REGLAS GENERALES A LAS QUE DEBERÁN SUJETARSE LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN

(Publicado en el Diario Oficial de la Federación el 14 de mayo de 2018)

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

Con fundamento en lo dispuesto por los artículos 95 bis 3, 95 bis 6, 102, 104, 105, 110, 111, 112 y 113 del Código de Comercio, 2o., 5o., 6o., 7o., 8o., 9o., 10o., 11o., 12o., 16o., 17o., 18o., 19o., 26o., 27o. y 29o. del Reglamento del Código de Comercio en materia de Prestadores de Servicios de Certificación, 5 fracción XVII del Reglamento Interior de la Secretaría de Economía, y

CONSIDERANDO

Que de conformidad con lo dispuesto en el artículo 6 apartado B fracción I de la Constitución Política de los Estados Unidos Mexicanos, el Estado garantizará a la población su integración a la sociedad de la información y el conocimiento, mediante una política de inclusión digital universal, con metas anuales y sexenales.

Que de conformidad con el Plan Nacional de Desarrollo 2013–2018, la “Estrategia para Democratizar la Productividad”, incluye entre sus líneas de acción el “llevar a cabo políticas públicas que eliminen los obstáculos que limitan el potencial productivo de los ciudadanos y las empresas”, así como “incentivar entre todos los actores de la actividad económica el uso eficiente de los recursos productivos”.

Que conforme al enfoque transversal, México Próspero, la estrategia “Democratizar la Productividad”, tiene entre sus líneas de acción el “impulsar la economía digital y fomentar el desarrollo de habilidades en el uso de tecnologías de la información y la comunicación”.

Que el Gobierno Federal, a través de la Secretaría de Economía busca fortalecer las políticas, estrategias y directrices sobre el uso de la firma electrónica avanzada como factor en el gobierno electrónico y la simplificación de la interacción entre los comerciantes y el gobierno.

Que le corresponde a la Secretaría de Economía expedir las Reglas Generales en materia de Servicios de Certificación a efecto de que las prácticas y políticas que se apliquen garanticen la continuidad del servicio, la seguridad de la información y su confidencialidad, a través de procedimientos claros y definidos, así como establecer los estándares en materia de seguridad informática relacionada con el comercio electrónico y firma electrónica avanzada y, emitir la acreditación de Prestadores de Servicios de Certificación para expedición de certificados digitales y otros servicios adicionales de firma electrónica avanzada.

Que el 7 de abril del 2016 se publicó en el Diario Oficial de la Federación el Decreto por el que se reforman y adicionan diversas disposiciones del Código de Comercio y del Código Penal Federal, mediante el cual se adicionó al Código de Comercio, entre otros, un Capítulo I BIS “De la Digitalización”, en el cual se dispone que los comerciantes podrán digitalizar la documentación que hayan generado en el desarrollo cotidiano de sus actividades con plenos efectos jurídicos sin necesidad de conservar el papel, tales como

convocatorias de asambleas, libros de actas y comprobantes, dicha documentación también podrá generarse en medios electrónicos desde su inicio y conservarse en el tiempo de forma íntegra e inalterable.

Que el 30 de marzo de 2017 se publicó en el Diario Oficial de la Federación la Norma Oficial Mexicana NOM-151-SCFI-2016, Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos, en la cual se señalan los métodos que deberán observar los comerciantes para conservar los mensajes de datos, así como para la digitalización de toda o parte de la documentación en soporte físico relacionada con sus negocios, y

Que con el objeto de contar con reglas claras y definidas y a efecto de dar cumplimiento al Acuerdo que fija los lineamientos que deberán ser observados por las dependencias y organismos descentralizados de la Administración Pública Federal, en cuanto a la emisión de los actos administrativos de carácter general a los que les resulta aplicable el artículo 69-H de la Ley Federal de Procedimiento Administrativo, publicado en el Diario Oficial de la Federación el 8 de marzo de 2017, se eliminan 3 actos regulatorios que se contemplaban en las Reglas generales a las que deberán sujetarse los prestadores de servicios de certificación, publicadas en el mismo órgano de difusión, el 10 de agosto de 2004, en específico, en las Reglas 2.1.1.6, 2.4.15.1.2 y 2.4.15.4, por lo que, a fin de modernizar y facilitar el cumplimiento a las disposiciones legales que regulan la acreditación, operación y el correcto desempeño de los Prestadores de Servicios de Certificación, se expiden las siguientes:

REGLAS GENERALES A LAS QUE DEBERÁN SUJETARSE LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN

TÍTULO PRIMERO

Disposiciones Generales

1. El presente instrumento establece las Reglas que deberán cumplir los interesados en obtener la acreditación por parte de la Secretaría de Economía para poder ser Prestadores de Servicios de Certificación y ofrecer los servicios de emisión de Certificados Digitales, Sellos Digitales de Tiempo, Conservación de Mensajes de Datos, Digitalización de Documentos en Soporte Físico, así como para actuar como Tercero Legalmente Autorizado, de acuerdo con lo establecido en el artículo 100 del Código de Comercio y la NOM-151-SCFI-2016, publicada en el Diario Oficial de la Federación el 30 de marzo de 2017.

2. Para efectos de las presentes Reglas, además de lo establecido en el artículo 89 del Código de Comercio, se entenderá por:

I. Autoridad Certificadora: a las dependencias y entidades de la Administración Pública Federal y los Prestadores de Servicios de Certificación que, conforme a las disposiciones jurídicas, tengan reconocida esta calidad y cuenten con la infraestructura tecnológica para la emisión, administración y registro de certificados digitales, así como para proporcionar servicios relacionados con los mismos;

II. Autoridad Registradora: aquella que lleva el registro de los elementos de identificación de los firmantes y de la información con la que haya verificado el

cumplimiento de fiabilidad de las firmas electrónicas avanzadas y de emitir certificados digitales;

III. CRL: Certificate Revocation List;

IV. Digitalizadora: persona física o moral que realiza el servicio de Digitalización de Documentos en Soporte Físico conforme a lo dispuesto en el TÍTULO OCTAVO de las presentes Reglas;

V. Equipo HSM: dispositivo criptográfico basado en hardware que genera, almacena y protege claves criptográficas y aporta funcionalidad criptográfica de clave pública (PKI) de alto rendimiento efectuada dentro del mismo;

VI. ETSI TS: European Telecommunications Standards Institute Technical Specification;

VII. FIPS: Federal Information Processing Standards;

VIII. ISO/IEC: International Organization for Standardization/International Electrotechnical Commission;

IX. LDAP: Lightweight Directory Access Protocol;

X. NIST: National Institute of Standards and Technology;

XI. Nube o Cómputo en la Nube: modelo que permite el acceso ubicuo, conveniente y bajo demanda de red a un conjunto de recursos informáticos configurables;

XII. OCSP: Online Certificate Status Protocol;

XIII. Reglas: a las presentes Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación;

XIV. Reglamento: Reglamento del Código de Comercio en materia de Prestadores de Servicios de Certificación;

XV. RFC: Request for Comments, y

XVI. Sistema Cliente: aplicación informática instalada en una computadora de un usuario, que solicita a un servidor de un Prestador de Servicios de Certificación, a través de una red de telecomunicaciones.

TÍTULO SEGUNDO

De los Requisitos y del Trámite de Acreditación

3. Conforme a lo dispuesto por el artículo 102 inciso A) del Código de Comercio y 5o. del Reglamento, los interesados para poder ser Prestadores de Servicios de Certificación y ofrecer los servicios de emisión de Certificados Digitales, Sellos Digitales de Tiempo, Conservación de Mensajes de Datos, Digitalización de Documentos en Soporte Físico, así como para actuar como Tercero Legalmente Autorizado, de acuerdo con lo establecido en el artículo 100 del Código de Comercio y la NOM-151-SCFI-2016, podrán presentar solicitud para uno o varios Servicios.

Para tales efectos, los solicitantes deberán comprobar que cuentan con los elementos humanos, materiales, económicos, tecnológicos y procedimientos establecidos en los TÍTULOS QUINTO, SEXTO, SÉPTIMO y OCTAVO de las presentes Reglas, de acuerdo con el servicio que se trate.

4. En caso de que un Prestador de Servicios de Certificación solicite la acreditación para prestar servicios adicionales a los previamente autorizados, la Secretaría tomará en consideración los recursos humanos, materiales, tecnológicos y procedimientos del servicio ya acreditado. Por lo anterior, el Prestador de Servicios de Certificación únicamente deberá cumplir con los requisitos faltantes correspondientes al servicio solicitado.

Lo anterior, no es aplicable tratándose de los recursos económicos, toda vez que el Prestador de Servicios de Certificación deberá exhibir dicho requisito por cada servicio solicitado.

5. La Secretaría señalará en la Ficha de Trámite correspondiente en el Registro Federal de Trámites y Servicios, los requisitos y procedimientos para presentar las solicitudes. Dicha información también estará disponible en el sitio electrónico www.firmadigital.gob.mx.

6. A los actos, procedimientos y resoluciones contemplados en las presentes Reglas, les aplica lo previsto al respecto en la Ley Federal de Procedimiento Administrativo.

7. De conformidad con lo dispuesto en el artículo 89 del Código de Comercio y observando los principios de neutralidad tecnológica, autonomía de la voluntad, compatibilidad internacional y equivalencia funcional, los solicitantes podrán utilizar los avances tecnológicos para cumplir con los elementos materiales y tecnológicos señalados en estas Reglas.

8. Los solicitantes podrán optar por tener su equipo de cómputo y comunicación, software y/o sistemas e infraestructura informática en uno o más centros de datos, principal y alternos, pudiendo utilizar para cualquiera de ellos, cómputo en la nube, siempre y cuando cumplan con lo siguiente:

I. Para la utilización de cómputo en la nube, deberá acreditar los estándares y certificaciones nacionales y/o internacionales de calidad y seguridad con que cuentan los dos centros de datos. La seguridad deberá ser compatible con las normas y criterios internacionales y al menos con el estándar NIST Special Publication 800-144 Guidelines on Security and Privacy in Public Cloud Computing, December 2011, o el que le sustituya;

II. Deberá incluir en toda su documentación de seguridad informática, el apartado específico para cómputo en la nube, en el cual quedará definido el servicio;

III. Deberá desarrollar los aspectos de administración, operación y seguridad que realizará en la nube de los servicios de Certificados Digitales, Sellos Digitales de Tiempo, Conservación de Mensajes de Datos y Digitalización de Documentos en Soporte Físico;

IV. Contar con sistemas propios de Autoridad Certificadora y Autoridad Registradora, Sellos Digitales de Tiempo, Conservación de Mensajes de Datos, Digitalización de Documentos en Soporte Físico, así como equipos HSM propios o arrendados, para uso exclusivo del Prestador de Servicios, que no comparta con ninguna organización;

V. Asegurar que la Secretaría cuente con los accesos, información y documentos necesarios para realizar las visitas de verificación a que se refiere el TÍTULO TERCERO de las presentes Reglas, pudiendo realizarse esta inspección de forma remota, siempre que se cumplan con los mecanismos de comunicación segura requeridos;

VI. Los dos centros de datos con cómputo en la nube deberán estar separados cuando menos por 200 Kms., cuando estén localizados en zonas de alta sismicidad;

VII. Si el solicitante opta por la utilización de una nube privada, la infraestructura será administrada, operada y asegurada por el Prestador de Servicios de Certificación.

La administración de la infraestructura para los servicios de emisión de Certificados Digitales, Sellos Digitales de Tiempo, Conservación de Mensajes de Datos y Digitalización de Documentos en Soporte Físico podrá realizarse a través de un tercero contratado por el Prestador de Servicios de Certificación, cumpliendo con lo especificado en sus documentos de seguridad informática, y

VIII. Si el solicitante opta por la utilización de una nube comunitaria, la infraestructura será compartida por diversas organizaciones y el Prestador de Servicios de Certificación.

La administración, operación y seguridad de la infraestructura para los servicios de emisión de Certificados Digitales, Sellos Digitales de Tiempo, Conservación de Mensajes de Datos y Digitalización de Documentos en Soporte Físico, deberán quedar especificadas en el contrato de prestación de servicios, que para tal efecto deberá firmar el Prestador de Servicios de Certificación con el prestador de servicios en la nube.

9. Los solicitantes podrán resguardar uno o más Datos de Creación de Firma Electrónica de los diferentes servicios acreditados por la Secretaría o de otros servicios del Prestador de Servicios de Certificación, en los equipos HSM, principal y redundancia.

Si el equipo lo permite, podrá ser fragmentado para contener uno o más Datos de Creación de Firma Electrónica por partición, considerando la descripción de la partición o particiones de dicho equipo, en los documentos de seguridad informática. Los equipos HSM del Prestador de Servicios de Certificación no resguardarán Datos de Creación de Firma Electrónica de otras organizaciones.

En todo caso, la Secretaría deberá analizar la propuesta del solicitante y privilegiar la seguridad en la prestación del servicio.

10. El solicitante deberá incluir en toda su documentación de seguridad informática, el apartado específico para cómputo en la nube o partición, en el cual quedará definido el servicio.

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

I. Una vez resuelta la procedencia de la solicitud de acreditación en términos del artículo 7o. fracción IV del Reglamento, el solicitante deberá presentar la fianza de compañía debidamente autorizada a favor de la Tesorería de la Federación, en el término establecido en el artículo 8o. del mismo ordenamiento legal, y

II. 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.

12. El periodo de validez de los certificados emitidos a los Prestadores de Servicios de Certificación por la Secretaría, será de hasta cuatro quintas partes del periodo de validez del Certificado de la Autoridad Certificadora de esta Secretaría.

TÍTULO TERCERO

De los Procedimientos de Visitas de Verificación de Obligaciones a cargo de los Prestadores de Servicios de Certificación

13. En todo momento, el Prestador de Servicios de Certificación deberá actuar con transparencia, probidad y elevar sus estándares de seguridad, combatir malas prácticas e implementar medidas para fortalecer la secrecía, así como hacer efectiva su responsabilidad.

Para tales efectos deberá demostrar que cumple con sus obligaciones conforme a lo dispuesto por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

14. De conformidad con lo dispuesto en el artículo 95 bis 6 fracción II del Código de Comercio, la Secretaría podrá requerir informes, documentos y otros datos a los Prestadores de Servicios de Certificación para verificar en cualquier tiempo el adecuado desarrollo de las operaciones.

15. La Secretaría a fin de verificar el cumplimiento de las obligaciones de los Prestadores de Servicios de Certificación podrá practicar auditorías a los Prestadores de Servicios de Certificación, y requerirles, la información y documentación necesaria para llevar a cabo sus funciones de visitas de verificación respecto al cumplimiento de sus obligaciones, siempre y cuando reciba notificación conforme a lo dispuesto en la Ley Federal de Procedimiento Administrativo.

Cuando los Prestadores de Servicios de Certificación arrenden centros de datos, se asegurarán que la Secretaría cuente con los accesos, información y documentos necesarios para realizar las visitas de verificación, concernientes a las auditorías a que se refiere el párrafo anterior, siempre y cuando reciba notificación conforme a lo dispuesto en la Ley Federal de Procedimiento Administrativo.

16. Las visitas de verificación realizadas en los domicilios de las oficinas administrativas y en los centros de datos de los Prestadores de Servicios de Certificación, se desarrollarán conforme a lo dispuesto en la Ley Federal de Procedimiento Administrativo.

17. Para efectos de lo dispuesto en el artículo 3o. del Reglamento, la Secretaría publicará en el sitio electrónico www.firmadigital.gob.mx la relación de los Prestadores de Servicio de Certificación acreditados o suspendidos y de las personas físicas o morales que actúen en su nombre de conformidad con lo previsto en el artículo 104 fracción I del Código de Comercio.

Asimismo, la Secretaría publicará el padrón de profesionistas en las materias jurídica e informática a que se refiere el artículo 4o. del Reglamento a efecto de que coadyuven a impulsar la utilización de los medios electrónicos en los actos de comercio.

Los interesados en integrarse a dicho padrón deberán acreditar la Norma Técnica de Competencia Laboral que se emita para tal efecto, con el propósito de que éstos puedan ser designados peritos o árbitros en materia de Prestación de Servicios de Certificación y Firma Electrónica.

TÍTULO CUARTO

Del Cese de Funciones

18. El Prestador de Servicios de Certificación que en términos del artículo 104 fracción VI del Código de Comercio, quiera cesar de manera voluntaria su actividad, previo pago de derechos, tiene que informar a la Secretaría, el motivo de dicho cese con un término de cuarenta y cinco días de anticipación, a efecto de que la misma se cerciore que se ha cumplido con lo establecido en el artículo 16o. del Reglamento, así como con lo estipulado en los TÍTULOS QUINTO, SEXTO, SÉPTIMO y OCTAVO de las presentes Reglas.

En este supuesto los registros y archivos pasarán a otro Prestador de Servicios de Certificación que cumpla con las características similares al que llevaba dicho servicio.

TÍTULO QUINTO

De la Emisión de Certificados Digitales

19. Para efectos de lo dispuesto en los artículos 102 apartado A fracción II del Código de Comercio y 5o. fracción III del Reglamento, para obtener la acreditación como Prestador de Servicios de Certificación en la emisión de Certificados Digitales, los solicitantes deberán comprobar que cuentan con los elementos humanos, económicos, materiales y tecnológicos que se mencionan en el presente apartado:

CAPÍTULO I

De los Elementos Humanos

20. El solicitante deberá contar con un Profesional Jurídico que deberá cumplir con los siguientes requisitos:

I. Ser licenciado en derecho con título y cédula profesional expedidos por la Secretaría de Educación Pública o su equivalente;

II. Demostrar al menos dos años de experiencia en correduría pública, derecho notarial o derecho mercantil;

III. Acreditar al menos un año de experiencia en derecho informático, y

IV. Declarar bajo protesta de decir verdad que no ha sido condenado por delito contra el patrimonio de las personas o que haya merecido pena privativa de la libertad, ni que por cualquier motivo haya sido inhabilitado para el ejercicio de su profesión, para desempeñar un puesto en el servicio público, en el sistema financiero o para ejercer el comercio.

21. Podrá contar con un Agente Certificador, quien será la persona física o moral encargado de llevar a cabo la verificación de la identidad de los usuarios y su vinculación con los medios de identificación electrónica para la emisión de Certificados Digitales, estas funciones podrán ser ejecutadas también por el Profesional Jurídico, siendo responsable en todo momento el Prestador de Servicios de Certificación.

