

# LEY 188

13ra ASAMBLEA 3ra SESION  
LEGISLATIVA ORDINARIA  
(P. del S. 423)

## LEY NÚM. 188

(Aprobada el 7 de Agosto de 1998)

Para adoptar la Ley de Firmas Digitales de Puerto Rico, a fin de reconocer a la rúbrica digital que se realiza a través de claves de algoritmo el mismo efecto legal que se reconoce en nuestro ordenamiento a la firma de puño y letra; autorizar y reglamentar el uso de firmas digitales; facultar al Departamento de Estado para conceder licencias a las autoridades certificadoras; establecer los requisitos y salvaguardas necesarios para garantizar la confidencialidad de las firmas; establecer penalidades; enmendar los incisos (a) y (b) del Artículo 3 de la Ley Núm. 5 de 8 de diciembre de 1955, según enmendada, conocida como "Ley de la Administración de Documentos Públicos"; y enmendar los incisos (10), (13) y (28) del Artículo 7 de la Ley Núm. 115 de 22 de julio de 1974, según enmendada, conocida como "Código Penal del Estado Libre Asociado de Puerto Rico".

## EXPOSICION DE MOTIVOS

Cuando el mundo comience a utilizar a gran escala el comercio electrónico, la firma de puño y letra sobre el papel comenzará a representar un símbolo del pasado. A pesar de la gradual desaparición del papel como medio para plasmar acuerdos, las firmas serán aún necesarias en la era electrónica que se avecina.

El interés del Estado en los adelantos del comercio electrónico motiva a aprobar una serie de guías generales de autenticación electrónica que fomenten el desarrollo de su industria y a la vez provean cierto grado de confiabilidad a las transacciones comerciales que se realizan a través de los medios electrónicos.

Con el propósito de minimizar la incidencia del uso apócrifo de firmas digitales y fraude electrónico en el futuro cercano, se autoriza al use comercial de la rúbrica digital que se realiza a través de claves de algoritmo sobre unas estructuras legales que faciliten su utilización y permitan el intercambio de datos a información confiable implantando legalmente los estándares prevalecientes en este campo que se han desarrollado conjuntamente con otras jurisdicciones.

Este Gobierno interesado en que Puerto Rico forme parte del nuevo orden comercial que se avecina y se mantenga competitivo en los mercados internacionales creados por la globalización, reconoce y acepta la firma digital y le confiere el mismo valor y efecto legal que a la firma de puño y letra en papel.

La mecanización de la actividad pública y privada, necesaria para enfrentar los retos del nuevo milenio, permitirá agilizar los procesos y brindar de la manera más efectiva y adecuada los servicios que exige la ciudadanía para realizar las gestiones y transacciones cotidianas que mantienen en curso la actividad de Puerto Rico.

Decrétase por la Asamblea Legislativa de Puerto Rico:

PARTE I

TITULO, INTERPRETACION Y DEFINICIONES

## Artículo 1 - Título

Esta Ley se conocerá como "Ley de Firmas Digitales de Puerto Rico".

## Artículo 2 - Propósito y Política Pública

La mecanización de la actividad pública y privada, necesaria para enfrentar los retos del nuevo milenio, permitirá agilizar los procesos y brindar de la manera más efectiva y adecuada los servicios que exige la ciudadanía para realizar las gestiones y transacciones cotidianas que mantienen en curso la actividad de Puerto Rico, así como brindar la información más exacta y confiable. La operación de los sistemas automatizados contribuirá al crecimiento de la economía y facilitará la entrada en los mercados internacionales, así como fomentará el desarrollo de todos los aspectos de la sociedad puertorriqueña. Es por ello, que se reconoce y acepta la firma digital y se le confiere el mismo valor y efecto legal que la firma de puño y letra escrita en papel.

Esta Ley se interpretará de forma consistente con las normas y usos razonables de la informática y del comercio con el propósito de facilitar la comunicación por medios electrónicos confiables minimizar la incidencia en la falsificación de las firmas digitales y el fraude en el comercio electrónico; implantar legalmente los estándares prevalecientes en este campo como es, por ejemplo, el denominado X.509 de la "International Telecommunication Union" (antes "International Telegraph and Telephone Consultative Committee" o CCITT); y establecer, en coordinación con otras jurisdicciones, normas uniformes relacionadas con la autenticación y confiabilidad de la comunicación electrónica.

## Artículo 3 - Definiciones

A los fines de esta Ley, y a menos que el contexto expresamente indique otra cosa, los siguientes términos tendrán el significado que a continuación se expresa:

(1) "Aceptar un certificado" es:

- (a) manifestar la aprobación de un certificado, del cual se tiene conocimiento o información sobre su contenido: o
- (b) solicitar un certificado de una autoridad certificadora, el cual posteriormente es emitido.

(2) "Autoridad certificadora" es una persona que emite un certificado.

(3) "Autoridad certificadora licenciada" es una autoridad certificadora que posee una licencia en vigor expedida por el Departamento de Estado.

(4) "Banco de Información" es el sistema desarrollado para recopilar y restablecer certificados y otra Información relevante relacionada con las firmas digitales.

(5) "Banco de información reconocido" es un sistema de recopilación de datos o información sobre firmas digitales reconocido por el Departamento de Estado, conforme a lo dispuesto en esta Ley.

(6) "Certificado" es un documento electrónico el cual:

- (a) identifica la autoridad certificadora que lo emite;
- (b) nombra o identifica al subscriptor;

