DEPARTAMENTO DE ESTADO

Núm. 6295
Fecha: 9 de febrero de 2001

Aprobado: Ferdinand Mercado
Secretario de Estado

Por: Secretaria Auxiliar de Servicios

ESTADO LIBRE ASOCIADO DE PUERTO RICO
DEPARTAMENTO DE ESTADO

REGLAMENTO PARA ESTABLECER LAS GUÍAS GENERALES PARA EL USO DE FIRMAS DIGITALES

INDICE

			Página
•	Guía I	Titulo	2
•	Guía II	Autoridad Legal y Propósito	2
•	Guía III	Definiciones	2
•	Guía IV	Interpretación	2
•	Guía V	Solicitud o Renovación de Licencia para Operar como Autoridad Certificadora	2
•	Guía VI	Expedición y Renovación de Licencia para Operar como Autoridad Certificadora	4
•	Guía VII	Revocación o Suspección de la Licencia de una Autoridad Certificadora	5
•	Guía VIII	Sistema Confiable	5
•	Guía IX	Certificación Sobre el Personal de Operaciones	5
•	Guía X	Requisitos de Fianza y Reclamaciones contra la Fianza	5
•	Guía XI	Contenido y Forma del Certificado	6
•	Guía XII	Archivos de la Autoridad Certificadora	7
•	Guía XIII	Cese de Operaciones de una Autoridad Certificadora	8
•	Guía XIV	Procedimiento para Reconocer Autoridades Certificadoras Localizadas fuera de la Jurisdicción de Puerto Rico	9
•	Guía XV	Auditorias Anuales a Las Entidades Certificadoras	10
•	Guía XVI	Acreditación del Auditor	10
•	Guía XVII	Reconocimiento de un Banco de Información	11
•	Guía XVIII	Revocación de Reconocimiento a un Banco de Datos	12
•	Guía XIX	Renovación de Reconocimiento de Banco de Datos	13
•	Guía XX	Expediente Manifiesto de la Autoridad Certificadora	13
•	Guía XXI	Informes de Práctica de Certificación	14
•	Guía XXII	Criterios para Determinar el Monto de las Sanciones	14
•	Guía XXII	Misceláneo	15
•	Guía XXIV	Sanciones Administrativas	15
•	Guía XXV	Procedimiento Adjudicativo	16
•	Guía XXVI	Vigencia	17

ESTADO LIBRE ASOCIADO DE PUERTO RICO
DEPARTAMENTO DE ESTADO

REGLAMENTO PARA ESTABLECER LAS GUÍAS GENERALES PARA EL USO DE FIRMAS DIGITALES

GUÍA I – TÍTULO

Este Reglamento se conocerá como "Guías Generales Para el Uso de Firmas Digitales".

GUÍA II – AUTORIDAD LEGAL Y PROPOSITO

Estas guías se promulgan al amparo de las disposiciones de la Ley Número 188 de 7 de agosto de 1998, según enmendada, conocida como la "Ley de Firmas Digitales de Puerto Rico", con el fin de facilitar la implantación de la Ley de Firmas Digitales de Puerto Rico.

GUÍA III - DEFINICIONES

3.1 A los fines de estas guías, y en adición a las definiciones contenidas en la Ley de Firmas Digitales de Puerto Rico, los siguientes términos tendrán el significado que a continuación se expresa:

(a) "Departamento de Estado" - significa el Departamento de Estado del Estado Libre Asociado de Puerto Rico.

(b) "Ley de Firmas Digitales" - significa la Ley Núm. 188 de 7 de agosto de 1998, según enmendada, conocida como "Ley de Firmas Digitales de Puerto Rico".

(c) "Nombre Cibernético" - data que identifique sin lugar a dudas a la persona natural o jurídica que utilice ese nombre.

(d) "Secretario" - significa el Secretario de Estado

GUÍA IV - INTERPRETACIÓN

Las disposiciones de estas Guías deben ser interpretadas de manera consistente con el Artículo 2 - Propósito y Política Pública - de la Ley de Firmas Digitales de Puerto Rico.

GUÍA V - SOLICITUD O RENOVACIÓN DE LICENCIA PARA OPERAR COMO AUTORIDAD CERTIFICADORA

5.1 Toda persona natural o jurídica que interese solicitar o renovar su licencia de autoridad certificadora deberá cumplir con los requisitos dispuestos en el Artículo 5 de la Ley de Firmas Digitales y lo dispuesto en estas Guías. La solicitud o renovación de licencia de autoridad certificadora deberá ***demostrar su observancia*** con la Ley de Firmas Digitales de Puerto Rico.

5.2 Toda persona natural o jurídica pagará al momento de solicitar o renovar su licencia de autoridad certificadora las siguientes cantidades:

(a) Un cargo de radicación de $500;

(b) Cualquier costo adicional incurrido por el Departamento de Estado en la contratación de cualquier contador públicos autorizado y/o abogado debidamente entrenado o acreditado como perito en seguridad de computadoras a tenor con la Guía XVI para determinar si los sistemas de computadoras y la programación (*software* y *hardware*) utilizada por la autoridad certificadora son confiables y que los mismos cumplen con los estándares nacionales e internacionales generalmente aceptados.

5.3 Todo solicitante deberá someter por escrito (cualquier documento sometido por la vía electrónica y firmado mediante una firma digital se considerará como que ha sido sometido por escrito) la siguiente información al Registro de Transacciones Comerciales y Firmas Digitales del Departamento de Estado, P.O. Box 9023271, San Juan, Puerto Rico 00902-3271.

