

## REPUBLICA DE PANAMA

### ANTEPROYECTO DE LEY

POR MEDIO DEL CUAL SE DEFINE Y REGLAMENTA

**EL ACCESO, Y USO DEL COMERCIO  
ELECTRÓNICO, FIRMAS DIGITALES Y  
SE AUTORIZAN LAS ENTIDADES  
DE CERTIFICACIÓN**

## REPUBLICA DE PANAMA

### ANTEPROYECTO DE LEY POR MEDIO DEL CUAL SE DEFINE Y REGLAMENTA EL ACCESO Y USO DEL COMERCIO ELECTRÓNICO, FIRMAS DIGITALES Y SE AUTORIZAN LAS ENTIDADES DE CERTIFICACIÓN

#### PARTE I. COMERCIO ELECTRÓNICO EN GENERAL

##### Capítulo I. Disposiciones generales

###### **Artículo 1. *Ámbito de aplicación***

La presente Ley será aplicable a todo tipo de información en forma de mensaje de datos utilizada en el contexto de actividades comerciales, **y para todas aquellas actividades que realice el Estado panameño que implique el intercambio de mensajes a través de las redes**, salvo en los siguientes casos:

- a) En las obligaciones contraídas por el Estado panameño en virtud de Convenios o Tratados internacionales
- b) En las advertencias escritas que por disposición legal deban ir necesariamente impresas en cierto tipo de productos en razón del riesgo que implica su comercialización, uso o consumo.

###### **Artículo 2. *Definiciones***

Para los efectos de la presente Ley se entenderá por:

**Comercio electrónico:** Abarca las cuestiones suscitadas por toda relación de índole comercial, sea o no contractual, estructurada a partir de la utilización de uno o más mensajes de datos o de cualquier otro medio similar. Las relaciones de índole comercial comprenden, sin limitarse a ellas, las siguientes operaciones: toda operación comercial de suministro o intercambio de bienes o servicio; todo acuerdo de distribución; toda operación de representación o mandato comercial; de facturaje ("factoring"); de arrendamiento de bienes de equipo con opción de compra ("leasing"); de construcción de obras; de consultoría; de ingeniería; de concesión de licencias; de inversión; de financiación; de banca; de seguros; todo acuerdo de concesión o explotación de un servicio público; de empresa conjunta y otras formas de cooperación industrial o comercial; de transporte de mercancías o de pasajeros por vía aérea, marítima y férrea, o por carretera.

**Mensaje de Datos:** La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax;

**Firma digital:** Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un proceso matemático conocido, vinculado a la clave del iniciador y al texto del mensaje, permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación.

**Criptografía:** Es la rama de las matemáticas aplicadas que se ocupa de transformar mensajes en formas aparentemente ininteligibles y devolverlas a su forma original.

**Intercambio Electrónico de Datos (EDI):** La transmisión electrónica de información de una computadora a otra, estando estructurada la información conforme a alguna norma técnica convenida al efecto.

**Iniciador:** Toda persona que, a tenor del mensaje, haya actuado por su cuenta o en cuyo nombre se haya actuado, para enviar o generar ese mensaje antes de ser archivado, si éste es el caso, pero que no haya actuado a título de intermediario con respecto a ese mensaje.

**Destinatario:** La persona designada por el iniciador para recibir el mensaje, pero que no esté actuando a título de intermediario con respecto a ese mensaje.

**Intermediario:** Toda persona que, actuando por cuenta de otra, envíe, reciba o archive dicho mensaje o preste algún otro servicio con respecto a él.

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

**Entidad de certificación:** Es aquella persona que, autorizada conforme a la presente Ley, está facultada para emitir certificados en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensaje de datos así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales.

**Certificado:** Es la manifestación que hace la entidad de certificación, como resultado de la verificación que efectúa sobre la autenticidad, veracidad y legitimidad de las firmas digitales o la integridad de un mensaje.

**Repositorio:** Es un sistema de información utilizado para guardar y recuperar certificados u otro tipo de información relevante para la expedición de los mismos.

**Suscriptor:** Dícese de la persona que contrata con una Entidad de certificación la expedición de un certificado, par que sea nombrada o identificada en él. Esta persona mantiene bajo su estricto y exclusivo control el procedimiento para generar su firma digital.

**Usuario:** Dícese de la personal que sin ser suscriptor y sin contratar los servicios de emisión de certificados de una Entidad de certificación, puede sin embargo validar la integridad y autenticidad de un mensaje de datos, con un certificados del suscriptor originador del mensaje.

**Revocar un certificado:** Finalizar definitivamente el período de validez de un certificado, desde una fecha específica, en adelante.

**Suspender un certificado:** Interrumpir temporalmente el período operacional de un certificado desde una fecha específica, en adelante.

### **Artículo 3. Interpretación**

En la interpretación de la presente Ley habrán de tenerse en cuenta su origen internacional, la necesidad de promover la uniformidad de su aplicación y la observancia de la buena fe.

Las cuestiones relativas a materias que se rijan por la presente Ley y que no estén

expresamente resueltas en ella, serán dirimidas de conformidad con los principios generales en que ella se inspira.

#### **Artículo 4. Modificación mediante acuerdo**

Salvo que se disponga otra cosa, en las relaciones entre las partes que generan envían, reciben, archivan o procesan de alguna otra forma mensajes de datos, las disposiciones del Capítulo III, Parte I podrán ser modificadas mediante acuerdo.

Lo dispuesto en este artículo no se aplicará a las disposiciones contenidas en el Capítulo II de la Parte I de la presente Ley.

