Lic. Sergio Javier Reynoso Talamantes, Secretario de Gobierno del Estado de Aguascalientes, con fundamento en los artículos 1, 2, 3, 4, 5, 6, 10, 11, 12, SEGUNDO TRANSITORIO y demás relativos de la Ley Sobre el Uso de Medios Electrónicos de Aguascalientes; 24 fracciones I y XII, 25 fracciones III y IV inciso d), 26 y 29 fracciones XXVI y XLVIX de la Ley Orgánica de la Administración Pública del Estado de Aguascalientes; 32, 35, 36, 38, 40 párrafo primero, 1684, 1686, 1688, 1691, 1691A al 1691K, 1706A al 1706E, 2873A al 2873D, 2874 BIS, 2877, 2878, 2881, 2882, 2884, 2885, 2887, 2890, 2891, 2894 y 2905 BIS del Código Civil del Estado de Aguascalientes; 143 de la Ley del Notariado para el Estado de Aguascalientes; 8 fracciones III y IV de la Ley del Periódico Oficial del Estado y 138 del Reglamento del Registro Público de la Propiedad y del Comercio del Estado de Aguascalientes, tengo a bien modificar los Lineamientos necesarios para instaurar las herramientas tecnológicas de la Firma Electrónica Avanzada aplicable a los actos notariales y registrales que atañen al Registro Público de la Propiedad y del Comercio del Estado, que se emitieron el día ocho de octubre de dos mil doce y se publicaron en el Periódico Oficial del Estado con fecha diecinueve de noviembre del mismo año para incluir en tales lineamientos los actos del Instituto Catastral, del Registro Civil y cualquier otro acto que se emita con fundamento y sustento en la Ley Sobre el Uso de Medios Electrónicos de Aguascalientes a través de las siguientes que constituyen la segunda versión de las:

POLÍTICAS DE CERTIFICACIÓN Y DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN APLICABLES A LA AUTORIDAD CERTIFICADORA DEL ESTADO DE AGUASCALIENTES.

1.0 Introducción

1.1 Resumen

La Ley Sobre el Uso de Medios Electrónicos de Aguascalientes, El Código Civil del Estado de Aguascalientes, la Ley del Notariado para el Estado de Aguascalientes, la Ley de Transparencia y Acceso a la Información Pública del Estado de Aguascalientes, la Ley de Catastro del Estado de Aguascalientes, la Ley del Procedimiento Administrativo del Estado de Aguascalientes, la Ley del Procedimiento Contencioso Administrativo para el Estado de Aguascalientes, el Reglamento del Registro Civil y el Reglamento del Registro Público de la Propiedad y del

Comercio del Estado de Aguascalientes contienen una serie de normas que permiten realizar comunicaciones electrónicas, negocios jurídicos y procedimientos administrativos entre los participantes de estos actos.

Por tal motivo la Secretaría de Gobierno del Estado de Aguascalientes, ha decido implantar una Infraestructura de Llave Pública, la cual dotará de Certificados Digitales que permitan el uso de la Firma Electrónica Avanzada (FEA).

El presente documento contiene las Políticas de Certificación y la Declaración de Prácticas de Certificación las cuales representan los mecanismos que la Secretaría de Gobierno ha llevado a cabo para la operación y administración de la infraestructura, así como los procedimientos que se han implementado para cumplir con su objetivo.

La estructura de este documento está basada en lo dispuesto por en el estándar **RFC 3647**:

- IETF (*Internet Engineering Task Force*) en el documento de referencia denominado "*Internet X.509 Public Key Infraestructure Certificate Policy and Certification Practices Framework*" en su interpretación en español como Infraestructura de Clave Pública: Políticas de Certificación y Declaración de Prácticas de Certificación. El contenido de una política de certificación se encuentra estructurado en base al estándar técnico publicado en los sitios oficiales http://tools.ietf.org/html/rfc3647 y http://www.ietf.org/rfc/rfc3647.txt

  X.509 es un estándar criptográfico de Sector de Normalización de las Telecomunicaciones el cual es el órgano permanente de la Unión Internacional de Telecomunicaciones; X.509 es usado para infraestructuras de claves públicas (en inglés, Public Key Infrastructure o PKI) y especifica, entre otras cosas, formatos estándar para certificados de claves públicas y un algoritmo de validación de la ruta de certificación, para mayor información consulte el sitio oficial de ITU (International Telecommunication Union) http://www.itu.int/rec/T-REC-X.509

Asimismo, se rige bajo la siguiente Normatividad Técnica:

- **RFC 3280**: *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile* en su interpretación en español como el Estándar de internet X.509, Infraestructura de Clave Pública y la lista de Certificados Revocados (CRL) el cual es un estándar para la generación de Certificados y de la lista de Certificados Revocados. Para mayor información revisar la documentación publicada en la siguiente página electrónica: http://www.ietf.org/rfc/rfc3280.txt .
- **RFC 2459**: *Internet X.509 Public Key Infrastructure and CRL Profile* en español como el Estándar de internet X.509, Infraestructura de clave pública y Perfil del CRL. Documento en el que se especifican los perfiles de formato y semántica de los certificados y de la lista de Revocación de Certificados, describe los procedimientos para los procesos de las rutas de certificación. Para mayor información favor de revisar la siguiente página electrónica http://www.ietf.org/rfc/rfc2459.txt, dónde se describe completamente el estándar.
- **RFC 2560:** X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP, en español el Estándar de Internet X.509, infraestructura de clave pública en línea Protocolo de estado de certificados - OCSP. Este documento especifica el uso del protocolo OCSP para determinar el status actual del certificado digital. En el siguiente enlace de la dirección de página web se describe su especificación técnica (http://www.ietf.org/rfc/rfc2560.txt).
- **ITFEA:** Infraestructura Tecnológica de Firma Electrónica Avanzada, regida por la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico (CIDGE) en el país de México, conformada por Secretaría de Economía (SE), Secretaría de la Función Pública (SFP) y Servicios de Administración Tributaria (SAT). Encargadas de emitir los lineamientos para integrarse a ITFEA como Autoridad Certificadora (AC) y por ende, homologas a las AC de México, que tiene como objetivo emitir Certificados Digitales de Firma Electrónica Avanzada, para mayor información consultar la siguiente página electrónica: http://www.cidge.gob.mx/

Por otro lado, para el desarrollo de su contenido, se han tenido en cuenta las normas relativas que contiene la Ley Sobre el Uso de Medios Electrónicos de Aguascalientes, el Código Civil del Estado de Aguascalientes, la Ley del Notariado para el Estado de Aguascalientes, la Ley de

Transparencia y Acceso a la Información Pública del Estado de Aguascalientes, la Ley de Catastro del Estado de Aguascalientes, la Ley del Procedimiento Administrativo del Estado de Aguascalientes, la Ley del Procedimiento Contencioso Administrativo para el Estado de Aguascalientes, el Reglamento del Registro Civil y el Reglamento del Registro Público de la Propiedad y del Comercio del Estado de Aguascalientes.

Además el presente documento incluye todas las actividades que se desarrollarán durante la gestión de los certificados electrónicos en su ciclo de vida, por lo que sirve de guía de la relación que existe entre el operador de la infraestructura y sus suscriptores.

La Autoridad Certificadora del Estado de Aguascalientes asume que el lector conoce los conceptos que se manejan en una Infraestructura de llave pública, conceptos de certificados electrónicos, así como los conceptos relacionados con la firma electrónica; en caso contrario se recomienda al lector que se forme en el conocimiento de los conceptos mencionados antes de seguir en el presente documento.

1.2 Nombre del Documento e Identificación

Nombre del documento	Políticas de Certificación y Declaración de Prácticas de Certificación aplicables a la Autoridad Certificadora del Estado de Aguascalientes
Versión del documento	2.0
Estado del documento	Finalizado.
Fecha de emisión	30/10/2013
Fecha de caducidad	-
OID (Object Identifier)	**2.16.484.201.1.1**
Sitio electrónico de las Políticas de Certificación y Declaración de Prácticas de Certificación	http://www.aguascalientes.gob.mx/AC

1.3 Personas y Entidades Participantes

Este documento regula la comunidad de usuarios que obtienen Certificados Digitales de FEA para diversas relaciones administrativas dentro del Gobierno del Estado de Aguascalientes. Las personas y entidades participantes son:

- La Secretaría de Gobierno, como entidad encargada de la emisión y administración de los Certificados Digitales de FEA.
- La Secretaría de Gobierno, como Autoridad Certificadora del Estado de Aguascalientes.
- La Secretaría de Gobierno, como Entidad encargada de la aprobación y administración de las Políticas de Certificación y la Declaración de Prácticas de Certificación.
- Los servidores públicos y los notarios públicos del Estado de Aguascalientes como solicitantes del certificado de firma electrónica.
- Los servidores públicos y los notarios públicos del Estado de Aguascalientes como titulares del certificado de firma electrónica.
- Las Autoridades de Certificación/Registro encargadas de validar la identidad de los solicitantes de certificados digitales de FEA.
- Los terceros aceptantes de los certificados digitales de FEA emitidos por las autoridades de Certificación/Registro a través de la Autoridad Certificadora del Estado de Aguascalientes.

1.4 Autoridades de Certificación

La Secretaría de Gobierno, actuó como Autoridad de Certificadora Raíz, encargada de realizar el vínculo del par de claves necesarias para emitir certificados digitales de Firma Electrónica Avanzada, mismos que se emitieron de conformidad con los términos de las presentes Políticas de Certificación y Declaración de Prácticas de Certificación en su versión 1.0.

En el momento de emisión de las versión 2.0 de las presentes Políticas de Certificación y Declaración de Prácticas de Certificación, la Autoridad Certificadora que compone la Infraestructura de Llave Pública (PKI) del Estado de Aguascalientes es la siguiente:

Nombre Distintivo	CN = AUTORIDAD CERTIFICADORA DEL ESTADO DE AGUASCALIENTES, OU = SECRETARIA DE GOBIERNO, O = GOBIERNO DEL ESTADO DE AGUASCALIENTES, C = MX, S = AGUASCALIENTES L = AGUASCALIENTES, PostalCode = 20000
Número de serie	30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 31
Periodo de validez	Desde la fecha de publicación en el periódico oficial a las 12:00 PM. Hasta 6 años después de la publicación en el periódico oficial a las 12:00 PM.
Estado	Operativa
Huella digital (SHA-1)	42 61 88 77 82 d5 b4 d3 3a 74 c4 46 10 54 f3 8e da 25 5d 09

1.5 Autoridades de Registro

La Autoridad de Certificación/Registro estará constituida por el personal que dispuso la Secretaría de Gobierno para realizar la expedición de los certificados digitales de FEA, estos servidores públicos tienen por misión realizar las funciones de asistencia a la Autoridad Certificadora del Estado de Aguascalientes en los procedimientos y trámites relacionados con los usuarios de la Firma Electrónica Avanzada, para su identificación, registro y autenticación, garantizando con esto, la correcta asignación de claves a los solicitantes de un certificado de firma electrónica.

La oficina para registro se encuentra ubicada en las instalaciones del Registro Público de la Propiedad y del Comercio del Estado de Aguascalientes.

1.6 Validación de Estatus

Como parte de la infraestructura que la Autoridad Certificadora del Estado de Aguascalientes ha desplegado, se encuentra el servicio de validación de estatus en línea, el cual mediante el protocolo de OCSP (Online Certificate Status Protocol) consistirá en informar, a solicitud de un tercero aceptante, el estado actual de un certificado de firma electrónica emitido por la Autoridad Certificadora del Estado de Aguascalientes. Este servicio está respaldado por un

esquema de alta disponibilidad que garantiza la consulta sobre la vigencia y validez de los certificados digitales de FEA de una manera segura y rápida.

Los convenios que regulen las relaciones entre la Autoridad Certificadora del Estado de Aguascalientes con otras Autoridades Certificadoras, quedará fuera del alcance del presente documento.

1.7 Terceros Aceptantes

Los terceros aceptantes son las personas o dependencias diferentes del titular del certificado de firma electrónica que decidan aceptar y confiar en los certificados emitidos por la Autoridad Certificadora del Estado de Aguascalientes y en las transacciones electrónicas que se lleven a cabo utilizando dichos certificados.

1.8 Uso de los Certificados

1.8.1 Uso apropiado de los Certificados Digitales de FEA

Las Políticas de Certificación y Declaración de Prácticas de Certificación correspondientes a cada tipo de certificados digitales en concreto emitidos por la Autoridad Certificadora del Estado de Aguascalientes, constituye el documento en el que se determinan los usos y limitaciones de cada certificado que tienen como finalidad proveer:

- **Autenticación**: que es la garantía de la identidad del titular del Certificado Digital de FEA al momento de realizar cualquier transacción electrónica con un tercero, el certificado dará la certeza de que la comunicación electrónica se realiza con la persona que dice ser. El titular de un certificado de firma electrónica podrá acreditar su identidad frente a cualquiera ya que se encuentra en posesión del certificado y de la clave privada asociada al mismo.
- **No repudio de origen**: asegura que el documento proviene del suscriptor de quien dice provenir. Esta característica se obtiene mediante la FEA realizada por el Certificado Digital de FEA. El receptor de un mensaje firmado electrónicamente podrá verificar el certificado empleado para esa firma utilizando el servicio de validación de certificados del Gobierno del Estado de Aguascalientes.