(a) El nombre del solicitante;

(b) El número de teléfono y fax del solicitante;

(c) La dirección postal y física del solicitante;

(d) La dirección electrónica del solicitante;

(e) Nombre y dirección física y postal del agente residente del solicitante en Puerto Rico para propósitos de emplazamientos;

(f) Certificado de una autoridad certificadora que demuestre que el solicitante es un suscriptor y que está publicado en un banco de información reconocido;

(g) Declaración jurada del solicitante certificando que no se emplean como personal de operaciones a personas convictas de delito grave o delito menos grave que envuelva fraude, falsas declaraciones o engaño. En caso de que el solicitante sea una persona jurídica, la declaración jurada será suscrita por la persona autorizada por dicha persona jurídica. El solicitante será responsable de mantener en sus archivos la evidencia necesaria para demostrar que todos sus empleados cumplen con esta disposición;

(h) Registrar en el Departamento de Estado y a favor del Estado Libre Asociado una garantía o fianza por una suma no menor de $75,000. Este requisito no aplicará a aquellos funcionarios gubernamentales expresamente exentos de prestarla a tenor con al Artículo 5(d) de la Ley de Firmas Digitales. Si esta garantía o fianza es expedida por una compañía de seguros, la misma debe estar autorizada a hacer negocios en Puerto Rico por la autoridad gubernamental correspondiente. En caso de ser expedida por una institución bancaria, ésta debe igualmente estar autorizada a hacer negocios en Puerto Rico por la autoridad gubernamental correspondiente;

(i) El solicitante afirmará que posee capital de trabajo (activos corrientes - pasivos corrientes) suficiente para operar durante el año siguiente a la fecha de la solicitud. No obstante, el capital mínimo de operaciones de todo solicitante será $10,000;

(j) Reporte de auditoría a tenor con el Articulo 6 de la Ley de Firmas Digitales emitida por un contador público autorizado, un perito en seguridad de computadoras o profesional acreditado en seguridad de

computadoras a tenor con la Guía XVI de estas Guías, a los efectos de que el solicitante tiene un sistema confiable, según definido en el Artículo 3(35) de la Ley de Firmas Digitales. En casos de renovación de licencia, la opinión del auditor tiene que clasificar el cumplimiento de la autoridad certificadora como "cumplimiento total" o "cumplimiento sustancial." La licencia no será renovada si el cumplimiento de la autoridad certificadora, en la opinión del auditor, no es de "cumplimiento total" o "cumplimiento sustancial." En aquellos casos donde la opinión del auditor es de "cumplimiento sustancial," la licencia tampoco será renovada si el solicitante obtuvo en el año inmediatamente anterior a la solicitud una igual opinión de "cumplimiento sustancial." Este reporte debe certificar además que el solicitante posee procedimientos seguros para controlar y proteger el uso de su clave privada;

(k) La(s) clave[es] pública(s) del solicitante en disco ("floppy disk"). Se debe incluir además en este disco un documento firmado digitalmente por el solicitante con el cual se pueda verificar su firma;

(l) El solicitante deberá informar al Departamento de Estado de cualquier cambio en la información presentada en su solicitud. No habrá cargo alguno por radicar este tipo de enmienda a la solicitud; y

(m) El Departamento de Estado no aceptará solicitudes incompletas.

GUÍA VI - EXPEDICIÓN O RENOVACIÓN DE LICENCIA PARA OPERAR COMO AUTORIDAD CERTIFICADORA

6.1 El Departamento expedirá una licencia a la autoridad certificadora que cumpla con los requisitos establecidos en el Artículo 5 de la Ley de Firmas Digitales y esta Guía, y así lo solicite por escrito, previo el pago de los derechos requeridos. El Departamento de Estado podrá 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.

6.2 El Departamento de Estado podrá rechazar o aprobar la expedición de una licencia para operar como autoridad certificadora dentro de los próximos sesenta (60) días a la radicación de la solicitud.

6.3 Una autoridad certificadora podrá continuar operaciones como tal mientras el Departamento de Estado evalúa su solicitud de renovación de licencia. Para que aplique esta dispensa, el solicitante deberá haber radicado toda la documentación necesaria con anterioridad a la fecha de expiración de su licencia anterior. De no cumplir con este requisito, la licencia de la autoridad certificadora se considerará como vencida mientras el Departamento de Estado evalúa su solicitud de renovación.

6.4 Toda licencia emitida por el Departamento de Estado será vigente por el término de un año.

6.5 El Departamento de Estado no emitirá notificaciones a los efectos de que la licencia de una autoridad certificadora ha vencido o está próxima a vencer. Será responsabilidad de cada autoridad certificadora de radicar su solicitud de renovación con no menos de treinta (30) días con anterioridad a la fecha de expiración de su licencia.

GUÍA VII - REVOCACIÓN O SUSPENSIÓN DE LICENCIA DE AUTORIDAD CERTIFICADORA

7.1 El Departamento podrá revocar o suspender la licencia a una autoridad certificadora que no cumpla con las disposiciones de estas Guías, cuando no reúna los requisitos de la Ley de Firmas Digitales, o por incumplir con cualquier orden del Departamento de Estado según dispone el Artículo 7 de la Ley de Firmas Digitales.

7.2 El Departamento de Estado emitirá una resolución por escrito a una autoridad certificadora, enviada por correo, personalmente o mediante correo electrónico, de la decisión de revocar o suspender la licencia. La notificación indicará cuándo la revocación o suspensión entrará en vigor.

