POLÍTICA DE CERTIFICADOS DE LA AUTORIDAD CERTIFICADORA INTERMEDIA DE LA SECRETARÍA DE LA CONTRALORIA DEL PODER EJECUTIVO DEL ESTADO DE QUERÉTARO.

Fecha de Elaboración: Junio de 2008.

1. INTRODUCCIÓN.

La Política de Certificados es un conjunto de reglas que indican la aplicabilidad de un certificado a una comunidad y clase de aplicaciones con requerimientos comunes de seguridad.

Que el objetivo básico de la firma electrónica es aportar a los documentos electrónicos la misma funcionalidad que otorga la firma autógrafa a un documento impreso, incrementar la eficiencia en el quehacer gubernamental al reducir costos y sobre todo tiempo en el envío de información que contenga una firma válida.

En este documento se describe la Política de Certificados de la Autoridad Certificadora Intermedia de la Secretaría de la Contraloría del Poder Ejecutivo del Estado de Querétaro (ACI-SC), la cual deriva de la Autoridad Certificadora Raíz del Poder Ejecutivo del Estado de Querétaro conforme a la "Declaración de Prácticas de Certificación de la Autoridad Certificadora Raíz del Poder Ejecutivo del Estado de Querétaro". La Política de Certificados se aplica a la solicitud, validación, aceptación, emisión y revocación de los certificados digitales dentro de una Infraestructura de Clave Pública (PKI por sus siglas en inglés).

2. ALCANCE.

Con la finalidad de que los servidores públicos de la Administración Pública Estatal cuenten con los medios necesarios para poder producir firma electrónica respecto de mensajes de datos en los cuales tenga intervención, la Autoridad Certificadora Raíz del Poder Ejecutivo del Estado de Querétaro generará el Certificado Digital de la Autoridad Certificadora Intermedia a favor de la Secretaría de la Contraloría del Poder Ejecutivo del Estado de Querétaro (ACI-SC), quien a su vez, y de acuerdo a la estructura jerárquica de certificación descrita en el apartado COMUNIDAD Y APLICABILIDAD DE LA ACI-SC, procederá a generar los Certificados Digitales para la creación de la Firma Electrónica Avanzada a favor de:

a) Los servidores públicos adscritos a la Dirección de Prevención y Evaluación de la Secretaría de la Contraloría del Poder Ejecutivo del Estado de Querétaro en su calidad de Agente Certificador General y Agentes Certificadores Derivados.

b) Los servidores públicos de la Administración Pública del Estado de Querétaro o de aquellos Municipios, Dependencias o Entidades que requieran y acepten su integración a la presente infraestructura, que debido a la naturaleza de sus funciones requieran firmar electrónicamente algún tipo de mensaje de datos.

3. REFERENCIAS.

• RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, noviembre 2003. http://www.faqs.org/rfcs/rfc3647.html
• Ley Estatal de Acceso a la Información Gubernamental en el Estado de Querétaro
publicada en el Periódico Oficial “La Sombra de Arteaga” del 27 de septiembre de 2002.
• *RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile abril 2002*, http://www.faqs.org/rfcs/rfc3280.html .
• ISO/IEC 9594-8:2001 Information technology -- Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.

4. DEFINICIONES.

Certificado: Todo Mensaje de Datos u otro registro que confirme el vínculo entre un Firmante y los datos de creación de Firma Electrónica.

Comunidad: Estará integrada por los servidores públicos referidos en los incisos a) y b) del punto 2 “Alcance” del presente documento.

Distinguished Names (DN): Serie de información a través de la cual se puede identificar a una persona en un directorio de servidor, organizada de forma tal, que facilita la ubicación de sus datos.

Dispositivo: Aparato electrónico que se le asigna a un usuario el cual estará identificado con un número de serie que lo hace único y que contendrá sus claves pública y privada.

Emisor: Toda persona que, al tenor del Mensaje de Datos, haya actuado para enviar o generar ese mensaje antes de ser archivado.

Firma Electrónica Avanzada: Los datos en forma electrónica consignados en un Mensaje de Datos, o adjuntados o lógicamente asociados al mismo por cualquier tecnología, que son utilizados para identificar al Firmante en relación con el Mensaje de Datos e indicar que el Firmante aprueba la información contenida en el Mensaje de Datos, que produce los mismos

efectos jurídicos que la firma autógrafa y que cumpla con los requisitos contemplados en la Declaración de Prácticas de Certificación de la Autoridad Certificadora Raíz del Poder Ejecutivo del Estado de Querétaro.