- (c) consigna la clave pública del subscriptor; y
  - (d) está firmado digitalmente por la autoridad certificadora que lo emite.
- (7) "Certificar" es la declaración sobre hechos pertinentes que expide la autoridad en el certificado.
- (8) "Certificado de Transacción" es un certificado válido, el cual incorpora por referencia una o más firmas digitales.
- (9) "Certificado válido" es un certificado que:
- (a) ha sido emitido por una autoridad certificadora licenciada;
  - (b) que ha sido aceptado por el subscriptor;
  - (c) no ha sido revocado o suspendido; y
  - (d) no ha expirado.
- (10) "Clave privada" es la clave del par de claves utilizada para crear una firma digital.
- (11) "Clave pública" es la clave del par de claves utilizada para verificar una firma digital.
- (12) "Confirmar" es cerciorarse mediante la indagación e investigación apropiada.
- (13) "Corresponder" en relación a las claves es que pertenece al mismo par de claves.
- (14) "Criptosistema asimétrico" es un algoritmo o serie de algoritmos que proveen un par de claves seguras.
- (15) "Departamento" es el Departamento de Estado del Gobierno de Puerto Rico.
- (16) "Derecho de indemnización" es la concesión de daños en una acción civil por un tribunal con jurisdicción sobre una autoridad certificadora licenciada por violaciones a esta Ley.
- (17) "Emitir un certificado" es el acto el cual una autoridad certificadora produce un certificado y notifica su contenido al subscriptor.
- (18) "Falsificar una firma digital" es:
- (a) crear o producir una firma digital sin la autorización del tenedor legal de la clave privada; o
  - (b) crear o producir una firma digital que pueda ser verificada mediante un certificado que designe como subscriptor a una persona que no existe o que no la una clave privada que corresponda a la clave pública registrada en el certificado.
- (19) "Firma digital" es la conversión de un mensaje usando un criptosistema asimétrico de manera que una persona que tiene el mensaje o comunicación inicial y la clave pública del signatario pueda determinar con exactitud sí:
- (a) la conversión se hizo utilizando la clave privada que corresponde a la clave pública del signatario; y

(b) el mensaje o comunicación ha sido alterado desde que se hizo la conversión.

(20) "Garantía o Garantía Suficiente" es la fianza que preste un fiador autorizado por el Comisionado de Seguros de Puerto Rico o una carta de crédito irrevocable emitida por una institución financiera autorizada para hacer negocios en Puerto Rico por el Comisionado de Instituciones Financieras. la cual en cualquiera de los casos, debe cumplir con los siguientes requisitos:

(a) sea pagadera al Departamento para beneficio de las personas que tengan derecho a indemnización contra la autoridad certificadora licenciada nombrada como principal o el cliente de la carta de crédito.

(b) expresa la cantidad establecida mediante reglamento del Departamento de Estado. Según se dispone en el Artículo 4 de esta Ley;

(c) que indique que se ha emitido para registrarse, según dispone esta Ley;

(d) indique que el período de vigencia se extiende, al menos, por la duración del término de la licencia emitida por la autoridad certificadora; y

(e) que está hecha en la forma prescrita por las normas del Departamento de Estado.

Una garantía suficiente también podrá disponer que la responsabilidad anual total no excederá la cantidad establecida en la misma.

Una institución financiera que actúa como una autoridad certificadora podrá cumplir con los requisitos de este inciso con sus activos o capital, hasta el límite permitido conforme con lo dispuesto en la Ley Núm. 4 de 11 de octubre de 1985, según enmendada.

(21) "Incorporar por referencia" es hacer un mensaje o comunicación parte de otro mensaje identificando el mensaje que se ha incorporado y expresando el propósito para el cual se incorporó.

(22) "Informe de prácticas de certificación" es una declaración de las prácticas que emplea generalmente una autoridad certificadora al emitir certificados o al emitir información pertinente del certificado.

(23) "Límite máximo de responsabilidad" es el monto de la cantidad fijada en un certificado que responde por los daños y perjuicios ocasionados, según se dispone en el Artículo 17 de esta Ley.

(24) "Mensaje o Comunicación" es una representación digital de información.

(25) "Notificación o Aviso" es comunicar un hecho a otra persona de modo, que razonablemente conlleve la información a conocimiento de la otra persona.

(26) "Par de claves" es una clave privada y su correspondiente clave pública en un criptosistema asimétrico, las cuales se caracterizan porque la clave pública puede verificar una firma digital creada o producida por una clave privada.

(27) "Persona" es un individuo o cualquier entidad capaz de firmar un documento, bien legalmente o como cuestión de hecho.

(28) "Personal de operaciones" es la persona natural que se desempeña como autoridad certificadora o su agente, o ha sido empleada o contratada por una autoridad certificadora y que

posee responsabilidades administrativas o establece política en la autoridad certificadora; o cuyos deberes se relacionan directamente con la emisión de certificados, la producción de claves privadas o la administración de los centros de cómputos de la autoridad certificadora.

(a) responsabilidades ejecutivas o de establecer la política para la autoridad certificadora; o

(b) deberes que envuelven directamente la emisión de certificados, la creación de claves privadas o la administración de los centros de cómputos de la autoridad certificadora.

(29) "Publicar" es registrar o archivar en un banco de información.

(30) "Receptor" es la que recibe o posee una firma digital y en condiciones de confiar en ella.

(31) "Registro de autoridades certificadoras" es el récord en línea ("on -line") accesible al público que sobre las autoridades certificadoras licenciadas debe mantener el Departamento de Estado y cuyo contenido reglamento, según se dispone en el Artículo 4 de esta Ley.

(32) "Revocar un certificado" es invalidar un certificado a partir de un momento específico. La revocación se efectúa por la anotación o inclusión en un grupo de certificados revocados y no implica su destrucción o elegibilidad.

(33) "Sellar el registro" ("Time-stamp") es:

(a) anejar o acompañar una anotación firmada digitalmente indicando por lo menos la fecha y hora en la cual se anejó la misma y la identidad de la persona que lo hizo; o

(b) la anotación que así se acompaña.

(34) "Signatario" es la persona que crea o produce una firma digital en un mensaje o comunicación.

(35) "Sistema confiable" es la serie de programas y discos de computadoras que:

(a) están protegidos contra interferencia o uso ilegal;

(b) están razonablemente accesibles y son seguros, confiables y funcionan correctamente; y

(c) son adecuadas para realizar su función.

(36) "Subscriptor" es la persona que:

(a) aparece designada en el certificado;

(b) acepta el certificado: y

(c) posee la clave privada que corresponda a la clave pública indicada en el certificado.

(37) "Suspender un certificado" es invalidar un certificado temporariamente a partir de un momento específico.

(38) "Poseer legalmente una clave privada" es estar capacitado para utilizar una clave privada que:

(a) el tenedor o su agente no la ha divulgado a nadie en violación a las disposiciones del Artículo 12 de esta Ley; y

(b) el tenedor no la ha adquirido mediante robo, engaño o al escucharla secretamente por medio de dispositivos electrónicos u otros medios ilegales e ilícitos.

(39) "Poseer una clave privada" es estar capacitado para utilizar una clave privada.

(40) "Verificar una firma digital" es en relación a determinada firma digital, mensaje o clave pública digital, determinar con precisión que:

(a) la firma digital fue creada por la clave privada correspondiente a la clave pública; y

(b) el mensaje no ha sido alterado desde que se produjo la firma digital.

