GUÍA DE SUPERVISIÓN DE PRESTADORES DE SERVICIOS DE CERTIFICACIÓN

Dirección General de Normatividad Mercantil
Coordinación de Política Mercantil

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

Índice

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

I. Introducción.

De conformidad con lo previsto por el artículo 38 fracción IX del Reglamento Interior de la Secretaría de Economía, la Dirección General de Normatividad Mercantil, tiene como atribución acreditar a los Prestadores de Servicios de Certificación para ofrecer los servicios de emisión de certificados digitales, sellos digitales de tiempo, constancias de conservación de mensajes de datos, digitalización de documentos en soporte físico, así como para actuar como tercero legalmente autorizado, en términos de lo previsto por el artículo 100 del Código de Comercio y la NOM-151-SCFI-2016, Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos (cancela la NOM-151-SCFI-2002).

Asimismo, en términos de lo previsto por los artículos 95 bis 6 fracción II del Código de Comercio, 22 del Reglamento del Código de Comercio en materia de Prestadores de Servicios de Certificación, y los numerales 13, 14, 15 y 16 de las Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación, la Dirección General de Normatividad Mercantil podrá verificar en cualquier tiempo el adecuado desarrollo de las operaciones de los Prestadores de Servicios de Certificación, así como la continuidad en el cumplimiento de los requisitos exigidos para obtener la acreditación de los servicios correspondientes. Para tal efecto, podrá requerir informes, documentos y otros datos a los Prestadores de Servicios de Certificación, así como requerirles información necesaria para llevar a cabo sus funciones de visitas de verificación.

En este sentido, la presente guía contiene un primer apartado en el que se establece el objetivo relacionado con las acciones de visitas de verificación, un segundo apartado relativo al marco normativo aplicable a dichas acciones, un tercer apartado en el que se describen las facultades de verificación relacionadas con las atribuciones con las que cuenta la Secretaría de Economía a través de la Dirección General de Normatividad, un cuarto apartado en el que se describen los elementos que deben contener los oficios de visitas de verificación, un quinto apartado en el que se establece como se conformarán las actas circunstanciadas que se levantarán con motivo de las visitas de verificación, un sexto apartado en el que se establecen los periodos con los que contarán los Prestadores de Servicios de Certificación para atender o subsanar las observaciones que, en su caso, se deriven de la acciones de visitas de verificación y finalmente un séptimo apartado en el que se establecen los requisitos y elementos sujetos a verificación relacionados con los servicios acreditados a los Prestadores de Servicios de Certificación objeto de las visitas de verificación.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

II. Objetivo.

Esta guía tiene como objetivo, establecer los elementos que sirvan de apoyo para especificar y estandarizar las acciones de supervisión para constatar el adecuado desarrollo de las operaciones y la continuidad en el cumplimiento de los requisitos de los Prestadores de Servicios de Certificación, con base en la normatividad aplicable. Por lo tanto, esta guía debe ser considerada como apoyo en la planeación y ejecución del trabajo de las acciones de supervisión, tomando en cuenta las disposiciones legales y reglamentarias aplicables al ejercicio de la actividad de los Prestadores de Servicios de Certificación. Este material tiene por objetivo ser ilustrativo y de utilidad en beneficio de los Prestadores de Servicios de Certificación, sin generar mayores obligaciones y supuestos que los previstos en la normatividad aplicable.

III. Acrónimos.

DGNM.- Dirección General de Normatividad Mercantil.

PSC.- Prestadores de Servicios de Certificación (en singular o plural).

IV. Marco normativo.

El marco normativo para verificar a los PSC acreditados por la Secretaría de Economía, así como para realizar las visitas de verificación correspondiente es el siguiente:

Constitución Política de los Estados Unidos Mexicanos.
https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf

Código de Comercio.
https://www.diputados.gob.mx/LeyesBiblio/ref/ccom.htm

Ley Federal de Procedimiento Administrativo (Documento completo)

https://www.diputados.gob.mx/LeyesBiblio/pdf/112_180518.pdf

Reglamento del Código de Comercio en materia de Prestadores de Servicios de Certificación. (Documento completo)
https://www.diputados.gob.mx/LeyesBiblio/regley/Reg_CComer_MPSC.pdf

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

Reglamento Interior de la Secretaría de Economía.
https://www.dof.gob.mx/nota_detalle.php?codigo=5615588&fecha=12/04/2021#gsc.tab=0

Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación.
https://www.dof.gob.mx/nota_detalle.php?codigo=5522462&fecha=14/05/2018#gsc.tab=0

Norma Oficial Mexicana NOM-151-SCFI-2016, Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos.
https://www.dof.gob.mx/normasOficiales/6499/seeco11_C/seeco11_C.html

V. Facultades de verificación.

La DGNM tiene como atribuciones ordenar visitas de verificación a los PSC, requerirles información respecto de los servicios acreditados y, en su caso, sancionarlos por el incumplimiento de sus obligaciones, conforme a lo previsto en los ordenamientos legales referidos en el apartado denominado "*Marco normativo*" de la presente guía. En ese sentido, los interesados en ser PSC desde la solicitud presentada a la Secretaría de Economía para ser acreditados, establecen por escrito su conformidad para ser sujetos de visitas de verificación.

De esta manera, la Secretaría de Economía a través de la DGNM, ejercerá sus facultades de verificación y comprobación en los siguientes términos:

1. Requerir informes, documentos y otros datos para para verificar en cualquier tiempo el adecuado desarrollo de las operaciones de los PSC (Artículo 95 bis 6 fracción II del Código de Comercio y numeral 14 de las Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación), con el objetivo de comprobar la continuidad en el cumplimiento de los elementos necesarios para seguir prestando el servicio para el que hayan sido acreditados.

2. Realizar las visitas de verificación correspondientes al PSC, a fin de comprobar la continuidad en el cumplimento de los elementos humanos, materiales, económicos y tecnológicos requeridos para prestar los servicios para los cuales hayan sido acreditados (Artículos 102 del Código de Comercio; 5 y 21 del Reglamento del Código de Comercio en materia de Prestadores de Servicios de Certificación), las cuales se desahogarán previa notificación, la cual podrá hacerse personalmente, mediante oficio entregado por mensajero o correo certificado, con acuse de recibo, telefax, medios de comunicación electrónica o cualquier otro medio, cuando

así lo haya aceptado expresamente el promovente y siempre que pueda comprobarse fehacientemente la recepción de los mismos, en el caso de comunicaciones electrónicas certificadas, deberán realizarse conforme a los requisitos previstos en la Norma Oficial Mexicana a que se refiere el artículo 49 del Código de Comercio, por edicto, o por correo ordinario, mensajería, telegrama u otro medio similar, en términos de lo previsto por la Ley Federal del Procedimiento Administrativo para las visitas de verificación, de oficio o a petición del Titular del Certificado, Firmante o de la Parte que Confía (Artículo 22 del Reglamento del Código de Comercio en materia de Prestadores de Servicios de Certificación).

VI. Oficio de visita de verificación.

Las visitas de verificación se practicarán previa orden escrita, a través del oficio correspondiente, el cual deberá señalar los elementos que se describen a continuación conforme a lo previsto en el artículo 63 de la Ley Federal de Procedimiento Administrativo:

1. Nombre del PSC, su representante legal, domicilio y cuentas de correo electrónico con la finalidad de efectuar notificaciones electrónicas, cuando así lo haya aceptado expresamente;

2. Lugar y día en que deba tener lugar la visita de verificación;

3. Objeto y alcance de la visita de verificación;

4. Disposiciones legales que lo fundamenten;

5. Nombre del visitador, y

6. Nombre y firma del funcionario público de la DGNM que lo expide.[1]

[1] Artículo 63 de la Ley Federal de Procedimiento Administrativo.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

VII. Acta circunstanciada.

Al efectuar las visitas de verificación, los funcionarios públicos de la DGNM levantarán un acta circunstanciada relativa a la demostración que el PSC realice, con la finalidad de comprobar la continuidad en el cumplimiento de los requisitos, con base en lo respectivamente previsto en los ordenamientos legales establecidos en el apartado denominado "*Marco normativo*" de la presente guía.

Las personas designadas por el PSC para atender la visita de verificación, se encontrarán obligados a permitir el acceso y otorgar las facilidades e informes a los funcionarios públicos de la DGNM, con la finalidad de lograr el cumplimiento de su labor.

Al iniciar la visita de verificación, los funcionarios públicos de la DGNM se identificarán ante el PSC con credencial vigente con fotografía expedida por la Secretaría de Economía, en la que aparezca la fotografía e informarán el motivo de su asistencia, entregando el oficio de verificación correspondiente.

El acta circunstanciada se levantará en presencia de dos testigos propuestos por la persona responsable designada por el PSC para atender la visita de verificación, o bien, por el funcionario público de la DGNM que la practique si la persona responsable antes indicada se negare a proponerlos.

Del acta circunstanciada se proporcionará copia a la persona responsable designada por el PSC para atender la visita de verificación, aún y cuando éste se negaré a firmar, lo que no afectará la validez de la visita de verificación ni del acta circunstanciada y/o documento de que se trate, siempre y cuando el funcionario público de la DGNM haga constar tal circunstancia en la propia acta.

En las actas circunstanciadas se hará constar los elementos que se establecen en el artículo 67 de la Ley Federal de Procedimiento Administrativo.

El responsable designado por el PSC para atender la visita de verificación con quien se haya levantado el acta circunstanciada podrá formular observaciones en el acto de la visita de verificación

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

y ofrecer pruebas en relación a los hechos contenidos en ella, o bien, por escrito, haciendo uso de tal derecho dentro del término de cinco días siguientes a la fecha en que se hubiere levantado.[2]

VIII. Elementos y requisitos sujetos a verificación.

Las obligaciones sujetas a verificación se encuentran vinculadas con los servicios acreditados al PSC, en términos de lo previsto por el Código de Comercio, el Reglamento del Código de Comercio en materia de Prestadores de Servicios de Certificación, así como en las Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación, los cuales serán auditados conforme a lo siguiente:

VIII.1 Código de Comercio.	
VIII.1.1 Titulo Segundo Del Comercio Electrónico Capítulo I BIS De la Digitalización.	
Fundamento.	**Elementos para acreditar el cumplimiento.**
Artículo 95 bis 1.- Para el caso de los servicios de digitalización se estará a lo siguiente:	
a. En todo caso, los documentos podrán ser digitalizados en el formato que determine el comerciante.	Presentar contrato en donde se especifica el formato en que se obtendrá el mensaje de datos. Presentar el mensaje de datos obtenido de la digitalización.
b. Una vez concluida la digitalización del documento, deberá acompañarse al mismo, así como a cada uno de los anexos que en su caso se generen, la firma electrónica avanzada del comerciante, y del prestador de servicios de certificación que ejecutó las actividades de digitalización, en caso de que así haya sido.	Presentar el mensaje de datos obtenido de la digitalización con las firmas electrónicas avanzadas correspondientes.
d. La información que en virtud de acuerdos contractuales quede en poder de un prestador de servicios de certificación, se regirá por lo dispuesto en la Ley	Presentar contrato en donde se especifique que la información que quede bajo resguardo del PSC, será protegida conforme a los dispuesto en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

[2] Artículo 68 de la Ley Federal de Procedimiento Administrativo.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

Federal de Protección de Datos Personales en Posesión de los Particulares.	
e. En todo caso, el prestador de servicios de certificación que ejecutó las actividades de digitalización deberá mantener la confidencialidad de la información, salvo por mandato judicial.	Presentar los contratos de confidencialidad celebrados con cada recurso humano respecto de la información a la que tengan acceso.
Artículo 95 bis 4.-	
En caso que los servicios de digitalización sean contratados a un prestador de servicios de certificación, éste presumirá la buena fe del contratante, así como la legitimidad de los documentos que le son confiados a digitalizar, limitándose a reflejarlos fiel e íntegramente en los medios electrónicos que le sean solicitados, bajo las penas en que incurren aquellos que cometen delitos en materia de falsificación de documentos.	Presentar el Contrato relativo al servicio de Digitalización de Documentos en Soporte Físico.
Contra la entrega de la información digitalizada y su correspondiente cotejo, el contratante deberá firmar una cláusula de satisfacción del servicio prestado, y proceder a adjuntar su firma electrónica avanzada a la información.	Presentar el acta circunstanciada relativa a las actividades de cotejo de la documentación en soporte físico y mensajes de datos que se realizaron, en la que conste que el comerciante recibió de conformidad los mensajes de datos resultantes.
Si el contratante no adjunta su firma electrónica avanzada a la información digitalizada, ésta no podrá surtir efecto legal alguno, y será de carácter meramente informativo.	Presentar el mensaje de datos obtenido de la digitalización con las firmas electrónicas avanzadas correspondientes.
Asimismo, el prestador de servicios deberá implementar el mecanismo tecnológico necesario, a fin de que, una vez digitalizado y entregado el documento electrónico a satisfacción del cliente, éste no pueda ser modificado, alterado,	Presentar la Constancia de Conservación del Mensaje de Datos obtenida de la digitalización.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

enmendado o corregido de modo alguno, en los términos que se establezca en la norma oficial mexicana sobre digitalización y conservación de mensajes de datos que para tal efecto emita la Secretaría.	
VIII.1.2 Capítulo III De los Prestadores de Servicios de Certificación.	
102.- Los Prestadores de Servicios de Certificación que hayan obtenido la acreditación de la Secretaría deberán notificar a ésta la iniciación de la prestación de los servicios a que hayan sido autorizados, dentro de los 45 días naturales siguientes al comienzo de dicha actividad.	
III. Contar con procedimientos definidos y específicos para la prestación de los servicios, y medidas que garanticen la seriedad de los Certificados, la conservación y consulta de los registros, si es el caso;	▪ Presentar certificado emitido durante el periodo solicitado. ▪ Presentar el expediente con el que se verificó la identidad del usuario. ▪ Presentar registros a nivel de base de datos de la emisión del certificado.
103.- Las responsabilidades de las Entidades Prestadoras de Servicios de Certificación deberán estipularse en el contrato con los firmantes.	Presentar los contratos correspondientes aplicables a cada servicio.
104.- Los Prestadores de Servicios de Certificación deben cumplir las siguientes obligaciones:	
I. Comprobar por sí o por medio de una persona física o moral que actúe en nombre y por cuenta suyos, la identidad de los solicitantes y cualesquiera circunstancias pertinentes para la emisión de los Certificados, utilizando cualquiera de los medios admitidos en derecho, siempre y cuando sean previamente notificados al solicitante;	Presentar procedimiento de verificación de la identidad del usuario el cual deberá llevarse a cabo conforme a su Política de Certificados y a su Declaración de Prácticas de Certificación.
II. Poner a disposición del Firmante los dispositivos de generación de los Datos de Creación y de verificación de la Firma Electrónica;	Guía de usuario, o bien, capturas de pantallas del sistema mediante el cual se generan las claves criptográficas.
III. Informar, antes de la emisión de un Certificado, a la persona que solicite sus servicios, de su precio, de las condiciones precisas para la utilización del Certificado, de sus limitaciones de uso y, en su caso, de la forma en que garantiza su posible responsabilidad;	Evidencia del mecanismo de notificación al usuario.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