- **Integridad**: con el empleo del Certificado Digital de FEA, se permite comprobar que el documento no ha sido modificado por ningún agente externo a la comunicación. Para garantizar la integridad, la criptografía ofrece soluciones basadas en funciones de características especiales, denominadas funciones de resumen, que se utilizan siempre que se utiliza una FEA. El uso de este sistema permite comprobar que un mensaje firmado no ha sido alterado entre el envío y la recepción.
- **Firma electrónica**: que es el mensaje electrónico cifrado criptográficamente que permite al titular firmar trámites o documentos de manera electrónica, fundada en la Ley Sobre el Uso de Medios Electrónicos de Aguascalientes, el Código Civil del Estado de Aguascalientes, la Ley del Notariado para el Estado de Aguascalientes, la Ley de Transparencia y Acceso a la Información Pública del Estado de Aguascalientes, la Ley de Catastro del Estado de Aguascalientes, la Ley del Procedimiento Administrativo del Estado de Aguascalientes, la Ley del Procedimiento Contencioso Administrativo para el Estado de Aguascalientes, el Reglamento del Registro Civil y el Reglamento del Registro Público de la Propiedad y del Comercio del Estado de Aguascalientes. El certificado permitirá la sustitución de la firma autógrafa por la firma electrónica con el fin de facilitar y agilizar los actos y negocios jurídicos notariales y las comunicaciones y procedimientos administrativos entre las dependencias, entidades y organismos que conforman el sector público del Poder Ejecutivo del Estado de Aguascalientes. El certificado digital de FEA emitido por la Autoridad Certificadora del Estado de Aguascalientes vinculado con los documentos electrónicos donde se aplique su Firma Electrónica Avanzada tendrá valor de prueba plena, respecto al hecho de que asegura la integridad, no repudio y autenticidad de los mismos, en los términos que definen las leyes citadas.

1.8.2 Limitaciones y Restricciones en el Uso de los Certificados

Los certificados digitales de FEA emitidos por la Autoridad Certificadora del Estado de Aguascalientes, se expedirán de conformidad a lo que establecen la Ley Sobre el Uso de Medios Electrónicos de Aguascalientes, el Código Civil del Estado de Aguascalientes, la Ley del Notariado para el Estado de Aguascalientes, la Ley de Transparencia y Acceso a la Información

Pública del Estado de Aguascalientes, la Ley de Catastro del Estado de Aguascalientes, la Ley del Procedimiento Administrativo del Estado de Aguascalientes, la Ley del Procedimiento Contencioso Administrativo para el Estado de Aguascalientes, el Reglamento del Registro Civil y el Reglamento del Registro Público de la Propiedad y del Comercio del Estado de Aguascalientes.

Los certificados digitales de FEA emitidos por la Autoridad Certificadora del Estado de Aguascalientes, solamente podrán utilizarse para autenticar al titular (acreditar su identidad) para efectos de la firma electrónica (integridad, no repudio y compromiso con lo firmado). Los certificados no podrán ser empleados para actuar como Autoridad de Registro y/o Autoridad Certificadora, para firmar otros certificados digitales, ni para firmar listas de certificados revocados.

Los servicios de certificación que ofrece la Secretaría de Gobierno, no han sido diseñados ni autorizados para ser utilizados en procesos de alto riesgo o en actividades que sean a prueba de fallos tales como el funcionamiento de equipos hospitalarios, de control de tráfico aéreo o ferroviario, nucleares, o cualquier otra actividad que pudiera conllevar la muerte, lesiones o daños graves al medio ambiente.

Los sistemas ofrecidos por la Autoridad Certificadora/Registradora, aseguran que el par de claves permanecerán desde el momento de su creación bajo el control del usuario, por lo que el titular del certificado de firma electrónica será el único responsable del resguardo y custodia de las mismas.

1.9 Definiciones y Acrónimos

Término	Definición
Autoridad Certificadora:	A la Secretaría de Gobierno del Estado de Aguascalientes en los términos del artículo 2° fracción I de la Ley Sobre el Uso de Medios Electrónicos de Aguascalientes.

Autoridad de Registro	A la Unidad de Firma Electrónica en los términos del artículo 2° fracción XVI de la Ley Sobre el Uso de Medios Electrónicos de Aguascalientes
Certificado Digital	Documento firmado electrónicamente por la Autoridad Certificadora que vincula datos de verificación de firma electrónica al firmante y confirma su identidad, basado en el estándar X.509 V3.
Clave Privada	Las claves criptográficas, datos o códigos únicos que genera el firmante de manera secreta para crear y vincular su Firma Electrónica Avanzada.
Clave Pública	Las claves criptográficas, datos o códigos únicos que utiliza el destinatario para verificar la autenticidad de la firma electrónica del firmante. Ésta se encuentra contenida en el Certificado Digital.
Políticas de Certificación y Declaración de Prácticas de Certificación	El presente documento; mismo que indica el nivel de seguridad asociado al tipo de certificado estructurado con base en el estándar técnico RFC 3647, y además contiene un conjunto de prácticas y procedimientos sobre la información, sobre el sistema de seguridad, soporte, administración, emisión y ciclo de vida del certificado digital.
Dispositivo de creación de firma electrónica	El programa o sistema informático que sirve para aplicar los datos de creación de firma electrónica.
Dispositivo de verificación de firma electrónica	El programa o sistema informático que sirve para aplicar los datos de verificación de firma electrónica.
Firma Electrónica Avanzada (FEA)	Los datos que en forma electrónica son vinculados o asociados a un mensaje de datos y que corresponden inequívocamente al firmante con la finalidad de asegurar la integridad y autenticidad del mismo y que ha sido certificada por el prestador de servicios de certificación.
Agente Certificador/Registrador	El servidor público que preste servicios relacionados con la Firma Electrónica Avanzada y que expide certificados electrónicos.
SEGOB	Secretaría de Gobierno del Estado de Aguascalientes.
Suscriptor	El titular de un certificado de firma electrónica, que voluntariamente confía y hace uso del certificado emitido en su favor por la Autoridad Certificadora del Estado de Aguascalientes. En el momento que el titular de un certificado de firma electrónica decida voluntariamente confiar y hacer uso de su certificado, le serán obligatorias las

	disposiciones contenidas en el presente documento.
Usuario	Los notarios públicos del Estado de Aguascalientes y todos los servidores públicos que desempeñen un cargo en la Administración Pública, incluyendo empleados de confianza, empleados de base, empleados temporales, empleados contratados por terceros, haciendo uso de los recursos informáticos propiedad o bajo responsabilidad del Estado de Aguascalientes.
Token	Dispositivo Criptográfico para el resguardo de la Clave Privada.

1.10 Algoritmos y Parámetros Utilizados

Los algoritmos de firma utilizados para la certificación son RSA con digestión Sha-1, los tamaños de claves son de al menos 1024 bits para usuarios y de 2048 bits para Autoridad Certificadora.

2.0 Disposiciones Generales

2.1.1 Obligaciones y Responsabilidades de los Participantes de la Infraestructura de Clave Pública

En este subcomponente se describen las obligaciones y responsabilidades que aplican en cada uno de los participantes involucrados en la Infraestructura de Clave Pública.

2.1.2 Obligaciones de la Autoridad Certificadora

La Autoridad Certificadora del Estado de Aguascalientes actuará relacionando a un determinado suscriptor con su clave pública mediante la expedición de un certificado de firma electrónica.

Las obligaciones a las que estará sujeta la Autoridad Certificadora del Estado de Aguascalientes se encuentran plasmadas en las presentes Políticas de Certificación y Declaración de Prácticas de Certificación.

La Autoridad Certificadora del Estado de Aguascalientes ha nombrado y podrá nombrar Agentes Certificadores/Registradores para los procesos de identificación y autenticación del solicitante del certificado. En los casos en que la Autoridad Certificadora haya nombrado un Agente Certificador/Registrador para realizar la identificación y la autenticación del suscriptor, será ella misma la responsable de la identificación y la autenticación de sus suscriptores.

No obstante lo anterior, la Autoridad Certificadora del Estado de Aguascalientes llevará a cabo revisiones regulares de los Agentes Certificadores/Registradores para asegurar que cumplan con sus obligaciones según el marco normativo aplicable (incluyendo las tareas de identificación y autenticación). La Secretaría de Gobierno asegurará que todos los aspectos de los servicios que se ofrecen y se gestionen dentro de la Infraestructura de Clave Pública de la Autoridad Certificadora del Estado de Aguascalientes son acordes en todo momento con estas Políticas de Certificación y Declaración de Prácticas de Certificación.

Sin perjuicio de todo lo anterior, se considera relevante mencionar que la Autoridad Certificadora del Estado de Aguascalientes está obligada a prestar los servicios relacionados con la Firma Electrónica Avanzada, dentro de los cuales se encuentran:

- Proporcionar la infraestructura operacional, servicios de certificación, servicios de revocación y servicios de validación de estatus de certificados OCSP (Online Certificate Status Protocol).
- Usar productos confiables y sistemas protegidos contra manipulaciones o modificaciones no autorizadas, que pueden asegurar su seguridad técnica y criptográfica.
- Llevar a cabo los esfuerzos razonables para emplear al personal con la calificación, conocimientos y experiencia necesarios para prestar los servicios de certificación y aplicar las medidas de seguridad fijadas en las Políticas de Certificación y Declaración de Prácticas de Certificación.
- Publicar su certificado de Autoridad Certificadora en http://www.aguascalientes.gob.mx/AC

- Conservar por medios electrónicos toda la información y documentos relacionados con los certificados emitidos, en particular para verificar las firmas hechas usando los certificados ya mencionados.
- Realizar sus operaciones de conformidad con las Políticas de Certificación y Declaración de Prácticas de Certificación.
- Aprobar o rechazar las solicitudes de certificados de acuerdo a las presentes Políticas de Certificación y Declaración de Prácticas de Certificación.
- Emitir certificados conforme a la información proporcionada por el solicitante en el momento de su emisión, misma que debe estar libre de errores en la captura de datos.
- Revocar certificados de acuerdo a lo que marcan las Políticas de Certificación y Declaración de Prácticas de Certificación, asimismo publicar y actualizar la lista de certificados revocados con la frecuencia estipulada.
- Contar con un servicio de validación en línea que implemente el protocolo OCSP para la verificación del estado de un certificado determinado.

2.1.3 Obligaciones del Agente Certificador/Registrador

EL Agente Certificador/Registrador de la Autoridad Certificadora del Estado de Aguascalientes actuará relacionando a un determinado titular con su clave pública mediante la expedición de un certificado de firma electrónica, todo ello de conformidad con la Ley Sobre el Uso de Medios Electrónicos de Aguascalientes, el Código Civil del Estado de Aguascalientes, la Ley del Notariado para el Estado de Aguascalientes, la Ley de Transparencia y Acceso a la Información Pública del Estado de Aguascalientes, la Ley de Catastro del Estado de Aguascalientes, la Ley del Procedimiento Administrativo del Estado de Aguascalientes, la Ley del Procedimiento Contencioso Administrativo para el Estado de Aguascalientes, el Reglamento del Registro Civil, y el Reglamento del Registro Público de la Propiedad y del Comercio del Estado de Aguascalientes y con las presentes Políticas de Certificación y Declaración de Prácticas de Certificación.

Los servicios que prestará el Agente Certificador/Registrador de la Autoridad Certificadora del Estado de Aguascalientes en el contexto de estas Políticas de Certificación y Declaración de

Prácticas de Certificación, son los servicios de emisión y revocación de certificados digitales de FEA, así pues la Autoridad Certificadora tiene las siguientes obligaciones:

- Realizar sus operaciones en conformidad con las presentes Políticas de Certificación y Declaración de Prácticas de Certificación.
- Realizar sus operaciones conforme a la legislación aplicable, es decir, de acuerdo a la Ley Sobre el Uso de Medios Electrónicos de Aguascalientes, el Código Civil del Estado de Aguascalientes, la Ley del Notariado para el Estado de Aguascalientes, la Ley de Transparencia y Acceso a la Información Pública del Estado de Aguascalientes, la Ley de Catastro del Estado de Aguascalientes, la Ley del Procedimiento Administrativo del Estado de Aguascalientes, la Ley del Procedimiento Contencioso Administrativo para el Estado de Aguascalientes, el Reglamento del Registro Civil y el Reglamento del Registro Público de la Propiedad y del Comercio del Estado de Aguascalientes.
- Realizar la publicación de las presentes Políticas de Certificación y Declaración de Prácticas de Certificación en el sitio electrónico designado, y en el Periódico Oficial del Estado.
- Comunicar cualquier cambio o adecuación de las presentes Políticas de Certificación y Declaración de Prácticas de Certificación, la comunicación o notificación se realizará tal y como viene marcado en la sección 8.0 del presente documento, y se publicará en el Periódico Oficial del Estado.
- Utilizar sistemas y productos fiables que estén protegidos contra toda alteración, que aseguren la seguridad criptográfica de los procesos de certificación.
- Atender las solicitudes de certificados digitales de FEA de los usuarios en un tiempo razonable.
- Aprobar o rechazar las solicitudes de acuerdo a lo que marcan las presentes Políticas de Certificación y Declaración de Prácticas de Certificación.
- Emitir certificados digitales de FEA conforme a la información proporcionada por el solicitante en el momento de su emisión, misma que esté libre de errores en la entrada de datos.
- Revocar certificados digitales de FEA de acuerdo a lo que marca la sección *4.4 Revocación de Certificados Digitales de FEA,* asimismo de publicar y actualizar la Lista de Certificados Revocados con la frecuencia estipulada.

