Declaración de Prácticas de Certificación aplicables a la Autoridad Certificadora del Gobierno del Estado de Hidalgo

Versión 1.0
Clave: HIDDPCAC
Julio, 2019

Sección de Firmas de Aprobación

Elaboró

SeguriData, Consultor
Ing. Bernardo Calatayud Lira

Revisó

Director de Firma Electrónica Avanzada y
Calidad en Procesos
Ing. Héctor Sánchez Bautista

Autorizó

Director General de Innovación Gubernamental y Mejora Regulatoria
L.C.C. José Martín Salazar Ávila

Versión:	1.0		
Copia Asignada a:		Firma:	
Dueño del documento:	Dirección General de Innovación Gubernamental y Mejora Regulatoria	Firma:	

Las copias de este documento deberán ser conservadas por:

Nombre	Puesto
L.C.C. José Martín Salazar Ávila	Director General de Innovación Gubernamental y Mejora Regulatoria
Ing. Héctor Sánchez Bautista	Director de Firma Electrónica Avanzada y Calidad en Procesos

Sección de Control de Cambios			
Versión	**Pág (s) Afectadas**	**Descripción del Cambio**	**Fecha de Emisión**
1.0	-	Generación inicial del Documento.	18/07/2019

Contenido

1.0 Introducción

1.1 Resumen

La ley de Uso de Medios Electrónicos y Firma Electrónica Avanzada para el Estado de Hidalgo contiene una serie de iniciativas que tienen por objeto simplificar y agilizar las comunicaciones electrónicas, negocios jurídicos y procedimientos administrativos entre los participantes de estos actos.

Por tal motivo la Dirección General de Innovación Gubernamental y Mejora Regulatoria, ha decido implantar una Infraestructura de Llave Pública, la cual dotará a todos los servidores públicos del Estado de Hidalgo de certificados electrónicos que, para los efectos de su cargo, necesiten plasmar su voluntad mediante el uso de la firma electrónica avanzada.

El presente documento incluye las Prácticas de Certificación las cuales representan las prácticas que el Prestador de Servicios de Certificación de la Dirección General de Innovación Gubernamental y Mejora Regulatoria, lleva a cabo para la operación y administración de la infraestructura, así como los procedimientos que éste implementa para cumplir con los requerimientos plasmados en el documento de Políticas de Certificación.

La estructura de esta declaración de prácticas están basadas en lo dispuesto por la fuerza de tarea de la IETF (*Internet Engineering Task Force*) en el documento de referencia RFC 3647, denominado como "*Internet X.509 Public Key Infraestructure Certificate Policy and Certification Practices Framework*". Asimismo, para el desarrollo de su contenido, se ha tenido en cuenta los requisitos establecidos por la ley de Uso de medios Electrónicos y Firma Electrónica Avanzada para el Estado de Hidalgo.

Además, la DPC incluye todas las actividades que se desarrollan durante la gestión de los certificados electrónicos en su ciclo de vida, por lo que sirve de guía de la relación que existe entre el PSC y sus suscriptores.

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

1.2 Identificación del documento

Nombre del documento	Declaración de Prácticas de Certificación aplicables a la Autoridad Certificadora del Gobierno del Estado de Hidalgo
Versión del documento	1.0
Estado del documento	Aprobado
Fecha de emisión	18/07/2019
Fecha de caducidad	-
OID (Object Identifier)	2.16.484.201.13.1.2

Sitio electrónico de la DPC	http://firmaelectrónica.hidalgo.gob.mx

1.3 Personas y Entidades Participantes

Las personas y entidades participantes son:

- La Dirección General de Innovación Gubernamental y Mejora Regulatoria, como Entidad encargada de la emisión y administración de los certificados de firma electrónica a través de la AC del estado de Hidalgo.
- La Dirección General de Innovación Gubernamental y Mejora Regulatoria, como Entidad encargada de la aprobación y administración de las Políticas de Certificados.
- Los servidores públicos del Estado de Hidalgo como solicitantes del Certificado de firma electrónica.
- Los servidores públicos del Estado de Hidalgo como titulares del Certificado de firma electrónica.
- Las Autoridades de Registro encargadas de validar la identidad de los solicitantes de Certificados de firma electrónica.
- Las entidades terceras aceptantes de los Certificados de firma electrónica emitidos por el PSC a través de la AC del estado de Hidalgo.

1.4 Autoridades de Certificación

La Dirección General de Innovación Gubernamental y Mejora Regulatoria, actúa como un Prestador de Servicios de Certificación, realizando el vínculo del par de claves con servidores públicos del Estado de Hidalgo en concreto por medio de la emisión de Certificados de firma electrónica que están bajo conformidad en los términos de la presente DPC.

En el momento de publicación de la presente DPC, la Autoridad Certificadora que compone la PKI del estado de Hidalgo es la siguiente:

Nombre Distintivo	CN = AUTORIDAD CERTIFICADORA DEL ESTADO DE HIDALGO OU = DIRECCIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL Y MEJORA REGULATORIA O = GOBIERNO DEL ESTADO DE HIDALGO C = MX, S = PACHUCA L = HIDALGO, PostalCode = 42000
Número de serie	00000000000000000001
Periodo de validez	DESDE EL 18 DE JULIO DE 2019 HASTA EL 18 DE JULIO DE 2029
Estado	OPERATIVA
Huella digital (SHA-2)	

1.5 Autoridades de Registro

La Autoridad de Registro estará constituida por las oficinas que haya dispuesto la Dirección General de Innovación Gubernamental y Mejora Regulatoria, para realizar la expedición de los Certificados de firma electrónica, estas autoridades tienen por misión realizar las funciones de asistencia a la AC del estado de Hidalgo en los procedimientos y trámites relacionados con los servidores públicos para su

identificación, registro y autenticación, garantizando con esto, la correcta asignación de claves a los servidores públicos solicitantes de un Certificado de firma electrónica.
La oficina de registro se encuentra ubicada en Palacio de Gobierno, Primer Piso, Plaza Juárez S/N, Colonia Centro, Pachuca, Hidalgo.

1.6 Validación de estatus

Como parte de la infraestructura que la AC de estado de Hidalgo ha desplegado, se encuentra el servicio de validación de estatus en línea, el cual mediante el protocolo de OCSP (Online Certificate Status Protocol) se encarga de proporcionar, a solicitud de un tercero aceptante, el estado actual de un Certificado de firma electrónica emitido por la AC del estado de Hidalgo.
Este servicio está respaldado por un esquema de alta disponibilidad, por lo que garantiza la consulta sobre la vigencia y validez de los Certificados de firma electrónica de una manera segura y rápida.
Los convenios que regulen las relaciones entre la AC del estado de Hidalgo con otras AC, quedan fuera del alcance del presente documento.

1.7 Terceros aceptantes

Los terceros aceptantes son los sujetos o entidades diferentes del titular de Certificado de firma electrónica que deciden aceptar y confiar en los certificados emitidos por la AC del estado de Hidalgo, así como en las transacciones electrónicas que se lleven a cabo utilizando dichos certificados.

1.8 Uso de los Certificados

1.8.1 Uso apropiado de los Certificados de firma electrónica

Los Certificados de firma electrónica emitidos por la AC del estado de Hidalgo tienen como finalidad lo siguiente:

- **Autenticación**: garantizar la identidad del titular de certificado al momento de realizar cualquier transacción electrónica con un tercero, el certificado dará la certeza de que la comunicación electrónica se realiza con la persona que dice ser. El titular de un Certificado de firma electrónica podrá acreditar su identidad frente a cualquiera ya que se encuentra en posesión del certificado y de la clave privada asociada al mismo.
- **Firma electrónica**: permite al titular firmar trámites o documentos de manera electrónica. Basado en la Ley de Uso de Medios Electrónicos y Firma Electrónica Avanzada para el Estado de Hidalgo, este certificado permitirá la sustitución de la firma autógrafa por la electrónica con el fin de facilitar y agilizar los actos y negocios jurídicos, comunicaciones y procedimientos administrativos entre las dependencias, entidades y organismos que conforman el sector público. Todo titular de un Certificado de firma electrónica emitido por la AC del estado de Hidalgo obtendrá el valor de plena prueba legal para los documentos electrónicos donde éste aplique su firma electrónica avanzada, respecto al hecho de que asegura la integridad, no repudio y autenticidad de los mismos.

1.8.2 Limitaciones y restricciones en el uso de los certificados

Los Certificados de firma electrónica emitidos por la AC del estado de Hidalgo, están sujetos a lo que la Ley de Uso de Medios Electrónicos y Firma Electrónica Avanzada para el Estado de Hidalgo indica.

Los Certificados de firma electrónica emitidos por la AC del estado de Hidalgo, solamente podrán utilizarse para autenticar (acreditación de identidad) al titular, para firma electrónica (integridad, no repudio y compromiso con lo firmado). Los certificados no podrán ser empleados para actuar como Autoridad de Registro y/o Autoridad Certificadora, para firmar otros certificados digitales ni para firmar Listas de Certificados Revocados.

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

Los sistemas ofrecidos por el PSC, aseguran que el par de claves permanecen desde el momento de su creación bajo el control del solicitante o funcionario, por lo que el titular de Certificado de firma electrónica deberá hacer énfasis en el resguardo y custodia de las mismas.

1.9 Definiciones y Acrónimos

Término	Definición
Certificado Electrónico	Documento firmado electrónicamente por la Autoridad Certificadora que vincula datos de verificación de firma electrónica al firmante y confirma su identidad.
Clave Privada	Las claves criptográficas, datos o códigos únicos que genera el firmante de manera secreta para crear y vincular su firma electrónica.
Clave Pública	Las claves criptográficas, datos o códigos únicos que utiliza el destinatario para verificar la autenticidad de la firma electrónica del firmante.
DPC	Declaración de Prácticas de Certificación
Dispositivo de creación de firma electrónica	El programa o sistema informático que sirve para aplicar los datos de creación de firma electrónica.
Dispositivo de verificación de firma electrónica	El programa o sistema informático que sirve para aplicar los datos de verificación de firma electrónica.
Firma electrónica avanzada	Los datos que en forma electrónica son vinculados o asociados a un mensaje de datos y que corresponden inequívocamente al firmante con la finalidad de asegurar la integridad y autenticidad del mismo y que ha sido certificada por el prestador de servicios de certificación.
PSC	Prestador de Servicios de Certificación: la persona o entidad pública que preste servicios relacionados con la firma electrónica avanzada y que expide certificados electrónicos.
PC	Política de Certificados.
DIGIGMER	Dirección General de Innovación Gubernamental y Mejora Regulatoria

Suscriptor	Se entiende por suscriptor, todo aquel funcionario titular de un Certificado de firma electrónica, que voluntariamente confía y hace uso de su certificado emitido por la AC del estado de Hidalgo. En el momento que un funcionario titular de Certificado de firma electrónica decida voluntariamente confiar y hacer uso de su certificado, le será de aplicación la presente DPC.
Usuario	Todos los funcionarios que desempeñan un cargo en la Administración Pública, incluyendo empleados de confianza, empleados de base, empleados temporales, empleados contratados por terceros, haciendo uso de los recursos informáticos propiedad o bajo responsabilidad del Estado de Hidalgo.

