PERIÓDICO OFICIAL

DEL GOBIERNO CONSTITUCIONAL DEL ESTADO DE MICHOACÁN DE OCAMPO

Fundado en 1867

Las leyes y demás disposiciones son de observancia obligatoria por el solo hecho de publicarse en este periódico. Registrado como artículo de 2a. clase el 28 de noviembre de 1921.

Director: Lic. José Juárez Valdovinos

Tabachín # 107, Col. Nva. Jacarandas, C.P. 58099 **SÉPTIMA SECCIÓN** **Tels. y Fax: 3-12-32-28, 3-17-06-84**

TOMO CLXXII	Morelia, Mich., Martes 16 de Julio de 2019	NÚM. 94

Responsable de la Publicación
Secretaría de Gobierno

DIRECTORIO

Gobernador Constitucional del Estado de Michoacán de Ocampo
Ing. Silvano Aureoles Conejo

Secretario de Gobierno
Ing. Carlos Herrera Tello

Director del Periódico Oficial
Lic. José Juárez Valdovinos

Aparece ordinariamente de lunes a viernes.

Tiraje: 50 ejemplares
Esta sección consta de 36 páginas

Precio por ejemplar:
$ 28.00 del día
$ 36.00 atrasado

Para consulta en Internet:
www.michoacan.gob.mx/noticias/p-oficial
www.congresomich.gob.mx

Correo electrónico
periodicooficial@michoacan.gob.mx

CONTENIDO

TRIBUNAL DE JUSTICIA ADMINISTRATIVA DEL ESTADO DE MICHOACÁN DE OCAMPO

ACUERDO DE PLENO POR EL QUE SE APRUEBA QUE EL TRIBUNAL DE JUSTICIA ADMINISTRATIVA DEL ESTADO DE MICHOACÁN DE OCAMPO ACTÚE COMO AUTORIDAD CERTIFICADORA PARA EMITIR LA FIRMA ELECTRÓNICA CERTIFICADA EN TÉRMINOS DE LA LEY DE FIRMA ELECTRÓNICA CERTIFICADA DEL ESTADO DE MICHOACÁN DE OCAMPO.

CONSIDERANDO

I. Conforme al artículo 95 de la Constitución Política del Estado Libre y Soberano del Estado de Michoacán de Ocampo y al precepto 143 del Código de Justicia Administrativa del Estado de Michoacán de Ocampo, el Tribunal de Justicia Administrativa del Estado de Michoacán de Ocampo es un órgano autónomo, independiente en sus resoluciones y de jurisdicción plena en materia administrativa con sujeción a los principios de igualdad, publicidad, audiencia y legalidad.

II. El 18 dieciocho de julio de 2017 dos mil diecisiete se publicó en el Periódico Oficial del Gobierno Constitucional del Estado de Michoacán de Ocampo, el Decreto Legislativo número 383 que contiene diversas reformas y adiciones al Código de Justicia Administrativa en materia de Juicio en Línea;

En virtud de la reforma aludida se prevé la promoción, substanciación y resolución del juicio administrativo en todas sus etapas, a través del Sistema Informático que deberá establecer y desarrollar el Tribunal de Justicia Administrativa, y que la firma electrónica permite actuar en el Juicio en Línea.

De igual manera, se estableció que la firma electrónica avanzada será proporcionada por el Tribunal de Justicia Administrativa a través de su Sistema Informático;

III. El 14 catorce de agosto del 2018 dos mil dieciocho, se publicó en el Periódico Oficial del Gobierno Constitucional del Estado de Michoacán de Ocampo, el Decreto Legislativo número 619, por el que se establece la entrada en vigor del Juicio en Línea a partir del dieciocho de julio de dos mil diecinueve;

IV. Para que los documentos digitales firmados electrónicamente adquieran plena validez, esto es, que brinden confianza, certidumbre y seguridad jurídica en la identificación de su autor, el certificado de firma electrónica avanzada expedido por una autoridad certificadora constituye un elemento indispensable, ya que además de distribuir una clave, sirve para asociar de manera segura y fiable, la identidad de una persona concreta a una clave privada determinada, es decir, permite identificar quién es el autor o emisor y asegura que el mensaje no ha sido manipulado o modificado durante la comunicación; y,

V. La Ley de Firma Electrónica Certificada del Estado de Michoacán de Ocampo que regula el uso de medios electrónicos y de la firma electrónica certificada en los actos, procedimientos y trámites que se lleven a cabo entre los sujetos obligados; que otorga el mismo valor jurídico a la firma electrónica certificada que a la firma autógrafa y que regula los procedimientos para la generación de la firma electrónica certificada, establece además en su artículo 2 fracción V que los sujetos obligados son los organismos públicos autónomos previstos en la Constitución Política del Estado y demás ordenamientos estatales; y en su artículo 14 que los mismos órganos autónomos son autoridades certificadoras en su respectivo ámbito de competencia; en cumplimiento a la reforma que establece el Juicio en Línea, el Tribunal de Justicia Administrativa del Estado de Michoacán de Ocampo ha implementado una infraestructura de llave pública para actuar como Autoridad Certificadora.

Por lo antes expuesto y para dar cumplimiento a la implementación para la promoción, substanciación y resolución del Juicio en Línea, el Pleno del Tribunal de Justicia Administrativa del Estado de Michoacán de Ocampo, emite el siguiente:

A C U E R D O

PRIMERO. El Tribunal de Justicia Administrativa del Estado de Michoacán de Ocampo actuará como **Autoridad Certificadora** para emitir la firma electrónica certificada a través del Sistema Informático del Tribunal (SIT), necesaria para promover, substanciar y resolver el Juicio en Línea conforme a lo dispuesto por el Código de Justicia Administrativa del Estado de Michoacán de Ocampo y la Ley de Firma Electrónica Certificada del Estado de Michoacán de Ocampo.

SEGUNDO. Todo trámite relacionado con la firma electrónica avanzada se realizará conforme a la Ley de Firma Electrónica Certificada del Estado de Michoacán de Ocampo; así como los Lineamientos para la utilización del Juicio en Línea ante el Tribunal de Justicia Administrativa del Estado de Michoacán de Ocampo, Declaración de Prácticas y Políticas de Certificación; Términos y Condiciones para la Utilización del Juicio en Línea y Aviso de Privacidad del Sistema Informático del Tribunal de Justicia Administrativa del Estado de Michoacán de Ocampo, que para tales efectos se expidan.

T R A N S I T O R I O S

PRIMERO. El presente Acuerdo entrará en vigor al día siguiente de su publicación en el Periódico Oficial del Gobierno Constitucional del Estado de Michoacán de Ocampo.

SEGUNDO. Para su debido conocimiento y cumplimiento, publíquese en el Periódico Oficial del Gobierno Constitucional del Estado de Michoacán de Ocampo, en los estrados del Tribunal de Justicia Administrativa del Estado de Michoacán de Ocampo.

Así lo acordaron por **UNANIMIDAD** de votos, los Magistrados que integran el Pleno del Tribunal de Justicia Administrativa del Estado de Michoacán de Ocampo, ante el Coordinador de Asuntos Jurídicos habilitado para ejercer funciones de Secretario General de Acuerdos que autoriza y da fe. (Firmado).

Así lo acordó el Pleno del Tribunal de Justicia Administrativa del Michoacán de Ocampo, en Sesión del día 11 once de julio de 2019 dos mil diecinueve.

EL SUSCRITO LICENCIADO EN DERECHO JORGE LUIS ARROYO MARES, COORDINADOR DE ASUNTOS JURÍDICOS HABILITADO PARA EJERCER LAS FUNCIONES DE SECRETARIO GENERAL DE ACUERDOS DEL TRIBUNAL DE JUSTICIA ADMINISTRATIVA DE MICHOACÁN DE OCAMPO, CON FUNDAMENTO EN LO DISPUESTO POR LOS ARTÍCULOS 145 FRACCIÓN I, 159 FRACCIÓN XVI, 164 ÚLTIMO PÁRRAFO Y 165 FRACCIONES I, VI Y XII DEL CÓDIGO DE JUSTICIA ADMINISTRATIVA DEL ESTADO DE MICHOACÁN DE OCAMPO, ASÍ COMO 30 FRACCIONES III Y VII DEL REGLAMENTO INTERIOR DEL TRIBUNAL DE JUSTICIA ADMINISTRATIVA DE MICHOACÁN DE OCAMPO.

C E R T I F I C A

QUE EL PRESENTE ACUERDO DE PLENO POR EL QUE SE APRUEBA QUE EL TRIBUNAL DE JUSTICIA

ADMINISTRATIVA DEL ESTADO DE MICHOACÁN DE OCAMPO ACTÚE COMO AUTORIDAD CERTIFICADORA PARA EMITIR LA FIRMA ELECTRÓNICA CERTIFICADA EN TÉRMINOS DE LA LEY DE FIRMA ELECTRÓNICA CERTIFICADA DEL ESTADO DE MICHOACÁN DE OCAMPO FUE APROBADO POR EL PLENO DEL TRIBUNAL DE JUSTICIA ADMINISTRATIVA DE MICHOACÁN DE OCAMPO, EN SESIÓN DEL DÍA 11 ONCE DE JULIO DE 2019 DOS MIL DIECINUEVE, POR UNANIMIDAD DE VOTOS DE LOS MAGISTRADOS SERGIO MECINO MORALES, PRESIDENTE Y TITULAR DE LA QUINTA SALA ESPECIALIZADA, ARTURO BUCIO IBARRA, TITULAR DE LA SEGUNDA SALA ADMINISTRATIVA, GRISELDA LAGUNAS VÁZQUEZ, TITULAR DE LA TERCERA SALA ADMINISTRATIVA, RAFAEL ROSALES CORIA, TITULAR DE LA CUARTA SALA ESPECIALIZADA Y CARLOS PAULO GALLARDO BALDERAS, MAGISTRADO POR MINISTERIO DE LEY DE LA PRIMERA SALA ADMINISTRATIVA.- MORELIA, MICHOACÁN DE OCAMPO, A 11 ONCE DE JULIO DE 2019 DOS MIL DIECINUEVE.- CONSTE. (Firmado).

Con fundamento en el artículo 74 de la Ley de Firma Electrónica Certificada para el Estado de Michoacán de Ocampo; Capítulo Décimo Cuarto bis del Código de Justicia Administrativa del Estado de Michoacán de Ocampo, artículo 15, fracciones VI, VIII y X, del Reglamento Interior del Tribunal de Justicia Administrativa del Estado de Michoacán de Ocampo, el Pleno de este órgano jurisdiccional expide los siguientes:

LINEAMIENTOS PARA LA UTILIZACIÓN DEL JUICIO EN LÍNEA ANTE EL TRIBUNAL DE JUSTICIA ADMINISTRATIVA DEL ESTADO DE MICHOACÁN DE OCAMPO

CAPÍTULO PRIMERO
DISPOSICIONES GENERALES

Objeto

Artículo 1. Los presentes Lineamientos son de carácter general y de observancia obligatoria para todos los usuarios del sistema para la promoción, substanciación y resolución del Juicio en Línea y los servidores públicos del Tribunal de Justicia Administrativa del Estado de Michoacán de Ocampo, y tienen por objeto:

I. Establecer el procedimiento para el acceso, operación y asistencia en la promoción, substanciación y resolución del proceso administrativo en su modalidad de Juicio en Línea; y,

II. Establecer las disposiciones reglamentarias, administrativas y técnicas a las que deberán sujetarse todos los usuarios y operadores del Tribunal, que hagan uso del mismo.

