Al margen un sello que dice: Gobierno de Jalisco. Poder Ejecutivo. Secretaría General de Gobierno. Estados Unidos Mexicanos.

DIGELAG/ACU-087/2008
DIRECCIÓN GENERAL DE
ESTUDIOS LEGISLATIVOS Y
ACUERDOS GUBERNAMENTALES

ACUERD0 DEL CIUDADANO
GOBERNADOR CONSTITUCIONAL
DEL ESTADO DE JALISCO

Guadalajara, Jalisco, a 19 de noviembre de 2008

Emilio González Márquez, Gobernador Constitucional del Estado de Jalisco, con fundamento en los artículos 36, 46 y 50 fracciones VIII y XXV de la Constitución Política; 1, 2, 3, 5, 6, 19 fracción II, 21, 22 fracciones I y XXIV y 30 de la Ley Orgánica del Poder Ejecutivo; así como las disposiciones de la Ley de Firma Electrónica Certificada para el Estado de Jalisco y sus Municipios, todos ordenamientos de esta entidad federativa, y con base en los siguientes

CONSIDERANDOS

I. Que el artículo 50 fracción VIII de la Constitución Política del Estado de Jalisco faculta al Titular del Poder Ejecutivo a expedir los reglamentos que resulten necesarios a fin de proveer en la esfera administrativa la exacta observancia de las leyes y el buen despacho de la administración pública.

II. Que la actual dinámica de la sociedad crea la exigencia de contribuir con la generación de condiciones que permitan y garanticen incorporar, desarrollar y potenciar nuevas tecnologías en los diferentes contextos de la actividad humana. Para ello, resulta trascendental la participación de las entidades e instituciones de la administración pública y el sector privado, mediante la creación de un marco jurídico confiable que permita fomentar, promover y difundir el uso de medios electrónicos, como instrumento para optimizar los servicios técnicos, financieros y administrativos.

El uso de la firma electrónica certificada se ha constituido en muchos países como una herramienta indispensable en el desarrollo de las actividades de la administración pública y de los particulares. Es por ello, que mediante Decreto No. 21432 publicado en el Periódico Oficial "El Estado de Jalisco" el 14 de septiembre de 2006 se expidió la Ley de Firma Electrónica Certificada para el Estado de Jalisco y sus Municipios, misma que entró en vigor el 1 de enero de 2007. Dicha ley tiene por objeto regular la firma electrónica certificada y la prestación de servicios de certificación para simplificar, facilitar y agilizar los actos y negocios jurídicos, comunicaciones y procedimientos administrativos, entre las dependencias, entidades y organismos que conforman el sector público, los particulares y las relaciones que mantengan éstos entre sí.

III. Que la Ley antes mencionada señala que para efectos de creación y validez de la firma electrónica certificada existirán prestadores de servicios de certificación debidamente acreditados por la Secretaría General de gobierno, quienes serán los facultados para expedir los certificados electrónicos que avalen el uso de la firma electrónica certificada.

Para que dichos prestadores de servicios de certificación puedan ser autorizados por la Secretaría General de Gobierno, deben cumplir con una serie de requisitos generales plasmados en la ley. En virtud de ello, resulta necesario establecer de manera detallada todos y cada uno de los elementos humanos, materiales, económicos y tecnológicos que, debe tener el solicitante de la autorización como prestador de servicios de certificación, y determinar los estándares internacionales con los que debe cumplir, de tal forma, que se garantice la seguridad y confiabilidad de los certificados expedidos, así como la confidencialidad de los datos proporcionados por los particulares al solicitar la expedición, de un certificado electrónico.

IV. Que a través del Reglamento que ahora se propone se adicionan una serie de obligaciones que tiene que cumplir el prestador de servicios de certificación con la finalidad de garantizar al titular del

certificado electrónico la seguridad del uso del mismo, el conocimiento de las condiciones precisas para su utilización, sus limitaciones y la forma en que garantiza su posible responsabilidad; y proporcionar al destinatario, medios de acceso que le permitan determinar la identidad del Prestador de Servicios de Certificación, que los datos de creación de la firma electrónica eran válidos en la fecha en que se expidió el certificado, si existe un medio para que el firmante dé aviso de que los datos de creación de la firma electrónica han sido de alguna manera controvertidos, entre otros. Esto genera mayor seguridad tanto para el firmante como para el destinatario de un mensaje de datos.

V. Que, de igual forma, resulta indispensable regular la operación de los prestadores de servicios de certificación, los mecanismos mediante los cuales dichos prestadores garantizarán el cumplimiento de sus obligaciones, el procedimiento mediante el cual la Secretaría General de Gobierno realizará visitas de verificación e inspección para comprobar la subsistencia del cumplimiento de los requisitos exigidos a los prestadores para otorgarles su autorización, el procedimiento que deberá seguirse en caso de terminación o cese de las actividades del prestador de servidos de certificación; así como las sanciones que les serán aplicadas por las omisiones o actuaciones que realicen en contravención a la Ley y al presente Reglamento.

Por lo anteriormente expuesto y fundado, tengo a bien emitir el siguiente

ACUERDO

ARTÍCULO ÚNICO.- Se expide el Reglamento de la Ley de Firma Electrónica Certificada para el Estado de Jalisco y sus Municipios, para quedar como sigue:

REGLAMENTO DE LA LEY DE FIRMA ELECTRÓNICA CERTIFICADA PARA EL ESTADO DE JALISCO Y SUS MUNICIPIOS

CAPÍTULO I
Disposiciones Generales

Artículo 1. El presente ordenamiento tiene por objeto regular el uso de medios electrónicos y firma electrónica certificada, así como establecer las normas reglamentarias a las que deben sujetarse los Prestadores de Servicios de Certificación, de conformidad con la Ley de Firma Electrónica Certificada para el Estado de Jalisco y sus Municipios.