GUÍA VIII - SISTEMA CONFIABLE

Un sistema será considerado confiable si satisface sustancialmente con la versión más reciente del "Common Criteria (CC) Protection Profile (PP) for Commercial Security 2(CS2) (CCPPCS)", desarrollado por el "National Institute of Standards and Technology" (NIST). Para propósitos de estas Guías, CCPPCS será interpretado en la manera más razonable dentro del contexto en la cual un sistema es utilizado y consistente con otras leyes estatales y federales. Mientras el NIST no adopte un estándar uniforme, el estándar aplicable para propósitos de estas guías será la última versión del CCPPCS. En la alternativa se podrá determinar que un sistema es confiable si cumple con los siguientes requisitos:

(a) Acceso exclusivo de personas debidamente autorizadas;

(b) Procedimientos adecuados para restringir el acceso a la información para asuntos oficiales únicamente;

(c) Existencia de medidas adecuadas para proteger el sistema de la creación de datos falsos, alteración o destrucción de la base de datos; y;

(d) Existencia de métodos y procedimientos de operación y seguridad, tanto primarios como secundarios, en caso de emergencias tales como desastres naturales, dificultades fiscales y sabotaje. Disponiéndose, que en cualquiera de estos casos, la autoridad certificadora tendrá que notificar a toda persona que pueda resultar afectada y seguir los procedimientos enunciados en su Informe de Prácticas de Certificación.

GUÍA IX - CERTIFICACIÓN SOBRE EL PERSONAL DE OPERACIONES

La autoridad certificadora será responsable de determinar si sus empleados o personas actuando como personal operativo están cualificados para desempeñarse como tal. Esta determinación será hecha luego de investigar los antecedentes penales de cada persona y basado en el conocimiento de las responsabilidades de una autoridad certificadora bajo la Ley de Firmas Digitales, estas Guías, y cualquier otra información pertinente a criptosistemas asimétricos. Será suficiente para propósito de esta sección que la autoridad certificadora obtenga de cada empleado de operaciones, domiciliado en Puerto Rico, un certificado negativo de antecedentes penales reciente, expedido por la Policía de Puerto Rico.

GUÍA X - REQUISITOS DE FIANZA Y RECLAMACIONES CONTRA LA MISMA

10.1 Cada autoridad certificadora deberá prestar garantía o fianza a favor del

Gobierno de Puerto Rico, y sujeta a la aprobación del Secretario de Estado, por una suma no menor de $75,000.

10.2. Dicha garantía o fianza especificará que la misma estará vigente desde la fecha de efectividad de la licencia para operar como autoridad certificadora hasta su eventual expiración, cancelación o revocación;

10.3 Esta fianza responderá por las reclamaciones hechas en contra de la autoridad certificadora en los siguientes casos:

(a) La alegada violación ocurrida durante el periodo de efectividad de la licencia de la autoridad certificadora;

(b) El reclamante radicó su notificación de reclamación en el Departamento de Estado dentro de los dos años siguiente al evento que da origen a su reclamación.

10.4 Todo reclamante deberá cumplir con los siguientes requisitos para poder recobrar cantidad alguna de la fianza prestada:

(a) Radicar una notificación de reclamación ante el Departamento de Estado indicando su nombre, dirección postal, física y electrónica, cantidad reclamada, los fundamentos de hecho y de derecho por los cuales entiende que procede su reclamación y la fecha del hecho que origina su reclamación;

(b) Anejar copia certificada de la sentencia final y firme expedida por un Tribunal con jurisdicción ordenando el pago de la cantidad reclamada.

10.5 En caso de que se radique la notificación de reclamación antes de existir sentencia final y firme, el Departamento de Estado retendrá dicha notificación, sin emitir resolución alguna, hasta que el reclamante o la autoridad certificadora radique copia certificada de la sentencia final y firme que disponga finalmente de la controversia.

10.6 El Departamento de Estado eliminará de sus archivos la notificación de reclamación si de la sentencia surge que el reclamante no tiene derecho a recobrar cantidad alguna de la fianza. Si por el contrario, de la sentencia surge que el reclamante tiene derecho a recobrar de la fianza, el Departamento de Estado ordenará al fiador el pago inmediato de la cantidad correspondiente.

10.7 El Departamento de Estado notificará al fiador mediante correo certificado sobre la radicación de una notificación de reclamación y de su determinación en cuanto a la Guía X, Párrafo 10.6 de estas Guías.

10.8 El Departamento de Estado rechazará *motu proprio,* o a petición de parte interesada, cualquier notificación de reclamación hecha pasado dos años del evento que origina la reclamación.

GUÍA XI - CONTENIDO Y FORMA DEL CERTIFICADO

11.1 Cada certificado expedido por la autoridad certificadora deberá contener o incorporar por referencia lo siguiente:

(a) Indicar que el certificado se expide a tenor con estas Guías;

(b) Indicar que la autoridad certificadora que emite el certificado está debidamente autorizada por el Departamento de Estado;

(c) Número de serie del certificado, el cual debe ser único entre los certificados expedidos por la autoridad certificadora;

(d) Nombre cibernético del subscriptor;

(e) Nombre común del subscriptor;

(f) La clave publica correspondiente a la clave privada del subscriptor;

(g) Un identificador de los algoritmos para ser utilizados por la clave pública del subscriptor;

(h) La fecha y hora en que el certificado fue expedido y aceptado;

(i) La fecha y hora de expiración del certificado;

(j) El nombre cibernético de la autoridad certificadora;

(k) Un identificador de los algoritmos utilizados para firmar el certificado;

(l) El límite máximo de responsabilidad de la autoridad certificadora;

(m) El nombre cibernético del banco de información designado para la publicación de una notificación de revocación o suspensión del certificado o el método por el cual la notificación de revocación o suspensión del certificado será divulgada.

