DECLARACIÓN DE PRÁCTICAS DE CERTIFIACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DE LA SECRETARÍA DE ECONOMÍA

VERSIÓN 1.01
Fecha: 12-2005
OID: en proceso

1. INTRODUCCIÓN

En la actualidad los conceptos ***clave pública*** y ***clave privada,*** se escuchan frecuentemente alrededor del ambiente de los usuarios de Internet, en particular, en aquellos usuarios que requieren efectuar transacciones comerciales mediante el uso del correo electrónico, con un nivel confiable de seguridad que les ofrezca confidencialidad, integridad, autenticación y no repudio, en este documento se describen las reglas y procedimientos que deberán permitirle a dichos usuarios, confiar en los servicios ofrecidos por las Autoridades Certificadoras para realizar sus transacciones seguras mediante el uso de la Clave Pública y la Clave Privada, este documento se encuentra apoyado en estándares internacionales como el RFC 3647.

1.1 Propósito

Describir la Declaración de Prácticas de Certificación para la Autoridad Certificadora Raíz de la Secretaría de Economía (ACR-SE), dentro de la Infraestructura de Clave Pública (PKI) de la Dirección General de Normatividad Mercantil (DGNM).

La Autoridad Certificadora Raíz de la Secretaría de Economía, a través de la Dirección General de Normatividad Mercantil (DGNM), certificará las claves públicas de las Autoridades Certificadoras y demás entidades que hallan sido acreditadas por la DGNM y los servidores públicos que así lo requieran, dentro de la infraestructura de ésta.

Más información referente de la ACR-SE en:

http://ac.economia.gob.mx
http://www.economia.gob.mx
http://www.firmadigital.gob.mx

1.2 Identificación

Este documento es denominado como **"Declaración de Prácticas de Certificación de la Autoridad Certificadora Raíz de la Secretaría de Economía"**. Esta versión podrá consultarla en la dirección siguiente:

http://ac.economia.gob.mx
http://www.firmadigital.gob.mx

Por el momento no se cuenta con el OID.

1.3 Comunidad y aplicabilidad

La comunidad que comprende a la ACR-SE, son fedatarios públicos, registradores, Unidades Administrativas de la SE, funcionarios públicos y particulares que realicen trámites ante la Secretaría de Economía.
Su ámbito o aplicabilidad principal de los certificados es el desarrollo del comercio electrónico, así como para realizar cualquier trámite ante la Secretaría de Economía y otras entidades similares.

1.3.1 Autoridad Certificadora

La Autoridad Certificadora Raíz de la Secretaría de Economía es una entidad cuyo propósito es la emisión y/o revocación de certificados de Autoridades Certificadoras subordinadas, para tal efecto la responsable de dicha entidad es la Dirección General de Normatividad Mercantil.

1.3.2 Autoridad Registradora

La Autoridad Registradora (RA), la cual forma parte de la ACR-SE, será la encargada de la autenticación e identificación de las entidades o usuarios finales, verificar la

identidad del solicitante del certificado a favor de éste y de llevar acabo el procedimiento para la emisión y/o revocación de certificados.

1.3.3 Entidades o usuarios finales

La Autoridad Certificadora de la Dirección General de Normatividad Mercantil.

- Ésta a su vez podrá certificar las clave públicas de autoridades certificadoras para Instituciones Públicas Gubernamentales desconcentradas o descentralizadas de la SE; para entidades de la SE; de identidad personal (CDIP) para funcionarios públicos de la SE y para los particulares que realicen trámites ante esta Secretaría.

La Autoridad Certificadora del Sistema de Gestión Registral.

- Ésta a su vez podrá certificar las claves públicas de los Registros Públicos de Comercio (RPC), fedatarios públicos y a sus respectivos agentes certificadores del SIGER.

Las Autoridades Certificadoras de los Prestadores de Servicios de Certificación acreditados por la DGNM.

- Éstos podrán certificar las claves públicas de identidad personal (CDIP) de personas físicas o morales para efectos comerciales y a sus respectivos agentes certificadores, entre otros.

Servidores ubicados en el área de Autoridades Certificadoras.

Agentes Certificadores

- Auxiliares en la emisión de certificados y/o revocaciones.

1.4 Contacto

En la Dirección General de Normatividad Mercantil, podrá enviar sus comentarios, dudas u observaciones referentes a esta Declaración de Practicas de certificación.

Ubicación:
Insurgentes Sur #1940, 1er. Piso, Del. Álvaro Obregón
C.P. 01030, México, D.F.
Correo electrónico de la ACR-SE: acrse@economia.gob.mx
Teléfono (+52) (55) 52.29.61.00 ext. 33533
Fax : 52.29.91.00 ext. 33599

Información sobre la Infraestructura de Clave Pública de la ACR-SE:
http://ac.economia.gob.mx.
http://www.firmadigital.gob.mx

2. OBLIGACIONES Y RESPONSABILIDADES

2.1 Obligaciones

2.1.1 Obligaciones de la ACR-SE

- Ofrecer un servicio constante mediante la infraestructura requerida de un PKI, manteniendo los requerimientos de seguridad necesarios para proteger las claves privadas de las autoridades certificadoras y la misma ACR-SE.
- Respaldar y mantener los certificados emitidos y revocados en un sitio de alta disponibilidad para que la parte que confía o cualquier interesado en transigir con dichos certificados, pueda consultar el estatus de los mismos. Para tal efecto, se mantendrá actualizada dicha información en las páginas Web destinadas a la ACR-SE en (http://ac.economia.gob.mx/acrse)
- Emitir o revocar los certificados de acuerdo con lo establecido en este documento, así como de actualizar y publicar la Lista de Certificados Revocados.
- En caso de compromiso de la clave privada de la ACR-SE, notificar, a las entidades o usuarios de la ACR-SE, para que no se emita ningún certificado, hasta que no se restaure la nueva clave privada de la ACR-SE. De conformidad con lo establecido en este documento.

