Políticas de Certificados aplicables a la Autoridad Certificadora del Gobierno del Estado de Hidalgo.

Versión 1.0
Clave: HIDPCAC
Julio de, 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 la Unidad 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	**Páginas Afectadas**	**Descripción del Cambio**	**Fecha de Emisión**
1.0	-	Generación inicial del Documento.	19/07/2019
1.2	-	Revisión en el nombre del responsable de la Autoridad Certificadora	04/12/2019

Contenido

1.0 Introducción

1.1 Resumen

La ley sobre el uso de medios electrónicos y Firma Electrónica Avanzada para el Estado de Hidalgo contiene una serie de iniciativas que tienen por objeto regular en el estado el uso de la firma electrónica avanzada, la aplicación y uso de medios electrónicos, el reconocimiento de su eficacia jurídica y la prestación al público de servicios de certificación.

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 Políticas de Certificados las cuales regirán el funcionamiento y operación de la Infraestructura de Llave Pública, contiene el conjunto de reglas que indican la aplicabilidad, las responsabilidades y uso que le pueden dar los titulares a un certificado electrónico, así como la gestión que se emplea sobre los certificados electrónicos emitidos.

Las estructuras de estas políticas 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 Sobre el Uso de Medios Electrónicos y Firma Electrónica Avanzada para el Estado de Hidalgo.

1.2 Identificación del documento

Nombre del documento	Políticas de Certificados 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)	2.16.484.201.13.1.1.
Sitio electrónico de la PC	http://firmaelectronica.hidalgo.gob.mx

1.3 Personas y Entidades Participantes

Las personas y entidades participantes son:

- La Dirección General de Innovación y Mejora Regulatoria del Gobierno del Estado de Hidalgo como Entidad encargada de la emisión y administración de los certificados de firma electrónica a través de su AC Autoridad Certificadora.
- 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 firma electrónica.
- Las Autoridades de Registro encargadas de validar la identidad de los solicitantes de Certificados de firma electrónica.

1.4 Alcance

La presente Política de Certificación tiene por objeto el permitir que electrónicamente se autentique la identidad del firmante, se asegure la integridad de los documentos firmados electrónicamente y se evite el repudio de los mismos.

Todo titular de un Certificado electrónico emitido por la AC del Gobierno del Estado de Hidalgo obtendrá el valor de plena prueba legal para los documentos electrónicos donde el titular aplique su firma electrónica avanzada, respecto al hecho de que asegura la integridad y autenticidad de los mismos; por lo cual la firma electrónica avanzada tiene, en relación a la información consignada en los documentos electrónicos, el mismo valor que la firma autógrafa tiene, en relación a los datos consignados en papel.

1.5 Definiciones y Acrónimos

Término	Definición
Certificado de firma electrónica avanzada	Documento firmado electrónicamente por una Autoridad Certificadora que vincula datos de verificación de firma electrónica al firmante y confirma su identidad.
Clave Privada o datos de creación de firma electrónica avanzada	Los datos o códigos únicos que genera el firmante con cualquier tecnología de manera secreta para crear y vincular su firma electrónica.
Clave Pública o datos de verificación del firma electrónica avanzada	Las claves criptográficas, datos o códigos únicos que utiliza el destinatario para verificar la firma electrónica avanzada del firmante.
Declaración de Prácticas de Certificación	Declaración de Prácticas de Certificación
Dispositivo de creación de firma electrónica avanzada	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	A la firma electrónica que permite la identificación del signatario y ha sido creada por medios que esté tiene bajo su exclusivo control, de manera que está vinculada al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos.
Prestador de Servicios de Certificación	A la entidad pública o privada que ha sido facultada por la Autoridad Certificadora para prestar servicios relacionados con la firma electrónica avanzada y que expide certificados electrónicos.

Políticas de Certificados	Política de Certificados.
Titular del certificado	A la persona a cuyo favor se expida el certificado de la firma electrónica avanzada.
Firmante	A la persona física que cuenta con un dispositivo de creación de firma electrónica y que actúa en nombre propio o en el de una persona física o jurídica a la que representa.