11.2 Un certificado expedido por una autoridad certificadora podrá, a opción del subscriptor y la autoridad certificadora, incluir o incorporar por referencia cualquier información adicional que autorice la autoridad certificadora.

11.3 La información contenida en el certificado será expresada en la forma y manera generalmente aceptada para el tipo de transacción por el cual el certificado será utilizado por el suscriptor.

GUÍA XII - ARCHIVOS DE LA AUTORIDAD CERTIFICADORA

12.1 Toda autoridad certificadora mantendrá archivos que demuestren lo siguiente:

(a) Posee suficiente evidencia documental para demostrar la identidad de cada persona natural o jurídica para la cual se ha expedido un certificado;

(b) Posee suficiente evidencia documental para demostrar la identidad de cada persona natural o jurídica que ha solicitado la revocación de un certificada para cada certificado revocado;

(c) Posee suficiente evidencia documental para demostrar la validez y corrección de todo la información contenida en cada certificado expedido;

(d) Posee suficiente evidencia documental para demostrar que ha cumplido con los requisitos de la ley y estas Guías en la expedición, publicación, suspensión o revocación de cada certificado según sea aplicable.

12.2 La identidad de una persona natural o jurídica en un certificado expedido por la autoridad certificadora será establecida por cualquiera de estos documentos:

(a) Documento de identidad con retrato y firma, expedido por las autoridades públicas competentes del Estado Libre Asociado de Puerto Rico, de los Estados Unidos, o de uno de los estados de la Unión, cuyo objeto sea identificar a las personas o por pasaporte debidamente expedido por autoridad competente.

(b) Documento auténtico expedido por las autoridades públicas competentes del Estado Libre Asociado de Puerto Rico, de los Estados Unidos, de uno de los estados de la Unión o autoridad extranjera, que demuestre su personalidad jurídica.

12.3 En todo caso, excepto aquellos de solicitud de suspensión de certificado, la autoridad certificadora podrá exigir del subscriptor o su mandatario que provea la evidencia necesaria para poder cumplir con esta disposición.

12.4 La autoridad certificadora conservará todos sus registros por un término de diez (10) años contados a partir de la fecha de revocación o expiración del certificado. Se exceptúa de esta disposición aquellos casos donde la autoridad certificadora ha entregado sus archivos al Departamento de Estado al cesar sus funciones.

12.5 La autoridad certificadora deberá mantener sus archivos protegidos en un lugar seguro a prueba de fuego.

GUÍA XIII - CESE DE OPERACIONES DE UNA AUTORIDAD CERTIFICADORA

13.1 Antes de cesar operaciones una autoridad certificadora deberá:

(a) Notificar por escrito su intención de cesar operaciones con noventa (90) días de anticipación al subscriptor de cada certificado vigente;

(b) Revocar todos los certificados vigentes luego de transcurrir los noventa (90) días dispuestos en el inciso anterior. La autoridad certificadora revocará los mismos sin importar que el subscriptor de éstos haya solicitado o no su revocación;

(c) Notificar por escrito a cada subscriptor cuyo certificado ha sido revocado dentro de los quince (15) días de su revocación.

13.2 A fin de proveer un servicio ininterrumpido a los subscriptores, la autoridad certificadora que cesa operaciones podrá hacer arreglos con otra autoridad certificadora para que ésta vuelva a emitir los certificados.

13.3 La autoridad certificadora tendrá que notificar por escrito al Departamento de Estado con sesenta (60) días de anticipación a la fecha del cese de sus operaciones. La notificación contendrá la siguiente información:

(a) Nombre de la autoridad certificadora;

(b) Nombre cibernético de la autoridad certificadora;

(c) Número de certificados expedidos y válidos en ese momento;

(d) La fecha del cese de operaciones;

(e) La fecha en que se notificará del cese de operaciones a los

subscriptores de cada certificado vigente;

(f) Incluir copia de la notificación a los subscriptores de cada certificado vigente;

(g) Indicar si la autoridad certificadora ha nombrado alguna entidad certificadora como su sucesora. En tal caso deberá incluir además el nombre legal y cibernético de la entidad certificadora sucesora;

(h) Si una persona natural con licencia para operar una entidad certificadora fallece durante la vigencia de su licencia, su sucesión será responsable de cumplir con lo aquí dispuesto;

(i) Si una persona natural con licencia para operar una entidad certificadora se incapacita, su tutor legal será responsable de cumplir con lo aquí dispuesto;

GUÍA XIV - PROCEDIMIENTO PARA RECONOCER AUTORIDADES CERTIFICADORAS AUTORIZADAS FUERA DE LA JURISDICCION DE PUERTO RICO

14.1 El Departamento podrá reconocer la licencia o autorización de autoridades certificadoras emitida por entidades gubernamentales de un estado de los Estados Unidos o extranjeras, siempre que los requisitos para obtener la licencia o autorización sean sustancialmente similares a los dispuestos en la Ley de Firmas Digitales. En el caso en que se reconoce la expedición de una licencia por una entidad gubernamental de un estado de los Estados Unidos o extranjera le aplicarán a los certificados las presunciones y efectos legales a los límites de responsabilidad que establece la Ley de Firmas Digitales en la misma forma en que aplican a las demás autoridades certificadoras licenciadas en Puerto Rico.

