Declaración de Prácticas de Certificación
Autoridad Certificadora y Autoridad Registradora Cecoban

OID: 2.16.484.101.10.316.2.3.1.1.1.1.2

Versión 1.3

07/02/2017

Histórico de Cambios

Fecha	Versión	Descripción
07/02/2017	1.3	Se elimina del documento lo referente a la reexpedición en línea de certificados.
21/10/2015	1.2	Derivado de la auditoría de Manuales se revisa el documento y se concluye que no presenta cambios mayores en su contenido por lo que se conserva la versión
19/04/2013	1.2	Actualización del documento en función al cambio de domicilio de Cecoban y actual estructura organizacional.

Revisiones y Aprobaciones

Nombre / Rol	Fecha	Firma
Lic. Víctor Prieto Vélez **Director General**		
Lic. Jesús Ramírez Blancarte. **Profesional Jurídico**		
Ing. Joel Alejandro Núñez Hernández. **Profesional Informático**		
Lic. Ivonne Flores Acosta **Oficial de Seguridad**		
Mtro. Jonathan Gabriel Garzón Galván **Responsable de las Agencias AC-AR y NOM**		

CONTENIDO

1. INTRODUCCIÓN

Cecoban S.A de C.V. es una empresa constituida por instituciones de crédito que participan en la Cámara de Compensación Bancaria, dentro de los servicios se encuentran: Compensación Electrónica de Cheques, Compensación de Transferencias de Abonos, Compensación de Transferencias de Cargos (Domiciliación de Recibos), Intercambio de imágenes de cheques, y otros Servicios Complementarios, la infraestructura tecnológica con que se realizan los procesos tiene la capacidad de procesar operaciones en Moneda Nacional y Dólares Americanos.

Los Servicios que otorga Cecoban S.A. de C.V., incluyen el uso de firma electrónica. Para brindar mayor confianza a sus clientes, en marzo de 2004 Cecoban firmó con Banco de México los contratos que lo acreditan como Agencia Certificadora y Registradora dentro de la Infraestructura Extendida de Seguridad y en septiembre del 2008 fue acreditado por la Secretaría de Economía como Prestador de Servicios de Certificación Autorizado para operar los servicios de solicitud de Certificados Digitales a la AC y de constancias de Conservación de Mensajes de Datos de acuerdo a la NOM-151. Ya en 2011 Cecoban fue acreditado como Prestador de Servicios de Certificación por el Servicio de Administración Tributaria, agregando a su portafolio de servicios la generación y timbrado de comprobantes fiscales digitales (CFDI) o facturas electrónicas.

1.1 Objetivo

La presente Declaración de Prácticas de Certificación, tiene como objetivo dar a conocer en detalle, los procedimientos y condiciones inherentes a los servicios de certificación de certificados digitales.

1.2 Alcance

Esta declaración establece los términos, condiciones y procedimientos que rigen la prestación de los servicios de certificación (solicitud de CD a la AC, registro, publicación, administración, almacenamiento y revocación de los certificados digitales) de la Autoridad Certificadora Cecoban y su ámbito de aplicación se extiende a los Solicitantes, Titulares y a los terceros que Confían en los certificados emitidos por esta Autoridad.

2. DEFINICIONES Y ACRÓNIMOS

- **ACR-SE:** Autoridad Certificadora Raíz de la Secretaría de Economía
- **Acreditación de Identidad:** Dar certeza de que los rasgos propios del solicitante del Certificado Digital corresponden a los documentos que presenta para identificarlo.
- **Acreditación de Personalidad:** Garantizar que la representación legal de la persona moral está debidamente conferida a una persona física mediante la documentación necesaria.
- **Autoridad Certificadora Cecoban (AC Cecoban):** Es el Prestador de Servicios de Certificación (PSC) autorizado por la Secretaría de Economía para la expedición de Certificados Digitales.
- **Autoridad Registradora Cecoban (AR Cecoban):** Es la persona física o moral que autorizada por la AC Cecoban es la responsable de la acreditación de identidad y la personalidad de los Solicitantes de un Certificado Digital, por medio de los documentos de identificación de los Solicitantes y Titulares de un Certificado Digital, así como de realizar la solicitud de expedición o revocación de un Certificado Digital ante la AC Cecoban. Esta Autoridad podrá auxiliarse de las personas físicas que así considere conveniente para la óptima realización de sus funciones.
- **Certificado Digital: Es el documento electrónico (mensaje de datos**) generado y firmado electrónicamente por un Prestador de Servicios de Certificación el cual vincula un par de claves (pública y privada) con una persona determinada confirmando su identidad.
- **Clave de Anulación:** Datos proporcionados por el solicitante de un Certificado Digital en su requerimiento electrónico y empleado por él como Titular del Certificado Digital correspondiente para la revocación del mismo. Esta clave sólo la debe conocer el Titular del Certificado Digital y por tanto permite a la AC Cecoban proceder con una solicitud de revocación, vía el sitio de Internet.
- **Claves.** Claves criptográficas que pueden ser públicas o privadas.
- **Clave Privada:** Véase Datos de Creación de Firma Electrónica.
- **Clave Pública:** Véase Datos de Verificación de Firma Electrónica.
- **Comunidad:** Estará integrada por los Titulares, las Instituciones Solicitantes y los Terceros que Confían los cuales hacen uso de Certificados Digitales.
- **Datos de Creación de Firma Electrónica:** Son los datos únicos, como claves criptográficas privadas, que el Firmante genera de manera secreta y utiliza para crear su Firma Electrónica, a fin de lograr el vínculo entre dicha Firma Electrónica y el Firmante.
- **Datos de Verificación de Firma Electrónica:** Los datos como claves criptográficas públicas únicas que se utilizan para verificar la autenticidad de la firma electrónica del firmante.

- **Dependiente:** Aquellas personas físicas que desempeñen constantemente alguna o algunas gestiones propias del trafico u objeto de una persona moral, en nombre y por cuenta de ella, quienes deberán ser autorizadas para ser Titulares de Certificados Digitales de una Institución Solicitante por un Funcionario Facultado. Artículos 309 a 331 del Código de Comercio.

- **Dispositivo de Creación de Firma Electrónica:** Es el programa y equipo de cómputo que sirve para aplicar los Datos de Creación de Firma Electrónica a un Mensaje de Datos y generar la Firma Electrónica del referido Mensaje de Datos.

- **Dispositivo Generador de Datos de creación y verificación de firma electrónica (DGDFE):** Sistema de cómputo proporcionado por la AC Cecoban que permite al Solicitante generar bajo su exclusivo control sus Datos de Creación y Datos de Verificación de Firma Electrónica, estos últimos contenidos en un Requerimiento de Certificado digital.

- **Dispositivo de Verificación de Firma Electrónica:** Es el programa y equipo de cómputo que sirve para aplicar los Datos de Verificación de Firma Electrónica a la Firma Electrónica de un Mensaje de Datos y comprobar su autenticidad.

- **Ensobretar:** Se define como la acción de encriptar un archivo con la clave pública del destinatario con la finalidad de resguardar la confidencialidad del mismo.

- **Factor:** Aquellas personas físicas que tenga la dirección de una persona moral (Institución Solicitante), o estén autorizados para contratar respecto de los negocios concernientes a dicha empresa, quienes deberán ser autorizadas para ser Titulares de Certificados Digitales de una Institución Solicitante por un Funcionario Facultado. Artículos 309 a 331 del Código de Comercio.

- **Firma Electrónica:** Es el conjunto de datos que se agrega o adjunta a un Mensaje de Datos, el cual está asociado en forma lógica a éste y es atribuible al Titular una vez utilizado el Dispositivo de Verificación de Firma Electrónica.

- **Funcionario Facultado:** Es la persona física con facultades legales para representar a una persona moral (Institución Solicitante) en actos de tipo comercial, la cual podrá realizar trámites de Certificados Digitales ante la Autoridad Certificadora Cecoban y fungirá como el Titular de los mismos.

- **Generador de Requerimiento de Certificado Digital:** Es el programa que instalado en un equipo de cómputo sirve para generar los Datos de Creación de Firma Electrónica y los Datos de Verificación de Firma Electrónica; estos últimos datos contenidos en un archivo de Requerimiento de Certificado Digital.

- **Institución Solicitante:** Es la persona moral que requiere el uso de Certificados Digitales para actos de tipo comercial a través de uno o varios funcionarios facultados, factores o dependientes.

- **Lista de Certificados Revocados "CRL" (Certificate Revocation List):** Se le conoce así al listado emitido periódicamente, firmado por una Autoridad Certificadora, que identifica los Certificados Digitales que han sido revocados.

- **Medio Magnético, Óptico o Electrónico:** Son los dispositivos que se utilizan para guardar un Requerimiento de Certificado Digital y/o un Certificado Digital. Ejemplo CD, USB, etc.

- **Mensaje de Datos:** Es la información generada, enviada, recibida, archivada y/o comunicada a través de medios electrónicos u otras tecnologías.

- **Online Certificate Status Protocol (OCSP**): Es un método para determinar el estado de un Certificado Digital X.509. Al realizar una consulta para las respuestas de OCSP son firmadas, lo cual significaría que el Certificado Digital indicado en la petición es "bueno" (good), "revocado" (revoked) o "desconocido" (unknown).

- **Prestador de Servicios de Certificación (PSC**): La persona o institución pública que preste servicios relacionados con Firmas Electrónicas y que expide los Certificados, en su caso.

- **Requerimiento de Certificado Digital** Archivo electrónico (mensaje de datos) generado a través del DGDFE que contiene los Datos de Verificación de firma electrónica del solicitante y sirve para que la AC Cecoban pueda expedir el certificado digital.

- **Revocación:** Es el acto que deja sin efecto un Certificado Digital.

- **Secretaría de Economía:** Es un órgano de la Administración Pública Federal Centralizada que coordina y actúa como Autoridad Certificadora, y Registradora, respecto de los Prestadores de Servicios de Certificación (PSC).

- **Solicitante:** A la persona que inicia el trámite para obtener un Certificado Digital.

- **Terceros que confían:** Persona física o moral que confía en los servicios de un Prestador de Servicios de Certificación y además siendo o no el titular, puede actuar sobre la base de un Certificado Digital o de una Firma Electrónica.

- **Titular del Certificado:** A la persona física a cuyo favor fue expedido el Certificado Digital.

3. PARTICIPANTES EN EL SERVICIO DE CERTIFICACIÓN, RESPONSABILIDADES Y LÍMITES DE RESPONSABILIDAD.

3.1 Participantes.

Autoridades Certificadoras

- **Autoridad Certificadora Raíz de la Secretaría de Economía (ACR-SE).-** Es la entidad cuyo propósito es la expedición y/o revocación de certificados de Autoridades Certificadoras, para tal efecto la responsable de dicha entidad es la Dirección General de Normatividad Mercantil de la propia Secretaria de Economía.
- **Autoridad Certificadora Cecoban (AC-Cecoban).-** Es el Prestador de Servicios de Certificación (PSC) autorizado por la Secretaría de Economía para la expedición de Certificados Digitales.

Autoridades Registradoras

Es la persona física o moral responsable de la verificación de la documentación requerida, así como de la identidad de los Solicitantes y de requerir a la Autoridad Certificadora la expedición o revocación de los Certificados Digitales.

Titulares

Son las personas físicas o representantes de las personas morales a cuyo favor fueron expedidos Certificados Digitales.

Terceros que Confían

Personas físicas o morales que confían en los servicios de un Prestador de Servicios de Certificación y además siendo o no el titular, puede actuar sobre la base de un Certificado Digital o de una firma electrónica.

3.2 Responsabilidades de los Participantes

Autoridad Certificadora Raíz de la Secretaría de Economía (ACR-SE)

- Normar y administrar la estructura jerárquica de certificación de acuerdo con las políticas que ella misma establezca.
- Crear su propio Certificado Digital.

- Expedir los Certificados Digitales de Autoridad Certificadora a las personas físicas o representantes de personas morales de carácter privado o público que hayan sido acreditados como Prestadores de Servicios de Certificación.
- Administrar la base de datos de las claves públicas correspondientes a los Certificados Digitales que las Autoridades Certificadoras tengan registradas en sus bases de datos.
- Difundir su clave pública y las claves públicas de las Autoridades Certificadoras a través del sitio que la Secretaría de Economía tiene en su sitio de internet.
- Recibir en línea copia de los Certificados Digitales expedidos por la AC Cecoban y entregar el acuse de recibo correspondiente.
- Recibir, a través de correo electrónico firmado y encriptado, un mensaje de la Autoridad Certificadora a través del cual hace entrega de (los) archivo(s) que contiene(n) copia de los Certificados Digitales expedidos y revocados dentro de las (24) horas (o dentro de las seis (6) horas cuando no sea posible enviar en línea y tiempo real). Entregar un acuse de recibo firmado electrónicamente por el personal designado por la Dirección General de Normatividad Mercantil (DGNM-SE).

Autoridad Certificadora:

- Resguardar la confidencialidad, integridad y disponibilidad de los Datos de Creación de Firma Electrónica que correspondan a su propio Certificado.
- Expedir y registrar Certificados Digitales siempre y cuando se confirme la unicidad de las claves públicas.
- Administrar las bases de datos con los Certificados Digitales registrados, tanto vigentes como históricas.
- Proporcionar a los usuarios que lo soliciten a través de medios electrónicos, información respecto de Certificados Digitales.
- Revocar Certificados Digitales en los supuestos previstos en las disposiciones aplicables Auxiliarse de Autoridades Registradoras en la realización de sus funciones, de conformidad con las disposiciones aplicables y de acuerdo a lo establecido en este documento.
- Responder por los daños y perjuicios que, con motivo de la realización de sus actividades, ocasione por negligencia en el proceso de certificación, de conformidad con las disposiciones aplicables.
- Responder por los actos que realicen sus Autoridades Registradoras, así como de los daños y perjuicios que éstos generen en el cumplimiento de sus funciones, de conformidad con lo previsto en las disposiciones aplicables.
- Resguardar y proteger los datos personales de los titulares de los Certificados Digitales.
- Proporcionar al Solicitante de un Certificado Digital los medios necesarios para la generación de datos de creación y verificación de su firma electrónica.
- Proporcionar el servicio que permita a los titulares de Certificados Digitales revocar en línea, su Certificado Digital en cualquier momento.