#### Artículo 4 - Funciones y Deberes del Departamento de Estado

El Departamento de Estado será una autoridad certificadora y podrá emitir, suspender y revocar certificados en la forma prescrita en esta Ley y tendrá las siguientes funciones:

(1) Mantendrá una base de datos accesible y pública que contendrá un registro declaratorio para cada una de las autoridades certificadas y que será publicada en por lo menos un banco de información reconocido, según se dispone en esta Ley.

(2) Aprobará las reglas y reglamentos para el cumplimiento de los propósitos de esta Ley, incluyendo normas para:

(a) Regulen las autoridades certificadoras licenciadas y su práctica, así como su disolución.

(b) Establecer el monto o cantidad apropiada de la garantía suficiente, tomando en consideración la carga que impone la prestación de la garantía; y

(c) la seguridad, en cuanto a la responsabilidad financiera, que se provee a las personas que se valen de los certificados expedidos por las autoridades certificadoras licenciadas.

(3) Revisar programas o aplicaciones utilizados para firmas digitales y publicar informes relacionados con los programas.

(4) Establecer los requisitos razonables, de forma que pueda cumplir los certificados emitidos por las autoridades certificadoras licenciadas, conforme las normas generalmente aceptadas para los certificados de firmas digitales.

(5) Establecer los requisitos para archivar adecuadamente los expedientes.

(6) Establecer los requisitos razonables en cuanto al contenido, forma y fuentes de información en los registros de las autoridades certificadoras y las normas para mantener y actualizar dicha información y regular otras prácticas y controles relacionados a los registros.

(7) Establecer la forma de los informes de la práctica de certificación. Los procedimientos para la reglamentación, concesión de licencias, fiscalización, investigación y adjudicación de controversias se regirán por la Ley Núm. 170 de 12 de agosto de 1988, según enmendada, conocida como "Ley de Procedimiento Administrativo Uniforme"

#### PARTE 2

#### LICENCIAMIENTO Y REGLAMENTACION DE LAS AUTORIDADES CERTIFICADORAS

## Artículo 5 - Concesión de Licencias, Requisitos

(1) Para obtener o retener una licencia, una autoridad certificadora deberá cumplir con los siguientes requisitos:

(a) ser el subscriptor de un certificado publicado en un banco de información reconocido:

(b) no emplear como personal de operaciones a personas que han sido convictas por delito grave o un delito que envuelva fraude, declaraciones falsas o engaño;

(c) emplear como personal de operaciones a personas que posean conocimientos y destrezas para cumplir con los requisitos establecidos en esta Ley;

(d) registrar en el Departamento una garantía suficiente, excepto, cuando la autoridad certificadora sea el Gobernador, un departamento o agencia del Gobierno, sus dependientes o municipios, la Rama Legislativa y la Judicial, siempre que cumplan con los siguientes requisitos:

(i) actúen a través de un funcionario debidamente autorizado por Ley, ordenanza o reglamento, para desempeñar y ejecutar las funciones como autoridad certificadora; y

(ii) que la entidad gubernamental sea subscriptor de todos los certificados emitidos por la autoridad certificadora;

(e) tener el derecho a usar un sistema confiable, incluyendo un método seguro para controlar el uso de la clave privada;

(f) presentar prueba al Departamento de que posee capital de trabajo suficiente, según las normas que apruebe el Departamento, que le permite hacer negocio como autoridad certificadora:

(g) mantener una oficina en Puerto Rico o tener un agente designado para recibir emplazamientos en Puerto Rico; y

(h) cumplir con todos los demás requisitos establecidos mediante reglamento por el Departamento.

El Departamento expedirá una licencia a la autoridad certificadora que cumpla con los requisitos establecidos en este Artículo y así lo solicite por escrito, previo el pago de los derechos de inscripción requeridos. Se faculta al Departamento para clasificar y expedir licencias bajo condiciones específicas, tales como el número máximo de certificados emitidos, límites máximos acumulativos de responsabilidad máxima en los certificados emitidos por la autoridad certificadora, o la emisión por sólo una empresa u organización. Se entenderá que una autoridad certificadora actúa como una autoridad certificadora no licenciada cuando emite un certificado que excede los términos de la licencia. El Departamento podrá revocar o suspender la licencia a una autoridad certificadora que no cumpla con las disposiciones de esta Ley o cuando no reúna los requisitos. Además, el Departamento podrá reconocer la licencia o autorización de autoridades certificadoras emitida por entidades gubernamentales, siempre que los requisitos para obtener la licencia o autorización sean substancialmente similares a los dispuestos en esta Ley. En el caso en que se reconoce la expedición de una licencia por una entidad gubernamental le aplicarán a los certificados las presunciones y efectos legales a los límites de responsabilidad que establece esta Ley en la misma forma en que aplican a las demás autoridades certificadoras licenciadas en Puerto Rico.

Los requisitos para la concesión de una licencia establecida en este Artículo no afectarán la efectividad a validez de una firma digital. Salvo que se disponga lo contrario por contrato. Los límites de responsabilidad que establece el Artículo 17 de esta Ley no serán aplicables a las autoridades certificadoras que no posean licencia.

#### Artículo 6 - Auditorías e Investigaciones

Las operaciones de cada una de las autoridades certificadoras licenciadas serán auditadas por un contador público autorizado, un perito en seguridad de computadoras o un profesional acreditado en seguridad de computadoras por lo menos una (1) vez al año, para evaluar el cumplimiento de las disposiciones de esta Ley. El Departamento determinará mediante reglamento los requisitos y condiciones que deberán cumplir los auditores. El auditor, a base de la información obtenida en el transcurso de la auditoría, clasificará el cumplimiento de la autoridad certificadora licenciada en una de las siguientes categorías:

(1) "cumplimiento total" es cuando la autoridad certificadora demuestra que ha cumplido todos los requisitos que establece la ley y los reglamentos;

(2) "cumplimiento sustancial" es cuando la autoridad certificadora demuestra que ha cumplido generalmente con los requisitos que establece la ley y los reglamentos, aunque se encuentran algunas instancias de incumplimiento o en que no se ha podido demostrar el cumplimiento. Pero las mismas no son de importancia;

(3) "cumplimiento parcial" es cuando la autoridad certificadora demuestra haber cumplido algunos de los requisitos que establece la ley y los reglamentos, pero determina que no cumple o no pudo demostrar haber cumplido salvaguardas de mayor importancia; o

(4) "incumplimiento" es cuando la autoridad certificadora cumple con pocos o ninguno de los reglamentos, no mantiene expedientes adecuados que mayor demuestren el cumplimiento con la mayor parte de los requisitos o rehúsa someterse a la auditoría.

