DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

DE LA AUTORIDAD CERTIFICADORA DEL

GOBIERNO DE ESTADO DE GUERRERO

VERSIÓN 1.00
Fecha: 03-2010
OID: 30.32.30.30.39.39.30.30.30.31.32.30

1. INTRODUCCIÓN

La Ley 874 que Regula el Uso de la Firma Electrónica Certificada del Estado de Guerrero, tiene como objetivo fundamental regular su uso y sus medios de certificación, teniendo como finalidad simplificar, facilitar y agilizar los actos y negocios jurídicos, comunicaciones, procedimientos administrativos, trámites y prestación de servicios públicos. Para ello es necesario adecuar y modernizar las actividades y funciones de la administración pública centralizada, a las necesidades, deseos y aspiraciones de los guerrerenses, para así servir y coordinarse con una sociedad organizada y participativa en los avances tecnológicos de vanguardia.

1.1 Propósito

Describir la Declaración de Prácticas de Certificación para la Autoridad Certificadora del Gobierno de Estado de Guerrero (ACGEG), dentro de la Infraestructura de Clave Pública (PKI) del Proveedor de Servicios de Certificación (PSC) Advantage Security (AS) acreditado ante la Secretaría de Economía (SE).

1.2 Identificación

Este documento es denominado como **"Declaración de Prácticas de Certificación de la Autoridad Certificadora del Gobierno del Estado de Guerrero"**. Esta versión podrá consultarla en la dirección siguiente: http://autoridadcertificadora.guerrero.gob.mx/, sección *Políticas y Prácticas de Certificación*.

1.3 Comunidad y aplicabilidad

La aplicabilidad de la Firma Electrónica Certificada (FEC) es la simplificación, facilitación y agilización de los actos y negocios jurídicos, comunicaciones, procedimientos administrativos, trámites y prestación de servicios públicos de la Administración Pública Centralizada y Paraestatal del Estado de Guerrero y su aplicabilidad es obligatoria para los servidores públicos que la integran.

1.3.1 Autoridad Certificadora

La ACGEG, de acuerdo al Reglamento sobre el Uso de Firma Electrónica del Poder Ejecutivo del Estado, es la Subsecretaría de Asuntos Jurídicos y Recursos Humanos (SAJDH) de la Secretaría General de Gobierno, y ejercerá las atribuciones correspondientes de acuerdo a lo previsto por la Ley y el Reglamento. La infraestructura de la Autoridad Certificadora es la arrendada al PSC Advantage Security.

1.3.2 Autoridad Registradora

La Subsecretaría de Administración (SA) de la Secretaría de Finanzas y Administración, funge como Autoridad Registradora (ARGEG) en el ámbito de su competencia y auxiliará a la ACGEG en el cumplimiento de sus labores de registro y certificación de usuarios en los términos de los lineamientos establecidos, así como en la operación y mantenimiento del Portal de Internet de la ACGEG y de las aplicaciones informáticas de firmado, visualización y verificación de documentos electrónicos.

1.3.3 Titular

La persona a la cual se le expide a su favor un certificado de firma electrónica.

1.4 Contacto

Podrá hacer a la ARGEG sus comentarios, dudas u observaciones referentes a esta Declaración de Practicas de Certificación (DPC), de alguna de las suguientes maneras.

- Centro de Atención Telefónica, disponible de lunes a viernes de 9:00 a 15:00 horas, llamando al (747) 471-9900 extensión 9609.
- Vía correo electrónico a la cuenta: autoridadcertificadora@guerrero.gob.mx
- En las oficinas de la ARGEG ubicada en las instalaciones de la Coordinación General de Tecnología y Desarrollo (CGTD) en el Palacio de Gobierno, Edificio Costa Grande, Sótano, Blvd. Lic. René Juárez Cisneros No. 62, Col. Cd. de los Servicios, en la ciudad de Chilpancingo, Guerrero.

2. OBLIGACIONES Y RESPONSABILIDADES

2.1 Obligaciones

2.1.1 Obligaciones de la ACGEG

Ofrecer un servicio constante mediante la infraestructura requerida de un PKI, manteniendo los requerimientos de seguridad necesarios para proteger las claves privadas de los titulares.

Respaldar y mantener los certificados emitidos y revocados en un sitio de alta disponibilidad 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 ACGEG en http://autoridadcertificadora.guerrero.gob.mx/, sección *Consulta de Certificados Digitales.*

Emitir o revocar los certificados de acuerdo con lo establecido en este documento, así como de actualizar y publicar la Lista de Certificados Revocados (CRL).

