

SECRETARIA DE ECONOMIA

REGLAS generales a las que deberán sujetarse los prestadores de servicios de certificación.

Al margen un sello con el Escudo Nacional, que dice: Estados Unidos Mexicanos.- Secretaría de Economía.

FERNANDO DE JESUS CANALES CLARIOND, Secretario de Economía, con fundamento en lo dispuesto por los artículos 102 inciso A) fracción V, 104 fracciones IV y VI, 105 y 113 del Código de Comercio, artículos 2o., 3o. primer párrafo, 4o. fracciones IV y V, 5o. segundo párrafo, 6o. segundo párrafo, 9o., 10 fracción III, 11, 12, y 16 fracción III del Reglamento del Código de Comercio en materia de Prestadores de Servicios de Certificación, y

CONSIDERANDO

Que el Plan Nacional de Desarrollo 2001-2006 establece que dentro del proceso de globalización corresponde al Estado promover las condiciones para la inserción competitiva de México en el nuevo orden económico mundial. Por lo que se promoverán todas las reformas necesarias para que la economía funcione mejor, los mercados sean más eficaces y se reduzca el poder de mercado de monopolios y oligopolios. Asimismo se buscará aumentar y extender la competitividad del país, la competitividad de las empresas, la competitividad de las cadenas productivas y la competitividad de las regiones. Lo anterior implica regulación apropiada, disponibilidad oportuna y eficaz de infraestructura económica para el desarrollo, fomento de capacidades para el trabajo productivo de clase mundial, desarrollo tecnológico y científico para la nueva economía; todo ello en el marco de una moderna cultura laboral y empresarial;

Que el Decreto por el que se reforman y adicionan diversas disposiciones del Código de Comercio en Materia de Firma Electrónica, publicado en el **Diario Oficial de la Federación** el 29 de agosto de 2003, en el capítulo III que se adiciona denominado: "De los Prestadores de Servicios de Certificación", determina que la Secretaría de Economía coordinará y actuará como autoridad certificadora, y registradora, respecto de los Prestadores de Servicios de Certificación a los que se refiere dicho capítulo, en ese mismo capítulo se señala que la Secretaría de Economía tiene que determinar algunos de los requisitos y obligaciones solicitados en el Código de Comercio, y

Que el Reglamento del Código de Comercio en materia de Prestadores de Servicios de Certificación, publicado en el **Diario Oficial de la Federación** el 19 de julio de 2004, señala que los elementos humanos, materiales, económicos y tecnológicos, así como el monto y condiciones de la fianza y demás procedimientos con los que tiene que cumplir el Prestador de Servicios de Certificación, serán determinados por la Secretaría de Economía, he tenido a bien expedir las siguientes:

REGLAS GENERALES A LAS QUE DEBERAN SUJETARSE LOS PRESTADORES DE SERVICIOS DE CERTIFICACION

1. En la aplicación de las presentes Reglas Generales se estará a las definiciones a que se refiere el artículo 89 del Código de Comercio y se entenderá por Reglamento al Reglamento del Código de Comercio en materia de Prestadores de Servicios de Certificación.

2. Conforme a lo dispuesto por el artículo 102 inciso A) fracciones II y III del Código de Comercio y la fracción III del artículo 5 del Reglamento, la Secretaría tendrá por satisfechos los elementos humanos, materiales, económicos y tecnológicos y procedimientos a que se refieren dichas disposiciones, por parte de un Solicitante de Acreditación como Prestador de Servicios de Certificación, en adelante el Solicitante de Acreditación, y por un Prestador de Servicios de Certificación ya acreditado, en los términos siguientes:

2.1.- Elementos humanos

Los profesionales jurídico e informático, serán responsables de aprobar el plan de continuidad del negocio que señalan las presentes Reglas Generales. El grado académico, los cursos con los que deben contar los profesionales jurídico, informático, así como el personal auxiliar del profesional informático y los requisitos que deben cumplir serán al menos los siguientes:

2.1.1. El profesional jurídico deberá:

2.1.1.1. Ser licenciado en derecho o abogado con título y cédula profesional registrados en la Secretaría de Educación Pública;

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

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

2.1.1.4. Cumplir con el requisito establecido en el artículo 102 inciso A) fracción IV del Código de Comercio y el artículo 5 fracción V del Reglamento;

2.1.1.5. Comprobar que conoce la operación como usuarios de los sistemas informáticos que habrá de utilizar el Solicitante de Acreditación y el Prestador de Servicios de Certificación, y

2.1.1.6. Solicitud de examen para encargado de identificación correspondiente, mismo que aplicará la Secretaría dentro de los cuarenta y cinco días siguientes a la presentación de la solicitud del Solicitante de Acreditación, previa notificación de fecha, hora y lugar en el que se aplicará el mismo.

2.1.1.7. Los requisitos de los apartados del 2.1.1.2. al 2.1.1.5. podrán acreditarse con declaración ante fedatario público en la cual el profesionista jurídico manifieste bajo protesta de decir verdad y advertido de las penas en que incurrirán los que declaran falsamente ante una autoridad distinta a la judicial, que cumple con cada uno de los requisitos y que incluya los datos de las empresas o instituciones y fechas en las que adquirió la experiencia, sus cargos y las actividades y funciones desempeñadas.

