Declaración de Prácticas y Políticas de Certificación del Tribunal de Justicia Administrativa de Michoacán de Ocampo

Contenido

1. INTRODUCCIÓN

La Ley de Firma Electrónica Certificada del Estado de Michoacán de Ocampo tiene por objeto regular el uso de medios electrónicos y de la misma firma electrónica, regular los procedimientos para su generación, certificación y de los servicios conexos, lo que permitirá 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, los ayuntamientos y los organismos públicos autónomos, a efecto de que éstos promuevan el uso de medios electrónicos y firma electrónica en sus actos jurídicos.

El Código de Justicia Administrativa del Estado de Michoacán de Ocampo, en su artículo 297 A, establece que el juicio administrativo podrá promoverse, substanciarse y resolverse en línea, a través del Sistema Informático del Tribunal (SIT) que deberá establecer y desarrollar el Tribunal.

Por tal motivo, el Tribunal de Justicia Administrativa de Michoacán de Ocampo, acatando la reforma al Código de Justicia Administrativa del Estado de Michoacán de Ocampo, acordó implementar una "Infraestructura de Llave Pública" que dotará de certificados de firma electrónica a los funcionarios jurisdiccionales o administrativos que integran a dicho Tribunal y que serán usuarios o administradores del Juicio en Línea, así como las personas físicas o morales por conducto de sus representantes legales, que sean susceptibles de ser actoras o demandadas, terceros interesados, autorizados de las partes, peritos, peritos terceros, y en los casos permitidos en el Código de Justicia Administrativa del Estado de Michoacán de Ocampo, los Lineamientos y la presente Declaración de Prácticas y Políticas de Certificación de la Autoridad Certificadora (**DPC**), para la promoción de juicios administrativos en línea, mediante el uso de medios electrónicos y con el respaldo de la firma electrónica certificada.

El presente documento incluye la Declaración de Prácticas y Políticas de Certificación que representan y orientan las actividades del Tribunal de Justicia Administrativa de Michoacán de Ocampo, como Autoridad Certificadora, 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 las acciones y controles de la Autoridad Certificadora.

1.1 Alcance de las Políticas de Certificados

Las políticas de certificación contenidas en éste 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.

Permitiendo que electrónicamente se autentique la identidad del firmante, asegurando la integridad de los documentos firmados electrónicamente y se evite el rechazo de los mismos.

1.2 Definiciones y Acrónimos

Término	**Definición**
Agente Certificador	Servidor público del Tribunal facultado para prestar servicios relacionados con la Firma Electrónica Certificada y que expide certificados electrónicos.
Autoridad Certificadora	El Tribunal de Justicia Administrativa de Michoacán de Ocampo.
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.
Certificado de Firma Electrónica	El documento firmado electrónicamente por la Autoridad Certificadora mediante el cual se confirma el vínculo existente entre el firmante y la firma electrónica, confirmando su identidad.
Dispositivo de creación de firma electrónica certificada	El programa o sistema informático que sirve para aplicar los datos de creación de firma electrónica certificada.
Dispositivo de verificación de firma electrónica	El programa o sistema informático que sirve para aplicar los datos de verificación de firma electrónica.
DPC	La Declaración de Prácticas y Políticas de Certificación.
Firma electrónica	La firma electrónica certificada como el conjunto de datos electrónicos integrados o asociados inequívocamente a un mensaje, que permite asegurar la integridad de ésta y la identidad del firmante y que

	ha sido certificada por la Autoridad Certificadora en términos de la Ley de Firma Electrónica Certificada del Estado de Michoacán de Ocampo.
Firmante	La persona que hace uso de su firma electrónica certificada.
Código	Código de Justicia Administrativa del Estado de Michoacán de Ocampo.
Ley	La Ley de Firma Electrónica Certificada del Estado de Michoacán de Ocampo.
Pleno	El Pleno del Tribunal de Justicia Administrativa de Michoacán de Ocampo.
Tribunal	El Tribunal de Justicia Administrativa de Michoacán de Ocampo.

1.3 Identificación del documento

Nombre del documento	La Declaración de Prácticas y Políticas de Certificación de la Autoridad Certificadora.
Versión del documento	1.0
Estado del documento	En vigor
Fecha de emisión	DD/MM/AAAA
Fecha de caducidad	DD/MM/AAAA
Sitio electrónico de la DPC	www.tjamich.gob.mx

1.4 Personas y Entidades Participantes

Las personas y entidades participantes son:

El Tribunal en su carácter de Autoridad Certificadora.

El Tribunal, por conducto de la Secretaría General de Acuerdos, apoyada por la Coordinación de Informática.

Cualquier otro prestador de servicios de certificación autorizado por la Autoridad Certificadora.