2.1.2 Obligaciones de la ARGEG

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

Realizará la identificación y autentificación para determinar su emisión o revocación de certificados, de conformidad con el numeral 3.1.2 de este documento, según sea el caso.

Realizará la carga de las solicitudes de certificados y revocaciones válidas en el sistema.

Proteger los datos personales de los solicitantes, que no podrán ser cedidos a terceros bajo ningún concepto (Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental).

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

2.1.3 Obligaciones de los titulares de las entidades

Mantener en todo momento protegida su clave privada con un nivel de seguridad adecuado.

Notificar a la ARGEG, su solicitud de revocación de su certificado o cualquier sospecha de compromiso de sus claves, en sucaso.

Los titulares de las entidades certificadas por la ACGEG, deben conocer y aceptar esta Declaración de Prácticas de Certificación, y sus responsabilidades de conformidad con el numeral 2.2 de este documento.

Informar a las partes que confíen en certificados firmados por la ACGEG, que tienen la obligación de verificar su validez o el estado que guardan éstos cada vez que vayan a ser utilizados, verificar que no hallan expirado y que no aparezcan en la CRL de la ACGEG en https://ca.advantage-security.com/acGuerrero/crl/guerrero.crl.

2.1.4 Obligaciones de repositorio

La ACGEG publicará su certificado, su CRL y los certificados emitidos por ésta, en el portal de Internet destinado al servicio de la Autoridad Certificadora del Gobierno del Estado de Guerrero en http://autoridadcertificadora.guerrero.gob.mx. Ésta publicación se realizará como máximo 2 horas después de la emisión y firma de los certificados, en caso de revocación de algún certificado la CRL se publicará en el menor tiempo posible.

Permitir consultar esta información en las portal de Internet destinado al servicio de la ACGEG.

2.2 Responsabilidades

2.2.1 Responsabilidades de la ACGEG

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

Los problemas derivados del compromiso de la clave privada de la ACGEG y la notificación de la revocación de la misma.

Revocar cualquier certificado en cuanto le sea notificado o se detecte algún incumplimiento de los requisitos establecidos en el marco jurídico aplicable, compromiso o mal uso del mismo.

Proteger la clave privada de la ACGEG, mediante el uso de un modulo criptográfico que por lo menos cumpla con el estándar FIPS 140-2 nivel 3 (infraestructura PKI de Advantage Security).

La SA, como administrador de la ACGEG, garantiza el cumplimiento de las obligaciones descritas en este documento.

2.2.2 Responsabilidades de la ARGEG

Verificar que los solicitantes cuenten con lo requisitos establecidos en la normatividad aplicable.

La identificación y autenticación de los solicitantes, para poder emitir su certificado o revocarlo según sea el caso.

2.2.3 Responsabilidades de los titulares

Proporcionar datos exactos, completos y veraces cuando se emplee un certificado en relación con la firma electrónica.

Actuar con la debida responsabilidad y diligencia para evitar la utilización no autorizada de los datos de creación de la firma electrónica, así como evitar el uso no autorizada de la misma.

Responder por las obligaciones del uso no autorizado de su firma electrónica certificada, cuando no hubiese obrado con la debida responsabilidad para impedir su utilización.

Actualizar los datos contenidos en el certificado de firma electrónica.

Dar aviso oportunamente a la ARGEG cuando exista riesgo de que su firma electrónica certificada sea utilizada por terceros no autorizados, para la suspensión o extinción del certificado.

2.4 Política de confidencialidad de la información

2.4.1 Información confidencial

La información clasificada como confidencial será de acuerdo a la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

Cualquier dato de carácter personal suministrado por los titulaes a la ARGEG.

Material criptográfico privado asociado con la ACGEG.

La información derivada de una revocación de algún certificado.

Información sobre las personas que administran la ARGEG excepto su nombre, teléfono, correo electrónico, cargo dentro de ARGEG e información que aparece en el propio certificado que posean.

Registros de los eventos registrados por los sistemas de monitoreo de la red y cualquier sistema de seguridad.

2.4.2 Información no confidencial

La ACGEG y la ARGEG manejan como información no confidencial la siguiente: información incluida en los certificados, CRLs, DPC, marco jurídico.

