DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ DEL PODER EJECUTIVO DEL ESTADO DE QUERETARO

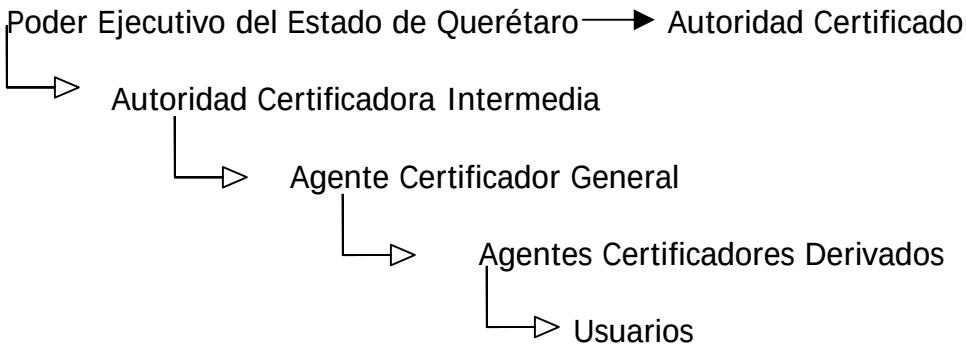
1. INTRODUCCIÓN

En virtud de los avances tecnológicos que a nivel mundial se van presentando día con día, tendientes a agilizar los medios de comunicación y envío de información a nivel global, incluido el uso de medios electrónicos como un mecanismo que permite la toma de decisiones de manera rápida y transparente como lo es la utilización de Firma Electrónica Simple y Firma Electrónica Avanzada. En nuestro país, la legislación federal ha incorporado el mecanismo de firma electrónica como un medio para reconocer y autentificar el contenido de un documento a través de medios electrónicos con seguridad técnica y jurídica, tal es el caso de las materias de derecho mercantil, fiscal, procesal y civil. Es el caso del Estado de Querétaro, quien con la necesidad de mantenerse a la vanguardia como el resto del país en tecnología de la información, a incorporado la utilización de medios electrónicos en su propia legislación, destacando recientemente las reformas a la Ley que establece las bases para la Entrega Recepción Administrativa en el Estado de Querétaro publicadas en el Periódico Oficial "La Sombra de Arteaga" de fecha 27 de julio de 2007, a través de las cuales se permite realizar el Proceso de Entrega Recepción por medio del uso de medios electrónicos y aún más con la publicación de la Nueva Ley de Entrega Recepción publicado en el mismo órgano de difusión de fecha 20 de marzo de 2009, en donde se establece un Capítulo Quinto denominado "*De la utilización de los medios electrónicos*", reconociendo en la Secretaría de la Contraloría del Poder Ejecutivo del Estado de Querétaro la calidad de Autoridad Certificadora.

Derivado de lo anterior, el Poder Ejecutivo del Estado de Querétaro a tomado la decisión de incorporar en el Entidad el esquema de producción de Firma Electrónica para diversos actos administrativos y de servicios que presta la Administración Pública Estatal, constituyéndose como Autoridad Certificadora Raíz, a efecto de que los usuarios de la misma efectúen operaciones con un nivel confiable de seguridad que les ofrezca integridad, autenticación y no repudio, por lo que en este documento se describen las reglas y procedimientos que deberán de permitirle a dichos usuarios, confiar en los servicios ofrecidos por dicha Autoridad Certificadora mediante el uso de claves públicas y privadas.

1.1 Propósito

Describir la Declaración de Prácticas de Certificación para la Autoridad Certificadora Raíz del Poder Ejecutivo del Estado de Querétaro (ACR-PEEQ), dentro de la Infraestructura de Clave Pública (PKI), establecida de la siguiente manera:



La Autoridad Certificadora Raíz (ACR-PEEQ) certificará las claves públicas de las Autoridades Certificadoras Intermedias (ACI) que hayan sido acreditadas por esta última, para la prestación de servicios o generación de actos administrativos a cargo de la Administración Pública Estatal conforme a la normatividad aplicable a través de la utilización de medios electrónicos para el cumplimiento de sus funciones dentro de la infraestructura de llave pública (PKI) de aquella.

Más información referente de la ACR-PEEQ en:

https://ca.advantage-security.com/asusuario/

1.2 Identificación

Este documento es denominado como **"Declaración de Prácticas de Certificación de la Autoridad Certificadora Raíz del Poder Ejecutivo del Estado de Querétaro ".** Esta versión podrá consultarla en la dirección siguiente:

https://ca.advantage-security.com/asusuario/

1.3 Comunidad y aplicabilidad

La comunidad que comprende la ACR-PEEQ, son los usuarios que realicen actos administrativos o requieran de la prestación de servicios públicos que prestan las diversas Dependencia o Entidades que integran la Administración Pública del Poder Ejecutivo del Estado de Querétaro, que en los términos de la normatividad

correspondiente utilicen medios electrónicos en dichos actos o servicios dentro de la infraestructura de llave pública (PKI).

