FISCALÍA GENERAL DEL ESTADO DE MICHOACÁN

ACUERDO 21/2021 POR EL QUE SE EXPIDE LINEAMIENTOS DE LA FIRMA ELECTRÓNICA CERTIFICADA DE LA FISCALÍA GENERAL DEL ESTADO.

PUBLICADO EL 31 DE DICIEMBRE DE 2021

ADRIÁN LÓPEZ SOLÍS, Fiscal General del Estado, en ejercicio de las facultades que me confieren los artículos 100 de la Constitución Política del Estado Libre y Soberano de Michoacán de Ocampo; 2, 18 y 30 fracciones I, XX, XXII, XLI y LI de la Ley Orgánica de la Fiscalía General del Estado de Michoacán; 6 fracciones I y XXXI del Reglamento de la Ley Orgánica de la Fiscalía General del Estado de Michoacán; y,

C O N S I D E R A N D O

Que la Constitución Política del Estado Libre y Soberano de Michoacán de Ocampo, establece que la Fiscalía General del Estado es un órgano autónomo, con personalidad jurídica, patrimonio propio, autonomía financiera, presupuestaria, técnica y de gestión en los términos que determina su Ley Orgánica.

Que la Ley Orgánica de la Fiscalía General del Estado de Michoacán, señala que la persona titular de la Fiscalía General, es el responsable de su conducción, mando y desempeño, en cuanto titular de la institución y superior jerárquico de todas las personas servidoras públicas que la integran y, establece como una de sus atribuciones, expedir su normatividad interna.

Que el Reglamento de la Ley Orgánica de la Fiscalía General del Estado de Michoacán, señala que la Dirección General de Tecnologías de la Información, Planeación y Estadística, es la unidad administrativa especializada competente para establecer y supervisar las directrices en materia tecnológica, coadyuvar en el cumplimiento de los objetivos y gobernanza digital de la institución, así como, contribuir a la eficiencia y la eficacia de la gestión institucional a través de la implementación de la firma electrónica.

Que el Plan de Persecución de Delitos 2.0, 2019-2028, dicta en el Eje Estratégico 6 "*Fortalecimiento Institucional*", la Línea de Acción "*Fiscalía Digital*", la cual considera

como acción específica “*Implementación de la Firma Electrónica Institucional*”, con el objeto de incluir soluciones tecnológicas en apoyo a los procesos operativos y organizacionales, y a su vez, optimizar recursos en pro de la eficiencia y eficacia en la gestión institucional.

Que la Ley de Firma Electrónica Certificada del Estado de Michoacán de Ocampo, establece a la Fiscalía General como autoridad certificadora con atribuciones de expedir certificados de firma electrónica y prestar servicios relacionados con la misma; la disposición de aceptar el uso de mensajes de datos y la presentación de documentos electrónicos, a través de medios de comunicación electrónica; la obligación de crear y administrar un sistema de gestión digital que dicte el control de accesos, los respaldos y la recuperación de información; así como, las condiciones, formalidades y modalidades que deberán observar las personas interesadas en la gestión digital, realizada por medios de comunicación electrónica y conlleve el uso de la firma electrónica certificada.

Que en observancia a las disposiciones jurídicas aplicables, es necesario que la Fiscalía General, implemente un sistema de información de gestión digital, al igual que un dispositivo de creación y verificación de firma electrónica certificada, a fin de disponer de una herramienta eficaz y eficiente, que permita comunicar digitalmente a las diferentes personas usuarias, agilizar procesos al interior y exterior de la institución, mejorar la interacción entre las diversas autoridades del sector público y personas del ámbito privado, facilitar el acceso a la información, optimizar la integridad de la misma, y blindar la seguridad en servicios digitales.

Por lo anteriormente expuesto y fundado se emite el Acuerdo 21/2021 por el cual se expiden los:

LINEAMIENTOS DE LA FIRMA ELECTRÓNICA CERTIFICADA
DE LA FISCALÍA GENERAL DEL ESTADO

CAPÍTULO I

DISPOSICIONES GENERALES

ARTÍCULO 1. Las disposiciones de los Lineamientos de la Firma Electrónica Certificada de la Fiscalía General del Estado, son de carácter general y de observancia obligatoria para las personas servidoras públicas de la Fiscalía General del Estado de Michoacán y, usuarios que elijan utilizar la firma electrónica certificada ante esta institución.

ARTÍCULO 2. Los Lineamientos de la Firma Electrónica Certificada de la Fiscalía General del Estado tienen por objeto:

I. Regular el uso de la firma electrónica certificada en la gestión y servicios digitales de la Fiscalía General del Estado de Michoacán; y,

II. Establecer las bases para la generación, administración y registro de certificados digitales, así como los servicios conexos relacionados con la firma electrónica certificada.

ARTÍCULO 3. Para los efectos de los Lineamientos de la Firma Electrónica Certificada de la Fiscalía General del Estado se entenderá por:

I. **ACTUACIONES ELECTRÓNICAS:** Las diligencias que emite la Fiscalía General que son comunicadas por medios electrónicos;

II. **ACUSE DE RECIBO ELECTRÓNICO**: El mensaje de datos que se emite o genera a través de medios de comunicación electrónica, para acreditar de manera fehaciente la fecha y hora de recepción de documentos electrónicos relacionados con los actos establecidos por estos Lineamientos;

III. **AGENTE CERTIFICADOR:** La persona física autorizada por la Autoridad Certificadora para recibir los datos de los usuarios y personas servidoras públicas interesadas en obtener a firma electrónica certificada, así como administrar lo relacionado con la misma;

IV. **AUTORIDAD CERTIFICADORA:** La Fiscalía General del Estado de Michoacán, órganos autónomos, dependencias y entidades de la Administración Pública Federal o Estatal reconocidos en las normativas aplicables y, los prestadores de servicios de certificación que, conforme a las disposiciones jurídicas, tengan reconocida esta calidad y cuenten con la infraestructura tecnológica para la emisión, administración y registro de certificados digitales, así como para proporcionar servicios conexos;