Glosario

Artículo 2. Además de lo previsto en el artículo 3 de la Ley de Firma Electrónica Certificada para el Estado de Michoacán de Ocampo, para efecto de los presentes Lineamientos se entenderá por:

I. Autoridad Certificadora: Al Tribunal de Justicia Administrativa de Michoacán de Ocampo;

II. Administrador: Al titular de la Coordinación de Informática del Tribunal, responsable de garantizar la integridad, veracidad, actualización y mantenimiento permanente de la información del Juicio en Línea y del propio Sistema Informático del Tribunal;

III. Agentes certificadores: Es la persona física autorizada por la autoridad certificadora para recibir los datos de los solicitantes, registrar, emitir, modificar, suspender o revocar los certificados de firma electrónica, así como intervenir en cualquiera de los procesos relacionados con los certificados de firma electrónica;

IV. Archivo electrónico: A la información contenida en texto, imagen, audio o video generada, enviada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología que forma parte del expediente electrónico, con el objeto de asegurar la identidad y la integridad de la información en el transcurso del tiempo;

V. Centro de atención de usuarios: A la oficina del Tribunal responsable de asesorar a los usuarios respecto del uso del Sistema Informático del Tribunal en todas sus modalidades;

VI. Certificado de firma electrónica: Al documento firmado electrónicamente por el Tribunal, mediante el cual se confirma el vínculo existente entre el firmante y la firma electrónica;

VII. Clave de acceso: Al conjunto único de caracteres alfanuméricos asignado por el Sistema Informático del Tribunal a los usuarios, como medio de identificación de las personas facultadas en el juicio en que promuevan para utilizar el sistema, y asignarles los privilegios de consulta del expediente respectivo o envío por vía electrónica de promociones relativas a las actuaciones procesales con el uso de la firma electrónica certificada;

VIII. Código: Al Código de Justicia Administrativa del Estado de Michoacán de Ocampo;

IX. Código de barras: A la técnica para el ingreso de datos al Sistema Informático del Tribunal, con equivalencia a la captura manual, mediante instrumentos aportados por la ciencia que permitan la incorporación de datos por imágenes formadas a través de combinaciones de barras y espacios paralelos, de anchos variables, que representen números que a su vez pueden ser leídos, descifrados y vinculados a los interesados por lectores ópticos o escáner;

X. Consulta electrónica de expedientes: Al acceso que realizan los usuarios al Sistema Informático del Tribunal mediante una contraseña, a los expedientes que contienen los procesos administrativos;

XI. Contraseña: Al conjunto único de caracteres

alfanuméricos, asignados de manera confidencial por el Sistema Informático del Tribunal a los usuarios, la cual permite validar la identificación de la persona a la que se le asignó una Clave de Acceso;

XII. Coordinación de Informática: A la Coordinación de Informática del Tribunal de Justicia Administrativa de Michoacán de Ocampo;

XIII. Coordinación de la Defensoría Jurídica: A la Coordinación de la Defensoría Jurídica del Tribunal de Justicia Administrativa de Michoacán de Ocampo;

XIV. Correo spam: Se refiere a mensajes electrónicos masivos no solicitados, no esperado o de remitentes desconocidos, habitualmente de tipo publicitario, enviados en cantidades masivas, generalmente por correo electrónico, cuyo objetivo es realizar un daño o un uso indebido de los medios y servicios electrónicos;

XV. Datos personales: Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información;

XVI. Defensoría Jurídica: Oficinas de la Defensoría gratuita establecidas en el Estado de Michoacán adscritas al Tribunal de Justicia Administrativa del Estado de Michoacán de Ocampo;

XVII. Depuración: A la desintegración material de documentos y/o transferencia de documentos electrónicos a un medio secundario a fin de liberar espacio en el Sistema Informático del Tribunal;

XVIII. Destinatario: A la parte, en términos del artículo 190 del Código, así como cualquier otro interviniente en el proceso administrativo, que autoriza o está obligado a que se le practiquen las notificaciones procesales vía electrónica, también en términos del Código;

XIX. Declaración de Prácticas y Políticas de Certificación: A la Declaración de Prácticas y Políticas de Certificación del Tribunal de Justicia Administrativa del Estado de Michoacán de Ocampo;

XX. Dirección de correo electrónico: Al sistema de comunicación a través de redes informáticas, señalado por las partes en el Juicio en Línea;

XXI. Encriptación: Al método que utiliza el proceso de firma electrónica para brindar seguridad a los usuarios de la misma, basado en un algoritmo indescifrable a simple vista;

XXII. Expediente electrónico: Al conjunto de información contenida en archivos electrónicos o documentos digitales que conforman el Juicio en Línea, independientemente de que sea texto, imagen, audio o video, identificado por un número específico;

XXIII. Firma Electrónica Avanzada: A la Firma Electrónica Certificada;

XXIV. Información: A los datos contenidos en los documentos o archivos que el Tribunal genere, obtenga, adquiera, transforme o conserve por cualquier título, en papel o medio electrónico;

XXV. Interesado: A todo aquél particular que tenga un interés respecto de un acto o procedimiento;

XXVI. Internet: Al conjunto de redes de comunicación interconectadas cuya finalidad es intercambiar información entre computadoras que se encuentren físicamente distantes;

XXVII. Jueces Administrativos: A los titulares de los Juzgados del Tribunal de Justicia Administrativa del Estado de Michoacán;

XXVIII. Juicio en la vía tradicional: El Juicio Administrativo que se substancia recibiendo las promociones y demás documentales en manuscrito o impresos en papel, y formando un expediente también en papel, donde se agregan las actuaciones procesales, incluso en los casos en que sea procedente la vía sumaria;

XXIX. Juicio en Línea: Al proceso contencioso administrativo en todas sus etapas, a través del Sistema Informático del Tribunal;

XXX. Ley: A la Ley de Firma Electrónica Certificada del Estado de Michoacán de Ocampo;

XXXI. Ley de Protección de Datos Personales: A la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo;

XXXII. Módulo de Registro: Al lugar en el que se lleva a cabo el registro, la modificación, convalidación, cancelación de los datos aportados por los usuarios del sistema, y entrega de la firma electrónica;

XXXIII. Notificación Electrónica: A la comunicación procesal a que se alude en términos del artículo 297 N, del Código;

XXXIV. Operador: Al Servidor Público del Tribunal que por su perfil, ámbito de competencia y demás cuestiones relativas a la función que desempeña, requiera utilizar o administrar el sistema;

XXXV. Promoción: A los escritos presentados por las partes para la substanciación del Juicio en Línea;

XXXVI. Secretaría: A la Secretaría General de Acuerdos del Tribunal de Justicia Administrativa del Estado de Michoacán de Ocampo;

XXXVII. Sistema Informático del Tribunal (SIT): Al conjunto de servicios electrónicos, implementado por el Tribunal para la realización de notificaciones vía electrónica, la consulta electrónica de expedientes y cualquier otro servicio

para el cumplimiento de su función;

XXXVIII. SIT: Al Sistema Informático del Tribunal;

XXXIX. Términos y condiciones: Al conjunto de disposiciones administrativas y técnicas previstas en la Ley y demás disposiciones que regulen el uso de los medios electrónicos y la firma electrónica, que deberán aceptar los usuarios o los interesados que tengan la intención de instar el proceso administrativo en la modalidad de Juicio en Línea;

XL. Tribunal: Al Tribunal de Justicia Administrativa del Estado de Michoacán de Ocampo;

XLI. Usuario: A cualquier persona física o moral o autoridad administrativa que, sin actuar como servidor público del Tribunal en funciones, sea parte en el proceso administrativo en su modalidad de Juicio en Línea y utilice el Sistema Informático del Tribunal para acceder y operar el Juicio en Línea en términos de los Lineamientos;

XLII. Vinculación al expediente: Al acceso de un usuario a un expediente de Juicio en Línea en trámite;

XLIII. Virus: Al programa o aplicación que tiene por objeto alterar o dañar el funcionamiento del equipo de cómputo, sistema o información, sin el permiso o el conocimiento del usuario; y,

XLIV. Web: Red global mundial basada en un sistema de documentos de hipertexto y/o hipermedios enlazados y accesibles a través de internet y conocido por sus siglas www (World Wide Web).

Interpretación

Artículo 3. La interpretación de las disposiciones establecidas en los presentes Lineamientos corresponderá al Pleno del Tribunal, bajo los principios previstos en el párrafo primero del artículo 5 del Código. Así como resolver cualquier situación técnica o administrativa no prevista.

CAPÍTULO SEGUNDO
REGISTRO AL SISTEMA INFORMÁTICO DEL TRIBUNAL

Registro al Sistema Informático

Artículo 4. Los interesados en instar el proceso administrativo en la modalidad de Juicio en Línea, deberán registrarse como usuarios del SIT, conforme a lo establecido en el Capítulo Tercero de estos Lineamientos.

Los interesados que ya tengan la calidad de usuarios, podrán acceder y usar el Juicio en Línea, sujetándose a las disposiciones contenidas en el Código, en la Ley, los presentes Lineamientos; los Acuerdos Generales de Pleno y demás disposiciones legales que resulten aplicables al uso de medios electrónicos y firma electrónica.

Artículo 5. Para la tramitación del Juicio en Línea los interesados deberán registrarse a través del Sistema Informático del Tribunal.

Trámite electrónico

Artículo 6. Para realizar el trámite en forma electrónica, el interesado accederá al Sistema Informático del Tribunal, donde previa aceptación de los términos y condiciones, completará los campos de información correspondientes.

Alcances del registro y aceptación de los términos y condiciones

Artículo 7. La aceptación de los términos y condiciones, así como del ingreso de la información correspondiente a la solicitud de acceso, expresará la voluntad del interesado para instar el proceso administrativo en su modalidad de Juicio en Línea.

La aceptación de los términos y condiciones dará lugar a tenerlos por leídos y comprendidos plenamente; en similar circunstancia, el aviso de privacidad del Tribunal.

La sola captura de los datos del interesado, no podrá equipararse a la correcta finalización del trámite para acceder al Juicio en Línea.

Activación de la cuenta

Artículo 8. El interesado ingresará su dirección de correo electrónico al sistema de Juicio en Línea. El sistema le enviará un correo electrónico con una liga para continuar con el registro, validando con esto la existencia y veracidad de la dirección electrónica. Después el interesado entrará al sistema por medio de la liga y comenzará con su trámite de registro aceptando los términos y condiciones, luego de ingresar los datos requeridos el sistema emitirá una constancia de registro que contendrá la clave de acceso y contraseña y la enviará al correo electrónico del interesado.

A partir de ese momento, podrá acceder al SIT para optar por el Juicio en Línea, conforme a las especificaciones que se detallan en estos Lineamientos.

Convalidación de identidad

Artículo 9. El interesado que haya realizado el trámite de su registro a través del Sistema Informático del Tribunal, tendrá a su disposición la expedición del acuse de recibo a que se refiere el artículo 24 de estos Lineamientos.

Así mismo, deberá acudir a convalidar su identidad, presentando la documentación señalada en el artículo 12 de los presentes lineamientos, dentro de los siguientes tres días hábiles, ante cualquiera de los módulos de registro que se encuentran en la sede del Tribunal y en las oficinas regionales de la Coordinación de la Defensoría Jurídica, en el horario de atención al público establecido en el Reglamento Interior del Tribunal, todos los días del año, a excepción de los sábados y domingos y los días que estén declarados como inhábiles en el Calendario Oficial de Labores o por el Pleno del Tribunal.

Obligatoriedad de registro para las autoridades

Artículo 10. Las autoridades cuyos actos sean susceptibles de impugnarse ante el Tribunal, así como aquéllas encargadas de su defensa en juicio deberán registrarse y convalidar su identidad, a fin de que puedan apersonarse en los procesos administrativos

que se tramiten en la modalidad de Juicio en Línea. Para concluir el registro, deberán cumplir además con los requisitos señalados en la fracción III del artículo 12 de éstos Lineamientos.