2.1.2 Obligaciones de la RA-SE

- Atender las solicitudes, aprobar o denegar dichas solicitudes promovidas por las entidades que pretenden ser autoridades certificadoras o usuarios de la ACR-SE.
- Cumplir con los procedimientos que le competen en la emisión de certificados por parte de la ACR-SE, de acuerdo con el numeral 4 de este documento.
- Realizará la identificación y autentificación para determinar su emisión o revocación de certificados, de conformidad con el numeral 3.1.2 de este documento, según sea el caso.
- Realizará la carga de las solicitudes de certificados y revocaciones válidas en el sistema.
- Proteger los datos personales de los solicitantes, que no podrán ser cedidos a terceros bajo ningún concepto (Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental).
- Atenderá las solicitudes, de las entidades referidas en el numeral 1.3 de este documento ..

2.1.3 Obligaciones de entidades

- Mantener en todo momento protegida su clave privada con un nivel de seguridad adecuado, para las autoridades certificadoras subordinadas tendrá que ser de acuerdo con la seguridad establecida para la ACR-SE.
- Notificar a la Autoridad Registradora de la ACR-SE, su solicitud de revocación de su certificado o cualquier sospecha de compromiso de sus claves, en su caso.
- Las entidades certificadas por la ACR-SE, debe conocer y aceptar esta CPS, y sus responsabilidades de conformidad con el numeral 2.2 de este documento.
- Informar a las partes que confíen en certificados firmados por la ACR-SE, que tienen la obligación de verificar su valides o el estado que guardan éstos cada vez que vayan a ser utilizados, verificar que no halla expirado y que aparezca en la Lista de Certificados Revocados de la ACR-SE.

2.1.4 Obligaciones de repositorio

- La ACR-SE publicará su certificado, su CRL y los certificados firmados por ésta, en el Web destinada al servicio de la Autoridad Certificadora ACR-SE (http://ac.economia.gob.mx). Ésta publicación se realizará como máximo 2 horas después de la emisión y firma de los certificados, en caso de revocación de algún certificado la CRL se publicará en el menor tiempo posible.
- Permitir consultar esta información en las páginas Web destinadas al servicio de la ACR-SE.
- Mantendrá un respaldo de los certificados emitido por las autoridades certificadoras subordinadas.

2.2 Responsabilidades

2.2.1 Responsabilidades de la ACR-SE

- La correcta emisión de los certificados y de los posibles errores surgidos del sistema durante los procedimientos de generación y revocación de certificados.
- Los problemas derivados del compromiso de la clave privada de la ACR-SE y la notificación de la revocación de la misma.
- Revocar cualquier certificado en cuanto le sea notificado o se detecte algún incumplimiento de los requisitos establecidos en el marco jurídico aplicable en la materia a los PSC, compromiso o mal uso del mismo.
- Proteger la clave privada de la ACR-SE, mediante el uso de un modulo criptográfico que por lo menos cumpla con el estándar FIPS 140-2 nivel 3.
- La DGNM, como administrador de la ACR-SE, garantiza el cumplimiento de las obligaciones descritas en este documento.

2.2.2 Responsabilidades de la RA-SE

- Verificar que cuenten con lo requisitos establecidos en la normatividad aplicable.
- Es responsabilidad de la RA-SE, la identificación y autenticación de los solicitantes, para poder emitir su certificado o revocarlo según sea el caso.

2.2.3 Responsabilidades de las Autoridades Certificadoras subordinadas y los usuarios

- El compromiso de su clave privada, como pérdida, uso indebido etc.
- Los PSC deberán cumplir con el marco jurídico en lo referente a las responsabilidades de PSC conformado por el CoCo, RPSC y RGPSC.
- Problemas surgidos durante notificación de una emisión o revocación, de un certificado a la ACR-SE.

2.3 Cumplimiento de auditoria

Se están integrando los procedimientos con información necesaria para obtener la certificación WebTrust y BS7799.

2.4 Política de confidencialidad de la información

2.4.1 Información confidencial

- La información clasificada como confidencial será de acuerdo a la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.
- Cualquier dato de carácter personal suministrado por las entidades a la Autoridad Certificadora o Registradora de la ACR-SE.

- Material criptográfico privado asociado con la ACR-SE.
- La información derivada de una revocación de algún certificados.
- Información sobre las personas que administran la ACR-SE excepto su nombre, teléfono, correo electrónico, cargo dentro de ACR-SE e información que aparece en el propio certificado que posean.
- Registros de los eventos registrados por los sistemas de monitoreo de la red y cualquier sistema de seguridad.

2.4.2 Información no confidencial

La ACR-SE y la RA-SE manejan como información no confidencial la siguiente: Información incluida en los certificados, CRLs, CPs y CPSs, marco jurídico.

2.4.3 Causas de revocación

Se determinarán como causas de revocación las descritas el numeral 15 de las Política de Certificados (CP) de la ACR-SE, según el caso.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1 Registro

3.1.1 Tipos de nombres

La ACR-SE sólo acepta solicitudes de firma donde su DN refleje el ámbito organizacional bajo el cual se va a certificar.