2.4.3 Causas de revocación

Se determinarán como causas de revocación las descritas el Capítulo IV de la Ley 874 que Regula el Uso de la Firma Electrónica Certificada del Estado de Guerrero.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1 Registro

3.1.1 Tipos de nombres

La ARGEG sólo acepta solicitudes de firma donde su DN refleje el ámbito bajo el cual se va a certificar.
Todos los nombres asociados con los certificados tienen que ser únicos.
Cada titular debe tener un DN (*Distinguished Name*) único y claro contenido en el campo “Subject” del certificado firmado por la ARGEG.
El DN de los Certificados Digitales de Identidad Personal deben proporcionar los siguientes atributos:

- C=MX
- O=GOBIERNO DEL ESTADO DE GUERRERO
- OU=<Dependencia>
- CN= <Nombre del titular>
- Email=<correo electrónico del titular>

3.1.2 Autenticación de los solicitantes de certificados a la ARGEG

El funcionario solicitante de cualquiera de las entidades descritas en el numeral 1.3 deberá presentar ante la ARGEG.
CURP
RFC
Documento de identidad (cartilla, pasaporte vigente, cédula profesional o credencial del IFE)
Documento probatorio de identidad (acta de nacimiento, documento migratorio, carta de naturalización, certificado de nacionalidad mexicana)
Comprobante de domicilio (agua, luz o teléfono con antigüedad no mayor a 2 meses y con el mismo domicilio del documento de identidad)
Nombramiento

3.2 Procedimientos de generación de claves

Los solicitantes de los certificados, serán los encargados de la generación de los archivos .req y .key utilizando la aplicación Generador de Requerimiento de Certificado Digital de FEC.

3.3 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, tendrá que volver a generar el par de claves.

3.4 Solicitud de revocación

La ACGEG revocará cualquier clave privada que incurra alguno de los supuestos del numeral 15.1 de la Política de Certificados de la ACGEG, o que ésta detecte que ha sido comprometida clave en cuestión.
De otra manera la solicitud de revocación será llevara a cabo de conformidad con el numeral 15.2 de la Política de Certificados de la ACR-SE, 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

4.1 Solicitud de certificados

La ACGEG se reserva el derecho de rechazar las solicitudes que incumplan algún requisito solicitado en el marco jurídico aplicable. Si es rechazada, la ARGEG informará mediante oficio las razones por las que se rechaza dicha solicitud.

La ACGEG sólo aceptar solicitudes para las entidades descritas en el numeral 3.1.2. de este documento.

4.1.1 Certificados de Agentes Certificadores de la ACGEG

El solicitante generará su par de claves publica y privada, previo a la solicitud de certificación de su clave pública, presentará su clave pública ante la AR de AS. El usuario tendrá la obligación de conservar su clave privada en un lugar seguro.

Es responsabilidad de la AR de AS verificar si cumple con el procedimiento descrito en el numeral 3.1.2 de este documento, según el caso que le aplique. La AR pedirá al solicitante que firme, en su presencia, original y copia del documento de confidencialidad. posteriormente, verificará la firma autógrafa del documento de confidencialidad con la que aparece en la identificación oficial presentada.

La AR de SA enviará a la ARGEG la solicitud y la clave pública en el medio electrónico para la certificación de la misma.

La ARGEG hará llegar el certificado o clave pública para que le sea entregado al titular del mismo.

Los datos y documentos proporcionados por el solicitante quedrá en custodia de la AR de AS.

4.2 Firma y entrega de certificados.

El certificado deberá cumplir con lo establecido en el marco jurídico aplicable, utilizando las extensiones necesarias para contener la información como la URL de la ACGEG, la URL del OCSP, la CRL.

El certificado se le entregará al titular del mismo en un medio de almacenamiento removible y se le enviará una copia a su correo electrónico.

Asimismo se tendrá un a copia de los certificados emitidos en una dirección del Portal de Interner de la ACGEG, para que pueda obtener las copias necesarias del mismo.

4.3 Revocación de certificados

Se determinarán como causas de revocación las descritas el numeral 15 de la Política de Certificados (CP) de la ACGEG, según el caso.

4.4 Frecuencia de firmado de la CRL

ACGEG firmará una nueva CRL cada que se revoque un certificado, se llevara a cabo la actualización, incluyendo las listas anteriores.

La entidad que confié en los certificados emitidos por la ACGEG, tendrá la obligación de verificar su estado en la CRL.