Su ámbito o aplicabilidad principal de los certificados es para realizar cualquier trámite ante cualquier Autoridad Certificadora Intermedia (ACI) que derive de la Autoridad Certificadora Raíz (ACR-PEEQ).

1.3.1 Autoridad Certificadora Raíz

La Autoridad Certificadora Raíz del Poder Ejecutivo del Estado de Querétaro (ACR-PEEQ) es una entidad cuyo propósito es la emisión y/o revocación de certificados de las Autoridades Certificadoras Intermedias (ACI), siendo responsable de dicha Autoridad el Titular del Poder Ejecutivo del Estado de Querétaro o la persona que éste designe para ello a través del acuerdo delegatorio correspondiente.

1.3.2 Autoridad Certificadora Intermedia

Las Autoridades Certificadoras Intermedias (ACI) derivara de la ACR-PEEQ, quienes serán las encargadas de autenticación e identificación del Agente Certificador General, Agentes Certificadores Derivados y de los usuarios finales, así como verificar la identidad del solicitante del certificado a favor de éste y de llevar acabo el procedimiento para la emisión y/o revocación de certificados.

1.3.3 Entidades o usuarios finales

La Autoridad Certificadora Raíz del Poder Ejecutivo del Estado de Querétaro

- Esta a su vez podrá certificar las claves públicas de las Autoridades Certificadoras Intermedias (ACI), y a su vez de ésta derivaran las claves del Agente Certificador General, de los Agentes Certificadores Derivados y de los usuarios finales que utilicen medios electrónicos para el cumplimiento de sus funciones o realizar cualquier trámite relacionado con la prestación de servicios a cargo del Poder Ejecutivo del Estado de Querétaro dentro de la infraestructura de llave pública (PKI) de la ACR-PEEQ.

- El manejo de certificados por parte de la ACR-PEEQ lo lleva a cabo a través del Prestador de Servicios de Certificación (PSC), Advantage Security, S. de R.L. de C.V. cuyas políticas se encuentran basadas en la norma **NOM**-151-SCFI-2002.

1.4 Contacto

En la Secretaría de la Contraloría del Poder Ejecutivo del Estado de Querétaro, podrá enviar sus comentarios, dudas u observaciones referentes a esta Declaración de Practicas de certificados.

Ubicación
Pasteur esquina 5 de Mayo
Colonia Centro Histórico
Correo electrónico de la ACR-PEEQ: acrpeeq@queretaro.gob .mx
Teléfono (+52) (442) 2.38.50.00 ext. 5742 y 5190
Fax: 442. 2.38.51.22
Información sobre la Infraestructura de Clave Pública de la ACR-PEEQ

https://ca.advantage-security.com/asusuario/

2. OBLIGACIONES Y RESPONSABILIDADES

2. OBLIGACIONES Y RESPONSABILIDADES

2.1 Obligaciones

2.1.1 Obligaciones de la ACR-PEEQ

- Ofrecer un servicio constante mediante la infraestructura requerida de un (PKI), manteniendo los requerimientos de seguridad necesarios para proteger las claves privadas de los usuarios que utilicen medios electrónicos para el cumplimiento de sus funciones o realicen trámites con relación a los servicios que presta el Poder Ejecutivo del Estado de Querétaro dentro de la infraestructura de llave pública (PKI) de la ACR-PEEQ.

- Respaldar y mantener los certificados emitidos y revocados en un sitio de alta disponibilidad custodiado por el PSC Advantage Security, S. de R.L. de C.V., para que la parte que confía o cualquier interesado en transigir con dichos certificados, pueda consultar el estatus de los mismos. Para tal efecto se mantendrá actualizada dicha información en las páginas Web destinadas a la ACR-PEEQ por el PSC Advantage Security, S. de R.L. de C.V.

- Emitir o revocar los certificados de las Autoridades Certificadoras Intermedias de acuerdo con lo establecido en este documento, así como actualizar y publicar la Lista de Certificados Revocados, por conducto del PSC Advantege Security, S. de R.L. de C.V.

- Solo podrán emitirse certificados digitales cuando los mismos sean depositados en un dispositivo de almacenamiento criptográfico específico, a

fin de brindar mayor seguridad en el acceso y utilización del certificado digital, así como de las llaves, pública y privada, depositadas en el mismo.

- En caso de compromiso de la clave privada de la ACR-PEEQ, notificar a los usuarios de esta última, para que no se emita ningún certificado, hasta que no se restaure la nueva clave privada de la ACR-PEEQ, de conformidad con lo establecido en este documento.

2.1.2 Obligaciones de la Autoridad Certificadora Intermedia (ACI-SC)

- Atender las solicitudes, aprobar o denegar dichas solicitudes promovidas por los usuarios de la ACR-PEEQ, que utilicen medios electrónicos para el cumplimiento de sus funciones o que realicen trámites en la prestación de servicios que presta la ACR-PEEQ de conformidad con la normatividad aplicable y dentro de la infraestructura de llave pública (PKI) de la ACR-PEEQ.