- Contar con un servicio de validación en línea que implemente el protocolo OCSP para la verificación del estado de un certificado de firma electrónica determinado.
- Poner a disposición de sus suscriptores el certificado de firma electrónica de la Autoridad Certificadora del Estado de Aguascalientes.
- No almacenar en ningún caso los datos de creación de firma, clave privada, de los titulares de certificados digitales de FEA.
- Otorgar todas las facilidades para que se realicen los debidos procesos de auditoría.

2.1.4 Obligaciones del Solicitante de Certificado de Firma Electrónica

Es obligación de los solicitantes de certificados digitales de FEA bajo las presentes Políticas de Certificación y Declaración de Prácticas de Certificación:

- Presentar un dispositivo de almacenamiento nuevo y con empaque sellado para el resguardo de su par de claves criptográficas.
- Proporcionar toda la información que marca el procedimiento de solicitud de certificado de firma electrónica.
- Proporcionar información veraz para realizar la comprobación de su identidad.
- Notificar cualquier cambio de los datos proporcionados para la generación de su certificado de firma electrónica durante el período de validez de éste.
- Aceptar las condiciones y términos que la Autoridad Certificadora del Estado de Aguascalientes dispone en las presentes Políticas de Certificación y Declaración de Prácticas de Certificación para los certificados digitales de FEA.

2.1.5 Obligaciones de los Titulares de Certificado de Firma Electrónica

Es obligación de los titulares de certificados digitales de FEA bajo las presentes Políticas de Certificación y Declaración de Prácticas de Certificación:

- Suministrar a los Agentes Certificadores/Registradores información exacta, completa y veraz con relación a los datos que estos le soliciten para completar el proceso de certificación de firma electrónica.
- Conservar y utilizar de forma correcta el certificado de firma electrónica y su par de claves de acuerdo a la normatividad vigente.

- Proteger y custodiar su clave de anulación, su clave privada y su certificado electrónico asociado, empleando las medidas necesarias para evitar su pérdida, revelación, alteración o uso no autorizado.
- Proteger el dispositivo de almacenamiento empleando las medidas necesarias para evitar su pérdida, revelación, alteración o uso no autorizado.
- Respetar las condiciones y términos firmados durante la solicitud de certificado de firma electrónica.
- Solicitar de manera oportuna al Agente Certificador/Registrador de la Autoridad Certificadora del Estado de Aguascalientes la revocación de su certificado de firma electrónica en caso de sospechar o tener conocimiento de que su clave privada ha sido: robada, extraviada o sea conocida por terceros; la forma de solicitar dicha revocación se especifica en la sección *3.4 Solicitud de revocación.*
- Aceptar las restricciones impuestas a su par de claves y certificado de firma electrónica emitidas por el Agente Certificador/Registrador de la Autoridad Certificadora del Estado de Aguascalientes.
- No manipular o realizar actos de ingeniería inversa sobre la implementación técnica de los servicios de certificación y Firma Electrónica Avanzada (incluye hardware/software).

2.1.6 Obligaciones de los Usuarios y Terceros Aceptantes

Es obligación de los usuarios y terceros que confían y aceptan los certificados digitales de FEA emitidos por la Autoridad Certificadora del Estado de Aguascalientes en los términos de las presentes Políticas de Certificación y Declaración de Prácticas de Certificación:

- Verificar la validez de los certificados digitales de FEA en el momento de realizar cualquier transacción basada en estos.
- Conocer y sujetarse a las garantías, límites y responsabilidades derivadas de la aceptación de los certificados digitales de FEA en los que confía y asumir sus obligaciones.
- Limitarse a los usos permitidos de los certificados digitales de FEA establecidos en las extensiones de los mismos y en estas Políticas de Certificación y Declaración de Prácticas de Certificación.

- Asumir su responsabilidad en la comprobación de la validez o revocación de los certificados digitales de FEA en que confía.
- Asumir su responsabilidad en la correcta verificación de las firmas electrónicas.
- Notificar cualquier hecho o situación fuera de lo común relativa al certificado de firma electrónica a través de los medios electrónicos que disponga el Agente Certificador/Registrador de la Autoridad Certificadora del Estado de Aguascalientes, en el sitio http://www.aguascalientes.gob.mx/AC o en el correo electrónico autoridad.certificadora@aguascalientes.gob.mx.
- Para confiar en los certificados digitales de FEA emitidos por la Autoridad Certificadora del Estado de Aguascalientes todos los involucrados en el proceso de firma electrónica deberán conocer y aceptar toda restricción a la que está sujeto el certificado de firma electrónica.

Respecto de la confianza en las firmas electrónicas:

- Los involucrados en un proceso de firma electrónica y el personal de informática o sistemas a su servicio, deberán adoptar las medidas necesarias para determinar la fiabilidad de la firma a través del establecimiento de toda la cadena de certificación y verificando la vigencia y el estado de cada uno de los certificados de dicha cadena.
- El personal encargado de proporcionar los sistemas donde se integre la firma electrónica, deberá conocer e informarse del contenido de las presentes Políticas de Certificación y Declaración de Prácticas de Certificación.
- Cuando se realice una operación o transacción electrónica que pueda ser considerada como ilícita o se dé un uso no conforme a lo establecido en las presentes Políticas de Certificación y Declaración de Prácticas de Certificación, no se deberá confiar en la firma electrónica.

2.1.7 Obligaciones de la Autoridad de Registro (Agentes Registradores)

Es obligación de la Autoridad de Registro:

- Realizar sus operaciones en conformidad con las presentes Políticas de Certificación y Declaración de Prácticas de Certificación.

- Realizar la comprobación exhaustiva de la identidad de los solicitantes de certificado de firma electrónica.
- Comunicar al solicitante la correcta emisión del certificado de firma electrónica.
- Notificar a los titulares de certificados digitales de FEA la revocación de sus certificados cuando se produzca a petición de una autoridad competente o mediante un oficio de la Secretaría de Gobierno.
- Tramitar las peticiones de revocación lo antes posible.
- Comprobar que toda la información incluida en el certificado de firma electrónica sea correcta.

2.2 Responsabilidades

2.2.1 Limitaciones de Responsabilidad

La Secretaría de Gobierno restringe su responsabilidad mediante la inclusión de los límites de uso de la Firma Electrónica Avanzada plasmada en las presentes Políticas de Certificación y Declaración de Prácticas de Certificación al grado establecido en la legislación aplicable, los acuerdos del titular de certificado de firma electrónica y los acuerdos de terceros aceptantes de los certificados digitales de FEA emitidos por la Autoridad Certificadora del Estado de Aguascalientes.

Las limitaciones de responsabilidad suponen la exclusión de responsabilidad por daños y perjuicios fortuitos o imprevistos directos o indirectos.

2.2.2 Responsabilidad del Agente Certificador/Registrador.

La Secretaría de Gobierno, como dependencia encargada de la Autoridad Certificadora responderá en caso de incumplimiento de las obligaciones contenidas en la Ley Sobre el Uso de Medios Electrónicos de Aguascalientes, el Código Civil del Estado de Aguascalientes, la Ley del Notariado para el Estado de Aguascalientes, la Ley de Transparencia y Acceso a la Información Pública del Estado de Aguascalientes, la Ley de Catastro del Estado de Aguascalientes, la Ley del Procedimiento Administrativo del Estado de Aguascalientes, la Ley del Procedimiento Contencioso Administrativo para el Estado de Aguascalientes, el Reglamento del Registro Civil y el Reglamento del Registro Público de la Propiedad y del

Comercio del Estado de Aguascalientes y conforme a lo establecido en las presentes Políticas de Certificación y Declaración de Prácticas de Certificación deberá:

- Garantizar el cumplimiento de las obligaciones descritas en este documento.
- Asegurar que no existen errores en la información contenida en el certificado de firma electrónica que fueron introducidos por la Autoridad Certificadora durante la generación de éste o al emitir la Firma Electrónica Avanzada.
- Asegurar que no exista información falsa en el certificado de firma electrónica que sean de conocimiento u originadas por los agentes de registro que aprueban las solicitudes de certificados digitales de FEA.
- Llevar a cabo la correcta identificación de los solicitantes de certificados digitales de FEA para la emisión de los mismos.
- Llevar a cabo la correcta identificación de los solicitantes de revocación de certificados digitales de FEA para realizar la referida revocación.
- Actuar con diligencia profesional en las tareas inherentes a la administración de la solicitud de certificado de firma electrónica y emisión del certificado de firma electrónica.
- Garantizar que su firma electrónica cumpla con todos los requerimientos descritos en estas Políticas de Certificación y Declaración de Prácticas de Certificación.
- Garantizar que los servicios de revocación y uso de los repositorios se lleven acabo de acuerdo a lo estipulado en estas Políticas de Certificación y Declaración de Prácticas de Certificación.
- La Secretaría de Gobierno no será responsable del contenido de aquellos documentos firmados electrónicamente por los titulares de un certificado de firma electrónica.
- La Secretaría de Gobierno no garantizará los algoritmos criptográficos ni se hará responsable por los daños causados a través de ataques externos a los referidos algoritmos criptográficos empleados en la tecnología dispuesta, siempre y cuando hubiere guardado el proceso debido de acuerdo a la situación actual de la técnica y haya procedido respetando las presentes Políticas de Certificación y Declaración de Prácticas de Certificación, la Ley Sobre el Uso de Medios Electrónicos de Aguascalientes, el Código Civil del Estado de Aguascalientes, la Ley del Notariado para el Estado de Aguascalientes, la Ley de Transparencia y Acceso a la Información Pública

del Estado de Aguascalientes, la Ley de Catastro del Estado de Aguascalientes, la Ley del Procedimiento Administrativo del Estado de Aguascalientes, la Ley del Procedimiento Contencioso Administrativo para el Estado de Aguascalientes, el Reglamento del Registro Civil y el Reglamento del Registro Público de la Propiedad y del Comercio del Estado de Aguascalientes.

2.2.3 Responsabilidad de los Titulares de Certificados Digitales de FEA

La Secretaría de Gobierno requiere que sus suscriptores aseguren y garanticen que:

- Ninguna persona distinta al titular ha tenido acceso a su clave privada.
- Todas las declaraciones efectuadas ante la Autoridad de Registro y la información proporcionada al solicitar su certificado de firma electrónica son verdaderas.
- Toda la información contenida en su Firma Electrónica Avanzada es verdadera.
- Cada Firma Electrónica Avanzada ha sido generada usando su clave privada correspondiente a la clave pública incluida en su certificado de firma electrónica; que dicho certificado ha sido aceptado y está en operación, es decir está vigente y no ha sido revocado al momento de la generación de la firma electrónica.
- La firma electrónica se utiliza exclusivamente para propósitos autorizados y legales conforme a lo establecido en estas Políticas de Certificación y Declaración de Prácticas de Certificación y la Ley Sobre el Uso de Medios Electrónicos de Aguascalientes, el Código Civil del Estado de Aguascalientes, la Ley del Notariado para el Estado de Aguascalientes, la Ley de Transparencia y Acceso a la Información Pública del Estado de Aguascalientes, la Ley de Catastro del Estado de Aguascalientes, la Ley del Procedimiento Administrativo del Estado de Aguascalientes, la Ley del Procedimiento Contencioso Administrativo para el Estado de Aguascalientes, el Reglamento del Registro Civil, y el Reglamento del Registro Público de la Propiedad y del Comercio del Estado de Aguascalientes.
- El titular es un servidor público o un notario público del Estado de Aguascalientes y no un Agente Certificador/Registrador.

- El titular no utilizará su clave privada para firmar electrónicamente certificados digitales de FEA, listas de certificados revocados u otro elemento relativo a las funciones atribuibles a un Agente Certificador/Registrador.

2.2.4 Responsabilidad de la Autoridad de Registro

Las Autoridades de Registro asumirán toda responsabilidad sobre la correcta identificación de los solicitantes de certificados digitales de FEA, así como la validación de la información proporcionada. Las autoridades de registro se suscribirán a las mismas limitaciones que establece la Autoridad Certificadora del Estado de Aguascalientes.

2.2.5 Responsabilidad de los Usuarios y Terceros Aceptantes

- Los terceros aceptantes asumirán la responsabilidad de confiar en la información contenida en la Firma Electrónica Avanzada ya que reconocen que cuentan con la suficiente información para tomar una decisión apropiada y compatible con el grado de confianza que ellos decidan asignar.
- Serán los únicos responsables de decidir si confían o no en la información recibida y asumen las consecuencias legales en el caso de incumplir las obligaciones a las que están sujetos dentro de estas Políticas de Certificación y Declaración de Prácticas de Certificación.
- El Agente Certificador/Registrador asegurará y garantizará que toda la información contenida en el certificado de firma electrónica emitido por éste, es veraz.
- El Agente Certificador/Registrador, incorporará los mecanismos criptográficos necesarios para que el suscriptor o titular de un certificado de firma electrónica genere su par de claves y para constatar que el suscriptor ha aceptado el certificado de acuerdo a lo previsto en las presentes Políticas de Certificación y Declaración de Prácticas de Certificación.