El auditor informará la fecha de la auditoría a la autoridad certificadora licenciada y la clasificación las cuales serán publicadas en el registro de autoridades certificadoras.

El Departamento podrá eximir a una autoridad certificadora licenciada de cumplir con el requisito de la auditoría establecido en este Artículo en las siguientes circunstancias:

(1) la autoridad certificadora solicita la exención por escrito;

(2) la auditoría más reciente de las ejecutorias de la autoridad certificadora, si alguna, demostró que se cumplió total o substancialmente con los requisitos; y

(3) la autoridad certificadora declara, bajo juramento o afirmación, que se encuentra bajo una o más de las siguientes circunstancias:

(a) ha emitido menos de seis (6) certificados durante el pasado año y el total de los límites máximos de responsabilidad en todos esos certificados no excede de diez mil (10,000) dólares:

(b) la suma agregada de la vigencia de todos los certificados emitidos durante el pasado año es menor de treinta (30) días y el total de los límites máximos de responsabilidad de todos esos certificados no exceden de diez mil (10,000) dólares; o

(c) el total de los límites máximos de responsabilidad en todos los certificados pendientes y emitidos es menor de mil (1,000) dólares.

El Departamento publicará en el registro de autoridades certificadoras que la autoridad certificadora está exenta del requisito de auditoría dispuesto en este Artículo. Se entenderá que la autoridad certificadora incumple con el requisito de la auditoría establecido en este Artículo, si al solicitar la exención ofrece información falsa sobre algún hecho pertinente.

#### Artículo 7 - Ordenes; Sanciones Administrativas

Se autoriza al Departamento para investigar las actividades de las autoridades certificadoras licenciadas emitir las órdenes necesarias para llevar a cabo las investigaciones y poner en vigor las disposiciones de esta Ley. Si la autoridad certificadora dejare de cumplir con una orden, al Departamento podrá suspender o revocar la licencia que le ha expedido conforme dispone esta Ley. Además, podrá imponer a cualquier persona que a sabiendas o intencionalmente viole una orden, una multa administrativo que no excederá de cinco mil (5,000) dólares por cada violación, o noventa por ciento (90%) del límite máximo de responsabilidad establecido en el certificado, lo que sea menor. El Departamento podrá ordenar a la autoridad certificadora al pago de los gastos incurridos en el procedimiento y en el caso en que solicite un interdicto para compeler el cumplimiento de sus órdenes podrá recobrar los gastos incurridos en ello, conforme lo dispuesto en la Regla 44 de Procedimiento Civil, según enmendada.

#### Artículo 8 - Prácticas Prohibidas

Se prohíbe a las autoridades certificadoras, licenciadas o no, conducir sus negocios en forma tal que creen un riesgo de pérdida irrazonable a los subscriptores de la autoridad certificadora,

A las personas que se valen de los certificados emitidos por la autoridad certificadora o a los bancos de información reconocidos.

El Departamento podrá publicar en los bancos reconocidos un breve informe, sobre situaciones de prácticas prohibidas de las cuales tiene conocimiento. La autoridad certificadora en cuestión podrá presentar, por escrito, sus objeciones a la publicación del informe. En este caso, el Departamento publicará el escrito e informará sobre la celebración de una vista y podrá determinar a base de la evidencia presentada, lo siguiente:

- (1) anular el aviso si concluye que no existen fundamentos para la publicación conforme lo dispuesto en este Artículo:
- (2) cancelar el aviso si la publicación deja de estar justificada;
- (3) continuar publicando o enmendar el informe si aún se justifica; o
- (4) tomar acción legal para eliminar o reducir un riesgo.

El Departamento publicará su decisión en uno o más bancos de información. Además, podrá emitir órdenes e interponer cualquier recurso o remedio legal disponible para cesar y desistir o prohibir que una autoridad certificadora violente lo dispuesto en este Artículo, independientemente de que la autoridad certificadora esté o no licenciada.

### PARTE 3

#### DEBERES DE LA AUTORIDAD CERTIFICADORA Y EL SUBSCRIPTOR

## Artículo 9 - Deberes Generales de las Autoridades Certificadoras

Una autoridad certificadora licenciada o un suscriptor tiene la obligación de utilizar sistemas confiables para emitir, suspender o revocar los certificados, para publicar y notificar la emisión, suspensión o revocación de los certificados, y para producir la clave privada.

La autoridad certificadora licenciada debe divulgar las prácticas de certificación y cualquier dato pertinente relativo a la confiabilidad de un certificado o de su capacidad para prestar los servicios. Como requisito previo a la divulgación de lo dispuesto en este Artículo, la autoridad certificadora contratará los servicios de una persona particular para que realice una investigación y presente un informe por escrito.

## Artículo 10 - Emisión del Certificado

La autoridad certificadora emitirá un certificado a un suscriptor si cumple con los siguientes requisitos:

- (1) el suscriptor presenta la correspondiente solicitud; y
- (2) la autoridad certificadora verifica lo siguiente:
  - (a) que el suscriptor es la persona a cuyo nombre se emitirá el certificado;
  - (b) que actúa mediante un agente que la autorizó a tener bajo su custodia la clave privada y a requerir la emisión del certificado en que se designa la clave pública correspondiente.
  - (c) que la información contenida en el certificado a ser emitido es exacta;
  - (d) que el suscriptor es el tenedor legal de la clave privada que corresponde a la clave pública que se designa en el certificado;
  - (e) que el suscriptor es tenedor de una clave privada capaz de producir una firma digital;
  - (f) que la clave pública indicada en el certificado puede ser utilizada para verificar una firma digital con la clave privada que tiene el suscriptor.

Si el suscriptor acepta el certificado emitido, la autoridad certificadora publicará una copia firmada del certificado en el banco de información reconocido que ambos determinen, a menos que se provea otra cosa por contrato. Si el suscriptor no acepta al certificado, la autoridad certificadora licenciada no publicará el certificado o cancelará su publicación si el certificado ha sido publicado.