Consecuencias de la falta de registro para la autoridad:

Artículo 11. Las autoridades cuyos actos sean susceptibles de impugnarse ante el Tribunal, así como aquéllas encargadas de su defensa en juicio que sean omisas en efectuar su registro para comparecer al Juicio en Línea, serán notificadas en los términos previstos en el artículo 297 O del Código de Justicia Administrativa del Estado de Michoacán de Ocampo.

Requisitos para el trámite de registro

Artículo 12. Para concluir el trámite administrativo de registro el interesado deberá presentar en el Módulo de Registro, la siguiente documentación:

I. En caso de ser persona física:

a) Original y copia simple de alguna de las siguientes identificaciones oficiales vigentes con fotografía: Credencial de elector, cédula profesional o pasaporte; y,

b) Una cuenta de correo electrónico personal válido y una cuenta de correo opcional.

II. En caso de ser persona moral:

a) Instrumento público mediante el que se acredite la personalidad o en su caso la personería; y,

b) El representante legal de la persona moral, deberá presentar además la documentación referida en el apartado a) de la fracción I.

III. Tratándose de las autoridades cuyos actos sean susceptibles de ser impugnados ante el Tribunal y autoridades que pretendan instar el juicio de lesividad, deberán comparecer en forma personal y directa o por conducto de sus representantes legales y presentarán la documentación siguiente:

a) Original o copia certificada del nombramiento o de la constancia de mayoría en el caso de autoridades electas, así como una copia simple para su cotejo;

b) Original y copia simple de alguna de las siguientes identificaciones oficiales vigentes con fotografía: Credencial de elector, cédula profesional o pasaporte; y,

c) Una cuenta de correo electrónico institucional válido y una cuenta de correo opcional.

Usuarios

Artículo 13. Los interesados que hayan convalidado su identidad y, por ende, completado su trámite ante los módulos de registro, tendrán la calidad de usuarios del sistema. Podrán hacer uso del Juicio en Línea a través del SIT, dando clic en el ícono de Juicio en Línea, previo inicio de sesión en el mismo sistema, mediante el uso de su clave de acceso y contraseña y la aceptación de los términos y condiciones ahí establecidos. Dicha aceptación implica tenerlos por leídos y comprendido su alcance.

Formalidades del Juicio en Línea

Artículo 14. Para realizar el registro y utilizar el Juicio en Línea, el interesado deberá capturar la información en idioma español, completando la totalidad de los campos marcados como obligatorios, aportando de manera correcta los datos que permitan advertir la calidad con la que comparece, su identidad y correos electrónicos válidos, identificando el documento por medio del cual acredita su personalidad.

Es obligación de los interesados proporcionar datos veraces, debiendo abstenerse de formular pretensiones ilegales, esgrimir hechos contrarios a la verdad o promover diligencias meramente dilatorias, así como abstenerse de presentar documentos no exigidos por las normas aplicables o que ya se encuentren en poder de la autoridad demandada y correo spams.

No se activará más de una cuenta para una misma autoridad, por lo que de existir un registro previo, deberá solicitarse la cancelación o modificación de la clave de acceso y contraseña en términos de los capítulos cuarto y quinto de estos Lineamientos.

CAPÍTULO TERCERO
MODIFICACIÓN DE LOS DATOS DEL REGISTRO DE LAS AUTORIDADES

Modificación del registro para las autoridades

Artículo 15. Cuando las autoridades pretendan modificar la información de su registro, deberán hacerlo en el módulo de registro, a través del servidor público autorizado para esos efectos.

Acreditada la calidad del funcionario y exhibidos los documentos señalados en la fracción III del artículo 12 de estos Lineamientos, el agente certificador le generará la solicitud correspondiente, donde asentará los datos de la dependencia, organismo o autoridad correspondiente, cuya información será actualizada.

Tramitada la solicitud se le entregará al servidor público el documento en el que conste la información actualizada, así como la fecha de realización del trámite.

Actualización de la información proporcionada

Artículo 16. Las autoridades durante la substanciación del Juicio en Línea, deberán mantener actualizada la información proporcionada al Tribunal con motivo de su registro como usuario de los servicios informáticos; podrán actualizar la cuenta de correo electrónico y cuenta de correo alternativa, para efecto de recibir las notificaciones con motivo del proceso administrativo; así como la autorización que en términos del artículo 198 del Código, hayan manifestado a favor de servidor público de su adscripción informando tal circunstancia al Juez Administrativo que esté conociendo del proceso.

Asimismo, de actualizarse algún cambio las autoridades deberán señalar nueva cuenta de correo electrónico y cuenta de correo opcional o alternativa, a fin de que continúen siendo notificadas durante el proceso administrativo. En caso de ser omisas, las notificaciones les serán practicadas según lo previsto en el artículo 297 O del Código.

CAPÍTULO CUARTO
CLAVE DE ACCESO Y CONTRASEÑA

Clave de acceso y contraseña

Artículo 17. Las claves de acceso serán asignadas por el Sistema Informático del Tribunal a los usuarios, y se otorgarán exclusivamente a personas físicas o morales por conducto de sus representantes legales, sean promoventes, apoderados, terceros interesados, peritos de las partes, peritos terceros, así como a las personas físicas que ostenten la calidad de titular de una dependencia, organismo, unidad administrativa o autoridad, tanto susceptibles de ser actoras o demandadas, así como las encargadas de su defensa en juicios.

Uso, recuperación y cancelación de la clave de acceso y contraseñas

Artículo 18. El interesado será responsable del uso de la clave de acceso y contraseña, ésta tendrá vigencia permanente mientras no se solicite la baja o cancelación de la cuenta, ni su modificación o recuperación.

Modificación de contraseñas

Artículo 19. La recuperación y modificación de la contraseña podrá realizarse a través del Sistema Informático del Tribunal o de manera personal ante los módulos de registro.

Modificación de los términos y condiciones

Artículo 20. El Tribunal podrá en todo momento adicionar o eliminar todo o en parte los términos y condiciones, así como modificar en cualquier momento el SIT o cualquier módulo del mismo.

Registro y su falta de conclusión

Artículo 21. El interesado podrá registrarse una sola vez. Serán eliminados los datos ingresados cuando no se haya concluido el trámite o transcurra el término de tres días hábiles otorgados por estos lineamientos para concluirlo, sin perjuicio de que pueda volver a iniciarse el registro.

CAPÍTULO QUINTO
CANCELACIÓN DE LA CLAVE DE ACCESO Y CONTRASEÑA

Baja y modificación del registro

Artículo 22. Los usuarios que requieran cancelación de la clave de acceso y contraseña en el Sistema Informático del Tribunal o modificar los datos de su registro deberán cumplir con los siguientes requisitos:

I. Llenar la solicitud de cancelación en el sistema o modificación de información proporcionada para la obtención de la clave de acceso y contraseña, en este último caso, precisando la información objeto de actualización;

II. Proporcionar su nombre completo;

III. Presentar identificación oficial vigente; y,

IV. Exhibir el documento que acredite su personalidad cuando el trámite lo realice en representación de otra persona física, moral o en representación de una autoridad.

Los documentos mencionados en las fracciones III y IV de este artículo, deberán presentarse en original o copia certificada, para su cotejo y copia simple.

Realizado el trámite se otorgará al solicitante una constancia impresa que indicará, además de la información antes precisada, la fecha de baja o modificación, según sea el caso, en el SIT.

CAPÍTULO SEXTO
USO DEL JUICIO EN LÍNEA Y ENVIO DE PROMOCIONES ELECTRÓNICAS

Envío de documentos

Artículo 23. El interesado tendrá la calidad de usuario del Sistema Informático del Tribunal y accederá al servicio del Juicio en Línea.

Para iniciar el proceso en la modalidad de Juicio en Línea, en el Sistema Informático del Tribunal, adjuntará el escrito de la demanda debidamente firmada con la firma electrónica certificada y los demás documentos que deban acompañarse a la misma en forma legible y bajo las condiciones descritas en las especificaciones técnicas de éstos Lineamientos, así como las promociones subsecuentes y sus anexos.

Asimismo, los interesados deberán contar con el equipo y programas necesarios para establecer la interacción con el SIT, en términos de las características señaladas en el anexo técnico de los presentes Lineamientos, donde se especifican los requisitos tecnológicos mínimos e indispensables.

Formalidades de los medios de prueba

Artículo 24. Los documentos que el interesado ofrezca como pruebas, deberá exhibirlos e incorporarlos en forma legible y en términos de lo señalado en el artículo 297 K del Código de Justicia Administrativa del Estado de Michoacán de Ocampo.

Acuse de recibo electrónico

Artículo 25. Una vez que se haya agregado la demanda, los anexos correspondientes y completado los campos requeridos, o en su defecto la promoción subsecuente, el interesado dará clic al botón «*enviar*» para concluir la remisión de la demanda al Sistema Informático del Tribunal.

Realizado lo anterior, el sistema emitirá un acuse de *recibo electrónico* de la demanda y sus anexos y a la par enviará un correo

electrónico con la misma información.

El acuse de recibo electrónico de la demanda y sus anexos o de la promoción subsecuente, contendrá la fecha y hora de recepción, folio, nombre del promovente, una referencia a los anexos y una leyenda informativa.

La fecha y hora asentada en el acuse de recibo de la demanda, corresponderá al huso horario correspondiente al Estado de Michoacán.

Validación de demandas y promociones

Artículo 26. El interesado podrá repetir la operación cuantas demandas o promociones subsecuentes pretenda interponer, siempre y cuando cuente con firma electrónica, clave de acceso y contraseña.

Tratándose de promociones subsecuentes, el interesado sólo las podrá promover en línea una vez que la demanda haya sido validada y remitida por el SIT y aceptada por el Juez Administrativo al que por turno corresponda conocer de la misma.

Para lo anterior, el SIT validará y remitirá la demanda a más tardar dentro del plazo tres hábiles siguientes, a partir de la presentación de la demanda.

CAPÍTULO SÉPTIMO
DE LA FIRMA ELECTRÓNICA Y LOS REQUERIMIENTOS PARA SU TRÁMITE

Usuarios de la firma electrónica certificada

Artículo 27. Los usuarios que sean titulares de una firma electrónica, clave de acceso y contraseña, así como los Operadores en el ejercicio de sus funciones jurisdiccionales, para la obtención de la firma electrónica, deberán cumplir con los requisitos que le solicite el Tribunal en términos de lo establecido en estos Lineamientos y la Ley.

Una vez que el Tribunal expida la firma electrónica, podrán firmar las actuaciones generadas durante la substanciación del Juicio en Línea y que integrarán el expediente electrónico correspondiente.

De igual forma los peritos terceros tendrán la opción de firmar sus actuaciones de forma autógrafa y el Secretario de Acuerdos del Juzgado Administrativo que conozca del asunto se encargará de digitalizar el documento e integrarlo al expediente electrónico.

Obtención de la firma electrónica

Artículo 28. Para que los Operadores y usuarios puedan firmar las actuaciones generadas durante la substanciación del Juicio en Línea, deberán tramitar y obtener el certificado de firma electrónica, en términos de los requisitos señalados en estos Lineamientos, la Ley y la Declaración de Prácticas y Políticas de Certificación.

Artículo 29. El Tribunal por conducto del SIT, llevará a cabo un registro de Profesionales del Derecho y un registro de Peritos que pretendan instar en el Juicio en Línea, quienes deberán registrar su cédula profesional, tramitar clave de acceso, contraseña y firma electrónica certificada ante el módulo establecido para tal fin.

Una vez que cuenten con la firma electrónica certificada podrán utilizarla para firmar las actuaciones generadas durante la substanciación del Juicio en Línea en los que hayan sido autorizados por las partes.