2.1.2. El profesional informático deberá:

2.1.2.1. Ser licenciado o ingeniero en área Informática o afín, con título y cédula profesional registrados en la Secretaría de Educación Pública;

2.1.2.2. Comprobar al menos dos años de experiencia en el campo de seguridad informática con declaración ante fedatario público en la cual el profesionista informático manifieste bajo protesta de decir verdad y advertido de las penas en que incurrirán los que declaran falsamente ante una autoridad distinta a la judicial, que cumple con la misma y que incluya los datos de las empresas o instituciones y fechas en las que adquirió la experiencia, sus cargos y las actividades y funciones desempeñadas. Además, deberá contar con diploma en seguridad informática o, en su caso, tener alguna certificación en esta área como: "GIAC Gold Standard Certificates (GGSC), GIAC Security Leadership Certificate (GSLC), CISSP Certification y SSCP Certification" o equivalentes, y

2.1.2.3. Cumplir con el requisito establecido en el artículo 102 inciso A) fracción IV del Código de Comercio y el artículo 5 fracción V del Reglamento.

2.1.3. El Personal Auxiliar del Profesional Informático estará conformado por:

2.1.3.1. Un Oficial de Seguridad;

2.1.3.2. Un administrador de sistemas;

2.1.3.3. Un operador de sistemas;

2.1.3.4. Un administrador de bases de datos, y

2.1.3.5. Un administrador de redes.

2.1.3.6. El personal indicado en los apartados 2.1.3.2 a 2.1.3.5 deberán:

2.1.3.6.1. Ser técnico, licenciado o ingeniero en área Informática o afín;

2.1.3.6.2. Tener experiencia comprobable en el área de informática de cuando menos cuatro años, con declaración ante fedatario público en la cual el personal auxiliar del profesionista informático, a excepción del Oficial de Seguridad manifiesten cada uno bajo protesta de decir verdad y advertido de las penas en que incurrir los que declaran falsamente ante una autoridad distinta a la judicial, que cumple con la misma y que incluya 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;

2.1.3.6.3. Comprobar experiencia en el campo de la seguridad informática de cuando menos dos años, con declaración ante fedatario público en la cual el personal auxiliar del profesionista informático, a excepción del Oficial de Seguridad manifiesten cada uno bajo protesta de decir verdad y advertido de las penas en que incurrir los que declaran falsamente ante una autoridad distinta a la judicial, que cumple con la misma y que incluya 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.

2.1.3.6.4. Acreditar al menos una certificación en manejo de software o hardware referente a seguridad informática.

2.1.3.7. El Oficial de Seguridad será responsable del diseño, implantación, cumplimiento de los procedimientos y prácticas de seguridad en las instalaciones y deberá acreditar:

2.1.3.7.1. Los requisitos exigidos en el apartado 2.1.2.

2.1.3.8. A partir del inicio de operaciones en los términos previstos por el Reglamento, el Prestador de Servicios de Certificación deberá contar y notificar a la Secretaría, en un plazo no mayor a seis meses, que cuenta con la totalidad del personal auxiliar del profesional informático, salvo el caso del Oficial de Seguridad que deberá estar designado desde el momento de la solicitud de acreditación y podrá ser el propio Profesional Informático.

2.1.4. La Secretaría, a efecto de verificar los conocimientos y habilidades de los elementos humanos de un solicitante de acreditación o de un Prestador de Servicios de Certificación, podrá requerir los exámenes que se hayan aplicado a dicho personal. Asimismo, en el caso del profesional informático y sus auxiliares se constatará que la elaboración y alcance de dichos exámenes sea compatible con el estándar ISO 17799, además en el caso del Oficial de Seguridad deberá ser compatible con el estándar ETSI TS 102 042.

2.1.5. El Solicitante de Acreditación y el Prestador de Servicios de Certificación, presentará y mantendrá actualizado ante la Secretaría, el procedimiento que utilizarán para reclutar, seleccionar, evaluar y contratar al personal a que se refieren las presentes Reglas Generales, el cual deberá describir la forma de corroborar los antecedentes del personal antes de contratarlo.

2.1.6. El Prestador de Servicios de Certificación deberá suscribir con el personal que maneje información confidencial un contrato de confidencialidad que se extienda más allá de la vigencia del contrato laboral del empleado o de servicios en caso de una empresa externa.

2.2.- Elementos Materiales y sus procedimientos:

En atención al dinamismo del avance tecnológico y la necesidad de preservar la seguridad física y lógica en la prestación del servicio de certificación, los elementos materiales que deberán estar en disposición del Solicitante de Acreditación y del Prestador de Servicios de Acreditación y los procedimientos aplicables en este ámbito, deberán contener como mínimo las características siguientes:

2.2.1. Las áreas y los servicios en los cuales se maneja información confidencial requerirán procedimientos de controles de acceso, deberán estar supervisados continuamente, a efecto de reducir al mínimo los riesgos.

2.2.2. Las implantaciones de los controles deberán evitar riesgo, daño o pérdida, de los activos, alteración o sustracción de información.

2.2.3. Los accesos físicos a las áreas de generación de certificados, gestión de revocación de certificados y área de residencia de servidores, deberán estar protegidas con puertas y muros sólidos y firmes, chapas seguras, controles de acceso, sistemas de extinción de incendios y alarmas de seguridad, y se encontrarán limitados sólo al personal autorizado mediante controles de autenticación de por lo menos dos factores para asegurar que no habrán accesos no autorizados. Los servicios compartidos por otra entidad distinta al Prestador de Servicios de Certificación o por personal de éste no dedicado al servicio de certificación, deberán estar fuera del perímetro de seguridad.