Las personas físicas o morales por conducto de sus representantes legales, que sean susceptibles de ser actoras o demandadas, terceros interesados, autorizados de las partes, peritos, peritos terceros, aceptantes de los Certificados de Firma Electrónica emitidos por El Tribunal como Autoridad Certificadora.

1.4.1 Autoridad Certificadora

El Tribunal es la Autoridad Certificadora, quien realizará ésta función por conducto de la Secretaría General de Acuerdos con apoyo en la Coordinación de Informática.

La Secretaría General de Acuerdos, a través del personal que designe para tal efecto, podrá ejercer directamente las funciones inherentes a la Autoridad Certificadora; también podrá delegarlas en los 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 Tribunal es la siguiente:

Nombre Distintivo	CN = TRIBUNAL DE JUSTICIA ADMINISTRATIVA DEL ESTADO DE MICHOACÁN DE OCAMPO OU = SECRETARÍA GENERAL DE ACUERDOS O = TRIBUNAL DE JUSTICIA ADMINISTRATIVA DEL ESTADO DE MICHOACÁN DE OCAMPO C = MX, S = MICHOACÁN L = MICHOACÁN PostalCode = 58190
Número de serie	30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 31
Periodo de validez	Desde DD/MM/AAAA 00:00:00 p.m. hasta DD/MM/AAAA 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

1.4.2 Administradores / Operadores de la Autoridad Certificadora

Área comisionada como responsable de la Autoridad Certificadora

Nombre	Secretaría General de Acuerdos del Tribunal de Justicia Administrativa Michoacán de Ocampo
Correo electrónico	juicioenlinea@tjamich.gob.mx

Dirección	Av. Francisco I. Madero Pte. #1622
Teléfono	(443)3152726 ext. 113.
Teléfono	(443)3152726 ext. 104

1.4.3 Agentes Certificadores y prestadores de servicio de certificación

El Titular de la Secretaría General de Acuerdos con apoyo del personal que para el efecto se designe, así como el personal que se designe en la sede de las defensorías foráneas del Tribunal, 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 extinción de los Certificados de Firma Electrónica correspondientes.

La Coordinación 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.

1.4.4 Solicitante y Titular del Certificado de Firma Electrónica

El solicitante es el servidor público o el particular en los casos autorizados en la presente 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 la presente DPC a favor del cual se ha otorgado el Certificado de Firma Electrónica.

1.5 Uso de los Certificados de Firma Electrónica

1.5.1 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 Tribunal, sólo podrán ser usados para:

Firmar electrónicamente las actuaciones jurisdiccionales y comunicaciones procesales cuando la Ley, el Código y los Lineamientos para la utilización del Juicio en Línea así lo autoricen.

Firmar electrónicamente actos, convenios, comunicaciones, trámites y procedimientos de naturaleza administrativa dentro de un Juicio, que correspondan a su esfera de competencia, autorizados por el Código, la Ley, los Lineamientos o el Pleno.

Los Certificados de Firma Electrónica emitidos por la Autoridad Certificadora a favor de personas físicas o morales por conducto de sus representantes legales que sean susceptibles de ser actoras o demandadas, terceros interesados, autorizados de las partes, peritos, peritos terceros, sólo podrán ser usados para:

Firmar electrónicamente actos y trámites autorizados por el Código, la Ley, los Lineamientos o el Pleno, cuando requieran de la Firma Electrónica Certificada.

Firmar electrónicamente la demanda, promociones o los actos procesales que les correspondan en su carácter de parte en los procesos seguidos ante el Tribunal, dentro del Juicio en Línea y cuando la Ley establezca el uso de la Firma Electrónica Certificada para esos casos.

1.5.2 Limitaciones y restricciones en el uso de los Certificados de Firma Electrónica

Los Certificados de Firma Electrónica emitidos por la Autoridad Certificadora se sujetarán a las disposiciones contenidas en la Ley y 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 rechazo 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, pues fue diseñado únicamente para la substanciación y resolución del proceso administrativo que se lleva a cabo en el Tribunal.

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.

1.5.3 Algoritmos y Parámetros Utilizados

Los Algoritmos de Firma son RSA con digestión **SHA-1**, los tamaños de claves son de al menos 2048 bits.

1.6 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 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.

2. 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 usuario con su clave pública mediante la expedición de un Certificado de Firma Electrónica, de conformidad con la Ley.

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

No obstante lo anterior, se exige que la Autoridad Certificadora lleve a cabo revisiones regulares al Agente certificador 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 la presente 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, verificando la vigencia y el estado de cada uno de los Certificados de Firma Electrónica de dicha cadena.

El personal encargado de proporcionar los sistemas donde se integre la Firma Electrónica Certificada, deberá conocer e informarse sobre las políticas de certificados y la presente DPC publicadas por la Autoridad Certificadora.

