Secretaría de Finanzas

ACUERDO NÚMERO 283-2021

Tegucigalpa, M.D.C., 19 de marzo de 2021

EL SECRETARIO DE ESTADO EN EL DESPACHO DE FINANZAS

CONSIDERANDO: Que el Artículo 247, de la Constitución de la República establece que los Secretarios de Estado son colaboradores del Presidente de la República en la orientación, coordinación, dirección y supervisión de los órganos y entidades de la Administración Pública Nacional, en el área de su competencia.

CONSIDERANDO: Que en el Decreto Legislativo 149-2013 establece la Ley Sobre Firmas Electrónicas, el cual tiene por objeto reconocer y regular el uso de firmas electrónicas aplicable a todo tipo de información en forma de mensaje de datos, otorgándoles, la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga, que conlleve manifestación de voluntad de las partes.

CONSIDERANDO:Que en la LEY SOBRE FIRMAS ELECTRÓNICAS (Decreto No. 149-2013), fomenta la Utilización de la Firma Electrónica por el Estado tal como lo establece el Artículo 5.- "Se autoriza a los Poderes Legislativo, Ejecutivo y Judicial, al Tribunal Superior de Cuentas, así como a todas las instituciones públicas descentralizadas y entes públicos no estatales y cualquier dependencia del sector público, para la utilización de las firmas electrónicas en los documentos electrónicos en sus relaciones internas, entre ellos y con los particulares".

CONSIDERANDO: Que el Decreto Legislativo 033-2020 publicado en La Gaceta No.35,217 del 03 de abril del 2020, en la Sección Octava, artículo 38 establece que con el fin de permitir la continuidad del Estado y de las entidades privadas que prestan servicios esenciales para la sostenibilidad de la economía nacional sin causar niveles de exposición innecesarios entre las personas, deben tomarse las siguientes medidas:

A) Reformar los artículos 7 de la LEY SOBRE FIRMAS ELECTRÓNICAS (Decreto No.149-2013), los cuales se deberán leer así:

"ARTÍCULO 7.- REQUERIMIENTO DE FIRMA ELECTRÓNICA AVANZADA. La firma electrónica avanzada será siempre de aplicación general, probando la existencia de obligaciones, dando acceso a la inscripción de estos documentos en los registros públicos. No obstante, con el objeto de promover la transformación digital, la administración podrá otorgar la equivalencia

de efectos a la firma electrónica avanzada para ciertos casos a otros tipos de firma o medios de identificación de las personas, entre otros: 1) Híbrido de tecnologías basado en la Infraestructura de Llave Pública (PKI) y Firma Biométrica o cualquier otra tecnología equivalente o substitutiva; 2) Sistemas de firma electrónica en la nube; 3) Sistemas de doble factor; 4) Sistemas biométricos incluyendo medios fotográficos; 5) Otros que puedan ir desarrollándose según el avance de las tecnologías.

CONSIDERANDO: Que el Decreto Legislativo 033- 2020 publicado en La Gaceta No. 35,217 el 03 de abril del 2020, en la Sección Octava artículo 38 reforma el ARTÍCULO 27 de la LEY SOBRE FIRMAS ELECTRÓNICAS (Decreto No.149-2013), los cuales se deberán leer así:

RECONOCIMIENTO DE IDENTIDADES, FIRMAS ELECTRÓNICAS Y CERTIFICADOS EXTRANJEROS. Toda firma electrónica creada o utilizada fuera de la República de Honduras producirá los mismos efectos jurídicos que una firma creada o utilizada en Honduras, si presenta un grado de fiabilidad equivalente. Los certificados de firmas electrónicas emitidos por Autoridades o Entidades de Certificación extranjeras producirán los mismos efectos jurídicos que un certificado expedido por Autoridades Certificadoras nacionales, siempre y cuando tales certificados presenten un grado de fiabilidad en cuanto a la regularidad de los detalles de éste, así como su validez y vigencia.

Las entidades del sector público o privado podrán designar a uno o más responsables de certificar las autorizaciones que correspondan para asegurar la fluidez de sus operaciones por medios electrónicos. Estas personas tendrán el carácter de fedatarios. Las personas designadas deberán ser comunicadas al Instituto de la Propiedad, el cual llevará un registro de éstas. Las entidades del Estado deberán tener por válidas las certificaciones realizadas por estos medios y surtirán los efectos señalados en el Artículo 7 de la Ley Sobre Firmas Electrónicas.