Tratándose de personas morales, éstas deberán señalar quienes serán las personas físicas que realizarán las actividades para la verificación de la identidad de los usuarios y su vinculación con los medios de identificación electrónica para la emisión de Certificados Digitales.

En todo caso, las personas físicas deberán demostrar que cumplen con los siguientes requisitos:

I. Declarar bajo protesta de decir verdad que no ha sido condenado por delito contra el patrimonio de las personas o que haya merecido pena privativa de la libertad, ni que por cualquier motivo haya sido inhabilitado para el ejercicio de su profesión, para desempeñar un puesto en el servicio público, en el sistema financiero o para ejercer el comercio, y

II. Demostrar relación laboral con el Agente Certificador o con el solicitante como Prestador de Servicios de Certificación, según corresponda.

22. Contar con un Profesional Informático que deberá cumplir con los siguientes requisitos:

I. Ser licenciado o ingeniero en área informática o afín, con título y cédula profesional expedidos por la Secretaría de Educación Pública o su equivalente;

II. Comprobar al menos dos años de experiencia en el área de criptografía;

III. Acreditar estudios en manejo de software o hardware relacionados con criptografía, y

IV. Declarar bajo protesta de decir verdad que no ha sido condenado por delito contra el patrimonio de las personas o que haya merecido pena privativa de la libertad, ni que por cualquier motivo haya sido inhabilitado para el ejercicio de su profesión, para desempeñar un puesto en el servicio público, en el sistema financiero o para ejercer el comercio.

23. Contar con un Auxiliar de Apoyo Informático de Seguridad, quien será el responsable del diseño, implantación, cumplimiento del sistema de gestión, planes, políticas, procedimientos y prácticas de seguridad de las instalaciones del Prestador de Servicios de Certificación, este elemento humano podrá ser el Profesional Informático, mismo que deberá acreditar los siguientes requisitos:

I. Ser licenciado o ingeniero en área informática o afín, con título y cédula profesional expedidos en la Secretaría de Educación Pública o su equivalente;

II. Comprobar al menos dos años de experiencia en el área de criptografía;

III. Acreditar estudios en manejo de software o hardware relacionados con criptografía, y

IV. Declarar bajo protesta de decir verdad que no ha sido condenado por delito contra el patrimonio de las personas o que haya merecido pena privativa de la libertad, ni que por cualquier motivo haya sido inhabilitado para el ejercicio de su profesión, para desempeñar un puesto en el servicio público, en el sistema financiero o para ejercer el comercio.

24. Contar con un Auxiliar de Apoyo Informático de Administrador de Redes, un Auxiliar de Apoyo Informático de Operador de Sistemas, un Auxiliar de Apoyo Informático de Administrador de Sistemas y un Auxiliar de Apoyo Informático de Administrador de Bases de Datos, quienes deberán cumplir con los siguientes requisitos:

I. Ser técnico, licenciado o ingeniero en área informática o afín, con título y cédula profesional expedidos por la Secretaría de Educación Pública o su equivalente, según corresponda;

II. Tener experiencia comprobable en las áreas de seguridad informática, redes y/o sistemas informáticos, de cuando menos dos años, según sea el caso;

III. Acreditar al menos una certificación nacional o extranjera, en manejo de software o hardware referente a seguridad informática, seguridad en redes y/o sistemas informáticos, la cual deberá contar con una antigüedad de dos años como máximo, y

IV. Declarar bajo protesta de decir verdad que no ha sido condenado por delito contra el patrimonio de las personas o que haya merecido pena privativa de la libertad, ni que por cualquier motivo haya sido inhabilitado para el ejercicio de su profesión, para desempeñar un puesto en el servicio público, en el sistema financiero o para ejercer el comercio.

25. El solicitante podrá presentar ante la Secretaría una cantidad mayor de recursos humanos si las necesidades para la prestación del servicio así lo requieren.

26. El solicitante deberá presentar el procedimiento que utilizará para reclutar, seleccionar, evaluar y contratar al personal, el cual deberá describir la forma de corroborar los antecedentes del personal antes de contratarlo, así como su actualización.

En todo caso, la Secretaría deberá autorizar la modificación que el Prestador de Servicios de Certificación realice respecto de los recursos humanos antes mencionados.

27. El solicitante deberá presentar los contratos de confidencialidad celebrados con cada recurso humano respecto de la información a la que tengan acceso, el cual deberá extenderse cuando menos un año posterior a la conclusión laboral del empleado o de servicios en caso de una empresa externa.

CAPÍTULO II

De los Elementos Económicos

28. El solicitante deberá contar con capital que deberá comprender al menos el equivalente a una cuarta parte de la inversión requerida en los términos señalados en el artículo 5 fracción III inciso c del Reglamento.

De igual forma, deberá contar con un seguro de responsabilidad civil que cubrirá el equivalente a 16800 (Dieciséis mil ochocientos) unidades de medida y actualización (UMA) diaria en México para cada año y durante el tiempo que permanezca acreditado el Prestador de Servicios de Certificación.

La Secretaría podrá establecer una cantidad mayor a la referida en el párrafo anterior, en caso de que, derivado del análisis de las operaciones en que sea utilizado el servicio de emisión de Certificados Digitales, así lo considere necesario. En este supuesto, se obliga hasta el límite de la suma asegurada a pagar la indemnización que el asegurado deba a un tercero a consecuencia de un hecho que cause un daño previsto en el contrato de seguro.

29. Contar con una fianza cuyo monto no será menor al equivalente a 16800 (Dieciséis mil ochocientos) unidades de medida y actualización (UMA) diaria en México para cada año y durante el tiempo que permanezca acreditado el Prestador de Servicios de Certificación.

La Secretaría podrá establecer una cantidad mayor a la referida en el párrafo anterior, en caso de que, derivado del análisis de las operaciones en que sea utilizado el servicio

de emisión de Certificados Digitales, así lo considere necesario. En este supuesto, 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, por actuar en sustitución del Prestador de Servicios de Certificación, cuando éste sea suspendido, inhabilitado o cancelado en su ejercicio.

30. Por cada agente certificador que realice la verificación de la identidad de los usuarios y su vinculación con los medios de identificación electrónica para la emisión de Certificados Digitales se cubrirá una fianza equivalente a 5000 (Cinco mil) unidades de medida y actualización en México para cada año.

La Secretaría podrá determinar una cantidad mayor con base en un análisis de las operaciones en que sea utilizado el servicio de emisión de Certificados Digitales, así como la valorización de la totalidad del daño que en su caso pudiera causar por la mala práctica del servicio acreditado ofrecido.

CAPÍTULO III

De los Elementos Materiales

31. El solicitante deberá contar con el espacio físico, controles de seguridad, accesos, perímetros de seguridad física, medidas de protección, así como con las políticas necesarias para garantizar la seguridad para la emisión de Certificados Digitales.

32. Contar con una oficina administrativa sujeta a los procedimientos y prácticas de seguridad firmados por el Profesional Jurídico, el Profesional Informático y el Auxiliar de Apoyo Informático de Seguridad, los cuales deberán detallar por lo menos los siguientes elementos:

I. Los recursos humanos y las áreas donde se maneja información confidencial y los controles de acceso.

Los controles de acceso deberán estar supervisados continuamente, a efecto de reducir al mínimo los riesgos;

II. Los controles para evitar riesgo, daño, pérdida, alteración o sustracción de la información confidencial, incluso fuera de horario laboral;

III. Las áreas seguras donde se resguardará la información concerniente al servicio de emisión de Certificados Digitales.

Para efecto de lo dispuesto en el párrafo anterior, las áreas deberán permanecer aisladas y cerradas dentro del perímetro de seguridad física, contener mobiliario específico con mecanismos de seguridad;

IV. Las áreas donde residan los sistemas de autoridades registradoras, con accesos físicos controlados, los cuales deberán estar protegidos con mecanismos de seguridad, controles de acceso, alarmas de seguridad, y se encontrarán limitados sólo al personal autorizado;

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

VI. La infraestructura de computación y comunicaciones instaladas, así como los contratos de mantenimiento preventivo y correctivo requeridos para garantizar la continua disponibilidad e integridad de los equipos y su software, de acuerdo a las especificaciones y periodos recomendados por los fabricantes, y

VII. Personal especializado o, en su caso, contratos de mantenimiento preventivo y correctivo, requerido para garantizar la continua disponibilidad e integridad de los sistemas, de acuerdo a las especificaciones y periodos recomendados por los fabricantes.

33. Contar con dos centros de datos, uno principal y otro alterno, que deberán cumplir con las certificaciones y estándares de calidad y seguridad, así como contar con procedimientos y prácticas de seguridad firmados por el Profesional Jurídico, el Profesional Informático y el Auxiliar de Apoyo Informático de Seguridad, dichos centros de datos deberán detallar por lo menos los siguientes elementos:

I. Las áreas y los servicios en los cuales se maneja información confidencial, controles de acceso y mecanismos de supervisión continua, a efecto de reducir al mínimo los riesgos.

Los controles deberán evitar riesgo, daño o pérdida, de los activos, alteración o sustracción de información confidencial, incluso en horario no laboral;

II. Los accesos físicos a las áreas del servicio de emisión de Certificados Digitales, y/o la gestión de revocación de Certificados Digitales y área de residencia de servidores, así como los recursos humanos que tendrán acceso a éstas.

Dichas áreas deberán estar protegidas con puertas y muros sólidos y firmes, chapas seguras, controles de acceso, sistemas de extinción de incendios, 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 habrá accesos no autorizados;

III. Para el caso de los servicios compartidos con otra organización, deberá asegurarse la separación física de los estantes de equipos del Prestador de Servicios de Certificación;

IV. El acceso de visitas a las áreas en donde se maneje información confidencial deberá ser autorizado por el Auxiliar de Apoyo Informático de Seguridad y se deberá registrar toda actividad que realice el visitante con la fecha y hora de ingreso y salida;

V. Para la selección y el diseño de áreas seguras se debe tomar en cuenta la posibilidad de daños por fuego, sismo, inundación, explosión, desorden civil, y otras formas de desastres naturales y causados por el hombre;

VI. Todos los servicios claves, como la generación de Certificados Digitales, Sellos Digitales de Tiempo, revocación de Certificados Digitales, publicación de CRL,

respuestas del servicio de OCSP, administración de bases de datos, deberán situarse alejados de las áreas de acceso y atención al público;

VII. Detalle de los dispositivos electrónicos y su ubicación dentro de las áreas seguras que así lo requieran, siempre bajo control y supervisión para no comprometer la seguridad de la información confidencial;

VIII. Procedimiento para destruir material de desecho como cajas de cartón, empaques, entre otros, sin posibilidad de recuperación antes de desecharlo;

IX. Los 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, y

X. Procedimientos para la gestión de los servicios de procesamiento de información, la cual deberá estar físicamente separada del resto de los servicios, dicha separación podrá ser mediante el empleo de estantes destinados para su uso exclusivo.

34. Los dos centros de datos deberán estar separados cuando menos por 200 Kms**.,** cuando estén localizados en zonas de alta sismicidad.

35. Los procedimientos y prácticas de seguridad de los centros de datos, firmados por el Profesional Jurídico, el Profesional Informático y el Auxiliar de Apoyo Informático de Seguridad, deberán establecerse para el personal dentro del perímetro de seguridad, que contemplarán lo siguiente:

I. Los recursos humanos que deberán observar los procedimientos y prácticas de seguridad;

II. Bitácora del acceso a las áreas restringidas autorizado por el Profesional Informático o el Auxiliar de Apoyo Informático de Seguridad;

III. Procedimiento para autorizar y dejar constancia de los accesos dentro del perímetro de seguridad de equipo de grabación, audio o video, con excepción del propio equipo de seguridad y de comunicaciones, los cuales deberán ser autorizados por Profesional Informático o el Auxiliar de Apoyo Informático de Seguridad, dejando evidencia de lo mismo;

IV. Los mecanismos que impidan que personal no autorizado acceda a las áreas del perímetro de seguridad;

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

VI. El equipo instalado y las protecciones físicas para reducir amenazas;

VII. Medios y procedimientos de respaldo de sistemas, deberá contar con un sistema no interrumpible de energía eléctrica e incluir una planta de energía eléctrica de emergencia para asegurar la continuidad del servicio;

VIII. Cableado eléctrico y de datos de los servicios de información confidencial, así como los estándares en la materia que proteja contra daños e intervenciones;

IX. La identificación de las líneas eléctricas las cuales no deberán interferir con el funcionamiento del cableado de datos;

X. La infraestructura de computación y comunicaciones las cuales deberán contar con el personal y refacciones necesarias o, en su caso, los contratos de mantenimiento preventivo y correctivo, requeridos para garantizar la continua disponibilidad e integridad de los equipos y su software, de acuerdo a las especificaciones y periodos recomendados por los fabricantes;

XI. Los sistemas informáticos, los cuales deberán de contar con el personal especializado o, en su caso, con los contratos de mantenimiento preventivo y correctivo, requerido para garantizar la continua disponibilidad e integridad de los sistemas, de acuerdo a las especificaciones y periodos recomendados por los fabricantes;

XII. Procedimientos para evitar que equipos, información y software salgan de los perímetros de seguridad sin autorización;

XIII. Procedimientos para 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 del servicio, éstos nunca deberán salir del perímetro de seguridad designado;

XIV. Procedimientos para evitar que los equipos sean reutilizados o queden en desuso conteniendo información confidencial;

XV. Procedimientos para destrucción de discos duros y demás medios de almacenamiento de información magnético u óptico antes de salir del perímetro de seguridad, dejando la evidencia correspondiente, y

XVI. Mecanismo para registrar el mal funcionamiento, fallas, mantenimientos preventivos y correctivos, de los equipos y sistemas, sensibles para la operación del servicio.

36. La seguridad física deberá ser compatible con las normas y criterios nacionales y/o internacionales y al menos con el estándar ETSI TS 102 042-sección 7.4.4 Physical and Environmental Security o el que le sustituya.

37. Las actualizaciones y/o modificaciones derivadas de las revisiones realizadas a los procedimientos y prácticas que lleve a cabo el Prestador de Servicios de Certificación, deberán ser notificadas a la Secretaría, para su revisión y aprobación.

38. En caso de que los centros de datos principal y alterno sean arrendados, se deberá acreditar los estándares y certificaciones nacionales y/o internacionales, así como la calidad y seguridad con que cuenta el mismo.

Cuando se trate de la infraestructura de computación y comunicaciones éstas deberán contar con el personal y refacciones o, en su caso, con los contratos de mantenimiento preventivo y correctivo, requeridos para garantizar la continua disponibilidad e integridad de los equipos y su software, de acuerdo a las especificaciones y periodos recomendados por los fabricantes.

Para el caso de los sistemas informáticos, éstos deberán contar con el personal especializado o, en su caso, con los contratos de mantenimiento preventivo y correctivo, requerido para garantizar la continua disponibilidad e integridad de los sistemas, de acuerdo a las especificaciones y periodos recomendados por los fabricantes.

Las actualizaciones y/o modificaciones derivadas de las revisiones realizadas a los procedimientos y prácticas que se elaboren en los centros de datos arrendados, deberán ser notificadas a la Secretaría.

CAPÍTULO IV

De los Elementos Tecnológicos

39. El solicitante deberá contar con el equipo de cómputo y comunicación, software y/o sistemas que se detalla a continuación:

I. Un servidor de misión crítica para la Autoridad Certificadora y otro, o PC, para la Autoridad Registradora, en caso de utilizar lo anterior de manera virtual, dicha implementación deberá ser incluida en todos los documentos de seguridad informática;

II. Un servidor de misión crítica, para el servicio de LDAP o equivalente, CRL y OCSP, en caso de utilizar lo anterior de manera virtual, dicha implementación deberá ser incluida en todos los documentos de seguridad informática;

III. Un sistema de sellado digital de tiempo, para insertar fecha y hora de emisión y/o revocación de los certificados, el cual puede ser propio, siempre que se considere el RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) y el RFC 3628 Policy Requirements for Time-Stamping Authorities (TSAs) o un servicio subcontratado a otro Prestador de Servicios de Certificación acreditado por esta Secretaría;

IV. Un dispositivo de alta seguridad, que cumpla con estándares de seguridad nacionales y/o internacionales, compatibles como mínimo con el estándar FIPS 140-2 nivel 3 en sus elementos de seguridad e implantación de los algoritmos criptográficos estándares, o el que le sustituya, para almacenar los Datos de Creación de Firma Electrónica del Certificado de la Autoridad Certificadora del Prestador de Servicios de Certificación;

V. Un enlace mínimo de 100 MB a Internet;

VI. Un ruteador;

VII. Un muro de fuego (firewall);

VIII. Una computadora para gestionar el sistema de administración del servicio emisión de Certificados Digitales;

IX. Un sistema de monitoreo de red;

X. Un sistema confiable de antivirus;

XI. Herramientas confiables de detección de vulnerabilidades;

XII. Sistemas confiables de detección y protección de intrusión, y

XIII. Las computadoras personales e impresoras necesarias para la prestación de los servicios de emisión de Certificados Digitales.

40. Todos los elementos descritos en la Regla 39 deberán considerar redundancia por seguridad.

41. Las tecnologías de virtualización deberán ser compatibles con las normas y criterios nacionales y/o internacionales y al menos con el estándar NIST Guide to Security for Full Virtualization Security, Special Publication 800-125, 2011, o el que le sustituya.

42. Contar con la infraestructura informática que se detalla a continuación:

I. Una Autoridad Certificadora y su redundancia por seguridad;

II. Una Autoridad Registradora y su redundancia por seguridad;

III. Repositorios para: Datos de Creación de Firma Electrónica del Certificado de la Autoridad Certificadora del Prestador de Servicios de Certificación, certificados y CRL´s basadas en un servicio de LDAP o equivalente, y su redundancia por seguridad;

IV. Un servicio de OCSP y su redundancia por seguridad;

V. Los procesos de administración de la Infraestructura Informática;

VI. Un manual de Política de Certificados;

VII. Una Declaración de Prácticas de Certificación, y

VIII. Los Manuales de Operación de las Autoridades Certificadora y Registradora.

43. Contar con un documento de Análisis y Evaluación de Riesgos y Amenazas que deberá detallar por lo menos los siguientes elementos:

I. Los activos críticos;

II. Requerimientos de seguridad;

III. Vulnerabilidades y amenazas de la infraestructura con la que proveerá el o los servicios y determinar los requerimientos de seguridad para las áreas de atención a clientes;

IV. Estudio que identifique y evalúe los riesgos e impactos que existen sobre la organización, personas, equipos, sistemas e instalaciones, así como recomendaciones de medidas para mitigarlos, y el impacto que sufrirá el negocio, en caso de interrupciones no planificadas;

V. Medidas de seguridad para la mitigación de los riesgos detectados;

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

VII. Los impactos que sufrirán los servicios del Prestador de Servicios de Certificación, en caso de interrupciones no planificadas, y

VIII. Adoptar Guide for Conducting Risk Assessments. NIST Special Publication 800-30 Revision 1. September 2012, equivalente o el que le sustituya.

