Referencia: CPS_002.0

Fecha: 18/07/2018
http://www.eguanajuato.gob.mx
Estado del documento: Publicado

PRÁCTICAS Y POLÍTICAS DE CERTIFICACIÓN

Coordinación de Firma Electrónica, Normas y Procedimientos

(Versión 2.0)

INDICE

1. Introducción

En apego a lo establecido en los artículos 27 veinte y siete de la Ley sobre el Uso de Medios Electrónicos y Firma Electrónica, 9 nueve y 20 veinte fracción III del Reglamento sobre el Uso de Medios Electrónicos y Firma Electrónica en el Poder Ejecutivo del Estado de Guanajuato, "La Autoridad Certificadora" del Poder Ejecutivo del Estado de Guanajuato, expide las presentes Políticas y Prácticas de Certificación.

1.1 Glosario:

Para efectos de las presentes Políticas y Prácticas de Certificación se entenderá por:

(C.F.E.N y P.).- La Coordinación de Firma Electrónica, Normas y Procedimientos

(AC).- Autoridad Certificadora.

(PSC).- Prestador de Servicios de Certificación.

(AR).- Autoridad de Registro.

(CRL).- Listas de Revocación de Certificados.

(PC).- Computadora.

(URL).- Dirección de Internet.

(CPS).- Prácticas y Políticas de Certificación.

1.2 Generalidad

El presente documento especifica la Política de Certificación de la **C.F.E.N y P.** (Coordinación de Firma Electrónica, Normas y Procedimientos),

Por lo que respecta al contenido de esta Política de Certificación, se considera que el lector conoce los conceptos básicos de certificación y firma digital, recomendando que en caso de desconocimiento de dichos conceptos, el lector se informe a este respecto.

1.3 Identificación

Nombre: CPS_002.0

Descripción: PRÁCTICAS Y POLÍTICAS DE CERTIFICACIÓN DE LA C.F.E.N y P Versión: 002.0

Fecha de Emisión: 18/07/2018 Localización:
www.eguanajuato.gob.mx

1.4 Comunidad y Ámbito de Aplicación.

1.4.1 Autoridad Certificadora (AC).

Se denomina Autoridad Certificadora a la entidad que emite certificados de usuarios y/o de otras autoridades de certificación.

1.4.2 Prestador de servicios de certificación (PSC).

Entendemos bajo la presente Política a un PSC como aquella entidad que presta servicios concretos relativos al ciclo de vida de los certificados.

Las funciones de PSC pueden ser desempeñadas directamente por la AC o por una entidad delegada.

1.4.3 Autoridad de Registro (AR)

Las Autoridades de registro podrán ser Internas (la propia AC) o Externas.

1.4.4 Solicitante

El solicitante es el sujeto que se encuentra en un estado previo a la obtención del certificado y posterior a su solicitud.

En los certificados de persona moral y/o vinculada, el solicitante es la organización con la cual el suscriptor mantiene una vinculación. Es decir a través de su Representante Legal.

1.4.5 Titular y Firmante

Es la persona física o jurídica a favor de la que se emite el certificado. En el caso de los certificados reconocidos emitidos a una persona física, recibe el nombre de “Firmante”, como se define en el Art. 3 fracción X de la “Ley sobre el uso de Medios Electrónicos y Firma Electrónica para el Estado de Guanajuato y sus Municipios”.

1.4.6 Usuario

En esta política se entiende por Usuario, tercera parte confiante, la persona que voluntariamente confía en el certificado de entidad final emitido por la **AC**, en virtud de la confianza depositada en la propia **AC**., estableciéndose por lo tanto círculo de confianza a tres partes.

1.4.7 Ámbito de Aplicación y Usos

Los Certificados de Firma Electrónica que emite la Autoridad podrán ser usados para:

- Comunicaciones entre el Poder Ejecutivo, Legislativo y Judicial, así como con los organismos Autónomos, los Ayuntamientos y cualquier dependencia o entidad de la Administración Pública Estatal o Municipal.

- Así como en los actos convenios, comunicaciones, procedimientos administrativos, trámites y la prestación de los servicios públicos que correspondan a éstos; así como en las solicitudes y promociones que en relación con los mismos realicen los particulares.

- Para firmar las Listas de Revocación de Certificados u otros sistemas de información sobre el estado de los mismos.

- Firma de comunicaciones internas entre componentes de la infraestructura de certificación.

1.4.8. Usos Prohibidos y no Autorizados

Se prohíbe el uso de los certificados según lo dispuesto en las CPS correspondientes.

No se permite el uso que sea contrario a la legislación vigente en el Estado de Guanajuato, a los convenios internacionales ratificados por el estado Mexicano, a las costumbres, a la moral y al orden público. Tampoco se permite la utilización distinta de lo establecido en esta Política, en la política específica aplicable a cada certificado y en la Declaración de Prácticas de Certificación.