- Cumplir con los procedimientos que le competen en la emisión de certificados por parte de la ACR-PEEQ de acuerdo con el numeral 4 de este documento.

- Realizar la identificación y autentificación para determinar su emisión o revocación de certificados, de conformidad con el numeral 3.1.2 de este documento.

- Realizar la carga de las solicitudes de certificados y revocaciones validas en el sistema.

- Proteger los datos personales de los solicitantes, que no podrán ser cedidos a terceros bajo ningún concepto (Ley Estatal de Acceso a la Información Gubernamental en el Estado de Querétaro)

- Atenderá las solicitudes, de las entidades referidas en el numeral 1.3 de este documento.

- El certificado raíz de la ACR-PEEQ, se encuentra almacenado en el dispositivo HSM Luna, el cual está bajo el resguardo del PSC Advantage Security, S. de R.L. de C.V.

2.1.3 Obligaciones de las entidades certificadas

- Mantener en todo momento protegida su clave privada con un nivel de seguridad adecuado a través de un dispositivo de almacenamiento criptográfico específico establecido por la ACR-PEEQ.

- Notificar a la Autoridad Certificadora Intermedia de la ACR-PEEQ, su solicitud de revocación de su certificado o cualquier sospecha de compromiso de sus claves, en su caso.

- Las entidades certificadas por la ACR-PEEQ, deben de conocer y aceptar esta CPS y sus responsabilidades de conformidad con el numeral de 2.2 de este documento.

- Informar a las partes que confíen en certificados firmados por la ACR-PEEQ, que tienen la obligación de verificar si son validos o el estado que guardan éstos cada vez que vayan a ser utilizados, verificar que no haya expirado y que aparezca en la Lista de Certificados Revocados (CRL) de la ACR-PEEQ

2.1.4 Obligaciones del repositorio

- La ACR-PEEQ publicará su certificado, su CRL y los certificados firmados por ésta, en la Web destinada al servicio de la Autoridad Certificadora ACR-PEEQ a cargo del PSC Advantage Security, S. de R.L. de C.V. **(https://ca.advantage-security.com/asusuario).**

- Permitir consultar esta información en las páginas web destinadas al servicio de la ACR-PEEQ por el PSC Advantage Security, S. de R.L. de C.V.

2.2 Responsabilidades

2.2.1 Responsabilidades de la ACR-PEEQ

- La correcta emisión de los certificados y de los posibles errores surgidos del sistema durante los procesos de generación y revocación de los certificados.

- Los problemas derivados del compromiso de la clave privada de la ACR-PEEQ y la notificación de la revocación de la misma

- Revocar a través de la Autoridad Certificadora Intermedia correspondiente cualquier certificado en cuanto le sea notificado o se detecte algún incumplimiento de los requisitos establecidos en el marco jurídico aplicable en la materia a los PSC, compromiso o mal uso del mismo.

- Proteger la clave privada de la ACR-PEEQ mediante el uso de un módulo criptográfico que por lo menos cumpla con el estándar FIPS 140-2 nivel 3.

- La Secretaría de la Contraloría como administrador de la ACR-PEEQ, garantiza el cumplimiento de las obligaciones descritas en este documento.

2.2.2 Responsabilidades de las ACI

- Verificar que cuenten con los requisitos en la normatividad aplicable.

- Es responsabilidad de la ACI la identificación y autenticación de los solicitantes para poder emitir su certificado o revocarlo según sea el caso.

2.2.3 Responsabilidades del Agente Certificador General (ACG) y Agentes Certificadores Derivados (ACD)

- El ACG será el único en revocar los certificados digitales emitidos a las entidades certificadas.

- Tanto el ACG como los ACD mantienen el compromiso de su clave privada, como pérdida, uso indebido, etc.

- Problemas surgidos mediante una emisión o revocación de un certificado a la ACR-PEEQ.

2.3 Cumplimiento de Auditoria

El PSC Advantage Security, S. de R.L. de C.V., proporciona el servicio de certificación de la ACR-PEEQ, por lo que la información correspondiente a los certificados digitales emitidos por esta última se encuentran resguardados en un sitio seguro a cargo del propio PSC.

2.4 Política de confidencialidad de la información

2.4.1 Información confidencial

- La información clasificada como confidencial será de acuerdo a la Ley Estatal de Acceso a la Información Gubernamental en el Estado de Querétaro.
- Cualquier dato de carácter personal suministrado por las entidades a la Autoridad Certificadora Raíz ACR-PEEQ
- Material criptográfico privado asociado con la ACR-PEEQ
- La información derivada de una revocación de algún certificado.

- Información sobre las personas que administran la ACR-PEEQ, excepto su nombre, teléfono, correo electrónico, cargo dentro de la ACR-PEEQ e información que aparece en el propio certificado que posean.
- Registro de los eventos registrados por los sistemas de monitoreo de la red y cualquier sistema de seguridad.