V. **CERTIFICADO DIGITAL:** El mensaje de datos o registro que confirma el vínculo entre un titular y la llave privada;

VI. **DOCUMENTOS ELECTRÓNICOS:** Los generados, consultados, modificados o procesados por medios electrónicos;

VII. **DGTIPE:** La Dirección General de Tecnologías de la Información, Planeación y Estadística;

VIII. **FIRMA ELECTRÓNICA CERTIFICADA:** Conjunto de datos electrónicos integrados o asociados al mensaje de datos, esta permite asegurar la integridad, autenticidad y la identidad del titular; que ha sido expedida por una Autoridad Certificadora y, que tiene los mismos efectos jurídicos que la firma autógrafa;

IX. **FIRMANTE:** La persona que utiliza su firma electrónica certificada para suscribir documentos electrónicos y, en su caso, mensajes de datos;

X. **FISCALÍA GENERAL:** La Fiscalía General del Estado de Michoacán;

XI. **GESTIÓN DIGITAL:** Las acciones o trámites que se llevan a cabo para obtener un beneficio o cumplir una obligación, a través de medios de comunicación electrónica;

XII. **LEY:** La Ley de Firma Electrónica Certificada del Estado de Michoacán de Ocampo;

XIII. **LINEAMIENTOS:** Los Lineamientos de la Firma Electrónica Certificada de la Fiscalía General del Estado;

XIV. **LLAVE PRIVADA:** La llave de método de cifrado asimétrico, la cual se usa de forma personal o privada para firmar o cifrar datos para ser enviados por medios seguros o inseguros, siendo los poseedores de su par la llave pública los únicos que puedan descifrar los datos;

XV. **LLAVE PÚBLICA:** La llave de método de cifrado asimétrico, la cual se puede entregar a cualquiera y permite descifrar los datos que su par la llave privada haya cifrado;

XVI. **MEDIOS DE COMUNICACIÓN ELECTRÓNICA:** Los dispositivos tecnológicos que permiten efectuar la transmisión y recepción de mensajes de datos y documentos electrónicos;

XVII. **MEDIOS ELECTRÓNICOS:** Los dispositivos tecnológicos para el procesamiento, impresión, despliegue, conservación y, en su caso, modificación de información;

XVIII. **MENSAJES DE DATOS:** La información generada, enviada, recibida, archivada o comunicada a través de medios de comunicación electrónica, que puede contener documentos electrónicos;

XIX. **PROMOCIONES ELECTRÓNICAS:** Las diligencias que realicen los usuarios a través de medios electrónicos;

XX. **REGLAMENTO:** El reglamento de la Ley de Firma Electrónica Certificada del Estado de Michoacán de Ocampo;

XXI. **REQUIRENTE:** El solicitante de firma electrónica certificada o certificado digital homologado;

XXII. **SELLO DIGITAL**: El mensaje de datos que acredita que un documento electrónico fue recibido por el destinatario y estará sujeto a los Lineamientos y la normativa aplicable en materia de firma electrónica certificada;

XXIII. **SERVICIOS CONEXOS:** Los servicios de firmado de documentos electrónicos, de verificación de la vigencia de certificados digitales, de verificación y validación de la unicidad de la llave pública, así como de consulta de certificados digitales revocados, entre otros, que en términos de los Lineamientos y las disposiciones jurídicas aplicables pueden ser proporcionados por la autoridad certificadora;

XXIV. **SERVICIOS DIGITALES:** La actividad que brinda la Fiscalía General de carácter potestativo, general, continuo y disponible a usuarios que tienen por objeto satisfacer una necesidad pública;

XXV. **SISTEMA DE INFORMACIÓN DE GESTIÓN DE FIRMA ELECTRÓNICA:** El sitio desarrollado por la Fiscalía General para el envío y recepción de

documentos y diligencias, así como para la consulta de información relacionada con los actos a que se refieren estos Lineamientos;

XXVI. **TABLERO ELECTRÓNICO:** El medio electrónico a través del cual se pone a disposición de los usuarios y personas servidoras públicas que utilicen la firma electrónica certificada, las actuaciones electrónicas que emita la Fiscalía General, y que genera un acuse de recibo electrónico. Dicho tablero estará ubicado en el Sistema de Información de Gestión de Firma Electrónica de la institución;

XXVII. **TITULAR:** Persona física a quien corresponden los datos personales y representación legal en la firma electrónica certificada; y,

XXVIII. **USUARIOS:** Persona física o moral o autoridad, que utilice la firma electrónica certificada para realizar gestiones digitales por medios de comunicación electrónica ante esta institución.

ARTÍCULO 4. Las personas servidoras públicas de la institución, podrán utilizar la firma electrónica certificada en los casos siguientes:

I. Cuando el Fiscal General, instruya su implementación al caso concreto; y,

II. Cuando las personas servidoras públicas titulares de unidades administrativas lo soliciten y tengan autorización del Fiscal General.

ARTÍCULO 5. La firma electrónica certificada, será de uso obligatorio para las personas servidoras públicas de la institución, cuando en cumplimiento de sus atribuciones se requiera realizar gestión y servicios digitales, así como actuaciones electrónicas.

ARTÍCULO 6. Los usuarios que elijan realizar gestión digital ante la Fiscalía General a través de medios de comunicación electrónica, deberán contar con firma electrónica certificada vigente, cumplir con los requisitos establecidos en estos Lineamientos, la Ley, su reglamento, la normativa aplicable y, manifestar expresamente a la Fiscalía General su conformidad para que la gestión digital se efectúe desde su inicio hasta su conclusión, a través de medios de comunicación electrónica conforme lo señalado en el Anexo 1 de los presentes Lineamientos.

ARTÍCULO 7. La información que se genere en mensajes de datos y documentos electrónicos y en todo lo referente a la firma electrónica certificada, estará sujeta a lo establecido en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo, y la Ley de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Michoacán de Ocampo.