Todos los nombres asociados con los certificados tienen que ser únicos.

Cada entidad debe tener un DN (*Distinguished Names*) único y claro contenido en el campo “Subject” del certificado firmado por la ACR-SE.

- El DN de los Certificados Digitales de Identidad Personal deben proporcionar los siguientes atributos:
    - C=mx
    - O= Secretaria de Economia
    - OU<DG....>
    - CN= <Nombre del usuario>
    - Email=<correo electrónico-mail del usuario>

- El DN de los Certificados Digitales de Autoridad Certificadora subordinada, deben proporcionar al menos los siguientes atributos:
    - C=mx
    - O=<empresa>
    - OU<unidad organizacional>
    - DC=<>
    - CN=<Nombre del servicio>
    - Email=<e-mail asociado al servicio>

- El DN de los Certificados Digitales de Servidor, deben proporcionar los siguientes atributos:
    - C=mx
    - O=<>
    - OU=<>
    - DC=<ACRSE>

- DN=<Nombre canónico de la máquina donde reside el servidor>
- CN=<Nombre del servidor tal y como va a ser usado>

3.1.2 Autenticación de los solicitantes de certificados a la ACR-SE

Para la Autoridad Certificadora de la Dirección General de Normatividad Mercantil.

- El solicitante del certificado para esta entidad, deberá presentar original y copia para su cotejo de una identificación oficial (Cartilla, cedula profesional, pasaporte vigente o credencial del IFE), así como una identificación institucional y un escrito en el que determine su nombre y cargo firmado por el Director General de Normatividad Mercantil, precisando su autorización para tal efecto.

Para la Autoridad Certificadora del Sistema de Gestión Registral.

- El solicitante del certificado para esta entidad, deberá presentar original y copia para su cotejo de una identificación oficial (Cartilla, cedula profesional, pasaporte vigente o credencial del IFE) así como una identificación institucional y un escrito en el que determine su nombre y cargo firmado por el Director General de Normatividad Mercantil, precisando su autorización para tal efecto.

Para Autoridades Certificadoras de los Prestadores de Servicios de Certificación acreditados por la DGNM.

- El solicitante del certificado para esta entidad, deberá presentar una identificación oficial (Cartilla, pasaporte vigente o credencial del IFE), la acreditación otorgada por la DGNM,

Para servidores ubicados en el área de autoridades certificadoras de la ACR-SE.

- El solicitante del certificado de servidor(debe ser el responsable directo del servidor), deberá presentar una identificación de la institución, un escrito en el que determine su nombre y cargo firmado por el Director General de la DGNM, indicando su autorización para tal efecto.

Identidad Personal para sus Agentes Certificadores de la ACR-SE,

- El solicitante del certificado de esta entidad, deberá presentar una identificación de la institución, un escrito en el que determine su nombre y cargo firmado por el Director General de la DGNM, indicando su autorización para tal efecto.

El personal jurídico de las Autoridades Registradora y Certificadora de la ACR-SE, serán los encargados de llevar a cabo la identificación y autenticación de los solicitantes de certificados, requiriendo en cualquier caso la presencia física del solicitante o de la persona que será el titular del certificado, para verificar que tenga coincidencia con la fotografía contenida en la identificación presentada.

3.2 Procedimientos de generación de claves

Los titulares de los certificados, serán los encargados de la generación del par de claves privada y pública, igualmente para el de la ACR-SE.

Cuando se haya superado cuatro quintos del tiempo de vida de la ACR-SE, se generará un nuevo certificado digital y en su caso una nueva identidad. A partir de ese momento, las nuevas inscripciones se harán firmando certificados con esa nueva identidad. De este modo las Autoridades Certificadoras Subordinadas dispondrán de una quinta parte del tiempo para solicitar nuevos certificados a la nueva identidad.

3.3 Generación de claves nuevas después de la revocación

Si no ha existido compromiso de la clave privada, el procedimiento de generación de claves se realizará de acuerdo a lo especificado en el párrafo anterior.
Si ha existido compromiso de clave, no se podrá firmar un nuevo certificado a partir de dicho par de claves, tendrá que volver a generar el par de claves.

3.4 Solicitud de revocación

La ACR-SE revocará cualquier clave privada que incurra alguno de los supuestos del numeral 15.1 de la Política de Certificados de la ACR-SE, o que ésta detecte que ha sido comprometida clave en cuestión.

De otra manera la solicitud de revocación será llevara a cabo de conformidad con el numeral 15.2 de la Política de Certificados de la ACR-SE, según el caso.

Para cualquiera de los casos, la autenticación se realizará según lo descrito en el numeral 3.1.2 de este documento.

4. REQUERIMIENTOS OPERACIONALES

4.1 Solicitud de certificados

ACR-SE se reserva el derecho de rechazar las solicitudes que incumplan algún requisito solicitado en el marco jurídico aplicable. Si es rechazada, la ACR-SE informará mediante oficio las razones por las que se rechaza dicha solicitud.
La ACR-SE sólo aceptar solicitudes para las entidades descritas en el numeral 3.1.2. de este documento.