2.2.6 Delimitación de Responsabilidad

La Autoridad Certificadora del Estado de Aguascalientes no asume ninguna responsabilidad ante cualquiera de las siguientes circunstancias:

- Estado de guerra, desastres naturales, funcionamiento defectuoso de los servicios eléctricos, redes de telecomunicaciones, redes telefónicas, virus informático, ni funcionamiento defectuoso de los equipos informáticos utilizados por el titular o por los terceros o cualquier otro supuesto de caso fortuito o de fuerza mayor.
- Uso indebido o fraudulento del directorio de certificados digitales de FEA y lista de certificados revocados emitidas por la Autoridad Certificadora del Estado de Aguascalientes.
- Uso de certificados digitales de FEA que exceda los límites establecidos por los mismos y el presente documento.
- Uso indebido de la información contenida en la Firma Electrónica Avanzada.
- Por el contenido de los mensajes de datos o documentos electrónicos firmados o cifrados mediante la Firma Electrónica Avanzada.
- En relación a acciones u omisiones del solicitante o titular de certificado de firma electrónica:
  - Falta de veracidad de la información suministrada durante la solicitud de certificado de firma electrónica.
  - Retraso en la comunicación/notificación de las causas de revocación del certificado de firma electrónica.
  - Ausencia de solicitud de revocación del certificado de firma electrónica cuando proceda.
  - Negligencia en la conservación de sus datos de creación de firma o clave privada, en el aseguramiento de su confidencialidad y en la protección de todo acceso o revelación.
  - Uso del certificado de firma electrónica fuera de su periodo de vigencia, o cuando la Secretaría de Gobierno le notifique la revocación del mismo.

- En relación a acciones u omisiones de los usuarios o terceros aceptantes del certificado de firma electrónica:

- Falta de comprobación de las restricciones que figuren en el certificado de firma electrónica o en estas Políticas de Certificación y Declaración de Prácticas de Certificación en cuanto a sus posibles usos.
- Falta de comprobación de la revocación o pérdida de vigencia del certificado de firma electrónica publicada en el servicio de consulta de lista de certificados revocados, o falta de verificación de la Firma Electrónica Avanzada.

2.3 Responsabilidades Económicas

2.3.1 Indemnización por Parte de los Titulares

En los términos del Código Civil del Estado de Aguascalientes, de la Ley del Notariado para el Estado de Aguascalientes, la Ley de Transparencia y Acceso a la Información Pública del Estado de Aguascalientes, la Ley de Catastro del Estado de Aguascalientes, y de la Ley de Responsabilidades de los Servidores Públicos del Estado de Aguascalientes, los titulares del certificado de firma electrónica indemnizarán a la Secretaría de Gobierno por:

- Falsedad o mala representación de hecho por parte del titular en la solicitud de certificado de Firma Electrónica Avanzada.
- Omisión por parte del titular de revelar un hecho destacado en la solicitud de certificado de firma electrónica, si la falsedad u omisión fue realizada negligentemente o con la intención de engañar a una persona o Autoridad de Registro.
- Errores del titular en la protección de su clave privada, en el uso de un sistema de confianza, o en la toma de las precauciones necesarias para prevenir el compromiso, pérdida, entrega, modificación o uso no autorizado de su clave privada.
- El uso de parte del titular de un nombre (incluyendo sin limitación un nombre común, nombre de dominio, o correo electrónico) que infrinja los derechos de propiedad intelectual de un tercero.

2.3.2 Indemnización por Parte de los Usuarios o Terceros Aceptantes de Certificados Digitales de FEA.

En los términos de la Ley Sobre el Uso de Medios Electrónicos de Aguascalientes, del Código Civil del Estado de Aguascalientes, de la Ley del Notariado para el Estado de Aguascalientes, la Ley de Transparencia y Acceso a la Información Pública del Estado de Aguascalientes, la Ley de Catastro del Estado de Aguascalientes, y de la Ley de Responsabilidades de los Servidores Públicos del Estado de Aguascalientes, los usuarios o terceros aceptantes de certificados digitales indemnizarán a la Secretaría de Gobierno por:

- Incumplimiento de los terceros aceptantes del certificado de firma electrónica respecto a las obligaciones a las que está sujeto al aceptar la presente declaración.
- Omisión por parte de los terceros aceptantes de certificado de firma electrónica de verificar el estado del certificado de firma electrónica que estuviese vencido o esté revocado.

2.4 Normatividad y Legislación Aplicable

Las operaciones y funcionamiento de la Autoridad Certificadora del Estado de Aguascalientes, así como las presentes Políticas de Certificación y Declaración de Prácticas de Certificación se fundamentan y son de aplicación para cada tipo de certificado en los términos establecidos en la Ley Sobre el Uso de Medios Electrónicos de Aguascalientes, el Código Civil del Estado de Aguascalientes, la Ley del Notariado para el Estado de Aguascalientes, la Ley de Transparencia y Acceso a la Información Pública del Estado de Aguascalientes, la Ley de Catastro del Estado de Aguascalientes, la Ley del Procedimiento Administrativo del Estado de Aguascalientes, la Ley del Procedimiento Contencioso Administrativo para el Estado de Aguascalientes, el Reglamento del Registro Civil y el Reglamento del Registro Público de la Propiedad y del Comercio del Estado de Aguascalientes.

2.4.1 Independencia

En el caso de que una o más disposiciones de estas Políticas de Certificación y Declaración de Prácticas de Certificación se declarasen inválidas, nulas, o inexigibles legalmente, se entenderán por no puestas, conservando su vigencia aquellas sobre las que no se hubiese decretado tal pronunciamiento.

2.5 Tarifas

2.5.1 Tarifas de emisión de Certificados Digitales de FEA o Recertificación

La Secretaría de Gobierno prestará a los suscriptores de la Autoridad Certificadora los servicios de emisión, administración de certificados digitales de FEA, y recertificación, por los que se cobrarán en los términos de la legislación de ingresos que determine los derechos que correspondan.

2.5.2 Tarifas de Acceso a los Certificados Digitales de FEA

Por los servicios que prestará la Secretaría de Gobierno como Autoridad Certificadora consistentes en tener disponibles dentro de un repositorio o mediante otra forma de hacer disponibles los certificados digitales de FEA a terceros que confían en éstos, no se cobrará derecho alguno.

2.5.3 Tarifas de Acceso a la Información Relativa al Estado de los Certificados Digitales de FEA o Revocación.

Por los servicios que prestará la Secretaría de Gobierno como Autoridad Certificadora consistentes en tener disponibles dentro de un repositorio o mediante otra forma de hacer disponibles la lista de certificados revocados a terceros que confían en éstos, tampoco se cobrará derecho alguno, sin embargo, se cobrará el servicio de entrega de listas de certificados revocados adaptadas a necesidades específicas, servicios de validación en línea y otros servicios de valor agregado relacionados con la revocación del certificado de Firma Electrónica Avanzada o la información relativa al estado de los certificados digitales de FEA en los términos de la legislación de ingresos que determine los derechos que correspondan.

2.5.4 Tarifas de Otros Servicios

No se cobrará derecho alguno por el servicio de información sobre las presentes Políticas de Certificación y Declaración de Prácticas de Certificación. Sin embargo cualquier uso para propósitos diversos al de conocer el contenido de este documento, como la reproducción,

redistribución, modificación o creación de obras derivadas, queda sujeto a un acuerdo de licencia con la Secretaría de Gobierno.

2.6 Publicación y Repositorios de Información

La Secretaría de Gobierno pone a disposición de los suscriptores, usuarios y terceros que confían en los certificados emitidos por ésta, información de carácter público que está relacionada con la Autoridad Certificadora y los servicios que ofrece, dentro de esta información se incluye:

- Sitio electrónico para la consulta del Certificado de firma electrónica de la Autoridad Certificadora del Estado de Aguascalientes URL: ***http://www.aguascalientes.gob.mx/AC***
- Sitio electrónico para la consulta de las Políticas de Certificación y Declaración de Prácticas de Certificación de la Autoridad Certificadora del Estado de Aguascalientes.URL: ***http:// www.aguascalientes.gob.mx/AC***
- Sitio electrónico para la consulta de los términos y condiciones de los servicios de la Autoridad Certificadora del Estado de Aguascalientes.URL: ***http:// www.aguascalientes.gob.mx/AC***

Esta información estará disponible veinticuatro horas al día los siete días de la semana; en caso de falla del sistema u otros factores que no se encuentren bajo el control de a Secretaría de Gobierno, ésta realizará todas las acciones pertinentes con la debida diligencia para restablecer el servicio.

2.6.1 Frecuencia de Publicación de la Lista de Certificados Revocados

La Secretaría de Gobierno publicará la lista de certificados revocados en el momento en que se tramite una petición de revocación autenticada.

La Secretaría de Gobierno publicará de forma inmediata cualquier modificación en las políticas y prácticas de certificación, manteniendo un histórico de versiones.

2.6.2 Controles de Acceso a los Repositorios

El acceso a la información mencionada con anterioridad (certificado de la Autoridad Certificadora, Políticas de Certificación y Declaración de Prácticas de Certificación, términos y condiciones) permanecerá publicada en los repositorios de forma abierta, sin embargo la Secretaría de Gobierno es la única dependencia autorizada para modificar, sustituir o eliminar información del repositorio y sitios electrónicos; para ello ha establecido controles de seguridad físicos y lógicos que impiden a otras personas no autorizadas manipular esta información.

La Secretaría de Gobierno requiere que los terceros emitan su consentimiento y manifiesten plena conformidad al acuerdo establecido para tales efectos, y al acuerdo de uso de la lista de certificados revocados, como condición para acceder a la información de que se encuentra en los repositorios.

2.7 Auditoría de Cumplimiento

2.7.1 Frecuencia de la auditoría

Se llevará a cabo una auditoría anual sobre la infraestructura de llave pública montada para soportar la Autoridad Certificadora del Estado de Aguascalientes; sin perjuicio de las auditorías contempladas dentro del sistema normativo general.

2.7.2 Aspectos Cubiertos por los Controles

La auditoría determinará la adecuación de los servicios que ha prestado durante el periodo en revisión la Autoridad Certificadora con lo dispuesto en las presentes Políticas de Certificación y Declaración de Prácticas de Certificación.

2.7.3 Comunicación de Resultados

La Secretaría de Fiscalización y Rendición de Cuentas comunicará los resultados de la auditoría a la Secretaría de Gobierno que es la responsable de custodiar a la Autoridad Certificadora,

encargada de la administración y actualización de las Políticas de Certificación y Declaración de Prácticas de Certificación; la comunicación de los mismos se realizará con absoluta discreción.

2.8 Confidencialidad y Privacidad de la Información

2.8.1 Ámbito de la Información Confidencial

La Secretaría de Gobierno considerará confidencial o reservada toda la información que así se determine por la legislación en la materia. No se difundirá información confidencial o reservada sin el consentimiento expreso por escrito del interesado, a menos que resulte obligatorio por mandato de ley, reglamento o judicial.

Se declara expresamente como información confidencial:

- La clave privada de la Autoridad Certificadora del Estado de Aguascalientes, la cual, al ser el punto de máxima confianza será generada y custodiada conforme a lo especificado en las presentes Políticas de Certificación y Declaración de Prácticas de Certificación.
- La clave privada de los suscriptores de la Autoridad Certificadora del Estado de Aguascalientes.
- Los registros de solicitud de certificado de firma electrónica.
- Los registros de transacciones (registros completos y registros de auditoría de dichas transacciones)
- Los registros de auditoría creados o retenidos por la Secretaría de Gobierno.
- Los planes de contingencia y planes de recuperación de desastres.
- Las medidas de seguridad que controlen las operaciones de hardware/software de la Autoridad Certificadora del Estado de Aguascalientes, así como la administración del servicio de certificados electrónicos y servicios de solicitudes designados.

2.8.2 Información No Confidencial

Se considera información pública y por lo tanto accesible por terceros:

- La contenida en el presente documento.

- La información contenida en los certificados digitales de FEA que la Autoridad Certificadora del Estado de Aguascalientes emita.
- La Lista de Certificados Revocados.
- La información sobre el estado de los certificados digitales de FEA.

2.8.3 Entrega de Información a Autoridades Competentes

La Secretaría de Gobierno deberá revelar información confidencial o reservada en los términos de la legislación aplicable en cumplimiento de mandatos judiciales o derivados de procedimientos administrativos en forma de juicio.

2.8.4 Deber de Secreto Profesional

Los servidores públicos de la Secretaría de Gobierno que participen en tareas derivadas de la operación de la Autoridad Certificadora del Estado de Aguascalientes, están obligados a guardar secreto profesional y por lo tanto quedarán sujetos a la normatividad de la materia. De igual forma, el personal contratado que participe en la operación o cualquier actividad relacionada con la Autoridad Certificadora del Estado de Aguascalientes estará obligado a guardar secreto en el marco de las obligaciones contractuales contraídas con la Secretaría de Gobierno.

2.9 Derechos de Propiedad Intelectual

La Secretaría de Gobierno será el único titular de los derechos de propiedad intelectual sobre los certificados digitales de FEA que emita.

La Secretaría de Gobierno será el único titular de los derechos de propiedad intelectual que puedan derivarse del sistema de infraestructura de llave pública que regulan las presentes Políticas de Certificación y Declaración de Prácticas de Certificación.

2.10 Derechos de Propiedad en el Par de Claves y Componentes de las Claves

El par de claves correspondientes a los certificados de la Autoridad Certificadora del Estado de Aguascalientes, sin importar el medio físico donde estén almacenadas y protegidas, serán propiedad exclusiva del Gobierno del Estado por conducto de la Secretaría de Gobierno.

