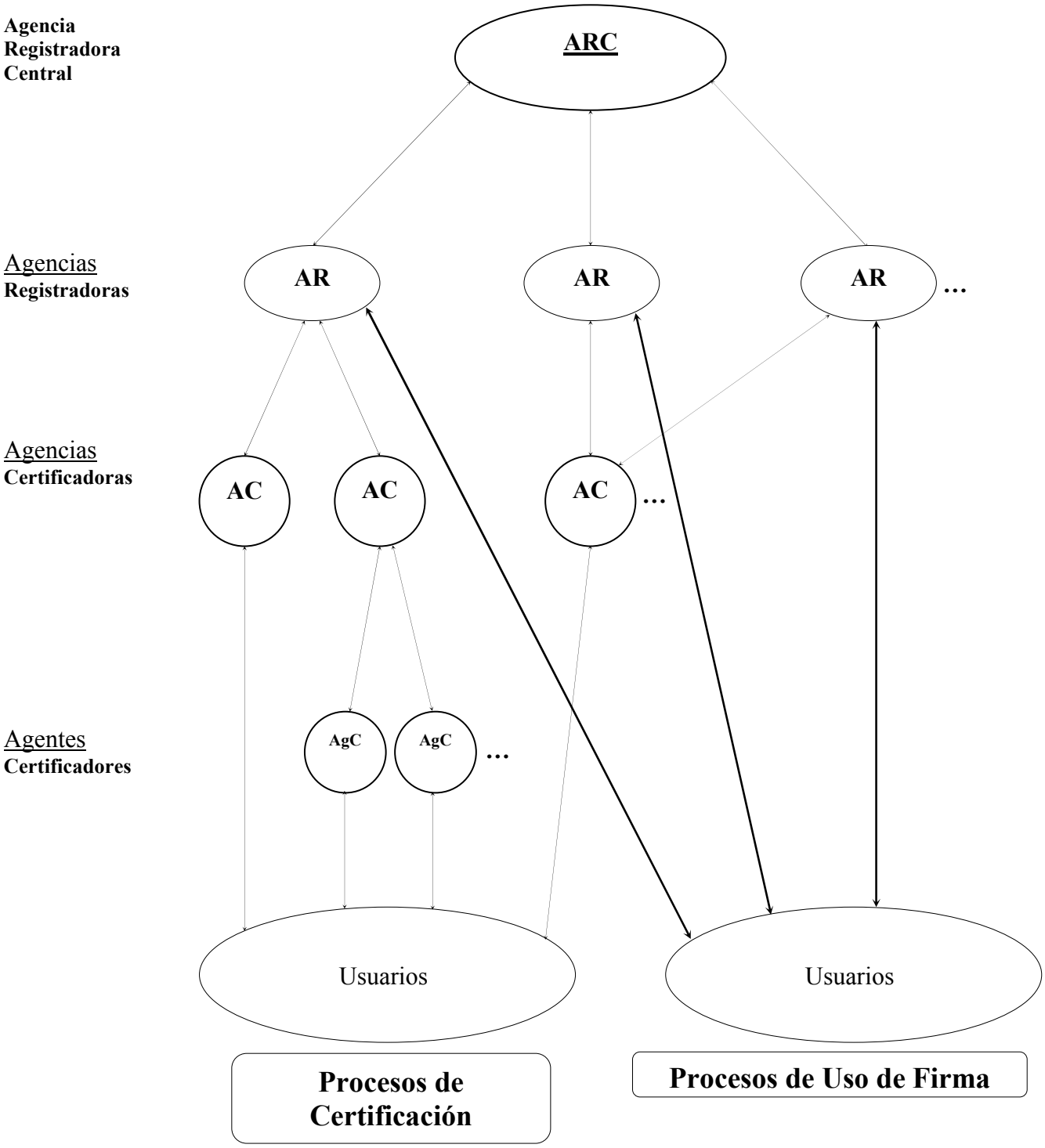
Ernesto Luna Vázquez	5237-20-86	eluna@banxico.org.mx
Lorenzo Jiménez Vázquez	5237-20-82	ljimenez@banxico.org.mx
José Antonio Cortés Olivera	5237-20-80	jcortes@banxico.org.mx

Para cualquier consulta sobre información referente a las disposiciones aplicables a la IES o, respecto de la obtención de autorización para actuar como AC y/o AR en dicha infraestructura, los interesados deberán dirigirse a la Gerencia de Autorizaciones, Consultas y Control de Legalidad de Banco de México, con las personas que se indican a continuación:

Nombre:	**Teléfono:**	**Dirección de correo electrónico:**
Napoleón Damián Serrano	5237-20-00 ext. 3310	ndamian@banxico.org.mx
Humberto Rivero Silva	5237-23-17	hrivero@banxico.org.mx
Héctor Helú Carranza	5237-23-08	hhelu@banxico.org.mx

Anexo 1

MODELO GENERAL DE ORGANIZACIÓN DE LA IES



Anexo 2

Infraestructura Extendida de Seguridad IES

Uso de Firmas Electrónicas

(Sistema WebSecBM versión 1.0)

Manual del Usuario

BANCO DE MÉXICO
Dirección General de Operaciones de Banca Central
Dirección de Sistemas Operativos y de Pagos

Í N D I C E

1. INTRODUCCIÓN

En este documento se describe la versión 1.0 del sistema WebSecBM, que permite hacer uso de las firmas electrónicas, ya sea para firmar documentos o verificar firmas, realizar procesos de cifrado y descifrado de documentos, así como ensobretar documentos o hacer la apertura de tales documentos. El sistema WebSecBM es una herramienta para los usuarios de la IES.

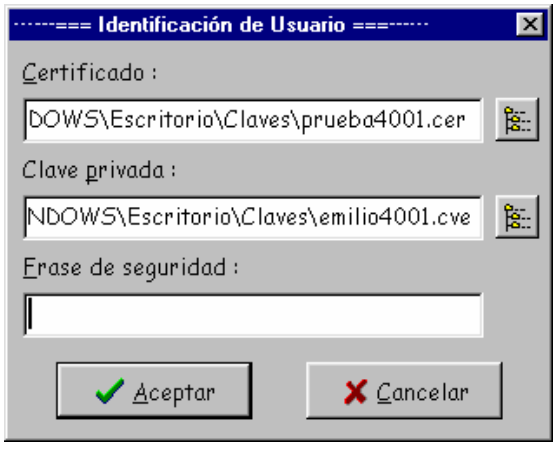
El sistema proporciona además los servicios siguientes:

- Identificación de usuarios, mediante el archivo de certificado digital, el archivo de clave privada y la correspondiente frase de seguridad.
- Conexión con un participante de la IES a fin de obtener, a través de ésta, la información de los certificados que se requieran para la ejecución de operaciones en el propio sistema.
- Almacenamiento de los certificados que se usan para verificar firmas, cifrar y ensobretar archivos.
- Asociación de archivos con procesos, con base en la extensión del propio archivo *.fbm*, *.sbm* y *.cbm*, a fin de que al pulsar dos veces sobre el nombre de un archivo con alguna de estas extensiones, automáticamente se ejecute el proceso que corresponda al tipo de archivo de que se trate.
- Integración en forma transparente del WebSecBM con aplicaciones de Microsoft® Office®.

2. IDENTIFICACIÓN DEL USUARIO.

Al entrar al sistema, automáticamente se inicia el proceso de *Identificación de Usuario*.

Este proceso solicita que el usuario proporcione su certificado digital, clave privada y frase de seguridad, tanto para fines de identificación, como para poder realizar cualquiera de los procesos que permite el WebSec. Para ello, el sistema muestra la ventana siguiente:



En el campo *Certificado* especificar el nombre del archivo que contiene su certificado, y en el campo *Clave Privada* introducir el nombre del archivo que contiene su clave privada. Se pueden seleccionar dichos archivos desde un cuadro de diálogo estándar, utilizando los botones situados a la derecha de las cajas de texto.

En el campo *Frase de Seguridad* introducir la frase de seguridad correspondiente a la clave privada. Este campo no muestra los caracteres que se escriben ya que despliega asteriscos (*) en su lugar.

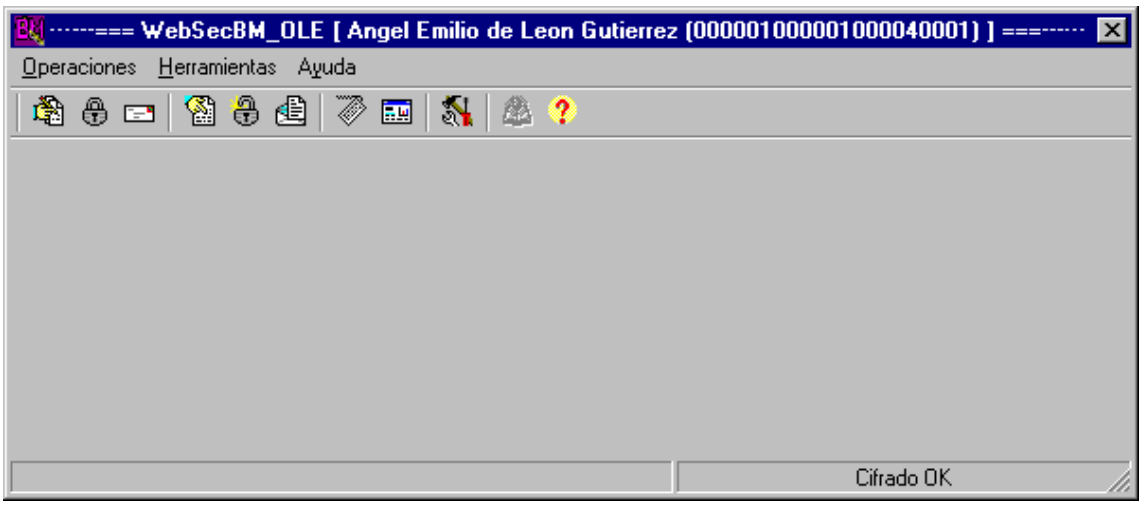
Pulsar el botón *Aceptar*. Si los datos proporcionados son correctos el usuario queda identificado a partir de ese momento y en el título de la ventana principal del sistema, se muestra el nombre y número del certificado del usuario registrado.

En caso de que los archivos proporcionados no existan, sean inválidos ó la frase de seguridad no corresponda a la clave privada, se muestra un mensaje de error y debe repetirse la operación. El sistema da 3 oportunidades para ingresar correctamente los datos, en el evento de que en el tercer intento aún exista algún problema, el programa se cierra en forma automática.

Si se pulsa el botón *Cancelar* termina la ejecución del programa.

3. PANTALLA PRINCIPAL

Una vez identificado el usuario, aparece la pantalla principal del sistema como sigue:



En esta pantalla se tienen los elementos siguientes:

- **Barra de Título de la Ventana:**
  Situada en la parte superior de la ventana. Junto al nombre del sistema se despliega el nombre común y el número de serie del certificado con el que se identificó el usuario.