Una autoridad certificadora localizada fuera de la jurisdicción de Puerto Rico que desee que su licencia sea reconocida por el Departamento de Estado deberá así solicitarlo, por escrito, y cumplir con todos los requisitos establecidos en el Artículo 5 de la Ley de Firmas Digitales y estas Guías.

14.2 Cualquier entidad certificadora con licencia otorgada por una entidad gubernamental de un estado de los Estados Unidos o extranjera podrá actuar como tal dentro de la jurisdicción del Estado Libre Asociado de Puerto Rico solamente si cumple con uno de los siguientes requisitos:

(a) Obtiene una licencia para operar como entidad certificadora del Departamento de Estado a tenor con la Ley de Firmas Digitales y esta Guía;

(b) Radicar ante el Departamento de Estado una copia certificada de su licencia para operar como entidad certificadora expedida por una entidad gubernamental que el Secretario de Estado haya determinado que sus requisitos para expedir licencias de autoridad certificadoras se asemejan sustancialmente a los de Puerto Rico, paga el costo de radicación establecido en el registro en el Departamento de Estado y a favor del Estado Libre Asociado de Puerto Rico una garantía por una suma no menor de $25,000.

(c) Que la jurisdicción donde la autoridad certificadora esta autorizada tenga una disposición de reciprocidad para las autoridades certificadoras autorizadas bajo la Ley de Firmas Digitales.

14.3 El Secretario de Estado podrá certificar que los requisitos de licencia de otra jurisdicción son similares a los del Estado Libre Asociado de Puerto Rico si para obtener

dicha licencia sus leyes o reglamentos exigen que la autoridad certificadora cumpla con los siguientes requisitos:

(a) Los certificados expedidos son basados en claves públicas y privadas generadas por un criptosistema asimétrico dentro de un sistema confiable.

(b) Emplear personal de operaciones que cumplan con lo dispuesto en la Guía V, subsección 5.3.

(c) Estar sujeta a un andamiaje legal establecido para hacer valer los requisitos de licencia.

14.4 El Secretario de Estado publicará un listado de las jurisdicciones que ha certificado como similar para efectos de esta sección. El Secretario podrá evaluar jurisdicciones excluidas de la lista a petición de parte interesada o de la propia jurisdicción luego de recibir copia en inglés o español de la ley y reglamentos aplicables.

GUÍA XV - AUDITORIAS ANUALES A LAS ENTIDADES CERTIFICADORAS

15.1. Cada autoridad certificadora será auditada a tenor con el Artículo 6 de la Ley de Firmas Digitales emitida por un contador público autorizado, un perito de seguridad en computadoras o profesional acreditado en seguridad de computadoras a los efectos de que el solicitante tenga un sistema confiable.

15.2 El auditor emitirá su opinión sobre el cumplimiento de la autoridad certificadora con los requisitos de la Ley de Firmas Digitales y esta Guía. En aquellos casos que la autoridad certificadora sea además un banco de información reconocido, la auditoria tendrá entonces que incluir dicho banco de información reconocido.

15.3 El auditor, perito o profesional ejercerá razonablemente su juicio profesional dentro de las circunstancias para determinar la materialidad de alguna circunstancia que no cumpla estrictamente con los requisitos de la Ley de Firmas Digitales o esta Guía. Además de cualquier incumplimiento que el auditor, perito o profesional determine como material, las siguientes circunstancias serán consideradas como material:

(a) Cualquier incumplimiento con los requisitos impuestos por la Ley o esta Guía en cuanto a la validez y contenido de un certificado;

(b) La existencia de algún empleado operacional que no cumpla con las disposiciones de la sección 5.3 de esta Guía;

(c) Cualquier indicio material de que la autoridad certificadora ha utilizado un sistema que no cumple con los requisitos de sistema confiable establecidos en la Guía IX.

15.4 La entidad certificadora radicará copia del reporte de auditoría con treinta (30) días de anticipación a la fecha de renovación de su licencia. El reporte puede ser radicado electrónicamente siempre y cuando el mismo haya sido firmado digitalmente por el auditor utilizando otra entidad certificadora a la auditada y debidamente licenciada por el Departamento de Estado.

GUÍA XVI - ACREDITACIONES DEL AUDITOR, PERITO O PROFESIONAL

16.1 Las auditorias a una entidad certificadora realizadas a tenor con el Artículo 6 de la Ley de Firmas Digitales serán efectuadas por un contador público autorizado, un perito de seguridad en computadoras o profesional acreditado en seguridad de computadoras que cumpla con los siguientes requisitos:

(a) Ser contador público autorizado con licencia vigente expedida por el Departamento de Estado de Puerto Rico; o,

(b) Ser un perito de seguridad en computadoras; o,

(c) Ser un profesional en seguridad de computadoras; y,

(d) Poseer conocimientos suficientes de sistemas seguros de informática y telecomunicaciones, y procedimientos de auditoria para convalidar estos sistemas; y,

(e) Poseer conocimientos suficientes sobre la tecnología, estándares y normas generalmente aceptadas en el ámbito de firmas digitales.

16.2 Cada auditor que radique un informe de auditoria en el Departamento de Estado proveerá una declaración afirmando que cumple con los requisitos de esta sección.