El par de claves correspondientes a los certificados digitales de FEA de los suscriptores de la Autoridad Certificadora del Estado de Aguascalientes, serán propiedad de los suscriptores que son los titulares de certificado de firma electrónica.

3.0 Identificación y Autenticación de los Titulares de Certificados Digitales de FEA

En este componente se describen los procedimientos que utilizará el Agente Certificador/Registrador para autenticar la identidad y otros atributos de un usuario solicitante de un certificado antes de la emisión del mismo.

Este componente también aborda las prácticas relacionadas con los nombres o denominaciones de las personas, incluyendo el reconocimiento de los derechos de marca registrada en algunos nombres.

Además, el componente establece los procedimientos para autenticar la identidad y los criterios de aceptación de los solicitantes que deseen convertirse en agentes certificadores u otras entidades que actúan o interactúan en la Infraestructura de Clave Pública.

También describe cómo se autentican las partes que soliciten renovación de claves o revocación.

3.1 Nombres

3.1.1 Tipos de Nombres

Los certificados emitidos por la Autoridad Certificadora del Estado de Aguascalientes contienen el nombre distintivo (DN) del emisor y el del solicitante del certificado en los campos *Nombre Emisor* (*issuer name)* y *Nombre de Sujeto (subject name).*

El nombre distintivo (DN) de la Autoridad Certificadora del Estado de Aguascalientes contiene los siguientes valores:

Nombre distintivo (DN) Certificado de firma electrónica de la Autoridad Certificadora del Estado de Aguascalientes.	
CN	AUTORIDAD CERTIFICADORA DEL ESTADO DE AGUASCALIENTES.
O	GOBIERNO DEL ESTADO DE AGUASCALIENTES
OU	SECRETARIA DE GOBIERNO
C	MX
S	AGUASCALIENTES

El nombre distintivo (DN) del *Nombre de Sujeto* contiene los siguientes valores:

Nombre distintivo (DN) certificado de firma electrónica del suscriptor.	
CN	<NOMBRES><APELLIDO1> <APELLIDO2>
O	GOBIERNO DEL ESTADO DE AGUASCALIENTES
OU	<AREA A LA QUE PERTENECE>
C	MX
SN	CURP TITULAR DEL CERTIFICADO DE FIRMA ELECTRÓNICA
X.500uniqueIdentifier (2.5.4.45)	RFC TITULAR DEL CERTIFICADO DE FIRMA ELECTRÓNICA

3.1.2 Necesidad de que los Nombres Sean Significativos

Los certificados digitales de FEA emitidos a los usuarios contienen nombres con semántica comúnmente entendible, lo cual permite la determinación de la identidad del individuo y que para tales efectos viene representada en el campo *Nombre de Sujeto* dentro del certificado de firma electrónica.

La Autoridad Certificadora del Estado de Aguascalientes no autorizará que los suscriptores hagan uso de seudónimos, o sobrenombres distintos al verdadero nombre personal para solicitar ni hacer uso de cualquier certificado de firma electrónica.

El certificado de firma electrónica de la Autoridad Certificadora del Estado de Aguascalientes contendrá el nombre distintivo (DN) con semántica comúnmente entendible que permita la determinación de la identidad de la Autoridad Certificadora al suscriptor o al tercero que confía en dicho certificado.

3.1.3 Reglas para Interpretar Varios Formatos de Nombres

Las reglas utilizadas por la Autoridad Certificadora del Estado de Aguascalientes para interpretar los nombres distintivos (DN) de los titulares o suscriptores de certificados digitales de FEA serán las definidas en los estándares internacionales ISO/IEC 9594-8 y el RFC 3280.

Así mismo cumplirán las reglas que marca la ITFEA en su Anexo 6: *Estándares y Estructura del Certificado Digital*, por lo tanto todos los certificados digitales de FEA emitidos utilizarán la codificación *UTF8String* para los atributos *DirectoryString* de los campos *Emisor* y *Nombre de Sujeto*, mientras que para la codificación de los campos país *(C)* y número de serie *(SN)* es *PrintableString*.

3.1.4 Unicidad de los Nombres

La Autoridad Certificadora del Estado de Aguascalientes se encargará de que los nombres distintivos (DN) del *Nombre de Sujeto* del suscriptor sean únicos mediante el uso de la CURP Clave Única de Registro Poblacional y a través de componentes automatizados en el proceso de inscripción del suscriptor que garanticen la unicidad del nombre distintivo (DN).

3.1.5 Procedimiento de Resolución de Conflictos Sobre Nombres

Será responsabilidad de los solicitantes de certificados digitales de FEA el cerciorarse de que el nombre que están utilizando en el apartado *Nombre de Sujeto* de su certificado de firma electrónica no infringe los derechos de propiedad intelectual de otros solicitantes, así pues el Agente Certificador/Registrador no realizará dicha verificación con alguna institución de Gobierno, ni resolverá cualquier disputa sobre propiedad intelectual del nombre.

En caso de que existiera alguna disputa relacionada con el uso del nombre de los solicitantes, la Autoridad Certificadora del Estado de Aguascalientes y sin alguna responsabilidad hacia cualquier solicitante o suscriptor de certificados digitales de FEA, tendrá la facultad de rechazar la solicitud o suspender el certificado de firma electrónica debido a tal disputa.

3.1.6 Reconocimiento, Autenticación y Papel de las Marcas Registradas

La Autoridad Certificadora del Estado de Aguascalientes no emitirá certificados digitales de FEA a solicitantes que hayan usado deliberadamente un nombre que no sea el propio o alguna denominación respecto de la cual no tengan derecho a usar, así mismo la Autoridad Certificadora del Estado de Aguascalientes no verificará con alguna institución de gobierno la posesión del nombre o marca registrada en el proceso de certificación.

3.1.7 Método de Prueba de Posesión de la Clave Privada

Los dos pares de claves asociados al certificado de firma electrónica se generarán mediante la implementación por parte del Agente Certificador/Registrador del procedimiento fiable diseñado por la Autoridad Certificadora del Estado de Aguascalientes. La generación de la clave privada del solicitante sólo se realizará desde terminales autorizadas y debidamente reforzadas, dotadas de todos los mecanismos de seguridad que se requieren para el envío y exportación de información segura.

Durante el proceso de emisión de certificados digitales de FEA, el Agente Certificador/Registrador se asegurará de que el solicitante realmente posea la clave privada

correspondiente a la solicitud que está en trámite mediante el uso de componentes automatizados que incorporan estándares internacionales como el uso del PKCS#10.

3.1.8 Autenticación de la Identidad de un Agente Certificador/Registrador

La Secretaría de Gobierno nombrará al Agente Certificador/Registrador conforme a lo que señala el anexo F5 de la Normatividad de ITFEA.

Los documentos a presentar para la obtención del nombramiento de Agente Certificador/Registrador serán:

- El nombramiento oficial emitido en términos de la legislación administrativa aplicable; y
- Cualquiera de los documentos de identificación siguientes:
  - Cartilla del Servicio Militar Nacional.
  - Pasaporte expedido por la Secretaría de Relaciones Exteriores.
  - Cédula Profesional expedida por la Secretaría de Educación Pública.
  - Credencial de Elector expedida por el Instituto Federal Electoral.
- Adicionalmente recabará la información biométrica que garantice tecnológicamente la identidad del Agente Certificador/Registrador.

3.1.9 Autenticación de la Identidad de un Individuo

El Agente Certificador/Registrador recabará una serie de datos y de documentos para realizar una correcta verificación de la identidad del solicitante de certificado de firma electrónica, contando para ello con su consentimiento explícito y conforme a lo que señala el anexo F5 de la Normatividad de ITFEA; por lo tanto, en caso de que se trate de una primera inscripción, el solicitante deberá de acudir a las oficinas dispuestas para este fin por la Secretaría de Gobierno. El trámite es personal e intransferible por lo que el interesado deberá presentarse en las instalaciones para realizarlo.

Los documentos a presentar para la obtención del certificado son:

- Acta de Nacimiento.
- Constancia de Residencia en el Estado de Aguascalientes.
- En caso de ser notario público copia certificada del FIAT.
- Y cualquiera de los documentos de identificación siguientes:
    - Cartilla del Servicio Militar Nacional.
    - Pasaporte expedido por la Secretaría de Relaciones Exteriores.
    - Cédula Profesional expedida por la Secretaría de Educación Pública.
    - Credencial de Elector expedida por el Instituto Federal Electoral.
- Adicionalmente recabará la información biométrica que garantice tecnológicamente la identidad del individuo.

3.1.10 Criterios para Operar con Autoridad Certificadora Externas

A la entrada en vigor de las presentes Políticas de Certificación y Declaración de Prácticas de Certificación no se contempla el establecimiento de relaciones de confianza con autoridades de certificación externas.

3.2 Identificación y Autenticación en las Peticiones de Renovación de Claves y Certificados Digitales de FEA

Se requiere que todos los titulares de un certificado de firma electrónica emitidos por la Autoridad Certificadora del Estado de Aguascalientes tramiten un nuevo certificado de firma electrónica una vez llegado el término de su vigencia, con el fin de mantener su continuidad en el uso de su firma electrónica.

El Agente Certificador/Registrador requerirá para efectos de renovación que el titular genere un nuevo par de claves para realizar el reemplazo del par de claves próximos a vencer, a este procedimiento se le conoce coloquialmente como “renovación de claves y certificado de firma electrónica”.

El Agente Certificador/Registrador verificará que la información proporcionada por el solicitante durante la primera inscripción continúe siendo válida, además comprobará su identidad con la documentación y biométricos mencionados en el apartado 3.1.9 antes de emitir un nuevo certificado de firma electrónica, por lo que cualquier actualización a dicha información se realizará conforme al apartado relativo.

3.3 Identificación y Autenticación para la Renovación de Claves y Certificados Digitales de FEA tras una revocación

Se aplicará lo dispuesto en el apartado anterior para efectos de identificación y autenticación del solicitante que pretenda la renovación de sus claves y certificado de firma electrónica, sólo si la revocación es acompañada de una sustitución de certificado de firma electrónica.

Sin obstar lo anterior, el Agente Certificador/Registrador podrá negar la renovación del certificado de firma electrónica en los casos siguientes:

- Cuando el certificado de firma electrónica hubiese sido emitido sin la autorización del individuo nombrado en el campo *Nombre de Sujeto*.
- Cuando se hubiese aplicado la revocación en virtud de que el certificado de firma electrónica hubiese sido emitido a una persona distinta a la nombrada en el campo *Nombre de Sujeto.*
- Cuando se descubra que la información proporcionada en la solicitud de certificado de firma electrónica es falsa.

3.4 Solicitud de Revocación

Las solicitudes de revocación se realizarán por el titular del certificado de firma electrónica mediante dos métodos dispuestos por el Agente Certificador/Registrador, sin perjuicio de cualquier otro procedimiento que pudiera establecerse por la Secretaría de Gobierno para estos efectos en un futuro.

El primer método de revocación se hará electrónicamente y en función del mismo el titular deberá de comprobar la posesión de su clave privada por medio de la clave de anulación

definida durante el proceso de emisión de certificado de firma electrónica, en caso de no contar con dicha clave deberá de revocarse mediante el segundo método.

El segundo método de revocación se hará personalmente sin que se autorice el uso de apoderados o representantes, para tales efectos el Agente Certificador/Registrador tendrá a disposición del titular de certificado de firma electrónica oficinas debidamente equipadas para realizar la revocación del certificado de firma electrónica, que se hará mediante una solicitud de revocación presentada por escrito y la comparecencia del titular en función de los mecanismos biométricos de seguridad del sistema.

Para llevar a cabo la revocación mediante el segundo método será necesario:

- Presentar identificación oficial vigente con fotografía (Credencial del IFE, Pasaporte o Cédula Profesional).
- Verificar la identidad mediante los biométricos aceptados.
- El Agente Certificador/Registrador validará los rasgos físicos de la fotografía de la identificación vigente con los rasgos físicos del suscriptor, y en caso de que existiese una duda o conflicto para la identificación del suscriptor, se le podrán pedir adicionalmente los siguientes documentos.
- Comprobante de domicilio a nombre del suscriptor con la dirección que aparece en los datos que registró para la emisión del certificado.
- Acta de nacimiento.
- CURP impresa.

Una vez valorada y aprobada la identidad el suscriptor y solicitante de revocación llenará la solicitud de revocación y la firmará autógrafamente, para que el Agente Certificador/Registrador proceda a su remisión a la Autoridad Certificadora del Estado de Aguascalientes.

4.0 Requerimientos de Operación para el Ciclo de Vida de los Certificados

En este componente se especifican los requisitos impuestos a la emisión de certificados con respecto a su ciclo de vida para los suscriptores y para los otros participantes en la Infraestructura de clave pública.

4.1 Solicitud de Certificados Digitales de FEA

El Agente Certificador/Registrador sólo aceptará solicitudes de certificado de firma electrónica en los términos de la Ley Sobre el Uso de Medios Electrónicos de Aguascalientes, el Código Civil del Estado de Aguascalientes, de la Ley del Notariado para el Estado de Aguascalientes, la Ley de Transparencia y Acceso a la Información Pública del Estado de Aguascalientes, la Ley de Catastro del Estado de Aguascalientes, de la Ley del Procedimiento Administrativo del Estado de Aguascalientes, de la Ley del Procedimiento Contencioso Administrativo para el Estado de Aguascalientes, del Reglamento del Registro Civil y del Reglamento del Registro Público de la Propiedad y del Comercio del Estado de Aguascalientes.