IV. Mantener un registro de Certificados, en el que quedará constancia de los emitidos y figurarán las circunstancias que afecten a la suspensión, pérdida o terminación de vigencia de sus efectos. A dicho registro podrá accederse por medios electrónicos, ópticos o de cualquier otra tecnología y su contenido público estará a disposición de las personas que lo soliciten, el contenido privado estará a disposición del Destinatario y de las personas que lo soliciten cuando así lo autorice el Firmante, así como en los casos a que se refieran las reglas generales que al efecto establezca la Secretaría;	Evidencia del sistema de consulta de la lista de certificados emitidos, así como de la consulta de la CRL.
V. Guardar confidencialidad respecto a la información que haya recibido para la prestación del servicio de certificación;	Verificación física del espacio en el que se resguardan los expedientes, así como los contratos de confidencialidad del personal correspondiente.
VII. Asegurar las medidas para evitar la alteración de los Certificados y mantener la confidencialidad de los datos en el proceso de generación de los Datos de Creación de la Firma Electrónica;	Guía de usuario, o bien, capturas de pantallas del sistema mediante el cual se generan las claves criptográficas.Evidencia de los canales de comunicación seguros entre la Autoridad Certificadora y la Autoridad Registradora.
VIII. Establecer declaraciones sobre sus normas y prácticas, las cuales harán del conocimiento del usuario y el Destinatario, y	Evidencia de su publicación en la URL o sitio electrónico del PSC (Políticas y Declaraciones del servicio acreditado).
IX. Proporcionar medios de acceso que permitan a la Parte que Confía en el Certificado determinar:	Cumplir con los incisos señalados a continuación.
a) La identidad del Prestador de Servicios de Certificación;	Presentar certificado emitido durante el periodo solicitado. Evidencia del sistema de consulta de la lista de certificados emitidos.
b) Que el Firmante nombrado en el Certificado tenía bajo su control el dispositivo y los Datos de Creación de la Firma en el momento en que se expidió el Certificado;	URL en donde se encuentren publicadas su Política de Certificados y su Declaración de Prácticas de Certificación. Guía de usuario, o bien, capturas de pantallas del sistema mediante el cual se generan las claves criptográficas.
c) Que los Datos de Creación de la Firma eran válidos en la fecha en que se expidió el Certificado;	Presentar certificado emitido durante el periodo solicitado, donde se verificará que la fecha de vigencia del certificado emitido se encuentre dentro del periodo de vigencia del certificado del PSC.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

d) El método utilizado para identificar al Firmante;	Procedimiento de validación de la identidad del usuario, el cual se deberá llevar a cabo conforme a su Política de Certificados y a su Declaración de Prácticas de Certificación.
e) Cualquier limitación en los fines o el valor respecto de los cuales puedan utilizarse los Datos de Creación de la Firma o el Certificado;	URL en donde se encuentren publicadas su Política de Certificados y su Declaración de Prácticas de Certificación.
f) Cualquier limitación en cuanto al ámbito o el alcance de la responsabilidad indicada por el Prestador de Servicios de Certificación;	URL en donde se encuentren publicadas su Política de Certificados y su Declaración de Prácticas de Certificación.
g) Si existe un medio para que el Firmante dé aviso al Prestador de Servicios de Certificación de que los Datos de Creación de la Firma han sido de alguna manera controvertidos, y	URL en donde se encuentren publicadas su Política de Certificados y su Declaración de Prácticas de Certificación. Presentar evidencia de solicitud de revocación relacionada con este supuesto.
h) Si se ofrece un servicio de terminación de vigencia del Certificado.	URL en donde se encuentren publicadas su Política de Certificados y su Declaración de Prácticas de Certificación.
108.- Los Certificados, para ser considerados válidos, deberán contener:	
I. La indicación de que se expiden como tales;	Presentar certificado emitido durante el periodo solicitado para validar su contenido.
II. El código de identificación único del Certificado;	Presentar certificado emitido durante el periodo solicitado para validar su contenido.
III. La identificación del Prestador de Servicios de Certificación que expide el Certificado, razón social, su nombre de dominio de Internet, dirección de correo electrónico, en su caso, y los datos de acreditación ante la Secretaría;	Presentar certificado emitido durante el periodo solicitado para validar su contenido.
IV. Nombre del titular del Certificado;	Presentar certificado emitido durante el periodo solicitado para validar su contenido.
V. Periodo de vigencia del Certificado;	Presentar certificado emitido durante el periodo solicitado para validar su contenido.
VI. La fecha y hora de la emisión, suspensión, y renovación del Certificado;	Presentar certificado emitido durante el periodo solicitado para validar su contenido.
VII. El alcance de las responsabilidades que asume el Prestador de Servicios de Certificación, y	Presentar certificado emitido durante el periodo solicitado para validar su contenido.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

VIII. La referencia de la tecnología empleada para la creación de la Firma Electrónica.	Presentar certificado emitido durante el periodo solicitado para validar su contenido.

VIII.2 Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación.

VIII.2.1 Titulo Quinto
De la Emisión de Certificados Digitales.

ELEMENTOS HUMANOS.[3]

Presentar la lista de los últimos elementos humanos con los que cuenta actualmente, los cuales deberán coincidir con los previamente autorizados por la DGNM, en caso de que se detecte que alguno de los elementos no coincide con los ya autorizados o que se deba actualizar alguno de los requisitos, se deberá presentar lo siguiente:

Fundamento.	Elementos para acreditar el cumplimiento.
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;	Título profesional expedido por la Secretaría de Educación Pública y cédula profesional expedida 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;	Documentos que acrediten la experiencia señalada en la presente fracción, los siguientes ejemplos se señalan de manera enunciativa mas no limitativa: • Curriculum Vitae firmado autógrafamente, bajo protesta de decir verdad, en el cual deberán detallar las actividades que realizó o realiza en el área de correduría pública, derecho notarial o derecho mercantil. • Constancia laboral para acreditar el periodo y las actividades que realizó o realiza en el área de correduría pública, derecho notarial o derecho mercantil.
III. Acreditar al menos un año de experiencia en derecho informático, y	Documentos que acrediten la experiencia señalada en la presente fracción, los siguientes ejemplos se señalan de manera enunciativa mas no limitativa: • Curriculum Vitae firmado autógrafamente, bajo protesta de decir verdad, en el cual deberán detallar las actividades que realizó o realiza en el área de derecho informático. • Constancia laboral para acreditar el periodo y las actividades que realizó o realiza en el área de derecho informático.
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	Escrito libre firmado autógrafamente, mediante el cual declara 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, actualizado.

[3] Los Elementos Humanos se refieren de forma general en el artículo 5, fracción III, inciso a), del Reglamento del Código de Comercio en materia de Prestadores de Servicios de Certificación.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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,	Escrito libre firmado autógrafamente, mediante el cual declara 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, actualizado.
II. Demostrar relación laboral con el Agente Certificador o con el solicitante como Prestador de Servicios de Certificación, según corresponda.	Contrato laboral que acredite la relación entre el Agente Certificador y el PSC acreditado.
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;	Título profesional expedido por la Secretaría de Educación Pública y cédula profesional expedida por la Secretaría de Educación Pública o su equivalente.
II. Comprobar al menos dos años de experiencia en el área de criptografía;	Documentos que acrediten la experiencia señalada en la presente fracción, los siguientes ejemplos se señalan de manera enunciativa mas no limitativa: • Curriculum Vitae firmado autógrafamente, bajo protesta de decir verdad, en el cual deberán detallar las actividades que realizó o realiza en el área de criptografía. • Constancia laboral para acreditar el periodo y las actividades que realizó o realiza en el área de criptografía.
III. Acreditar estudios en manejo de software o hardware relacionados con criptografía, y	Documentos que acrediten que cuenta con estudios en manejo de software o hardware relacionados con criptografía como pueden ser: certificaciones y/o título de especialidad y/o título de maestría que acredite estudios en manejo de software o hardware relacionados con criptografía.
IV. Declarar bajo protesta de decir verdad que no ha sido	Escrito libre firmado autógrafamente, mediante el cual declara bajo protesta de decir verdad que no ha sido condenado por delito contra el

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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.	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, actualizado.
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;	Título profesional expedido por la Secretaría de Educación Pública y cédula profesional expedida por la Secretaría de Educación Pública o su equivalente.
II. Comprobar al menos dos años de experiencia en el área de criptografía;	Documentos que acrediten la experiencia señalada en la presente fracción, los siguientes ejemplos se señalan de manera enunciativa mas no limitativa: • Curriculum Vitae firmado autógrafamente, bajo protesta de decir verdad, en el cual deberán detallar las actividades que realizó o realiza en el área de criptografía. • Constancia laboral para acreditar el periodo y las actividades que realizó o realiza en el área de criptografía.
III. Acreditar estudios en manejo de software o hardware relacionados con criptografía, y	Documentos que acrediten que cuenta con estudios en manejo de software o hardware relacionados con criptografía como pueden ser: certificaciones y/o título de especialidad y/o título de maestría y/o diploma que acredite estudios en manejo de software o hardware relacionados con criptografía.
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.	Escrito libre firmado autógrafamente, mediante el cual declara 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, actualizado.
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	Título profesional expedido por la Secretaría de Educación Pública y cédula profesional expedida por la Secretaría de Educación Pública o su equivalente.

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;	Documentos que acrediten la experiencia señalada en la presente fracción, los siguientes ejemplos se señalan de manera enunciativa mas no limitativa: • Curriculum Vitae firmado autógrafamente, bajo protesta de decir verdad, en el cual deberán detallar las actividades que realizó o realiza en las áreas de seguridad informática, redes y/o sistemas informáticos, de cuando menos dos años, según sea el caso. • Constancia laboral para acreditar el periodo y las actividades que realizó o realiza 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	Certificación nacional o extranjera en manejo de software o hardware referente a seguridad informática, seguridad en redes y/o sistemas informáticos que cuente con una antigüedad de dos años como máximo.
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.	Escrito libre firmado autógrafamente, mediante el cual declara 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, actualizado.
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	Presentar la lista de los últimos elementos humanos con los que cuenta actualmente, los cuales deberán coincidir con los previamente autorizados por la DGNM, de acuerdo a la presente Regla.
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	Documento que se utiliza para reclutar, seleccionar, evaluar y contratar al personal, para verificar si han llevado a cabo las revisiones establecidas y en su caso si se ha modificado.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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.	Contratos de confidencialidad debidamente suscritos por las partes, los cuales deberán extenderse cuando menos un año posterior a la conclusión laboral del empleado o de servicios en caso de una empresa externa.
ELEMENTOS ECONÓMICOS.[4]	
Fundamento.	**Elementos para acreditar el cumplimiento.**
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	Documentos que acrediten que cuenta con capital que comprende al menos el equivalente a una cuarta parte de la inversión requerida. Se señalan de manera enunciativa mas no limitativa los siguientes: • Estados financieros. • Desglose de la inversión realizada. En caso de personas morales de carácter privado, además se deberán presentar los documentos que acrediten el capital social actual de la empresa. Presentar el Seguro de responsabilidad civil para corroborar que esté vigente y que corresponde al presentado.

[4] Los Elementos Económicos se refieren de forma general en el artículo 5, fracción III, inciso c), del Reglamento del Código de Comercio en materia de Prestadores de Servicios de Certificación.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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.	Póliza de fianza para corroborar que está vigente y que corresponde a la presentada.
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	Póliza de fianza para corroborar que está vigente y que corresponde a la presentada.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

práctica del servicio acreditado ofrecido.	
ELEMENTOS MATERIALES.[5]	
Fundamento.	**Elementos para acreditar el cumplimiento.**
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.	Los controles de acceso físico y bitácoras que tengan tanto en sus Oficinas administrativas como en sus Centros de Datos. En la visita de verificación, la revisión de los elementos de seguridad con los que cuentan tanto en sus Oficinas administrativas como en sus Centros de Datos, mismos que deberán coincidir con las Políticas aprobadas por la DGNM.
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;	Los controles de acceso físico y bitácoras que tenga en su Oficina administrativa. En la visita de verificación, la revisión de los elementos de seguridad con los que cuentan en su Oficina administrativa, mismos que deberán coincidir con las Políticas aprobadas por la DGNM.
II. Los controles para evitar riesgo, daño, pérdida, alteración o sustracción de la información confidencial, incluso fuera de horario laboral;	En la visita de verificación, la revisión de los elementos de seguridad con los que cuentan en su Oficina administrativa, mismos que deberán coincidir con las Políticas aprobadas por la DGNM.
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;	Los controles de acceso físico y bitácoras que tengan tanto en su Oficina administrativa como en las áreas seguras en donde se resguarda la información concerniente al servicio de emisión de Certificados Digitales. En la visita de verificación, la revisión de los elementos de seguridad con los que cuentan en su Oficina administrativa como en las áreas seguras en donde se resguarda la información concerniente al servicio de emisión de Certificados Digitales, mismos que deberán coincidir con las Políticas aprobadas por la DGNM.
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;	En la visita de verificación, la revisión de los elementos de seguridad con los que cuentan en su Oficina administrativa, mismos que deberán coincidir con las Políticas de Certificación y/o Modelos Operacionales y/o Plan de Seguridad de Sistemas y/o Declaración de Prácticas de Certificación aprobados por la DGNM.

[5] Los Elementos Materiales se refieren de forma general en el artículo 5, fracción III, inciso b), del Reglamento del Código de Comercio en materia de Prestadores de Servicios de Certificación.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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;	En la visita de verificación, la revisión de los requerimientos de seguridad que deberán coincidir con el Análisis y Evaluación de Riesgos y Amenazas.
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	En la visita de verificación, la revisión de la infraestructura de computación y comunicaciones instaladas, así como los contratos de mantenimiento preventivo y correctivo y las bitácoras de mantenimiento.
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.	Documentación que acredite que el PSC cuenta con el personal especializado o en su caso, los contratos de mantenimiento preventivo y correctivo para garantizar la continua disponibilidad e integridad de los sistemas.
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:	
Certificaciones y estándares de calidad y seguridad vigentes, así como los procedimientos y prácticas de seguridad firmados por el Profesional Jurídico, el Profesional Informático y el Auxiliar de Apoyo Informático de Seguridad.	
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;	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
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	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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;	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
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;	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
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;	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
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;	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
VII. Detalle de los dispositivos electrónicos y su ubicación dentro de las áreas seguras que así lo requieran, siempre bajo	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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;	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
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	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
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.	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
34. Los dos centros de datos deberán estar separados cuando menos por 200 Kms., cuando estén localizados en zonas de alta sismicidad.	Verificar que la localización de los Centros de Datos coincida con la autorizada.
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;	Procedimientos y prácticas de seguridad que contengan detalladamente a los recursos humanos que deben observar dichos procedimientos y prácticas.
II. Bitácora del acceso a las áreas restringidas autorizado por el Profesional Informático o el Auxiliar de Apoyo Informático de Seguridad;	La última bitácora de acceso del PSC a los Centros de Datos.
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	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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;	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
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;	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
VI. El equipo instalado y las protecciones físicas para reducir amenazas;	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
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;	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
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;	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
IX. La identificación de las líneas eléctricas las cuales no deberán interferir con el funcionamiento del cableado de datos;	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
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;	En la visita de verificación, la revisión de la infraestructura de computación y comunicaciones instaladas, así como los contratos de mantenimiento preventivo y correctivo y las bitácoras de mantenimiento.
XI. Los sistemas informáticos, los cuales deberán de contar con el personal especializado o, en su caso, con los contratos de	Documentación que acredite que el Centro de Datos cuenta con el personal especializado o en su caso, los contratos de mantenimiento preventivo y correctivo para garantizar la continua disponibilidad e integridad de los sistemas.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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;	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
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;	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
XIV. Procedimientos para evitar que los equipos sean reutilizados o queden en desuso conteniendo información confidencial;	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
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	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
XVI. Mecanismo para registrar el mal funcionamiento, fallas, mantenimientos preventivos y correctivos, de los equipos y sistemas, sensibles para la operación del servicio.	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
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.	Verificación de que únicamente el personal autorizado del PSC pueda ingresar y administrar los equipos de la autoridad certificadora y de la autoridad registradora.
38. En caso de que los centros de datos principal y alterno sean arrendados, se deberá acreditar	Certificaciones y estándares de calidad y seguridad vigentes. En la visita de verificación, la revisión de la infraestructura de computación y comunicaciones instaladas, así como los contratos de

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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.	mantenimiento preventivo y correctivo y las bitácoras de mantenimiento. Documentación que acredite que el Centro de Datos cuenta con el personal especializado o en su caso, los contratos de mantenimiento preventivo y correctivo para garantizar la continua disponibilidad e integridad de los sistemas.
ELEMENTOS TECNOLÓGICOS.[6]	
Presentar el inventario de los elementos tecnológicos con los que cuenta actualmente, los cuales deberán coincidir con los previamente autorizados por la DGNM, en caso de que se detecte que alguno de los elementos no coincide con los ya autorizados o que se deba actualizar alguno de los requisitos, se deberá presentar lo siguiente:	
Fundamento.	**Elementos para acreditar el cumplimiento.**
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	Documentos que acrediten que cuenta con el/los equipos señalados en esta fracción, y/o visita de verificación.