- Publicar su Manual de Política de Certificación y su Declaración de Prácticas de Certificación en su sitio de internet con acceso al público en general.
- Suscribir con el Cliente un contrato en el que se ratifiquen las obligaciones y responsabilidades de las partes, sanciones por incumplimiento, procedimientos para resolución de conflictos y el procedimiento para dejar de operar como AC.
- Poner a disposición del público en general y a través de su sitio de Internet la información siguiente:
    a. Lista de Certificados Revocados CRL.
    b. El estatus de los Certificados Digitales
    c. Descarga de Certificados Digitales.
    d. Consulta de estatus de Certificados
    e. Consulta de Certificados revocados
- Facultar a Personas físicas o Morales para que la auxilien en la realización de sus funciones de conformidad con las disposiciones aplicables y de acuerdo a lo establecido en este documento.
- Publicar en su sitio de internet los datos de las Autoridades Registradoras facultadas para auxiliar a la AC en sus funciones, así como las Autoridades Registradoras que por algún motivo haya causado baja, lo anterior de conformidad con las disposiciones aplicables y de acuerdo a lo establecido en este documento.
- Recibir de las Autoridades Registradoras la documentación digitalizada con imágenes legibles del Solicitante/Titular del Certificado Digital de acuerdo a lo que establece la AC Cecoban en este documento, en el Manual de Política de Certificación y en el Manual de Operación de la AC y AR Cecoban.
- Recibir el expediente físico con la documentación que se utilizó para acreditar la identidad y personalidad de los titulares de Certificados Digitales expedidos de conformidad con las disposiciones aplicables, a lo establecido en este documento, en el Manual de Política de Certificación y en el Manual de Operación de la AC y AR Cecoban.
- Supervisar las funciones que realizan las Autoridades Registradoras facultadas para solicitar la expedición o revocación de Certificados Digitales.
- Mantener respaldo de la información que se derive del proceso de Expedición y Revocación de Certificados Digitales, conforme a la Norma Oficial Mexicana NOM-151 SCFI 2002.
- Facturar el pago por concepto de expedición de acuerdo al proceso de facturación establecido en Cecoban.
- Designar a un responsable para enviar copia de los Certificados Digitales expedidos y revocados por la AC Cecoban al personal autorizado de la DGNM-SE, y recibir el acuse de recibo correspondiente, de acuerdo al proceso establecido por la Secretaría de Economía.
- Informar por escrito a la DGNM-SE el nombre del personal autorizado por la AC Cecoban para entregar copia de los Certificados Digitales expedidos y revocados.

- Verificar la identidad entre el personal designado por la AC Cecoban y el autorizado por la DGNM-SE para realizar el intercambio de llaves públicas en formato digital (certificado X.509 en formato binario), así como levantar y firmar la minuta correspondiente a esta actividad.
- Realizar una prueba de envío de Certificados Digitales, entre el responsable designado por la AC Cecoban y el personal autorizado de la DGNM-SE de acuerdo al procedimiento de Envío de Copias de Certificados Digitales de la AC Cecoban y Recepción en la DRySPSC, registrando por escrito y firmando los resultados de la prueba realizada.
- Enviar en línea copia de los Certificados Digitales expedidos y revocados por la AC Cecoban a la Dirección General Normatividad Mercantil de Secretaría de Economía (DGNM-SE)
- Enviar copia de los Certificados Digitales expedidos y revocados por la AC Cecoban a la DGNM-SE dentro de las veinticuatro (24) horas de haber emitido el CD (o dentro de las seis (6) horas cuando no sea posible enviar en línea y tiempo real),
- Enviar por correo electrónico copia de los Certificados Digitales expedidos y revocados por la AC Cecoban, para lo cual deberá enviar un paquete por día o sub paquetes y recibir del subdirector de Seguridad Regional de la DGNM-SE el acuse de recibo correspondiente.

Autoridad Registradora:

- Auxiliar a la Autoridad Certificadora en la realización de sus funciones de conformidad con las disposiciones aplicables y de acuerdo a lo establecido en este documento.
- Verificar la identidad de los Solicitantes que desean obtener Certificados Digitales, con base en los documentos oficiales que éstos le presenten.
- Recibir y verificar el Requerimiento de Certificado Digital y la Solicitud de Certificado Digital correspondiente.
- Solicitar a la Autoridad Certificadora Cecoban la expedición y/o revocación del Certificado Digital.
- Obtener “Carta de aceptación de Certificado Digital” con firma autógrafa del solicitante que entre otros aspectos informa al Solicitante de un Certificado Digital sus derechos y obligaciones.
- Entregar al titular su Certificado Digital.
- Recibir y verificar la Solicitud de Revocación de Certificado Digital correspondiente.
- Obtener “Carta de aceptación de Certificado Digital” con firma autógrafa del solicitante que entre otros aspectos informa al Solicitante de un Certificado Digital sus derechos y obligaciones.
- Entregar al titular su Certificado Digital.
- Recibir y verificar la Solicitud de Revocación de Certificado Digital correspondiente.
- Enviar a la Autoridad Certificadora la documentación digitalizada con imágenes legibles del Solicitante/Titular del Certificado Digital de acuerdo a lo establecido en este documento y en el Manual de Operación de la AC y AR Cecoban.

- Resguardar los expedientes físicos por un periodo mínimo de 10 años y en caso de dejar de operar como AR deberá enviarlos a la AC Cecoban de acuerdo a lo establecido en el presente manual y en el Manual de Operación de la AC y AR Cecoban.
- Enviar a la Autoridad Certificadora el expediente con la documentación que acreditó la identidad y personalidad de los titulares de Certificados Digitales expedidos de conformidad con las disposiciones aplicables, a lo establecido en este documento y en el Manual de Operación de la AC y AR Cecoban.
- Utilizar los datos obtenidos de los Solicitantes durante el proceso de expedición y revocación de Certificados Digitales sólo para los propósitos que se establecen en este documento, por lo que no deben utilizarlos para propósitos diferentes.

Titulares:

- Solicitar su Certificado Digital a la AC Cecoban o a través de una Autoridad Registradora, presentando su Requerimiento de Certificado Digital y en su caso los documentos oficiales para su identificación y la solicitud correspondiente.
- Estar informado de sus derechos y obligaciones, y las disposiciones aplicables a la firma electrónica.
- Manifestar su conformidad firmando de forma autógrafa o con su Firma Electrónica lo que se establece en la Carta de aceptación de Certificado Digital.
- Establecer, en secreto y en forma individual, su contraseña de seguridad con la que se cifra su clave privada para protegerla, y su clave de anulación para poder revocar en línea en caso necesario su Certificado Digital.
- Generar, en secreto y en forma individual, su par de claves (pública y privada) mismas que se encuentran en dos archivos, uno que contendrá la clave privada y el segundo que contiene la calve pública; este último conocido también como Requerimiento de Certificado Digital.
- Recibir copia de la Carta de aceptación de su Certificado Digital en la que conste su firma autógrafa y datos de su Certificado Digital ya registrado.
- Resguardar su clave privada y tomar las medidas necesarias para evitar su uso por persona diferente.
- Recordar su frase de seguridad, así como su clave de anulación y mantenerlas en secreto.
- Solicitar en caso necesario la Revocación de su Certificado Digital a través del Sitio WEB de la Autoridad Certificadora Cecoban utilizando su clave de anulación o a través de una Autoridad Registradora, presentando la solicitud correspondiente.

3.3 Límites de Responsabilidad de los Participantes

De la Autoridad Certificadora Raíz de la Secretaría de Economía.

- La ACR-SE a través de la Dirección General de Normatividad Mercantil, es responsable único de cualquier incidente o responsabilidad nacidos de la clave privada de la ACR-SE.
- Cualquier anomalía o incidente producido entre el momento de la revocación de la clave privada de la ACR-SE y el momento de la notificación de tal acto a las Autoridades Certificadoras así como la revocación de los Certificados Digitales emitidos por ésta es responsabilidad única y exclusiva de la ACR-SE.

De la Autoridad Certificadora Cecoban.

La Autoridad Certificadora Cecoban deberá responder por las irregularidades que ocasione siempre y cuando se compruebe que el acto que originó la irregularidad, fue una conducta negligente llevada a cabo por la Autoridad Certificadora en el proceso de Expedición, Registro, Revocación o Administración de Certificados Digitales.

La Autoridad Certificadora no será responsable en los siguientes casos:

- Por cualquier tipo de daños y/o perjuicios que sufran sus usuarios y/o Titulares de Certificados Digitales, siempre que estos deriven de la indebida utilización de los servicios, el Certificado Digital y/o sus datos de creación de firma electrónica por parte de dichos usuarios y/o Titulares de Certificados Digitales.
- Frente a terceros afectados, que tengan una relación directa o indirecta con los servicios que presta la Autoridad Certificadora.
- Por los daños y/o perjuicios de cualquier naturaleza como pueden ser de manera enunciativa mas no limitativa, pérdida de utilidades, suspensión de operaciones, pérdida de información comercial o cualquier otro daño monetario; si éstos son causa de la mala o indebida utilización de los servicios por parte de los usuarios y/o Titulares de Certificados Digitales.
- Por los daños y/o perjuicios de la errónea interpretación, análisis, síntesis o conclusión a que los usuarios y/o Titulares de Certificados Digitales lleguen en el uso de los servicios.
- Por los daños y/o perjuicios que se causen, si el Solicitante de un Certificado Digital aporta datos o documentos falsos, para la obtención de dicho Certificado Digital.
- Por la interrupción o alteración temporal de los servicios por causas ajenas a la Autoridad Certificadora, como pueden ser de manera enunciativa más no limitativa, condiciones climatológicas adversas, sismos, inundaciones, fallas en la energía eléctrica, fuego, actos vandálicos, huelgas, cualquier otro motivo que afecte sus instalaciones o limiten la libertad en las comunicaciones.

De la Autoridad Registradora.

La Autoridad Registradora deberá responder por las irregularidades que ocasione, siempre y cuando se compruebe que el acto que originó la irregularidad, fue una conducta negligente llevada a cabo por la Autoridad Registradora, en los procesos de acreditación de la identidad de solicitantes de certificados digitales.

La Autoridad Registradora no será responsable en los siguientes casos:

- Por cualquier tipo de daños y/o perjuicios que sufran sus usuarios y/o titulares de Certificados Digitales, siempre que estos deriven de la indebida utilización de los servicios, el Certificado Digital y/o sus datos de creación de firma electrónica por parte de dichos usuarios y/o Titulares de Certificados Digitales.
- Frente a terceros afectados, que tengan una relación directa o indirecta con los servicios que presta la Autoridad Certificadora.
- Por los daños y/o perjuicios de cualquier naturaleza como pueden ser de manera enunciativa mas no limitativa, pérdida de utilidades, suspensión de operaciones, pérdida de información comercial o cualquier otro daño monetario; si éstos son causa de la mala o indebida utilización de los servicios por parte de los usuarios y/o Titulares de Certificados Digitales.
- Por los daños y/o perjuicios de la errónea interpretación, análisis, síntesis o conclusión a que los usuarios y/o Titulares de Certificados Digitales lleguen en el uso de los servicios.
- Por los daños y/o perjuicios que se causen, si el Solicitante de un Certificado Digital aporta datos o documentos falsos para la obtención de dicho certificado.
- Por la interrupción o alteración temporal de los servicios por causas ajenas a la Autoridad Certificadora, como pueden ser de manera enunciativa más no limitativa, condiciones climatológicas adversas, sismos, inundaciones, fallas en la energía eléctrica, fuego, actos vandálicos, huelga, cualquier otro motivo que afecte sus instalaciones o limiten la libertad en las comunicaciones.

Del Titular (Usuarios)

Responder por los daños y/o perjuicios que se causen directa o indirectamente, por la utilización indebida de su Certificado Digital.

Del Tercero que Confía.

El Tercero que Confía deberá cerciorarse del tipo y vigencia de las facultades legales del Titular de un Certificado Digital con quién pretenda realizar actos en que se involucre la firma electrónica.

4. TIPOS DE CERTIFICADO Y APLICACIÓN

Los Certificados que se describen a continuación son emitidos y les aplican las disposiciones contenidas en el Código de Comercio, Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación y Reglas generales a las que deberán sujetarse los prestadores de Servicios de Certificación.

4.1 Certificados de Identidad Personal.

Permiten vincular la identidad del Titular del Certificado Digital con sus Datos de Verificación de Firma Electrónica, este tipo de certificados son emitidos a personas físicas para garantizar a terceros la autenticidad e integridad de sus mensajes y dar validez jurídica a los actos de comercio electrónico que se realicen con ellos con el uso de aplicaciones como las que se indican a continuación:

Aplicaciones Frecuentes:

- Comercio Electrónico
- Correo Seguro
- Firma de documentos
- Autenticación en sitio Web

4.2 Certificados de Representación.

Permiten vincular la identidad del Titular del Certificado Digital con sus Datos de Verificación de Firma Electrónica permitiéndole ejercer de manera electrónica las facultades otorgadas a él por alguna otra persona física o moral y, este tipo de certificados son emitidos a personas físicas con facultades legales para representar a una persona moral (Institución Solicitante) en actos de tipo comercial con el objeto de garantizar a terceros la autenticidad e integridad de sus mensajes.

Independientemente de lo anterior el Tercero que Confía deberá cerciorarse del tipo y vigencia de las facultades legales del Titular del certificado con quién pretenda realizar actos de tipo comercial, a través de los documentos y/o actos establecidos en la ley y que se realicen a través de aplicaciones como las que se indican a continuación:

Aplicaciones Frecuentes:

- Comercio Electrónico
- Correo Seguro
- Firma de documentos
- Autenticación en sitio Web

4.3 Certificados de Servidor

Permiten vincular la identidad del Titular del Certificado Digital con un equipo de cómputo responsabilidad del Titular y con sus Datos de Verificación de Firma Electrónica, este tipo de Certificados Digitales son emitidos a personas físicas responsables de algún equipo de cómputo que permiten asegurar la autenticación de las operaciones que se realicen a través de éste.

Aplicaciones Frecuentes:

- Comercio Electrónico
- Autenticación del Servidor (con el protocolo **Secure Sockets Layer** “SSL”)

4.4 Usos apropiados del Certificado Digital

Los Certificados Digitales que emita la Autoridad Certificadora Cecoban, pueden ser utilizados para las aplicaciones frecuentes mencionadas en los puntos 4.1, 4.2 y 4.3 siempre en apego a lo dispuesto por el Código de Comercio, el Manual de Política de Certificación, el presente documento y la normatividad vigente que aplique al uso de Certificados Digitales. La AC Cecoban en ningún momento será

responsable por el mal uso de los Certificados Digitales o porque los Titulares de los Certificados Digitales o Terceros que Confían no se apeguen al presente documento, al Manual de Política de Certificación, a la normatividad vigente o su empleo sea para fines no contemplados en éstas.

4.5 Usos prohibidos del Certificado Digital

La limitación de uso de un Certificado Digital está establecida por la legislación vigente aplicable a Firma Electrónica Avanzada, por el Manual de Política de Certificación y la Declaración de Prácticas de Certificación establecidas por la Autoridad Certificadora Cecoban y por las características habilitadas en el Certificado Digital al momento de su expedición; mismas que el Titular y Terceros que Confían pueden verificar en "las extensiones del mismo Certificado Digital. La Autoridad Certificadora Cecoban en ningún momento será responsable por el uso que los Titulares de Certificados Digitales, realicen, en actos o fines ilícitos y/o contrarios a la normatividad vigente.

5. COMUNIDAD DE USUARIOS DE LA AUTORIDAD CERTIFICADORA CECOBAN

La Autoridad Certificadora Cecoban a través de sus autoridades registradoras, expedirá Certificados Digitales a las personas físicas y morales.

Los Certificados Digitales que emite la Autoridad Certificadora Cecoban se generarán de acuerdo con lo establecido por la Secretaría de Economía y al Sistema Internacional de Criptografía de clave pública (PKI) de algoritmo RSA, bajo el formato X.509 versión 3, con un tamaño en sus claves públicas y privadas de hasta 2048 bits.

