Iniciativa con proyecto de decreto por el que se reforman y adicionan diversas disposiciones del Código de Comercio, en materia de firma electrónica.

Título Segundo del Comercio Electrónico

Capítulo I. De los Mensajes de Datos ➦

Artículo 89.

- Las disposiciones de este Título regirán en toda la República Mexicana en asuntos del orden comercial, sin perjuicio de lo dispuesto en los tratados internacionales de los que México sea parte.

Las actividades reguladas por este Título se someterán en su interpretación y aplicación a los principios de neutralidad tecnológica, autonomía de la voluntad, compatibilidad internacional y equivalencia funcional del mensaje de datos en relación con la información documentada en medios no electrónicos y de la firma electrónica en relación con la firma autógrafa.

En los actos de comercio y en la formación de los mismos, podrán emplearse los medios electrónicos, ópticos o cualquier otra tecnología. Para efecto del presente Código, se deberán tomar en cuenta las siguientes definiciones:

Certificado: Por certificado se entenderá todo mensaje de datos u otro registro que confirme el vínculo entre un firmante y los datos de creación de firma electrónica.

Datos de creación de firma: Los datos de creación de la firma son los datos únicos, como códigos o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica.

Destinatario: Por destinatario se entenderá la persona designada por el emisor para recibir el mensaje de datos, pero que no esté actuando a título de intermediario con respecto a dicho mensaje.

Emisor o iniciador: Por emisor se entenderá a toda persona que, al tenor del mensaje de datos, haya actuado a nombre propio o en cuyo nombre se haya enviado o generado ese mensaje antes de ser archivado, si éste es el caso, pero que no haya actuado a título de intermediario.

Firma electrónica: Por firma electrónica se entenderán los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo por cualquier tecnología, que son utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información contenida en el mensaje de datos, y que produce los mismos efectos jurídicos que la firma autógrafa.

Firma electrónica avanzada o fiable: Se considerará firma electrónica avanzada o fiable, aquella firma electrónica que cumpla con los requisitos contemplados en las fracciones I a IV del artículo 97.

En aquellas disposiciones que se refieran a firma digital, se considerará a ésta como una especie de la firma electrónica.

Firmante: Por firmante se entenderá a la persona que posee los datos de la creación de la firma y que actúa en nombre propio o de la persona a la que representa.

Intermediario: Por intermediario, en relación con un determinado mensaje de datos, se entenderá toda persona que, actuando por cuenta de otra, envíe, reciba o archive dicho mensaje o preste algún otro servicio con respecto a él.

Mensaje de datos: Por mensaje de datos se entenderá la información generada, enviada, recibida, archivada o comunicada por medios electrónicos, ópticos o cualquier otra tecnología.

Parte que confía: Por parte que confía se entenderá a la persona que, siendo o no el destinatario, actúa sobre la base de un certificado o de una firma electrónica.

Prestador de servicios de certificación: Por prestador de servicios de certificación, se entenderá a la persona o institución pública que preste servicios relacionados con firmas electrónicas y que expide los certificados, en su caso.

Secretaría: Por Secretaría, se entenderá la Secretaría de Economía.

Sistema de información: Por sistema de información, se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos.

Titular del certificado: Por titular del certificado, se entenderá a la persona que utiliza bajo su exclusivo control un certificado de firma electrónica

Artículo 89 bis.

- No se negarán efectos jurídicos, validez o fuerza obligatoria a cualquier tipo de información por la sola razón de que esté contenida en un mensaje de datos.

Artículo 90.

- Se presumirá que un mensaje de datos proviene del emisor, si ha sido enviado:

I. Por el propio emisor

II. Usando medios de identificación, tales como claves o contraseñas del emisor o por alguna persona facultada para actuar en nombre del emisor respecto a ese mensaje de

datos; o

III. Por un sistema de información programado por el emisor o en su nombre para que opere automáticamente.

Artículo 90 bis.

- Se presume que un mensaje de datos ha sido enviado por el emisor y por lo tanto, el destinatario o la parte que confía, en su caso, podrá actuar en consecuencia, cuando:

I. Haya aplicado en forma adecuada el procedimiento acordado previamente con el emisor, con el fin de establecer que el mensaje de datos provenía efectivamente de éste; o

II. El mensaje de datos que reciba el destinatario o la parte que confía, resulte de los actos de un intermediario que le haya dado acceso a algún método utilizado por el emisor para identificar un mensaje de datos como propio.