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

I. Realizar la publicación de la presente DPC en el sitio electrónico designado;
II. Comunicar cualquier cambio o adecuación de la presente DPC;

III. Utilizar sistemas y productos fiables que estén protegidos contra toda alteración, que aseguren la seguridad criptográfica de los procesos de certificación;

IV. Atender las solicitudes de Certificados de Firma Electrónica en un tiempo razonable, no mayor a 3 días hábiles;

V. Aprobar o rechazar las solicitudes de acuerdo a lo que marca la DPC vigente;

VI. Proporcionar la infraestructura operacional, servicios de certificación, servicios de extinción de certificados y servicios de validación de estatus de los Certificados de Firma Electrónica;

VII. Usar productos confiables y sistemas protegidos contra manipulaciones o modificaciones no autorizadas, que pueden asegurar su seguridad técnica y criptográfica;

VIII. 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;

IX. Conservar por medios electrónicos toda la información y documentos relacionados con los Certificados de Firma Electrónica emitidos durante un lapso de al menos quince años desde su emisión, en particular para verificar las firmas hechas usando los Certificados de Firma Electrónica ya mencionados;

X. Publicar su Certificado de Firma Electrónica de Autoridad Certificadora en el micro sitio del Juicio el Línea;

XI. Realizar sus operaciones de conformidad con la presente DPC;

XII. Aprobar o rechazar las solicitudes de Certificados de Firma Electrónica, conforme a la presente DPC;

XIII. Emitir Certificados de Firma Electrónica conforme a la información proporcionada por el solicitante siempre que esté libre de errores en la captura de datos;

XIV. Revocar Certificados de Firma electrónica de acuerdo a lo que establece la presente DPC, la Ley y los Lineamientos;

XV. Contar con un servicio de validación en línea para la verificación del estado de un Certificado de Firma electrónica determinado;

XVI. Publicar y actualizar la Lista de Certificados de Firma electrónica revocados, suspendidos o cancelados con la frecuencia estipulada;

XVII. Poner a disposición de sus suscriptores el Certificado de Firma Electrónica de la Autoridad Certificadora;

XVIII. No almacenar en ningún caso los datos de creación de llave o clave privada de los titulares de Certificados de Firma Electrónica; y,

XIX. 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 presente DPC, en la Ley, tratándose de las actividades que les hubieren sido encomendadas por la Autoridad Certificadora.

2.1.3 Obligaciones del Solicitante de Certificado de Firma Electrónica

Además de las establecidas en los Lineamientos y la Ley, los solicitantes de los Certificados de Firma Electrónica, tendrán las obligaciones siguientes:

I. Presentar un dispositivo USB de almacenamiento (nuevo o en blanco ya que será formateado previo a obtener la Firma Electrónica) 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 Tribunal por parte de la Autoridad Certificadora, según la disponibilidad presupuestaria;
II. Proporcionar toda la información que marca el procedimiento de solicitud de Certificado de Firma Electrónica;
III. Proporcionar información veraz para realizar la comprobación de su identidad;
IV. Notificar cualquier cambio de los datos proporcionados para la generación de su Certificado de Firma Electrónica durante el período de validez de éste; y,
V. Aceptar los términos y condiciones que la Autoridad Certificadora disponga en la DPC vigente para los Certificados de Firma Electrónica.

2.1.4 Obligaciones del Titular de Certificado de Firma Electrónica

Además de las establecidas en los Lineamientos y la Ley, el titular de Certificado de Firma Electrónica, tendrá las obligaciones siguientes:

I. Suministrar a los 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;
II. Conservar y utilizar de forma correcta el Certificado de Firma Electrónica y su clave privada de acuerdo con la normatividad vigente;
III. Proteger y custodiar su clave privada y su Certificado de Firma Electrónica asociado, empleando las medidas necesarias para evitar su pérdida, revelación, alteración o uso no autorizado;
IV. 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;
V. Respetar los términos y condiciones firmados durante la solicitud de Certificado de Firma Electrónica;

VI. Solicitar de manera oportuna al Prestador de Servicios de Certificación asociado a la Autoridad Certificadora la extinción de su Certificado de Firma Electrónica, revocación suspensión o cancelación según proceda, en caso de sospechar o tener conocimiento de que su clave privada ha sido robada, extraviada o sea conocida por terceros;

VII. Aceptar las restricciones impuestas a su clave privada y Certificado de Firma Electrónica, emitida por el Prestador de Servicios de Certificación de la Autoridad Certificadora;

VIII. 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;

IX. Solicitar se le expida constancia de la existencia y registro del Certificado de Firma Electrónica; y,

X. 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 de la Firma Electrónica Certificada

Son obligaciones del Usuario de la Firma Electrónica Certificada, las siguientes:

I. Verificar la validez de los Certificados de Firma Electrónica en el momento de realizar cualquier transacción basada en éstos;

II. 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;

III. Limitarse a los usos permitidos de los Certificados de Firma Electrónica estipulados en las extensiones de los mismos y en la presente DPC;

IV. Asumir su responsabilidad en la comprobación de la validez o revocación de los Certificados de Firma Electrónica en que confía;

V. Asumir su responsabilidad en la correcta verificación de las firmas electrónicas;

VI. Notificar cualquier hecho o situación fuera de lo común relativa al Certificado de Firma Electrónica y que pudiera tener como consecuencia su revocación, suspensión o cancelación; lo que hará a través de los medios electrónicos que disponga la Autoridad Certificadora;

VII. Conocer y aceptar toda restricción a la que está sujeto el Certificado de Firma Electrónica; y,

VIII. 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, la Ley o los Lineamientos.

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.