Para verificar los dos puntos anteriores se tendrá en línea la información en la siguiente dirección del portal de Internet de la ACGEG en https://ca.advantage-security.com/acGuerrero/crl/guerrero.crl.

4.5 Procedimientos de Auditorias de Seguridad

El PSC Advnatage Security está implementando procedimientos de la información necesaria para obtener la certificación WebTrust y BS7799.

4.6 Archivo de registros

4.6.1 Tipos de eventos registrados

Se llevará un registro de los eventos ocurridos en el servicio de la ACGEG, 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 ACGEG y respaldos cada vez que se genere o revoque un certificado. Los respaldos se resguardarán en lugar seguro y estarán protegidas criptográficamente, teniendo acceso a éstos exclusivamente personal autorizado.

Mantendrá el equipo redundante para ofrecer el servicio continuo de la AGEG y de consulta del portal de Internet.

Se conservarán registros de los accesos al portal de Internet de la ACGEG.

La ACGEG 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 ACGEG enviada en papel, medio magnético o digital, se resguardará en un lugar seguro.

4.6.2 Periodo de resguardo de la información
La información concerniente a los registros de la ACGEG, proporcionada por los solicitantes a PSC, se resguardará durante 10 años en un lugar seguro posterior a su revocación, transcurrido el tiempo anterior, se valorará si requiere ser conservado más tiempo.

4.6.3 Protección de la información
La información que pertenece al centro de datos del Gobierno del Estado, es respaldada y protegida en lugares seguros bajo custodia apropiada, solo tiene acceso a ésta el personal autorizado, se cuenta con controles de acceso físicos y lógicos.
Se mantiene un respaldo del *software* utilizado en el servicio de la ACR-SE, para poder acceder a la información respaldada en otro sitio autorizado para tal fin.

4.6.4 Procedimientos de respaldos
Se establecerá un sistema periódico de respaldos del la información de la ACGEG, en base a la Política de Respaldos.

4.7 Renovación de claves pública y privada de las entidades
Cuando se haya superado cuatro quintos del tiempo de vida de la ACGEG, se generará una nueva identidad raíz. A partir de ese momento, se firmarán certificados con la nueva identidad.
Los certificados emitidos por la ACGEG están disponibles en la página Web en http://autoridadcertificadora.guerrrero.gob.mx/, sección *Consulta de Certificados Digitales*.

4.8 Compromiso y recuperación de desastres
En caso de que la clave privada de la ACGEG 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-SE y se emitirá una CRL mostrando el estatus de revocación del certificado de la ACGEG.
Una vez generadas las nuevas claves de la ACGEG, se emitirá el certificados correspondiente a las ARGEG, y ésta a su vez deberá llevar a cabo la revocación y emisión de los nuevos certificados de sus usuarios.
En caso de compromiso de la clave privada de la ARGEG, ésta tendrá el deber de notificarlo a la AR de AS y a sus usuarios correspondientes.

4.8.1 Recuperación de hardware, software o datos
En caso de corrupción de *hardware* que da el servicio de la ACGEG, se cuenta con equipo redundante en otro sitio para continuar ofreciendo el servicio.

En caso de corrupción de *software* que da el servicio de la ACGEG, se 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 ACGEG estará en todo momento cifrada almacenada de modo permanente en el modulo criptográfico FIPS 140-2 nivel 3.

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 ACGEG.

5. CONTROLES DE SEGURIDAD FÍSICOS, PERSONALES Y DE PROCEDIMIENTOS

La Subsecretaría de Administración quien funge como la ARGEG ha implementado la Política de Seguridad la que considera lo establecido en esta DPC.

5.1 Controles físicos

5.1.1 Ubicación física de la ACGEG

El servidor que administra la ACGEG esta ubicado en el centro de datos del PSC Advantage Security.

5.1.2 Acceso físico a la ACR-SE

El acceso a el área de la ACGEG, está restringido únicamente a personal autorizado el cual es responsable de los servidores de las Autoridades Certificadoras de los clientes del PSC Advantage Security. Cuenta con 5 niveles de seguridad. El acceso a cada nivel esta protegido por diferentes factores de seguridad como tarjetas proximidad, lector volumétrico, lector de huella digital y claves de acceso.
El área más segura no permite el acceso a una sola persona, por lo menos deben ser dos y deben estar autorizadas para acceder a este nivel, se requieren dos factores de seguridad para su acceso.