La Autoridad Registradora Cecoban es la encargada de verificar la identidad del solicitante de un Certificado Digital, requiriendo para tal efecto su comparecencia personal y directa como lo establece en el Manual de Operación de la AC y AR Cecoban.

5.1 Cobertura de Servicio de la AC Cecoban.

La AC Cecoban cuenta con dos Centros de Datos:

- En instalaciones (Espacio con facilidades de un centro de cómputo) rentadas con la empresa TRIARA en Querétaro, Qro., con equipo de cómputo y telecomunicaciones propiedad de Cecoban.

- En instalaciones (Espacio con facilidades de un centro de cómputo) rentadas con la empresa Axtel, Apodaca, N.L., con equipo de cómputo y telecomunicaciones propiedad de Cecoban.

Las Autoridades Registradoras ofrecen sus servicios desde cualquier punto de la República Mexicana accediendo de forma remota a la infraestructura de la AC Cecoban para solicitarle la expedición o revocación de Certificados Digitales. Este acceso se realiza considerando los elementos de seguridad que se establecen en el numeral 11.17 Elementos de Seguridad en las instalaciones de una Autoridad Registradora y a través de los esquemas que se indican a continuación:

1. Desde las oficinas corporativas de Cecoban, ubicadas en Av. Constituyentes 119, Col. San Miguel Chapultepec, Del. Miguel Hidalgo, C.P. 11850, México D.F., podrá acceder el personal de Cecoban autorizado para operar como AR Cecoban.

2. Desde las instalaciones de alguna Institución con acceso a la red privada de telecomunicaciones de Cecoban, podrán acceder siempre y cuando esté autorizado para operar como AR. Respecto de los equipos a utilizar requerirán cumplir con lo descrito en el numeral 8.2.4 Infraestructura TI de Autoridades Registradoras, de este documento.

3. Las Autoridades Registradoras deben contar con Oficinas de Trabajo fijas; teniendo la opción de solicitar Certificados Digitales a la AC desde cualquier punto de la República Mexicana a través de Internet, estableciendo un Canal Seguro hacia los Centros de Datos donde residen los servicios de la AC Cecoban.

6. ADMINISTRACIÓN DEL DOCUMENTO

6.1 Nombre e identificación del documento

Este documento es denominado como “Declaración de Prácticas de Certificación”. Esta versión podrá ser consultada en la dirección de Internet http://www.cecoban.org.mx

El objeto identificador de la “Declaración de Practicas Certificación” de acuerdo al documento de “Árbol de Identificación de Objetos (OIDs)” emitido por la “Dirección General de Normatividad Mercantil, Dirección de Regulación y Supervisión de los Prestadores de Servicios de Certificación, es: **2.16.484.101.10.316.2.3.1.1.1.2.2**

6.2 Política de Administración del documento

A continuación, se presenta la identificación del Prestador de Servicios, así como el área que servirá como medio de contacto para recibir comentarios de esta Declaración de Prácticas de Certificación, así como los responsables de realizar la actualización del mismo.

6.3 Organización que administra el documento

Organización: Cecoban, S.A. de C.V.

Autoridad Certificadora: Cecoban

Ubicación:
Av. Constituyentes 119,

Col. San Miguel Chapultepec,
Del. Miguel Hidalgo,
C.P. 11850, México D.F.
Correo electrónico: serviciosdigitales@cecoban.org.mx

Teléfono: 56 98 02 19

Sitio de Internet http://www.cecoban.org.mx

6.4 Contacto

El Profesional Jurídico y el Profesional Informático son responsables de la actualización de este documento, por lo que recibirán los comentarios, dudas u observaciones referentes a la presente Declaración de Prácticas.

Ubicación:
Av. Constituyentes 119,
Col. San Miguel Chapultepec,
Del. Miguel Hidalgo,
C.P. 11850, México D.F.

Correo electrónico: serviciosdigitales@cecoban.org.mx
Teléfono: 56 98 02 19
Sitio de Internet http://www.cecoban.org.mx

6.5 Responsable que verifica la concordancia entre el Manual de la Política de Certificación y la Declaración de Prácticas de Certificación

La Autoridad Certificadora Cecoban, asigna al Profesional Jurídico y al Profesional Informático, como responsables de verificar la concordancia plena entre la Política de Certificados y la Declaración de Prácticas de Certificación.

6.6 Procedimiento de Publicación de la Declaración de Prácticas de Certificación

La presente Declaración de Prácticas se publicará, de Internet http://www.cecoban.org.mx

7. RESPONSABILIDADES DE PUBLICACIÓN DE INFORMACIÓN

Autoridad Certificadora Cecoban pone a disposición del público en general:

1. La información relacionada con los Certificados revocados a través de Internet en una Lista de Certificados Revocados CRL, la cual debe ser actualizada cada 24 hrs.

2. El estatus de los Certificados Digitales a través del sitio de internet http://www.cecoban.org.mx utilizando el protocolo OSCP.
3. El acceso a su sitio de internet http://www.cecoban.org.mx para:
    a. Descarga de Certificados Digitales.
    b. Consulta de estatus de Certificados.
    c. Consulta de Certificados revocados.
    d. Consulta de Autoridades Registradoras autorizadas.

7.1 Tiempo o frecuencia de publicación

La Lista de Certificados Revocados y la lista de Autoridades Registradoras se encuentran publicadas en el Sitio de la AC Cecoban http://www.cecoban.org.mx y se actualizan cada 24 horas.

El estado de Certificados Digitales se puede consultar en línea a través del servicio OCSP o a través del Sitio http://www.cecoban.org.mx. La descarga de Certificados Digitales también es en línea a través de dicho Sitio.

7.2 Acceso a la consulta de información

La AC Cecoban pone a disposición del público en general, la información relacionada con el estado de Certificados Digitales a través del sitio de Internet http://www.cecoban.org.mx

8. IDENTIFICACIÓN Y AUTENTICACIÓN DEL CERTIFICADO

8.1 Identificación del Certificado

8.1.1 Nombre Distinguido "DN (Distinguished Name)"

La validación de la identificación univoca del usuario en base al Nombre Distinguido (DN Distinguished Name) se hará de acuerdo a lo siguiente:

i. El Nombre Distinguido de los Certificados Digitales de identidad personal emitidos por la AC Cecoban se compondrá de los siguientes atributos:

Address=<Dirección del titular> (obligatorio)
C= mx (fijo obligatorio)
CN=<Nombre del Titular del Certificado Digital > (obligatorio)
E=<Correo electrónico del Titular del Certificado Digital> (obligatorio)

ii. El Nombre Distinguido de los Certificados Digitales de Representación emitidos por la AC Cecoban se constituirá de los siguientes atributos:

Address=<Dirección del titular> (obligatorio)
C= mx (fijo obligatorio)
O=<Institución a la que pertenece el Titular del Certificado Digital> (obligatorio)
OU=<Unidad Organizacional del Titular del Certificado> (obligatorio)
CN=<Nombre del Titular del Certificado Digital > (obligatorio)
E=<Correo electrónico del Titular del Certificado Digital> (obligatorio)

iii. El Nombre Distinguido de los Certificados Digitales de Servidor emitidos por la AC Cecoban se constituirá de los siguientes atributos:

Address=<Dirección del titular> (obligatorio)
C= mx (fijo obligatorio)
O=<Institución a la que pertenece el Titular del Certificado Digital> (Opcional)
OU=<Nombre del Titular del Certificado Digital Administrador del equipo> (obligatorio)
CN=<Nombre del equipo servidor> (obligatorio)
E=<Correo electrónico del Titular del Certificado Digital > (obligatorio)

8.1.2 Unicidad del DN (Distinguished Name).

La AR Cecoban consulta el nombre del solicitante a través de la aplicación de la AC Cecoban para identificar si existen Certificados Digitales emitidos con dicho nombre.

a) Si no hay Certificados Digitales emitidos a dicho nombre, la AR Cecoban solicita a la AC Cecoban la expedición del Certificado Digital correspondiente.

b) Si hay Certificados Digitales emitidos a su nombre, la AR Cecoban verifica si los datos que integran el Nombre Distinguido son iguales:

- Si no son iguales, se corroboran los datos con la documentación presentada por el solicitante del Certificado Digital y si todo es correcto, la AR Cecoban procede a tramitar el Certificado ante la AC Cecoban.
- Si son iguales, la AR Cecoban debe confirmar con el solicitante la existencia de Certificados Digitales a su nombre:
  i. Si es afirmativo, tramita el Certificado Digital ante la AC Cecoban.
  ii. Si no es afirmativo, se harán las aclaraciones pertinentes hasta garantizar la identificación unívoca del Solicitante, y hasta entonces podrá expedirse el nuevo Certificado Digital. En caso contrario, no se expedirá el Certificado Digital y se informará al Profesional Jurídico para que se tomen las medidas que correspondan.

Para los incisos anteriores, la AR Cecoban debe verificar la información contenida en el archivo de requerimiento, así como de manera personal, directa y físicamente la identidad del solicitante apoyándose con la revisión de los documentos entregados.

La AC Cecoban, una vez obtenida la solicitud de expedición de certificado por parte de la AR Cecoban, realizará la generación del Certificado Digital, previa validación de la unicidad de la Clave Pública.

La AR Cecoban entregará el Certificado Digital al solicitante en un medio magnético, óptico o electrónico, convirtiéndose éste en el Titular del mismo; requiriendo al Titular la firma de la Carta de Aceptación del Certificado Digital correspondiente.

Nota: Un Titular de Certificado Digital también podrá descargarlo desde el sitio de Internet http://www.cecoban.org.mx con el que la AC Cecoban cuenta para la prestación de sus servicios.

8.2 Autenticación del Certificado

8.2.1 Método para comprobar la posesión de la Clave Privada

La Autoridad Certificadora Cecoban verifica la firma electrónica contenida en el Requerimiento de Certificado Digital. Dicha verificación la realiza con los Datos de Verificación de Firma contenidos en el mismo requerimiento.

8.2.2 Acreditación de la identidad de un Solicitante de Certificado Digital

Para el trámite de cualquiera de los tipos de Certificado Digital que emite la AC Cecoban, el solicitante debe enviar por correo electrónico la información digitalizada para su revisión previa por parte de la Autoridad Registradora y posteriormente deberá acudir con dicha Autoridad Registradora autorizada por la Autoridad Certificadora Cecoban, y entregar la siguiente documentación para llevar a cabo el trámite de acreditación de identidad.

- Identificación Oficial, original para cotejo y copia fotostática de una de las siguientes identificaciones:
  - Credencial para votar emitida por el Instituto Nacional Electoral (INE).
  - Pasaporte vigente emitido por la Secretaría de Relaciones Exteriores (SRE).
  - Cédula profesional, con antigüedad no mayor 10 años.
  - Cartilla del Servicio Militar Nacional, con antigüedad no mayor 10 años.

- Para el solicitante extranjero con residencia en el país, deberá presentar: Pasaporte original para cotejo y copia fotostática, además la documentación que acredite su estancia legal en el país.

- Documento oficial original para cotejo y copia fotostática, en el cual conste la nacionalidad, fecha y lugar de nacimiento del solicitante: Acta de nacimiento, Cedula Única de Registro de Población, carta de naturalización o Pasaporte vigente emitido por la SRE. Para el solicitante extranjero bastará el pasaporte.

- Comprobante de Domicilio, original para cotejo y copia fotostática de cualquiera de los siguientes comprobantes:

- Servicio de energía eléctrica.
- Servicio telefónico
- Servicio de agua potable.
- Impuesto predial.
- Estados de cuenta bancarios.

- Para el caso de certificados de Representación o Servidor será necesario que el Funcionario Facultado, presente ante la AR Cecoban la siguiente documentación:

  - Instrumento público mediante el cual acredite la legal constitución de la Institución Solicitante (Ejemplo: Acta Constitutiva, Publicación en el Diario Oficial o su equivalente)
  - Instrumento público el cual consten sus facultades o en su caso carta membretada firmada en forma autógrafa por el representante legal de la Institución Solicitante que contenga como mínimo: nombre completo del que fungirá como Titular, uso o funcionalidad que se le dará al Certificado Digital y vigencia.
  - Registro Federal de Contribuyente de la Institución Solicitante.
  - Comprobante de Domicilio de la Institución Solicitante.

  NOTAS:
  - ✓ El comprobante de servicio de energía eléctrica, el comprobante de servicio telefónico y los estados de cuenta bancaria no deberán tener antigüedad mayor a tres meses al momento de su presentación.
  - ✓ El comprobante de servicio de agua potable y el comprobante de impuesto predial no deberán tener antigüedad mayor a un año al momento de su presentación.
  - ✓ Para el solicitante extranjero con residencia en el país, se consideran como comprobantes de domicilio válidos, los mismos que aplican al solicitante nacional.
  - ✓ En el caso de Certificados de Representación en el cual se entregue carta membretada deberá anexarse original y copia fotostática del poder notarial e identificación oficial del representante legal. Independientemente de lo anterior el Tercero que Confía deberá cerciorarse del tipo y vigencia de las facultades legales del Titular del Certificado Digital con quién pretenda realizar actos de tipo comercial.

8.2.3 Acreditación de Solicitantes para fungir como Autoridades Registradoras

En términos del Artículo 104 fracción I del Código de Comercio, la AC Cecoban podrá acreditar a personas físicas y morales como Autoridades Registradoras que auxilien a la AC en sus funciones, siempre que cumplan con los requisitos establecidos en el punto 8.2.3.1 Requisitos para acreditar a Solicitantes para Operar como AR Cecoban.

El Profesional Jurídico y el Profesional Informático serán responsables de acreditar a las personas físicas y morales que cumplan con lo establecido en este apartado; adicionalmente el Profesional Jurídico será el encargado de atender el proceso de acreditación de personalidad y expedición de Certificados Digitales a quienes hayan acreditado el proceso para operar como Autoridad Registradora.

8.2.3.1 Requisitos para acreditar a Solicitantes para Operar como AR Cecoban

El solicitante para operar como AR Cecoban debe cumplir con los requisitos siguientes:

1. Contar con escolaridad mínima de licenciatura o equivalente, para lo cual debe presentar como parte de la documentación de su solicitud un título o cédula expedidos por una Institución de Educación.

2. Cumplir con el requisito establecido en el artículo 102 inciso A) fracción IV del Código de Comercio y el artículo 5 fracción V del Reglamento. Para cumplir con este requisito deberá presentar declaración ante fedatario público en la cual el solicitante manifieste bajo protesta de decir verdad y advertido de las penas en que incurren los que declaran falsamente ante una autoridad distinta a la judicial, que cumple con dicho requisito que establece:

   Código de Comercio:

   Artículo 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 servicios de certificación dentro de los 45 días naturales siguientes al comienzo de dicha actividad.

   A) Para que las personas indicadas en el artículo 100 puedan ser Prestadores de Servicios de Certificación, se requiere acreditación de la Secretaría, la cual no podrá ser negada si el solicitante cumple los siguientes requisitos, en el entendido de que la Secretaría podrá requerir a los Prestadores de Servicios de Certificación que comprueben la subsistencia del cumplimento de los mismos:

   ...