El Agente Certificador/Registrador podrá rechazar aquellas solicitudes de certificado de firma electrónica que no cumplan con algún requisito señalado en la Ley Sobre el Uso de Medios Electrónicos de Aguascalientes, el Código Civil del Estado de Aguascalientes, la Ley del Notariado para el Estado de Aguascalientes, la Ley de Transparencia y Acceso a la Información Pública del Estado de Aguascalientes, la Ley de Catastro del Estado de Aguascalientes, la Ley del Procedimiento Administrativo del Estado de Aguascalientes, la Ley del Procedimiento Contencioso Administrativo para el Estado de Aguascalientes, el Reglamento del Registro Civil y el Reglamento del Registro Público de la Propiedad y del Comercio del Estado de Aguascalientes.

En caso de que el Agente Certificador/Registrador rechace la solicitud de certificado de firma electrónica, lo hará saber al solicitante mediante oficio fundando y motivando las razones del rechazo.

4.1.1 Tramitación de Solicitudes de Certificados Digitales de FEA

Para obtener un certificado de firma electrónica los solicitantes deberán completar el procedimiento de enrolamiento dispuesto por el Agente Certificador/Registrador de la Autoridad Certificadora del Estado de Aguascalientes, el cual incluye las siguientes actividades:

- Generar una cita vía telefónica, correo electrónico u oficio y confirmar su asistencia vía telefónica.
- Los usuarios deberán presentarse con un dispositivo en el que se pueda almacenar la clave privada y el certificado que incluye la clave pública.

El día y hora señalados para la cita deberá:

El Agente Certificador/Registrador

- Abrir expediente para iniciar proceso de enrolamiento, basado en el número de folio.
- Capturar los datos y recabar los documentos que presenta el solicitante en su expediente de enrolamiento.
- Revisar la CURP y el RFC.
- Verificar en su caso el estado de los certificados con los que pudiera contar el solicitante.
- Capturar o actualizar la información siguiente:
  - Datos Generales:
    1. Nombre Completo.
    2. CURP.
    3. RFC.
    4. Escolaridad.
    5. Identificación oficial.
    6. Tipo de trámite.
    7. Folio.
    8. Fecha y Hora de Registro.
    9. Datos del Acta de Nacimiento
       a) Fecha de registro del acta (dd/mm/aaaa).
       b) Número del acta de nacimiento.

c) Datos de identificación del acta de nacimiento en los libros del Registro Civil.

- Datos Laborales:
  1. Dependencia u Organización.
  2. Domicilio.
  3. Nombramiento.
  4. Teléfono oficina y extensión.
  5. Ciudad.
  6. Municipio.
  7. Estado.
  8. Código postal.
  9. Correo electrónico.
- Datos particulares:
  1. Domicilio.
  2. Teléfono.
  3. Ciudad.
  4. Municipio.
  5. Estado.
  6. Código postal.
  7. Correo electrónico.
  8. Nacionalidad.
  9. Estado civil.

- Fotografía:
  - Se deberá utilizar la pose frontal o de cara completa, verificando que la persona se encuentre bien sentada, recargada y con la mirada al frente.
  - La distancia a la que se debe encontrar la cámara no será mayor a un metro.
- Firmar autógrafamente la solicitud de expedición de certificado de firma electrónica. En caso de que se acepte se continuará con el trámite, en caso de rechazo el trámite se cancelará.
- Documentos digitalizados:

- Se digitalizarán los documentos solicitados por el Agente Certificador/Registrador.

Certificación:

- El Agente Certificador/Registrador entregará al solicitante un documento en el que se indicará el procedimiento a seguir y los archivos que quedarán almacenados en el medio electrónico proporcionado por el solicitante.

- El solicitante generará los archivos necesarios en el equipo de cómputo especificado por el Agente Certificador/Registrador para iniciar el proceso de certificación. Los archivos de clave privada solamente serán manejados y almacenados por el solicitante y el Agente Certificador/Registrador indicará cuál es el archivo necesario para la certificación.
- Una vez realizada la certificación, es decir una vez que se ha generado el archivo ".cer" el Agente Certificador/Registrador generará el archivo PKCS12 correspondiente al solicitante y lo almacenará en el dispositivo electrónico.

- Para terminar el proceso, el solicitante deberá firmar en electrónico en el sistema la aceptación del servicio de certificación.

- El solicitante recibirá por medio de un correo electrónico la confirmación de la certificación así como información importante sobre el uso, y las responsabilidades que asume respecto el manejo de certificados para firma.

En caso de haber cumplido con todos los requerimientos, se aprobará y se concluirá con el procedimiento de solicitud de certificado de firma electrónica.

4.2 Emisión de Certificados Digitales de FEA

4.2.1 Actuación de la Autoridad Certificadora del Estado de Aguascalientes Durante la Emisión de los Certificados Digitales de FEA

Una vez que se haya resuelto la aprobación definitiva de la solicitud por parte del Agente Certificador/Registrador de la Autoridad Certificadora del Estado de Aguascalientes, se procederá a la emisión segura del certificado de firma electrónica.

Durante la emisión de estos certificados la Autoridad Certificadora del Estado de Aguascalientes:

- Vinculará de forma segura mediante un procedimiento de generación de certificados electrónicos el certificado de firma electrónica con la información contenida en la solicitud, incluyendo también la clave pública.
- Protegerá la integridad y confidencialidad de los datos contenidos en la solicitud.
- Realizará la notificación al suscriptor de la emisión de su certificado de firma electrónica tal y como se describe en el apartado 4.2.2.
- Pondrá a disposición del suscriptor una copia del certificado de firma electrónica en el sitio oficial de la Autoridad Certificadora del Estado de Aguascalientes, para que éste pueda obtener las copias que requiera.

Todos los certificados digitales de FEA iniciarán su vigencia en el momento de su emisión. El periodo de vigencia fenecerá anticipadamente cuando se actualicen las hipótesis de revocación del certificado de firma electrónica.

4.2.2 Notificación del Agente Certificador/Registrador de la Autoridad Certificadora del Estado de Aguascalientes al Solicitante de la Emisión del Certificado de Firma Electrónica

El solicitante conocerá la emisión efectiva de su certificado de firma electrónica con la entrega del comprobante de certificado de firma electrónica, el cual contiene el número de serie designado por la Autoridad Certificadora para su certificado.

Asimismo, el solicitante recibirá un correo electrónico que indicará entre otros datos el número de serie, la fecha de vigencia y la URL (dirección electrónica) para descargar el certificado de firma electrónica.

4.3 Aceptación de los Certificados Digitales de FEA

El solicitante deberá de conocer los derechos y obligaciones que adquiere como titular de un certificado de firma electrónica. Para tales efectos se le entregará una copia ya sea impresa o remitida por correo electrónico de las presentes Políticas de Certificación y Declaración de Prácticas de Certificación.

En caso de aceptar estos derechos y obligaciones el solicitante firmará de manera autógrafa el acuse de recibo que el Agente Certificador/Registrador le expida; en caso de que no esté de acuerdo, el solicitante deberá de expresar su rechazo y firmar de manera autógrafa dicho rechazo para que el Agente Certificador/Registrador de la Autoridad Certificadora del Estado de Aguascalientes proceda a la revocación del certificado.

Al aceptar y firmar de manera autógrafa el acuse de recibo, el titular del certificado de firma electrónica estará listo para participar en procesos electrónicos que requieran su Firma Electrónica Avanzada.

4.4 Revocación de los Certificados Digitales de FEA

Se podrá revocar un certificado de firma electrónica ante cualquiera de las siguientes causas:

- Solicitud expresa del titular,
- En caso de que el usuario sea servidor público, a solicitud de su superior jerárquico mediante oficio en el que se corra copia del mismo al interesado indicando la causa de la solicitud de revocación del certificado en cuestión,
- Incapacidad jurídica declarada por una autoridad competente,
- Fallecimiento,
- Resolución judicial,

- Incumplimiento del titular de sus obligaciones, previa comunicación del Agente Certificador/Registrador especificando la causa, fecha y hora en que tendrá efecto la revocación,
- Falsedad o errores en la información proporcionada en la solicitud de certificado de firma electrónica,
- Duplicidad de la clave privada asociada al certificado de firma ;
- Cualquier motivo que comprometa la integridad o confidencialidad de la clave privada (a solicitud del titular).

4.4.1 Actuación de la Autoridad Certificadora del Estado de Aguascalientes Durante la Revocación de los Certificados Digitales de FEA

Durante la revocación del certificado de firma electrónica que involucra la presencia física del titular.

- El titular del certificado presentará la solicitud de revocación, misma que obtendrá en la oficina del Agente Certificador/Registrador y que debe contener una sección para que el solicitante en escritura libre señale la causa de la revocación del certificado que solicita. La solicitud deberá contener firma autógrafa del titular, su nombre, CURP, RFC y domicilio.

- La Autoridad Certificadora verificará la coincidencia y veracidad de los datos incluidos en la solicitud de revocación con los datos contenidos en el documento probatorio de identidad y la información del titular del certificado. En caso de cumplir todos los requisitos, se aprobará la solicitud de revocación.

- La Autoridad Certificadora procederá a la revocación del certificado de firma electrónica y emitirá el comprobante que respalde esta transacción. El comprobante incluirá la fecha y hora de la revocación. El titular recibirá vía correo electrónico la información de revocación del certificado correspondiente.

- La Autoridad Certificadora deberá acusar recibo de la entrega del comprobante de revocación al titular.

4.4.2 Período de Gracia de la Solicitud de Revocación

La revocación tendrá efecto de manera inmediata a la tramitación de cada solicitud aprobada, por lo tanto no existe un periodo de gracia asociado a este proceso.

4.5 Auditoría de Seguridad

Para tener un mayor control y contar con los indicadores necesarios que ayuden a determinar si existen los suficientes mecanismos de seguridad, el Agente Certificador/Registrador de la Autoridad Certificadora del Estado de Aguascalientes llevará el registro de manera manual o automática de cualquier evento significativo relacionado con los siguientes eventos:

- La Administración del ciclo de vida del certificado de firma electrónica.
- La operación de la infraestructura que esta alrededor de la Autoridad Certificadora del Estado de Aguascalientes; y
- El registro de los datos que entren en los distintos procedimientos asociados a los servicios del Agente Certificador/Registrador de la Autoridad Certificadora del Estado de Aguascalientes.

4.5.1 Frecuencia con que se Revisan los Registros

Los registros deberán revisarse semanalmente y generar los reportes necesarios, así como tomar las medidas preventivas por los responsables de cada parte del proceso para corregir errores y prevenir fallas en los servicios que preste la Autoridad Certificadora.

4.5.2 Periodo de Disponibilidad de los Registros de Auditoría

Los registros de auditoría se mantienen de forma local al menos durante cinco meses después de haber sido generados, posteriormente se almacenarán con el debido procedimiento.

4.5.3 Mecanismos Destinados para Proteger los Registros de Auditoría

El Agente Certificador/Registrador de la Autoridad Certificadora del Estado de Aguascalientes ha dispuesto mecanismos de seguridad que garantizarán la debida protección de los registros de auditoría, con esto se evitará que puedan ser borrados, modificados y que sean accedidos de forma no autorizada.

4.6 Respaldo

4.6.1 Planes de Respaldo

El Agente Certificador/Registrador de la Autoridad Certificadora del Estado de Aguascalientes ha establecido los procedimientos necesarios para contar oportunamente con copias de respaldo de toda la información contenida en su infraestructura de llave pública.

Los planes de respaldo efectuados sobre la infraestructura de llave pública desplegada, obedecen a los mismos planes que se siguen dentro de la Secretaría de Gobierno para respaldar el resto de los sistemas informáticos, información con carácter de confidencial, y toda aquella que requiera ser almacenada por un período de tiempo definido.

Las copias de respaldo se almacenarán de forma segura en sitios remotos debidamente custodiados.

4.7 Recuperación

El Agente Certificador/Registrador de la Autoridad Certificadora del Estado de Aguascalientes dentro de su procedimiento de recuperación ha incluido los siguientes elementos:

- Uso de copias de respaldo de la información más reciente.
- Solución de problemas relacionados con el hardware.
- Método para restaurar el sistema operativo que soporta la infraestructura de llave pública, debidamente configurado bajo los estándares de la Secretaría de Gobierno.

El Administrador de la Autoridad Certificadora y los demás roles encargados de recuperar los respaldos realizarán las siguientes acciones coordinadas:

- Establecerán todas las conexiones de red, así como las conexiones al módulo criptográfico encargado de resguardar el par de claves de la Autoridad Certificadora.
- Recuperarán los respaldos de los componentes de software involucrados en la operación de la infraestructura de llave pública.
- Realizarán la reconfiguración del software que opere la Autoridad Certificadora de acuerdo al manual proporcionado.
- Realizarán la restauración del módulo criptográfico; y
- Verificarán que la restauración fue exitosa.

4.8 Destrucción de Medios de Almacenamiento

El Agente Certificador/Registrador de la Autoridad Certificadora del Estado de Aguascalientes ha incorporado mecanismos de seguridad para la correcta destrucción y reutilización de los medios utilizados para los respaldos.

No podrán ser reutilizados ni desechados los medios de almacenamiento sin antes haber pasado por un proceso de borrado seguro.

