SECRETARÍA GENERAL DEL CONSEJO

PODER JUDICIAL DEL ESTADO DE GUANAJUATO

Declaración de Prácticas y Políticas de Certificación de la Autoridad Certificadora del Poder Judicial del Estado de Guanajuato

Versión 1.0
junio, 2012

Sección de Control de Cambios			
Versión	**Pág (s) Afectadas**	**Descripción del Cambio**	**Fecha de Emisión**
1.0	Todas	Generación inicial del Documento.	12/06/2012

CONTENIDO

1.0 INTRODUCCIÓN

1.1 Resumen

La Ley sobre el Uso de Medios Electrónicos y Firma Electrónica para el Estado de Guanajuato y sus Municipios contiene una serie de iniciativas que tienen por objeto agilizar, facilitar el acceso y simplificar los actos, convenios, comunicaciones, procedimientos administrativos, trámites y la prestación de servicios públicos que corresponden a los tres Poderes, a efecto de que éstos promuevan el uso de medios electrónicos y firma electrónica en sus relaciones y actos.

Por tal motivo, el Consejo del Poder Judicial ha decido implementar una Infraestructura de Llave Pública que dotará de Certificados de firma electrónica a los titulares de los órganos jurisdiccionales o administrativos y demás servidores públicos que integran el Poder Judicial, así como a los particulares en los casos permitidos en la presente DPC, para la realización de los actos autorizados mediante el uso de medios electrónicos y firma electrónica certificada.

El presente documento incluye la Declaración de Prácticas y Políticas de Certificación que representan y orientan las actividades de la Autoridad Certificadora, Prestador de Servicios de Certificación y Agente Certificador del Poder Judicial, para la operación y administración de la Infraestructura de Llave Pública y sus procedimientos.

Además, 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 la Autoridad Certificadora y sus suscriptores.

1.2 Alcance de las Políticas de Certificados

Las políticas de certificación contenidas a lo largo de este documento tienen por objeto el reconocimiento e implementación de los principios generales que rigen la firma electrónica certificada, como son: Neutralidad Tecnológica, Equivalencia Funcional, Autenticidad, Conservación, Confidencialidad e integridad.

Y concretamente, 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.

1.3 Definiciones y Acrónimos

Término	Definición
Autoridad Certificadora	Autoridad Certificadora del Poder Judicial.
Certificado de firma electrónica	Documento firmado electrónicamente por la Autoridad Certificadora mediante el cual se confirma el vínculo existente entre el firmante y la firma electrónica y confirma su identidad.
Clave Privada o datos de creación de firma electrónica certificada	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 de la firma electrónica certificada	Las claves criptográficas, datos o códigos únicos que utiliza el destinatario para verificar la autenticidad de la firma electrónica del firmante.

Consejo	Consejo del Poder Judicial.
DPC	Declaración de Prácticas y Políticas de Certificación.
Dispositivo de creación de firma electrónica certificada	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 certificada	Aquélla que ha sido certificada por la autoridad certificadora, consistente en el conjunto de datos electrónicos integrados o asociados inequívocamente a un mensaje de datos que permite asegurar la integridad y autenticidad de ésta y la identidad del firmante.
Firmante	A la persona física que cuenta con un dispositivo de creación de firma y que actúa en nombre propio o en el de una persona física o jurídica a la que representa.
OCSP	Protocolo de Validación de certificados en línea (Online Certificate Status Protocol).
Poder Judicial	Poder Judicial del Estado de Guanajuato.
Prestador de Servicios de Certificación o Agente Certificador	Al órgano del Poder Judicial, persona o entidad pública o privada que ha sido facultada por la Autoridad Certificadora para prestar servicios relacionados con la Firma electrónica Certificada y que expide certificados electrónicos.

1.4 Identificación del documento

Nombre del documento	Declaración de Prácticas y Políticas de Certificación de la Autoridad Certificadora del Poder Judicial del Estado de Guanajuato.
Versión del documento	1.0
Estado del documento	En vigor
Fecha de emisión	12/06/2012
Fecha de caducidad	-
Sitio electrónico de la DPC	http://fec.poderjudicial-gto.gob.mx/dpc/

1.5 Personas y Entidades Participantes

Las personas y entidades participantes son:

- El Poder Judicial en su carácter de Autoridad Certificadora.
- La Secretaría General del Consejo a quien corresponde ejercer las funciones inherentes de la Autoridad Certificadora.

- Los titulares de las Oficialías Común de Partes, Encargados de Zona dependientes de la Dirección de Informática o cualquier otro órgano administrativo del Poder Judicial, según lo autorice el Consejo y la Autoridad Certificadora, en su carácter de Agentes Certificadores.
- La Dirección de Informática, como Prestador de Servicios de Certificación.
- Cualquier otro Prestador de Servicios de Certificación autorizado por la Autoridad Certificadora.
- Los titulares de los órganos jurisdiccionales o administrativos y demás servidores públicos que integran el Poder Judicial; así como los particulares en los casos autorizados en esta DPC; en su carácter de *solicitantes* o *titulares* del Certificado de firma electrónica.
- Los usuarios y terceros aceptantes de los Certificados de firma electrónica emitidos por la Autoridad Certificadora.

1.5.1 Autoridad Certificadora

El Poder Judicial es la Autoridad Certificadora, quien realizará esta función por conducto de la Secretaría General del Consejo con apoyo en la Dirección de Informática, los titulares de las Oficialías Común de Partes y excepcionalmente los Encargados de Zona dependientes de la Dirección de Informática o cualquier otro órgano administrativo del Poder Judicial según lo autorice el Consejo y la propia Autoridad Certificadora.

La Secretaría General del Consejo, por sí o a través del Secretario Técnico o personal que designe para tal efecto, podrá ejercer directamente las funciones inherentes a la Autoridad Certificadora; también podrá delegarlas en los Prestadores de Servicios de Certificación o Agentes Certificadores que estime pertinentes.

