Política de Certificados
Autoridad Certificadora Raíz Segunda de la Secretaría de Economía.

Versión 1.1
julio de 2018

OID: 2.16.484.101.10.316.10.1.

Índice

1. Introducción.

La Política de Certificados es un conjunto de reglas que define la aplicabilidad de un certificado digital de firma electrónica avanzada en una comunidad de usuarios, sistemas o aplicaciones con requerimientos de seguridad en común.

En este documento se describe la Política de Certificados para la Autoridad Certificadora Raíz Segunda de la Secretaría de Economía. La Política de Certificados se aplica a la solicitud, validación, aceptación, emisión o revocación de los certificados digitales dentro de una Infraestructura de Clave Pública.

2. Alcance.

Esta Política de Certificados especifica los requerimientos de la ACR2-SE que emite CDs de clave pública. Estos requerimientos de la Política aplican a las prácticas de operación y gestión de la ACR2-SE para emitir y administrar CDs, para que los usuarios y las partes que confían en la ACR2-SE puedan tener confianza en el uso del certificado con el apoyo de mecanismos criptográficos.

Los requisitos de la Política relativos a la ACR2-SE incluyen requisitos sobre la prestación de servicios de registro, generación y difusión del certificado, gestión de la revocación, y estado de revocación.

La Política aplica a los CDs de la ACR2-SE emitidos a sí misma, a las ACs subordinadas de la DGNM, Siger, y PSCs, a las autoridades de servicios adicionales de firma electrónica avanzada, y a las entidades de la SE de alto nivel.

La DGNM puede hacer revisiones y actualizaciones de esta Política de Certificados cómo y cuándo lo crea conveniente o requerido por las circunstancias. La Política de Certificados actualizada será publicada en el sitio de Internet de la ACR2-SE.

3. Nombre del documento e identificación.

El nombre de este documento es “Política de Certificados de la Autoridad Certificadora Raíz Segunda de la Secretaría de Economía” V1.0, emitida el 12 de mayo de 2017, con OID: 2.16.484.101.10.316.10.1. Los CDs emitidos de acuerdo con esta Política y asociados con la Autoridad Certificadora Raíz Segunda de la Secretaría de Economía usarán el OID mencionado arriba en el campo Directivas del Certificado del CD.

4. Referencias.

- Código de Comercio;
- Decreto por el que se reforman y adicionan diversas disposiciones del Código de Comercio y del Código Penal Federal, publicado el 7 de abril de 2016, 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 en el Diario Oficial de la Federación;

- Reglas generales a las que deberán sujetarse los prestadores de servicios de certificación. Publicadas el 14 de mayo de 2018, en el Diario Oficial de la Federación;
- RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, November 2003. http://www.faqs.org/rfcs/rfc3647.html
- RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008. https://www.ietf.org/rfc/rfc5280.txt
- ISO/IEC 9594-8:2014 Information technology -- Open Systems Interconnection --The Directory: Public-key and attribute certificate frameworks.

5. Definiciones.

En la aplicación de esta Política de Certificados se estará a las definiciones a que se refiere el artículo 89 del Código de Comercio.

6. Acrónimos.

ACR2-SE	Autoridad Certificadora Raíz Segunda de la Secretaría de Economía.
AC	Autoridad Certificadora.
AR-SE	Autoridad Registradora de la ACR2-SE.
DGNM	Dirección General de Normatividad Mercantil.
CD	Certificado Digital.
CRL	Lista de Certificados Revocados (por sus siglas en inglés).
DN	Nombre Distintivo (por sus siglas en inglés).
DPC	Declaración de Prácticas de Certificación.
OCSP	Protocolo de Estatus de Certificados en Línea (por sus siglas en inglés).
LFEA	Ley de Firma Electrónica Avanzada.
PKI	Infraestructura de Clave Pública (por sus siglas en inglés).
PSC	Prestadores de Servicios de Certificación.
RGPSC	Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Servicios de Certificación.
RPSC	Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación.
SE	Secretaría de Economía.

SSL	Capa de Puertos Seguros (por sus siglas en inglés).
URL	Localizador Uniforme de Recurso (por sus siglas en inglés).

7. Autoridad Certificadora Raíz Segunda de la Secretaría de Economía.

La ACR2-SE sustituye a la AC Raíz de la Secretaría de Economía, para actualizar los algoritmos criptográficos y tamaños de clave utilizados de acuerdo a recomendaciones internacionales.

La ACR2-SE es la colección de hardware, software y personal, que genera, firma y emite CDs de clave pública a sí misma, a su servicio de OCSP, a sus servicios adicionales de firma electrónica avanzada, a ACs de la DGNM y del Siger, a ACs de los PSCs, a las autoridades de servicios adicionales de firma electrónica avanzada de los PSCs, y a entidades de la SE de alto nivel, de acuerdo al Código de Comercio, el RPSC, las RGPSC, esta Política, y LFEA.

La ACR2-SE es responsable de la emisión y administración de CDs, incluyendo:

- Generar los certificados;
- Publicar los certificados;
- Revocar los certificados;
- Generar y destruir las claves criptográficas de la ACR2-SE;
- Poner el certificado a disposición de las entidades, después de confirmar que éstas han reconocido formalmente sus obligaciones como se describe en el Código de Comercio, RPSC, RGPSC, y esta Política;
- Asegurar que todos los aspectos de los servicios, operaciones e infraestructura de la ACR2-SE relacionados con los CDs emitidos bajo esta Política de Certificados, se realicen de acuerdo con los requisitos de esta Política.

8. Autoridad Registradora de la Autoridad Certificadora Raíz Segunda de la Secretaría de Economía.

La AR-SE será la encargada y responsable de:

- Verificar la identidad del solicitante del CD;
- Verificar la integridad de la información en el requerimiento de certificado;
- Autenticar la información que quedará en el CD a ser expedido por la ACR2-SE;
- Controlar el proceso de registro; y
- Completar el procedimiento definido para la emisión de CDs.