ARTÍCULO 8. Las personas servidoras públicas que hagan mal uso de la información que administre la Fiscalía General como Autoridad Certificadora, así como el uso indebido de la firma electrónica certificada y el certificado digital, estarán sujetas a las responsabilidades administrativas, civiles y penales, establecidas en los ordenamientos que al caso sean aplicables.

ARTÍCULO 9. La DGTIPE es la unidad administrativa responsable de llevar a cabo la aplicación, interpretación y resolución del contenido de los Lineamientos sobre aspectos técnicos u operativos.

En los casos no previstos en los presentes Lineamientos o en caso de que las disposiciones jurídicas aplicables, tengan una interpretación diversa, la DGTIPE es la unidad administrativa encargada de proponer la solución al caso concreto.

ARTÍCULO 10. Quedan exceptuados de la aplicación de estos Lineamientos, los actos de autoridad para los cuales la Constitución Política de los Estados Unidos Mexicanos, la Constitución Política del Estado Libre y Soberano de Michoacán de Ocampo y demás ordenamientos jurídicos que exijan la firma autógrafa por escrito o bien, requieran la concurrencia propia de las personas servidoras públicas o de los usuarios.

ARTÍCULO 11. En materia de recursos y sanciones se observará lo establecido en la Ley y su reglamento.

ARTÍCULO 12. A falta de disposición expresa en estos Lineamientos, se aplicará de forma supletoria la Ley, su reglamento y la normativa aplicable.

CAPÍTULO II
FIRMA ELECTRÓNICA CERTIFICADA

ARTÍCULO 13. La firma electrónica certificada es personal e intransferible, tiene los mismos efectos y validez jurídica que la firma autógrafa.

Puede utilizarse en documentos electrónicos y mensajes de datos, para la gestión y servicios digitales, actuaciones y promociones electrónicas en la Fiscalía General.

La obtención y uso de la firma electrónica certificada implica mantener su reserva, confidencialidad y no comprometerla de forma alguna para un ejercicio indebido.

ARTÍCULO 14. La firma electrónica tendrá el carácter de certificada, cuando cumpla con los elementos siguientes:

I. Tenga un certificado digital vigente;

II. Los datos de creación correspondan únicamente al titular y se encuentren

bajo su control exclusivo;

III. Sea susceptible de verificación y auditoría con los datos incluidos en el certificado digital;

IV. Sea posible detectar cualquier alteración de la firma electrónica hecha después del momento de la firma; y,

V. Esté vinculada al mensaje de datos de modo tal que cualquier modificación de los datos del mensaje ponga en evidencia su alteración.

ARTÍCULO 15. La firma electrónica certificada debe cumplir con los principios rectores siguientes:

I. **Autenticidad:** Otorgar certeza de que el documento electrónico o mensaje de datos, ha sido emitido por el titular, de manera que su contenido le es atribuible al igual que las consecuencias jurídicas que de él deriven;

II. **Confidencialidad:** Garantizar que sólo pueda ser cifrado por el titular y receptor;

III. **Equivalencia Funcional:** Satisfacer el requisito de igualdad entre la firma electrónica certificada y la firma autógrafa, ante documentos impresos, documentos electrónicos y mensajes de datos;

IV. **Integridad:** Dar seguridad de que el documento electrónico o mensaje de datos, ha permanecido completo e inalterado desde su firma, con independencia de los cambios que hubiera podido sufrir el medio que lo contiene como resultado del proceso de comunicación, archivo o presentación;

V. **Neutralidad Tecnológica:** Avalar que la tecnología utilizada para la emisión de certificados digitales y para la prestación de los servicios relacionados con la firma electrónica certificada será aplicada de modo tal que no excluya, restrinja o favorezca la utilización de alguna marca en particular; y,

VI. **No Repudio:** Garantizar que la autoría e integridad de los documentos electrónicos, mensajes de datos y firma electrónica certificada corresponde

exclusivamente al titular.

ARTÍCULO 16. Para el uso correcto de la firma electrónica certificada, las personas servidoras públicas y usuarios deberán contar con los requisitos indispensables siguientes:

I. Un certificado digital vigente, emitido u homologado en términos de los presentes Lineamientos; y,

II. Una llave privada, generada bajo su exclusivo control.

ARTÍCULO 17. Para obtener la firma electrónica certificada, las personas servidoras públicas y los usuarios, deben gestionar el trámite personalmente ante la DGTIPE y cumplir con lo señalado en el Anexo 1, 2 y 3.

ARTÍCULO 18. En el caso de persona moral, sólo podrá obtener la firma electrónica certificada, el representante legal con facultades para actos de dominio o de administración o con su nombramiento respectivo según sea el caso.

ARTÍCULO 19. Cuando la firma electrónica certificada se tramite para ejercer un poder o mandato, su certificado digital deberá incluir los límites con los que se otorga dicha representación.

ARTÍCULO 20. Los usuarios también podrán obtener la firma electrónica certificada, ante las autoridades certificadoras de su elección.

ARTÍCULO 21. La firma electrónica certificada debe ser elaborada mediante los dispositivos de creación y verificación que establezca la DGTIPE.

ARTÍCULO 22. El dispositivo de creación es seguro siempre que:

I. Garantice que los datos utilizados para la generación de la firma electrónica certificada, sólo pueden producirse una vez y se asegure su confidencialidad; y,

II. El dispositivo de creación no altere o modifique los datos del mensaje.

ARTÍCULO 23. El dispositivo de verificación validará que:

I. La firma electrónica certificada es segura;

II. Los datos de la firma electrónica certificada no han sido alterados o modificados; y,

III. El mensaje de datos enviado pertenece al emisor.

CAPÍTULO III
CERTIFICADO DIGITAL

ARTÍCULO 24. El certificado digital es un elemento y requisito indispensable de la firma electrónica certificada. Debe utilizarse por su titular conforme a lo establecido en la Ley, su reglamento, los Lineamientos y demás ordenamientos generados por esta institución.