En el momento de publicación de la presente DPC, la Autoridad Certificadora que compone la Infraestructura de Llave Pública del Poder Judicial es la siguiente:

Nombre Distintivo	CN = AUTORIDAD CERTIFICADORA DEL PODER JUDICIAL DE GUANAJUATO OU = DIRECCIÓN DE INFORMÁTICA O = PODER JUDICIAL DEL ESTADO DE GUANAJUATO, C = MX, S = GUANAJUATO L = GUANAJUATO PostalCode = 36050
Número de serie	30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 31
Periodo de validez	Desde 12 de junio de 2012 00:00:00 p.m. hasta 11 de junio de 2022 23:59:59 p.m.
Estado	Operativa
Huella digital (SHA-1)	35 c6 13 9a 4b 6e 35 50 e8 02 92 77 fa 94 34 9a 77 5f cd 41

1.5.2 Administradores / Operadores de la Autoridad Certificadora

Área comisionada como responsable de toda la infraestructura de la Autoridad Certificadora	
Nombre	Dirección de Informática del Poder Judicial del Estado de Guanajuato
Correo electrónico	firma.electronica@poderjudicial-gto.gob.mx
Dirección	Circuito Superior Pozuelos #1
Teléfono	52 473 7352200 ext. 1250, 1251 Y 1252.
Fax	52 473 7352200 ext. 1252

Dependencia encargada de custodiar la infraestructura de la Autoridad Certificadora	
Nombre	Dirección de Informática el Poder Judicial del Estado de Guanajuato
Correo electrónico	firma.electronica@poderjudicial-gto.gob.mx
Dirección	Circuito superior pozuelos #1
Teléfono	52 473 7352200 ext. 1250, 1251 Y 1252
Fax	52 473 7352200 ext. 1252

1.5.3 Agentes Certificadores y Prestadores de Servicios de Certificación

Los titulares de las Oficialías Común de Partes y excepcionalmente los Encargados de Zona dependientes de la Dirección de Informática o cualquier otro órgano administrativo del Poder Judicial, según lo autorice el Consejo y la propia Autoridad Certificadora, fungirán como Agentes Certificadores; quienes realizarán las funciones de asistencia en los procedimientos y trámites para identificación, registro y autenticación de los solicitantes, así como la expedición y revocación de los Certificados de firma Electrónica correspondientes.

La Dirección de Informática funcionará como un Prestador de Servicios de Certificación y se encargará de todo lo concerniente a los ciclos de vida y administración de Certificados de firma electrónica, de las actividades señaladas en el párrafo anterior cuando les sean encomendadas por la Autoridad Certificadora y cualquier otra que se le atribuya en la presente DPC.

La Autoridad Certificadora podrá autorizar a un Prestador de Servicios de Certificación externo para las actividades respectivas.

1.5.4 Solicitante y Titular del Certificado de firma electrónica

El solicitante es el servidor público o el particular en los casos autorizados en esta DPC que se encuentra en un estado previo a la obtención del certificado y posterior a su solicitud.

El titular es el servidor público o el particular en los casos autorizados en esta DPC a favor del cual se ha otorgado el Certificado de firma electrónica.

1.5.5 Usuarios y Terceros aceptantes

Los usuarios y 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 Autoridad Certificadora, así como en las transacciones electrónicas que se lleven a cabo utilizando dichos certificados.

1.6 Uso de los Certificados

1.6.1 Uso apropiado de los Certificados de firma electrónica

Los Certificados de firma electrónica emitidos por la Autoridad Certificadora a favor de los servidores públicos del Poder Judicial sólo podrán ser usados para:

- Firmar electrónicamente las actuaciones judiciales y comunicaciones procesales cuando la ley así lo autorice.
- Firmar electrónicamente los actos, convenios, comunicaciones, trámites y procedimientos de naturaleza administrativa que correspondan a su esfera de competencia, autorizados por la ley o el Consejo.

Los Certificados de firma electrónica emitidos por la Autoridad Certificadora a favor de los particulares sólo podrán ser usados para:

- Firmar electrónicamente los actos y trámites autorizados por la ley o el Consejo cuando requieran de firma electrónica certificada.
- Firmar electrónicamente los actos procesales que les correspondan en su carácter de parte en los procesos seguidos ante los órganos jurisdiccionales del Poder Judicial, cuando la ley establezca el uso de la firma electrónica certificada para esos casos.

1.6.2 Limitaciones y restricciones en el uso de los certificados

Los Certificados de firma electrónica emitidos por la Autoridad Certificadora se sujetarán a las disposiciones contenidas en la Ley sobre el Uso de Medios Electrónicos y Firma Electrónica para el Estado de Guanajuato y sus Municipios, su reglamento expedido por el Poder Judicial y por la presente DPC.

Los Certificados de firma electrónica emitidos por la Autoridad Certificadora solamente podrán utilizarse para autenticar (acreditación de identidad) al titular respecto de su 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, ni para firmar otros certificados digitales o Listas de Certificados Revocados.

Los servicios de certificación que ofrece la Autoridad Certificadora 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 la Autoridad Certificadora 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 del Certificado de firma electrónica deberá hacer énfasis en el resguardo y custodia de las mismas.

1.6.3 Algoritmos y Parámetros Utilizados

Los Algoritmos de Firma son RSA con digestión **SHA-1**, los tamaños de claves son de al menos 1024 bits para usuarios y de 2048 bits para Autoridad Certificadora

1.7 Validación de estatus

Como parte de la infraestructura que la Autoridad Certificadora ha desplegado, se encuentra el servicio de validación de estatus de certificados en línea, el cual mediante el protocolo de OCSP se encarga de proporcionar, a solicitud de un tercero aceptante, el estado actual de un Certificado de firma electrónica emitido por la Autoridad Certificadora.

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 Autoridad Certificadora con otras Autoridades Certificadoras, quedan fuera del alcance del presente documento.

Los Algoritmos de Firma son RSA con digestión **SHA-1**, 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 Obligaciones y Responsabilidades de los Participantes de la Infraestructura de Llave Pública

2.1.1 Obligaciones de la Autoridad Certificadora

La Autoridad Certificadora actuará relacionando a un determinado suscriptor con su clave pública mediante la expedición de un Certificado de firma Electrónica, de conformidad con Ley sobre el Uso de Medios Electrónicos y Firma Electrónica para el Estado de Guanajuato y sus Municipios.

La Autoridad Certificadora puede confiar en el Agente Certificador o Prestador de Servicios de Certificación para los procesos de identificación y autenticación del solicitante del Certificado. En este caso, dicha autoridad correrá con toda la responsabilidad de la identificación y la autenticación de sus suscriptores.

No obstante lo anterior, se exige que la Autoridad Certificadora lleve a cabo revisiones regulares al Prestador de Servicios de Certificación para asegurar que cumple con sus obligaciones según el acuerdo aplicable en cuanto a las tareas de identificación y autenticación.

La Autoridad Certificadora asegura que todos los aspectos de los servicios que ofrece y gestiona dentro de la Infraestructura de Llave Pública son acordes en todo momento con esta DPC.

El personal de sistemas o los involucrados en un proceso de firma electrónica 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 DPC publicadas por la Autoridad Certificadora.