Para verificar la identidad del solicitante de CDs para las ACs de la DGNM y del SIGER, la directora o director del SIGER hará un escrito a la DGNM solicitando los CDs para estas ACs, quedando bajo resguardo de la misma la DGNM.

Para verificar la identidad de los solicitantes de CDs para las ACs y de las autoridades de servicios adicionales de firma electrónica avanzada de PSCs, la AR-SE seguirá lo especificado en el Código de Comercio, RPSC y en las RGPSC.

Para el caso de verificar la identidad de los solicitantes de CDs para entidades de la SE de alto nivel, la AR-SE verificará la información de identidad de la entidad solicitante de acuerdo a la normatividad bajo la cual opere dicha entidad. La identidad se verificará en no más de un mes antes de la emisión del CD. El solicitante debe presentarse personalmente en la AR-SE, pero en caso de no poder hacerlo la AR-SE puede aceptar la autenticación de la identidad de un solicitante remoto mediante un Notario Público que sirva como sustituto de la AR-SE. El Notario Público enviará el paquete de información recopilada del solicitante asegurado de manera inviolable directamente a la AR-SE de manera segura para que ésta lo revise. El requisito para registrar un biométrico del solicitante se puede satisfacer proporcionando fotografías de tipo pasaporte al Notario Público. El Notario Público verificará las fotografías recientes contra la apariencia del solicitante y la biometría en las credenciales presentadas, e incorporará de forma segura el componente biométrico en el paquete notariado. Otros métodos seguros también son aceptables. La autenticación por parte de un Notario Público no exime a la AR-SE de su responsabilidad de revisar toda la documentación.

9. Convención de nombres.

El DN (Distinguished Name) de los campos Emisor y Sujeto del CD de la ACR2-SE, utilizará el siguiente nombre:

E= acr2se@economia.gob.mx
O= Secretaria de Economía
OU= Dirección General de Normatividad Mercantil
CN= Autoridad Certificadora Raíz Segunda de Secretaria de Economía
C= MX
Street= Insurgentes Sur 1940, Col. Florida
PostalCode= 01030
S= Ciudad de México
L= Álvaro Obregón

El DN del campo Sujeto de los CDs que emita la ACR2-SE para las ACs de la DGNM y SIGER, utilizará el siguiente nombre:

E= <Correo electrónico>
O= <Nombre de la organización>
OU= <Unidad de la organización>
CN= <Nombre completo de la AC o servicio adicional>
C= MX
Street= Insurgentes Sur 1940, Col. Florida

PostalCode= 01030
S= Ciudad de México
L= Álvaro Obregón

El campo Nombre Alternativo del Sujeto (Subject Alternative Name) de los CDs que emita la ACR2-SE para las ACs de la DGNM y SIGER, utilizará:

DNSName= <Nombre de dominio de Internet>

El DN del campo Sujeto de los CDs que emita la ACR2-SE para las ACs de los PSCs y autoridades de servicios adicionales de firma electrónica avanzada, utilizará el siguiente nombre:

E= <Correo electrónico>
O= <Nombre de la organización>
OU= <Unidad de la organización>
CN= <Nombre completo de la AC o servicio adicional>
C= MX

El campo Nombre Alternativo del Sujeto (Subject Alternative Name) de los CDs que emita la ACR2-SE para ACs de los PSCs y autoridades de servicios adicionales de firma electrónica avanzada, utilizará:

dNSName= <Nombre de dominio de Internet>

El DN del campo Sujeto de los CDs que emita la ACR2-SE para entidades de la SE de alto nivel, utilizará un nombre de la siguiente forma:

E= <Correo electrónico>
O= <Nombre de la organización>
OU= <Unidad de la organización>
CN= <Nombre completo de la persona
>
C= MX
Street= <Calle, número y colonia>
PostalCode= <Código postal>
S= <Estado>
L= <Delegación o municipio>

El campo Nombre Alternativo del Sujeto (Subject Alternative Name) de los CDs que emita la ACR2-SE para entidades de la SE de alto nivel utilizará, en su caso:

dNSName= <Nombre de dominio de Internet>

La ACR2-SE asegurará que el nombre sea único, pero la unicidad del nombre no se violará cuando se emitan varios CDs a la misma entidad.

10. Identidad de la Autoridad Certificadora.

El DN del CD de la ACR2-SE contendrá en el campo Emisor los siguientes datos:

E	acr2se@economia.gob.mx
O	Secretaría de Economía
OU	Dirección General de Normatividad Mercantil
CN	Autoridad Certificadora Raíz Segunda de Secretaria de Economía
Street	Insurgentes Sur #1940, Col. Florida
PostalCode	01030
C	MX
S	Ciudad de México
L	Álvaro Obregón

La información sobre la PKI de la ACR2-SE y la Política de Certificados se publicarán en la dirección electrónica https://psc.economia.gob.mx/

11. Comunidad y aplicabilidad.

La comunidad y aplicabilidad de la ACR2-SE se determinan en esta Política de Certificados.

La comunidad estará integrada por la ACR2-SE, su AR-SE, su servidor OCSP, sus relojes de tiempo atómicos, su Autoridad de Sellado Digital de Tiempo, su autoridad de conservación de mensajes de datos, y su personal operativo; las ACs subordinadas, sus ARs, sus servidores OCSP, sus Agentes Certificadores y su personal operativo; las autoridades de servicios adicionales de firma electrónica avanzada de los PSC y su personal operativo; los usuarios de los CDs y de servicios adicionales de firma electrónica avanzada.

La aplicabilidad principal de los CDs emitidos por la ACR2-SE, es desarrollar el Comercio Electrónico, modernizar el Registro Público de Comercio, y realizar trámites ante la SE.