4.1.1 Certificados de Agentes Certificadores de la ACR-SE

- El solicitante generará su par de claves publica y privada, previo a la solicitud de certificación de su clave pública, presentará su clave pública ante la RA de la ACR-SE, en un disco flexible de 3.5", en formato PKCS#10, junto con el oficio firmado y autorizado para tal efecto por el responsable de la ACR-SE. El usuario tendrá la obligación de conservar su clave privada en un lugar seguro.
- Es responsabilidad de la RA de la ARC-SE verificar si cumple con el procedimiento descrito en el numeral 3.1.2 de este documento, según el caso que le aplique. La RA pedirá al solicitante que firme, en su presencia, original y copia del documento de confidencialidad. posteriormente, verificará la firma autógrafa del documento de confidencialidad con la que aparece en la identificación oficial presentada.
- La RA enviará a la ACR-SE la solicitud y la clave pública en el medio electrónico para la certificación de la misma.
- LA ACR-SE hará llegar a la RA el certificado o clave pública para que le sea entregado al titular del mismo.
- Los datos y documentos proporcionados por el solicitante quedrá en custodia de la

4.1.2 Solicitud de certificados digitales de Autoridad Certificadora subordinada.

- El solicitante de un certificado digital de Autoridad Certificadora deberá ser el responsable de ésta.
- El responsable de la Autoridad Certificadora generará su par de claves pública y privada en la parte más segura de sus instalaciones. La privada quedará almacenada en su dispositivo de alta seguridad compatible con el estándar FIPS-140 nivel 3, mientras que con la pública (PKCS#10), solicitará el certificado a la

ARC-SE. De otra manera, podrá generar su par de claves en la parte más segura de sus instalaciones y autocertificará su clave pública, solicitará el certificado a la ARC-SE.

- Derivado de lo anterior, el responsable del la AC, se presentará ante la RA de la ACR-SE con su requerimiento (PKCS#10) o el certificado (en caso de autocertificación) contenido en algún medio de almacenamiento electrónico.
- Es responsabilidad de la RA de la ARC-SE verificar si cumple con el procedimiento descrito en el numeral 3.1.2 de este documento, según sea el caso, también verificar que el requerimiento (PKCS#10) o el certificado (en caso de autocertificación) cumplan con lo estipulado en el artículo 108 del CóCo.
- La RA pedirá al solicitante que muestre su acreditación y que firme, en su presencia, original y copia del documento de confidencialidad del certificado. posteriormente, la RA verificara la firma autógrafa del documento de confidencialidad con la que aparece en la identificación oficial presentada por el solicitante.
- La RA enviará a la ACR-SE la solicitud y la clave pública en el medio electrónico para la certificación de la misma.
- EL certificado será entregado al titular a más tardar en dos días hábiles después aprobada la solicitud.
- LA ACR-SE hará llegar a la RA el certificado o clave pública para que le sea entregado al titular del mismo.

4.1.3 Solicitud de certificados digitales de servidor

- El solicitante de certificado digital de Servidor será su responsable directo y deberá disponer de un certificado digital de identidad personal emitido por la ACR-SE.
- El responsable de la Autoridad Certificadora generará su par de claves pública y privada en la parte más segura de sus instalaciones. Conservando de manera segura la clave privada. Con la clave pública (PKCS#10), solicitará el certificado del servidor a la ARC-SE., mediante oficio dirigido al responsable de la ACR-SE o al oficial de seguridad, indicando en este lo siguiente: el URL del servidor, correo electrónico del contacto, tipo de certificado y en un medio de almacenamiento removible el formato PKCS#10.
- Una vez hecho esto, el solicitante de certificado se presentará ante la RA para completar el procedimiento de identificación descrito en el numeral 3.1.2, de este documento, según el caso.
- El solicitante deberá firmar, original y copia del documento de solicitud en presencia de la RA. La RA comprobará la firma autógrafa del documento de solicitud con la que aparece en la identificación oficial presentada.
- La RA enviará a la ACR-SE la solicitud y la clave pública en el medio de almacenamiento presentado por el solicitante, para la certificación de la misma.
- EL certificado será entregado al titular a más tardar en dos días hábiles después aprobada la solicitud.
- LA ACR-SE hará llegar a la RA el certificado o clave pública para que le sea entregado al titular del mismo.

4.2 Firma y entrega de certificados.

- El certificado deberá cumplir con lo establecido en el marco jurídico aplicable a PSC, utilizando las extensiones necesarias para contener la información como la URL del Psc, la URL de la secretaría, la CRL y la información requerida en el artículo 108 del

CoCo y lo aplicable en reglamento del CoCo y Reglas Generales.

- El certificado se le entregará al titular del mismo en un medio de almacenamiento removible y se le enviará una copia a su correo electrónico.
- Asimismo se tendrá un a copia de los certificados emitidos en una dirección del WEB de la ARC-SE, para que pueda obtener las copias necesarias del mismo.
- EL certificado es entregado en un disco flexible de 3.5 pulgadas de forma personal y enviado al correo electrónico del titular de éste, el titular firmará un acuse de recibido.

4.3 Revocación de certificados

Se determinarán como causas de revocación las descritas el numeral 15 de la Política de Certificados (CP) de la ACR-SE, según el caso, la puede consultar en la dirección siguiente (http://ac.economia.gob.mx/acrse/doctos).

4.4 Frecuencia de firmado de la CRL

- ACR-SE firmará una nueva CRL cada que se revoque un certificado, se llevara a cabo la actualización, incluyendo las listas anteriores.
- La entidad que confié en los certificados emitidos por la ACR-SE, tendrá la obligación de verificar su estado en la CRL.
- Para verificar los dos puntos anteriores se tendrá en línea la información el la siguiente dirección de la WEB de la ARC-SE. (http://ac.economia.gob.mx/crl/se.crl)

4.5 Procedimientos de Auditorias de Seguridad

Se están integrando los procedimientos de la información necesaria para obtener la certificación WebTrust y BS7799.

