CIRCULAR – TELEFAX 19/2002

Ciudad de México, D.F., a 5 de julio de 2002.

A LAS INSTITUCIONES
DE CRÉDITO DEL PAÍS:

ASUNTO: INFRAESTRUCTURA EXTENDIDA DE SEGURIDAD.

El Banco de México, con fundamento en lo previsto en los artículos 3º fracción I y 24 de su Ley, y considerando:

a) que con el desarrollo de las nuevas tecnologías de telecomunicaciones y transmisión de datos por vía electrónica, se ha generalizado en el sistema financiero el uso de los sistemas de intercambio electrónico de información y se han ampliado las posibilidades de ofrecer nuevos servicios financieros en línea con el fin de mejorar la productividad y reducir costos;

b) que el Instituto Central administra el sistema denominado "Infraestructura Extendida de Seguridad" (IES) cuya función principal es mantener el control sobre las claves públicas que se utilizan en la verificación de las firmas electrónicas, mediante la expedición y administración de certificados digitales, y

c) que la utilización de la firma electrónica a través de la IES permitirá dar mayor seguridad y confianza a las operaciones bancarias que se realicen a través de medios electrónicos en los sistemas de pagos, ya que hace posible atribuir al signatario cada mensaje de datos firmado y asegurar que dicho mensaje de datos no ha sido modificado,

ha resuelto autorizar a las instituciones de crédito interesadas, a emitir certificados digitales a sus clientes para celebrar operaciones con ellos y realizar los procesos de registro y distribución de tales certificados, a través de la IES.

Para tales efectos, a partir del día 9 de septiembre de 2002, este Instituto Central podrá expedir en su carácter de Agencia Registradora Central (ARC) de la IES, certificados digitales para actuar como Agencia Registradora (AR) y/o Agencia Certificadora (AC) de dicha Infraestructura, a las instituciones de crédito que lo soliciten por escrito mediante comunicación dirigida a la Dirección de Trámite Operativo del propio Banco de México, en términos del modelo que se adjunta como Anexo 1.

Adicionalmente, las instituciones interesadas deberán cumplir con los requisitos que se señalan en el Anexo 2 y, una vez que su solicitud haya sido aprobada, deberán suscribir el contrato respectivo con Banco de México a fin de estar en posibilidad de emitir y/o registrar certificados digitales a sus clientes para los efectos señalados, según corresponda.

El documento en el que se describen las características y funciones de los participantes de la IES, los manuales para su uso y el directorio para la atención de consultas, están a disposición de esas instituciones en 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, en el rubro "Infraestructura Extendida de Seguridad" de la sección "Otros Servicios".

Atentamente,

BANCO DE MÉXICO

DR. MANUEL GALÁN MEDINA
DIRECTOR DE SISTEMAS OPERATIVOS Y DE PAGOS

LIC. FERNANDO CORVERA CARAZA
DIRECTOR DE DISPOSICIONES DE BANCA CENTRAL

La presente Circular-Telefax consta de 11 páginas, incluyendo sus anexos. Para cualquier aclaración sobre su transmisión favor de comunicar a nuestra Oficina de Telecomunicaciones Intencionales a los Tels. 5237-2121 ó 5237-2142. Para cualquier consulta sobre su contenido, sírvanse acudir a la Gerencia de Autorizaciones, Consultas y Control de Legalidad, ubicada en Avenida 5 de Mayo número 1 (Anexo Guardiola), tercer piso, Colonia Centro, México, Distrito Federal, C.P. 06059, o a los teléfonos 5237-2308, 5237-2317.

LA PRESENTE CIRCULAR-TELEFAX SE EXPIDE CON FUNDAMENTO EN LOS ARTÍCULOS 8º, 12 Y 17 DEL REGLAMENTO INTERIOR DEL BANCO DE MÉXICO.

ANEXO 1

MODELO DE COMUNICACIÓN PARA SER ENVIADA POR LAS INSTITUCIONES DE CRÉDITO QUE SOLICITEN LA EXPEDICIÓN POR PARTE DEL BANCO DE MÉXICO DE CERTIFICADOS DIGITALES PARA PODER ACTUAR COMO AC Y/O AR

(MEMBRETE DE LA INSTITUCIÓN)

México, D.F., a ___ de _____de _____.

BANCO DE MÉXICO
Dirección de Trámite Operativo,
Av. 5 de mayo número 2, 3er. Piso,
Col. Centro.
06059 México, D.F.