Tiene una vigencia no mayor a cuatro años, la cual iniciará a partir del momento de su emisión, y expirará el día y en la hora señalada en el mismo.

ARTÍCULO 25. Los efectos del certificado digital son los siguientes:

I. Autentificar que la firma electrónica pertenece a determinada persona; y,

II. Verificar la vigencia de la firma electrónica.

ARTÍCULO 26. El certificado digital se otorga a las personas servidoras públicas de la institución o a los usuarios, una vez que se cumplan los requisitos establecidos en el Artículo 17 y que la DGTIPE revise la información y valide la documentación requerida en la solicitud.

ARTÍCULO 27. El certificado digital, se debe entregar en un medio electrónico y mantenerse bajo el resguardo y responsabilidad del titular.

Una vez recibido el certificado digital por el titular, este debe verificar que ha sido emitido por la DGTIPE, con la finalidad de comprobar su validez.

ARTÍCULO 28. La DGTIPE tiene un término que no debe exceder de cinco días hábiles contados a partir de la fecha de recepción de los requisitos, para resolver sobre el otorgamiento o no del certificado digital.

En caso de negativa, la DGTIPE se debe comunicar con el requirente a través de medios de comunicación electrónica, fundando y motivando las razones de la misma.

Aplicará la negativa ficta, si durante el plazo de cinco días hábiles, la DGTIPE no resuelve sobre el otorgamiento del certificado digital.

ARTÍCULO 29. En caso de que la DGTIPE detecte inconsistencias o duplicidad en los datos y elementos de identificación, se debe rechazar el trámite de firma electrónica certificada y certificado digital homologado.

En los casos en que la información y documentación presentada tenga inconsistencias o errores subsanables, la DGTIPE debe informar al requirente para que acuda ante las Autoridades responsables, para rectificarlas o corregirlas.

En caso de no subsanar las inconsistencias en un plazo de 10 días hábiles posteriores a la entrega de los requisitos, se entenderá como rechazado el trámite, por lo que el requirente deberá iniciar nuevamente el proceso.

ARTÍCULO 30. La estructura de los certificados digitales debe considerar los estándares internacionales ISO/IEC 9594-8:2014 *"The Directory: Public-key and attribute certificate frameworks"* y RFC 5280 *"Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"* actualizado con el RFC 6818 y contendrá, cuando menos, los elementos establecidos en el Anexo 4**.**

ARTÍCULO 31. El certificado digital quedará sin efectos, cuando se actualice alguno de los supuestos siguientes:

I. Expiración de su vigencia;
II. Revocación por la Autoridad Certificadora que lo expidió;
III. Suspensión;
IV. Cancelación;
V. A solicitud del firmante;
VI. Pérdida, extravío, robo o inutilización;
VII. Resolución judicial o administrativa;
VIII. Fallecimiento del firmante o su representante, incapacidad superveniente, total o parcial, de cualquiera de ellos, terminación de la representación o extinción de la persona moral representada;
IX. Cuando se compruebe que los documentos que presentó el requirente de la firma electrónica certificada o certificado digital homologado para acreditar su identidad son falsos; y,
X. Cuando se ponga en riesgo la confidencialidad, integridad o seguridad de los datos de creación de la firma electrónica certificada o certificado digital homologado.

Para los supuestos I, II, III y IV, se estará a lo establecido en la Ley y su reglamento.

ARTÍCULO 32. En materia de los casos de las fracciones V y VI, del artículo 31, el requirente deberá comunicarlo vía correo electrónico a la cuenta oficial firma@tecnologias.fiscaliamichoacan.gob.mx, señalando y adjuntando los requisitos siguientes:

I. Nombre (s) y apellidos del titular del certificado digital;
II. Dirección de correo electrónico del titular del certificado digital;
III. Identificación oficial; y,
IV. Motivo por el cual solicita que el certificado digital quede sin efectos.

Una vez cumplidos estos requisitos, se otorgará al titular un acuse que indicará, la fecha a partir de la cual quedará sin efectos el certificado digital.

ARTÍCULO 33. Respecto a los casos a que se refiere la fracción VIII del artículo 31, el tercero legalmente autorizado, deberá exhibir la documental que acredite el hecho.

ARTÍCULO 34. En cuanto a la fracción IX del artículo 31, la DGTIPE dará vista a las autoridades competentes.

ARTÍCULO 35. Los usuarios que tengan firma electrónica certificada expedida por Autoridad Certificadora distinta a la Fiscalía General, podrán utilizarla ante esta institución siempre y cuando exista convenio de colaboración o coordinación entre ambas, en materia de firma electrónica certificada, reconocimiento u homologación de certificado digital.

ARTÍCULO 36. Los usuarios interesados en la homologación del certificado digital de la firma electrónica certificada observarán lo establecido en el reglamento.

CAPÍTULO IV
MENSAJES DE DATOS Y DOCUMENTOS ELECTRÓNICOS

ARTÍCULO 37. La Fiscalía General acepta, recibe, hace uso y presenta, mensajes de datos y documentos electrónicos que cuenten con firma electrónica certificada a través de medios de comunicación electrónica, con motivo de la gestión digital.

ARTÍCULO 38. Los mensajes de datos y documentos electrónicos que cuenten con firma electrónica certificada, tienen los mismos efectos y certeza jurídica que los presentados con firma autógrafa.

La certificación y validación respecto de su originalidad será potestad del destinatario o receptor.

ARTÍCULO 39. Los mensajes de datos y documentos electrónicos tendrán valor probatorio, cuando se acredite lo siguiente:

- **I.** Que contengan la firma electrónica certificada;
- **II.** La fiabilidad del método en que hayan sido generados, archivados o conservados; y,
- **III.** Que se ha conservado la integridad de la información a partir del momento en que se generaron por primera vez en su forma definitiva como tales o en alguna otra forma.

Las disposiciones del presente artículo no podrán ser aplicables cuando así lo dispongan otras leyes en la materia.