   IV. Quienes operen o tengan acceso a los sistemas de certificación de los Prestadores de Servicios de Certificación no podrán haber sido condenados por delito contra el patrimonio de las personas o que haya merecido pena privativa de la libertad, ni que por cualquier motivo hayan sido inhabilitados para el ejercicio de su profesión, para desempeñar un puesto en el servicio público, en el sistema financiero o para ejercer el comercio.

   Reglamento del Código de Comercio:

   ARTÍCULO 5o.- Los interesados en obtener la acreditación como Prestador de Servicios de Certificación deberán:
   ...

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

3. Entregar al Profesional Jurídico de Cecoban su solicitud formal junto con comprobante de estudios, y la documentación que se indica en el punto 8.2.3.2 Verificación de Identidad de Solicitantes para Operar como AR Cecoban, para que el profesional Jurídico de Cecoban pueda iniciar el trámite de acreditación de identidad.

4. Acreditar la evaluación de conocimientos teóricos y prácticos que la AC Cecoban establezca. Ésta deberá ser confidencial e incluir, entre otros temas, lo siguiente:

   a. El conocimiento de la operación como usuario de los Sistemas Informáticos que habrá de utilizar un Solicitante de Certificado Digital y una AR Cecoban.

b. El conocimiento de los procedimientos para verificar la identidad y personalidad de los solicitantes de Certificados Digitales de acuerdo a lo descrito en 8.2.3.2 del presente documento.

c. El conocimiento de la operación de los sistemas que utilizará para operar como AR Cecoban para la solicitud de Certificados Digitales a la AC.

d. El conocimiento de sus funciones, obligaciones y responsabilidades como Autoridad Registradora.

e. Conocimientos sobre conceptos relacionados a los servicios de Firma Electrónica Avanzada, la Autoridad Certificadora y de las Autoridades Registradoras.

f. Conocimientos respecto de la Política de Privacidad y protección de datos personales del servicio de Certificados Digitales.

5. Comprobar que cuenta con la infraestructura de cómputo y comunicaciones necesaria para operar como AR Cecoban y brindar las facilidades al Oficial de Seguridad de la AC Cecoban para que verifique que cumple con dicha infraestructura, misma que se indica en el numeral 8.2.4

6. Comprobar que cuenta con el lugar de trabajo seguro para que resguarde documentación y los elementos inherentes al ejercicio de sus funciones, conforme al Manual de Política de Certificación.

7. Brindar las facilidades para que los Profesional Informático, el profesional Jurídico o aquellas personas que estos últimos designen en conjunto, a nombre de la AC Cecoban verifiquen que cuenta con los elementos de seguridad, la infraestructura y conocimientos desglosadas en el presente documento y necesarios para la prestación del servicio. Proceso que deberá ser aplicado por lo menos por una ocasión de forma anual.

8. Firmar la carta de aceptación que en caso de no contar con los elementos referidos en el punto anterior la acreditar como AR podrá ser revocada.

9. Firmar el contrato de prestación de servicios con la AC Cecoban para fungir como AR Cecoban

8.2.3.2 Verificación de Identidad de Solicitantes para Operar como AR

La AC Cecoban a través del Profesional Jurídico realiza el proceso de verificación de identidad de los solicitantes considerando que estos podrán ser persona física, notario público, corredor público o persona moral.

NOTARIO PÚBLICO:

1. Identificación Oficial de uno de los siguientes comprobantes:

   - ✓ Credencial para votar emitida por el Instituto Federal Electoral (IFE).
   - ✓ Pasaporte vigente emitido por la Secretaría de Relaciones Exteriores (SRE).

- ✓ Cédula profesional, con antigüedad no mayor a 10 años.

2. Clave Única de Registro de Población (CURP)
3. Comprobante de Domicilio de cualquiera de los siguientes comprobantes:

   - ✓ Servicio de energía eléctrica.
   - ✓ Servicio telefónico (excepto telefonía celular).
   - ✓ Servicio de agua potable.
   - ✓ Impuesto predial.
   - ✓ Estados de cuenta bancarios.

   NOTAS:

   En el caso de que la identificación oficial no contemple domicilio o el domicilio no sea el actual, el comprobante de domicilio deberá estar a nombre del solicitante. En el caso de que la identificación oficial contemple el domicilio actual, el comprobante de domicilio puede ser a su nombre o a nombre de un tercero.

   El comprobante de servicio de energía eléctrica, el comprobante de servicio telefónico y los estados de cuenta bancarios no deberán tener antigüedad mayor a tres meses al momento de su presentación.

   El comprobante de servicio de agua potable y el comprobante de impuesto predial no deberán tener antigüedad mayor a un año al momento de su presentación.

4. Patente de Notario o credencial de notario.

CORREDOR PÚBLICO:

Mismos requisitos que para Notario Público, a excepción del último punto que deberá ser:

1. Habilitación para ejercer como Corredor Público.

PERSONAS FÍSICAS:

1. Identificación Oficial, de uno de los siguientes comprobantes:
   - ✓ Credencial para votar emitida por el Instituto Federal Electoral (IFE).
   - ✓ Pasaporte vigente emitido por la Secretaría de Relaciones Exteriores (SRE).
   - ✓ Cédula profesional, con antigüedad no mayor 10 años.
   - ✓ Cartilla del Servicio Militar Nacional, con antigüedad no mayor 10 años.

2. Para el solicitante extranjero con residencia en el país, deberá presentar: Pasaporte original para cotejo y copia fotostática, además la documentación que acredite su estancia legal en el país.

3. Documento oficial, en el cual conste la nacionalidad, fecha y lugar de nacimiento del solicitante: Acta de nacimiento, Cedula Única de Registro de Población, carta de naturalización o Pasaporte vigente emitido por la SRE. Para el solicitante extranjero bastará el pasaporte.

4. Comprobante de Domicilio, de cualquiera de los siguientes comprobantes:
   - ✓ Servicio de energía eléctrica.
   - ✓ Servicio telefónico (excepto telefonía celular).
   - ✓ Servicio de agua potable.
   - ✓ Impuesto predial.
   - ✓ Estados de cuenta bancarios.

PERSONAS MORALES:

Para el caso de acreditación de personas físicas en representación de una Persona Moral será necesario que el Funcionario Facultado, presente ante la AC Cecoban la siguiente documentación:

- ✓ Instrumento público mediante el cual acredite su legal constitución (Ejemplo: Acta Constitutiva que contenga los datos de inscripción del Registro Público de Comercio, Publicación en el Diario Oficial o su equivalente).
- ✓ Instrumento público el cual consten sus facultades del solicitante.
- ✓ Registro Federal de Contribuyentes de la Institución.
- ✓ Comprobante de Domicilio de la Institución.
- ✓ Listado de personas que apoyaran a la AR en la acreditación de la identidad y personalidad de los solicitantes de certificados digitales, los cuales deberán cumplir con lo establecido en este documento según corresponda.

Adicionalmente deberán cumplir con los requisitos y presentar la misma documentación establecida para una persona Física en este mismo numeral.

NOTA:

- ✓ El comprobante de servicio de energía eléctrica, el comprobante de servicio telefónico y los estados de cuenta bancaria no deberán tener antigüedad mayor a tres meses.
- ✓ El comprobante de servicio de agua potable y el comprobante de impuesto predial no deberán tener antigüedad mayor a un año.
- ✓ Para el solicitante extranjero con residencia en el país, se consideran como comprobantes de domicilio válidos, los mismos que aplican al solicitante nacional.
- ✓ En el caso de acreditación de personas morales deberá anexarse original y copia fotostática del poder notarial e identificación oficial del representante legal.

8.2.4 Infraestructura de TI de las Autoridades Registradoras

Los equipos de cómputo fijo o portátil desde donde accedan las Autoridades Registradoras, deberán estar alineadas a las políticas de Seguridad que establezca la AC Cecoban, entre las que se encuentran las siguientes:

a. Aseguramiento de los equipos de acuerdo a lo establecido en los estándares de configuración de Cecoban.

b. Sistema Operativo con parches actualizados, Antivirus y Firewall personal habilitado.

c. Protegido con contraseña de arranque.

d. Control de acceso para el inicio de sesión a través de usuario y contraseña que cumplan con las políticas descritas en el Manual de Políticas de Seguridad de Cecoban.

e. Acceso a la infraestructura de Cecoban a través de un canal seguro.

f. Mecanismo para el cifrado de información de todo el disco duro.

8.3 Identificación y autenticación para la expedición de un nuevo Certificado Digital

8.3.1 Identificación y autenticación para la expedición de un nuevo Certificado por expiración

Se considera para este punto, los certificados digitales cuya expiración haya ocurrido, por lo que, para expedir un Certificado Digital, los Titulares deberán iniciar un nuevo trámite de expedición de Certificado y cumplir nuevamente con el proceso de acreditación de identidad y entregar la documentación ante la Autoridad Registradora.

Es responsabilidad del Titular del Certificado Digital verificar la fecha de vencimiento y estatus de su certificado.

8.3.2 Identificación y autenticación para la expedición de un nuevo Certificado Digital después de una revocación

En caso de que un Certificado Digital sea revocado, los Titulares deberán iniciar un nuevo trámite como se señala en el punto anterior para obtener un nuevo Certificado Digital.

8.4 Identificación y autenticación para solicitud de revocación de Certificado Digital

La solicitud de revocación puede proceder del Titular de Certificado Digital o de un funcionario facultado de la Institución que solicitó la expedición del Certificado Digital en cuestión.

8.4.1 Titular

El Titular consulta la Lista de Autoridades Registradoras autorizadas por Cecoban y selecciona una para acudir a entregar la siguiente documentación para llevar a cabo el trámite de acreditación de identidad:

- Identificación Oficial, original para cotejo y copia fotostática de uno de las siguientes identificaciones:
  - ✓ Credencial para votar emitida por el Instituto Federal Electoral (IFE).

- ✓ Pasaporte vigente emitido por la Secretaría de Relaciones Exteriores (SRE).
- ✓ Cédula profesional, con antigüedad no mayor 10 años.
- ✓ Cartilla del Servicio Militar Nacional, con antigüedad no mayor 10 años.

- Para el solicitante extranjero con residencia en el país, deberá presentar: Pasaporte original para cotejo y copia fotostática, además la documentación vigente que acredite su estancia legal en el país.

- El Formato "Revocación de Certificado" debidamente requisitado y firmado de manera autógrafa por el Titular.

El Titular también puede comunicarse vía telefónica con una Autoridad Registradora para solicitar la revocación de su Certificado debiendo para ello enviar la documentación digitalizada indicada en los puntos anteriores.

8.4.2 Funcionario facultado:

Debe acudir personalmente con una Autoridad Registradora una persona debidamente facultada, para que en representación de quien haya solicitado el Certificado Digital entregue la siguiente documentación para llevar a cabo el trámite de Revocación del Certificado Digital.

a) Carta de autorización de revocación de Certificado Digital, debidamente firmada.

b) Identificación oficial y comprobante de domicilio, en original para cotejo y copia fotostática de uno de los comprobantes autorizados en el presente manual en el Capítulo 8, numeral 8.2.2 Acreditación de identidad y personalidad del Solicitante.

c) Documento que acredite sus facultades para solicitar dicha revocación (poder notarial para actos de administración o de dominio).

La carta de autorización y documentación establecida en los incisos anteriores se podrá realizar de forma electrónica siempre que se establezca en el contrato de prestación de servicios entre Cecoban, S.A. de C.V. y la persona moral en cuestión.

9. REQUERIMIENTOS OPERACIONALES DEL CICLO DE VIDA DEL CERTIFICADO

9.1 Solicitud de Certificado Digital

9.1.1 Persona que puede solicitar un Certificado Digital

Cualquier Persona Física y Moral, corredor público y notario público, bajo las modalidades antes establecidas, puede solicitar un Certificado Digital para garantizar frente a terceros la autenticidad e integridad de sus mensajes electrónicos.

9.1.2 Proceso para solicitar un Certificado Digital y responsabilidades del solicitante

El solicitante de un Certificado Digital debe:

1. Asegurarse de la existencia de una relación jurídica entre Cecoban y el mismo Solicitante o la Institución Solicitante.

   La Autoridad Certificadora Cecoban por su parte también asegura la existencia de la relación jurídica entre las partes.

2. Requisitar el formato Solicitud de Certificado Digital. Es responsabilidad del solicitante proporcionar información precisa y verdadera de acuerdo a las especificaciones de la solicitud que la AC Cecoban mantiene pública en su sitio de internet http://www.cecoban.org.mx.

3. Generar su archivo de requerimiento y su clave privada a través del uso del Dispositivo Generador de Datos de creación y verificación de firma electrónica que la AC Cecoban mantiene pública en su sitio de internet http://www.cecoban.org.mx

4. Asistir con la Autoridad Registradora para la acreditación de identidad referida en el punto 8.2.2 Acreditación de la identidad de un solicitante de Certificado Digital.

5. Entregar a la Autoridad Registradora:

   - Solicitud de Certificado Digital debidamente requisitada y firmada de manera autógrafa.
   - Archivo de Requerimiento de Certificado Digital en medio óptico o electrónico (CD o USB).
   - Documentación necesaria para la acreditación de identidad referida en el punto 8.2.2.

   Nota: El solicitante opcionalmente podrá generar el archivo de requerimiento en las instalaciones de la Autoridad Registradora.

9.2 Procedimiento para la generación de Datos de Creación de Firma Electrónica y Datos de Verificación de Firma Electrónica.

El Solicitante genera bajo su total control los Datos de Creación de Firma Electrónica y Datos de Verificación de Firma Electrónica (Par de claves privada y pública) ejecutando las siguientes actividades:

Expedición:

a) Descarga el software generador de requerimiento de Certificado Digital del sitio de internet http://www.cecoban.org.mx

b) Instala el software generador de requerimientos de Certificados Digitales en su equipo de cómputo.

c) Ejecuta la aplicación de generación de requerimiento.

d) Ingresa sus datos generales.

e) Genera su par de claves.

- Los Datos de Creación de Firma Electrónica se almacenan en un archivo con extensión “key” al que le denominamos archivo de clave privada.

- Los Datos de Verificación de Firma Electrónica se almacenan en un archivo con extensión “req” al que le denominamos archivo de Requerimiento de Certificado Digital.

f) Presenta a la Autoridad Registradora Cecoban el archivo de requerimiento de Certificado Digital.

Notas:

- Para mayor detalle de este procedimiento, consulte el manual “Generador de Requerimiento de Certificado Digital” que la AC Cecoban mantiene público en su sitio de internet http://www.cecoban.org.mx

- El solicitante puede generar su Requerimiento de Certificado Digital desde un equipo de cómputo de la AR con la cual realice su proceso de expedición de Certificado Digital.

9.3 Importancia de la protección de los Datos de Creación de Firma Electrónica.

Es esencial que el Titular de un Certificado Digital, tome todas las precauciones disponibles para proteger sus Datos de Creación de Firma Electrónica (Clave Privada) dado que la confidencialidad de estos datos es crucial para mantener la seguridad de que solamente él tenga acceso a dicha clave privada. Por esto, es que la clave privada debe ser almacenada en forma encriptada, protegida por una contraseña o frase de seguridad que la desencripta cuando requiera ser utilizada por el Titular del Certificado Digital al que está relacionado.