2.4.2 Información no confidencial

La ACR-PEEQ y la ACI-SC manejan como información no confidencial la siguiente: información incluida en los certificados, CRLs, CPs y CPSs, marco jurídico. Cabe mencionar que dicha información se encuentra bajo el resguardo del PSC Advantage Security, S. de R.L. de C.V..

2.4.3 Causas de revocación

Se determinarán como causas de revocación las descritas en el numeral 15 de las Políticas de Certificados (CP) de ACR-PEEQ, según sea el caso.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

Registro

Tipos de nombres

La ACR-PEEQ solo acepta solicitudes de firma donde su DN (Distinguished Names) refleje el ámbito organizacional bajo el cual se va a certificar.

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

Cada entidad debe de tener un DN único y claro contenido en el campo “Subject” del certificado firmado por la ACR-PEEQ.

- 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 las Autoridades Certificadoras Intermedias, deben de proporcionar los siguientes atributos:

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

- El DN de los Certificados Digitales del Agente Certificador General (ACG), Agentes Certificadores Derivados (ACD) y Usuario, deben de proporcionar los siguientes atributos:
    - CN=<Nombre del ACG, ACD o Usuario>
    - E=<correo electrónico-mail del ACG, ACD o Usuario>
    - O= <Nombre de la Dependencia o Entidad del ACG, ACD o Usuario>
    - OU= <Nombre de la Unidad Organizativa del ACG, ACD o Usuario>
    - STREET= <Domicilio del ACG, ACD o Usuario>
    - PostalCode= <Código Postal del ACG, ACD o Usuario>
    - L= <Municipio del domicilio del ACG, ACD o Usuario>
    - S= <Entidad Federativa del ACG, ACD o Usuario>
    - C= MX

Autenticación de los solicitantes de certificados a la ACR-PEEQ.

Para Autoridades Certificadoras Intermedias (ACI)

- El solicitante del Certificado, deberá presentar original y copia para su cotejo de una (Cartilla, cédula profesional, pasaporte vigente o credencial de IFE), acompañado del nombramiento que lo acredita como Titular de la Dependencia o Entidad del Poder Ejecutivo del Estado de Querétaro que solicita la generación del certificado para ser considerada Autoridad Certificadora Raíz.

Para el Agente Certificador General (ACG)

- El solicitante del certificado, deberá de presentar original y copia para su cotejo de una identificación oficial (Cartilla, cédula profesional, pasaporte vigente, credencial de IFE, etc.), acompañada del Formato de solicitud de certificado digital debidamente requisitado en el que se determine su nombre y cargo, y demás datos que permitan dar identidad a su persona,

el cual será autorizado por el titular de la ACI-PEEQ o la persona que éste designe para ello a través del acuerdo delegatorio correspondiente.

Identidad Personal para sus Agentes Certificadores Derivados (ACD) de la ACI

- El solicitante del certificado de esta entidad, deberá de presentar una identificación oficial (Cartilla, cédula profesional, pasaporte vigente, credencial de IFE, etc.), acompañado del formato de solicitud de certificado digital a través del cual se identifique su nombre y cargo y demás datos de identidad, para lo cual el ACG revisará que la información proporcionada por el ACD corresponda a la requisitada en dicho formato.

Identidad Personal para los usuarios:

- El solicitante del certificado, deberá presentar original y copia para su cotejo de una identificación oficial (Cartilla, cedula profesional, pasaporte vigente, credencial del IFE, credencial institucional, etc.) acompañada de la solicitud de emisión de certificado digital y demás requisitos que determine cada ACI en su declaración de prácticas.

- El agente certificador general y sus derivados de la ACI serán los encargados de llevar a cabo la identificación y autenticación de los solicitantes de certificados, requiriendo en cualquier caso la presencia física del solicitante o de la persona que será el titular del certificado, para verificar que tenga coincidencia con la fotografía contenida en la identificación presentada.

Procedimiento de generación de claves.

Los titulares de los certificados, serán los encargados de la generación del par de claves, privada y pública, igualmente para el de la ACR-PEEQ a través del Gobernador del Estado de Querétaro o a quien delegue dicha facultad a través del acuerdo correspondiente y para las ACI a través de su Titular.

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

Generación de claves nuevas después de la revocación

Si no ha existido compromiso de la clave privada, el procedimiento de generación de claves se realizará de acuerdo a lo especificado en el párrafo anterior.

Si ha existido compromiso de clave, no se podrá firmar un nuevo certificado a partir de dicho par de claves y se tendrá que volver a generar el par de claves correspondientes.

Solicitud de revocación

La ACR-PEEQ a través de la ACI y esta a su vez por medio de su Agente Certificador General (ACG) revocará cualquier clave privada que incurra alguno de los supuestos del numeral 15.1 de la Política de Certificados de la ACR-PEEQ, o que esta detecte que ha sido comprometida clave en cuestión.

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

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

4 REQUERIMIENTOS OPERACIONALES

Solicitud de certificados

ACR-PEEQ se reserva el derecho de rechazar las solicitudes que incumplan algún requisito solicitado en el marco jurídico aplicable. Si es rechazada, la ACR-PEEQ a través de la ACI correspondiente informará al solicitante las razones por las que se rechaza dicha solicitud.