CAPÍTULO OCTAVO
CONSULTA DEL JUICIO EN LÍNEA

Vinculación de cuenta del autorizado

Artículo 30. Las partes que pretendan autorizar licenciados en derecho en términos del artículo 198 del Código, deberán efectuar la solicitud de vinculación al expediente, proporcionando el nombre o correo electrónico del autorizado que deberá estar previamente registrado como usuario del Juicio en Línea, en el escrito de demanda o en promoción subsecuente ante el Juez Administrativo que conozca del proceso. Este mismo procedimiento se seguirá para solicitar la revocación de la vinculación al expediente.

La solicitud de vinculación al expediente en términos amplios o únicamente para consulta del expediente en la modalidad de Juicio en Línea, podrá realizarse vía electrónica a través del Sistema Informático del Tribunal, debiendo el Juez acordar lo conducente.

Artículo 31. Los usuarios que pretendan apersonarse en un expediente de Juicio en Línea como mandatarios o en términos del tercer párrafo del artículo 191 del Código, deberán acudir ante el módulo de registro de Juicio en Línea a solicitar la vinculación al expediente.

CAPÍTULO NOVENO
CONSIDERACIONES TÉCNICAS PARA EL ENVÍO DE PROMOCIONES Y ANEXOS

Requisitos técnicos

Artículo 32. Las promociones y sus anexos que pretendan ser enviados por las partes, deberán digitalizarse de tal manera que sean accesibles, de fácil manejo, inalterables y sin restricciones de copiado del texto o de cualquier contenido, impresión y consulta, así como las demás características precisadas en el anexo técnico de los presentes Lineamientos.

Requisitos de la información ingresada al sistema

Artículo 33. Para el registro y envío de las promociones y sus anexos, las partes deberán verificar lo siguiente:

I. El correcto y completo registro de la información solicitada en el Sistema Informático del Tribunal;

II. El adecuado funcionamiento, integridad, legibilidad y formato de los archivos electrónicos, incluso los digitalizados, que se agreguen al Sistema Informático del Tribunal; y,

III. Que los archivos electrónicos que pretendan remitir a través del Sistema Informático del Tribunal se encuentren libres de virus.

Diferencias entre la información registrada y la información enviada a través del SIT

Artículo 34. En caso de que no exista coincidencia entre la información registrada por los usuarios en los campos de captura y el contenido de la promoción enviada a través del SIT, el Juez Administrativo podrá requerir al usuario que corresponda para que dentro del plazo de tres días hábiles, señale la información correcta que deberá considerar el Tribunal.

CAPÍTULO DÉCIMO
MEDIDAS TÉCNICAS Y ADMINISTRATIVAS DE SEGURIDAD

Seguridad y confidencialidad de la información

Artículo 35. El Tribunal a través de los administradores del Sistema Informático del Tribunal, adoptará las medidas físicas, técnicas y administrativas de seguridad que garanticen la integridad, confidencialidad e inalterabilidad de las promociones, de su contenido, de la información proporcionada por las partes, la contenida en las notificaciones electrónicas y demás mensajes de datos, como de la información transmitida y almacenada vía internet en el Sistema Informático del Tribunal en términos de lo señalado en el artículo 49 de los presentes Lineamientos, así como realizar las acciones de depuración de la información que pueda ser perjudicial.

Número de identificación

Artículo 36. Para la demanda y cada promoción presentada en el Juicio en Línea, el Sistema Informático del Tribunal le generará un número del documento para su identificación, seguimiento, vinculación a las partes y control.

Las demandas y promociones que integren el expediente electrónico, podrán ser verificadas con el número de identificación del documento por las partes a través del SIT.

Idoneidad del documento

Artículo 37. El Tribunal a través de los Operadores adscritos la Secretaría o Juzgado Administrativo, adoptará las medidas necesarias para identificar, verificar y hacer constar las deficiencias técnicas que desde el origen obren en las promociones y sus anexos, a fin de proveer de certeza y seguridad a los interesados respecto de la idoneidad del contenido de los documentos.

CAPÍTULO DÉCIMO PRIMERO
ASISTENCIA A USUARIOS DEL JUICIO EN LÍNEA

Asistencia técnica

Artículo 38. El Tribunal de manera permanente proporcionará la orientación y asistencia técnica necesaria a los usuarios que utilicen el Juicio en Línea.

La asistencia será proporcionada a través del personal adscrito a la Secretaría, de manera personal, telefónica o mediante los mecanismos ofrecidos en el SIT, en un horario comprendido entre las 9:00 y las 16:00 horas todos los días del año, a excepción de sábados y domingos, así como los declarados inhábiles en términos del Calendario Oficial de Labores del Tribunal y los acordados por el Pleno en términos del artículo 7 del Reglamento Interior del Tribunal de Justicia Administrativa de Michoacán de Ocampo.

Impartición de talleres

Artículo 39. A fin de fomentar la accesibilidad y ventajas de la substanciación del proceso administrativo en su modalidad de Juicio en Línea, el Tribunal impartirá periódicamente talleres sobre el acceso y utilización del mismo.

CAPÍTULO DÉCIMO SEGUNDO
DEL TRIBUNAL

ATRIBUCIONES

Empleo de tecnologías

Artículo 40. A fin de posibilitar el cumplimiento de los presentes lineamientos, el Tribunal contará con los equipos y sistemas tecnológicos que le permitan la realización y adecuada recepción de las notificaciones electrónicas, la digitalización y consulta electrónica de expedientes, el inicio, la substanciación y resolución del proceso administrativo en línea, así como cualquier otro servicio integrante del Sistema Informático que brinde el Tribunal, procurando la celeridad, la disminución de costos, así como el incremento de la eficiencia, transparencia y productividad en la impartición de justicia.

De las Disposiciones Administrativas

Artículo 41. El Tribunal emitirá y publicará en su página de internet, los Lineamientos para la Utilización del Juicio en Línea, la Declaración de Prácticas y Políticas de Certificación y los Acuerdos Generales de Pleno que considere pertinentes.

De los principios rectores

Artículo 42. En los mecanismos que se establezcan para la realización de notificaciones electrónicas, la gestión electrónica de expedientes, la consulta electrónica de los mismos, el Juicio en Línea y demás servicios del Sistema Informático, el Tribunal deberá adoptar todas aquellas medidas de seguridad que garanticen la integridad, autenticidad, confidencialidad y demás principios previstos en el artículo 4 de la Ley.

Del contenido de instrumentos

Artículo 43. Los programas informáticos, formatos electrónicos y demás instrumentos que expida el Tribunal con motivo de los presentes lineamientos, contendrán todos aquellos elementos exigibles que permitan incorporar los datos de identificación de los particulares y posibiliten el cumplimiento del artículo 297 D del Código.

Atribuciones del Tribunal

Artículo 44. En la materia de los presentes Lineamientos, al Tribunal le corresponden las siguientes atribuciones:

I. Interpretar los Lineamientos y resolver sobre los aspectos

administrativos relativos a los actos y trámites electrónicos que se realicen en los Sistemas de Información del Tribunal;

II. Emitir la Declaración de Prácticas y Políticas de Certificación, Acuerdos Generales de Pleno y demás disposiciones administrativas para la utilización del Sistema Informático del Tribunal;

III. Revocar, suspender y cancelar los certificados de Firma Electrónica en los casos establecidos en los Lineamientos y la ley de la materia; y,

IV. Las demás que establezcan las leyes aplicables y la Declaración de Prácticas y Políticas de Certificación expedidas por el Tribunal.

De los servidores públicos del Tribunal

Artículo 45. Los servidores públicos del Tribunal acreditados como Operadores, sólo podrán contar con un usuario y contraseña y serán responsables de su correcta utilización.

Atribuciones de la Secretaría General de Acuerdos

Artículo 46. La Secretaría tendrá las siguientes atribuciones:

I. Asegurar la integridad y veracidad de la información registrada en los Sistemas de Información;

II. Resguardar la documentación original que sirvió de soporte para la realización de los trámites administrativos en los Sistemas de Información;

III. Integrar, resguardar y mantener actualizada la información de los Usuarios que contengan los expedientes sobre las solicitudes de las altas, bajas o modificación de claves de acceso y contraseñas, así como la extinción de los certificados de firma electrónica, a partir de la información que le proporcione la Coordinación de Informática;

IV. Generar las condiciones necesarias para que los Usuarios puedan obtener su Certificado de Firma Electrónica y firmar electrónicamente en los Sistemas de Información;

V. Registrar, verificar y validar en el Sistema Informático, las demandas, promociones subsecuentes y anexos que se interpongan a través del Juicio en Línea; y,

VI. Las demás que establezcan los Lineamientos, los Acuerdos Generales de Pleno, la Declaración de Prácticas y Políticas de Certificación expedidas por el Tribunal y las leyes aplicables.

Atribuciones de la Coordinación de Informática

Artículo 47. La Coordinación de Informática del Tribunal además de las establecidas en los diversos ordenamientos tendrá las atribuciones siguientes:

I. Recibir las solicitudes de altas, modificación y cancelación de claves de acceso y contraseña, e informarlo de inmediato a la Secretaría;

II. Mantener actualizado el software necesario para la ejecución de estos Lineamientos;

III. Instalar en caso necesario, el equipo correspondiente para el funcionamiento de los Sistemas de Información;

IV. Cuidar la seguridad, protección y confidencialidad de las bases de datos y los Sistemas de Información;

V. Atender las instrucciones que le gire el Tribunal y auxiliar a la Secretaría en el cumplimiento de sus atribuciones; y,

VI. Las demás atribuciones que establezcan la Ley, los Acuerdos Generales de Pleno, los Lineamientos, la Declaración de Prácticas y Políticas de Certificación y demás ordenamientos legales aplicables.

Conservación y administración de la información electrónica

Artículo 48. La Coordinación de Informática será responsable de la conservación y administración de la información contenida en los mensajes de datos y demás medios electrónicos con motivo de los servicios del Sistema Informático del Tribunal, debiendo observar como normas mínimas de seguridad, las siguientes:

I. La información deberá ser respaldada en cada proceso de actualización de documentos;

II. Se deberá mantener una copia de seguridad en el lugar de operación del Sistema Informático y otra en un centro especializado de almacenamiento de datos;

III. El esquema de respaldo deberá incrementarse en forma gradual con objeto de mantener la historia de la información en el mínimo de versiones posibles; y,

IV. Las demás que establezca la Ley, los Acuerdos Generales de Pleno, los Lineamientos, la Declaración de Prácticas y Políticas de Certificación y demás ordenamientos aplicables.

CAPÍTULO DÉCIMO TERCERO
DE LOS USUARIOS

De la validez de las notificaciones

Artículo 49. Las notificaciones electrónicas por mensajes de datos, así como los acuses de recibo que genere el Sistema Informático del Tribunal, realizados conforme a la Ley y los presentes Lineamientos, tendrán la validez jurídica y surtirán los efectos legales dentro de los procesos administrativos que prevé el Código, de conformidad con su artículo 219 y demás relativos y aplicables.

Los documentos suscritos con firma electrónica, deberán permitir verificar la integridad y autenticidad de los mismos al ser impresos, mediante una cadena de caracteres asociados al documento y constituirán una copia fiel del documento original.

Del acceso de los particulares a los servicios informáticos

Artículo 50. De conformidad con el Código, será optativo para

los particulares la substanciación del proceso en la modalidad de Juicio en Línea; así como la recepción de notificaciones vía electrónica.

Los particulares que opten por los servicios electrónicos, deberán proporcionar todos aquellos datos requeridos por el Tribunal y acreditarán su identidad o el carácter con el que comparecen; al igual que aquellos otros que les sean solicitados a fin de observar lo exigido en el Código o en la Ley.