1.6 Administradores/Operadores de la Autoridad Certificadora

Dependencia o área comisionada como responsable de toda la infraestructura de la Autoridad Certificadora	
Nombre	Dirección General de Innovación Gubernamental y Mejora Regulatoria
Correo electrónico	autoridad.certificadora@hidalgo.gob.mx
Dirección	Palacio de Gobierno, Primer Piso, Plaza Juárez S/N
Teléfono	01771 7176258
Fax	01 771 7176256

Dependencia encargada de custodiar la infraestructura de la Autoridad Certificadora	
Nombre	Dirección General de Innovación Gubernamental y Mejora Regulatoria
Correo electrónico	autoridad.certificadora@hidalgo.gob.mx
Dirección	Palacio de Gobierno, Primer Piso, Plaza Juárez S/N
Teléfono	01771 7176258
Fax	01 771 7176256

2.0 Disposiciones Generales

2.1 Obligaciones

2.1.1 Obligaciones de la Autoridad Certificadora y del Prestador de servicios de Certificación.

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 sobre el Uso de Medios Electrónicos y Firma Electrónica Avanzada para el Estado de Hidalgo.

El detalle de todas las obligaciones a las que estará sujeta la AC del Estado de Hidalgo se encuentra plasmada en su correspondiente DPC. Sin embargo, se considera relevante mencionar que la AC está obligada a prestar los servicios relacionados con la firma electrónica avanzada, dentro de los cuales se encuentran:

- Realizar sus operaciones conforme a la legislación aplicable, es decir de acuerdo a la ley sobre el Uso de Medios Electrónicos y Firma Electrónica Avanzada para el Estado de Hidalgo.
- Realizar sus operaciones en conformidad a la DPC
- 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 el 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.*
- Contar con un servicio de validación en línea que implementa el protocolo OCSP para la verificación del estatus 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.

2.1.2 Obligaciones del Solicitante de Certificado de Firma electrónica

Es obligación de los solicitantes de Certificados de firma electrónica cumplir con las siguientes PC, incluyendo:

- Presentar dispositivo USB de almacenamiento / token 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.
- Aceptar las condiciones y términos que la AC del Estado de Hidalgo dispone en la presente PC para los Certificados de firma electrónica.

2.1.3 Obligaciones de los Titulares de Certificado de firma electrónica

Es obligación de los titulares de Certificados de firma electrónica cumplir con la presente PC, incluyendo:

- Solicitar se le expida constancia de la existencia y registro del Certificado.
- Conservar y utilizar de forma correcta el Certificado de firma electrónica y su par de claves de acuerdo a la normatividad vigente.
- Proteger y custodiar su clave de anulación, su clave privada y su Certificado electrónico asociado, empleando las medidas necesarias para evitar su pérdida, revelación, alteración o uso no autorizado.
- Respetar las condiciones y términos firmados durante la solicitud de Certificado de firma electrónica.
- Solicitar de manera oportuna a la Dirección General de Innovación Gubernamental y Mejora Regulatoria 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.
- El notificar cualquier cambio de los datos proporcionados para la generación de su Certificado de firma electrónica durante el período de validez de éste.

2.1.4 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 Autoridad Certificadora del estado de Hidalgo cumplir con la presente PC, incluyendo:
- 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.

2.1.5 Obligaciones de la Autoridad de Registro

Es obligación de la Autoridad de Registro cumplir con la presente PC, incluyendo:
- Realizar sus operaciones en conformidad con la vigente DPC.
- Realizar la comprobación tomando como base los documentos que ha recibido de buena fe de la identidad de los solicitantes de Certificado de firma electrónica.
- Comunicar al solicitante la 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 del Gobierno del Estado de Hidalgo

2.1.6 Obligaciones de enlaces de certificación

Es obligación de los enlaces de certificación cumplir con la presente PC, incluyendo:
- Realizar sus operaciones en conformidad con la vigente DPC.
- Realizar la comprobación tomando como base los documentos que ha recibido de buena fe de la identidad de los solicitantes de Certificado de firma electrónica.
- Comunicar al solicitante la 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 del Gobierno del Estado de Hidalgo

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 vigente 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 el Gobierno 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 Prestador de Servicios de Certificación

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 sobre el Uso de Medios Electrónicos y de Firma Electrónica Avanzada para el Estado de Hidalgo, 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.
- Procurar que no existan 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 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 acuerdo a los documentos presentados.
- 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 la DPC.
- Que los servicios de revocación y uso de los repositorios se lleven a cabo de acuerdo a lo estipulado en la DPC.