Los certificados no se han diseñado, no se pueden destinar y no se autoriza su uso o reventa como equipos de control de situaciones peligrosas o para usos que requieren actuaciones a prueba de fallos, como el funcionamiento de instalaciones nucleares, sistemas de navegación o comunicaciones aéreas, o sistemas de control de armamento, donde un fallo pudiera directamente conllevar la muerte, lesiones personales o daños medio ambientales severos.

Los certificados de usuarios no pueden emplearse para firmar en el sistema peticiones de emisión, renovación, suspensión, cancelación o revocación de certificados, ni para firmar certificados de clave pública de ningún tipo, ni firmar listas de revocación de certificados (**CRL**).

No están autorizadas las alteraciones en los Certificados, que deberán utilizarse tal y como son suministrados por la **AC**.

1.5. Datos de contacto

Organización responsable: Poder Ejecutivo del Estado de Guanajuato

Autoridad Certificadora: La Secretaría de Finanzas, Inversión y Administración a través de la C. F. E. N y P.

E-mail: soporteti@guanajuato.gob.mx **Teléfono: (473) 73 5 15 79**
Dirección: Conjunto Administrativo Yerbabuena, Carretera Guanajuato- Juventino Rosas Km. 9,5, Col. Yerbabuena**,** Guanajuato, Gto.**C.P.** 36250

2. Cláusulas Generales

2.1. Obligaciones

2.1.1 AC

La **AC** se obligan a lo estipulado en la "Ley sobre el uso de Medios Electrónicos y Firma Electrónica para el Estado de Guanajuato y sus Municipios" y el "Reglamento sobre el Uso de Medios Electrónicos y Firma Electrónica:

- Respetar lo dispuesto en las CPS.
- Emitir certificados conforme a las CPS y a los estándares de aplicación.
- Emitir certificados según la información que obra en su poder y libres de errores de entrada de datos.
- Emitir certificados cuyo contenido mínimo sea el definido por la normativa vigente, cuando sea aplicable.
- Publicar los certificados emitidos en un Registro de Certificados, respetando en todo caso lo dispuesto en materia de protección de datos por la normativa vigente, cuando sea aplicable.
- Suspender, cancelar y revocar los certificados según lo dispuesto en las políticas y publicar las mencionadas revocaciones en la CRL.
- Informar a los Suscriptores de la revocación, cancelación o suspensión de sus certificados, en tiempo y forma de conformidad a la Ley y Reglamento de la materia que nos ocupa.
- Publicar la información del servicio en su página Web.
- Informar sobre las modificaciones de las condiciones del servicio a los Suscriptores, AR que estén vinculadas a ella y usuarios, mediante la publicación de estas y sus modificaciones en su página Web.
- Proteger, con el debido cuidado, los datos de creación de firma mientras estén bajo su custodia si así se contemplase en algún tipo de certificado.
- Establecer los mecanismos de generación y custodia de la información relevante en las actividades descritas, protegiéndolas ante pérdida, destrucción o falsificación.
- Conservar la información sobre el certificado emitido por el período mínimo exigido por la normativa vigente, cuando sea aplicable.

2.1.2 AR

Las Autoridades de Registro son delegadas por la **AC** para realizar determinadas labores, por lo tanto las **AR** también se obligan en los términos definidos en las CPS para la emisión de certificados en aquellas tareas que ejecutan.

2.1.3 Solicitante

El solicitante de un Certificado estará obligado a cumplir con lo dispuesto por la normativa vigente, cuando sea aplicable, y además a:

- Suministrar la información necesaria para realizar una correcta identificación.
- Realizar los esfuerzos que razonablemente estén a su alcance para confirmar la exactitud y veracidad de la información suministrada.
- Notificar cualquier cambio en los datos aportados para la creación del certificado durante su periodo de validez.

2.1.4 Suscriptor

El Suscriptor de un Certificado estará obligado a cumplir con lo dispuesto por la normativa vigente, cuando sea aplicable, y además a:

- Custodiar su clave privada de manera diligente y no deberá proporcionarla
- Realizar los respaldos de su certificado de firma electrónica
- Usar el certificado según lo establecido en las CPS aplicables y en la normativa vigente, si es aplicable.
- Respetar lo dispuesto en los documentos firmados con la **AC** y/o la **AR**.
- Informar a la brevedad de la existencia de alguna causa de suspensión /revocación.
- Notificar cualquier cambio en los datos aportados para la creación del certificado durante su periodo de validez.

2.1.5 Usuario

Será obligación de los Usuarios, terceros que confían en los certificados, cumplir con lo dispuesto por la normativa vigente y además:

- Verificar la validez de los certificados en el momento de realizar cualquier operación basada en los mismos.
- Conocer y sujetarse a las garantías, límites y responsabilidades aplicables en la aceptación y uso de los certificados en los que confía, y aceptar sujetarse a las mismas.

2.1.6 **Registro de Certificados**

La información relativa a la emisión y el estado de los certificados se mantendrá accesible al público en los términos establecidos en la normativa vigente, cuando sea aplicable.