Tratándose del acceso y utilización del Juicio en Línea, los interesados deberán sujetarse a los términos y condiciones que para tal fin se prevean, los Lineamientos, la Declaración de Prácticas y Políticas de Certificación, los Acuerdos Generales del Pleno, y demás disposiciones administrativas que para el efecto expida el Tribunal.

Responsabilidades

Artículo 51. Los Usuarios del Sistema Informático del Tribunal, serán responsables de:

I. El uso adecuado del Sistema, la dirección de correo electrónico, clave de acceso, contraseña, de las consultas que realicen del expediente electrónico y de su certificado de firma electrónica;

II. Utilizar la firma electrónica y contraseña de manera personal e intransferible y no difundirla;

III. Acudir al módulo de registro a convalidar clave de acceso y contraseña y tramitar la Firma Electrónica Certificada, presentando una identificación oficial vigente, así como los documentos señalados en estos Lineamientos;

IV. Mantener informado al Tribunal sobre cualquier cambio en los datos personales o laborales;

V. Del certificado de firma electrónica, la captura y actualización del expediente en todas sus modalidades; y,

VI. Las demás que establezcan los presentes Lineamientos, la Ley y la Declaración de Prácticas y Políticas de Certificación y los Acuerdos Generales del Pleno que expida el Tribunal.

CAPÍTULO DÉCIMO CUARTO
DE LA CONSULTA ELECTRÓNICA DE EXPEDIENTES

Operación

Artículo 52. Los usuarios que accedan al Sistema Informático del Tribunal, deberán proporcionar la información que en él se le soliciten y previo cumplimiento de los requisitos que dispongan sus Lineamientos.

Alcances

Artículo 53. La información contenida en el servicio de consulta electrónica de expedientes, será meramente informativa y siempre deberá garantizar la protección de los datos personales en poder del Tribunal, como sujeto obligado en los términos previstos en la Ley de Protección de Datos Personales y Ley de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Michoacán de Ocampo.

CAPÍTULO DÉCIMO QUINTO
DEL JUICIO EN LÍNEA

Condiciones de uso del Juicio en Línea

Artículo 54. En los términos del artículo 297 A del Código, el proceso administrativo se promoverá, substanciará y resolverá en línea a través del Sistema Informático del Tribunal. Su uso será gratuito y optativo para los particulares y deberá ceñirse a los Términos y Condiciones, Lineamientos, Acuerdos Generales de Pleno y demás disposiciones administrativas que para tal efecto emita el Tribunal.

Para los efectos del Juicio en Línea son hábiles las veinticuatro horas del día a excepción de los sábados y domingos y los días que estén declarados como inhábiles en el Calendario Oficial de Labores o por el Pleno del Tribunal.

Inmutabilidad de la vía

Artículo 55. Si las partes acceden al Sistema Informático del Tribunal, aceptan los términos y condiciones, completan los campos de información correspondientes y envían su demanda, se entenderá que expresan su voluntad en ese sentido y ésta no podrá cambiar si posteriormente el interesado presenta demanda en la vía tradicional contra el mismo acto o resolución que fue impugnado a través del Juicio en Línea.

Resguardo de la información

Artículo 56. Las actuaciones del Juicio en Línea se efectuarán a través del Sistema Informático, en términos del Código y de la Ley y deberán caracterizarse con datos únicos, irrepetibles y vinculantes a las partes y proceso en que se actúe, de tal manera que permitan su identificación, verificación y relación con el emisor y receptor, en el tiempo y en forma íntegra respecto a su contenido.

Para proveer a lo anterior, el Tribunal podrá auxiliarse de los mecanismos tecnológicos y electrónicos aportados por la ciencia, que sean compatibles entre estos y el Sistema Informático del Tribunal.

Artículo 57. El Tribunal, a través de la Secretaría General de Acuerdos con auxilio de la Coordinación de Informática, brindará asistencia a los Usuarios del Sistema Informático e interesados que pretendan acceder al Juicio en Línea.

La asistencia será proporcionada en horario de oficina, ya sea en forma personal, mediante los mecanismos ofrecidos en el SIT o vía telefónica a través del personal calificado para tal encomienda.

CAPÍTULO DÉCIMO SEXTO
DE LA AUTORIDAD CERTIFICADORA

El Tribunal como autoridad certificadora

Artículo 58. En los términos del artículo 14 fracción V, de la Ley,

el Tribunal es autoridad certificadora. Esta función la ejercerá por conducto de la Secretaría General de Acuerdos con apoyo de la Coordinación de Informática y de cualquier otro órgano del Tribunal, conforme a lo dispuesto en los Acuerdos Generales del Pleno del Tribunal y la Declaración de Prácticas y Políticas de Certificación emitidos para tal efecto.

El Tribunal podrá celebrar convenio para que un tercero haga las funciones de autoridad certificadora. De actualizarse este supuesto, se subrogará a las disposiciones generales que regulen la administración y operación de la infraestructura tecnológica que permitan al tercero el uso e implementación de la firma electrónica certificada, su eficacia jurídica y la prestación de servicios de certificación relacionados con la misma.

Atribuciones como autoridad certificadora

Artículo 59. Además de lo previsto en la Ley, corresponde al Tribunal como autoridad certificadora, por conducto de sus órganos internos conducentes, ejercer las siguientes atribuciones:

I. Establecer un Registro de Certificados de Firma Electrónica que garantice la disponibilidad de la información de manera regular y continua;

II. Iniciar el procedimiento para actualizar las disposiciones técnicas que permitan el uso de tecnologías y medios electrónicos, de conformidad con la Ley y estos Lineamientos;

III. Expedir la Declaración de Prácticas y Políticas de Certificación, donde se detallarán las prácticas, políticas, procedimientos y mecanismos, que el propio Tribunal se obliga a cumplir en la prestación de sus servicios de certificación y homologación, así como adherirse a aquella que resulte acorde con sus necesidades;

IV. Analizar los informes sobre la evaluación de los prestadores de servicios de certificación;

V. Establecer y administrar el Registro de Prestadores de Servicios de Certificación del Tribunal;

VI. Inscribir en los Certificados de Firma Electrónica, la fecha y hora en que se expidieron, o en su caso, se dejó sin efectos el Certificado de Firma Electrónica;

VII. Asesorar a los usuarios de medios electrónicos y firma electrónica;

VIII. Mantener permanentemente actualizada la tecnología aplicada al uso de medios electrónicos y firma electrónica; y,

IX. Las demás que resulten necesarias para la prestación del Sistema Informático del Tribunal.

Identidad del solicitante

Artículo 60. El Tribunal como autoridad certificadora y los prestadores de servicio de certificación acreditados, deberán comprobar fehacientemente la identidad del solicitante antes de la emisión del certificado correspondiente.

CAPÍTULO DÉCIMO SÉPTIMO
DEL CERTIFICADO DE FIRMA ELECTRÓNICA

Características de eficacia

Artículo 61. El certificado de firma electrónica deberá permitir a quien lo reciba, verificar que ha sido emitido por el Tribunal, como autoridad certificadora, con la finalidad de comprobar la validez del mismo.

Uso

Artículo 62. El certificado de firma electrónica deberá ser utilizado por su titular conforme a lo establecido en la Ley y demás ordenamientos generales expedidos por el Tribunal en relación con los servicios comprendidos en el Sistema Informático que proporciona.

Contenido

Artículo 63. Los Certificados de Firma Electrónica que expida el Tribunal con motivo de los presentes Lineamientos, deberán contener:

I. La denominación de la Autoridad Certificadora; y,

II. Los datos de identidad del Titular del Certificado de Firma Electrónica, mencionando nombre y dirección de correo electrónico.

Del Registro de Certificados de Firma Electrónica

Artículo 64. El Tribunal, en cuanto autoridad certificadora, integrará y operará un Registro de Certificados de Firma Electrónica del Tribunal, conforme a lo siguiente:

I. Será público y deberá mantener permanentemente actualizada la información que corresponda a los certificados de firma electrónica, indicando si los mismos se encuentran vigentes, revocados, suspendidos, cancelados, traspasados a otro prestador de servicios de certificación u homologados;

II. Dicho Registro, presentado en forma de lista con el status de cada uno de los certificados expedidos por el Tribunal, podrá ser consultado en la página de internet del Tribunal;

III. Igualmente, el Registro comprenderá aquellos Certificados de Firma Electrónica expedidos por una autoridad certificadora diversa al Tribunal, en virtud de los convenios celebrados por éste en términos del artículo 17 último párrafo de la Ley; y,

IV. Asimismo, incluirá los convenios que se suscriban entre el Tribunal y los sujetos de la Ley, así como la constancia de homologación de los Certificados de Firma Electrónica.

De la extinción de los certificados

Artículo 65. El Tribunal podrá suspender, revocar o cancelar un certificado de firma electrónica para la substanciación del

procedimiento correspondiente.

Toda suspensión, revocación o cancelación de un certificado de firma electrónica, deberá inscribirse en el registro aludido en el artículo 65 fracción I, de estos Lineamientos.

Los procedimientos respectivos para dicha extinción, se substanciarán y resolverán por el Tribunal en apego a las disposiciones de la Ley y de estos Lineamientos,

El certificado de firma electrónica quedará sin efectos, cuando se realice su suspensión, revocación o cancelación.

Supuestos de la suspensión

Artículo 66. La autoridad certificadora podrá suspender temporalmente los certificados de firma electrónica expedidos, cuando así lo solicite el firmante, sus representados o lo ordene una autoridad competente. Toda suspensión deberá inscribirse sin demora en el registro respectivo.

Las causas por las que se podrá solicitar la suspensión del certificado de firma electrónica certificada serán, cuando:

I. Haya indicios de que un tercero no autorizado utilice la clave privada o de la firma electrónica certificada;

II. El titular del certificado de firma electrónica certificada requiera modificar alguno de los datos contenidos en el mismo;

III. Exista un caso fortuito o de fuerza mayor; y,

IV. Cuando la autoridad certificadora lo estime conveniente, fundando y motivando por escrito las razones de la suspensión.

Artículo 67. Tratándose de la suspensión del certificado de un servidor público o del certificado de una dependencia, el titular o el sujeto autorizado deberán informar del hecho al superior jerárquico y notificarlo a la autoridad certificadora, la cual suspenderá el uso del certificado y dará vista al encargado de la firma electrónica para los efectos legales correspondientes.

Artículo 68. La suspensión del uso de un certificado tendrá el efecto de detener temporalmente aquellos trámites, procedimientos, actos y resoluciones que el titular o los sujetos autorizados indiquen expresamente, y que se encuentren asociados al propio certificado.

Lo anterior, hasta en tanto la autoridad certificadora, autorice su reanudación, de acuerdo con la resolución que derive del procedimiento respectivo. Si no se hace indicación específica de los trámites, procedimientos, actos y resoluciones que deben suspenderse temporalmente, la autoridad certificadora suspenderá todos los que se encuentren asociados al certificado en cuestión.

La autoridad certificadora publicará en su portal de Internet una relación de los certificados cuyo uso se encuentre suspendido.

Procedimiento de la suspensión

Artículo 69. El procedimiento para la suspensión de un certificado de firma electrónica, será el mismo que el de la revocación, previsto en estos Lineamientos y demás disposiciones aplicables establecidas en la Ley.

Causas de revocación

Artículo 70. El certificado de firma electrónica podrá ser revocado por la autoridad certificadora, con motivo de las siguientes causas:

I. Cuando se detecten inexactitudes en los datos aportados por el titular para la obtención del certificado de firma electrónica certificada;

II. Por haberse comprobado que al momento de la expedición del certificado de firma electrónica certificada, no se cumplieron uno o más de los requisitos establecidos en la ley, situación que no afectará los derechos de terceros de buena fe;

III. Cuando se compruebe el uso indebido o ilícito del certificado de firma electrónica certificada; y,

IV. Cuando el titular de la firma electrónica certificada modifique, altere, destruya o provoque la pérdida de información contenida en el Sistema del Juicio en Línea.