- **Barra de Menú de Procesos:**
  Situada debajo de la barra de título de la ventana y sirve para tener acceso a los diferentes servicios que proporciona el sistema.

- **Barra de Herramientas:**
  Situada debajo de la barra de menú de procesos y contiene los iconos asociados con las opciones de procesos, para facilitar el acceso a las mismas.

- **Barra de Estado:**
  Situada en la parte inferior de la ventana y sirve para que el sistema despliegue mensajes de ayuda e información sobre el resultado de los procesos realizados.

3.1 BARRA DE MENÚ DE PROCESOS

En la pantalla principal en la barra de menú de procesos, se muestran 3 tipos de procesos, cada uno a su vez, representa un menú de opciones de procesos que se describen a continuación:

3.1.1 Opciones del Menú de Operaciones

Las operaciones que se pueden ejecutar se dividen en dos grupos: el primero, incluye aquellos procesos que permiten crear archivos protegidos con algoritmos criptográficos, y el segundo grupo, consta de los procesos que se requieren aplicar para poder visualizar archivos que están asegurados con alguno de los procesos del primer grupo. Las opciones del menú de operaciones son:

- ***Firmar archivos***: Permite firmar en forma electrónica uno ó más archivos. Este proceso, se utiliza para garantizar la autenticidad e integridad de dichos archivos.

- ***Cifrar***: Permite aplicar un método de cifrado a un archivo, con el fin de asegurar la confidencialidad del mismo.

- ***Ensobretar***: Permite llevar a cabo el proceso de cifrado y firmado de un archivo, para garantizar la confidencialidad y autenticidad del mismo, así como, enviarlo a uno o varios destinatarios que podrán ver el contenido del archivo.

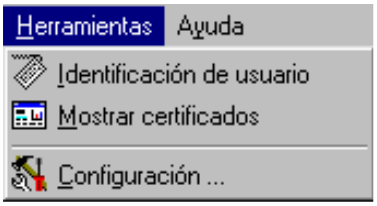
- ***Verificar***: Permite establecer si la firma electrónica de un archivo en particular es válida o inválida. Si un archivo fue firmado pidiendo acuse de recibo por correo electrónico, éste se envía de manera automática.

- ***Descifrar***: Permite descifrar un archivo siempre y cuando el usuario sea el destinatario del archivo.

- ***Abrir sobre***: Permite llevar a cabo el proceso inverso al de ensobretar, siempre y cuando el usuario sea el destinatario del sobre.

Cuando los procesos de Verificar, Descifrar y Abrir Sobre, resultan exitosos, el usuario tiene acceso al archivo original, pudiendo elegir entre salvarlo ó visualizarlo con la aplicación con la que fue generado, siempre y cuando esta última opción se encuentre instalada en la computadora.

3.1.2 Opciones del Menú de Herramientas



- ***Identificación de usuario****:* Permite que el usuario se identifique proporcionando los archivos que contienen su certificado digital y clave privada, así como la frase de seguridad correspondiente, a fin de que, a partir de ese momento y hasta que se identifique otro usuario, los datos que obtenga el sistema mediante este proceso se usen en todas las operaciones que los requieran.

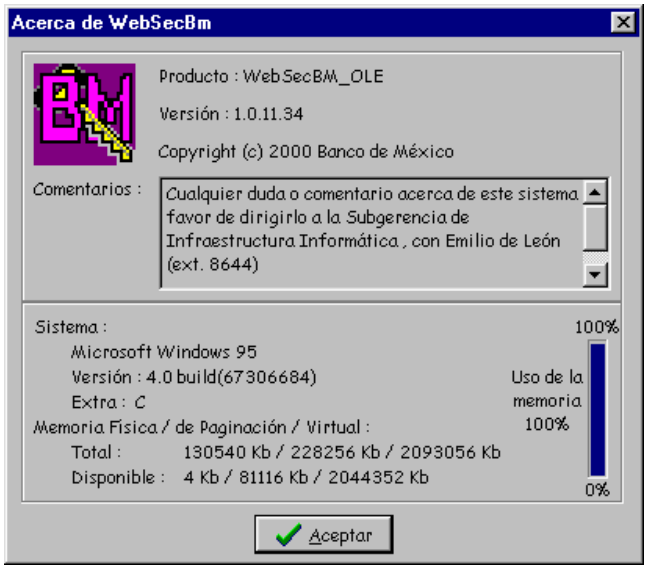
- ***Mostrar Certificados****:* Muestra la lista de los certificados que el sistema tiene registrados en una base de datos local y permite visualizar el contenido de los mismos. Además, permite agregar o eliminar certificados en dicho registro. Este proceso no modifica los certificados que estén registrados en la IES.

- ***Configuración***: Permite especificar tanto los parámetros necesarios para establecer conexión con la IES, esto es, con una Agencia Registradora, como los parámetros del servidor de correo para estar en posibilidad de enviar acuses de recibo al verificar archivos firmados.

3.1.3 Opciones del Menú de Ayuda

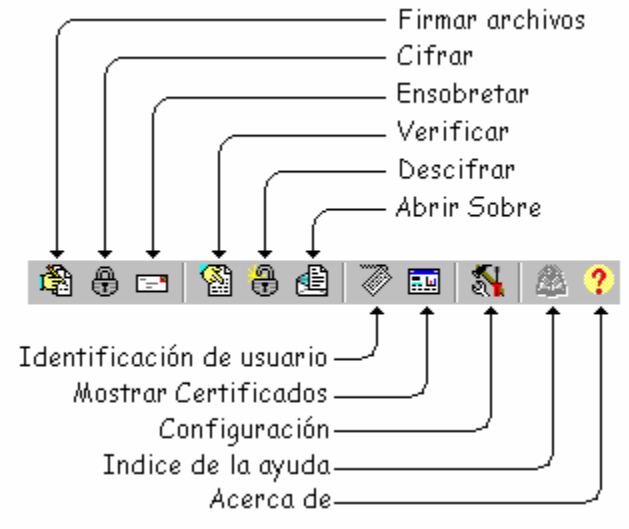
- ***Índice****:* Muestra la ventana de ayuda de Windows®, con el índice de ayuda del sistema WebSecBM. Esta opción puede estar inhabilitada.

- ***Acerca de****:* Muestra información referente al sistema WebSecBM en una ventana como la siguiente:



3.2 BARRA DE HERRAMIENTAS

La barra de herramientas que se localiza en la pantalla principal del sistema consta de los botones siguientes:



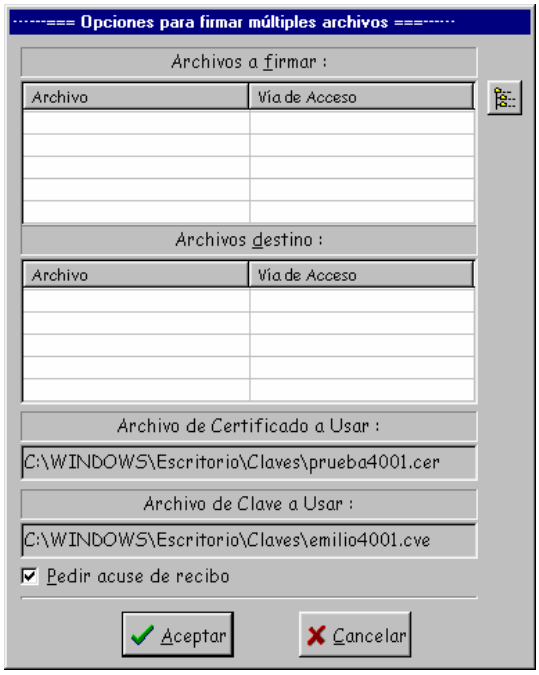
Cada botón corresponde a una opción de los menús de procesos. La descripción de cada uno de los procesos que se ejecuta al pulsar el botón o al seleccionar la opción respectiva de un menú se señala en el numeral siguiente.

4. DESCRIPCIÓN DE PROCESOS

4.1 FIRMAR ARCHIVOS

Con esta opción, se puede agregar una firma electrónica a los archivos que se seleccionen, para asegurar su integridad y autenticidad.

El sistema muestra el siguiente cuadro de diálogo para obtener los datos necesarios y poder llevar a cabo el proceso de firma.



En el campo *Archivos a firmar* se deben incluir los nombres y ubicación (vía de acceso) de los archivos que desea firmar. Para agregar archivos a la lista, se puede utilizar el botón de la derecha, o bien, utilizar la tecla <*INS*>, a fin de que aparezca un cuadro de diálogo estándar de Windows y seleccionar el archivo ó archivos a firmar.

El sistema no admite que se dupliquen los nombres de los archivos a firmar. Para eliminar archivos de la lista, deben seleccionarse y después oprimir la tecla <*DEL*>.

En el campo *Archivos destino*, el sistema muestra la lista de los nombres de archivos donde depositará los archivos ya firmados, los cuales genera automáticamente tomando el nombre original y agregándole la extensión *.fbm*.

Si se desea modificar alguno de los nombres de archivos destino, debe pulsar dos veces en el nombre, para que se despliegue un cuadro de diálogo estándar de Windows® de *Guardar Archivo* y cambiar la ruta y/o el nombre del archivo destino.

Si desea modificar el directorio destino de todos los archivos firmados, debe pulsar sobre el título de la columna con la leyenda *Vía de Acceso* en el área *Archivos destino*, para que se despliegue un cuadro de diálogo en el cual se puede elegir el directorio en el que se desea almacenar todos los archivos firmados.

Los campos *Archivo de Certificado a Usar* y *Archivo de Clave a Usar* señalan los nombres de archivo del certificado y la clave privada que utilizará el sistema en el proceso de firma, los cuales corresponden a los que el usuario especificó en el proceso de *Identificación de Usuario*.

Si se desea acuse de recibo, cada vez que alguna persona verifique la firma de alguno de los archivos, deberá marcar la casilla *Pedir acuse de recibo*. El sistema recuerda el estado de esta casilla la próxima vez que firme archivos.