Artículo 2. Para los efectos del presente Reglamento se entenderá por:

l. Certificado electrónico: el documento firmado electrónicamente por el prestador de servicios de certificación que vincula datos de verificación de firma electrónica al firmante y confirma su identidad;

II. Datos de creación de firma electrónica o clave privada: las claves criptográficas, datos o códigos únicos que genera el firmante de manera secreta para crear y vincular su firma electrónica;

III. Datos de verificación de firma electrónica o clave pública: las claves criptográficas, datos o códigos únicos que utiliza el destinatario para verificar la autenticidad de la firma electrónica del firmante;

IV. Destinatario: la persona que recibe el mensaje de datos que envía el firmante como receptor designado; por este último con relación a dicho mensaje;

V. Dispositivo de creación de firma electrónica: el programa o sistema informático que sirve para aplicar los datos de creación de firma electrónica;

VI. Dispositivo de verificación de firma electrónica; el programa o sistema informático que sirve para aplicar los datos de verificación de firma electrónica;

VII. Fecha electrónica: los datos que en forma electrónica son utilizados para constatar la fecha y hora en que un mensaje de datos es enviado por el firmante y es emitido un acuse de recibo por el destinatario;

VIII. Firma electrónica certificada: los datos que en forma electrónica son vinculados o asociados a un mensaje de datos y, que corresponden inequívocamente al firmante con la finalidad, de asegurar la integridad y autenticidad del mismo y que ha sido certificada por un prestador de servicios de certificación debidamente autorizado ante la Secretaría;

IX. Firmante: la persona que posee los datos de creación de firma electrónica;

X. Intermediario: la persona que envía o recibe un mensaje de datos a nombre de un tercero o bien que preste algún otro servicio con relación a dicho mensaje;

XI Ley: la Ley de Firma Electrónica Certificada para el Estado de Jalisco y sus Municipios;

XII. Medios electrónicos: los dispositivos tecnológicos utilizados para transmitir o almacenar datos e información, a través de computadoras, líneas telefónicas, enlaces dedicados, microondas o de cualquier otra tecnología;

XIII. Mensaje de datos: la información generada, enviada, recibida, archivada, reproducida o procesada por el firmante y recibida o archivada por el destinatario a través de medios electrónicos, ópticos o cualquier otra tecnología;

XIV. Prestador de servicios de certificación: la persona física o jurídica, notario público, dependencia, entidad pública o unidad administrativa que preste servicios relacionados con la firma electrónica certificada y que expide, administra, revoca y renueva certificados electrónicos, así como valida, aprueba y rechaza solicitudes de certificados electrónicos, previa autorización otorgada por la Secretaría;

XV. Reglamento: el presente Reglamento;

XVI. Secretaría: la Secretaría General de Gobierno del Estado de Jalisco a través de la Dirección de Firma Electrónica;

XVII. Sistema de información: el sistema utilizado para generar, enviar, recibir, archivar o procesar un mensaje de datos;

XVIII. Tercera parte confiada: persona o entidad pública que consulta el listado de los certificados electrónicos, así como el estado de los mismos, a través de los medios autorizados por la Secretaría; y

XIX. Titular: la persona a favor de quien se expide un certificado de firma electrónica.

Artículo 3. La Secretaría aceptará cualquier método o sistema para crear una firma electrónica o certificado electrónico, y promoverá que éstos puedan concurrir o funcionar con diferentes equipos y programas de cómputo, de conformidad con el principio de neutralidad tecnológica establecido en la Ley.

Artículo 4. La Secretaría elaborará una relación de los Prestadores de Servicios de Certificación acreditados o suspendidos y de las personas físicas o jurídicas que actúen en su nombre. La relación deberá contener también a las personas físicas que formen parte del personal de los sujetos antes señalados.

La Secretaría deberá mantener actualizada y disponible dicha relación para todos los usuarios, lo que podrá hacer a través de la página web de la Secretaría.

CAPÍTULO II
De los Requisitos y del Trámite de Acreditación

Artículo 5. Los interesados en obtener la autorización de la Secretaría como Prestador de Servicios de Certificación deberán:

I. Presentar, previo pago de derechos correspondiente, la solicitud de acreditación por escrito ante la Secretaría;

II. Tener domicilio legal o sucursal en el Estado de Jalisco;

III. Adjuntar a la solicitud, según corresponda, lo siguiente:

a) En caso de los notarios, copia certificada de la patente, título de habilitación o documento que en términos de la legislación de la materia les acredite estar en ejercicio de la fe pública;

b) En caso de las personas jurídicas, copia certificada de su acta constitutiva u otro instrumento público, que acredite su constitución de acuerdo con las leyes mexicanas y que dentro de su objeto social tenga alguna de las siguientes actividades:

1. Verificar la identidad de los titulares y su vinculación con los dispositivos de verificación de firma electrónica y certificado electrónico;

2. Comprobar la integridad y suficiencia del Mensaje de Datos del solicitante;

3. Llevar a cabo registros de los elementos de identificación de los Firmantes y de aquella información con la que haya verificado el cumplimiento de fiabilidad de las Firmas Electrónicas Certificadas y expedir el Certificado electrónico; y

4. Cualquier otra actividad no incompatible con las anteriores;

c) En caso de las personas físicas, copia del documento que acredite su actividad empresarial, constancia de inexistencia de antecedentes penales que acredite no haber sido condenado por delitos en contra del patrimonio que merezca pena privativa de la libertad; y

d) En caso de las dependencias y entidades públicas estatales o municipales, así como sus unidades administrativas, copia del instrumento jurídico de su creación;

IV. Comprobar que se cuenta con los elementos señalados en el artículo 22 fracción II de la Ley, de conformidad con lo establecido por el artículo 6 del presente Reglamento;