Por medios electrónicos podrán celebrarse todo tipo de actos, contratos y cualquier otro tipo de negocios jurídicos siempre que sea posible mostrar de manera fehaciente la voluntad de las partes de llevar a cabo el negocio jurídico por ese medio. El consentimiento de las partes se prueba con el intercambio de correos electrónicos, vídeos, grabaciones de voz, intercambio de mensajes de texto, aceptación electrónica de contratos estandarizados o mediante el envío de un autorretrato electrónico sosteniendo el documento de identidad de forma visible junto al rostro del firmante tomado a través

de la aplicación correspondiente previo al envío de la solicitud o formulario respectivo.

Se interpretan los artículos; 2; 23 literal 4), 52; 57; 60; 67 numeral 2); 78; 81; 99; y, 100 numeral 13) de la LEY ORGÁNICA DEL TRIBUNAL SUPERIOR DE CUENTAS (TSC), en el sentido de que cuando los mismos hagan referencia a documentos, se entiende por tales aquellos que consten en físico o en formato digital teniendo ambos la misma validez de manera indistinta.

CONSIDERANDO: Que conforme al Acuerdo Ministerial No. 485-2020 publicado en La Gaceta 35,445 el 30 de noviembre del 2020, se aprueba el **"EL USO DE LA FIRMA ELECTRÓNICA AVANZADA EN LOS PROCESOS DE LA SECRETARÍA DE ESTADO EN EL DESPACHO DE FINANZAS, Y PARA TODOS LOS SISTEMAS DE INFORMACIÓN Y SERVICIOS DE TECNOLOGÍA QUE RECTORA"**. Que en dicho Acuerdo en el Artículo 3 se establece la necesidad de un Reglamento de Uso de la Firma Electrónica.

POR TANTO:

En uso de las facultades contenidas en los artículos 59, 247, 255 de la Constitución de la República; 33, 36 numeral 1, 6, 8 y artículos 118 y 119 de la Ley General de la Administración Pública; 23, 24 del Reglamento de Organización, Funcionamiento y Competencias del Poder Ejecutivo; Decreto Legislativo 33-2020, Decreto Ejecutivo PCM-005-2020, Decreto Ejecutivo PCM-016-2020.

ACUERDA:

PRIMERO: Aprobar **"EL REGLAMENTO PARA EL USO Y OPERACIÓN DE LA FIRMA ELECTRÓNICA EN LA SECRETARÍA DE ESTADO EN EL DESPACHO DE FINANZAS Y PARA TODOS LOS SISTEMAS DE INFORMACIÓN Y SERVICIOS DE TECNOLOGÍA QUE RECTORA"**.

CAPÍTULO I.

DISPOSICIONES GENERALES

Artículo 1. Objetivo.

El presente Reglamento tiene por objeto establecer las bases que reconocen y regulan la Firma Electrónica aplicable en todo tipo de información en forma de mensaje de datos, otorgándoles, la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga, que conlleve manifestación de voluntad de los firmantes.

Artículo 2. Siglas, Abreviaturas y Definiciones

Para la correcta aplicación de las disposiciones de este Reglamento se entenderá por:

A. SIGLAS Y ABREVIATURAS

Siglas	Significado
SEFIN	Secretaría de Finanzas
UIT	Unidad de Innovación y Tecnología
UDEM	Unidad de Modernización
CA	Autoridad de Certificación
PSC	Prestador de Servicios de Certificación
FIEL	Firma Electrónica que utiliza dos métodos: FIEL PSC y FIEL CA-SEFIN
FIEL PSC	Firma Electrónica Avanzada En cualquier de las modalidades presentadas por el PSC: Token, certificado de software o el que la tecnología permita adquirir. Siendo su uso para procesos internos y externos de la SEFIN.
FIEL CA-SEFIN	Firma Electrónica Equivalente de uso interno y generado por la SEFIN

B. DEFINICIONES TÉCNICAS

I. "FIRMA ELECTRÓNICA": Los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos y para indicar la voluntad que tiene tal parte respecto de la información consignada en el mensaje de datos;

II. "LA CLAVE PRIVADA". Se genera simultáneamente con la clave pública y se relacionan entre sí en un sistema de criptografía asimétrica. La llave privada debe mantenerse en secreto y en posesión solamente por su titular. Con ella es posible firmar digitalmente documentos y archivos de forma inequívoca por su titular.