Los requisitos establecidos de este inciso no pueden ser renunciados o negados por la autoridad certificadora licenciada o el suscriptor. Nada de lo dispuesto en este Artículo impide que la autoridad certificadora licenciada se rija por normas, informes de prácticas de certificación, planes de seguridad o requisitos contractuales más rigurosos, siempre que los mismo sean consistentes con lo dispuesto en esta Ley.

La autoridad certificadora licenciada que ha emitido un certificado lo revocará si verifica que no fue emitido conforme lo dispuesto en este Artículo, o podrá optar por suspenderlo por un período de tiempo razonable que no excederá de cuarenta y ocho (48) horas, para llevar a cabo una investigación y hacer una determinación, la cual notificará prontamente al suscriptor.

El Departamento ordenará a la autoridad certificadora que suspenda o revoque un certificado previa notificación y vista a la autoridad certificadora y al suscriptor, cuando determine que el certificado no cumple con los requisitos establecidos en este Artículo y que el incumplimiento representa un riesgo significativo para las personas que se valen del certificado. Si existiera una situación de emergencia que exige un remedio inmediato, al Departamento podrá suspender el certificado por un período razonable de tiempo que no excederá cuarenta y ocho (48) horas.

#### Artículo 11- Garantías y Obligaciones de la Autoridad Certificadora

La autoridad certificadora licenciada, al emitir un certificado, garantiza al suscriptor que el mismo no contiene información falsa que cumple con los requisitos que establece esta Ley y que ha actuado dentro de la autoridad que le confiere la licencia que se le ha expedido. La autoridad certificadora licenciada no podrá renunciar o limitar las garantías que reconoce este Artículo.

Cuando una autoridad certificadora licenciada emite un certificado, a menos que acuerde otra cosa con el suscriptor, tiene la obligación de actuar prontamente en el caso de suspensión o revocación de un certificado conforme se dispone en los Artículos 14 y 15 de esta Ley y de notificar al suscriptor dentro de un término razonable, cualquier hecho que afecte significativamente la validez o confiabilidad del certificado.

Al emitir un certificado, se entiende que la autoridad certificadora licenciada certifica a las personas que se valen del mismo lo siguiente:

- (1) que la información contenida en el certificado es exacta;
- (2) que consideró toda la información pertinente y que los términos del certificado se basan en la misma;
- (3) que el suscriptor ha aceptado el certificado; y
- (4) que la autoridad certificadora licenciada ha cumplido con las leyes que reglamentan la emisión de certificados.

Al publicar un certificado, se entiende que la autoridad certificadora licenciada certifica al banco de información en el cual se publica y a todos los que se valen del mismo, que ha emitido un certificado al suscriptor.

#### Artículo 12 - Aceptación del Certificado; Deberes

Al aceptar un certificado, se entiende que el suscriptor certifica a las personas que se valen del mismo, lo siguiente:

- (1) que es el tenedor legal de la clave privada que corresponde a la clave pública designada en el certificado:
- (2) que toda la información ofrecida por el suscriptor a la autoridad certificadora y consignada en el certificado es correcta; y
- (3) que toda la información ofrecida por el suscriptor a una autoridad certificadora o contenida en el certificado aunque no haya sido verificada por la autoridad certificadora al emitirlo, es correcta.

Cuando un agente solicita que se emita un certificado en el cual se designe a su representado como suscriptor, se entiende que certifica lo siguiente:

(1) que posee la autoridad legal necesaria para solicitar la emisión del certificado designado a su representante como subscriptor; y

(2) que está autorizado para firmar digitalmente a nombre de su representante. Si existieren restricciones a dicha autoridad, se entenderá que existen salvaguardas adecuadas para evitar que se produzcan firmas digitales que excedan la misma.

Una persona no podrá renunciar o limitar mediante contrato la aplicación de este Artículo, ni obtener indemnización por esa causa si ello limita la responsabilidad debida a las personas que se valen del certificado cuando se presenta información falsa.

El subscriptor que acepta un certificado tiene la obligación de indemnizar a la autoridad certificadora que lo emite por cualquier pérdida o daño causado por la emisión o certificación de un certificado basado en datos falsos o por dejar de divulgar datos pertinentes, se lo hizo con la intención de engañar a la autoridad certificadora o a la persona que se vale del certificado, o por negligencia. Si la autoridad certificadora emitió el certificado a solicitud de un agente del subscriptor, responde igualmente el agente como si fuese el subscriptor. La responsabilidad de indemnizar no será renunciable ni podrá limitarse por contrato. Sin embargo, se podrán pactar por contrato sus términos.

La autoridad certificadora podrá requerir que el subscriptor certifique bajo juramento o afirmación la veracidad de la información que ofrece al solicitar un certificado, bajo pena de perjurio.

#### Artículo 13 - Control de la Clave Privada

Al aceptar un certificado, el subscriptor tiene el deber de ejercer el debido cuidado para mantener el control de la clave privada y evitar que sea divulgada a cualquier persona que no esté autorizada a producir la firma digital del subscriptor. La clave privada es propiedad personal del subscriptor como tenedor legal de la misma.

La autoridad certificadora tiene una clave privada que corresponde a una clave pública registrada en el certificado, posee la clave privada como fiduciaria del subscriptor y sólo podrá utilizarla si el subscriptor lo autoriza previamente por escrito, a menos que expresamente le conceda la clave privada a la autoridad certificadora y le permita tenerla bajo las condiciones que establezcan.

#### Artículo 14 - Suspensión del Certificado; Penalidades

El Departamento o la autoridad certificadora licenciada que emitió un certificado que no sea un certificado de transacción, a menos que se acuerde otra cosa, suspenderá el mismo por un período que no excederá de cuarenta y ocho (48) horas cuando así lo solicite el subscriptor o una persona con conocimiento de la obligación del subscriptor de guardar la clave privada como es un agente, socio de negocios, empleado o miembro de la familia inmediata al subscriptor. Así mismo, el Departamento también podrá ordenar que la autoridad certificadora licenciada suspenda el certificado, conforme dispone el Artículo 10 de esta Ley. No será necesario que la autoridad certificadora verifique la identidad o la autoridad de la persona que solicita la suspensión. No obstante, cuando se solicite la suspensión al Departamento, deberá demostrarse que la autoridad certificadora que emitió el certificado no está disponible.