#### **Artículo 5. Reconocimiento jurídico de los mensajes de datos**

No se negarán efectos jurídicos, validez o fuerza obligatoria a todo tipo de información por la sola razón de que esté en forma de mensaje de datos o que figure simplemente en el mensaje de datos en forma de remisión.

### **Capítulo II Aplicación de los requisitos jurídicos a los mensajes de datos**

#### **Artículo 6. Escrito**

Cuando la Ley requiera que la información conste por escrito, ese requisito quedará satisfecho con un mensaje de datos, si la información que éste contiene es accesible para su posterior consulta.

Lo dispuesto en este artículo se aplicará tanto si el requisito en él previsto constituye una obligación, como si la ley simplemente prevé consecuencias en el caso de que la información no conste por escrito.

Lo dispuesto en el presente artículo no será aplicable a: [...].

#### **Artículo 7. Firma**

Cuando la Ley exija la presencia de una firma o establezca ciertas consecuencias en ausencia de la misma, en relación con un mensaje de datos, se entenderá satisfecho dicho requerimiento si éste ha sido firmado.

Lo dispuesto en este artículo se aplicará tanto si el requisito en él previsto constituye una obligación, como si la ley simplemente prevé consecuencias en el caso de que no exista una firma.

Lo dispuesto en el presente artículo no será aplicable a: [...].

#### **Artículo 8. Original**

Cuando la Ley requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho con un mensaje de datos, sí:

- a) Existe alguna 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.

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

Lo dispuesto en este artículo se aplicará tanto si el requisito en él previsto constituye una obligación, como si la ley simplemente prevé consecuencias en el caso de que la información no conste en su forma original.

Lo dispuesto en el presente artículo no será aplicable a: [...].

### **Artículo 9. Integridad de un mensaje de datos**

Para efectos del artículo anterior, se considerará que la información consignada en un mensaje de datos es íntegra, si ésta ha permanecido completa e inalterada, salvo la adición de algún endoso o de algún cambio que sea inherente al proceso de comunicación, archivo o presentación. El grado de confiabilidad requerido, será determinado a la luz de los fines para los que se generó la información y de todas las circunstancias relevantes del caso.

### **Artículo 10. Admisibilidad y fuerza probatoria de los mensajes de datos**

Los mensajes de datos serán admisibles como medios de prueba y tendrá la misma fuerza probatoria otorgada a los documentos en el Capítulo III, del Título VII del Libro Segundo de Procedimiento Civil del Código Judicial.

En toda actuación administrativa o judicial, no se negará eficacia, validez o fuerza obligatoria y probatoria a todo tipo de información en forma de un mensaje de datos, por el solo hecho de que se trate de un mensaje de datos o que éste no haya sido presentado en su forma original.

### **Artículo 11. Criterio para valorar probatoriamente un mensaje de datos**

Para la valoración de la fuerza probatoria del mensaje de datos a que se refiere esta Ley, se tendrán en cuenta las reglas de la sana crítica y demás criterios reconocidos legalmente para la apreciación de las pruebas.

Por consiguiente, al valorar la fuerza probatoria de un mensaje de datos se habrá de tener presente la confiabilidad de la forma en la que se haya generado, archivado o comunicado el mensaje, la confiabilidad de la forma en la que se haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente.

### **Artículo 12. Conservación de los mensajes de datos**

Cuando la Ley requiera que ciertos documentos, registros o informaciones sean conservados, ese requisito quedará satisfecho mediante la conservación de los mensajes de datos, siempre que se cumplan las siguientes condiciones:

- a) Que la información que contengan sea accesible para su posterior consulta;
- b) Que el mensaje de datos sea conservado en el formato en que se haya generado, enviado o recibido o con algún formato que permita demostrar que reproduce con exactitud la información generada, enviada o recibida; y

- c) Que se conserve, de haber alguna, todo dato que permita determinar el origen, el destino del mensaje, la fecha y la hora en que fue enviado o recibido.

No estará sujeta a la obligación de conservación, la información que tenga por única finalidad facilitar el envío o recepción de los mensajes de datos.

Los libros y papeles del comerciante podrán ser conservados en cualquier medio técnico que garantice su reproducción exacta. Los comerciantes están obligados a conservar por 10 años, los originales de cartas, telegramas, mensajes de datos, o cualquier otro documento que consigne la transacción.

**Artículo 13. Conservación de mensajes de datos y archivo de documentos a través de terceros.**

El cumplimiento de la obligación de conservar documentos, registros o informaciones en mensajes de datos, se podrá realizar a través de terceros, siempre y cuando se cumplan las condiciones enunciadas en el artículo anterior.

**Capítulo III  
Comunicación de los mensajes de datos**

**Artículo 14. Formación y validez de los contratos**

En la formación del contrato, salvo acuerdo expreso entre las partes, la oferta y su aceptación podrá ser expresadas por medio de un mensaje de datos. No se negará validez o fuerza obligatoria a un contrato por la sola razón de haberse utilizado en su formación uno o más mensajes de datos.

Lo dispuesto en el presente artículo no será aplicable a: [...].

**Artículo 15. Reconocimiento de los mensajes de datos por las partes**

En las relaciones entre el iniciador y el destinatario de un mensaje de datos, no se negarán efectos jurídicos, validez o fuerza obligatoria a una manifestación de voluntad u otra declaración por la sola razón de haberse hecho en forma de mensaje de datos.

**Artículo 16. Atribución de los mensajes de datos**

Se entenderá que un mensaje de datos proviene del iniciador, cuando éste ha sido enviado por:

1. El propio iniciador.
2. Por alguna persona facultada para actuar en nombre del iniciador respecto de ese mensaje;
- o
3. Por un sistema de información programado por el iniciador o en su nombre para que opere automáticamente.