La ACR2-SE emitirá CDs para asuntos del orden comercial a la **AC de la DGNM,** a la AC del Siger, a las ACs de los PSCs que hayan sido acreditados por la DGNM y, cuyas Políticas de Certificados sean tan restrictivas como lo descrito en este documento, **a las autoridades de servicios adicionales de firma electrónica avanzada, y** las entidades de la SE de alto nivel.

La ACR2-SE podrá emitir CDs de prueba cuando sea necesario y por un periodo de validez corto tomando todas las precauciones de seguridad necesarias.

La ACR2-SE emitirá otro tipo de CD diferente a asuntos del orden comercial en caso de ser necesario, para la operación de alguna necesidad particular de la SE y, deberá ser autorizado por la DGNM.

12. Estructura jerárquica de la Autoridad Certificadora.

La estructura jerárquica de certificación se compone de los siguientes elementos:

1. Autoridad Certificadora Raíz Segunda de la Secretaría de Economía (ACR2-SE);
2. Autoridad Registradora (AR-SE) de la ACR2-SE; y
3. Autoridades Certificadoras Subordinadas de la ACR2-SE:

- Dirección General de Normatividad Mercantil (DGNM). Ésta AC podrá certificar las claves públicas y revocar los CDs de su servicio de OCSP, Agentes Certificadores, entidades de la SE de medio y bajo nivel, funcionarios públicos de la SE, particulares que realicen trámites ante esta SE, y otras entidades federales del país. El CD de esta AC y los CDs que expida cumplirán con el Código de Comercio y la Tercera Disposición de las Disposiciones Generales de la Ley de Firma Electrónica Avanzada. Los CDs emitidos por está AC se regirán bajo su Política de Certificados y su Declaración de Prácticas de Certificación.
- Sistema Integral de Gestión Registral (Siger). Esta AC podrá certificar las claves públicas y revocar los CDs de su servicio de OCSP, de registradores del Registro Público de Comercio y fedatarios públicos. Los CDs emitidos por está AC se regirán bajo su Política de Certificados y la Declaración de Prácticas de Certificación.
- Prestadores de Servicios de Certificación (PSC). Estas ACs podrán certificar las claves públicas y revocar los CDs de su servicio de OCSP, Agentes Certificadores, personas físicas y morales, y servidores (equipos) para efectos comerciales. Los CDs emitidos por estás ACs se regirán bajo sus Políticas de Certificados y Declaraciones de Prácticas de Certificación.

13. Objetivo de la Autoridad Certificadora y de las Autoridades Certificadoras subordinadas.

El objetivo de la ACR2-SE, de las ACs de la DGNM y del Siger, y de las ACs de los PSCs, será la emisión y revocación de CDs.

14. Perfiles de los Certificados Digitales, CRL Y OCSP.

- Los CDs emitidos por la ACR2-SE se ajustarán a los estándares internacionales ISO/IEC 9594-8:2014 "The Directory: Public-key and attribute certificate frameworks" y al RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" actualizado con el RFC 6818 “Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”:

- La ACR2-SE emitirá CDs X.509 V3 y CRLs X.509 V2 o los que le sustituyan; Los CDs emitidos deberán utilizar Sha256WithRSA o el que le sustituya para firmas;
- Los certificados emitidos usarán el algoritmo hash Sha256 o el que le sustituya;
- Los CDs de la ACR2-SE y de la AC de la DGNM se ajustarán a lo mencionado en el Código de Comercio y en la Tercera Disposición de las Disposiciones Generales de la Ley de Firma Electrónica Avanzada para ACs;
- Los CDs de la AC del Siger se ajustarán a lo mencionado en la normatividad correspondiente;

El servicio de estado de certificados de la ACR2-SE firmará respuestas utilizando algoritmos designados para la firma de CRL y utilizará OCSP V1 o el que le sustituya.

15. Período de validez de los Certificados Digitales.

El período de validez de los CDs de la ACR2-SE y de OCSP será máximo de quince años, y de los servicios adicionales de firma electrónica avanzada de la SE será máximo de doce años.

El período de validez de los CDs de ACs subordinadas, de su OCSP, y de las autoridades de servicios adicionales de firma electrónica avanzada será máximo de doce años.

El período de validez de los CDs de entidades de la SE de alto nivel será máximo de cuatro años.

La fecha de expiración de los CDs emitidos por la ACR2-SE será menor a la fecha de expiración del CD de la ACR2-SE.

Cuando se haya superado cuatro quintos del tiempo de vida de la ACR2-SE o en un tiempo menor si la tecnología se vuelve obsoleta o por razones de fuerza mayor, se generará un nuevo CD y en su caso una nueva identidad de Autoridad Certificadora. A partir de ese momento, las nuevas inscripciones se harán firmando CDs con el nuevo CD. De este modo, los CDs para los servicios adicionales de firma electrónica avanzada de la SE; las ACs subordinadas; las autoridades de servicios adicionales de firma electrónica avanzada de los PSC; y las entidades de la SE de alto nivel, dispondrán de una quinta parte del tiempo para solicitar nuevos CDs a la nueva Autoridad Certificadora de la SE. Sin embargo, la ACR2-SE podrá continuar firmando CRLs con el CD anterior y utilizando el CD del servicio de OCSP para la validación de CDs hasta el final de la vigencia de ambos CDs.

16. Disposición de Certificados Digitales.

- La ACR2-SE y las ACs subordinadas mantendrán un repositorio o base de datos con los CDs que emita, de manera que estarán disponibles al público mediante un servicio de publicación de CDs.

- Los CDs emitidos por la ACR2-SE se publicarán en la dirección electrónica http://www.firmadigital.gob.mx.
- Así mismo, las ACs subordinadas mantendrán constancia, en las páginas Web habilitadas para tal fin, de los CDs emitidos o revocados por éstas.