[6] Los Elementos Tecnológicos se refieren de forma general en el artículo 5, fracción III, inciso d), del Reglamento del Código de Comercio en materia de Prestadores de Servicios de Certificación.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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;	Documentos que acrediten que cuenta con el/los equipos señalados en esta fracción, y/o visita de verificación.
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;	Documentos que acrediten que cuenta con el sistema señalado en esta fracción, y/o visita de verificación, así como ejemplos de Sellos Digitales de Tiempo derivados de la emisión y/o revocación de los certificados digitales.
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;	Documentos que acrediten que cuenta con el/los equipos y estándares señalados en esta fracción, y/o visita de verificación.
V. Un enlace mínimo de 100 MB a Internet;	Documentos que acrediten que cuenta con el enlace señalado en esta fracción, y/o visita de verificación.
VI. Un ruteador;	Documentos que acrediten que cuenta con el/los equipos señalados en esta fracción, y/o visita de verificación.
VII. Un muro de fuego (firewall);	Documentos que acrediten que cuenta con el/los elementos señalados en esta fracción, y/o visita de verificación.
VIII. Una computadora para gestionar el sistema de administración del servicio emisión de Certificados Digitales;	Documentos que acrediten que cuenta con el/los equipos señalados en esta fracción, y/o visita de verificación.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

IX. Un sistema de monitoreo de red;	Documentos que acrediten que cuenta con el licenciamiento actualizado del elemento señalado en esta fracción, y/o visita de verificación.
X. Un sistema confiable de antivirus;	Documentos que acrediten que cuenta con el licenciamiento actualizado del elemento señalado en esta fracción, y/o visita de verificación.
XI. Herramientas confiables de detección de vulnerabilidades;	Documentos que acrediten que cuenta con el licenciamiento actualizado del elemento señalado en esta fracción, y/o visita de verificación.
XII. Sistemas confiables de detección y protección de intrusión, y	Documentos que acrediten que cuenta con el licenciamiento actualizado del elemento señalado en esta fracción, y/o visita de verificación.
XIII. Las computadoras personales e impresoras necesarias para la prestación de los servicios de emisión de Certificados Digitales.	Documentos que acrediten que cuenta con el/los equipos señalados en esta fracción, y/o visita de verificación.
40. Todos los elementos descritos en la Regla 39 deberán considerar redundancia por seguridad.	Documentos que acrediten que cuenta con la redundancia de los elementos descritos en la Regla 39, y/o visita de verificación.
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.	Presentar la guía de virtualización de los elementos tecnológicos virtualizados.
42. Contar con la infraestructura informática que se detalla a continuación:	
I. Una Autoridad Certificadora y su redundancia por seguridad;	Documentos que acrediten que cuenta con el/los equipos (servidores y HSM) señalados en esta fracción, y/o visita de verificación.
II. Una Autoridad Registradora y su redundancia por seguridad;	Documentos que acrediten que cuenta con el/los equipos señalados en esta fracción, y/o visita de verificación.
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;	Documentos que acrediten que cuenta con el/los equipos señalados en esta fracción, y/o visita de verificación.
IV. Un servicio de OCSP y su redundancia por seguridad;	Documentos que acrediten que cuenta con el sistema OCSP y guía de usuario del elemento señalado en esta fracción, y/o visita de verificación.
V. Los procesos de administración de la Infraestructura Informática;	Documentos que acrediten que cuenta con el/los procesos de administración señalados en esta fracción, y/o visita de verificación.
VI. Un manual de Política de Certificados;	Aplica lo requerido en las Reglas 63, 64, 65 y 66.
VII. Una Declaración de Prácticas de Certificación, y	Aplica lo requerido en las Reglas 67 y 68.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

VIII. Los Manuales de Operación de las Autoridades Certificadora y Registradora.	Aplica lo requerido en las Reglas 57, 58, 59, 60, 61 y 62.
43. Contar con un documento de Análisis y Evaluación de Riesgos y Amenazas que deberá detallar por lo menos los siguientes elementos:	
Última versión del documento, en caso de que se haya modificado se verificará lo siguiente:	
I. Los activos críticos;	Que el documento contenga la información señalada en la presente fracción.
II. Requerimientos de seguridad	Que el documento contenga la información señalada en la presente fracción.
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;	Que el documento contenga la información señalada en la presente fracción.
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;	Que el documento contenga la información señalada en la presente fracción.
V. Medidas de seguridad para la mitigación de los riesgos detectados;	Que el documento contenga la información señalada en la presente fracción.
VI. Proceso de evaluación continua, para adecuar la valoración de riesgos a condiciones cambiantes del entorno;	Que el documento contenga la información señalada en la presente fracción.
VII. Los impactos que sufrirán los servicios del Prestador de Servicios de Certificación, en caso de interrupciones no planificadas, y	Que el documento contenga la información señalada en la presente fracción.
VIII. Adoptar Guide for Conducting Risk Assessments. NIST Special Publication 800-30 Revision 1. September 2012, equivalente o el que le sustituya.	Que el documento contenga la información señalada en la presente fracción.
44. Contar con un calendario de revisión y actualización del documento de Análisis y Evaluación de Riesgos y Amenazas.	Que el documento contenga la información señalada en la presente regla.
45. Contar con un documento de Política de Seguridad de la Información que deberá detallar por lo menos los siguientes elementos:	
Última versión del documento, en caso de que se haya modificado se verificará lo siguiente:	
I. Que el objeto de la Política de Seguridad sea congruente con el objeto del servicio de emisión de	Que el documento contenga la información señalada en la presente fracción.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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;	Que el documento contenga la información señalada en la presente fracción.
III. Estar basada en las recomendaciones de los estándares ISO/IEC de la serie 27000 o los que le sustituyan	Que el documento contenga la información señalada en la presente fracción.
IV. La Política de Seguridad de la Información deberá constar por escrito;	Que el documento contenga la información señalada en la presente fracción.
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;	Que el documento contenga la información señalada en la presente fracción.
VI. Las reglas que indiquen cómo son provistos los servicios y las medidas de seguridad asociadas;	Que el documento contenga la información señalada en la presente fracción.
VII. Ser consistente con la Política de Certificados y con la Declaración de Prácticas de Certificación, a que se refieren en el presente TÍTULO;	Que el documento contenga la información señalada en la presente fracción.
VIII. Adoptar el proceso Internet Security Policy: A Technical Guide, by the National Institute of Standards and Technologies (NIST) o un proceso similar, y	Que el documento contenga la información señalada en la presente fracción.
IX. Desarrollar procedimientos y buenas prácticas de seguridad para apoyar la aplicación de las políticas de seguridad.	Que el documento contenga la información señalada en la presente fracción.
46. Contar con un calendario de revisión y actualización del documento de Política de Seguridad de la Información	Que el documento contenga la información señalada en la presente regla.
47. Contar con un documento de Política de Seguridad Física que deberá detallar por lo menos los siguientes elementos:	
Última versión del documento, en caso de que se haya modificado se verificará lo siguiente:	

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

I. Control de acceso físico;	Que el documento contenga la información señalada en la presente fracción.
II. Protección y recuperación ante desastres;	Que el documento contenga la información señalada en la presente fracción.
III. Protecciones contra robo, forzamiento y entrada no autorizada a los espacios físicos;	Que el documento contenga la información señalada en la presente fracción.
IV. Medidas de protección en caso de incendio, contra fallas de servicios eléctricos o de telecomunicaciones, y	Que el documento contenga la información señalada en la presente fracción.
V. Un procedimiento de actualización para autorización de acceso al personal a las áreas restringidas.	Que el documento contenga la información señalada en la presente fracción.
48. Contar con un calendario de revisión y actualización del documento de Política de Seguridad Física.	Que el documento contenga la información señalada en la presente regla.
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.	Que el documento contenga la información señalada en la presente regla.
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.	Que el documento contenga la información señalada en la presente regla.
51. Contar con un calendario de revisión y actualización del documento de Sistema de Gestión de Seguridad de la información.	Que el documento contenga la información señalada en la presente regla.
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	Que el documento contenga la información señalada en la presente regla.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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.	Que el documento contenga la información señalada en la presente regla.
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: Última versión del documento, en caso de que se haya modificado se verificará lo siguiente:	
I. Afectación al funcionamiento de los sistemas y/o software;	Que el documento contenga la información señalada en la presente fracción.
II. Incidente de seguridad que afecte la operación de los sistemas y/o software;	Que el documento contenga la información señalada en la presente fracción.
III. Falla en el hardware donde se ejecuta el producto;	Que el documento contenga la información señalada en la presente fracción.
IV. Robo de los Datos de Creación de Firma Electrónica de los Certificados Digitales del Prestador de Servicios de Certificación;	Que el documento contenga la información señalada en la presente fracción.
V. Falla de los mecanismos de auditoría;	Que el documento contenga la información señalada en la presente fracción.
VI. Mecanismos para preservar evidencia del mal uso de los sistemas, y	Que el documento contenga la información señalada en la presente fracción.
VII. Demás casos que por su naturaleza pongan en riesgo el servicio acreditado.	Que el documento contenga la información señalada en la presente fracción.
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	Que el documento contenga la información señalada en la presente regla.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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.	Que el documento contenga la información señalada en la presente regla.
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:	
Última versión del documento, en caso de que se haya modificado se verificará lo siguiente:	
I. Cuáles son los servicios prestados;	Que el documento contenga la información señalada en la presente fracción.
II. Cómo se interrelacionan los diferentes servicios;	Que el documento contenga la información señalada en la presente fracción.
III. En qué lugares se operará;	Que el documento contenga la información señalada en la presente fracción.
IV. Cómo se protegerán los activos;	Que el documento contenga la información señalada en la presente fracción.
V. Qué tipos de Certificados Digitales se entregarán;	Que el documento contenga la información señalada en la presente fracción.
VI. Si se generarán Certificados Digitales con diferentes niveles de seguridad;	Que el documento contenga la información señalada en la presente fracción.
VII. Cuáles son las políticas y procedimientos de cada tipo de Certificado Digital;	Que el documento contenga la información señalada en la 94.
VIII. Interfaces con las Autoridades Registradoras e Interfaces con la Autoridad de Sellado Digital de Tiempo;	Que el documento contenga la información señalada en la presente fracción.
IX. Implementación de elementos de seguridad;	Que el documento contenga la información señalada en la presente fracción.
X. Procesos de administración;	Que el documento contenga la información señalada en la presente fracción.
XI. Sistema de directorios para los Certificados Digitales y sellos digitales de tiempo;	Que el documento contenga la información señalada en la presente fracción.
XII. Procesos de auditoría y respaldo;	Que el documento contenga la información señalada en la presente fracción.
XIII. Bases de datos a utilizar, y	Que el documento contenga la información señalada en la presente fracción.
XIV. Los requerimientos de seguridad física del personal, de	Que el documento contenga la información señalada en la presente fracción.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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.	Que el documento contenga la información señalada en la presente regla.
59. Contar con un calendario de revisión y actualización del documento de Modelo Operacional de la Autoridad Certificadora.	Que el documento contenga la información señalada en la presente regla.
60. Contar con un documento de Modelo Operacional de la Autoridad Registradora que deberá incluir como mínimo los apartados siguientes:	
Última versión del documento, en caso de que se haya modificado se verificará lo siguiente:	
I. Cuáles son los servicios de registro que se prestarán;	Que el documento contenga la información señalada en la presente fracción.
II. En qué lugares se ofrecerán dichos servicios;	Que el documento contenga la información señalada en la presente fracción.
III. Qué tipos de Certificados Digitales generados por la Autoridad Certificadora se entregarán;	Que el documento contenga la información señalada en la presente fracción.
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;	Que el documento contenga la información señalada en la presente fracción.
V. Interfaces con la Autoridad Certificadora;	Que el documento contenga la información señalada en la presente fracción.
VI. Implementación de dispositivos de seguridad;	Que el documento contenga la información señalada en la presente fracción.
VII. Procesos de administración;	Que el documento contenga la información señalada en la presente fracción.
VIII. Procesos de auditoría y respaldo;	Que el documento contenga la información señalada en la presente fracción.
IX. Bases de datos a utilizar;	Que el documento contenga la información señalada en la presente fracción.
X. Privacidad de datos, y	Que el documento contenga la información señalada en la presente fracción.
XI. Descripción de la seguridad física de las instalaciones.	Que el documento contenga la información señalada en la presente fracción.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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.	Que el documento contenga la información señalada en la presente regla.
62. Contar con un calendario de revisión y actualización del documento de Modelo Operacional de la Autoridad Registradora.	Que el documento contenga la información señalada en la presente regla.
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:	
Última versión del documento, en caso de que se haya modificado se verificará lo siguiente:	
I. Asegurar su concordancia con la Declaración de Prácticas de Certificación y los procedimientos operacionales;	Que el documento contenga la información señalada en la presente fracción.
II. Permitir la interoperabilidad con los Prestadores de Servicios de Certificación ya acreditados y con la Secretaría;	Que el documento contenga la información señalada en la presente fracción.
III. Indicar a quién se le puede otorgar un Certificado Digital;	Que el documento contenga la información señalada en la presente fracción.
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;	Que el documento contenga la información señalada en la presente fracción.
V. Describir las medidas de privacidad y de protección de datos que se aplicarán en materia de Firma Electrónica Avanzada;	Que el documento contenga la información señalada en la presente fracción.
VI. Establecer bajo qué circunstancias se puede revocar un Certificado Digital y quiénes pueden solicitarlo, y	Que el documento contenga la información señalada en la presente fracción.
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	Que el documento contenga la información señalada en la presente fracción.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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.	Que el documento contenga la información señalada en la presente regla.
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.	Que el documento contenga la información señalada en la presente regla.
66. Contar con un calendario de revisión y actualización del documento de Política de Certificados.	Que el documento contenga la información señalada en la presente regla.
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:	
Última versión del documento, en caso de que se haya modificado se verificará lo siguiente:	
I. Los procedimientos de operación para otorgar un Certificado y el alcance de aplicación de los mismos;	Que el documento contenga la información señalada en la presente fracción.
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;	Que el documento contenga la información señalada en la presente fracción.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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.	Que el documento contenga la información señalada en la presente fracción.
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;	Que el documento contenga la información señalada en la presente fracción.
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;	Que el documento contenga la información señalada en la presente fracción.
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;	Que el documento contenga la información señalada en la presente fracción.
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;	Que el documento contenga la información señalada en la presente fracción.
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;	Que el documento contenga la información señalada en la presente fracción.
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;	Que el documento contenga la información señalada en la presente fracción.
X. Los controles que se utilizarán para asegurar las auditorías y	Que el documento contenga la información señalada en la presente fracción.

almacenamiento de información relevante;	
XI. La fecha de inicio de operaciones, una vez otorgada la acreditación por la Secretaría;	Que el documento contenga la información señalada en la presente fracción.
XII. La Declaración de Prácticas de Certificación o parte de ésta, de acuerdo a la seguridad, será pública, y	Que el documento contenga la información señalada en la presente fracción.
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.	Que el documento contenga la información señalada en la presente fracción.
68. Contar con un calendario de revisión y actualización del documento de Declaración de Prácticas de Certificación.	Que el documento contenga la información señalada en la presente regla.
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:	
Última versión del documento, en caso de que se haya modificado se verificará lo siguiente:	
I. Claves de la Autoridad Certificadora;	Que el documento contenga la información señalada en la presente fracción.
II. Almacenamiento, respaldo, recuperación y uso de las claves privadas de Autoridad Certificadora y Autoridades Registradoras (en su caso);	Que el documento contenga la información señalada en la presente fracción.
III. Distribución del Certificado de la Autoridad Certificadora;	Que el documento contenga la información señalada en la presente fracción.
IV. Administración del ciclo de vida del hardware criptográfico que utilice la Autoridad Certificadora y Autoridades Registradoras (en su caso);	Que el documento contenga la información señalada en la presente fracción.
V. Los procedimientos que garanticen la seguridad de las claves en todo momento, aun en caso de cambios de personal y componentes tecnológicos;	Que el documento contenga la información señalada en la presente fracción.
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;	Que el documento contenga la información señalada en la presente fracción.
VII. Dispositivos seguros para que los usuarios almacenen sus Datos de Creación de Firma Electrónica, compatibles como mínimo con el	Que el documento contenga la información señalada en la presente fracción.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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	Que el documento contenga la información señalada en la presente fracción.
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.	Que el documento contenga la información señalada en la presente fracción.
70. Contar con un calendario de revisión y actualización del documento de Plan de Administración de Claves.	Que el documento contenga la información señalada en la presente regla.
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.	Evidencia del sitio electrónico, en donde se verifique que se pueden consultar lo señalado en la presente regla.
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.	Documentos que acrediten que cuenta con el/los procedimientos señalados en esta fracción, y/o visita de verificación.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

73. Establecer un calendario de revisión y actualización de los procedimientos descritos en la Regla 72.	Documentos que acrediten que cuenta con el calendario de revisión señalados en esta regla.
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 nternet 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:	
Certificados emitidos en el periodo solicitado. CRL vigente.	
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;	Certificados emitidos en el periodo solicitado.
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	Certificados emitidos en el periodo solicitado.
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.	Certificados emitidos en el periodo solicitado.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

75. La estructura de la CRL deberá ser compatible con la última versión del estándar ISO/IEC 9594-8 Information TechnologyâOpen Systems InterconnectionâThe DirectoryâPart 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:	
CRL vigente.	
I. Número de serie de los Certificados Digitales revocados por el emisor con fecha y hora de revocación;	CRL vigente.
II. La identificación del algoritmo de firma utilizado;	CRL vigente.
III. El nombre del emisor;	CRL vigente.
IV. La fecha y hora en que fue emitida la CRL;	CRL vigente.
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	CRL vigente.
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.	CRL vigente.
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	Verificación de historial de entrega a la Secretaría de Economía de certificados digitales emitidos.
II. El Prestador de Servicios de Certificación deberá cerciorarse que la Secretaría recibió la copia de cada Certificado Digital.	Verificación de historial de entrega a la Secretaría de Economía de certificados digitales emitidos.
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;	Presentar certificado emitido durante el periodo solicitado para validar su contenido.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

II. La dirección electrónica en donde se podrá consultar la CRL, y	Presentar certificado emitido durante el periodo solicitado para validar su contenido.
III. La dirección electrónica del servicio de OCSP en donde se podrá verificar el estado del Certificado Digital.	Presentar certificado emitido durante el periodo solicitado para validar su contenido.