ARTÍCULO 40. La información contenida en los mensajes de datos y en los documentos electrónicos, se manejará de la forma siguiente:

I. Será pública, salvo que la misma esté clasificada como reservada o confidencial en términos de la normatividad aplicable en materia de transparencia y acceso a la información pública; y,

II. De conformidad con las disposiciones previstas en materia de protección de datos personales.

ARTÍCULO 41. Las personas servidoras públicas y los usuarios, cuando envíen mensajes de datos y documentos electrónicos, deberán verificar la firma electrónica certificada, la vigencia del certificado y, la fecha y hora electrónica con que se emiten.

ARTÍCULO 42. El momento de recepción de un mensaje de datos y documentos electrónicos se determinará de la forma siguiente:

I. Al ingresar en el Sistema de Información de Gestión de Firma Electrónica designado por la DGTIPE o por el destinatario; o,

II. En el momento en que la DGTIPE o el destinatario se manifieste sabedor de dicha información.

ARTÍCULO 43. Para que surta efectos un mensaje de datos y los documentos electrónicos, se requiere un acuse de recibo electrónico que contenga sello digital que permita dar plena certeza sobre la fecha y hora de recepción.

La DGTIPE establecerá los medios para que las personas servidoras públicas y los usuarios puedan verificar la autenticidad de los acuses de recibo electrónico.

ARTÍCULO 44. La notificación de los mensajes de datos y documentos electrónicos que cuenten con la firma electrónica certificada, se tendrá por realizada desde el momento en que esta es recibida a través de los medios de comunicación electrónica que se trate, por lo que el uso de estos medios implicará la aceptación.

Las personas servidoras públicas y los usuarios deben asegurarse que los medios de comunicación electrónica elegidos, registren fecha y hora de entrega.

ARTÍCULO 45. Las personas servidoras públicas y los usuarios son responsables de consultar el Tablero electrónico dentro de los plazos y términos que corresponda respecto del asunto del que se trate, de acuerdo a la normatividad aplicable.

ARTÍCULO 46. En los casos de notificaciones que emita la Fiscalía General que se efectúen por medio del Tablero electrónico, los días hábiles se considerarán de veinticuatro horas, comprendidas de las 00:00 a las 23:59 horas.

El sistema del Tablero electrónico deberá estar sincronizado a la hora oficial para los Estados Unidos Mexicanos, generada por el Centro Nacional de Metrología.

ARTÍCULO 47. La Fiscalía General debe conservar en medios electrónicos, los mensajes de datos y los documentos electrónicos con firma electrónica certificada derivados de la gestión digital, durante los plazos de conservación previstos en los ordenamientos aplicables, según la naturaleza de la información.

Podrán hacerse constar íntegramente en forma impresa, cuando así lo soliciten expresamente los interesados o lo determine la autoridad competente.

ARTÍCULO 48. Cuando las personas servidoras públicas y los usuarios, emitan alguna comunicación o promuevan cualquier acción por medios de comunicación

electrónica en hora o día inhábil, se tendrán por emitidos o presentados en la primera hora del día hábil siguiente y día hábil siguiente.

Los mensajes de datos o documentos electrónicos enviados por medios de comunicación electrónica que se refiere el párrafo anterior, se tendrán por no presentados o emitidos, cuando carezcan de la firma electrónica certificada.

ARTÍCULO 49. Cuando se requiera que un documento impreso y con firma autógrafa, sea presentado o conservado en su forma original, tal requisito quedará satisfecho si la copia se genera en un documento electrónico, y se cumple con lo siguiente:

I. Que la migración a una forma digital haya sido realizada o supervisada por la DGTIPE;

II. Que la información contenida en el documento electrónico se mantenga íntegra a partir del momento en que se generó por primera vez en su forma definitiva y sea accesible para su consulta;

III. Que el documento electrónico permita conservar el formato del documento impreso y reproducirlo con exactitud; y,

IV. Que se observe lo previsto en la normativa aplicable en materia de conservación de mensajes de datos y de los documentos electrónicos con firma electrónica certificada.

Además, se observará lo establecido en materia de archivo y disposiciones jurídicas aplicables.

ARTÍCULO 50. La información de un mensaje de datos se considerará presentada en forma original, si conserva la integridad y autenticidad de los componentes con los que se generó por primera vez, en su forma definitiva.

ARTÍCULO 51. Todo mensaje de datos se tendrá por expedido en el lugar donde el emisor tenga su domicilio registrado en el certificado digital y por recibido en el lugar donde el destinatario tenga el suyo, salvo prueba o acuerdo en contrario.

ARTÍCULO 52. En el supuesto de que por causas imputables a la Fiscalía General los usuarios se encuentren imposibilitados para consultar el Tablero electrónico o abrir los documentos electrónicos que contengan la información depositada en el mismo, lo harán del conocimiento de la propia institución a más tardar dentro de los tres días hábiles siguientes a aquél en que ocurra dicho impedimento, a través de los siguientes:

I. Por medios de comunicación electrónica;
II. Mediante su registro en el Tablero electrónico;
III. Por correo electrónico dirigido a firma@tecnologias.fiscaliamichoacan.gob.mx; y,
IV. Mediante escrito con firma autógrafa dirigido a la Fiscalía General y presentado en el inmueble donde se ubiquen las oficinas de la DGTIPE.

ARTÍCULO 53. Cuando las promociones electrónicas y gestión digital o la documentación que la acompaña no pueda atenderse por contener virus informáticos u otros problemas técnicos imputables al usuario, la Fiscalía General debe requerirlo a efecto de que subsane la deficiencia respectiva dentro del término de tres días hábiles, contados a partir del día hábil siguiente a aquel en que se haya realizado la notificación, apercibiéndolo de que en caso de no atender el requerimiento, se tendrá por no presentada su proceder o por no exhibida la documentación en su caso.