La C.F.E.N y P mantendrá un sistema seguro de almacén y recuperación de certificados públicos y un Registro de Certificados emitidos y de su estado, cuando sea aplicable, pudiendo delegar estas funciones en una tercera entidad. El acceso al Registro de Certificados se realizará desde la Web de la Autoridad de Certificación C.F.E.N y P (www.eguanajuato.gob.mx).

2.2. Responsabilidad

La Autoridad Certificadora del Poder Ejecutivo a través de la C.F.E.N y P, en su actividad de prestación de servicios de certificación, responderá por el incumplimiento de lo establecido en las CPS y, allí donde sea aplicable, por lo que dispone la Ley sobre el uso de Medios Electrónicos y Firma Electrónica para el Estado de Guanajuato y sus Municipios.

Sin perjuicio de lo anterior la C.F.E.N y P. no garantizará los algoritmos y estándares criptográficos utilizados ni responderá de los daños causados por ataques externos a los mismos, siempre que hubiere aplicado la diligencia debida según el estado de la técnica en cada momento, y hubiere actuado conforme a lo dispuesto en la Ley y Reglamento sobre el Uso de Medios Electrónicos y Firma Electrónica para el Estado de Guanajuato y sus Municipios, las CPS.

2.2.1 Exoneración de responsabilidad

La C.F.E.N y P. no será responsable en ningún caso cuando se encuentre ante cualquiera de estas circunstancias:

- Estado de Guerra, desastres naturales, funcionamiento defectuoso de los servicios eléctricos, las redes telemáticas y/o telefónicas o de los equipos informáticos utilizados por el Suscriptor o por los Terceros, o cualquier otro caso de fuerza mayor.

- Por el uso indebido o fraudulento del directorio de certificados y CRL emitidos por la Autoridad de Certificación.

- Por el uso indebido de la información contenida en el Certificado o en la CRL.

- Por el contenido de los mensajes o documentos firmados o encriptados mediante los certificados.

- En relación a acciones u omisiones del Solicitante y Suscriptor:

    - Falta de veracidad de la información suministrada para emitir el certificado.

    - Retraso en la comunicación de las causas de suspensión o revocación del certificado.

    - Ausencia de solicitud de suspensión o revocación del certificado cuando proceda.

    - Negligencia en la conservación de sus datos de creación de firma, en el aseguramiento de su confidencialidad y en la protección de todo acceso o revelación.

    - Uso del certificado fuera de su periodo de vigencia, o cuando la C.F.E.N y P. o la AR le notifique la revocación o suspensión del mismo.

    - Extralimitación en el uso del certificado, según lo dispuesto en la normativa vigente y las CPS en particular.

- En relación a acciones u omisiones del Usuario, tercero que confía en el certificado:

    - Falta de comprobación de las restricciones que figuren en el certificado electrónico o en las PC en cuanto a sus posibles usos.

    - Falta de comprobación de la suspensión o pérdida de vigencia del certificado electrónico publicada en el servicio de consulta sobre la vigencia de los certificados o falta de verificación de la firma electrónica.

2.2.2 Límite de responsabilidad.

La C.F.E.N y P limita su responsabilidad mediante la inclusión de los límites de uso del certificado personal reconocido, expresada en las CPS.

2.3. Interpretación y ejecución

2.3.1 Legislación
La ejecución, interpretación, modificación o validez de las CPS se regirá por lo dispuesto en la legislación del estado de Guanajuato vigente, cuando sea aplicable.

2.3.2 Independencia

La invalidez de una de las cláusulas contenidas en las CPS no afectará al resto de cláusulas. En tal caso se tendrá la mencionada cláusula por no puesta.

2.3.3 Notificación

Cualquier notificación se realizará por correo electrónico dirigido a cualquiera de las direcciones electrónicas referidas en el apartado datos de contacto.

2.4. Tarifas

2.4.1 Tarifas de emisión de certificados En función de lo que se señale en la Ley de Ingresos para el Estado de Guanajuato, para el Ejercicio Fiscal que aplique; y al Acuerdo Administrativo para el Cobre de Productos.

2.4.2 Tarifas de acceso a los certificados

No Estipulado

2.4.3 Tarifas de acceso a la información relativa al estado de los certificados o los certificados revocados

No estipulado.

2.4.4 Tarifas por otros servicios

En función de las condiciones contractuales en cada momento.

2.4.5 Política de reintegros

No aplica.

2.5. Publicación y Registro de Certificados

2.5.1 Publicación de información de la AC

2.5.1.1 CPS

La información sobre el servicio actual y sus distintas versiones están disponibles públicamente en el sitio de Internet http://www.eguanajuato.gob.mx

2.5.1.2 Términos y condiciones

La AC a través de la C.F.E.N y P pone a disposición de los Suscriptores y Usuarios los términos y condiciones del servicio en el sitio de Internet, http://www.eguanajuato.gob.mx

2.5.1.3 Difusión de los certificados

Los certificados de Firma Electrónica que expida la Autoridad son públicos y se encontrarán disponibles en el sitio de Internet http://www.eguanajuato.gob.mx/NuevoPortalFEC/busqueda-de-certificados.
Esta información estará disponible 24 horas al día, 7 días por semana. En caso de fallo del sistema u otros factores que no se encuentran bajo el control de la AC, ésta hará todos los esfuerzos para conseguir que este servicio informativo no esté inaccesible durante un período máximo de 24 horas.