GUÍA XVII - RECONOCIMIENTO DE UN BANCO DE INFORMACIÓN

17.1 El Departamento de Estado podrá reconocer un banco de información si éste cumple con los requisitos dispuestos en el Artículo 25 de la Ley de Firmas Digitales y radique una solicitud por escrito que cumpla con los siguientes requisitos:

(a) Nombre, dirección postal y física, dirección física donde se encuentran los sistemas de computadoras ("hardware") que contienen el banco de datos, número de teléfono, dirección electrónica y el nombre cibernético de la persona que radica la solicitud.

(b) Nombre, dirección postal y física, dirección electrónica y el nombre cibernético de la autoridad certificadora que opera el banco de datos.

(c) Describe detalladamente lo siguiente:

(i) Diseño e implementación de un sistema confiable en el banco de datos;
(ii) El contenido del banco de datos;
(iii) Todos los requisitos de forma aplicables al contenido del banco de datos;
(iv) Criterios para determinar quién puede publicar información en al banco de datos;
(v) Procedimientos para procesar y publicar certificados nuevos y notificaciones de suspensión y revocación de certificados;
(vi) Procedimientos para contabilizar el uso del banco de datos y el acceso a la información;
(vii) Cargos, si alguno, por accesar el expediente manifiesto de la autoridad certificadora y órdenes emitidas por el Departamento de Estado;

(d) Aceptar publicar prontamente la siguiente información:

(i) Todos los expedientes manifiestos de autoridades certificadoras publicados en el banco de datos por el Departamento de Estado.
(ii) Cualquier cambio o cancelación en los expedientes manifiestos de autoridades certificadoras publicados en el banco de datos por el Departamento de Estado.

(iii) Cualquier orden o determinación administrativa publicada en el banco de datos por el Departamento de estado.

(e) Incluir copia de todos los informes de práctica de certificación del banco de datos y su la política de archivos. Nada de lo aquí dispuesto obligará a un banco de datos a divulgar información privilegiada o secretos de negocio que pueda afectar adversamente la confiabilidad de su sistema.

(f) La autoridad certificadora que opera el banco de datos deberá certificar que mantendrá continuamente dentro de la jurisdicción del Estado Libre Asociado de Puerto Rico lo siguiente:

(i) Un agente residente quien a su vez será una persona natural residente en esta jurisdicción, una corporación doméstica o una corporación foránea debidamente autorizada a hacer negocios en Puerto Rico;

(ii) Designar un custodio de la información y archivos del banco de datos quien podrá ser emplazado o citado a tenor con las Reglas de Procedimiento Civil. El agente residente podrá ser el custodio de la información y archivo de datos.

(g) Nombre completo, dirección postal y física, dirección electrónica y número de teléfono del agente residente y el custodio de la información y archivo de datos.

(h) La autoridad certificadora notificará al Departamento de Estado de cualquier cambio en la información aquí solicitada.

(i) Incluir comprobante de rentas internas por la cantidad de $250.

GUÍA XVIII - REVOCACIÓN DE RECONOCIMIENTO A UN BANCO DE DATOS

Esta guía describe el procedimiento para revocar el reconocimiento del banco de datos sin revocar la licencia de la autoridad certificadora que lo opera.

18.1 Debido a que es un requisito estatutario que el banco de datos funcione bajo la dirección de una autoridad certificadora licenciada, el Departamento de Estado renovará automáticamente el reconocimiento a cualquier banco de datos operado por una entidad certificadora cuya licencia haya expirado o haya sido suspendida o revocada.

18.2 El Departamento de Estado podrá revocar o suspender el reconocimiento de un banco de datos por los siguientes motivos:

(a) Dejar de cumplir con cualquier requisito establecido por la Ley de Firmas Digitales o esta Guía;

(b) Incumplir con alguna orden emitida por el Departamento de Estado a tenor con la Ley de Firmas Digitales o esta Guía.

18.3 El Departamento de Estado notificará por correo certificado a la autoridad certificadora su orden de revocar su reconocimiento al banco de datos designando su fecha de efectividad. Esta notificación será dirigida a la ultima dirección conocida de la autoridad certificadora.

18.4 La parte afectada por una orden del Departamento de Estado en revocar o suspender el reconocimiento de un banco de datos tendrá derecho al procedimiento adjudicativo establecido en la sección XXV de estas Guías.

18.5 Un banco de datos que decida cesar voluntariamente sus operaciones tendrá que notificar al Departamento de Estado con treinta (30) días de anticipación y republicar sus datos en otro banco de datos reconocido por el Departamento de Estado.

GUÍA XIX - RENOVACIÓN DE RECONOCIMIENTO DE BANCO DE DATOS

19.1 A petición escrita de un banco de datos, el Departamento de Estado renovará su reconocimiento si cumple con los siguiente requisitos:

(a) Cumple con todos los requisitos de documentación y cargos impuestos por estas Guías y

(b) Cumple con todos los requisitos establecidos por la Ley de Firmas Digitales y estas Guías.

19.2 Cada renovación de reconocimiento de banco de datos será válida por un período de un año.

19.3 El Departamento de Estado no emitirá notificaciones a los efectos de que su reconocimiento ha vencido o está próxima a vencer. Será responsabilidad de cada banco de datos radicar su solicitud de renovación con no menos de treinta (30) días con anterioridad a la fecha de expiración de su reconocimiento.

19.4 La autoridad certificadora que opera el banco de datos será responsable de notificar en diez (10) días al Departamento de Estado de cualquier cambio en la información suministrada. No habrá cargo alguno por esta notificación.