**Artículo 17. Presunción del origen de un mensaje de datos**

Se presume que un mensaje de datos ha sido enviado por el iniciador, y por lo tanto puede actuar en consecuencia, cuando:

- a) Haya aplicado en forma adecuada el procedimiento acordado previamente con el iniciador, con el fin de establecer que el mensaje de datos provenía efectivamente de éste; o
- b) El mensaje de datos que reciba el destinatario resulte de los actos de una persona cuya relación con el iniciador, o con algún mandatario suyo, le haya dado acceso a algún método utilizado por el iniciador para identificar un mensaje de datos como propio.

**PARÁGRAFO.-** Lo dispuesto en el presente artículo no se aplicará:

- a) A partir del momento en que el destinatario haya sido informado por el iniciador de que el mensaje de datos no provenía de éste y haya dispuesto de un plazo razonable para actuar en consecuencia; o
- b) A partir del momento en que el destinatario sepa, o debiera saber de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que el mensaje de datos no provenía de éste.

### **Artículo 18. Concordancia del mensaje de datos enviado con el mensaje de datos recibido**

Siempre que un mensaje de datos provenga del iniciador o que se entienda que proviene de él, o siempre que el destinatario tenga derecho a actuar con arreglo a este supuesto, en las relaciones entre el iniciador y el destinatario, éste último 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 convenido, que la transmisión había dado lugar a un error en el mensaje de datos recibido.

### **Artículo 19. Mensajes de datos duplicados**

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

### **Artículo 20. Acuse de recibo**

Si al enviar o antes de enviar un mensaje de datos, el iniciador 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:

- a) Toda comunicación del destinatario, automatizada o no, o
- b) Todo acto del destinatario, que baste para indicar al iniciador que se ha recibido el mensaje de datos.

Si el iniciador ha solicitado o acordado con el destinatario que se acuse recibo del mensaje de datos, y expresamente aquél ha 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.

Si el iniciador ha solicitado o acordado con el destinatario que se acuse recibo del mensaje de datos, pero aquél no indicó expresamente que los efectos del mensaje de datos están condicionados a la recepción del acuse de recibo y, si no se ha recibido acuse en el plazo fijado o

convenido o no se ha fijado o convenido ningún plazo, en un plazo no mayor de 48 horas a partir del momento del envío o el vencimiento del plazo fijado o convenido, el iniciador:

- a) Podrá dar aviso al destinatario de que no ha recibido acuse de recibo y fijar un nuevo plazo para su recepción el cual será de 48 horas, contadas a partir del momento del envío del nuevo mensaje de datos; y
- b) De no recibirse acuse de recibo dentro del término señalado conforme al literal anterior, podrá, dando aviso de ello al destinatario, considerar que el mensaje de datos no ha sido enviado o ejercer cualquier otro derecho que pueda tener

**Artículo 21. Presunción de recepción de un mensaje de datos**

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

Esa presunción no implicará que el mensaje de datos corresponda al mensaje recibido. Cuando en el acuse de recibo se indique que el mensaje de datos recibido cumple con los requisitos técnicos convenidos o enunciados en alguna norma técnica aplicable, se presumirá que ello es así.

Salvo en lo que se refiere al envío o recepción del mensaje de datos, el presente artículo no obedece al propósito de regir las consecuencias jurídicas que puedan derivarse de ese mensaje de datos o de su acuse de recibo.

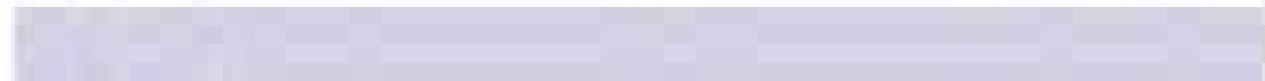
**Artículo 22. Tiempo del envío de un mensaje de datos**

De no convenir otra cosa el iniciador 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 iniciador o de la persona que envió el mensaje de datos en nombre de éste.

**Artículo 23. Tiempo de la recepción de un mensaje de datos**

De no convenir otra cosa el iniciador y el destinatario, el momento de recepción de un mensaje de datos se determinará como sigue:

- a) Si el destinatario ha designado un sistema de información para la recepción de mensajes de datos, la recepción tendrá lugar:
  - i) En el momento en que ingrese el mensaje de datos en el sistema de información designado; o



- a) Si el iniciador 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;
- b) Si el iniciador o el destinatario no tienen establecimiento, se tendrá en cuenta su lugar de residencia habitual.

## **PARTE II. COMERCIO ELECTRÓNICO EN MATERIAS ESPECÍFICAS**

### **Capítulo I. Transporte de mercancías**

#### **Artículo 25. Actos relacionados con los contratos de transporte de mercancías**

Sin perjuicio de lo dispuesto en la parte I de la presente Ley, este capítulo será aplicable a cualquiera de los siguientes actos que guarde relación con un contrato de transporte de mercancías, o con su cumplimiento, sin que la lista sea taxativa.

- a) i) Indicación de las marcas, el número, la cantidad o el peso de las mercancías; ii) declaración de la naturaleza o valor de las mercancías; iii) emisión de un recibo por las mercancías; iv) confirmación de haberse completado el embarque de las mercancías;
- b) i) Notificación a alguna persona de las cláusulas y condiciones del contrato; ii) comunicación de instrucciones al **porteador**;
- c) i) Reclamación de la entrega de las mercancías; ii) autorización para proceder a la entrega de las mercancías; iii) notificación de la pérdida de las mercancías o de los daños que hayan sufrido;
- d) Cualquier otra notificación o declaración relativas al cumplimiento del contrato;
- e) Promesa de hacer entrega de las mercancías a la persona designada o a una persona autorizada para reclamar esa entrega;
- f) Concesión, adquisición, renuncia, restitución, transferencia o negociación de algún derecho sobre mercancías;
- g) Adquisición o transferencia de derechos y obligaciones con arreglo al contrato.