V. Contar con procedimientos claros y definidos de conformidad con lo establecido por el presente Reglamento;

VI. Adjuntar a la solicitud una carta suscrita por cada persona física que pretenda operar o tener acceso a los sistemas que utilizará en caso de ser acreditado, donde dicha persona manifieste, bajo protesta de decir verdad y advertido de las penas en que incurren los que declaran falsamente ante una autoridad distinta a la judicial, de que no fue condenado por delito contra el patrimonio de las personas y mucho menos, inhabilitado para el ejercicio de la profesión o para desempeñar un puesto en el servicio público, en el sistema financiero o para ejercer el comercio;

VII. Acreditar que tienen la posibilidad de contar con una póliza de fianza por el monto y condiciones que se determinan en el presente Reglamento; y

VIII. Acompañar a su solicitud, escrito de conformidad para ser sujeto de revisión por parte de la Secretaría en todo momento, para que ésta verifique el cumplimiento de los requisitos para obtener y mantener la acreditación como Prestador de Servicios de Certificación.

Cuando el interesado pretenda que los datos de creación de firma electrónica certificada permanezcan en resguardo fuera del territorio del estado de Jalisco, deberá solicitarlo a la

Secretaría. En este caso, el interesado manifestará por escrito su conformidad de asumir los costos que impliquen a la Secretaría el traslado de su personal para efectuar sus revisiones; y

IX. Registrar ante la Secretaría su Certificado, en los términos que establece el presente Reglamento.

Artículo 6. La Secretaría tendrá por satisfechos los elementos humanos, materiales, económicos y tecnológicos a que se refieren los artículos 22 fracción II de la Ley y 5 fracción IV del presente Reglamento, cuando el solicitante acredite cuando menos, lo siguiente:

I. Humanos:

a) Un profesionista jurídico que deberá cumplir con los siguientes requisitos:

1. Ser licenciado en derecho o abogado con título y cédula profesional registrado en la Dirección de Profesiones del Estado;

2. Demostrar al menos dos años de experiencia en materia notarial o en materia mercantil y servicios, procedimientos o actividades relacionadas con la acreditación de la personalidad;

3. Acreditar al menos un año de experiencia comprobable en actividades relacionadas con cualquier área del derecho informático o comercio electrónico;

4. Cumplir con el requisito establecido en el artículo 22 fracción IV de la Ley;

5. Comprobar que conoce la operación como usuarios de los sistemas informáticos que habrá de utilizar el Prestador de Servicios de Certificación;

5 (sic). Presentar la solicitud de examen para encargado de identificación correspondiente, mismo que aplicará la Secretaría dentro de los veinte días siguientes a la presentación de la solicitud para la autorización como Prestador de Servicios de Certificación; este requisito no será aplicable en el caso de notarios y dependencias y entidades públicas;

b) Un profesionista informático que deberá ser licenciado o ingeniero en el área informática o carrera afín, con título y cédula profesionales debidamente registrados; comprobar al menos dos años de experiencia en el campo de seguridad informática, incluyendo los datos de las empresas o instituciones y fechas en las que adquirió la experiencia, sus cargos y las actividades y funciones desempeñadas; deberá contar con diploma en seguridad informática o, en su caso, tener alguna certificación en esta área; así como cumplir con el requisito establecido en el artículo 22 fracción IV de la Ley; y

c) Cinco auxiliares de apoyo informático consistentes en un oficial de seguridad, un administrador de sistemas, un operador de sistemas, un administrador de bases de datos y un administrador de redes. Dicho personal deberá ser técnico, licenciado o ingeniero en área informática o en carrera afín; tener experiencia comprobable en el área de informática de cuando menos cuatro años incluyendo los datos de las empresas o instituciones y fechas en las que adquirió la experiencia, sus cargos y las actividades y funciones desempeñadas, así como las cartas de las empresas o instituciones públicas en donde la haya adquirido; acreditar al menos una certificación en manejo de software o hardware referente a seguridad informática; así como cumplir con el requisito establecido en el artículo 22 fracción IV de la Ley.

II. Materiales: Espacio físico apropiado para la actividad, controles de seguridad, accesos y perímetros de seguridad física, medidas de protección, así como con las políticas necesarias para garantizar la seguridad del área. El solicitante anexará a su solicitud un documento que se denominará "Política de Seguridad Física" a que se sujetará la prestación del servicio y que deberá mantener actualizado, el cual contemplará y desarrollará, por lo menos, los siguientes conceptos:

a) Control de acceso físico;

b) Medidas, procedimientos y prácticas de seguridad;

c) Protección y recuperación ante desastres;

d) Protecciones contra robo, forzamiento y entrada no autorizada a los espacios físicos;

e) Medidas de protección en caso de incendio, sismo, inundación, explosiones, desórdenes civiles y otras formas de desastres naturales, contra fallas de servicios eléctricos o de telecomunicaciones; y

f) Un procedimiento de actualización para autorización de acceso al personal a las áreas restringidas.

La seguridad física propuesta por el solicitante deberá ser compatible con las normas y criterios internacionales;

III. Económicos: Capital que comprenderá al menos el equivalente a una cuarta parte de la inversión requerida para cumplir con los elementos humanos, tecnológicos y materiales, y un seguro de responsabilidad civil cuyo monto será de cincuenta veces el salario mínimo general diario vigente en la Zona Metropolitana de Guadalajara correspondiente a un año. Este requisito no será aplicable para las dependencias y entidades públicas; y

IV. Tecnológicos: Consistentes en:

a) Documento denominado "Análisis y Evaluación de Riesgos y Amenazas" que desarrolle los siguientes aspectos:

1. Identificación de riesgos e impactos que existen sobre las personas y los equipos, así corno recomendaciones de medidas para reducirlos;