Mensaje de Datos: La información generada, enviada, recibida o archivada por medios electrónicos, ópticos o cualquier otra tecnología.

Prestador de Servicios de Certificación: Advantage Security, S. de R.L. de C.V., quien presta los servicios de certificación de firma electrónica en virtud de su contratación por parte de la Secretaría de la Contraloría para tales efectos.

Secretaría: Se entenderá la Secretaría de la Contraloría del Poder Ejecutivo del Estado de Querétaro.

Titular del Certificado: Se entenderá a la persona a cuyo favor sea expedido el certificado.

Usuario: Los servidores públicos de la Administración Pública del Estado de Querétaro o de aquellos Municipios, Dependencias o Entidades que requieran y acepten su integración a la presente infraestructura, que debido a la naturaleza de sus funciones requieran firmar electrónicamente algún tipo de mensaje de datos.

5. ABREVIACIONES:

ACI-SC Autoridad Certificadora Intermedia de la Secretaría de la Contraloría.

DECLARACIÓN DE PRÁCTICAS.- Declaración de Prácticas de Certificación de la Autoridad Certificadora Raíz del Poder Ejecutivo del Estado de Querétaro.

CDIPAC Certificados Digitales de Identidad Personal para sus Agentes Certificadores de la Secretaría.

CDIP Certificados Digitales de Identidad Personal.

CRL Lista de Certificados Revocados.

OCSP Protocolo de Estatus de Certificados en Línea (por sus siglas en inglés *"Online Certicate Status Protocol"*). Permite hacer consultas en línea a las autoridades certificadoras y usuarios sobre el estatus de revocación o validez de un certificado. Permite

comprobar que al momento que se recibe la firma el estatus del certificado del firmante es válido.

CLAVES Clave Pública y Clave Privada.

URL *"Uniform Resource Locator"*, Localizador uniforme de recurso.

SolcSER Solicitud de Certificado para Firma Electrónica.

6. IDENTIDAD DE LA ACI-SC

Ubicación: Cinco de Mayo esquina Pasteur, sin número,
Colonia Centro Histórico; C.P. 76000, Santiago de Querétaro, Qro.
Tel: (442) 238 5000, extensión 5014.
Fax: (442) 238 5122.

Información sobre la Infraestructura de Clave Pública de la ACI-SC:
https://ca.advantage-security.com

7. COMUNIDAD Y APLICABILIDAD DE LA ACI-SC.

La comunidad y aplicabilidad de la ACI-SC están determinadas en esta Política de Certificados. La ACI-SC solamente podrá generar certificados de identidad personal (CDIPAC) para sus agentes certificadores, así como Certificados Digitales de identidad personal (CDIP) para los usuarios, que debido a la naturaleza de sus funciones, requieran producir firma electrónica respecto de un mensaje de datos.

La ACI-SC emitirá un certificado digital el cual solamente podrá ser almacenado en un dispositivo electrónico en los términos de las presentes políticas; a través de dicho procedimiento se vincula y autentifica al usuario con el mensaje de datos generado por éste al utilizar un acceso alfanumérico o biométrico que le permita el encriptamiento de su información.

7.1. ESTRUCTURA JERÁRQUICA

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

1.- Autoridad Certificadora Raíz del Poder Ejecutivo del Estado de Querétaro.- Entidad cuyo único propósito es servir como base para la creación de las Autoridades Certificadoras Intermedias.

2.- Autoridad Certificadora Intermedia de la Secretaría de la Contraloría.- Entidad derivada de la autoridad certificadora raíz cuyo propósito es brindar servicios de certificación de clave pública para su agente certificador

General así como los Derivados y los Usuarios.

3.- Agente Certificador General.- Servidor Público responsable de generar los certificados de los Agentes Certificadores Derivados así como de los usuarios. Asimismo, será la única autoridad facultada para llevar a cabo el procedimiento de revocación de un certificado digital de firma electrónica avanzada.

4.- Agentes Certificadores Derivados.- Personas responsables de llevar a cabo la identificación y autenticación de los solicitantes de certificados para la emisión del mismo.

5.- Usuario.- Persona que recibe por parte del Agente Certificador General o del Derivado un certificado digital y el cual se conceptualiza en el apartado de definiciones de las presentes políticas.