VIII.2.2 Título Sexto De la Emisión de Sellos Digitales de Tiempo.	
ELEMENTOS HUMANOS.[7]	
Presentar la lista de los últimos elementos humanos con los que cuenta actualmente, los cuales deberán coincidir con los previamente autorizados por la DGNM, en caso de que se detecte que alguno de los elementos no coincide con los ya autorizados o que se deba actualizar alguno de los requisitos, se deberá presentar lo siguiente:	
Fundamento.	**Elementos para acreditar el cumplimiento.**
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;	Título profesional expedido por la Secretaría de Educación Pública y cédula profesional expedida 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;	Documentos que acrediten la experiencia señalada en la presente fracción, los siguientes ejemplos se señalan de manera enunciativa mas no limitativa: • Curriculum Vitae firmado autógrafamente, bajo protesta de decir verdad, en el cual deberán detallar las actividades que realizó o realiza en el área de correduría pública, derecho notarial o derecho mercantil. • Constancia laboral para acreditar el periodo y las actividades que realizó o realiza en el área de correduría pública, derecho notarial o derecho mercantil.
III. Acreditar al menos un año de experiencia en derecho informático, y	Documentos que acrediten la experiencia señalada en la presente fracción, los siguientes ejemplos se señalan de manera enunciativa mas no limitativa: • Curriculum Vitae firmado autógrafamente, bajo protesta de decir verdad, en el cual deberán detallar las actividades que realizó o realiza en el área de derecho informático. • Constancia laboral para acreditar el periodo y las actividades que realizó o realiza en el área de derecho informático.
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	Escrito libre firmado autógrafamente, mediante el cual declara 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, actualizado.

[7] Los Elementos Humanos se refieren de forma general en el artículo 5, fracción III, inciso a), del Reglamento del Código de Comercio en materia de Prestadores de Servicios de Certificación.

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;	Título profesional expedido por la Secretaría de Educación Pública y cédula profesional expedida por la Secretaría de Educación Pública o su equivalente.
II. Comprobar al menos dos años de experiencia en el área de criptografía;	Documentos que acrediten la experiencia señalada en la presente fracción, los siguientes ejemplos se señalan de manera enunciativa mas no limitativa: • Curriculum Vitae firmado autógrafamente, bajo protesta de decir verdad, en el cual deberán detallar las actividades que realizó o realiza en el área de criptografía. • Constancia laboral para acreditar el periodo y las actividades que realizó o realiza en el área de criptografía.
III. Acreditar estudios en manejo de software o hardware relacionados con criptografía, y	Documentos que acrediten que cuenta con estudios en manejo de software o hardware relacionados con criptografía como pueden ser: certificaciones y/o título de especialidad y/o título de maestría que acredite estudios en manejo de software o hardware relacionados con criptografía.
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.	Escrito libre firmado autógrafamente, mediante el cual declara 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, actualizado.
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;	Título profesional expedido por la Secretaría de Educación Pública y cédula profesional expedida por la Secretaría de Educación Pública o su equivalente.
II. Comprobar un año de experiencia en el área de criptografía;	Documentos que acrediten la experiencia señalada en la presente fracción, los siguientes ejemplos se señalan de manera enunciativa mas no limitativa: • Curriculum Vitae firmado autógrafamente, bajo protesta de decir verdad, en el cual deberán detallar las actividades que realizó o realiza en el área de criptografía. • Constancia laboral para acreditar el periodo y las actividades que realizó o realiza en el área de criptografía.
III. Acreditar estudios en manejo de software o hardware relacionados con criptografía, y	Documentos que acrediten que cuenta con estudios en manejo de software o hardware relacionados con criptografía como pueden ser: certificaciones y/o título de especialidad y/o título de maestría que

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

	acredite estudios en manejo de software o hardware relacionados con criptografía.
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.	Escrito libre firmado autógrafamente, mediante el cual declara 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, actualizado.
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.	Presentar la lista de los últimos elementos humanos con los que cuenta actualmente, los cuales deberán coincidir con los previamente autorizados por la DGNM, de acuerdo a la presente Regla.
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.	Documento que se utiliza para reclutar, seleccionar, evaluar y contratar al personal, para verificar si han llevado a cabo las revisiones establecidas y en su caso si se ha modificado.
ELEMENTOS ECONÓMICOS.[8]	
Fundamento.	**Elementos para acreditar el cumplimiento.**
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.	Documentos que acrediten que cuenta con capital que comprende al menos el equivalente a una cuarta parte de la inversión requerida. Se señalan de manera enunciativa mas no limitativa los siguientes: • Estados financieros. • Desglose de la inversión realizada. En caso de personas morales de carácter privado, además se deberán presentar los documentos que acrediten el capital social actual de la empresa. Presentar Seguro de responsabilidad civil para corroborar que esté vigente y que corresponde al presentado.

[8] Los Elementos Económicos se refieren de forma general en el artículo 5, fracción III, inciso c), del Reglamento del Código de Comercio en materia de Prestadores de Servicios de Certificación.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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.	Póliza de fianza para corroborar que está vigente y que corresponde a la presentada.
ELEMENTOS MATERIALES.[9]	
Fundamento.	**Elementos para acreditar el cumplimiento.**
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	Los controles de acceso físico y bitácoras que tengan tanto en sus Oficinas administrativas como en sus Centros de Datos. En la visita de verificación, la revisión de los elementos de seguridad con los que cuentan tanto en sus Oficinas administrativas como en

[9] Los Elementos Materiales se refieren de forma general en el artículo 5, fracción III, inciso b), del Reglamento del Código de Comercio en materia de Prestadores de Servicios de Certificación.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

necesarias para garantizar la seguridad para la emisión de Sellos Digitales de Tiempo.	sus Centros de Datos, mismos que deberán coincidir con las Políticas aprobadas por la DGNM.
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	En la visita de verificación, la revisión de los elementos de seguridad con los que cuentan en su Oficina administrativa, mismos que deberán coincidir con las Políticas aprobadas por la DGNM.
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.	Los controles de acceso físico y bitácoras que tengan tanto en su Oficina administrativa como en las áreas seguras en donde se resguarda la información concerniente al servicio de emisión de Sellos Digitales de Tiempo. En la visita de verificación, la revisión de los elementos de seguridad con los que cuentan en su Oficina administrativa como en las áreas seguras en donde se resguarda la información concerniente al servicio de emisión de Sellos Digitales de Tiempo, mismos que deberán coincidir con las Políticas aprobadas por la DGNM.
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:	
Certificaciones y estándares de calidad y seguridad vigentes, así como los procedimientos y prácticas de seguridad firmados por el Profesional Jurídico, el Profesional Informático y el Auxiliar de Apoyo Informático de Seguridad.	
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;	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
II. Para el caso de los servicios compartidos con otra organización,	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento

deberá asegurarse la separación física de los estantes de equipos del Prestador de Servicios de Certificación;	a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
III. El acceso de visitas a las áreas deberá ser autorizado por el Auxiliar de Apoyo Informático de Seguridad;	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
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;	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
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;	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
VI. Procedimiento para destruir material de desecho sin posibilidad de recuperación antes de desecharlo;	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
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	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
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.	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
89. Los dos centros de datos deberán estar separados cuando menos por 200 Kms., cuando estén localizados en zonas de alta sismicidad.	Verificar que la localización de los Centros de Datos coincida con la autorizada.
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;	Procedimientos y prácticas de seguridad que contengan detalladamente a los recursos humanos que deben observar dichos procedimientos y prácticas.
II. Bitácora del acceso a las áreas donde se ubique la infraestructura de tiempo confiable autorizado por	La última bitácora de acceso del PSC a los Centros de Datos.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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;	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
IV. Los mecanismos que impidan que personal no autorizado acceda a las áreas del perímetro de seguridad;	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
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;	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
VI. El equipo instalado y las protecciones físicas para reducir amenazas;	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
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;	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
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;	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
IX. La identificación de las líneas eléctricas, las cuales no deberán interferir con el funcionamiento del cableado de datos;	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
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	En la visita de verificación, la revisión de la infraestructura de computación y comunicaciones instaladas, así como los contratos de mantenimiento preventivo y correctivo y las bitácoras de mantenimiento.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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;	Documentación que acredite que el Centro de Datos cuenta con el personal especializado o en su caso, los contratos de mantenimiento preventivo y correctivo para garantizar la continua disponibilidad e integridad de los sistemas.
XII. Procedimientos para evitar que equipos, información y software salgan de los perímetros de seguridad sin autorización;	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
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;	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
XIV. Procedimientos para evitar que los equipos sean reutilizados o queden en desuso conteniendo información confidencial;	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
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	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
XVI. Mecanismo para registrar el mal funcionamiento, fallas, mantenimientos preventivos y correctivos, de los equipos y sistemas., sensibles para la operación del servicio.	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
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.	Verificación de que únicamente el personal autorizado del PSC pueda ingresar y administrar los equipos de la autoridad de sellado digital de tiempo.
93. En caso que, los centros de datos principal y alterno sean arrendados,	Certificaciones y estándares de calidad y seguridad vigentes.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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 notificados a la Secretaría.	En la visita de verificación, la revisión de la infraestructura de computación y comunicaciones instaladas, así como los contratos de mantenimiento preventivo y correctivo y las bitácoras de mantenimiento. Documentación que acredite que el Centro de Datos cuenta con el personal especializado o en su caso, los contratos de mantenimiento preventivo y correctivo para garantizar la continua disponibilidad e integridad de los sistemas.
ELEMENTOS TECNOLÓGICOS.[10]	
Presentar el inventario de los elementos tecnológicos con los que cuenta actualmente, los cuales deberán coincidir con los previamente autorizados por la DGNM, en caso de que se detecte que alguno de los elementos no coincide con los ya autorizados o que se deba actualizar alguno de los requisitos, se deberá presentar lo siguiente:	
Fundamento.	**Elementos para acreditar el cumplimiento.**
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	Documentos que acrediten que cuenta con el/los equipos señalados en esta fracción, y/o visita de verificación.

[10] Los Elementos Tecnológicos se refieren de forma general en el artículo 5, fracción III, inciso d), del Reglamento del Código de Comercio en materia de Prestadores de Servicios de Certificación.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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;	Documentos que acrediten que cuenta con el/los equipos y estándares señalados en esta fracción, y/o verificación visita de verificación.
III. Un enlace mínimo de 100 MB a Internet;	Documentos que acrediten que cuenta con el enlace señalado en esta fracción, y/o visita de verificación.
IV. Un ruteador;	Documentos que acrediten que cuenta con el/los equipos señalados en esta fracción, y/o visita de verificación.
V. Un muro de fuego (firewall);	Documentos que acrediten que cuenta con el/los elementos señalados en esta fracción, y/o visita de verificación.
VI. Un sistema cliente de solicitud de Sellos Digitales de Tiempo compatible con el equipo para la Autoridad de Sellado Digital de Tiempo (opcional);	Documentos que acrediten que en su caso, cuenta con el aplicativo para llevar a cabo la emisión de Sellos Digitales de Tiempo.
VII. Una computadora para gestionar el sistema de administración del servicio emisión de Sellos Digitales de Tiempo;	Documentos que acrediten que cuenta con el/los equipos señalados en esta fracción, y/o visita de verificación.
VIII. Un sistema de monitoreo de red;	Documentos que acrediten que cuenta con el licenciamiento actualizado del elemento señalado en esta fracción, y/o visita de verificación.
IX. Un sistema confiable de antivirus;	Documentos que acrediten que cuenta con el licenciamiento actualizado del elemento señalado en esta fracción, y/o visita de verificación.
X. Herramientas confiables de detección de vulnerabilidades;	Documentos que acrediten que cuenta con el licenciamiento actualizado del elemento señalado en esta fracción, y/o visita de verificación.
XI. Sistemas confiables de detección y protección de intrusión, y	Documentos que acrediten que cuenta con el licenciamiento actualizado del elemento señalado en esta fracción, y/o visita de verificación.
XII. Las computadoras personales e impresoras necesarias para la prestación del servicio de emisión de Sellos Digitales de Tiempo.	Documentos que acrediten que cuenta con el/los equipos señalados en esta fracción, y/o visita de verificación.
95. Las tecnologías de virtualización deberán ser compatibles con las normas y criterios nacionales y/o internacionales y, al menos con el	Presentar la guía de virtualización de los elementos tecnológicos virtualizados.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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.	Documentos que acrediten que cuenta con la redundancia de los elementos descritos en la Regla 94, y/o visita de verificación.
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;	Documentos que acrediten que cuenta con el/los equipos (servidores y HSM) y de ser el caso, con el sistema cliente, señalados en esta fracción, y/o visita de verificación.
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;	Documentos que acrediten que cuenta con el/los equipos señalados en esta fracción, y/o visita de verificación.
III. Los procesos de administración de la infraestructura informática;	Documentos que acrediten que cuenta con el/los procesos de administración señalados en esta fracción, y/o visita de verificación.
IV. Un manual de Política de Sellos Digitales de Tiempo;	Aplica lo requerido en las Reglas 116 y 117.
V. Un manual de Declaración de Prácticas de Sellos Digitales de Tiempo, y	Aplica lo requerido en las Reglas 118 y 119.
VI. Un manual de operación de la Autoridad de Sellado Digital de Tiempo.	Aplica lo requerido en las Reglas 112, 113 y 114.
98. Contar con un documento de Análisis y Evaluación de Riesgos y Amenaza que deberá detallar por lo menos los siguientes elementos:	
Última versión del documento, en caso de que se haya modificado se verificará lo siguiente:	
I. Los activos críticos;	Que el documento contenga la información señalada en la presente fracción.
II. Vulnerabilidades y amenazas de la infraestructura con la que proveerá el o los servicios y determinar los requerimientos de seguridad;	Que el documento contenga la información señalada en la presente fracción.
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;	Que el documento contenga la información señalada en la presente fracción.
IV. Medidas de seguridad para la mitigación de los riesgos detectados;	Que el documento contenga la información señalada en la presente fracción.
V. Proceso de evaluación continua, para adecuar la valoración de riesgos a condiciones cambiantes del entorno;	Que el documento contenga la información señalada en la presente fracción.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