2. Implementación de medidas de seguridad para la disminución de los riesgos detectados;

3. Proceso de evaluación continua para adecuar la valoración de riesgos a condiciones cambiantes del entorno;

4. Determinar un proceso equivalente o adoptar el descrito en los documentos siguientes: "Risk Management Guide for Information Technology Systems, Special Publication 800-30, Recommendations of the Nacional Institute of Standards and Technology, October 2001", "Handbook 3, Risk Management, Version 1, Australian Communications Electronic Security Instruction 33 (ACSI 33)", o aquellos que les sustituyan; e

5. Impacto que sufrirá el negocio en caso de interrupciones no planificadas.

b) Infraestructura informática: deberá incluir una autoridad certificadora y una autoridad registradora; depósitos para datos de creación de firma electrónica del prestador de servicios de certificación y su respaldo, certificados y listas de certificados revocados (LCR) basadas en un servicio de Protocolo de Acceso de Directorio de Peso Ligero (LDAP) o equivalente y un Protocolo de Estatus de Certificados en Línea (OCSP); procesos de administración de la infraestructura; un manual de política de certificados; una declaración de prácticas de certificación; y los manuales de operación de las autoridades certificadora y registradora;

c) Equipo de cómputo y software: el solicitante deberá contar, por lo menos, con un servidor de misión crítica para la autoridad certificadora y la autoridad registradora, contemplando otro servidor de las mismas características para redundancia por seguridad; un servidor de misión crítica, contemplando redundancia por seguridad, para LDAP, LCR y OCSP; una computadora para almacenar el sistema de administración de la infraestructura que se opera; un sistema de sello o estampado de tiempo para disertar, fecha y hora de emisión de los certificados, con las especificaciones establecidas en el artículo 17 del presente Reglamento; un enlace mínimo de 512 kilo bytes, contemplando redundancia con un enlace de al menos 256 bytes a Internet; un ruteador,

contemplando redundancia por seguridad; un cortafuegos, (firewall), contemplando redundancia por seguridad; un sistema de monitoreo de red; un sistema confiable de antivirus; herramienta confiable de detección de vulnerabilidades; sistemas confiables de detección y protección de intrusión; y las computadoras personales e impresoras necesarias para la prestación del servicio;

d) Política de Seguridad de la Información: la cual deberá constar por escrito y cumplir con los siguientes requisitos:

1. Ser congruente con el objeto del solicitante;

2. Los objetivos de seguridad determinados deberán ser claros, generales, no técnicos y resultado del Análisis y Evaluación de Riesgos y Amenazas;

3. Estar basada en las recomendaciones del estándar ISO 17799 sección tres;

4. Tener manuales de política general y los necesarios para establecer políticas específicas;

5. Deberán identificarse los objetivos de seguridad relevantes y las amenazas potenciales relacionadas a los servicios suministrados, así como las medidas a tomar para evitar y limitar los efectos de tales riesgos y amenazas, con base en el Análisis y Evaluación de Riesgos y Amenazas;

6. Describir las reglas, directivas y procedimientos que indiquen cómo son provistos los servicios y las medidas de seguridad asociadas;

7. Señalar el periodo de revisión y evaluación de la Política de Seguridad;

8. Ser consistentes con la Declaración de Prácticas de Certificación y con la Política de certificados; y

9. Incluir un proceso similar al descrito en: Internet Security Policy: a Technical Guide, by the National Institute of Standards and Technology (NIST).

e) Plan de Continuidad del Negocio y Recuperación ante Desastres: se deberá elaborar un plan que describa cómo actuará el Prestador de Servicios de Certificación en caso de interrupciones del servicio. El plan será mantenido y probado periódicamente, asimismo, describirá los procedimientos de emergencia a seguir en al menos los siguientes casos:

1. Afectación al funcionamiento de software en el que se basarán los servicios del Prestador de Servicios de Certificación;

2. Incidente de seguridad que afecte la operación del sistema en el que se basan los servicios del Prestador de Servicios de Certificación;

3. Robo de los datos de creación de firma electrónica del Prestador de Servicios de Certificación;

4. Falla de los mecanismos de auditoría;

5. Falla en el hardware donde se ejecuta el producto en el que se basarán los servicios del Prestador de Servicios de Certificación; y

6. Mecanismos para preservar evidencia del mal uso de los sistemas.

El plan deberá ser compatible con las normas y criterios internacionales y al menos con los lineamientos descritos en el estándar ISO 17799 o el estándar ETSITS 102 042, o los que les sustituyan. De igual forma, el plan deberá ser coherente con los niveles de riesgo determinados en el Análisis y Evaluación de Riesgos y Amenazas y seguirá un proceso similar al descrito en: NIST ITL Bulletin June 2002, Contingency Planning Guide for Information Systems; NIST Special

Publication 800-34, Contingency Planning Guide for Information Systems, June 2002; y NIST Special Publication 800-30 Risk Management Guide, u otros textos posteriores equivalentes.

f) Plan de Seguridad de Sistemas: este plan, coherente con la Política de Seguridad de la Información, describirá los requerimientos de seguridad de los sistemas y de los controles a implantar y cumplir, así como las responsabilidades y acceso de las personas a los sistemas. El plan incorporará:

1. La política de seguridad de la información, seguridad organizaciónal, control y clasificación de activos, administración de operaciones y comunicaciones, control de accesos, desarrollo y mantenimiento de sistemas, seguridad del personal y seguridad ambiental y física que sean compatibles con los señalados por la norma ISO 17799;

2. Los mecanismos y procedimientos de seguridad propuestos que se aplicarán en todo momento;

3. La forma en que se garantizará el logro de los objetivos de la Política de Certificados y la Declaración de Prácticas de Certificación, la cual debe de ser compatible, por lo menos, con las secciones 4 a 10 del estándar ISO 17799, o las que le sustituyan. En caso de claves criptográficas, la manera en que se efectuará su administración; y

4. Las medidas de protección del depósito público de certificados y de información privada obtenida durante el registro.

g) Estructura de Certificados: La estructura de datos del Certificado debe ser compatible con el estándar ISO/IEC 9594-8, además de contener los datos establecidos en el artículo 11 de la Ley para ser considerados como válidos.