1.10 Algoritmos y Parámetros Utilizados

Los Algoritmos de Firma son RSA con digestión Sha-2, los tamaños de claves son de al menos 1024 bits para usuarios y de 2048 bits para Autoridad Certificadora**.**

2.0 Disposiciones Generales

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

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

2.1.2 Obligaciones de la Autoridad Certificadora

La Autoridad Certificadora del estado de Hidalgo actuará relacionando a un determinado suscriptor con su clave pública mediante la expedición de un Certificado.
El detalle de todas las obligaciones a las que estará sujeta la Autoridad Certificadora del estado de Hidalgo se encuentra plasmada en la correspondiente Declaración de Prácticas de Certificación.
La Autoridad Certificadora puede confiar en los PSC Prestadores de Servicios de Certificación para los procesos de identificación y autenticación del solicitante del Certificado. En los casos en que la Autoridad Certificadora haya confiado en un PSC para realizar la identificación y la autenticación del suscriptor. La Autoridad Certificadora correrá con toda la responsabilidad de la identificación y la autenticación de sus suscriptores.
No obstante, lo anterior, se exige que la Autoridad Certificadora del estado de Hidalgo lleve a cabo revisiones regulares, de obligado cumplimiento, de los PSC para asegurar que cumplen con sus obligaciones según el acuerdo aplicable, (incluyendo las tareas de identificación y autenticación). La Dirección General de Innovación Gubernamental y Mejora Regulatoria, debe asegurar que todos los aspectos de los servicios que ofrecen y gestionan dentro de la Infraestructura de Clave Pública de la Autoridad Certificadora del estado de Hidalgo son acordes en todo momento con esta Declaración de Practicas de Certificación.
Sin perjuicio de todo lo anterior, se considera relevante mencionar que la Autoridad Certificadora del estado de Hidalgo está obligada a prestar los servicios relacionados con la firma electrónica avanzada, dentro de los cuales se encuentran:

- Proporcionar la infraestructura operacional, servicios de certificación, servicios de revocación y servicios de validación de estatus de certificados OCSP.
- Usar productos confiables y sistemas protegidos contra manipulaciones o modificaciones no autorizadas, que pueden asegurar su seguridad técnica y criptográfica.
- Llevar a cabo los esfuerzos razonables para emplear al personal con la calificación, conocimientos y experiencia necesarios para llevar a cabo los servicios de certificación y aplicar las medidas de seguridad fijadas en la Política de Certificados.
- Publicar su certificado de Autoridad Certificadora en http://firmaelectronica.hidalgo.gob.mx.
- Conservar por medios electrónicos toda la información y documentos relacionados con los Certificados emitidos durante un lapso de al menos 5 años desde su emisión, en particular para verificar las firmas hechas usando los Certificados ya mencionados.
- Realizar sus operaciones en conformidad a la Declaración de Prácticas de Certificación.
- Aprobar o rechazar las solicitudes de certificados de acuerdo a lo que marca la Declaración de Prácticas de Certificación vigente.
- Emitir Certificados conforme a la información proporcionada por el solicitante en el momento de su emisión y que esté libre de errores en la captura de datos.
- Revocar Certificados de acuerdo a lo que marca la Declaración de Prácticas de Certificación, asimismo de publicar y actualizar la Lista de Certificados Revocados con la frecuencia estipulada.
- Contar con un servicio de validación en línea que implemente el protocolo OCSP para la verificación del estado de un Certificado determinado.

2.1.3 Obligaciones del PSC (AC)

EL Prestador de Servicios de Certificación asociado a la Autoridad Certificadora del estado de Hidalgo actuará relacionando a un determinado titular con su clave pública mediante la expedición de un certificado de firma electrónica, todo ello de conformidad con la ley de Uso de Medios Electrónicos y Firma Electrónica Avanzada para el Estado de Hidalgo y con la presente DPC.

Los servicios prestados por el PSC asociado a la AC del estado de Hidalgo en el contexto de esta DPC, son los servicios de emisión y revocación de Certificados de firma electrónica, así pues, la AC tiene las siguientes obligaciones:

- Realizar sus operaciones en conformidad con la presente DPC.
- Realizar sus operaciones conforme a la legislación aplicable, es decir de acuerdo a la ley de Uso de Medios Electrónicos y Firma Electrónica Avanzada para el Estado de Hidalgo.
- Realizar la publicación de la presente DPC en el sitio electrónico designado, revisar sección 9.2 del presente documento.
- Comunicar cualquier cambio o adecuación de la presente DPC, la comunicación o notificación se realizará tal y como viene marcado en la sección 8.0 de la presente DPC.
- Utilizar sistemas y productos fiables que estén protegidos contra toda alteración, que aseguren la seguridad criptográfica de los procesos de certificación.

- Atender las solicitudes de Certificados de firma electrónica de los servidores públicos del Estado de Hidalgo en un tiempo razonable.
- Aprobar o rechazar las solicitudes de acuerdo a lo que marca la DPC vigente.
- Emitir Certificados de firma electrónica conforme a la información proporcionada por el solicitante en el momento de su emisión y que estén libre de errores en la entrada de datos.
- Revocar Certificados de firma electrónica de acuerdo a lo que marca la sección *4.4 Revocación de Certificados de firma electrónica,* asimismo de publicar y actualizar la Lista de Certificados Revocados con la frecuencia estipulada.
- Contar con un servicio de validación en línea que implementa el protocolo OCSP para la verificación del estado de un Certificado de firma electrónica determinado.
- Poner a disposición de sus suscriptores el Certificado de firma electrónica de la AC del estado de Hidalgo.
- No almacenar en ningún caso los datos de creación de firma, clave privada, de los titulares de Certificados de firma electrónica.
- Dar todas las facilidades para que se realicen los debidos procesos de auditoría.

2.1.4 Obligaciones del Solicitante de Certificado de firma electrónica

Es obligación de los solicitantes de Certificados de firma electrónica bajo la presente DPC:

- Presentar un dispositivo de almacenamiento según sea el caso, nuevo y con empaque sellado para el resguardo de su par de claves criptográficas.
- El proporcionar toda la información que marca el procedimiento de solicitud de Certificado de firma electrónica.
- El proporcionar información veraz para realizar la comprobación de su identidad.
- El notificar cualquier cambio de los datos proporcionados para la generación de su Certificado de firma electrónica durante el período de validez de éste.
- Aceptar las condiciones y términos que la AC del estado de Hidalgo dispone en la vigente PC para los Certificados de firma electrónica.

2.1.5 Obligaciones de los Titulares de Certificado de Firma Electrónica

Es obligación de los titulares de Certificados de firma electrónica bajo la presente DPC:

- Suministrar a los Agentes Registradores información exacta, completa y veraz con relación a los datos que estos le soliciten para completar el proceso de Certificación de firma electrónica.
- Conservar y utilizar de forma correcta el Certificado de firma electrónica y su par de claves de acuerdo a la normatividad vigente.
- Proteger y custodiar su clave privada y su Certificado electrónico asociado, empleando las medidas necesarias para evitar su pérdida, revelación, alteración o uso no autorizado.
- Proteger el dispositivo USB, según sea el caso, empleando las medidas necesarias para evitar su pérdida, revelación, alteración o uso no autorizado.
- Respetar las condiciones y términos firmados durante la solicitud de Certificado de firma electrónica.

- Solicitar de manera oportuna al PSC asociado a la AC del estado de Hidalgo la revocación de su Certificado de firma electrónica en caso de sospechar o tener conocimiento de que su clave privada ha sido: robada, extraviada, sea conocida por terceros; la forma de solicitar dicha revocación viene especificada en la sección *3.4 Solicitud de revocación*
- Aceptar las restricciones impuestas a su par de claves y Certificado de firma electrónicas emitidas por el PSC de la AC del estado de Hidalgo.
- No manipular o realizar actos de ingeniería en reversa sobre la implementación técnica de los servicios de certificación y firma electrónica avanzada (incluye hardware / software).

2.1.6 Obligaciones de los usuarios y terceros aceptantes

Es obligación de los usuarios y terceros que confían y aceptan los Certificados de firma electrónica emitidos por la AC del estado de Hidalgo bajo la presente DPC:

- Verificar la validez de los Certificados de firma electrónica en el momento de realizar cualquier transacción basada en estos.
- Conocer y sujetarse a las garantías, límites y responsabilidades derivadas de la aceptación de los Certificados de firma electrónica en los que confía y asumir sus obligaciones.
- Limitarse a los usos permitidos de los Certificados de firma electrónica estipulados en las extensiones de los mismos y en esta DPC.
- Asumir su responsabilidad en la comprobación de la validez, revocación de los Certificados de firma electrónica en que confía.
- Asumir su responsabilidad en la correcta verificación de las firmas electrónicas.
- Notificar cualquier hecho o situación fuera de lo común relativa al Certificado de firma electrónica y que calificará a ser revocado, a través de los medios electrónicos que disponga el PSC de la AC del estado de Hidalgo, http://firmaelectronica.hidalgo.gob.mx.
- Para confiar en los Certificados de firma electrónica emitidos por la AC del estado de Hidalgo todos los involucrados en el proceso de firma electrónica deberán conocer y aceptar toda restricción a la que está sujeto el Certificado de firma electrónica.

Sobre la confianza en las firmas electrónicas se incluye:

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

2.1.7 Obligaciones de la Autoridad de Registro (Agentes Registradores)

Es obligación de la Autoridad de Registro cumplir con siguientes obligaciones:

- Realizar sus operaciones en conformidad con la presente DPC.