8. PRIVACIDAD Y SEGURIDAD

8.1. REQUERIMIENTOS DE SEGURIDAD PARA LA ACI-SC Y SUS CLAVES.

- La ACI-SC se sujeta a los lineamientos de seguridad que determine el prestador del servicio de certificación.
- Tanto el *hardware* como el *software* de misión crítica que opera la ACI-SC se mantendrá en todo momento físicamente en un lugar seguro, bajo el cuidado y responsabilidad del prestador del servicio de certificación.
- El par de claves RSA de la ACR Poder Ejecutivo del Estado de Querétaro, tendrá una longitud de 4096 bits.
- El par de claves RSA de la ACI-SC tendrá una longitud de 2048 bits.
- Se establecerá un procedimiento periódico de respaldo de los servidores que opere la ACI-SC. Las copias se guardarán en un lugar seguro protegido de accesos no autorizados conforme a lo establecido en los lineamientos del prestador de servicios de certificación.
- Si la clave privada de la ACI-SC estuviera comprometida, se procedería a la revocación de la misma y del certificado de la ACI-SC, así como todos los certificados emitidos por ella, no importando la fecha de emisión. A partir de ese momento, deberán revocarse todos los certificados emitidos por los Agentes Certificadores de la ACI-SC y no deberán emitir certificados válidos hasta que no se restaure la identidad de la ACI-SC y se vuelvan a generar certificados respectivos.
- El par de claves RSA de los certificados emitidos por la Autoridad Certificadora Intermedia ACI-SC tendrán una longitud de 1024 bits.

9. POLITICA DE CERTIFICACIÓN

9.1.POLÍTICA DE SEGURIDAD

El objetivo de la ACI-SC será únicamente la validación, y en su caso, aceptación y emisión de la solicitud de los Certificados Digitales a favor de los Usuarios que de acuerdo a la naturaleza de sus funciones requieran producir firma electrónica en algún mensaje de datos.

La revocación de cualquier certificado se realizará de acuerdo a lo establecido en el apartado "REVOCACIONES".

9.2.PERÍODO DE VALIDEZ DE LOS CERTIFICADOS DIGITALES

El período de validez del Certificado Digital de la ACI-SC será de 8 años a partir de su fecha de emisión.

El período de validez de los Certificados Digitales de los Agentes Certificadores General y Derivados (CDIPAC), así como de los Certificados Digitales de Identidad Personal (CDIP) otorgados a los servidores públicos de la Administración Pública Estatal, será de 2 años a partir de la fecha de su emisión.

9.3.CONVENCIONES DE NOMBRES

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

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

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

- El DN de los Certificados Digitales de Identidad Personal deben de proporcionar los siguientes atributos:
    - CN = Poder Ejecutivo del Estado de Queretaro
    - E = firmaelectronica@queretaro.gob.mx
    - = Poder Ejecutivo del Estado de Queretaro
    - STREET = Pasteur y 5 de Mayo, Centro Historico
    - PostalCode = 76000
    - L = Santiago de Queretaro
    - S = Queretaro
    - C = MX

- El DN de los Certificados Digitales de la Autoridad Certificadora Intermedia, deben de proporcionar los siguientes atributos:

    - CN = <Nombre de la ACI-SC>
    - E = <firmaelectronica@queretaro.gob.mx>
    - O= Poder Ejecutivo del Estado de Querétaro
    - STREET = <domicilio de la ACI-SC>
    - Postal Code = <Código Postal de la ACI-SC>
    - L = <Municipio del domicilio d de la ACI-SC >
    - S = <Entidad Federativa de la ACI-SC>
    - C = MX

- El DN de los Certificados Digitales del Usuario, deben de proporcionar los siguientes atributos:
    - CN=<Nombre del Usuario>
    - E=<correo electrónico-mail del usuario>
    - O= <Organismo o Dependencia de adscripción del usuario>
    - OU<Área de adscripción del usuario>
    - STREET= <Domicilio laboral del Usuario>
    - Postal Code= <Código Postal del Usuario>
    - L= <Municipio del domicilio laboral del Usuario>
    - S= <Entidad Federativa del Usuario>
    - C= mx

10. DISPOSICIÓN DE CERTIFICADOS

La Secretaría en su calidad de Autoridad Certificadora Intermedia mantendrá un repositorio o base de datos con los certificados que emita a través del prestador de servicios de certificación, de manera que estén disponibles a través de un servicio de distribución de certificados.

Así mismo, la ACI-SC mantendrá constancia de los certificados digitales en la página Web señalada en el apartado 6 de las presentes políticas.

11. LISTA DE CERTIFICADOS REVOCADOS (CRL)

La ACI-SC, a través de su Agente Certificador General, es el responsable de determinar la revocación de un certificado previa solicitud del Agente Certificador Derivado o del Usuario por la existencia de algún supuesto de los señalados en el punto 14 de las presentes Políticas, debiéndose generar para tal efecto una Lista de Certificados Revocados misma que se mantendrá en todo momento actualizada y bajo el resguardo del prestador de servicios de certificación.