17. Revocaciones.

17.1. Causas de Revocación de Certificados Digitales de la Autoridad Certificadora Raíz Segunda de la Secretaría de Economía.

Siempre que ocurra alguna de las siguientes causas, el CD será revocado y colocado en la CRL:

- Ha existido pérdida, robo, modificación, divulgación no autorizada u otro compromiso de la clave privada asociada al CD;
- Se han incumplido alguna de las obligaciones descritas en esta Política de Certificados;
- Se conoce o se tiene motivos para creer razonablemente que uno de los hechos representados en el CD es falso;
- Los atributos declarados en el CD del suscriptor se reducen;
- Se conoce que alguno de los requisitos de emisión del CD no se cumplió;
- El sistema de certificación se vio comprometido de modo tal que afecta a la fiabilidad del CD;
- Fallecimiento del titular del CD;
- Cambio de información relativa al titular;
- Se sospecha que la información contenida en el CD es inexacta;
- Resolución administrativa o judicial que lo ordene;
- Se produce un error en la emisión de un CD;
- Cese voluntario, en el caso de los PSCs deberán cumplir con lo establecido en el númeral 18 de la RGPSC.
- La clave privada de la ACR2-SE esté comprometida, en cuyo caso, serían revocados todos los CDs de las entidades a las que se les han emitido CDs. Las ACs no podrían emitir CDs válidos hasta que no se restaure la identidad de la ACR2-SE y se vuelvan a generar los CDs de las entidades registradas por la ACR2-SE; y
- Además de cualquiera de las causas que se señalan en el Código de Comercio, RPSC y RGPSC, que le sean aplicables.

17.2. Revocación de un Certificado Digital.

La revocación de un CD firmado por la ACR2-SE, se realizará siguiendo el proceso descrito a continuación:

- Cuando se trate de los CDs de la ACR2-SE y del servicio de OCSP, la solicitud por escrito se hará al director o directora de la DGNM para su autorización, anexando los documentos que fundamenten dicha autorización;

- Cuando se trate de CDs de autoridades de servicios adicionales de firma electrónica avanzada de la SE, la solicitud por escrito se hará al director o directora de la DGNM para su autorización, anexando los documentos que fundamenten dicha autorización;
- Cuando se trate de los CDs de la AC de la DGNM o del Siger y del servicio de OCSP, el director o directora del Siger lo solicitará por escrito al director o directora de la DGNM para su autorización, anexando los documentos que fundamenten dicha solicitud;
- Cuando se trate del CD de un PSC, será el representante legal del PSC y los profesionales jurídico e informático de la AC o de las autoridades de servicios adicionales de firma electrónica avanzada, quienes solicitarán por escrito a la ACR2-SE la revocación de su CD. Para que dicha revocación se lleve a cabo, los responsables deberán cumplir con lo establecido en el artículo 16 del RPSC, anexando los documentos que fundamenten en dicha solicitud. En su caso el PSC deberá entregar la documentación que recibieron de los titulares de cada CD que emitieron; y
- En caso de ser CDs emitidos a entidades de la SE de alto nivel, serán éstos los que soliciten por escrito la revocación dirigido al director o directora de la DGNM, anexando los documentos que fundamenten dicha solicitud.

17.3. Tiempo para Procesar la Solicitud de Revocación.

Las ACR2-SE revocará el CD lo más rápido posible cuando reciban una solicitud de revocación apropiada. Las solicitudes de revocación se procesarán antes de que se publique la siguiente CRL, exceptuando las solicitudes recibidas dentro de las dos horas antes de la emisión de la CRL, las cuales se procesarán antes de que se publique la siguiente CRL.

17.4. Identificación y Autenticación para Solicitud de Revocación.

Las solicitudes de revocación deben identificarse y autenticarse. Las solicitudes de revocación de un CD pueden autenticarse utilizando la clave pública de dicho certificado, independientemente de que la clave privada asociada se haya visto comprometida o no.

18. Lista de Certificados Revocados.

- La ACR2-SE publicará en su página Web la CRL mensualmente o cada vez que revoque un CD.
- Las ACs de la DGNM y del Siger publicarán las CRLs de acuerdo a su Política de Certificados.
- Las ACs de los PSCs deben publicar sus CRLs, por lo menos con la periodicidad establecida en el numeral 75 fracción V de las RGPSC. siendo responsables de indicar en los CDs que emitan, las direcciones en Internet (URL) en donde se localizarán la CRL y el OCSP, para que de esta manera sea fácilmente accesible por los usuarios.

- La ACR2-SE y las ACs subordinadas se comprometerán a mantener actualizada la CRL y el OCSP, incluyendo todos los CDs revocados desde la última actualización.

19. Privacidad y Seguridad.

19.1. Privacidad.

La DGNM protegerá los datos de carácter personal que sean suministrados por los solicitantes a acreditación de PSCs y de solicitantes de CDs de entidades de la SE de alto nivel, de acuerdo con la Ley de Transparencia y de Acceso a la Información Pública Gubernamental.