44. Contar con un calendario de revisión y actualización del documento de Análisis y Evaluación de Riesgos y Amenazas.

45. Contar con un documento de Política de Seguridad de la Información que deberá detallar por lo menos los siguientes elementos:

I. Que el objeto de la Política de Seguridad sea congruente con el objeto del servicio de emisión de Certificados Digitales que ofrecerá el solicitante o el Prestador de Servicios de Certificación;

II. Los objetivos de seguridad claros, generales, no técnicos, que se desarrollarán a partir del resultado del Análisis y Evaluación de Riesgos y Amenazas;

III. Estar basada en las recomendaciones de los estándares ISO/IEC de la serie 27000 o los que le sustituyan;

IV. La Política de Seguridad de la Información deberá constar por escrito;

V. Identificar 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, los cuales deberán desarrollarse a partir del resultado del Análisis y Evaluación de Riesgos y Amenazas;

VI. Las reglas que indiquen cómo son provistos los servicios y las medidas de seguridad asociadas;

VII. Ser consistente con la Política de Certificados y con la Declaración de Prácticas de Certificación, a que se refieren en el presente TÍTULO;

VIII. Adoptar el proceso Internet Security Policy: A Technical Guide, by the National Institute of Standards and Technologies (NIST) o un proceso similar, y

IX. Desarrollar procedimientos y buenas prácticas de seguridad para apoyar la aplicación de las políticas de seguridad.

46. Contar con un calendario de revisión y actualización del documento de Política de Seguridad de la Información.

47. Contar con un documento de Política de Seguridad Física que deberá detallar por lo menos los siguientes elementos:

I. Control de acceso físico;

II. Protección y recuperación ante desastres;

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

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

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

48. Contar con un calendario de revisión y actualización del documento de Política de Seguridad Física.

49. Contar con un documento de Sistema de Gestión de Seguridad de la Información conforme a los estándares ISO/IEC de la serie 27000 o los que les sustituyan.

50. El Sistema de Gestión de Seguridad de la Información deberá garantizar el logro de los objetivos de la Política de Certificados y de la Declaración de Prácticas de Certificación.

51. Contar con un calendario de revisión y actualización del documento de Sistema de Gestión de Seguridad de la Información.

52. Contar con un documento de Plan de Seguridad de Sistemas el cual deberá ser coherente con el Sistema de Gestión de Seguridad de la Información y la Política de Seguridad de la Información y, de aplicación para el servicio de emisión de Certificados Digitales, mismo que deberá describir los requerimientos de seguridad de los sistemas, los controles a implantar y cumplir; así como delinear las responsabilidades de los individuos que accedan a los sistemas.

El Plan de Seguridad de Sistemas deberá ser compatible con las normas y criterios nacionales y/o internacionales y, al menos con el estándar NIST Special Publication 800-18 Revisión 1, Guide for Developing Security Plans for Federal Information Systems, February 2006, o el que le sustituya.

53. Contar con un calendario de revisión y actualización del documento de Plan de Seguridad de Sistemas.

54. Contar con un documento de Plan de Continuidad del Negocio y Recuperación ante Desastres que describa cómo actuará en caso de interrupciones del servicio de emisión Certificados Digitales.

El o los planes deberán ser mantenidos y probados periódicamente, describir los procedimientos de emergencia a seguir que deberán incluir por lo menos los siguientes elementos:

I. Afectación al funcionamiento de los sistemas y/o software;

II. Incidente de seguridad que afecte la operación de los sistemas y/o software;

III. Falla en el hardware donde se ejecuta el producto;

IV. Robo de los Datos de Creación de Firma Electrónica de los Certificados Digitales del Prestador de Servicios de Certificación;

V. Falla de los mecanismos de auditoría;

VI. Mecanismos para preservar evidencia del mal uso de los sistemas, y

VII. Demás casos que por su naturaleza pongan en riesgo el servicio acreditado.

55. El Plan de Continuidad del Negocio y Recuperación ante Desastres deberá ser compatible con las normas y criterios nacionales y/o internacionales, o al menos con los lineamientos descritos en los estándares ISO/IEC serie 27000 o el estándar ETSI TS 102 042 sección 7.4.8 Business continuity management and incident handling, 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 a los descritos 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.

56. Contar con un calendario de revisión y actualización del documento de Plan de Continuidad del Negocio y Recuperación ante Desastres.

57. Contar con un documento de Modelo Operacional de la Autoridad Certificadora conforme al cual operará y prestará sus servicios a efecto de lograr confiabilidad e interoperabilidad, y deberá incluir como mínimo los apartados siguientes:

I. Cuáles son los servicios prestados;

II. Cómo se interrelacionan los diferentes servicios;

III. En qué lugares se operará;

IV. Cómo se protegerán los activos;

V. Qué tipos de Certificados Digitales se entregarán;

VI. Si se generarán Certificados Digitales con diferentes niveles de seguridad;

VII. Cuáles son las políticas y procedimientos de cada tipo de Certificado Digital;

VIII. Interfaces con las Autoridades Registradoras e Interfaces con la Autoridad de Sellado Digital de Tiempo;

IX. Implementación de elementos de seguridad;

X. Procesos de administración;

XI. Sistema de directorios para los Certificados Digitales y sellos digitales de tiempo;

XII. Procesos de auditoría y respaldo;

XIII. Bases de datos a utilizar, y

XIV. Los requerimientos de seguridad física del personal, de las instalaciones y del módulo criptográfico.

58. El Modelo Operacional de la Autoridad Certificadora deberá considerar la Política de Certificados, la Declaración de Prácticas de Certificación, el Sistema de Gestión de Seguridad de la Información, Política de Seguridad de la Información y el Plan de Seguridad de Sistemas por lo que se refiere a la generación de Datos de Creación de Firma Electrónica de los certificados de los usuarios.

59. Contar con un calendario de revisión y actualización del documento de Modelo Operacional de la Autoridad Certificadora.

60. Contar con un documento de Modelo Operacional de la Autoridad Registradora que deberá incluir como mínimo los apartados siguientes:

I. Cuáles son los servicios de registro que se prestarán;

II. En qué lugares se ofrecerán dichos servicios;

III. Qué tipos de Certificados Digitales generados por la Autoridad Certificadora se entregarán;

IV. Los mecanismos para que el propio usuario genere en forma privada y segura sus Datos de Creación de Firma Electrónica.

Asimismo, deberá indicar al usuario el grado de fiabilidad de los mecanismos y dispositivos utilizados;

V. Interfaces con la Autoridad Certificadora;

VI. Implementación de dispositivos de seguridad;

VII. Procesos de administración;

VIII. Procesos de auditoría y respaldo;

IX. Bases de datos a utilizar;

X. Privacidad de datos, y

XI. Descripción de la seguridad física de las instalaciones.

61. 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 Avanzada.

62. Contar con un calendario de revisión y actualización del documento de Modelo Operacional de la Autoridad Registradora.

63. Contar con un documento de Política de Certificados que deberá establecer la Política conforme a la cual se establecerá la confianza del usuario en el servicio, observando lo siguiente:

I. Asegurar su concordancia con la Declaración de Prácticas de Certificación y los procedimientos operacionales;

II. Permitir la interoperabilidad con los Prestadores de Servicios de Certificación ya acreditados y con la Secretaría;

III. Indicar a quién se le puede otorgar un Certificado Digital;

IV. Describir el proceso de verificación en forma fehaciente de la identidad del usuario y su registro, describiendo la forma en que se precisarán los objetivos y alcances de los certificados, y sus limitaciones, incluyendo las obligaciones y responsabilidades que contrae con el usuario en la emisión y utilización del Certificado Digital;

V. Describir las medidas de privacidad y de protección de datos que se aplicarán en materia de Firma Electrónica Avanzada;

VI. Establecer bajo qué circunstancias se puede revocar un Certificado Digital y quiénes pueden solicitarlo, y

VII. Definir el procedimiento para la renovación del Certificado Digital, pudiéndose llevar a cabo de manera alterna, entre presencial y vía remota, siempre y cuando el certificado se encuentre vigente. En ningún caso podrá renovarse el Certificado Digital de manera remota por más de una ocasión.

Para efectos de la renovación remota, deberá describirse de manera fehaciente el proceso de verificación de la identidad del usuario y su registro, describiendo la forma en que se precisarán los objetivos y alcances de los Certificados Digitales, y sus limitaciones, incluyendo las obligaciones y responsabilidades que contrae con el usuario en la emisión y utilización del Certificado Digital.

64. La Política de Certificados será publicada, en el sitio electrónico de cada uno de los Prestadores de Servicios de Certificación.

65. La Política de Certificados tendrá que ser compatible por lo menos con el estándar ETSI TS 102 042 Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates o RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, o los que les sustituyan nacionales y/o internacionales.

66. Contar con un calendario de revisión y actualización del documento de Política de Certificados.

67. Contar con un documento de Declaración de Prácticas de Certificación que deberá establecer la confianza del usuario en el servicio y deberá incluir como mínimo los apartados siguientes:

I. Los procedimientos de operación para otorgar un Certificado y el alcance de aplicación de los mismos;

II. Las responsabilidades y obligaciones del Prestador de Servicios de Certificación y de las personas físicas y/o morales a identificar.

Particularmente desarrollará aquellas inherentes a la emisión, revocación y expiración de certificados; implantando en su caso, lo establecido en la Regla 63 fracción VII si fuera el caso de llevar a cabo una renovación;

III. La vigencia de los Certificados Digitales;

IV. Los controles que se utilizarán para asegurar que el propio usuario genere sus Datos de Creación de Firma Electrónica, autenticación de usuarios, emisión y revocación de certificados;

V. El método detallado de verificación de identidad de la persona física o moral, que se utilizará para la emisión de los certificados, implantando en su caso, lo establecido en la Regla 63 fracción VII si fuera el caso de llevar a cabo una renovación;

VI. Los procedimientos de protección de confidencialidad de la información de los solicitantes de conformidad con la Ley Federal de Protección de Datos Personales en Posesión de Particulares o la que en su momento le sustituya;

VII. El procedimiento para registrar la fecha y hora de todas las operaciones relacionadas con la emisión de los Certificados Digitales y resguardarlas de manera confiable;

VIII. 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 certificados emitidos, pasarán a la Secretaría o a otro Prestador de Servicios de Certificación, en el caso, de suspensión definitiva;

IX. Las medidas de seguridad adoptadas para proteger los Datos de Creación de Firma Electrónica del Certificado de la Autoridad Certificadora del Prestador de Servicios de Certificación;

X. Los controles que se utilizarán para asegurar las auditorías y almacenamiento de información relevante;

XI. La fecha de inicio de operaciones, una vez otorgada la acreditación por la Secretaría;

XII. La Declaración de Prácticas de Certificación o parte de ésta, de acuerdo a la seguridad, será pública, y

XIII. Deberá ser compatible por lo menos con el estándar ETSI TS 102 042 y el RFC 3647 o los que les sustituyan nacionales y/o internacionales.

68. Contar con un calendario de revisión y actualización del documento de Declaración de Prácticas de Certificación.

69. Contar con un documento de Plan de Administración de Claves que deberá establecer el procedimiento conforme al cual generará, protegerá y administrará sus claves criptográficas, y deberá incluir como mínimo los apartados siguientes:

I. Claves de la Autoridad Certificadora;

II. Almacenamiento, respaldo, recuperación y uso de las claves privadas de Autoridad Certificadora y Autoridades Registradoras (en su caso);

III. Distribución del Certificado de la Autoridad Certificadora;

IV. Administración del ciclo de vida del hardware criptográfico que utilice la Autoridad Certificadora y Autoridades Registradoras (en su caso);

V. Los procedimientos que garanticen la seguridad de las claves en todo momento, aun en caso de cambios de personal y componentes tecnológicos;

VI. Utilizar claves con longitud mínima de 2048 bits para los usuarios y mínima de 4096 bits para los Prestadores de Servicios de Certificación, y ajustarse cuando así el avance tecnológico lo requiera y se establezca mediante comunicado por parte de la Secretaría;

VII. Dispositivos seguros para que los usuarios almacenen sus Datos de Creación de Firma Electrónica, compatibles como mínimo con el estándar FIPS 140-2 nivel 3 en sus elementos de seguridad e implantación de los algoritmos criptográficos estándares o el que le sustituya;

VIII. Dispositivos seguros para los usuarios, y

IX. 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, almacenamiento, respaldo y recuperación de la clave, Distribución de la clave pública, uso de clave, Fin del ciclo de vida de la clave, y administración del ciclo de vida del hardware criptográfico, o el que le sustituya.

70. Contar con un calendario de revisión y actualización del documento de Plan de Administración de Claves.

71. Contar con 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 Digitales 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 Declaración de Prácticas de Certificación.

72. Definir los procedimientos que informen de las características de los procesos de creación y verificación de Firma Electrónica Avanzada, así como aquellos que aplicará para dejar sin efecto los certificados, conforme a lo establecido en la Política de Certificados.

73. Establecer un calendario de revisión y actualización de los procedimientos descritos en la Regla 72.

CAPÍTULO V

Obligaciones de Operación

74. La estructura de los Certificados debe ser compatible con la última versión del estándar ISO/IEC 9594-8 Information technology--Open Systems Interconnection--The Directory--Part 8: Public-key and attribute certificate frameworks, y el RFC 5280 *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,* o los que les sustituyan nacionales y/o internacionales, contener los datos que señala el artículo 108 del Código de Comercio para ser considerados como válidos y considerando los siguientes elementos:

I. Los algoritmos utilizados para la Firma Electrónica Avanzada deben ser compatibles con los estándares de la industria, FIPS PUB 186-4. Digital Signature Standard (DSS) o el que le sustituya, que provean un nivel adecuado de seguridad tanto para la firma del Prestador de Servicios de Certificación como del usuario;

II. En el caso de las claves utilizadas para la generación de una Firma Electrónica Avanzada, su tamaño deberá proveer el nivel de seguridad mínimo de 2048 bits para los usuarios y mínimo de 4096 bits para los Prestadores de Servicios de Certificación.

Deberán utilizar la función hash 256 conforme a estándares de la industria o las que la sustituyan, que provean el adecuado nivel de seguridad para este tipo de firmas, tanto del Prestador de Servicios de Certificación como del usuario, y ajustarse cuando así el avance tecnológico lo requiera y se comunique por parte de la Secretaría, y

III. 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 Digitales y al menos los que indican las presentes Reglas.

75. La estructura de la CRL deberá ser compatible con la última versión del estándar ISO/IEC 9594-8 Information Technology–Open Systems Interconnection–The Directory–Part 8: Public Key and attribute certificate frameworks y RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, o los que les sustituyan, nacionales y/o internacionales, e incluir por lo menos la siguiente información:

I. Número de serie de los Certificados Digitales revocados por el emisor con fecha y hora de revocación;

II. La identificación del algoritmo de firma utilizado;

III. El nombre del emisor;

IV. La fecha y hora en que fue emitida la CRL;

V. La fecha en que emitirá la próxima CRL, que no podrá exceder de veinticuatro horas, con independencia de mantener el servicio de OCSP, y

VI. La CRL deberá ser firmada por el Prestador de Servicios de Certificación que la haya emitido, con sus Datos de Creación de Firma Electrónica.

76. Para los efectos del artículo 16o del Reglamento, el procedimiento para obtener la copia de cada Certificado Digital generado por un Prestador de Servicios de Certificación, será mediante envío en línea de cada Certificado Digital a la Secretaría, lo cual será en tiempo real, es decir, se enviará una copia de cada Certificado Digital inmediatamente después del momento de expedición de los certificados generados por el Prestador de Servicios de Certificación en su Autoridad Certificadora.

I. En 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 la Regla anterior, el Prestador de Servicios de Certificación deberá hacer la réplica por cualquier medio en un término no mayor a veinticuatro horas y entregarla a la Secretaría, y

II. El Prestador de Servicios de Certificación deberá cerciorarse que la Secretaría recibió la copia de cada Certificado Digital.

77. Para los efectos del artículo 108 fracción III del Código de Comercio y 17o. fracción III del Reglamento, los Certificados emitidos por el Prestador de Servicios de Certificación deben contener los datos de acreditación ante la Secretaría observarán los siguientes elementos:

I. Los datos que refiere el artículo 108 del Código de Comercio para ser considerado válido;

II. La dirección electrónica en donde se podrá consultar la CRL, y

III. La dirección electrónica del servicio de OCSP en donde se podrá verificar el estado del Certificado Digital.

TÍTULO SEXTO

De la Emisión de Sellos Digitales de Tiempo

78. Para efectos de lo dispuesto en los artículos 102 apartado A fracción II del Código de Comercio y 5o. fracción III del Reglamento, los elementos humanos, económicos, materiales, y tecnológicos que se deberán cubrir para obtener la acreditación como Prestador de Servicios de Certificación en la emisión de Sellos Digitales de Tiempo son:

CAPÍTULO I

De los Elementos Humanos

79. El solicitante deberá contar con un Profesional Jurídico que deberá cumplir con los siguientes requisitos:

I. Ser licenciado en derecho con título y cédula profesional expedidos por la Secretaría de Educación Pública o su equivalente;

II. Demostrar al menos dos años de experiencia en materia notarial, correduría pública o derecho mercantil;

III. Acreditar al menos un año de experiencia en derecho informático, y

IV. Declarar bajo protesta de decir verdad que no ha sido condenado por delito contra el patrimonio de las personas o que haya merecido pena privativa de la libertad, ni que por cualquier motivo haya sido inhabilitado para el ejercicio de su profesión, para desempeñar un puesto en el servicio público, en el sistema financiero o para ejercer el comercio.

