



GOBIERNO DE TAMAULIPAS
PODER JUDICIAL

ACUERDO GENERAL 4/2024

PÚBLICO EN GENERAL P R E S E N T E.-

En sesión ordinaria celebrada en esta propia fecha, el Pleno del Consejo de la Judicatura del Estado, emitió el siguiente Acuerdo:

Acuerdo General 4/2024 del Pleno del Consejo de la Judicatura del Estado, mediante el cual se designa a la Dirección de Informática como Autoridad Certificadora de ésta Judicatura.

CONSIDERANDO

PRIMERO.- Que de conformidad con los párrafos segundo y tercero del artículo 100 de la Constitución Política del Estado, la administración, vigilancia y disciplina del Poder Judicial del Estado, con excepción del Pleno del Supremo Tribunal de Justicia, estará a cargo del Consejo de la Judicatura del Estado contando con independencia técnica, de gestión y para emitir sus resoluciones. Que congruente con lo anterior, el artículo 114, apartado B, fracciones XV, XVII y XXVIII de la Constitución Política del Estado, confiere al Consejo de la Judicatura, entre otras atribuciones, elaborar los reglamentos, acuerdos y circulares necesarios para la buena marcha administrativa del Poder Judicial, dentro del ámbito de su competencia, tendientes a mejorar la impartición de justicia; dictar las medidas que estime pertinentes para que la impartición de justicia sea pronta, completa e imparcial; y, las demás facultades y obligaciones que las leyes le otorguen.

SEGUNDO.- Que el precepto 122, en sus fracciones XVI y XVIII, de la Ley Orgánica del Poder Judicial, establece que son atribuciones del Consejo de la Judicatura elaborar reglamentos, acuerdos y circulares necesarios para la buena marcha administrativa del Poder Judicial, así como la de dictar, en Pleno, Comisiones o por conducto de su Presidente, las medidas que se estimen pertinentes para que la impartición de justicia sea pronta, completa e imparcial.

TERCERO.- Que la fracción I, del artículo 3º de la Ley de Firma Electrónica Avanzada para el Estado de Tamaulipas, establece que para los efectos de ese ordenamiento, se entiende por Autoridad Certificadora a la dependencia o entidad facultada para otorgar un certificado de firma electrónica avanzada o, en su caso, autorizar la prestación de servicios de certificación, así como la prestación de otros servicios relacionados con la firma electrónica avanzada. Por su parte, el artículo 23 de esa Ley, señala que serán autoridades certificadoras en su respectivo ámbito de competencia: I.- El Poder Ejecutivo, por conducto de la Secretaría; II.- El Poder Legislativo; III.- El Poder Judicial; IV.- Los organismos autónomos; y V.- Los ayuntamientos. Refiriendo que los sujetos establecidos en las fracciones II a V de ese artículo, designarán a la dependencia o entidad encargada de llevar a cabo la función de autoridad certificadora, dentro de sus respectivos ámbitos de competencia.

CUARTO.- Que el artículo 24 de la Ley de Firma Electrónica Avanzada para el Estado de Tamaulipas, señala que son atribuciones de las autoridades certificadoras, las siguientes: I.- Otorgar a las personas físicas o morales y organismos públicos certificados de firma electrónica y prestar servicios relacionados con la certificación; II.- Facultar a los organismos públicos para que expidan certificados de firma electrónica y a prestar servicios relacionados con la certificación; III.- Llevar el registro de certificados de firma electrónica, así como el de prestadores de servicios de certificación, autorizados para expedir certificados de firma electrónica; IV.-