Los algoritmos utilizados para la firma electrónica deben ser compatibles con los estándares de la industria RFC 3280. Internet X509 Public Key Infraestructure Certificate and Certificate Revocation List (CRL) Profile, o los que les sustituyan que provean un nivel adecuado de seguridad tanto para la firma del Prestador de Servicios de Certificación como del usuario.

El tamaño de las claves utilizadas para la generación de una firma electrónica, deberá proveer el nivel de seguridad de 1024 bits para los usuarios y de 2048 bits para los Prestadores de Servicios de Certificación. Deberán utilizar funciones hash conforme a estándares de la industria, actuales y que provean el adecuado nivel de seguridad para este tipo de firmas.

Contendrán referencia o información suficiente para identificar o localizar uno o más sitios de consulta donde se publiquen las notificaciones de revocación de los certificados.

h) Estructura de la lista de Certificados Revocados: deberá ser compatible con la última versión del estándar ISO/IEC 9594-8 o la que le sustituya, e incluir por lo menos la siguiente información:

1. Número de serie de los certificados revocados por el emisor con fecha y hora de revocación;

2. La identificación del algoritmo de firma utilizado;

3. El nombre del emisor;

4. La fecha y hora en que fue emitida la Lista de Certificados Revocados;

5. La fecha en que emitirá la próxima Lista de certificados Revocados que no podrá exceder de veinticuatro horas, con independencia de mantener el Protocolo de Estatus de Certificados en Línea (OCSP); y

6. La Lista de Certificados Revocados deberá ser firmada por el Prestador de Servicios de Certificación que la haya emitido, con sus Datos de Creación de Firma.

i) Sitio electrónico: se deberá señalar un sitio electrónico de alta disponibilidad con mecanismos redundantes o alternativos de conexión y de acceso público a través de Internet que permitirá a los usuarios consultar los certificados emitidos de forma remota, continua y segura compatible con el estándar ISO/IEC 9594-8 o el que le sustituya, a efecto de garantizar la integridad y disponibilidad de la información ahí contenida. En dicho sitio se incluirá la Política de Certificados y la Declaración de Prácticas de Certificación.

j) Procedimientos que informen de las características de los procesos de creación y verificación de firma electrónica, así como aquellos que aplicarán para dejar sin efecto definitivo los certificados.

k) Política de Certificados: ésta debe asegurar su concordancia con la Declaración de Prácticas de Certificación y los procedimientos operacionales, será pública, tendrá que ser compatible por lo menos con el estándar ETSI TS 102 042 o el que le sustituya y deberá establecer bajo qué circunstancias se puede revocar un certificado y quienes pueden solicitarlo.

Deberá indicar a quién se le puede otorgar un certificado y cómo se aplicará el proceso de registro, que se deberá verificar en forma fehaciente la identidad del usuario y deberá describir la forma en que se precisarán los propósitos, objetivos y alcances del certificado y sus limitaciones. Asimismo, se deberán establecer las obligaciones que contrae el Prestador de Servicios de Certificación y el usuario en la emisión y utilización del certificado.

l) Declaración de Prácticas de Certificación: la cual deberá ser compatible por lo menos con el estándar ETSI TS 102 042 y el RFC 36470 o el que le sustituya, y determinará lo siguiente:

1. Los procedimientos de operación para otorgar certificados y el alcance de aplicación de los mismos;

2. Las responsabilidades y obligaciones del Prestador de Servicios de Certificación y de la persona a identificar. Particularmente desarrollará aquellas inherentes a la emisión, revocación y expiración de certificados;

3. La vigencia de los certificados, y, una vez otorgada la acreditación por la Secretaría, la fecha de inicio de operaciones;

4. El método de verificación, de identidad del usuario que se utilizará para la emisión de los certificados;

5. Procedimientos de protección de confidencialidad de la información de los solicitantes;

6. Un procedimiento para registrar la fecha y hora de todas las operaciones relacionadas con la emisión de un Certificado y conservarlas de manera confiable;

7. Los procedimientos que se seguirán en los casos de suspensión temporal o definitiva del Prestador de Servicios de Certificación y la forma en que la administración de los certificados emitidos pasarán al Archivo de Instrumentos Públicos o a otro Prestador de Servicios de Certificación;

8. Las medidas de seguridad adoptadas para proteger los datos de creación de firma electrónica; y

9. Los controles que se utilizarán para asegurar que el propio usuario genere sus datos de la creación de firma electrónica, autenticación de usuarios, emisión de certificados, revocación de certificados, auditoría y almacenamiento de información relevante.

m) Modelo Operacional de la Autoridad Certificadora: dicho modelo deberá contener la siguiente información:

1. Cuáles son los servicios prestados, cómo se interrelacionan los diferentes servicios, en qué lugares se operará, qué tipos de certificados se entregarán, si se generarán certificados con

diferentes niveles de seguridad, cuáles son las políticas y procedimientos de cada tipo de certificado y cómo se protegerán los activos;

2. Un resumen que incluya el contenido del documente, la historia del Prestador de Servicios de Certificación y las relaciones comerciales con proveedores de insumos o servicios para sus operaciones;

3. Interfaces con las autoridades registradoras;

4. Implementación de elementos de seguridad;

5. Procesos de administración;

6. Sistema de directorios para los certificados;

7. Procesos de auditoría y respaldo;

8. Bases de datos a utilizar; y

9. Requerimientos de seguridad física del personal, de las instalaciones y del módulo criptográfico.

n) Modelo Operacional de la Autoridad Registradora: dicho modelo deberá contener la siguiente información:

1. Cuáles son los servicios de registro que se prestarán, en qué lugares se ofrecerán dichos servicios y qué tipos de certificados generados por la autoridad Certificadora se entregarán;