80. Contar con un Profesional Informático que deberá cumplir con los siguientes requisitos:

I. Ser licenciado o ingeniero en área informática o afín, con título y cédula profesional expedidos por la Secretaría de Educación Pública o su equivalente;

II. Comprobar al menos dos años de experiencia en el área de criptografía;

III. Acreditar estudios en manejo de software o hardware relacionados con criptografía, y

IV. Declarar bajo protesta de decir verdad que no ha sido condenado por delito contra el patrimonio de las personas o que haya merecido pena privativa de la libertad, ni que por cualquier motivo haya sido inhabilitado para el ejercicio de su profesión, para desempeñar un puesto en el servicio público, en el sistema financiero o para ejercer el comercio.

81. Contar con un Auxiliar de Apoyo Informático de Seguridad quien será responsable del diseño, implementación, cumplimiento del sistema de gestión, planes, políticas, procedimientos y prácticas de seguridad de las instalaciones del Prestador de Servicios de Certificación, este elemento humano podrá ser el Profesional Informático, mismo quien deberá acreditar los siguientes requisitos:

I. Ser licenciado o ingeniero en área informática o afín, con título y cédula profesional expedidos por la Secretaría de Educación Pública o su equivalente;

II. Comprobar un año de experiencia en el área de criptografía;

III. Acreditar estudios en manejo de software o hardware relacionados con criptografía, y

IV. Declarar bajo protesta de decir verdad que no ha sido condenado por delito contra el patrimonio de las personas o que haya merecido pena privativa de la libertad, ni que por cualquier motivo haya sido inhabilitado para el ejercicio de su profesión, para desempeñar un puesto en el servicio público, en el sistema financiero o para ejercer el comercio.

82. El solicitante podrá presentar ante la Secretaría una cantidad mayor de recursos humanos si las necesidades para la prestación del servicio así lo requieren.

83. El solicitante deberá presentar el procedimiento que utilizará para reclutar, seleccionar, evaluar y contratar al personal, el cual deberá describir la forma de corroborar los antecedentes del personal antes de contratarlo, así como su actualización.

En todo caso, la Secretaría deberá autorizar la modificación que el Prestador de Servicios de Certificación realice respecto de los recursos humanos antes mencionados.

CAPÍTULO II

De los Elementos Económicos

84. El solicitante deberá contar con capital que deberá comprender al menos el equivalente a una cuarta parte de la inversión requerida en los términos señalados en el artículo 5 fracción III inciso c del Reglamento.

De igual forma, deberá contar con un seguro de responsabilidad civil que cubrirá el equivalente a 11600 (Once mil seiscientos) unidades de medida y actualización (UMA) diaria en México para cada año y durante el tiempo que permanezca acreditado el Prestador de Servicios de Certificación.

La Secretaría podrá establecer una cantidad mayor a la referida en el párrafo anterior, en caso de que, derivado del análisis de las operaciones en que sea utilizado el servicio de emisión de Sellos Digitales de Tiempo, así lo considere necesario. En este supuesto, se obliga hasta el límite de la suma asegurada a pagar la indemnización que el asegurado deba a un tercero a consecuencia de un hecho que cause un daño previsto en el contrato de seguro.

85. Contar con una fianza cuyo monto no será menor al equivalente a 11600 (Once mil seiscientos) unidades de medida y actualización (UMA) diaria en México para cada año y durante el tiempo que permanezca acreditado el Prestador de Servicios de Certificación.

La Secretaría podrá establecer una cantidad mayor a la referida en el párrafo anterior, en caso de que, derivado del análisis de las operaciones en que sea utilizado el servicio de emisión de Sellos Digitales de Tiempo, así lo considere necesario. En este supuesto, 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, por actuar en sustitución del Prestador de Servicios de Certificación, cuando éste sea suspendido, inhabilitado o cancelado en su ejercicio.

CAPÍTULO III

De los Elementos Materiales

86. El solicitante deberá contar con el espacio físico, controles de seguridad, accesos, perímetros de seguridad física, medidas de protección, así como con las políticas necesarias para garantizar la seguridad para la emisión de Sellos Digitales de Tiempo.

87. Contar con una oficina administrativa sujeta a los procedimientos y prácticas de seguridad firmada por el Profesional Jurídico y el Profesional Informático, los cuales deberán detallar por lo menos los siguientes elementos.

I. Los controles de acceso a efecto de reducir al mínimo los riesgos, y

II. Las áreas seguras donde se resguardará la información concerniente al servicio de emisión de Sellos Digitales de Tiempo.

Para efecto de lo dispuesto en el párrafo anterior, las áreas deberán permanecer aisladas y cerradas dentro del perímetro de seguridad física y contener mobiliario específico con mecanismos de seguridad.

88. Contar con dos centros de datos, uno principal y otro alterno, que deberán cumplir con las certificaciones y estándares de calidad y seguridad, así como contar con procedimientos y prácticas de seguridad firmados por el Profesional Jurídico, el Profesional Informático y el Auxiliar de Apoyo Informático de Seguridad, dichos centros de datos deberán detallar por lo menos los siguientes elementos:

I. Las áreas del servicio de emisión de Sellos Digitales de Tiempo, área de residencia de servidores, así como los recursos humanos que tendrán acceso a éstas.

Dichas áreas deberán estar protegidas con puertas y muros sólidos y firmes, chapas seguras, controles de acceso, sistemas de extinción de incendios, alarmas de seguridad, y se encontrarán limitados sólo al personal autorizado mediante controles de autenticación de por lo menos dos factores.

Para la selección y el diseño de áreas seguras se debe tomar en cuenta la posibilidad de daños por fuego, sismo, inundación, explosión, desorden civil, y otras formas de desastres naturales y causados por el hombre;

II. Para el caso de los servicios compartidos con otra organización, deberá asegurarse la separación física de los estantes de equipos del Prestador de Servicios de Certificación;

III. El acceso de visitas a las áreas deberá ser autorizado por el Auxiliar de Apoyo Informático de Seguridad;

IV. Todos los servicios claves como son, la generación de Sellos Digitales de Tiempo y administración de base de datos, deberán situarse alejados de las áreas de acceso y atención al público;

V. Detalle de los dispositivos electrónicos y su ubicación dentro de las áreas seguras que así lo requieran, siempre bajo control y supervisión para no comprometer la seguridad;

VI. Procedimiento para destruir material de desecho sin posibilidad de recuperación antes de desecharlo;

VII. Los 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, y

VIII. Procedimientos para la gestión de los servicios de procesamiento de información, la cual deberá estar físicamente separada del resto de los servicios, dicha separación podrá ser mediante el empleo de estantes destinados para su uso exclusivo.

89. Los dos centros de datos deberán estar separados cuando menos por 200 Kms., cuando estén localizados en zonas de alta sismicidad.

90. Los procedimientos y prácticas de seguridad de los centros de datos se deberán firmar por el Profesional Jurídico, el Profesional Informático y el Auxiliar de Apoyo Informático de Seguridad, los cuales deberán detallar por lo menos los siguientes elementos:

I. Los recursos humanos que deberán observar los procedimientos y prácticas de seguridad;

II. Bitácora del acceso a las áreas donde se ubique la infraestructura de tiempo confiable autorizado por el Profesional Informático o el Auxiliar de Apoyo Informático de Seguridad;

III. Procedimiento para autorizar y dejar constancia de los accesos dentro del perímetro de seguridad de equipo de grabación, audio o video, con excepción del propio equipo de seguridad y de comunicaciones, los cuales deberán ser autorizados por Profesional Informático o el Auxiliar de Apoyo Informático de Seguridad, dejando evidencia de lo mismo;

IV. Los mecanismos que impidan que personal no autorizado acceda a las áreas del perímetro de seguridad;

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

VI. El equipo instalado y las protecciones físicas para reducir amenazas;

VII. Medios y procedimientos de respaldo de sistemas, deberá contar con un sistema no interrumpible de energía eléctrica e incluir una planta de energía eléctrica de emergencia para asegurar la continuidad del servicio;

VIII. Cableado eléctrico y de datos de los servicios de información confidencial, así como los estándares en la materia que proteja contra daños e intervenciones;

IX. La identificación de las líneas eléctricas, las cuales no deberán interferir con el funcionamiento del cableado de datos;

X. La infraestructura de computación y comunicaciones, la cual deberá contar con el personal y refacciones necesarias o, en su caso, los contratos de mantenimiento preventivo y correctivo, requeridos para garantizar la continua disponibilidad e integridad de los equipos y su software, de acuerdo a las especificaciones y periodos recomendados por los fabricantes;

XI. Los sistemas informáticos, los cuales deberán contar con el personal especializado o, en su caso, con los contratos de mantenimiento preventivo y correctivo, requerido para garantizar la continua disponibilidad e integridad de los sistemas, de acuerdo a las especificaciones y periodos recomendados por los fabricantes;

XII. Procedimientos para evitar que equipos, información y software salgan de los perímetros de seguridad sin autorización;

XIII. Procedimientos para 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 del servicio, éstos nunca deberán salir del perímetro de seguridad designado;

XIV. Procedimientos para evitar que los equipos sean reutilizados o queden en desuso conteniendo información confidencial;

XV. Procedimientos para destrucción de discos duros y demás medios de almacenamiento de información magnético u óptico antes de salir del perímetro de seguridad, dejando la evidencia correspondiente, y

XVI. Mecanismo para registrar el mal funcionamiento, fallas, mantenimientos preventivos y correctivos, de los equipos y sistemas, sensibles para la operación del servicio.

91. La seguridad física deberá ser compatible con las normas y criterios nacionales y/o internacionales y al menos con el estándar ETSI TS 102 042-sección 7.4.4 Physical and environmental security o el que le sustituya.

92. Las actualizaciones y/o modificaciones derivadas de las revisiones realizadas a los procedimientos y prácticas que lleve a cabo el Prestador de Servicios de Certificación deberán ser notificadas a la Secretaría, para su revisión y aprobación.

93. En caso que, los centros de datos principal y alterno sean arrendados, éstos deberán acreditar los estándares y certificaciones nacionales y/o internacionales, de calidad y seguridad con que cuenta el mismo.

Para el caso de la infraestructura de computación y comunicaciones éstas deberán contar con el personal y refacciones o, en su caso, con los contratos de mantenimiento preventivo y correctivo, requeridos para garantizar la continua disponibilidad e integridad de los equipos y su software, de acuerdo a las especificaciones y periodos recomendados por los fabricantes.

Para el caso de los sistemas informáticos, éstos deberán contar con el personal especializado o, en su caso, con los contratos de mantenimiento preventivo y correctivo,

requerido para garantizar la continua disponibilidad e integridad de los sistemas, de acuerdo a las especificaciones y periodos recomendados por los fabricantes.

Las actualizaciones y/o modificaciones derivadas de las revisiones realizadas a los procedimientos y prácticas que se elaboren en los centros de datos arrendados, deberán ser notificadas a la Secretaría.

CAPÍTULO IV

De los Elementos Tecnológicos

94. El solicitante deberá contar con el equipo de cómputo y comunicación, software y/o sistemas que se detalla a continuación:

I. Un servidor de misión crítica para la Autoridad de Sellado Digital de Tiempo o un equipo integrado con los elementos de un sellador digital de tiempo, en caso de utilizar lo anterior de manera virtual, dicha implementación deberá ser incluida en todos los documentos de seguridad informática;

II. Un dispositivo de alta seguridad, que cumpla con estándares de seguridad nacional y/o internacional, compatibles como mínimo con el estándar FIPS 140-2 nivel 3 en sus elementos de seguridad e implantación de los algoritmos criptográficos estándares, o el que le sustituya, para almacenar los Datos de Creación de Firma Electrónica del Certificado de la Autoridad de Sellado Digital de Tiempo del Prestador de Servicios de Certificación;

III. Un enlace mínimo de 100 MB a Internet;

IV. Un ruteador;

V. Un muro de fuego (firewall);

VI. Un sistema cliente de solicitud de Sellos Digitales de Tiempo compatible con el equipo para la Autoridad de Sellado Digital de Tiempo (opcional);

VII. Una computadora para gestionar el sistema de administración del servicio emisión de Sellos Digitales de Tiempo;

VIII. Un sistema de monitoreo de red;

IX. Un sistema confiable de antivirus;

X. Herramientas confiables de detección de vulnerabilidades;

XI. Sistemas confiables de detección y protección de intrusión, y

XII. Las computadoras personales e impresoras necesarias para la prestación del servicio de emisión de Sellos Digitales de Tiempo.

95. Las tecnologías de virtualización deberán ser compatibles con las normas y criterios nacionales y/o internacionales y, al menos con el estándar NIST Guide to Security for Full Virtualization Security, Special Publication 800-125, 2011, o el que le sustituya.

96. Todos los elementos descritos en la Regla 94 deberán considerar redundancia por seguridad.

97. Contar con la infraestructura informática que se detalla a continuación:

I. Una Autoridad de Sellado Digital de Tiempo y el sistema cliente (opcional) que solicita los Sellos Digitales de Tiempo y su redundancia por seguridad;

II. Repositorios para: Datos de Creación de Firma Electrónica del Certificado de la Autoridad de Sellado Digital de Tiempo del Prestador de Servicios de Certificación y sellos digitales de tiempo, y su redundancia por seguridad;

III. Los procesos de administración de la infraestructura informática;

IV. Un manual de Política de Sellos Digitales de Tiempo;

V. Un manual de Declaración de Prácticas de Sellos Digitales de Tiempo, y

VI. Un manual de operación de la Autoridad de Sellado Digital de Tiempo.

98. Contar con un documento de Análisis y Evaluación de Riesgos y Amenaza que deberá detallar por lo menos los siguientes elementos:

I. Los activos críticos;

II. Vulnerabilidades y amenazas de la infraestructura con la que proveerá el o los servicios y determinar los requerimientos de seguridad;

III. Estudio que identifique y evalúe los riesgos e impactos que existen sobre la organización, personas, equipos, sistemas e instalaciones, así como recomendaciones de medidas para mitigarlos, y el impacto que sufrirá el negocio, en caso de interrupciones no planificadas;

IV. Medidas de seguridad para la mitigación de los riesgos detectados;

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

VI. Los impactos que sufrirán los servicios del Prestador de Servicios de Certificación en caso de interrupciones no planificadas, y

VII. Adoptar Adoptar Guide for Conducting Risk Assessments. NIST Special Publication 800-30 Revision 1. September 2012, equivalente o el que le sustituya.

99. Contar con un calendario de revisión y actualización del documento de Análisis y Evaluación de Riesgos y Amenazas.

100. Contar con un documento de Política de Seguridad de la Información que deberá detallar por lo menos los siguientes elementos:

I. Ser congruente con el objeto del servicio de emisión de Sellos Digitales de Tiempo que ofrecerá el Prestador de Servicios de Certificación;

II. Los objetivos de seguridad claros, generales, no técnicos, que se desarrollarán a partir del resultado del Análisis y Evaluación de Riesgos y Amenazas;

III. Estar basada en las recomendaciones de los estándares ISO/IEC de la serie 27000 o los que le sustituyan;

IV. La Política de Seguridad de la Información puede estar conformada con una política general y soportada con políticas específicas;

V. Identificar 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, los cuales deberán desarrollarse a partir del resultado del Análisis y Evaluación de Riesgos y Amenazas;

VI. Las reglas que indiquen cómo son provistos los servicios y las medidas de seguridad asociadas;

VII. Ser consistente con la Política de Sellos Digitales de Tiempo y con la Declaración de Prácticas de Sellos Digitales de Tiempo, a que se refiere el presente TÍTULO;

VIII. Adoptar el proceso de Internet Security Policy: A Technical Guide, by the National Institute of Standards and Technologies (NIST), o uno similar, y

IX. Desarrollar procedimientos y buenas prácticas de seguridad para apoyar la aplicación de las políticas de seguridad.

101. Contar con un calendario de revisión y actualización del documento de Política de Seguridad de la Información.

102. Contar con un documento de Política de Seguridad Física que deberá detallar por lo menos los siguientes elementos:

I. Control de acceso físico;

II. Protección y recuperación ante desastres;

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

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

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

103. Contar con un calendario de revisión y actualización del documento de Política de Seguridad Física.

104. Contar con un documento de Sistema de Gestión de Seguridad de la Información conforme a los estándares ISO/IEC de la serie 27000 o los que les sustituyan.

105. El Sistema de Gestión de Seguridad de la Información deberá garantizar el logro de los objetivos de la Política de Sellos Digitales de Tiempo y de la Declaración de Prácticas de Sellos Digitales de Tiempo.

106. Contar con un calendario de revisión y actualización del documento de Sistema de Gestión de Seguridad de la Información.

107. Contar con un documento de Plan de Seguridad de Sistemas el cual deberá ser coherente con el Sistema de Gestión de Seguridad de la Información, así como con la Política de Seguridad de la Información y, de aplicación para el servicio de emisión de Sellos Digitales de Tiempo, mismo que deberá describir los requerimientos de seguridad de los sistemas, los controles a implantar, las responsabilidades y acceso de las personas a los sistemas.

El Plan de Seguridad de Sistemas deberá ser compatible con las normas y criterios nacionales y/o internacionales y, al menos con el estándar NIST Special Publication 800-18 Revisión 1, Guide for Developing Security Plans for Federal Information Systems, February 2006 o los que le sustituyan.

108. Contar con un calendario de revisión y actualización del documento de Plan de Seguridad de Sistemas.

109. Contar con un documento de Plan de Continuidad del Negocio y Recuperación ante Desastres que describa cómo actuará en caso de interrupciones del servicio de emisión Sellos Digitales de Tiempo.

El o los planes deberán ser mantenidos y probados periódicamente, describir los procedimientos de emergencia a seguir que deberán incluir por lo menos los siguientes elementos:

I. Afectación al funcionamiento de los sistemas y/o software;

II. Incidente de seguridad que afecte la operación de los sistemas y/o software;

III. Falla en el hardware donde se ejecuta el producto;

IV. Robo de los Datos de Creación de Firma Electrónica Avanzada del Certificado de la Autoridad de Sellado Digital de Tiempo del Prestador de Servicios de Certificación;

V. Falla de los mecanismos de auditoría;

VI. Mecanismos para preservar evidencia del mal uso de los sistemas, y

VII. Demás casos que por su naturaleza pongan en riesgo el servicio acreditado.

110. El Plan de Continuidad del Negocio y Recuperación ante Desastres, deberá ser compatible con las normas y criterios nacionales y/o internacionales, o al menos con los lineamientos descritos en el estándar ISO/IEC serie 27000 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 a los descritos 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.

111. Contar con un calendario de revisión y actualización del documento de Plan de Continuidad del Negocio y Recuperación ante Desastres.