Lo dispuesto en el presente artículo no se aplicará:

I. A partir del momento en que el destinatario o la parte que confía, haya sido informado por el emisor, de que el mensaje de datos no provenía de éste, y haya dispuesto de un plazo razonable para actuar en consecuencia; o

II. A partir del momento en que el destinatario o la parte que confía, tenga conocimiento, o debiere tenerlo, de haber actuado con la debida diligencia o aplicado algún método convenido, que el mensaje de datos no provenía del emisor.

Salvo prueba en contrario y sin perjuicio del uso de cualquier otro método de verificación de la identidad del emisor, se presumirá que se actuó con la debida diligencia si el método que usó el destinatario o la parte que confía, cumple con los requisitos establecidos en éste Código para la verificación de la fiabilidad de las firmas electrónicas.

Artículo 91.

- Salvo pacto en contrario entre el emisor y el destinatario, el momento de recepción de un mensaje de datos se determinará como sigue:

I. Si el destinatario ha designado un sistema de información para la recepción de mensajes de datos, ésta tendrá lugar en el momento en que ingrese en dicho sistema de información; o

II. De enviarse el mensaje de datos a un sistema de información del destinatario que no sea el Sistema de Información designado, o de no haber un sistema de información designado, en el momento en el que el destinatario recupere el mensaje de datos; y

III. Si el destinatario no ha designado un sistema de información, la recepción tendrá lugar cuando el mensaje de datos ingrese a un sistema de información del destinatario.

Lo dispuesto en este artículo será aplicable aun cuando el sistema de información esté ubicado en un lugar distinto de donde se tenga por recibido el mensaje de datos conforme al artículo 94.

Artículo 91 bis.

- Salvo pacto en contrario entre el emisor y el destinatario, el mensaje de datos se tendrá por expedido cuando ingrese en un sistema de información que no esté bajo el control del emisor.

Artículo 92.

En lo referente a acuse de recibo de mensajes de datos, se estará a lo siguiente:

I. Si al enviar o antes de enviar un mensaje de datos, el emisor solicita o acuerda con el destinatario que se acuse recibo del mensaje de datos, pero no se ha acordado entre éstos una forma o método determinado para efectuarlo, se podrá acusar recibo mediante:

1. Toda comunicación del destinatario, automatizada o no; o

2. Todo acto del destinatario, que baste para indicar al emisor que se ha recibido el mensaje de datos.

II. Cuando el emisor haya indicado que los efectos del mensaje de datos estarán condicionados a la recepción de un acuse de recibo, se considerará que el mensaje de datos no ha sido enviado en tanto que no se haya recibido el acuse de recibo en el plazo fijado por el emisor o dentro de las cuarenta y ocho horas a partir del momento del envío del mensaje de datos.

III. Cuando el emisor haya solicitado o acordado con el destinatario que se acuse recibo del mensaje de datos, excepto que:

i) El emisor no indicó expresamente que los efectos del mensaje de datos están condicionados a la recepción del acuse de recibo, y;

ii) No ha recibido el acuse de recibo en el plazo solicitado o acordado, o en su defecto, dentro de las cuarenta y ocho horas siguientes a su envío, entonces el emisor podrá dar aviso al destinatario de que no ha recibido el acuse de recibo solicitado o acordado y fijar un nuevo plazo razonable para su recepción, contado a partir del momento de este aviso. Si aún así no se recibe el acuse de recibo dentro del nuevo plazo señalado, el emisor podrá considerar que el mensaje de datos no fue enviado, o ejercer cualquier otro derecho que pueda tener, dando aviso de ello al destinatario.

IV. Cuando el emisor reciba acuse de recibo del destinatario, se presumirá que éste ha recibido el mensaje de datos correspondiente.

V. Cuando en el acuse de recibo se indique que el mensaje de datos recibido cumple con los requisitos técnicos convenidos o establecidos en Ley, se presumirá que ello es así.

Artículo 93.