Sin perjuicio de lo anterior, la Autoridad Certificadora está obligada a lo siguiente:

- Realizar la publicación de la presente DPC en el sitio electrónico designado.
- Comunicar cualquier cambio o adecuación 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 en un tiempo razonable, no mayor a 3 días.
- Aprobar o rechazar las solicitudes de acuerdo a lo que marca la DPC vigente.
- 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 mencionadas en la presente DPC.
- Conservar por medios electrónicos toda la información y documentos relacionados con los Certificados emitidos durante un lapso de al menos quince años desde su emisión, en particular para verificar las firmas hechas usando los Certificados ya mencionados.
- Publicar su certificado de Autoridad Certificadora en http://fec.poderjudicial-gto.gob.mx/AC.der
- Realizar sus operaciones de conformidad con la DPC.
- Aprobar o rechazar las solicitudes de certificados de acuerdo a lo que marca la DPC vigente.
- Emitir Certificados conforme a la información proporcionada por el solicitante siempre que esté libre de errores en la captura de datos.
- Revocar Certificados de acuerdo a lo que marca la DPC.
- Contar con un servicio de validación en línea que implemente el protocolo OCSP para la verificación del estado de un Certificado determinado.
- Publicar y actualizar la Lista de Certificados Revocados con la frecuencia estipulada.
- Poner a disposición de sus suscriptores el Certificado de firma electrónica de la Autoridad Certificadora.
- No almacenar en ningún caso los datos de creación de llave o clave privada de los titulares de Certificados de firma electrónica.
- Dar todas las facilidades para que se realicen los debidos procesos de auditoría.

2.1.2 Obligaciones del Prestador de Servicios de Certificación o Agente Certificador

El Prestador de Servicios de Certificación y los Agentes Certificadores se obligan en los términos definidos en la preste DPC, en la Ley sobre el Uso de Medios Electrónicos y Firma Electrónica para el Estado de Guanajuato y sus Municipios y su reglamento, tratándose de las actividades que les hubieren sido encomendadas por la Autoridad Certificadora.

2.1.3 Obligaciones del Solicitante de Certificado de firma electrónica

Son obligaciones de los solicitantes de Certificados de firma electrónica bajo la presente DPC, además de las que estipule la Ley sobre el Uso de Medios Electrónicos y Firma Electrónica para el Estado de Guanajuato y sus Municipios y su reglamento, las siguientes:

- Presentar un dispositivo USB de almacenamiento (Token) o cualquier otro que disponga la Autoridad Certificadora, para el resguardo de su par de claves criptográficas.

  Dicho dispositivo podrá ser proporcionado a los servidores públicos del Poder Judicial por parte de la Autoridad Certificadora, según la disponibilidad presupuestaria.
- Proporcionar toda la información que marca el procedimiento de solicitud de Certificado de firma electrónica.
- Proporcionar información veraz para realizar la comprobación de su identidad.
- 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 Autoridad Certificadora dispone en la vigente DPC para los Certificados de firma electrónica.

2.1.4 Obligaciones del Titular de Certificado de firma electrónica

Son obligaciones del titular de Certificado de firma electrónica bajo la presente DPC, además de las que estipule la Ley sobre el Uso de Medios Electrónicos y Firma Electrónica para el Estado de Guanajuato y sus Municipios y su reglamento, las siguientes:

- Suministrar a los Agentes de Registro o Prestadores de Servicios de Certificación información exacta, completa y veraz con relación a los datos que éstos le soliciten para completar el proceso de Certificación de firma electrónica.
- Conservar y utilizar de forma correcta el Certificado de firma electrónica y su clave privada de acuerdo con 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 o el que determine la Autoridad Certificadora, 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 Prestador de Servicios de Certificación asociado a la Autoridad Certificadora la revocación de su Certificado de firma electrónica en caso de sospechar o tener conocimiento de que su clave privada ha sido robada, extraviada o sea conocida por terceros.
- Aceptar las restricciones impuestas a su clave privada y Certificado de firma electrónicas emitidas por el Prestador de Servicios de Certificación de la Autoridad Certificadora.
- No manipular o realizar actos de "Ingeniería inversa" sobre la implementación técnica de los servicios de certificación y firma electrónica certificada, tanto en hardware como en software.
- Solicitar se le expida constancia de la existencia y registro del Certificado de firma electrónica.
- Notificar cualquier cambio de los datos proporcionados para la generación de su Certificado de firma electrónica durante el periodo de validez de éste.

2.1.5 Obligaciones del Usuario y Tercero Aceptante

Son obligaciones del usuario y tercero aceptante bajo la presente DPC, las siguientes:

- Verificar la validez de los Certificados de firma electrónica en el momento de realizar cualquier transacción basada en éstos.
- 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 o 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 pudiera tener como consecuencia su revocación; lo que hará a través de los medios electrónicos que disponga la Autoridad Certificadora.
- Conocer y aceptar toda restricción a la que está sujeto el Certificado de firma electrónica.
- No confiar en la firma electrónica cuando se realice una operación o transacción electrónica que pueda ser considerada como ilícita o se dé un uso no autorizado en la presente DPC.

2.2 Responsabilidades

2.2.1 Límite de responsabilidad

La Autoridad Certificadora limita su responsabilidad mediante la inclusión de los límites de uso del Certificado de firma electrónica reconocido.

La Autoridad Certificadora 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, si guardó el proceso debido de acuerdo a la situación actual de la técnica y si procedió bajo lo que está publicado en la presente DPC y la Ley sobre el Uso de Medios Electrónicos y Firma Electrónica para el Estado de Guanajuato y sus Municipios.

La Autoridad Certificadora únicamente es responsable por los errores que llegase a cometer con motivo de culpa grave en el proceso de generación, registro, entrega y revocación del certificado digital, según corresponda.

No será responsable por los daños y perjuicios que se pudieran causar al solicitante o a terceros cuando por caso fortuito o fuerza mayor no puedan realizarse registros, verificaciones, revocaciones o tramitar documentos electrónicos cifrados con las claves públicas y privadas relacionadas con dicho certificado.

Por caso fortuito o fuerza mayor se entenderá todo acontecimiento o circunstancia inevitable, más allá del control razonable de la Autoridad Certificadora que le impida el cumplimiento de sus funciones con el carácter que le corresponde.

2.2.2 Responsabilidad de la Autoridad Certificadora

La Autoridad Certificadora es responsable del cumplimiento a las disposiciones establecidas en la presente DPC y en la Ley sobre el Uso de Medios Electrónicos y Firma Electrónica para el Estado de Guanajuato y sus Municipios, respecto de las atribuciones que le sean conferidas.