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 la DPC y en la ley sobre el Uso de Medios Electrónicos y Firma Electrónica Avanzada para el Estado de Hidalgo.
- El titular es un servidor público del Gobierno 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 Prestador de Servicios de Certificación.

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 estable la AC de la Dirección General de Innovación Gubernamental y Mejora Regulatoria.

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 PC y la DPC.

2.2.6 Delimitación de Responsabilidad

La Dirección General de Innovación Gubernamental y Mejora Regulatoria 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 Gobierno 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 la PC 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 Normatividad y legislación aplicable

Las operaciones y funcionamiento de la AC del Estado de Hidalgo, así como las presentes Políticas de Certificados que sean de aplicación para cada tipo de certificado, estarán sujetas a la legislación que les sea aplicable, que incluyen:

- Ley sobre el Uso de Medios Electrónicos y Firma Electrónica avanzada para el Estado de Hidalgo.
- Reglamento sobre el Uso de Medios Electrónicos y Firma Electrónica avanzada del Estado de Hidalgo.

La invalidez de una de las cláusulas contenidas en la PC y en la DPC no afectará al resto de las cláusulas. En tal caso se tendrá la mencionada cláusula por no puesta.

2.3.1 Divisibilidad, Continuidad, Fusión, Notificaciones

Al grado permitido por la ley sobre el Uso de Medios Electrónicos y Firma Electrónica Avanzada para el Estado de Hidalgo, se deben contener, cláusulas relacionadas con la divisibilidad, continuidad, fusión y notificaciones.

- Una cláusula de divisibilidad en un acuerdo previene la determinación de la invalidez o falta de ejecución de una cláusula en dicho acuerdo, sin que se vea afectada la validez del resto del acuerdo.
- Una cláusula de continuidad determina cuales de las disposiciones de un acuerdo continuarán en vigencia a pesar del término o vencimiento del mismo.
- Una cláusula de fusión dice que todo el entendimiento referente al tema del acuerdo se incorpora en el acuerdo.
- Una cláusula de notificaciones en un acuerdo establece la forma en que las partes efectuarán las notificaciones una de la otra. Cualquier notificación se realizará por correo electrónico o mediante correo certificado dirigido a cualquiera de las direcciones referidas en el apartado datos de contacto.

2.4 Tarifas

2.4.1 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.

2.4.2 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.

2.4.3 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.

2.4.4 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

2.5 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 Gobierno del estado de Hidalgo.
  URL: **http://firmaelectrónica.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://firmaelectrónica.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://firmaelectrónica.hidalgo.gob.mx**
- Sitio electrónico para la revocación de certificado. Conforme al punto 3.4 de la PC.
  URL: **http://firmaelectrónica.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.

2.5.1 Frecuencia de publicación

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.
El PSC de la AC del estado de Hidalgo publicará de forma inmediata cualquier modificación en las políticas y prácticas de certificación, manteniendo un histórico de versiones.

2.5.2 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.

2.6 Auditoría de cumplimiento

2.6.1 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.**

2.6.2 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.

2.6.3 Aspectos cubiertos por los controles

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

2.6.4 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 y al área 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.

2.7 Confidencialidad y Privacidad de la Información

2.7.1 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 en su Artículo 18.

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, o de un Suscriptor,
- Los planes de contingencia y planes de recuperación ante 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.

2.7.2 Información no confidencial

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

- La contenida en las presentes Políticas de Certificados.
- La contenida en la Declaración de Prácticas de Certificación.
- 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.

2.7.3 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, con la excepción de la clave privada de la AC.

2.7.4 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.

2.8 Derechos de propiedad intelectual

La Dirección General de Innovación Gubernamental y Mejora Regulatoria es titular en exclusiva de todos los derechos de propiedad intelectual de las presentes Políticas de Certificados.
Asimismo, 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 presentes Políticas de Certificados.