2.2.4. El acceso de visitas a las áreas con información confidencial deberá ser autorizado por el Oficial de Seguridad. El visitante deberá portar una credencial en todo momento para identificarse. Se deberá registrar toda actividad que realice el visitante con la fecha y hora de ingreso y salida.

2.2.5. Un documento que se denominará “Política de Seguridad Física”, a que se sujetará la prestación del servicio, el cual será presentado por el Solicitante de Acreditación con su solicitud y que el Prestador de Servicios de Certificación deberá mantener actualizado. El documento denominado “Política de Seguridad Física” deberá contemplar y desarrollar por lo menos los siguientes aspectos:

2.2.5.1. Control de acceso físico;

2.2.5.2. Protección y recuperación ante desastres;

2.2.5.3. Protecciones contra robo, forzamiento y entrada no autorizada a los espacios físicos;

2.2.5.4. Medidas de protección en caso de incendio, contra fallas de servicios eléctricos o de telecomunicaciones, y

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

2.2.6. Las áreas seguras deben ser oficinas cerradas dentro del perímetro de seguridad física, contener mobiliario con gabinetes y chapas seguras.

2.2.7. Para la selección y el diseño de áreas seguras se debe tomar en cuenta la posibilidad de daños por fuego, sismo, inundación, explosiones, desórdenes civiles, y otras formas de desastres naturales y causadas por el hombre.

2.2.8. Todos los servicios claves deberán situarse alejados de las áreas de acceso y atención al público.

2.2.9. Los dispositivos como fax y fotocopiadoras deberán ubicarse dentro de las áreas seguras que así lo requieran, siempre bajo control para no comprometer la seguridad ni la confidencialidad de la información.

2.2.10. Todo material de desecho deberá ser destruido sin posibilidad de recuperación antes de desecharlo.

2.2.11. Las puertas y ventanas deberán estar siempre cerradas y aseguradas, instalando protecciones internas o externas en las mismas.

2.2.12. Deberá contarse con sistemas de detección de intrusión física en puertas y ventanas del perímetro de seguridad. Aquellas salas desocupadas que estén dentro del perímetro de seguridad, deberán tener activado el sistema de detección de intrusos todo el tiempo.

2.2.13. La gestión de los servicios de procesamiento de información deberá estar físicamente separada del resto de los servicios.

2.2.14. Deberán establecerse procedimientos y prácticas de seguridad para el personal dentro del perímetro de seguridad, que contemplen por lo menos lo siguiente:

2.2.14.1. El personal deberá conocer y entender los procedimientos y prácticas de seguridad dentro del perímetro de seguridad;

2.2.14.2. Las áreas vacías deberán cerrarse y revisarse periódicamente llevando una bitácora de tal revisión;

2.2.14.3. El personal de soporte que no es parte del personal del Solicitante de Acreditación o del Prestador de Servicios de Certificación, deberá acceder a las áreas restringidas sólo en caso necesario y si es autorizado por el Profesional Informático o el Oficial de Seguridad, además de ser acompañado por personal que sí lo esté;

2.2.14.4. No se deberá permitir dentro del perímetro de seguridad equipo de grabación, audio o video, con excepción del propio equipo de seguridad; y de comunicaciones.

2.2.14.5. Las actividades sin supervisión dentro de las áreas seguras deberán definirse para evitar problemas de seguridad, y prevenir actividades contrarias al servicio;

2.2.14.6. La recepción de insumos y la salida de basura deberán estar controladas y separadas del área de procesamiento de la información, para evitar accesos no autorizados;

2.2.14.7. Los requerimientos de seguridad para las áreas de atención a clientes se determinarán a partir del Análisis y Evaluación de Riesgos y Amenazas a que se refieren las presentes Reglas Generales;

2.2.14.8. El personal que acceda a las áreas externas de recepción de insumos y de desechos deberá estar controlado. Se deberá contar con los mecanismos que impidan que el personal no autorizado acceda a través de estas áreas al perímetro de seguridad;

2.2.14.9. Los procedimientos y prácticas para inspeccionar el material que ingrese, en busca de potenciales peligros antes de ser trasladados desde las áreas externas a las áreas de uso;

2.2.14.10. El equipo instalado deberá estar protegido para reducir las amenazas;

2.2.14.11. Contar con respaldo de sistemas no interrumpible de energía eléctrica, y con planta de energía eléctrica de emergencia para asegurar la continuidad del servicio de certificación;

2.2.14.12. El cableado eléctrico y de datos de los servicios de información confidencial deberá ser compatible con los estándares vigentes en la materia y protegidos contra daños e intervenciones;

2.2.14.13. Las líneas eléctricas no deberán interferir el funcionamiento del cableado de datos;

2.2.14.14. Contar con el personal o los contratos de mantenimiento requerido para garantizar la continua disponibilidad e integridad de los equipos, de acuerdo a las especificaciones y periodos recomendados por los fabricantes;

2.2.14.15. Evitar que equipos, información y software salgan de los perímetros de seguridad sin autorización.

2.2.14.16. Evitar que el equipo portátil contenga información confidencial. Si hay alguna razón que justifique equipos portátiles que contengan información confidencial o procesos críticos de la operación o información de los usuarios de los certificados, éstos nunca deberán salir del perímetro de seguridad designado;