5.1.3 Acondicionado de aire y energía eléctrica

La ACGEG 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.
Se cuenta con UPS con el cual mantiene la carga eléctrica constante sin interrupciones ni picos.

5.1.4 Protección contra de inundaciones

La ACGEG se localiza en un piso elevado del inmueble del PSC Advantage Security.

5.1.5 Protección y prevención contra incendios

Se cuenta con sistemas de detección de humo y extinción de incendios.

5.1.6 Almacenamiento de medios

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

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 Coordinación de Infraestructura del CETIC, respectivamente.

5.2 Controles de seguridad personales

5.2.1 Antecedentes y requisitos para el personal responsable de la ACGEG

El personal responsable de la ACGEG, está contratado por el PSC Advantage Security y cuenta con el nivel y conocimientos necesarios para dicha responsabilidad.

5.2.2 Procedimientos de verificación del personal

El área de Recursos Humanos de Advantage Security verifica previamente los antecedentes del personal contratado, 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 de Advantage Security, 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 ACGEG, y serán determinadas por el PSC Advantage Security.

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 ACGEG
Políticas de Seguridad, Políticas de Certificados, DPC, 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 ACGEG.

Personal de operación de la ACGEG:
- Administración, mantenimiento y manejo del servidor que opera la ACGEG.
- Respaldos.

Personal que administra las funciones de la ACGEG:
- 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 ARGEG:
- Identificar y autenticar a los solicitantes y su documentación
- Remitir las solicitudes de certificación y/o revocación de certificados a la ACGEG.

6. CONTROLES DE SEGURIDAD TÉCNICOS

6.1 Generación e Instalación del par de claves

El par de claves de la ACGEG serán generadas utilizando el software de Advantage Security, éste se utiliza para la administración de la Autoridad Certificadora de la ACGEG.
La clave privada estará en todo momento cifrada esta 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 ACGEG serán generadas por el personal responsable del servidor que administra la ACGEG.
El par de claves de las entidades no son generadas ni entregadas por la ACGEG.
Las entidades que formarán parte de los usuarios de la ARGEG, deberán generar su par de claves en el lugar más seguro de sus instalaciones.

6.1.2 Entrega de la clave pública a las entidades.

Las entidades finales presentarán su clave pública (mediante un requerimiento PKCS#10 ó mediante el certificado autofimado por la ARGEG) a la ACGEG 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 ACGEG publicará en su portal de Internet los certificados emitidos y revocados a través de las páginas destinadas para tal fin.

6.1.4 Tamaño de claves

El par de claves de la ACGEG será RSA de 2048 bits, para la ARGEG será de 2048 bits y para los de Identidad Personal será de 1024 bits.
Las claves no podrán ser diferentes a los tamaños especificados en el párrafo anterior según cada caso.

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

El software es el Generador de requerimiento de certificad digital de FEC 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 ACGEG, esta extensión, deberá marcarse como crítica.
La ACGEG 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 esta se encuentra almacenada en el modulo criptográfico el cual cumple con el FIPS 140-2 nivel 3.

6.2.1 Normas que deberán cumplir el módulo criptográfico

El modulo criptográfico, que contendrá la clave privada de la ACGEG, deberá cumplir por lo menos con el FIPS 140 nivel 3.

6.2.2 Medida de seguridad para el uso de las claves de la ACGEG

La ACGEG 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 esta se encuentra en un segundo modulo criptográfico que igualmente cumple con el FIPS 140-2 nivel3.

6.2.4 Mantenimiento de copias
Al término del ciclo de vida de las claves de la ACGEG, éstas se conservarán en un medio de almacenamiento electrónico criptográficamente al cual solo tendrán acceso los responsables de la ACGEG.

6.2.5 Entrada de la clave privada en módulo criptográfico
La clave privada se genera únicamente en el modulo criptográfico de la ACGEG

6.2.6 Método de activación de clave privada
Para poder activar la clave privada de la ACGEG, 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 ACGEG esta fura de la red de datos, al término de la emisión de los o del certificado, se desactiva tanto el servidor como el modulo 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 modulo eliminando el formato de las tarjetas de activación.