III. "ENTE CERTIFICADOR" La SEFIN desempeñará la figura de Ente Certificador en la emisión de la CA-SEFIN a través del Agente Certificador y a través del PSC para la FIEL PSC.

IV. "AUTORIDAD DE CERTIFICACIÓN": En criptografía, las expresiones autoridad de certificación, o certificadora, o certificante, o las siglas AC o CA, señalan a una entidad de confianza, responsable de emitir y revocar los certificados, utilizando en ellos la firma electrónica, para lo cual se emplea la criptografía de clave pública.

V. "CERTIFICADO DIGITAL": es el documento electrónico que garantiza protección a las transacciones en línea (vía internet) y el intercambio virtual de documentos, mensajes y datos, con validez jurídica

VI. CASEFIN: Se refiere a la infraestructura interna de la Secretaría de Finanzas para la generación de certificados con grado de equivalencia propios de esta Secretaría.

VII. "FIRMA ELECTRÓNICA AVANZADA, FIEL PSC": Aquella certificada por un prestador acreditado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control de manera que se vincule únicamente al mismo y a los datos a los que se refiere, permitiendo la detección posterior de cualquier modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría, la cual se usará para procesos internos y externos de SEFIN. Este puede ser para la Firma con Certificado portado en Token o instalado en Software.

VIII. **"FIRMA ELECTRÓNICA EQUIVALENTE, FIEL CA-SEFIN":** Aquella certificada por un prestador local en SEFIN a través del Agente Certificador, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control de manera que se vincule únicamente al mismo y a los datos a los que se refiere, permitiendo la detección posterior de cualquier modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría, la cual se usará para procesos internos de SEFIN.

IX. **"CERTIFICADO":** Todo mensaje de datos u otro registro que confirme el vínculo entre un firmante y los datos de creación de la firma.

X. **"CERTIFICADO DE SOFTWARE":** Todo mensaje de datos proporcionado por un "Prestador de servicios de Certificación que le atribuye certeza y validez a la firma electrónica.

XI. **"MENSAJE DE DATOS":** Es la información generada enviada, recibida o archivada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros el Intercambio Electrónico de Datos (EDD), el correo electrónico, o telefax.

XII. **"FIRMANTE":** La persona que posee los datos de creación de la firma y que actúa por cuenta propia o por cuenta de la persona a la que representa.

XIII. **"CERTIFICADOR O PRESTADOR DE SERVICIOS DE CERTIFICACIÓN":** La persona natural o jurídica acreditada que expide certificados y puede prestar otros servicios relacionados con las firmas electrónicas.

XIV. **"ACREDITACIÓN":** Es el título que otorga la SEFIN para proporcionar certificados electrónicos y autenticar firmas, una vez cumplidos los requisitos establecidos en la presente Ley; y

XV. **"TOKEN":** Es el dispositivo donde se almacena el Certificado Digital y que se conecta directamente al puerto USB del ordenador, dispensando cualquier tipo de adaptador.

XVI. **"CRIPTOGRAFÍA ASIMÉTRICA":** También llamada criptografía de clave pública o criptografía de dos claves o llaves, es el método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona que recibirá el mensaje.

XVII. **"LLAVE PRIVADA":** Componente de la criptografía asimétrica que consiste en una clave privada que el propietario debe custodiar de modo que nadie tenga acceso a ella. Si el propietario del par de claves usa su clave privada para cifrar un mensaje, cualquiera puede descifrarlo utilizando la clave pública del primero. En este caso se consigue la identificación y autentificación del remitente, ya que se sabe que sólo pudo haber sido él quien empleó su clave privada. Esta idea es el fundamento de la firma digital, donde jurídicamente existe la presunción de que el firmante es efectivamente el dueño de la clave privada.

XVIII. **"LLAVE PÚBLICA":** Componente de la criptografía asimétrica que consiste en una clave pública que es entregada a cualquier persona mediante el envío de mensajes. La llave pública es distribuida a todas las

entidades o individuos con los que se desea mantener comunicaciones seguras. Los métodos criptográficos garantizan que cada pareja de llaves sólo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas obtengan la misma pareja de llaves.