2.2.3 Exoneración de responsabilidad

La Autoridad Certificadora 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 Autoridad Certificadora.
- Por el uso de los Certificados de firma electrónica que exceda los límites establecidos por los mismos y la DPC.
- Por el uso indebido de la información contenida en la firma electrónica certificada.
- Por el contenido de los mensajes de datos o documentos electrónicos firmados o cifrados mediante la firma electrónica certificada.
- Por la falla técnica originada por cualquier motivo que produzca un mal funcionamiento del dispositivo USB, Token u otro, donde se contenga el Certificado de firma electrónica y la correspondiente clave privada.
- 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 Secretaría General del Consejo le notifique la revocación del mismo.

- En relación con 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 certificada.

2.2.4 Responsabilidad del Prestador de Servicios de Certificación y Agente Certificador

El Prestador de Servicios de Certificación y los Agentes Certificadores serán responsables del cumplimiento a las obligaciones contenidas en esta DPC y la Ley sobre el Uso de Medios Electrónicos y Firma Electrónica para el Estado de Guanajuato y sus Municipios, en cuanto a los servicios que la Autoridad Certificadora les haya encomendado en su auxilio.

2.2.5 Responsabilidad de los Titulares de Certificados de firma electrónica

Los titulares de Certificados de firma electrónica serán responsables y deberán garantizar que:

- Ninguna persona distinta al titular ha tenido acceso a su clave privada.
- Son verdaderas todas las declaraciones efectuadas ante la Autoridad Certificadora, Prestador de Servicios de Certificación o Agente Certificador durante la solicitud de su Certificado de firma electrónica.
- Toda la información contenida en su firma electrónica certificada es verdadera.
- Cada firma electrónica certificada 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, está vigente y no ha sido revocado al momento de la generación y validación de la firma electrónica certificada.
- La firma electrónica certificada se utiliza exclusivamente para los actos autorizados conforme a lo estipulado en esta DPC y en Ley sobre el Uso de Medios Electrónicos y Firma Electrónica para el Estado de Guanajuato y sus Municipios.
- El titular es un servidor público del Poder Judicial, en su caso, y no un Prestador de Servicios de Certificación.

- 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.

2.2.6 Responsabilidad del Usuario y Tercero Aceptante

El usuario y tercero aceptante asumirán la responsabilidad de confiar en la información contenida en la firma electrónica certificada, de acuerdo con los principios que la rigen así como las disposiciones contenidas en la presente DPC y en la Ley sobre el Uso de Medios Electrónicos y Firma Electrónica para el Estado de Guanajuato y sus Municipios.

2.3 Normatividad y legislación aplicable

La ejecución, interpretación, modificación o validez de la presente DPC se regirá por lo dispuesto en la legislación vigente del Estado de Guanajuato, y concretamente por la Ley sobre el Uso de Medios Electrónicos y Firma Electrónica para el Estado de Guanajuato y sus Municipios, y el Reglamento sobre el Uso de Medios Electrónicos y Firma Electrónica del Poder Judicial del Estado de Guanajuato.

2.3.1 Independencia

En el caso de que una o más estipulaciones de esta DPC sean o llegasen a ser inválidas, nulas, o inexigibles 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.

2.4 Tarifas

2.4.1 Tarifas de emisión de Certificados de firma electrónica o recertificación

La Autoridad Certificadora tiene derecho a cobrar a sus suscriptores una tarifa por concepto de emisión, administración o recertificación de Certificados de firma electrónica.

2.4.2 Tarifas de acceso a los Certificados de firma electrónica

La Autoridad Certificadora no aplicará una tarifa por tener disponibles dentro de un repositorio o de otra forma de hacer disponibles los Certificados de firma electrónica a usuarios tercero aceptantes.

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

La Autoridad Certificadora no aplicará una tarifa por tener disponibles dentro de un repositorio o de otra forma de hacer disponibles la Lista de Certificados Revocados, a usuarios y terceros aceptantes, sin embargo, la Autoridad Certificadora 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 certificada o la información relativa al estado de los Certificados de firma electrónica certificada.

2.4.4 Tarifas de otros servicios

La Autoridad Certificadora no aplicará ninguna tarifa por el servicio de información sobre la DPC. Sin embargo, cualquier uso para propósitos más allá de su simple consulta, 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 Autoridad Certificadora pone a disposición de los titulares de Certificados de firma electrónica y usuarios y terceros aceptantes la información de carácter público que está relacionada con la autoridad certificadora y los servicios que ofrece, conforme a lo siguiente:

- Sitio electrónico para la consulta del Certificado de firma electrónica de la Autoridad Certificadora.

  URL: **http://fec.poderjudicial-gto.gob.mx/ac.der**

- Sitio electrónico para la consulta de la DPC.

  URL: **http:// fec.poderjudicial-gto.gob.mx/dpc**

- Sitio electrónico para la consulta de los términos y condiciones de los servicios de la Autoridad Certificadora.

  URL: **http:// fec.poderjudicial-gto.gob.mx/dpc**

- Sitio electrónico para la revocación de Certificados.

  URL: **http:// fec.poderjudicial-gto.gob.mx/revoca_certificado**

Esta información estará disponible las 24 horas del día, los siete días de la semana.

En caso de falla del sistema u otros factores que no se encuentren bajo el control de la Autoridad Certificadora, ésta realizará todas las acciones pertinentes con la debida diligencia para restablecer el servicio en un período no mayor a 72 horas.

2.5.1 Frecuencia de publicación de la lista de Certificados Revocados

La Autoridad Certificadora generará la Lista de Certificados Revocados en el momento en que tramita una petición de revocación autenticada y de manera periódica de acuerdo al tiempo establecido por la Autoridad Certificadora.

Asimismo, 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 es publicada en los repositorios de forma abierta, sin embargo, sólo la Autoridad Certificadora con auxilio de la Dirección de Informática podrá modificar, sustituir o eliminar información del repositorio y sitios electrónicos.

Para ello, la Dirección de Informática establecerá controles de seguridad físicos y lógicos que impidan a otras personas no autorizadas manipular esta información.

Los usuarios y terceros aceptantes deberán dar su consentimiento al acuerdo de uso de Lista de Certificados Revocados, para tener acceso a la información respectiva.

2.6 Confidencialidad y Privacidad de la Información

2.6.1 Ámbito de la información confidencial

Se considerará confidencial toda la información que no esté catalogada expresamente como pública.

No se difundirá 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 Autoridad Certificadora 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 Autoridad Certificadora, 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 Autoridad Certificadora.
- Los registros de solicitud de Certificado de Firma Electrónica.
- Los registros de transacciones (registros completos y registros de auditoria de dichas transacciones).
- Los registros de auditoría creados o retenidos por la Secretaría General del Consejo.
- Los planes de contingencia y planes de recuperación de desastres.
- Las medidas de seguridad que controlen las operaciones de hardware/software de la Autoridad Certificadora, así como la administración del servicio de Certificados electrónicos y servicios de solicitudes designados.
- Toda la información clasificada como confidencial.