#### **Artículo 26. Documentos de transporte**

Con sujeción a lo dispuesto en el inciso tercero del presente artículo, en los casos en que la Ley requiera que alguno de los actos enunciados en el artículo 25 se lleve a cabo por escrito o mediante un documento que conste en papel, ese requisito quedará satisfecho cuando el acto se lleve a cabo por medio de uno o más mensajes de datos.

Lo anterior será aplicable, tanto si el requisito en él previsto está expresado en forma de obligación o si la Ley simplemente prevé consecuencias en el caso de que no se lleve a cabo el acto por escrito o mediante un documento emitido en papel.

Cuando se conceda algún derecho a una persona determinada y a ninguna otra, o ésta adquiera

alguna obligación, y la Ley requiera que, para que ese acto surta efecto, el derecho o la obligación hayan de transferirse a esa persona mediante el envío, o utilización, de un documento emitido en papel, ese requisito quedará satisfecho si el derecho o la obligación se transfiere mediante la utilización de uno o más mensajes de datos, siempre que se emplee un método confiable para garantizar la singularidad de ese mensaje o esos mensajes de datos.

Para los fines del párrafo anterior, el nivel de confiabilidad requerido será determinado a la luz de los fines para los que se transfirió el derecho o la obligación y de todas las circunstancias del caso, incluido cualquier acuerdo pertinente.

Cuando se utilicen uno o más mensajes de datos para llevar a cabo alguno de los actos enunciados en los literales f) y g) del artículo 25, no será válido ningún documento emitido en papel utilizado para llevar a cabo cualquiera de esos actos, a menos que se haya puesto fin al uso de mensajes de datos para sustituirlo por el de documentos **emitidos en papel**. Todo documento que se emita en esas circunstancias deberá contener una declaración a tal efecto. La sustitución de mensajes de datos por documentos emitidos en papel no afectará los derechos ni las obligaciones de las partes.

Cuando se aplique obligatoriamente una norma jurídica a un contrato de transporte de mercancías que esté consignado, o del que se haya dejado constancia en un documento emitido en papel, esa norma no dejará de aplicarse a dicho contrato de transporte de mercancías del que se haya dejado constancia en uno o más mensajes de datos por razón de que el contrato conste en ese mensaje o esos mensajes de datos en lugar de constar en documento emitidos en papel.

### **PARTE III. FIRMAS DIGITALES, CERTIFICADOS Y ENTIDADES DE CERTIFICACIÓN**

#### **CAPÍTULO I. FIRMAS DIGITALES**

##### ***Artículo 27. Atributos de la firma digital.***

El uso de una firma digital tendrá la misma fuerza y efectos que el uso de una firma manuscrita, si aquélla incorpora los siguientes atributos:

1. Es única a la persona que la usa.
2. Es susceptible de ser verificada.
3. Está bajo el control exclusivo de la persona que la usa.
4. Está ligada a la información o mensaje, de tal manera que si éstos son cambiados, la firma digital es invalidada.
5. Está conforme a las reglamentaciones adoptadas por el Gobierno Nacional

##### ***Artículo 28. Firma Digital Segura***

Una firma digital es una firma digital que puede ser verificada de conformidad con un sistema o procedimiento de seguridad autorizado por la presente Ley o autorizado por las partes.

##### ***Artículo 29. Mensaje de datos firmado digitalmente***

Se entenderá que un mensaje de datos ha sido firmado, si el símbolo o la metodología adoptada

por la parte, cumple con un procedimiento de autenticación o seguridad previamente acordado.

Cuando una firma digital haya sido fijada en un mensaje de datos se presume que el suscriptor de aquella tenía la intención de acreditar ese mensaje de datos y de ser vinculado con el contenido del mismo.

## **CAPÍTULO II**

### **Entidades de certificación**

#### ***Artículo 30. La Autoridad***

El otorgamiento de licencias y la emisión de certificados los cuales serán utilizados para firmar certificados y los certificadores así como la supervisión del cumplimiento de esta Ley corresponde a la Secretaría Nacional de Ciencia, Tecnología e Innovación como Autoridad de Acreditación Raíz.

Por medio de la presente Ley, la Autoridad queda facultada para acreditar y regular a las entidades de certificación a fin de garantizar un nivel básico de calidad de sus servicios, que son de vital importancia para la confiabilidad de las firmas digitales

#### ***Artículo 31. Naturaleza, Características y requerimientos de las entidades de certificación***

Las actividades que esta Ley asigna a las entidades de certificación se considerarán como la prestación de un servicio público.