ARTÍCULO 54. La Fiscalía General debe generar un acuse de recibo electrónico para hacer constar la recepción de promociones electrónicas, el cual deberá contener como datos mínimos los siguientes:

I. Fecha y hora del depósito de las promociones electrónicas;
II. Fecha y hora de apertura de las promociones electrónicas;
III. Descripción de las promociones electrónicas;
IV. Nombre de la unidad administrativa que recibe;
V. Datos de quien realiza las promociones electrónicas; y,
VI. La aceptación expresa del usuario de que las subsiguientes notificaciones se efectuarán por el mismo medio.

Los usuarios que utilicen la firma electrónica certificada, deberán generar un acuse de recibo electrónico que contenga su firma electrónica certificada para hacer constar la recepción de las actuaciones electrónicas de la Fiscalía General por la gestión digital realizada, el cual deberá contener los datos mínimos establecidos en el presente artículo.

ARTÍCULO 55. Los mensajes de datos y documentos electrónicos suscritos con firma electrónica certificada, deberán permitir y verificar la integridad y autenticidad de los mismos al ser impresos.

Su representación impresa debe contener una cadena de caracteres asociados a los mensajes de datos o documentos electrónicos de que se trate, a la firma electrónica certificada y al sello digital que permita comprobar la autenticidad de su contenido y, cuando corresponda, el momento de su recepción.

CAPÍTULO V
AUTORIDAD CERTIFICADORA, DGTIPE Y AGENTES CERTIFICADORES

ARTÍCULO 56. La Fiscalía General es Autoridad Certificadora reconocida en la Ley, con facultades para expedir firma electrónica certificada, servicios conexos, homologar y dejar sin efectos certificados digitales; el ejercicio de esta autoridad se realiza a través de la DGTIPE y los agentes certificadores que estime pertinentes.

Para efectos del trámite para la obtención de la firma electrónica certificada, servicios conexos, homologación y dejar sin efectos certificados digitales se señala lo siguiente:

I. La unidad administrativa operadora de la Fiscalía General, es la DGTIPE;

II. El domicilio al que deberán acudir las personas servidoras públicas y los usuarios es el inmueble donde se ubiquen las oficinas de la DGTIPE;

III. El correo electrónico para información en la materia es firma@tecnologias.fiscaliamichoacan.gob.mx; y,

IV. El teléfono para información en la materia es 443 298 2600.

ARTÍCULO 57. La Fiscalía General como Autoridad Certificadora a través de la DGTIPE, tiene las atribuciones y obligaciones siguientes:

I. Generar la firma electrónica certificada y brindar los servicios conexos;

II. Expedir y homologar certificados digitales;

III. Implementar el Registro de Certificados Digitales de Firma Electrónica Certificada que se expiden, se dejen sin efectos o se homologan;

IV. Autorizar a otra entidad o dependencia de la administración pública estatal o municipal para expedir certificados digitales y servicios conexos, señalando los límites y alcances de cada autorización;

V. Crear un Sistema de Información de Gestión de Firma Electrónica;

VI. Dejar sin efectos certificados digitales de firma electrónica certificada, cuando se actualice alguno de los supuestos previstos en el Artículo 37 de los

Lineamientos;

VII. Garantizar la autenticidad, integridad, conservación, confidencialidad y confiabilidad de la firma electrónica certificada, así como de los servicios conexos;

VIII. Preservar la confidencialidad, integridad y seguridad de los datos personales de los titulares de la firma electrónica certificada y los certificados digitales;

IX. Celebrar convenios de colaboración o coordinación con otras Autoridades Certificadoras, en materia de firma electrónica certificada, reconocimiento u homologación de certificado digital;

X. Reunirse con otras Autoridades Certificadoras en comité técnico para colaborar entre sí a efecto de establecer los estándares tecnológicos y operativos de la infraestructura de la firma electrónica certificada y servicios electrónicos, aplicables en el ámbito de su competencia;

XI. Colaborar en el desarrollo de sistemas informáticos internos y externos para la prestación de servicios;

XII. Establecer el Registro Público de Prestadores de Servicios de Certificación;

XIII. Prestar el servicio de consignación de la fecha electrónica, respecto de los mensajes de datos;

XIV. Contar con un archivo electrónico; y,

XV. Las demás que establezcan las disposiciones jurídicas aplicables.

ARTÍCULO 58. Respecto a la fracción III del artículo 57, la Fiscalía General debe mantener el Registro de Certificados Digitales de Firma Electrónica Certificada de forma pública, mantenerlo actualizado y garantizar a cualquier interesado la consulta a través de medios de comunicación electrónica.

ARTÍCULO 59. En materia de la fracción V del artículo 57, el Sistema de Información de Gestión de Firma Electrónica debe establecer el control de accesos, los respaldos y la recuperación de información, con mecanismos confiables de seguridad, disponibilidad, integridad, autenticidad, confidencialidad y custodia.

ARTÍCULO 60. En lo correspondiente a la fracción IX del artículo 57, la Fiscalía General establecerá los requisitos jurídicos, técnicos, materiales, financieros y observará lo dispuesto en el reglamento.

ARTÍCULO 61. Respecto a la fracción XIV del artículo 57, la Fiscalía General observará lo establecido en la Ley, su reglamento y las disposiciones normativas aplicables.

ARTÍCULO 62. La DGTIPE como unidad administrativa competente para establecer y supervisar las directrices en materia tecnológica, así como responsable de la implementación de la firma electrónica certificada tiene las facultades siguientes:

I. Elaborar planes de seguridad y emergente, por el uso de medios electrónicos y firma electrónica certificada;

II. Contar con medidas de seguridad para proteger la infraestructura tecnológica, los procesos, la información y los datos derivados de la operación como Autoridad Certificadora;

III. Contar con medidas y mecanismos de respaldo de información de acuerdo con las disposiciones normativas aplicables en la materia;

IV. Actualizar la tecnología aplicada al uso de medios electrónicos y firma electrónica certificada de conformidad con los estándares tecnológicos internacionales vigentes y a la disponibilidad presupuestal;

V. Adoptar medidas físicas, técnicas y administrativas que garanticen la integridad, confidencialidad e inalterabilidad de la gestión digital, actuaciones y promociones electrónicas, llaves criptográficas asociadas a la Autoridad Certificadora, así como todo lo relacionado con la firma electrónica certificada y servicios conexos;