2.6.2 Información no confidencial

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

- La contenida en la presente DPC.
- La contenida en los Certificados de firma electrónica que emita la Autoridad Certificadora.
- La Lista de Certificados Revocados (CRL).

- La información sobre el estado de los Certificados de firma electrónica.
- Toda otra información clasificada como pública.

2.6.3 Entrega de información a Autoridades Competentes

La Autoridad Certificadora deberá revelar la información confidencial o privada si es solicitada en respuesta a procesos judiciales, administrativos y otros legales, durante una acción civil o administrativa, con la excepción de la clave privada de la Autoridad Certificadora.

2.6.4 Deber de secreto profesional

Los miembros de la Secretaría General del Consejo y demás servidores públicos del Poder Judicial que participen en tareas derivadas de la operación de la Autoridad Certificadora 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 Autoridad Certificadora está obligado al deber de secreto en el marco de las obligaciones contractuales contraídas con dicha autoridad certificadora.

2.7 Derechos de propiedad intelectual

El Poder Judicial es el titular de los derechos de propiedad intelectual sobre los Certificados de firma electrónica que emita por conducto de la Autoridad Certificadora.

Asimismo, el Poder Judicial es el titular exclusivo de todos los derechos de propiedad intelectual que puedan derivarse del sistema de Infraestructura de Llave Pública que regula la DPC.

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

El par de claves correspondientes a los Certificados de la Autoridad Certificadora, sin importar el medio físico donde estén almacenadas y protegidas, son propiedad del Poder Judicial.

El par de claves correspondientes a los Certificados de firma electrónica de los suscriptores de la Autoridad Certificadora son propiedad de los suscriptores que son los titulares de Certificado de firma electrónica.

3 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 Autoridad Certificadora 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 Autoridad Certificadora contempla como mínimo los siguientes valores:

Nombre distintivo (DN) Certificado de firma electrónica de la Autoridad Certificadora.	
CN	Autoridad Certificadora del Poder Judicial del Estado de Guanajuato
O	Poder Judicial del Estado de Guanajuato
OU	Dirección de Informática
C	MX
S	GUANAJUATO

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

Nombre distintivo (DN) Certificado de firma electrónica del suscriptor.	
CN	<NOMBRES><APELLIDO1> <APELLIDO2>
O	<DEPENDENCIA EDO. GUANAJUATO >
OU	<AREA A LA QUE PERTENECE>
C	MX
SN	CURP TITULAR DEL CERTIFICADO DE FIRMA ELECTRONICA
X.500uniqueIdentifier (2.5.4.45)	RFC TITULAR DEL CERTIFICADO DE FIRMA ELECTRONICA

3.1.2 Necesidad de que los nombres sean significativos

Los Certificados de firma electrónica 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 Autoridad Certificadora 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 Autoridad Certificadora contiene el nombre distintivo (DN) con semántica comúnmente entendible que permite al suscriptor o al usuario tercero aceptante identificar a la Autoridad Certificadora.

3.1.3 Reglas para interpretar varios formatos de nombres

Las reglas utilizadas por la Autoridad Certificadora 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.

3.1.4 Unicidad de los nombres

La Autoridad Certificadora asegura que los nombres distintivos (DN) del *Nombre de Sujeto* del suscriptor son únicos, virtud a la utilización de su CURP y componentes automatizados en el proceso de inscripción del suscriptor.

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 la Autoridad Certificadora o el Prestador de Servicios de Certificación 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 Autoridad Certificadora, sin responsabilidad alguna 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 Autoridad Certificadora no emitirá Certificados de firma electrónica a solicitantes que hayan usado deliberadamente un nombre cuyo derecho de uso no es de su propiedad; asimismo no verificará con 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 la Autoridad Certificadora o el Prestador de Servicios de Certificación.

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, la Autoridad Certificadora o el Prestador de Servicios de Certificación se asegurarán de que el solicitante realmente posea 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

No estipulado.

3.1.9 Autenticación de la identidad de un individuo

La Autoridad Certificadora por sí o por conducto del Agente Certificador o Prestador de Servicios de Certificación recabará una serie de documentos para realizar una correcta verificación de la identidad del solicitante de Certificado de firma electrónica, bajo consentimiento explícito.

Tratándose de la primera inscripción, el solicitante deberá acudir a las oficinas dispuestas para este fin por la Autoridad Certificadora.

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

Los documentos de identidad podrán ser cualquiera de los siguientes:

- Cartilla del Servicio Militar Nacional.
- Pasaporte expedido por la Secretaría de Relaciones Exteriores.
- Cédula Profesional expedida por la Secretaría de Educación Pública.
- Credencial de Elector expedida por el Instituto Federal Electoral.
- Identificación oficial expedida por el Gobierno Federal, Estatal o Municipal, incluyendo el Gobierno del Distrito Federal, que cuente con fotografía, firma y CURP del Titular.

Los documentos probatorios de identidad podrán ser:

- Copia certificada de Acta de nacimiento
- Documento migratorio
- Carta de naturalización
- Certificado de nacionalidad mexicana

3.1.10 Autenticación de la identidad de una Organización

No estipulado.

3.1.11 Criterios para operar con Autoridades Certificadoras externas

A la entrada en vigor de la presente DPC la Autoridad Certificadora podrá establecer 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

El titular de un Certificado de firma electrónica emitido por la Autoridad Certificadora deberá tramitar un nuevo certificado al término de su fecha de vigencia, con el fin de mantener su continuidad en el uso de su firma electrónica.

En consecuencia, el titular generará un nuevo par de claves que reemplazarán a las que estén próximas a perder su vigencia. Este procedimiento se denominará “Renovación de Claves y Certificado de firma electrónica”.

La Autoridad Certificadora verificará que la información proporcionada por el solicitante durante la primera inscripción continúa siendo válida; además, comprobará su identidad antes de emitir un nuevo Certificado de firma electrónica.

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

El apartado anterior sólo será aplicable si la renovación es acompañada de una sustitución de Certificado de firma electrónica.

La Autoridad Certificadora podrá negar la renovación del Certificado de firma electrónica en los siguientes supuestos:

- Si el Certificado de firma electrónica fue emitido sin la autorización del individuo nombrado en el campo *Nombre de Sujeto*.
- Si 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.*
- Si descubre que la información proporcionada en la solicitud de Certificado de firma electrónica es falsa.

3.4 Solicitud de Revocación

La solicitud de revocación se realizará personalmente por el titular del Certificado de firma electrónica o por el superior jerárquico, según se trate, mediante los dos procedimientos establecidos por la Autoridad Certificadora, sin perjuicio de cualquier otro que pudiera disponer con posterioridad.