- Cuando la ley exija la forma escrita para los actos, convenios o contratos, este supuesto se tendrá por cumplido tratándose de mensaje de datos, siempre que la información en él contenida se mantenga íntegra y sea accesible para su ulterior consulta, sin importar el formato en el que se encuentre o represente.

Cuando la Ley disponga alguna formalidad diferente a la forma escrita, la misma también

deberá cumplirse respecto al mensaje de datos.

En los casos en que la ley establezca como requisito que un acto jurídico deba otorgarse en instrumento ante fedatario público, éste y las partes obligadas podrán, a través de mensajes de datos, expresar los términos exactos en que las partes han decidido obligarse, en cuyo caso el fedatario público, deberá hacer constar en el propio instrumento los elementos a través de los cuales se atribuyen dichos mensajes a las partes y conservar bajo su resguardo una versión íntegra de los mismos para su ulterior consulta, otorgando dicho instrumento de conformidad con la legislación aplicable que lo rige

Artículo 93 bis.

- Sin perjuicio de lo dispuesto en el artículo 49 de este Código, cuando la Ley requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho respecto a un mensaje de datos:

I. Si existe garantía confiable de que se ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos o en alguna otra forma; y

II. De requerirse que la información sea presentada, si dicha información puede ser mostrada a la persona a la que se deba presentar.

Para efectos de este artículo, se considerará que el contenido de un mensaje de datos es íntegro, si éste ha permanecido completo e inalterado independientemente de los cambios que hubiere podido sufrir el medio que lo contiene, resultado del proceso de comunicación, archivo o presentación. El grado de confiabilidad requerido será determinado conforme a los fines para los que se generó la información y de todas las circunstancias relevantes del caso.

Artículo 94.

- Salvo pacto en contrario entre el emisor y el destinatario, el mensaje de datos se tendrá por expedido en el lugar donde el emisor tenga su establecimiento y por recibido en el lugar donde el destinatario tenga el suyo. Para los fines del presente artículo:

I. Si el emisor o el destinatario tienen más de un establecimiento, su establecimiento será el que guarde una relación más estrecha con la operación subyacente o, de no haber una operación subyacente, su establecimiento principal;

II. Si el emisor o el destinatario no tienen establecimiento, se tendrá en cuenta su lugar de residencia habitual.

Artículo 95.

- Conforme al artículo 90, siempre que se entienda que el mensaje de datos proviene del emisor, o que el destinatario tenga derecho a actuar con arreglo a este supuesto, dicho destinatario tendrá derecho a considerar que el mensaje de datos recibido corresponde al que quería enviar el iniciador, y podrá proceder en consecuencia. El destinatario no gozará de este derecho si sabía o hubiera sabido, de haber actuado con la debida diligencia, o de haber aplicado algún método previamente acordado, que la transmisión había dado lugar a un error en el mensaje de datos recibido.

Se presume que cada mensaje de datos recibido es un mensaje de datos diferente, salvo que el destinatario sepa, o debiera saber, de haber actuado con la debida diligencia, o de haber aplicado algún método previamente acordado, que el nuevo mensaje de datos era un duplicado.

Capítulo II. De las Firmas ➦

Artículo 96.

Las disposiciones del presente Código serán aplicadas de modo que no excluyan, restrinjan o priven de efecto jurídico cualquier método para crear una firma electrónica.

Artículo 97.

Cuando la Ley requiera o las partes acuerden la existencia de una firma en relación con un mensaje de datos, se entenderá satisfecho dicho requerimiento si se utiliza una firma electrónica que resulte apropiada para los fines para los cuales se generó o comunicó ese mensaje de datos.

Salvo pacto en contrario, la firma electrónica se considerará fiable o avanzada, si:

I. Los datos de creación de la firma, en el contexto en que son utilizados, corresponden exclusivamente al firmante;

II. Los datos de creación de la firma estaban, en el momento de la firma, bajo el control exclusivo del firmante;

III. Es posible detectar cualquier alteración de la firma electrónica hecha después del momento de la firma;

IV. Respecto a la integridad de la información de un mensaje de datos es posible detectar cualquier alteración de ésta hecha después del momento de la firma; y

Lo dispuesto en el presente artículo, se entenderá sin perjuicio de la posibilidad de que cualquier persona demuestre de cualquier otra manera, la fiabilidad de una firma electrónica; o presente pruebas de que una firma electrónica no es fiable.