2. Interfaces con la autoridad certificadora;

3. Implementación de dispositivos de seguridad;

4. Procesos de administración;

5. Procesos de auditoría y respaldo;

6. Bases de datos a utilizar;

7. Privacidad de datos;

8. Descripción de la seguridad física de las instalaciones;

9. Método para proveer de una identificación unívoca del usuario y el procedimiento de uso de los datos de creación de firma electrónica; y

10. Los mecanismos para que el propio usuario genere en forma privada y segura sus datos de creación de firma electrónica y la inclinación al usuario del grado de fiabilidad de los mecanismos y dispositivos utilizados; y

ñ) Plan de administración de claves: se definirá este plan conforme al cual se generarán, protegerán y administrarán las claves criptográficas. El mismo tendrá que ser compatible, por lo menos, con el estándar ETSI TS 102 042 sección 7.2 o el que le sustituya. El plan deberá desarrollar los siguientes apartados:

1. Claves de la Autoridad Certificadora;

2. Almacenamiento, respaldo; recuperación y uso de los datos de creación de firma electrónica de la autoridad certificadora del Prestador de Servidos de Certificación;

3. Distribución del certificado de la Autoridad Certificadora;

4. Administración del ciclo de vida del hardware criptográfico que utilice la Autoridad Certificadora;

5. Dispositivos seguros para los usuarios; y

6. Dispositivos seguros para almacenar los datos de creación de firma electrónica, compatibles como mínimo con el estándar FIPS-140 nivel 3 en sus elementos de seguridad e implantación de los algoritmos criptográficos estándares, o el que le sustituya.

Los procedimientos implantados de acuerdo a este plan deberán garantizar la seguridad de las claves en todo momento, aun en caso de cambios de personal o componentes tecnológicos.

Artículo 7. Los notarios podrán solicitar la autorización a través de personas jurídicas, conforme a lo que establezca la legislación que les rige. En ningún caso se les eximirá de la responsabilidad individual, ni aun cuando para obtener la acreditación compartan la infraestructura que les permita prestar los servicios de certificación.

Artículo 8. La obtención de la autorización como Prestador de Servicios de Certificación se realizará conforme al siguiente procedimiento:

I. La Secretaría, una vez recibida la solicitud, previo el pago de derechos correspondientes, revisará y evaluará la información y documentación recibida; así como visitará el domicilio señalado por el interesado a efecto de llevar a cabo una revisión para comprobar los requisitos para obtener la acreditación como Prestador de Servicios de Certificación.

Cuando de la revisión detecte la falta de cualquiera de los requisitos señalados en la Ley y en este Reglamento, dentro de los veinticinco días hábiles siguientes a la recepción de la solicitud prevendrá al interesado por escrito y por una sola ocasión, para que subsane la omisión dentro del término de veinte días hábiles contados a partir de su notificación.

Transcurrido dicho plazo sin que sea desahogada la prevención se desechará el trámite;

II. La Secretaría podrá, durante todo el proceso, solicitar documentación adicional y realizar visitas a las instalaciones del interesado para comprobar el cumplimiento de los requisitos establecidos; y

III. La Secretaría resolverá en un plazo no mayor a sesenta días hábiles contados a partir de la presentación de la solicitud, la procedencia o no de otorgar la autorización como Prestador de Servicios de Certificación, en caso contrario se tendrá por no concedida.

CAPÍTULO III
De la Operación

SECCIÓN PRIMERA
Del Inicio de Operaciones

Artículo 9. Para efectos del artículo 22 fracción V de la Ley, previo al otorgamiento de la autorización y al inicio de operaciones como Prestadores de Servicios de Certificación, los interesados contarán con un plazo de diez días hábiles, a partir de que se haya resuelto la procedencia de la autorización, para obtener de compañía debidamente autorizada una fianza a favor de la Secretaría de Finanzas, la cual deberá presentarse ante la Secretaría. El monto de la fianza será de acuerdo a lo siguiente:

l. En caso de notarios, el equivalente a cinco mil días de salario mínimo general diario vigente en la Zona Metropolitana de Guadalajara; y

II. En caso de personas jurídicas, el resultante de multiplicar cinco mil veces el salario mínimo general diario vigente en la Zona Metropolitana de Guadalajara por cada persona física de su

personal o integrante de persona jurídica distinta que se contemple para efectos del artículo 16 fracción I del presente Reglamento.

Lo anterior no será aplicable para las dependencias y entidades públicas.

Artículo 10. La Secretaría, una vez que reciba la fianza, expedirá, previo el pago de derechos correspondiente, la autorización respectiva al interesado y lo registrará a efecto de que éste pueda iniciar operaciones.

El titular de la Secretaría publicará en el Periódico Oficial "El Estado de Jalisco" las autorizaciones que otorgue, dentro de los treinta días siguientes al otorgamiento de la autorización.

Artículo 11. El Prestador de Servicios de Certificación deberá mantener la fianza vigente y actualizada en los casos siguientes:

I. Durante todo el periodo en que opere y el año siguiente a su cese;

II. Cuando sea sancionado con suspensión temporal; y

III. Si se hubiere iniciado procedimiento administrativo o judicial en su contra, hasta que concluya el mismo.

Lo anterior deberá consignarse expresamente en la póliza de fianza.

Artículo 12. La fianza que otorgue el Prestador de Servicios de Certificación se podrá hacer efectiva cuando éste cause daños o perjuicios a los usuarios de sus servicios por incumplimiento de sus obligaciones o por el indebido desempeño de sus funciones. Su monto también se aplicará para cubrir los gastos que erogue la Secretaría a través del Archivo de Instrumentos Públicos, por actuar en sustitución del Prestador de Servicios de Certificación, cuando éste sea sancionado con suspensión o cancelación de su autorización.