Es sumamente importante que el proceso de generación de los Datos de Creación de Firma Electrónica y Datos de Verificación de Firma Electrónica se realice de la forma más segura posible, que esté en absoluto control del Solicitante para asegurar que la clave privada resultante se mantenga integra y confidencial.

9.4 Software Generador de Requerimientos de Certificado Digital para Expedición.

Con la finalidad de proveer a los Solicitantes de la herramienta que les permita alcanzar los objetivos mencionados en los párrafos anteriores, la AC Cecoban pone a su disposición el software Generador de Requerimientos de Certificado Digital al que se le han incorporado los controles de seguridad para proveer una confiabilidad del proceso, entre los cuales destacan:

1. La generación de Datos de Creación de Firma Electrónica y de Datos de Verificación de Firma Electrónica
2. La introducción de adecuados generadores de números Aleatorios de acuerdo a la recomendación NIST SP 800-90 *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*
3. Incorporación de validaciones en los campos de datos generales del Solicitante para cumplir con las políticas de la AC Cecoban.
4. Asistentes visuales que ayudan a seleccionar una adecuada conformación de la contraseña o Frase de seguridad para proteger la clave privada, incluyendo la validación de la longitud mínima confiable.

5. La clave privada es almacenada encriptada en formato PKCS-8.
6. Facilidades para seleccionar la ruta específica en que se desea almacenar la clave privada
7. Facilidad de resguardar su clave privada en Dispositivo Seguro.
8. Facilidad para importar y validar archivos de requerimiento de certificación generados por otros sistemas.
   a. Esta facilidad se pone a disposición del Solicitante en caso de que requiera que la generación de sus Datos de Creación y de Verificación de Firma Electrónica se generen en otro dispositivo, porque esto le represente mayor certeza de la seguridad del proceso o por necesidades técnicas.
   b. La validación permite que el Solicitante pueda verificar si el requerimiento de certificación importado cumple con las políticas de la AC Cecoban, o en su caso identificar la información del requerimiento que requiera complementar.
   c. El que no se requiera la clave privada para este proceso, representa un grado mayor de seguridad para el Solicitante, ya que ésta no se requiere para importar el requerimiento por lo que se mantiene, en todo momento, almacenada en el dispositivo en el que se generó por primera vez.
9. La AC Cecoban pondrá a disposición de los solicitantes de Certificados y del público en general el software Generador de Requerimiento de Certificado Digital y los elementos para autenticar y verificar su integridad.

9.5 Recomendaciones que el usuario debe considerar en la generación de sus Datos Creación de Firma Electrónica y para resguardar su integridad y confidencialidad.

1. Verificar que el sistema operativo tenga:
   a. Todos los parches de seguridad instalados
   b. Un firewall personal
   c. Una aplicación antispyware
   d. Un Antivirus
   e. La protección con clave de arranque
   f. La protección de acceso con clave con las siguientes características: Longitud mínima de 8 caracteres, que combinen letras mayúsculas, minúsculas, números y caracteres especiales y que ésta se cambie periódicamente.
2. Tener habilitada la opción de actualización automática para las aplicaciones que tenga instaladas en su equipo de cómputo.
3. Asegurar que ninguna persona tenga acceso al archivo donde resguarda su clave privada.
4. Asegurar que ninguna persona conozca la contraseña de acceso de su clave privada
5. Resguardar su clave privada en la medida de lo posible en un dispositivo seguro.

Otras recomendaciones:

1. Evitar hacer transacciones a través de equipo de cómputo que no estén bajo su control en cuanto a elementos de seguridad (equipos de café internet, aeropuertos, hoteles, etc.).

9.6 Verificación de la Firma Electrónica del Solicitante de un Certificado Digital.

Solicitante del Certificado Digital

1. Presenta a la Autoridad Registradora Cecoban el archivo de requerimiento de Certificado Digital.

Autoridad Registradora

2. Previa acreditación de identidad del solicitante descrito en el numeral 8.2.2 Acreditación de la identidad de un Solicitante de Certificado Digital, ingresa el archivo de requerimiento al sistema de la AC Cecoban para la realizar la solicitud del Certificado Digital.

Autoridad Certificadora

3. Recibe el archivo de requerimiento de Certificado Digital.
4. Verifica la firma electrónica del solicitante contenida en el requerimiento para asegurar la integridad del requerimiento y posesión de los Datos de Creación de Firma Electrónica.
5. Emite el Certificado Digital correspondiente al requerimiento, firmándolo digitalmente haciendo uso del hardware criptográfico HSM.

9.7 Verificación de la firma electrónica de la AC Cecoban.

Para el caso de verificación de la firma electrónica de la AC Cecoban en los Certificados Digitales emitidos por ésta, el usuario podrá hacer uso de cualquier aplicación que sea compatible con los estándares de firma electrónica “X.509” y deberá emplear para ello los Datos de Verificación de Firma Electrónica (clave pública) contenidos en el Certificado Digital de la AC Cecoban.

Uno de los mecanismos para la verificación de la firma electrónica de la AC Cecoban es el que se describe a continuación utilizando el almacén de certificados de Windows.

Procedimiento:

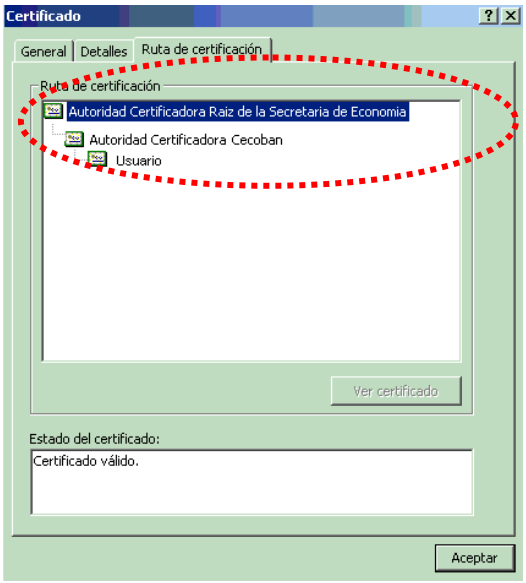
a) Descargar el Certificado Digital de la Autoridad Certificadora Raíz de la Secretaria de Economía de su sitio de Internet.

b) Descargar el certificado de la Autoridad Certificadora Cecoban de su sitio de Internet

c) Instalar ambos Certificados en el almacén de Certificados de su PC.

d) Instalar el Certificado que se desee validar en el almacén de Certificados de su PC.

e) Abrir el Certificado del usuario y verificar la ruta de certificación, la cual no debe presentar errores, ver la siguiente figura:



f) Si la validación no es correcta indicará con un error la razón por la cual no se puede comprobar o no es correcta la ruta de certificación del certificado digital en cuestión.

9.8 Proceso para la expedición de un Certificado Digital

9.8.1 Identificación del solicitante

La Autoridad Registradora debe:

a) Informar al solicitante del Certificado Digital que la Autoridad Certificadora, pone a su disposición el generador de Requerimiento de Certificado Digital, a través del sitio de Internet http://www.cecoban.org.mx.

b) Revisar que la Solicitud de Certificado Digital esté requisitada correctamente.

c) Verificar que la documentación presentada por el Solicitante cubra los requisitos establecidos en el punto 8.2.2 Acreditación de la identidad de un Solicitante de Certificado Digital.

d) Realizar el cotejo de documentos originales contra las copias presentadas por el Solicitante.

e) Abrir el archivo de requerimiento y visualizar la información contenida a través del Módulo de Agente Certificador.

f) Comparar que la información contenida en la documentación presentada en la Solicitud de Certificado Digital y el archivo de Requerimiento de Certificado Digital, corresponda fielmente con la información consignada en los documentos oficiales presentados por el Solicitante para acreditar su identidad.

9.8.2 Aprobación o rechazo de Certificados Digitales

a) Si la Autoridad Registradora encuentra alguna discrepancia entre la documentación y el archivo de requerimiento de Certificado Digital, o si no es posible hacer una identificación univoca del solicitante, la solicitud será rechazada y se requerirá al Solicitante que genere un nuevo archivo de Requerimiento de Certificado Digital o que actualice su documentación.

b) Si la validación de la identidad del solicitante es correcta se realizan las actividades siguientes:

La Autoridad Registradora debe:

c) Tramitar ante la Autoridad Certificadora la expedición del Certificado Digital como se establece en el "Manual de Operación de la AC y AR Cecoban".

La Autoridad Certificadora debe:

d) Autenticar a las Autoridades Registradoras y mantener evidencia de no repudio, con la fecha y hora, de las operaciones de trámite de expedición de Certificados Digitales que realice una Autoridad Registradora.

e) Asegurar que la clave privada de una AR se resguarde en un dispositivo seguro que cumpla con el estándar FIPS-140 nivel 3 soportado por el sistema de la AC Cecoban.

9.8.3 Tiempo para procesar un Certificado Digital

El tiempo estimado para la expedición de un Certificado Digital es de 5 a 10 minutos, siempre que la documentación se encuentre completa, correcta y cuando el Titular haya enviado la información digitalizada por correo electrónico previamente a la cita con la Autoridad Registradora.

9.8.3.1 Sello Digital de Tiempo de los Certificados Digitales.

La aplicación de la AC Cecoban cuenta con un procedimiento automático para solicitar a un tercero autorizado, el Sello Digital de Tiempo para dejar constancia de la fecha y la hora de la expedición de los Certificados generados por ésta.

Antes de la entrega del Certificado Digital al cliente, la AC Cecoban debe obtener un sello digital de tiempo de dicho Certificado Digital

9.8.3.2 Entrega del Certificado Digital al Solicitante.

La Autoridad Registradora Cecoban requisita la Carta Aceptación del Certificado Digital y la imprime dos veces para ser usadas como original y copia.

La carta de aceptación debe contener por lo menos la siguiente información:

- Autorización del Titular para la publicación y descarga de su Certificado Digital (clave pública) a través de sitio público de la Autoridad Certificadora Cecoban.
- Consentimiento del Titular para que la Autoridad Registradora mantenga un registro de la información y datos personales obtenida de él en el trámite del Certificado durante el tiempo que dure la relación jurídica y hasta por 10 años más.
- Conocimiento del Titular del uso de la clave privada y Certificado Digital así como del razonable cuidado para prevenir el uso no autorizado de su clave privada.
- Reconocimiento de que la información contenida en el Certificado Digital es correcta.
- Las obligaciones y responsabilidades del Titular del Certificado Digital
- Firma autógrafa del Titular
- La fecha y hora de entrega del Certificado Digital.

Una vez que el Titular firma la carta de aceptación se entregará el Certificado Digital al Titular en medio óptico o electrónico.

9.8.3.3 Compromiso de Privacidad

Al recibir y archivar los datos personales de los Solicitantes de Certificados Digitales, Cecoban como Autoridad Certificadora se compromete a guardar y cumplir estrictamente con las disposiciones contenidas en la fracción II del inciso A) del Art. 102, fracción V y VII del Art. 104 del Código de Comercio; y último párrafo de la fracción III del Art. 5, fracción VII y VIII del Art. 27 del Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación sobre la seguridad de la información así como el contenido de la Ley Federal de Protección de Datos Personales en Posesión de Particulares.

Con arreglo a dicho compromiso, Cecoban en su carácter de Autoridad Certificadora garantiza el estricto cumplimiento en materia de seguridad y confidencialidad por parte del personal que autorice como Autoridad Registradora.

La Autoridad Certificadora Cecoban establece un compromiso de privacidad aplicable a todas las Autoridades Registradoras.

9.8.4 Integración de Expediente

Las Autoridades Registradoras deberán integrar los expedientes físicos y electrónicos con la información que se derive del proceso de Expedición y Revocación de Certificados Digitales, para lo cual podrán auxiliarse de otras personas que al efecto designen y hayan firmado el convenio de confidencialidad correspondiente.

- Los expedientes electrónicos deberán ser integrados con imágenes legibles de los documentos obtenidos durante el proceso de expedición de Certificados Digitales y se enviará por correo electrónico firmado a la Autoridad Certificadora en un lapso no mayor de 1 día hábil y de acuerdo a como le sea instruido por ésta.

- Los expedientes físicos deberán ser resguardados por la Autoridad Registradora por lo menos 10 años a partir de la fecha de expedición del Certificado Digital y en caso de dejar de operar como AR los enviará a la AC Cecoban.

Nota: La Autoridades Registradoras no deberán utilizar para propósitos diferentes los documentos y los datos obtenidos durante el proceso de expedición de Certificados Digitales.

9.8.5 Notificación de la expedición y revocación de Certificados Digitales a otras entidades

La Autoridad Certificadora Cecoban informará a la Autoridad Certificadora Raíz de la Secretaría de Economía acerca de la expedición y revocación de Certificados Digitales.

- ✓ Cada Certificado Digital expedido o revocado por la AC Cecoban deberá enviarse a la Secretaría de Economía en línea, es decir en tiempo real inmediatamente después del momento de su expedición o revocación. En el caso que la Autoridad Certificadora Cecoban por caso fortuito o de fuerza mayor debidamente comprobado ante la Secretaría de Economía, no pudiese llevar a cabo el envío a que se refiere el apartado anterior, deberá hacer el envío por correo electrónico en un término no mayor a seis (6) horas.
- ✓ Además del envío en línea de los Certificados Digitales, la Autoridad Certificadora Cecoban, enviará a la de la DGNM-SE copia de los Certificados Digitales expedidos y revocados por ésta, vía correo electrónico firmado y encriptado, dentro de las veinticuatro (24) horas de haberlos expedido o revocado de acuerdo al proceso establecido por la Secretaría de Economía.

  La Autoridad Certificadora Cecoban deberá cerciorarse de recibir un acuse de recibo, señalando el paquete o sub paquetes de Copias de Certificados Digitales entregados. El acuse estará firmado electrónicamente por el subdirector de Seguridad Regional de la DGNM-SE.

9.9 Uso del par de Claves Privada y Pública

9.9.1 Uso de la Clave Privada

El Titular de un Certificado Digital que cuente con su clave privada, podrá firmar mensajes electrónicos hacia otros Titulares o Terceros que Confían con el objeto de garantizar la no repudiación, integridad y autenticidad de los mismos. Como ejemplo los mensajes electrónicos que se podrán firmar son:

- Correo Seguro
- Firma de documentos y/o Contratos
- Autenticación en sitio Web

9.9.2 Uso de la Clave Pública por parte de los terceros que confían

La clave pública permite a un Tercero que Confía verificar la firma electrónica del Titular del Certificado Digital correspondiente, e identificarlo.

Un Tercero que Confía podrá enviar al Titular de un Certificado Digital, mensajes electrónicos encriptados con la clave pública contenida en dicho Certificado Digital otorgándole confidencialidad a los mensajes.

9.10 Expedición de un nuevo Certificado

9.10.1 Circunstancias para la expedición de un nuevo Certificado

El Titular de un Certificado Digital podrá solicitar un nuevo certificado, previo a su vencimiento, o bien cuando su vigencia ha expirado.