4.6 Archivo de registros

4.6.1 Tipos de eventos registrados

Se llevará un registro de los eventos ocurridos en el servicio de la ACR-SE, derivado de los procedimientos de solicitudes, emisión de certificados, revocación de certificados, actualización de la CRL entre otros que permitan mantener el servicio de consulta.

Respaldos periódicos de toda información de la ACR-SE y respaldos cada vez que se genere o revoque un certificado.

Los respaldos se resguardarán en lugar seguro y estarán protegidas criptográficamente, teniendo acceso a éstos exclusivamente personal autorizado,

Mantendrá el equipo redundante para ofrecer el servicio continuo de la ACR-SE y de consulta del WEB.

- Se conservarán registros de los accesos al WEB de la ACR-SE.
- La ACR-SE mantendrá una copia de las comunicaciones electrónicas con los usuarios de ésta.

Toda la información de los solicitantes descritos en el apartado “Alcance” de la Política de Certificados de la ACR-SE enviada en papel, medio magnético o digital, se resguardará en un lugar seguro.

4.6.2 Periodo de resguardo de la información

La información concerniente a los registros de la ACR-SE, proporcionada por los

solicitantes a prestadores de servicios de certificación, se resguardará durante 30 años en un lugar seguro posterior a su revocación, transcurrido el tiempo anterior, se valorará si requiere ser conservado más tiempo o se remitirá al Archivo General de la Nación donde se conservará cinco años más.

La información registrada pro la ACR-SE de las demás entidades se resguardará durante 5 años, posteriormente se remitirá al Archivo General de la Nación donde se conservará cinco años más

4.6.3 Protección de la información

La información que pertenece al centro de datos de la SE, es respaldada y protegida en lugares seguros bajo custodia apropiada, solo tiene acceso a ésta el personal autorizado, se cuenta con controles de acceso físicos y lógicos.

Se mantiene un respaldo del software utilizado en el servicio de la ACR-SE, para poder acceder a la información respaldada en otro sitio autorizado para tal fin.

4.6.4 Procedimientos de respaldos

Se establecerá un sistema periódico de respaldos del la información de la ACR-SE, en base a la Política de Respaldos.

4.7 Renovación de claves pública y privada de las entidades

Cuando se haya superado cuatro quintos del tiempo de vida de la Autoridad Certificadora de la ACR-SE, se generará una nueva identidad raíz. A partir de ese momento, se firmarán certificados con la nueva identidad.
Las Autoridades Certificadoras subordinadas dispondrán de una quinta parte del tiempo para solicitar nuevos certificados.
Los certificados emitidos por la ACR-SE están disponibles en la página Web en http://ac.economia.gob.mx/acrse/certificados.html.

4.8 Compromiso y recuperación de desastres

En caso de que la clave privada de la ACR-SE se viese comprometida, se llevaría a cabo el procedimiento de revocación de la misma. A partir de ese momento, quedarán revocados todos los certificados emitidos por la ACR-SE y se emitirá una CRL mostrando el estatus de revocación del certificado de la ACR-SE.

Una vez generadas las nuevas claves de la ACR-SE, se emitirán los certificados correspondientes a las Autoridades Certificadoras subordinadas, éstas a su vez deberán llevar a cabo la revocación y emisión de los nuevos certificados de sus usuarios.

En caso de compromiso de la clave privada de las Autoridades Certificadoras subordinadas, éstas tendrán el deber de notificarlo a la ACR-SE y a sus usuarios correspondientes.

4.8.1 Recuperación de hardware, software o datos

- En caso de corrupción de hardware que da el servicio de la ACR-SE, se cuenta con equipo redundante en otro sitio para continuar ofreciendo el servicio.
- En caso de corrupción de software que da el servicio de la ACR-SE, se cuenta con respaldos periódicos para poder recuperar la información necesaria, de la misma forma en caso de corrupción de la información.
- La clave privada de la ACR-SE estará en todo momento cifrada almacenada de modo permanente en el modulo criptográfico FIPS 140-2 nivel 3.

4.8.2 Recuperación ante desastres

- Se cuenta con un sitio y redundante, mediante el cual se mitigarían cualquier tipo de desastre el cual permitirá ofrecer el servicio de la ACR-SE.

5. CONTROLES DE SEGURIDAD FÍSICOS, PERSONALES Y DE PROCEDIMIENTOS

La Dirección General de Normatividad Mercantil a implementado la Política de Seguridad la que considera lo establecido en esta CPS.

5.1 Controles físicos

5.1.1 Ubicación física de la ACR-SE

El servidor que administra la ACR-SE esta ubicado en el área de Autoridades Certificadoras de la DGNM, es el área más segura de la PKI de la Secretaría de Economía ubicada en la Dirección General de Normatividad Mercantil.

5.1.2 Acceso físico a la ACR-SE

El acceso a el área de las Autoridades Certificadoras de la SE, está restringido únicamente a personal autorizado el cual es responsable de los servidores de las Autoridades Certificadoras de la Secretaría de Economía. Cuenta con 5 niveles de seguridad. El acceso a cada nivel esta protegido por diferentes factores de seguridad como tarjetas proximidad, lector volumétrico, lector de huella digital y claves de acceso.