Podrán ser entidades de certificación, las personas jurídicas, tanto públicas como privadas, de origen nacional o extranjero, que previa solicitud sean autorizadas por la Secretaría Nacional de Ciencia, Tecnología e Innovación (SENACYT) a través de su Centro de Seguridad de Datos y que cumplan con los requerimientos establecidos por el Gobierno Nacional, con base en las siguientes condiciones:

- a) Ser persona jurídica
- b) Contar con la capacidad económica y financiera suficiente para prestar los servicios autorizados como entidad de certificación
- c) Tener y acreditar el acceso a hardware y software suficientes y además contar con los elementos técnicos necesarios para la generación de firmas digitales, la emisión de certificados sobre la autenticidad de las mismas y la conservación y archivo de documentos soportados en mensajes de datos.
- d) Los representantes legales, administradores y personal operativo no podrán ser personas que hayan sido condenadas a pena privativa de libertad, excepto por delitos políticos o culposos; O que hayan sido suspendidas en el ejercicio de su profesión por faltas graves contra la ética o hayan sido excluidas de aquélla.
- e) Obtener de la Secretaría Nacional de Ciencia, Tecnología e Innovación a través de su Centro de Seguridad de Datos la correspondiente autorización para operar como entidad de certificación, siempre y cuando cumpla con todos los requerimientos técnicos establecidos por el Gobierno Nacional.

#### ***Artículo 32. Actividades de las entidades de certificación***

Las entidades de certificación autorizadas por el Centro de Seguridad de Datos de la Secretaría Nacional de Ciencia, Tecnología e Innovación para prestar sus servicios en el país, podrán realizar

las siguientes actividades:

1. Emitir certificados en relación con las firmas digitales de personas naturales o jurídicas.
2. Emitir certificados sobre la verificación respecto de la alteración entre el envío y la recepción del mensaje de datos
3. Ofrecer o facilitar los servicios de creación de firmas digitales certificadas
4. Ofrecer o facilitar los servicios de registro y estampado cronológico en la transmisión y recepción de mensajes de datos
5. Ofrecer los servicios de archivo y conservación de mensajes de datos.
6. Emitir certificados en relación con la persona que posea un derecho con respecto a los documentos enunciados en los literales f y g del artículo 25 de la presente Ley.

### **Artículo 33. Auditorias a las Entidades de Certificación**

La Secretaría Nacional de Ciencia, Tecnología e Innovación a través de su Centro de Seguridad de Datos realizará por lo menos una vez al año una visita de auditoria a cada entidad de certificación autorizada para operar, con el objeto de evaluar el cumplimiento y desempeño de sus operaciones dentro de los parámetros fijados en la Ley y en los reglamentos.

Como resultado de las visitas de auditoria, el Centro de Seguridad de Datos evaluará el desempeño de cada una de las entidades de certificación, formulando las recomendaciones e imponiendo las medidas pertinentes que deben ser atendidas por las entidades vigiladas para efectos de normalizar y optimizar la prestación del servicio de conformidad con las exigencias legales y reglamentarias.

Si como resultado de la auditoria se establece que la entidad de certificación no ha cumplido con los requerimientos legales y reglamentarios en el desempeño de sus operaciones, el Centro de Seguridad de Datos de la SENACYT podrá imponer cualquiera de las sanciones previstas en la presente Ley.

El resultado de la evaluación será incluido en la manifestación de práctica de la correspondiente entidad de certificación. Esta manifestación de práctica se deberá publicar en el repositorio que la SENACYT designe.

### **Artículo 34. Manifestación de práctica de la entidad de certificación**

Cada entidad de certificación autorizada publicará, en un repositorio de la SENACYT o en el que ésta designe, una manifestación de práctica de entidad de certificación que contenga la siguiente información:

- a) El nombre, la dirección y el número telefónico de la entidad de certificación.
- b) La clave pública actual de la entidad de certificación
- c) El resultado de la evaluación obtenida por la entidad de certificación en la última auditoria realizada por el Centro de Seguridad de Datos
- d) Si la autorización para operar como Entidad de certificación ha sido revocada o suspendida. Para ambos casos, se entenderá revocada o suspendida la clave pública de la entidad de certificación. Este registro deberá incluir igualmente la fecha de la revocación o suspensión y los motivos de la misma.
- e) Los límites impuestos a la entidad de certificación, en la autorización para operar.
- f) Cualquier evento que sustancialmente afecte la capacidad de la entidad de certificación para operar

- g) **Lista de normas y procedimientos de certificación de firmas**
- h) **Lista de nómina e identificación de personal**
- i) **Denominación del sistema de encriptación utilizado**
- j) **Método algorítmico o identificación de dicho método**
- k) **Descripción del plan de contingencia que garantice los servicios**
- l) **Cualquier información que se requiera mediante reglamento**

### ***Artículo 35. Remuneración por la prestación de servicios***

La remuneración por los servicios de las entidades de certificación será establecida libremente por éstas.

### ***Artículo 36. Deberes de las entidades de certificación.***

Las entidades de certificación tendrán, entre otros, los siguientes deberes:

- a) Emitir certificados conforme a lo solicitado o acordado por el suscriptor;
- b) Implementar los sistemas de seguridad para garantizar la emisión y creación de firmas digitales, la conservación y archivo de certificados y documentos en soporte de mensaje de datos
- c) Garantizar la protección, confidencialidad y debido uso de la información suministrada por el suscriptor
- d) Garantizar la prestación permanente del servicio de la entidad de certificación
- e) Atender oportunamente las solicitudes y reclamaciones hechas por los suscriptores
- f) Efectuar los avisos y publicaciones conforme a lo dispuesto en la presente Ley
- g) Suministrar la información que le requieran las entidades administrativas competentes o judiciales en relación con las firmas digitales y certificados emitidos y en general sobre cualquier documento electrónico que se encuentre bajo su custodia y administración
- h) Actualizar permanentemente los medios técnicos conforme a las especificaciones adoptadas por el Gobierno Nacional mediante reglamento
- i) Permitir y facilitar la realización de las auditorias por parte del Centro de Seguridad de Datos de la SENACYT
- j) Publicar en un repositorio un listado de los certificados suspendidos o revocados
- k) Publicar en un repositorio su práctica de autoridad de certificación
- l) Elaborar los reglamentos que definen las relaciones con el suscriptor y la forma de prestación del servicio
- m) Llevar un registro de los certificados

### ***Artículo 37. Terminación unilateral***

Salvo acuerdo entre las partes, la entidad de certificación podrá dar por terminado el acuerdo de vinculación con el suscriptor dando un preaviso no menor de noventa (90) días. Vencido este término, la entidad de certificación revocará los certificados que se encuentren pendientes de expiración.