VI. Los impactos que sufrirán los servicios del Prestador de Servicios de Certificación en caso de interrupciones no planificadas, y	Que el documento contenga la información señalada en la presente fracción.
VII. Adoptar Guide for Conducting Risk Assessments. NIST Special Publication 800-30 Revision 1. September 2012, equivalente o el que le sustituya.	Que el documento contenga la información señalada en la presente fracción.
99. Contar con un calendario de revisión y actualización del documento de Análisis y Evaluación de Riesgos y Amenazas.	Que el documento contenga la información señalada en la presente regla.
100. Contar con un documento de Política de Seguridad de la Información que deberá detallar por lo menos los siguientes elementos:	
Última versión del documento, en caso de que se haya modificado se verificará lo siguiente:	
I. Ser congruente con el objeto del servicio de emisión de Sellos Digitales de Tiempo que ofrecerá el Prestador de Servicios de Certificación;	Que el documento contenga la información señalada en la presente fracción.
II. Los objetivos de seguridad claros, generales, no técnicos, que se desarrollarán a partir del resultado del Análisis y Evaluación de Riesgos y Amenazas;	Que el documento contenga la información señalada en la presente fracción.
III. Estar basada en las recomendaciones de los estándares ISO/IEC de la serie 27000 o los que le sustituyan;	Que el documento contenga la información señalada en la presente fracción.
IV. La Política de Seguridad de la Información puede estar conformada con una política general y soportada con políticas específicas;	Que el documento contenga la información señalada en la presente fracción.
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;	Que el documento contenga la información señalada en la presente fracción.
VI. Las reglas que indiquen cómo son provistos los servicios y las medidas de seguridad asociadas;	Que el documento contenga la información señalada en la presente fracción.
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;	Que el documento contenga la información señalada en la presente fracción.
VIII. Adoptar el proceso de Internet Security Policy: A Technical Guide, by	Que el documento contenga la información señalada en la presente fracción.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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.	Que el documento contenga la información señalada en la presente fracción.
101. Contar con un calendario de revisión y actualización del documento de Política de Seguridad de la Información.	Que el documento contenga la información señalada en la presente regla.
102. Contar con un documento de Política de Seguridad Física que deberá detallar por lo menos los siguientes elementos:	
Última versión del documento, en caso de que se haya modificado se verificará lo siguiente:	
I. Control de acceso físico;	Que el documento contenga la información señalada en la presente fracción.
II. Protección y recuperación ante desastres;	Que el documento contenga la información señalada en la presente fracción.
III. Protecciones contra robo, forzamiento y entrada no autorizada a los espacios físicos;	Que el documento contenga la información señalada en la presente fracción.
IV. Medidas de protección en caso de incendio, contra fallas de servicios eléctricos o de telecomunicaciones, y	Que el documento contenga la información señalada en la presente fracción.
V. Un procedimiento de actualización para autorización de acceso al personal a las áreas restringidas.	Que el documento contenga la información señalada en la presente fracción.
103. Contar con un calendario de revisión y actualización del documento de Política de Seguridad Física.	Que el documento contenga la información señalada en la presente regla.
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.	Última versión del documento, en caso de que se haya modificado se verificará lo siguiente: Que el documento contenga la información señalada en la presente regla.
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.	Que el documento contenga la información señalada en la presente regla.
106. Contar con un calendario de revisión y actualización del documento de Sistema de Gestión de Seguridad de la Información.	Que el documento contenga la información señalada en la presente regla.
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	Última versión del documento, en caso de que se haya modificado se verificará lo siguiente: Que el documento contenga la información señalada en la presente regla.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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.	Que el documento contenga la información señalada en la presente regla.
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;	Que el documento contenga la información señalada en la presente fracción.
II. Incidente de seguridad que afecte la operación de los sistemas y/o software;	Que el documento contenga la información señalada en la presente fracción.
III. Falla en el hardware donde se ejecuta el producto;	Que el documento contenga la información señalada en la presente fracción.
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;	Que el documento contenga la información señalada en la presente fracción.
V. Falla de los mecanismos de auditoría;	Que el documento contenga la información señalada en la presente fracción.
VI. Mecanismos para preservar evidencia del mal uso de los sistemas, y	Que el documento contenga la información señalada en la presente fracción.
VII. Demás casos que por su naturaleza pongan en riesgo el servicio acreditado.	Que el documento contenga la información señalada en la presente fracción.
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	Que el documento contenga la información señalada en la presente regla.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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.	Que el documento contenga la información señalada en la presente regla.
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;	Que el documento contenga la información señalada en la presente fracción.
II. Cómo se interrelacionan los diferentes servicios;	Que el documento contenga la información señalada en la presente fracción.
III. En qué lugares se operará;	Que el documento contenga la información señalada en la presente fracción.
IV. Cómo se protegerán los activos;	Que el documento contenga la información señalada en la presente fracción.
V. Implementación de elementos de seguridad;	Que el documento contenga la información señalada en la presente fracción.
VI. Procesos de administración;	Que el documento contenga la información señalada en la presente fracción.
VII. Sistema de directorios para los sellos digitales de tiempo;	Que el documento contenga la información señalada en la presente fracción.
VIII. Procesos de auditoría y respaldo, y	Que el documento contenga la información señalada en la presente fracción.
IX. Bases de datos a utilizar.	Que el documento contenga la información señalada en la presente fracción.
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.	Que el documento contenga la información señalada en la presente regla.
114. Contar con un calendario de revisión y actualización del documento de Modelo Operacional	Que el documento contenga la información señalada en la presente regla.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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	Que el documento contenga la información señalada en la presente fracción.
II. Indicar a quién se le puede otorgar un sello digital de tiempo.	Que el documento contenga la información señalada en la presente fracción.
116. La Política de Sellos Digitales de Tiempo tendrá que ser compatible con el RFC 3628 "Policy Requirements for TimeStamping Authorities (TSAs)" o el que le sustituya nacional y/o internacional.	Que el documento contenga la información señalada en la presente regla.
117. Contar con un calendario de revisión y actualización del documento de Política de Sellos Digitales de Tiempo.	Que el documento contenga la información señalada en la presente regla.
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;	Que el documento contenga la información señalada en la presente fracción.
II. Las responsabilidades y obligaciones del Prestador de Servicios de Certificación y de sus usuarios;	Que el documento contenga la información señalada en la presente fracción.
III. Las medidas de seguridad adoptadas para proteger sus Datos de Creación de Firma Electrónica para sellos digitales de tiempo;	Que el documento contenga la información señalada en la presente fracción.
IV. Los controles que se utilizarán para asegurar las auditorías y almacenamiento de información relevante;	Que el documento contenga la información señalada en la presente fracción.
V. Una vez otorgada la acreditación por la Secretaría, la fecha de inicio de operaciones;	Que el documento contenga la información señalada en la presente fracción.
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	Que el documento contenga la información señalada en la presente fracción.
VII. La Declaración de Prácticas de Sellos Digitales de Tiempo o parte de ésta, de acuerdo a la seguridad, será pública.	Que el documento contenga la información señalada en la presente fracción.
119. Contar con un calendario de revisión y actualización del documento de Declaración de	Que el documento contenga la información señalada en la presente regla.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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;	Que el documento contenga la información señalada en la presente fracción.
II. Almacenamiento, respaldo, recuperación y uso de las claves privadas de la Autoridad de Sellado Digital de Tiempo;	Que el documento contenga la información señalada en la presente fracción.
III. Distribución del Certificado de la Autoridad de Sellado Digital de Tiempo;	Que el documento contenga la información señalada en la presente fracción.
IV. Administración del ciclo de vida del hardware criptográfico que utilice la Autoridad de Sellado Digital de Tiempo;	Que el documento contenga la información señalada en la presente fracción.
V. Los procedimientos que garanticen la seguridad de las claves en todo momento, aun en caso de cambios de personal y componentes tecnológicos;	Que el documento contenga la información señalada en la presente fracción.
VI. Utilizar claves con longitud mínima de 4096 bits y ajustarse cuando así el avance tecnológico lo requiera previo comunicado de la Secretaría.	Que el documento contenga la información señalada en la presente fracción.
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	Que el documento contenga la información señalada en la presente fracción.
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.	Que el documento contenga la información señalada en la presente fracción.
121. Contar con un calendario de revisión y actualización del documento de Plan de Administración de Claves.	Que el documento contenga la información señalada en la presente regla.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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.	Evidencia del sitio electrónico, en donde se verifique que se pueden consultar lo señalado en la presente regla.
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.	Presentar contrato para corroborar que está vigente y que corresponde al que se registró.

VIII.2.3 Título Séptimo De la Constancia de Conservación de Mensaje de Datos emitida de conformidad con la NOM-151-SCFI-2016.	
ELEMENTOS HUMANOS.[11]	
Presentar la lista de los últimos elementos humanos con los que cuenta actualmente, los cuales deberán coincidir con los previamente autorizados por la DGNM, en caso de que se detecte que alguno de los elementos no coincide con los ya autorizados o que se deba actualizar alguno de los requisitos, se deberá presentar lo siguiente:	
Fundamento.	**Elementos para acreditar el cumplimiento.**
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;	Título profesional expedido por la Secretaría de Educación Pública y cédula profesional expedida 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;	Documentos que acrediten la experiencia señalada en la presente fracción, los siguientes ejemplos se señalan de manera enunciativa mas no limitativa: • Curriculum Vitae firmado autógrafamente, bajo protesta de decir verdad, en el cual deberán detallar las actividades que realizó o realiza en el área de correduría pública, derecho notarial o derecho mercantil. • Constancia laboral para acreditar el periodo y las actividades que realizó o realiza en el área de correduría pública, derecho notarial o derecho mercantil.
III. Acreditar al menos un año de experiencia en derecho informático, y	Documentos que acrediten la experiencia señalada en la presente fracción, los siguientes ejemplos se señalan de manera enunciativa mas no limitativa:

[11] Los Elementos Humanos se refieren de forma general en el artículo 5, fracción III, inciso a), del Reglamento del Código de Comercio en materia de Prestadores de Servicios de Certificación.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

	• Curriculum Vitae firmado autógrafamente, bajo protesta de decir verdad, en el cual deberán detallar las actividades que realizó o realiza en el área de derecho informático. • Constancia laboral para acreditar el periodo y las actividades que realizó o realiza en el área de derecho informático.
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.	Escrito libre firmado autógrafamente, mediante el cual declara 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, actualizado.
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;	Título profesional expedido por la Secretaría de Educación Pública y cédula profesional expedida por la Secretaría de Educación Pública o su equivalente.
II. Comprobar al menos dos años de experiencia en el área de criptografía;	Documentos que acrediten la experiencia señalada en la presente fracción, los siguientes ejemplos se señalan de manera enunciativa mas no limitativa: • Curriculum Vitae firmado autógrafamente, bajo protesta de decir verdad, en el cual deberán detallar las actividades que realizó o realiza en el área de criptografía. • Constancia laboral para acreditar el periodo y las actividades que realizó o realiza en el área de criptografía.
III. Acreditar estudios en manejo de software o hardware relacionados con criptografía, y	Documentos que acrediten que cuenta con estudios en manejo de software o hardware relacionados con criptografía como pueden ser: certificaciones y/o título de especialidad y/o título de maestría que acredite estudios en manejo de software o hardware relacionados con criptografía.
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.	Escrito libre firmado autógrafamente, mediante el cual declara 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, actualizado.
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:	

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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;	Título profesional expedido por la Secretaría de Educación Pública y cédula profesional expedida por la Secretaría de Educación Pública o su equivalente.
II. Comprobar al menos dos años de experiencia en el área de criptografía;	Documentos que acrediten la experiencia señalada en la presente fracción, los siguientes ejemplos se señalan de manera enunciativa mas no limitativa: • Curriculum Vitae firmado autógrafamente, bajo protesta de decir verdad, en el cual deberán detallar las actividades que realizó o realiza en el área de criptografía. • Constancia laboral para acreditar el periodo y las actividades que realizó o realiza en el área de criptografía.
III. Acreditar estudios en manejo de software o hardware relacionados con criptografía, y	Documentos que acrediten que cuenta con estudios en manejo de software o hardware relacionados con criptografía como pueden ser: certificaciones y/o título de especialidad y/o título de maestría que acredite estudios en manejo de software o hardware relacionados con criptografía.
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.	Escrito libre firmado autógrafamente, mediante el cual declara 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, actualizado.
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.	Presentar la lista de los últimos elementos humanos con los que cuenta actualmente, los cuales deberán coincidir con los previamente autorizados por la DGNM, de acuerdo a la presente regla.
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.	Documento que se utiliza para reclutar, seleccionar, evaluar y contratar al personal, para verificar si han llevado a cabo las revisiones establecidas y en su caso si se ha modificado.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

ELEMENTOS ECONÓMICOS.[12]	
Fundamento.	**Elementos para acreditar el cumplimiento.**
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.	Documentos que acrediten que cuenta con capital que comprende al menos el equivalente a una cuarta parte de la inversión requerida. Se señalan de manera enunciativa mas no limitativa los siguientes: • Estados financieros. • Desglose de la inversión realizada. En caso de personas morales de carácter privado, además se deberán presentar los documentos que acrediten el capital social actual de la empresa. Presentar el Seguro de responsabilidad civil para corroborar que esté vigente y que corresponde al presentado.
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	Póliza de fianza para corroborar que está vigente y que corresponde al presentado.

[12] Los Elementos Económicos se refieren de forma general en el artículo 5, fracción III, inciso c), del Reglamento del Código de Comercio en materia de Prestadores de Servicios de Certificación.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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.	
ELEMENTOS MATERIALES.[13]	
Fundamento.	**Elementos para acreditar el cumplimiento.**
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.	Los controles de acceso físico y bitácoras que tengan tanto en sus Oficinas administrativas como en sus Centros de Datos. En la visita de verificación, la revisión de los elementos de seguridad con los que cuentan tanto en sus Oficinas administrativas como en sus Centros de Datos, mismos que deberán coincidir con las Políticas aprobadas por la DGNM.
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	Los controles de acceso físico y bitácoras que tenga en su Oficina administrativa. En la visita de verificación, la revisión de los elementos de seguridad con los que cuentan en su Oficina administrativa, mismos que deberán coincidir con las Políticas aprobadas por la DGNM.
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.	Los controles de acceso físico y bitácoras que tengan tanto en su Oficina administrativa como en las áreas seguras en donde se resguarda la información concerniente al servicio de Constancias de Conservación de Mensaje de Datos que se emitan de conformidad con la NOM-151-SCFI-2016. En la visita de verificación, la revisión de los elementos de seguridad con los que cuentan en su Oficina administrativa como en las áreas seguras en donde se resguarda la información concerniente al servicio de Constancias de Conservación de Mensaje de Datos que se emitan de conformidad con la NOM-151-SCFI-2016, mismos que deberán coincidir con las Políticas aprobadas por la DGNM.

[13] Los Elementos Materiales se refieren de forma general en el artículo 5, fracción III, inciso b), del Reglamento del Código de Comercio en materia de Prestadores de Servicios de Certificación.

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:	
Certificaciones y estándares de calidad y seguridad vigentes, así como los procedimientos y prácticas de seguridad firmados por el Profesional Jurídico, el Profesional Informático y el Auxiliar de Apoyo Informático de Seguridad.	
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;	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
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;	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
III. El acceso de visitas a las áreas deberá ser autorizado por el Auxiliar de Apoyo Informático de Seguridad;	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
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;	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
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;	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

VI. Procedimiento para destruir material de desecho, como cajas de cartón, empaques, entre otros, sin posibilidad de recuperación antes de desecharlo;	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
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	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
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.	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
135. Los dos centros de datos deberán estar separados cuando menos por 200 Kms., cuando estén localizados en zonas de alta sismicidad.	Verificar que la localización de los Centros de Datos coincida con la autorizada.
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;	Procedimientos y prácticas de seguridad que contengan detalladamente a los recursos humanos que deben observar dichos procedimientos y prácticas.
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;	La última bitácora de acceso del PSC a los Centros de Datos.
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;	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

IV. Los mecanismos que impidan que personal no autorizado acceda a las áreas del perímetro de seguridad;	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
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;	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
VI. El equipo instalado y las protecciones físicas para reducir amenazas.	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
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;	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
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;	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
IX. La identificación de las líneas eléctricas las cuales no deberán interferir con el funcionamiento del cableado de datos;	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
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;	En la visita de verificación, la revisión de la infraestructura de computación y comunicaciones instaladas, así como los contratos de mantenimiento preventivo y correctivo y las bitácoras de mantenimiento.
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	Documentación que acredite que el Centro de Datos cuenta con el personal especializado o en su caso, los contratos de mantenimiento preventivo y correctivo para garantizar la continua disponibilidad e integridad de los sistemas.