El proceso de borrado seguro será documentado con el fin de dejar constancia y registro de haber dado de baja de la bitácora de respaldos el medio de almacenamiento destruido.

4.9 Protección de las bitácoras

El Agente Certificador/Registrador de la Autoridad Certificadora del Estado de Aguascalientes ha incorporado mecanismos de protección que controlarán el acceso a los registros que se generen durante sus operaciones, con el fin de detectar posibles violaciones a los procedimientos o entradas sospechosas e incidentes.

Se ha creado un registro de seguimiento en la que se anotarán todos los eventos de los diversos roles que han solicitado el acceso a las bitácoras.

- El custodio de estas bitácoras se asegurará que el registro se lleve a cabo de forma debida, incluyendo en las mismas:
    - Fecha de revisión
    - Nombre de la persona autorizada que realizó la revisión
    - Fecha de la bitácora que se está revisando
    - Nombre que identifica la bitácora que se está revisando.

4.10 Cambio del Par de Claves de la Autoridad Certificadora

Antes de que fenezca la vigencia del certificado de la Autoridad Certificadora del Estado de Aguascalientes se requerirá lo siguiente:

- Que se dejen de emitir nuevos certificados digitales de FEA al menos 30 días antes de que expire la vigencia del certificado.
- Que la Secretaría de Gobierno realice, haga público y comunique la transición que se efectuará para hacer el cambio de claves de la Autoridad Certificadora.
- Que se lleve a cabo la transición del par de claves antiguo al nuevo par de la Autoridad Certificadora.
- Que se realice la re-certificación de todos los servicios a los que se les emitió un certificado de la Autoridad Certificadora del Estado de Aguascalientes y pertenezcan a su infraestructura de llave pública.
- Las nuevas solicitudes de certificado de firma electrónica se procesarán una vez que la Autoridad Certificadora tenga su nuevo par de claves y esté lista para realizar la firma de certificados digitales de FEA. Dicho procedimiento está descrito en las presentes Políticas de Certificación y Declaración de Prácticas de Certificación.

4.11 Finalización de la Autoridad Certificadora del Estado de Aguascalientes.

En caso de que el Agente Certificador/Registrador requiera dar por terminada la operación de la Autoridad Certificadora y los servicios que ésta ofrece, la Secretaría de Gobierno realizará todos los esfuerzos necesarios para notificar a sus suscriptores, a los terceros aceptantes y a otros afectados, apegándose a los lineamientos que marcan la Ley Sobre el Uso de Medios

Electrónicos de Aguascalientes, el Código Civil del Estado de Aguascalientes, la Ley del Notariado para el Estado de Aguascalientes, la Ley de Transparencia y Acceso a la Información Pública del Estado de Aguascalientes, la Ley de Catastro del Estado de Aguascalientes, la Ley del Procedimiento Administrativo del Estado de Aguascalientes, la Ley del Procedimiento Contencioso Administrativo para el Estado de Aguascalientes, el Reglamento del Registro Civil, el Reglamento del Registro Público de la Propiedad y del Comercio del Estado de Aguascalientes, y las presentes Políticas de Certificación y Declaración de Prácticas de Certificación vigentes.

5.0 Controles de Seguridad Física, Instalaciones, Gestión y de Operación

El Agente Certificador/Registrador de la Autoridad Certificadora del Estado de Aguascalientes implementará políticas de seguridad que den soporte a los requerimientos de seguridad establecidos en las presentes Políticas de Certificación y Declaración de Prácticas de Certificación.

5.1 Controles Físicos

Los aspectos referentes a los controles de seguridad física, por cuestiones de confidencialidad, no serán publicados en las presentes Políticas de Certificación y Declaración de Prácticas de Certificación, sólo estarán presentes todos aquellos considerados como relevantes.

5.1.1 Ubicación Física y Construcción

El edificio donde se encuentra la infraestructura de la Autoridad Certificadora del Estado de Aguascalientes, es el que se ubica en Av. López Mateos esq. Héroe de Nacozari, específicamente en el Registro Público de la Propiedad y del Comercio del Estado, ciudad de Aguascalientes, México. Este centro de procesamiento cumple con todas las exigencias y requerimientos de seguridad y auditoría de la Autoridad Certificadora del Estado de Aguascalientes. El diseño de seguridad de este centro de procesamiento es tal, que previene y detiene cualquier intento de intrusión.

5.1.2 Acceso Físico

La infraestructura de Firma Electrónica Avanzada cuenta con un sistema de acceso físico de personas con varios niveles de control.

Las operaciones clasificadas como sensibles se desarrollarán dentro de un recinto físicamente seguro con diversos niveles de seguridad para acceder a los equipos de cómputo y aplicaciones críticas.

El acceso físico será registrado automáticamente y se grabará en video; ninguna persona podrá acceder al recinto si no es acompañada por personal autorizado de la Secretaría de Gobierno del Estado de Aguascalientes, por lo tanto ningún tercero, proveedor, notario o servidor público no autorizado tendrá permitido el acceso a las áreas identificadas como de alto riesgo.

5.1.3 Alimentación Eléctrica y Aire Acondicionado

El centro de procesamiento donde está instalada la infraestructura de la Autoridad Certificadora del Estado de Aguascalientes cuenta con sistemas de energía eléctrica que garantizan alimentación continua e ininterrumpida y sistema de aire acondicionado que mantiene el nivel de temperatura y humedad adecuado para los equipos instalados.

5.1.4 Exposición al Agua

El centro de procesamiento está ubicado estratégicamente para minimizar el impacto que resulte de exponer al agua el cableado y los equipos instalados.

5.1.5 Protección y Prevención de Incendios

Se han dispuesto los medios adecuados, como sistemas automáticos de detección de humo y extinción de incendios, para la protección de los equipos y cableado instalado en el centro de procesamiento.

Las medidas de prevención y protección cumplen con las regulaciones locales de seguridad.

5.1.6 Almacenamiento de Medios

Todos los medios de almacenamiento que contienen activos de software y de información, registros de auditoría, o respaldos, serán almacenados en las instalaciones externas de la Secretaría de Gobierno dispuestas para este fin.

Se han implementado mecanismos de seguridad diseñados para proteger los medios de almacenamiento contra acceso no autorizado, daño causado por agua, incendio y magnetismo.

5.1.7 Copias de Seguridad Fuera de las Instalaciones

La Secretaría de Gobierno mantendrá las copias de seguridad en instalaciones propias que cumplen con las medidas precisas de seguridad establecidas por la propia Secretaría.

5.2 Controles de los Procedimientos

Por cuestiones de seguridad, la información que contiene los controles sobre los procedimientos se considera confidencial por lo que sólo se hace referencia a los mismos.
La Secretaría de Gobierno procurará que toda la gestión se lleve a cabo de forma segura y conforme a lo publicado en las presentes Políticas de Certificación y Declaración de Prácticas de Certificación, además de realizar las auditorías periódicas que vienen descritas en este documento.

Uno de los mecanismos que se ha diseñado para tales efectos es la separación de funciones con el fin de evitar que una o un grupo de personas puedan conseguir el control total de la infraestructura.

5.2.1 Roles Identificados Como de Confianza

Los roles identificados como confiables incluyen pero no están limitados a:

- Administradores de sistemas
- Administradores y operadores del módulo criptográfico
- Administrador Técnico de la PKI
- Agente Certificador/Registrador (Agente certificador)
- Gente de ingeniería y diseño de soluciones criptográficas

Los anteriores roles son considerados confiables por la Secretaría de Gobierno, sin embargo aquellas personas que quieran ser identificadas como de confianza tendrán que sujetarse a los controles establecidos en el presente documento.

Son roles incompatibles los denominados así por no poder una misma persona ostentar dos de ellos al mismo tiempo, estos son:

- Administradores de sistemas y operadores del módulo criptográfico.
- Agente registrador y los administradores del módulo criptográfico.
- Administrador de sistema, agente registrador y administrador de la PKI.

5.2.2 Número de Personas Requeridas por Tarea

A fin de proveer seguridad derivada del control riguroso que tiene la Infraestructura de Firma Electrónica Avanzada, en los procedimientos clasificados de alta criticidad se ha implementado la separación de funciones en base a las responsabilidades de cada persona.

Como práctica autorizada, se requiere el trabajo conjunto de cuando menos dos personas con capacidad profesional para realizar las tareas correspondientes con la administración y establecimiento del módulo criptográfico.
Este grupo de personas no tiene ni tendrá acceso, contraseña o manera alguna de activar la llave privada.

Una vez establecido el módulo criptográfico, se requiere del grupo de operadores para dar acceso a la clave privada resguardada en el mismo.

5.2.3 Identificación y Autenticación para Cada Usuario

Todo el personal que ha alcanzado o pretenda alcanzar el nivel de persona de confianza para los efectos de la Infraestructura de Firma Electrónica Avanzada, previamente fue sometido y en el futuro deberá de ser sometido a una verificación de identidad ante el personal encargado de los recursos humanos de la Secretaría de Gobierno.

Para la verificación de identidad de los evaluados se han recabado o en caso futuro se recabarán los siguientes documentos:

- Credencial para votar expedida por el Instituto Federal Electoral, Cartilla Militar o Pasaporte vigente emitido por la Secretaría de Relaciones Exteriores.
- CURP.

Así mismo, el personal encargado de administrar y operar los módulos criptográficos que resguardarán la clave privada de la Autoridad Certificadora, han sido identificados, autentificados y validados mediante técnicas de secreto compartido en tarjetas inteligentes específicas del módulo criptográfico.

5.3 Controles Sobre el Personal

5.3.1 Requerimientos de Antecedentes, Cualidades y Experiencia Profesional

Todo el personal del Agente Certificador/Registrador de la Autoridad Certificadora del Estado de Aguascalientes deberá contar con el conocimiento, experiencia y formación suficiente para el mejor desempeño de sus funciones asignadas. Para ello, la Secretaría de Gobierno ha seleccionado y seleccionará al personal buscando que el perfil profesional del empleado se adecue lo más posible a la descripción de puesto.

5.3.2 Requerimientos de Capacitación

El personal encargado de la operación y administración de la infraestructura de la Autoridad Certificadora del Estado de Aguascalientes ha recibido y en lo futuro recibirá el entrenamiento y capacitación necesaria para asegurar la correcta y competente realización de sus funciones.

Tales programas de entrenamiento y capacitación están adaptados a las responsabilidades de cada individuo e incluyen los siguientes temas:

- Conceptos básicos de PKI.
- Responsabilidades de la posición.
- Políticas de Certificación y Declaración de Prácticas de Certificación vigentes.
- Uso y operación del hardware/software utilizado.
- Procedimientos de seguridad para cada rol.
- Procedimientos para la recuperación de la operación en caso de algún desastre.
- Sensibilización sobre la seguridad física, lógica y técnica.

5.3.3 Sanciones Disciplinarias por Acciones No Autorizadas

Las acciones disciplinarias adecuadas se tomarán ante acciones no autorizadas, negligentes, mal intencionadas o análogas por violaciones a las presentes Políticas de Certificación y Declaración de Prácticas de Certificación de la Autoridad Certificadora del Estado de Aguascalientes. Las sanciones disciplinarias serán aplicadas de conformidad con lo establecido por la Ley de Responsabilidades de los Servidores Públicos del Estado de Aguascalientes.

6.0 Controles de Seguridad Técnica

La infraestructura de la Autoridad Certificadora del Estado de Aguascalientes utiliza sistemas y productos confiables, los cuales están protegidos contra toda alteración, con el fin de garantizar la seguridad técnica y criptográfica de los procesos de certificación que dan soporte a la operación del Agente Certificador/Registrador.

6.1 Generación del Par de Claves

El par de claves de la Autoridad Certificadora del Estado de Aguascalientes se generó bajo dispositivos criptográficos de seguridad que cumplieron con el estándar FIPS 140-2 nivel 3; se deberán utilizar estos dispositivos para generar la firma de los certificados digitales que emita en el futuro el Agente Certificador/Registrador de la Autoridad Certificadora del Estado de Aguascalientes.

6.2 Generación de la Clave Privada del Titular

El par de claves del solicitante deberá ser generado por el mismo, por tal motivo la Autoridad Certificadora del Estado de Aguascalientes pone a disposición del solicitante sistemas criptográficos para la generación de su par de claves.

El Agente Certificador/Registrador garantizará que en todo momento la clave privada permanezca bajo el poder del solicitante mediante el uso de dispositivos biométricos, que eviten transferencias de la misma con algún otra sujeto .

6.3 Entrega de la Clave Pública al Solicitante

El Agente Certificador/Registrador de la Autoridad Certificadora del Estado de Aguascalientes, pondrá a disposición de los solicitantes sistemas criptográficos confiables que tramiten el requerimiento de certificación con la Autoridad Certificadora cumpliendo con el estándar PKCS#10.

6.4 Entrega de la Clave Pública de la Autoridad Certificadora a los Terceros Aceptantes

La clave pública de la Autoridad Certificadora del Estado de Aguascalientes está incluida en el certificado de dicha Autoridad Certificadora. El certificado de la Autoridad Certificadora deberá estar disponible en el repositorio electrónico especificado en este documento para ser consultado y obtenido por los titulares de certificados, así como por los terceros aceptantes.