El Departamento podrá requerir al solicitante que provea la evidencia necesaria, incluyendo una declaración bajo juramento o afirmación, para determinar, en su sana discreción, si suspende o deniega la suspensión del certificado. Se faculta al Departamento y al Secretario del Departamento de Justicia para investigar cualquier actuación ilícita por parte de las personas que solicitan la suspensión.

Se releva a suscriptor de su obligación de mantener la clave privada asegurada, según se dispone en el Artículo 12, mientras el certificado esté suspendido.

El Departamento o la autoridad certificadora licenciada que suspende un certificado publicará la suspensión del certificado en un aviso firmado en el banco de información que indique el certificado, y si éste no existe, rehúsa aceptar la publicación, o no está reconocido, según lo dispuesto en el Artículo 24 de esta Ley, la autoridad certificadora licenciada publicará el aviso en cualquier banco de información reconocido. Cuando el Departamento es quien hace la publicación, la persona que solicita la suspensión deberá pagar los derechos requeridos por el banco de información para la publicación del aviso.

La autoridad certificadora dejará sin efecto la suspensión cuando el suscriptor así lo solicite y verifique que el solicitante es el suscriptor o su agente autorizado y que la solicitud de suspensión se hizo sin autorización de éste. No se requiere que la autoridad certificadora verifique la información provista en la solicitud de suspensión.

El suscriptor y la autoridad certificadora licenciada podrán, mediante contrato, limitar o excluir lo relacionado con la suspensión mediante solicitud por la autoridad certificadora o disponer la forma para dejarla sin efecto. Sin embargo, si el contrato limita o excluye la suspensión por parte del Departamento cuando la autoridad certificadora no esté disponible, esta cláusula sólo será válida si se publica el certificado.

#### Artículo 15 - Revocación del Certificado

Dentro del término de un día laborable de haber recibido la solicitud, la autoridad certificadora licenciada revocará un certificado que no sea un certificado de transacción, cuando así le sea solicitado por escrito y verifique que el solicitante es el suscriptor o su agente con autoridad.

La autoridad certificadora licenciada también revocará el certificado en las siguientes circunstancias.

(1) cuando tenga conocimiento de la muerte del suscriptor por haber recibido copia certificada del certificado de defunción o verificado el hecho de su muerte; y

(2) al presentarle documentos o al verificar que el suscriptor no existe.

La autoridad certificadora licenciada podrá revocar uno o más certificados si los certificados son dudosos, independientemente de que el suscriptor consienta a la revocación.

Al revocar un certificado, la autoridad certificadora licenciada publicará un aviso firmado de la revocación en el banco de información que indique el certificado. Si éste no existiera, rehusare aceptar la publicación o ya no estuviese reconocido, según se dispone en el Artículo 24 de esta Ley, la autoridad certificadora licenciada publicará el aviso en cualquier otro banco reconocido.

Una vez revocado el certificado, cesarán las obligaciones del suscriptor establecidas en los Artículos 12 y 13 de esta Ley, cuando se publique el aviso que dispone este Artículo o luego de transcurridos dos (2) días de haber solicitado su revocación, presenta a la autoridad certificadora evidencia fehaciente que confirma lo solicitado y paga los derechos acordados en el contrato.

Al publicarse el aviso, según se dispone en este Artículo, la autoridad certificadora licenciada queda liberada de las garantías que conlleva la emisión del certificado y cesa de certificar la información según se dispone en el Artículo 11 de esta Ley, en relación al certificado revocado.

## Artículo 16 - Expiración del Certificado

El certificado indicara la fecha de su expiración. Transcurrido dicho término cesarán las obligaciones del subscriptor y la autoridad certificadora cesará de certificar la información contenida en el certificado, según se dispone en esta Ley y queda liberada de las obligaciones que conlleva la emisión del certificado.

## Artículo 17 - Límite Máximo de Responsabilidad

Al establecer un límite máximo de responsabilidad en un certificado, la certificadora y el subscriptor, advierten a las personas que se valen del mismo que el riesgo no está cubierto por una cantidad mayor al límite máximo fijado.

Salvo que renuncie a lo aquí dispuesto, la autoridad certificador licenciada no será responsable por pérdida alguna causada al reconocer una firma digital falsa o falsificada si cumplió con todos los requisitos que establece esta Ley. Tampoco responderá por una suma mayor a la establecida en el certificado como máximo de responsabilidad cuando la pérdida es ocasionada al dar crédito a información falsa sobre algún dato que debió verificar o por incumplimiento con lo dispuesto en el Artículo 10 de esta Ley al emitir el certificado.

En una acción para recobrar una pérdida basada en la confiabilidad de un certificado, la autoridad certificadora licenciada será responsable por datos y perjuicios, excluyendo daños punitivos, por la pérdida de ganancias, ahorros u oportunidades o por sufrimientos y angustias mentales.

## Artículo 18 - Ejecución de la Garantía

No obstante, cualquier disposición en contrato establecida en la garantía:

(1) Si la garantía es una fianza, la persona puede recobrar del fiador la cantidad total de la indemnización, o si hay más de una persona con derecho a indemnización, le corresponderá una parte proporcional hasta el máximo de responsabilidad de la garantía igual a la cantidad de la fianza; o

(2) Si la garantía es una carta de crédito, la persona puede recobrar de la institución financiera que la expide, la cantidad total de la indemnización, o si hay más de una persona con derecho a indemnización, le corresponderá la parte proporcional, hasta el máximo de responsabilidad del librador, igual a la cantidad del crédito.

Los reclamantes podrán recobrar sucesivamente de la misma garantía, si la responsabilidad total en la garantía no excede la cantidad de la misma. Además de la indemnización, un reclamante podrá recobrar de los créditos de la garantía, hasta que éstos se agoten, honorarios razonables de abogado y las costas incurridas en la reclamación, si la responsabilidad total de la garantía no excede la cantidad de la garantía.

El reclamante debe notificar por escrito de la reclamación al Departamento haciendo constar su nombre y dirección, la cantidad reclamada, los fundamentos bajo los cuales reclama su derecho a ser indemnizado y cualquier otra información requerida por los reglamentos adoptados por el Departamento.

Ninguna persona tendrá derecho a ser indemnizada conforme lo dispuesto, a menos que: presente una reclamación, según se dispone en este Artículo y presente la notificación dentro de los dos (2) años de haber ocurrido la violación a esta Ley en que basa su reclamación.