- Realizar la comprobación exhaustiva de la identidad de los solicitantes de Certificado de firma electrónica.
- Comunicar al solicitante la correcta emisión del Certificado de firma electrónica.
- Notificar a los titulares de Certificados de firma electrónica la revocación de sus certificados cuando se produzca a petición de una autoridad competente o mediante un oficio de la Dirección General de Innovación Gubernamental y Mejora Regulatoria.
- Tramitar las peticiones de revocación lo antes posible.
- Comprobar que toda la información incluida en el Certificado de firma electrónica es correcta.

2.1.8 Obligaciones de enlaces de certificación

Es obligación de Enlace de Certificación cumplir con siguientes obligaciones:

- Realizar sus operaciones en conformidad con la presente DPC.
- Realizar la comprobación exhaustiva de la identidad de los solicitantes de Certificado de firma electrónica.
- Comunicar al solicitante la correcta emisión del Certificado de firma electrónica.
- Notificar a los titulares de Certificados de firma electrónica la revocación de sus certificados cuando se produzca a petición de una autoridad competente o mediante un oficio de la Dirección General de Innovación Gubernamental y Mejora Regulatoria.
- Tramitar las peticiones de revocación lo antes posible.

Comprobar que toda la información incluida en el Certificado de firma electrónica es correcta.

2.2 Responsabilidades

2.2.1 Limitaciones de responsabilidad

La Dirección General de Innovación Gubernamental y Mejora Regulatoria, limita su responsabilidad mediante la inclusión de los límites de uso de la firma electrónica avanzada plasmada en la presente DPC. Al grado permitido por la legislación aplicable, los acuerdos del titular de Certificado de firma electrónica y los acuerdos de terceras partes aceptantes de los Certificados de firma electrónica emitidos por la AC del estado de Hidalgo limitan la responsabilidad de la Dirección General de Innovación Gubernamental y Mejora Regulatoria.

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

2.2.2 Responsabilidad del PSC (AC)

La Dirección General de Innovación Gubernamental y Mejora Regulatoria, como Dependencia encargada de la AC responderá en el caso de incumplimiento de las obligaciones contenidas en la ley de Uso de Medios Electrónicos y Firma Electrónica avanzada para el Estado de Hidalgo, en el Reglamento de la ley de Uso de Medios Electrónicos y Firma Electrónica avanzada para el Estado de Hidalgo, y conforme a lo establecido en la DPC:

- La Dirección General de Innovación Gubernamental y Mejora Regulatoria, garantiza el cumplimiento de las obligaciones descritas en este documento.

- Asegurar que no existen errores en la información contenida en el Certificado de firma electrónica que fueron introducidos por la AC durante la generación de éste o al emitir la firma electrónica avanzada.
- Asegurar que no exista información falsa en el Certificado de firma electrónica que sean de conocimiento u originadas por las Autoridades de Registro que aprueban las solicitudes de Certificados de firma electrónica.
- De llevar a cabo la correcta identificación de los solicitantes de Certificados de firma electrónica para la emisión de los mismos.
- De llevar a cabo la correcta identificación de los solicitantes de revocación de Certificados de firma electrónica para realizar la revocación de los mismos.
- De actuar con diligencia profesional en las tareas inherentes a la administración de la solicitud de Certificado de firma electrónica y emisión del Certificado de firma electrónica.
- Garantizar que su firma electrónica avanzada cumple con todos los requerimientos materiales descritos en esta DPC.
- Que los servicios de revocación y uso de los repositorios se lleven a cabo de acuerdo a lo estipulado en esta DPC.
- La Dirección General de Innovación Gubernamental y Mejora Regulatoria no será responsable del contenido de aquellos documentos firmados electrónicamente por los titulares de un Certificado de firma electrónica.
- La Dirección General de Innovación Gubernamental y Mejora Regulatoria no garantiza los algoritmos criptográficos ni se hará responsable por los daños causados a través de exitosos ataques externos a los algoritmos criptográficos empleados en la tecnología dispuesta, sí guardó el proceso debido de acuerdo a la situación actual de la técnica y sí procedió bajo lo que está publicado en la presente DPC y la Ley de Uso de Medios Electrónicos y Firma Electrónica Avanzada para el Estado de Hidalgo.

2.2.3 Responsabilidad de los Titulares de Certificados de firma electrónica

La Dirección General de Innovación Gubernamental y Mejora Regulatoria requiere que sus suscriptores aseguren que:

- Ninguna persona distinta al titular ha tenido acceso a su clave privada.
- Todas las declaraciones efectuadas ante la Autoridad de Registro durante la solicitud de su Certificado de firma electrónica son verdaderas.
- Toda la información contenida en su firma electrónica avanzada es verdadera.
- Cada firma electrónica avanzada ha sido generada usando su clave privada correspondiente a la clave pública incluida en su Certificado de firma electrónica; que dicho certificado ha sido aceptado y está operacional es decir está vigente y no ha sido revocado al momento de la generación de la firma electrónica avanzada.
- La firma electrónica avanzada se utiliza exclusivamente para propósitos autorizados y legales conforme a lo estipulado en esta DPC y en la ley de Uso de Medios Electrónicos y Firma Electrónica Avanzada para el Estado de Hidalgo.
- El titular es un servidor público del Estado de Hidalgo y no un PSC.
- El titular no utilizará su clave privada para firmar electrónicamente Certificados de firma electrónica, Listas de Certificados Revocados u otro elemento relativo a las funciones atribuibles a un PSC.

2.2.4 Responsabilidad de la Autoridad de Registro

Las Autoridades de Registro asumirán toda responsabilidad sobre la correcta identificación de los solicitantes de Certificados de firma electrónica, así como la validación de la información proporcionada. Las Autoridades de Registro se suscribirán a las mismas limitaciones que establece la AC del estado de Hidalgo.

2.2.5 Responsabilidad de los usuarios y terceros aceptantes

- Los terceros aceptantes asumirán la responsabilidad de confiar en la información contenida en la firma electrónica avanzada ya que reconocen que cuentan con la suficiente información para tomar una decisión apropiada y compatible con el grado de confianza que ellos decidan asignar.
- Serán los únicos responsables de decidir si confían o no en la información recibida y asumen las consecuencias legales en el caso de fallar en el cumplimiento de las obligaciones a las que está sujeto dentro de esta DPC y la PC actual.
- El PSC asegura que toda la información contenida en el Certificado de firma electrónica emitido por éste, es veraz.
- El PSC, incorpora los mecanismos criptográficos necesarios para que el suscriptor o titular de un Certificado de firma electrónica genere su par de claves y que el suscriptor ha aceptado el certificado de acuerdo a lo previsto en la presente DPC.

2.2.6 Delimitación de Responsabilidad

La AC del estado de Hidalgo no asume ninguna responsabilidad cuando se encuentre ante cualquiera de estas circunstancias:

- Estado de Guerra, desastres naturales, funcionamiento defectuoso de los servicios eléctricos, las redes de telecomunicaciones, las redes telefónicas, virus informático, de los equipos informáticos utilizados por el titular o por los terceros o cualquier otro supuesto de caso fortuito.
- Por el uso indebido o fraudulento del directorio de Certificados de firma electrónica y Lista de Certificados Revocados emitidas por la AC del estado de Hidalgo.
- Por el uso de los Certificados de firma electrónica que exceda los límites establecidos por los mismos y los documentos de PC y DPC.
- Por el uso indebido de la información contenida en la firma electrónica avanzada.
- Por el contenido de los mensajes de datos o documentos electrónicos firmados o cifrados mediante la firma electrónica avanzada.
- En relación a acciones u omisiones del solicitante y/o titular de Certificado de firma electrónica:
  - Falta de veracidad de la información suministrada durante la solicitud de Certificado de firma electrónica.
  - Retraso en la comunicación/notificación de las causas de revocación del Certificado de firma electrónica.
  - Ausencia de solicitud de revocación del Certificado de firma electrónica cuando proceda.
  - Negligencia en la conservación de sus datos de creación de firma o clave privada, en el aseguramiento de su confidencialidad y en la protección de todo acceso o revelación.

  - Uso del Certificado de firma electrónica fuera de su periodo de vigencia, o cuando la Dirección General de Innovación Gubernamental y Mejora Regulatoria le notifique la revocación del mismo.
- En relación a acciones u omisiones de los usuarios o terceros aceptantes del Certificado de firma electrónica:
  - Falta de comprobación de las restricciones que figuren en el Certificado de firma electrónica o en esta DPC en cuanto a sus posibles usos.
  - Falta de comprobación de la revocación o pérdida de vigencia del Certificado de firma electrónica publicada en el servicio de consulta CRL o falta de verificación de la firma electrónica avanzada.

2.3 Responsabilidades Económicas

2.3.1 Indemnización por parte de los titulares

Al grado permitido por la ley General de Responsabilidades Administrativas de los Servidores Públicos del Estado de Hidalgo, la Dirección General de Innovación Gubernamental y Mejora Regulatoria requiere que los titulares indemnicen a la Dirección General de Innovación Gubernamental y Mejora Regulatoria por:

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

2.3.2 Indemnización por parte de los usuarios o terceros aceptantes de Certificados de firma electrónica

Al grado permitido por la ley General de Responsabilidades Administrativas de los Servidores Públicos del Estado de Hidalgo, la Dirección General de Innovación Gubernamental y Mejora Regulatoria requiere que los titulares indemnicen a la Dirección General de Innovación Gubernamental y Mejora Regulatoria por:

- Falla de la tercera parte aceptante del Certificado de firma electrónica para ejecutar las obligaciones a las que está sujeto.
- La omisión de la tercera parte aceptante de Certificado de firma electrónica de verificar el estado del Certificado de firma electrónica que determina si éste ha vencido o está revocado.

2.4 Normatividad y legislación aplicable

Las operaciones y funcionamiento de la AC del estado de Hidalgo, así como la presente Declaración de Prácticas de Certificación que sean de aplicación para cada tipo de certificado, estarán sujetas a la legislación que les sea aplicable, que incluyen:

- Ley de Uso de Medios Electrónicos y Firma Electrónica Avanzada para el Estado de Hidalgo.
- Reglamento de la Ley de Uso de Medios Electrónicos y Firma Electrónica Avanzada para el Estado de Hidalgo.