El área más segura no permite el acceso a una sola persona, por lo menos deben ser dos y deben estar autorizadas para acceder a este nivel, se requieren dos factores de seguridad para su acceso.

5.1.3 Acondicionado de aire y energía eléctrica

La ACR-SE cuenta con aire acondicionado el cual está en operación continua, se tiene uno de respaldo, que se activa en caso de que falle la unidad principal.

La humedad y la temperatura están controladas en caso de aumento de temperatura o problemas con los sistemas de refrigeración de respaldo.

Se cuenta con UPS con el cual mantiene la carga eléctrica constante sin interrupciones ni picos.

5.1.4 Protección contra de inundaciones

La ACR-SE se localiza en el primer piso del inmueble de la Secretaría de Economía, por lo que no se ve expuesta a tal situación.

5.1.5 Protección y prevención contra incendios

Se cuenta con sistemas de detección de humo y extinción de incendios.

5.1.6 Almacenamiento de medios

Los medios que contienen información referente al software o datos con los que ofrece el servicios la ACR-SE, son respaldados y enviados a lugares seguros dentro y fura del área de la ACR-SE.

5.1.7 Respaldos

Los respaldos se llevan a cabo cumpliendo con lo estipulado en el numeral 4.6.3,

4.6.4 y bajo la Política de Respaldos de la DGNM, respectivamente.

5.2 Controles de seguridad personales

5.2.1 Antecedentes y requisitos para el personal responsable de la ACR-SE.

El personal responsable de la ACR-SE, esta contratado por la SE y cuentan con el nivel y conocimientos necesarios para dicha responsabilidad, El procedimiento se esta integrando, por el momento el personal cuenta con la capacitación necesaria para la administración y mantenimiento del la ARC-SE.

5.2.2 Procedimientos de verificación del personal.

El área de Recursos Humanos verifica previamente los antecedentes del personal contratado por la Secretaría de Economía, comprueba que cumpla con los requisitos establecido por Ley.

5.2.3 Requerimientos de capacitación

El personal que pertenece al área de seguridad, desarrollo y administración del la DGNM, cuenta con el perfil requerido para el área respectiva.
De acuerdo con las necesidades de cada área, el personal es enviado a capacitación constantemente.

5.2.4 Sanciones por acciones no autorizadas

Las sanciones se valorarán dependiendo el riesgo que representen a la ACR-SE, y serán determinadas por la Dirección General de Normatividad Mercantil.

5.2.5 Controles sobre la contratación de personal

Descrito en el numeral 5.2.2 de este documento.

5.2.6 Documentación proporcionada al personal de la ACR-SE

Políticas de Seguridad, Políticas de Certificados, CPS, entre otros, dependiendo su perfil y puesto.

5.3 Controles de Procedimientos

5.3.1 Funciones de confianza

El personal que interviene directamente en las funciones siguientes es personal de confianza de la ACR-SE:
Personal de operación de la ACR-SE:

- Administración, mantenimiento y manejo del servidor que opera la ACR-SE.
- Respaldos.

Personal que administra las funciones de la ACR-SE:

- Administración del software de certificación (emisión, revocación de certificados, creación de cuentas de agentes certificadores entre otras).
- Administración del modulo criptográfico.
- Actualizar la CRL.

Personal de la RA-SE:

- Identificar y autenticar a los solicitantes y su documentación
- Remitir las solicitudes de certificación y/o revocación de certificados a la ACR-SE.

6. CONTROLES DE SEGURIDAD TÉCNICOS

6.1 Generación e Instalación del par de claves

El par de claves de la ACR-SE serán generadas utilizando el software SeguriServer, éste se utiliza para la administración de la Autoridad Certificadora de la ACR-SE.
La clave privada estará en todo momento cifrada esta se encuentra almacenada en el modulo criptográfico el cual cumple con el FIPS 140-2 nivel 3.

6.1.1 Generación del par de claves.

El par de claves de la ACR-SE serán generadas por el personal responsable del servidor que administra la ACR-SE.

El par de claves de las entidades no son generadas ni entregadas por la ACR-SE Las entidades que formarán parte de los usuarios de la ACR-SE, deberán generar su par de claves en el lugar más seguro de sus instalaciones, bajo la supervisión de la Secretaría de Economía.

6.1.2 Entrega de la clave pública a las entidades.

Las entidades finales presentarán su clave pública (mediante un requerimiento PKCS#10 ó mediante el certificado autofimado por la Autoridad Certificadota subordinada) a la ACR-SE para que sea certificada, una vez que se complete el procedimiento del numeral 3.1.2 según sea el caso

Si la solicitud es de un certificado de servidor, el responsable directo del servidor deberá incluir la clave pública, en formato PKCS#10 (CSR), la cual será enviada a la ACR-SEAR una vez que se complete el procedimiento del numeral 3.1.2 según sea el caso

6.1.3 Distribución de claves públicas

La ACR-SE publicará en su servidor WEB los certificados emitidos y revocados a través de las páginas destinadas para tal fin (http://ac.economia.gob.mx /acrse/).

6.1.4 Tamaño de claves

El par de claves de la ACR-SE será RSA de 2048 bits, para las Autoridad Certificadora subordinadas será de 2048 bits y para los de Identidad Personal y de Servidor será de 1024 bits.
Las claves no podrán ser diferentes a los tamaños especificados en el párrafo anterior según cada caso.