Igualmente, el suscriptor podrá dar por terminado el acuerdo de vinculación con la entidad de certificación dando un preaviso no inferior a treinta (30) días.

### ***Artículo 38. Responsabilidad de la entidad de certificación***

Salvo acuerdo entre las partes, las entidades de certificación responderán por los daños y

perjuicios que por dolo o culpa leve causen a toda persona de buena fe exenta de culpa.

### **Artículo 39. Cesación de actividades por parte de las entidades de certificación**

Las entidades de certificación autorizadas pueden cesar en el ejercicio de actividades, siempre y cuando hayan recibido autorización por parte del CCE de SENACYT.

Una vez éste haya autorizado la cesación de actividades, la entidad de certificación que cesará de operar, deberá enviar a cada suscriptor un aviso con no menos de noventa (90) días de anterioridad a la fecha de la cesación efectiva de actividades, en el cual solicitará autorización para revocar o publicar en otro repositorio de otra entidad de certificación, los certificados que aún se encuentran pendientes de expiración.

Pasados sesenta (60) días sin obtenerse respuesta por parte del suscriptor, la entidad de certificación podrá revocar los certificados no expirados u ordenar su publicación, dentro de los quince (15) días siguientes, en un repositorio de otra entidad de certificación; en ambos casos, dando aviso de ello al suscriptor.

Si la entidad de certificación no ha efectuado la publicación en los términos del inciso anterior, el Centro ordenará la publicación de los certificados no expirados en los repositorios de la entidad de certificación por ella designada.

En el evento de no ser posible la publicación de esos certificados en los repositorios de cualquier entidad de certificación, el Centro efectuará la publicación de los certificados no expirados en un repositorio de su propiedad.

## **CAPITULO III CERTIFICADOS**

### **Artículo 40. Contenido de los certificados**

Un certificado emitido por una entidad de certificación autorizada, además de estar firmado digitalmente por ésta, debe contener por lo menos lo siguiente:

1. Nombre, dirección y domicilio del suscriptor
2. Identificación del suscriptor nombrado en el certificado
3. El nombre, la dirección y el lugar donde realiza actividades la entidad de certificación
4. La clave pública del usuario
5. La metodología para verificar la firma digital del suscriptor impuesta en el mensaje de datos
6. El número de serie del certificado
7. Fecha de emisión y expiración del certificado

### **Artículo 41. Expiración de un certificado**

Un certificado emitido por una entidad de certificación expira en la fecha indicada en el mismo. Sin embargo, la fecha de expiración de un certificado en ningún caso podrá ser superior a un (1) año.

### **Artículo 42. Aceptación de un certificado**

Salvo acuerdo entre las partes, se entiende que un suscriptor ha aceptado un certificado cuando

la entidad de certificación, a solicitud de éste o de una persona en nombre de éste, lo ha publicado en un repositorio o lo ha enviado a una o más personas.

#### **Artículo 43. Garantía derivada de la aceptación de un certificado**

El suscriptor al momento de aceptar un certificado, garantiza a todas las personas de buena fe exenta de culpa que se soportan en la información en él contenida, que:

- a) La firma digital autenticada mediante éste, está bajo su control exclusivo
- b) Que ninguna persona ha tenido acceso al procedimiento de generación de la firma digital
- c) Que la información contenida en el certificado es verdadera y corresponde a la suministrada por éste a la entidad de certificación

#### **Artículo 44. Suspensión y Revocación de certificados**

El suscriptor de una firma digital certificada, podrá solicitar a la entidad de certificación que expidió un certificado, la suspensión o revocación del mismo.

La revocación o suspensión del certificado se hace efectiva a partir del momento en que se registra por parte de la entidad de certificación. Este registro debe hacerse en forma inmediata, una vez recibida la solicitud de suspensión o revocación.

#### **Artículo 45. Causales para la revocación de certificados**

El suscriptor de una firma digital certificada está obligado a solicitar la revocación del certificado en los siguientes casos:

- a. Por pérdida de la clave privada
- b. La clave privada ha sido expuesta o corre peligro de que se le dé un uso indebido.

Si el suscriptor no solicita la revocación del certificado en el evento de presentarse las anteriores situaciones, será responsable por las pérdidas o perjuicios en los cuales incurran terceros de buena fe exentos de culpa que confiaron en el contenido del certificado.

Una entidad de certificación revocará un certificado emitido por las siguientes razones:

- a. A petición del suscriptor o un tercero en su nombre y representación
- b. Por muerte del suscriptor
- c. Por disolución del suscriptor en el caso de las personas jurídicas
- d. Por la confirmación de que alguna información o hecho contenido en el certificado es falso
- e. La clave privada de la entidad de certificación o su sistema de seguridad ha sido comprometido de manera material que afecte la confiabilidad del certificado
- f. Por el cese de actividades de la entidad de certificación
- g. Por orden judicial o de autoridad administrativa competente

#### **Artículo 46. Notificación de la suspensión o revocación de un certificado**

Una vez registrada la suspensión o revocación de un certificado, la entidad de certificación debe publicar, en forma inmediata, un aviso de suspensión o revocación en todos los repositorios en los cuales la entidad de certificación publicó el certificado. También deberá notificar de este hecho a las

personas que soliciten información acerca de una forma digital verificable por remisión al certificado suspendido o revocado.