La ACR-PEEQ, sólo acepta solicitudes para las entidades descritas en el numeral 3.1.2.

El requerimiento de certificado digital de la ACR-PEEQ deberá realizarse a través de la página web: https://ca.advantage-security.com/asusuario, a cargo del PSC-Advantege Security.

4.1.1 Certificado de las Autoridades Certificadoras Intermedias

- El solicitante generará un par de claves públicas y privadas, previo a la solicitud de su clave pública. Todos los datos de solicitud de certificado serán iguales a los del Poder Ejecutivo del Estado de Querétaro, excepto por la Unidad Organizativa (OU). El usuario tendrá la obligación de conservar su clave privada en un lugar seguro.

4.1.1 Certificado del Agente Certificador General

- El solicitante generará un par de claves pública y privada, previo a la solicitud de certificación de su clave pública. El usuario tendrá la obligación de conservar su clave privada en un lugar seguro, misma que estará almacenada en un dispositivo de almacenamiento específico.

4.1.2 Certificados de los Agentes Certificadores Derivados

- El solicitante generará un par de claves pública y privada, previo a la solicitud de certificación digital a través de la página web: https://ca.advantage-security.com/asusuario, a cargo del PSC- Advantege Security, S. de R.L. de C.V., debiendo presentar conjuntamente con su requerimiento el Formato de Solicitud de Certificado Digital de Agente Certificador Derivado acompañado de una identificación oficial, el cual será revisado por el Agente Certificador General (ACG) a fin de dar identidad al ACD.

- El ACD tendrá la obligación de conservar su clave privada en un lugar seguro.

- Es responsabilidad del ACG verificar si se cumple con el procedimiento descrito en el numeral 3.1.2 de este documento, según el caso que le aplique.

- El ACG procederá a acreditar la información señalada en el requerimiento, a fin de constatar que la misma coincida con la señalada en el Formato correspondiente y con la identificación oficial presentada. Una vez verificada la integridad del solicitante el ACG procederá a emitir el certificado correspondiente el cual será depositado en un dispositivo de almacenamiento criptográfico específico.

- Los datos y documentos proporcionados por el solicitante quedaran en custodia de la ACI correspondiente.

4.1.3 Solicitud de certificados digitales de usuarios.

- El solicitante del certificado digital de usuarios será su responsable directo y deberá disponer de un certificado digital de identificación personal emitido por la ACR-PEEQ a través de la ACI correspondiente.

- El solicitante del certificado se presentará en las instalaciones de la ACI con el formato que determine ésta en su declaración de políticas debidamente requisitado y firmado acompañado de su identificación personal, procediendo la ACI a través de sus agentes certificadores (ACG o ACD) a verificar la identidad del usuario solicitante a través de dichos documentos.

- El usuario solicitante a través de la aplicación https://ca.advantage-security.com/asusuario, a cargo del PSC- Advantege Security, S. de R.L de C.V., generará de manera personal el requerimiento de su certificado, así como sus datos de creación de firma electrónica o clave privada.

- La ACI a través de sus agentes certificadores (ACG o ACD) a través de la página web https://ac.advantage-security.com/asoper acreditará que la documentación presentada por el servidor público y los datos contenidos en su requerimiento guardan consistencia y procederá a emitir el certificado digital correspondiente, el cual será almacenado en un token o en un dispositivo de almacenamiento equivalente, conjuntamente con el par de claves pública y privada, esta última del exclusivo conocimiento del solicitante.

4.2 Firma y entrega de certificados.

- La ACI correspondiente a través de sus agentes certificadores (ACG o ACD) emitirá el comprobante de emisión de certificado digital de firma electrónica avanzada, el cual deberá ser firmado por el usuario, quedando un original del mismo en custodia de la ACI.

- La ACI a través de sus agentes certificadores (ACG o ACD) entregará al usuario el certificado digital en el dispositivo de almacenamiento criptográfico conjuntamente con su clave pública y privada.

4.3 Revocación de certificados

- Se determinarán como causa de revocación las descritas en el numeral 15 de la Política de Certificados (CP) de la ACR-PEEQ.

4.4 Frecuencia de firmado de la CRL

- ACR-PEEQ a través de la ACI correspondiente firmará una nueva CRL cada vez que se revoque un certificado, cuya administración corresponderá a la ACI y su resguardo al PSC Advantage Security, S. de R.L. de C.V. Se llevará a cabo la actualización incluyendo las listas anteriores.
- La entidad que confié en los certificados emitidos por la ACR-PEEQ, tendrá la obligación de verificar su estado en la CRL

- Para verificar los puntos anteriores se tendrá en línea la información en la aplicación que para tal efecto determine el PSC Advantage Security, S. de R.L. de C.V. a favor de la ACR-PEEQ.