9.10.2 Personas que puede solicitar la expedición de un nuevo Certificado

El Titular o el Funcionario Facultado podrán solicitar la expedición de un nuevo Certificado Digital.

9.10.2.1 Trámite ante una AR

La Autoridad Registradora Cecoban se encarga de revisar la identidad y personalidad a través de documentos de identificación que proporcionan los Solicitantes de un Certificado Digital, así como de realizar la solicitud de expedición de un Certificado Digital ante la Autoridad Certificadora Cecoban, para tal efecto se realizan las siguientes actividades:

El solicitante:

1. Tramita un Certificado Digital cuando incurre en alguno de los siguientes puntos:
   - Solicitar por primera vez el Certificado Digital,
   - Ser Titular de un Certificado Digital vigentes cuyos datos de acreditación hayan cambiado respecto a los contendidos en dicho Certificado,
   - Ser Titular de un Certificado Digital revocado o cuya vigencia esté vencida,
2. Acude personalmente ante la AR Cecoban con la documentación requerida (ver numeral 8.2.2 Acreditación de la identidad de un Solicitante de Certificado Digital) y el archivo de requerimiento de Certificado Digital (ver numeral 9.2. Procedimiento para la generación de Datos de Creación de Firma Electrónica y Datos de Verificación de Firma Electrónica)
3. Firma de forma autógrafa dos cartas de aceptación del Certificado Digital y recibe un ejemplar en la que conste su Certificado Digital ya registrado.
4. Resguarda en un lugar seguro su clave privada, así como recordar su contraseña y su clave de anulación del Certificado Digital y los mantiene en secreto.
5. El solicitante se mantiene informado a través de la Autoridad Certificadora o, en su caso, por una Autoridad Registradora, de las reglas, procedimientos y características generales de los servicios de certificación y de los Certificados Digitales.
6. El solicitante puede acceder al sitio de Internet de la AC Cecoban para descargar el Certificado Digital.
7. Adicionalmente el solicitante tiene acceso a un servicio que le permita revocar en línea, su Certificado Digital en cualquier momento.

La Autoridad Registradora:

8. Recibe la solicitud con la documentación requerida (ver numeral 8.2.2 Acreditación de la identidad de un Solicitante de Certificado Digital) y el archivo de requerimiento de Certificado Digital (ver numeral 9.2. Procedimiento para la generación de Datos de Creación de Firma Electrónica y Datos de Verificación de Firma Electrónica)
9. Realiza el procedimiento de verificación de documentación física y electrónica para determinar si es viable continuar con el proceso de solicitud de CD ante la AC.

10. Rechaza la solicitud en caso de encontrar diferencias entre la documentación y el archivo de requerimiento y pide al solicitante que genere un nuevo archivo de requerimiento o bien que actualice su documentación.
11. Valida la identificación unívoca del usuario en base al Nombre Distinguido (DN Distinguished Name) ver numeral 8.1.1 Nombre Distingido “DN (Distinguished Name)
12. Valida la identificación unívoca del usuario realizando la consulta del nombre del solicitante a través de la aplicación de la AC Cecoban e identifica si existen Certificados Digitales emitidos con dicho nombre, ver numeral 8.1.2. Unicidad del DN (Distinguished Name)
13. Tramita ante la Autoridad Certificadora Cecoban la expedición del Certificado Digital accediendo de forma remota a la infraestructura de la AC Cecoban y de acuerdo a lo establecido en el ”Manual de Operación de la AC y AR Cecoban”.
14. Almacena en los medios previstos el requerimiento y Certificado Digital correspondiente.
15. Obtiene la Carta de Aceptación y solicita firma autógrafa del titular.
16. Obtiene la Carta de Aceptación con firma autógrafa del Titular, en la que manifiesta su conformidad con las condiciones siguientes:
    I. Ser responsable del uso de su Firma Electrónica, toda vez que cualquier Mensaje de Datos firmado que se pueda comprobar con sus Datos de Verificación de Firma Electrónica le será atribuible y producirá los mismos efectos que las leyes otorgan a los documentos suscritos con firma autógrafa y, en consecuencia, tendrán el mismo valor probatorio, y
    II. Acepta las condiciones de operación y los límites de responsabilidad de la Autoridad Certificadora Raíz de la Secretaría de Economía, Autoridad Certificadora Cecoban y Autoridad Registradora Cecoban.
17. La AR Cecoban entregará el Certificado Digital al solicitante en un medio magnético, óptico o electrónico, convirtiéndose éste en el Titular del mismo.

    Nota: Un Titular de Certificado Digital también podrá descargarlo desde el sitio de Internet con el que la AC Cecoban cuenta para la prestación de sus servicios.
18. Envía al Profesional Jurídico de la AC Cecoban, en calidad de respaldo, la imagen correspondiente a la documentación recibida del Solicitante/Titular de Certificado Digital.

    Las imágenes deberán ser legibles y enviadas por cada expedición que se realice en un lapso no mayor de 1 día hábil posterior a la expedición del Certificado Digital.

    La Autoridad Registradora conservara la documentación recibida por el solicitante (expediente) por lo menos 10 años a partir de la fecha de expedición del certificado por parte de la AC. Y en caso de dejar de operar como AR enviara los documentos físicos a la AC Cecoban.

    La Autoridad Registradora no debe utilizar los documentos y sus datos para propósitos diferentes al del trámite para expedición de un certificado.

La Autoridad Certificadora

19. La AC Cecoban, una vez obtenida la solicitud de expedición de certificado por parte de la AR Cecoban, realizará la generación del Certificado Digital, previa validación de la unicidad de la clave pública.

20. Obtiene un sello digital de tiempo que indique la fecha y hora de la expedición de dicho Certificado Digital.
21. Pone el Certificado Digital emitido a disposición de la Autoridad Registradora.
22. Informa de la expedición de Certificados Digitales a la Autoridad Certificadora Raíz de la Secretaría de Economía.
23. Cuenta con un sitio de Internet para que el Titular pueda descargar su Certificado Digital.

9.11 Revocación de certificados

9.11.1 Circunstancias para revocar un Certificado

Las causas para solicitar la revocación de un Certificado Digital son:

a) Por olvido o extravío de la contraseña de la clave privada.

b) Por robo o extravío de la propia clave privada.

c) Por la sospecha de uso por terceros de su clave privada.

d) Por el cambio de alguno de los datos contenidos en el Certificado Digital.

e) Cuando el Titular de un certificado de Representación o Servidores ha dejado de pertenecer o laborar en la Institución Solicitante o sus facultades han sido canceladas o limitadas. Esta revocación será exclusiva y total responsabilidad de la Institución Solicitante.

f) Al recibir la documentación que acredite el fallecimiento del Titular.

g) Por resolución judicial.

h) Cuando la Autoridad Certificadora Raíz de la Secretaría de Economía o la Autoridad Certificadora, tengan conocimiento de que el Titular incumplió sus obligaciones.

i) Por haberse comprobado que al momento de su expedición, el Certificado no cumplió con los requisitos establecidos en la ley, situación que no afectará los derechos de tercero de buena fe.

9.11.2 Procedimiento de revocación de un Certificado

El Titular o la Institución podrán realizar la revocación de su certificado por Internet o a través de una Autoridad Registradora.

a) Revocación por Internet.

El Titular o la Institución pueden revocar su Certificado Digital a través del sitio de Internet http://www.cecoban.org.mx. Para ello es indispensable que el Titular cuente con el número de serie del Certificado Digital y la Clave de Anulación, registrada cuando se generó el “Requerimiento de Certificado Digital”.

En caso de no contar con el número de serie del Certificado Digital y la Clave de Anulación el Titular deberá llevar a cabo la revocación a través de una Autoridad Registradora.

b) Revocación a Través de una Autoridad Registradora.

El Titular o la Institución Solicitante deben:

1. Obtener la solicitud de revocación a través del sitio de Internet http://www.cecoban.org.mx para requisitar el formato de acuerdo a las especificaciones señaladas en la misma solicitud.

2. Imprimir y firmar la solicitud, ver punto 8.4 Identificación y autenticación para la solicitud de revocación de Certificado Digital.

3. Consultar la lista de Autoridades Registradoras autorizada por la Autoridad Certificadora Cecoban en la página de Internet www.cecoban.org.mx > Prestador de Servicios de Certificación > Autoridad Certificadora Acreditada por la Secretaría de Economía > Autoridades Registradoras Autorizadas por la AC Cecoban y selecciona una para acudir y entregar la documentación referida en el punto 8.4 Identificación y autenticación para la solicitud de revocación de Certificado Digital o comunicarse vía telefónica con una Autoridad Registradora Cecoban para solicitar la revocación de su Certificado Digital debiendo para ello enviar la información digitalizada.

La Autoridad Registradora debe:

4. Recibir del Titular o de la Institución Solicitante la documentación señalada en el punto anterior y realizar las validaciones correspondientes.
5. Solicitar a través del Sistema de la AC Cecoban la Revocación del Certificado Digital, como se establece en el Manual de Operación de la AC y AR Cecoban. Para esto, la Autoridad Registradora debe ejecutar el siguiente proceso.

Autoridad Registradora:

a) Solicita a través del sistema a la Autoridad Certificadora Cecoban, la revocación del Certificado Digital.

Autoridad Certificadora Cecoban:

b) Realiza el proceso automático de validaciones y procede con la revocación.

c) Actualiza el Registro Público de Certificados Digitales para dejar constancia de la fecha y hora en que se realizó la revocación del Certificado Digital.

Autoridad Registradora:

d) Recibe respuesta de la Autoridad Certificadora Cecoban a través del sistema.

e) Incluye en la Solicitud de Revocación del Certificado Digital los siguientes datos:

- Número de Serie del Certificado Digital y la fecha en que se revocó.
- Tipo de identificación, nombre de la identificación oficial usada por el Titular para acreditar su identidad.
- Número de identificación, número que se encuentra registrado en la identificación oficial. Para la credencial IFE el número válido es el OCR (Reconocimiento Óptico de Caracteres) que aparece al reverso.
- Nombre y firma de la Autoridad Registradora que realizó la Revocación del Certificado Digital.

f) Resguarda en expediente la solicitud de revocación incluyendo los datos del inciso anterior

9.11.3 Tiempo en el que la AC debe tramitar una revocación

Si la revocación del Certificado Digital se realiza a través del sitio de Internet de Cecoban y el tiempo de respuesta es inmediato.

Si la revocación del Certificado Digital se realiza ante una Autoridad Registradora, y el Titular ha requisitado y firmado correctamente su solicitud, el tiempo máximo de trámite será de 10 minutos.

9.11.4 Mecanismos que deben utilizar los terceros que confían para verificar el estatus de un Certificado revocado

A través de la lista de Certificados Revocados "CRL" publicada en el sitio de Internet http://www.cecoban.org.mx o el servicio OCSP que permite la consulta en línea del estado de Certificado los terceros que confían podrán verificar el estatus de Certificados Digitales.

- Servicio OCSP

  La Autoridad Certificadora Cecoban brinda el servicio de verificación de estatus de Certificados Digitales a través del Protocolo de Estatus de Certificados en Línea (OCSP Online Certificate Status Protocol), las 24 hrs los 365 días del año a través de su sitio de Internet http://www.ceoban.org.mx

- Página de consulta de estatus en línea

  La Lista de Certificados Revocados podrá ser consultada en el siguiente sitio de Internet http://www.ceoban.org.mx. Dicha lista de Certificados Revocados es actualizada, firmada y publicada por la Autoridad Certificadora Cecoban cada veinticuatro horas.

9.11.5 Suspensión temporal o definitiva del PSC Cecoban.

La AC Cecoban debe asegurar que las interrupciones resultado de la suspensión de los servicios de la AC sean minimizados para los Titulares y Terceros que Confían, y asegurar el mantenimiento continuo de los registros para proveer evidencia para los propósitos legales que procedan.

SUSPENSIÓN TEMPORAL

Este escenario se presenta cuando la Dirección General de Normatividad Mercantil de la Secretaria de Economía sancione al PSC Cecoban con la suspensión temporal por incumplir con alguna de las reglas generales a las que deberán sujetarse los prestadores de servicio de certificación.

Durante el periodo de tiempo definido por la Secretaría de Economía la AC Cecoban dejará de expedir Certificados Digitales y continuará proporcionando los servicios de consulta y revocación de certificados para no afectar la operación de los Titulares y Terceros que Confían.

SUSPENSIÓN DEFINITIVA

Cuando el PCS Cecoban solicite la suspensión definitiva ante la Secretaría de Economía debe realizar lo siguiente:

a. Solicitar a la Dirección General de Normatividad Mercantil de la Secretaría de Economía, la revocación de la autorización que ésta le haya otorgado, con una antelación no menor a 60 días naturales a la fecha en que pretenda cesar sus actividades como Prestador de Servicio de Certificación.
b. Dentro de los 5 días hábiles siguientes a la presentación de la mencionada solicitud, deberá notificar a los Titulares cuyos Certificados Digitales administra, su intención de dejar de actuar como PSC y que la base de datos que contiene los Certificados Digitales y su estado, será transferida a la Dirección General de Normatividad Mercantil de la Secretaría de Economía, o al PSC que ésta indique, así como la fecha en que ocurrirá.
c. Asimismo, debe proporcionar a Dirección General de Normatividad Mercantil de la Secretaría de Economía la información física que se haya recibido de los solicitantes de Certificados Digitales así como la demás información que ésta le requiera.
d. Una vez transferida la información a la que se refieren los dos puntos anteriores, la AC Cecoban revocará los Certificados Digitales de sus Autoridades Registradoras, retirará de uso su clave privada y deshabilitará los servidores donde residan sus servicios en las fechas acordadas con la Secretaría de Economía.

Cuando la Secretaría de Economía suspenda definitivamente al PSC Cecoban.

Este escenario se presenta cuando la Dirección General de Normatividad Mercantil de la Secretaria de Economía sancione al PSC Cecoban con la suspensión definitiva por incumplir con alguna de las reglas generales a las que deberán sujetarse los prestadores de servicio de certificación debiendo realizar lo mismo que en el punto anterior a excepción de la solicitud por parte del PSC Cecoban.

10. CONTROLES ADMINISTRATIVOS Y OPERATIVOS

10.1 Ubicación física de la Autoridad Certificadora Cecoban

Los servidores donde operan los Sistemas de la Autoridad Certificadora Cecoban están ubicados en los Centros de Datos de Cecoban ubicados en:

- Instalaciones (Espacio con facilidades de un centro de cómputo) rentadas con la empresa TRIARA en Querétaro, Qro., con equipo de cómputo y telecomunicaciones propiedad de Cecoban.

- Instalaciones (Espacio con facilidades de un centro de cómputo) rentadas con la empresa Axtel, Apodaca, N.L., con equipo de cómputo y telecomunicaciones propiedad de Cecoban.

Dichos Centros de Datos cuentan con los elementos de seguridad que se establecen en el "Modelo Operativo" y en la política y prácticas de seguridad física establecidos por la AC Cecoban y que proporciona a la Secretaría de Economía como Autoridad que Acredita a los Prestadores de Servicios de Certificación.