6.1.5 Software y hardware utilizado para la generación de las claves.

El software es SEGURISERVER y el hardware es un modulo criptográfico el cual cumple con el FIPS 140-2 nivel 3.

6.1.6 Uso de las claves.

La extensión KeyUsage deberá incluirse en los certificados emitidos por la ACR-SE, esta extensión, deberá marcarse como crítica.
La ACR-SE contendrá la extensión keyUsage con los siguientes bits activados:

- cRLSign, keyCertSign, digitalSignature, nonRepudiation

Para sus entidades que contengan claves RSA el valor del KeyUsage será:

- digitalSignature, nonRepudiation, KeyEncipherment, dataEncipherment

6.2 Protección de la clave privada

La clave privada estará en todo momento cifrada esta se encuentra almacenada en el modulo criptográfico el cual cumple con el FIPS 140-2 nivel 3.
La misma se encuentra en el nivel más seguro del área de autoridades certificadoras de la Dirección general de Normatividad Mercantil.

6.2.1 Normas que deberán cumplir el módulo criptográfico

El modulo criptográfico, que contendrá la clave privada de la ACR-SE, deberá cumplir por lo menos con el FIPS 140 nivel 3.

6.2.2 Medida de seguridad para el uso de las claves de la ACR-SE

La ACR-SE implementará una configuración en el modulo criptográfico, para el uso de su clave privada, el cual determina que para poder utilizar la clave privada deberán estar presentes por lo menos dos de los responsables de ésta.

6.2.3 Respaldo de clave privada

Existe únicamente un respaldo de la clave privada y esta se encuentra en un segundo modulo criptográfico que igualmente cumple con el FIPS 140-2 nivel3.

6.2.4 Mantenimiento de copias

Al término del ciclo de vida de las claves de la ACR-SE, éstas se conservarán en un medio de almacenamiento electrónico criptográficamente al cual solo tendrán acceso los responsables de la ACR-SE.

6.2.5 Entrada de la clave privada en módulo criptográfico

La clave privada se genera únicamente en el modulo criptográfico, de la ACR-SE.

6.2.6 Método de activación de clave privada

Para poder activar la clave privada de la ACR-SE, deberán estar presentes por lo menos dos de los responsables de la misma.

6.2.7 Método de desactivación de clave privada

Debido a que el servidor de la ACR-SE esta fura de la red de datos, al termino de la emisión de los o del certificado, se desactiva tanto el servidor como el modulo criptográfico.

6.2.8 Método de destrucción de la clave privada

Todas las claves privadas utilizadas son almacenadas de modo permanente y de forma criptográfica y segura, se accede al modulo eliminando el formato de las tarjetas de activación.

6.3 Otros aspectos de la Administración de las claves de la ACR-SE

6.3.1 Almacenamiento de claves públicas

Las claves públicas serán almacenadas de acuerdo con la Política de Respaldos según sea el caso.

6.3.2 Periodo de uso del par de claves

El periodo se dará por terminado cuando se concluya la vigencia indicada en el certificado o cuando por alguna razón por la cual tenga que ser revocado.

El actual certificado de la ACR-SE es válido hasta 20 años

Para las Autoridades Certificadoras será de 10 años, de conformidad con el artículo 11 del Reglamento del CoCo.

6.4 Datos de activación

6.4.1 Generación e instalación de datos de activación

La clave de paso utilizada para la protección de la clave privada deberá tener una longitud suficiente (al menos 14 caracteres) y con combinaciones de letras (mayúsculas y minúsculas), números y otros caracteres que la hagan robusta a un ataque de fuerza bruta (no se aceptan password con significado ni palabras que se encuentren en el diccionario).

6.4.2 Protección de datos de activación

Los password para la activación de la ACR-SE pertenecen y están bajo custodia del personal autorizado para tal fin, cada persona autorizada cuenta con un password, y para activar la ACR-SE, se requiere de por lo menos dos personas autorizadas.

6.5 Controles de seguridad en las computadoras

6.5.1 Requerimientos técnicos de seguridad de la computadora

Los sistemas instalados y archivos de datos de la ACR-SE son confiables protegidos contra los accesos no autorizados.

Las Autoridades Certificadoras se mantienen aisladas de todo el equipo que pertenece a la DGNM, manteniéndolo físicamente seguro.

Servicio, manteniendo seguros aquellos que sean necesarios.

El acceso físico al servidor que administra la ACR-SE, es controlado.

El personal responsable del servidor de la ACR-SE, deberá mantendrá una relación constante con el equipo de respuesta a incidentes y el responsable de seguridad del área de datos de la DGNM.

El software instalado en el servidor de la ACR-SE será actualizado continuamente con las últimas actualizaciones críticas de seguridad.

6.6 Seguridad de red.

El servidor que administra a la ACR-SE NO está conectado a la red, por lo que el intercambio de información entre este equipo y sus usuarios será exclusivamente al momento de certificar y revocar, mediante dispositivos de almacenamiento removibles. Este servidor tiene deshabilitados todos los servicios de red.

7. PERFILES DE CERTIFICADOS Y CRL

7.1 Certificados

En función de la interoperabilidad, la ACR-SE firmará las claves públicas de acuerdo con el RFC 3280 *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile* .