GUÍA XX - EXPEDIENTE MANIFIESTO DE LA AUTORIDAD CERTIFICADORA

20.1 El Secretario de Estado preparará un expediente manifiesto de cada autoridad certificadora con la siguiente información:

(a) El expediente manifiesto indicará que es provisto por el Departamento de Estado;

(b) El nombre legal, dirección postal y física y número de teléfono y fax de la autoridad certificadora;

(c) La dirección electrónica de la autoridad certificadora;

(d) El nombre cibernético de la autoridad certificadora;

(e) Las claves públicas con las que pueda verificarse su firma digital que utiliza en los certificados;

(f) Las restricciones, si alguna, que impone en sus certificados;

(g) De ser aplicable, la fecha de revocación o suspensión de la licencia de la firma certificadora;

(h) La cantidad de la fianza prestada por la autoridad certificadora;

(i) El número de reclamaciones y la cantidad reclamada radicadas en su contra en el Departamento de Estado para recobrar de la fianza prestada;

(j) Descripción de cualquier límite legal de responsabilidad o capacidad de pago conocido por el Departamento de Estado para responder por

reclamaciones de naturaleza extracontractual;

(k) Clasificación sobre el cumplimiento con la Ley y estas Guías dada por el auditor a tenor con el Artículo 6 de la Ley en la última auditoria y la fecha de la misma;

(l) Cualquier evento que afecte la habilidad de la autoridad certificadora en realizar sus funciones o afecte la validez de sus certificados;

(m) De ser aplicable, la fecha en que un certificado que contenga la clave pública de la autoridad certificadora haya sido revocado o suspendido.

20.2 El Secretario de Estado publicará cada expediente manifiesto en su banco de datos o cualquier otro banco de datos debidamente licenciado para operar en el Estado Libre Asociado de Puerto Rico.

20.3 Cada expediente manifiesto contendrá la firma digital del Departamento de Estado.

20.4 Los expedientes manifiestos de las autoridades certificadoras serán públicos.

20.5 El Secretario de Estado utilizará la información en sus archivos para preparar el expediente manifiesto. El Secretario no estará obligado investigar más allá del contenido de la información bajo su control.

20.6 El Secretario de Estado mantendrá al día la información del expediente manifiesto según surja cualquier variación a la misma.

GUÍA XXI - INFORMES DE PRÁCTICA DE CERTIFICACIÓN

Cada autoridad certificadora radicará en el Departamento de Estado un informe de práctica de certificación. Este informe detallará las normas y prácticas utilizadas por la agencia certificadora en expedir, suspender o revocar un certificado. Deberá ademas contener la siguiente información:

(a) su dirección;

(b) el método o procedimiento para recuperarlo para su utilización;

(c) la forma y estructura del informe;

(d) la auditoría del informe;

(e) la fecha del informe.

GUÍA XXII - CRITERIOS PARA DETERMINAR EL MONTO DE LAS SANCIONES

22.1 Para determinar el monto de las sanciones a ser impuesta a una autoridad certificadora por alguna violación a la Ley o estas Guías, el Secretario podrá tomar en consideración la naturaleza y severidad de la violación. Factores a ser considerados incluyen:

(a) Los daños y perjuicios causados por la violación incluyendo lo siguiente:

(i) El impacto financiero causado a cualquier persona;

(ii) Los gastos incurridos por el Estado Libre Asociado en investigar y procesar la violación;

(b) La naturaleza de la violación, si la misma continúa o envuelve conducta criminal o afectó negativamente la confiabilidad de cualquier certificado o par de claves;

(c) La presencia de cualquier factor agravante, tales como:

(i) Que la conducta constitutiva de la violación fue intencional;
(ii) Intentar encubrir la violación;
(iii) Mentir u obstruir la investigación;
(iv) La comisión de violaciones anteriores;

(d) Factores mitigantes:

(i) Actos afirmativos para corregir la violación;
(ii) Resarcimiento a cualquier parte afectada por la violación;
(iii) La violación no fue el resultado de una conducta intencional de infringir la Ley de Firmas Digitales y estas Guías.

GUÍA XXIII - MISCELÁNEO

Cualquier persona obligada a radicar en el Departamento de Estado cualquier documento a tenor con la Ley de Firmas Digitales o estas Guías podrá hacerlo digitalmente si el mismo cumple con los requisitos establecidos en la Ley de Firmas Digitales y estas Guías.

GUÍA XXIV - SANCIONES ADMINISTRATIVAS

24.1 El Departamento de Estado podrá 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 la Ley de Firmas Digitales.

24.2 A esos efectos y a tenor con el Artículo 7 de la Ley de Firmas Digitales, el Departamento de Estado podrá revocar o suspender una licencia para operar como autoridad certificadora por los siguientes motivos:

(a) Dejar de cumplir con cualquier requisito establecido por la Ley de Firmas Digitales;

(b) Incumplir con alguna orden emitida por el Departamento de Estado a tenor con la Ley de Firmas Digitales.

24.3 El Secretario notificará a la autoridad certificadora la revocación o suspensión de su licencia por correo certificado. La notificación expresará la fecha de efectividad de la revocación o suspensión, la cual podrá ser inmediata. La notificación informará además a la autoridad certificadora de su derecho a solicitar el procedimiento adjudicativo detallado en la Guía XXV de esta Guía.

24.4. Además, podrá imponer a cualquier persona que a sabiendas o intencionalmente viole una orden, una multa administrativa 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 el 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.