## PARTE 4

### EFFECTOS DE UNA FIRMA DIGITAL

#### Artículo 19 - Requisitos de la Firma Digital

Cuando una disposición legal exige una firma o establece los efectos de no firmar un documento se cumple la norma utilizando una firma digital cuando se dan las siguientes circunstancias:

- (1) la firma digital es verificada con la clave pública designada en un certificado válido emitido por una autoridad certificadora licenciada;
- (2) la firma digital fue añadida por el signatario con la intención de firmar el mensaje o comunicación: y
- (3) el receptor no tiene conocimiento ni se le ha notificado que el signatario no cumplió con sus deberes como subscriptor o que no es el tenedor legal de la clave privada utilizada para añadir la firma digital.

Nada de lo dispuesto en esta Ley, impide que mediante disposición legal se autorice la utilización de cualquier símbolo como sustituto de la firma.

#### Artículo 20 - Firmas Digitales no Confiables

El receptor de una firma digital, salvo que se disponga otra cosa por ley o por contrato, asume el riesgo de que la firma digital sea falsificada si no toma las medidas de seguridad razonables que exigen las circunstancias. Si el receptor determina no reconocer la firma digital, deberá notificarlo inmediatamente al signatario.

#### Artículo 21 - Valor Legal del Documento Firmado Digitalmente

Se reconoce el mismo valor legal que se confiere a un escrito en papel, a un mensaje o comunicación cuando cumple con lo siguiente:

- (1) está sujeto totalmente a una firma digital; y
- (2) la firma digital es verificada con la clave pública designada en el certificado emitido por la autoridad certificadora licenciada, el cual es válido al momento en que se produce la firma digital.

Nada de lo dispuesto en esta Ley impide que cualquier mensaje, documento o expediente sea considerado como un escrito bajo otras disposiciones de ley.

#### Artículo 22 - Originales Firmados Digitalmente

Una copia de un mensaje o comunicación firmada digitalmente tiene el mismo valor legal que el original, a menos que el signatario disponga que una parte del mismo sea el original, en cuyo caso sólo esa parte será reconocida como válida.

#### Artículo 23 - Reconocimiento de la Firma

El certificado emitido por una autoridad certificadora licenciada, salvo que se disponga otra cosa por ley o por contrato, constituye un reconocimiento de una firma digital verificada con referencia la clave pública designada en el mismo, independientemente de que contenga palabras expresas de

reconocimiento o de que el signatario haya comparecido personalmente ante la autoridad certificadora cuando se registro la firma digital, si dicha firma es verificable mediante el certificado y fue añadida mientras el certificado era válido.

#### Artículo 24 - Presunciones

Al adjudicar una controversia sobre una firma digital, el tribunal debe presumir lo siguiente:

(1) que un certificado firmado digitalmente por una autoridad certificadora licenciada y publicado en un banco reconocido o que lo pone a la disposición de la autoridad certificadora o el subscriptor, es emitido por la autoridad certificadora que lo firmó digitalmente y aceptado por el subscriptor.

(2) que la información contenida en un certificado válido, según se define éste en el Artículo 2. y verificada por la autoridad certificadora, es exacta.

(3) que cuando la firma digital es verificada por la clave pública registrada es un certificado válido emitido por una autoridad certificadora licenciada:

(a) la firma digital es la firma digital del subscriptor;

(b) la firma digital fue añadida por el signatario con la intención de firmar el mensaje o comunicación: y

(c) el receptor de la firma digital no tiene conocimiento ni ha sido notificado que el signatario incumplió con su deber como subscriptor o que no es el tenedor legal de la clave privada utilizada para añadir la firma digital, y la firma digital la produjo una persona desinteresada utilizando un sistema confiable antes de sellar el registro.

#### Artículo 25 - Reconocimiento del Banco de Información

Un banco de información podrá ser reconocido presentando al Departamento una solicitud escrita, con evidencia de que reúne los requisitos que se establecen en este Artículo.

El Departamento reconocerá el banco de información si determina que cumple con lo siguiente:

(1) funciona bajo la dirección de una autoridad certificadora licenciada;

(2) posee una base de datos que contiene los certificados publicados, suspendidos o revocados, según lo dispuesto en los Artículos 14 y 15 de esta Ley, los registros de las autoridades certificadoras licenciadas, las órdenes y opiniones consultivas publicadas por el Departamento al reglamentar las autoridades certificadoras; y cualquier otra información que el Departamento determine mediante reglamento;

(3) opera mediante un sistema confiable:

(4) no contiene información que el Departamento considere que es o pueda ser falsa, inexacta o que no es confiable;

(5) contiene certificados publicados por las autoridades certificadoras para cumplir con normas de la práctica, consideradas por el Departamento, substancialmente similares o más estrictas, que las establecidas por ley.

(6) mantiene un archivo de los certificados que han suspendido o revocado o que han expirado durante por lo menos tres (3) años; y

(7) cumple con cualquier otro requisito establecido mediante reglamento por el Departamento.

El reconocimiento de un banco de información puede ser dejado sin efecto si éste lo solicita por escrito al Departamento por lo menos treinta (30) días antes del cese. El Departamento puede dejar sin efecto el reconocimiento de un banco de información si ha transcurrido la fecha de expiración establecida.

## PARTE 5

### SERVICIOS DEL GOBIERNO Y BANCO DE INFORMACION

#### Artículo 26 - Responsabilidad de los Bancos de Información

No obstante cualquier renuncia del banco de información o cualquier contrato en contrario con una autoridad certificadora o un suscriptor, el banco de información es responsable por la pérdida ocasionada a una persona que confía en la firma digital verificada por la clave pública registrada en un certificado suspendido o revocado si:

(1) la pérdida fue causada más de un (1) día después de que el banco de información recibió la solicitud para publicar el aviso de la suspensión o revocación; y

(2) el banco de información no publicó el aviso de la suspensión o revocación cuando la persona confió en la firma digital.

Un banco de información reconocido o su dueño o administrador, a menos que renuncie a ello, no es responsable de lo siguiente:

(3) publicar el aviso de la suspensión o revocación, a menos que haya recibido la solicitud para su publicación y haya transcurrido un (1) día laborable desde que fue recibida;

(4) por daño alguno conforme dispone este Artículo, en exceso de la cantidad establecida en el certificado como máximo de responsabilidad;

(5) por declaraciones en el certificado publicado por la autoridad certificadora licenciada:

(6) por registrar o divulgar con exactitud información que ha sido publicada por una autoridad certificadora licenciada o el Departamento, incluyendo información sobre la suspensión o revocación de certificado, según se dispone en esta Ley; o

(7) por divulgar información sobre una autoridad certificadora, un certificado o un suscriptor, si tal información se publica, según se dispone en esta Ley o los reglamentos del Departamento o se publica por orden del Departamento, en el ejercicio de su deber de expedir licencias y adoptar reglamentación, conforme lo dispuesto en esta Ley.