2.4.1 Independencia

En el caso de que una o más estipulaciones de esta DPC y la actual PC sean o llegasen a ser inválida, nula, o inexigible legalmente, se entenderá por no puesta, salvo que dichas estipulaciones fueran esenciales de manera que al excluirlas de esta DPC careciera ésta de toda eficacia jurídica.

2.5 Tarifas

2.5.1 Tarifas de emisión de Certificados de firma electrónica o recertificación

La Dirección General de Innovación Gubernamental y Mejora Regulatoria tiene derecho a cobrar a los suscriptores de su AC por concepto de emisión, administración de Certificados de firma electrónica, así como por concepto de recertificación.

2.5.2 Tarifas de acceso a los Certificados de firma electrónica

La Dirección General de Innovación Gubernamental y Mejora Regulatoria no aplicará una tarifa por tener disponibles dentro de un repositorio o de otra forma de hacer disponibles los Certificados de firma electrónica a terceros que confía en estos.

2.5.3 Tarifas de acceso a la información relativa al estado de los Certificados de firma electrónica o revocación

La Dirección General de Innovación Gubernamental y Mejora Regulatoria no aplicará una tarifa por tener disponibles dentro de un repositorio o de otra forma de hacer disponibles la Lista de Certificados Revocados a terceros que confía en estos, sin embargo, la Dirección General de Innovación Gubernamental y Mejora Regulatoria tiene derecho a cobrar una tarifa por entregar Listas de Certificados Revocados(LCR) adaptadas a necesidades específicas, servicios de validación en línea (OCSP) u otros servicios de valor agregado relacionados con la revocación del Certificado de firma electrónica avanzada o la información relativa al estado de los Certificados de firma electrónica avanzada.

2.5.4 Tarifas de otros servicios

No se aplicará ninguna tarifa por el servicio de información sobre estas Políticas de Certificado o sobre la Declaración de Prácticas de Certificación. Sin embargo cualquier uso para propósitos más allá de simplemente ver el documento, como por ejemplo la reproducción, redistribución, modificación o creación de obras derivadas, queda sujeto a un acuerdo de licencia con la entidad que tiene el derecho de autor del documento

2.6 Publicación y repositorios de información

La Dirección General de Innovación Gubernamental y Mejora Regulatoria pone a disposición de los suscriptores, usuarios y terceros que confían en los certificados emitidos por ésta, información de carácter público y que está relacionada con la AC y los servicios que ofrece, dentro de esta información se incluye:

- Sitio electrónico para la consulta del Certificado de firma electrónica de la AC del estado de Hidalgo.
  URL: http://firmaelectronica.hidalgo.gob.mx
- Sitio electrónico para la consulta de las Políticas de Certificados y Declaración de Prácticas de Certificación de la AC del estado de Hidalgo.
  URL: http://firmaelectronica.hidalgo.gob.mx
- Sitio electrónico para la consulta de los términos y condiciones de los servicios de la AC del estado de Hidalgo.
  URL: http://firmaelectronica.hidalgo.gob.mx

Esta información estará disponible bajo un esquema de 24 x 7, es decir 24 horas al día los 7 días de la semana; en caso de falla del sistema u otros factores que no se encuentren bajo el control de la Dirección General de Innovación Gubernamental y Mejora Regulatoria, ésta realizará todas las acciones pertinentes con la debida diligencia para restablecer el servicio en un período no mayor a 24 horas.

2.6.1 Frecuencia de publicación de la lista de Certificados Revocados

La Dirección General de Innovación Gubernamental y Mejora Regulatoria publicará la Lista de Certificados Revocados en el momento en que tramita una petición de revocación autenticada.
La Dirección General de Innovación Gubernamental y Mejora Regulatoria publicará de forma inmediata cualquier modificación en las políticas y prácticas de certificación, manteniendo un histórico de versiones.

2.6.2 Controles de acceso a los repositorios

El acceso a la información mencionada con anterioridad (certificado de la AC, Políticas de Certificados y Declaración de Prácticas de Certificación, términos y condiciones) es publicada en los repositorios de forma abierta, sin embargo la Dirección General de Innovación Gubernamental y Mejora Regulatoria es la única Dependencia autorizada para modificar, sustituir o eliminar información del repositorio y sitios electrónicos; para ello la Dirección General de Innovación Gubernamental y Mejora Regulatoria establece controles de seguridad físicos y lógicos que impiden a otras personas no autorizadas manipular esta información.
La Dirección General de Innovación Gubernamental y Mejora Regulatoria requiere que los terceros den su conformidad al acuerdo establecido para los terceros que confían o para el acuerdo de uso de la Lista de Certificados Revocados, como condición para acceder a la información de que se encuentra en los repositorios.

2.7 Auditoría de cumplimiento

2.7.1 Frecuencia de la auditoría

Se llevará a cabo una auditoría anual sobre la infraestructura de llave pública montada para soportar la AC del estado de Hidalgo y será realizada por la Secretaría de Contraloría; sin perjuicio de las auditorías contempladas dentro de la ley de Uso de Medios Electrónicos y Firma Electrónica Avanzada para el Estado de Hidalgo y conforme al Reglamento de Ley de Uso de Medios Electrónicos y Firma Electrónica Avanzada para el Estado de Hidalgo.

2.7.2 Relación entre el Auditor y la AC

Al margen de la función de auditoría, la Secretaría de Contraloría y la parte auditada (AC) no deberán de tener relación alguna que pueda derivar en un conflicto de intereses así como una relación funcional con el área objeto de la auditoría.

2.7.3 Aspectos cubiertos por los controles

La auditoría determinará la adecuación de los servicios de la AC con su respectiva DPC.

2.7.4 Comunicación de resultados

La Secretaría de Contraloría comunicará los resultados de la auditoría a la Dirección General de Innovación Gubernamental y Mejora Regulatoria que es la responsable de custodiar la AC, encargada de la administración y actualización de las Políticas de Certificados y la Declaración de Prácticas de Certificación; la comunicación de los mismos se realizará con absoluta discreción.

2.8 Confidencialidad y Privacidad de la Información

2.8.1 Ámbito de la información confidencial

La Dirección General de Innovación Gubernamental y Mejora Regulatoria considerará confidencial toda la información que no esté catalogada expresamente como pública. No se difunde información declarada como confidencial sin el consentimiento expreso por escrito de la entidad u organización que le haya otorgado el carácter de confidencialidad, a no ser que exista una imposición legal.

La Dirección General de Innovación Gubernamental y Mejora Regulatoria dispone de una adecuada política de tratamiento de la información y de los acuerdos que deberán firmar todas las personas que tengan acceso a información confidencial.

La Dirección General de Innovación Gubernamental y Mejora Regulatoria cumple en todo caso con la normatividad vigente en materia de protección de datos y concretamente con lo dispuesto por la Ley de Acceso a la Información.

Se declara expresamente como información confidencial:

- La clave privada de la AC del estado de Hidalgo, la cual, al ser el punto de máxima confianza será generada y custodiada conforme a lo especificado en la DPC.
- La clave privada de los suscriptores de la AC del estado de Hidalgo.
- Los registros de solicitud de Certificado de Firma Electrónica.
- Los registros de transacciones (registros completos y registros de auditoría de dichas transacciones)
- Los registros de auditoría creados o retenidos por la Dirección General de Innovación Gubernamental y Mejora Regulatoria.
- Los planes de contingencia y planes de recuperación de desastres,
- Las medidas de seguridad que controlen las operaciones de hardware/software de la AC del estado de Hidalgo, así como la administración del servicio de Certificados electrónicos y servicios de solicitudes designados.
- Toda la información clasificada como confidencial.

2.8.2 Información no confidencial

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

- La contenida en las Políticas de Certificados vigente.
- La información contenida en los Certificados de firma electrónica que la AC del estado de Hidalgo emita.
- La Lista de Certificados Revocados (CRL).
- La información sobre el estado de los Certificados de firma electrónica.
- Toda otra información clasificada como pública.

2.8.3 Entrega de información a Autoridades Competentes

La Dirección General de Innovación Gubernamental y Mejora Regulatoria está en el derecho de revelar información confidencial o privada si es solicitada en respuesta a procesos judiciales, administrativos y otros legales, durante una acción civil o administrativa.

2.8.4 Deber de secreto profesional

Los miembros de la Dirección General de Innovación Gubernamental y Mejora Regulatoria que participen en tareas derivadas de la operación de la AC del estado de Hidalgo, están obligados al deber de secreto profesional y por lo tanto sujetos a la normativa reguladora que les es aplicable. De igual forma, el personal contratado que participe en la operación o cualquier actividad relacionada con la AC del estado de Hidalgo está obligado al deber de secreto en el marco de las obligaciones contractuales contraídas con la Dirección General de Innovación Gubernamental y Mejora Regulatoria.

2.9 Derechos de propiedad intelectual

La Dirección General de Innovación Gubernamental y Mejora Regulatoria es la única Dependencia que tiene los derechos de propiedad intelectual sobre los Certificados de firma electrónica que emita.

La Dirección General de Innovación Gubernamental y Mejora Regulatoria es la única entidad en exclusiva de todos los derechos de propiedad intelectual que puedan derivarse del sistema de infraestructura de llave pública que regula las Políticas de Certificados y la Declaración de Prácticas de Certificación.

2.10 Derechos de propiedad en el par de claves y componentes de las claves

El par de claves correspondientes a los Certificados de la AC del estado de Hidalgo, sin importar el medio físico donde estén almacenadas y protegidas, son propiedad de la Dirección General de Innovación Gubernamental y Mejora Regulatoria.
El par de claves correspondientes a los Certificados de firma electrónica de los suscriptores de la AC del estado de Hidalgo, son propiedad de los suscriptores que son los titulares de Certificado de firma electrónica.

3.0 Identificación y Autenticación de los titulares de Certificados de firma electrónica

En este componente se describen los procedimientos que utilizan los PSC para autenticar la identidad y/u otros atributos de un usuario solicitante de un Certificado antes de la emisión del Certificado.
Este componente también aborda las prácticas de nombres, incluyendo el reconocimiento de los derechos de marca registrada en algunos nombres.
Además, el componente establece los procedimientos para autenticar la identidad y los criterios de aceptación de los solicitantes de entidades que desean convertirse en Agentes Certificadores u otras entidades que actúan o interactúan en la Infraestructura de Clave Pública.
También describe cómo se autentican las partes que soliciten renovación de claves o revocación.