Mantener actualizado un directorio o relación permanente de los prestadores de servicios de certificación y publicarlo en el Periódico Oficial del Estado en el mes de enero de cada año; V.- Celebrar los convenios de colaboración entre sí, para la prestación de servicios de certificación, así como establecer los estándares tecnológicos y operativos de la infraestructura de la firma electrónica avanzada y servicios electrónicos, aplicables en el ámbito de su competencia; VI.- Colaborar en el desarrollo de sistemas informáticos internos y externos para la prestación de servicios; VII.- Recibir las solicitudes para la creación de la firma; VIII.- Ejecutar el procedimiento para la creación de la firma; IX.- Expedir o negar la firma; X.- Establecer un registro de firmas, que contenga: el número de registro asignado, datos de identificación del titular y demás datos requeridos para el otorgamiento de la certificación, que garantice la disponibilidad de la información, de manera regular y continua, a través de su página de Internet. Dicho registro será público en los términos de la Ley; XI.- Mantener actualizado y disponible el Registro Único de Prestadores de Servicios de Certificación y publicarlo en el Periódico Oficial del Estado en el mes de enero de cada año; XII.- Expedir los lineamientos, políticas, procedimientos y mecanismos que el certificador se obliga a cumplir en la prestación de sus servicios de certificación; XIII.- Iniciar el procedimiento para actualizar las disposiciones técnicas que permitan el uso de tecnologías y medios electrónicos, de conformidad con la Ley; XIV.- Facilitar al solicitante de un certificado de firma electrónica certificada, los mecanismos necesarios para la generación de sus claves privada y pública, en forma secreta y bajo su total control; XV.- Elaborar planes de seguridad y de contingencia, que garanticen permanentemente el acceso a los servicios que ofrece la Autoridad Certificadora, por el uso de medios electrónicos y de la firma por parte de los usuarios; XVI.- Contar con medidas de seguridad para proteger la infraestructura tecnológica, los procesos, la información y los datos derivados de la operación como Autoridad Certificadora; XVII.- Contar con medidas y mecanismos de respaldo de información de acuerdo a la normatividad establecida en la materia; XVIII.- Asesorar a los usuarios de medios electrónicos y de la firma que efectúen trámites y/o servicios ante las Dependencias y Entidades, en su manejo y utilización; XIX.- Asesorar y capacitar, previa solicitud o convenio, a los sujetos establecidos en el artículo 2º de la Ley, en el manejo y utilización de medios electrónicos y de la firma cuando así se solicite por los mismos; XX.- Evaluar los informes técnicos de los Prestadores de Servicios de Certificación que se encuentren autorizados; XXI.- Actualizar la tecnología aplicada al uso de medios electrónicos y de la firma de conformidad con los estándares tecnológicos internacionales vigentes, que garantice un servicio eficaz; XXII.- Desarrollar un programa de calidad para la mejora continua del uso de medios electrónicos y de la firma para los sujetos que hagan uso de los mismos, que se considere dentro de su ámbito de competencia; XXIII.- Emitir certificados digitales que cumplan como mínimo con los requisitos establecidos en la Ley, así como revocarlos inmediatamente después de tener conocimiento de cualquiera de los supuestos previstos; XXIV.- Implementar los programas informáticos que permitan registrar los datos de identificación del usuario de la firma; XXV.- Emitir lineamientos que garanticen la integridad, confidencialidad y autenticidad de la información y de la firma, contenidas en las actuaciones electrónicas; XXVI.- Establecer y difundir los requisitos que debe cubrir el solicitante y el procedimiento para la creación de la firma; XXVII.- Difundir, impulsar y promover el uso de medios electrónicos y firma electrónica; XXVIII.- Ofrecer el servicio de revocación de certificados en línea; XXIX.- Decretar la revocación o extinción de la firma; XXX.- Celebrar convenios de colaboración con cualquier otra entidad, a fin de asumir total o parcialmente las funciones y servicios en materia de firma electrónica que establece la presente Ley. En los convenios que se celebren conforme a la presente fracción, se debe incluir lo siguiente: a) Homologación normativa y técnica; b) Registro; c) Alcance; y d) Límites y vigencia. XXXI.- Las demás que les otorga esa Ley.



CONSEJO DE LA JUDICATURA
DEL ESTADO DE TLAXCALA
SECRETARÍA DE JUSTICIA
CD. MCT



GOBIERNO DE TAMAULIPAS
PODER JUDICIAL

QUINTO.- Que el artículo 3º del Reglamento para el Acceso a los Servicios del Tribunal Electrónico del Poder Judicial del Estado de Tamaulipas define a “Entidades Certificadoras” como las áreas responsables de recibir y corroborar la documentación de los usuarios solicitantes del Certificado Digital y a su vez de generar la Firma Electrónica Avanzada para su entrega al usuario solicitante, conforme sea determinado por el Consejo de la Judicatura y pudiendo operar como tal los departamentos de Informática en el Estado o las áreas jurisdiccionales o administrativas que designe el propio.