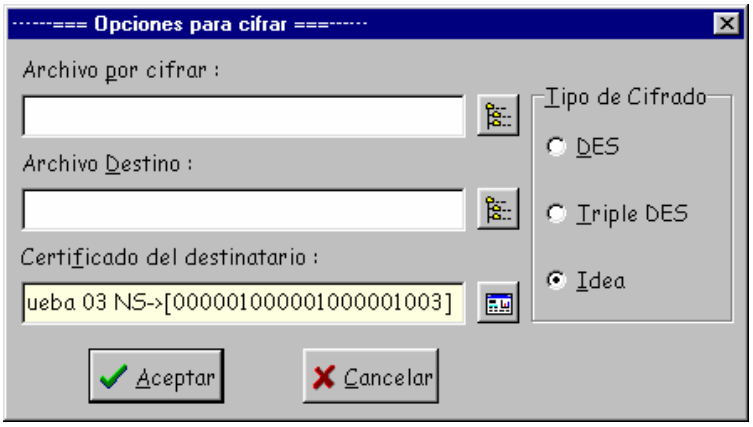
Al terminar de especificar los datos, pulsar el botón *Aceptar* para que se inicie el proceso de firma. El sistema verifica que los archivos destino no estén duplicados, de ser así, muestra un mensaje de error, en el caso de que los archivos destino ya existan, el sistema pide una confirmación para sobreescribir. En el evento de que no exista error alguno en el proceso de firma, el sistema muestra la confirmación de que todo estuvo correcto mediante un sonido y un mensaje en el ángulo inferior derecho de la pantalla principal.

Si se presenta algún error, el sistema muestra un cuadro de diálogo indicando el error correspondiente.

4.2 CIFRAR

Con esta opción se puede cifrar un archivo para enviarlo a un destinatario de forma confidencial.

Para llevar a cabo el proceso de cifrado, el sistema presenta un cuadro de diálogo como el que se muestra a continuación:



En el campo *Archivo por cifrar* especificar el nombre del archivo que se desea cifrar, ya sea, escribiendo el dato en el espacio de captura ó bien, utilizando el botón de la derecha de la caja de texto, para que se despliegue una ventana estándar de Windows y seleccionar el archivo.

En el campo *Archivo Destino* el sistema genera de manera automática, el nombre y ruta del destino del archivo cifrado, utilizando al nombre del archivo por cifrar con la extensión *.cbm*. El nombre del archivo destino antes mencionado puede ser modificado, ya sea escribiendo en la caja de texto el nombre correspondiente, o bien, usando el botón de la derecha para abrir una ventana estándar de Windows del tipo *Guardar Archivo*. Se recomienda respetar la extensión *.cbm* para permitir que las asociaciones de archivos y procesos funcionen adecuadamente.

En el campo *Tipo de Cifrado* elegir entre 3 posibles, un algoritmo de cifrado simétrico. Por omisión el sistema utiliza el algoritmo IDEA.

La clave simétrica que se utiliza para cifrar el archivo, es a su vez cifrada con la clave pública contenida en el certificado del destinatario.

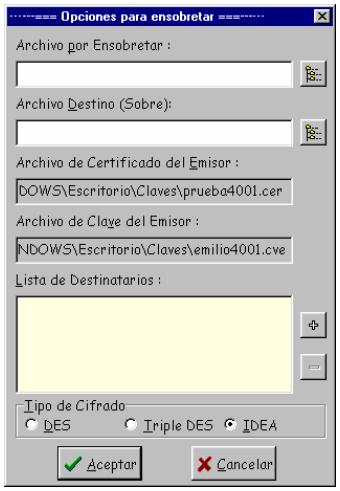
En el campo *Certificado del destinatario* se debe elegir el certificado del destinatario, de la Lista de Certificados que muestra el sistema pulsando el botón de la derecha de este campo. Una vez seleccionado el certificado del destinatario, en la caja de texto aparece el nombre común y el número de serie del certificado elegido. El sistema recuerda la última elección que haya hecho en este campo.

Una vez que se proporcionaron todos los datos, pulsar el botón *Aceptar* para que inicie el proceso de cifrado. Si la información es correcta, el sistema emite un sonido y muestra un mensaje en el ángulo inferior derecho de la pantalla principal.

4.3 ENSOBRETAR

Esta opción permite firmar y cifrar un archivo para su envío a uno ó más destinatarios, asegurando su confidencialidad y autenticidad.

Para llevar a cabo el proceso de ensobretado, el sistema presenta un cuadro de diálogo como el que se muestra a continuación:



En el campo *Archivo por ensobretar* especificar el nombre y ruta del archivo que se desea ensobretar, ya sea escribiendo el dato en el espacio de captura ó bien, utilizando el botón de la derecha de la caja de texto para que se despliegue una ventana estándar de Windows y seleccionar el archivo.

El campo *Archivo Destino* contiene el nombre que genera en forma automática el sistema, que corresponde al nombre original del archivo con extensión *.sbm.* Esta es una extensión registrada en las asociaciones de archivos y procesos por lo que se sugiere no cambiarla. El nombre del archivo destino antes mencionado puede ser modificado, ya sea escribiendo en la caja de texto el nombre correspondiente, o bien, usando el botón de la derecha para abrir una ventana estándar de Windows del tipo *Guardar Archivo*. Se recomienda respetar la extensión *.sbm* para permitir que las asociaciones de archivos y procesos funcionen adecuadamente.

En los campos de *Archivo de Certificado del Emisor* y *Archivo de Clave del Emisor* el sistema señala los archivos que utilizará en el proceso de firma, y son los que el usuario especificó en el proceso de *Identificación de Usuario*.

En el campo *Lista de Destinatarios,* agregar los Certificados de las personas a las que va dirigido el archivo ensobretado. Para ello, pulsar el botón con el signo "+" situado a la derecha de la lista, a fin de que aparezca la ventana de Lista de Certificados y elegir los de las personas que serán destinatarios.

Para eliminar de la *Lista de Destinatarios* uno o más certificados, seleccionar los que se desea eliminar y pulsar el botón de la derecha que tiene el signo "-".

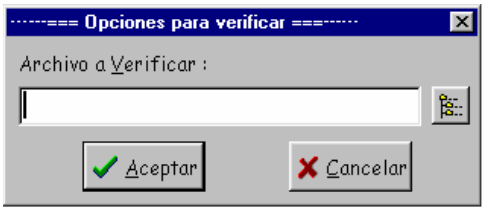
Por último, seleccionar el *Tipo de Cifrado* que debe ejecutar el sistema, marcando una de las tres opciones (DES, Triple DES, IDEA).

Para iniciar el proceso de ensobretado, pulsar el botón *Aceptar.* Si la operación es exitosa, el sistema emite un sonido y muestra un mensaje en la parte inferior derecha de la pantalla principal.

4.4 VERIFICAR

Esta opción permite verificar la validez de las firmas de un archivo y, en su caso, vincularla con el titular del certificado, a quien le será atribuible el archivo correspondiente y asegurar que el archivo no ha sido alterado.

Al seleccionar esta opción de proceso, el sistema muestra el cuadro de diálogo siguiente:



En el campo *Archivo a Verificar,* especificar el nombre y ruta del archivo firmado que se desea verificar, o bien, pulsar el botón de la derecha de la caja de texto a fin de que aparezca una ventana estándar de Windows y seleccionar el archivo respectivo.

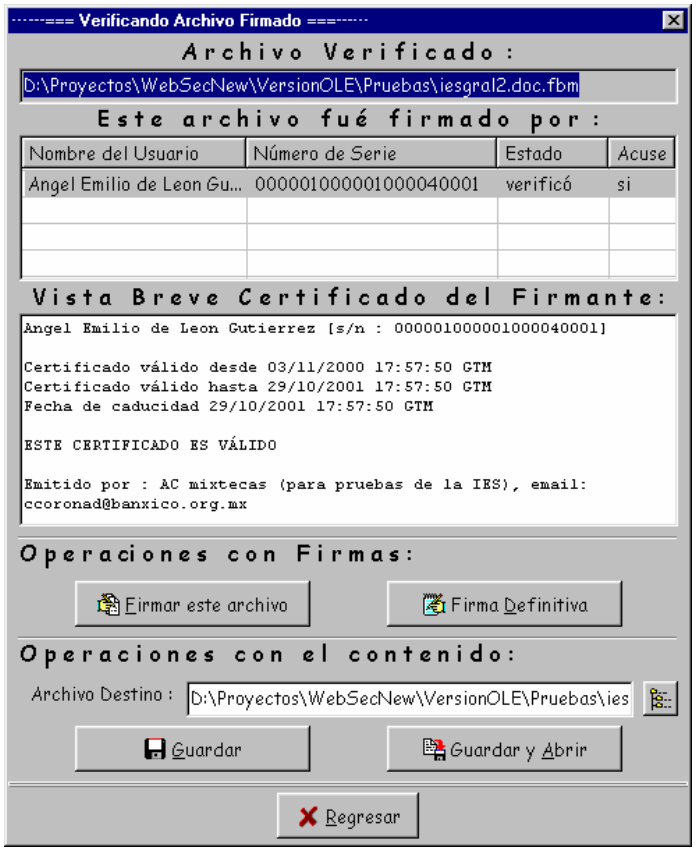
Al pulsar el botón *Aceptar* el sistema lleva a cabo los procesos siguientes:

- Verificación del formato del archivo.
- Obtención de los certificados necesarios para verificar las firmas contenidas en el archivo.
- En el caso de que alguno de los firmantes haya solicitado acuse de recibo, envía dicho acuse a través de correo electrónico.

Si por cualquier motivo, no se puede enviar el correo, el sistema muestra un mensaje de error, e interrumpe el proceso de verificación.

Si el envío del acuse de recibo es exitoso, el sistema muestra un aviso confirmando tal circunstancia.

Al finalizar los procesos anteriores, el sistema muestra una ventana que tiene el aspecto siguiente:

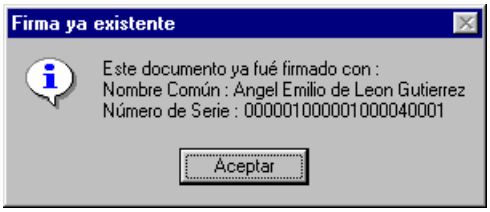


En esta ventana, el sistema presenta las características del archivo firmado y además, solicita se le indique qué operaciones se desea realizar respecto del archivo firmado. La ventana consta de seis partes:

- Nombre del archivo verificado.

- Un cuadro de información sobre la identidad de los firmantes del archivo, el resultado del proceso de verificación de la firma, y si el firmante solicitó acuse de recibo o no.
- Información sobre el certificado del firmante que está seleccionado.
- Sección de operaciones a ejecutar con firmas.
  Esta sección consta de dos botones, uno para agregar al documento la firma del usuario, y otro botón para reemplazar todas las firmas contenidas en el documento por la del usuario.

  Botón *Firmar este archivo*
  Este botón de proceso se utiliza para agregar la firma del último usuario identificado. El sistema presenta al usuario la opción de indicar si se desea acuse de recibo e inmediatamente después comienza el proceso de firma del documento. Si el procedimiento se realizó de manera adecuada, se agrega la firma del usuario al archivo y la información correspondiente aparece en el cuadro de *firmantes*. Si el archivo ya había sido firmado por el usuario, se muestra un cuadro de diálogo como el siguiente:



  Botón *Firma Definitiva*
  Este botón de proceso permite sustituir TODAS las firmas contenidas en el documento, por la firma del último usuario identificado. El sistema requiere que el usuario confirme su decisión de ejecutar el proceso, así como, si se desea acuse de recibo. Al decidir ejecutar este proceso, es importante considerar que es irreversible, por lo que se recomienda conservar una copia de respaldo del archivo para recuperar las firmas eliminadas.