En relación con la Circular-Telefax __/2002 del __ de ____ de 2002, (*nombre de la institución*) solicita a Banco de México la expedición del certificado digital para actuar como (*tipo de Agencia(s) cuya función pretende realizar*), a nombre de (*nombres de los apoderados de la institución para dicho propósito*) a fin de estar en posibilidad de actuar con tal carácter en la IES.

Al efecto, adjunto a la presente sometemos a la consideración de ese Instituto Central la documentación que acredita que (*nombre de la institución*) cumple con los requisitos establecidos en la Circular-Telefax mencionada para actuar como (*tipo de Agencia(s) cuya función pretende realizar*), así como la copia certificada de la escritura pública en la que consta el poder otorgado a las personas señaladas en el primer párrafo de la presente comunicación.

Asimismo, esta institución se obliga a proporcionar a Banco de México la información adicional que nos requiera en relación con las actividades mencionadas, así como permitir el acceso a nuestras instalaciones al personal autorizado por el Instituto Central a fin de que puedan corroborar el cumplimiento de los citados requisitos.

Atentamente,

(*Denominación de la institución*)
(*Nombres de los funcionarios facultados*)
(*Cargos*)

ANEXO 2

REQUISITOS PARA OPERAR COMO AGENCIA REGISTRADORA Y/O AGENCIA CERTIFICADORA DE LA INFRAESTRUCTURA EXTENDIDA DE SEGURIDAD

I. Definiciones

Para los efectos de este Anexo, en singular o plural se entenderá por:

Agencia Certificadora (AC)	A la institución de crédito autorizada por Banco de México para prestar servicios de certificación mediante la expedición de Certificados Digitales a través de la IES.
Agencia Registradora (AR)	A la institución de crédito autorizada por Banco de México para llevar el registro electrónico de los Certificados Digitales expedidos por las AC's.
Agencia Registradora Central (ARC)	A Banco de México en su carácter de administrador de la IES que, entre otras funciones, establece las normas de operación de dicha infraestructura, emite y registra los Certificados Digitales de AC's y AR's, y lleva el registro de las claves públicas.
Certificado Digital	Al Mensaje de Datos firmado electrónicamente que confirma el vínculo entre la identidad del Titular con los respectivos Datos de Verificación de Firma Electrónica.
Datos de Creación de Firma Electrónica	A la información única, como códigos o claves criptográficas privadas, que el Titular genera bajo su total control y utiliza personalmente para crear una Firma Electrónica.
Datos de Verificación de Firma Electrónica	A la información única, como códigos o claves criptográficas públicas, que se utiliza para comprobar una Firma Electrónica.
Dispositivo de Creación de Firma Electrónica	Al programa o hardware de computadora que sirve para aplicar los Datos de Creación de Firma Electrónica a un Mensaje de Datos y obtener la Firma Electrónica del referido Mensaje de Datos.

Dispositivo de Verificación de Firma Electrónica	Al programa o hardware de computadora que sirve para aplicar los Datos de Verificación de Firma Electrónica a la Firma Electrónica de un Mensaje de Datos y comprobar su autenticidad.
Firma Electrónica	Al conjunto de datos que se agrega o adjunta a un Mensaje de Datos, el cual está asociado en forma lógica a éste y es atribuible al Titular.
Infraestructura Extendida de Seguridad (IES)	Al sistema de seguridad diseñado y administrado por Banco de México cuyo propósito es fortalecer la seguridad de la información que se transmite en los sistemas de pagos y a su vez acreditar la identidad del remitente, mediante el uso de Firmas Electrónicas y Certificados Digitales.
Mensaje de Datos	A la información generada, enviada, recibida, archivada o comunicada a través de medios electrónicos.
Titular	A la persona que conoce los Datos de Creación de Firma Electrónica y los utiliza bajo su exclusivo control, los cuales están íntimamente relacionados con los Datos de Verificación de Firma Electrónica que aparecen en el Certificado Digital correspondiente.

II. Requisitos

Banco de México podrá autorizar a las instituciones de crédito que lo soliciten, para actuar en la IES como AR y/o AC, expidiendo a su favor en su carácter de ARC Certificados Digitales de AR y/o AC según corresponda.