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.

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, revocación suspensión o cancelación 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, suspensiones, cancelaciones 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, los Lineamientos y en la Ley, 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 las siguientes circunstancias:

I. 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;

II. Por el uso indebido o fraudulento del directorio de Certificados de Firma Electrónica y Lista con el status de los Certificados de Firma electrónica, (revocados suspendidos o cancelados) emitidas por la Autoridad Certificadora;

III. Por el uso de los Certificados de Firma Electrónica que exceda los límites establecidos por los mismos y la presente DPC;

IV. Por el uso indebido de la información contenida en la Firma Electrónica Certificada;

V. Por el contenido de los mensajes de datos o documentos electrónicos firmados o cifrados mediante la Firma Electrónica Certificada;

VI. Por la falla técnica originada por cualquier motivo que produzca un mal funcionamiento del dispositivo USB u otro, donde se contenga el Certificado de Firma Electrónica y la correspondiente clave privada;

VII. En relación a acciones u omisiones del solicitante y/o titular de Certificado de Firma Electrónica;

VIII. Falta de veracidad de la información suministrada durante la solicitud de Certificado de Firma Electrónica;

IX. Retraso en la comunicación/notificación de las causas de revocación, suspensión o cancelación del Certificado de Firma Electrónica;

X. Ausencia de solicitud de revocación, suspensión o cancelación del Certificado de Firma Electrónica cuando proceda;

XI. 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;

XII. Uso del Certificado de Firma Electrónica fuera de su periodo de vigencia, o cuando la Secretaría General de Acuerdos le notifique la revocación, suspensión o cancelación del mismo;

XIII. Falta de comprobación de las restricciones que figuren en el Certificado de Firma Electrónica o en la presente DPC en cuanto a sus posibles usos; y,

XIV. Falta de comprobación de la revocación, suspensión, cancelación o pérdida de vigencia del Certificado de Firma Electrónica publicada en el servicio de consulta de la Lista de status de los Certificados 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 la presente DPC, los Lineamientos y la Ley, 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:

I. Ninguna persona distinta al titular ha tenido acceso a su clave privada;

II. 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;

III. Toda la información contenida en su Firma Electrónica Certificada es verdadera;

IV. La Firma Electrónica Certificada se utiliza exclusivamente para los actos autorizados conforme a lo estipulado en la presente DPC, Lineamientos y en Ley; y,

V. 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 al personal que para efecto se designe.

2.2.6. Responsabilidad del Usuario.

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 Michoacán, y concretamente por la Ley, el Código, Los Lineamientos y la demás normatividad aplicable en la materia.

2.3.1 Independencia

En el caso de que una o más estipulaciones de la presente 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 la presente 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 no 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.

2.4.3 Tarifas de acceso a la información relativa al estado de 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 la Lista de Certificados revocados, suspendidos o cancelados, a usuarios, sin embargo, la Autoridad Certificadora tiene derecho a cobrar una tarifa por entregar Listas de Certificados Revocados, Suspendidos o Cancelados, adaptadas a necesidades específicas, servicios de validación en línea 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.

2.4.4 Tarifas de otros servicios

La Autoridad Certificadora no aplicará ninguna tarifa por el servicio de información sobre la presente 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 la información de carácter público que está relacionada con la autoridad certificadora y los servicios que ofrece, conforme a lo siguiente:

I. Sitio electrónico para la consulta del Certificado de Firma Electrónica de la Autoridad Certificadora:

   a) URL: **http://tjamich.gob.mx/Juicio-En-Linea**

II. Sitio electrónico para la consulta de la DPC:

   a) URL: **http://tjamich.gob.mx/Juicio-En-Linea**

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

   a) URL: **http://tjamich.gob.mx/Juicio-En-Linea**

IV. Sitio electrónico para la revocación de Certificados:

   a) URL: **http://tjamich.gob.mx/Juicio-En-Linea**

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, Suspendidos o Cancelados

La Autoridad Certificadora generará la Lista de Certificados Revocados, Suspendidos o Cancelados en el momento en que tramita una petición 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 Coordinación de Informática podrá modificar, sustituir o eliminar información del repositorio y sitios electrónicos.