SEXTO.- Que el artículo 148 de la Ley Orgánica del Poder Judicial del Estado de Tamaulipas, refiere que la Dirección de Informática funcionará a través de tres vertientes fundamentales que se encargarán del desarrollo y tecnologías de información, de la operación y el mantenimiento, y la de Internet. Por su parte, el numeral 150 de ese ordenamiento hace referencia que corresponde a esa Dirección, como función esencial, proporcionar el soporte técnico necesario en materia de informática en apoyo a las funciones administrativas y de impartición de justicia, susceptibles de ser sistematizadas y automatizadas mediante equipos electrónicos, a cuyo efecto tendrá las siguientes funciones: I.- Diseñar los programas y sistemas informáticos de apoyo a todas las áreas del Poder Judicial, que permitan su constante desarrollo; II.- Establecer políticas de seguridad sobre información, sistemas y programas informáticos; entre otras.

SÉPTIMO.- Que la Organización Civil México Evalúa, en el “Diagnóstico de implementación de herramientas tecnológicas en los poderes judiciales en México”, señala:

“El Poder Judicial de Tamaulipas es uno de los poderes judiciales que ha implementado el uso de la firma electrónica avanzada para usuarios internos y externos, por lo que se ha integrado tanto en los sistemas de gestión, como en el Tribunal Electrónico. Al respecto, el titular del departamento de Informática y Telecomunicaciones mencionó lo siguiente:

[Quisiera] subrayar qué significa que estén firmados todos los documentos en el juzgado con firma electrónica avanzada. Le damos una transparencia y una seguridad al usuario toda vez que la firma electrónica avanzada lleva fecha, hora, minuto y segundo en el que se firmó. Aquello que antaño existía que escondían los documentos y los acuerdos o que los hacían después, que costuraban y descosturaban, eso nosotros [no lo tenemos] (...) Poco a poco fuimos fortaleciendo los sistemas de gestión [desde] hace cuatro o cinco años para acá. Porque la firma electrónica avanzada la tenemos por uso del usuario externo por el tribunal electrónico, pero ya el usuario interno nuestro, como jueces y secretarios que firman cada documento, cada acuerdo que hagan, de 2018 para acá, [lo hacen] al 100%. Incluso los actuarios, no nada más los jueces y secretarios, sino también los actuarios. Entonces eso da una seguridad tremenda, los documentos están asegurados con esa información (A. Cantú Garza, comunicación personal, 11 de agosto de 2021).¹

OCTAVO.- Que en fecha veinticuatro de mayo de dos mil veintitrés, se instaló y tomó protesta el Comité de Innovación y Tecnología Judicial, que dentro de las atribuciones con las que cuenta y que fueron establecidas por acuerdo de veinte abril del año pasado, destacando: “I. Proponer al Pleno del Consejo de la Judicatura y, en su caso, a la Comisión que por competencia corresponda, los criterios considerados como buenas prácticas, reglamentos, acuerdos, lineamientos, políticas, bases, estrategias y prioridades institucionales para implementar en aspectos relacionados a la innovación y tecnología judicial;”

NOVENO.- Que mediante oficio CITJ/3/2024 de fecha doce de febrero del presente año, la Presidenta del Comité de Innovación y Tecnología Judicial, informa que en la

¹ Consultable en: <https://www.mexicoevalua.org/wp-content/uploads/2022/02/diagnostico-3feb-ok.pdf>

Segunda Sesión Ordinaria de ese Comité en el presente año, se aprobó un punto de acuerdo, a efecto de proponer a este Órgano Colegiado, que se designe a la Dirección de Informática como Autoridad Certificadora de ésta Judicatura, asimismo que se emitan Lineamientos de operatividad.