- Sección de operaciones a ejecutar con el contenido del archivo:

  Esta sección consta de un cuadro de texto para especificar el nombre del archivo destino. El nombre que el sistema presenta de manera automática, es el del archivo original antes de ser firmado. Se puede modificar este campo escribiendo el nombre en el espacio de captura ó bien, utilizando el botón de la derecha de la caja de texto para que se despliegue una ventana estándar de Windows y seleccionar el archivo.

- La sección de operaciones a ejecutar con el contenido del archivo muestra dos botones adicionales, a saber:

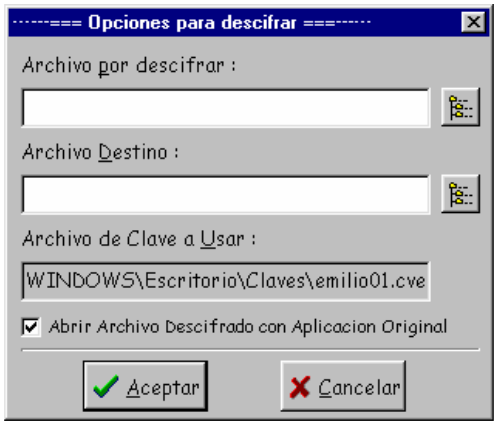
  Botón *Guardar*
  Este botón permite para almacenar una copia del archivo original verificado en la ruta dada por el nombre del archivo destino.

  Botón *Guardar y Abrir*
  Con este botón además de guardar el archivo original, se puede visualizar con la aplicación con la que fue creado, si por alguna razón el sistema no puede ejecutar dicha aplicación, muestra un mensaje de error.

4.5 DESCIFRAR

Con esta opción se puede ver el contenido de un archivo cifrado cuyo destinatario es el usuario.

Para llevar a cabo el proceso de descifrado de un archivo, el sistema muestra el siguiente cuadro de diálogo para obtener los datos necesarios.

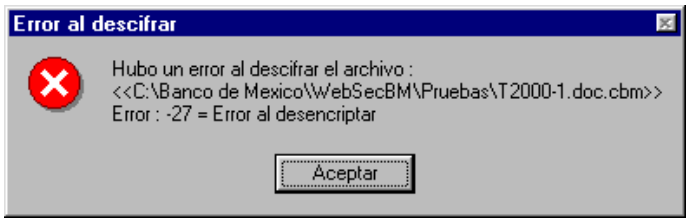


En el campo *Archivo por descifrar* se debe especificar el nombre y ruta del archivo que se desea descifrar, ya sea escribiendo el dato en el espacio de captura o bien, utilizando el botón de la derecha para que aparezca un cuadro de diálogo estándar de Windows y seleccionar el archivo.

En el campo *Archivo Destino*, el sistema genera un nombre de manera automática, que corresponde al del nombre del archivo a descifrar sin la extensión *.cbm*. Este nombre se puede modificar.

En el campo *Archivo de Clave a Usar* el sistema señala la clave privada que utilizará para descifrar el archivo, la cual corresponde al último usuario identificado.

Pulsar el botón de *Aceptar* para comenzar el proceso de descifrado. En el evento que se verifique un error durante el proceso, el sistema muestra un mensaje parecido al siguiente:



Este error se presenta generalmente cuando se intenta descifrar un archivo no destinado al usuario.

Si el proceso tiene éxito, el sistema emite un sonido y muestra un mensaje en el ángulo inferior derecho de la Pantalla Principal. Si además el usuario seleccionó la casilla de verificación con la leyenda *Abrir Archivo Descifrado con Aplicación Original*, el sistema ejecuta el proceso correspondiente a fin de abrir el archivo destino con la aplicación con la que fue creado, utilizando para ello la extensión del mismo. En este caso el sistema muestra un cuadro de diálogo con información sobre el proceso de apertura del archivo.

4.6 ABRIR SOBRE

Si el usuario identifica un archivo ensobretado y desea ver y/o guardar su contenido, esta opción le brinda la facilidad de abrir dicho archivo siempre y cuando el usuario sea el destinatario del archivo ensobretado.

Para ello, el sistema requiere que el usuario proporcione algunos datos en un cuadro de diálogo como el siguiente:

En el campo *Archivo Ensobretado* se debe especificar el nombre y ruta del archivo que se quiere abrir, ya sea escribiendo el dato en el espacio de captura o bien, utilizando el botón de la derecha para que se despliegue un cuadro de diálogo estándar de Windows a fin de seleccionar el archivo en cuestión.

En el campo *Archivo Destino*, el sistema genera en forma automática un nombre de archivo, basado en la ruta actual del archivo ensobretado, y cambiando el nombre por el del documento original. Si dicho nombre original no se encuentra almacenado en el sobre, el sistema proporciona de manera automática el nombre: *sinnombre.abm*. Este nombre se puede modificar.

En el campo *Certificado del Emisor* el sistema muestra el número de serie del certificado del emisor del archivo ensobretado que obtiene al indicársele de qué archivo se trata.

Pulsar el botón de *Aceptar* para comenzar el proceso de apertura. Si en este proceso ocurre algún error derivado, entre otras razones, por el hecho de que el sobre no esté destinado al usuario, el sistema muestra una ventana indicando el error correspondiente.

Si el proceso de apertura del sobre es exitoso, el sistema almacena el archivo original con el nombre indicado en *Archivo Destino*, emite un sonido y muestra un mensaje en el ángulo inferior derecho de la Pantalla Principal.

Si además, el usuario seleccionó la casilla con la leyenda *Abrir Sobre Abierto con Aplicación Original*, el sistema abre el archivo destino con la aplicación con la que fue creado, basándose para ello en la extensión del propio archivo, en este caso el sistema muestra un mensaje indicando el resultado de este proceso.

4.7 IDENTIFICACIÓN DEL USUARIO

Mediante este proceso, el usuario proporciona al sistema su certificado digital, clave privada y frase de seguridad con el objeto de que el sistema cuente con los elementos necesarios para realizar las operaciones que el usuario solicite.

Al inicio de cada sesión, el sistema siempre ejecuta el proceso de identificación de usuario conforme al procedimiento que se describe en el numeral 2 de este manual.

Sin embargo, esta opción se utiliza cuando en una misma sesión se desea continuar realizando operaciones pero bajo el nombre de un usuario distinto al que tiene registrado el sistema en ese momento.

4.8 MOSTRAR CERTIFICADOS

Se incorporó al sistema esta opción en el Menú de Herramientas, a fin de que el usuario esté en posibilidad de almacenar en una base de datos local, copias de los certificados que se obtengan de la IES. Estos certificados se pueden consultar o eliminar de la base de datos local, así como incorporar nuevos certificados.

Para llevar a cabo este proceso, el sistema muestra la ventana siguiente:

A través de esta ventana el usuario puede administrar las referencias de diversos certificados, así como, seleccionar los certificados que en ella figuren para ejecutar las aplicaciones de *Cifrar un Archivo* y *Ensobretar un Archivo*.

En la lista de certificados que se despliega en la ventana antes mencionada, se puede observar los campos siguientes:

- ***Número de Serie***: Es el número que identifica de manera única a cada certificado.
- ***Nombre Común***: Es parte del nombre distinguido del propietario del certificado y, usualmente, es el nombre de la persona que posee dicho certificado.
- ***Fecha de Actualización***: Es la última fecha y hora en que se consultó el certificado de manera satisfactoria en la IES. La hora es local y depende del sistema del usuario.
- ***Fecha de Inicio***: Identifica la fecha y hora de inicio de validez del certificado, referida al horario del Meridiano de Greenwich.
- ***Fecha del Fin***: Corresponde a la fecha de terminación de vigencia del certificado de que se trate, misma que se encuentra referenciada al huso horario del Meridiano de Greenwich. Después de dicha hora y fecha, el certificado no debe ser aceptado como válido.
- ***Fecha de Caducidad***: Un certificado caduca en la fecha y hora, referida al Meridiano de Greenwich, en que dicho certificado es revocado, o bien, en la misma fecha señalada en el campo *Fecha del Fin,* referida al mismo huso horario.

Además en la pantalla, se tienen los botones siguientes:

- ***Elimina**:* Permite eliminar referencias de certificados de la base de datos local. Este botón sólo aparece si se selecciona la opción desde el menú y no, cuando se invoca esta ventana desde las opciones de cifrado ó ensobretado.

- ***Agrega:*** Permite agregar nuevas referencias de certificados en la base de datos local, siempre y cuando, se conozca el número de serie de los certificados deseados.

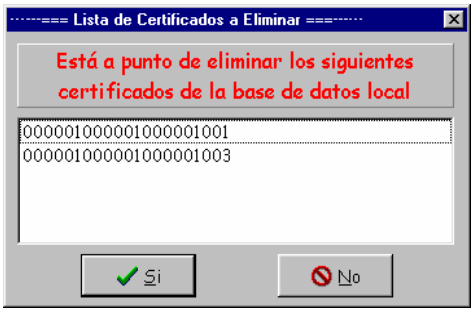
- ***Muestra**:* Una vez que se selecciona una referencia de la lista de certificados, se puede ver la ventana de *Contenido del Certificado* pulsando este botón.

- ***Aceptar**:* Cierra la ventana, llevando a cabo de forma definitiva las modificaciones realizadas en la sesión que se cierra.

- ***Cancelar**:* Cierra la ventana, sin considerar las modificaciones realizadas en la sesión que se cierra .

Botón Elimina un Certificado

Para eliminar una ó más referencias de la *Lista de Certificados*, primero el usuario deberá seleccionar los certificados que desea eliminar, y pulsar el botón *Elimina*. A continuación, el sistema requiere que el usuario confirme su elección mediante el cuadro de diálogo siguiente:



Si el usuario selecciona el botón *Si*, el sistema procederá a borrar los certificados elegidos de la base de datos en pantalla y cuando se pulse el botón *Aceptar* en la ventana de la Lista de Certificados, la base de datos en el disco se modificará en forma definitiva. Pulsando el botón *Cancelar* en la ventana de Lista de Certificados, el usuario estará en posibilidad de revertir el proceso de eliminación de certificados.