112. Contar con un documento de Modelo Operacional de la Autoridad de Sellado Digital de Tiempo conforme al cual operará y prestará sus servicios a efecto de lograr confiabilidad e interoperabilidad, que deberá detallar por lo menos los siguientes elementos:

I. Cuáles son los servicios prestados;

II. Cómo se interrelacionan los diferentes servicios;

III. En qué lugares se operará;

IV. Cómo se protegerán los activos;

V. Implementación de elementos de seguridad;

VI. Procesos de administración;

VII. Sistema de directorios para los sellos digitales de tiempo;

VIII. Procesos de auditoría y respaldo, y

IX. Bases de datos a utilizar.

113. El Modelo Operacional de la Autoridad de Sellado Digital de Tiempo deberá incluir los requerimientos de seguridad física del personal, de las instalaciones y del módulo criptográfico.

114. Contar con un calendario de revisión y actualización del documento de Modelo Operacional de la Autoridad de Sellado Digital de Tiempo.

115. Contar con un documento de Política de Sellos Digitales de Tiempo la cual establecerá la confianza del usuario en el servicio, observando lo siguiente:

I. Asegurar su concordancia con la Declaración de Prácticas de Sellos Digitales de Tiempo y los procedimientos operacionales, y

II. Indicar a quién se le puede otorgar un sello digital de tiempo.

116. La Política de Sellos Digitales de Tiempo tendrá que ser compatible con el RFC 3628 “Policy Requirements for Time-Stamping Authorities (TSAs)” o el que le sustituya nacional y/o internacional.

117. Contar con un calendario de revisión y actualización del documento de Política de Sellos Digitales de Tiempo.

118. Contar con un documento de Declaración de Prácticas de Sellos Digitales de Tiempo la cual establecerá la confianza del usuario en el servicio y deberá detallar por lo menos los siguientes elementos:

I. Los procedimientos de operación para otorgar un sello digital de tiempo y el alcance de aplicación de los mismos;

II. Las responsabilidades y obligaciones del Prestador de Servicios de Certificación y de sus usuarios;

III. Las medidas de seguridad adoptadas para proteger sus Datos de Creación de Firma Electrónica para sellos digitales de tiempo;

IV. Los controles que se utilizarán para asegurar las auditorías y almacenamiento de información relevante;

V. Una vez otorgada la acreditación por la Secretaría, la fecha de inicio de operaciones;

VI. La Declaración de Prácticas de Sellos Digitales de Tiempo deberá ser compatible con el RFC 3628 o el que le sustituya nacional o internacional, y

VII. La Declaración de Prácticas de Sellos Digitales de Tiempo o parte de ésta, de acuerdo a la seguridad, será pública.

119. Contar con un calendario de revisión y actualización del documento de Declaración de Prácticas de Sellos Digitales de Tiempo.

120. Contar con un documento de Plan de Administración de Claves el cual establecerá el procedimiento conforme al cual generará, protegerá y administrará sus claves criptográficas, detallando por lo menos los siguientes elementos:

I. Claves de la Autoridad de Sellado Digital de Tiempo;

II. Almacenamiento, respaldo, recuperación y uso de las claves privadas de la Autoridad de Sellado Digital de Tiempo;

III. Distribución del Certificado de la Autoridad de Sellado Digital de Tiempo;

IV. Administración del ciclo de vida del hardware criptográfico que utilice la Autoridad de Sellado Digital de Tiempo;

V. Los procedimientos que garanticen la seguridad de las claves en todo momento, aun en caso de cambios de personal y componentes tecnológicos;

VI. Utilizar claves con longitud mínima de 4096 bits y ajustarse cuando así el avance tecnológico lo requiera previo comunicado de la Secretaría.

VII. La Autoridad de Sellado Digital de Tiempo utilizará dispositivos seguros para almacenar sus Datos de Creación de Firma Electrónica para Sellos Digitales de Tiempo compatibles como mínimo con el estándar FIPS 140-2 nivel 3 en sus elementos de seguridad e implantación de los algoritmos criptográficos estándares, o el que le sustituya, y

VIII. 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, almacenamiento, respaldo y recuperación de la clave, Distribución de la clave pública, uso de clave, fin del ciclo de vida de la clave y Administración del ciclo de vida del hardware criptográfico, o el que le sustituya.

121. Contar con un calendario de revisión y actualización del documento de Plan de Administración de Claves.

122. Contar con 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 la Política de Sellos Digitales de Tiempo y Declaración de Prácticas de Sellos Digitales de Tiempo.

123. Celebrar un contrato de prestación de servicios anual con el Centro Nacional de Metrología (CNM), para obtener la transferencia segura de la escala de tiempo (Tiempo Universal Coordinado) UTC, por sus siglas en inglés, que se envíe a la Autoridad de Sellado Digital de Tiempo, así como su redundancia por seguridad.

TÍTULO SÉPTIMO

De la Constancia de Conservación de Mensaje de Datos emitida de conformidad con la NOM-151-SCFI-2016

124. Para efectos de lo dispuesto en los artículos 102 apartado A fracción II del Código de Comercio y 5o. fracción III del Reglamento, los elementos humanos, económicos, materiales y tecnológicos que se deberán cubrir para obtener la acreditación como Prestador de Servicios de Certificación en el servicio de Constancias de Conservación de Mensaje de Datos emitidas de conformidad con la NOM-151-SCFI-2016 son:

CAPÍTULO I

De los Elementos Humanos

125. El solicitante deberá contar con un Profesional Jurídico que deberá cumplir con los siguientes requisitos:

I. Ser licenciado en derecho con título y cédula profesional expedidos por la Secretaría de Educación Pública o su equivalente;

II. Demostrar al menos dos años de experiencia en materia notarial, correduría pública o derecho mercantil;

III. Acreditar al menos un año de experiencia en derecho informático, y

IV. Declarar bajo protesta de decir verdad que no ha sido condenado por delito contra el patrimonio de las personas o que haya merecido pena privativa de la libertad, ni que por cualquier motivo haya sido inhabilitado para el ejercicio de su profesión, para desempeñar un puesto en el servicio público, en el sistema financiero o para ejercer el comercio.

126. Contar con un Profesional Informático que deberá cumplir con los siguientes requisitos.

I. Ser licenciado o ingeniero en área informática o afín, con título y cédula profesional expedidos por la Secretaría de Educación Pública o su equivalente;

II. Comprobar al menos dos años de experiencia en el área de criptografía;

III. Acreditar estudios en manejo de software o hardware relacionados con criptografía, y

IV. Declarar bajo protesta de decir verdad que no ha sido condenado por delito contra el patrimonio de las personas o que haya merecido pena privativa de la libertad, ni que por cualquier motivo haya sido inhabilitado para el ejercicio de su profesión, para desempeñar un puesto en el servicio público, en el sistema financiero o para ejercer el comercio.

127. Contar con un Auxiliar de Apoyo Informático de Seguridad quien será el responsable del diseño, implantación, cumplimiento del sistema de gestión, planes, políticas, procedimientos y prácticas de seguridad de las instalaciones del Prestador de Servicios de Certificación, este elemento humano podrá ser el Profesional Informático, mismo quien deberá acreditar los siguientes requisitos:

I. Ser licenciado o ingeniero en área informática o afín, con título y cédula profesional expedidos por la Secretaría de Educación Pública o su equivalente;

II. Comprobar al menos dos años de experiencia en el área de criptografía;

III. Acreditar estudios en manejo de software o hardware relacionados con criptografía, y

IV. Declarar bajo protesta de decir verdad que no ha sido condenado por delito contra el patrimonio de las personas o que haya merecido pena privativa de la libertad, ni que por cualquier motivo haya sido inhabilitado para el ejercicio de su profesión, para desempeñar un puesto en el servicio público, en el sistema financiero o para ejercer el comercio.

128. El solicitante podrá presentar ante la Secretaría una cantidad mayor de recursos humanos si las necesidades para la prestación del servicio así lo requieren.

129. El solicitante deberá presentar el procedimiento que utilizará para reclutar, seleccionar, evaluar y contratar al personal, el cual deberá describir la forma de corroborar los antecedentes del personal antes de contratarlo, así como su actualización.

En todo caso, la Secretaría deberá autorizar la modificación que el Prestador de Servicios de Certificación realice respecto de los recursos humanos antes mencionados.

CAPÍTULO II

De los Elementos Económicos

130. El solicitante deberá contar con capital que deberá comprender al menos el equivalente a una cuarta parte de la inversión requerida en los términos señalados en el artículo 5 fracción III inciso c del Reglamento.

De igual forma, deberá contar con un seguro de responsabilidad civil que cubrirá el equivalente a 11600 (Once mil seiscientos) unidades de medida y actualización (UMA) diaria en México para cada año y durante el tiempo que permanezca acreditado el Prestador de Servicios de Certificación.

La Secretaría podrá establecer una cantidad mayor a la referida en el párrafo anterior, en caso de que, derivado del análisis de las operaciones en que sea utilizado el servicio de emisión de Constancias de Conservación de Mensajes de Datos, así lo considere necesario. En este supuesto, se obliga hasta el límite de la suma asegurada a pagar la indemnización que el asegurado deba a un tercero a consecuencia de un hecho que cause un daño previsto en el contrato de seguro.

131. Contar con una fianza cuyo monto no será menor al equivalente a 11600 (Once mil seiscientos) unidades de medida y actualización (UMA) diaria en México para cada año y durante el tiempo que permanezca acreditado el Prestador de Servicios de Certificación.

La Secretaría podrá establecer una cantidad mayor a la referida en el párrafo anterior, en caso de que, derivado del análisis de las operaciones en que sea utilizado el servicio de emisión de Constancias de Conservación de Mensajes de Datos, así lo considere necesario. En este supuesto, 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, por actuar en sustitución del Prestador de Servicios de Certificación, cuando éste sea suspendido, inhabilitado o cancelado en su ejercicio.

CAPÍTULO III

De los Elementos Materiales

132. El solicitante deberá contar con el espacio físico, controles de seguridad, accesos, perímetros de seguridad física, medidas de protección, así como con las políticas necesarias para garantizar la seguridad para la emisión de Constancias de Conservación de Mensaje de Datos de conformidad con la NOM-151-SCFI-2016.

133. Contar con una oficina administrativa sujeta a los procedimientos y prácticas de seguridad firmados por el Profesional Jurídico, el Profesional Informático y el Auxiliar de Apoyo Informático de Seguridad, los cuales deberán detallar por lo menos los siguientes elementos:

I. Los controles de acceso a efecto de reducir al mínimo los riesgos, y

II. Las áreas seguras donde se resguardará la información concerniente al servicio de Constancias de Conservación de Mensaje de Datos que se emitan de conformidad con la NOM-151-SCFI-2016.

Para efecto de lo dispuesto en el párrafo anterior, las áreas deberán permanecer aisladas y cerradas dentro del perímetro de seguridad física, contener mobiliario específico con mecanismos de seguridad.

134. Contar con dos centros de datos, uno principal y otro alterno, que deberán cumplir con las certificaciones y estándares de calidad y seguridad, así como contar con procedimientos y prácticas de seguridad firmados por el Profesional Jurídico, el Profesional Informático y el Auxiliar de Apoyo Informático de Seguridad, dichos centros deberán detallar por lo menos los siguientes elementos:

I. Las áreas de emisión de las Constancias de Conservación de Mensaje de Datos que se emitan de conformidad con la NOM-151-SCFI-2016, Área de residencia de servidores, así como los recursos humanos que tendrán acceso a éstas.

Dichas áreas deberán estar protegidas con puertas y muros sólidos y firmes, chapas seguras, controles de acceso, sistemas de extinción de incendios, alarmas de seguridad, y se encontrarán limitados sólo al personal autorizado mediante controles de autenticación de por lo menos dos factores.

Para la selección y el diseño de áreas seguras se debe tomar en cuenta la posibilidad de daños por fuego, sismo, inundación, explosión, desorden civil, y otras formas de desastres naturales y causados por el hombre;

II. Para el caso de los servicios compartidos con otra organización, deberá asegurarse la separación física de los racks de equipos del Prestador de Servicios de Certificación;

III. El acceso de visitas a las áreas deberá ser autorizado por el Auxiliar de Apoyo Informático de Seguridad;

IV. Todos los servicios claves como son, la emisión de Constancia de Conservación de Mensaje de Datos y administración de base de datos, deberán situarse alejados de las áreas de acceso y atención al público;

V. Detalle de los dispositivos electrónicos y su ubicación dentro de las áreas seguras que así lo requieran, siempre bajo control y supervisión para no comprometer la seguridad;

VI. Procedimiento para destruir material de desecho, como cajas de cartón, empaques, entre otros, sin posibilidad de recuperación antes de desecharlo;

VII. Los 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, y

VIII. Procedimientos para la gestión de los servicios de procesamiento de información, la cual deberá estar físicamente separada del resto de los servicios, dicha

separación podrá ser mediante el empleo de estantes destinados para su uso exclusivo.

135. Los dos centros de datos deberán estar separados cuando menos por 200 Kms., cuando estén localizados en zonas de alta sismicidad.

136. Los procedimientos y prácticas de seguridad de los centros de datos se deberán firmar por el Profesional Jurídico, el Profesional Informático y el Auxiliar de Apoyo Informático de Seguridad, detallando los siguientes elementos para el personal dentro del perímetro de seguridad:

I. Los recursos humanos que deberán observar los procedimientos y prácticas de seguridad;

II. Bitácora del acceso a las áreas donde se ubique la infraestructura de emisión de Constancias de Conservación de Mensaje de Datos autorizado por el Profesional Informático o el Auxiliar de Apoyo Informático de Seguridad;

III. Procedimiento para autorizar y dejar constancia de los accesos dentro del perímetro de seguridad de equipo de grabación, audio o video, con excepción del propio equipo de seguridad y de comunicaciones, los cuales deberán ser autorizados por Profesional Informático o el Auxiliar de Apoyo Informático de Seguridad, dejando evidencia de lo mismo;

IV. Los mecanismos que impidan que personal no autorizado acceda a las áreas del perímetro de seguridad;

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

VI. El equipo instalado y las protecciones físicas para reducir amenazas;

VII. Medios y procedimientos de respaldo de sistemas, deberá contar con un sistema no interrumpible de energía eléctrica e incluir una planta de energía eléctrica de emergencia para asegurar la continuidad del servicio;

VIII. Cableado eléctrico y de datos de los servicios de información confidencial, así como los estándares en la materia que proteja contra daños e intervenciones;

IX. La identificación de las líneas eléctricas las cuales no deberán interferir con el funcionamiento del cableado de datos;

X. La infraestructura de computación y comunicaciones las cuales deberán contar con el personal y refacciones necesarias o, en su caso, los contratos de mantenimiento preventivo y correctivo, requeridos para garantizar la continua disponibilidad e integridad de los equipos y su software, de acuerdo a las especificaciones y periodos recomendados por los fabricantes;

XI. Los sistemas informáticos los cuales deberán contar con el personal especializado o, en su caso, con los contratos de mantenimiento preventivo y correctivo,

requerido para garantizar la continua disponibilidad e integridad de los sistemas, de acuerdo a las especificaciones y periodos recomendados por los fabricantes;

XII. Procedimientos para evitar que equipos, información y software salgan de los perímetros de seguridad sin autorización;

XIII. Procedimientos para 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 del servicio, éstos nunca deberán salir del perímetro de seguridad designado;

XIV. Procedimientos para evitar que los equipos sean reutilizados o queden en desuso conteniendo información confidencial;

XV. Procedimientos para destrucción de discos duros y demás medios de almacenamiento de información magnético u óptico antes de salir del perímetro de seguridad, dejando la evidencia correspondiente, y

XVI. Mecanismo para registrar el mal funcionamiento, fallas, mantenimientos preventivos y correctivos, de los equipos y sistemas, sensibles para la operación del servicio.

137. La seguridad física deberá ser compatible con las normas y criterios nacionales y/o internacionales y al menos con el estándar ETSI TS 102 042-sección 7.4.4 Physical and Environmental Security o el que le sustituya.

138. Las actualizaciones y/o modificaciones derivadas de las revisiones realizadas a los procedimientos y prácticas que lleve a cabo el Prestador de Servicios de Certificación, deberán ser notificadas a la Secretaría, para su revisión y aprobación.

139. En caso de que los centros de datos principal y alterno sean arrendados, deberán acreditar cuáles son los estándares y certificaciones nacionales y/o internacionales, de calidad y seguridad con que cuentan los mismos.

Para el caso de la infraestructura de computación y comunicaciones éstas deberán contar con el personal y refacciones o, en su caso, con los contratos de mantenimiento preventivo y correctivo, requeridos para garantizar la continua disponibilidad e integridad de los equipos y su software, de acuerdo a las especificaciones y periodos recomendados por los fabricantes.

Para el caso de los sistemas informáticos, éstos deberán contar con el personal especializado o, en su caso, con los contratos de mantenimiento preventivo y correctivo, requerido para garantizar la continua disponibilidad e integridad de los sistemas, de acuerdo a las especificaciones y periodos recomendados por los fabricantes.

Las actualizaciones y/o modificaciones derivadas de las revisiones realizadas a los procedimientos y prácticas que se elaboren en los centros de datos arrendados, deberán ser notificadas a la Secretaría.

CAPÍTULO IV

De los Elementos Tecnológicos

140. El solicitante deberá contar con el equipo de cómputo y comunicación, software y/o sistemas que se detalla a continuación:

I. Un servidor de misión crítica para la Autoridad de Constancias de Conservación de Mensaje de Datos emitidas de conformidad con la NOM-151-SCFI-2016, en caso de utilizar lo anterior de manera virtual, dicha implementación deberá ser incluida en todos los documentos de seguridad informática;

II. Un dispositivo de alta seguridad, que cumpla con estándares de seguridad nacional y/o internacional, compatibles como mínimo con el estándar FIPS 140-2 nivel 3 en sus elementos de seguridad e implantación de los algoritmos criptográficos estándares, o el que le sustituya, para almacenar los Datos de Creación de Firma Electrónica del Certificado de la Autoridad de Constancias de Conservación de Mensaje de Datos del Prestador de Servicios de Certificación;

III. Un enlace mínimo de 100 MB a Internet;

IV. Un ruteador;

V. Un muro de fuego (firewall);

VI. Un sistema cliente de Constancia de Conservación de Mensaje de Datos compatible con el equipo para la Autoridad de Constancias de Conservación de Mensaje de Datos emitidas de conformidad con la NOM-151-SCFI-2016 (opcional);

VII. Una computadora para gestionar el sistema de administración del servicio de Constancias de Conservación de Mensaje de Datos emitidas de conformidad con la NOM-151-SCFI-2016;

VIII. Un sistema de monitoreo de red;

IX. Un sistema confiable de antivirus;

X. Herramientas confiables de detección de vulnerabilidades;

XI. Sistemas confiables de detección y protección de intrusión, y

XII. Las computadoras personales e impresoras necesarias para la prestación del servicio de Constancias de Conservación de Mensaje de Datos emitidas de conformidad con la NOM-151-SCFI-2016.