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;	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
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;	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
XIV. Procedimientos para evitar que los equipos sean reutilizados o queden en desuso conteniendo información confidencial;	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
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	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
XVI. Mecanismo para registrar el mal funcionamiento, fallas, mantenimientos preventivos y correctivos, de los equipos y sistemas, sensibles para la operación del servicio.	Procedimientos y prácticas de seguridad que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
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.	Verificación de que únicamente el personal autorizado del PSC pueda ingresar y administrar los equipos de la autoridad certificadora y de la autoridad registradora.
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.	Certificaciones y estándares de calidad y seguridad vigentes. En la visita de verificación, la revisión de la infraestructura de computación y comunicaciones instaladas, así como los contratos de mantenimiento preventivo y correctivo y las bitácoras de mantenimiento. Documentación que acredite que el Centro de Datos cuenta con el personal especializado o en su caso, los contratos de mantenimiento preventivo y correctivo para garantizar la continua disponibilidad e integridad de los sistemas.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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.	
ELEMENTOS TECNOLÓGICOS.[14]	
Presentar el inventario de los elementos tecnológicos con los que cuenta actualmente, los cuales deberán coincidir con los previamente autorizados por la DGNM, en caso de que se detecte que alguno de los elementos no coincide con los ya autorizados o que se deba actualizar alguno de los requisitos, se deberá presentar lo siguiente:	
Fundamento.	**Elementos para acreditar el cumplimiento.**
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;	Documentos que acrediten que cuenta con el/los equipos señalados en esta fracción, y/o visita de verificación.

[14] Los Elementos Tecnológicos se refieren de forma general en el artículo 5, fracción III, inciso d), del Reglamento del Código de Comercio en materia de Prestadores de Servicios de Certificación.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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;	Documentos que acrediten que cuenta con el/los equipos y estándares señalados en esta fracción, y/o visita de verificación.
III. Un enlace mínimo de 100 MB a Internet;	Documentos que acrediten que cuenta con el enlace señalado en esta fracción, y/o visita de verificación.
IV. Un ruteador;	Documentos que acrediten que cuenta con el/los equipos señalados en esta fracción, y/o visita de verificación.
V. Un muro de fuego (firewall);	Documentos que acrediten que cuenta con el/los elementos señalados en esta fracción, y/o visita de verificación.
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);	Documentos que acrediten que en su caso, cuenta con el aplicativo para llevar a cabo la emisión de Constancias de Conservación de Mensaje de Datos emitidas de conformidad con la NOM-151-SCFI-2016.
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;	Documentos que acrediten que cuenta con el/los equipos señalados en esta fracción, y/o visita de verificación.
VIII. Un sistema de monitoreo de red;	Documentos que acrediten que cuenta con el licenciamiento actualizado del elemento señalado en esta fracción, y/o visita de verificación.
IX. Un sistema confiable de antivirus;	Documentos que acrediten que cuenta con el licenciamiento actualizado del elemento señalado en esta fracción, y/o visita de verificación.
X. Herramientas confiables de detección de vulnerabilidades;	Documentos que acrediten que cuenta con el licenciamiento actualizado del elemento señalado en esta fracción, y/o visita de verificación.
XI. Sistemas confiables de detección y protección de intrusión, y	Documentos que acrediten que cuenta con el licenciamiento actualizado del elemento señalado en esta fracción, y/o visita de verificación.
XII. Las computadoras personales e impresoras necesarias para la prestación del servicio de Constancias de Conservación de	Documentos que acrediten que cuenta con el/los equipos señalados en esta fracción, y/o visita de verificación.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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.	Presentar la guía de virtualización de los elementos tecnológicos virtualizados.
142. Todos los elementos mencionados en la Regla 140 deberán considerar redundancia por seguridad.	Documentos que acrediten que cuenta con la redundancia de los elementos descritos en la Regla 140, y/o visita de verificación.
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-SCFI2016 y el sistema cliente (opcional) que solicita la constancia de conservación de mensaje de datos, y su redundancia por seguridad;	Documentos que acrediten que cuenta con el/los equipos (servidores y HSM) y de ser el caso, con el sistema cliente, señalados en esta fracción, y/o visita de verificación.
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;	Documentos que acrediten que cuenta con el/los equipos señalados en esta fracción, y/o visita de verificación.
III. Los procesos de administración de la Infraestructura Informática;	Documentos que acrediten que cuenta con el/los procesos de administración señalados en esta fracción, y/o visita de verificación.
IV. Un manual de Política de Constancias de Conservación de Mensaje de Datos emitidas de conformidad con la NOM-151- SCFI-2016;	Aplica lo requerido en las Reglas 161 y 162.
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	Aplica lo requerido en las Reglas 163 y 164.
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.	Aplica lo requerido en las Reglas 158, 159 y 160.
144. Contar con un documento de Análisis y Evaluación de Riesgos y Amenazas que deberá detallar por lo menos los siguientes elementos:	
Última versión del documento, en caso de que se haya modificado se verificará lo siguiente:	
I. Los activos críticos;	Que el documento contenga la información señalada en la presente fracción.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

II. Vulnerabilidades y amenazas de la infraestructura con la que proveerá el o los servicios y determinar los requerimientos de seguridad;	Que el documento contenga la información señalada en la presente fracción.
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;	Que el documento contenga la información señalada en la presente fracción.
IV. Medidas de seguridad para la mitigación de los riesgos detectados;	Que el documento contenga la información señalada en la presente fracción.
V. Proceso de evaluación continua, para adecuar la valoración de riesgos a condiciones cambiantes del entorno;	Que el documento contenga la información señalada en la presente fracción.
VI. Los impactos que sufrirán los servicios del Prestador de Servicios de Certificación, en caso de interrupciones no planificadas, y	Que el documento contenga la información señalada en la presente fracción.
VII. Adoptar la Guide for Conducting Risk Assessments. NIST Special Publication 800-30 Revision 1. September 2012, equivalente o el que le sustituya.	Que el documento contenga la información señalada en la presente fracción.
145. Contar con un calendario de revisión y actualización del documento de Análisis y Evaluación de Riesgos y Amenazas.	Que el documento contenga la información señalada en la presente regla.
146. Contar con un documento de Política de Seguridad de la Información que deberá detallar por lo menos los siguientes elementos:	
Última versión del documento, en caso de que se haya modificado se verificará lo siguiente:	
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;	Que el documento contenga la información señalada en la presente fracción.
II. Los objetivos de seguridad claros, generales, no técnicos, que se desarrollarán a partir del resultado del Análisis y Evaluación de Riesgos y Amenazas;	Que el documento contenga la información señalada en la presente fracción.
III. Estar basada en las recomendaciones de los estándares ISO/IEC de la serie 27000 o los que le sustituyan;	Que el documento contenga la información señalada en la presente fracción.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

IV. La Política de Seguridad de la información puede estar conformada con una política general y soportada con políticas específicas;	Que el documento contenga la información señalada en la presente fracción.
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;	Que el documento contenga la información señalada en la presente fracción.
VI. Las reglas que indiquen cómo son provistos los servicios y las medidas de seguridad asociadas;	Que el documento contenga la información señalada en la presente fracción.
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;	Que el documento contenga la información señalada en la presente fracción.
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	Que el documento contenga la información señalada en la presente fracción.
IX. Procedimientos y buenas prácticas de seguridad para apoyar la aplicación de las políticas de seguridad.	Que el documento contenga la información señalada en la presente fracción.
147. Contar con un calendario de revisión y actualización del documento de Política de Seguridad de la Información.	Que el documento contenga la información señalada en la presente regla.
148. Contar con un documento de Política de Seguridad Física que deberá detallar por lo menos los siguientes elementos:	
Última versión del documento, en caso de que se haya modificado se verificará lo siguiente:	
I. Control de acceso físico;	Que el documento contenga la información señalada en la presente fracción.
II. Protección y recuperación ante desastres;	Que el documento contenga la información señalada en la presente fracción.
III. Protecciones contra robo, forzamiento y entrada no autorizada a los espacios físicos;	Que el documento contenga la información señalada en la presente fracción.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

IV. Medidas de protección en caso de incendio, contra fallas de servicios eléctricos o de telecomunicaciones, y	Que el documento contenga la información señalada en la presente fracción.
V. Un procedimiento de actualización para autorización de acceso al personal a las áreas restringidas.	Que el documento contenga la información señalada en la presente fracción.
149. Contar con un calendario de revisión y actualización del documento de Política de Seguridad Física.	Que el documento contenga la información señalada en la presente regla.
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.	Última versión del documento, en caso de que se haya modificado se verificará lo siguiente: Que el documento contenga la información señalada en la presente regla.
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.	Que el documento contenga la información señalada en la presente regla.
152. Contar con un calendario de revisión y actualización del documento de Sistema de Gestión de Seguridad de la Información.	Que el documento contenga la información señalada en la presente regla.
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	Última versión del documento, en caso de que se haya modificado se verificará lo siguiente: Que el documento contenga la información señalada en la presente regla.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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.	Que el documento contenga la información señalada en la presente regla.
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:	
Última versión del documento, en caso de que se haya modificado se verificará lo siguiente:	
I. Afectación al funcionamiento de los sistemas y/o software;	Que el documento contenga la información señalada en la presente fracción.
II. Incidente de seguridad que afecte la operación de los sistemas y/o software;	Que el documento contenga la información señalada en la presente fracción.
III. Falla en el hardware donde se ejecuta el producto;	Que el documento contenga la información señalada en la presente fracción.
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;	Que el documento contenga la información señalada en la presente fracción.
V. Falla de los mecanismos de auditoría;	Que el documento contenga la información señalada en la presente fracción.
VI. Mecanismos para preservar evidencia del mal uso de los sistemas, y	Que el documento contenga la información señalada en la presente fracción.
VII. Demás casos imprevistos en las presentes Reglas y que por su naturaleza pongan en riesgo el servicio acreditado.	Que el documento contenga la información señalada en la presente fracción.
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	Que el documento contenga la información señalada en la presente regla.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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.	Que el documento contenga la información señalada en la presente regla.
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:	
Última versión del documento, en caso de que se haya modificado se verificará lo siguiente:	
I. Cuáles son los servicios prestados;	Que el documento contenga la información señalada en la presente fracción.
II. Cómo se interrelacionan los diferentes servicios;	Que el documento contenga la información señalada en la presente fracción.
III. En qué lugares se operará;	Que el documento contenga la información señalada en la presente fracción.
IV. Cómo se protegerán los activos;	Que el documento contenga la información señalada en la presente fracción.
V. Implementación de elementos de seguridad;	Que el documento contenga la información señalada en la presente fracción.
VI. Procesos de administración;	Que el documento contenga la información señalada en la presente fracción.
VII. Sistema de directorios para la constancia de conservación de mensaje de datos;	Que el documento contenga la información señalada en la presente fracción.
VIII. Procesos de auditoría y respaldo, y	Que el documento contenga la información señalada en la presente fracción.
IX. Bases de datos a utilizar.	Que el documento contenga la información señalada en la presente fracción.
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.	Que el documento contenga la información señalada en la presente regla.
160. Contar con un calendario de revisión y actualización del documento de Modelo	Que el documento contenga la información señalada en la presente regla.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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:	
Última versión del documento, en caso de que se haya modificado se verificará 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	Que el documento contenga la información señalada en la presente fracción.
II. Indicar a quién se le puede otorgar una Constancia de Conservación de Mensaje de Datos.	Que el documento contenga la información señalada en la presente fracción.
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.	Que el documento contenga la información señalada en la presente regla.
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:	
Última versión del documento, en caso de que se haya modificado se verificará lo siguiente:	
I. Los procedimientos de operación para otorgar la constancia de conservación de mensaje de datos y el alcance de aplicación de los mismos;	Que el documento contenga la información señalada en la presente fracción.
II. Las responsabilidades y obligaciones del Prestador de Servicios de Certificación y de sus usuarios;	Que el documento contenga la información señalada en la presente fracción.
III. Las medidas de seguridad adoptadas para proteger sus Datos de Creación de Firma Electrónica para la Constancia de Conservación de Mensaje de Datos;	Que el documento contenga la información señalada en la presente fracción.
IV. Los controles que se utilizarán para asegurar las auditorías y almacenamiento de información relevante;	Que el documento contenga la información señalada en la presente fracción.
V. Una vez otorgada la acreditación por la Secretaría, la fecha de inicio de operaciones, y	Que el documento contenga la información señalada en la presente fracción.
VI. La Declaración de Prácticas de Constancias de Conservación de Mensaje de Datos emitidas de	Que el documento contenga la información señalada en la presente fracción.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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.	Que el documento contenga la información señalada en la presente regla.
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:	
Última versión del documento, en caso de que se haya modificado se verificará lo siguiente:	
I. Claves de la Autoridad de Constancias de Conservación de Mensaje de Datos emitidas de conformidad con la NOM-151- SCFI-2016;	Que el documento contenga la información señalada en la presente fracción.
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;	Que el documento contenga la información señalada en la presente fracción.
III. Distribución del Certificado de la Autoridad de Constancias de Conservación de Mensaje de Datos emitidas de conformidad con la NOM-151-SCFI-2016;	Que el documento contenga la información señalada en la presente fracción.
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;	Que el documento contenga la información señalada en la presente fracción.
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;	Que el documento contenga la información señalada en la presente fracción.
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;	Que el documento contenga la información señalada en la presente fracción.
VII. La Autoridad de Constancias de Conservación de Mensaje de Datos	Que el documento contenga la información señalada en la presente fracción.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

emitidas de conformidad con la NOM-151-SCFI2016 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.	Que el documento contenga la información señalada en la presente fracción.
166. Contar con un calendario de revisión y actualización del documento de Plan de Administración de Claves.	Que el documento contenga la información señalada en la presente regla.
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.	Evidencia del sitio electrónico, en donde se verifique que se pueden consultar lo señalado en la presente regla.

VIII.2.4 Título Octavo De la Digitalización de Documentos en Soporte Físico de conformidad con la NOM151-SCFI-2016.	
REQUISITOS.	
Fundamento.	**Elementos para acreditar el cumplimiento.**
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	Presentar el documento que compruebe la subsistencia del objeto social señalado en la presente regla.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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. 49 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.	Documentos que acrediten que el PSC verificó que la digitalizadora cumpliera con los requisitos señalados en esta regla, y/o visita de verificación.
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.	Presentar actas circunstanciadas de la ceremonia de cotejo.
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	Documentos que acrediten que cuenta con el/los equipos y estándares señalados en esta fracción, y/o visita de verificación.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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;	Última versión del documento donde se definieron las medidas se seguridad adoptadas, en caso de que se haya modificado se verificará lo siguiente: Que el documento contenga la información señalada en la presente fracción.
III. Contar con un Plan de Administración de Claves de acuerdo a lo dispuesto en el presente CAPÍTULO, y	Última versión del documento autorizado.
IV. Desarrollar un procedimiento en caso de robo de los Datos de Creación de Firma Electrónica del Certificado del Tercero Legalmente Autorizado	Última versión del documento donde se desarrolló el procedimiento en caso de robo de los Datos de Creación de Firma Electrónica del Certificado del Tercero Legalmente Autorizado, en el supuesto de que se haya modificado se verificará que el documento contenga la información señalada en la presente fracción.
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.	Última versión del documento donde se definió el proceso de digitalización señalado en la presente fracción y visita de verificación.
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.	Contratos suscritos y relación de procesos realizados.
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.	Última versión de los documentos señalados en el presente artículo autorizados.
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	Contratos suscritos entre el PSC y los comerciantes.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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.	Última versión de los documentos autorizados.
ELEMENTOS HUMANOS.[15]	
Presentar la lista de los últimos elementos humanos con los que cuenta actualmente, los cuales deberán coincidir con los previamente autorizados por la DGNM, en caso de que se detecte que alguno de los elementos no coincide con los ya autorizados o que se deba actualizar alguno de los requisitos, se deberá presentar lo siguiente:	
Fundamento.	**Elementos para acreditar el cumplimiento.**
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;	Título profesional expedido por la Secretaría de Educación Pública y cédula profesional expedida 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;	Documentos que acrediten la experiencia señalada en la presente fracción, los siguientes ejemplos se señalan de manera enunciativa mas no limitativa: • Curriculum Vitae firmado autógrafamente, bajo protesta de decir verdad, en el cual deberán detallar las actividades que realizó o realiza en el área de correduría pública, derecho notarial o derecho mercantil. • Constancia laboral para acreditar el periodo y las actividades que realizó o realiza en el área de correduría pública, derecho notarial o derecho mercantil.
III. Acreditar al menos un año de experiencia en derecho informático, y	Documentos que acrediten la experiencia señalada en la presente fracción, los siguientes ejemplos se señalan de manera enunciativa mas no limitativa: • Curriculum Vitae firmado autógrafamente, bajo protesta de decir verdad, en el cual deberán detallar las actividades que realizó o realiza en el área de derecho informático. • Constancia laboral para acreditar el periodo y las actividades que realizó o realiza en el área de derecho informático.
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	Escrito libre firmado autógrafamente, mediante el cual declara 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, actualizado.