Botón Agrega un Certificado

Para agregar referencias a la Lista de Certificados, solicitándolos de la base de datos de la IES, el usuario deberá pulsar el botón *Agrega*. El sistema despliega el cuadro de diálogo siguiente:

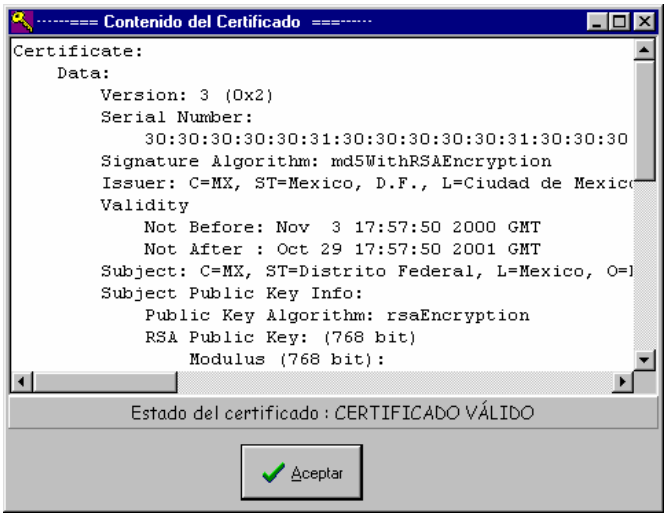
En el cuadro de texto *Número de serie del certificado*, indicar el número de serie (20 dígitos) que identifica al certificado que se desea agregar.

Habiendo proporcionado el número de certificado, el usuario deberá pulsar el botón *Aceptar* a fin de que el sistema procese la solicitud respectiva. Si el proceso es exitoso, el certificado solicitado aparece en la

Lista de Certificados, en caso contrario, el sistema muestra un cuadro de diálogo indicando el error correspondiente.

Botón Muestra el Contenido de un Certificado

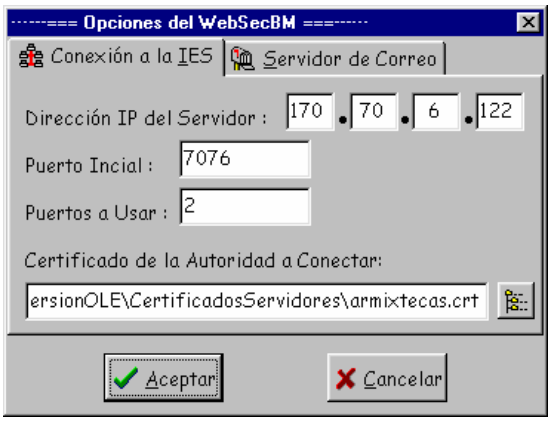
Para ver la información contenida en un certificado que esté referido en la base de datos local, el usuario deberá seleccionar el certificado deseado de la Lista de Certificados y pulsar el botón *Muestra*. El sistema despliega la ventana que se indica a continuación, con el contenido del certificado y el estado de validez del mismo. Si el certificado no está vigente o fue revocado, la ventana proporciona la información relativa a la validez o vigencia, según se trate.



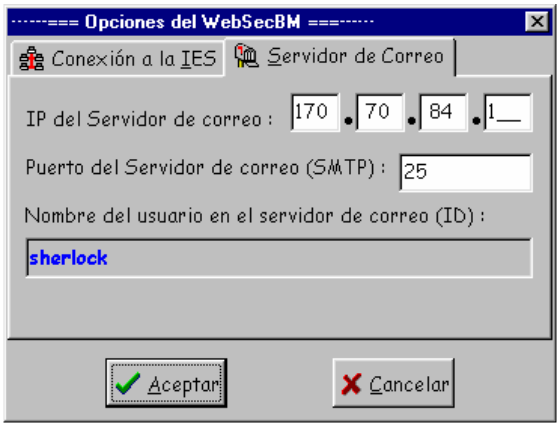
4.9 CONFIGURACIÓN

Esta opción permite especificar los parámetros necesarios tanto para establecer conexión con una Agencia Registradora de la IES, como para enviar a través del servidor de correo los acuses de recibo de los documentos firmados cuya firma se verificó.

Al seleccionar esta opción, el sistema muestra el cuadro de diálogo siguiente, que consta de dos páginas, *Conexión a la IES* y *Servidor de Correo.*



En la página *Conexión a la IES* se especifica la dirección IP del servidor de la IES, el puerto inicial al que se conectaría el usuario y el número de puertos disponibles en el servidor. Además, se proporciona el archivo que contiene el certificado digital de la Agencia Registradora (AR) con la que se desea conectar.



En la página *Servidor de Correo* se especifica la dirección IP del servidor de correo y el Puerto de Comunicación con dicho servidor. Además, el sistema muestra el nombre del usuario que aparece en el certificado, mismo que no se puede modificar. Estos datos se emplean para el envío de acuses de recibo requeridos en algunos archivos firmados.

Si se tiene alguna duda respecto de la información que el usuario debe proporcionar en esta opción, se recomienda solicitar asesoría a su administrador de correo.

Los parámetros especificados en estas páginas quedan actualizados en cuanto se pulsa el botón *Aceptar*.

5. ASOCIACIÓN DE ARCHIVOS Y PROCESOS

El WebSecBM es un programa de cómputo (software) que, entre otras funciones, asocia un proceso en particular a un archivo de acuerdo con la extensión del archivo de que se trate.

Están definidos 3 tipos de archivos según su extensión:

Extensión	**Proceso que se Asocia**
fbm : para archivos firmados.	Verificación de la firma
cbm : para archivos cifrados.	Descifrado del archivo
sbm : para archivos ensobretados.	Apertura del sobre, esto es, verificación de la firma y descifrado del archivo.

En el ambiente del explorador de Windows®, cuando se pulsa dos veces sobre el nombre de un archivo con alguna de estas extensiones, el sistema operativo ejecuta el sistema WebSecBM de manera automática, presentando primero la pantalla de *Identificación de Usuario*.

A continuación, se realiza el proceso que corresponda al tipo de archivo seleccionado. Una vez que termina de procesar el archivo, el control de la computadora regresa al sistema operativo.

Si se está visualizando una página del WWW con Microsoft Explorer®, y se pulsa sobre una liga a un archivo que tenga alguna de estas extensiones, es posible configurar el navegador para que abra el WebSecBM de manera automática y ejecute el proceso que corresponda.

Al respecto, en el navegador Netscape Navigator® sólo funcionan, por el momento, las ligas que se refieran a un archivo situado en un servidor FTP, pero no funciona en todas las ligas a archivos situados en servidores http, esto es un comportamiento estándar del Netscape Navigator® y es poco probable que cambie en el futuro, por lo que si el usuario desea publicar archivos generados con este sistema en Internet, es recomendable que todas las ligas se realicen hacia un servidor de FTP a fin de proveer la máxima compatibilidad posible.

6. CONEXIÓN ENTRE EL SISTEMA WebSecBM Y LA IES

Para llevar a cabo el proceso de algunas operaciones como son: *Cifrar, Verificar* y *Abrir Sobre*, el sistema requiere los certificados digitales de aquellos usuarios que estén involucrados en la operación, ya sea como destinatarios, firmantes o emisores de los archivos. Por ello, el sistema requiere mantener comunicación con la IES, a fin de estar en posibilidad de solicitarla información de los certificados que sea necesaria.

Para tales efectos, el sistema WebSecBM permite establecer comunicación con la IES a través de cualquier Agencia Registradora (AR); sin embargo, con el propósito de proveer a una mayor rapidez de respuesta y eficiencia en el servicio, se recomienda establecer comunicación con la AR en la que esté registrado el certificado del usuario con el que se hacen las solicitudes de certificados.

La IES sólo atiende peticiones de aquellos usuarios que cuenten con un certificado válido registrado en la misma, por lo que en el evento de que el certificado del usuario no se encuentre registrado, haya caducado ó haya sido revocado, la IES no se encuentra en posibilidad de proporcionar el servicio respectivo.

Otro motivo por el cual la IES puede desconocer un certificado, ocurre cuando se hace uso de él, con una clave privada que no corresponde a la clave pública del certificado. En este caso la IES también niega el servicio y cualquier archivo que haya sido firmado o ensobretado en estas circunstancias, no puede ser validado.

7. USO DEL WebSecBM CON APLICACIONES DE MICROSOFT® OFFICE®

Se ha integrado el WebSecBM con las siguientes aplicaciones de la suite Microsoft Office: Microsoft® PowerPoint®, Microsoft® Word® y Microsoft® Excel®.

Dentro de dichas aplicaciones, quedan disponibles tres operaciones: Cifrado OLE, Ensobretado OLE y Firmado OLE. Al seleccionar cualquiera de estas opciones, se lleva a cabo el proceso siguiente:

- Se guarda la presentación, el documento o la hoja de trabajo activa según la aplicación de que se trate, pidiendo el nombre del archivo si no se había guardado antes.
- Se cierra el archivo activo en la aplicación de Office®, esto debido a que las aplicaciones de Office® abren los archivos en modo exclusivo, por lo que ninguna otra aplicación puede abrir un archivo mientras Office® lo mantenga abierto.
- Se solicita acceso a la función correspondiente en el WeSecBM™, atendiendo a los criterios siguientes:
    - Si no hay una instancia del WebSecBM en proceso, se ejecuta el mismo en un modo especial que permite llamar a la función solicitada conforme a los criterios mencionados en este manual, y una vez terminado el proceso, se cierra la aplicación.

- Si ya hay una instancia del WebSecBM en proceso, no se ejecuta otra instancia, sino que se avisa que ya está ejecutándose el WebSecBM y debe cerrarse primero para poderlo utilizar desde adentro de la aplicación de Office®.

- En caso de que se presente algún error, habrá que notarlo mediante los cuadros de diálogo que muestre el WebSecBM, pues dentro del Office® no se da indicio del evento.

- Una vez que termina la ejecución de la función elegida, se vuelve a abrir el archivo dentro de la aplicación del Office®.

Breve explicación de los métodos matemáticos usados en los sistemas de criptografía de la Firma Electrónica Avanzada.

De una forma general se puede decir que las claves públicas y privadas se definen como argumentos de las funciones de verificación y creación de firmas electrónica avanzada respectivamente. En un sistema de criptografía público privada general se definen dos funciones diferentes $f(m_a,c_{priv}):MxC \rightarrow M$ (donde M es el espacio de mensajes y C es el espacio de claves) y $g(m_c,c_{pub}):MxC \rightarrow M$ en donde f cifra el mensaje m_a y lo transforma en un mensaje m_c usando una clave c_{priv} que llamaremos clave privada, y g descifra m_c usando la clave c_{pub} que está relacionada unívocamente con c_{priv}, a esta clave c_{pub} se le llamará clave publica. A partir de las demostraciones de existencia de estas claves con las técnicas matemáticas correspondientes se demuestra que estas funciones y estas claves existen y que a partir de una de dichas claves es computacionalmente imposible encontrar la otra.