141. Las tecnologías de virtualización deberán ser compatibles con las normas y criterios nacionales y/o internacionales y, al menos con el estándar NIST Guide to Security for Full Virtualization Security, Special Publication 800-125, 2011, o el que le sustituya.

142. Todos los elementos mencionados en la Regla 140 deberán considerar redundancia por seguridad.

143. Contar con la infraestructura Informática que deberá incluir al menos lo siguiente:

I. Una Autoridad de Constancias de Conservación de Mensaje de Datos emitidas de conformidad con la NOM-151-SCFI-2016 y el sistema cliente (opcional) que solicita la constancia de conservación de mensaje de datos, y su redundancia por seguridad;

II. Repositorios para: Datos de Creación de Firma Electrónica del Certificado de la Autoridad de Constancias de Conservación de Mensaje de Datos del Prestador de Servicios de Certificación, y su redundancia por seguridad;

III. Los procesos de administración de la Infraestructura Informática;

IV. Un manual de Política de Constancias de Conservación de Mensaje de Datos emitidas de conformidad con la NOM-151-SCFI-2016;

V. Un manual de Declaración de Prácticas de Constancias de Conservación de Mensaje de Datos emitidas de conformidad con la NOM-151-SCFI-2016, y

VI. Un manual de operación de la Autoridad de Constancias de Conservación de Mensaje de Datos emitidas de conformidad con la NOM-151-SCFI-2016.

144. Contar con un documento de Análisis y Evaluación de Riesgos y Amenazas que deberá detallar por lo menos los siguientes elementos:

I. Los activos críticos;

II. Vulnerabilidades y amenazas de la infraestructura con la que proveerá el o los servicios y determinar los requerimientos de seguridad;

III. Estudio que identifique y evalúe los riesgos e impactos que existen sobre la organización, personas, equipos, sistemas e instalaciones, así como recomendaciones de medidas para mitigarlos, y el impacto que sufrirá el negocio, en caso de interrupciones no planificadas;

IV. Medidas de seguridad para la mitigación de los riesgos detectados;

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

VI. Los impactos que sufrirán los servicios del Prestador de Servicios de Certificación, en caso de interrupciones no planificadas, y

VII. Adoptar la Guide for Conducting Risk Assessments. NIST Special Publication 800-30 Revision 1. September 2012, equivalente o el que le sustituya.

145. Contar con un calendario de revisión y actualización del documento de Análisis y Evaluación de Riesgos y Amenazas.

146. Contar con un documento de Política de Seguridad de la Información que deberá detallar por lo menos los siguientes elementos:

I. Ser congruente con el objeto del servicio de Constancias de Conservación de Mensaje de Datos emitidas de conformidad con la NOM-151-SCFI-2016 que ofrecerá el Prestador de Servicios de Certificación;

II. Los objetivos de seguridad claros, generales, no técnicos, que se desarrollarán a partir del resultado del Análisis y Evaluación de Riesgos y Amenazas;

III. Estar basada en las recomendaciones de los estándares ISO/IEC de la serie 27000 o los que le sustituyan;

IV. La Política de Seguridad de la información puede estar conformada con una política general y soportada con políticas específicas;

V. Identificar 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, los cuales deberán desarrollarse a partir del resultado del Análisis y Evaluación de Riesgos y Amenazas;

VI. Las reglas que indiquen cómo son provistos los servicios y las medidas de seguridad asociadas;

VII. Ser consistente con la Política de Constancias de Conservación de Mensaje de Datos emitidas de conformidad con la NOM-151-SCFI-2016 y con la Declaración de Prácticas de Constancias de Conservación de Mensaje de Datos emitidas de conformidad con la NOM-151-SCFI-2016, a que se refieren en el presente TÍTULO;

VIII. Adoptar un proceso de Internet Security Policy: A Technical Guide, by the National Institute of Standards and Technologies (NIST), o un proceso similar, y

IX. Procedimientos y buenas prácticas de seguridad para apoyar la aplicación de las políticas de seguridad.

147. Contar con un calendario de revisión y actualización del documento de Política de Seguridad de la Información.

148. Contar con un documento de Política de Seguridad Física que deberá detallar por lo menos los siguientes elementos:

I. Control de acceso físico;

II. Protección y recuperación ante desastres;

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

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

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

149. Contar con un calendario de revisión y actualización del documento de Política de Seguridad Física.

150. Contar con un documento de Sistema de Gestión de Seguridad de la Información conforme a los estándares ISO/IEC de la serie 27000 o los que les sustituyan.

151. El Sistema de Gestión de Seguridad de la Información deberá garantizar el logro de los objetivos de la Política de Constancias de Conservación de Mensaje de Datos emitidas de conformidad con la NOM-151-SCFI-2016 y de la Declaración de Prácticas de Constancias de Conservación de Mensaje de Datos emitidas de conformidad con la NOM-151-SCFI-2016.

152. Contar con un calendario de revisión y actualización del documento de Sistema de Gestión de Seguridad de la Información.

153. Contar con un documento de Plan de Seguridad de Sistemas el cual deberá ser coherente con el Sistema de Gestión de Seguridad de la Información y la Política de Seguridad de la Información y, de aplicación para el servicio de Constancias de Conservación de Mensaje de Datos emitidas de conformidad con la NOM-151-SCFI-2016 a acreditar, mismo que deberá describir los requerimientos de seguridad de los sistemas y los controles a implantar y cumplir; así como delinear las responsabilidades y acceso de las personas a los sistemas.

El Plan de Seguridad de Sistemas deberá ser compatibles con las normas y criterios nacionales y/o internacionales y, al menos con el estándar NIST Special Publication 800-18 Revisión 1, Guide for Developing Security Plans for Federal Information Systems, February 2006 o los que le sustituyan.

154. Contar con un calendario de revisión y actualización del documento de Plan de Seguridad de Sistemas.

155. Contar con un documento de Plan de Continuidad del Negocio y Recuperación ante Desastres que describa cómo actuará en caso de interrupciones del servicio de emisión de Constancias de Conservación de Mensaje de Datos emitidas de conformidad con la NOM-151-SCFI-2016 y los servicios a acreditar, según sea el caso.

El o los planes deberán ser mantenidos y probados periódicamente, describir los procedimientos de emergencia a seguir que deberán incluir por lo menos los siguientes elementos:

I. Afectación al funcionamiento de los sistemas y/o software;

II. Incidente de seguridad que afecte la operación de los sistemas y/o software;

III. Falla en el hardware donde se ejecuta el producto;

IV. Robo de los Datos de Creación de Firma Electrónica Avanzada del Certificado de la Autoridad de Constancias de Conservación de Mensaje de Datos del Prestador de Servicios de Certificación;

V. Falla de los mecanismos de auditoría;

VI. Mecanismos para preservar evidencia del mal uso de los sistemas, y

VII. Demás casos imprevistos en las presentes Reglas y que por su naturaleza pongan en riesgo el servicio acreditado.

156. El Plan de Continuidad del Negocio y Recuperación ante Desastres, deberá ser compatible con las normas y criterios nacionales y/o internacionales, o al menos con los lineamientos descritos en los estándares ISO/IEC serie 27000 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 a los descritos 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.

157. Contar con un calendario de revisión y actualización del documento de Plan de Continuidad del Negocio y Recuperación ante Desastres.

158. Contar con un documento de Modelo Operacional de la Autoridad de Constancias de Conservación de Mensaje de Datos emitidas de conformidad con la NOM-151-SCFI-2016 conforme al cual operará y prestará sus servicios a efecto de lograr confiabilidad e interoperabilidad, que deberá detallar por lo menos los siguientes elementos:

I. Cuáles son los servicios prestados;

II. Cómo se interrelacionan los diferentes servicios;

III. En qué lugares se operará;

IV. Cómo se protegerán los activos;

V. Implementación de elementos de seguridad;

VI. Procesos de administración;

VII. Sistema de directorios para la constancia de conservación de mensaje de datos;

VIII. Procesos de auditoría y respaldo, y

IX. Bases de datos a utilizar.

159. El Modelo Operacional de la Autoridad de Constancias de Conservación de Mensaje de Datos emitidas de conformidad con la NOM-151-SCFI-2016 deberá incluir los requerimientos de seguridad física del personal, de las instalaciones y del módulo criptográfico.

160. Contar con un calendario de revisión y actualización del documento de Modelo Operacional de la Autoridad de Constancias de Conservación de Mensaje de Datos emitidas de conformidad con la NOM-151-SCFI-2016.

161. Contar con un manual de Política de Constancias de Conservación de Mensaje de Datos emitidas de conformidad con la NOM-151-SCFI-2016, deberá establecer la Política conforme a la cual se establecerá la confianza del usuario en el servicio, observando lo siguiente:

I. Asegurar su concordancia con la Declaración de Prácticas de Constancias de Conservación de Mensaje de Datos emitidas de conformidad con la NOM-151-SCFI-2016 y los procedimientos operacionales, y

II. Indicar a quién se le puede otorgar una Constancia de Conservación de Mensaje de Datos.

162. Contar con un calendario de revisión y actualización del documento de Política de Constancias de Conservación de Mensaje de Datos emitidas de conformidad con la NOM-151-SCFI-2016.

163. Contar con un manual de Declaración de Prácticas de Constancias de Conservación de Mensaje de Datos emitidas de conformidad con la NOM-151-SCFI-2016, deberá establecer la confianza del usuario en el servicio y deberá detallar por lo menos los siguientes elementos:

I. Los procedimientos de operación para otorgar la constancia de conservación de mensaje de datos y el alcance de aplicación de los mismos;

II. Las responsabilidades y obligaciones del Prestador de Servicios de Certificación y de sus usuarios;

III. Las medidas de seguridad adoptadas para proteger sus Datos de Creación de Firma Electrónica para la Constancia de Conservación de Mensaje de Datos;

IV. Los controles que se utilizarán para asegurar las auditorías y almacenamiento de información relevante;

V. Una vez otorgada la acreditación por la Secretaría, la fecha de inicio de operaciones, y

VI. La Declaración de Prácticas de Constancias de Conservación de Mensaje de Datos emitidas de conformidad con la NOM-151-SCFI-2016 o parte de ésta, de acuerdo a la seguridad, será pública.

164. Contar con un calendario de revisión y actualización del documento de Declaración de Prácticas de Constancias de Conservación de Mensaje de Datos emitidas de conformidad con la NOM-151-SCFI-2016.

165. Contar con un documento de Plan de Administración de Claves, deberá establecer el procedimiento conforme al cual generará, protegerá y administrará sus claves criptográficas, detallando por lo menos los siguientes elementos:

I. Claves de la Autoridad de Constancias de Conservación de Mensaje de Datos emitidas de conformidad con la NOM-151-SCFI-2016;

II. Almacenamiento, respaldo, recuperación y uso de las claves privadas de la Autoridad de Constancias de Conservación de Mensaje de Datos emitidas de conformidad con la NOM-151-SCFI-2016;

III. Distribución del Certificado de la Autoridad de Constancias de Conservación de Mensaje de Datos emitidas de conformidad con la NOM-151-SCFI-2016;

IV. Administración del ciclo de vida del hardware criptográfico que utilice la Autoridad de Constancias de Conservación de Mensaje de Datos emitidas de conformidad con la NOM-151-SCFI-2016;

V. Los procedimientos que garanticen la seguridad de las claves en todo momento, aun en caso de cambios de personal, componentes tecnológicos, y demás que señalan las presentes Reglas;

VI. Utilizar claves con longitud mínima de 4096 bits para los Prestadores de Servicios de Certificación, y ajustarse cuando así el avance tecnológico lo requiera y se establezca mediante comunicado por parte de la Secretaría;

VII. La Autoridad de Constancias de Conservación de Mensaje de Datos emitidas de conformidad con la NOM-151-SCFI-2016 del Prestador de Servicios de Certificación, utilizará dispositivos seguros para almacenar sus Datos de Creación de Firma Electrónica, compatibles como mínimo con el estándar FIPS 140-2 nivel 3 en sus elementos de seguridad e implantación de los algoritmos criptográficos estándares, o el que le sustituya, y

VIII. 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, almacenamiento, respaldo y recuperación de la clave, Distribución de la clave pública, uso de clave, fin del ciclo de vida de la clave y Administración del ciclo de vida del hardware criptográfico, o el que le sustituya.

166. Contar con un calendario de revisión y actualización del documento de Plan de Administración de Claves.

167. Contar con 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 la Política de Constancias de Conservación de Mensaje de Datos emitidas de conformidad con la NOM-151-SCFI-2016 y Declaración de Prácticas de Constancias de Conservación de Mensaje de Datos emitidas de conformidad con la NOM-151-SCFI-2016.

TÍTULO OCTAVO

De la Digitalización de Documentos en Soporte Físico de conformidad con la NOM-151-SCFI-2016

168. Para efectos de lo dispuesto en el Capítulo I BIS, De la Digitalización, del Código de Comercio, los Prestadores de Servicios de Certificación que realicen la Digitalización de Documentos en Soporte Físico o deseen actuar como Tercero Legalmente Autorizado conforme a lo dispuesto en la NOM-151-SCFI-2016 deberán cubrir los requisitos señalados en el presente TÍTULO, según corresponda.

Para tales efectos, el Prestador de Servicios de Certificación y el Tercero Legalmente Autorizado deberá incluir en su objeto social, la actividad que requieran acreditar ya sea Digitalización de Documentos en Soporte Físico o fungir como Tercero Legalmente Autorizado.

169. Si el Prestador de Servicios de Certificación únicamente solicita acreditación para actuar como Tercero Legalmente Autorizado conforme a lo dispuesto en la NOM-151-SCFI-2016 deberá cerciorarse que la Digitalizadora que realice la Digitalización de Documentos en Soporte Físico cumpla con lo dispuesto en el presente TÍTULO.

170. En todo momento se podrá incorporar en el proceso de digitalización la participación de un Fedatario Público que llegare a intervenir en la Ceremonia de Cotejo de conformidad con las disposiciones legales que le apliquen.

CAPÍTULO I

Del Tercero Legalmente Autorizado

171. El Prestador de Servicios de Certificación interesado en actuar como Tercero Legalmente Autorizado, deberá cumplir con los elementos humanos y económicos establecidos en el presente TÍTULO y, con lo siguiente:

I. Contar con dos equipos HSM que instalará y resguardará en los lugares más seguros dentro de sus instalaciones, los cuales deberán cumplir con estándares de seguridad nacionales o internacionales, compatibles como mínimo con el estándar FIPS 140-2 nivel 3 en sus elementos de seguridad e implantación de los algoritmos criptográficos estándares, o el que le sustituya, para almacenar los Datos de Creación de Firma Electrónica del Certificado del Tercero Legalmente Autorizado.

II. Definir las medidas de seguridad adoptadas para proteger los Datos de Creación de Firma Electrónica del Certificado del Tercero Legalmente Autorizado;

III. Contar con un Plan de Administración de Claves de acuerdo a lo dispuesto en el presente CAPÍTULO, y

IV. Desarrollar un procedimiento en caso de robo de los Datos de Creación de Firma Electrónica del Certificado del Tercero Legalmente Autorizado.

172. El Tercero Legalmente Autorizado deberá controlar en todo momento el proceso de digitalización siendo responsable de la verificación que realice respecto de la migración y firmará el mensaje de datos que resulte de dicho proceso, siempre y cuando constate que la migración se realizó de manera íntegra e inalterablemente tal y como se generó por primera vez en su forma definitiva.

173. Por cada proceso de digitalización el Tercero Legalmente Autorizado deberá firmar un contrato con la Digitalizadora, en el que se acordarán sus responsabilidades y obligaciones, así como los de la Digitalizadora y de los usuarios, lo anterior conforme al Modelo Operacional y la Declaración de Prácticas de cada proceso de digitalización.

174. El Tercero Legalmente Autorizado deberá presentar a la Secretaría, el Modelo Operacional y la Declaración de Prácticas de cada proceso de digitalización, lo anterior a efecto de que la Secretaría emita su conformidad.

CAPÍTULO II

Del Prestador de Servicios de Certificación sobre el Servicio de Digitalización de Documentos en Soporte Físico

175. Cuando se acredite a un Prestador de Servicios de Certificación para que directamente preste el servicio de Digitalización de Documentos en Soporte Físico, se entenderá que también funge como Tercero Legalmente Autorizado y cumplirá con los elementos humanos, económicos, materiales y tecnológicos establecidos en el presente CAPÍTULO.

176. Por cada proceso de digitalización el Prestador de Servicios de Certificación deberá firmar un contrato con el comerciante, en el que se acordarán sus responsabilidades y obligaciones, así como los usuarios, lo anterior conforme al Modelo Operacional y la Declaración de Prácticas de cada proceso de digitalización.

177. El Prestador de Servicios de Certificación deberá presentar a la Secretaría, el Modelo Operacional y la Declaración de Prácticas de cada proceso de digitalización, lo anterior a efecto de que la Secretaría emita su conformidad.

CAPÍTULO III

De los Elementos Humanos

178. El Solicitante deberá contar con un Profesional Jurídico que deberá cumplir con los siguientes requisitos:

I. Ser licenciado en derecho con título y cédula profesional expedidos por la Secretaría de Educación Pública o su equivalente;

II. Demostrar al menos dos años de experiencia en materia notarial, correduría pública o derecho mercantil;

III. Acreditar al menos un año de experiencia en derecho informático, y

IV. Declarar bajo protesta de decir verdad que no ha sido condenado por delito contra el patrimonio de las personas o que haya merecido pena privativa de la libertad, ni que por cualquier motivo haya sido inhabilitado para el ejercicio de su profesión, para desempeñar un puesto en el servicio público, en el sistema financiero o para ejercer el comercio.