4.5 Procedimientos de Auditorias de Seguridad

Se integrarán los procedimientos con información necesaria para obtener la certificación WebTrust y BS7799

4.6 Archivo de Registros

4.6.1 Tipos de Eventos Registrados

- Se llevara un registro de los eventos ocurridos en el servicio de ACR-PEEQ, derivado de los procedimientos de solicitudes, emisión de certificados, revocación de certificados, actualización de la CRL entre otros que permitan mantener el servicio de consulta.
- Respaldos periódicos de toda información de la ACR-PEEQ y respaldos cada vez que se genere o revoque un certificado.
- Los respaldos se resguardaran en un lugar seguro y estarán protegidos criptográficamente, teniendo acceso exclusivamente personal autorizado.
- Mantendrá el equipo redundante para ofrecer el servicio continuo de la ACR-PEEQ y de consulta del web.
- Se conservarán registros de los accesos al web de la ACR-PEEQ.
- La ACR-PEEQ a través de la ACI correspondiente mantendrá una copia de las comunicaciones electrónicas con los usuarios de ésta.
- Toda la información de los solicitantes descritos en el apartado “Alcance” de la Política de Certificados de la ACR-PEEQ enviada en papel, medio magnético digital, se resguardará en un lugar seguro.

4.6.2 Periodo de resguardo de la información

- La información concerniente a los registros de la ACR-PEEQ, se resguardará durante 5 años, en un lugar seguro.

4.6.3 Protección de la Información

- La información que pertenece al centro de datos de la ACR-PEEQ es respaldada y protegida en lugares seguros bajo custodia apropiada, solo tiene acceso a esta el personal autorizado, se cuenta con control de acceso físicos y lógicos.
- Se mantiene un respaldo del software utilizado en el servicio de la ACR-PEEQ, para poder proceder a la información respaldada en otro sitio autorizado para tal fin.

4.6.4. Procedimiento de respaldo

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

4.7. Renovación de claves públicas y privadas de las entidades.

Cuando se haya superado cuatro quintos del tiempo de vida de la Autoridad Certificadora de la ACR-PEEQ, se generará una nueva identidad raíz. A partir de ese momento, se firmarán certificados con la nueva identidad.

La Autoridad Certificadora de la ACI correspondiente dispondrá de una quinta parte del tiempo para solicitar nuevo certificado.

Los certificados emitidos por las ACI están disponibles en la página Web en https://ac.advantage-security.com/asusuarios.

4.8 Compromiso y recuperación de desastres

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

Una vez generadas las nuevas claves de la ACR-PEEQ, se emitirá el certificado correspondiente a cada Autoridad Certificadora Intermedia ACI, ésta a su vez deberá llevar a cabo la revocación y emisión de los nuevos certificados de los agentes certificadores (ACG y ACD) y de sus usuarios.

En caso de compromiso de la clave privada de la Autoridad Certificadora Intermedia (ACI), ésta tendrá el deber de notificarlo a la ACR-PEEQ y a sus usuarios.

4.8.1 Recuperación de hardware, software o datos

- En caso de corrupción de hardware que da el servicio de la ACR-PEEQ a cargo del sitio que señale el PSC Advantage Security, S. de R.L. de C.V., éste cuenta con equipo redundante en otro sitio para continuar ofreciendo el servicio.

- En caso de corrupción de software que da el servicio de la ACR-PEEQ a cargo del PSC Advantage Security, S. de R.L. de C.V., éste cuenta con

respaldos periódicos para poder recuperar la información necesaria, de la misma forma en caso de corrupción de la información.

- La clave privada de la ACR-PEEQ estará en todo momento cifrada y almacenada de modo permanente en el modulo criptográfico HSM Luna el cual se encuentra bajo el resguardo del PSC Advantage Security, S. de R.L. de C.V.

4.8.2 Recuperación ante desastres

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

5. CONTROLES DE SEGURIDAD FÍSICOS, PERSONALES Y DE PROCEDIMIENTOS

La ACR a implementado la Política de Seguridad la que considera lo establecido en esta CPS.

5.1 Controles físicos
5.1.1 Ubicación física de la ACR-PEEQ

- El servidor que administra la ACR-PEEQ esta ubicado en el área de Autoridades Certificadoras que se encuentra bajo custodia del PSC Advantage Security, S. de R.L. de C.V., es el área más segura de la PKI del Poder Ejecutivo del Estado de Querétaro.

5.1.2 Acceso físico a la ACR-PEEQ

- El acceso a el área de la ACR-PEEQ, está restringido únicamente a personal autorizado el cual es responsable el PSC Advantage Security, S. de R.L. de C.V.

5.1.3 Acondicionado de aire y energía eléctrica

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

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

5.1.6 Almacenamiento de medios

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

5.1.7 Respaldos

- Los respaldos se llevan a cabo cumpliendo con lo estipulado en el numeral 4.6.3,4.6.4 y bajo la Política de Respaldos de la ACR-PEEQ respectivamente.

5.2 Controles de seguridad personales

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

- El personal responsable de la ACR-PEEQ, esta contratado por el Poder Ejecutivo del Estado de Querétaro y cuenta con el nivel y conocimientos necesarios para dicha responsabilidad, El procedimiento se esta integrando, por el momento el personal cuenta con la capacitación necesaria para la administración y mantenimiento del la ACR-PEEQ.