Procedimiento de revocación

Artículo 71. La autoridad certificadora iniciará de oficio el procedimiento de revocación, el cual deberá notificarse al titular en forma personal, a efecto que dentro de cinco días hábiles contados a partir del día siguiente al de la notificación, manifieste lo que a su interés convenga.

Artículo 72. La autoridad certificadora emitirá su resolución dentro de los quince días hábiles contados a partir del vencimiento del plazo señalado en el artículo anterior, y deberá notificarla personalmente al titular del certificado de la firma electrónica, entregando en su caso, el comprobante de revocación de la misma.

La autoridad certificadora deberá realizar la anotación de revocación en el registro de certificados de firma electrónica.

Artículo 73. Los titulares de los certificados de firma electrónica que incurran en las causas de revocación señaladas, en las fracciones I y II del artículo 71 no podrán solicitar certificado de firma electrónica, sino transcurridos seis meses.

Por lo que respecta a la causal establecida en la fracción III, del referido artículo, no podrá solicitar certificado sino transcurridos dos años.

El titular de la firma electrónica que incurra en la causa de revocación establecida en la fracción IV del artículo 71, no tendrá posibilidad de volver a promover Juicios en Línea.

Los plazos establecidos en este artículo se contarán a partir de que haya quedado firme la resolución de revocación.

Procedimiento de la cancelación

Artículo 74. La cancelación del certificado de firma electrónica

será a solicitud del titular o bien, cuando se surta alguno de los supuestos siguientes:

I. A solicitud del titular por pérdida, robo, inutilización del Certificado de Firma Electrónica, o por así convenir a sus intereses;

II. Por fallecimiento del titular;

III. Por incapacidad superveniente, total o parcial, del titular;

IV. Por extinción de la persona moral titular de Certificado de Firma Electrónica; y,

V. Por expiración de su vigencia que nunca será superior a cuatro años.

Artículo 75. Cuando un servidor público deje el cargo y cuente con un certificado de firma electrónica como autoridad, será responsabilidad de la propia autoridad hacerlo del conocimiento del Tribunal, y solicitar la cancelación del certificado de la firma electrónica, la cancelación de la clave de acceso y contraseña, y la desvinculación a los expedientes en los que sea parte con el carácter de autoridad.

Artículo 76. Para la cancelación del certificado de firma electrónica a petición de parte, deberá solicitarse por escrito en el módulo de registro. La cancelación por expiración de la vigencia del certificado se realizará de manera oficiosa.

Notificaciones y plazos de los procedimientos de extinción

Artículo 77. La pérdida de eficacia de los certificados de firma electrónica, en el supuesto de expiración de vigencia, tendrá lugar desde que esta circunstancia se produzca. En los demás casos, la extinción de un certificado de firma electrónica surtirá efectos desde la fecha en que la autoridad certificadora, tenga conocimiento cierto de la causa que la origina y así lo haga constar en el registro de certificados.

Artículo 78. La autoridad certificadora ratificará la causa de la extinción del certificado y hará constar la misma en el registro de certificados de firma electrónica.

Artículo 79. Para la realización de notificaciones y el cómputo de plazos dentro de los procedimientos de extinción de los Certificados de Firma Electrónica, se atenderá a lo dispuesto en el Código, en todo lo que no se contraponga a la Ley o a los presentes Lineamientos.

T R A N S I T O R I O S

Inicio de vigencia

ARTÍCULO PRIMERO. Los presentes Lineamientos entrarán en vigor al día siguiente de su publicación en el Periódico Oficial del Gobierno Constitucional del Estado de Michoacán de Ocampo.

Morelia, Michoacán, a los 11 días de Julio de 2019 dos mil diecinueve, por los Magistrados que integran el Pleno.

Lic. Sergio Mecino Morales.- Magistrado Presidente y titular de la Quinta Sala Especializada en Materia de Anticorrupción y Responsabilidades Administrativas.- Dr. Arturo Bucio Ibarra.- Magistrado de la Segunda Sala Administrativa Ordinaria.- Lic. Griselda Lagunas Vázquez.- Magistrada de la Tercera Sala Administrativa Ordinaria.- Mtro. Rafael Rosales Coria.- Magistrado de la Cuarta Sala Especializada en Materia de Anticorrupción y Responsabilidades Administrativas.- Lic. Carlos Paulo Gallardo Balderas.- Magistrado por Ministerio de Ley Titular de la Primera Sala Administrativa Ordinaria. (Firmados).

Anexo Técnico

Sistema de Juicio en Línea del Tribunal de Justicia Administrativa de Michoacán de Ocampo

El usuario deberá cumplir con los requisitos técnicos y recomendaciones siguientes:

1. Computadora con las siguientes características mínimas:

CONCEPTO	REQUISITO MÍNIMO
Sistema Operativo	**Windows**: 7 o superior **Mac OS**: Leopard o superior **Linux:** Ubuntu, Mint u otro con interfaz gráfica
Procesador	1 GHZ de velocidad
Memoria RAM	2 GB
Navegador web	Google Chrome actualizado
Lector de PDF	Adobe Reader, Foxit Reader u otro

2. Una cuenta de correo electrónico válido y en uso.

3. Conexión a internet con velocidad de subida de mínimo 5 mb /s.

4. Para usuarios nuevos, un correo comercial (se recomienda Gmail o Outlook) o institucional válido. Para correos no comerciales (de institución o empresa) se recomienda revisar las restricciones para correos de entrada desconocidos así como evitar la saturación de la bandeja de entrada.

5. Para operadores del Sistema de Juicio en Línea, una cuenta válida institucional.

6. Todos los documentos presentados por el usuario a través del módulo deberán ser en formato PDF, JPG, MP3 y MP4.

7. Los nombres de los archivos a subir deberán de ser lo más cortos posibles, sin exceder los quince caracteres. No contener caracteres especiales, acentos o ñ. El sistema no puede identificar el contenido de los documentos, por lo tanto el nombre de los mismos es relevante, pero si debe ser lo más corto evitando utilizar caracteres de signos como puntos, comas, @, entre otros poco convencionales.

8. Cada archivo deberá tener un tamaño de memoria como

máximo de 25 mb (mega bytes). De exceder el tamaño máximo de los anexos, los usuarios podrán fraccionar el documento en varios archivos que no excedan los 25 mb., e incorporarlos al Sistema Informático del Tribunal.

9. El usuario procurará en la medida de lo posible escanear documentos legibles, por lo tanto evitará el escaneo en copia de los documentos, si cuenta con los originales.

10. La calidad mínima de escaneo será 200 x 200 pixeles siempre y cuando el documento sea legible.

11. El servicio de Juicio en Línea emite correos electrónicos a la cuenta proporcionada por el usuario, de no recibir dichos correos en su bandeja principal, el usuario deberá consultar su bandeja de correo no deseado y otorgarle los permisos necesarios para recibir correctamente futuros avisos.

La calidad en la velocidad del servicio dependerá de su velocidad de subida de internet del usuario y del tamaño de los archivos proporcionados.

Así lo acordó el Pleno del Tribunal de Justicia Administrativa del Michoacán de Ocampo, en Sesión del día 11 once de julio de 2019 dos mil diecinueve.

El suscrito, licenciado en derecho Jorge Luis Arroyo Mares, Coordinador de Asuntos Jurídicos habilitado para ejercer las funciones de Secretario General de Acuerdos del Tribunal de Justicia Administrativa de Michoacán de Ocampo, con fundamento en lo dispuesto por los artículos 145 fracción I, 159 fracción XVI, 164 último párrafo y 165 fracciones I, VI y XII del Código de Justicia Administrativa del Estado de Michoacán de Ocampo, así como 30 fracciones III y VII del Reglamento Interior del Tribunal de Justicia Administrativa de Michoacán de Ocampo.

C E R T I F I C A

Que los presentes Lineamientos para la utilización del Juicio en Línea ante el Tribunal de Justicia Administrativa del Estado de Michoacán de Ocampo fueron aprobados por el Pleno del Tribunal de Justicia Administrativa de Michoacán de Ocampo, en sesión del día 11 once de julio de 2019 dos mil diecinueve, por unanimidad de votos de los Magistrados Sergio Mecino Morales, presidente y Titular de la Quinta Sala Especializada, Arturo Bucio Ibarra, titular de la Segunda sala Administrativa, Griselda Lagunas Vázquez, titular de la Tercera Sala Administrativa, Rafael Rosales Coria, titular de la Cuarta Sala Especializada y Carlos Paulo Gallardo Balderas, magistrado por Ministerio de Ley de la Primera Sala Administrativa.- Morelia, Michoacán de Ocampo, a 11 once de julio de 2019 dos mil diecinueve.- Conste. (Firmado).

DECLARACIÓN DE PRÁCTICAS Y POLÍTICAS DE CERTIFICACIÓN DEL TRIBUNAL DE JUSTICIA ADMINISTRATIVA DE MICHOACÁN DE OCAMPO

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

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:

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/.

Así lo acordó el Pleno del Tribunal de Justicia Administrativa del Michoacán de Ocampo, en Sesión del día 11 once de julio de 2019 dos mil diecinueve.

EL SUSCRITO LICENCIADO EN DERECHO JORGE LUIS ARROYO MARES, COORDINADOR DE ASUNTOS JURÍDICOS HABILITADO PARA EJERCER LAS FUNCIONES DE SECRETARIO GENERAL DE ACUERDOS DEL TRIBUNAL DE JUSTICIA ADMINISTRATIVA DE MICHOACÁN DE OCAMPO, CON FUNDAMENTO EN LO DISPUESTO POR LOS ARTÍCULOS 145 FRACCIÓN I, 159 FRACCIÓN XVI, 164 ÚLTIMO PÁRRAFO Y 165 FRACCIONES I, VI Y XII DEL CÓDIGO DE JUSTICIA ADMINISTRATIVA DEL ESTADO DE MICHOACÁN DE OCAMPO, ASÍ COMO 30 FRACCIONES III Y VII DEL REGLAMENTO INTERIOR DEL TRIBUNAL DE JUSTICIA ADMINISTRATIVA DE MICHOACÁN DE OCAMPO.

C E R T I F I C A

QUE LA PRESENTE DECLARACIÓN DE PRÁCTICAS Y POLÍTICAS DE CERTIFICACIÓN DEL TRIBUNAL DE JUSTICIA ADMINISTRATIVA DE MICHOACÁN DE OCAMPO FUE APROBADA POR EL PLENO DEL TRIBUNAL

DE JUSTICIA ADMINISTRATIVA DE MICHOACÁN DE OCAMPO, EN SESIÓN DEL DÍA 11 ONCE DE JULIO DE 2019 DOS MIL DIECINUEVE, POR UNANIMIDAD DE VOTOS DE LOS MAGISTRADOS SERGIO MECINO MORALES, PRESIDENTE Y TITULAR DE LA QUINTA SALA ESPECIALIZADA, ARTURO BUCIO IBARRA, TITULAR DE LA SEGUNDA SALA ADMINISTRATIVA, GRISELDA LAGUNAS VÁZQUEZ, TITULAR DE LA TERCERA SALA ADMINISTRATIVA, RAFAEL ROSALES CORIA, TITULAR DE LA CUARTA SALA ESPECIALIZADA Y CARLOS PAULO GALLARDO BALDERAS, MAGISTRADO POR MINISTERIO DE LEY DE LA PRIMERA SALA ADMINISTRATIVA.- MORELIA, MICHOACÁN DE OCAMPO, A 11 ONCE DE JULIO DE 2019 DOS MIL DIECINUEVE.- CONSTE. (Firmado).