Artículo 13. El Prestador de Servicios de Certificación, una vez que haya cumplido con lo señalado en esta sección, deberá notificar por escrito a la Secretaría la fecha en que inicie su actividad, misma que podrá efectuarse dentro de los quince días naturales siguientes al comienzo de dicha actividad.

Artículo 14. La Secretaría, como autoridad certificadora y registradora, deberá comprobar la identidad del Prestador de Servicios de Certificación o su representante, para que éste pueda generar sus Datos de Creación de Firma Electrónica.

Artículo 15. El Prestador de Servicios de Certificación o su representante no podrán revelar los Datos de Creación de Firma Electrónica que correspondan a su propio Certificado y; en todo caso, serán responsables de su mala utilización. Dicho Certificado tendrá una vigencia de diez años.

Artículo 16. El Prestador de Servicios de Certificación tendrá, además de las obligaciones establecidas en el artículo 23 de la Ley, las siguientes:

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

II. Informar a la persona que solicite sus servicios, antes de la expedición de un certificado, los costos, las condiciones precisas para la utilización del mismo, sus limitaciones de uso y, en su caso, la forma en que garantiza su posible responsabilidad;

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

IV. En caso de cesar su actividad deberán comunicarlo a la Secretaría a fin de determinar el destino que se dará a sus registros y archivos; y

V. Proporcionar medios de acceso que permitan al Destinatario determinar:

a) La identidad del Prestador de Servicios de Certificación;

b) Que el firmante nombrado en el Certificado tenía bajo su control el dispositivo y los datos de creación de la firma electrónica en el momento en que se expidió el Certificado;

c) Que los datos de creación de la firma electrónica eran válidos en la fecha en que se expidió el certificado;

d) El método utilizado para identificar al firmante;

e) Cualquier limitación en los fines o el valor respecto de los cuales puedan utilizarse los datos de creación de la firma electrónica o el certificado;

f) Cualquier limitación en cuanto al ámbito o el alcance de la responsabilidad indicada por el Prestador de Servicios de Certificación;

g) Si existe un medio para que el firmante dé aviso al Prestador de Servicios de Certificación de que los datos de creación de la firma electrónica han sido de alguna manera controvertidos; y

h) Si se ofrece un servicio de terminación de vigencia del certificado.

SECCIÓN SEGUNDA
De los Certificados

Artículo 17. El Prestador de Servicios de Certificación deberá proporcionar a la Secretaría su dirección electrónica, la que deberá incluir en cada Certificado que expida para verificar en forma inmediata su validez, suspensión o revocación.

Esta dirección se utilizará por la Secretaría para agregarla a un dominio propio de consulta en línea, a través del cual el Destinatario podrá cerciorarse del estado que guarda cualquier certificado emitido por un Prestador de Servicios de Certificación.

Artículo 18. Para los efectos del artículo 11 fracción V de la ley, los datos del Prestador de Servicios de Certificación que contendrán los certificados que se expidan incluirán al menos:

I. El nombre, denominación o razón social y domicilio del Prestador de Servicios de Certificación; y

II. La dirección electrónica donde podrá verificarse la lista de certificados revocados.

El Prestador de Servicios de Certificación deberá notificar a la Secretaría cualquier cambio que pretenda efectuar respecto de los datos a que se refiere el presente artículo.

Artículo 19. Para efectos del artículo 11 fracción II de la ley, la fecha y hora de emisión del certificado se determinará conforme a lo siguiente:

l. El Prestador de Servicios de Certificación deberá llevar un registro del Sistema de Sello o Estampado de Tiempo que se sincronizará con el de la Secretaría, para asegurar la fecha y la hora de la emisión de los certificados generados;

II. El Sistema de Sello o Estampado de Tiempo deberá cumplir por lo menos con el estándar internacional Internet X.509 Public Key Infrastructure Time Stamp y considerar el RFC 3161; y

III. El Sistema de Sello o estampado de tiempo podrá ser del propio Prestador de Servicios de Certificación o de una persona física o jurídica que lo lleve en nombre y por cuenta del mismo.

Artículo 20. La emisión, registro y conservación de los certificados por parte de los Prestadores de Servicios de Certificación se efectuará dentro del territorio del estado de Jalisco.

Artículo 21. La Secretaría podrá autorizar el resguardo de los Datos de Creación de Firma Electrónica del Prestador de Servicios de Certificación fuera del territorio del estado de Jalisco. En este caso, el Prestador de Servicios de Certificación asumirá los costos que impliquen a la Secretaría el traslado de sus servidores públicos para efectuar las visitas de verificación a que se refiere la sección V de este Reglamento.

SECCIÓN TERCERA
Del Reconocimiento de Certificados y Firmas Electrónicas Nacionales y Extranjeros

Artículo 22. Todo certificado expedido fuera del estado de Jalisco producirá los mismos efectos jurídicos en el mismo que un certificado expedido en dicha entidad federativa si presenta un grado de fiabilidad equivalente a los contemplados por la Ley y el presente Reglamento.

A efectos de determinar si un certificado o una firma electrónica presentan un grado de fiabilidad equivalente para los fines del párrafo anterior, se tomarán en consideración las normas internacionales reconocidas por el estado de Jalisco y cualquier otro medio de convicción pertinente, que será validado por los prestadores de servicios de certificación autorizados por la Secretaría.

SECCIÓN CUARTA
Del Domicilio, Objeto Social y Estatutos de los Prestadores de Servicios de Certificación

Artículo 23. Los Prestadores de Servicios de Certificación deberán dar aviso a la Secretaría dentro de los quince días siguientes de cualquier cambio de domicilio o modificaciones a su objeto social o estatutos, a efecto de que ésta verifique la continuidad en el cumplimiento de los requisitos exigidos para obtener la autorización.