2.2.14.17. Evitar que los equipos sean reutilizados o queden en desuso conteniendo información confidencial;

2.2.14.18. Los discos duros, disquetes y demás medios de almacenamiento de información magnético u óptico que ya no se utilicen deberán ser destruidos antes de salir del perímetro de seguridad;

2.2.14.19. Establecer un mecanismo para registrar el mal funcionamiento, fallas, mantenimientos preventivos y correctivos, de los equipos sensibles para la operación del servicio;

2.2.14.20. Adoptar la política de “escritorio limpio y pantalla limpia” enfocados a evitar riesgos de acceso no autorizado, pérdidas o daños a la información durante o fuera del horario de trabajo, y

2.2.15. La Seguridad Física propuesta por el Solicitante de Acreditación y el Prestador de Servicios de Certificación, deberá ser compatible con las normas y criterios internacionales y al menos con el estándar ETSI TS 102 042 -sección 7.4.4 Physical and Environment security- e ISO/IEC 17799 sección 7.

2.3.- Elementos económicos:

Los elementos económicos con que deberá contar el Solicitante de Acreditación y el Prestador de Servicios de Certificación comprenderán al menos:

2.3.1. El seguro, cuyo monto aplicable para cada año será determinado por la Secretaría con base en un análisis de las operaciones comerciales y mercantiles en las que sean utilizados los Certificados, monto que se dará a conocer mediante publicación en el **Diario Oficial de la Federación**.

2.4.- Elementos tecnológicos y sus procedimientos.

Los elementos tecnológicos y sus procedimientos garantizarán la continuidad del servicio, por lo que deberán ser compatibles con las normas y criterios internacionales, en atención a lo siguiente:

2.4.1. Análisis y Evaluación de Riesgos y Amenazas.

El Solicitante de Acreditación o el Prestador de Servicios de Certificación deberá elaborar un documento denominado Análisis y Evaluación de Riesgos y Amenazas, en el que desarrolle los apartados y aspectos que a continuación se indican:

2.4.1.1. Realizar un estudio que identifique los riesgos e impactos que existen sobre las personas y los equipos, así como recomendaciones de medidas para reducirlos;

2.4.1.2. Implementación de medidas de seguridad para la disminución de los riesgos detectados o riesgos mínimos;

2.4.1.3. Proceso de evaluación continua para adecuar la valoración de riesgos a condiciones cambiantes del entorno, y

2.4.1.4. 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 National 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.

2.4.2. Infraestructura informática:

Deberá incluir al menos lo siguiente:

2.4.2.1. Una Autoridad Certificadora;

2.4.2.2. Una Autoridad Registradora;

2.4.2.3. 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);

2.4.2.4. Los procesos de administración de la Infraestructura;

2.4.2.5. Un manual de Política de Certificados;

2.4.2.6. Una Declaración de Prácticas de Certificación, y

2.4.2.7. Los manuales de operación de las Autoridades Certificadora y Registradora.

2.4.3. Equipo de cómputo y software:

2.4.3.1. Por lo menos un servidor de misión crítica para la Autoridad Certificadora y la Autoridad Registradora, contemplando otro servidor de las mismas características para redundancia por seguridad.

2.4.3.2. Un servidor de misión crítica, contemplando redundancia por seguridad, para LDAP, LCR y OCSP.

2.4.3.3. Una computadora para almacenar el sistema de administración de la Infraestructura que se opera.

2.4.3.4. Un Sistema de Sello o Estampado de Tiempo, para insertar fecha y hora de emisión de los certificados, con las especificaciones y en los términos del apartado 7 de las presentes Reglas.

2.4.3.5. Un dispositivo de alta seguridad que sea compatible con el estándar FIPS-140 nivel 3, contemplando redundancia por seguridad, para almacenar los Datos de Creación de Firma Electrónica del Prestador de Servicios de Certificación.

2.4.3.6. Un enlace mínimo de 512 Kilo Bytes, contemplando redundancia con un enlace de al menos 256 Kilo Bytes a Internet.

2.4.3.7. Un ruteador, contemplando redundancia por seguridad.

2.4.3.8. Un muro de fuego (firewall), contemplando redundancia por seguridad.

2.4.3.9. Un sistema de monitoreo de red.

2.4.3.10. Un sistema confiable de antivirus.

2.4.3.11. Herramientas confiables de detección de vulnerabilidades.

2.4.3.12. Sistemas confiables de detección y protección de intrusión.

2.4.3.13. Las computadoras personales e impresoras necesarias para la prestación del servicio.

2.4.4. Política de seguridad de la información.

La Política de Seguridad deberá constar por escrito y cumplir con los siguientes requisitos:

2.4.4.1. Ser congruente con el objeto del Prestador de Servicios de Certificación;

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

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

2.4.4.4. Contar con los manuales de Política General y los necesarios para establecer políticas específicas;

2.4.4.5. Con base en el Análisis y Evaluación de Riesgos y Amenazas 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;

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

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

2.4.4.8. Ser consistente con la Declaración de Prácticas de Certificación y con la Política de Certificados a que se refieren las presentes Reglas Generales, y

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

2.4.5. Plan de Continuidad del Negocio y Recuperación ante Desastres.

2.4.5.1. El Solicitante de Acreditación y el Prestador de Servicios de Certificación deberán elaborar y presentar un Plan de Continuidad del Negocio y Recuperación ante Desastres, que describa cómo actuará en caso de interrupciones del servicio. El Plan deberá ser mantenido y probado periódicamente, y describir los procedimientos de emergencia a seguir en al menos los siguientes casos:

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

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

2.4.5.1.3. Robo de los Datos de Creación de Firma Electrónica del Prestador de Servicios de Certificación;

2.4.5.1.4. Falla de los mecanismos de auditoría;

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

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

2.4.5.2. En el Análisis y Evaluación de Riesgos y Amenazas se considerará el impacto que sufrirá el negocio, en caso de interrupciones no planificadas.