Los certificados emitidos por la ACR-SE contendrán al menos los siguientes campos:

- **Versión**: Número de versión del certificado X.509
- **SerialNumber**: Número único asignado al certificado

- **Signature**: Algoritmo usado para generar la firma, normalmente RSA/SHA-1Firma de autenticación realizada usando la clave privada de la CA en cuestión.
- **Issuer**: Nombre de la CA firmante
- **Validity:** Periodo de validez del certificado
- **Subject**: Distinguished Name del certificado.
- **Subject Public Key Information**: algorithmID, clave.
- ExtKeyUsage Extension
- CertificatePolicies

7.1.1 Versión del certificado

Los certificados emitidos por la ACR-SE deberán ser certificados X.509 versión 3. El campo de versión del certificado debe contener el valor hexadecimal 0x2 para indicar este número de versión.

7.1.2 Extensiones del certificado

Las extensiones X509v3 serán fijadas por defecto por la ACR-SE según el tipo de certificado.
La extensión KeyUsage deberá ser incluida en los certificados emitidos por la ACR-SE, esta extensión, debe ser marcada como crítica.
Para más información sobre la extensión KeyUsage consultar el numeral 6.1.6 de este documento.
La ACR-SE tendrá al menos las siguientes extensiones establecidas:

- crlDistributionPoints, subjectKeyIdentifier, authorityKeyIdentifier, basicConstraints, keyUsage (crítica): digitalSignature, nonRepudiation, cRLSign y keyCertSign y subjectAltName

Los Certificados Digitales de las entidades que contengan claves RSA tendrán las siguientes extensiones X509v3:

- keyUsage (críticas digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment) y authorityKeyIdentifier

Los Certificados Digitales de Servidor (que sólo contendrán claves RSA) tendrán las siguientes extensiones X509v3:

- keyUsage (crítica: digitalSignature, nonRepudiation) y authorityKeyIdentifier

7.1.3 Identificadores de objetos de algoritmo

RSA, DSA, MD5, SHA-1, DES, AES y triple DES entre otros.

7.2 Perfil de la CRL

7.2.1 Número de versión

La ACR-SE emite su CRL de acuerdo con el RFC 3280 *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*., esta versión “RFC 3280” sustituye a la versión “RFC 2459”.

7.2.2 CRL y extensiones de entrada de CRL

Deberá ser de acuerdo con el RFC 3280 *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, l*os algoritmos utilizados para la Firma Electrónica Avanzada deben ser compatibles con los estándares de la industria.

8. ESPECIFICACIONES ADMINISTRATIVAS

8.1 Procedimientos de cambio de especificación

Las modificaciones efectuadas a esta CPS se publicarán en el apartado versiones anteriores en http://ac.economia.gob.mx/acr-se/doctos.
Si lo cambios son tipográficos se efectuaran sin previo aviso, de otra manera se publicarán durante 15 días para recibir comentarios, antes de ser autorizados.
Al término de esos 15 días, serán autorizados y publicados los cambios.
Los comentarios serán recibidos al correo electrónico acrse@economia.gob.mx.

8.2 Procedimientos de publicación y notificación

- La ACR-SE publicará su certificado, su CRL y los certificados firmados por ésta, su declaración de prácticas de certificación, política de certificados en el Web destinada al servicio de la Autoridad Certificadora ACR-SE (http://ac.economia.gob.mx). Ésta publicación se realizará como máximo 2 horas después de la emisión y firma de los certificados, en caso de revocación de algún certificado la CRL se publicará en el menor tiempo posible.
- En caso de modificación de estas CPS o CP, será informado dicho cambio a sus usuarios.

9. VERSIÓN DE ESTA CPS

Versión 1.0 junio del 2005

10. ABREVIACIONES

ACR-SE: Autoridad Certificadora Raíz de la Secretaría de Economía
C: CountryName
CA: Certification Authority
CDIP: Certificado Digital de Identidad Personal
CDS: Certificado Digital de Servidor
CDACS: Certificado Digital de Autoridad Certificadora subordinada.
CDTS: Certificado Digital de Estampas de Tiempo.
CN: Common Name
CoCo: Código de Comercio
CPS: Declaración de Prácticas de Certificación de ACR-SE.
CRL: Certificate Revocation List
CSR: Certificate Signing Requets
DC: Domain Component
DN: Distinguished Name
DSA: Digital Signature Algorithm.
Email: Dirección de correo electrónico
RA: Autoridad Registradora
RCoCo: Reglamento del CoCo
RGPSC: REGLAS gnerales a las que deberán sujetarse los prestadores de servicios de certificación.
RPC : Registro Público de Comercio
O: OrganizationName
PC: Poltica de Certificados
PKCS#10: Public-Key Cryptography Standard 10 (Certification Request Standard Syntax Standard)
PKI: Public Key Infraestructure o Infraestructura de Clave Pública
RSA: Algoritmo criptográfico de clave pública (sus creadores: Rivest, Shamir y Adleman
SSL: Secure Socket Layer
OID: Object Identifier
UID: Unique Identifier

11. REFERENCIAS

- RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, noviembre 2003. http://www.faqs.org/rfcs/rfc3647.html
- Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, publicada en el Diario Oficial de la Federación el 11 de junio de 2002. https://www.firmadigital.gob.mx
- *RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile abril 2002*, http://www.faqs.org/rfcs/rfc3280.html .
- ISO/IEC 9594-8:2001 Information technology -- Open Systems Interconnection -- The Directory: Public-key and attribute certificate frameworks.
- Código de Comercio, publicado el 29 de agosto de 2003, en el Diario Oficial de la Federación.
- REGLAMENTO del Código de Comercio en Materia de Prestadores de Servicios de Certificación, Publicado el 19 de julio de 2004
- 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.