2.5.2 Frecuencia de publicación

Ordinariamente las AC publicaran una lista de certificados revocados en el momento en que tramita una petición de suspensión o revocación autenticada.

La C.F.E.N y P publicará de forma inmediata cualquier modificación en las políticas y prácticas de certificación, manteniendo un histórico de versiones.

2.6. Auditorias

2.6.1 Frecuencia de las auditorías

Se realizarán a criterio de la AC.

2.6.2 Identificación y calificación del auditor

El auditor deberá demostrar solvencia técnica acreditada en la realización de tareas similares. La C.F.E.N yP. Deberá homologar y autorizar a los auditores acreditados.

2.6.3 Relación entre el auditor y la AC

No deberá existir ningún conflicto de intereses que pueda desvirtuar la actuación en su relación con la C.F.E.N y P

2.6.4 Resolución de incidencias

En caso de que sean detectadas incidencias o no-conformidades, se habilitarán las medidas oportunas para su resolución en el menor tiempo posible.

2.7. Confidencialidad

2.7.1 Tipo de información a mantener confidencial

La C.F.E.N y P considerará confidencial toda la información que no esté catalogada expresamente como pública. No se difunde información declarada como confidencial sin el consentimiento expreso por escrito de la entidad u organización que le haya otorgado el carácter de confidencialidad, a no ser que exista una imposición legal.

La C.F.E.N y P dispone de una adecuada política de tratamiento de la información y de los modelos de acuerdos de aceptación que deberán firmar todas las personas que tengan acceso a información confidencial.

La C.F.E.N y P cumplen en todo caso con la normativa vigente en materia de protección de datos y concretamente con lo dispuesto por la Ley de Acceso a la Información en su Artículo 18. Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Guanajuato, Reglamento de Procedimiento de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados y demás normatividad aplicable.

2.7.2 Tipo de información considerada no confidencial

La siguiente información será considerada no confidencial:

- La contenida en las Prácticas y Política de Certificación.
- La información contenida en los certificados, puesto que para su emisión el suscriptor otorga previamente su consentimiento, incluyendo de manera no exhaustiva:
  - Los certificados emitidos o en trámite de emisión.
  - La vinculación del suscriptor a un certificado emitido por el Prestador de Servicios de Certificación.
  - El nombre y los apellidos del suscriptor del certificado, en caso de certificados individuales, así como cualquier otra circunstancia o dato personal del titular, en el supuesto de que sea significativa en función de la finalidad del certificado.

- La dirección de correo electrónico del suscriptor del certificado.
- El periodo de validez del certificado, así como la fecha de emisión del certificado y la fecha de caducidad.
- El número de serie del certificado.
- Los diferentes estados o situaciones del certificado y la fecha del inicio de cada uno de ellos, en concreto: pendiente de generación y/o entrega, válido, revocado, suspendido o caducado y el motivo que provocó el cambio de estado.

- Las listas de revocación de certificados (CRL), así como las restantes informaciones de estado de revocación.
- La información contenida en los depósitos de certificados.
- Cualquier información cuya publicidad sea impuesta normativamente.

2.7.3 Divulgación de información de revocación / suspensión de certificados.

La AC difundirá la información relativa a la suspensión o revocación de un certificado mediante la publicación periódica de las correspondientes CRL.

Se dispondrá de un servicio de consulta de CRL y Certificados en la dirección http://www.eguanajuato.gob.mx

2.7.4 Envío a la Autoridad Competente

Se proporcionará la información solicitada por la autoridad competente en los casos y forma establecidos legalmente.

2.8 Derechos de propiedad intelectual

La propiedad intelectual de estas políticas pertenece a la C.F.E.N y P

La AC será la única entidad que gozará de los derechos de propiedad intelectual sobre los certificados que emita.

La AC concederá licencia no exclusiva para reproducir y distribuir certificados, siempre y cuando la reproducción sea íntegra y no altere elemento alguno del certificado, y sea necesaria en relación con firmas digitales y/o sistemas de cifrado dentro del ámbito de aplicación de esta política.

Las anteriores reglas figuran en los instrumentos vinculantes entre la AC y los suscriptores y los terceros que confían en certificados.

3. Identificación y Autenticación

3.1. Registro inicial

3.1.1 Unicidad de los nombres

Los nombres de los certificados de Autoridad serán únicos.

3.1.2 Procedimiento de resolución de disputas de nombres

La AC no tiene responsabilidad en el caso de resolución de disputas de nombres. La AC no deberá determinar que un solicitante de certificados tiene derecho sobre el nombre que aparece en una solicitud de certificado. Asimismo, no actuará como árbitro o mediador, ni de ningún otro modo deberá resolver disputa alguna concerniente a la propiedad de nombres de personas u organizaciones, nombres de dominio, marcas o nombres comerciales.