12. OBLIGACIONES.

12.1.OBLIGACIONES DE LA SECRETARÍA DE LA CONTRALORÍA COMO ACI-SC:

- Mantener la infraestructura necesaria para el establecimiento de una estructura jerárquica de certificación a través de su Agente Certificador General y los Derivados, según la Política de Certificados descrita en este documento.
- Implementar y mantener los requerimientos de seguridad impuestos a las claves de la ACI-SC, según lo descrito en este documento en el apartado "PRIVACIDAD Y SEGURIDAD".
- Aprobar o denegar las solicitudes de acreditación así como de certificados y, en el primer caso, emitir los certificados de acuerdo con lo establecido en el apartado "POLÍTICA DE SEGURIDAD" de este documento.
- Verificar que el prestador de servicios de certificación mantenga las copias de sus certificados y de cualquier información de revocación a disposición de quien desee verificar una firma electrónica avanzada con referencia a estos.
- Verificar que el prestador de servicios de certificación del servicio de firma electrónica mantenga en todo momento actualizada la CRL, incluyendo todos los certificados revocados desde la última actualización.
- Proteger los datos de carácter personal que sean suministrados por los usuarios a acreditación en términos de la Ley Estatal de Acceso a la Información Gubernamental en el Estado de Querétaro.
- Comunicar inmediatamente, al prestador de servicios de certificación el compromiso, pérdida, divulgación, modificación, uso no autorizado de la clave privada de la ACI-SC, con el fin de restaurar la jerarquía lo antes posible según lo establecido en el apartado "PRIVACIDAD Y SEGURIDAD" de este documento.

12.2.OBLIGACIONES DE LOS AGENTES CERTIFICADORES DE LA ACI-SC

12.2.1.- Obligaciones Comunes de los Agentes Certificadores General y Derivados de la ACI-SC.-

- Llevarán a cabo cada uno de los pasos descritos en el procedimiento de emisión de certificados digitales por parte de la ACI-SC, según lo descrito en el **Anexo I** de este documento.
- Protegerán los datos personales de los solicitantes de certificados digitales, que no podrán ser cedidos a terceros bajo ningún concepto de acuerdo a la Ley Estatal de Acceso a la Información Gubernamental en el Estado de Querétaro.

12.2.2.- Obligaciones en particular del Agente Certificador General de

la ACI-SC.-

- Realizar la expedición de los certificados digitales a favor de los Agentes Certificadores Derivados.
- Llevar a cabo la revocación de certificados digitales en los supuestos previstos en el numeral 14 de las presentes políticas.

13. RESPONSABILIDADES.-

13.1.RESPONSABILIDADES DE LA ACI-SC

- La ACI-SC, garantiza el cumplimiento de las obligaciones descritas en este documento.
- Cualquier incidente o responsabilidad nacidos de la clave privada de la ACI-SC que se encuentra comprometida, es responsabilidad única y exclusiva de esta misma.

13.2.RESPONSABILIDADES DE LOS AGENTES CERTIFICADORES.

- Recibir y dar trámite a las solicitudes de expedición y revocación de los certificados de firma electrónica.
- Realizar la correcta identificación de los solicitantes para la emisión de certificados.
- Expedir los certificados de firma electrónica.
- Guardar confidencialidad respecto de la información que haya recibido para la expedición del certificado de firma electrónica.
- En general, dar cumplimento a cada una de las obligaciones establecidas en los distintos procedimientos contenidos en estas políticas.

14. CAUSAS DE REVOCACIÓN Y EXTINCIÓN.

14.1.Causas de Revocación.

I.- Cuando se observen inexactitudes en los datos aportados por el firmante para la obtención del certificado de la firma electrónica avanzada;
II.- Por haberse comprobado que al momento de la expedición del certificado de firma electrónica avanzada no cumplió con los requisitos que marca esta Ley; y
III.- Uso indebido o ilícito del certificado de firma electrónica o de la firma electrónica avanzada.
IV.- Cambio de información relativa al suscriptor.
V.- Se produce un error en la emisión de un certificado.
VI.- Resolución administrativa o judicial que lo ordene.
VII.- La clave privada de la ACI-SC fuese comprometida, en cuyo caso, serían revocados todos los certificados emitidos y no se podrán emitir certificados válidos hasta que no se restaure la identidad de la ACI-SC y se vuelvan a generar los

certificados de los Agentes Certificadores.