Para el caso del algoritmo RSA las claves pública y privada son dos pares de números relacionados matemáticamente de la forma siguiente: sean p y q dos números pseudoprimos que satisfacen las pruebas de primalidad aceptadas para el algoritmo RSA con los que se calcula $n = pq$ y $m = (p-1)(q-1)$ y se elige un numero e que sea primo relativo con m (usualmente se elige siempre el mismo número y las opciones más utilizadas son: el cuarto número de Fermat[1] = 65537 ó 010001 en base 16, o el número 3; ambas opciones permiten implementar el algoritmo del RSA de manera muy eficiente; la elección puede depender solamente de que e cumpla con ser primo relativo con m)
Se define como clave pública a la pareja (e, n).
Se define como clave privada a la pareja (d, n) en donde d cumple que **$e\ d$ módulo $m = 1$.**

La explicación de los métodos matemáticos usados en la RSA se hará usando una técnica de construcción de métodos aritméticos a partir de conceptos simples y se usará el sistema *Mathematica*[2] para realizar los cálculos.
Se procederá de la forma siguiente:

1. Se empezará por mostrar el algoritmo de la división que está basado en la división de números enteros, de hecho este algoritmo es usado para calcular el Máximo Común Divisor de dos números enteros y se denota con **GCD** por su nombre en ingles. Para este punto es necesario aclarar que el cociente entero de la división de dos números enteros se denotará como **Quotient** y el residuo como **Mod**;
2. Se mostrará el concepto de inverso multiplicativo en un conjunto de números enteros llamado **Zn** con el propósito de explicar qué es un inverso multiplicativo y que sirva como motivación para el algoritmo RSA;

[1] Números de Fermat: los números de Fermat son de la forma (2^(2^n)+1), el número 1 de Fermat es (2^(2^1)+1)=5, el número 2 de Fermat es (2^(2^2)+1)=17, el siguiente es (2^(2^3)+1)=257, y el 4 es (2^(2^4)+1)=65537. Fermat había afirmado que todos estos números eran primos aunque esto no es cierto.
[2] Se usa el sistema *Mathematica* para poder hacer los cálculos numéricos cuando se usan número grandes. El usar este sistema demuestra que todo lo que se explica es factible de realizarse con la ayuda de una computadora y refuerza la necesidad de usar números muy grandes que no puedan ser manejados facilmente.

3. Se aplicará este concepto para ejemplificar un sistema criptográfico muy simple no seguro, pero que se puede repetir usando una calculadora, para después mostrar un ejemplo más difícil de calcular , y finalmente
4. Se construirá el método RSA que usa la función **PowerMod[msg, e, n]** que eleva la cantidad **msg** a la potencia **e** módulo **n** y que se puede definir como multiplicar **msg** por si mismo **e** veces módulo **n**..

Es necesario aclarar que se omitirán todas las demostraciones de existencia de los números que se obtienen en los algoritmos, y se dejará a la intuición comprender que siempre que el problema matemático está bien planteado existe la solución buscada. En los ejemplos numéricos que se muestran siempre se encuentra la solución.

A manera de introducción de las ideas necesarias para explicar estos métodos, es útil reflexionar acerca de cómo funciona el sistema que se usa para denotar la hora del día. Dependiendo de la preferencia personal, se usan los dígitos **0** a **12** ó **0** a **24** y cada vez que la manecilla del reloj pasa por el **12** ó el **24** se vuelve a empezar a contar en cero las horas del día. Esta forma de trabajar se llama en matemáticas un grupo módulo **12** ó **24**, y estos grupos tienen la gracia que se puede definir con ellos las operación de suma y producto, por ejemplo, si se trabaja módulo **24** horas siempre se puede calcular qué hora será después de que transcurran **16** horas a partir de este momento, si en este momento fueran las **12** horas del día, la respuesta sería: las **4** horas de la mañana del día siguiente.

¿Qué significa que un número sea divisible por otro?

La respuesta es simple y se visualiza mejor con dos ejemplos, 8 es divisible entre 4 porque el residuo entero de la división 8/4 es cero, y 9 no es divisible entre 4 porque el residuo entero de la división 9/4 es 1.

¿Qué significa que un número sea primo?

Se sabe que los números enteros existen en dos presentaciones:

1. bien son divisibles por ellos y por la unidad únicamente, en cuyo caso los llamamos números primos, ejemplo: 1, 2, 3, 5, 7, 11, …;
2. o bien son un producto de números primos, ejemplo 4 = 2 * 2, 6 = 2* 3, 8 = 2 * 2 * 2 * 2, 9 = 3 * 3, 10 = 2 * 5, 12 = 2 * 2 * 3, ….

y se puede demostrar que todo número natural o es primo o es un producto de primos, y no existe otra posibilidad.

¿Qué es un inverso multiplicativo de a con a diferente de cero?

Es el número **b** que multiplicado por **a** dentro del conjunto de reglas que se este usando arroja como resultado de la multiplicación el número**1**, ejemplo usando los número racionales se tiene que: **2 * (1/2) = 1**.
Para explicar el tema que interesa, se va a usar la definición de inverso multiplicativo en **Zn**, en donde las multiplicaciones se realizan **módulo n**, lo que es lo mismo, que decir que primero se realiza la multiplicación entera y luego se divide ente **n** y el residuo de la división que es un número entero es el resultado de la multiplicación.

¿Qué es Zn?

Es el conjunto de números **{0, 1, 2, 3, … , (n -1)}**, ejemplo para **Z11** los elementos son: **{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10}** y para **Z24** son **{0, 1, 2, … 23}**.
Se puede mostrar para **Z11** a cada uno de sus elementos y su inverso multiplicativo:

Elemento de ***Z11***	Inverso multiplicativo	
1	**1**	Residuo de (*1 * 1*) / *11* = *1*
2	**6**	Residuo de (*2 * 6*) / *11* = *1*
3	**4**	Residuo de (*3 * 4*) / *11* = *1*
4	**3**	Residuo de (*4 * 3*) / *11* = *1*
5	**9**	Residuo de (*5 * 9*) / *11* = *1*
6	**2**	Residuo de (*6 * 2*) / *11* = *1*
7	**8**	Residuo de (*7 * 8*) / *11* = *1*
8	**7**	Residuo de (*8 * 7*) / *11* = *1*
9	**5**	Residuo de (*9 * 5*) / *11* = *1*
10	**10**	Residuo de (*10 * 10*) / *11* = *1*

Se puede observar en la tabla precedente que todos los elementos de **Z11** tienen un inverso multiplicativo en **Z11**.
Para **Z12** la situación es más compleja, es necesario decir que **12 = 2 * 2 * 3** porque no todos los elementos de **Z12** tienen inverso multiplicativo **módulo 12** y algunos lo tienen bajo otro número primo que está en la descomposición factorial de **12**:

En este caso el **6** en **Z12** no tiene inverso multiplicativo, y no todos los inversos son **módulo 12**.

Elemento de *Z12*	Inverso multiplicativo	módulo
1	**1**	*12*
2	**2**	*3*
3	**3**	*4 = 2 * 2*
4	**1**	*3*
5	**5**	*12*
6		
7	**7**	*12*
8	**2**	*3*
9	**1**	*4*
10	**1**	*3*
11	**11**	*12*

A continuación se presentan ejercicios numéricos en donde se muestran este tipo de cálculos y la forma de aplicarlos para obtener sistemas criptográficos.

Los ejemplos son los siguientes:

a) Algoritmo de la división para **n = 15485863**, **n** es primo.
b) Cálculo del inverso multiplicativo en **Zn** (con **n** primo).
c) Ejemplo de cifrado en **Zn** (con números pequeños).
d) Ejemplo de cifrado usando RSA.

a) Algoritmo de la división para n = 15485863, n es primo.

En este ejercicio simplemente se calculará el algoritmo de la división para conocer todos los valores que se usarán en los ejemplos de cálculo del inverso multiplicativo en **Zn** cuando **n** es primo y diferente de cero.
Los números que se usaran como ejemplos **son n = 15485863** y **a = 33951**.
ACLARACIÓN: las negrillas que aparecen un renglón sin texto adicional representan texto que se introduce al sistema *Mathematica* y la línea siguiente representa el resultado que calcula el sistema. Es necesario saber que este sistema realiza cálculos simbólicos y numéricos indistintamente.

```
n = 15485863
15485863
```

Se puede verificar fácilmente que **n** es primo usando la función **PrimeQ**

```
PrimeQ[n]
True
a = 33951
33951
```

Para calcular el cociente y el residuo de **n / a** se usan las funciones **Quotient** y **Mod**

```
q1 = Quotient[n, a]
456
r1 = Mod[n, a]
4207
```

Los pasos siguientes corresponden a las divisiones adicionales que es necesario realizar en el algoritmo de la división, el cual sirve adicionalmente para calcular el Máximo Común Divisor de dos números. Este algoritmo termina cuando el residuo que se calcula es cero. Al residuo inmediato anterior se le llama Máximo Común divisor.

```
q2 = Quotient[a, r1]
8
r2 = Mod[a, r1]
295
q3 = Quotient[r1, r2]
14
r3 = Mod[r1, r2]
77
q4 = Quotient[r2, r3]
3
r4 = Mod[r2, r3]
64
q5 = Quotient[r3, r4]
1
r5 = Mod[r3, r4]
13
q6 = Quotient[r4, r5]
4
r6 = Mod[r4, r5]
12
q7 = Quotient[r5, r6]
1
r7 = Mod[r5, r6]
1
q8 = Quotient[r6, r7]
12
r8 = Mod[r6, r7]
0
```

Como se puede ver, el residuo **r8** es cero, por lo tanto el algoritmo ha terminado.

En este caso, el Máximo Común Divisor de **15485863** y **33951** es **1**

b) Cálculo del inverso multiplicativo en Zn (Caso con **n** primo)

A continuación se transcriben los resultados numéricos que resultan del algoritmo de la división de dos números enteros como texto y no como datos para el sistema *Mathematica* para poder realizar los cálculos simbólicos que se desea mostrar, en este caso se usaran **n = 15485863** y α **= 33951** y se busca un número γ tal que el residuo de la división entre n del producto de **g** por α sea igual a 1.

Empezamos por dividir **n** entre α, los valores que resultan del algoritmo de la división son:

q1 = 456, q2 = 8, q3 = 14, q4 = 3, q5 = 1, q6 = 4, q7 = 1, q8 = 12, r1 = 4207,r2 = 295, r3 = 77, r4=64, r5 = 13, r6 = 12, r7 = 1 y r8 = 0.

Se verifica fácilmente que **n = 456 *** α **+ 4207**.

La idea que se usará a continuación consiste en crear un sistema de ecuaciones para mostrar que se puede encontrar el inverso multiplicativo haciendo sustituciones sucesivas de las ecuaciones que arroja el algoritmo de la división, se utilizará el sistema *Mathematica* para crear dicho sistema de ecuaciones simultáneas. Este ejemplo es muy simple debido a que podemos calcular todos los valores del algoritmo de la división y mostrarlos en el documento lo cual permite hacer el proceso de la forma como se está mostrando.