3.1 Nombres

3.1.1 Tipos de nombres

Los certificados emitidos por la AC del estado de Hidalgo contienen el nombre distintivo (DN) del emisor y el del solicitante del certificado en los campos *Nombre Emisor* (*issuer name)* y *Nombre de Sujeto (subject name).*
El nombre distintivo (DN) de la AC del estado de Hidalgo mínimo contempla los siguientes valores:

Nombre distintivo (DN) Certificado de firma electrónica de la AC del Gobierno del Estado de Hidalgo.	
CN	AUTORIDAD CERTIFICADORA DEL ESTADO DE HIDALGO
O	GOBIERNO DEL ESTADO DE HIDALGO
OU	DIRECCIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL Y MEJORA REGULATORIA
C	PACHUCA
S	HIDALGO

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

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

3.1.2 Necesidad que los nombres sean significativos

Los Certificados de firma electrónica emitidos a los servidores públicos contienen nombres con semántica comúnmente entendible, lo cual permite la determinación de la identidad del individuo y que para tales efectos viene representada en el campo *Nombre de Sujeto* dentro del Certificado de firma electrónica.
La AC del estado de Hidalgo no permite que los suscriptores hagan uso de seudónimos, es decir que no sea su verdadero nombre personal el que utilicen para efectos de solicitar un Certificado de firma electrónica.
El Certificado de firma electrónica de la AC del estado de Hidalgo contiene el nombre distintivo (DN) con semántica comúnmente entendible que permite la determinación de la identidad de la AC al suscriptor o al tercero que confía en dicho certificado.

3.1.3 Reglas para interpretar varios formatos de nombres

Las reglas utilizadas por la AC del estado de Hidalgo para interpretar los nombres distintivos (DN) de los titulares o suscriptores de Certificados de firma electrónica cumplen con los estándares internacionales ISO/IEC 9594-8 y el RFC 3280.
Asimismo cumplen con lo que marca la ITFEA en su Anexo 6: *Estándares y Estructura del Certificado Digital*, por lo tanto todos los Certificados de firma electrónica emitidos utilizan la codificación *UTF8String* para los atributos *DirectoryString* de los campos *Emisor* y *Nombre de Sujeto*, mientras que la codificación para los campos país *(C)* y número de serie *(SN)* es *PrintableString*.

3.1.4 Unicidad de los nombres

La AC del estado de Hidalgo asegura que los nombres distintivos (DN) del *Nombre de Sujeto* del suscriptor son únicos, la utilización de su CURP y a través de componentes automatizados en el proceso de inscripción del suscriptor garantizan la unicidad del nombre distintivo (DN).

3.1.5 Procedimiento de resolución de conflictos sobre nombres

Será responsabilidad de los solicitantes de Certificados de firma electrónica el cerciorarse de que el nombre que están utilizando en el apartado *Nombre de Sujeto* de su Certificado de firma electrónica no infringe los derechos de propiedad intelectual de

otros solicitantes, así pues el PSC no realizará dicha verificación con alguna institución de Gobierno, ni resolverá cualquier disputa sobre propiedad intelectual del nombre.

En caso de que existiera alguna disputa relacionada con el uso del nombre de los solicitantes, la AC del estado de Hidalgo y sin alguna responsabilidad hacia cualquier solicitante o suscriptor de Certificados de firma electrónica, tendrá la facultad de rechazar la solicitud o suspender el Certificado de firma electrónica debido a tal disputa.

3.1.6 Reconocimiento, autenticación y papel de las marcas registradas

La AC del estado de Hidalgo no emitirá Certificados de firma electrónica a solicitantes que hayan usado deliberadamente un nombre cuyo derecho de uso no es de su propiedad, asimismo la AC del estado de Hidalgo no verificará con alguna institución de Gobierno la posesión del nombre o marca registrada en el proceso de Certificación.

3.1.7 Método de prueba de posesión de la clave privada

Los dos pares de claves asociados al Certificado de firma electrónica se generan en virtud del procedimiento fiable diseñado por el PSC. La generación de la clave privada del solicitante sólo se generará desde terminales autorizadas y debidamente reforzadas, dotadas de todos los mecanismos de seguridad que se requieren para el envío y exportación de información segura.
Durante el proceso de emisión de Certificados de firma electrónica, el PSC se asegura que el solicitante realmente posee la clave privada correspondiente a la solicitud que está en trámite mediante el uso de componentes automatizados que incorporan estándares internacionales como el uso del PKCS#10.

3.1.8 Autenticación de la identidad de un PSC

No estipulado.

3.1.9 Autenticación de la identidad de un individuo

El PSC recaba una serie de documentos para realizar una correcta verificación de la identidad del solicitante de Certificado de firma electrónica, esto bajo consentimiento explícito y conforme a lo que señala el anexo F5 de la Normatividad de ITFEA; por lo tanto, en caso de que se trate de una primera inscripción, el solicitante deberá de acudir a las oficinas dispuestas para este fin por la Dirección General de Innovación Gubernamental y Mejora Regulatoria. El trámite es personal e intransferible por lo que el interesado deberá presentarse en las instalaciones para realizarlo.

Los documentos a presentar para la obtención del Certificado son:

- Original de cualquiera de las siguientes identificaciones oficiales: credencial para votar expedida por el Instituto Federal Electoral, pasaporte vigente expedido por la Secretaría de Relaciones Exteriores, cédula profesional expedida por la Secretaría de Educación Pública.
- Clave Única de Registro de Población (CURP).
- Solicitud de Certificado Digital de Firma Electrónica Avanzada

3.1.10 Autenticación de la identidad de una Organización mayor

No estipulado.

3.1.11 Criterios para operar con AC externas

A la entrada en vigor de la presente DPC se contempla el establecimiento de relaciones de confianza con Prestadores de Servicio de Certificación externos.

3.2 Identificación y Autenticación en las peticiones de renovación de claves y Certificados de firma electrónica

Se requiere que todos los titulares de un Certificado de firma electrónica emitido por la AC del estado de Hidalgo tramiten un nuevo Certificado de firma electrónica una vez llegado el término de su fecha de vigencia, con el fin de mantener su continuidad en el uso de su firma electrónica.

El PSC requiere que el titular genere un nuevo par de claves para realizar el reemplazo del par de claves próximos a vencer, a este procedimiento se le conoce coloquialmente como “renovación de claves y Certificado de firma electrónica”.

El PSC verificará que la información proporcionada por el solicitante durante la primera inscripción continua siendo válida, además comprobará su identidad con la documentación mencionada en el apartado 3.1.9 antes de emitir un nuevo Certificado de firma electrónica, por lo que cualquier actualización a dicha información se realizará conforme al apartado 3.1.

3.3 Identificación y Autenticación para una renovación de claves y Certificados de firma electrónica tras una revocación

Será de aplicación lo contemplado en el apartado anterior, sólo si la revocación es acompañada de una sustitución de Certificado de firma electrónica.
Asimismo, el PSC se reserva el derecho de negar la renovación del Certificado de firma electrónica sí suceden los siguientes casos:

- El Certificado de firma electrónica fue emitido sin la autorización del individuo nombrado en el campo *Nombre de Sujeto*.
- Se aplicó la revocación porque el Certificado de firma electrónica fue emitido a una persona distinta a la nombrada en el campo *Nombre de Sujeto.*
- Se descubre que la información proporcionada en la solicitud de Certificado de firma electrónica es falsa.

3.4 Solicitud de Revocación

Las solicitudes de revocación se realizarán personalmente por el titular del Certificado de firma electrónica mediante los dos métodos dispuestos por el PSC, sin perjuicio de cualquier otro procedimiento que pudiera establecerse por la Dirección General de Innovación Gubernamental y Mejora Regulatoria a estos efectos.
Para el primer método de revocación, el titular deberá de comprobar la posesión de su clave privada por medio de la clave de anulación definida durante el proceso de emisión de Certificado de firma electrónica, en caso de no contar con dicha clave deberá de remitirse al segundo método.
Para el segundo método, el PSC pone a disposición del titular de Certificado de firma electrónica oficinas debidamente equipadas para realizar la revocación del Certificado

de firma electrónica, por lo tanto es necesaria la presencia física del titular acompañado de una solicitud de revocación de Certificado de firma electrónica.

La documentación a presentar para llevar a cabo la revocación por el segundo método es:

- Identificación oficial vigente con fotografía. (Credencial del IFE, Pasaporte o Cédula Profesional)

El PSC, validará los rasgos físicos de la fotografía de la identificación vigente con los rasgos físicos del suscriptor, y en caso de que existiese una controversia para la identificación del suscriptor, se le pediría además los siguientes documentos.

- Comprobante de Domicilio a nombre del suscriptor con la dirección que aparece en los datos que registró para la emisión del certificado.
- Acta de nacimiento
- CURP impresa.

Una vez aprobada la identidad del suscriptor, este mismo debe llenar la solicitud de revocación y firmarla autógrafamente, para que el PSC proceda con la solicitud de revocación hacia la Autoridad Certificadora.

En ambos casos la comunicación entre el PSC y el titular del Certificado de firma electrónica se realizarán de forma telemática y de forma verbal según sea el caso.

4.0 Requerimientos de Operación para el ciclo de vida de los Certificados

En este componente se especifican los requisitos impuestos a la emisión de Certificados con respecto a su ciclo de vida para: suscriptores o de otros participantes de la Infraestructura de Clave Pública.

4.1 Solicitud de Certificados de firma electrónica

El PSC sólo acepta solicitudes de Certificado de firma electrónica para las entidades que recoge la Ley de Uso de Medios Electrónicos y Firma Electrónica Avanzada para el Estado de Hidalgo y el Reglamento de la Ley de Uso de Medios Electrónicos y Firma Electrónica Avanzada para el Estado de Hidalgo.

El PSC se reserva el derecho de rechazar aquellas solicitudes de Certificado de firma electrónica que incumplan con algún requisito dispuesto en la Ley de Uso de Medios Electrónicos y Firma Electrónica Avanzada para el Estado de Hidalgo. En caso de que el PSC haya rechazado la solicitud de Certificado de firma electrónica, éste informará mediante oficio las razones por las que se rechaza dicha solicitud.