[15] Los Elementos Humanos se refieren de forma general en el artículo 5, fracción III, inciso a), del Reglamento del Código de Comercio en materia de Prestadores de Servicios de Certificación.

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;	Título profesional expedido por la Secretaría de Educación Pública y cédula profesional expedida por la Secretaría de Educación Pública o su equivalente.
II. Comprobar al menos dos años de experiencia en el área de seguridad informática, y	Documentos que acrediten la experiencia señalada en la presente fracción, los siguientes ejemplos se señalan de manera enunciativa mas no limitativa: • Curriculum Vitae firmado autógrafamente, bajo protesta de decir verdad, en el cual deberán detallar las actividades que realizó o realiza en el área de seguridad informática de cuando menos dos años, según sea el caso. • Constancia laboral para acreditar el periodo y las actividades que realizó o realiza en el área de seguridad informática, de cuando menos dos años.
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.	Documentos que acrediten la experiencia señalada en la presente fracción, el siguiente ejemplo se señala de manera enunciativa mas no limitativa: • Certificaciones y/o título de especialidad y/o título de maestría que acredite estudios en seguridad informática.
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;	Título profesional expedido por la Secretaría de Educación Pública y cédula profesional expedida por la Secretaría de Educación Pública o su equivalente.
II. Comprobar al menos dos años de experiencia en el área de seguridad informática;	Documentos que acrediten la experiencia señalada en la presente fracción, los siguientes ejemplos se señalan de manera enunciativa mas no limitativa: • Curriculum Vitae firmado autógrafamente, bajo protesta de decir verdad, en el cual deberán detallar las actividades que realizó o realiza en el área de seguridad informática de cuando menos dos años, según sea el caso. • Constancia laboral para acreditar el periodo y las actividades que realizó o realiza en el área de seguridad informática, de cuando menos dos años.
III. Acreditar estudios en manejo de software o hardware relacionados con seguridad informática;	Documentos que acrediten que cuenta con estudios en manejo de software o hardware relacionados con criptografía como pueden ser: certificaciones y/o título de especialidad y/o título de maestría que acredite estudios en manejo de software o hardware relacionados con seguridad informática.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

IV. Contar con conocimientos comprobados de procesos de digitalización, y	Curriculum Vitae firmado autógrafamente, bajo protesta de decir verdad, en el cual deberán detallar las actividades que realizó o realiza en procesos de digitalización y constancia laboral para acreditar el periodo y las actividades que realizó en procesos de digitalización y/o certificaciones y/o título de especialidad y/o título de maestría que acredite conocimientos comprobados de procesos de digitalización.
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.	Escrito libre firmado autógrafamente, mediante el cual declara 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, actualizado.
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;	Última versión del documento donde se definan las obligaciones, funciones y responsabilidades señaladas en la presente fracción, en el supuesto de que se haya modificado se verificará que el documento contenga la información señalada en la presente fracción.
II. Supervisar las actividades de cotejo a que se refiere el artículo 95 bis 4 del Código de Comercio, y	Última versión del documento donde se definan las obligaciones, funciones y responsabilidades señaladas en la presente fracción, en el supuesto de que se haya modificado se verificará que el documento contenga la información señalada en la presente fracción.
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.	Última versión del documento donde se definan las obligaciones, funciones y responsabilidades señaladas en la presente fracción, en el supuesto de que se haya modificado se verificará que el documento contenga la información señalada en la presente fracción.
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	Última versión del documento donde se definan las obligaciones, funciones y responsabilidades señaladas en la presente fracción, en el supuesto de que se haya modificado se verificará que el documento contenga la información señalada en la presente fracción.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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;	Última versión del documento donde se definan las obligaciones, funciones y responsabilidades señaladas en la presente fracción, en el supuesto de que se haya modificado se verificará que el documento contenga la información señalada en la presente fracción.
III. Supervisar el personal que lleva a cabo procesos de Digitalización de Documentos en Soporte Físico;	Última versión del documento donde se definan las obligaciones, funciones y responsabilidades señaladas en la presente fracción, en el supuesto de que se haya modificado se verificará que el documento contenga la información señalada en la presente fracción.
IV. Establecer el flujo de trabajo para el proceso de Digitalización de Documentos en Soporte Físico y asegurar su cumplimiento;	Última versión del documento donde se definan las obligaciones, funciones y responsabilidades señaladas en la presente fracción, en el supuesto de que se haya modificado se verificará que el documento contenga la información señalada en la presente fracción.
V. Acordar el formato de la imagen con el comerciante;	Última versión del documento donde se definan las obligaciones, funciones y responsabilidades señaladas en la presente fracción, en el supuesto de que se haya modificado se verificará que el documento contenga la información señalada en la presente fracción.
VI. Seleccionar el hardware de digitalización y asegurar su cumplimiento.	Última versión del documento donde se definan las obligaciones, funciones y responsabilidades señaladas en la presente fracción, en el supuesto de que se haya modificado se verificará que el documento contenga la información señalada en la presente fracción.
VII. Estar presente en las actividades de cotejo a que se refiere el artículo 95 bis 4 del Código de Comercio;	Última versión del documento donde se definan las obligaciones, funciones y responsabilidades señaladas en la presente fracción, en el supuesto de que se haya modificado se verificará que el documento contenga la información señalada en la presente fracción.
VIII. Asegurar que el proceso de Digitalización de Documentos en Soporte Físico incluye la Conservación de Mensaje de Datos resultante del proceso, y	Última versión del documento donde se definan las obligaciones, funciones y responsabilidades señaladas en la presente fracción, en el supuesto de que se haya modificado se verificará que el documento contenga la información señalada en la presente fracción.
IX. Supervisar pruebas de monitoreo.	Última versión del documento donde se definan las obligaciones, funciones y responsabilidades señaladas en la presente fracción, en el supuesto de que se haya modificado se verificará que el documento contenga la información señalada en la presente fracción.
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;	Última versión del documento donde se definan las obligaciones, funciones y responsabilidades señaladas en la presente fracción, en el supuesto de que se haya modificado se verificará que el documento contenga la información señalada en la presente fracción.
II. Llevar a cabo la ejecución de los procesos de Digitalización de	Última versión del documento donde se definan las obligaciones, funciones y responsabilidades señaladas en la presente fracción, en el

Documentos en Soporte Físico, validar la calidad de las imágenes durante dicho proceso conforme a la fracción anterior y las pruebas de configuraciones;	supuesto de que se haya modificado se verificará que el documento contenga la información señalada en la presente fracción.
III. Determinar los requisitos de mejora de la imagen y/o grabaciones en audio o video;	Última versión del documento donde se definan las obligaciones, funciones y responsabilidades señaladas en la presente fracción, en el supuesto de que se haya modificado se verificará que el documento contenga la información señalada en la presente fracción.
IV. Monitorear y asegurar la correcta indexación y la calidad de las imágenes y sus metadatos;	Última versión del documento donde se definan las obligaciones, funciones y responsabilidades señaladas en la presente fracción, en el supuesto de que se haya modificado se verificará que el documento contenga la información señalada en la presente fracción.
V. Llevar el control y reportes del proceso;	Última versión del documento donde se definan las obligaciones, funciones y responsabilidades señaladas en la presente fracción, en el supuesto de que se haya modificado se verificará que el documento contenga la información señalada en la presente fracción.
VI. Agregar los metadatos al mensaje de datos, y	Última versión del documento donde se definan las obligaciones, funciones y responsabilidades señaladas en la presente fracción, en el supuesto de que se haya modificado se verificará que el documento contenga la información señalada en la presente fracción.
VII. Comprobar la calidad de los mensajes de datos a la entrega de los archivos digitales y físicos.	Última versión del documento donde se definan las obligaciones, funciones y responsabilidades señaladas en la presente fracción, en el supuesto de que se haya modificado se verificará que el documento contenga la información señalada en la presente fracción.
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.	Presentar la lista de los últimos elementos humanos con los que cuenta actualmente, los cuales deberán coincidir con los previamente autorizados por la DGNM, de acuerdo a la presente regla.
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.	Documento que se utiliza para reclutar, seleccionar, evaluar y contratar al personal, para verificar si han llevado a cabo las revisiones establecidas y en su caso si se ha modificado.
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.	Contratos de confidencialidad debidamente suscritos por las partes, los cuales deberán extenderse cuando menos un año posterior a la conclusión laboral del empleado o de servicios en caso de una empresa externa.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

ELEMENTOS ECONÓMICOS.[16]	
Fundamento.	**Elementos para acreditar el cumplimiento.**
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.	Documentos que acrediten que cuenta con capital que comprende al menos el equivalente a una cuarta parte de la inversión requerida. Se señalan de manera enunciativa mas no limitativa los siguientes: • Estados financieros • Desglose de la inversión realizada. En caso de personas morales de carácter privado, además se deberán presentar los documentos que acrediten el capital social actual de la empresa. Presentar el Seguro de responsabilidad civil para corroborar que esté vigente y que corresponde al presentado.
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	Póliza de fianza para corroborar que está vigente y que corresponde a la presentada.

[16] Los Elementos Económicos se refieren de forma general en el artículo 5, fracción III, inciso c), del Reglamento del Código de Comercio en materia de Prestadores de Servicios de Certificación.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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.	
ELEMENTOS MATERIALES.[17]	
Fundamento.	**Elementos para acreditar el cumplimiento.**
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:	
Los controles de acceso físico y bitácoras que tengan tanto en sus Oficinas administrativas como en sus Centros de Datos. En la visita de verificación, la revisión de los elementos de seguridad con los que cuentan en los espacios físicos, mismos que deberán coincidir con las Políticas aprobadas por la DGNM.	
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;	Los controles de acceso físico y bitácoras para las áreas seguras donde se maneja documentación que contenga información confidencial. En la visita de verificación, la revisión de los controles de acceso a las áreas seguras donde se maneja documentación que contenga información confidencial concerniente al servicio de digitalización de documentos en soporte físico.
II. La implementación de los controles deberá evitar riesgo, daño, pérdida, alteración o sustracción de la documentación que contenga información confidencial;	En la visita de verificación, la revisión de los elementos de seguridad con los que cuentan en los espacios físicos, mismos que deberán coincidir con las Políticas aprobadas por la DGNM.
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;	Los controles de acceso físico y bitácoras que tengan para las áreas seguras en donde se resguarda la información concerniente al servicio de digitalización de documentos en soporte físico. En la visita de verificación, la revisión de los elementos de seguridad con los que cuentan en su espacio físico en donde se resguarda la información concerniente al servicio de digitalización de documentos en soporte físico, mismos que deberán coincidir con las Políticas aprobadas por la DGNM.

[17] Los Elementos Materiales se refieren de forma general en el artículo 5, fracción III, inciso b), del Reglamento del Código de Comercio en materia de Prestadores de Servicios de Certificación.

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;	Procedimientos para la recepción de insumos y la salida de basura que contengan detalladamente las medidas implementadas para dar cumplimiento a la presente fracción y/o visita de verificación donde se corroboren las medidas implementadas.
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;	En la visita de verificación, la revisión de los accesos físicos controlados con los que cuentan en su espacio físico, mismos que deberán coincidir con las Políticas de digitalización de documentos en soporte físico y/o Modelos Operacionales y/o Plan de Seguridad de Sistemas y/o Declaración de Prácticas de digitalización de documentos en soporte físico aprobados por la DGNM.
VI. Los requerimientos de seguridad para las áreas de atención a clientes se determinarán a partir del Análisis y Evaluación de Riesgos y Amenazas;	En la visita de verificación, la revisión de los requerimientos de seguridad que deberán coincidir con el 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;	Documentos que acrediten que cuenta con la política señalada en esta fracción, y/o visita de verificación.
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	En la visita de verificación, la revisión de la infraestructura de computación y comunicaciones instaladas, así como los contratos de mantenimiento preventivo y correctivo y las bitácoras de mantenimiento. Documentación que acredite que cuenta con el personal especializado o en su caso, los contratos de mantenimiento preventivo y correctivo para garantizar la continua disponibilidad e integridad de los sistemas.
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.	En la visita de verificación, la revisión de la infraestructura de computación y comunicaciones instaladas, así como los contratos de mantenimiento preventivo y correctivo y las bitácoras de mantenimiento Documentación que acredite que cuenta con el personal especializado o en su caso, los contratos de mantenimiento preventivo y correctivo para garantizar la continua disponibilidad e integridad de los sistemas.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

190. El personal contratado deberá conocer y entender los procedimientos y prácticas de seguridad dentro del perímetro de seguridad.	Documentos que acrediten que el personal contratado conoce y entiende los procedimientos y prácticas de seguridad dentro del perímetro de seguridad y/o visita de verificación.
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.	La última bitácora de acceso del personal de soporte a las áreas restringidas y procedimiento de acceso autorizado por el Profesional Informático o el Auxiliar de Apoyo Informático de Seguridad.
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.	Verificación de que únicamente el personal autorizado del PSC pueda ingresar y administrar los equipos de la autoridad certificadora y de la autoridad registradora.
ELEMENTOS TECNOLÓGICOS.[18]	
Presentar el inventario de los elementos tecnológicos con los que cuenta actualmente, los cuales deberán coincidir con los previamente autorizados por la DGNM, en caso de que se detecte que alguno de los elementos no coincide con los ya autorizados o que se deba actualizar alguno de los requisitos, se deberá presentar lo siguiente:	
Fundamento.	**Elementos para acreditar el cumplimiento.**
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;	Documentos que acrediten que cuenta con el/los equipos señalados en esta fracción, y/o visita de verificación.
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;	Documentos que acrediten que cuenta con el/los equipos señalados en esta fracción, y/o visita de verificación.
III. Contar con un dispositivo de alta seguridad, que cumpla con estándares de seguridad nacional o	Documentos que acrediten que cuenta con el/los equipos y estándares señalados en esta fracción, y/o visita de verificación.