19.2. Requerimientos de Seguridad Física.

- La ubicación y construcción del centro de datos que aloja el equipo de la ACR2-SE, cumplirá con altos estándares internacionales de seguridad. Otros mecanismos físicos de protección de seguridad tales como guardias, cerraduras de alta seguridad y sensores de intrusión, proporcionarán una protección robusta contra el acceso no autorizado a los equipos y registros de la ACR2-SE;

Se realizará periódicamente una verificación de seguridad del centro de datos que aloja el equipo de la ACR2-SE. Como mínimo, se verificará lo siguiente:

- El equipo está en un estado apropiado;
- Los sistemas de seguridad física (cerraduras de puertas, tapas de ventilación, etc.) funcionan correctamente; y
- El área está protegida contra accesos no autorizados.
- Una persona o un grupo de personas serán explícitamente responsables de hacer las verificaciones anteriores. Cuando un grupo de personas es responsable, se mantendrá un registro identificando a la persona que realiza la verificación en cada instancia. Si el centro de datos no es atendido continuamente, la última persona que salga debe informar en una hoja de salida la fecha/hora y afirme que todos los mecanismos de protección física necesarios están en su lugar y activados;
- Los *módulos de seguridad en hardware* de la ACR2-SE estarán protegidos contra robo, pérdida y uso no autorizado;
- La ACR2-SE tendrá capacidad de respaldo suficiente para terminar cualquier acción que esté realizando y registrar el estado del equipo automáticamente antes de que la falta de energía eléctrica o aire acondicionado cause que se apague. Los repositorios (que contengan CDs y CRLs) deberán estar provistos de energía eléctrica ininterrumpida suficiente para un mínimo de 6 horas de operación en ausencia de electricidad, para mantener la disponibilidad y evitar la negación de servicio;
- Los medios se almacenarán para protegerlos de daños accidentales (agua, fuego u ondas electromagnéticas) y acceso físico no autorizado;

- La ACR2-SE operará en un servidor de misión crítica (considerando otro servidor de redundancia de las mismas características) desconectado de la red de computadoras, el intercambio de información con sus ACs subordinadas será mediante dispositivos de almacenamiento removible, únicamente para efectos de certificación de las mismas;
- El intercambio de información entre el servidor de la ACR2-SE con las ACs subordinadas, será en los términos establecidos en el numeral 76 de las RGPSC.
- Tanto el *hardware* como el *software* que opera la ACR2-SE se mantendrá en todo momento física y lógicamente seguro. Como mínimo, los controles de acceso físico para el equipo de la ACR2-SE serán:
- Asegurar que no se permite el acceso no autorizado al hardware;
- Asegurar que todos los soportes extraíbles se almacenen en contenedores seguros;
- Estar supervisado para detectar intrusiones no autorizadas en todo momento;
- Asegurar que un registro de acceso se mantenga e inspeccione periódicamente; y
- Requerir control de acceso físico de dos personas tanto al módulo de seguridad en hardware como a los sistemas informáticos.
- Se realizarán periódicamente copias de seguridad completas del sistema de la ACR2-SE que sean suficientes para recuperarse de alguna falla del sistema de la ACR2-SE. Al menos una copia de seguridad completa se almacenará en un lugar fuera del centro de datos (separado del equipo de ACR2-SE). Sólo se conservará la última copia. La copia de seguridad se almacenará en un sitio con controles físicos y de procedimiento similares a los de la ACR2-SE operacional.

19.3. Recuperación ante Desastres.

La DGNM será notificada si la ACR2-SE experimenta lo siguiente:

- Compromiso sospechoso o detectado en los sistemas de la ACR2-SE;
- Conflicto sospechoso o detectado en el servicio de OCSP;
- Penetración física o lógica a los sistemas de la ACR2-SE;
- Ataques de negación de servicio con éxito en componentes de la ACR2-SE; y,
- Cualquier incidente que impida que la ACR2-SE emita una CRL.

La DGNM tomará las medidas apropiadas para proteger la integridad de la ACR2-SE.

El personal de soporte técnico de la ACR2-SE restablecerá las capacidades operacionales lo más rápido posible, de acuerdo a un plan de recuperación ante desastres.

19.4. Recursos Informáticos, *Software* y/o Datos Dañados.

Cuando los recursos de computación, software y/o datos estén dañados, las ACR2-SE responderá de la siguiente manera:

- Antes de volver a la operación, se asegurará de que se ha restaurado la integridad del sistema;
- Si las claves de la ACR2-SE no se destruyeron, se restablecerá la operación de la ACR2-SE, dando prioridad a la generación de información de estado de certificado con la emisión de la CRL; o
- Si las claves de la ACR2-SE se destruyeron, la operación de la ACR2-SE se restablecerá lo más rápido posible, dando prioridad a la generación de un nuevo par de claves para la ACR2-SE.

19.3. Procedimiento de Compromiso de Clave Privada.

En el caso de compromiso de clave privada de la ACR2-SE, deben realizarse las siguientes operaciones:

- Se informará inmediatamente a la DGNM, ACs subordinadas, autoridades de servicios adicionales de firma electrónica avanzada, y a las entidades de la SE de alto nivel;
- Se procedería a la revocación de las claves y del CD de la ACR2-SE, así como todos los CDs emitidos por ella, no importando la fecha de emisión. A partir de ese momento, deberán revocarse todos los CDs emitidos por las ACs subordinadas a la ACR2-SE y éstas no deberán emitir CDs hasta que no se restaure la identidad de la ACR2-SE y se vuelvan a generar CDs respectivos a las ACs subordinadas, y
- La ACR2-SE generará nuevas claves.