Si los repositorios en los cuales se publicó el certificado no existen al momento de la publicación del aviso, o los mismos son desconocidos, la entidad de certificación deberá publicar dicho aviso en un repositorio que designe el Centro para tal efecto.

#### **Artículo 47. Registro de Certificados**

Toda entidad de certificación autorizada deberá llevar un registro de todos los certificados emitidos, que se encuentre a disposición del público, el cual debe indicar las fechas de emisión, expiración y los registros de suspensión, revocación o reactivación de los mismos.

#### **Artículo 48. Término de conservación de los registros**

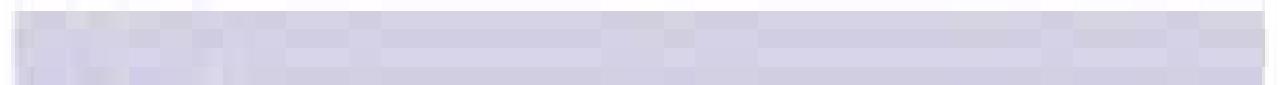
Los registros de certificados expedidos por una entidad de certificación deben ser conservados por el término de cuarenta (40) años contados a partir de la fecha de revocación o expiración del correspondiente.

### **CAPÍTULO IV Suscriptores de firmas digitales**

#### **Artículo 49. Deberes de los suscriptores**

Son deberes de los suscriptores:

1. Recibir de las claves por parte de la entidad de certificación o generar las claves utilizando un sistema de seguridad exigido por la entidad de certificación
2. Suministrar información completa, precisa y verídica a la entidad de certificación



## CAPÍTULO V

### CENTRO DE SEGURIDAD DE DATOS DE LA SECRETARÍA NACIONAL DE CIENCIA, TECNOLOGÍA E INNOVACIÓN

#### **Artículo 52. Funciones del Centro de Seguridad de Datos**

El Centro de Seguridad de Datos de la SENACYT ejercerá la función de entidad de vigilancia y control de las actividades desarrolladas por las entidades de certificación y en especial tendrá las siguientes funciones:

- a) Autorizar, conforme a la reglamentación expedida por el Gobierno Nacional, la operación de entidades de certificación en el territorio nacional.
- b) Velar por el adecuado funcionamiento y la eficiente prestación del servicio por parte de las entidades de certificación y el cabal cumplimiento de las disposiciones legales y reglamentarias de la actividad
- c) Efectuar las auditorias de que trata la presente Ley
- d) Definir reglamentariamente los requerimientos técnicos que califiquen la idoneidad de las actividades desarrolladas por las entidades de certificación
- e) Evaluar las actividades desarrolladas por las entidades de certificación autorizadas conforme a los requerimientos definidos en los reglamentos técnicos
- f) Revocar o suspender la autorización para operar como entidad de certificación
- g) Requerir en cualquier momento a las entidades de certificación para que suministren información relacionada con los certificados, las firmas digitales emitidas y los documentos en soporte informático que custodien o administren
- h) Imponer sanciones a las entidades de certificación por el no-cumplimiento o cumplimiento parcial de las obligaciones derivadas de la prestación del servicio
- i) Ordenar la revocación o suspensión de certificados cuando en la entidad de certificación los emita sin el cumplimiento de las formalidades legales
- j) Designar los repositorios y entidades de certificación en los eventos previstos en la Ley
- k) Proponer al Gobierno la implementación de políticas en relación con la regulación de las actividades de las entidades de certificación y la adopción de los avances tecnológicos para la generación de firmas digitales, la emisión de certificados, la conservación y archivo de documentos en soporte electrónico
- l) Aprobar los reglamentos internos de la prestación del servicio, así como sus reformas
- m) Emitir certificados en relación con las firmas digitales de las entidades de certificación
- n) Velar por la observancia de las disposiciones constitucionales y legales sobre la promoción de

la competencia y prácticas comerciales restrictivas en los mercados atendidos por las entidades de certificación

### **Artículo 53. Sanciones**

El Centro de Seguridad de Datos de acuerdo con el debido proceso y el derecho de defensa, podrá imponer según la naturaleza y la gravedad de la falta, las siguientes sanciones a las entidades de certificación que incumplan o violen las normas a las cuales debe sujetarse su actividad:

1. Amonestación
2. Multas hasta por el equivalente a 3,000 salarios mínimos mensuales. El monto de la multa se graduará atendiendo al impacto de la infracción sobre la calidad del servicio ofrecido, y el factor de reincidencia. La entidades multadas podrán repetir contra quienes hubieran realizado los actos u omisiones que dieron lugar a la sanción
3. Suspender de inmediato todas o algunas de las actividades de la entidad infractora
4. Separar a los administradores o empleados responsables, de los cargos que ocupan en la entidad de certificación sancionada. También se les prohibirá a los infractores trabajar en empresas similares por el término de diez (10) años
5. Prohibir a la entidad de certificación infractora prestar directa o indirectamente los servicios de la entidad de certificación por el término de diez (10) años
6. Revocación definitiva de la autorización para operar como entidad de certificación, cuando la aplicación de las sanciones anteriormente enumeradas, no haya sido efectiva y se pretenda evitar perjuicios reales o potenciales a terceros

## **CAPÍTULO VI**

### **Repositorios**

#### **Artículo 54. Reconocimiento y Actividades de los Repositorios**

La SENACYT autorizará únicamente la operación de los repositorios que mantengan las entidades de certificación autorizadas.