179. Contar con un Profesional Informático que deberá cumplir con los siguientes requisitos:

I. Ser licenciado o ingeniero en área informática o afín, con título y cédula profesional expedidos por la Secretaría de Educación Pública o su equivalente;

II. Comprobar al menos dos años de experiencia en el área de seguridad informática, y

III. Comprobar estudios en seguridad informática y/o alguna certificación nacional o extranjera o su equivalente, en la misma materia. En caso de contar con experiencia en certificaciones, las mismas deberán contar con una vigencia de dos años como máximo.

180. Contar con un Auxiliar de Apoyo Informático de Seguridad quien será el responsable de ejecutar el sistema de gestión, planes, políticas, procedimientos y prácticas de seguridad, quien deberá acreditar los siguientes requisitos:

I. Ser licenciado o ingeniero en área informática o afín, con título y cédula profesional expedidos por la Secretaría de Educación Pública o su equivalente;

II. Comprobar al menos dos años de experiencia en el área de seguridad informática;

III. Acreditar estudios en manejo de software o hardware relacionados con seguridad informática;

IV. Contar con conocimientos comprobados de procesos de digitalización, y

V. Declarar bajo protesta de decir verdad que no ha sido condenado por delito contra el patrimonio de las personas o que haya merecido pena privativa de la libertad, ni que por cualquier motivo haya sido inhabilitado para el ejercicio de su profesión, para desempeñar un puesto en el servicio público, en el sistema financiero o para ejercer el comercio.

181. El Profesional Jurídico tendrá por lo menos las siguientes obligaciones, funciones y responsabilidades:

I. Colaborar con el Profesional Informático en el tratamiento de los elementos jurídicos del sistema de gestión, planes, políticas, procedimientos y prácticas que se pudieran establecer, para garantizar la autenticidad e integridad de los mensajes de datos que resulten de la Digitalización de Documentos en Soporte Físico, los cuales deberá firmar y dar a conocer al personal involucrado en la digitalización;

II. Supervisar las actividades de cotejo a que se refiere el artículo 95 bis 4 del Código de Comercio, y

III. Elaborar el acta circunstanciada en la que se deje constancia de las actividades de cotejo de Digitalización de Documentos en Soporte Físico a que se refiere el artículo 95 bis 4 del Código de Comercio, la cual podrá ser generada de manera electrónica.

182. El Profesional Informático tendrá por lo menos las siguientes obligaciones, funciones y responsabilidades:

I. Diseñar, implantar y dar cumplimiento al sistema de gestión, planes, políticas, procedimientos y prácticas para garantizar la autenticidad e integridad de los mensajes de datos que resulten de la Digitalización de Documentos en Soporte

Físico, los cuales deberá firmar y dar a conocer al personal involucrado en la digitalización;

II. Supervisar los equipos y suministros de Digitalización de Documentos en Soporte Físico;

III. Supervisar el personal que lleva a cabo procesos de Digitalización de Documentos en Soporte Físico;

IV. Establecer el flujo de trabajo para el proceso de Digitalización de Documentos en Soporte Físico y asegurar su cumplimiento;

V. Acordar el formato de la imagen con el comerciante;

VI. Seleccionar el hardware de digitalización y asegurar su cumplimiento;

VII. Estar presente en las actividades de cotejo a que se refiere el artículo 95 bis 4 del Código de Comercio;

VIII. Asegurar que el proceso de Digitalización de Documentos en Soporte Físico incluye la Conservación de Mensaje de Datos resultante del proceso, y

IX. Supervisar pruebas de monitoreo.

183. El Auxiliar de Apoyo Informático de Seguridad tendrá por lo menos las siguientes obligaciones, funciones y responsabilidades:

I. Ejecutar el sistema de gestión, planes, políticas, procedimientos y prácticas para garantizar la autenticidad e integridad de los mensajes de datos resultantes de la Digitalización de Documentos en Soporte Físico;

II. Llevar a cabo la ejecución de los procesos de Digitalización de Documentos en Soporte Físico, validar la calidad de las imágenes durante dicho proceso conforme a la fracción anterior y las pruebas de configuraciones;

III. Determinar los requisitos de mejora de la imagen y/o grabaciones en audio o video;

IV. Monitorear y asegurar la correcta indexación y la calidad de las imágenes y sus metadatos;

V. Llevar el control y reportes del proceso;

VI. Agregar los metadatos al mensaje de datos, y

VII. Comprobar la calidad de los mensajes de datos a la entrega de los archivos digitales y físicos.

184. El solicitante podrá presentar ante la Secretaría una cantidad mayor de recursos humanos si las necesidades para la prestación del servicio así lo requieren.

185. El solicitante deberá presentar el procedimiento que utilizará para reclutar, seleccionar, evaluar y contratar al personal, el cual deberá describir la forma de corroborar los antecedentes del personal antes de contratarlo, así como su actualización.

En todo caso, la Secretaría deberá autorizar la modificación que se realice respecto de los recursos humanos antes mencionados.

186. El solicitante deberá presentar los contratos de confidencialidad celebrados con cada recurso humano respecto de la información a la que tengan acceso, el cual deberá extenderse cuando menos un año posterior a la conclusión laboral del empleado o de servicios en caso de una empresa externa.

CAPÍTULO IV

De los Elementos Económicos

187. El solicitante deberá contar con capital que deberá comprender al menos el equivalente a una cuarta parte de la inversión requerida en los términos señalados en el artículo 5 fracción III inciso c del Reglamento.

De igual forma, deberá contar con un seguro de responsabilidad civil que cubrirá el equivalente a 16800 (Dieciséis mil ochocientos) unidades de medida y actualización (UMA) diaria en México para cada año y durante el tiempo que permanezca acreditado el Prestador de Servicios de Certificación.

La Secretaría podrá establecer una cantidad mayor a la referida en el párrafo anterior, en caso de que, derivado del análisis de las operaciones en que sea utilizado el servicio de emisión de Digitalización de Documentos en Soporte Físico o para fungir como Tercero Legalmente Autorizado, así lo considere necesario. En este supuesto se obliga hasta el límite de la suma asegurada a pagar la indemnización que el asegurado deba a un tercero a consecuencia de un hecho que cause un daño previsto en el contrato de seguro.

188. Contar con una fianza cuyo monto no será menor al equivalente a 16800 (Dieciséis mil ochocientos) unidades de medida y actualización (UMA) diaria en México para cada año y durante el tiempo que permanezca acreditado el Prestador de Servicios de Certificación.

La Secretaría podrá establecer una cantidad mayor a la referida en el párrafo anterior, en caso de que, derivado del análisis de las operaciones en que sea utilizado el servicio de emisión de Digitalización de Documentos en Soporte Físico o para fungir como Tercero Legalmente Autorizado, así lo considere necesario. En este supuesto, 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, por actuar en sustitución del Prestador de Servicios de Certificación, cuando éste sea suspendido, inhabilitado o cancelado en su ejercicio.

CAPÍTULO V

De los Elementos Materiales

189. El Solicitante deberá contar con un espacio físico, controles de seguridad, accesos, perímetros de seguridad física, medidas de protección, así como con las políticas necesarias para garantizar la seguridad de la prestación del servicio, observando lo siguiente:

I. Las áreas en los cuales se maneja documentación que contenga información confidencial requerirán de controles de acceso, los cuales deberán estar supervisados continuamente, a efecto de reducir al mínimo los riesgos;

II. La implementación de los controles deberá evitar riesgo, daño, pérdida, alteración o sustracción de la documentación que contenga información confidencial;

III. Las áreas seguras donde se resguarda información documental concerniente al servicio, deben ser oficinas cerradas dentro del perímetro de seguridad física, contener mobiliario específico, constante en gabinetes con chapas de seguridad;

IV. La recepción de insumos y la salida de basura deberán estar controladas y separadas del área de procesamiento de la información, para evitar la pérdida de documentación confidencial;

V. Para el caso de las áreas donde residan los sistemas de Digitalización de Documentos en Soporte Físico se deberá contar con accesos físicos controlados, los cuales deberán estar protegidos con chapas seguras, controles de acceso, alarmas de seguridad, y se encontrarán limitados sólo al personal autorizado;

VI. Los requerimientos de seguridad para las áreas de atención a clientes se determinarán a partir del Análisis y Evaluación de Riesgos y Amenazas;

VII. 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;

VIII. Para el caso de la infraestructura de computación y comunicaciones deberán contar con el personal y refacciones o, en su caso, con los contratos de mantenimiento preventivo y correctivo, requeridos para garantizar la continua disponibilidad e integridad de los equipos y su software, de acuerdo a las especificaciones y periodos recomendados por los fabricantes, y

IX. Para el caso de los sistemas informáticos utilizados, deberán contar con el personal especializado o, en su caso, con los contratos de mantenimiento preventivo y correctivo, requerido para garantizar la continua disponibilidad e integridad de los sistemas, de acuerdo a las especificaciones y periodos recomendados por los fabricantes.

190. El personal contratado deberá conocer y entender los procedimientos y prácticas de seguridad dentro del perímetro de seguridad.

191. El personal de soporte deberá acceder a las áreas restringidas sólo en caso necesario y sólo si dicho acceso es autorizado por el Profesional Informático o el Auxiliar de Apoyo Informático de Seguridad, dejando evidencia de las mismas.

192. La seguridad física deberá ser compatible con las normas y criterios nacionales y/o internacionales y al menos con el estándar ETSI TS 102 042-sección 7.4.4 Physical and Environment Security o el que le sustituya.

CAPÍTULO VI

De los Elementos Tecnológicos

193. El Solicitante deberá contar con el equipo de cómputo y comunicación, software y/o sistema que se detalla a continuación:

I. Al menos un equipo digitalizador que será del tipo de producción, con al menos las siguientes características: 130 hojas por minuto, alimentador de 500 hojas, digitalizar 60,000 hojas por día, de preferencia con conexión SCSI;

II. Un servidor de misión crítica (tendrá la capacidad necesaria en RAM, velocidad del procesador y disco duro) para la gestión del software y/o sistema de Digitalización de Documentos en Soporte Físico, en caso de utilizar lo anterior de manera virtual, dicha implementación deberá ser incluida en todos los documentos de seguridad informática;

III. Contar con un dispositivo de alta seguridad, que cumpla con estándares de seguridad nacional o internacional, compatibles como mínimo con el estándar FIPS 140-2 nivel 3 en sus elementos de seguridad e implantación de los algoritmos criptográficos estándares, o el que le sustituya, para almacenar los Datos de Creación de Firma Electrónica de los certificados del Prestador de Servicios de Certificación para firmar la digitalización y/o el del Tercero Legalmente Autorizado;

IV. Un enlace mínimo de 100 MB a Internet;

V. Un ruteador;

VI. Un muro de fuego (firewall);

VII. Una computadora para gestionar el o los sistemas de administración;

VIII. Un sistema de monitoreo de red;

IX. Un sistema confiable de antivirus;

X. Herramientas confiables de detección de vulnerabilidades;

XI. Sistemas confiables de detección y protección de intrusión;

XII. Equipo de alta capacidad de almacenamiento;

XIII. Canales seguros de comunicación entre equipo digitalizador, servidor de misión crítica del software y/o sistema de digitalización de documentos en soporte físico, equipo HSM, el equipo de almacenamiento, y cualquier enlace que se requiera por cuestiones de seguridad, y

XIV. En su caso, las tecnologías de virtualización deberán ser compatibles con las normas y criterios nacionales y/o internacionales y al menos con el estándar NIST Guide to Security for Full Virtualization Security, Special Publication 800-125, 2011, o el que le sustituya.

194. Contar con la siguiente infraestructura informática:

I. Una Autoridad de Digitalización de Documentos en Soporte Físico;

II. Repositorios para: Datos de Creación de Firma Electrónica de los certificados del Prestador de Servicios de Certificación para firmar la digitalización y actuar como Tercero Legalmente Autorizado y para los mensajes de datos procedentes de la documentación digitalizada por el Prestador de Servicios de Certificación y la digitalizadora;

III. Los procesos de administración de la Infraestructura Informática;

IV. Una Política de Digitalización de Documentos en Soporte Físico;

V. Una Declaración de Prácticas de Digitalización de Documentos en Soporte Físico;

VI. Los manuales de operación de la Autoridad de Digitalización de Documentos en Soporte Físico, y

VII. La Infraestructura Informática, señalada en la Regla 194 fracción I y II, deberá considerar redundancia por seguridad.

195. Contar con un documento de Análisis y Evaluación de Riesgos y Amenazas que deberá detallar por lo menos los siguientes elementos:

I. Los activos críticos;

II. Identificar sus requerimientos de seguridad;

III. Vulnerabilidades y amenazas de la infraestructura con la que proveerá el o los servicios y determinar los requerimientos de seguridad;

IV. Estudio que identifique y evalúe los riesgos e impactos que existen sobre la organización, personas, equipos, sistemas e instalaciones, así como recomendaciones de medidas para mitigarlos, y el impacto que sufrirá el negocio, en caso de interrupciones no planificadas;

V. Medidas de seguridad para la mitigación de los riesgos detectados;

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

VII. Los impactos que sufrirán los servicios del Prestador de Servicios de Certificación, en caso de interrupciones no planificadas, y

VIII. Adoptar Guide for Conducting Risk Assessments. NIST Special Publication 800-30 Revision 1. September 2012, equivalente o el que le sustituya.

196. Contar con un calendario de revisión y actualización del documento de Análisis y Evaluación de Riesgos y Amenazas.

197. Contar con un documento de Política de Seguridad de la Información que deberá detallar por lo menos los siguientes elementos:

I. Ser congruente con el objeto del servicio de Digitalización de Documentos en Soporte Físico;

II. Los objetivos de seguridad deberán ser claros, generales, no técnicos, que se desarrollarán a partir del resultado del Análisis y Evaluación de Riesgos y Amenazas;

III. Estar basada en las recomendaciones de los estándares ISO/IEC serie 27000, o los que le sustituyan;

IV. La Política de Seguridad de la información, puede estar conformada con una política general y soportada con políticas específicas;

V. 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;

VI. Describir las reglas que indiquen cómo son provistos los servicios y las medidas de seguridad asociadas;

VII. Ser consistente con la Política de Digitalización de Documentos en Soporte Físico y con la Declaración de Prácticas de Digitalización de Documentos en Soporte Físico;

VIII. Determinar un proceso o adoptar un proceso similar al descrito en Internet Security Policy: A Technical Guide, by the National Institute of Standards and Technologies (NIST), y

IX. Desarrollar procedimientos y buenas prácticas para apoyar las políticas de seguridad.

198. Contar con un calendario de revisión y actualización del documento de Política de Seguridad de la Información.

199. Contar con un documento de Política de Seguridad Física que deberá detallar por lo menos los siguientes elementos:

I. Control de acceso físico;

II. Protección y recuperación ante desastres;

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

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

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

200. Contar con un calendario de revisión y actualización del documento de Política de Seguridad Física.

201. Contar con un documento de Sistema de Gestión de Seguridad de la Información conforme a los estándares ISO/IEC serie 27000, o los que le sustituyan.

202. El Sistema de Gestión de Seguridad de la Información deberá garantizar el logro de los objetivos de la Política de Digitalización de Documentos en Soporte Físico y de la Declaración de Prácticas de Digitalización de Documentos en Soporte Físico.

203. Contar con un calendario de revisión y actualización del documento de Sistema de Gestión de Seguridad de la Información.

204. Contar con un documento de Plan de Seguridad de Sistemas el cual deberá ser coherente con el Sistema de Gestión de Seguridad de la Información y la Política de Seguridad de la Información y, de aplicación para el servicio de Digitalización de Documentos en Soporte Físico, mismo que deberá describir los requerimientos de seguridad de los sistemas y los controles a implantar y cumplir; así como delinear las responsabilidades y acceso de las personas a los sistemas.

El Plan de Seguridad de Sistemas deberá ser compatibles con las normas y criterios nacionales y/o internacionales y, al menos con el estándar NIST Special Publication 800-18 Revisión 1, Guide for Developing Security Plans for Federal Information Systems, February 2006, o el que le sustituya.

205. Contar con un calendario de revisión y actualización del documento de Plan de Seguridad de Sistemas.

206. Contar con un documento de Plan de Continuidad del Negocio y Recuperación ante Desastres que describa cómo actuará en caso de interrupciones del servicio de Digitalización de Documentos en Soporte Físico a acreditar.

El o los planes deberán ser mantenidos y probados periódicamente, y describir los procedimientos de emergencia a seguir que deberán incluir por lo menos los siguientes elementos:

I. Afectación al funcionamiento del software y/o sistema;

II. Incidente de seguridad que afecte la operación del software y/o sistema;

III. Falla en el hardware donde se ejecuta el producto en el que se basarán los servicios;

IV. Robo de los Datos de Creación de Firma Electrónica Avanzada del Certificado de Digitalización de Documentos en Soporte Físico del Prestador de Servicios de Certificación;

V. Falla de los mecanismos de auditoría;

VI. Mecanismos para preservar evidencia del mal uso de los sistemas, y

VII. Demás casos imprevistos en las presentes Reglas y que por su naturaleza pongan en riesgo el servicio acreditado.

207. El Plan de Continuidad del Negocio y Recuperación ante Desastres, deberá ser compatible con las normas y criterios nacionales y/o internacionales, o al menos con los lineamientos descritos en el estándar ISO/IEC serie 27000 o el estándar ETSI TS 102 042 sección 7.4.8, o los que le 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 a los descritos 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.

208. Contar con un calendario de revisión y actualización del documento de Plan de Continuidad del Negocio y Recuperación ante Desastres.

209. Contar con un Modelo Operacional de la Autoridad de Digitalización de Documentos en Soporte Físico conforme al cual operará y prestará sus servicios a efecto de lograr confiabilidad e interoperabilidad, que deberá detallar por lo menos los siguientes elementos:

I. Los procesos de Digitalización de Documentos en Soporte Físico a fin de describirlos conceptual y gráficamente para su posterior aplicación;

II. Restauración del documento en soporte físico**,** deberá definir las actividades que desarrollará para llevar a cabo en su caso, la restauración de la documentación en soporte físico, de conformidad con lo establecido en la NOM-151-SCFI-2016;

III. El proceso de recepción y resguardo para la protección de la documentación en soporte físico;

IV. Mecanismos mínimos para la recepción de la documentación en soporte físico;

V. Elaborar un contrato marco en donde se definan las obligaciones y responsabilidades del comerciante, así como los procesos, obligaciones y responsabilidades de los involucrados, etapas en que se lleve a cabo el cotejo, la intervención de las partes para realizar el firmado electrónico a que hace referencia el Capítulo I BIS, De la Digitalización, del Código de Comercio, así como

el proceso de Conservación de Mensajes de Datos a que hace referencia la NOM-151-SCFI-2016;

VI. Definir un control documental de la documentación en soporte físico que se recibirá por parte del comerciante, relacionando principalmente la cantidad y el tipo de documentación que recibe, definiendo esencialmente si es original, copia simple o copia certificada, y cualquier otro elemento que permita identificarlos, y

VII. Protección de la documentación en soporte físico, tales como mecanismos de control de acceso autorizado de cuando menos 2 factores de seguridad, detectores de humo, detectores de movimiento, extintores, equipo de circuito cerrado de televisión.