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

Los usuarios deberán dar su consentimiento al acuerdo de uso de Lista de Certificados Revocados, Suspendidos o Cancelados, 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 personales.

Se declara expresamente como información confidencial:

I. 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 presente DPC;
II. La clave privada de los usuarios de la Autoridad Certificadora;
III. Los registros de solicitud de Certificado de Firma Electrónica;
IV. Los registros de transacciones (registros completos y registros de auditoria de dichas transacciones);
V. Los planes de contingencia y planes de recuperación de desastres;

VI. 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; y,
VII. Toda la información clasificada como confidencial.

2.6.2 Información no confidencial

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

I. La contenida en la presente DPC;
II. La contenida en los Certificados de Firma Electrónica que emita la Autoridad Certificadora;
III. La Lista de Certificados Revocados, Suspendidos o Cancelados;
IV. La información sobre el estado de los Certificados de Firma Electrónica; y,
V. 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

La Secretaría General de Acuerdos y demás servidores públicos del Tribunal, 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 Tribunal, 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 Tribunal, 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 Tribunal de Justicia Administrativa del Estado de Michoacán de Ocampo.

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 (CN) del emisor y el del solicitante del certificado en los campos *Emitido por* y *Emitido para.*

El nombre distintivo (CN) de la Autoridad Certificadora contempla como mínimo los siguientes valores:

Nombre distintivo (CN) Certificado de Firma Electrónica de la Autoridad Certificadora.

CN	Tribunal de Justicia Administrativa del Estado de Michoacán de Ocampo
O	Tribunal de Justicia Administrativa del Estado de Michoacán de Ocampo
OU	Secretaría General de Acuerdos
C	Mx
S	Michoacán

El nombre distintivo (CN) del *Sujeto* (usuario) contempla los siguientes valores:

Nombre distintivo (DN) Certificado de Firma Electrónica del usuario.

CN	<NOMBRES><APELLIDO1> <APELLIDO2>
O	Tribunal de Justicia Administrativa de Michoacán de Ocampo
OU	Secretaría General de Acuerdos
C	MX
E	<CORREO ELECTRÓNICO>
SN	<RFC/CURP DEL TITULAR DEL CERTIFICADO>

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 *Sujeto* dentro del Certificado de Firma Electrónica.

La Autoridad Certificadora no permite que los usuarios 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 (CN) con semántica comúnmente entendible que permite al usuario 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 (CN) 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 (CN) del *Sujeto* del usuario son únicos, en 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 *Sujeto* de su Certificado de Firma Electrónica no infringe los derechos de propiedad intelectual de otros solicitantes, así la Autoridad Certificadora o el Agente Certificador 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 usuario 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.

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 se asegurará 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.

3.1.8 Autenticación de la identidad de un individuo

La Autoridad Certificadora por sí o por conducto del Agente Certificador 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:

I. Cartilla del Servicio Militar Nacional;
II. Pasaporte expedido por la Secretaría de Relaciones Exteriores;
III. Cédula Profesional con fotografía;;
IV. Credencial de Elector expedida por el Instituto Nacional Electoral; y,
V. Identificación oficial expedida por el Gobierno Federal, Estatal o Municipal, incluyendo el Gobierno de la Ciudad de México, que cuente con fotografía, firma y CURP del Titular.

Los documentos probatorios de identidad podrán ser:

I. Copia certificada de Acta de nacimiento;
II. Documento migratorio;
III. Carta de naturalización; y,
IV. Certificado de nacionalidad mexicana.

3.1.9 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:

I. 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); o,*
II. Si descubre que la información proporcionada en la solicitud de Certificado de Firma Electrónica es falsa.

3.4 Solicitud de Revocación, Suspensión o Cancelación

La autoridad certificadora iniciará de oficio el procedimiento de revocación, en cuanto a la suspensión y la cancelación, será el titular del Certificado de Firma Electrónica, apoderado jurídico, el superior jerárquico, según se trate o cualquier otro que disponga la ley y los lineamientos.

La documentación necesaria para llevar a cabo la suspensión o cancelación será:

I. Identificación oficial vigente con fotografía. (Credencial del IFE, CURP, Pasaporte o Cédula Profesional);
II. La Autoridad Certificadora validará los rasgos físicos de la fotografía de la identificación vigente con los rasgos físicos del usuario,; y,
III. Acta de nacimiento.

Una vez aprobada la identidad del usuario, este mismo debe llenar la solicitud y firmarla autógrafamente, para que la Autoridad Certificadora o el Prestador de Servicios de Certificación procedan con la solicitud.

La comunicación de la resolución emitida por la Autoridad Certificadora para el titular del Certificado de Firma Electrónica se realizará en términos de lo establecido en la Ley y los Lineamientos.

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. En este caso, informará por los medios establecidos por la Autoridad Certificadora, señalando las razones por las que se rechaza la solicitud.