2.4.5.3. El Plan de Continuidad del Negocio y Recuperación ante Desastres deberá ser compatible con las normas y criterios internacionales, al menos con los lineamientos descritos en el estándar ISO 17799 sección 11 o el estándar ETSI TS 102 042 sección 7.4.8, o los que les sustituyan. Además 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.

2.4.6. Plan de Seguridad de Sistemas.

Los solicitantes de acreditación o los Prestadores de Servicios de Certificación deberán contar con un Plan de Seguridad de Sistemas coherente con la Política de Seguridad de la Información, que describa los requerimientos de seguridad de los sistemas y de los controles a implantar y cumplir; así como delinear las responsabilidades y acceso de las personas a los sistemas.

2.4.6.1. El Plan de Seguridad de Sistema incorporará:

2.4.6.1.1. La Política de Seguridad de la Información, seguridad organizacional, control y clasificación de activos, administración de operaciones y comunicaciones, control de accesos, desarrollo y mantenimiento de sistemas, seguridad del personal, seguridad ambiental y física que sean compatibles con los señalados por la norma ISO 17799;

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

2.4.6.1.3. La forma en que se garantizará el logro de los objetivos de la Política de Certificados y la Declaración de Prácticas de Certificación. En caso de claves criptográficas, la manera en que se efectuará su administración, y

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

2.4.6.2. Implantación del Plan de Seguridad de Sistemas.

2.4.6.2.1. El Solicitante de Acreditación y el Prestador de Servicios de Certificación, verificarán que operaciones, procedimientos y mecanismos permitan alcanzar sus objetivos y lograr el riesgo mínimo determinado en el Análisis y Evaluación de Riesgos y Amenazas, así como los controles de los aspectos mencionados en el apartado 2.4.6.1.1. La capacidad de administrar las instalaciones debe ser acorde con el Plan de Seguridad de Sistemas.

2.4.6.2.2. La Implantación del Plan debe garantizar el logro de los objetivos de la Política de Certificados y la Declaración de Prácticas de Certificación, el cual debe de ser compatible por lo menos con las secciones 4 a 10 del estándar ISO 17799, o las que le sustituyan.

2.4.7. Estructura de Certificados.

2.4.7.1. La estructura de datos del Certificado debe ser compatible con el estándar ISO/IEC 9594-8; además de contener los datos que aparecen en el artículo 108 del Código de Comercio, para ser considerados como válidos.

2.4.7.2. Los algoritmos utilizados para la Firma Electrónica Avanzada deben ser compatibles con los estándares de la industria RFC 3280. Internet X509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (Obsoletes 2459), R. Housley, W. Polk, W. Ford, D. Solo, April 2002, 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.

2.4.7.3. En el caso de las claves utilizadas para la generación de una Firma Electrónica Avanzada, su tamaño 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 tanto del Prestador de Servicios de Certificación como del usuario.

2.4.7.4. 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 y al menos los que indican estas Reglas Generales.

2.4.8. Estructura de la Lista de Certificados Revocados (LCR).

2.4.8.1. La estructura e información 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:

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

2.4.8.1.2. La identificación del algoritmo de firma utilizado;

2.4.8.1.3. El nombre del emisor;

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

2.4.8.1.5. 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

2.4.8.1.6. 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.

2.4.9. El solicitante de acreditación y el Prestador de Servicios de Certificación deberán 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.

2.4.10. El solicitante de acreditación y el Prestador de Servicios de Certificación definirán procedimientos que informen de las características de los procesos de creación y verificación de Firma Electrónica Avanzada, así como aquellos que aplicarán para dejar sin efecto definitivo los certificados.

2.4.11. Política de Certificados

2.4.11.1. El solicitante de Acreditación y el Prestador de Servicios de Certificación deberán establecer una Política de Certificados conforme a la cual se establecerá la confianza del usuario en el servicio, que:

- 2.4.11.1.1.** Asegure su concordancia con la Declaración de Prácticas de Certificación y los procedimientos operacionales;
- 2.4.11.1.2.** Permita la interoperabilidad con los Prestadores de Servicios de Certificación ya acreditados y con la Secretaría de Economía;
- 2.4.11.1.3.** Indique a quién se le puede otorgar un Certificado y cómo se aplicará el proceso de registro, y que se deberá verificar en forma fehaciente la identidad del usuario. Cuando se trate de un certificado que habrá de ser utilizado para **generar** Firma Electrónica Avanzada deberá describir la forma en que se precisarán los propósitos, objetivos y alcances del Certificado y sus limitaciones. Asimismo, se deberán describir las obligaciones que contrae el Prestador de Servicios de Certificación y el usuario en la emisión y utilización del Certificado;
- 2.4.11.1.4.** Dé a conocer las medidas de privacidad y de protección de datos que se aplicarán en materia de Firma Electrónica Avanzada. La Política de Certificados será pública;
- 2.4.11.1.5.** Deberá establecer bajo qué circunstancias se puede revocar un Certificado y quiénes pueden solicitarlo, y
- 2.4.11.1.6.** Tendrá que ser compatible por lo menos con el estándar ETSI TS 102 042 o el que le sustituya.
- 2.4.12.** Declaración de Prácticas de Certificación
- 2.4.12.1.** En la Declaración de Prácticas de Certificación, que deberá elaborar y mantener actualizado el solicitante de acreditación y el Prestador de Servicios de Certificación, determinarán:
- 2.4.12.1.1.** Los procedimientos de operación para otorgar certificados y el alcance de aplicación de los mismos;
- 2.4.12.1.2.** 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;
- 2.4.12.1.3.** La vigencia de los certificados. Y una vez otorgada la acreditación por la Secretaría, la fecha de inicio de operaciones;
- 2.4.12.1.4.** Detalladamente el método de verificación de identidad del usuario que se utilizará para la emisión de los certificados;
- 2.4.12.1.5.** Procedimientos de protección de confidencialidad de la información de los solicitantes;
- 2.4.12.1.6.** Un procedimiento para registrar la fecha y hora de todas las operaciones relacionadas con la emisión de un Certificado y conservarlas de manera confiable;
- 2.4.12.1.7.** 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 a la Secretaría o a otro Prestador de Servicios de Certificación, en el caso, de suspensión definitiva;
- 2.4.12.1.8.** Las medidas de seguridad adoptadas para proteger sus Datos de Creación de Firma Electrónica;
- 2.4.12.1.9.** Los controles que se utilizarán para asegurar que el propio usuario genere sus Datos de Creación de Firma Electrónica, autenticación de usuarios, emisión de certificados, revocación de certificados, auditoría y almacenamiento de información relevante, y

2.4.12.1.10. La Declaración de Prácticas de Certificación deberá ser compatible por lo menos con el estándar ETSI TS 102 042 y el RFC 3647 o el que le sustituya.

2.4.13. Modelo Operacional de la Autoridad Certificadora;

2.4.13.1. El solicitante de acreditación y el Prestador de Servicios de Certificación deberán definir su Modelo Operacional de la Autoridad Certificadora conforme al cual operará y prestará sus servicios al fungir como autoridad certificadora a efecto de lograr confiabilidad e interoperabilidad, que desarrollará los apartados siguientes:

2.4.13.1.1. Cuáles son los servicios prestados;

2.4.13.1.2. Cómo se interrelacionan los diferentes servicios;

2.4.13.1.3. En qué lugares se operará;

2.4.13.1.4. Qué tipos de certificados se entregarán;

2.4.13.1.5. Si se generarán certificados con diferentes niveles de seguridad;

2.4.13.1.6. Cuáles son las políticas y procedimientos de cada tipo de certificado, y

2.4.13.1.7. Cómo se protegerán los activos.

2.4.13.2. El Modelo Operacional de la Autoridad Certificadora deberá contener un resumen que incluya:

2.4.13.2.1. Contenido del documento;

2.4.13.2.2. La historia del posible Prestador de Servicios de Certificación, y

2.4.13.2.3. Relaciones comerciales con proveedores de insumos o servicios para sus operaciones.

2.4.13.3. El Modelo Operacional de la Autoridad Certificadora deberá comprender los siguientes aspectos:

2.4.13.3.1. Interfaces con las Autoridades Registradoras;

2.4.13.3.2. Implementación de elementos de seguridad;

2.4.13.3.3. Procesos de administración;

2.4.13.3.4. Sistema de directorios para los certificados;

2.4.13.3.5. Procesos de auditoría y respaldo, y

2.4.13.3.6. Bases de Datos a utilizar.

2.4.13.4. El Modelo Operacional de la Autoridad Certificadora deberá considerar la Política de Certificados, la Declaración de Prácticas de Certificación, la Política de Seguridad de la Información y el Plan de Seguridad de Sistemas por lo que se refiere a la generación de claves.

2.4.13.5. El Modelo Operacional de la Autoridad Certificadora deberá incluir los requerimientos de seguridad física del personal, de las instalaciones y del módulo criptográfico.

2.4.14. Modelo Operacional de la Autoridad Registradora.

2.4.14.1. El solicitante de acreditación y el Prestador de Servicios de Certificación deberán definir su Modelo Operacional de la Autoridad Registradora conforme al cual operará y prestará sus servicios con su autoridad registradora a efecto de lograr confiabilidad e interoperabilidad, que desarrollará los apartados siguientes:

2.4.14.1.1 Cuáles son los servicios de registro que se prestarán;

2.4.14.1.2 En qué lugares se ofrecerán dichos servicios, y

2.4.14.1.3 Qué tipos de certificados generados por la Autoridad Certificadora se entregarán.

2.4.14.2. El Prestador de Servicios de Certificación deberá ofrecer los mecanismos para que el propio usuario genere en forma privada y segura sus Datos de Creación de Firma Electrónica. Deberá indicar al usuario el grado de fiabilidad de los mecanismos y dispositivos utilizados.