Se Escriben simbólicamente las ecuaciones que se obtienen con el algoritmo de la división:

```
e1 := q1 a + r1 - n
e2 := q2 r1 + r2 - a
e3 := q3 r2 + r3 - r1
e4 := q4 r3 + r4 - r2
e5 := q5 r4 + r5 - r3
e6 := q6 r5 + r6 - r4
e7 := q7 r6 + r7 - r5
e8 := q8 r7 - r6
```

estas ecuaciones muestrar que es posible encontrar el inverso multiplicativo de α en **Zn** debido a que les posibleresolver el sistema y mostrar que el resultado es una combinación lineal de **n** y α igual a 1, con este propósito se resuelve el sistema para **r7**, se eliminan las variables **r1** a **r6** del sistema anterior, esto se logra con la instrucción siguiente:

```
Simplify[Reduce[e1 == 0 && e2 == 0 && e3 == 0 && e4 == 0 && e5 == 0 && e6 == 0 && e7 == 0,
r7, {r1, r2, r3, r4, r5, r6}]]
```

n (1 + q6 q7 + q4 (q5 + q7 + q5 q6 q7)+ q2 (q5 + q7 + q5 q6 q7 + q3 (1 + q6 q7 + q4 (q5 + q7 + q5 q6 q7))))==
r7 + (q5 + q7 + q5 q6 q7 + q3 (1 + q6 q7 + q4 (q5 + q7 + q5 q6 q7))+ q1 (1 + q6 q7 +
q4 (q5 + q7 + q5 q6 q7)+ q2 (q5 + q7 + q5 q6 q7 + q3 (1 + q6 q7 + q4 (q5 + q7 + q5 q6 q7)))))α

el resultado que se ha obtenido está expresado únicamente usando **q1 … q7**, **n**, α y **r7** han desparecido de la expresión **r1 … r6** lo que demuestra que n y α se pueden escribir como una combinación lineal, que es lo que se buscaba, ya que se conocen los valores **q1 … q7** gracias al algoritmo de la división. El cálculo en *Mathematica* hasta este momento es puramente simbólico, falta introducir los valores numéricos que ya se conocen de antemano.
Se definen los valores de **q1 … q7** dentro del sistema *Mathematica* para encontrar la expresión de la combinación lineal,

```
q1 = 456
456
q2 = 8
8
q3 = 14
14
q4 = 3
3
q5 = 1
1
q6 = 4
4
q7 = 1
1
q8 = 12
12
```

se repite el cálculo, esta vez de forma numérica para obtener la combinación lineal que se está buscando

```
Reduce[e1 == 0 && e2 == 0 && e3 == 0 && e4 == 0 && e5 == 0 && e6 == 0 && e7 == 0 ,
r7, {r1, r2, r3, r4, r5, r6}]
2647 n - 1207360 α == r7
```

Se busca que el residuo de la división de $\alpha\gamma$ dividido entre **n** sea igual a 1, ya se sabe que **r7** es igual a **1**, y los dos coeficientes **2647** y **-1297360** impiden ver el resultado claramente ya que el coeficiente de α, **-1207360** que no está en **Zn** (los elementos de **Zn** son : {0, 1, 2, ..., n -1}). Para corregir el problema se suma **n** al coeficiente actual de α **módulo n** y así se obtiene el inverso multiplicativo correcto

```
n = 15485863
15485863
a = 33951
33951
2647 n - 1207360 a
1
γ = -1207360 + n
14278503
```

ya que **14,278,503** es menor a **15,485,863**. Y la verificación final del cálculo consiste en calcular el producto $\alpha\,\gamma$ **módulo n**

```
Mod[α γ, n]
1
```

lo cual por definición significa que γ **=** `14278503` **es el inverso multiplicativo de** α **en Zn.**
Con esto hemos mostrado que podemos encontrar las expresiones simbólicas y los algoritmos computacionales necesarios para calcular los inversos multiplicativos en Zn.
Este cálculo se puede realizar fácilmente con el sistema *Mathematica* de la forma siguiente:

```
Solve[a x = 1 && Modulus = n, x]
```

{{Modulus ->15485863, x->14278503}}

Como se puede ver **x =** γ**.**
De ahora en adelante usaremos esta forma simple que ofrece el sistema de computo que estamos usando para calcular los inversos multiplicativos módulo n.

c) Ejemplo de cifrado en Zn (con números pequeños)

Como objetivo de este ejemplo se propone crear un criptosistema simple usando **Z11**.
Se considera el conjunto **Zn = {0,1,...,n-1}**, y se definea la operación suma y multiplicación **módulo n** de la siguiente forma:
Sean α y β ε **Zn**.
La suma $\alpha+\beta$ **módulo n** se denota como **Mod[**$\alpha+\beta$**,n]** y es el residuo que resulta de dividir entre **n** la suma de α y β , que pertenece al conjunto **Zn**.
El producto $\alpha\beta$ **módulo n** se denota como **Mod[**$\alpha\beta$**,n]** y es el residuo que resulta de dividir entre **n** el producto de α y β , que pertenece al conjunto **Zn**.
Ejemplo:

```
n = 15
15
a = 5
5
b = 10
10
```

la suma de **a** y **b** es:

```
Mod[a + b, n]
0
```

y el producto es:

```
Mod[a b, n ]
5
```

Definición: Se Dice que α es congruente con β **módulo n**, si β **= Mod[**α**,n]**, o lo que es lo mismo si **n** divide a α-β.
Definición: Se define el máximo común divisor de dos números **a** y **b** como el número más grande que divide a ambos y se denota como **GCD[a,b]**.
Ejemplo:

```
GCD[225, 120]
15
GCD[12, 20]
4
```

Para calcularlo se usa el algoritmo de la división o algoritmo de Euclides como en los,
1) a = q1 b + r1
2) b = q2 r1 + r2
3) r1 = q3 r2 + r3
4) r2 = q4 r3 + r4
.
.
.
n-1) rn-3 = qn-1 rn-2 + rn-1
n) rn-2 = qn rn-1 + rn
n+1) rn-1 = qn+1 rn + 0, con rn+1=0

y el Máximo Común Divisor es el último residuo diferente de cero, por lo tanto rn es el **GCD[a,b]**.
Como ya se mostró en el cálculo del inverso multiplicativo de **Zn**, es posible escribir **rn** como una combinación lineal de **a** y **b**, i.e**. rn = p a + q b**. Cuando **n** es primo, **Zn** es un campo para la multiplicación, esto quiere decir que para todo $\alpha \varepsilon$ **Zn** existe $\gamma \varepsilon$ **Zn** tal que $\alpha\gamma$ es congruente con **1 Mod n** (**Mod[**$\alpha\gamma$**,n] = 1**, definición de inverso multiplicativo).
Ejemplo:
Se considera un número primo cualquiera que se calculará con la función **Prime[k]** que entrega el **k**-ésimo primo

```
n = Prime[5]
11
```

se puede verificar que **n** es primo usando la función **PrimeQ[n]**

```
PrimeQ[n]
True
```

Se tom< un número

```
a = 6
6
```

se usa el algoritmo de Euclides que está programado en la función **Solve** para encontrar el inverso multiplicativo de α:

```
Solve[ x == 1 && Modulus == n, x]
88Modulus –>1, x –>2<<
```

lo cual dice que

```
γ = 2
2
```

esto se comprueba calculando

```
Mod[a g, n]
1
```

que cumple con la propiedad buscada.

¿Cómo se cifra y se descifra con este sistema?

Se llamarás ahora a α la ***clave privada*** y a γ la ***clave publica***, en este caso es muy simple calcularlas como se ha visto en los pasos anteriores.
Si el mensaje que se quiere enviar es el número 7,

```
msg = 7
7
```

el mensaje cifrado es el producto **msg** α **modulo n**, entonces:

```
cifrado = Mod[msg a, n]
9
```

y para descifrar se multiplica el mensaje cifrado por γ, lo que da:

```
descifrado = Mod[cifrado g, n]
7
```

este método es un ejemplo simple que no presenta las propiedades de seguridad necesarias para ser útil, sin embargo ejemplifica perfectamente la mecánica que se usará en un método RSA.

d) Ejemplo de cifrado usando RSA

Cuando se usan números muy grandes en el criptosistema que se presentará a continuación, es muy costoso el proceso de descifrado de un mensaje si no se conoce la clave correspondiente. Los tiempos estimados para el descifrado de mensajes cifrados con llaves de 1024 se estiman del orden de centenares de años.

El primer paso consiste en escoger dos números primos cualquiera, es necesario aclarar que no todos los números primos sirven para implementar un algoritmo RSA seguro, pero para los fines del ejemplo que estar qué es una clave pública y la correspondiente privada es suficiente.
En este ejemplo se usarán números primos cualesquiera.
La seguridad del algoritmo radica en usar números primos muy grandes y que tengan algunas propiedades predeterminadas.
En este caso se usaran las funciones **Prime** y **PrimeQ** que ya se han usado antes.
Sean
p = Prime[100000]

1299709
q = Prime[233124]
3243133
el algoritmo RSA define los números **n** y **m** como
n = p q
4215129148297
y
m = (p – 1)(q – 1)
4215124605456
cuando **p** y **q** son números primos muy grandes (i.e. con mas de 100 cifras decimales) toma demasiado tiempo de computadora calcular la factorización en números primos, en este detalle práctico se basa la seguridad del algoritmo, para este ejemplo este procedimiento puede ser realizado con el sistema *Mathematica*.
La factorización en números primos se realiza con la criba de Erastótenes, esta función está implementada en la función **FactorInteger** (es interesante mencionar que en las escuelas primarias se enseñaba a encontrar la descomposición en primos de un número dado hace 38 años,
nunca se mencionaba que si el numero era muy grande nunca íbamos a terminar la tarea).
Se calculara el tiempo que le toma a *Mathematica* calcular algunas factorizaciones para tener una idea de como crece el tiempo de cálculo (es posible que *Mathematica* haga algunas optimizaciones para hacerlo mas rápido en algunos casos).