Artículo 98.

Los prestadores de servicios de certificación, determinarán y harán del conocimiento de los usuarios, en qué grado las firmas electrónicas, fiables o avanzadas, que les ofrecen, cumplen con los requerimientos dispuestos en las fracciones I a IV del artículo 97.

La determinación que se haga, con arreglo al párrafo anterior, deberá ser compatible con las normas y criterios internacionales reconocidos.

Lo dispuesto en el presente artículo se entenderá sin perjuicio de la aplicación de las normas del derecho internacional privado.

Artículo 99.

El firmante deberá:

I. Actuar con diligencia y establecer los medios razonables para evitar la utilización no autorizada de los datos de creación de la firma.

II. En caso de que tenga conocimiento de error o violación de los datos de creación de la firma, o la posibilidad de ello, dar aviso sin dilación indebida, al prestador de servicios de certificación y a cualquier persona que pudiera considerar fiable la firma electrónica, así como la terminación de la vigencia del certificado en su caso.

III. Cuando se emplee un certificado para refrendar la firma electrónica, actuar con diligencia razonable para cerciorarse de que todas las declaraciones que haya hecho en relación con él, con la vigencia del certificado, o que hayan de consignarse en él son exactas.

Capítulo III. De los Prestadores de Servicios de Certificación ➦

Artículo 100.

- Podrán ser prestadores de servicios de certificación, previa acreditación ante la Secretaría:

I. Los notarios públicos, así como los corredores públicos;

II. Personas físicas o morales de carácter privado cuyo objeto social no se los impida;

III. Instituciones públicas, conforme a las leyes que les son aplicables.

La facultad de expedir certificados no conlleva fe pública por sí misma, así los notarios y corredores públicos podrán llevar a cabo certificaciones que impliquen o no la fe pública, en documentos en papel, archivos electrónicos, o en cualquier otro medio o sustancia en el que pueda incluirse información.

Artículo 101.

Los prestadores de servicios de certificación, podrán realizar, en forma enunciativa, cualesquiera de, o todas las actividades y aquellas conexas a las mismas, siguientes:

I. Verificar la identidad de los usuarios y su vinculación con los medios de identificación electrónica.

II. Comprobar la integridad y suficiencia del mensaje de datos del solicitante y verificar la firma electrónica de quien realiza la verificación.

III. Llevar a cabo registros de los elementos de identificación de los firmantes y de aquella información con la que haya verificado el cumplimiento de fiabilidad de las firmas electrónicas avanzadas y emitir el certificado.

Artículo 102.

Los prestadores de servicios de certificación que hayan obtenido la acreditación de la

Secretaría, deberán notificarle a ésta, la iniciación de la prestación de servicios de certificación dentro de los 45 días naturales siguientes al comienzo de dicha actividad.

A) Para que las personas indicadas en las fracciones II y III del artículo 100 puedan ser prestadores de servicios de certificación, se requiere acreditación de la Secretaría, la cual no podrá ser negada si el solicitante cumple con los siguientes requisitos, en el entendido de que la Secretaría podrá requerir a los prestadores de servicios de certificación, que comprueben la subsistencia del cumplimento de los mismos:

I. Solicitar a la Secretaría la acreditación como prestador de servicios de certificación;

II. Contar con los elementos humanos, materiales, económicos y tecnológicos requeridos para prestar el servicio, a efecto de garantizar la seguridad de la información y su confidencialidad;

III. Contar con procedimientos definidos y específicos para la tramitación del certificado, y medidas que garanticen la seriedad de los certificados emitidos, la conservación y consulta de los registros;

IV. Quienes operen o tengan acceso a los sistemas de certificación de los prestadores de servicios de certificación no podrán haber sido condenados por delito contra el patrimonio de las personas o que haya merecido pena privativa de la libertad, ni que por cualquier algún motivo hayan sido inhabilitados para el ejercicio de su profesión, para desempeñar un puesto en el servicio público, en el sistema financiero o para ejercer el comercio;

V. Contar con fianza vigente por el monto y condiciones que se determine en forma general en los lineamientos o reglas generales que al efecto se expida por la Secretaría.