19.6. Controles de Seguridad Técnicos.

Los siguientes controles de seguridad técnicos se aplicarán a la ACR2-SE:

- Las claves criptográficas de la ACR2-SE para firmar CD, CRL o información de estado (OCSP) se generarán en los módulos de seguridad en *hardware* que cumpla por lo menos con la norma FIPS 140-2 nivel 3, y estarán en todo momento cifradas;
- Los CDs emitidos bajo esta Política deberán contener claves públicas RSA;
- Las claves RSA de la ACR2-SE tendrán una longitud de por lo menos 4096 bits;
- La ACR2-SE usará el algoritmo *Sha256* al generar firmas electrónicas avanzadas;
- El servicio OCSP firmará las respuestas utilizando el mismo algoritmo de firma, tamaño de clave y algoritmo *hash* utilizado por la ACR2-SE para firmar CRLs;

- El acceso a la clave privada de la ACR2-SE, resguardada en el módulo de seguridad en hardware, será cuando menos de dos personas y mediante tarjetas y sus contraseñas;
- Habrá dos módulos de seguridad en hardware, uno para la ACR2-SE principal y otro para la AC de redundancia, donde se resguardarán las mismas claves privadas de la AC principal;
- El resguardo de las claves privadas de la ACR2-SE en el segundo módulo de seguridad en hardware se protegerán de la misma manera que las originales;
- Cuando las claves privadas se transporten de un módulo seguridad en hardware a otro, se usará un modelo de seguridad confiable durante el transporte;
- Las claves privadas de la ACR2-SE sólo se podrán exportar desde el módulo de seguridad en hardware para realizar procedimientos de copia de seguridad de clave;
- En ningún momento las claves privadas de la ACR2-SE existirán en texto plano fuera del módulo de seguridad en hardware;
- Los módulos de seguridad en hardware que se hayan activado no estarán disponibles para acceso no autorizado. Después del uso, el módulo de seguridad en hardware se apagará;
- La DGNM autorizará destruir las claves privadas de la ACR2-SE y del servicio de OCSP cuando ya no se necesiten. No se requiere la destrucción física de los módulos de seguridad en hardware.
- Las entidades de la SE de alto nivel destruirán sus claves privadas cuando ya no se necesiten.

19.7. Controles de Seguridad de los Servidores y Auditoría.

El sistema operativo puede proporcionar las siguientes funciones de seguridad informática o a través de una combinación de sistema operativo, software y salvaguardas físicas:

- Autenticar la identidad de los usuarios antes de permitir el acceso al sistema o a las aplicaciones;
- Administrar los privilegios de los usuarios para limitarlos a las funciones asignadas;
- Cumplir el control de acceso para los servicios de AC;
- Evitar que *software* malicioso se cargue en el equipo de la AC;
- Escanear el *hardware* y el *software* de la AC para identificar *software* malicioso cuando se use por primera vez y después periódicamente;
- Adquirir y actualizar el *hardware* y *software* por personal de confianza y especializado;
- Mantener exacto el reloj de los servidores; y
- Proporcionar la capacidad de auditoría de seguridad.

El software de la ACR2-SE que genere y revoque CDs generará archivos de registro de auditoría con fecha y hora. El personal que opera la AC archivará el historial y los archivos de registro de auditoría.

19.8. Controles de Seguridad de la Red.

Los siguientes controles de seguridad de la red se aplicarán a la ACR2-SE:

- Un enrutador de protección de red y un *firewall* protegerán el acceso a la red del equipo de la ACR2-SE, para limitar los servicios permitidos desde y hacia el equipo de la ACR2-SE;
- Se protegerá el equipo de la ACR2-SE contra ataques de red conocidos;
- El equipo encargado de la red desactivará los puertos y servicios de red no utilizados;
- Cualquier *software* de red presente en el equipo de la ACR2-SE será necesario para el funcionamiento de la aplicación de la misma y del equipo;
- Cualquier dispositivo de control utilizado para proteger la red en la que se aloja el equipo PKI negará todos los servicios, excepto los necesarios, al equipo PKI; y
- Los repositorios y los servidores de estado de CD emplearán controles de seguridad de red adecuados.

19.9. Requerimientos de Seguridad Impuestos a las Autoridades Certificadoras Subordinadas y Autoridades de Servicios Adicionales de Firma Electrónica Avanzada y sus Claves.

Los siguientes requerimientos de seguridad aplicarán a las ACs subordinadas y autoridades de servicios adicionales:

- Las ACs y las autoridades de servicios adicionales de firma electrónica avanzada operarán en un servidor de misión crítica (**considerando otro servidor de redundancia con las mismas características**);
- Éste servidor podrá estar conectado a la red de computadoras, en tal caso, el intercambio de información se hará entre el servidor y sus usuarios por lo menos vía SSL o la tecnología que ofrezca mayor seguridad, asimismo, deberá deshabilitar todos los servicios de red que no se requieran para el buen funcionamiento del servicio, manteniendo seguros y monitoreados aquellos que sean necesarios;
- Las claves privadas de las ACs y de las autoridades de servicios adicionales de firma electrónica avanzada estarán cifradas en un dispositivo que cumpla por lo menos con el estándar FIPS 140-2 nivel 3;
- Tanto el *hardware* como el *software* de los servidores de misión crítica que operan las ACs y las autoridades de servicios adicionales de firma electrónica avanzada, se mantendrá en todo momento física y lógicamente seguro;

- Las claves RSA de las ACs, de los servicios de OCSP, y de las autoridades de servicios adicionales de firma electrónica avanzada tendrán una longitud de por lo menos 4096 bits;
- Las claves RSA de los CDs emitidos por las ACs subordinadas tendrán una longitud de por lo menos 2048 bits; y
- Los responsables de las ACs y de las autoridades de servicios adicionales de firma electrónica avanzada, destruirán sus claves privadas cuando ya no se necesiten o cuando los CDs sean revocados.