Los repositorios autorizados para operar deberán:

- a) Mantener una base de datos de certificados de conformidad con los reglamentos que para tal efecto expida el Gobierno Nacional
- b) Garantizar que la información que mantienen se conserve íntegra, exacta y razonablemente confiable
- c) Ofrecer y facilitar los servicios de registro y estampado cronológico en la transmisión y recepción de mensajes de datos
- d) Ofrecer los servicios de archivo y conservación de mensajes de datos
- e) Mantener un registro de las publicaciones de los certificados revocados o suspendidos

## CAPÍTULO VII

### DISPOSICIONES VARIAS

#### **Artículo 55. Certificaciones Recíprocas**

Los certificados de firmas digitales emitidos por entidades de certificación extranjeras, podrán ser reconocidos en los mismos términos y condiciones exigidos en la Ley para la emisión de certificados por parte de las entidades de certificación nacionales, siempre y cuando tales certificados sean reconocidos por una entidad de certificación autorizada que garantice en la misma forma que lo hace con sus propios certificados, la regularidad de los detalles del certificado, así como su validez y vigencia.

#### **Artículo 56. Incorporación por Remisión**

Salvo acuerdo en contrario entre las partes, cuando en un mensaje de datos se haga remisión total o parcial a directrices, normas, estándares, acuerdos, cláusulas, condiciones o términos fácilmente accesibles con la intención de incorporarlos como parte del contenido o hacerlos vinculantes jurídicamente, se presume que estos términos están incorporados por remisión a ese mensaje de datos. Entre las partes, y conforme a la Ley, esos términos serán jurídicamente válidos como si hubieran sido incorporados en su totalidad en el mensaje de datos.

### PARTE IV

### REGLAMENTACIÓN Y VIGENCIA

#### CAPÍTULO I

**Artículo 57.** El Gobierno nacional deberá reglamentar la presente Ley dentro de los seis (6) meses siguientes a su entrada en vigencia, para lo relacionado con el funcionamiento del Centro de Seguridad de Datos de la Secretaría Nacional de Ciencia, Tecnología e Innovación, sin perjuicio de la potestad reglamentaria del Gobierno.

De conformidad con la anterior reglamentación, el Centro contará con un término adicional de seis (6) meses para organizar y asignar a una de sus dependencias la función de control y vigilancia de las actividades realizadas por las entidades de certificación.

#### CAPÍTULO II

#### VIGENCIA

#### **Artículo 58. Vigencia y Derogatorias**

La presente Ley rige desde la fecha de su publicación y deroga las normas que le sean contrarias, con excepción de las normas destinadas a la protección del consumidor.

El Centro de Seguridad de Datos autorizará únicamente la operación de los repositorios que mantengan las entidades de certificación autorizadas.

Los repositorios autorizados para operar deberán:

Mantener una base de datos de certificados de conformidad con los reglamentos que para tal

efecto expida el Gobierno Nacional

Garantizar que la información que mantienen se conserve íntegra, exacta y razonablemente confiable

Ofrecer y facilitar los servicios de registro y estampado cronológico en la transmisión y recepción de mensajes de datos

Ofrecer los servicios de archivo y conservación de mensajes de datos

Mantener un registro de las publicaciones de los certificados revocados o suspendidos

## ***CAPÍTULO VII. Disposiciones Varias***

### ***Artículo. Certificaciones Recíprocas***

Los certificados de firmas digitales emitidos por entidades de certificación extranjeras, podrán ser reconocidos en los mismos términos y condiciones exigidos en la Ley para la emisión de certificados por parte de las entidades de certificación nacionales, siempre y cuando tales certificados sean reconocidos por una entidad de certificación autorizada que garantice en la misma forma que lo hace con sus propios certificados, la regularidad de los detalles del certificado, así como su validez y vigencia.

### ***Artículo. Incorporación por Remisión***

Salvo acuerdo en contrario entre las partes, cuando en un mensaje de datos se haga remisión total o parcial a directrices, normas, estándares, acuerdos, cláusulas, condiciones o términos fácilmente accesibles con la intención de incorporarlos como parte del contenido o hacerlos vinculantes jurídicamente, se presume que esos términos están incorporados por remisión a ese mensaje de datos. Entre las partes y conforme a la Ley, esos términos serán jurídicamente válidos como si hubieran sido incorporados en su totalidad en el mensaje de datos.

## ***PARTE IV. REGLAMENTACIÓN Y VIGENCIA CAPÍTULO I. Reglamentación***

### ***Artículo.***

El Gobierno Nacional deberá reglamentar la presente Ley dentro de los seis meses siguientes a su entrada en vigencia, para lo relacionado con el funcionamiento del Centro de Seguridad de Datos de la Secretaría Nacional de Ciencia, Tecnología e Innovación, sin perjuicio de la potestad reglamentaria del Gobierno.

De conformidad con la anterior reglamentación, la Secretaría Nacional de Ciencia, Tecnología e Innovación contará con un término adicional de seis meses, para organizar y asignar a una de sus dependencias la función de control y vigilancia de las actividades realizadas por las entidades de certificación, sin perjuicio de que el Gobierno Nacional cree una unidad especializada dentro de ella, para tal efecto.

## **CAPITULO II. Vigencia**

### **Artículo . Vigencia y derogatorias**

La presente Ley rige desde la fecha de su publicación y deroga las normas que le sean contrarias, con excepción de las normas destinadas a la protección del consumidor.

### **Artículo 18. Resolución de Conflictos**