DÉCIMO.- Que es importante señalar que un certificado digital es un archivo electrónico utilizado para autenticar la identidad de una persona o entidad en línea, mientras que la firma electrónica es el proceso de firmar documentos de forma electrónica, que implicaría el uso de un certificado digital. Por su parte, en las actividades diarias dentro del personal del Poder Judicial del Estado de Tamaulipas, personal de otras dependencias, justiciables, el uso de los medios digitales de esta Judicatura es una labor constante, la cual requiere entre otras cosas el uso de la firma electrónica y la generación de los certificados digitales. Por lo que al contar la Dirección de Informática con la infraestructura y controles de seguridad necesarios para gestionar certificados digitales, se avala la integridad y autenticidad de los certificados emitidos; por tanto, se estima necesario designar a la Dirección de Informática como Autoridad Certificadora dentro de esta Judicatura. Asimismo, y a efecto de garantizar que los procesos relacionados con la emisión de certificados digitales sean consistentes y eficientes, en donde se genere un marco claro, seguro y uniforme, se estima pertinente aprobar y expedir los "Lineamientos de operatividad de la Autoridad Certificadora" los cuales serán aplicables tanto para los usuarios, como para el personal de la Dirección de Informática.

Por lo anteriormente expuesto, y por estimarse justificada la propuesta que hace la Presidenta del Comité de Innovación y Tecnología Judicial, con apoyo además en lo dispuesto por los artículos 121 y 122, fracciones XVI y XVIII, de la Ley Orgánica del Poder Judicial del Estado, el Pleno del Consejo de la Judicatura, procede a emitir el siguiente:

ACUERDO

PRIMERO.- Se designa a la Dirección de Informática como Autoridad Certificadora de ésta Judicatura.

SEGUNDO.- Se aprueban los "Lineamientos de operatividad de la Autoridad Certificadora", siendo los siguientes:

Lineamientos de operatividad de la Autoridad Certificadora

1. Los presentes lineamientos son de observancia obligatoria, para las y los servidores judiciales y usuarios que soliciten o cuenten con certificado digital.

2. Se entiende como Autoridad Certificadora a la Dirección de Informática.

3. **Emisión de certificados digitales en el Poder Judicial del Estado de Tamaulipas.**

La emisión de certificados digitales es la actividad principal de la Autoridad Certificadora del Poder Judicial del Estado de Tamaulipas. Ésta expedirá certificados digitales para:

- Servidores Judiciales dentro de la Judicatura Estatal.
- Personal de otras dependencias que haga uso de los servicios digitales del Poder Judicial del Estado.
- Justiciables y foro litigante.



GOBIERNO DE TAMAULIPAS
PODER JUDICIAL

4. Requisitos para obtener un certificado digital.

En cuanto a personal del Poder Judicial del Estado y de otras dependencias, los requisitos para obtener su certificado digital son:

- Realizar la solicitud en la oficina responsable de la Autoridad Certificadora.
- Proporcionar datos personales: nombre, apellido(s), lugar de trabajo, puesto, RFC, CURP y correo electrónico.

Para las y los justiciables y foro litigante, los requisitos consisten en:

- Realizar la solicitud en línea mediante el Tribunal Electrónico (<https://www.tribunalelectronico.gob.mx>).
- Número de registro en Secretaría General de Acuerdos.
- Presentarse en la oficina responsable de la Autoridad Certificadora o en cualquiera de las unidades de informática con la siguiente documentación:
 - Fotografía tipo credencial (puede ser tomada con cámara de celular, con fondo liso y claro).
 - Credencial de Elector (INE) o pasaporte (Frente y reverso).
 - Cédula Profesional (Frente y reverso).
 - CURP.
 - Comprobante de Domicilio.
 - Indicar el correo electrónico o cuenta de usuario con la que ingresa al Tribunal Electrónico.
 - En este caso quien reciba los documentos debe validar la identidad del interesado.

Además se podrá la modalidad de registro en línea, en la cual la o el interesado envía los requisitos señalados a través de correo electrónico y un escrito bajo protesta de decir verdad en donde refiera que son copia íntegra de los originales. Posteriormente, se realizará una videoconferencia de autenticación de identidad donde el interesado muestra su rostro y documentos originales.

5. Generación de certificados digitales.

Después de que se valide la identidad de la o el interesado, así como de los documentos presentados; el personal de la oficina responsable de la Autoridad Certificadora generará el certificado digital mediante el software destinado a ese fin, donde se realizarán las siguientes acciones:

- Captura de los datos de la o el interesado.
- Selección del tipo de algoritmo criptográfico.
- Teclear la contraseña proporcionada por la o el interesado para proteger el certificado digital.
- Especificar la vigencia del certificado digital.
- Generar el certificado que contiene un par de claves (pública y privada), y además generar un único archivo que contiene las claves mencionadas en formato .p12 o .pfx.