VI. Utilizar sistemas y productos fiables que estén protegidos contra toda alteración, que aseguren la seguridad técnica y criptográfica;

VII. Diseñar, ejecutar y administrar los dispositivos de creación y verificación de la firma electrónica certificada, enmarcados en las mejores prácticas en la materia;

VIII. Coordinar la administración de la infraestructura tecnológica necesaria para la implementación de la firma electrónica certificada;

IX. Establecer y operar los esquemas de monitoreo para garantizar la disponibilidad de la infraestructura que soporta los procesos operativos asociados a la firma electrónica certificada;

X. Brindar las facilidades para que se realicen procesos de auditoría en materia de firma electrónica certificada y seguridad informática, así como ejecutar los procesos de remediación que se consideren adecuados;

XI. Presupuestar los recursos necesarios para la implementación de la firma electrónica certificada; y,

XII. Las demás que se deriven de las disposiciones de los presentes Lineamientos y normatividad aplicable.

ARTÍCULO 63. Para dar cumplimiento a las atribuciones y obligaciones de la Fiscalía General como Autoridad Certificadora, los agentes certificadores tienen las funciones siguientes:

I. Recibir y dar trámite a las solicitudes de emisión de firma electrónica certificada y certificado digital homologado;

II. Solicitar la comparecencia del requirente de firma electrónica certificada y certificado digital homologado para su identificación;

III. Recabar datos personales directamente de los titulares de los mismos o con su consentimiento explícito;

IV. Obtener del requirente una carta responsiva, respecto del uso de la firma electrónica certificada;

V. Informar al requirente de firma electrónica certificada y certificado digital, previo a su expedición, sobre las condiciones precisas de utilización,

características y costo;

VI. Entregar al requirente un acuse oficial de haber solicitado la firma electrónica certificada;

VII. Generar un expediente de los requirentes de firma electrónica certificada y certificado homologado;

VIII. Revisar la información y validar la coincidencia entre los datos de la solicitud de firma electrónica certificada y los documentos presentados que la acompañan;

IX. Comprobar por los medios idóneos autorizados por las leyes, la identidad y cualesquiera circunstancias personales relevantes de los requirentes, para la expedición de la firma electrónica certificada y el certificado digital;

X. Notificar al requirente respecto de inconsistencias o duplicidades en la documentación que se presente;

XI. Informar a los requirentes, las razones por las cuales, en su caso, no fue posible emitir un certificado digital;

XII. Adoptar las medidas necesarias para difundir el uso correcto de la firma electrónica certificada;

XIII. Realizar el procedimiento de certificación electrónica de identidad;

XIV. Facilitar a los requirentes de firma electrónica certificada y certificado digital, los mecanismos de creación de llave pública o privada, de verificación de firma electrónica certificada y validez del certificado digital;

XV. Informar al requirente sus derechos y obligaciones como titular de la firma electrónica certificada y certificado digital;

XVI. Solicitar al requirente un acuse de conformidad de haberle entregado la firma electrónica certificada, homologación del certificado digital o en su caso, la invalidez;

XVII. Efectuar acciones para dotar de autenticidad, integridad, conservación, confidencialidad y confiabilidad a la firma electrónica certificada, el certificado digital y servicios conexos;

XVIII. Conservar, resguardar y hacer uso correcto de los datos personales, la

información y documentos presentados por los requirentes, de conformidad con las disposiciones jurídicas aplicables;

XIX. Administrar el Registro de Certificados Digitales de Firma Electrónica Certificada que se expiden, se dejen sin efectos o se homologan;

XX. Registrar y administrar certificados digitales;

XXI. Administrar el Sistema de Información de Gestión de Firma Electrónica;

XXII. Administrar el Tablero electrónico;

XXIII. Administrar el Registro Público de Prestadores de Servicios de Certificación;

XXIV. Llevar el control y administración de los requirentes de la firma electrónica certificada y certificado digital homologado;

XXV. Recibir y dar trámite a las solicitudes de homologación, revocación, suspensión y extinción de certificados digitales, así como las correspondientes para dejarlos sin efectos;

XXVI. Realizar adecuaciones a los certificados digitales para invalidarlos cuando sea necesario y actualizar su estado en el Registro correspondiente;

XXVII. Conservar y registrar toda la información y documentación relativa a la firma electrónica certificada y certificado digital, durante quince años, así como observar las disposiciones jurídicas aplicables en materia de archivo; y,

XXVIII. Las que le instruya la persona titular de la DGTIPE, las que se deriven de las disposiciones de los presentes lineamientos y demás normatividad aplicable.

ARTÍCULO 64. En lo relacionado a la fracción III del artículo 63, la Fiscalía General podrá recabar únicamente los datos necesarios para la expedición y actualización del certificado digital, y serán utilizados exclusivamente para los fines legales y legítimos para los que fueron otorgados.

CAPÍTULO VI
SERVICIOS INFORMÁTICOS CON LA FUNCIONALIDAD DE FIRMA ELECTRÓNICA CERTIFICADA

ARTÍCULO 65. Las unidades administrativas de la Fiscalía General que necesiten implementar procesos y procedimientos a través de servicios informáticos con la funcionalidad de firma electrónica certificada, deberán solicitar a la DGTIPE la asesoría y acompañamiento correspondiente.

ARTÍCULO 66. Las unidades administrativas de la Fiscalía General solicitantes cuando incorporen el uso de la firma electrónica certificada en los procesos y procedimientos o servicios en donde se lleven a cabo mensajes de datos, documentos y actuaciones electrónicas, gestión y servicios digitales, deberán atender y cumplir con los puntos y las características especificadas en la guía de operación que, como mínimo, deberá establecer lo siguiente:

I. Objetivo;
II. Glosario, siglas y abreviaturas;
III. Áreas encargadas de la interpretación y resolución de los casos no previstos;
IV. Ingreso al Sistema o de los beneficiarios o del procedimiento para el registro de los beneficiarios;
V. Operación del Sistema o flujos de operación o del mantenimiento del Sistema;
VI. Actividades de análisis y diagnóstico de la infraestructura o de la validación del comportamiento de la infraestructura; y,
VII. Los demás que se consideren necesarios.