2.4.14.3. El Modelo Operacional de la Autoridad Registradora deberá comprender los siguientes aspectos:

2.4.14.3.1. Interfaces con Autoridad Certificadora;

2.4.14.3.2. Implementación de dispositivos de seguridad;

2.4.14.3.3. Procesos de administración;

2.4.14.3.4. Procesos de auditoría y respaldo;

2.4.14.3.5. Bases de Datos a utilizar;

2.4.14.3.6. Privacidad de datos, y

2.4.14.3.7. Descripción de la seguridad física de las instalaciones

2.4.14.4. El Modelo Operacional de la Autoridad registradora deberá establecer el método para proveer de una identificación unívoca del usuario y el procedimiento de uso de los Datos de Creación de Firma Electrónica.

2.4.15. Plan de Administración de Claves.

2.4.15.1. El solicitante de acreditación y el Prestador de Servicios de Certificación deberán definir su Plan de Administración de Claves conforme al cual generará, protegerá y administrará sus claves criptográficas, respecto de los apartados siguientes:

2.4.15.1.1. Claves de la Autoridad Certificadora;

2.4.15.1.2. Almacenamiento, respaldo, recuperación y uso de los Datos de Creación de Firma Electrónica de la Autoridad Certificadora del Prestador de Servicios de Certificación;

2.4.15.1.3. Distribución del certificado de la Autoridad Certificadora;

2.4.15.1.4. Administración del ciclo de vida del hardware criptográfico que utilice la Autoridad Certificadora, y

2.4.15.1.5. Dispositivos seguros para los usuarios.

2.4.15.2. Los procedimientos implantados de acuerdo al Plan de Administración de Claves, deberán garantizar la seguridad de las claves en todo momento, aun en caso de cambios de personal, componentes tecnológicos, y demás que señalan las presentes Reglas Generales.

2.4.15.3. El Plan de Administración de Claves deberá establecer como requerimiento mínimo el utilizar aquellas con longitud de 1024 bits para los usuarios y de 2048 bits para los Prestadores de Servicios de Certificación.

2.4.15.4. El Prestador de Servicios de Certificación, su autoridad certificadora y registradoras, utilizarán dispositivos seguros para almacenar sus 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.

2.4.15.5. El Plan de Administración de Claves tendrá que ser compatible por lo menos con el estándar ETSI TS 102 042 sección 7.2 - Generación de la clave de la Autoridad Certificadora, Almacenamiento, Respaldo y Recuperación de la clave de la Autoridad Certificadora, Distribución de la clave pública de la Autoridad Certificadora, uso de clave de la Autoridad Certificadora, fin del ciclo de vida de la clave de la Autoridad Certificadora y Administración del ciclo de vida del Hardware criptográfico-, o el que le sustituya.

2.5. El Solicitante de Acreditación y el Prestador de Servicios de Certificación, deberán proporcionar a la Secretaría, la documentación con la que acredite el cumplimiento de los requisitos previstos en el Código, el Reglamento o en las presentes Reglas Generales conforme a lo siguiente:

2.5.1. Tratándose de documentos públicos en copia certificada o en copia simple con el original para cotejo, o

2.5.2. Tratándose de documentos privados en copia simple, y

2.5.3. Una copia en disco compacto de toda la documentación presentada.

3. Para los efectos del artículo 102, inciso A), fracción V del Código, las condiciones a que se sujetará la fianza que otorgarán los solicitantes que obtengan su acreditación en términos del artículo anterior, previo al inicio del ejercicio de sus funciones como Prestadores de Servicios de Certificación, serán conforme a lo siguiente:

3.1. Una vez resuelta la procedencia de la solicitud de acreditación, en términos de la fracción IV del artículo 7 del Reglamento, el interesado deberá presentar la fianza de compañía debidamente autorizada a favor de la Tesorería de la Federación, en el término establecido en el artículo 8 del mencionado Reglamento:

3.1.1. Tratándose de un notario o corredor públicos, por un monto equivalente a cinco mil veces el salario mínimo general diario vigente en el Distrito Federal;

3.1.2. Tratándose de personas morales de carácter privado o instituciones públicas, por el monto resultante de multiplicar cinco mil veces el salario mínimo general diario vigente en el Distrito Federal por cada persona física de su personal, o integrante de una persona moral distinta que se contemple para efectos del artículo 104 fracción I del Código dentro de la acreditación para prestar el servicio de certificación en nombre y por cuenta del solicitante conforme al artículo 104 fracción I del Código;

3.2. Cuando la fianza tenga que ser otorgada por un notario o corredor público, la Secretaría podrá acordar que se otorgue de manera solidaria por parte de los colegios o agrupaciones de notarios o corredores públicos.

4. Para los efectos del artículo 10 del Reglamento, la Secretaría a través de sus servidores públicos comprobarán la identidad del solicitante de acreditación o del Prestador de Servicios de Certificación o su representante, utilizando cualquiera de los medios admitidos en derecho.

4.1. Tratándose de la identificación del representante de un Prestador de Servicios de Certificación que sea persona moral privada o institución pública, éste deberá acreditar su personalidad y la legal existencia de su representado a la Secretaría.

4.2. El Prestador de Servicios de Certificación generará sus Datos de Creación de Firma Electrónica, en el nivel de seguridad más alto de sus instalaciones, a fin de dar certeza y seguridad a todos los elementos necesarios para la creación de los mismos y bajo la supervisión de la Secretaría, en dicha generación se podrá utilizar cualquier tecnología por lo que el procedimiento técnico variará de acuerdo a la que se utilice, lo anterior a fin de cumplir con el principio de neutralidad tecnológica.