La AC se reserva el derecho de rechazar una solicitud de certificado debido a conflicto de nombres.

La asignación de nombres se realizará basándose en la documentación comprobatoria presentada ante la AC.

3.1.3 Reconocimiento, autenticación y función de las marcas registradas

La AC no asume compromisos en la emisión de certificados respecto al uso por los suscriptores de una marca comercial. La C.F.E.N y P no permite deliberadamente el uso de un nombre cuyo derecho de uso no sea propiedad del suscriptor. Sin embargo la AC no está obligada a buscar evidencias de la posesión de marcas registradas antes de la emisión de los certificados.

3.1.4 Métodos de prueba de la posesión de la clave privada

La posesión de la clave privada se demuestra en virtud del procedimiento fiable de entrega y aceptación del correspondiente certificado y par de claves almacenados en su interior.

En los Certificados de usuario deberá asegurarse que posee la clave privada correspondiente.

3.1.5 Autenticación de la identidad de un individuo

Para realizar una correcta verificación de la identidad del suscriptor de certificados personales reconocidos, La C.F.E.N y P conforme al Art.32 de la Ley sobre el uso de medios electrónicos y firma electrónica para el estado de Guanajuato y sus municipios menciona que únicamente pueden recabar datos personales directamente de los titulares de los mismos o con su consentimiento explícito.

3.1.6 Autenticación de la identidad de una organización

Para realizar una correcta verificación de la identidad de una organización para la emisión de certificados, la C.F.E.N y P exige justificar adecuadamente:

- La identidad de la persona física solicitante, según lo expuesto en el punto 3.1.5 o en el caso que sea aplicable, los datos relativos a la constitución y personalidad jurídica de la organización titular

- La extensión y vigencia de las facultades de representación del solicitante.

- Los datos citados deberán comprobarse bien mediante consulta en el registro público en el que estén inscritos los documentos de constitución y de apoderamiento, bien mediante los documentos públicos que sirvan para acreditar los extremos citados de manera fehaciente, cuando aquéllos no sean de inscripción obligatoria.

3.2. Renovación de certificados

La renovación de certificados consiste en la emisión de un nuevo certificado al suscriptor a la fecha de caducidad del certificado original. Antes de renovar un certificado, la AC y/o la AR deberán comprobar que la información empleada para verificar la identidad y los restantes datos del suscriptor continúan siendo válidos.

Si cualquier información del suscriptor hubiere cambiado, se registrará adecuadamente la nueva información, de acuerdo con lo establecido en la sección 3.1.

3.3. Reemisión después de una revocación

La emisión de un nuevo certificado a un suscriptor tras la revocación del certificado previo se tratará de acuerdo con lo establecido en la sección 3.1. En todo caso la AC se reserva la facultad de denegar la reemisión si la causa de la revocación corresponde a los casos de compromiso de la clave privada del suscriptor.

3.4. Solicitud de revocación y/o Cancelación

Pueden solicitar la suspensión, cancelación o revocación de un certificado:

- El propio suscriptor, en cuyo caso deberá solicitar por escrito la cancelación respectiva de su certificado ante la AC y/o AR según lo establecido en el apartado 3.1.
- El superior jerárquico en el supuesto de que el titular del Certificado de Firma Electrónica deje de prestar sus servicios o fallezca
- El representante Legal de una persona jurídico – colectiva, en el caso de que el otrora representante legal deje de fungir como tal o en caso de fallecimiento
- Los operadores autorizados de la AC y/o AR del suscriptor.

4. Identificación y Autenticación

4.1 Solicitud de certificados

La AC gestionará las solicitudes de los certificados internos de administración y operación.

La AC gestionará las solicitudes de Certificados de usuario.

Certificados de usuario reconocidos:

La AC y/o AR informará al solicitante sobre el proceso de emisión, las responsabilidades y las condiciones de uso del certificado y del dispositivo.

La AC y/o AR verificará la identidad del solicitante, y los datos a incluir en el certificado.

Si la verificación es correcta se procederá a la firma del instrumento jurídico vinculante entre el solicitante y la AC y/o AR, convirtiéndose el solicitante en suscriptor, o asignando un suscriptor (persona física) determinado a una petición.

La AC y/o AR le hará entrega o verificará que el suscriptor posee un dispositivo criptográfico hardware de soporte de la clave privada y los dispositivos de acceso a él, si los hubiera. En caso de que el suscriptor aporte su propio dispositivo, éste deberá ser homologado por la C.F.E.N y P previamente a su utilización.

A continuación, el suscriptor generará el par de claves, y creará una contraseña de revocación del certificado a emitir.

4.2. Emisión de certificados

El proceso seguido para la emisión de certificados es el siguiente:

- La Mesa de Servicio ya sea telefónicamente o a través del correo servicioti@guanajuato.gob.mx, reciben la solicitud de certificación de firma electrónica, agendando previamente cita, para lo cual se les proporciona la lista de documentación requerida para el trámite así como los costos, para el caso en que aplique.