Para el primer procedimiento 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, la Autoridad Certificadora pone a disposición del titular de Certificado de firma electrónica las oficinas debidamente equipadas para realizar la revocación del Certificado de firma electrónica, donde el titular acudirá personalmente y presentará la solicitud de revocación de Certificado de firma electrónica.

La documentación necesaria para llevar a cabo la revocación por el segundo procedimiento es:

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

La Autoridad Certificadora 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 la Autoridad Certificadora o el Prestador de Servicios de Certificación procedan con la solicitud de revocación.

En ambos casos, la comunicación entre la autoridad certificadora o Prestador de Servicios de Certificación y el titular del Certificado de firma electrónica se realizará de forma telemática o de forma verbal según sea el caso.

4 REQUERIMIENTOS DE OPERACIÓN PARA EL CICLO DE VIDA DE LOS CERTIFICADOS

4.1 Solicitud de Certificados de firma electrónica

La Autoridad Certificadora sólo aceptará solicitudes de Certificado de firma electrónica respecto de los sujetos señalados como solicitantes en el cuerpo de la presente DPC.

Dicha autoridad podrá rechazar aquellas solicitudes de Certificado de firma electrónica que incumplan con algún requisito dispuesto en Ley sobre el Uso de Medios Electrónicos y Firma Electrónica para el Estado de Guanajuato y sus Municipios. En este caso, informará mediante oficio las razones por las que se rechaza la solicitud.

4.1.1 Solicitud de Certificados de firma electrónica para un Prestador de Servicios de Certificación

No estipulado.

4.1.2 Tramitación de las solicitudes de Certificados de firma electrónica

Para obtener un Certificado de firma electrónica el solicitante deberá completar el procedimiento de enrolamiento conforme a lo siguiente:

1. Los particulares, en los casos autorizados en esta DPC, concertarán una cita con la Autoridad Certificadora, Prestador de Servicios de Certificación o Agente Certificador, ya personalmente, por teléfono o correo electrónico, y confirmarán su asistencia vía telefónica dos días hábiles antes de su cita; sin perjuicio de que la solicitud pueda ser atendida inmediatamente de existir la posibilidad.

   Los servidores públicos del Poder Judicial serán citados por el Consejo o la Secretaría General para que acudan ante la Autoridad Certificadora, Prestador de Servicio de Certificación o Agentes Certificadores en la fecha, lugar y hora que se determinen, a efecto de realizar el trámite de solicitud de Certificado de firma electrónica correspondiente; sin perjuicio de que en casos urgentes acudan directamente ante la Autoridad Certificadora, Prestador de Servicio de Certificación o Agentes Certificadores.

2. El solicitante firmará autógrafamente la solicitud de firma electrónica que será proporcionada en las oficinas de la Autoridad Certificadora, Prestador de Servicios de Certificación o Agente Certificador.

   En caso de que se firme de aceptación se continúa con el trámite, en caso contrario, se cancela.

3. Los particulares solicitantes generarán los archivos necesarios ***.REQ** y ***.KEY** en el equipo de cómputo localizado en las oficinas de la Autoridad Certificadora, Prestador de Servicios de Certificación o Agente Certificador, capturando los datos requeridos por el sistema.

   Tratándose de los servidores públicos del Poder Judicial, generarán los archivos mencionados a través del programa correspondiente instalado en los equipos de cómputo de la unidad jurisdiccional o administrativa de su adscripción; sin perjuicio de que en casos urgentes lo hagan conforme al párrafo precedente.

   En todo caso el solicitante deberá guardar los archivos de que se habla en un dispositivo electrónico de almacenamiento USB o cualquier otro que disponga la Autoridad Certificadora.

4. La Autoridad Certificadora, Prestador de Servicios de Certificación o Agente Certificador:

   - Revisará los datos referentes a la CURP y el RFC.
   - Verificará y validará, en su caso, que los documentos de identidad proporcionados correspondan al solicitante.
   - Verificará el estatus de los certificados con los que cuenta el solicitante.

   En caso de no cumplirse con los requisitos de identificación y autenticación del solicitante, se comunicará a éste la imposibilidad de continuar con el trámite.

5. Una vez realizada la certificación (generación del archivo ***.CER**), la Autoridad Certificadora, Prestador de Servicios de Certificación o Agente Certificador generará el archivo **PKCS12** correspondiente al solicitante y lo almacenará en el dispositivo electrónico autorizado para tal efecto (Token, USB, etc.).

6. El solicitante firmará la carta de confidencialidad y responsabilidad respectiva.

7. La Autoridad Certificadora, Prestador de Servicios de Certificación o Agente Certificador expedirá el comprobante de emisión de Certificado de firma electrónica y lo entregará al solicitante junto con el dispositivo de almacenamiento electrónico correspondiente.

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

La Autoridad Certificadora, el Prestador de Servicios de Certificación o el Agente Certificador resolverán sobre el otorgamiento o no del Certificado de firma electrónica dentro de un término no mayor a tres días hábiles contados a partir de la fecha de recepción de la solicitud.

Si la solicitud fuese confusa o incompleta, se requerirá al solicitante para que en un término de cinco días hábiles posteriores a su recepción, la aclare o complete, apercibido de que de no hacerlo, se tendrá por no presentada la solicitud.

Si transcurrido el término que se señala en el primer párrafo no se resuelve nada respecto a la solicitud, ésta se entenderá resuelta en sentido negativo.

4.2 Emisión de Certificados de firma electrónica

4.2.1 Actuación de la Autoridad Certificadora durante la emisión de los Certificados de firma electrónica

Durante la emisión de los Certificados de firma electrónica la Autoridad Certificadora:

- 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.
- Pone a disposición del suscriptor una copia del Certificado de firma electrónica en el sitio oficial de la Autoridad Certificadora, para que aquél 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 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 Autoridad Certificadora.

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 los derechos y obligaciones referidos, el solicitante deberá firmar de manera autógrafa el acuse de recibo que la Autoridad Certificadora le expide; en caso contrario, deberá expresar su rechazo y firmar de manera autógrafa en tal sentido para que la autoridad certificadora proceda con la revocación del certificado.

Posterior a que el solicitante haya aceptado y firmado de manera autógrafa el acuse de recibo, el ahora titular del Certificado de firma electrónica podrá utilizarlo en los casos autorizados en esta DPC.

4.4 Revocación de los Certificados de firma electrónica

Además de las causas señaladas en el Reglamento sobre el Uso de Medios Electrónicos y Firma Electrónica del Poder Judicial del Estado de Guanajuato, 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 de la Autoridad Certificadora 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.
- Porque la Autoridad Certificadora detecte que la clave privada asociada al Certificado de firma electrónica está duplicada.
- Por cualquier motivo en que se encuentre comprometida la integridad o confidencialidad de la clave privada (a solicitud del titular).