10.2 Acceso Físico a la Autoridad Certificadora Cecoban

Los Centros de Datos donde residen los servidores para la prestación de los servicios se encuentran protegidos por:

1. Personal de vigilancia 7x24x365,
2. Circuito Cerrado de Televisión,
3. Detectores de movimiento,
4. Sistemas de control de acceso.

Adicionalmente el acceso de personas a estas áreas, debe ser previamente autorizado.

10.3 Clima controlado y Energía Eléctrica

El área donde se ubica la Autoridad Certificadora Cecoban, cuenta con un sistema de clima controlado de operación continua y redundante ya que se cuenta con varios equipos que permiten mantener las condiciones requeridas para un Centro de Cómputo aun cuando falla uno de estos equipos.
Adicionalmente se cuenta con sensores de temperatura y humedad que permiten mediante una alarma audible alertar al personal de un problema con estos equipos.

La alimentación eléctrica de los equipos de la Autoridad Certificadora Cecoban, es redundante, mediante el uso de Sistemas de Fuerza Ininterrumpida (UPS) y Generadores de Corriente Alterna de Emergencia con transferencia automática de carga al UPS y su banco de baterías, cuando se presenta algún problema en la acometida del suministro de energía eléctrica.

Adicionalmente se cuenta con sistemas de tierra física que cumplen con estándares internacionales (IEEE 1100, NEC 250) así como con la Norma Oficial Mexicana.

10.4 Protección contra Inundaciones

Los Centros de Datos donde se encuentran los servidores para la prestación de los servicios están ubicados en lugares que no están expuestos a inundaciones y las instalaciones están protegidas para evitar filtración de agua.

10.5 Protección y prevención contra incendios

Los Centros de Datos donde se encuentran los servidores para la prestación de los servicios así como el Centro Operativo donde se realiza la administración y operación de los servidores cuentan con Sistemas de detección y extinción de incendios, así como Programas de mantenimiento y de supervisión a las instalaciones para verificar que no se encuentre material o condiciones que puedan provocar un incendio.

10.6 Respaldos

La información referente al software o datos con los que se ofrece y resultado del servicio de la Autoridad Certificadora Cecoban, son respaldados y resguardados en un sistema para la administración de respaldos que se ubica dentro de un Centro de Datos de Cecoban.

La Autoridad Certificadora Cecoban realizará los respaldos de información de acuerdo al procedimiento enunciado en el numeral 10.8.3 Registro y Respaldos de Información.

10.7 Controles del personal

10.7.1 Perfil del personal responsable de la Autoridad Certificadora Cecoban.

El personal responsable de la Autoridad Certificadora Cecoban, cuenta con el nivel de conocimientos necesarios e indispensables para administrar y mantener en óptimas condiciones la infraestructura de hardware y software mediante los cuales se proporciona el servicio de certificación. Adicionalmente el personal debe cumplir con los perfiles profesionales, certificaciones y experiencia que establece la misma Secretaría de Economía.

10.7.2 Procedimiento de contratación del personal.

El área de Recursos Humanos de Cecoban, S. A. de C. V. verifica los antecedentes y conocimientos del personal que se contrata para efectos de la administración y mantenimiento de la infraestructura de hardware y software destinado para el servicio de certificación y cuenta para ello con un procedimiento

para reclutar, seleccionar, evaluar y contratar al personal de acuerdo a lo que establece la misma Secretaría de Economía.

Así mismo Cecoban suscribe un contrato de confidencialidad con el personal que tiene acceso a información clasificada como confidencial.

10.7.3 Requerimientos de capacitación

El personal asignado a la administración y mantenimiento de la infraestructura de hardware y software destinado para el servicio de certificación de la Autoridad Certificadora Cecoban, participa activamente en un proceso continuo de capacitación y actualización de nuevas tecnologías, además que se les proporciona cursos para mantenerse actualizados en las certificaciones que establece la Secretaría de Economía.

10.7.4 Sanciones por Acciones no autorizadas.

Las sanciones podrán ser desde una amonestación administrativa hasta rescindir el contrato laboral y en su caso las acciones legales que correspondan

10.7.5 Documentación de la Autoridad Certificadora Cecoban

Además del Manual de Política de Certificación y la Declaración de Prácticas de Certificación que se publican en el sitio de Internet de Cecoban, la Autoridad Certificadora Cecoban cuenta con los manuales y procedimientos que establece la Secretaría de Economía en las “Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación” y cuyo objetivo es garantizar la seguridad y continuidad en la prestación de los servicios.

10.8 Controles Administrativos

10.8.1 Funciones de Confianza

De acuerdo a lo que establece la Secretaría de Economía el prestador de servicios de Certificación debe contar al menos con las siguientes figuras:

- ✓ Un profesional informático,
- ✓ Un profesional jurídico,

Y como auxiliar del profesional informático

- Un Oficial de Seguridad
- Un Administrador de Sistemas
- Un Operador de Sistemas

- Un Administrador de Base de Datos y
- Un Administrador de Redes

El personal a quien se asigna estos roles de confianza, de acuerdo a lo establecido por la Secretaría de Economía, cuenta con el conocimiento, experiencia y certificaciones necesarias que garantizan el cumplimiento eficiente de los requerimientos de seguridad para desempeñar estos roles.

10.8.2 Auditorías de Seguridad

Cecoban realiza de forma periódica evaluaciones de seguridad informática, tanto por personal interno como externo, que permitan:

- Identificar las posibles vulnerabilidades inmersas en las tecnologías de información y establecer las acciones necesarias para eliminarlas o mitigarlas.
- Detectar oportunidades de mejora en la seguridad informática.

10.8.3 Registro y respaldos de información

10.8.3.1 Tipos de Eventos registrados

La Autoridad Certificadora Cecoban, llevará un registro de los eventos ocurridos durante el servicio de expedición de Certificados Digitales, revocación de Certificados Digitales y actualización de la CRL que permitan mantener el servicio de consulta del estado de Certificados Digitales. Estos registros incluyen los correspondientes a la actividad de los usuarios del sistema de la Autoridad Certificadora Cecoban.

Se realizan respaldos diarios de los registros indicados en el párrafo anterior.

Los respaldos se resguardan en un lugar seguro y se protegen con un control de acceso exclusivo a personal autorizado.

Toda la información recibida de los Solicitantes de un Certificado Digital se resguardará en un lugar seguro protegido con los elementos de seguridad indicados en los numerales 10.8.4 y 11.12.

10.8.3.2 Período de Almacenamiento y Respaldo

Los Certificados Digitales emitidos por la Autoridad Certificadora Cecoban así como la información asociada a estos se resguardarán por un periodo mínimo de 10 años; no obstante, la Autoridad Certificadora Cecoban podrá extender dicho periodo cuando así sea requerido por sus clientes o por una disposición expresa de alguna autoridad competente.

10.8.3.3 Protección de la Información

La información resultante de la operación normal de la Autoridad Certificadora Cecoban y la proporcionada por los usuarios de los servicios y por los Titulares de los Certificados Digitales emitidos por ésta, será almacenada en los medios que la Autoridad Certificadora Cecoban garantice razonablemente su integridad y disponibilidad para su posterior consulta.

Los respaldos y la protección de esa información se realizarán en lugares seguros bajo la custodia apropiada y sólo tendrá acceso a éstos el personal autorizado.

10.8.3.4 Resguardo de información

La Autoridad Certificadora Cecoban resguarda la información asociada a los Certificados Digitales respecto de su expedición, revocación o expiración, así como la información recibida de los Solicitantes de Certificados Digitales.

Los registros correspondientes incluirán toda la evidencia relevante y disponible para la Autoridad Certificadora relacionada con:

A. La obtención de certificados;
B. El intercambio con otras Autoridades Certificadoras;
C. Las peticiones de revocación hechas por una autoridad competente;
D. Las peticiones de revocación hechas por los Titulares de los certificados;
E. Los registros que para efectos de auditoría y/o por disposición legal se deban conservar.

La Autoridad Registradora conservará la documentación recibida por el solicitante (expediente) por lo menos 10 años a partir de la fecha de expedición del certificado por parte de la AC Cecoban y en caso de dejar de operar como AR enviará los documentos físicos a la AC Cecoban .

10.8.4 Seguridad y Confidencialidad de la información.

Cecoban en su calidad de Autoridad Certificadora emplea todos los medios necesarios que garantizan razonablemente la seguridad de los datos personales obtenidos de los Solicitantes o Titulares de Certificados Digitales.

Sólo el personal acreditado como Autoridad Registradora tendrá acceso a los datos personales que hayan recibido para tramitar la expedición del Certificado Digital a la AC.

El cumplimiento de las normas y políticas de seguridad por parte del personal que funge como Autoridad Registradora se controlan y se comprueba periódicamente a través de auditorías de operación.

La documentación recibida de los Solicitantes durante el proceso de registro para la expedición de Certificados Digitales se resguardará en archiveros provistos con chapa, dentro de un área de acceso restringido, con la finalidad de mantener su integridad y confidencialidad.

La Autoridades Registradoras que realice solicitudes de Certificados Digitales a la AC fuera de oficina y en caso de extravío de documentación del Cliente, deberán volver a obtener dicha documentación en un lapso de tres días y en caso de no obtenerla en ese plazo se procederá a revocar el Certificado Digital correspondiente, ya que se quedaría sin sustento la expedición.

Los datos que envía una Autoridad Registradora a la AC Cecoban durante el proceso de registro y expedición de Certificados Digitales son a través de canales seguros (información cifrada) con la finalidad de mantener su integridad y confidencialidad y haciendo uso de su firma electrónica para mantener registro de las operaciones.

Las Autoridades Registradoras serán autenticadas por la AC Cecoban por medio de Certificados Digitales, previa autorización y configuración en el sistema para fungir como tales.

10.8.5 Recuperación en Caso de Desastre

10.8.5.1 Recuperación ante desastres

- Se cuenta con un “Plan de Continuidad de Negocio y Recuperación ante desastres”, que contempla los elementos tecnológicos, humanos y de organización para garantizar que aún en casos de contingencia, se esté listo para actuar y continuar con los procesos en un tiempo de respuesta que minimiza los impactos para sus clientes.

10.8.5.2 Recuperación de Hardware, Software y Datos

- En caso de daños en el hardware o software que da servicio a la Autoridad Certificadora Cecoban, se cuenta con equipo redundante en un segundo Centro de Datos, para continuar ofreciendo el servicio.
- En caso de daños en los datos del servicio de la Autoridad Certificadora Cecoban, se cuenta con replicación periódica entre los equipos ubicados en los Centro de Datos; además de mantener respaldos de información de acuerdo a lo establecido en el Manual para la administración de respaldos de Cecoban.
- La clave privada de la Autoridad Certificadora Cecoban está en todo momento cifrada y almacenada permanentemente en dos módulos criptográficos FIPS 140 nivel 3, ubicados en los Centros de Datos de Cecoban.

11. CONTROLES DE SEGURIDAD TÉCNICOS

11.1 Generación e instalación del par de claves de la AC

El par de claves de la Autoridad Certificadora Cecoban serán generadas utilizando los sistemas de Cecoban de acuerdo al "Plan de Administración de Claves".

La clave privada estará en todo momento cifrada y almacenada en el módulo criptográfico el cual cumple con la norma FIPS 140 nivel 3.

11.2 Entrega de la Clave Pública de Titulares

La Autoridad Certificadora Cecoban hace entrega de los Certificados Digitales a sus Titulares quienes tienen la libertad de proporcionarlos a quienes ellos consideren conveniente. Adicionalmente, los Titulares y Terceros que Confían pueden descargar dichos Certificados del sitio de Internet http://www.cecoban.org.mx así como consultar el estado de los Certificados a través del mismo sitio.

11.3 Tamaño de claves de la AC Cecoban y Titulares

El par de Claves criptográficas de la Autoridad Certificadora Cecoban, tendrá una longitud de 2048 bits, y el par de Claves criptográficas de los Certificados Digitales emitidos por ésta, tendrán una longitud de 1024 bits de acuerdo a lo que establece la Secretaría de Economía.

11.4 Software y hardware utilizado para la generación de las Claves de la AC Cecoban y Solicitantes / Titulares de Certificados Digitales.

El software y el hardware utilizado para la generación de las Claves de la Autoridad Certificadora Cecoban corresponden a un sistema criptográfico el cual cumple con el estándar FIPS 140 nivel 3 de acuerdo a lo que establece la Secretaría de Economía.

Por otra parte la AC Cecoban a través de su sitio de internet http://www.cecoban.org.mx tiene disponible la aplicación (software) para que los solicitantes de Certificados Digitales generen bajo su total control su par de claves.

11.5 Protección de los Datos de Creación de Firma Electrónica de la Autoridad Certificadora Cecoban y seguridad del módulo criptográfico.

Los Datos de Creación de Firma Electrónica está en todo momento cifrada y almacenada en un módulo criptográfico que cumple con el (**Federal Information Processing Standard)** FIPS 140 nivel 3.

De acuerdo a lo indicado en el punto anterior los módulos criptográficos en los que se salvaguardan los Datos de Creación de Firma Electrónica de la Autoridad Certificadora Cecoban cumple con el estándar FIPS 140 nivel 3, el cual es un estándar de seguridad informática desarrollado por el gobierno de los Estados Unidos de América que estableció la Secretaría de Economía como necesario para funcionar como Prestador de Servicios de Certificación.

11.6 Medida de seguridad para habilitar el uso de los Datos de Creación de Firma Electrónica de la Autoridad Certificadora Cecoban

La Autoridad Certificadora Cecoban ha implementado una configuración en el módulo criptográfico para el uso de sus Datos de Creación de Firma Electrónica, el cual determina que para poder activar el uso de dichos datos, debe ser de forma mancomunada de acuerdo al Plan de Administración de Claves de la AC Cecoban.

11.7 Resguardo de los Datos de Creación de Firma Electrónica de la AC Cecoban

Los Datos de Creación de Firma Electrónica se encuentran salvaguardados en módulos criptográficos que cumple con el FIPS 140 nivel 3 alojados en los servidores asignados para las funciones de la Autoridad Certificadora en los dos Centros de Datos y un tercer respaldo resguardado en caja fuerte.

11.8 Control de Copias de la Clave Privada de la AC Cecoban

La Autoridad Certificadora cuenta con un Plan de Administración de Claves y con un Sistema que cumple con el FIPS 140 nivel 3 que establece y permite respectivamente que para la generación de copias de las claves de la AC Cecoban se requiera de la intervención mancomunada de personal de Confianza de la misma.

11.9 Protección de datos de activación de la clave privada de la AC Cecoban

Los datos de activación de la clave privada de la AC Cecoban se encuentran distribuidos de forma mancomunada de manera tal que al menos deben estar presentes tres facultados para la activación de la Autoridad Certificadora Cecoban. Por lo anterior los datos de activación de la clave privada de la AC Cecoban pertenecen y están bajo custodia del personal facultado para tal fin.

Para activar la clave privada de la Autoridad Certificadora Cecoban, deberán estar presentes al menos tres de los responsables de la misma de acuerdo a lo establecido en el “Plan de Administración de Claves” de Cecoban para administrar la clave privada de la AC Cecoban.