5.2.2 Procedimientos de verificación del personal.

- El área de Recursos Humanos verifica previamente los antecedentes del personal contratado por el Poder Ejecutivo del Estado de Querétaro, comprueba que cumpla con los requisitos establecido por Ley.

5.2.3 Requerimientos de capacitación

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

5.2.4 Sanciones por acciones no autorizadas

- Las sanciones se valorarán dependiendo el riesgo que representen a la ACR-PEEQ, y serán determinadas por la Secretaría de la Contraloría del Poder Ejecutivo del Estado de Querétaro.

5.2.5 Controles sobre la contratación de personal

- Descrito en el numeral 5.2.2 de este documento.

5.2.6 Documentación proporcionada al personal de la ACR-PEEQ

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

5.3 Controles de Procedimientos

5.3.1 Funciones de confianza

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

Personal de operación de la ACR-PEEQ:

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

Personal que administra las funciones de la ACR-PEEQ:

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

Personal de la ACI:

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

6.CONTROLES DE SEGURIDAD TÉCNICOS

6.1 Generación e Instalación del par de claves

(el par de claves fueron generadas utilizando un modulo criptográfico invocado del sw del AC de PSC Advantage)

El par de claves de la ACR-PEEQ serán generadas utilizando el software AC de PSC Advantage , éste se utiliza para la administración de la Autoridad Certificadora de la ACR-PEEQ.

La clave privada estará en todo momento cifrada, ésta se encuentra almacenada en el modulo criptográfico el cual cumple con el FIPS 140-2 nivel 3.

6.1.1 Generación del par de claves.

El par de claves de la ACR-PEEQ serán generadas por el personal responsable del servidor que administra la ACR-PEEQ y que se encuentra bajo el resguardo del PSC Advantage security, S. de R.L. de C.V.

El par de claves de las entidades no son generadas ni entregadas por la ACR-PEEQ.

Las entidades que formarán parte de los usuarios de la ACR-PEEQ, deberán generar su par de claves en un lugar seguro, bajo su exclusivo conocimiento y responsabilidad.

6.1.2 Entrega de la clave pública a las entidades.

Las entidades finales presentarán su clave pública (mediante un requerimiento PKCS#10) a la Autoridad Certificadora Intermedia ACI correspondiente para que sea certificada, una vez que se complete el procedimiento del numeral 3.1.2 según sea el caso.

6.1.3 Distribución de claves públicas

La ACR-PEEQ publicará en su servidor WEB los certificados emitidos y revocados a través de las páginas destinadas para tal fin https://ca.advantage-securituy.com/asusuarios/

6.1.4 Tamaño de claves

El par de claves de las entidades que conforman el PKI de la ACR-PEEQ será:

ACR-PEEQ	RSA de 4096 bits
ACI	RSA de 2048 bits
ACG	RSA de 1024 bits
ACD	RSA de 1024 bits
Usuarios	RSA de 1024 bits

Las claves no podrán ser diferentes a los tamaños especificados en la tabla anterior según cada caso.

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

El software es AC de PSC Advantage y el hardware es un modulo criptográfico el cual cumple con el FIPS 140-2 nivel 3.

6.1.6 Uso de las claves.

La extensión KeyUsage deberá incluirse en los certificados emitidos por la ACR-PEEQ, esta extensión deberá marcarse como crítica.

La ACR-PEEQ contendrá la extensión keyUsage con los siguientes bits activados:

- CRLSign, keyCertSign, digitalSignature, nonRepudiation

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

- DigitalSignature, nonRepudiation, KeyEncipherment, dataEncipherment

6.2 Protección de la clave privada

La clave privada estará en todo momento cifrada, ésta se encuentra almacenada en el módulo criptográfico el cual cumple con el estándar FIPS 140-2 nivel 3.

La misma se encuentra en el nivel más seguro del área de la ACR-PEEQ bajo el resguardo del PSC Advantage Security, S. de R.L. de C.V.

6.2.1 Normas que deberán cumplir el módulo criptográfico

El modulo criptográfico, que contendrá la clave privada de la ACR-PEEQ, deberá cumplir por lo menos con el estándar FIPS 140-2 nivel 3.

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

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

6.2.3 Respaldo de clave privada

Existe únicamente un respaldo de la clave privada y ésta se encuentra en un token criptográfico que cumple con el FIPS 140-2 nivel 3.

6.2.4 Mantenimiento de copias

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

6.2.5 Entrada de la clave privada en módulo criptográfico

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

6.2.6 Método de activación de clave privada

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

6.2.7 Método de desactivación de clave privada

Debido a que el servidor de la ACR-PEEQ esta fuera de la red de datos, al término de la emisión de los o del certificado, se desactiva tanto el servidor como el módulo criptográfico.