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

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	MX
S	PACHUCA

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

Nombre distintivo (DN) Certificado de firma electrónica del Administrador 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	MX

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, 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 dentro del dominio del estado de Hidalgo, 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 el equipo del solicitante o por 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 Prestador de Servicios de Certificación

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 él PSC. El trámite es personal e intransferible por lo que el interesado deberá presentarse en las instalaciones para realizarlo

3.1.10 Autenticación de la identidad de una Organización

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 el PSC 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 sigue 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 y Mejora Regulatoria del Gobierno del Estado de Hidalgo a estos efectos.
Para el primer método de revocación, el titular deberá 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 del Certificado de firma electrónica oficinas debidamente equipadas las cuales operan para el efecto en un horario de 9:00 a 15:00. 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.
En ambos casos la comunicación entre el PSC y el titular del Certificado de firma electrónica se realizarán de forma telemática para su comprobante de revocación y de forma verbal según sea el caso.

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

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, 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, 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 avanzada.
- 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 del PSC, 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 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 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 firmar de manera autógrafa el acuse de recibo que el PSC le expide; en caso de que no esté de acuerdo, el PSC procederá con la cancelación del proceso de enrolamiento.
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 duplicado,
- Por cualquier motivo, se encuentre comprometida la integridad o confidencialidad de la clave privada.

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 PSC:

- 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.

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 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

4.5.1 Frecuencia con que se revisan los registros

Los registros deberán revisarse mensualmente 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 dos 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 dispondrá 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.

4.5.4 Análisis de vulnerabilidades de seguridad

Se deberán incorporar evaluaciones periódicas de vulnerabilidades a los distintos sistemas que soportan la operación de la AC del estado de Hidalgo, con el fin de tener bien robustecida la infraestructura de Tecnologías de la Información de la AC del estado de Hidalgo.

4.6 Respaldo

El PSC deberá de incorporar mecanismos de respaldos de información, con el fin de mantener la disponibilidad de los servicios a un 99.00 % en caso de que surja alguna contingencia.
Se deberá llevar registro que dé seguimiento detallado de los respaldos que se han efectuado a la infraestructura de TI y de los dispositivos o medios que contienen tales respaldos.

4.7 Protección de las bitácoras

El PSC incorpora mecanismos de protección que controlan el acceso a los archivos que se generan durante sus operaciones, con el fin de detectar posibles violaciones a los procedimientos o entradas sospechosas e incidentes. El detalle de este procedimiento esta descrito en la DPC asociada a esta PC.

4.8 Cambio del par de claves del Prestador de Servicios de Certificación.

Antes de que llegue el vencimiento del Certificado de la AC del estado de Hidalgo la Dirección General de Innovación Gubernamental y Mejora Regulatoria, se deberán establecer procedimientos de cambio de llaves que faciliten la transición del par de claves antiguo al nuevo par de claves. Dicho procedimiento está contenido en la DPC asociada a esta PC.

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

El PSC implementa políticas de seguridad que dan soporte a los requerimientos de seguridad establecidos en el documento de la DPC.
Asimismo, el PSC implementa políticas de seguridad física para dar soporte y cumplir con los requerimientos de seguridad física establecidos en el documento de la DPC.

De la gestión y operación que garantizan que los servicios de certificación se lleven bajo un entorno seguro y confiable, están establecidos en el apartado 5 del documento de la DPC desarrollado para el PSC.

6.0 Controles de Seguridad Técnica

La infraestructura del PSC 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.

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 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 PSC

El PSC, 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 la presente 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 de acuerdo a la DPC de la AC.
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 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 en la respectiva 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.
- Posesión y conocimiento de la clave de acceso a la clave privada únicamente por el titular del par de claves Privada y pública.

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 acceso o uso de la 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.

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 de la extinción o borrado de la clave privada.
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 y el entorno bajo el cual fue creado.

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.

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 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 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 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 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 y está disponible en la dirección de acceso incluida en el apartado 9.2.

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 Política de Certificados y a la Declaración de Prácticas de Certificación 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 PC y DPC 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, adecuaciones y modificaciones de la PC y DPC se publicarán en la sección 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 de la PC 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 PC y DPC generada, accediendo a la siguiente dirección electrónica: http://firmaelectronica.hidalgo.gob.mx La información aquí publicada se encuentra aprobada y firmada por la Dirección General 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 los 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.