4.1.1 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:

I. Los particulares, en los casos autorizados en ésta DPC, concertarán una cita con la Autoridad Certificadora o Agente Certificador, ya sea personalmente, por teléfono o correo electrónico; sin perjuicio de que la solicitud pueda ser atendida inmediatamente de existir la posibilidad;

   Los servidores públicos del Tribunal serán citados por la Secretaría General de Acuerdos para que acudan ante la Autoridad Certificadora, 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 o Agentes Certificadores;

II. El solicitante firmará autógrafamente la solicitud de Firma Electrónica Certificada que será proporcionada en las oficinas de la Autoridad Certificadora o Agente Certificador;

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

III. Los particulares solicitantes acudirán a la Autoridad Certificadora o agente certificador para obtener los archivos *.CER y *.KEY.

Tratándose de los servidores públicos del Tribunal, el procedimiento será 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.

IV. La Autoridad Certificadora o Agente Certificador:
   a) Revisará los datos referentes a la CURP y el RFC, según sea el caso;
   b) Verificará y validará, en su caso, que los documentos de identidad proporcionados correspondan al solicitante; y,
   c) Verificará el estatus de los certificados con los que cuenta el solicitante (en caso de haber contado con alguno con anterioridad).

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.

V. Una vez realizada la certificación (generación del archivo *.CER), la Autoridad Certificadora o Agente Certificador generará el archivo correspondiente al solicitante y lo almacenará en el dispositivo electrónico requerido por la Autoridad Certificadora;

VI. El solicitante firmará la carta de confidencialidad y responsabilidad respectiva; y,

VII. 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.

4.1.2 Plazo para la tramitación de las solicitudes de Certificados de Firma Electrónica

La Autoridad Certificadora o el Agente Certificador resolverán de forma inmediata sobre el otorgamiento o no del Certificado de Firma Electrónica, si cumple o no con los requerimientos establecidos en la presente DPC.

Si la solicitud fuese confusa o incompleta, se requerirá al solicitante para que en un término de tres 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 párrafo anterior 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 declara que:

I. 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 incluyendo también la clave pública;
II. Protege la integridad y confidencialidad de los datos contenidos en la solicitud; y,
III. Realiza la notificación al usuario de la emisión de su Certificado de Firma Electrónica, tal y como se describe en el apartado 4.2.2.

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, suspensión o cancelación 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 ésta DPC.

4.4 Perdida de eficacia de los Certificados de Firma Electrónica

Además de las causas señaladas en la Ley y los Lineamientos, se puede solicitar la extinción de un Certificado de Firma Electrónica por cualquiera de las siguientes causas:

I. A solicitud expresa del titular;
II. A solicitud del superior jerárquico del servidor público, vía oficio con copia del mismo al interesado, indicando la causa de la extinción del certificado en cuestión;
III. Por incapacidad jurídica declarada por una autoridad competente;
IV. Por fallecimiento;
V. Por resolución judicial;

VI. Por incumplimiento del titular de sus obligaciones, previa comunicación de la Autoridad Certificadora especificando la causa, fecha y hora en que tendrá efecto la extinción;

VII. Por la falsedad o errores en la información proporcionada en la solicitud de Certificado de Firma Electrónica;

VIII. Porque la Autoridad Certificadora detecte que la clave privada asociada al Certificado de Firma Electrónica está duplicada; y,

IX. 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 extinción de los Certificados de firma electrónica

Durante la extinción del Certificado de Firma Electrónica se observará lo siguiente:

El titular del Certificado de Firma Electrónica deberá llenar una solicitud de suspensión o cancelación, según sea el caso en términos de la Ley, proporcionada por la Autoridad Certificadora, donde aquél mencionará la causa de extinción del Certificado de Firma Electrónica y firmará al calce de manera autógrafa.

Los datos que incluye ésta 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 extinción 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 y seguido el procedimiento, suspenderá o cancelará, conforme a la Ley, el Certificado de Firma Electrónica y emitirá el comprobante que respalda ésta transacción.

El comprobante incluye la fecha y hora de la extinción en cualquiera de su modalidad. El titular recibirá vía correo electrónico la información de extinción del certificado correspondiente.

La Autoridad Certificadora deberá recabar el acuse de recibo del comprobante.

4.4.2 Periodo de gracia de la solicitud de extinción

La extinción 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 extinción 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 Coordinación de Informática llevará el registro

de manera manual o automática de cualquier evento significativo relacionado con los siguientes eventos:

I. Administración del ciclo de vida del Certificado de Firma Electrónica; y,
II. La operación de la infraestructura que está 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 Coordinación de Informática revisará los registros trimestralmente 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 Coordinación 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 Coordinación 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 misma Coordinación, 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 podrán ser almacenadas de forma segura en sitios remotos debidamente custodiados.