6.2.8 Método de destrucción de la clave privada

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

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

6.3.1 Almacenamiento de claves públicas

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

6.3.2 Periodo de uso del par de claves

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

El actual certificado de la ACR-PEEQ es válido hasta 10 años

Para las ACI será de 8 años.

6.4 Datos de activación

6.4.1 Generación e instalación de datos de activación

La clave de paso utilizada para la protección de la clave privada deberá tener una longitud suficiente (la cual se realiza a través de la autenticación de un usuario

que resguarda un token de activación protegido por un teclado que cumple con el FIPS 140-2 nivel 3. Una vez autenticado el usuario existe una clave adicional de 8 posiciones con con combinación de letras, número y símbolos para acceder a las operaciones con la clave privada) y con combinaciones de letras (mayúsculas y minúsculas), números y otros caracteres que la hagan robusta a un ataque de fuerza bruta (no se aceptan password con significado ni palabras que se encuentren en el diccionario).

6.4.2 Protección de datos de activación

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

6.5 Controles de seguridad en las computadoras

6.5.1 Requerimientos técnicos de seguridad de la computadora

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

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

El personal responsable del servidor de la ACR-PEEQ, deberá mantener una relación constante con el equipo de respuesta a incidentes y el responsable de seguridad del área de datos del PSC Advantage Security, S. de R.L. de C.V.

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

6.6 Seguridad de red.

El servidor que administra a la ACR-PEEQ no está conectado a la red, por lo que el intercambio de información entre este equipo y sus usuarios será exclusivamente al momento de certificar y revocar, mediante dispositivos de almacenamiento removibles.

Este servidor tiene deshabilitados todos los servicios de red.

7. PERFILES DE CERTIFICADOS Y CRL

7.1 Certificados

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

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

- **Versión**: Número de versión del certificado X.509 V3
- **Número de Serie**: Número único asignado al certificado
- **Algoritmo de firma**: Algoritmo usado para generar la firma, sha1RSA de autenticación realizada usando la clave privada de la CA en cuestión.
- **Emisor**: Nombre de la CA firmante
- **Valido desde:** Fecha de emisión para la validez del certificado
- **Valido hasta:** Fecha de termino para la validez del certificado
- **Asunto**: Distinguished Name del certificado.
- **Clave Pública**: RSA (1024 bits).
- **Uso mejorado de claves:** autenticación del cliente

7.1.1 Versión del certificado

Los certificados emitidos por la ACR-PEEQ deberán ser certificados X.509 versión 3.

El campo de versión del certificado debe contener el valor hexadecimal 0x2 para indicar este número de versión.

7.1.2 Extensiones del certificado

Las extensiones X509v3 serán fijadas por defecto por la ACR-PEEQ según el tipo de certificado.

La extensión KeyUsage deberá ser incluida en los certificados emitidos por la ACR-PEEQ, esta extensión, debe ser marcada como crítica.

Para más información sobre la extensión KeyUsage consultar el numeral 6.1.6 de este documento.

La ACR-PEEQ tendrá al menos las siguientes extensiones establecidas:

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

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

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

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

- keyUsage (crítica: digitalSignature, nonRepudiation) y authorityKeyIdentifier

7.1.3 Identificadores de objetos de algoritmo

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

7.2 Perfil de la CRL

7.2.1 Número de versión

La ACR-PEEQ emite su CRL de acuerdo con el RFC 3280 *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.*

7.2.2 CRL y extensiones de entrada de CRL

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

8. VERSIÓN DE ESTA CPS

Versión 1.0 junio del 2008

09. ABREVIACIONES

ACD: Agentes Certificadores Derivados
ACG: Agente Certificador General
ACI: Autoridad Certificadora Intermedia
ACR-PEEQ: Autoridad Certificadora Raíz del Poder Ejecutivo del Estado de Querétaro
C: CountryName
CA: Certification Authority
CDIP: Certificado Digital de Identidad Personal

CDS: Certificado Digital de Servidor
CDACI: Certificado Digital de Autoridad Certificadora Intermedia.
CN: Common Name
CPS: Declaración de Prácticas de Certificación de ACR-PEEQ.
CRL: Lista de Certificados Revocados
CSR: Certificate Signing Requets
DC: Domain Component
DN: Distinguished Name
DSA: Digital Signature Algorithm.
Email: Dirección de correo electrónico
Entidad certificada: Cualquier usuario que forme parte de la Infraestructura de Llave Pública de la ACR-PEEQ (PKI)
FIPS 140 nivel 3: Es un estándar de seguridad de ordenadores para la acreditación de módulos criptográficos, también conocidos como Estándares Federales de Procesamiento de Información.
O: OrganizationName (Unidad Organizativa)
PC: Política de Certificados
PKCS#10: Public-Key Cryptography Standard 10 (Certification Request Standard Syntax
Standard)
PKI: Public Key Infraestructure o Infraestructura de Clave Pública
RSA: Algoritmo criptográfico de clave pública (sus creadores: Rivest, Shamir y Adleman
SSL: Secure Socket Layer
OID: Object Identifier
UID: Unique Identifier

10. 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 _____.
• *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.