TÉRMINOS Y CONDICIONES PARA LA UTILIZACIÓN DEL JUICIO EN LÍNEA ANTE EL TRIBUNAL DE JUSTICIA ADMINISTRATIVA DE MICHOACÁN DE OCAMPO

El servicio del Juicio en Línea se rige por el Código de Justicia Administrativa de Michoacán de Ocampo; los Lineamientos para la Utilización del Juicio en Línea ante el Tribunal de Justicia Administrativa del Estado de Michoacán de Ocampo; la Ley de Firma Electrónica Certificada del Estado de Michoacán de Ocampo; la Declaración de Prácticas y Políticas de Certificación del Tribunal de Justicia Administrativa de Michoacán de Ocampo, y por los siguientes Términos y Condiciones que deberán aceptar los usuarios o los interesados en instar el proceso administrativo a través de la modalidad de Juicio en Línea.

Lo anterior, para efecto de dar a conocer de manera conjunta a los usuarios del Tribunal de Justicia Administrativa del Estado de Michoacán de Ocampo, los supuestos de ley de las diversas disposiciones legales que norman el Juicio en Línea, facilitando la consulta de su contenido y alcances sobre la utilización de este servicio informático.

Las definiciones establecidas en el artículo 3 de los Lineamientos para la Utilización del Juicio en Línea ante el Tribunal de Justicia Administrativa de Michoacán de Ocampo, serán aplicables para este documento.

TÉRMINOS Y CONDICIONES

El usuario reconoce y acepta:

I. Cumplir con las disposiciones legales que rigen el Juicio en Línea, siendo éstas el Código de Justicia Administrativa de Michoacán de Ocampo; los Lineamientos para la Utilización del Juicio en Línea ante el Tribunal de Justicia Administrativa del Estado de Michoacán de Ocampo; la Ley de Firma Electrónica Certificada del Estado de Michoacán de Ocampo; la Declaración de Prácticas y Políticas de Certificación del Tribunal de Justicia Administrativa de Michoacán de Ocampo y demás normativa que resulte aplicable;

II. Registrarse en el SIT para tramitar un proceso administrativo en la modalidad de juicio en línea;

III. Que es su responsabilidad la captura correcta de los datos relativos a expresar el carácter conforme a las opciones de los campos requeridos que aparecen con motivo del registro electrónico;

IV. Señalar expresamente en el registro del Juicio en Línea, su identidad, domicilio, teléfono, correo electrónico válido y el documento por medio del cual acreditará su identidad;

V. Proporcionar toda la información requerida para el registro y acceso al Juicio en Línea;

VI. Que la simple captura de los datos del interesado, no significa la conclusión correcta del trámite para el acceso del Juicio en Línea;

VII. Acudir de manera directa y personal al Tribunal para convalidar su identidad mediante la documentación que señalan los Lineamientos en los módulos de registro establecidos, dentro de los tres días hábiles posteriores al registro electrónico;

VIII. Que podrá convalidar su identidad a través de un tercero, servidor público diverso o autorizado, acreditando su carácter legal cuando el trámite lo realice en representación de una persona física, moral o autoridad;

IX. Que los módulos de registro se encuentran en la Secretaría General de Acuerdos ubicada en Avenida Francisco I. Madero Poniente 1622, colonia Nueva Valladolid en la ciudad de Morelia, Michoacán, así como en las sedes regionales de la Defensoría Jurídica del Tribunal de Justicia Administrativa del Estado de Michoacán de Ocampo, ubicadas en las siguientes direcciones:

a) **URUAPAN:** Av. Juárez 125-C, Col. Morelos, Uruapan Michoacán, C.P. 60000, Tel. (452) 519 3692;

b) **ZAMORA:** Calle Galeana Sur # 14, Col. Centro, Zamora Michoacán, C.P. 59600, Tel. (351) 515 7411;

c) **ZITACUARO:** Calle Morelos Sur # 14, Col. Centro, Zitacuaro Michoacán, C.P. 61515, Tel. (715) 153 6324; y,

d) **LÁZARO CÁRDENAS:** Calle Río Tepalcatepec # 74, Col. Primer Sector de Fidelac, Lázaro Cárdenas, Michoacán.

X. Que el horario de atención será de 9:00 a 15:00 horas, todos los días del año, a excepción de los sábados y domingos y los días que estén declarados como inhábiles en el Calendario Oficial de Labores o por el Pleno del Tribunal;

XI. Que solo se podrá tramitar el registro y completar el mismo por una sola vez;

XII. Que ante la falta de convalidación, el registro será eliminado del Sistema del Juicio en Línea, sin perjuicio de iniciar un nuevo trámite;

XIII. Acceder y utilizar el Juicio en Línea, sujetándose a los presentes Términos y Condiciones y demás disposiciones legales aplicables;

XIV. Que el acceso y uso del SIT en la modalidad del Juicio en Línea es gratuito;

XV. Que al optar por el uso del SIT en la modalidad de Juicio en Línea, al presentar demanda administrativa, el usuario no podrá revertir el uso de este servicio;

XVI. Que el español es el idioma oficial para emplearse en el SIT en la modalidad del Juicio en Línea;

XVII. Que será responsable de la veracidad de los datos proporcionados a través del SIT;

XVIII. Que cuando se trate de una autoridad y pretenda modificar su registro, deberá hacerlo en el módulo correspondiente, a través de la persona autorizada para ello, acreditando su carácter y exhibiendo los documentos precisados en los Lineamientos para la Utilización del Juicio en Línea ante el Tribunal;

XIX. La facultad que el Tribunal se reserva para modificar o sustituir los presentes Términos y Condiciones, así como el SIT;

XX. Que el uso y manejo de la clave de acceso, la contraseña y la firma electrónica son intransferibles y de su exclusiva responsabilidad;

XXI. Que es su deber adjuntar el documento donde consta la demanda y en su caso, los anexos, en forma legible y conforme a las condiciones descritas en las especificaciones técnicas de los Lineamientos para la Utilización del Juicio en Línea ante el Tribunal, así como firmarla electrónicamente;

XXII. Que concluido el trámite y enviada la demanda en horario inhábil, la misma se tendrá por presentada en la primera hora del siguiente día hábil;

XXIII. Que el comprobante expedido por el SIT no implica la admisión de la demanda presentada mediante el sistema de Juicio en Línea;

XXIV. La responsabilidad de verificar el contenido y la descripción correcta de los archivos electrónicos anexos y que correspondan a los ofrecidos mediante el SIT;

XXV. Que una vez elegida la utilización del Juicio en Línea, las notificaciones le serán realizadas a través de su cuenta de correo electrónica válida;

XXVI. Que la consulta de expedientes en la modalidad del Juicio en Línea será a través de la página web: www.jel.tjamich.gob.mx, mediante el uso del dispositivos con las características descritas en el anexo técnico de los Lineamientos para la Utilización del Juicio en Línea ante el Tribunal;

XXVII. Que cuando el SIT le impida consultar un expediente en la modalidad del Juicio en Línea, deberá verificar la compatibilidad de su dispositivo con las características técnicas requeridas por la plataforma informática del Tribunal;

XXVIII. Que el representante legal de una persona moral pública o privada podrá solicitar la vinculación de la clave de acceso y contraseña de sus autorizados en términos amplios o únicamente para consulta del expediente del Juicio en Línea;

XXIX. Consultar el expediente en la modalidad del Juicio en Línea las veces que considere necesario, en cualquier día y hora, los 365 días del año;

XXX. Que la realización de alguna conducta prohibida será sancionada conforme a lo previsto en la Ley de Firma Electrónica Certificada del Estado de Michoacán de Ocampo, el Código de Justicia Administrativa del Estado de Michoacán de Ocampo y los Lineamientos para la Utilización del Juicio en Línea ante el Tribunal de Justicia Administrativa del Estado de Michoacán de Ocampo;

XXXI. Que los derechos de autor sobre el diseño conceptual, la imagen, presentación, logotipos y nombres, bajo los cuales opera el Sistema Informático, son propiedad del Tribunal de Justicia Administrativa del Estado de Michoacán de Ocampo y están protegidos por las leyes aplicables a derechos de autor y propiedad intelectual; y que conforme a dicha legislación queda estrictamente prohibido modificar, rentar, arrendar, prestar, vender, distribuir o crear obras derivadas del Sistema Informático del Tribunal de Justicia Administrativa del Estado de Michoacán de Ocampo, ya sea en todo o en parte, con o sin fines de lucro, con excepción a lo expresamente autorizado por el propio Tribunal de Justicia Administrativa del Estado de Michoacán de Ocampo;

XXXII. Que los requisitos técnicos y recomendaciones con las que debe contar su computadora para poder llevar a cabo el Juicio en Línea son las siguientes:

a) Computadora con las siguientes características mínimas: Sistema Operativo Windows: 7 o superior, Mac OS: Leopard o superior, Linux: Ubuntu, Mint u otro con interfaz gráfica, Procesador 1 GHZ de velocidad, Memoria RAM 2 GB, Navegador web Google Chrome actualizado, Lector de PDF Adobe Reader, Foxit Reader u otro;

b) Una cuenta de correo electrónico válido y en uso;

c) Conexión a internet con velocidad de subida de mínimo 5 mb /s;

d) Para usuarios nuevos, un correo comercial (se

recomienda Gmail o Outlook) o institucional válido. Para correos no comerciales (de institución o empresa) se recomienda revisar las restricciones para correos de entrada desconocidos así como evitar la saturación de la bandeja de entrada;

e) Para operadores del Sistema de Juicio en Línea, una cuenta válida institucional;

f) Todos los documentos presentados por el usuario a través del módulo deberán ser en formato PDF, JPG, MP3 y MP4;

g) Los nombres de los archivos a subir deberán de ser lo más cortos posibles, sin exceder los quince caracteres. No contener caracteres especiales, acentos o ñ. El sistema no puede identificar el contenido de los documentos, por lo tanto el nombre de los mismos es relevante, pero si debe ser lo más corto evitando utilizar caracteres de signos como puntos, comas, @, entre otros poco convencionales;

h) Cada archivo deberá tener un tamaño de memoria como máximo de 25 mb (mega bytes). De exceder el tamaño máximo de los anexos, los usuarios podrán fraccionar el documento en varios archivos que no excedan los 25 mb., e incorporarlos al Sistema Informático del Tribunal;

i) El usuario procurará en la medida de lo posible escanear documentos legibles, por lo tanto evitará el escaneo en copia de los documentos, si cuenta con los originales;

j) La calidad mínima de escaneo será 200 x 200 pixeles siempre y cuando el documento sea legible;

k) El servicio de Juicio en Línea emite correos electrónicos a la cuenta proporcionada por el usuario, de no recibir dichos correos en su bandeja principal, el usuario deberá consultar su bandeja de correo no deseado y otorgarle los permisos necesarios para recibir correctamente futuros avisos;

La calidad en la velocidad del servicio dependerá de su velocidad de subida de internet del usuario y del tamaño de los archivos proporcionados.

Considerar el tiempo suficiente para realizar el trámite de registro, remisión de demanda, sus anexos y de promociones subsecuentes, dentro de los plazos legales regulados por el Código de Justicia Administrativa del Estado de Michoacán de Ocampo, con la finalidad de evitar que la demanda o promoción subsecuente no pueda ser enviada dentro del día hábil del vencimiento; y,

XXXIII. Que el Juicio en Línea no aplica para el Procedimiento en materia de Responsabilidades Administrativas.

Así lo acordó el Pleno del Tribunal de Justicia Administrativa del Michoacán de Ocampo, en Sesión del día 11 once de julio de 2019 dos mil diecinueve.