Con el fin de que en dicha Infraestructura exista un grado adecuado de seguridad, calidad y confianza en la prestación de servicios de certificación de identidad de personas, así como de emisión y registro de Certificados Digitales, las instituciones que soliciten la referida autorización deberán demostrar previamente a Banco de México, con información que a su juicio resulte suficiente, la fiabilidad de los servicios que prestarán y comprobar que tienen la capacidad tecnológica y el personal calificado para realizar adecuadamente las actividades necesarias en el ámbito de la Firma Electrónica y de la IES en lo que resulte conducente.

Asimismo, las instituciones solicitantes deberán presentar las reglas y procedimientos a que se refieren los numerales 1 de los apartados III y IV, según corresponda al tipo de agencia que soliciten, así como asegurar que podrán cumplir con las demás obligaciones que se señalan en dichos apartados.

III. Obligaciones de la Agencia Certificadora.

1. Contar con reglas y procedimientos sobre prácticas de certificación de identidad que sean objetivas, precisas y no discriminatorias.
2. Emitir Certificados Digitales que cumplan al menos con los requisitos previstos en el apartado V de este Anexo, así como revocarlos inmediatamente después de tener conocimiento de cualquiera de los supuestos previstos en el numeral 3 de dicho apartado.
3. Requerir para la certificación de la identidad de los Titulares, la comparecencia personal y directa de la persona que solicite un Certificado Digital, así como la presentación de la credencial de elector, pasaporte vigente o cualquier otra identificación oficial fiable.
4. Hacer del conocimiento del solicitante sus derechos y obligaciones como Titular, conforme a lo señalado en el apartado VI de este Anexo.
5. Proporcionar al solicitante de un Certificado Digital, los medios necesarios para que genere sus Datos de Creación de Firma Electrónica y Datos de Verificación de Firma Electrónica, en forma secreta y bajo su total control. Además, poner a su disposición el Dispositivo de Creación de Firma Electrónica y el Dispositivo de Verificación de Firma Electrónica.
6. Obtener una declaración con firma autógrafa del Titular, en donde manifieste estar de acuerdo con las condiciones siguientes: i) ser responsable del uso de su Firma Electrónica, toda vez que cualquier Mensaje de Datos firmado que se pueda comprobar con sus Datos de Verificación de Firma Electrónica le será atribuible y producirá los mismos efectos que las leyes otorgan a los documentos suscritos con firma autógrafa y, en consecuencia, tendrán el mismo valor probatorio, y ii) aceptar las condiciones de operación y los límites de responsabilidad de la AC, AR y ARC.
7. Registrar ante una AR los Certificados Digitales que emita, así como informarle de la revocación de los mismos, para que exista constancia de los Certificados Digitales vigentes y revocados.
8. Conservar al menos durante 10 años los requerimientos que los interesados formulen a la AC para la emisión de Certificados Digitales. Dicha conservación deberá efectuarse de conformidad con la Norma Oficial Mexicana NOM-151-SCFI-2002, Prácticas comerciales-Requisitos que deben observarse para la conservación de mensajes de datos, publicada en el Diario Oficial de la Federación el 4 de junio de 2002.

9. Conservar copia de la información y documentación proporcionada por el Titular para su identificación, así como de la declaración a que se refiere el numeral 6 del presente Apartado, por un plazo de al menos 10 años contados a partir de la emisión del correspondiente Certificado Digital, así como no utilizar dicha información y documentación para fines diferentes a los relacionados con la IES.
10. Publicar en su página en la red mundial (Internet) las disposiciones que emita Banco de México en relación con la Firma Electrónica y la IES, así como las reglas y procedimientos previstos en el numeral 1 de este apartado III.
11. Proporcionar a Banco de México la información que éste le requiera en relación con sus actividades de certificación y permitir el acceso a sus instalaciones a las personas autorizadas por el propio Banco de México, a fin de que puedan corroborar el cumplimiento de los requisitos previstos en el presente Anexo.
12. Responder por los daños y perjuicios que, con motivo de la realización de sus actividades, ocasione por negligencia en el proceso de identificación del Titular, la emisión o revocación de Certificados Digitales. En todo caso, corresponderá a la AC demostrar que actuó con el debido cuidado.
13. Solicitar a la Dirección de Trámite Operativo de Banco de México con una antelación no menor a 60 días naturales, la revocación de la autorización que éste le haya otorgado, cuando pretenda dejar de prestar servicios como AC. En dicha solicitud deberá comunicar el nombre de la AC a quién vaya a transferir la información y documentación referida en los numerales 8 y 9 de este apartado, proporcionada por los Titulares cuyos Certificados Digitales haya emitido. Asimismo, a más tardar el tercer día hábil bancario siguiente a la presentación de su referida solicitud, deberá hacer del conocimiento de dichos Titulares su intención de dejar de actuar como AC y el destino que pretende dar a los datos de identificación que recibió de ellos.
14. Informar a los Titulares de la revocación de su Certificado Digital en la fecha en que ésta se lleve a cabo, cuando dicha revocación se deba a cualquiera de los últimos tres supuestos previstos en el numeral 3.2 del apartado V de este Anexo.
15. Contar con al menos un respaldo de la información referida en los incisos 8 y 9.