4.1.1 Solicitud de Certificados de firma electrónica para un PSC

No estipulado.

4.1.2 Tramitación de las solicitudes de Certificados de firma electrónica

Para obtener un Certificado de firma electrónica todos los solicitantes deberán completar el procedimiento de enrolamiento dispuesto por el PSC de la AC del Gobierno del Estado de Hidalgo, el cual incluye las siguientes actividades:

- Generar vía WEB su requerimiento de certificado de firma electrónica avanzada, de acuerdo al procedimiento establecido y publicado en el sitio electrónico de la Autoridad Certificadora http://firmaelectronica.hidalgo.gob.mx.

El Agente Registrador / Certificador:

- Verificar mediante el sistema de información automatizado de emisión de certificados digitales las solicitudes recibidas.
- Enviar mediante correo electrónico al solicitante fecha, hora y lugar de atención para la revisión de la documentación requerida y emisión del certificado digital.
- Verifica el estatus de los certificados con los que cuenta el solicitante.
- Revisar la documentación solicitada.
- Abrir expediente para iniciar proceso de enrolamiento, basado en el número de folio.
- Generar el certificado digital en el medio digital proporcionado por el solicitante
- Firmar autógrafamente la Solicitud de certificado de Firma Electrónica Avanzada.
- Proporcionará al solicitante la dirección del sitio WEB de la Autoridad Certificadora http://firmaelectronica.hidalgo.gob.mx, donde podrá encontrar el procedimiento para la instalación de su certificado digital en el equipo de cómputo especificado.
- El solicitante vinculará su par de claves (pública y privada) necesarias para poder firmar electrónicamente documentos en formato digital en el equipo de cómputo especificado.

4.1.3 Plazo para la tramitación de las solicitudes de Certificados de firma electrónica

Se tendrá un plazo de 72 hrs. hábiles para atender la emisión del certificado digital de firma electrónica avanzada solicitado, siempre y cuando el número de solicitudes no exceda la capacidad de respuesta de la autoridad certificadora.

4.2 Emisión de Certificados de firma electrónica

4.2.1 Actuación de la AC del estado de Hidalgo durante la emisión de los Certificados de firma electrónica

Una vez que se da la aprobación definitiva de la solicitud por parte del PSC de la AC del estado de Hidalgo, se procede con la emisión segura del Certificado de firma electrónica.

Durante la emisión de estos certificados la AC del estado de Hidalgo

- Utiliza un procedimiento de generación de certificados electrónicos que vincula de forma segura el Certificado de firma electrónica con la información utilizada en la solicitud, también es incluida la clave pública.
- Protege la integridad y confidencialidad de los datos contenidos en la solicitud.

- Realiza la notificación al suscriptor de la emisión de su Certificado de firma electrónica tal y como se describe en el apartado 4.2.2.
- Pone a disposición del suscriptor una copia del Certificado de firma electrónica en el sitio oficial de la AC del estado de Hidalgo, para que éste pueda obtener las copias que requiera.

Todos los Certificados de firma electrónica iniciarán su vigencia en el momento de su emisión. El periodo de vigencia estará sujeto a una posible extinción anticipada, cuando se den las causas que motiven la revocación del Certificado de firma electrónica.

4.2.2 Notificación del PSC de la AC del estado de Hidalgo al solicitante de la emisión del Certificado de firma electrónica

El solicitante conocerá la emisión efectiva de su Certificado de firma electrónica con la entrega del comprobante de Certificado de firma electrónica, el cual contiene el número de serie designado por la AC para su certificado, así como la fecha de vigencia y la URL para descargar el Certificado de firma electrónica en su caso.

4.3 Aceptación de los Certificados de firma electrónica

El solicitante deberá de conocer sus derechos y obligaciones que adquiere como titular de un Certificado de firma electrónica.
En caso de aceptar estos derechos y obligaciones el solicitante deberá de firmar de manera autógrafa el acuse de recibo que el PSC le expide; en caso de que no esté de acuerdo, el solicitante deberá de expresar su rechazo y firmar de manera autógrafa dicho rechazo para que el PSC de la AC del estado de Hidalgo proceda con la revocación del certificado.
Al término de haber aceptado y firmado de manera autógrafa el acuse de recibo, el titular del Certificado de firma electrónica estará listo para participar en procesos electrónicos que requieran su Firma Electrónica avanzada.

4.4 Revocación de los Certificados de firma electrónica

Se puede solicitar la revocación de un Certificado de firma electrónica por cualquiera de las siguientes causas:

- A solicitud expresa del titular,
- A solicitud del superior jerárquico del servidor público vía oficio con copia del mismo al interesado indicando la causa de la solicitud de revocación del certificado en cuestión,
- Por incapacidad jurídica declarada por una autoridad competente,
- Por fallecimiento,
- Por resolución judicial,
- Por incumplimiento del titular de sus obligaciones, previa comunicación del PSC especificando la causa, fecha y hora en que tendrá efecto la revocación,
- Por la falsedad o errores en la información proporcionada en la solicitud de Certificado de firma electrónica,
- Debido a que el PSC detectó que la clave privada asociada al Certificado de firma electrónica está duplicada,
- Por cualquier motivo, se encuentre comprometida la integridad o confidencialidad de la clave privada (a solicitud del titular).

4.4.1 Actuación de la AC del estado de Hidalgo durante la revocación de los Certificados de firma electrónica

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

- El titular del certificado debe obtener una solicitud de revocación en la oficina de PSC que contenga una sección para escrito libre con firma autógrafa del titular donde señale la causa de revocación. Los datos que incluye esta solicitud son el nombre del titular, CURP, RFC, domicilio del titular,
- Validará la coincidencia y veracidad de los datos incluidos en la solicitud de revocación con los datos contenidos en el documento probatorio de identidad. En caso de haberse cumplido con todos los requerimientos, se aprobará la solicitud de revocación,
- Procederá con la revocación del Certificado de firma electrónica y emitirá el comprobante que respalda esta transacción. El comprobante incluye la fecha y hora de la revocación. El titular recibirá vía correo electrónico la información de revocación del certificado correspondiente.
- Debe obtener el acuse de recibo del comprobante de revocación por parte del titular.

4.4.2 Periodo de gracia de la solicitud de revocación

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

4.5 Auditoría de Seguridad

Para tener un mayor control y contar con los indicadores necesarios que ayuden a determinar si existen los suficientes mecanismos de seguridad, el PSC de la AC del estado de Hidalgo lleva el registro de manera manual o automática de cualquier evento significativo relacionado con los siguientes eventos:

- Administración del ciclo de vida del Certificado de firma electrónica.
- La operación de la infraestructura que esta alrededor de la AC del estado de Hidalgo.
- El registro de los datos que entran en los distintos procedimientos asociados a los servicios del PSC de la AC del estado de Hidalgo.

4.5.1 Frecuencia con que se revisan los registros

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

4.5.2 Periodo de disponibilidad de los registros de auditoría

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

4.5.3 Mecanismos destinados para proteger los registros de auditoría

El PSC de la AC del estado de Hidalgo ha dispuesto de mecanismos de seguridad que realicen la debida protección de los registros de auditoría, con esto se evita que puedan ser borrados, modificados y que sean accedidos de forma no autorizada.

4.6 Respaldo

4.6.1 Planes de respaldo

El PSC de la AC del estado de Hidalgo ha establecido los procedimientos necesarios para tener a la mano las copias de respaldo efectuadas a toda la información contenida en su infraestructura de llave pública.

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

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

4.7 Recuperación

El PSC de la AC del estado de Hidalgo dentro de su procedimiento de recuperación incluye los siguientes requerimientos:

- El que se utilicen las copias de respaldo de la información más recientes.
- Están solucionados los problemas relacionados con el Hardware (en caso de que existan).
- Esta por completo restaurado el sistema operativo que soporta a la infraestructura de llave pública y debidamente configurado bajo los estándares que establece la Dirección General de Innovación Gubernamental y Mejora Regulatoria.

El Administrador de la AC y los demás roles encargados de recuperar los respaldos realizan las siguientes acciones coordinadas:

- Establecer todas las conexiones de red, así como las conexiones al módulo criptográfico encargado de resguardar el par de claves de la AC.
- Se recuperan los respaldos de los componentes de software involucrados en la operación de la infraestructura de llave pública.
- Se realiza la reconfiguración del software que opera la AC de acuerdo al manual proporcionado.
- Se realiza la restauración del módulo criptográfico.
- Se verifica que la restauración fue exitosa.

4.8 Destrucción de medios de almacenamiento

El PSC de la AC del estado de Hidalgo incorpora mecanismos de seguridad que ayudan con la correcta destrucción y reutilización de los medios utilizados para los respaldos. No podrán ser reutilizados ni desechados los medios de almacenamiento sin antes haber pasado por un proceso de borrado seguro.

El proceso de borrado seguro es debidamente documentado con el fin de que quede el registro que se dio de baja de la bitácora de respaldos el medio de almacenamiento destruido.

4.9 Protección de las bitácoras

El PSC de la AC del estado de Hidalgo incorpora mecanismos de protección que controlan el acceso a los registros que se generan durante las operaciones de éste, con el fin de detectar posibles violaciones a los procedimientos o entradas sospechosas e incidentes.

- Se crea una bitácora de seguimiento que lleva el registro de los roles que han solicitado el acceso a las bitácoras.
- El custodio de estas bitácoras se asegura que el registro se lleve a cabo de forma debida, los datos que incluyen son:
    - Fecha de revisión
    - Nombre de la persona autorizada que realizó la revisión
    - Fecha de la bitácora que se está revisando
    - Nombre que identifica la bitácora que se está revisando.

4.10 Cambio del par de claves de la AC

Antes de que llegue el vencimiento del Certificado de la AC del estado de Hidalgo la, se requiere lo siguiente:

- Se dejen de emitir nuevos Certificados de firma electrónica 30 días antes de que expire la fecha de vigencia del certificado de la AC.
- La Dirección General de Innovación Gubernamental y Mejora Regulatoria realizará un comunicando indicando la transición que se efectuará para hacer el cambio de claves de la AC.
- Se lleve a cabo la transición del par de claves antiguo al nuevo par de llaves de la AC.
- Se realice la re-certificación de todos los servicios a los que se les emitió un certificado de la AC del estado de Hidalgo y pertenecen a su infraestructura de llave pública.
- Las nuevas solicitudes de Certificado de firma electrónica se procesarán una vez que la AC tenga su nuevo par de claves y esté lista para realizar la firma de Certificados de firma electrónica. Dicho procedimiento está descrito en la presente DPC.