4.7 Recuperación

I. La Coordinación de Informática dentro del procedimiento de recuperación estará a lo siguiente:

a) Utilizará las copias de respaldo de la información más recientes;
b) Solucionará los problemas relacionados con el Hardware (en caso de que existan); y,
c) Restaurar el sistema operativo que soporta a la infraestructura de llave pública y debidamente configurado.

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

a) Establecer todas las conexiones de red, así como las conexiones al módulo criptográfico encargado de resguardar el par de claves de la Autoridad Certificadora;
b) Recuperar los respaldos de los componentes de software involucrados en la operación de la infraestructura de llave pública;
c) Reconfigurar el software que opera la Autoridad Certificadora de acuerdo a los parámetros necesarios;
d) Realizar la restauración del módulo criptográfico; y,
e) Verificar que la restauración fue exitosa.

4.8 Destrucción de medios de almacenamiento

La Coordinación de 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 Coordinación 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:

I. Crear una bitácora de seguimiento que lleva el registro de los roles que han solicitado el acceso a las bitácoras;
II. El custodio de éstas bitácoras se asegura que el registro se lleve a cabo de forma debida, los datos que incluyen son:

a) Fecha de revisión;

b) Nombre de la persona autorizada que realizó la revisión;
c) Fecha de la bitácora que se está revisando; y,
d) Nombre que identifica la bitácora que se está revisando.

4.10 Cambio del par de claves de la Autoridad Certificadora

El cambio del par de claves de la Autoridad Certificadora solo se podrá dar por acuerdo de Pleno del Tribunal y se dará por los supuestos siguientes:

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

I. Por ataque de hackeo exitoso;
II. Por robo de la infraestructura que contenga el par de claves de la Autoridad Certificadora; y,
III. cualquier situación que determine el pleno que pone en riesgo la integridad de las mismas.

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 de Acuerdos realizará todos los esfuerzos necesarios para notificar a sus usuarios, apegándose a los lineamientos que marcan la Ley 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 del Tribunal de Justicia Administrativa Michoacán de Ocampo, en la ciudad de Morelia, Michoacán, México.

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

5.1.2 Acceso físico

El acceso físico es registrado 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 respaldo de energía que proporciona alimentación, por un tiempo determinado, así como sistema 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 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 Secretaría Administrativa 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 Coordinación de Informática 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:

I. Administradores de sistemas;
II. Administradores y operadores del módulo criptográfico;
III. Administrador de la PKI (servicios);
IV. Agente certificador;
V. Personal de base de datos; y,
VI. 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 la presente DPC.

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 Tribunal.

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

I. Credencial de Elector;
II. Cartilla Militar; o,
III. Pasaporte vigente.

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 Coordinación de Recursos Humanos con apoyo con el área que corresponda 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:

I. Conceptos básicos de PKI;
II. Responsabilidades de la posición;
III. Entrega de una copia de la DPC vigente;
IV. Uso y operación del hardware / software utilizado;
V. Procedimientos de seguridad para cada rol;
VI. Procedimientos para la recuperación de la operación en caso de algún desastre; y,
VII. 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 de Acuerdos.

5.3.4 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.

5.3.5 Requisitos de contratación de terceros

Se aplicará la Ley de Adquisiciones, Arrendamientos y Prestación de Servicios Relacionados Con Bienes Muebles E Inmuebles Del Estado De Michoacán De Ocampo

5.3.6 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 utilizará 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; asimismo se deberán utilizar estos dispositivos para generar la firma de los certificados digitales que emite la Autoridad Certificadora o Agentes Certificadores.

6.2 Generación de la clave privada del titular

El par de claves del solicitante deberán ser generadas por el Agente Certificador.

La Autoridad Certificadora se asegurará 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 al momento de su entrega.

6.3 Entrega de la clave pública de la Autoridad Certificadora a los usuarios

La Autoridad Certificadora entregará al solicitante en el dispositivo electrónico el par de claves y se le entregará el comprobante que deberá firmar autógrafamente de conformidad con la misma.

6.4 Tamaño de las claves

El tamaño de las claves que la Autoridad Certificadora proporciona tiene una fortaleza, en cuanto a seguridad se refiere, del ciclo de vida que establece la Ley.

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

La clave pública de la Autoridad Certificadora y usuarios está generada y codificada dentro de módulos criptográficos adecuados y conforme a la normatividad vigente.

6.6 Usos admitidos de las claves

Los usos admitidos de la clave para cada certificado emitido por la Autoridad Certificadora son: autenticación y firma electrónica de documentos.

6.7 Protección de la clave privada del usuario

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 usuarios son protegidas por ellos mismos, el Agente Certificador no guarda copia alguna de la clave privada, por lo tanto los usuarios deberán incorporar al menos las siguientes medidas para proteger la clave privada:

I. Incorporar mecanismos de seguridad que ofrezcan la protección física de la estación de trabajo del usuario;
II. Incorporar políticas de seguridad que contemplen la protección de acceso a la estación de trabajo, incluyendo cuando éste es desatendido por el usuario; y,
III. Posesión y conocimiento de la clave de acceso a la clave privada únicamente por el usuario del par de claves privada y pública.