El banco de información es responsable por los daños y perjuicios, que ocasione, excluyendo daños por pérdida de ganancias, ahorros u oportunidades o por sufrimientos y angustias mentales.

## Artículo 27 - Exenciones: Confidencialidad

Ninguna entidad gubernamental revelará al público información alguna que divulgue o que pueda llevar a divulgar claves privadas, criptosistemas asimétricos o algoritmos o información que pueda perjudicar la seguridad de un certificado emitido o por emitirse.

## PARTE 6

### PENALIDADES

#### Artículo 28 - Penalidades

Toda persona que voluntariamente violare las disposiciones de esta Ley o de los reglamentos u órdenes promulgadas a su amparo, incurrirá en delito menos grave.

Artículo 29 - Se enmiendan los incisos (a) y (b) del Artículo 3 de la Ley de Núm. 5 de 8 de diciembre de 1955, según enmendada, para que se lean como sigue:

#### Artículo 3 - Definiciones

(1) "documento" es la palabra que comprenderá todo papel, libro, folleto, fotografía, película, microforma, cinta magnetofónica, mapa, dibujo, plano, cinta magnética, disco, video cinta o cualquier otro material leído por máquina y cualquier otro material informativo sin importar su forma o características físicas. Incluye también los generados de forma electrónica, aunque nunca sean impresos en papel u otro medio distinto al creado originalmente. El material bibliográfico, o de museo, adquirido para propósitos de exposición, consulta u otros relacionados y las publicaciones no están incluidos en la definición de la palabra documento.

(2) "documento público" es todo documento que se origine, conserve o reciba en cualquier dependencia del Estado Libre Asociado de Puerto Rico de acuerdo con la ley o en relación con el manejo de los asuntos públicos y que de conformidad con lo dispuesto en el Artículo 64 de esta Ley se haga conservar que se requiera conservar permanentemente o temporalmente como prueba de las transacciones o por su valor legal. Incluye aquellos producidos de forma electrónica que cumplan con los requisitos establecidos por las leyes y reglamentos...."

Artículo 30 - Se enmiendan los incisos (10), (13) y (28) del Artículo 7 de la Ley Núm. 115 de 22 de julio de 1974, según enmendada, para que se lean como siguen:

#### "DEFINICIONES"

Artículo 7 - Salvo que otra cosa resultare del contexto, las siguientes palabras y frases contenidas en el presente Código tendrán el significado que se señala a continuación:

(1)...

(2) Escrito.- Significa cualquier impreso, papel, carta, sello, escritura, documento o firma de una persona, moneda, papel moneda, fichas, tarjetas de crédito o cualquier otro símbolo o evidencia representativa de algún valor, derecho, privilegio u obligación. Incluye aquellos producidos de forma electrónica aunque nunca sean impresos en papel.

...

(13) Firma o suscripción.- Además del nombre escrito en mano propia, incluye el nombre o la marca o señal hecho a ruego de una persona, cuando dicha persona no puede escribir su nombre como testigo escribiéndose su nombre junto a tal marca o señal por otra persona que también firmará como testigo y la firma producida por medios electrónicos, según se establece por ley.

...

(28) Documento Público.- Incluirá cualquier escrito, impreso, papel, libro, folleto, fotografía, fotocopia, película, microforma, cinta magnetofónica, mapa, dibujo, plano, cinta o cualquier material leído por máquina o producido de forma electrónica aunque nunca sea impreso un papel, y cualquier otro material informativo, sin importar su forma o características físicas, que se origine, se reciba o se conserve en cualquier dependencia del Estado de acuerdo con la ley, cualquier escrito que se origine en el sector privado en el curso ordinario de transacciones con dependencias gubernamentales y que se conserven permanentemente o temporalmente en cualquier dependencia del Estado, por su utilidad administrativa o valor legal, fiscal o cultural."

Artículo 31 - Toda ley y reglamento que estén en vigor al aprobarse esta Ley deberá cumplir con lo dispuesto en esta Ley. Se concede un término de tres (3) años para que los documentos que se generen como resultado de la gestión gubernamental, sean tramitados de forma electrónica en el Gobierno de Puerto Rico, sus instrumentalidades y municipios. El Gobernador designará una Comisión, presidida por el Secretario del Departamento de Estado, compuesta por el Secretario del Departamento de Hacienda, el Director de la Oficina de Gerencia y Presupuesto, el Comisionado de Asuntos Municipales y el Presidente de la Junta Reguladora de Telecomunicaciones, un (1) representante de la Rama Judicial, nombrado por el Juez Presidente del Tribunal Supremo de Puerto Rico y dos (2) de la Rama Legislativa, nombrados por los Presidentes de los Cuerpos Legislativos y por tres (3) representantes del interés público, quienes deberán poseer conocimiento y experiencia en materia de informática o experiencia en el comercio. La Comisión tendrá la responsabilidad de supervisar y facilitar el proceso de implantación de esta Ley y tomar las medidas necesarias para ponerla en vigor. El Secretario del Departamento de Estado podrá aumentar el número de representantes de las entidades gubernamentales cuando así lo considere necesario y nombrará el personal especializado necesario para cumplir con la encomienda. La Comisión orientará a la ciudadanía sobre el sistema de firmas digitales y propiciará y establecerá la coordinación y cooperación necesaria con el sector privado.

La Comisión estará en funciones por cuatro (4) años contados a partir de la fecha de vigencia de esta Ley, pero su gestión podrá ser prorrogada por términos adicionales, a discreción del Gobernador. La primera reunión de la Comisión deberá celebrarse dentro de los tres (3) meses de entrar en vigor la Ley. La Comisión preparará un plan de trabajo y tiene el deber de informar semestralmente a la Asamblea Legislativa las gestiones realizadas y proponer aquellas modificaciones o enmiendas que considere necesarias para implantar lo dispuesto en esta Ley y alcanzar más efectivamente sus propósitos.

Artículo 32 - Esta Ley comenzará a regir inmediatamente después de su aprobación.