SECCIÓN QUINTA
De las Verificaciones

Artículo 24. La Secretaría realizará visitas de verificación al Prestador de Servicios de Certificación para vigilar el cumplimiento de la Ley y el presente Reglamento, las cuales se desahogarán en los términos previstos por la Ley del Procedimiento Administrativo del Estado de Jalisco y sus Municipios, y se practicarán de oficio o a petición del Titular del Certificado, del Firmante o del Destinatario.

SECCIÓN SEXTA
Del cese de actividades de los Prestadores de Servicios de Certificación

Artículo 25. Cuando un prestador de servicios de certificación haya sido sancionado o haya cesado el ejercicio de sus actividades de manera voluntaria, previo pago de derechos, su archivo y registro quedarán temporalmente en resguardo del Archivo de Instrumentos Públicos, hasta en tanto no se determine a qué prestador de servicios de certificación le serán transferidos.

La Secretaría tomará las medidas necesarias que garanticen, en beneficio de los usuarios, la continuidad del servicio materia del presente Reglamento.

CAPÍTULO IV
De las Sanciones

Artículo 26. Las sanciones previstas en el presente capítulo se aplicarán sin perjuicio de las demás responsabilidades en que pueda incurrir el Prestador de Servicios de Certificación o su personal.

Artículo 27. La Secretaría sancionará con suspensión temporal de uno hasta cuatro meses en el ejercicio de sus funciones al Prestador de Servicios de Certificación que:

I. Omita determinar y hacer del conocimiento de los usuarios si las firmas electrónicas que les ofrecen cumplen o no con los requerimientos dispuestos en el artículo 9 de la Ley;

II. Deje de cumplir con alguno de los requisitos señalados en las fracciones II a IV y VI del artículo 22 de la Ley;

III. Actúe en contravención a los procedimientos definidos y específicos para la tramitación de un certificado;

IV. No permita que se efectúe la consulta inmediata sobre la validez, suspensión o revocación de los certificados que emita; o

V. No informe, antes de la emisión de un certificado, a la persona que solicite sus servicios, de su precio, de las condiciones precisas para la utilización del mismo, de sus limitaciones de uso y, en su caso, de la forma en que garantiza su posible responsabilidad.

Artículo 28. La Secretaría sancionará al Prestador de Servicios de Certificación con suspensión temporal de cuatro y hasta seis meses en el ejercicio de sus funciones cuando:

I. Reincida en cualquiera de las conductas u omisiones a que se refiere el artículo anterior;

II. Cambie su domicilio, objeto social o estatutos sin dar aviso previo a la Secretaría, dentro del plazo previsto en el artículo 23 del presente Reglamento;

III. Omita notificar a la Secretaría la iniciación de la prestación de servicios de certificación dentro de los quince días naturales siguientes al comienzo de dicha actividad;

IV. Omita poner a disposición del firmante los dispositivos de generación de los datos de creación y de verificación de la firma electrónica; u

V. Omita proporcionar los medios de acceso al certificado que permitan al destinatario determinar las situaciones o circunstancias a que se refiere el artículo 16 fracción V del presente Reglamento.

Artículo 29. La Secretaría sancionará al Prestador de Servicios de Certificación con suspensión temporal de seis meses y hasta un año en el ejercicio de sus funciones cuando:

I. Reincida en cualquiera de las conductas a que se refiere el artículo anterior;

II. No cuente con fianza vigente por el monto y condiciones que, se determinan en este Reglamento;

III. Provoque la nulidad de un acto jurídico por su negligencia, imprudencia o dolo en la expedición de un certificado; y

IV. Omita notificar a la Secretaría cualquier cambio que pretenda efectuar respecto de los datos a que, se refiere el artículo 18 del presente Reglamento.

Artículo 30. La Secretaría sancionará con cancelación de la autorización al Prestador de Servicios de Certificación cuando:

I. Reincida en cualquiera de las conductas a que se refiere el artículo anterior;

II. No compruebe la identidad de los solicitantes y cualesquiera circunstancias pertinentes para la emisión de un certificado;

III. Proporcione documentación o información falsa para obtener la acreditación como Prestador de Servicios de Certificación;

IV. Altere, modifique o destruya los certificados que emita sin que medie resolución de la Secretaría o de autoridad judicial que lo ordene;

V. Emita, registre o conserve los certificados que expida, fuera del territorio del Estado de Jalisco;

VI. Impida a la Secretaría efectuar las revisiones a que se refiere la Ley y este Reglamento; o

VII. Difunda sin autorización la información que le ha sido confiada o realice cualquier otra conducta que vulnere la confidencialidad de la misma.

Artículo 31. Cuando la Secretaría suspenda a un Prestador de Servicios de Certificación en sus funciones, deberá publicar un extracto de la resolución en el Periódico Oficial "El Estado de Jalisco", a efecto de que cualquier usuario verifique en todo momento si un Prestador de Servicios de Certificación puede o no ejercer su función.

Asimismo, la Secretaría deberá revocar su correspondiente autorización, ya sea de manera temporal o definitiva.

TRANSITORIO

ÚNICO. El presente Reglamento entrará en vigor al día siguiente de su publicación en el Periódico Oficial "El Estado de Jalisco".

Así lo resolvió el Ciudadano Gobernador Constitucional del Estado, ante el Ciudadano Secretario General de Gobierno, quien lo refrenda.

EMILIO GONZÁLEZ MÁRQUEZ
Gobernador Constitucional del Estado
(rúbrica)

LIC. FERNANDO ANTONIO GUZMÁN PÉREZ PELÁEZ
Secretario General de Gobierno
(rúbrica)

REGLAMENTO DE LA LEY DE FIRMA ELECTRÓNICA CERTIFICADA PARA EL ESTADO DE JALISCO Y SUS MUNICIPIOS

EXPEDICIÓN: 19 DE NOVIEMBRE DE 2008.

PUBLICACIÓN: 27 DE NOVIEMRE DE 2008. SECCIÓN II.

VIGENCIA: 28 DE NOVIEMBRE DE 2008.