6.5 Tamaño de las Claves

El tamaño de las claves que la Autoridad Certificadora del Estado de Aguascalientes utiliza, proporciona una fortaleza, en cuanto a seguridad se refiere, de un período de 10 años.
El tamaño de las claves que utilizan sus suscriptores ofrece una fortaleza de 2 años.

6.6 Hardware/ Software Empleado para la Generación de la Clave Pública

La clave pública de la Autoridad Certificadora del Estado de Aguascalientes ha sido generada y codificada dentro de módulos criptográficos adecuados y conforme a la normatividad vigente.
Para los suscriptores se ofrecen componentes de software confiables que ayudan con la generación de su par de claves, estas piezas de software cumplen con los estándares marcados en las presentes Políticas de Certificación y Declaración de Prácticas de Certificación.

6.7 Usos Admitidos de las Claves

Los usos admitidos de la clave para cada certificado emitido por el Agente Certificador/Registrador de la Autoridad Certificadora del Estado de Aguascalientes son: autenticación, firma electrónica de documentos, correos electrónicos, transacciones y archivos, no repudio y establecimiento de intercambio de llaves.

Este uso deberá venir codificado dentro del Certificado Digital emitido a los suscriptores.

6.8 Protección de la Clave Privada

La Secretaría de Gobierno cumple con estrictos controles físicos, lógicos, así como con procedimientos para fortalecer la seguridad en el resguardo de su clave privada. La descripción de estos controles y procedimientos se incluye a lo largo de las presentes Políticas de Certificación y Declaración de Prácticas de Certificación.

Las claves privadas de los suscriptores son protegidas por ellos mismos, la Autoridad Certificadora del Estado de Aguascalientes no guarda copia alguna de la clave privada, por lo

tanto los suscriptores deberán incorporar al menos las siguientes medidas para proteger la clave privada:

- Incorporar mecanismos de seguridad que ofrezcan la protección física de la estación de trabajo del titular.
- Incorporar políticas de seguridad que contemplen la protección de acceso a la estación de trabajo, incluyendo cuando ésta es desatendida por el titular.

6.9 Método de Activación de la Clave Privada

La clave privada de la Autoridad Certificadora del Estado de Aguascalientes se ha activado mediante la puesta en marcha del módulo criptográfico estipulado en el apartado *6.1*, llevando a cabo las siguientes tareas:

- Inicialización del estado del módulo criptográfico.
- Cumplimiento de la combinación mínima definida para operar el módulo criptográfico.

La activación de las claves privadas de los suscriptores de la Autoridad Certificadora del Estado de Aguascalientes, requiere la autenticación del titular ante el dispositivo criptográfico, contenedor de certificados o archivo cifrado que protege el acceso a su clave privada.

6.10 Método de Desactivación de la Clave Privada

La persona encargada de administrar la Autoridad Certificadora puede proceder a la desactivación de la clave privada de la Autoridad Certificadora mediante los componentes de software/hardware encargados de operar y resguardar la clave privada. Para la reactivación es necesaria la intervención mínima de los roles definidos en las presentes Políticas de Certificación y Declaración de Prácticas de Certificación.

Los suscriptores de la Autoridad Certificadora del Estado de Aguascalientes pueden proceder a desactivar su clave privada eliminando las claves del repositorio que lo contenga, dejar que expire el tiempo definido tras la introducción de la contraseña de acceso y cerrando el componente de software que se utiliza para introducir la contraseña de acceso.

6.11 Método de Destrucción de la Clave Privada

En términos generales la destrucción de la clave privada siempre debe estar precedida por la revocación del certificado digital asociado a la misma, acompañado del procedimiento de eliminación de los archivos físicos del repositorio que contiene dichas claves.

En el caso de la clave privada de la Autoridad Certificadora del Estado de Aguascalientes, consiste en el borrado seguro de las claves resguardadas por el módulo criptográfico, así como las copias de seguridad.

6.12 Archivo de la Clave Pública

Para mantener la disponibilidad y continuidad de las operaciones de la Autoridad Certificadora se efectuarán respaldos periódicos de la base de datos de certificados digitales emitidos.

6.13 Periodos Operativos de los Certificados y Periodos de Uso para el Par de Claves.

Los periodos de utilización de las claves serán los determinados en el certificado digital o su revocación, y una vez transcurridos no se podrán seguir utilizando.

El certificado y el par de claves de la Autoridad Certificadora tienen una validez de 6 años.

Su caducidad producirá automáticamente la invalidación de los certificados, originando el cese permanente de su operatividad conforme a los usos que le son propios.

Los periodos operacionales máximos para el certificado de firma electrónica de los usuarios son de dos años, siempre y cuando:

- Los certificados digitales de FEA sean individuales.
- Los pares de claves de los suscriptores están en el repositorio de claves del mismo sistema operativo del equipo donde se realizo el trámite de obtención de claves o en dispositivo criptográficos portables llamados Tokens.

Si un suscriptor no puede completar los procesos de autenticación marcados en estas Políticas de Certificación y Declaración de Prácticas de Certificación, o no puede probar la posesión de su clave privada al ser requerida, el Agente Certificador/Registrador de la Autoridad Certificadora del Estado de Aguascalientes rechazará de forma automática el certificado de firma electrónica

6.14 Generación e Instalación de los Datos de Activación

Para la generación de los datos de activación de la clave de la Autoridad Certificadora se utilizó la combinación de cierto número de tarjetas inteligentes, las cuales operaron bajo el esquema de "compartir el secreto". Para esto se requirió la intervención de los operadores del módulo criptográfico.

En el caso de los suscriptores, los datos de activación consisten en el establecimiento de una contraseña, la cual se determina al momento de generar el requerimiento de certificación. Para el establecimiento de esta contraseña se deben tomar en cuenta las siguientes normas de seguridad:

- Debe ser generada por el usuario
- Debe contener al menos 8 caracteres
- Debe estar construida con caracteres alfanuméricos
- Debe contener mayúsculas y minúsculas
- No debe tener caracteres repetidos
- No debe de tener el nombre del suscriptor

6.15 Protección de los Datos de Activación

Para los suscriptores, la contraseña de acceso a su clave privada debe ser conocida solo por ellos, debe ser personal e intransferible, además se usarán los dispositivos biométricos que ha autorizado la Secretaría de Gobierno, y que consisten en lectores de huella digital. Esta contraseña y dispositivo biométrico son los parámetros que permiten la utilización de los

certificados digitales en los servicios ofrecidos por la Secretaría de Gobierno, por lo tanto deben tenerse en cuenta las siguientes normas de seguridad:

- La contraseña es personal, confidencial e intransferible
- No se deben elegir datos relacionados con la identidad de la persona para establecer la contraseña
- Si considera que su contraseña puede ser conocida por alguien más, deberá revocar el certificado
- No comunicar ni enviar la contraseña a nadie

6.16 Controles de Seguridad Informática

El Agente Certificador/Registrador de la Autoridad Certificadora del Estado de Aguascalientes ha incorporado sistemas confiables que cumplen con las medidas de seguridad y procesos de evaluación continúa establecidos por la Secretaría de Gobierno.

6.17 Controles de Seguridad de la Red

La infraestructura de red utilizada por los sistemas de la Autoridad Certificadora del Estado de Aguascalientes está dotada de todos los mecanismos de seguridad necesarios para garantizar el servicio de manera confiable e íntegra. La infraestructura de red está sujeta a los mismos periodos de evaluación de la Secretaría de Gobierno.

6.18 Perfil de Certificado

Los certificados digitales emitidos por el Agente Certificador/Registrador de la Autoridad Certificadora del Estado de Aguascalientes cumplen con las siguientes normas:

- Recomendación **X.509 ITU-T** (2005): Tecnología de información – Interconexión de sistemas abiertos – El directorio: plataforma de autenticación
- **RFC 3280:** Internet X.509 Infraestructura de Clave Pública Perfil de Certificado y LCR
- Los certificados digitales utilizan el estándar X.509 versión 3 que incluyen los siguientes campos:

- Versión, número de serie, estos valores son únicos para cada certificado digital emitido
- Nombre del algoritmo de firma utilizado
- Nombre distinguido del emisor
- Fecha de validez de inicio, el formato de la fecha está codificado en UTC (tiempo coordinado universal)
- Fecha de validez de término, el formato de la fecha está codificado en UTC (tiempo coordinado universal)
- Nombre Distinguido del sujeto
- Clave pública del sujeto

Las extensiones utilizadas son:

- *Auth. Key Identifier*
- *Subject Key Identifier*
- *Auth. Information Access*
- *Certificate Policies*
- *Basic Constraints*
- *Key Usage*

7.0 Descripción de Lista de Certificados Revocados y OCSP

El Agente Certificador/Registrador de la Autoridad Certificadora del Estado de Aguascalientes emitirá listas de certificados revocados (LCR) que se conformen de acuerdo el estándar descrito en el RFC 2459. Los datos que se incluyen en estas LCR son:

- La versión.
- El algoritmo de firma digital usado.
- El nombre del emisor y la entidad que ha emitido y firmado electrónicamente la LCR. El nombre del emisor cumple con los requisitos dispuestos para el Nombre Distinguido (DN) del emisor.
- Fecha y hora de emisión de la Lista de Certificados Revocados; la LCR es efectiva desde el momento de su emisión.
- Fecha y hora de vigencia de la Lista de Certificados Revocados.
- Fecha de cuando se emitirá la nueva LCR.

- El listado de los certificados revocados que contiene el número de serie y fecha de revocación del certificado de firma electrónica.

7.1 Disponibilidad de un Sistema en Línea de Verificación del Estado de los Certificados Digitales de FEA

El Agente Certificador/Registrador de la Autoridad Certificadora del Estado de Aguascalientes publicará un servicio mediante el cual se podrá verificar el estado de los certificados digitales de FEA que ha emitido. Este servicio implementa el protocolo OCSP cumpliendo con el RFC 2560. A través de este protocolo se determina el estado actual de un certificado de firma electrónica sin requerir el acceso a las LCR. Quien requiera consultar el estado de un certificado de firma electrónica sólo debe de enviar una petición al servicio de OCSP, este servicio ofrece una respuesta sobre el estado del certificado vía el protocolo http. Este servicio se encontrará disponible en la dirección de acceso incluida en el apartado 9.1.

Para hacer uso de este servicio, es responsabilidad del tercero aceptante contar con los componentes de software/hardware necesarios para realizar consultas de tipo OCSP apegado al RFC 2560.

Este servicio estará disponible de forma ininterrumpida todos los días del año.

8.0 Sobre la Actualización y Notificación

Es obligación de la Autoridad Certificadora del Gobierno del Estado de Aguascalientes publicar información relativa a sus certificados y al estado de dichos certificados a través de la Dirección de Informática y Modernización; será la Secretaría de Gobierno la responsable de determinar cualquier adecuación a las presentes Políticas de Certificación y Declaración de Prácticas de Certificación, así mismo, será la encargada de aprobar las correcciones y actualizaciones que hubiera en un futuro al presente documento.

El período de comentarios para cualquier corrección a las presentes Políticas de Certificación y Declaración de Prácticas de Certificación será de ocho días, comenzando en la fecha en que las enmiendas se publiquen en el repositorio de la Autoridad Certificadora del Estado de Aguascalientes.

Las correcciones, ajustes y modificaciones a las presentes Políticas de Certificación y Declaración de Prácticas de Certificación se publicarán en el URL **http://www.aguascalientes.gob.mx/AC** del repositorio perteneciente a la Autoridad Certificadora del Estado de Aguascalientes.

9.0 Políticas de Publicación

Es obligación de la Autoridad Certificadora publicar la información relativa a sus Prácticas y Políticas de Certificación, sus certificados y al estado actualizado de de dichos certificados.

9.1 Publicación de Información de Certificación

El contenido de las Políticas de Certificación y Declaración de Prácticas de Certificación estará publicado a título informativo en el repositorio designado para tales fines, bajo la siguiente dirección electrónica: **http://www.aguascalientes.gob.mx/AC.** Es responsabilidad de la Secretaría de Gobierno la adopción de medidas de seguridad necesarias para garantizar la integridad, autenticidad y disponibilidad de dicha información.

Todos los suscriptores de la Autoridad Certificadora del Estado de Aguascalientes podrán tener acceso de forma fiable a las Políticas de Certificación y Declaración de Prácticas de Certificación, ingresando a la siguiente dirección electrónica: **http://www.aguascalientes.gob.mx/AC**, la información ahí publicada se encuentra aprobada y firmada por la Secretaría de Gobierno y además deberá publicarse en el Periódico Oficial del Estado.

Las listas de certificados revocados emitidas estarán firmadas electrónicamente por la Autoridad Certificadora del Estado de Aguascalientes y estarán disponibles para terceras partes de confianza.

La información sobre el estado de los certificados digitales de FEA emitidos se podrá consultar a través del servicio de validación en línea que implementa el protocolo OCSP, este servicio estará disponible en la siguiente dirección electrónica: **http://www.aguascalientes.gob.mx/AC.**

9.2 Entrada en vigor

Las Presentes Políticas de Certificación y Declaración de Prácticas de Certificación entrarán en vigor al día siguiente de su publicación en el Periódico Oficial del Estado de Aguascalientes.

Se comunica lo anterior para todos los efectos a que haya lugar.

Aguascalientes, Ags; a los treinta días del mes de octubre de dos mil trece.

Atentamente

SUFRAGIO EFECTIVO. NO REELECCIÓN

Lic. Sergio Javier Reynoso Talamantes.

SECRETARIO DE GOBIERNO.