VI. Establecer por escrito su conformidad para ser sujeto a auditoría por parte de la Secretaría.

VII. Registrar su certificado ante la Secretaría.

B) En lo que respecta a la acreditación de las personas a que se refiere la fracción I del artículo 100, deberán acreditar que cumplen con los requisitos previstos en las fracciones anteriores del apartado A de este artículo, con excepción a lo establecido en su fracción V.

C) Si la Secretaría no ha resuelto respecto la petición del solicitante, dentro de los 45 días siguientes a la presentación de la solicitud, se tendrá por concedida la acreditación.

Artículo 103.

Los prestadores de servicios de certificación deben cumplir las siguientes obligaciones:

I. Comprobar por sí o por medio de una persona física o moral que actúe en nombre y por cuenta suyos, la identidad de los solicitantes y cualesquiera circunstancias pertinentes para la emisión de los certificados, utilizando cualquiera de los medios admitidos en derecho siempre y cuando sean previamente notificados al solicitante.

II. Poner a disposición del firmante los dispositivos de generación de los datos de creación y de verificación de la firma electrónica.

III. Informar, antes de la emisión de un certificado, a la persona que solicite sus servicios,

de su precio, de las condiciones precisas para la utilización del certificado, de sus limitaciones de uso y, en su caso, de la forma en que garantiza su posible responsabilidad.

IV. Mantener un registro de certificados, en el que quedará constancia de los emitidos y figurarán las circunstancias que afecten a la suspensión, pérdida o terminación de vigencia de sus efectos. A dicho registro podrá accederse por medios electrónicos, ópticos o de cualquier otra tecnología y su contenido público estará a disposición de las personas que lo soliciten, el contenido privado estará a disposición del destinatario y de las personas que lo soliciten cuando así lo autorice el firmante, así como en los casos a que se refieran los lineamientos o reglas generales que al efecto establezca la Secretaría.

V. Guardar confidencialidad respecto a la información que haya recibido para la prestación del servicio de certificación.

VI. En el caso de cesar en su actividad, los prestadores de servicios de certificación deberán comunicarlo a la Secretaría a fin de determinar, conforme a lo establecido en los lineamientos expedidos, el destino que se dará a sus registros y archivos.

VII. Asegurar las medidas para evitar la alteración de los certificados y mantener la confidencialidad de los datos en el proceso de generación de los datos de creación de la firma electrónica.

VIII. Establecer declaraciones sobre sus normas y prácticas, las cuales harán del conocimiento del usuario y el destinatario.

IX. Proporcionar medios de acceso que permitan a la parte que confía en el certificado determinar:

1. La identidad del prestador de servicios de certificación;

2. Que el firmante nombrado en el certificado tenía bajo su control el dispositivo y los datos de creación de la firma en el momento en que se expidió el certificado;

3. Que los datos de creación de la firma eran válidos en la fecha en que se expidió el certificado;

4. El método utilizado para identificar al firmante;

5. Cualquier limitación en los fines o el valor respecto de los cuales puedan utilizarse los datos de creación de la firma o el certificado;

6. Cualquier limitación en cuanto al ámbito o el alcance de la responsabilidad indicada por el prestador de servicios de certificación;

7. Si existe un medio para que el firmante dé aviso al prestador de servicios de certificación de que los datos de creación de la firma han sido de alguna manera controvertidos y;

8. Si se ofrece un servicio de terminación de vigencia del certificado.

Artículo 104.

-La Secretaría, coordinará y actuará como autoridad certificadora, y registradora, respecto

de los prestadores de servicios de certificación, previstos en este Capítulo.

Sin perjuicio de lo previsto en la legislación aplicable al sistema financiero mexicano, las instituciones que lo integran deberán observar las disposiciones del presente Capítulo.

Artículo 105.

Serán responsabilidad del destinatario y de la parte que confía, en su caso, las consecuencias jurídicas que entrañe el hecho de que no haya tomado medidas razonables para:

I. Verificar la fiabilidad de la firma electrónica; o

II. Cuando la firma electrónica esté sustentada por un certificado:

i) Que permita la posibilidad de verificar, incluso en forma inmediata, la validez, suspensión o revocación del certificado; y

ii) Tener en cuenta cualquier limitación de uso contenida en el certificado.

Artículo 106.

Los certificados, deberán contener:

I La indicación de que se expiden como tales.