IV. Obligaciones de la Agencia Registradora.

1. Contar con reglas y procedimientos de operación que sean objetivos, precisos y aseguren que los sistemas, las bases de datos y los equipos de cómputo estarán protegidos contra accesos y modificaciones no autorizados, revelaciones indebidas y/o pérdidas de información.
2. Mantener un registro público de Certificados Digitales, en el que quede constancia de la fecha y hora de su emisión, período de vigencia y, en su caso, fecha y hora de revocación. Conservar

en línea los datos de los Certificados Digitales por lo menos durante 10 años desde su emisión, de conformidad con la Norma Oficial Mexicana NOM-151-SCFI-2002, Prácticas comerciales-Requisitos que deben observarse para la conservación de mensajes de datos, publicada en el Diario Oficial de la Federación el 4 de junio de 2002.

3. Permitir la realización de consultas en línea por medios electrónicos al registro público de Certificados Digitales que administre.
4. No ofrecer servicios que permitan hacer una búsqueda sistemática de Certificados Digitales en el registro público mencionado en el numeral inmediato anterior.
5. Publicar en su página en la red mundial (Internet) las disposiciones de Banco de México en relación con la Firma Electrónica y la IES, así como las generalidades de las reglas y procedimientos previstos en el numeral 1 de este apartado IV.
6. Proporcionar a Banco de México la información que éste le requiera en relación con sus actividades de registro y permitir el acceso a sus instalaciones a las personas autorizadas por Banco de México, a fin de que puedan corroborar el cumplimiento de los requisitos previstos en el presente Anexo, incluyendo la revisión de la seguridad física y lógica de su infraestructura de cómputo.
7. Responder por los daños y perjuicios que, con motivo de la realización de sus actividades, ocasionen por negligencia en el proceso de registro o revocación de Certificados Digitales. En todo caso, corresponderá a la AR demostrar que se actuó con el debido cuidado.
8. Solicitar a la Dirección de Trámite Operativo de Banco de México la revocación de la autorización que éste le haya otorgado, con una antelación no menor a 60 días naturales a la fecha en que pretenda dejar de prestar el servicio de AR.

   Dentro de los 3 días hábiles siguientes a la presentación de la mencionada solicitud, deberá notificar a los Titulares cuyos Certificados Digitales administra, su intención de dejar de actuar como AR, así como la fecha en que revocará tales Certificados Digitales. La fecha de dichas revocaciones no podrá ser inferior a 15 ni superior a 20 días hábiles contados a partir de la fecha en que haya hecho la notificación a los aludidos Titulares.

   Adicionalmente, deberá transmitir a Banco de México la base de datos de los Certificados Digitales que administra en la forma y términos que éste le indique, dentro de los 3 días hábiles siguientes a la fecha en que haya revocado el último Certificado Digital. Asimismo, deberá proporcionar a Banco de México la demás información que éste le requiera.
9. Contar con al menos un respaldo electrónico de la base de datos de los Certificados Digitales que administra.

V. Características de los Certificados Digitales.

1. El formato del Certificado Digital deberá apegarse a la especificación ITU-T X.509v3.

2. Los Certificados Digitales tendrán al menos el contenido siguiente:

   2.1 La indicación de que se trata de un Certificado Digital.

   2.2 Un código de identificación único del Certificado Digital, de 21 dígitos, organizados de izquierda a derecha de la manera siguiente:

      2.2.1 Primeros 6 dígitos (posiciones de la 1 a la 6), para identificar a la AR que tiene almacenado el Certificado Digital. Este número es asignado por la ARC.