20. Obligaciones.

20.1. Obligaciones de la DGNM.

Las obligaciones que adquiere la DGNM son las siguientes:

- Ofrecer y mantener la infraestructura necesaria para el establecimiento de una estructura jerárquica de certificación de ACs subordinadas, autoridades de servicios adicionales de firma electrónica avanzada, y de entidades de la SE de alto nivel, según la Política de Certificados descrita en este documento;
- Implementar y mantener los requerimientos de seguridad impuestos a las claves de la ACR2-SE, según lo descrito en este documento en el apartado "PRIVACIDAD Y SEGURIDAD".
- Aprobar o denegar las solicitudes de acreditación así como de emisión de CDs;
- Poner copias de sus propios CDs y de cualquier información de revocación a disposición de quien desee verificar una firma electrónica avanzada con referencia a dichos CDs. Para ello, se publicará y mantendrá actualizada dicha información en las páginas Web destinadas a la infraestructura de certificación (ver apartado “IDENTIDAD DE LA ACR2-SE”);
- Revocar los CDs según el procedimiento establecido en el apartado "REVOCACIONES" de este documento;
- Mantener actualizada la CRL, incluyendo todos los CDs revocados desde la última actualización;
- Proteger los datos de carácter personal que sean suministrados por los solicitantes a acreditación de PSCs y de CDs, de acuerdo con la Ley de Transparencia y de Acceso a la Información Pública Gubernamental; y
- Comunicar inmediatamente a los responsables de las ACs subordinadas, PSCs de las autoridades de servicios adicionales de firma electrónica avanzada, y entidades de la SE de alto nivel, del compromiso, pérdida, divulgación, modificación, y uso no autorizado de la clave privada de la ACR2-SE, con el fin de restaurar la jerarquía lo antes posible según lo establecido en el apartado "PRIVACIDAD Y SEGURIDAD" de este documento.

20.2. Obligaciones de la AR-SE.

Las obligaciones que adquiere la AR-SE son las siguientes:

- Llevar a cabo cada uno de los pasos descritos en el procedimiento de emisión de CDS por parte de la ACR2-se para las ACS subordinadas, autoridades de servicios adicionales de firma electrónica avanzada, y entidades de la SE de alto nivel, según lo descrito en el documento de DPC;
- Llevar a término la identificación y autenticación para la revocación de CDS, de acuerdo con los procedimientos de validación establecidos en el apartado "revocaciones" de este documento; y
- Proteger los datos personales de los solicitantes de CDS, que no podrán ser cedidos a terceros bajo ningún concepto de acuerdo a la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

20.3. Obligaciones de las ACs Subordinadas.

Las ACs subordinadas y sus correspondientes ARs deben conocer la Política de Certificados y la Declaración de Prácticas de Certificación de la ACR2-SE, comprometiéndose a seguir las siguientes normas:

- Una AC en ningún caso emitirá certificados con una duración superior a la vigencia del vínculo administrativo existente entre el solicitante y la misma AC;
- Las ACs se comprometen y obligan a proteger sus claves privadas utilizadas en la emisión de CDs con el nivel de seguridad que se especifica en este documento en el apartado "Requerimientos de Seguridad Impuestos a las Autoridades Certificadoras Subordinadas y Autoridades de Servicios Adicionales de Firma Electrónica Avanzada y sus Claves".
- Las Políticas de Certificados de las ACs registradas bajo la ACR2-SE serán tan restrictivas o más que la especificada en este documento;
- Comunicar inmediatamente a la DGNM y a los titulares de los CDs emitidos por la AC, el compromiso, pérdida, divulgación, modificación, uso no autorizado de su clave privada, con el fin de revocar y solicitar a cada usuario volver a generar el par de claves; y
- Las ACs de los PSCs se comprometen y obligan a enviar una copia a la ACR2-SE, de los CDs emitidos de acuerdo a lo establecido en el numeral 76 de las RGPSC.

20.4. Obligaciones de las Entidades de la SE de Alto Nivel.

Es obligación de las entidades de la SE de alto nivel verificar el estado del CD de la ACR2- SE y, las partes que confían, el estado del CD de la entidad de la SE de alto nivel y la validez de su firma electrónica avanzada.

21. Responsabilidades.

21.1. Responsabilidades de la DGNM.

Las responsabilidades que adquiere la DGNM son las siguientes:

- La DGNM, como administrador de la ACR2-SE, garantiza el cumplimiento de las obligaciones descritas en este documento;
- Cualquier anomalía o incidente producidos entre el momento de la revocación de la clave privada de la ACR2-SE y el momento de la notificación de tal acto a las entidades a las que se le han emitido certificados y, posterior revocación de los certificados emitidos, es responsabilidad única y exclusiva de DGNM; y
- Cualquier incidente o responsabilidad nacidos de la clave privada de la ACR2-SE que se encuentra comprometida, es responsabilidad única y exclusiva de DGNM.

21.2. Responsabilidades de la AR-SE.

Es responsabilidad de la AR-SE la correcta identificación de los solicitantes para la emisión de CDs o para la revocación de los mismos.

21.3. Responsabilidades de las ACs Subordinadas.

Las responsabilidades que adquieren las ACs subordinadas son las siguientes:

- Las ACs generarán sus claves criptográficas de acuerdo al Plan de Administración de Claves señalado en los numerales 69, 120, 165, 214 de las RGPSC, del servicio correspondiente;
- Cualquier anomalía o incidente producidos entre el momento de la revocación de un CD emitido por la AC subordinada y el momento de la notificación de tal evento a los usuarios de esa AC, es responsabilidad de ésta última;
- Cualquier incidente o responsabilidad derivados del compromiso de la clave privada de la AC subordinada es responsabilidad de ésta;
- Toda AC subordinada será responsable de revisar el CD que le firme electrónicamente y le entregue la ACR2-SE y, hacer todas las pruebas necesarias antes de poner el CD en operación; igualmente aplica para los CDs de las autoridades de servicios adicionales de firma electrónica avanzada, y de entidades de la SE de alto nivel;
- Las ACs de la DGNM y del Siger deberán cumplir con el marco jurídico en lo referente a las responsabilidades de acuerdo a su normatividad; y
- Los PSCs deberán cumplir con el marco jurídico en lo referente a las responsabilidades de PSCs conformado por el Código de Comercio, RPSC y RGPSC.