Module[{}, t1 = TimeUsed[]; FactorInteger[n]; t2 = TimeUsed[]; t2 - t1]
0.44
Module[{}, t1 = TimeUsed[]; FactorInteger[m]; t2 = TimeUsed[]; t2 - t1]
0.
Module[{}, t1 = TimeUsed[]; FactorInteger[100!]; t2 = TimeUsed[]; t2 - t1]
0.33
gprime = Prime[10000000]Prime[10 !]Prime[100000000]
22377713242087589262689233
Module[{}, t1 = TimeUsed[]; FactorInteger[gprime]; t2 = TimeUsed[]; t2 - t1]
1.93

Como se puede ver, el tiempo de proceso crece rápidamente con el tamaño del número que se desea factorizar, el último ejemplo apenas tiene 26 digitos decimales o lo que es los mismo 81 bits, el numero **m** se factorizó en menos tiempo de lo que puede medir la máquina y **gprime** le tomo 1.93 segundos. No fue posible factorizar números más grandes sin hacer que el sistema deje de funcionar.
Para mostrar como funciona el algoritmo RSA, se debe escoger un número **e** que sea primo relativo con **m**, esto se expresa pidiendo que **GCD[e,m] = 1**.
Primero se calculala factorización en primos de **m** con la función **FactorInteger**
FactorInteger[m]
{{2, 4}, {3, 5}, {79, 1}, {457, 1}, {30029, 1}}
y se buscan con la función **Prime** dos primos que no aparezcan en la factorización anterior. Por ejemplo los primos
a = Prime[5000]
48611
b = 11
11
no están en la descomposición de **m** por lo cual
e = a b
534721
cumple
GCD[e, m]
1
Ahora falta encontrar el número **d** de tal suerte que el residuo de dividir entre **n** el producto de **e** por **d** sea **1**, lo que ya se sabe calcular con la función **Solve** (como se hizó en ejemplos anteriores),
Solve[e x == 1 && Modulus == m, x]
{{Modulus -> 4215124605456, x -> 3212985964993}}

el resultado de esta función entrega el valor de **d,**
d = 3212985964993
3212985964993
se verifica que
Mod[e d, m]
1

¿Cómo se usan estos números para cifrar y descifrar?

Para cifrar con este método se escoge como clave pública a la pareja de números **(e, n)** y como clave privada a **(d, n)**.
Si el mensaje que se desea enviar es el número
msg = 123456
123456
El mensaje cifrado se calcula elevando a la potencia **e** el mensaje **módulo n** (la potencia se realiza multiplicando el mensaje por si mismo **e** veces **módulo n**), o sea:
cifrado = PowerMod[msg, e, n]
242434560201
El descifrado se calcula elevando el mensaje cifrado a la potencia **d módulo n**, o sea:
descifrado = PowerMod[cifrado, d, n]
123456
Es necesario aclarar que los números **p**, **q** y **m** se deben borrar después de haber calculado **n**, **e** y **d**. Esto con el objetivo de hacer difícil la factorización de **n** y el cálculo de **e** y **d**. Cuando se implementa este algoritmo para un criptosistema los números primos **p** y **q** se calculan de forma aleatoria y se verifica que cumplan un conjunto de pruebas que tienen por objetivo que se escojan únicamente primos fuertes. Esta forma de plantear el problema matemático garantiza que la única forma algorítmica de encontrar **p** y **q** es a través de la factorización de **n** lo cual es muy costoso para números realmente grandes y los algoritmos para cifrar y descifrar son relativamente económicos en comparación.
Este ejemplo muestra que es simple factorizar el número **n** que se está usando, eso quiere decir que el método se puede romper y todo depende únicamente del tamaño y de la calidad de los primos que se usen, la selección de los primos es de importancia vital.
Este resultado ha sido conocido durante los últimos 300 años y nadie ha sido capaz de resolver el problema con un algoritmo económico.

Referencias

- Niven, Ivan y Zuckerman, Herbert S., *Introducción a la teoría de Números.* Limusa.
- Fraleigh, John B., *Álgebra abstracta*, Addison-Wesley Iberoamericana.
- Herstein, I. N., *Álgebra moderna*, Trillas.
- Schneier, Bruce, *Criptografía aplicada*, John Wiley & Sons.
- Menezes, Alfred J. et. al., *Handbook of Applied Cryptography*, CRC Press (disponible de manera gratuita en http://www.cacr.math.uwaterloo.ca/hac/)
- Bressoud, David M., *Factorization and Primality Testing*, Springer-Verlag.
- Yan, Song Y., *Number Theory for Computing*, Springer-Verlag.
- Schneier, Bruce, et. al., *The Twofish Encryption Algoritm*, Wiley.
- Salomaa, Arto, *Public-Key Cryptography*, Springer-Verlag.
- Wolfram, Sthephen. The Mathematica book. Cambridge.

ANEXO 4

Dirección de Sistemas Operativos y de Pagos
Gerencia de Informática

Esquema de Contingencia para Servidores de la IES

Agosto 2003[3]

Resumen

Se presenta el esquema de contingencia empleado para los servidores de la IES y haciendo uso del servidor IES_RESP y del sistema IES_CLUSTER.

[3] Ultimo cambio: Marzo 2005

1. Introducción.

El servidor IES_RESP es el encargado de llevar a cabo los respaldos diarios de la IES. Este mismo equipo puede cumplir la función de cualquiera de las entidades de la IES en caso de contingencia, debido a que contiene sus bases de datos, elementos criptográficos y binarios de producción y puede ser usado en una situación extrema donde no se cuente con el sistema de alta disponibilidad e implica que se pueda perder información debido a la imposibilidad técnica de no poder tener sistemas espejos en otras ciudades sincronizados totalmente sin perder desempeño.

El sistema IES_CLUSTER es un cluster de alta disponibilidad para la ARC que está diseñado para no perder información siempre que el sistema esté utilizable.

En este documento se describen las actividades necesarias a seguir en caso de contingencia cuando el servidor IES_RESP deba tomar el lugar de cualquier otro servidor perteneciente a la IES. Adicionalmente se describen las acciones y los eventos que suceden cuando entra en funcionamiento el sistema IES_CLUSTER.

1.1. Limitantes.

Es necesario recalcar que existen limitaciones en este esquema de contingencia y que se busca que el sistema funcione de la mejor forma posible dentro de las restricciones que se tienen actualmente.

1. Debido a que no es posible realizar respaldos en línea debido al tipo de proceso que es necesario utilizar en la IES para mantener el registro y la consulta de certificados en línea, se deberá tener en cuenta que en un momento dado el servidor IES_RESP pudiera no contener toda la información de la ARC o AR que deba sustituir. Es necesario aclarar que este hecho no aplica para las ARAs.

2. Aunque el servidor de respaldo puede sustituir a cualquier equipo de la IES que falle, no se debe perder de vista que su rendimiento será menor (velocidad de procesamiento, de transferencia de datos, etc.), ya que es un equipo de menor capacidad.

3. El servidor de respaldo no entra en línea al momento que falla uno de los equipos de la IES, se debe seguir primeramente el procedimiento de configuración descrito en el presente manual.

5. Las pruebas indican que esta reconfiguración toma 20 minutos para la ARC, AR y ARA’s.

2. Acciones a tomar durante la contingencia.

Actualmente el servidor IES_RESP cuenta con los elementos suficientes para poder sustituir de forma *temporal* a cualquier equipo de la IES en caso de contingencia, de hecho tiene los binarios, datos y elementos criptográficos necesarios (certificados y claves privadas).

Sin embargo, se debe notar que al respecto de la IES únicamente tiene habilitado de forma permanente el servicio de Sybase, ya que los servidores de ARC, AR o ARA están deshabilitados para evitar fallas en el procedimiento de respaldo diario. Esto quiere decir

solamente que los programas de ARC, AR y ARA no se encuentran en ejecución, y se deberá proceder a activarlos cuando se necesite sustituir algún servidor de producción.

2.1. Configuración de IES_RESP.

Debido a lo anterior, el procedimiento para levantar en IES_RESP cualquier servicio de la IES se describe en la tabla siguiente.

Tabla 1. *Configuración del servidor IES_RESP en casos de contingencia*

Paso	Acción
1	Cambiar dirección IP de IES_RESP por la correspondiente del servidor de la IES a recuperar[4]
2	Modificar las iptables para que permitan acceder a los puertos del servidor de la IES a recuperar en IES_RESP.
3	Para el caso de una AR o ARA revisar los archivos de configuración[5] correspondientes en IES_RESP.
4	Activar el servicio requerido de la IES en IES_RESP, utilizando para esto la frase de seguridad original correspondiente.

2.2. Operación recomendada durante la contingencia.

Mientras que se esté operando en el servidor IES_RESP como ARC o AR, se recomienda no llevar a cabo ninguna operación de registro de certificados, ni revocación de certificados, esto con el propósito de evitar que las bases de datos se desfasen una vez que se recupere el equipo de producción, sin embargo se pueden llevar a cabo los procesos de registro y revocación.

3. Acciones a tomar después de la contingencia.

En cuanto se pueda recuperar el servidor original de la IES que presentó la falla, será necesario dar de baja el servicio correspondiente que se hubiera activado en IES_RESP, así como cambiar la dirección IP a su valor original. En caso de haberse registrado o revocado algún certificado en el servidor de contingencia, será necesario actualizar la base de datos correspondientes de producción previo a la activación del servicio de producción.

4. Uso del IES_CLUSTER.

Además del esquema de contingencia utilizando el equipo IES_RESP, la ARC cuenta con un sistema de cluster en modo de alta disponibilidad, que funciona utilizando dos servidores prácticamente idénticos, que acceden a un banco de discos común. De esta manera, si el servicio de la IES se llegara a detener en el nodo que está activo, o si llegara a suceder una falla física en dicho nodo, el sistema IES_CLUSTER levanta de manera automática el servicio en el otro nodo.

[4] Se debe contar con cables de red físicamente conectados a la subred correspondiente. Al momento de escribir este documento se cuenta con al menos un cable de red conectado a Red Financiera, otro a Red Interna y uno más a la DMZ.

[5] Los archivos de configuración son: interfaces, confARA, direcciones.txt, servidor_sybase.txt y usuario_sybase.txt.

Este proceso no requiere atención directa por parte del personal de la Gerencia de Informática de la D. S. O. P., sin embargo los pasos que se siguen son:

Tabla 2. *Uso del servidor IES_CLUSTER en casos de falla en la ARC*

Paso	Acción
1	Se deben mantener los dos nodos funcionando y se debe levantar parcialmente el servicio de la ARC en ambos, utilizando para ello la frase de seguridad correspondiente y las contraseñas del usuario de la base de datos.
2	En caso de una falla física de uno de los nodos, el sistema de cluster notifica al otro nodo que debe levantarse y da de baja el servicio de la ARC y Sybase en el nodo defectuoso. Esto tiene el efecto de desconectar todos los clientes de la ARC en ese momento.
3	El sistema de cluster le notifica al otro nodo que debe activarse y procede a arrancar el servicio del Sybase. Una vez hecho esto, se procede a levantar completamente el servicio de la ARC. Dado que la frase de seguridad ya se había proporcionado anteriormente, no se requiere volver a introducirla.
4	Se mandan notificaciones vía correo electrónico y al sistema SkyTel del personal de la Gerencia de Informática de los eventos ocurridos.
5	Se debe proceder a revisar el fallo en el nodo que se desactivó, corregirlo y dejar el nodo listo para el siguiente evento. Esto incluye volver a levantar parcialmente el servicio de la ARC.

Sólo en caso de que el sistema IES_CLUSTER fallara totalmente o se destruyera y no fuera posible levantar al menos uno de los nodos, se sustituiría la ARC con el equipo IES_RESP, utilizando el procedimiento descrito en el punto 2 de este manual.