

CIRCULAR-TELEFAX 6/2005 Bis

México, D.F., a 23 de diciembre de 2005.

**A LAS INSTITUCIONES
DE CRÉDITO DEL PAÍS:**

**ASUNTO: INFRAESTRUCTURA EXTENDIDA DE SEGURIDAD
(IES).**

El Banco de México, con fundamento en lo previsto en los artículos 3º, fracción I, y 24 de su Ley, y considerando que se ha generalizado el uso de medios electrónicos de comunicación en la conducción de operaciones financieras que se realizan en los sistemas de pagos, así como en el intercambio de información en el sistema financiero, ha resuelto permitir a las instituciones y empresas que actúen con el carácter de Agencia Certificadora en la IES, emitir Certificados Digitales a favor de personas físicas responsables de la operación de páginas web seguras y/o de equipos para establecer enlaces virtuales seguros, designadas para tal efecto por instituciones de crédito, otras instituciones financieras, empresas que presten servicios auxiliares o complementarios relacionados con transferencias de fondos o valores a dichas instituciones, o autoridades financieras. Lo anterior, siempre y cuando tales páginas web seguras y/o equipos para establecer enlaces virtuales seguros, sean utilizados en la conducción de operaciones financieras que se realicen a través de medios electrónicos en los sistemas de pagos, o bien para el intercambio de información relacionada con las actividades propias de su objeto o con el cumplimiento de sus atribuciones, según corresponda.

Para tales efectos, a partir del 27 de diciembre de 2005 se modifican los numerales 2. del Anexo 3 y 2.4 del Anexo 4; así como, el primer y cuarto párrafos del Anexo 5 y se adicionan un sexto párrafo al apartado II y el Anexo 6, todos de la Circular-Telefax 6/2005, para quedar como sigue:

“REGLAS PARA OPERAR COMO AGENCIA REGISTRADORA Y/O AGENCIA CERTIFICADORA EN LA INFRAESTRUCTURA EXTENDIDA DE SEGURIDAD

...

II. Requisitos.

...

Las instituciones y empresas que, de conformidad con lo previsto en los párrafos que anteceden, obtengan un Certificado Digital para actuar con el carácter de AC en la IES, podrán emitir Certificados Digitales a personas físicas con el propósito de que sean utilizados dentro del sistema financiero. Asimismo, podrán emitir Certificados Digitales a personas físicas responsables de la operación de páginas web seguras y/o de equipos para establecer enlaces virtuales seguros, que sean designadas para tal efecto por instituciones de crédito, otras instituciones financieras, empresas que presten servicios auxiliares o complementarios relacionados con transferencias de fondos o valores a dichas instituciones, o autoridades financieras; lo anterior, siempre y cuando, dichos Certificados Digitales sean utilizados para la operación de páginas web seguras en la conducción de operaciones financieras que se realicen a través de medios electrónicos en los sistemas de pagos y/o en la operación de equipos para establecer enlaces virtuales seguros para el intercambio de información relacionada con las actividades propias de su objeto o con el cumplimiento de sus atribuciones, según corresponda.”

“ANEXO 3

CARACTERÍSTICAS DE LOS REQUERIMIENTOS DE LOS CERTIFICADOS DIGITALES

...

Los requerimientos de los Certificados Digitales tendrán al menos el contenido siguiente:

...

2. El nombre distinguido que identifica al Titular del requerimiento conteniendo, al menos, los campos siguientes:

- Nombre del Titular, en el campo commonName (OID¹³ 2.5.4.3). Tratándose de requerimientos de Certificados Digitales emitidos a personas físicas para la operación de páginas web seguras y/o de equipos para establecer enlaces virtuales seguros, los datos de identificación de la página web segura o del equipo para establecer enlaces virtuales seguros de que se trate, deberán incluirse en el referido campo commonName (OID 2.5.4.3), y el nombre de la persona física responsable del certificado, así como la denominación o razón social de la institución, empresa o autoridad financiera que la haya designado, deberán incluirse en el campo unstructuredName (OID 1.2.840.113549.1.9.2).

...”

“ANEXO 4

CARACTERÍSTICAS DE LOS CERTIFICADOS DIGITALES

...

2. Los Certificados Digitales deberán contar, al menos, con el contenido siguiente:

...

- 2.4 Datos de identificación del Titular, entre los cuales deben necesariamente incluirse el nombre y los Datos de Verificación de Firma Electrónica. Tratándose de Certificados Digitales emitidos a personas físicas para la operación de páginas web seguras y/o de equipos para establecer enlaces virtuales seguros, dichos Certificados deberán contener los datos de identificación de la página web segura o del equipo para establecer enlaces virtuales seguros de que se trate, el nombre de la persona física responsable del certificado, así como la denominación o razón social de la institución, empresa o autoridad financiera que la haya designado.

...”

¹³ OID Object Identifier – Identificador de Objeto por sus siglas en inglés. La definición formal se encuentra en la recomendación X.208 (ASN.1) de la ITU- T, disponible en la página de la red mundial (Internet) que se identifica con el nombre de dominio <http://www.itu.ch>.

“ANEXO 5

MODELO DE CARTA DE ACEPTACIÓN EN LA QUE DEBERÁ CONSTAR LA FIRMA AUTÓGRAFA DEL TITULAR DE UN CERTIFICADO DIGITAL

El suscrito (Usuario), para todos los efectos legales a que haya lugar, manifiesta haber solicitado a (Denominación o razón social de la institución o empresa) en su carácter de Agencia Certificadora, la emisión de un Certificado Digital en el que consten los Datos de Verificación de Firma Electrónica (clave pública) asociados a los Datos de Creación de Firma Electrónica (clave privada) y frase de seguridad, que generó previamente en absoluto secreto. Asimismo, afirma haber manifestado su conformidad en que la Agencia Certificadora utilizara el procedimiento descrito en sus reglas de operación. De igual forma, el Usuario reconoce y acepta que dicho Certificado se expide con el propósito de ser utilizado dentro del sistema financiero.