II. El código de identificación único del certificado.

III. La identificación del prestador de servicios de certificación que expide el certificado, nombre o razón social, su domicilio, dirección de correo electrónico, en su caso, y los datos de acreditación ante la Secretaría;

IV. Nombre del titular del certificado.

V. Periodo de vigencia del certificado.

VI. La fecha y hora de la emisión, suspensión, y renovación del certificado;

VII. El alcance de las responsabilidades que asume el prestador de servicios de certificación.

VIII. La referencia de la tecnología empleada para la creación de la firma electrónica.

Artículo 107.

Un certificado dejará de surtir efectos para el futuro, en los siguientes casos:

I. Expiración del período de vigencia del certificado, el cual no podrá ser superior a 2 años, contados a partir de la fecha en que se hubieren expedido. Antes de que concluya el periodo de vigencia del certificado podrá el firmante renovarlo ante el prestador de servicios de certificación.

II. Revocación por el prestador de servicio de certificación, a solicitud del firmante, o por la persona física o moral representada por éste o por un tercero autorizado.

III. Pérdida o inutilización por daños del dispositivo en el que se contenga dicho certificado.

IV. Por haberse comprobado que al momento de su expedición, el certificado no cumplió con los requisitos establecidos en la ley, situación que no afectará los derechos de terceros de buena fe.

V. Resolución judicial o de autoridad competente que lo ordene.

Artículo 108.

El prestador de servicios de certificación que incumpla con las obligaciones que se le imponen en el presente Capítulo, previa garantía de audiencia, y mediante resolución debidamente fundada y motivada, tomando en cuenta la gravedad de la situación y reincidencia, podrá ser sancionado por la Secretaría con suspensión temporal o definitiva de sus funciones. Este procedimiento tendrá lugar conforme a la Ley Federal de Procedimiento Administrativo.

Artículo 109.

- En el caso de que un prestador de servicios de certificación, sea suspendido, inhabilitado o cancelado en su ejercicio, el registro y los certificados que haya expedido pasarán, para su administración, a otro prestador de servicios de certificación, que para tal efecto señale la Secretaría mediante lineamientos o reglas generales.

Capítulo IV. Reconocimiento de Certificados y Firmas Electrónicas Extranjeros ➦

Artículo 110.

Para determinar si un certificado o una firma electrónica extranjeros producen efectos jurídicos, o en qué medida los producen, no se tomará en consideración cualquiera de los siguientes supuestos:

I.- El lugar en que se haya expedido el certificado o en que se haya creado o utilizado la firma electrónica.

II.- El lugar en que se encuentre el establecimiento del prestador de servicios de certificación o del firmante.

Todo certificado expedido fuera de la República Mexicana producirá los mismos efectos jurídicos en la misma, que un certificado expedido en la República Mexicana, si presenta un grado de fiabilidad equivalente a los contemplados por este Título.

Toda firma electrónica creada o utilizada fuera de la República Mexicana producirá los mismos efectos jurídicos en la misma, que una firma electrónica creada o utilizada en la República Mexicana, si presenta un grado de fiabilidad equivalente.

A efectos de determinar si un certificado o una firma electrónica presentan un grado de

fiabilidad equivalente para los fines de los dos párrafos anteriores, se tomarán en consideración las normas internacionales reconocidas por México y cualquier otro medio de convicción pertinente.

Cuando, sin perjuicio de lo dispuesto en los párrafos anteriores, las partes acuerden entre sí la utilización de determinados tipos de firmas electrónicas y certificados, se reconocerá que ese acuerdo es suficiente a efectos del reconocimiento transfronterizo, salvo que ese acuerdo no sea válido o eficaz conforme al derecho aplicable.

Transitorios ➦

Primero: El presente decreto comenzará su vigencia 90 días después de su publicación en el Diario Oficial de la Federación.

Segundo: Dentro del plazo de 90 días posteriores a la publicación del presente decreto, la Secretaría de Economía, emitirá los lineamientos o reglas generales a que se refieren las presentes disposiciones.

Tercero: En lo que se refiere al artículo 102, dentro de los doce meses siguientes a la entrada en vigor de este decreto, el plazo de 45 días a que se refiere el mismo, será de 120 días naturales.