11.10 Método de destrucción de la Clave Privada de la AC Cecoban

En caso de que se considere que los Datos de Creación de Firma Electrónica de la Autoridad Certificadora se encuentran comprometidos o en algún otro caso que se requiera el cese de operaciones de ésta, se cuenta con un procedimiento para inicializar los módulos criptográficos donde se encuentran en salvaguarda de manera que no puedan volver a ser obtenidos por ningún método hasta ahora conocido.

11.11 Medida de seguridad para habilitar el uso de los Datos de Creación de Firma Electrónica de la Autoridad Registradora Cecoban

La Autoridad Certificadora Cecoban ha establecido que una AR debe resguardar su clave privada dentro de un dispositivo seguro compatible con el estándar FIPS 140 nivel 3, lo cual permite asegurar que sólo el poseedor de dicho dispositivo podrá acceder a los Datos de Creación de Firma Electrónica siempre y cuando conozca la clave de acceso a dichos datos.

11.12 Resguardo de los Datos de Creación de Firma Electrónica de la AR Cecoban

Los Datos de Creación de Firma Electrónica se encuentran salvaguardados por el personal que opera como Autoridad Registradora dentro de un dispositivo seguro compatible con el estándar FIPS 140 nivel 3.

11.13 Control de Copias de la Clave Privada de la AR Cecoban

La clave privada de una AR se encuentra dentro de un dispositivo seguro compatible con FIPS 140 nivel 3, el cual no permite que se obtenga una copia de dicha clave privada.

11.14 Protección de datos de activación de la clave privada de la AR Cecoban

Los datos de activación de la clave privada de una AR corresponden a la clave de acceso a dicha clave la cual debe ser conocida únicamente por la misma AR.

11.15 Método de destrucción de la Clave Privada de la AR Cecoban

La AR Cecoban, no podrá destruir la clave privada, sin embargo, ésta dejará de ser válida a través de la revocación del Certificado Digital asociado a dicha clave privada una vez transcurrida su fecha de vencimiento.

11.16 Administración de las Claves Públicas de la Autoridad Certificadora Cecoban y Titulares

11.16.1 Resguardo de Claves Públicas de Titulares de Certificado y de la AC Cecoban

Las Claves públicas serán almacenadas con sus respaldos correspondientes con los elementos de seguridad físicos y lógicos que permiten salvaguardar la integridad y disponibilidad de los Certificados Digitales emitidos, así como los datos del estado en que se encuentran los mismos.

Las Claves de la AC Cecoban se resguardan en dispositivos que cumplen con el FIPS 140 nivel 3.

11.16.2 Tiempo de validez del par de Claves de Titulares de Certificados y de la AC Cecoban

El Certificado Digital de Usuario tendrá un tiempo de validez de 2 años a partir de la fecha que se emita, de acuerdo a la fracción I, del artículo 109, del Código de comercio.

El tiempo de validez del par de claves se dará por terminado cuando se concluya la vigencia indicada en el mismo certificado o cuando por alguna razón sea revocado.

El Certificado de la Autoridad Certificadora Cecoban tendrá una vigencia de 10 años a partir de la fecha que se emita, lo anterior de conformidad con lo establecido en el artículo 11 Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación.

11.16.3 Procedimiento en caso de comprometerse la Clave Privada de la AC Cecoban

En caso de que la clave privada de la Autoridad Certificadora Cecoban se viese comprometida, se solicitará la revocación inmediata ante la Autoridad Certificadora Raíz de la Secretaría de Economía y se ejecutarán en tiempo y forma las acciones que establezca la Secretaría de Economía en su respuesta a dicha solicitud.

11.16.4 Controles de Seguridad en los sistemas de cómputo y en red

En Cecoban se han implementado diversaselementos de control con el objetivo de proporcionar acceso a la información sólo al personal autorizado y que de acuerdo a sus funciones tiene “necesidad de conocerla” asignando en todos los casos el “mínimo privilegio necesario” para el desempeño de sus funciones.

Los elementos de control corresponden en esencia a funciones de seguridad que se habilitan en los sistemas operativos de los sistemas de cómputo y comunicaciones y por medio de aplicaciones especiales de seguridad informática como son firewalls, detectores de intrusos, antivirus, etc. Estos

elementos además de permitir un acceso controlado permiten prohibir el acceso o intento de acceso a la información o a los servicios que no han sido explícitamente autorizados.

11.17 Elementos de Seguridad en las instalaciones de una Autoridad Registradora

1. Las Autoridades Registradoras que operan en las Oficinas Corporativas de Cecoban se ubican en un área de acceso controlado a través de dispositivos biométricos vigilada por personal las 24 horas de los 365 días del año, con Circuito Cerrado de Televisión (CCTV), elementos de prevención, detección y extinción de incendios e infraestructura eléctrica, de cómputo y comunicaciones.

2. Las oficinas donde se resguardan los documentos y/o realicen sus operaciones otras Autoridades Registradoras autorizadas por la AC Cecoban, deberán ubicarse en oficinas de trabajo dentro de un área con seguridad física perimetral, Circuito Cerrado de Televisión (CCTV), elementos de prevención y extinción de incendios; adicionalmente deben contar con al menos archiveros con chapa y llave para el resguardo de documentos que reciban de los Solicitantes y Titulares para el trámite de un Certificado Digital.

3. Cuando las Autoridades Registradoras realicen el trámite de expedición de Certificados Digitales a la AC desde cualquier punto de la República Mexicana, deberán resguardar la documentación recibida del Solicitante/Titular en sus oficinas de trabajo, las cuales deberán apegarse a las características descritas anteriormente.

11.18 Seguridad en la Operación de las Autoridades Registradoras

1. Las Autoridades Registradoras deberán apegarse en todo momento a lo establecido en este documento, en el Manual de Operación de Ac y AR Cecoban, en el Manual de Políticas de Certificación y el contrato de prestación de servicios.

2. La AC Cecoban publicará en su sitio de internet los datos de las Autoridades Registradoras autorizadas, así como las que por algún motivo hayan causado baja. Lo anterior para que los Solicitantes del servicio realicen su trámite sólo con autoridades autorizadas.

3. Con independencia del lugar de las Oficinas de Trabajo de las Autoridades Registradoras, éstas deberán enviar al Profesional Jurídico de la AC Cecoban, en calidad de respaldo (el cual será por cada **expedición** que se realice), la imagen legible correspondiente a la documentación recibida del Solicitante/Titular de Certificado Digital de acuerdo a lo que le establece la AC Cecoban en su Declaración de Prácticas de Certificación. Las imágenes deberán ser enviadas en un lapso no mayor de 1 día hábil posterior a la **expedición** del Certificado Digital.

4. Las Autoridades Registradoras deben tener las solicitudes de expedición y revocación con la documentación que sustente sus operaciones, mismas que la AC Cecoban mantiene registradas en sus sistemas.

5. En caso de pérdida de información, la AR Cecoban deberá levantar un acta ante el Ministerio Público correspondiente en el mismo día del suceso y realizar las gestiones necesarias para reponer la documentación en un periodo máximo de 3 días hábiles.

6. La Autoridades Registradoras que realice solicitudes de Certificados Digitales a la AC fuera de oficina y en caso de extravío de documentación del Cliente, deberán informarlo inmediatamente al cliente y obtener nuevamente dicha documentación en un lapso de 3 días y en caso de no obtenerla en ese plazo se procederá a revocar el Certificado Digital correspondiente, ya que se quedaría sin sustento la expedición.

7. Las Autoridades Registradoras harán uso de sus Datos de Creación de Firma Electrónica para firmar y mantener evidencia de las operaciones de solicitud de expedición y revocación de Certificados Digitales que tramite ante la AC Cecoban, y ésta expedirá los Certificados y ejecutará la revocación de los mismos en respuesta.

8. La AC Cecoban habilitará para las Autoridades Registradoras dispositivos compatibles con FIPS 140 nivel 3 para resguardar y operar sus claves privadas.

9. Los elementos de seguridad con los que debe contar el equipo de trabajo de una AR Cecoban para operar en la AC Cecoban son:
    - Certificado Digital
    - Browser que soporte el cifrado del SSL de 128 bits
    - Componente ActiveX de firma

Además de estos elementos se debe considerar lo descrito en el numeral 8.2.3

11.19 Tiempo de validez del par de Claves de la AR Cecoban

El Certificado Digital de AR Cecoban tendrá un tiempo de validez de 2 años a partir de la fecha que se emita.

El tiempo de validez del par de claves se dará por terminado cuando se concluya la vigencia indicada en el mismo certificado o cuando por alguna razón sea revocado por la AC Cecoban.

12. ESTRUCTURA DE CERTIFICADOS Y CRL

12.1 Certificados

Con el propósito de mantener la interoperabilidad de los Certificados Digitales con productos y servicios relacionados con Firma Electrónica, la Autoridad Certificadora Cecoban emitirá las claves públicas de acuerdo con el RFC 3280 Internet x.509 Public Key Infraestructure Certificate and Certificate Revocation List (CRL) Profile.

Los certificados emitidos por la Autoridad Certificadora Cecoban contendrán al menos los siguientes campos:

• La indicación de que se expiden como tales;
• El código de identificación único del Certificado;
• La identificación del Prestador de Servicios de Certificación que expide el Certificado, razón social, su domicilio, dirección de correo electrónico, en su caso, y los datos de acreditación ante la Secretaría;
• Nombre del Titular del Certificado;
• Periodo de vigencia del Certificado;
• La fecha y hora de la expedición del Certificado;
• El alcance de las responsabilidades que asume el Prestador de Servicios de Certificación.
• La referencia de la tecnología empleada para la creación de la Firma Electrónica.

12.1.1 Versión del Certificado

Los Certificados Digitales emitidos por la Autoridad Certificadora Cecoban deberán cumplir con el estándar X.509 versión 3.

12.1.2 Extensiones del Certificado

Las extensiones de los certificados digitales serán fijadas por la Autoridad Certificadora Cecoban de acuerdo al RFC 3280 según el tipo de certificado. Entre las extensiones que se pueden incluir en un Certificado se encuentran las siguientes:

- Authority Key Identifier
- Subject Key Identifier.
- Key Usage
- Basic Constraints
- Extended Key Usage
- CRL Distribution Points
- Authority Info Access.
- Certificate Policies

La extensión Key Usage define el propósito que tendrá la clave contenida dentro del Certificado Digital, a continuación, se muestra diferentes valores que podrá contener:

Valor	✓ Firma digital (digitalSignature) ✓ No repudiación. (nonRepudiation) ✓ Encripción de Claves (keyEncipherment) ✓ Encripción de Datos (dataEncipherment) ✓ Firma de CRL (cRLSign) ✓ Negociación de Claves (keyAgreement)

|

12.2 Perfil de la CRL

12.2.1 Número de versión

La Autoridad Certificadora Cecoban emite su "Lista de Certificados Revocados (CRL)" de acuerdo con el RFC 3280 Internet X.509 Public Key Infraestructure Certificate Revocation List (CRL) Profile.

12.2.2 Estructura de la Lista de Certificados Revocados

La estructura de la Lista de Certificados Revocados (CRL) de Cecoban, se basa en el estándar RFC 3280, mismo que es utilizado por la Secretaría de Economía como a continuación se detalla:

- Número de serie de los Certificados Digitales revocados por el emisor con fecha y hora de revocación.
- La identificación del algoritmo de firma utilizado
- El nombre del emisor.
- La fecha y hora en que fue emitida la Lista de Certificados Revocados.
- La fecha en que emitirá la próxima Lista de Certificados Revocados que no podrá exceder de veinticuatro horas, con independencia de mantener el Protocolo de Estatus de Certificados en Línea (OCSP)
- La Lista de Certificados Revocados deberá ser firmada por el Prestador de Servicios de Certificación que la haya emitido, con sus Datos de Creación de Firma.

12.2.3 Extensiones OCSP

Los Certificados Digitales emitidos por la AC Cecoban deben incluir la extensión OCSP que contenga la dirección electrónica a la cual se podrá consultar el estado de los Certificados Digitales.

13. AUDITORÍAS

13.1 Frecuencia y tipos de Auditorias

13.1.1 Auditorías a la AC Cecoban

En la AC Cecoban se realizan evaluaciones conforme a lo siguiente:

a) Evaluaciones internas de cumplimiento a los procedimientos de las áreas operativas, de tecnología de información y comunicaciones y administrativas, las cuales se realizan una vez al año.

b) Análisis de seguridad y de Pruebas de Penetración al menos una vez al año, realizados a la infraestructura de cómputo y comunicaciones con personal de Seguridad Informática de Cecoban.

c) Análisis de seguridad y de Pruebas de Penetración anuales, realizados a la infraestructura de cómputo y comunicaciones con proveedores especializados en seguridad informática.

13.1.2 Auditorías a Autoridades Registradoras.

La Autoridad Certificadora Cecoban realizará auditorías a las Autoridades Registradoras conforme a lo siguiente:

a) Se auditará el cumplimiento con las Políticas de Certificación, Declaración de Prácticas y Manual de Operación.

b) Se verificará el cumplimiento a lo estipulado en el Contrato en donde se ratifican las obligaciones y responsabilidades de las partes.

13.2 Áreas de auditoría interna

Cecoban cuenta con áreas de Cumplimiento y Seguridad para llevar a cabo las funciones de evaluación a los procesos de negocio, a las tecnologías de información y comunicación y a la seguridad en toda la organización. Para el caso de seguridad; se cuenta con el perfil, competencias y conocimientos de un Oficial de Seguridad conforme lo requerido por la Secretaría de Economía necesarios para desempeñar la función.

13.3 Relación de la entidad que evalúa con la AC y la AR

Las áreas de Cumplimiento y Seguridad son independientes a las de Operación y Tecnologías de Información y Comunicaciones de la AC y AR´s.

13.4 Acciones a desarrollar en caso de la detección de deficiencias

Se tiene establecido en procedimiento que los hallazgos de las revisiones de cumplimiento internas, auditorías externas, assessments internos y externos sean atendidos por cada uno de los responsables en tiempo y forma, y que el personal de Cumplimiento y Seguridad da seguimiento y evalúa dicho cumplimiento.

13.5 Comunicación de los resultados

Conforme al procedimiento establecido, el informe de resultados de hallazgos se revisa en primera instancia con los responsables de los procesos o funciones revisadas para establecer acuerdos para su cumplimiento y posteriormente se presenta el informe de resultados finales a la administración de Cecoban; así también, de los reportes de avances y cumplimiento.

14. REFERENCIAS

- ✓ RFC 3647 – Internet X.509 Public Key Infrastructure Certificate Policy and Prectices Framework, noviembre 2003.
- ✓ RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile abril 2002.
- ✓ REGLAMENTO del Código de Comercio en Materia de Prestadores de Servicios de Certificación, Publicado el 19 de julio de 2004 en el Diario Oficial de la Federación.
- ✓ REGLAS generales a las que deberán sujetarse los prestadores de servicios de certificación. Publicadas el 10 de Agosto de 2004, en el Diario Oficial de la Federación.

NOTA: El presente documento entrará en vigor a partir de 9 de septiembre del 2008 conforme a lo establecido en la publicación del Diario Oficial de la Federación (DOF) del 8 de septiembre de 2008 respecto de la autorización de CECOBAN como Prestador de Servicios de Certificación para la Emisión de Certificados Digitales