21.4. Responsabilidades de las Entidades de la SE de Alto Nivel.

Las responsabilidades que adquieren las entidades de la SE de alto nivel son las siguientes:

- Las entidades de la SE de alto nivel generarán de manera segura sus claves criptográficas y sus requerimientos de CDs, mediante el programa de *software* que la ACR2-SE ponga a su disposición;
- Toda entidad de la SE de alto nivel será responsable de revisar el CD que le firme electrónicamente y le entregue la ACR2-SE y, hacer todas las pruebas necesarias antes de poner el CD en operación.

22. Fin de la Autoridad Certificadora Raíz Segunda de la Secretaría de Economía.

Cuando la ACR2-SE termine las operaciones antes de que hayan expirado todos los CDs, las claves de la ACR2-SE se entregarán a la DGNM. Antes de la terminación de ACR2-SE, ésta proporcionará los datos archivados a la DGNM. Tan pronto como sea posible, la DGNM informará a todas las entidades a las que haya emitido certificados de su terminación, utilizando como método de comunicación escrito físico en su caso de ser así acordado, mediante correo electrónico.

23. Procedimiento de Solicitud de Emisión de Certificados Digitales de Autoridad Certificadora y de Autoridades de Servicios Adicionales de Firma Electrónica Avanzada.

La emisión de un certificado digital firmado por la ACR2-SE se hará bajo el procedimiento descrito a continuación:

1. El director o directora del Siger deberá presentar a la AR-SE de la ACR2-SE el documento de solicitud del certificado de autoridad certificadora de la DGNM y/o del Siger firmado por el director o directora de la DGNM;
2. El director o directora del Siger deberá designar al responsable directo de la autoridad certificadora de la DGNM y mediante un escrito dirigido a la DGNM y firmado;
3. En caso de tratarse de un PSC, éste deberá presentar su documento mediante el cual fue acreditado por la DGNM de conformidad con lo requerido en los trámites SE-09-026-A y SE-09-027-A a la AR-SE. Para la identificación fehaciente del representante legal, se requerirá su presencia física y deberá presentar una identificación oficial vigente como el pasaporte, credencial del IFE o cedula profesional;
4. Confirmada la autenticidad y validez del o los documentos presentados por el PSC, la AR-SE verificará la razonable coincidencia entre la fotografía contenida en aquellas y la apariencia física del representante legal;
5. Las solicitudes quedarán en poder de la AR-SE. Es responsabilidad de la AR-SE comprobar que dichas solicitudes están debidamente requisadas y que todos los datos que aparecen en las mismas son correctos;

6. La AR-SE requerirá al representante legal que firme original y copia de la solicitud para verificar la firma autógrafa de la solicitud con la que aparece en las credenciales oficiales presentadas, considerada a partir de ese momento como aceptada;
7. El PSC deberá designar al profesional informático y responsable directo de la autoridad certificadora y/o autoridades de servicios adicionales de firma electrónica avanzada mediante escrito dirigido a la AR-SE;
8. La ACR2-SE, una vez celebrada la Ceremonia de Datos Creación de Firma Electrónica, emitirá el certificado correspondiente con el certificado que presentarán las autoridades certificadoras subordinadas o el requerimiento de certificado de los servicios adicionales de firma electrónica avanzada de la siguiente forma:

Los PSC emitirán, en el nivel más seguro de sus instalaciones, su certificado digital en formato PKCS#10 y lo auto-firmarán y, para el caso de los servicios adicionales de firma electrónica avanzada el requerimiento de certificado. Dicho certificado o requerimiento será presentado en un medio de almacenamiento removible o vía correo electrónico, para que su clave pública sea certificada por la ACR2-SE.

24. Procedimiento de Identificación de la AR-SE para la solicitud de emisión de CDs a Entidades de la SE de Alto Nivel.

La identificación de las entidades de la SE de alto nivel se hará bajo el procedimiento descrito a continuación:

Como mínimo, incluirá los siguientes pasos:

1. Solicitar por escrito al director o directora de la DGNM el CD.
2. Verificar que la solicitud de expedición del CD de la entidad fue presentada por dicha entidad de la SE;
3. Verificar la existencia de la entidad solicitante a través del uso de registros oficiales de la SE;
4. Establecer la identidad del solicitante mediante pruebas en persona ante la AR-SE, o bien, mediante lo mencionado en la Política al final del apartado "*8. AUTORIDAD REGISTRADORA DE LA AUTORIDAD CERTIFICADORA RAÍZ SEGUNDA DE LA SECRETARÍA DE ECONOMÍA*", basado en lo siguiente:

i. El solicitante presenta su credencial de empleado de la SE actualizada;
ii. El solicitante presenta una forma de identificación actualizada emitida por una autoridad competente (pasaporte o credencial del IFE) como prueba de identidad;
iii. La AR-SE examina la forma de identificación actualizada presentada para validar los datos biométricos que se pueden vincular al solicitante (fotografía o huella digital); y
iv. La legitimidad de la forma de identificación actualizada presentada será verificada por la AR-SE.

5. Registrar y mantener un biométrico del solicitante (fotografía o huella digital) por la AR-SE (las firmas autógrafas no se aceptan como biometría). Esto establece una pista de auditoría para la resolución de disputas.

Adicionalmente, la AR-SE registrará el proceso que se siguió para la emisión del CD. La documentación del proceso y los requisitos de autenticación deben incluir lo siguiente:

- La identidad de la persona que realiza la identificación;
- Una declaración firmada por la persona que verificó la identidad del solicitante (bajo protesta de decir verdad);
- Número(s) único(s) de identificación de la identificación del solicitante, o una copia fotostática legible de la misma;
- La información biométrica del solicitante;
- La fecha y hora de la verificación; y
- Una declaración de identidad firmada por el solicitante utilizando una firma autógrafa y realizada en presencia de la persona que realiza la autenticación de identidad (bajo protesta de decir verdad).

Fecha de última actualización: 31 de julio de 2023.