4.4.1 Actuación de la Autoridad Certificadora durante la revocación de los Certificados de firma electrónica

Durante la revocación del Certificado de firma electrónica se observará lo siguiente:

- El titular del Certificado de firma electrónica deberá llenar una solicitud de revocación proporcionada por la Autoridad Certificadora, donde aquél mencionará la causa de revocación y firmará al calce de manera autógrafa.

  Los datos que incluye esta solicitud son el nombre del titular, CURP, RFC y domicilio del titular.
- La Autoridad Certificadora 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, la Autoridad Certificadora aprobará la solicitud, revocará el 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.
- La Autoridad Certificadora deberá recabar el acuse de recibo del comprobante de 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, siendo importante subrayar que el proceso de revocación es irreversible.

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, la Dirección de Informática llevará 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 Autoridad Certificadora.
- El registro de los datos que entran en los distintos procedimientos asociados a los servicios de la Autoridad Certificadora.

4.5.1 Frecuencia con que se revisan los registros

La Dirección de Informática revisará los registros bimestralmente y generará los reportes necesarios, asimismo, tomará las medidas preventivas por los responsables de cada parte del proceso para corregir errores y prevenir fallas en los servicios que presta.

4.5.2 Periodo de disponibilidad de los registros de auditoría

Los registros de auditoría se mantendrán de forma local al menos durante los dos meses siguientes de haber sido generados, posteriormente se almacenarán con el debido procedimiento.

4.5.3 Mecanismos destinados para proteger los registros de auditoría

La Dirección de Informática dispondrá de mecanismos de seguridad para la debida protección de los registros de auditoría, con esto se evitará que puedan ser borrados, modificados o 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 Autoridad Certificadora, con el fin de mantener robusta la infraestructura de Tecnologías de la Información.

4.6 Respaldo

4.6.1 Planes de respaldo

La Dirección de Informática establecerá 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 Secretaría General del Consejo para respaldar el resto de los sistemas informáticos, información con carácter de confidencial y toda aquella que requiera ser almacenada por un periodo.

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

4.7 Recuperación

La Dirección de Informática dentro del procedimiento de recuperación estará a lo siguiente:

- Utilizará las copias de respaldo de la información más recientes.
- Solucionará los problemas relacionados con el Hardware (en caso de que existan).
- Restaurará el sistema operativo que soporta a la infraestructura de llave pública y debidamente configurado bajo los estándares que establece la Secretaría General del Consejo.

El Administrador de la Autoridad Certificadora y los demás roles encargados de recuperar los respaldos realizarán las siguientes acciones coordinadas:

- Establecerán todas las conexiones de red, así como las conexiones al módulo criptográfico encargado de resguardar el par de claves de la Autoridad Certificadora.
- Recuperarán los respaldos de los componentes de software involucrados en la operación de la infraestructura de llave pública.
- Reconfigurarán el software que opera la Autoridad Certificadora de acuerdo al manual proporcionado.
- Realizarán la restauración del módulo criptográfico.
- Verificarán que la restauración fue exitosa.

4.8 Destrucción de medios de almacenamiento

La Dirección e Informática incorporará mecanismos de seguridad que ayudan a 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 será debidamente documentado con el fin de registrar la baja en la bitácora de respaldos.

4.9 Protección de las bitácoras

La Dirección de Informática incorporará mecanismos de protección que controlan el acceso a los registros que se generan durante las operaciones de ésta, con el fin de detectar posibles violaciones a los procedimientos o entradas sospechosas e incidentes. En este sentido se estará a lo siguiente:

- Creará 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 Autoridad Certificadora

Antes de que llegue el vencimiento del Certificado de la Autoridad Certificadora, ésta observará lo siguiente:

- Dejará de emitir nuevos Certificados de firma electrónica 30 días antes de que expire la fecha de vigencia de su Certificado.
- La Secretaría General del Consejo realizará un comunicado donde indicará la transición que se efectuará para hacer el cambio de claves de la Autoridad Certificadora.
- Se llevará a cabo la transición del par de claves antiguo al nuevo par de llaves de la Autoridad Certificadora.
- Se realizará la recertificación de todos los servicios a los que se les emitió un certificado de la Autoridad Certificadora y que pertenecen a su Infraestructura de Llave Pública.
- Las nuevas solicitudes de Certificado de firma electrónica se procesarán una vez que la Autoridad Certificadora 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

En caso de que la Autoridad Certificadora requiera dar por terminada la operación y los servicios que ofrece, la Secretaría General del Consejo realizará todos los esfuerzos necesarios para notificar a sus suscriptores, a los usuarios y terceros aceptantes y a otras entidades afectadas; apegándose a los lineamientos que marcan la Ley sobre el Uso de Medios Electrónicos y Firma Electrónica para el Estado de Guanajuato y sus Municipios y la presente DPC.

5 CONTROLES DE SEGURIDAD FÍSICA, INSTALACIONES, GESTIÓN Y DE OPERACIÓN

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 aquéllos considerados como relevantes.

5.1.1 Ubicación física y construcción

La infraestructura de la Autoridad Certificadora estará en el Centro de datos ubicado en el Edificio Sede de los Jugados Civiles del Poder Judicial, en la ciudad de León, Guanajuato, México.

Este centro de procesamiento cumplirá con todas las exigencias de requerimientos de seguridad y auditoría de la Autoridad Certificadora. 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 Autoridad Certificadora 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 de datos.

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 de Informática 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 Secretaría General del Consejo mantiene copias de seguridad en instalaciones propias que cumplen con las medidas precisas para tal efecto.

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 Autoridad Certificadora procurará 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 alguna persona o 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 (servicios).
- Operador de Prestador de Servicios de Certificación (Agente certificador).
- Personal de base de datos.
- Personal de Infraestructura.

Los anteriores roles son considerados como confiables por la Autoridad Certificadora, sin embargo aquellas personas que quieran ser identificadas como de confianza tendrán que sujetarse a los controles establecidos en esta DPC.

Una misma persona no podrá ostentar dos roles marcados como incompatibles. Existe incompatibilidad de roles:

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

5.2.2 Número de personas requeridas por tarea

Para tener un control riguroso en ciertas tareas o procedimientos clasificados como de alta criticidad se implementará la separación de funciones con base en las responsabilidades de cada persona.

Se requiere reunir un mínimo de dos personas con capacidad profesional para realizar las tareas correspondientes a 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 dicho módulo.