4.11 Finalización de la Autoridad Certificadora AC

En caso de que el PSC requiera dar por terminada la operación de la AC y los servicios que ésta ofrece, la Dirección General de Innovación Gubernamental y Mejora Regulatoria realizará todos los esfuerzos necesarios para notificar a sus suscriptores, a los terceros aceptantes, a otras entidades afectadas, apegándose a los lineamientos que marcan la Ley de Uso de Medios Electrónicos y Firma Electrónica Avanzada para el Estado de Hidalgo y las Políticas de Certificados; y apegándose a los procedimientos que dictan sus Prácticas de Certificación vigentes.

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

El PSC de la AC del estado de Hidalgo implementa políticas de seguridad que dan soporte a los requerimientos de seguridad establecidos en la presente DPC.

5.1 Controles Físicos

Los aspectos referentes a los controles de seguridad física por cuestiones de seguridad no estarán publicados en la presente DPC, sólo estarán presentes todos aquellos considerados como relevantes.

5.1.1 Ubicación física y construcción

La dirección de la Autoridad Certificadora del estado de Hidalgo, se está ubicada en Palacio de Gobierno, Primer Piso, Plaza Juárez S/N, Colonia Centro, Pachuca, Hidalgo, México.
Este centro de procesamiento cumple con todas las exigencias de requerimientos de seguridad y auditoría de la Autoridad Certificadora del estado de Hidalgo. El diseño de seguridad de este centro de procesamiento es tal, que previene y detiene cualquier intento de intrusión.

5.1.2 Acceso físico

Se cuenta con un sistema de control de acceso físico de personas con varios niveles de control. Las operaciones clasificadas como sensibles se desarrollan dentro de un recinto físicamente seguro con diversos niveles de seguridad para acceder a los equipos de cómputo y aplicaciones críticas.
El acceso físico es registrado automáticamente y se graba en video; el personal como proveedores que no está acompañado por una persona autorizada no tiene permitido el acceso a las áreas identificadas como de alto riesgo.

5.1.3 Alimentación eléctrica y aire acondicionado

El centro de procesamiento donde está la AC del estado de Hidalgo cuenta con sistemas de energía que garantizan alimentación continua e ininterrumpida de energía eléctrica, así como sistemas de aire acondicionado que mantienen el nivel de temperatura y humedad adecuado para los equipos instalados en el centro.

5.1.4 Exposición al agua

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

5.1.5 Protección y prevención de incendios

Están dispuestos los medios adecuados, como sistemas automáticos de detección de humo y extinción de incendios, para la protección de los equipos y cableado instalado en el centro de procesamiento.
Las medidas de prevención y protección cumplen con las regulaciones locales de seguridad.

5.1.6 Almacenamiento de Medios

Todos los medios de almacenamiento que contienen activos de software y de información, registros de auditoría, o respaldos son almacenados en las instalaciones de la Dirección General de Innovación Gubernamental y Mejora Regulatoria en las instalaciones externas dispuestas para este fin.
Se tienen implementados mecanismos de seguridad diseñados para proteger los medios de almacenamiento contra acceso no autorizado, daño causado por agua, incendio y magnetismo.

5.1.7 Copias de seguridad fuera de las instalaciones

La Dirección General de Innovación Gubernamental y Mejora Regulatoria mantiene copias de seguridad en instalaciones propias que cumplen con las medidas precisas de seguridad que marca la Dirección General de Innovación Gubernamental y Mejora Regulatoria.

5.2 Controles de los procedimientos

Por cuestiones de seguridad, la información que contiene los controles sobre los procedimientos se considera como confidencial por lo que sólo se hace referencia a los mismos.
La Dirección General de Innovación Gubernamental y Mejora Regulatoria procuran que toda la gestión se lleve a cabo de forma segura y conforme a lo publicado en la presente DPC, además de realizar las auditorías periódicas que vienen descritas en el presente documento.
Uno de los mecanismos que se ha diseñado es la separación de funciones con el fin de evitar que una o un grupo de personas puedan conseguir el control total de la infraestructura.

5.2.1 Roles identificados como de confianza

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

- Administradores de sistemas
- Administradores y operadores del módulo criptográfico
- Administrador de la PKI
- Agentes registradores
- Operador de PSC (Agente certificador)
- Gente de ingeniería y diseño de soluciones criptográficas

Los anteriores roles son considerados como confiables por la Dirección General de Innovación Gubernamental y Mejora Regulatoria, sin embargo aquellas personas que quieran ser identificadas como de confianza tendrán que sujetarse a los controles establecidos en la sección 5.3 del presente documento.
Se definen roles incompatibles de forma que una misma persona no pueda ostentar dos roles marcados como incompatibles, estos roles son:

- Incompatibilidad entre los administradores de sistemas y operadores del módulo criptográfico.
- Incompatibilidad entre el Agente Registrador y los administradores del módulo criptográfico.
- Incompatibilidad entre el administrador de sistema, agente registrador y administrador de la PKI.

5.2.2 Número de personas requeridas por tarea

Uno de los puntos clave para tener un control riguroso en ciertas tareas o procedimientos clasificados como de alta criticidad se requiere implementar la separación de funciones en base a las responsabilidades de cada persona.
Se requiere juntar un mínimo de dos personas con capacidad profesional para realizar las tareas correspondientes con la administración y establecimiento del módulo criptográfico. Este grupo de personas no tienen el secreto para activar la llave privada.
Una vez que se ha establecido el módulo criptográfico, se requiere del grupo de operadores para dar acceso a la clave privada resguardada en el módulo criptográfico.

5.2.3 Identificación y autenticación para cada usuario

Para todo el personal que requiera convertirse en persona de confianza, previamente ha sido sometido a una verificación de identidad ante el personal encargado de los Recursos Humanos de la Dirección General de Innovación Gubernamental y Mejora Regulatoria. Para la verificación de identidad el evaluado deberá acreditar la misma, recabando los siguientes documentos:

- IFE, Cartilla Militar, Pasaporte vigente emitido por la Secretaría de Relaciones Exteriores
- CURP por RENAPO.

Asimismo, el personal encargado de administrar y operar los módulos criptográficos encargados de resguardar la clave privada de la AC, se identifican y autentican mediante técnicas de secreto compartido en tarjetas inteligentes específicas del módulo criptográfico.

5.3 Controles sobre el personal

5.3.1 Requerimientos de antecedentes, cualidades y experiencia profesional

Todo el personal que preste sus servicios en el ámbito del PSC de la AC del estado de Hidalgo deberá contar con el conocimiento, experiencia y formación suficiente para el mejor desempeño de sus funciones asignadas. Para ello, la Dirección General de Innovación Gubernamental y Mejora Regulatoria realiza el proceso debido durante la selección de personal buscando que el perfil profesional del empleado se adecue lo más posible a la descripción de puesto

Se llevan revisiones periódicas de los antecedentes de personas con posiciones de confianza.

5.3.2 Procedimiento de comprobación de antecedentes

Este procedimiento se lleva a cabo conforme a la normativa desplegada en la AC de la Dirección General de Innovación Gubernamental y Mejora Regulatoria, en la Ley de Firma Electrónica avanzada para el Estado de Hidalgo.

5.3.3 Requerimientos de capacitación

El personal encargado de la operación y administración de la infraestructura de la AC del estado de Hidalgo recibe el entrenamiento y capacitación necesaria para asegurar la correcta y competente realización de sus funciones.

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

- Conceptos básicos de PKI.
- Responsabilidades de la posición.
- Entrega de una copia de las PC y la DPC vigentes.
- Uso y operación del hardware / software utilizado.
- Procedimientos de seguridad para cada rol.
- Procedimientos para la recuperación de la operación en caso de algún desastre.
- Sensibilización sobre la seguridad física, lógica y técnica.

5.3.4 Frecuencia y requerimientos de la capacitación

La frecuencia y los requerimientos están conforme a lo establecido en la normatividad vigente de la AC del estado de Hidalgo así como en lo que marca los procedimientos de la Dirección General de Innovación Gubernamental y Mejora Regulatoria.

5.3.5 Secuencia y frecuencia de rotación de tareas

No estipulado

5.3.6 Sanciones disciplinarias por acciones no autorizadas

Las acciones disciplinarias adecuadas se toman ante acciones no autorizadas, negligentes, mal intencionado u otras violaciones a las PC y DPC de la AC del estado de Hidalgo.

Las sanciones disciplinarias serán aplicadas de conformidad con lo establecido por la Ley General de Responsabilidades Administrativas de Servidores Públicos del Estado de Hidalgo.

5.3.7 Requisitos de contratación de terceros

Se aplicará la normativa general de la Dirección General de Innovación Gubernamental y Mejora Regulatoria para las contrataciones.

5.3.8 Documentación proporcionada al personal

Se proporcionará el acceso a la normatividad de seguridad vigente, la PC junto con la DPC.

6.0 Controles de Seguridad Técnica

La infraestructura de la AC del estado de Hidalgo utiliza sistemas y productos confiables, los cuales están protegidos contra toda alteración con el fin de garantizar la seguridad técnica y criptográfica de los procesos de certificación que dan soporte a la operación del PSC.

6.1 Generación del par de claves

El par de claves de la AC del estado de Hidalgo se deberán generar bajo dispositivos criptográficos de seguridad que cumplan con el estándar FIPS 140-2 nivel 3; asimismo se deberán utilizar estos dispositivos para generar la firma de los certificados digitales que emite el PSC de la AC del estado de Hidalgo.

6.2 Generación de la clave privada del titular

El par de claves del solicitante deberán ser generadas por el mismo, por tal motivo el PSC de la AC del estado de Hidalgo pone a disposición del solicitante sistemas criptográficos para la generación de su par de claves.
El PSC se asegura en todo momento que la clave privada siempre permanece bajo el poder del solicitante y no sucede ninguna transferencia de la misma con alguna otra entidad o sujeto.

6.3 Entrega de la clave pública al solicitante

El PSC de la AC del estado de Hidalgo, pone a disposición de los solicitantes sistemas criptográficos confiables que tramitan el requerimiento de certificación con la AC cumpliendo con el estándar PKCS#10.