- Será a través del personal adscrito a la Coordinación de Mesa de Servicio, quienes fungirán como Agente Certificador de la AC, reciben, revisan documental requerida. Si está completa y correcta la pre- valida y turna al Coordinador de la C.F.E.N y P, para su aprobación y la realización del trámite. El Agente Certificador, genera el requerimiento técnico del certificado de firma electrónica.

- Una vez validados tanto el requerimiento técnico del certificado de firma electrónica y la documentación por parte del Coordinador de la C.F.E.N y P sobre la identidad del solicitante y esta coincide fielmente con el que la muestra, se procede a la firma del “Acuerdo de Aceptación de Certificación de Firma Electrónica” por parte del solicitante.

- Una vez suscrito el "Acuerdo de Aceptación de Certificación de Firma Electrónica" se emite el certificado electrónico. Mismo que es entregado al titular para que este sea almacenado en un dispositivo de almacenamiento, así como se envía vía correo electrónico.

- El certificado generado será enviado de forma segura al Registro de Certificados, que lo pondrá a disposición de los usuarios.

4.3. Aceptación de certificados

Sin perjuicio de lo indicado en el párrafo anterior, el suscriptor dispone de un periodo máximo de siete días naturales para notificar a la AC cualquier defecto en los datos del certificado, o en la publicación de los datos del mismo en el Registro de Certificados de certificados.

4.4. Suspensión, Cancelación y Revocación de certificados

La revocación y la Cancelación de un certificado es la pérdida de validez del mismo, y son irreversibles.

La suspensión, a diferencia de la revocación y cancelación, es la pérdida de validez temporal de un certificado, y es reversible.

4.4.1 Causas de revocación de certificados

La AC podrá revocar un certificado debido a las siguientes causas:

1.- Circunstancias que afectan a la información contenida en el certificado

- Modificación de alguno de los datos contenidos en el certificado.

- Identificación de que alguno de los datos contenidos en la solicitud de certificado es incorrecto.

- Pérdida o cambio del titular de la condición de que llevó a la emisión del certificado.

2.- Circunstancias que afectan a la seguridad de la clave privada o del certificado

- Compromiso de la clave privada o de la infraestructura o sistemas de la AC, siempre que afecte a la fiabilidad de los certificados emitidos a partir de ese incidente.

- Infracción, por parte de la AC o de la AR, de los requisitos previstos en los procedimientos de gestión de certificados, establecidos en las CPS.

- Compromiso o sospecha de compromiso de la seguridad de la clave o del certificado del suscriptor.
  Acceso o utilización no autorizados, por un tercero, de la clave privada del titular.
- El uso indebido del certificado por el titular.
- El incumplimiento por parte del titular de las normas de uso del certificado expuestas en las CPS o en el instrumento jurídico vinculante entre la AC y el titular.

3.- Circunstancias que afectan a la seguridad del dispositivo criptográfico

- Compromiso o sospecha de compromiso de la seguridad del dispositivo criptográfico.
- Pérdida o inutilización por daños del dispositivo criptográfico.
- Acceso no autorizado, por un tercero, a los datos de activación del titular.
- El incumplimiento por parte del suscriptor de las normas de uso del dispositivo criptográfico expuestas en las CPS o en el instrumento jurídico vinculante entre la AC, la AR y el titular.

La AC podrá cancelar un certificado debido a las siguientes:

1.- Circunstancias que afectan al titular.

- Finalización de la relación jurídica entre la AC y el titular.
- Modificación o extinción de la relación jurídica subyacente o causa que permitió la emisión del certificado al titular.
- Infracción por el solicitante del certificado de los requisitos preestablecidos para la solicitud del mismo.
- Infracción por el titular, de sus obligaciones, responsabilidad y garantías, establecidas en el instrumento jurídico correspondiente o en las CPS de la AC.
- La incapacidad sobrevenida, total o parcial.
- Por el fallecimiento del titular.

2. Otras circunstancias

- La suspensión del certificado digital por un período superior al establecido en las CPS.
- Por resolución judicial o administrativa que lo ordene.
- Por la concurrencia de cualquier otra causa especificada en las CPS.

Si la AC no dispone de toda la información necesaria para determinar la revocación cancelación o suspensión de un certificado, pero tienen indicios de su compromiso, podrán decidir su suspensión. En este caso se considerará que el uso del certificado realizado durante el período de suspensión no es válido siempre y cuando el certificado finalmente sea revocado. Será válido si se levanta la suspensión y el certificado vuelve a pasar a la situación de válido. Sin perjuicio de lo anterior, cuando el titular tenga conocimiento de la suspensión del certificado deberá abstenerse de utilizarlo, y contactar con la AC para proceder a su cancelación o al levantamiento de la suspensión, si hubiere lugar.

El instrumento jurídico que vincula a la AC con el titular o suscriptor establecerá que el mismo deberá solicitar la revocación y/o cancelación del certificado en caso de tener conocimiento de alguna de las circunstancias anteriormente indicadas.