14.2.Causas de Extinción.

I.- Fallecimiento del titular o incapacidad jurídica declarada por una Autoridad competente;
II.- Expiración de su vigencia;
III.- Pérdida, robo o inutilización del certificado de firma electrónica avanzada, divulgación no autorizada u otro compromiso de la clave privada asociada al certificado;
IV.- Terminación del empleo, cargo o comisión del servidor público, por el cual le haya sido concedida el uso de la firma electrónica avanzada; y
V.- A solicitud del titular del certificado de la firma electrónica avanzada;
VI.- En cualquiera de las causas que se señalan en la "DECLARACIÓN DE PRÁCTICAS" que le sean aplicables.

14.3. Procedimiento.

La revocación de un certificado digital emitido por la ACI-SC, se realizará siguiendo el procedimiento descrito a continuación:

a) El Agente Certificador General será el único facultado para llevar a cabo el procedimiento de revocación o extinción del certificado digital.

b) En el supuesto de alguna causal de extinción del certificado, los usuarios, o en su caso, las Unidades de Apoyo Administrativo o su equivalente en la Dependencia o Entidad, serán los responsables de solicitar por escrito la extinción del certificado correspondiente. Dicha solicitud deberá de expresar cual es el motivo que da origen a la petición, y dirigirse a la Dirección de Prevención y Evaluación de la Secretaría de la Contraloría.

c) En el caso de los supuestos señalados como causa de revocación, la Autoridad Certificadora iniciará de oficio el procedimiento correspondiente, el cual una vez que sea concluido, será notificado al usuario a través del correo electrónico proporcionado en su "Solicitud de Certificado para Firma Electrónica" (SolcSER).

ANEXO I. PROCEDIMIENTO DE EMISIÓN DE CERTIFICADOS

DIGITALES DE AUTORIDAD CERTIFICADORA.

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

1. La Dirección de Prevención y Evaluación de la Secretaría de la Contraloría tendrá a su cargo la función de determinar los puestos y funciones en la Administración Pública que de acuerdo a su nivel jerárquico, o bien, la naturaleza de sus funciones, tengan necesidad de firmar electrónicamente un mensaje de datos.

2. Una vez hecho lo anterior, la ACI-SC deberá de llevar a cabo la instalación en la máquina del usuario correspondiente, del software que le permita a este poder acceder al uso de la firma electrónica.

3. El Agente Certificador de la Secretaría de la Contraloría tendrá la obligación de verificar fehacientemente la identidad del titular del certificado, para lo cual, requerirá de su presencia física, quien deberá de identificarse plenamente a satisfacción del Agente Certificador; para tal efecto, deberá de presentar una identificación oficial vigente con fotografía.

4. Previo a la generación del certificado digital correspondiente, los Usuarios deberán de presentar al Agente Certificador el formato “Solicitud de Certificado para Firma Electrónica” (SolcSER) debidamente requisitado a mano en letra de molde, o bien, en computadora o máquina de escribir. Dicha solicitud quedará en poder del Agente Certificador, siendo su responsabilidad verificar que las mismas se encuentren debidamente requisitadas y que todos los datos que aparecen en las mismas, coincidan con la información proporcionada por el servidor público.

   Será de exclusiva responsabilidad del usuario que requisite el formato de “Solicitud de Certificado para Firma Electrónica” (SolcSER) la veracidad de los datos asentados en dicha solicitud.

5. El Agente Certificador requerirá a los Servidores Públicos responsables que firmen en original el documento de solicitud para verificar la coincidencia entre la firma autógrafa del documento de solicitud y la que aparece en las credenciales oficiales presentadas, considerándose a partir de ese momento, como aceptada dicha solicitud.

6. Una vez hecho lo anterior, el Agente Certificador, ingresará a la página web correspondiente a fin de generar el requerimiento de certificado de firma electrónica, así como también en su caso, llevar a cabo el procedimiento de autorización del mismo, previo a lo cual, deberá de verificar que los datos que sean capturados en dicho sistema, no contengan error alguno en relación a la información proporcionada por el solicitante.

   Concluido lo anterior, el Agente Certificador procederá a la emisión del certificado de firma electrónica respectivo, e imprimirá el “Comprobante de

Emisión de Certificado Digital de Firma Electrónica Avanzada” que arroja el mismo sistema, y a efecto de que sea firmado por el usuario respectivo.

7. Finalizado el paso anterior, el Agente Certificador procederá a almacenar en el dispositivo electrónico del usuario, el archivo que contiene el certificado digital de firma electrónica avanzada que ha sido expedido a su favor.