5. Para los efectos de los artículos 113 del Código y 16 del Reglamento, el procedimiento para obtener la copia de cada Certificado generado por un Prestador de Servicios de Certificación, será mediante envío en línea de cada Certificado a la Secretaría, lo cual será en tiempo real, es decir, se enviará una copia de cada certificado inmediatamente después del momento de expedición de los Certificados generados por el Prestador de Servicios de Certificación en su autoridad certificadora.

5.1. En el caso que el Prestador de Servicios de Certificación por caso fortuito o de fuerza mayor debidamente comprobado a la Secretaría, no pudiese llevar a cabo el envío a que se refiere el apartado anterior, el Prestador de Servicios de Certificación deberá hacer la réplica por cualquier medio en un término no mayor a seis horas.

5.2. Además del envío en línea de la copia de los Certificados, el Prestador de Servicios de Certificación remitirá dicha copia a la Secretaría en medios ópticos o electrónicos dentro de las veinticuatro horas siguientes a la generación de los Certificados, a fin de garantizar redundancia del procedimiento técnico descrito en el apartado 5 anterior de estas Reglas Generales.

5.3. El Prestador de Servicios de Certificación deberá cerciorarse que la Secretaría recibió la copia de cada certificado.

6. Para los efectos del artículo 108 fracción III del Código y 17 fracción III del Reglamento, los datos de acreditación ante la Secretaría observarán los siguientes elementos.

6.1. El Certificado emitido por el Prestador de Servicios de Certificación debe contener los datos que aparecen en el artículo 108 del Código de Comercio, para ser considerado válido.

6.2. Los certificados emitidos por el Prestador de Servicios de Certificación deberán contener la dirección electrónica de la Secretaría, en donde se podrá consultar la Lista de los Certificados Revocados de Prestadores de Servicios de Certificación.

7. Para los efectos del artículo 108 fracción VI del Código y 18 del Reglamento, la fecha y hora de emisión del Certificado se determinará conforme a lo siguiente:

7.1. 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 por el Prestador de Servicios de Certificación.

7.2. 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.

7.3. El Prestador de Servicios de Certificación deberá asegurar en todo momento el enlace del Sistema de Sello o Estampado de Tiempo con el de la Secretaría.

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

8. Para efectos del artículo 19 del Reglamento, la Secretaría verificará que los Prestadores de Servicios de Certificación cumplan con la estructura de certificados referida en las presentes Reglas Generales en los apartados 2.4.7. al 2.4.7.4., así como con los estándares internacionales, el Código de Comercio, el Reglamento y estas Reglas Generales, con el objetivo de asegurar que los certificados emitidos por los Prestadores de Servicios de Certificación, en ningún caso, contengan elementos que puedan generar confusión en la Parte que Confía.

9. Para los efectos del artículo 104 fracción IV del Código de Comercio, los casos en que estará a disposición el contenido privado del Registro de Certificados de un Prestador de Servicios de Certificación se sujetarán a lo dispuesto por la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

10. El Prestador de Servicios de Certificación que en términos del artículo 104 fracción VI, quiera cesar de manera voluntaria su actividad, previo pago de derechos tiene que informar el motivo de dicho cese con cuarenta y cinco días de anticipación a la Secretaría a efecto de que la misma se cerciore que se ha cumplido con lo establecido en el artículo 16 del Reglamento y el apartado 5, 5.1 y 5.2 de las presentes Reglas Generales.

11. Abreviaturas utilizadas en las presentes Reglas Generales.

11.1 GIAC-Global Information Assurance Certification.

11.2 GGSC GIAC Gold Standard Certificates.

11.3 GSLC-GIAC Security Leadership Certificat.

11.4 CISSP-Certified Information Systems Security Professionals.

11.5 SSCP-System Security Certified Practitioner.

11.6 ISO-International Organization for Standardization.

11.7 ETSI TS-European Telecommunications Standards Institute.

11.8 EIA/TIA-Electronic Industries Alliance/Telecommunications Industry Association.

11.9 ISO/IEC-International Organization for Standardization/International Electrotechnical Commission.

11.10 NIST-National Institute of Standards and Technology.

11.11 ACSI-Australian Communications Electronic Security Instruction.

11.12 LCR-Lista de Certificados Revocados.

11.13 LDAP-Protocolo de Acceso de Directorio de Peso ligero.

11.14 OCSP-Protocolo de Estatus de Certificados en Línea.

- 11.15 FIPS-Federal Information Processing Standards.
- 11.16 RFC-Request for Comments.
- 11.17 TCP/IP Transmission Control Protocol/Internet Protocol.
- 11.18 IPSEC-Internet Protocol Security.

TRANSITORIOS

PRIMERO.- Las presentes Reglas entrarán en vigor al día siguiente de su publicación en el **Diario Oficial de la Federación**.

SEGUNDO.- Estas Reglas estarán sujetas a cambios y a una revisión anual de la Secretaría de Economía, debido a los constantes cambios en la industria, a los estándares, normas y criterios internacionales reconocidos para prestar el servicio de certificación.

México, D.F., a 4 de agosto de 2004.- El Secretario de Economía, **Fernando de Jesús Canales Clariond**.- Rúbrica.