ARTÍCULO 67. La utilización de los sistemas de servicios informáticos en la Fiscalía General, así como de la información registrada en ellos, será de uso restringido y solamente las personas autorizadas podrán hacer uso de los mismos para los fines establecidos por la propia institución.

CAPÍTULO VII

REQUIRENTES DE FIRMA ELECTRÓNICA CERTIFICADA Y CERTIFICADO DIGITAL HOMOLOGADO

ARTÍCULO 68. Los requirentes de firma electrónica certificada y certificado digital homologado, tienen además de los derechos y obligaciones establecidos en la Ley, su reglamento y, la normatividad aplicable, los siguientes:

I. Derechos:

a) A ser informado sobre:

1. Los derechos y obligaciones que adquiere como titular de la firma electrónica certificada o certificado digital homologado;

2. Las características generales de los procedimientos para la generación y emisión del certificado digital y la creación de la llave privada; y,

3. Los supuestos por los que el certificado digital quedará sin efectos;

b) A que se proteja su información personal de conformidad a la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo, y la Ley de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Michoacán de Ocampo;

c) A solicitar la modificación de datos y elementos del certificado digital, cuando así convenga a sus intereses; y,

d) Intervenir cuando se actualice alguno de los supuestos por los que el certificado digital quede sin efectos.

II. Obligaciones:

a) Cumplir con todos los requisitos y requerimientos solicitados;

b) Usar bajo su única y exclusiva responsabilidad la firma electrónica certificada y el certificado digital;

c) Custodiar y controlar adecuadamente los datos de creación de la firma electrónica y la llave privada vinculada con ellos, a fin de mantenerlos en secreto;

d) Resguardar la firma electrónica certificada y todos sus componentes en un medio electrónico, óptico o magnético que sea de su uso exclusivo;

e) Solicitar a la DGTIPE la revocación o dejar sin efectos su certificado digital, cuando proceda en términos de los presentes Lineamientos, y en caso de que la integridad o confidencialidad de sus datos de creación de firma o su frase de seguridad hayan sido comprometidos y, presuma que su llave privada pudiera ser utilizada indebidamente; y,

f) Dar aviso a la DGTIPE de cualquier modificación de los datos que haya proporcionado para su identificación personal, a fin de que ésta incorpore las modificaciones en los registros correspondientes y emita una nueva firma electrónica certificada y certificado digital.

ARTÍCULO 69. Una vez que la Fiscalía General expida la firma electrónica certificada o autorice la homologación de certificado digital, los requirentes podrán

emplearla en esta institución y autoridades con las que exista convenio de colaboración o coordinación entre ambas, en materia de firma electrónica certificada, reconocimiento u homologación de certificado digital.

CAPÍTULO VIII
ANEXOS

ARTÍCULO 70. ANEXO 1. MANIFESTACIÓN SOBRE GESTIÓN DIGITAL A TRAVÉS DE MEDIOS DE COMUNICACIÓN ELECTRÓNICA.

ARTÍCULO 71. ANEXO 2. FORMATO DE SOLICITUD PARA FIRMA ELECTRÓNICA.

ARTÍCULO 72. ANEXO 3. CARTA RESPONSIVA USO DE LA FIRMA ELECTRÓNICA CERTIFICADA.

ARTÍCULO 73. ANEXO 4. ESTRUCTURA DE LOS CERTIFICADOS DIGITALES.

ARTÍCULO 74. ANEXO 5. ACUSE RECEPCIÓN DE SOLICITUD DE FIRMA ELECTRÓNICA CERTIFICADA.

ARTÍCULO 75. ANEXO 6. ACUSE DE GENERACIÓN Y ENTREGA DE FIRMA ELECTRÓNICA CERTIFICADA.

ARTÍCULO 76. ANEXO 7. ACUSE DE HOMOLOGACIÓN Y ENTREGA DE CERTIFICADO DIGITAL.

ARTÍCULO 77. ANEXO 8. ACUSE DE CERTIFICADO DIGITAL SIN EFECTOS.

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

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

SEGUNDO. Se instruye a la persona titular de la Dirección General Jurídica y de Derechos Humanos, realizar las acciones necesarias para la publicación del presente Acuerdo, en el Periódico Oficial del Gobierno Constitucional del Estado de Michoacán de Ocampo.

TERCERO. Notifíquese a las personas titulares de la Dirección General de Tecnologías de la Información, Planeación y Estadística, y Dirección General de Administración de la Fiscalía General del Estado, para que conforme a sus atribuciones den cumplimiento a lo establecido en el presente Acuerdo.

CUARTO. Notifíquese a las personas titulares de las unidades administrativas de la Fiscalía General del Estado, para que en el ámbito de su competencia y con la debida coordinación institucional, realicen las acciones necesarias para dar cumplimiento y difusión del presente Acuerdo a su personal adscrito.

QUINTO. La Dirección General de Tecnologías de la Información, Planeación y Estadística en coordinación con las unidades administrativas de la institución, elaborará el calendario para generar la firma electrónica certificada de las personas servidoras públicas, priorizando a las unidades administrativas que por su naturaleza deban implementar la firma electrónica certificada a la brevedad.

SEXTO. El uso de la firma electrónica certificada en la Fiscalía General, estará sujeta a que esta autoridad tenga las herramientas tecnológicas necesarias y el Fiscal General instruya en que unidades administrativas se implementará.

SÉPTIMO. La Dirección General de Administración, designará los recursos necesarios para implementar el desarrollo de la firma electrónica certificada, así como todo lo necesario para su operación y funcionamiento.

Así lo acordó y firma el Mtro. Adrián López Solís, Fiscal General del Estado.

(FIRMADO)

Morelia, Michoacán a 13 de diciembre de 2021.