5.2.3 Identificación y autenticación para cada usuario

Para todo el personal que requiera convertirse en persona de confianza, previamente será sometido a una verificación de identidad ante el personal encargado de los Recursos Humanos del Poder Judicial.

Para la verificación de identidad, el evaluado deberá acreditar la misma a través de los siguientes documentos:

- Credencial de Elector, Cartilla Militar o Pasaporte vigente.
- CURP con fotografía reciente emitido por RENAPO.

Asimismo, el personal encargado de administrar y operar los módulos criptográficos encargados de resguardar la clave privada de la Autoridad Certificadora, 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 cualidades y experiencia profesional

Todo el personal que presta sus servicios en el ámbito de la Autoridad Certificadora contará con el conocimiento, experiencia y formación suficiente para el mejor desempeño de sus funciones asignadas. Para ello, la Secretaría General del Consejo realizará el proceso debido durante la selección de personal buscando que el perfil profesional del empleado se adecue lo más posible a la descripción del puesto.

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

5.3.2 Requerimientos de capacitación

El personal encargado de la operación y administración de la infraestructura de la Autoridad Certificadora recibirá 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 la DPC vigente.
- 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.

5.3.3 Frecuencia y requerimientos de la capacitación

La frecuencia y los requerimientos estarán de acuerdo con lo establecido en la normatividad vigente de la Autoridad Certificadora así como con los procedimientos que indique la Secretaría General del Consejo.

5.3.4 Secuencia y frecuencia de rotación de tareas

No estipulado

5.3.5 Sanciones disciplinarias por acciones no autorizadas

Se tomarán las acciones disciplinarias adecuadas por acciones no autorizadas, negligentes, mal intencionadas u otras violaciones a la presente DPC, tomando en consideración las normas relativas al régimen de responsabilidad administrativa de los servidores públicos contenidas en la Ley Orgánica del Poder Judicial.

5.3.6 Requisitos de contratación de terceros

Se aplicará la normativa general del Poder Judicial para las contrataciones.

5.3.7 Documentación proporcionada al personal

Se proporcionará el acceso a la normatividad de seguridad vigente y la DPC.

6 CONTROLES DE SEGURIDAD TÉCNICA

La infraestructura de la Autoridad Certificadora 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 de la Autoridad Certificadora.

6.1 Generación del par de claves

El par de claves de la Autoridad Certificadora 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 la Autoridad Certificadora o Prestador de Servicios de Certificación.

6.2 Generación de la clave privada del titular

El par de claves del solicitante deberán ser generadas por él mismo, por tal motivo la Autoridad Certificadora pondrá a disposición del solicitante los sistemas criptográficos para la generación de su par de claves.

La Autoridad Certificadora o Prestador de Servicios de Certificación se aseguran 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

La Autoridad Certificadora pondrá a disposición del solicitante los sistemas criptográficos confiables que tramitan el requerimiento de certificación con el estándar PKCS#10.

6.4 Entrega de la clave pública de la Autoridad Certificadora a los usuarios y terceros aceptantes

La clave pública de la Autoridad Certificadora está incluida en el certificado de dicha autoridad.

El certificado de la Autoridad Certificadora deberá estar disponible en el repositorio electrónico especificado en esta DPC 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 Autoridad Certificadora 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 Autoridad Certificadora 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 la Autoridad Certificadora son: autenticación, firma electrónica de documentos y correos electrónicos.

Este uso deberá venir codificado dentro del Certificado Digital emitido a los suscriptores.

6.8 Protección de la clave privada

La Autoridad Certificadora 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 Autoridad Certificadora 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 Autoridad Certificadora se activa mediante la puesta en marcha del módulo criptográfico estipulado en el apartado correspondiente, 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 Autoridad Certificadora requiere la autenticación del titular ante el dispositivo 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 Autoridad Certificadora puede proceder a la desactivación de la clave privada de la Autoridad Certificadora 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 Autoridad Certificadora pueden 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 Autoridad Certificadora, 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 Autoridad Certificadora 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 Autoridad Certificadora 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.
- Si 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, la Autoridad Certificadora 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 Autoridad Certificadora 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 sólo 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 Autoridad Certificadora, 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

La Dirección de Informática incorpora sistemas confiables que cumplen con las medidas de seguridad y procesos de evaluación continua, establecidos por la Secretaría General del Consejo.

6.17 Controles de seguridad de la red

La infraestructura de red utilizada por los sistemas de la Autoridad Certificadora 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 establecidos por la Secretaría General del Consejo.

6.18 Perfil de certificado

Los certificados digitales emitidos por la Autoridad Certificadora 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 DESCRIPCIÓN DE LISTA DE CERTIFICADOS REVOCADOS Y OCSP

La Dirección de Informática emite listas de Certificados Revocados que se conforman de acuerdo el estándar descrito en el RFC 2459. Los datos que se incluyen en estas listas 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

La Dirección de Informática 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 la Lista de Certificados Revocados.

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 que determine la Autoridad Certificadora.

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 SOBRE LA ACTUALIZACIÓN Y NOTIFICACIÓN

La Secretaría General del Consejo será la responsable de determinar cualquier adecuación a la presente DPC, asimismo, será la encargada de aprobar las correcciones y actualizaciones que hubiera en un futuro de dichos documentos, apoyándose en todo momento por la Dirección de Informática.

El periodo de comentarios para cualquier corrección de la presente DPC será de quince días, comenzando en la fecha en que las enmiendas se publiquen en el repositorio de la Autoridad Certificadora.

Las correcciones, ajustes y modificaciones de la DPC se publicarán en el URL **http:// fec.poderjudicial-gto.gob.mx/dpc/** del repositorio perteneciente a la Autoridad Certificadora.

9 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 Secretaría General del Consejo no será revelado al público

9.2 Publicación de Información de Certificación

El contenido de la DPC estará publicado a título informativo en el repositorio designado para tales fines, bajo la siguiente dirección electrónica: **http:// fec.poderjudicial-gto.gob.mx/dpc/**.

Es responsabilidad de la Autoridad Certificadora la adopción de medidas de seguridad necesarias para garantizar la integridad, autenticidad y disponibilidad de dicha información.

Todos los suscriptores de la Autoridad Certificadora podrán tener acceso de forma fiable a la DPC generada, accediendo a la siguiente dirección electrónica: **http://fec.poderjudicial-gto.gob.mx/dpc/**.

La información ahí publicada se encuentra aprobada y firmada por la Secretaría General del Consejo.

Las Listas de Certificados Revocados emitidas estarán firmadas electrónicamente por la Autoridad Certificadora del Poder Judicial y estarán disponibles para usuarios y terceros aceptantes.

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://fec.poderjudicial-gto.gob.mx:8082/.**