6.8 Método de activación de la clave privada

La clave privada de la Autoridad Certificadora estará activa mientras tanto la infraestructura de la llave pública esté en ejecución.

La activación de las claves privadas de los usuarios de la Autoridad Certificadora se dará en el momento de la entrega de la clave.

6.9 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. En caso de actualización y mejoras se publicará en los medios proporcionados para tal efecto en el sitio web del juicio en línea.

6.10 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.

6.11 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.

6.12 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 Ley y una vez transcurrido no se pueden continuar utilizando.

6.13 Generación e instalación de los datos de activación

En el caso de los usuarios, 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 ésta contraseña se deben tomar en cuenta las siguientes normas de seguridad:

I. Debe ser generada por el usuario;
II. Debe contener al menos 8 caracteres;
III. Debe estar construida con caracteres alfanuméricos; y,
IV. Debe contener mayúsculas y minúsculas

6.14 Protección de los datos de activación.

Para los usuarios, la contraseña de acceso a su clave privada debe ser conocida sólo por ellos, debe ser personal e intransferible. Ésta 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:

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

6.15 Controles de seguridad informática

La Coordinación de Informática incorpora sistemas confiables que cumplen con las medidas de seguridad y procesos de evaluación continua.

6.16 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 Coordinación de Informática.

6.17 Perfil de certificado

Los certificados digitales emitidos por la Autoridad Certificadora cumplen con las siguientes normas:

I. Recomendación X.509 ITU-T (2005):
    a) Tecnología de información;
    b) Interconexión de sistemas abiertos; y,
    c) El directorio: plataforma de autenticación.
II. RFC 3280:

    Internet X.509 Infraestructura de llave pública perfil de certificado y LCR.

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

a) Versión;
b) Número de serie, este valor es único para cada certificado digital emitido;
c) Nombre del algoritmo de firma utilizado;
d) Nombre Distinguido del emisor;

e) Fecha de validez de inicio, el formato de la fecha está codificado en UTC (tiempo coordinado universal);
f) Fecha de validez de término, el formato de la fecha está codificado en UTC (tiempo coordinado universal);
g) Nombre Distinguido del sujeto; y,
h) Clave pública del sujeto.

IV. Las extensiones utilizadas son:
a) Auth. Key Identifier;
b) Subject Key Identifier;
c) Auth. Information Access;
d) Certificate Policies;
e) Basic Constraints; y,
f) Key Usage.

7. DESCRIPCIÓN DE LISTA DE CERTIFICADOS REVOCADOS, SUSPENDIDOS O CANCELADOS

La Secretaría General de Acuerdos emite listas de Certificados Revocados, Suspendidos o Cancelados que se conforman de acuerdo el estándar descrito en el RFC 2459. Los datos que se incluyen en estas listas son:

I. La versión;
II. El algoritmo de firma digital usado;
III. 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;
IV. Fecha y hora de emisión de la lista de status de los Certificados de Firma Electrónica;
V. Fecha y hora de vigencia de la lista de status de Certificados de Firma Electrónica Revocados;
VI. Fecha de cuando se emitirá la nueva lista de status de Certificados de Firma Electrónica; y,
VII. El listado de los Certificados de Firma Electrónica que contiene el número de serie y fecha de revocación, suspensión o cancelación 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. Las normas aplicables.

A través de este proceso se determina el estado actual de un Certificado de Firma Electrónica sin requerir el acceso a la Lista de status de Certificados.

Un sujeto que requiera consultar el estado de un Certificado de Firma Electrónica sólo debe de enviar una petición al servicio correspondiente, 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 usuario contar con los componentes de software / hardware necesarios para realizar la consulta.

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

8. SOBRE LA ACTUALIZACIÓN Y NOTIFICACIÓN

La Secretaría General de Acuerdos 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 Coordinación de Informática.

Las correcciones, ajustes y modificaciones de la DPC se publicarán en el URL http://jel. tjamich.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 de Acuerdos 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://jel.tjamich.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 usuarios de la Autoridad Certificadora podrán tener acceso de forma fiable a la DPC generada, accediendo a la siguiente dirección electrónica: http://jel.tjamich.gob.mx/dpc/.

La información ahí publicada se encuentra aprobada y firmada por la Secretaría General de Acuerdos.

Las Listas de status de Certificados emitidas estarán firmadas electrónicamente por la Autoridad Certificadora y estará disponible para usuarios.

La información sobre el estado de los Certificados de Firma Electrónica emitidos se podrá consultar a través del servicio de validación en línea, este servicio estará disponible en la siguiente dirección electrónica: http://jel.tjamich.gob.mx/.