GUÍA XXV - PROCEDIMIENTO ADJUDICATIVO

25.1 El Departamento de Estado podrá dilucidar cualquier controversia relacionada a todo asunto bajo su jurisdicción a tenor con la Ley de Firmas Digitales. El trámite adjudicativo deberá regirse a tenor con estas Guías y la Ley Número 170 de 12 de agosto de 1988, mejor conocida como la Ley de Procedimiento Administrativo Uniforme del Estado Libre Asociado de Puerto Rico, según enmendada (en adelante "LPAU").

25.2 El trámite adjudicativo comenzará a iniciativa propia del Secretario o mediante la presentación de una querella, solicitud o petición por escrito de parte interesada de la manera que se describe a continuación:

(a) Querellas originadas por el Departamento de Estado: El Departamento de Estado podrá radicar querellas ante el Secretario por infracciones a la Ley de Firmas Digitales o estas Guías. La querella deberá contener:

(i) El nombre y dirección postal del querellado.
(ii) Los hechos constitutivos de la infracción.
(iii) Las disposiciones legales o reglamentarias por las cuales se le imputa la violación.
(iv) Podrá contener una propuesta de multa o sanción a la que el querellado puede allanarse e informar su cumplimiento o pago, según sea el caso.

(b) Querellas originadas por una persona ajena al Departamento de Estado: Una persona interesada podrá radicar una querella ante el Departamento de Estado por infracciones a la Ley de Firmas Digitales o estas Guías. El promovente de una acción ante la agencia deberá incluir la siguiente información al formular su querella, solicitud o petición:

(i) Nombre y direcciones postales de todas las partes.
(ii) Hechos constitutivos del reclamo o infracción.
(iii) Referencia a las disposiciones legales aplicables si se conocen.
(iv) Remedio que se solicita.
(v) Firma de la persona promovente del procedimiento.

(c) La parte afectada por la decisión del Secretario relacionada a una querella originada por una persona ajena al Departamento de Estado podrá solicitar su reconsideración de la forma y manera que se expresa continuación:

(i) La parte afectada podrá radicar una solicitud de reconsideración ante el Secretario dentro de los diez días siguientes a la fecha de depósito en el correo de la notificación de resolución recurrida y exigir del Secretario de Estado la celebración de una vista administrativa.

25.3 Vista Administrativa: Toda vista administrativa se celebrará según los términos y requisitos dispuestos en la LPAU.

25.4 Orden o Resolución Final: Una orden o resolución final deberá ser emitida por escrito y bajo la firma del Secretario o su representante autorizadodentro de noventa (90) días después de concluida la vista o después de la radicación de las propuestas determinaciones de hechos y conclusiones de derecho, a menos que este término sea

renunciado o ampliado con el consentimiento escrito de todas las partes o por causa justificada. La orden deberá incluir y exponer separadamente determinaciones de hecho si éstas no se han renunciado, conclusiones de derecho, que fundamentan la adjudicación, la disponibilidad del recurso de reconsideración o revisión según sea el caso. La orden o resolución deberá ser firmada por el jefe de la agencia o cualquier otro funcionario autorizado por ley. La orden o resolución advertirá el derecho de solicitar la reconsideración o revisión de la misma, con expresión de los términos correspondientes. Cumplido este requisito comenzarán a correr dichos términos. La agencia deberá notificar a las partes la orden o resolución a la brevedad posible, por correo certificado y deberá archivar en autos copia de la orden o resolución final y de la constancia de la notificación. Una parte no podrá ser requerida a cumplir con una orden final a menos que dicha parte haya sido notificada de la misma.

25.5 Reconsideración: La parte adversamente afectada por una resolución u orden final podrá, dentro del término de veinte (20) días desde la fecha de archivo en autos de la notificación de la resolución u orden, presentar una moción de reconsideración de la resolución u orden. El Departamento de Estado deberá considerarla dentro de los quince (15) días de haberse presentado dicha moción. Si la rechazare de plano o no actuare dentro de los quince (15) días, el término para solicitar revisión judicial comenzará a correr nuevamente desde que se notifique dicha denegatoria o desde que expiren esos quince (15) días, según sea el caso. Si se tomare alguna determinación en su consideración, el término para solicitar revisión empezará a contarse desde la fecha en que se archive en autos una copia de la notificación de la resolución de la agencia resolviendo definitivamente la moción de reconsideración. Tal resolución deberá ser emitida y archivada en autos dentro de los noventa (90) días siguientes a la radicación de la moción de reconsideración. Si la agencia acoge la moción de reconsideración pero deja de tomar alguna acción con relación a la moción dentro de los noventa (90) días de ésta haber sido radicada, perderá jurisdicción sobre la misma y el término para solicitar la revisión judicial empezará a contarse a partir de la expiración de dicho término de noventa (90) días salvo que la agencia, por justa causa y dentro de esos noventa (90) días, prorrogue el término para resolver por un período que no excederá de treinta (30) días adicionales.

25.5 Revisión Judicial: Una parte adversamente afectada por la orden o resolución final podrá presentar una solicitud de revisión ante el Tribunal de Circuito de Apelaciones de la forma y manera dispuesta en la sección 3.15 de la LPAU.

GUÍA XXVI – VIGENCIA

Este Reglamento entrará en vigor a los treinta (30) días después de su radicación en el Departamento de Estado.

Aprobado, hoy 8 de febrero de 2001, en San Juan, Puerto Rico.

Ferdinand Mercado
Secretario de Estado