6.4 Entrega de la clave pública de la AC a los terceros aceptantes

La clave pública de la AC del estado de Hidalgo está incluida en el certificado de dicha AC. El certificado de la AC deberá estar disponible en el repositorio electrónico especificado en el documento de PC para ser consultado y obtenido por los titulares de certificados así como de terceros aceptantes.

6.5 Tamaño de las claves

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

6.6 Hardware/ software empleado para la generación de la clave pública

La clave pública de la AC del estado de Hidalgo está generada y codificada dentro de módulos criptográficos adecuados y conforme a la normatividad vigente.
Para los suscriptores se ofrecen componentes de software confiables que ayudan con la generación de su par de claves, estas piezas de software cumplen con los estándares marcados en la respectiva DPC.

6.7 Usos admitidos de las claves

Los usos admitidos de la clave para cada certificado emitido por el PSC de la AC del estado de Hidalgo son: autenticación, firma electrónica de documentos, correos electrónicos, transacciones y archivos; no repudio y para el establecimiento de intercambio de llaves.
Este uso deberá venir codificado dentro del Certificado Digital emitido a los suscriptores.

6.8 Protección de la clave privada

La Dirección General de Innovación Gubernamental y Mejora Regulatoria, cumple con estrictos controles físicos, lógicos, así como con procedimientos para fortalecer la seguridad en el resguardo de su clave privada. La descripción de estos controles y procedimientos se incluye a lo largo del presente DPC.
Las claves privadas de los suscriptores son protegidas por ellos mismos, la AC del estado de Hidalgo no guarda copia alguna de la clave privada, por lo tanto los suscriptores deberán incorporar al menos las siguientes medidas para proteger la clave privada:

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

6.9 Método de activación de la clave privada

La clave privada de la AC del estado de Hidalgo se activa mediante la puesta en marcha del módulo criptográfico estipulado en el apartado *6.1*, llevando a cabo las siguientes tareas:

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

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

6.10 Método de desactivación de la clave privada

La persona encargada de administrar la AC puede proceder a la desactivación de la clave privada de la AC mediante los componentes de software / hardware encargados de operar y resguardar la clave privada. Para la reactivación es necesaria la intervención mínima de los roles definidos en la respectiva DPC.
Los suscriptores de la AC del estado de Hidalgo pueden proceder a desactivar su clave privada eliminando las claves del repositorio que lo contenga, dejar que expire el tiempo definido tras la introducción de la contraseña de acceso y cerrando el componente de software que se utiliza para introducir la contraseña de acceso.

6.11 Método de destrucción de la clave privada

En términos generales la destrucción de la clave privada siempre debe estar precedida por la revocación del certificado digital asociado a dicha clave; acompañado del procedimiento de eliminación de los archivos físicos del repositorio que contiene dichas claves.
En el caso de la clave privada de la AC del estado de Hidalgo, consiste en el borrado seguro de las claves resguardadas por el módulo criptográfico así como las copias de seguridad.

6.12 Archivo de la clave pública

Para mantener la disponibilidad y continuidad de las operaciones de la AC se efectúan respaldos periódicos de la base de datos de certificados digitales emitidos.

6.13 Periodos operativos de los certificados y periodos de uso para el par de claves

Los periodos de utilización de las claves son los determinados por la duración del certificado digital o revocación, y una vez transcurrido no se pueden continuar utilizando.
El certificado y par de claves de la AC tiene una validez de 10 años. La caducidad producirá automáticamente la invalidación de los certificados, originando el cese permanente de su operatividad conforme a los usos que le son propios.
Los periodos operacionales máximos para el Certificado de firma electrónica son de dos años, si se cumple lo siguiente:

- Los Certificados de firma electrónica son individuales.
- Los pares de llaves de los suscriptores están en el repositorio de claves del mismo S.O.

- Sí un suscriptor no puede completar los procesos de autenticación marcados en esta DPC, o no puede probar la posesión de su clave privada al ser requerida, el PSC de la AC del estado de Hidalgo rechazará de forma automática el Certificado de firma electrónica

6.14 Generación e instalación de los datos de activación

Para la generación de los datos de activación de la clave de la AC se utiliza la combinación de cierto número de tarjetas inteligentes, las cuales operan bajo el esquema de compartir el secreto. Para esto se requiere la intervención de los operadores del módulo criptográfico.
En el caso de los suscriptores, los datos de activación consisten en el establecimiento de una contraseña, la cual se determina al momento de generar el requerimiento de certificación. Para el establecimiento de esta contraseña se deben tomar en cuenta las siguientes normas de seguridad:

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

6.15 Protección de los datos de activación

Para los suscriptores, la contraseña de acceso a su clave privada debe ser conocida solo por ellos, debe ser personal e intransferible. Esta contraseña es el parámetro que permite la utilización de los certificados digitales en los servicios ofrecidos por la Dirección General de Innovación Gubernamental y Mejora Regulatoria, por lo tanto deben tenerse en cuenta las siguientes normas de seguridad:

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

6.16 Controles de seguridad informática

El PSC de la AC del estado de Hidalgo incorpora sistemas confiables que cumplen con las medidas de seguridad y procesos de evaluación continua establecidos por la Dirección General de Innovación Gubernamental y Mejora Regulatoria.

6.17 Controles de seguridad de la red

La infraestructura de red utilizada por los sistemas de la AC del estado de Hidalgo está dotada de todos los mecanismos de seguridad necesarios para garantizar el servicio de manera confiable e íntegra. La infraestructura de red está sujeta a los mismos periodos de evaluación que sufre la Dirección General de Innovación Gubernamental y Mejora Regulatoria.

6.18 Perfil de certificado

Los certificados digitales emitidos por el PSC de la AC del estado de Hidalgo cumplen con las siguientes normas:

- Recomendación X.509 ITU-T (2005): Tecnología de información – Interconexión de sistemas abiertos – El directorio: plataforma de autenticación
- RFC 3280: Internet X.509 Infraestructura de llave pública perfil de certificado y LCR

Los certificados digitales utilizan el estándar X.509 versión 3 que incluyen los siguientes campos:

- Versión
- Número de serie, este valor es único para cada certificado digital emitido
- Nombre del algoritmo de firma utilizado
- Nombre Distinguido del emisor
- Fecha de validez de inicio, el formato de la fecha está codificado en UTC (tiempo coordinado universal)
- Fecha de validez de término, el formato de la fecha está codificado en UTC (tiempo coordinado universal)
- Nombre Distinguido del sujeto
- Clave pública del sujeto

Las extensiones utilizadas son:

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

7.0 Descripción de Lista de Certificados Revocados y OCSP

El PSC de la AC del estado de Hidalgo emite listas de Certificados Revocados que se conforman de acuerdo el estándar descrito en el RFC 2459. Los datos que se incluyen en estas LCR son:

- La versión.
- El algoritmo de firma digital usado.
- El nombre del emisor y la entidad que ha emitido y firmado electrónicamente la LCR. El nombre del emisor cumple con los requisitos dispuestos para el Nombre Distinguido (DN) del emisor.
- Fecha y hora de emisión de la lista de Certificados Revocados, el LCR es efectivo desde el momento de su emisión.
- Fecha y hora de vigencia de la lista de Certificados Revocados.
- Fecha de cuando se emitirá la nueva LCR.
- El listado de los certificados revocados, que contiene el número de serie y fecha de revocación del Certificado de firma electrónica.

7.1 Disponibilidad de un sistema en línea de verificación del estado de los Certificados de firma electrónica

El PSC de la AC del estado de Hidalgo publicará un servicio mediante el cual se podrá verificar el estado de los Certificados de firma electrónica que ha emitido. Este servicio implementa el protocolo OCSP cumpliendo con el RFC 2560. A través de este

protocolo se determina el estado actual de un Certificado de firma electrónica sin requerir el acceso a las LCR. Un sujeto que requiera consultar el estado de un Certificado de firma electrónica sólo debe de enviar una petición al servicio de OCSP, este servicio ofrece una respuesta sobre el estado del certificado vía el protocolo http. Este servicio se encuentra disponible en la dirección de acceso incluida en el apartado 9.2.

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

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

8.0 Sobre la Actualización y Notificación

La Dirección General de Innovación Gubernamental y Mejora Regulatoria será la responsable de determinar cualquier adecuación a la presente Declaración de Prácticas de Certificación y a la Política de Certificados asociadas, asimismo, será la encargada de aprobar las correcciones y actualizaciones que hubiera en un futuro de dichos documentos.

El período de comentarios para cualquier corrección de la presente DPC y PC será de quince días, comenzando en la fecha en que las enmiendas se publiquen en el repositorio de la AC del estado de Hidalgo.

Las correcciones, ajustes y modificaciones de la DPC y PC se publicarán en el URL http://firmaelectronica.hidalgo.gob.mx del repositorio perteneciente a la AC del estado de Hidalgo.

9.0 Políticas de Publicación

9.1 Elementos no publicados en la presente Política de Certificados

Por razones de seguridad el material considerado como confidencial por la Dirección General de Innovación Gubernamental y Mejora Regulatoria no será revelado al público

9.2 Publicación de Información de Certificación

El contenido parcial de la DPC estará publicado a título informativo en el repositorio designado para tales fines, bajo la siguiente dirección electrónica: http://firmaelectronica.hidalgo.gob.mx. Es responsabilidad de la Dirección General de Innovación Gubernamental y Mejora Regulatoria la adopción de medidas de seguridad necesarias para garantizar la integridad, autenticidad y disponibilidad de dicha información.

Todos los suscriptores de la AC del estado de Hidalgo podrán tener acceso de forma fiable a la DPC y PC generada, accediendo a la siguiente dirección electrónica: http://firmaelectronica.hidalgo.gob.mx. La información aquí publicada se encuentra aprobada y firmada por la Unidad de Innovación Gubernamental y Mejora Regulatoria.
Las Listas de Certificados Revocados emitidas estarán firmadas electrónicamente por la AC del estado de Hidalgo y estarán disponibles para terceras partes de confianza así como para otros Prestadores de Servicios de Certificación.

La información sobre el estado de los Certificados de firma electrónica emitidos se podrá consultar a través del servicio de validación en línea que implementa el protocolo OCSP, este servicio estará disponible en la siguiente dirección electrónica: http://firmaelectronica.hidalgo.gob.mx.