210. Contar con un documento de Política de Digitalización de Documentos en Soporte Físico conforme a la cual se establecerá la confianza del usuario en el servicio, observando por lo menos lo siguiente:

I. Asegurar su concordancia con la Declaración de Prácticas de Digitalización de Documentos en Soporte Físico y, los procedimientos operacionales;

II. Describir los objetivos y alcances de la digitalización de documentos en soporte físico y, sus limitaciones, asimismo, se deberán describir las obligaciones y responsabilidades que contrae el usuario en la digitalización de documentos en soporte físico, y

III. Dar a conocer las medidas de privacidad y de protección de datos que se aplicarán en materia de Firma Electrónica Avanzada. La Política de Digitalización de Documentos en Soporte Físico será pública.

211. Contar con un calendario de revisión y actualización de la Política de Digitalización de Documentos en Soporte Físico.

212. Contar con un documento de Declaración de Prácticas de Digitalización de Documentos en Soporte Físico conforme a las cuales se establecerá la confianza del usuario en el servicio, y deberá detallar por lo menos los siguientes elementos:

I. Los procedimientos de operación de la digitalización de documentos en soporte físico y el alcance de aplicación de la misma;

II. Las responsabilidades y obligaciones del Prestador de Servicios de Certificación y la de sus usuarios;

III. Procedimientos de protección de confidencialidad de la información de los solicitantes de conformidad con la Ley Federal de Protección de Datos Personales en Posesión de Particulares o la que le sustituya;

IV. Un procedimiento para registrar la fecha y hora de todas las operaciones relacionadas con la digitalización de documentos en soporte físico, y resguardarlas de manera confiable;

V. Las medidas de seguridad adoptadas para proteger sus Datos de Creación de Firma Electrónica del Prestador de Servicios de Certificación;

VI. Los controles que se utilizarán para asegurar las auditorías y almacenamiento de información relevante;

VII. Una vez otorgada la acreditación al Prestador de Servicios de Certificación por la Secretaría, la fecha de inicio de operaciones, y

VIII. La Declaración de Prácticas de Digitalización de documentos en Soporte Físico o parte de ésta, de acuerdo a la seguridad, será pública.

213. Contar con un calendario de revisión y actualización de la Declaración de Prácticas de Digitalización de Documentos en Soporte Físico.

214. Contar con un documento de Plan de Administración de Claves conforme al cual generará, protegerá y administrará sus claves criptográficas, detallando por lo menos los siguientes elementos:

I. Las claves privadas de la Autoridad Digitalizadora de Documentos en Soporte Físico;

II. Almacenamiento, respaldo, recuperación y uso de las claves privadas;

III. Distribución del Certificado de la Autoridad Digitalizadora de Documentos en Soporte Físico;

IV. Administración del ciclo de vida del hardware criptográfico de la Autoridad Digitalizadora de Documentos en Soporte Físico;

V. 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 y componentes tecnológicos;

VI. Utilizar claves con longitud mínima de 4096 bits y ajustarse cuando así el avance tecnológico lo requiera y se establezca mediante comunicado por parte de la Secretaría, y

VII. 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, almacenamiento, respaldo y recuperación de la clave, distribución de la clave pública, Uso de clave, Fin del ciclo de vida de la clave y administración del ciclo de vida del hardware criptográfico, o el que le sustituya.

215. Contar con un calendario de revisión y actualización del Plan de Administración de Claves.

216. Contar con un documento de Plan de Gestión de Calidad, el cual es el conjunto de operaciones de mantenimiento preventivo y comprobaciones rutinarias que permitan garantizar mediante su cumplimiento que, en todo momento, los procedimientos y el estado del sistema de digitalización y los dispositivos asociados produzcan imágenes fieles e íntegras. Su objetivo será el de velar por la correcta calidad de la imagen obtenida y de sus metadatos, independientemente del momento en el que se haga uso del sistema de digitalización.

El Plan describirá también aspectos que puedan afectar al sistema de digitalización de documentos en soporte físico como, por ejemplo, el seguimiento de la vigencia de las normas y algoritmos empleados, reglas de mantenimiento de la base de datos asociada, aspectos de mantenimiento de los sistemas operativos que pudieran afectar al rendimiento del sistema de digitalización y demás empleadas.

217. Contar con un calendario de revisión y actualización del Plan Gestión de Calidad.

218. Contar con una base de datos, software y/o sistema de digitalización de documentos en soporte físico con las siguientes funcionalidades de forma cronológica:

I. Aplicar un mecanismo de validación de la vigencia de los certificados digitales de firma electrónica avanzada utilizados en el proceso de digitalización;

II. Digitalizar el documento en soporte físico y resguardar el mensaje de datos obtenido en la memoria RAM del servidor que contiene el software y/o sistema de Digitalización de Documentos en Soporte Físico;

III. Asegurar que el mensaje de datos obtenido cumpla con el formato que se haya acordado con el comerciante;

IV. Permitir la firma electrónica del mensaje de datos por el Prestador de Servicios de Certificación y/o el Tercero Legalmente Autorizado, así como el comerciante una vez realizado el cotejo;

V. Asegurar la eliminación completa de los mensajes de datos, en caso que la imagen obtenida, audio y/o video del proceso de digitalización no cumpla con lo estipulado en el Plan de Gestión de Calidad, dejando un registro y evidencia de la eliminación;

VI. Solicitar un sello digital de tiempo a una Autoridad de Sello Digital de Tiempo o a un Prestador de Servicios de Certificación que preste el servicio de emisión de Sellos Digitales de Tiempo acreditado por la Secretaría, para asociarlo al mensaje de datos por cada una de las firmas asociadas;

VII. Solicitar la conservación de mensajes de datos a un Prestador de Servicios de Certificación que preste el servicio de Conservación de Mensajes de Datos de Conformidad con la NOM-151-SCFI-2016 acreditado por la Secretaría, para ser asociado al mensaje de datos debidamente firmado, y

VIII. Enviar el mensaje de datos una vez realizado el cotejo y la firma, así como metadatos, sello digital de tiempo, y constancia de conservación de mensaje de datos, a la base de datos acordada con el comerciante.

219. Diseñar, administrar y operar una base de datos. En el diseño se considerará indexar la base de datos, de tal manera que asegure la ulterior consulta de mensaje de datos, metadatos, sellos de tiempo y constancias de conservación de mensajes de datos, de conformidad a lo acordado con el usuario.

220. Definir las medidas de seguridad a fin de que permitan proteger el contenido en la memoria RAM del servidor donde se ejecute el software o sistema de digitalización de documentos en soporte físico, y en el equipo de alta capacidad de almacenamiento,

pudiendo utilizar en su caso, como protección de memoria, equipos no conectados a la red y/o algoritmos criptográficos.

221. Contar con 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 la Política de Digitalización de Documentos en Soporte Físico y la Declaración de Prácticas de Digitalización de Documentos en Soporte Físico.

222. Antes de iniciar un proceso de migración, se deberá contar con un esquema autónomo de verificación del software y/o sistema de Digitalización de Documentos en Soporte Físico, el cual deberá incluir un análisis de seguridad del código fuente y del código en ejecución, cuyo resultado será entregado a la Secretaría para su revisión.

CAPÍTULO VII

Procedimiento de Digitalización de Documentos en Soporte Físico

223. Para que el mensaje de datos se considere fiel e íntegro, se debe obtener en un proceso informático automático en el que sin interrupción del mismo y sin intervención en momento alguno de ningún recurso humano, se realice lo siguiente en el orden indicado:

I. Digitalizar el documento por un medio fotoeléctrico o el que le aplique, de modo que se obtenga un archivo en memoria RAM del software y/o sistema de digitalización de documentos en soporte físico;

II. Procesar de forma óptima la imagen y/o grabación de audio, para garantizar su claridad, de modo que todo el contenido del documento original pueda apreciarse y sea válido para su gestión (valor umbral, reorientación, eliminación de bordes negros, eliminación de ruido, u otros de naturaleza analógica), y

III. La validez de la imagen digitalizada y/o grabación de audio del documento requerirá disponer de los procedimientos y controles necesarios para garantizar la fidelidad de la imagen y/o grabación de audio con el documento digitalizado en el procedimiento de digitalización.

224. Para garantizar la confiabilidad de la imagen y/o grabación de audio, según sea el caso, durante el proceso se utilizará comunicación cifrada donde se requiera.

225. Para efectos de lo dispuesto en el artículo 95 bis 4 del Código de Comercio, se deberán aplicar las técnicas de muestreo para cotejar mensajes de datos contra documentos en soporte físico. El Prestador de Servicios de Certificación, presentará en su Declaración de Prácticas de Digitalización de documentos en Soporte Físico, el procedimiento donde se describa la forma administrativa de operar, tamaño de la muestra, mensajes de datos que conformarán la muestra, y modo de cotejo según la extensión del documento.

226. Los procesos administrativos, la muestra y su tamaño, que permitirán realizar un proceso de cotejo de los mensajes de datos resultantes de la digitalización contra los documentos en soporte físico son:

I. Control de folios. Deberá llevar un método de control identificado con folios, que no altere y/o modifique el documento en soporte físico y el mensaje de datos, el cual

podrá ser empleado para poder identificar los documentos en soporte físico y mensajes de datos, utilizados en el proceso de cotejo;

II. Lotes de documentos físicos a digitalizar. El comerciante que solicite el servicio de Digitalización de Documentos en Soporte Físico, podrá dividirlos en lotes y enviar, en su caso, cada lote para su digitalización, y

III. Determinación del tamaño de la muestra**.** El tamaño de una muestra, es el número de mensajes de datos que compone la muestra extraída del total de mensajes de datos, necesarios para que éstos sean representativos.

La siguiente fórmula se utilizará para calcular el tamaño de la muestra:

$$n = \frac{N S^2 Z_\alpha{}^2}{E^2(N-1) + S^2 Z_\alpha{}^2}$$, donde

n	Es el tamaño de la muestra.
N	Es el total de mensajes de datos.
S	Es la desviación estándar estimada (si no tiene su valor, generalmente suele utilizarse un valor de 0.5).
Z_α	Es el nivel de confianza (si no tiene su valor, puede utilizar el 95% de confianza que equivale a 1.96 [como más usual] o el 99% de confianza que equivale a 2.58. Los valores de Z_α se obtienen de la tabla de la distribución normal estándar N(0,1)).
E	Es el límite aceptable de error de la muestra (si no tiene su valor, puede utilizar un valor entre el 1% (0.01) y 9% (0.09)).

Fuente: Técnicas de muestreo. Sesgos más frecuentes.

Neus Canal Díaz

http://www.revistaseden.org/files/9-cap%209.pdf

227. Para obtener la muestra y de acuerdo a la documentación a digitalizar, se deberán utilizar cualquiera de las siguientes técnicas:

I. Muestreo aleatorio simple. El tamaño de la muestra se obtiene utilizando la fórmula de la Regla 226 fracción III y los mensajes de datos que formarán la muestra, se eligen aleatoriamente, entre el total de los mensajes de datos, utilizando un generador de números aleatorios por computadora;

II. Muestreo aleatorio sistemático. El tamaño de la muestra se obtiene utilizando la fórmula de la Regla 226 fracción III, y se divide el total (N) de mensajes de datos entre el tamaño de la muestra (n), obteniendo un intervalo de muestreo k = N/n. El folio (x) del primer mensaje de datos que forma parte de la muestra debe estar entre 1 <= x <= k, y se elige aleatoriamente utilizando un generador de números aleatorios por computadora; a partir de este mensaje de datos se recorre hasta el k-ésimo mensaje de datos, y así sucesivamente se van eligiendo los mensajes de datos de k en k hasta conseguir la muestra de tamaño n. En el caso de que k no sea entero, se toma el siguiente entero a N/n. Si k supera el último número del total (N) de mensajes de datos entonces se continúa por el principio. El Tercero Legalmente Autorizado debe asegurarse de que al aplicar el intervalo de muestreo no se esconda algún patrón que amenace la aleatoriedad;

III. Muestreo aleatorio estratificado desproporcionado. La empresa que solicita la digitalización de sus documentos dividirá éstos en tres estratos de acuerdo a su importancia:

1) Documentos de importancia baja;

2) Documentos de importancia media, y

3) Documentos de importancia alta.

Los documentos así clasificados se digitalizarán y el tamaño de la muestra de los estratos se puede calcular con las siguientes fracciones aproximadas:

No. DE CADA ESTRATO	IMPORTANCIA DE LOS DOCUMENTOS DEL ESTRATO	FRACCIÓN
1	**Baja**	**1/8**
2	**Media**	**1/4**
3	**Alta**	**1/2**

El solicitante podrá acordar otras fracciones conforme a sus necesidades.

El tamaño de la muestra de cada estrato (n_i) se calcula como sigue:

$n_i = N_i$ * fracción, para i = 1, 2 y 3, donde N_i, es el total de mensajes de datos contenidos en cada estrato.

Los mensajes de datos de la muestra de cada estrato se eligen utilizando muestreo aleatorio simple o sistemático, y

IV. Muestreo por grupos (*clusters*). Se dividen los mensajes de datos en un número adecuado de grupos de un mismo tamaño. Cada grupo debe contener todos los tipos de mensajes de datos digitalizados.

En una primera etapa, se seleccionan algunos grupos ya sea por muestreo aleatorio simple o sistemático. Una vez seleccionados los grupos, en una segunda etapa, se toman muestras de mensajes de datos de cada grupo, utilizando nuevamente muestreo aleatorio simple o sistemático.

228. Cotejo. Los mensajes de datos que aparecen en la muestra son los seleccionados para que el Tercero Legalmente Autorizado proceda a cotejarlos contra los respectivos documentos en soporte físico, debiendo tomar en cuenta los siguientes supuestos:

I. Documentos extensos. Cuando algún mensaje de datos de la muestra es extenso, se puede utilizar alguna de las técnicas de muestreo probabilístico de la Regla 227 para cotejarlo contra el respectivo documento en soporte físico;

II. Reporte del cotejo de la muestra. El reporte debe ser un mensaje de datos. Entre la información que debe contener el reporte, cabe destacar la siguiente:

No.	INFORMACIÓN
1	Nombre del comerciante que solicitó la digitalización, de su Representante Legal y su domicilio.
2	Nombre de la Digitalizadora.
3	Nombre del Tercero Legalmente Autorizado.
4	Nombres del Profesional Jurídico y del Informático.
5	Fechas en que se realizó la digitalización, el cotejo y el reporte.
6	Número de lote digitalizado (en su caso).
7	Número de documentos digitalizados.
8	Rango de folios de los documentos digitalizados.
9	Tamaño de la muestra(s), su nivel de confianza, límite de error de muestreo con el que se trabajó, y la desviación estándar estimada.
10	Listado de los números aleatorios generados por computadora y un sello digital de tiempo de este listado (emitido inmediatamente después generar el listado).
11	Lista de los folios de los mensajes de datos que forman parte de la muestra(s).
12	Técnica de muestreo probabilístico utilizada y las razones por las cuales se eligió.
13	Fracciones en los estratos (en su caso) y el criterio que se eligió.
14	En el caso de mensajes de datos extensos: los folios de los mensajes de datos, el tamaño de la muestra(s), los números de las hojas cotejadas y la técnica de muestreo utilizada.
15	Folios de los mensajes de datos digitalizados de la muestra que durante el cotejo se encontró con diferencias con los respectivos documentos en soporte físico.
16	En caso de no haber diferencias en el cotejo de la muestra se escribirá la leyenda “NO HUBO DIFERENCIAS EN LA MUESTRA”.
17	El reporte será firmado electrónicamente por el Tercero Legalmente Autorizado.

En todo momento, el Prestador de Servicios de Certificación o el Tercero Legalmente Autorizado, mantendrá a disposición de la Secretaría dicho reporte, y

III. En caso de haber diferencias en el cotejo de la muestra, el Tercero Legalmente Autorizado, realizará una investigación, y avisará inmediatamente por escrito a la Secretaría.

229. Ceremonia de cotejo**.** El Tercero Legalmente Autorizado con la finalidad de dar certeza al proceso de migración de la documentación en soporte físico a mensaje de datos y, el comerciante a fin de recibir de conformidad los mensajes de datos resultantes, deberán llevar a cabo el levantamiento de un acta circunstanciada, en la que se deje constancia de las actividades de cotejo de la documentación en soporte físico y mensajes de datos que se realizaron.

En su caso, se podrá estar ante la presencia de un Fedatario Público, para dar fe de la actuación que se lleve a cabo en dicha diligencia.

230. Metadatos**.** En el proceso de Digitalización de Documentos en Soporte Físico, el Prestador de Servicios de Certificación o el Tercero Legalmente Autorizado, podrá utilizar el marco de trabajo (framework) del estándar ISO/IEC 11179 Metadata Registry (MDR), el lenguaje XML, o el que determine la Secretaría, para los metadatos de los mensajes de datos.

TRANSITORIOS

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

SEGUNDO.- A la entrada en vigor de las presentes Reglas, se abrogan las Reglas Generales a las que deberán sujetarse los Prestadores de Servicio de Certificación, publicadas en el Diario Oficial de la Federación el 10 de agosto de 2004.

TERCERO.- Las acreditaciones para ejercer como Prestador de Servicios de Certificación, otorgadas por la Secretaría de Economía con anterioridad a la entrada en vigor de las presentes Reglas, continuarán vigentes para todos sus efectos legales.

CUARTO.- Las acreditaciones para ejercer como Prestador de Servicios de Certificación, que se encuentren en trámite antes de la entrada en vigor de las presentes Reglas, serán resueltas de conformidad con las disposiciones vigentes al momento de su presentación.

Ciudad de México, a 3 de mayo de 2018.- El Secretario de Economía, **Ildefonso Guajardo Villarreal**.- Rúbrica.