[18] Los Elementos Tecnológicos se refieren de forma general en el artículo 5, fracción III, inciso d), del Reglamento del Código de Comercio en materia de Prestadores de Servicios de Certificación.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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;	Documentos que acrediten que cuenta con el enlace señalado en esta fracción, y/o visita de verificación.
V. Un ruteador;	Documentos que acrediten que cuenta con el/los equipos señalados en esta fracción, y/o visita de verificación.
VI. Un muro de fuego (firewall);	Documentos que acrediten que cuenta con el/los elementos señalados en esta fracción, y/o visita de verificación.
VII. Una computadora para gestionar el o los sistemas de administración;	Documentos que acrediten que cuenta con el/los equipos señalados en esta fracción, y/o visita de verificación.
VIII. Un sistema de monitoreo de red;	Documentos que acrediten que cuenta con el licenciamiento actualizado del elemento señalado en esta fracción, y/o visita de verificación.
IX. Un sistema confiable de antivirus;	Documentos que acrediten que cuenta con el licenciamiento actualizado del elemento señalado en esta fracción, y/o visita de verificación.
X. Herramientas confiables de detección de vulnerabilidades;	Documentos que acrediten que cuenta con el licenciamiento actualizado del elemento señalado en esta fracción, y/o visita de verificación.
XI. Sistemas confiables de detección y protección de intrusión;	Documentos que acrediten que cuenta con el licenciamiento actualizado del elemento señalado en esta fracción, y/o visita de verificación.
XII. Equipo de alta capacidad de almacenamiento;	Documentos que acrediten que cuenta con el/los equipos señalados en esta fracción, y/o visita de verificación.
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	Documentos que acrediten que cuenta con los canales seguros de comunicación señalados en esta fracción, y/o visita de verificación.
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	Presentar la guía de virtualización de los elementos tecnológicos virtualizados.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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;	Documentos que acrediten que cuenta con el/los equipos (servidores y HSM) señalados en esta fracción, y/o visita de verificación.
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;	Documentos que acrediten que cuenta con el/los equipos señalados en esta fracción, y/o visita de verificación.
III. Los procesos de administración de la Infraestructura Informática;	Documentos que acrediten que cuenta con el/los procesos de administración señalados en esta fracción, y/o visita de verificación.
IV. Una Política de Digitalización de Documentos en Soporte Físico;	Aplica lo requerido en las Reglas 210 y 211.
V. Una Declaración de Prácticas de Digitalización de Documentos en Soporte Físico;	Aplica lo requerido en las Reglas 212 y 213.
VI. Los manuales de operación de la Autoridad de Digitalización de Documentos en Soporte Físico, y	Aplica lo requerido en la Regla 209.
VII. La Infraestructura Informática, señalada en la Regla 194 fracción I y II, deberá considerar redundancia por seguridad.	Documentos que acrediten que cuenta con la redundancia de los elementos descritos en la Regla 194, fracciones I y II, y/o visita de verificación.
195. Contar con un documento de Análisis y Evaluación de Riesgos y Amenazas que deberá detallar por lo menos los siguientes elementos:	
Última versión del documento, en caso de que se haya modificado se verificará lo siguiente:	
I. Los activos críticos;	Que el documento contenga la información señalada en la presente fracción.
II. Identificar sus requerimientos de seguridad;	Que el documento contenga la información señalada en la presente fracción.
III. Vulnerabilidades y amenazas de la infraestructura con la que proveerá el o los servicios y determinar los requerimientos de seguridad;	Que el documento contenga la información señalada en la presente fracción.
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;	Que el documento contenga la información señalada en la presente fracción.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

V. Medidas de seguridad para la mitigación de los riesgos detectados;	Que el documento contenga la información señalada en la presente fracción.
VI. Proceso de evaluación continua, para adecuar la valoración de riesgos a condiciones cambiantes del entorno;	Que el documento contenga la información señalada en la presente fracción.
VII. Los impactos que sufrirán los servicios del Prestador de Servicios de Certificación, en caso de interrupciones no planificadas, y	Que el documento contenga la información señalada en la presente fracción.
VIII. Adoptar Guide for Conducting Risk Assessments. NIST Special Publication 800-30 Revision 1. September 2012, equivalente o el que le sustituya.	Que el documento contenga la información señalada en la presente fracción.
196. Contar con un calendario de revisión y actualización del documento de Análisis y Evaluación de Riesgos y Amenazas.	Que el documento contenga la información señalada en la presente regla.
197. Contar con un documento de Política de Seguridad de la Información que deberá detallar por lo menos los siguientes elementos:	
Última versión del documento, en caso de que se haya modificado se verificará lo siguiente:	
I. Ser congruente con el objeto del servicio de Digitalización de Documentos en Soporte Físico;	Que el documento contenga la información señalada en la presente fracción.
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;	Que el documento contenga la información señalada en la presente fracción.
III. Estar basada en las recomendaciones de los estándares ISO/IEC serie 27000, o los que le sustituyan;	Que el documento contenga la información señalada en la presente fracción.
IV. La Política de Seguridad de la información, puede estar conformada con una política general y soportada con políticas específicas;	Que el documento contenga la información señalada en la presente fracción.
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;	Que el documento contenga la información señalada en la presente fracción.
VI. Describir las reglas que indiquen cómo son provistos los servicios y las medidas de seguridad asociadas;	Que el documento contenga la información señalada en la presente fracción.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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;	Que el documento contenga la información señalada en la presente fracción.
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	Que el documento contenga la información señalada en la presente fracción.
IX. Desarrollar procedimientos y buenas prácticas para apoyar las políticas de seguridad	Que el documento contenga la información señalada en la presente fracción.
198. Contar con un calendario de revisión y actualización del documento de Política de Seguridad de la Información.	Que el documento contenga la información señalada en la presente regla.
199. Contar con un documento de Política de Seguridad Física que deberá detallar por lo menos los siguientes elementos:	
Última versión del documento, en caso de que se haya modificado se verificará lo siguiente:	
I. Control de acceso físico;	Que el documento contenga la información señalada en la presente fracción.
II. Protección y recuperación ante desastres;	Que el documento contenga la información señalada en la presente fracción.
III. Protecciones contra robo, forzamiento y entrada no autorizada a los espacios físicos;	Que el documento contenga la información señalada en la presente fracción.
IV. Medidas de protección en caso de incendio, contra fallas de servicios eléctricos o de telecomunicaciones, y	Que el documento contenga la información señalada en la presente fracción.
V. Un procedimiento de actualización para autorización de acceso al personal a las áreas restringidas.	Que el documento contenga la información señalada en la presente fracción.
200. Contar con un calendario de revisión y actualización del documento de Política de Seguridad Física.	Que el documento contenga la información señalada en la presente regla.
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.	Última versión del documento, en caso de que se haya modificado se verificará el contenido.
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	Que el documento contenga la información señalada en la presente regla.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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.	Que el documento contenga la información señalada en la presente regla.
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.	Última versión del documento, en caso de que se haya modificado se verificará lo siguiente: Que el documento contenga la información señalada en la presente regla.
205. Contar con un calendario de revisión y actualización del documento de Plan de Seguridad de Sistemas.	Que el documento contenga la información señalada en la presente regla.
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:	
Última versión del documento, en caso de que se haya modificado se verificará lo siguiente:	
I. Afectación al funcionamiento del software y/o sistema;	Que el documento contenga la información señalada en la presente fracción.
II. Incidente de seguridad que afecte la operación del software y/o sistema;	Que el documento contenga la información señalada en la presente fracción.
III. Falla en el hardware donde se ejecuta el producto en el que se basarán los servicios;	Que el documento contenga la información señalada en la presente fracción.
IV. Robo de los Datos de Creación de Firma Electrónica Avanzada del Certificado de Digitalización de Documentos en Soporte Físico del	Que el documento contenga la información señalada en la presente fracción.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

Prestador de Servicios de Certificación;	
V. Falla de los mecanismos de auditoría;	Que el documento contenga la información señalada en la presente fracción.
VI. Mecanismos para preservar evidencia del mal uso de los sistemas, y	Que el documento contenga la información señalada en la presente fracción.
VII. Demás casos imprevistos en las presentes Reglas y que por su naturaleza pongan en riesgo el servicio acreditado.	Que el documento contenga la información señalada en la presente fracción.
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.	Que el documento contenga la información señalada en la presente regla.
208. Contar con un calendario de revisión y actualización del documento de Plan de Continuidad del Negocio y Recuperación ante Desastres.	Que el documento contenga la información señalada en la presente regla.
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:	
Última versión del documento, en caso de que se haya modificado se verificará lo siguiente:	
I. Los procesos de Digitalización de Documentos en Soporte Físico a fin de describirlos conceptual y gráficamente para su posterior aplicación;	Que el documento contenga la información señalada en la presente fracción.
II. Restauración del documento en soporte físico, deberá definir las actividades que desarrollará para llevar a cabo en su caso, la	Que el documento contenga la información señalada en la presente fracción.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

restauración de la documentación en soporte físico, de conformidad con lo establecido en la NOM-151-SCFI2016;	
III. El proceso de recepción y resguardo para la protección de la documentación en soporte físico;	Que el documento contenga la información señalada en la presente fracción.
IV. Mecanismos mínimos para la recepción de la documentación en soporte físico;	Que el documento contenga la información señalada en la presente fracción.
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-SCFI2016;	Que el documento contenga la información señalada en la presente fracción.
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	Que el documento contenga la información señalada en la presente fracción.
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.	Que el documento contenga la información señalada en la presente fracción.
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:	
Última versión del documento, en caso de que se haya modificado se verificará lo siguiente:	
I. Asegurar su concordancia con la Declaración de Prácticas de Digitalización de Documentos en Soporte Físico y, los procedimientos operacionales;	Que el documento contenga la información señalada en la presente fracción.
II. Describir los objetivos y alcances de la digitalización de documentos en soporte físico y, sus limitaciones,	Que el documento contenga la información señalada en la presente fracción.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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.	Que el documento contenga la información señalada en la presente fracción.
211. Contar con un calendario de revisión y actualización de la Política de Digitalización de Documentos en Soporte Físico.	Que el documento contenga la información señalada en la presente regla.
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:	
Última versión del documento, en caso de que se haya modificado se verificará lo siguiente:	
I. Los procedimientos de operación de la digitalización de documentos en soporte físico y el alcance de aplicación de la misma;	Que el documento contenga la información señalada en la presente fracción.
II. Las responsabilidades y obligaciones del Prestador de Servicios de Certificación y la de sus usuarios;	Que el documento contenga la información señalada en la presente fracción.
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;	Que el documento contenga la información señalada en la presente fracción.
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;	Que el documento contenga la información señalada en la presente fracción.
V. Las medidas de seguridad adoptadas para proteger sus Datos de Creación de Firma Electrónica del Prestador de Servicios de Certificación;	Que el documento contenga la información señalada en la presente fracción.
VI. Los controles que se utilizarán para asegurar las auditorías y almacenamiento de información relevante;	Que el documento contenga la información señalada en la presente fracción.
VII. Una vez otorgada la acreditación al Prestador de Servicios de Certificación por la	Que el documento contenga la información señalada en la presente fracción.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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.	Que el documento contenga la información señalada en la presente fracción.
213. Contar con un calendario de revisión y actualización de la Declaración de Prácticas de Digitalización de Documentos en Soporte Físico.	Que el documento contenga la información señalada en la presente regla.
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:	
Última versión del documento, en caso de que se haya modificado se verificará lo siguiente:	
I. Las claves privadas de la Autoridad Digitalizadora de Documentos en Soporte Físico;	Que el documento contenga la información señalada en la presente fracción.
II. Almacenamiento, respaldo, recuperación y uso de las claves privadas;	Que el documento contenga la información señalada en la presente fracción.
III. Distribución del Certificado de la Autoridad Digitalizadora de Documentos en Soporte Físico;	Que el documento contenga la información señalada en la presente fracción.
IV. Administración del ciclo de vida del hardware criptográfico de la Autoridad Digitalizadora de Documentos en Soporte Físico;	Que el documento contenga la información señalada en la presente fracción.
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;	Que el documento contenga la información señalada en la presente fracción.
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	Que el documento contenga la información señalada en la presente fracción.
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.	Que el documento contenga la información señalada en la presente fracción.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

215. Contar con un calendario de revisión y actualización del Plan de Administración de Claves.	Que el documento contenga la información señalada en la presente regla.
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.	Última versión del documento, en caso de que se haya modificado se verificará lo señalado en la presente regla.
217. Contar con un calendario de revisión y actualización del Plan Gestión de Calidad.	Última versión del documento, en caso de que se haya modificado se verificará lo señalado en la presente regla.
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:	
Se verificará en la visita de verificación que se cuente con la base de datos/software/sistema de digitalización acreditados	
I. Aplicar un mecanismo de validación de la vigencia de los certificados digitales de firma electrónica avanzada utilizados en el proceso de digitalización;	Se solicitará en la visita de verificación que se realicen uno o más ejercicios de validación de la vigencia de los certificados digitales de firma electrónica avanzada.
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;	Se solicitará en la visita de verificación una demostración del proceso de digitalización en donde se pruebe lo señalado en la presente regla.
III. Asegurar que el mensaje de datos obtenido cumpla con el	Presentar el contrato celebrado con el cliente donde se identifique el formato del mensaje de datos obtenido.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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;	Se solicitará en la visita de verificación una demostración del proceso de digitalización en donde se pruebe lo señalado en la presente fracción.
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;	Se solicitará en la visita de verificación una demostración del proceso de digitalización en donde se pruebe lo señalado en la presente fracción.
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;	Se solicitará en la visita de verificación una demostración del proceso de digitalización en donde se pruebe lo señalado en la presente fracción.
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	Se solicitará en la visita de verificación una demostración del proceso de digitalización en donde se pruebe lo señalado en la presente fracción.
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.	Se solicitará en la visita de verificación una demostración del proceso de digitalización en donde se pruebe lo señalado en la presente fracción.
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.	Se solicitará en la visita de verificación una demostración del proceso de digitalización en donde se pruebe lo señalado en la presente regla.
220. Definir las medidas de seguridad a fin de que permitan proteger el contenido en la memoria RAM del servidor donde	Última versión del documento, donde se definen las medidas de seguridad en caso de que se haya modificado se verificará que cuenta con lo señalado en el presente numeral, y/o visita de verificación.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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.	Evidencia del sitio electrónico, en donde se verifique que se pueden consultar lo señalado en la presente regla.
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.	Presentar el resultado de los análisis realizados antes de cualquier proceso de digitalización que cumpla con lo señalado en la presente regla.
PROCEDIMIENTO DE DIGITALIZACIÓN DE DOCUMENTOS EN SOPORTE FÍSICO.	
Fundamento.	**Elementos para acreditar el cumplimiento.**
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;	Se solicitará en la visita de verificación una demostración del proceso de digitalización en donde se pruebe lo señalado en la presente fracción.
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	Se solicitará en la visita de verificación una demostración del proceso de digitalización en donde se pruebe lo señalado en la presente fracción.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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.	Se solicitará en la visita de verificación una demostración del proceso de digitalización en donde se pruebe lo señalado en la presente fracción.
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.	Se solicitará en la visita de verificación una demostración del proceso de digitalización en donde se pruebe lo señalado en la presente regla.
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.	Última versión de la Declaración de Practicas de Digitalización, donde se señale 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, en caso de que se haya modificado se verificará que cuenta con lo señalado en el presente numeral y visita de verificación.
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;	Procedimientos que contengan detalladamente los controles establecidos para dar cumplimiento a la presente fracción y visita de verificación donde se corrobore el método de control implementado.
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	Procedimientos que contengan detalladamente la forma de división de los documentos físicos y visita de verificación donde se corrobore el método implementado.
III. Determinación del tamaño de la muestra. El tamaño de una muestra, es el número de mensajes de datos que compone la muestra	Procedimientos que contengan detalladamente la forma de división de los documentos físicos y visita de verificación donde se corrobore el método implementado.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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:	

$$n = \frac{N S^2 Z\hat{I}\pm^2}{E^2(N-1) + S^2 Z\hat{I}\pm^2}$$, 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).
ZÎ±	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 ZÎ± 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;	Última versión del documento donde se haya determinado la técnica de muestreo que se utilizará, contrato con el cliente y visita de verificación.
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	Última versión del documento donde se haya determinado la técnica de muestreo que se utilizará, contrato con el cliente y visita de verificación.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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:	Última versión del documento donde se haya determinado la técnica de muestreo que se utilizará, contrato con el cliente y visita de verificación.

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**	**¼**
3	**Alta**	**1/2**

El solicitante podrá acordar otras fracciones conforme a sus necesidades.
El tamaño de la muestra de cada estrato (ni) se calcula como sigue:
ni = Ni * fracción, para i = 1, 2 y 3, donde Ni, 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	Última versión del documento donde se haya determinado la técnica de muestreo que se utilizará, contrato con el cliente y visita de verificación.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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.	Última versión del documento donde se haya determinado la técnica de muestreo que se utilizará, contrato con el cliente y visita de verificación.
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:	Reportes de cotejo de sus procesos de digitalización, donde se observe lo señalado en la siguiente relación.

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.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

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.	Última versión del documento donde se señale el proceso de notificación a la Secretaría de Economía, así como los reportes de cotejo de sus procesos de digitalización.
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.	Actas circunstanciadas de sus ceremonias de cotejo.
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.	Última versión del documento donde se haya definido el método para resguardar los metadatos resultantes del proceso de digitalización y visita de verificación.

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se

IX. Contacto.

En caso de cualquier duda o comentario se podrá contactar a los siguientes servidores públicos adscritos a la DGNM:

Nombre: Diana Muñoz Flor
Cargo: Coordinadora de Política Mercantil
Correo electrónico: diana.munoz@economia.gob.mx
Teléfono (55) 52296100, extensión 33537

Nombre: Omar Yael Arenas Luna
Cargo: Subdirector de Supervisión de Prestadores de Servicios de Certificación
Correo electrónico omar.arenas@economia.gob.mx
Teléfono (55) 52296100, extensión 33503

Fecha de última actualización: 30 de noviembre de 2023

Calle Pachuca #189, Col. Condesa, C.P. 06140
Cuauhtémoc, CDMX t: (55) 57 29 91 00 www.gob.mx/se