...

Adicionalmente, el Usuario reconoce y acepta que el uso de la clave privada y frase de seguridad con base en las cuales dicho Certificado Digital fue elaborado, quedarán bajo su exclusiva responsabilidad, y que los documentos electrónicos que tengan asociada una firma electrónica generada con las referidas clave privada y frase de seguridad, que pueda ser verificada con la clave pública que aparece en el Certificado Digital impreso en este documento, le serán atribuibles, por lo que asume la responsabilidad de su información y contenido. Por lo anterior, se obliga a mantener absoluta confidencialidad respecto de las aludidas clave privada y frase de seguridad, así como a realizar los trámites necesarios para solicitar la revocación de dicho Certificado Digital ante la Agencia Certificadora, mediante los mecanismos y en los horarios que la misma establezca, en el evento de que por cualquier causa dicha información haya sido divulgada y, por tanto, la integridad y/o confidencialidad de dicha información haya sido comprometida.

...”

“ANEXO 6

MODELO DE CARTA DE ACEPTACIÓN EN LA QUE DEBERÁ CONSTAR LA FIRMA AUTÓGRAFA DEL TITULAR DE UN CERTIFICADO DIGITAL EMITIDO PARA LA OPERACIÓN DE PÁGINAS WEB SEGURAS Y/O DE EQUIPOS PARA ESTABLECER ENLACES VIRTUALES SEGUROS

México, D. F., a ____ de _____ de _____.

El suscrito (Usuario), para todos los efectos legales a que haya lugar, manifiesta haber solicitado a (Denominación o razón social de la institución o empresa) en su carácter de Agencia Certificadora, la emisión de un Certificado Digital en el que consten los Datos de Verificación de Firma Electrónica (clave pública), asociados a los Datos de Creación de Firma Electrónica (clave privada) y frase de seguridad que generó previamente en absoluto secreto, con el objeto de utilizar dicho Certificado para la operación de páginas web seguras en la conducción de operaciones financieras que se realicen a través de medios electrónicos en los sistemas de pagos y/o en la operación de equipos para establecer enlaces virtuales seguros para el intercambio de información relacionada con las actividades o atribuciones propias de la institución, empresa o autoridad financiera que lo ha designado. Asimismo, afirma haber manifestado su conformidad en que la Agencia Certificadora utilizara el procedimiento descrito en sus reglas de operación.

El Usuario reconoce que para la emisión del referido Certificado Digital, la Agencia Certificadora únicamente revisó la identificación oficial con fotografía, mediante la cual el propio Usuario se identificó, constatando a simple vista que dicho documento corresponde con sus rasgos fisonómicos y caligráficos, por lo que el Usuario asume responsabilidad exclusiva respecto de la autenticidad de tal documento, así como, de la veracidad de los demás datos que haya proporcionado a la Agencia Certificadora en el proceso de su identificación.

El Usuario en este acto acepta el Certificado Digital cuya clave pública consta al final del presente documento, sirviendo éste último como el recibo más amplio que en derecho proceda.

Adicionalmente, el Usuario reconoce y acepta que el uso de la clave privada y frase de seguridad con base en las cuales dicho Certificado Digital fue elaborado, quedarán bajo su exclusiva responsabilidad, por lo que se obliga a mantener absoluta confidencialidad respecto de las mismas; y a realizar los trámites necesarios para solicitar la revocación del Certificado Digital ante la Agencia Certificadora, mediante los mecanismos y en los horarios que la misma establezca, en el evento de que por cualquier causa dicha confidencialidad haya sido comprometida, así como, cuando tenga conocimiento de que el Certificado ha sido utilizado para fines distintos a la conducción de

operaciones financieras que se realicen a través de medios electrónicos en los sistemas de pagos o para el intercambio de información relacionada con las actividades o atribuciones propias de la institución, empresa o autoridad financiera que lo ha designado.

Por otra parte, el Usuario reconoce y acepta que la Agencia Certificadora y la Agencia Registradora únicamente serán responsables por los daños y perjuicios que le llegaren a causar, derivados de errores que, en su caso, cometan por negligencia en el proceso de generación, registro, entrega y revocación del Certificado Digital, así como, que no serán responsables por los daños y perjuicios que se pudieran causar al Usuario o a terceros, cuando por caso fortuito o fuerza mayor no puedan realizarse registros, verificaciones o cualquier otro trámite con las claves públicas y privadas relacionadas con dicho Certificado Digital.

De la misma forma, el Usuario reconoce y acepta que Banco de México, en su carácter de Agencia Registradora Central, 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, registro y revocación de Certificados Digitales.

Datos del Certificado:

Datos de la AC:

Datos de la página web segura y/o del equipo para establecer enlaces virtuales seguros:

Datos del Usuario:

Datos de la institución, empresa o autoridad financiera designante:

Clave Pública del Usuario:

Firma Electrónica de la AC:

(Nombre y firma autógrafa del Titular del Certificado Digital)

A t e n t a m e n t e,

LA PRESENTE CIRCULAR-TELEFAX SE EXPIDE CON FUNDAMENTO EN LOS ARTÍCULOS 8°, 10, 17 y 20 DEL REGLAMENTO INTERIOR DEL BANCO DE MÉXICO.