4.4.2 Quién puede solicitar la cancelación, suspensión y revocación

Pueden solicitar la suspensión y cancelación de un certificado:

- El propio suscriptor, quien deberá identificarse ante la AC,
- El superior jerárquico en el supuesto de que el titular del Certificado de Firma Electrónica deje de prestar sus servicios o fallezca
- El representante Legal de una persona jurídico – colectiva, en el caso de que el otrora representante legal deje de fungir como tal o en caso de fallecimiento

    - Los operadores autorizados de la AC y/o AR del suscriptor.

Pueden solicitar la revocación de un certificado.

- La Autoridad Certificadora AC.
- La Autoridad de Registro AR.

4.4.3 Procedimiento de cancelación, revocación o suspensión

El procedimiento de solicitud de revocaciones o suspensiones se desahogará en los tiempos y formas que lo establece el Reglamento sobre el Uso de Medios Electrónicos y Firma Electrónica en el Poder Ejecutivo del Estado de Guanajuato

4.4.4 Periodo de revocación

La decisión de revocar o no un certificado será tomada por la AC en un periodo máximo de 30 días hábiles Durante este tiempo el certificado permanecerá suspendido.

La C.F.E.N y P decidirá respecto al estado posterior a la suspensión del certificado (activo, si no procede la solicitud o revocado definitivamente) basándose en la información obtenida hasta ese momento respecto a las causas aducidas para la petición de revocación.

4.4.5 Suspensión

La suspensión es la pérdida de validez temporal de un certificado, y es reversible.

Si la AC a la que se dirige la solicitud de revocación no dispone de toda la información necesaria para determinar la revocación de un certificado, pero tiene indicios de su compromiso, puede decidir su suspensión.

4.4.6 Límites del periodo de suspensión
El periodo máximo de suspensión de un certificado es de 30 días naturales.

4.4.7 Frecuencia de emisión de CRL

La AC de la C.F.E.N y P emitirá una CRL cada vez que se revoca el certificado.

4.4.8 Obligación de comprobación de CRL

Los usuarios deben comprobar obligatoriamente el estado de los certificados en los cuales va a confiar, debiendo comprobar en todo caso la última CRL emitida.

El acceso a las CRL estará disponible también desde la página Web de la AC (www.eguanajuato.gob.mx).

La CRL está firmada por la autoridad de certificación que ha emitido el certificado.

El usuario deberá comprobar que la lista de revocación es la más reciente emitida ya que pueden encontrarse a la vez varias listas de revocación válidas. Los certificados incluyen la información necesaria para el acceso a la CRL.

El usuario deberá asegurarse que la lista de revocación está firmada por la autoridad que ha emitido el certificado que quiere validar.

4.4.9 Disponibilidad de servicios de comprobación del estado de los certificados

La AC proporciona un servicio online de comprobación de revocaciones de manera automática, el cual estará disponible las 24 horas del día los 7 días de la semana. La AC realizará todos los esfuerzos necesarios para que el servicio nunca se encuentre indisponible de forma continua más de 24 horas.

4.4.10 Requisitos de la comprobación del estado de los certificados

Para realizar la comprobación del estado de un certificado el usuario deberá conocer como mínimo el nombre del suscriptor o el número de serie asociado al certificado que desea verificar.

4.4.11 Obligación de consulta del servicio de comprobación del estado de los certificados

El usuario que no utilice la CRL para comprobar la validez de un certificado deberá consultar el Registro de Certificados para confiar en él.

4.5. Procedimientos de Control de Seguridad

4.5.1 Tipos de eventos registrados

La AC registrará y guardará los logs (Archivo electrónico de Registro) de todos los eventos relativos al sistema de seguridad de la AC. Estos incluyen los siguientes eventos:

- Intentos de creación, borrado, establecimiento de contraseñas o cambio de privilegios.
- Intentos de inicio y fin de sesión.
- Intentos de accesos no autorizados al sistema de la AC a través de la red.
- Intentos de accesos no autorizados a la red interna de la AC.
- Acceso físico a los logs.
- Cambios en la configuración y mantenimiento del sistema.
- Encendido y apagado de la aplicación de la AC.
- Cambios en los detalles de la AC y/o sus claves.
- Cambios en la creación de perfiles de certificados.
- Generación de claves propias.

Adicionalmente la AC conservará, ya sea manual o electrónicamente, la siguiente información:

- Registros de acceso físico.
- Mantenimiento y cambios de configuración del sistema.
- Cambios en el personal.
- Registros de la destrucción de material que contenga información de claves, datos de activación o información personal de suscriptor, si se gestiona esa información.

4.5.2 Frecuencia de procesado de *LOGS* de auditoría

Se revisarán los LOGS de auditoría cada semana y en todo caso cuando se produzca una alerta del sistema motivado por la existencia de algún incidente, en busca de actividad sospechosa o no habitual.

4.5.3 Periodos de retención para los LOGS de auditoría

Se almacenará la información de los LOGS de auditoría al menos durante 15 años, siempre que contemplen operaciones relacionadas con Certificados Reconocidos. En otros casos se guardarán durante 6 años.