6. Entrega e instalación del certificado digital a la o el interesado.

A las y los servidores judiciales y personal de otras dependencias, se les proporcionará el archivo .p12 para que se haga su instalación en el equipo en donde usarán el certificado para realizar firmas electrónicas de documentos.

En cuanto a las y los justiciables y el foro litigante, su certificado digital se encontrará alojado en los repositorios digitales del Tribunal Electrónico, en donde se relacionará a su cuenta de usuario, lo que



CONSEJO DE LA JUDICATURA
ESTADO DE TAMAULIPAS
SECRETARÍA EJECUTIVA
CD. VICTORIA, TAM.

se denomina "Firma Electrónica Avanzada Multiplataforma" y les permitirá realizar firmas electrónicas, en cualquier dispositivo.

7. Rechazo de una solicitud de certificado digital.

Los motivos de rechazo de solicitud pueden ser los siguientes:

- No se pueda comprobar la identidad del solicitante.
- Incumplimiento en algún requisito.

8. Cambio de contraseña del certificado digital.

No existe la opción de modificar la contraseña asignada al certificado digital. Por lo que, si se desea establecer una nueva contraseña, se procederá a cancelar o revocar el certificado digital vigente y emitir uno nuevo.

Para este trámite no se requiere cumplir con los requisitos de inicio, sino únicamente presentar la solicitud correspondiente por los medios oficiales establecidos.

9. Vigencia de un certificado digital.

La vigencia de los certificados digitales expedidos por la Autoridad Certificadora nunca será mayor de dos años.

10. Responsabilidades y obligaciones del usuario.

El usuario es el responsable de todo documento que esté firmado electrónicamente con su certificado digital. Esto implica que el usuario deberá hacer un uso adecuado del mismo y adoptar medidas de seguridad pertinentes. Algunas de las obligaciones y responsabilidades de las y los usuarios son:

- El usuario es el único responsable de la contraseña de su certificado digital.
- El usuario tiene la responsabilidad de cuidar que sólo él tenga acceso a la contraseña de su certificado digital.
- El usuario debe reportar inmediatamente a la oficina responsable de la Autoridad Certificadora cuando sospeche que su contraseña ha sido expuesta.

11. Revocación de un certificado digital.

Un certificado digital es revocado si alguna de las siguientes condiciones se cumple:

- La contraseña del certificado digital se ha puesto en peligro y el usuario lo reporta.
- En caso de que haya sido dado de baja una o un servidor judicial o personal de otra dependencia.
- El propietario del certificado digital lo solicite.
- Cuando alguna autoridad competente solicite la revocación.

12. Renovación de un certificado digital.

Cuando el certificado digital expire, el usuario solicitará su renovación directamente en la oficina responsable de la Autoridad Certificadora o en el medio electrónico dispuesto para esto. Para este fin la Oficina de Certificación proveerá formas de solicitud de renovación de certificado.

13. Firma Electrónica Avanzada

La firma electrónica avanzada es un conjunto de datos electrónicos que acompañan o que están asociados a un documento electrónico y cuyas funciones básicas son:



CONSEJO DE LA JUDICATURA
DEL ESTADO DE TAMAUCA
SECRETARÍA EJECUTIVA
CD. VICTORIA JARA



GOBIERNO DE TAMAULIPAS
PODER JUDICIAL

- *Identificar al firmante de manera inequívoca.*
- *Asegurar la integridad del documento firmado. Es decir que es exactamente el mismo que el original y que no ha sufrido alteración o manipulación.*
- *Asegurar el no repudio del documento firmado. Es decir, los datos que utiliza el firmante para realizar la firma son únicos y exclusivos y, por tanto, posteriormente, no puede negar la firma del mismo.*

14. Proceso de uso de una Firma Electrónica Avanzada.

El proceso que se sigue para el uso de la firma electrónica es el siguiente:

- *La o el usuario dispone de un documento electrónico (acuerdo, promoción, oficio, notificación personal, etc.) y de un certificado digital que le pertenece y le identifica.*
- *Se realiza un HASH al documento electrónico, que es el resultado de aplicar una función matemática de criptografía a un documento de cualquier longitud, que produce una salida alfanumérica de longitud fija, que permite identificar o comprobar la integridad de los datos, dado que si se llegara a alterar mínimamente, el HASH cambia por completo. MD5, SHA256 y SHA512 son ejemplos de funciones HASH.*
- *Se utiliza la clave privada para codificar el HASH.*
- *Se crea otro documento electrónico que contiene las evidencias de la firma electrónica avanzada.*
- *Las evidencias de todas las firmas electrónicas avanzadas son almacenadas en el servidor: documento firmado, HASH del documento firmado, firmante, fecha y hora. Existiendo una sincronización de la hora de acuerdo a la hora central del país proporcionada por el servidor del Centro Nacional de Metrología (CENAM).*

Así, el resultado de todo este proceso es un documento electrónico obtenido a partir del documento original y del certificado digital del firmante. Siendo la firma electrónica avanzada, el mismo documento electrónico resultante.

15. Proceso para la verificación de un documento firmado.

Cuando llegara a surgir una controversia sobre la veracidad de un documento firmado electrónicamente, se hará uso de la notaría electrónica, el cual es un software especializado que actúa como un repositorio seguro para almacenar las evidencias de las firmas electrónicas realizadas. Este sistema registra y guarda meticulosamente los detalles relacionados con las firmas electrónicas, como la fecha, hora; además de otros datos relevantes. Cuando surja una disputa sobre la autenticidad de un documento firmado electrónicamente, el proceso de verificación implicará comparar el documento controvertido con las evidencias almacenadas en la notaría electrónica. Este proceso se realizará mediante algoritmos y técnicas criptográficas avanzadas que garantizaran la integridad y seguridad de los datos.

El software de notaría electrónica analizará minuciosamente las características del documento controvertido, como su estructura, contenido y firma digital, y las comparará con las evidencias almacenadas. Esta comparación se basa en algoritmos de verificación que buscan similitudes y discrepancias entre el documento controvertido y las firmas almacenadas.



CONSEJO DE LA JUDICATURA
DEL ESTADO DE TAMAULIPAS
SECRETARÍA EJECUTIVA
ED. VICTORIA, TAM.

ACTUACIONES

Una vez que se completa el proceso de comparación, la notaría electrónica emitirá un dictamen sobre la autenticidad del documento. Si el documento coincide perfectamente con las evidencias almacenadas, se considera auténtico. Por otro lado, si se encuentran discrepancias significativas, se puede concluir que el documento es falso o ha sido alterado.

TRANSITORIOS

PRIMERO.- El presente acuerdo, surtirá efectos en esta propia fecha.

SEGUNDO.- Se instruye a la Dirección de Informática como Autoridad Certificadora, a efecto de realizar las gestiones correspondientes.

TERCERO.- Para conocimiento oportuno de las y los interesados, litigantes y público en general, instrúyese el Acuerdo General correspondiente; publíquese en los estrados de la Secretaría Ejecutiva de este Consejo, así como en la página web; asimismo, envíese mediante comunicación procesal a los órganos jurisdiccionales y administrativos de la Judicatura.

Notifíquese.- Así lo acordó el Pleno del Consejo de la Judicatura del Estado, con el voto que por unanimidad emitieron el Magistrado Presidente David Cerda Zúñiga, y Consejeros Ana Verónica Reyes Díaz, Xóchitl Selene Silva Guajardo, José Ángel Walle García y Carlos Ruhneb Pérez Céspedes; quienes firman ante el Secretario Ejecutivo, licenciado Arnoldo Huerta Rincón, que autoriza. Doy fe. SEIS FIRMAS ILEGIBLES. RÚBRICAS.

Lo que se hace de su conocimiento para los efectos legales conducentes.

A T E N T A M E N T E.

Cd. Victoria, Tam, a 13 de febrero de 2024
LIC. ARNOLDO HUERTA RINCÓN

SECRETARIO EJECUTIVO



CONSEJO DE LA JUDICATURA
DEL ESTADO DE TAMAULIPAS
SECRETARIA EJECUTIVA
CD. VICTORIA, TAM.