EL SUSCRITO, LICENCIADO EN DERECHO JORGE LUIS ARROYO MARES, COORDINADOR DE ASUNTOS JURÍDICOS HABILITADO PARA EJERCER LAS FUNCIONES DE SECRETARIO GENERAL DE ACUERDOS DEL TRIBUNAL DE JUSTICIA ADMINISTRATIVA DE MICHOACÁN DE OCAMPO, CON FUNDAMENTO EN LO DISPUESTO POR LOS ARTÍCULOS 145 FRACCIÓN I, 159 FRACCIÓN XVI, 164 ÚLTIMO PÁRRAFO Y 165 FRACCIONES I, VI Y XII DEL CÓDIGO DE JUSTICIA ADMINISTRATIVA DEL ESTADO DE MICHOACÁN DE OCAMPO, ASÍ COMO 30 FRACCIONES III Y VII DEL REGLAMENTO INTERIOR DEL TRIBUNAL DE JUSTICIA ADMINISTRATIVA DE MICHOACÁN DE OCAMPO.

C e r t i f i c a

QUE LOS PRESENTES TÉRMINOS Y CONDICIONES PARA LA UTILIZACIÓN DEL JUICIO EN LÍNEA ANTE EL TRIBUNAL DE JUSTICIA ADMINISTRATIVA DE MICHOACÁN DE OCAMPO FUERON APROBADOS POR EL PLENO DEL TRIBUNAL DE JUSTICIA ADMINISTRATIVA DE MICHOACÁN DE OCAMPO, EN SESIÓN DEL DÍA 11 ONCE DE JULIO DE 2019 DOS MIL DIECINUEVE, POR UNANIMIDAD DE VOTOS DE LOS MAGISTRADOS SERGIO MECINO MORALES, PRESIDENTE Y TITULAR DE LA QUINTA SALA ESPECIALIZADA, ARTURO BUCIO IBARRA, TITULAR DE LA SEGUNDA SALA ADMINISTRATIVA, GRISELDA LAGUNAS VÁZQUEZ, TITULAR DE LA TERCERA SALA ADMINISTRATIVA, RAFAEL ROSALES CORIA, TITULAR DE LA CUARTA SALA ESPECIALIZADA Y CARLOS PAULO GALLARDO BALDERAS, MAGISTRADO POR MINISTERIO DE LEY DE LA PRIMERA SALA ADMINISTRATIVA.- MORELIA, MICHOACÁN DE OCAMPO, A 11 ONCE DE JULIO DE 2019 DOS MIL DIECINUEVE.- CONSTE. (Firmado).

AVISO DE PRIVACIDAD INTEGRAL DEL SISTEMA INFORMÁTICO DEL TRIBUNAL DE JUSTICIA ADMINISTRATIVA DEL ESTADO DE MICHOACÁN DE OCAMPO

El Tribunal de Justicia Administrativa del Estado de Michoacán de Ocampo, con domicilio en Av. Francisco I. Madero Poniente N° 1622, Colonia Nueva Valladolid, Morelia, Michoacán, es el responsable del tratamiento de datos personales que proporcione, los cuales serán protegidos conforme a lo dispuesto por la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo y demás normatividad que resulte aplicable.

¿Para qué fines utilizaremos sus datos personales?

Sus datos personales serán recopilados y utilizados para obtener, renovar, revocar o cancelar el Certificado digital de la Firma

Electrónica Certificada necesaria para la utilización del Sistema del Juicio en Línea del Tribunal de Justicia Administrativa del Estado de Michoacán de Ocampo.

Asimismo, se le informa que no se realizarán transferencias de datos personales, salvo aquéllas que sean necesarias para atender requerimientos de una autoridad competente, que estén debidamente fundadas y motivadas, de conformidad con lo dispuesto por los artículos 18, 61, 62 y 66 de la Ley de Protección de Datos Personales del Estado de Michoacán de Ocampo.

¿Que finalidades requieren el consentimiento del Titular?

De conformidad con el artìculo 17 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo, al poner a su disposicioòn el presente Aviso de Privacidad otorga su consentimiento tácito para el tratamiento de sus datos personales para los fines descritos en el paìrrafo que antecede. Todo tratamiento distinto de aquel para el cual fueron recabados, salvo los casos exceptuados, requerirá de consentimiento por escrito de forma libre, expresa e informada por parte del titular de los mismos.

¿Qué datos personales serán recabados?

Para cumplir las finalidades descritas en el presente Aviso de Privacidad se informa que se recaban los siguientes datos personales:

- Nombre(s) y Apellidos;
- Ciudad;
- Estado;
- Identificación vigente con fotografía (Cédula profesional, pasaporte, identificación para votar);
- Fecha de nacimiento;
- Clave Única de Registro de Población;
- Clave de Registro Federal de Contribuyentes;
- Correo electrónico; y,
- Domicilio.

Fundamento para el tratamiento de datos personales.

El Tribunal de Justicia Administrativa del Estado de Michoacán de Ocampo, tratará los datos personales antes señalados con fundamento en lo dispuesto en los artículos 6° de la Constitución Política de los Estados Unidos Mexicanos; 8° de la Constitución Política del Estado Libre y Soberano de Michoacán de Ocampo; 297 E del Código de Justicia Administrativa del Estado de Michoacán de Ocampo; 3 fracción VIII, 18, 61, 62 y 66 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo; así como 8 y 33 de la Ley de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Michoacán de Ocampo; así como los Lineamientos para la Utilización del Juicio en Línea y la Declaración de Prácticas y Políticas de Certificación del Tribunal de Justicia Administrativa del Estado de Michoacán de Ocampo.

Mecanismos de seguridad.

Las áreas del Tribunal de Justicia Administrativa del Estado de Michoacán de Ocampo están obligadas en todo momento a emplear los mecanismos administrativos, técnicos y físicos que permitan garantizar la debida administración y custodia de los datos personales bajo su resguardo, debiendo asegurar su adecuado tratamiento.

¿Cómo ejercer sus derechos de Acceder, Rectificar, Cancelar u Oponerse al uso y tratamiento de sus datos personales (Derechos ARCO) o revocar su consentimiento para el tratamiento sus datos?

De conformidad con lo dispuesto en los artículos 39, 40, 41, 42 y 43 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo usted tiene derecho de: conocer qué datos personales suyos tenemos, para qué los utilizamos y las condiciones del uso que les damos (acceso); solicitar la correción de su información personal en caso de que esté desactualizada, inexacta o incompleta (rectificación); solicitar la eliminación de nuestros registros o bases de datos cuando considere que la misma no está siendo utilizada conforme a los principios, deberes y obligaciones previstas en la normativa (cancelación); y, oponerse al uso de sus datos personales para fines específicos (oposición).

Para ejercer estos derechos denominados ARCO, conforme a lo establecido por los artículos 44, 45, 46, 47, 48, 49, 50 y 51 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo deberá presentar la solicitud respectiva ante la Unidad de Transparencia de este Tribunal, ubicada en Av. Francisco I. Madero Poniente N° 1622, Colonia Nueva Valladolid, Morelia, Michoacán. Para conocer el procedimiento para el ejercicio de estos derechos puede acudir a la Unidad de Transparencia en un horario de lunes a viernes de 9:00 a 16:00 horas, llamar a los teléfonos 01 (443) 3 15 27 26, 3 15 27 40, 3 15, 27 62 o 3 16 14 59; o puede enviar un correo electrónico a la dirección unidaddetransparencia@tjamich.gob.mx.

En términos del artículo 48 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo, para el ejercicio de los derechos ARCO, se deberán observar los siguientes requisitos:

I. El nombre del titular y su domicilio o cualquier otro medio para recibir notificaciones;

II. Los documentos que acrediten la identidad del titular y, en su caso, la personalidad e identidad de su representante;

III. De ser posible, el área responsable que trata los datos personales y ante el cual se presenta la solicitud;

IV. La descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos ARCO, salvo que se trate del derecho de acceso;

V. La descripción del derecho ARCO que se pretende ejercer,

o bien, lo que solicita el titular;

VI. Cualquier otro elemento o documento que facilite la localización de los datos personales, en su caso;

VII. En caso de solicitar el acceso a datos personales, el titular deberá señalar la modalidad en la que prefiere que éstos se reproduzcan;

VIII. Tratándose de una solicitud de cancelación, el titular deberá señalar las causas que lo motiven a solicitar la supresión de sus datos personales en los archivos, registros o bases de datos del responsable; y,

IX. Para una solicitud de oposición, el titular deberá manifestar las causas legítimas o la situación específica que lo llevan a solicitar el cese en el tratamiento, así como el daño o perjuicio que le causaría la persistencia del tratamiento, o en su caso, las finalidades específicas respecto de las cuales requiere ejercer el derecho de oposición.

Transferencia de datos personales.

Le informamos que no se realizarán transferencias de datos personales, salvo aquéllas que sean necesarias para atender requerimientos de una autoridad competente, que estén debidamente fundadas y motivadas, de conformidad con lo dispuesto por los artículos 18, 61, 62 y 66 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo.

Modificaciones al Aviso de Privacidad.

En caso de que exista un cambio de este aviso de privacidad, de conformidad con los dispuesto en el artículo 24 fracción VII de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo, le informamos que lo haremos de su conocimiento a través de la página de internet http://www.tjamich.gob.mx/ o a través de correo electrónico (dirección proporcionada por el titular de los datos personales).

Así lo acordó el Pleno del Tribunal de Justicia Administrativa del Michoacán de Ocampo, en Sesión del día 11 once de julio de 2019 dos mil diecinueve.

EL SUSCRITO, LICENCIADO EN DERECHO JORGE LUIS ARROYO MARES, COORDINADOR DE ASUNTOS JURÍDICOS HABILITADO PARA EJERCER LAS FUNCIONES DE SECRETARIO GENERAL DE ACUERDOS DEL TRIBUNAL DE JUSTICIA ADMINISTRATIVA DE MICHOACÁN DE OCAMPO, CON FUNDAMENTO EN LO DISPUESTO POR LOS ARTÍCULOS 145 FRACCIÓN I, 159 FRACCIÓN XVI, 164 ÚLTIMO PÁRRAFO Y 165 FRACCIONES I, VI Y XII DEL CÓDIGO DE JUSTICIA ADMINISTRATIVA DEL ESTADO DE MICHOACÁN DE OCAMPO, ASÍ COMO 30 FRACCIONES III Y VII DEL REGLAMENTO INTERIOR DEL TRIBUNAL DE JUSTICIA ADMINISTRATIVA DE MICHOACÁN DE OCAMPO.

C E R T I F I C A

QUE EL PRESENTE AVISO DE PRIVACIDAD INTEGRAL DEL SISTEMA INFORMÁTICO DEL TRIBUNAL DE JUSTICIA ADMINISTRATIVA DEL ESTADO DE MICHOACÁN DE OCAMPO FUE APROBADO POR EL PLENO DEL TRIBUNAL DE JUSTICIA ADMINISTRATIVA DE MICHOACÁN DE OCAMPO, EN SESIÓN DEL DÍA 11 ONCE DE JULIO DE 2019 DOS MIL DIECINUEVE, POR UNANIMIDAD DE VOTOS DE LOS MAGISTRADOS SERGIO MECINO MORALES, PRESIDENTE Y TITULAR DE LA QUINTA SALA ESPECIALIZADA, ARTURO BUCIO IBARRA, TITULAR DE LA SEGUNDA SALA ADMINISTRATIVA, GRISELDA LAGUNAS VÁZQUEZ, TITULAR DE LA TERCERA SALA ADMINISTRATIVA, RAFAEL ROSALES CORIA, TITULAR DE LA CUARTA SALA ESPECIALIZADA Y CARLOS PAULO GALLARDO BALDERAS, MAGISTRADO POR MINISTERIO DE LEY DE LA PRIMERA SALA ADMINISTRATIVA.- MORELIA, MICHOACÁN DE OCAMPO, A 11 ONCE DE JULIO DE 2019 DOS MIL DIECINUEVE.- CONSTE. (Firmado).