      2.2.2 Segundos 6 dígitos (posiciones de la 7 a la 12), para identificar a la AC que expidió el Certificado Digital. Este número es asignado por la ARC.

      2.2.3 Últimos 9 dígitos (posiciones de la 13 a la 21), número consecutivo del Certificado Digital emitido por la AC que corresponda.

   2.3 Identificación de la AC que emite el Certificado Digital, con indicación de su nombre o razón social, domicilio y dirección de correo electrónico, así como su Firma Electrónica.

   2.4 Datos de identificación del Titular, entre los cuales deben necesariamente incluirse nombre, domicilio, dirección de correo electrónico y los Datos de Verificación de Firma Electrónica.

   2.5 La fecha y hora del inicio y fin del periodo de validez del Certificado Digital.

3. Los Certificados Digitales quedarán sin efecto en los casos siguientes:

   3.1 Por extinción del periodo de validez del propio Certificado Digital, el cual no podrá exceder de tres años contados desde la fecha de su emisión.

   3.2 Por revocación en las circunstancias siguientes:

      3.2.1 A solicitud del Titular;

      3.2.2 Por fallecimiento del Titular;

      3.2.3 Por resolución judicial;

      3.2.4 Por incumplimiento del Titular de sus obligaciones en relación con la IES, previa comunicación que le formule la AC en la que especifique la causa, fecha y hora en que se efectuará la revocación, o

      3.2.5 Al comprobar la ARC, la AC o la AR, que los Datos de Creación de Firma Electrónica del Titular se han duplicado o por cualquier razón se encuentre comprometida su integridad o confidencialidad.

   3.3 Por revocación de la autorización otorgada por Banco de México a la AR o cuando por cualquier otra causa deje de prestar el servicio de AR, o bien el servicio de banca y crédito.

VI. Derechos y obligaciones de los Titulares.

1. El Titular tendrá los derechos siguientes:

   1.1 Ser informado por la AC al menos de:

      1.1.1 Las reglas sobre las prácticas de certificación, los procedimientos que se seguirán en la prestación del servicio y los elementos técnicos que se utilizarán para brindar seguridad y confidencialidad a la información que proporcione para acreditar su identificación;

      1.1.2 Las tarifas de los servicios de certificación;

      1.1.3 Los procedimientos para la utilización del Certificado Digital y sus limitaciones de uso;

      1.1.4 Las características generales de los procedimientos de creación y verificación de Firmas Electrónicas;

      1.1.5 Los procedimientos para dirimir controversias, así como la ley aplicable y los tribunales competentes;

      1.1.6 Los medios que puede utilizar para solicitar aclaraciones, dar cuenta del mal funcionamiento del sistema o presentar reclamaciones;

      1.1.7 Los límites de las responsabilidades de la AC, AR y ARC, y

      1.1.8 La revocación de su Certificado Digital y la causa de dicha revocación.

   1.2 Ser informado por la AR de la revocación de su Certificado Digital en el supuesto previsto en el numeral 8 del apartado IV anterior.

   1.3 Estar en posibilidad de generar en secreto y en forma individual sus Datos de Creación de Firma Electrónica y sus Datos de Verificación de Firma Electrónica.

   1.4 Mantener en secreto sus Datos de Creación de Firma Electrónica.

   1.5 Tener acceso a un servicio que le permita revocar su Certificado Digital en cualquier momento.

   1.6 Tener acceso a un servicio en línea, que en todo momento le permita verificar el estado de cualquier Certificado Digital que le interese.

2. El Titular tendrá las obligaciones siguientes:

   2.1 Hacer declaraciones veraces y completas en relación con los datos que proporcione para su identificación personal o con otros datos que sean objeto de certificación.

   2.2 Dar aviso a la AC de cualquier modificación de los datos a que se refiere el numeral anterior, inmediatamente después de que éstos cambien.

2.3 Custodiar adecuadamente sus Datos de Creación de Firma Electrónica a fin de mantenerlos en secreto.

2.4 Solicitar inmediatamente a la AC la revocación de su Certificado Digital en caso de que la integridad y/o confidencialidad de sus Datos de Creación de Firma Electrónica, hayan sido comprometidas.

VII. Límites de responsabilidad de la ARC.

La ARC no responderá por los daños y/o perjuicios que se causen, directa o indirectamente, por la utilización que se realice o pretenda realizarse de la IES, incluyendo los que se causen con motivo de la emisión y registro de Certificados Digitales**.**