Artículo 3. Ámbito de Aplicación.

El Ámbito de Aplicación del presente reglamento es obligatorio para cualquier Servidor Público, Persona Natural o Jurídica que por su naturaleza requieran del uso de este medio, en el ejercicio de sus funciones o actividades contractuales lleve a cabo algún tipo de comunicación entre las Dependencias de la Secretaría de Finanzas y/o a lo externo de la Secretaría que utilicen la FIEL de la siguiente manera:

FIEL PSC: Firma electrónica avanzada para uso interno y externo de SEFIN. Sea este mediante Token o Certificado de Software.

FIEL CA-SEFIN: Firma electrónica equivalente para uso interno de SEFIN.

La SEFIN a través de la Secretaría General emitirá las Circulares correspondientes, que establecerán los lineamientos y gradualidad para el uso de la FIEL en la documentación, servicios de tecnología y sistemas de información que rectora la misma.

Artículo 4. Lo que no contemple el Reglamento

A falta de disposición expresa en el presente Reglamento, se atenderá lo dispuesto en: la Ley Sobre Firmas Electrónicas (Decreto No.149-2013), el Reglamento de Ley sobre Firmas Electrónicas Acuerdo Ejecutivo 41-2014, Decreto Legislativo 033-2020 publicado en La Gaceta el 03 de abril del 2020, Decreto Ejecutivo PCM 086-2020 y las normativas aplicables.

Artículo 5. Tecnología a Utilizar.

Las disposiciones del presente Reglamento serán aplicadas de modo que no excluyan, restrinjan o priven de efecto jurídico cualquier método para crear una firma electrónica, siempre que cumpla los requisitos enunciados en el Artículo 8 o que cumpla de otro modo los requisitos del derecho aplicable.

Artículo 6. Responsabilidades Administrativas.

Por lo que refiere a las responsabilidades administrativas, civiles y penales que se deriven del uso de la FIEL por parte de los usuarios, se contemplará lo dispuesto en los ordenamientos que al caso sean aplicables.

Artículo 7. Actos y Actuaciones Electrónicas.

Todos los actos y actuaciones electrónicas que se realicen o se deriven de la creación, implementación, revocación, uso y cancelación de la FIEL, deberán observar las disposiciones aplicables en materia de protección de datos personales y/o datos sensibles; así como aquellas en materia de transparencia y acceso a la información pública.

Artículo 8. Anexos y Requisitos

Las disposiciones contenidas en los anexos de este Reglamento forman parte integral del mismo, por lo que son obligatorias.

CAPÍTULO II.

DEL OTORGAMIENTO, USO Y VALIDEZ DE LA FIEL CA-SEFIN

Artículo 9. Otorgamiento.

Método I. Los certificados digitales requeridos para hacer uso de la FIEL MÉTODO CA-SEFIN para **uso exclusivo a lo interno de la Secretaría de Finanzas** podrán ser otorgados a los usuarios, a través de la CA de la SEFIN, para el ejercicio de sus atribuciones o para el cumplimiento de sus obligaciones o necesidades. (Requisitos de Enrolamiento en el Artículo 27) Que en su primera fase la cual ya se encuentra en ejecución,

estará a cargo de la UIT por un término de seis meses, posteriormente se sugiere sea la Subgerencia de Recursos Humanos quien sea la encargada del proceso.

Método II. Los certificados digitales para el uso de la FIEL para uso interno y externo de la SEFIN por medio de un Token o un Certificado de Software provisto por un PSC, se deberán de coordinar a través de la UIT (Requisitos de Enrolamiento en el Artículo 27). El proceso seguirá los siguientes pasos:

- ✓ Según asignación correspondiente, coordina con UIT la firma del acta y entrega del Token.
- ✓ Con el Token se presenta a las oficinas de la empresa del PSC.
- ✓ Se firma el "Contrato de Adhesión para uso de Certificado Digital por Persona Natural" entre el PSC y el usuario.