4.5.4 Protección de los LOGS de auditoría

- Los LOGS de los sistemas serán protegidos de su manipulación.
- Se protege su disponibilidad mediante el almacén en instalaciones externas al centro donde se ubica la Autoridad de Certificación.
- Los dispositivos son manejados en todo momento por personal autorizado.

4.5.5 Procedimientos de backup de los Logs de auditoria

La AC dispondrá de un procedimiento adecuado de backup, de manera que, en caso de pérdida o destrucción de archivos relevantes, estén disponibles en un periodo corto de tiempo las correspondientes copias de backup de los logs.

4.5.6 Sistema de almacenamiento de información de auditoria

La información de la auditoría de eventos será almacenada de manera externa y de forma automatizada por el sistema operativo y por el software de certificación.

4.5.7 Análisis de vulnerabilidades

La AC realizará periódicamente una revisión de discrepancias en la información de los logs y actividades sospechosas, de acuerdo al procedimiento interno establecido al efecto en las CPS.

4.6. Archivo de registros

4.6.1 Tipo de eventos registrados

Se deben guardar los eventos que tengan lugar durante el ciclo de vida del certificado, incluyendo la renovación del mismo. Se debe almacenar por la AC:

- todos los datos de la auditoría.
- todos los datos relativos a los certificados, incluyendo los contratos con los suscriptores y los datos relativos a su identificación.
- solicitudes de emisión y revocación de certificados
- todos los certificados emitidos o publicados
- CRL emitidas o registros del estado de los certificados generados
- la documentación requerida por los auditores

La AC es responsable del correcto archivo de todo este material y documentación.

4.6.2 Periodo de retención para el archivo

Los certificados se conservarán durante el periodo que establezca la legislación vigente aplicable o al menos un año desde su expiración. Los contratos con los suscriptores de certificados reconocidos y cualquier información relativa a la identificación y autenticación del suscriptor serán conservados durante al menos 15 años, o el periodo que establezca la legislación del estado de Guanajuato vigente.

4.6.3 Protección del archivo

La AC asegurará la correcta protección de los archivos mediante la asignación de personal cualificado para su tratamiento y el almacenamiento en cajas de seguridad e instalaciones externas en los casos en que así se requiera.

4.6.4 Procedimientos de backup del archivo

La AC dispondrá de un centro de almacenamiento externo para garantizar la disponibilidad de las copias del archivo de ficheros electrónicos. Los documentos físicos se encuentran almacenados en lugares seguros de acceso restringido solo a personal autorizado.

4.6.5 Procedimientos para obtener y verificar información archivada

Durante la auditoria requerida, el auditor verificará la integridad de la información archivada.

El acceso a la información archivada se realizará solo por personal autorizado.

La AC proporcionará la información y los medios al auditor para poder verificar la información archivada.

4.7. Cambio de clave

Antes de que el certificado de una AC expire se realizará un cambio de claves.

4.8. Recuperación en caso de compromiso de la clave o desastre

La AC deberá desarrollar un plan de contingencias para recuperar todos los sistemas en menos de 48 horas, aunque se asegura la revocación y publicación de información del estado de los certificados en menos de 24 horas.

Cualquier fallo en la consecución de las metas marcadas por este plan de contingencias, será tratado como razonablemente inevitable a no ser que dicho fallo se deba a un incumplimiento de las obligaciones de la AC para implementar dichos procesos.

4.8.1 Instalación de seguridad después de un desastre natural o algún otro tipo de desastre

La AC reestablecerá los servicios críticos (Revocación y publicación de revocados) de acuerdo con esta Política dentro de las 24 horas posteriores a un desastre o emergencia imprevista tomando como base el plan de contingencias y continuidad de negocio existente.

La AC dispondrá de un equipo de cómputo alternativo en caso de ser necesario para la puesta en funcionamiento de los sistemas de certificación.

4.9. Cese de la actividad de la AC

Antes del cese de su actividad la AC realizará las siguientes actuaciones:

- Informará a todos los suscriptores, solicitantes, usuarios, otras AC o entidades con los cuales tenga acuerdos u otro tipo de relación del cese con la anticipación mínima de 2 meses, o el periodo que establezca la legislación vigente.

- Revocará toda autorización a entidades subcontratadas para actuar en nombre de la AC en el procedimiento de emisión de certificados.

- De acuerdo con el artículo 25 de la Ley sobre el Uso de Medios Electrónicos y Firma Electrónica, la AC podrá transferir, con el consentimiento expreso de los suscriptores, la gestión de los certificados que sigan siendo válidos en la fecha en que el cese se produzca a otro prestador de servicios de certificación que los asuma o, en caso contrario, extinguir su vigencia. La AC informará, cuando sea el caso, sobre las características del prestador al que se propone la transferencia de la gestión de los certificados.

- Informará a la administración competente, con la antelación indicada, el cese de su actividad y el destino que se vaya a dar a los certificados, especificando, en su caso, si se va a transferir la gestión y a quien.