6.3 Otros aspectos de la Administración de las claves de la ACGEG
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 ACGEG es válido hasta 10 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 (al menos 14 caracteres) 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 ACGEG pertenecen y están bajo custodia del personal autorizado para tal fin, cada persona autorizada cuenta con un password, y para activar la ACR-SE, 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 ACGEG son confiables protegidos contra los accesos no autorizados.
El acceso físico al servidor que administra la ACGEG,es controlado.
El personal responsable del servidor de la ACGEG, deberá mantendrá una relación constante con el equipo de respuesta a incidentes y el responsable de seguridad del área de datos de la ARGEG.
El software instalado en el servidor de la ACGEG será actualizado continuamente con las últimas actualizaciones críticas de seguridad.

6.6 Seguridad de red
El servidor que administra a la ACGEG 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 ACGEG firmará 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 ACGEG contendrán al menos los siguientes campos:

Versión: Número de versión del certificado X.509

SerialNumber: Número único asignado al certificado

Signature: Algoritmo usado para generar la firma, normalmente RSA/SHA-1Firma de autenticación realizada usando la clave privada de la AC en cuestión.

Issuer: Nombre de la AC firmante

Validity: Periodo de validez del certificado

Subject: Distinguished Name del certificado.

Subject Public Key Information: algorithmID, clave.

ExtKeyUsage Extension

CertificatePolicies

7.1.1 Versión del certificado

Los certificados emitidos por la ACGEG 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 ACGEG según el tipo de certificado.
La extensión KeyUsage deberá ser incluida en los certificados emitidos por laACR-SE, esta extensión, debe ser marcada como crítica.
Para más información sobre la extensión KeyUsage consultar el numeral 6.1.6 de este documento.

La ACGEG 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 (crítica), digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment 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 ACGEG emite su CRL de acuerdo con el RFC 3280 *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*., esta versión “RFC 3280” sustituye a la versión “RFC 2459”.

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, l*os algoritmos utilizados para la Firma Electrónica Certificada deben ser compatibles con los estándares de la industria.

8. ESPECIFICACIONES ADMINISTRATIVAS

8.1 Procedimientos de cambio de especificación

Las modificaciones efectuadas a esta DPC se publicarán en el apartado versiones anteriores en http://autoridadcertificadora.guerrero.gob.mx/descargas.

Si lo cambios son tipográficos se efectuaran sin previo aviso, de otra manera se publicarán durante 15 días para recibir comentarios, antes de ser autorizados. Al término de esos 15 días, serán autorizados y publicados los cambios. Los comentarios serán recibidos al correo electrónico autoridadcertificadora@guerrero.gob.mx.

8.2 Procedimientos de publicación y notificación

• La ACGEG publicará su certificado, su CRL y los certificados firmados por ésta, su DPC en el portal de Internet al servicio de la Autoridad Certificadora ACGEG en http://autoridadcertificadora.guerrero.gob.mx. Ésta publicación se realizará como máximo 2 horas después de la emisión y firma de los certificados, en caso de revocación de algún certificado la CRL se publicará en el menor tiempo posible.

En caso de modificación de esta DPC, será informado dicho cambio a sus usuarios.

9. VERSIÓN DE ESTA DPC

Versión 1.0 marzo del 2010

10. ABREVIACIONES

ACGEG: Autoridad Certificadora del Gobierno del Estado de Guerrero
ARGEG: Autoridad Registradora del Gobierno del Estado de Guerrero
AS: Advantage Security
C: CountryName
CA: Certification Authority
CDIP: Certificado Digital de Identidad Personal
CETIC: Comité Estatal de Tecnologías de Información y Comunicaciones
CRL: Certificate Revocation List
CSR: Certificate Signing Requests
DC: Domain Component
DN: Distinguished Name
DPC: Declaración de Prácticas de Certificación
DSA: Digital Signature Algorithm.
Email: Dirección de correo electrónico
O: OrganizationName
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)
SA: Subsecretaría de Administración de la Secretaría de Finanzas y Administración
SAJDH: Subsecretaría de Asuntos Jurídicos y Derechos Humanos de la Secretaría de Gobierno
SE: Secretaría de Economía
SSL: Secure Socket Layer
OID: Object Identifier
UID: Unique Identifier

11. 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 Federal de Transparencia y Acceso a la Información Pública Gubernamental, publicada en el Diario Oficial de la Federación el 11 de junio de 2002.
https://www.firmadigital.gob.mx

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.

REGLAMENTO del Código de Comercio en Materia de Prestadores de Servicios de Certificación, Publicado el 19 de julio de 2004.

REGLAS generales a las que deberán sujetarse los Prestadores de Servicios de Certificación. Publicadas el 10 de agosto de 2004, en el Diario Oficial de la Federación.