Para el caso de los prestadores de servicios contratados por honorarios permanentes o eventuales, se podrán otorgar los certificados digitales requeridos para el uso de la FIEL, mismos que se asignarán con una vigencia máxima que corresponda al periodo de su contratación. Los usuarios deberán dar cumplimiento a lo expuesto en el presente Reglamento, para su uso en aquellos documentos, mensajes de datos, procesos y procedimientos o servicios informáticos en los que se requiera el uso de la FIEL.

Artículo 10. Uso de la FIEL

Los documentos podrán ser firmados con la FIEL por los usuarios que así lo requieran, ya sea para el ejercicio de sus **atribuciones y/o fines institucionales**; de igual forma podrá ser utilizada en los mensajes de datos; así como en aquellos actos o actuaciones electrónicas que se realicen a través de los sistemas y servicios informáticos. Los documentos y mensajes de datos que cuenten con la FIEL producirán los mismos efectos que los presentados con firma autógrafa y, en consecuencia, tendrán el mismo valor jurídico-administrativo que las disposiciones correspondientes les otorgan a éstos, según lo indicado en la LEY SOBRE FIRMAS ELECTRÓNICAS (Decreto No.149-2013) y sus reformas.

Artículo 11. Comunicación interna de la Secretaría. Todas las comunicaciones que se realicen entre dependencias de la Secretaría podrán llevarse a cabo vía electrónica, mediante la utilización de la FIEL. Sin embargo, se hará la excepción para aquellas situaciones que por algún motivo extraordinario requieran de una firma manuscrita, pero esto será la excepción y no la regla. Para el trámite y sustanciación de procedimientos de índole contenciosa o administrativa, se podrá hacer uso de la FIEL en los términos que señale la normativa en la Ley de Firma Electrónica y el Reglamento sobre Gobierno Electrónico PCM 086-2020.

En caso de que se presenten situaciones extraordinarias que pongan en riesgo la salud, seguridad o cualquier derecho humano del personal de la Secretaría y de la ciudadanía en general y la norma específica no contemple el uso de la FIEL, la autoridad correspondiente para tramitar o sustanciar el procedimiento en cuestión, podrá determinar su uso atendiendo el caso particular, siempre y cuando garantice el debido proceso.

Artículo 12. Validez jurídica de la Firma Electrónica La FIEL tiene la misma validez jurídica que la firma autógrafa, por lo que su uso implica:

a) La vinculación indubitable entre el firmante y las actuaciones electrónicas, actos, mensajes de datos o documentos, en que se asocia con los datos que se encuentran bajo el control exclusivo del firmante;

b) Dar certeza jurídica de que los documentos, mensajes de datos, actos y actuaciones fueron emitidos y/o remitidos por el usuario interno y/o externo que firma;

c) La responsabilidad de prevenir cualquier modificación o alteración en el contenido de las actuaciones electrónicas, actos, mensajes de datos o documentos electrónicos que se presentan en los procesos y procedimientos de servicios informáticos, al existir un control exclusivo de los medios electrónicos mediante la utilización de la FIEL;

d) Garantizar la integridad y autenticidad del documento contenido en las actuaciones electrónicas, actos, mensajes de datos o documentos electrónicos que sean firmados con la FIEL; y,

e) La correspondencia exclusiva entre la FIEL y el firmante, por lo que todos los documentos o mensajes de datos presentados con la misma serán responsabilidad de su titular y no serán susceptibles de repudio, con lo que se garantiza la autoría e integridad del documento.

Artículo 13. Responsabilidad del Uso de la Firma Avanzada

El uso de la FIEL debe ser:

I. **Personal e intransferible**, por lo que queda estrictamente prohibido compartirla, prestarla, traspasarla o cualquier otro acto que implique dar a otros la posibilidad de uso;

II. **Exclusivamente para fines laborales y/o fines institucionales.** No se debe utilizar para firmar documentos personales que no tengan vinculación con la SEFIN.

Artículo 14. Requisitos para el Uso de la FIEL

Para que los colaboradores puedan utilizar la FIEL en los actos, actuaciones y mensajes de datos a los que se refiere el presente Reglamento deberán contar con:

I. Formulario de Solicitud de Emisión de Certificado, requerido para ambos Métodos de la FIEL,

II. Políticas de Términos y Condiciones Firmado aceptando lo contenido en el (Ver Anexo 4),

III. Un certificado digital vigente, emitido u homologado,

IV. Una clave privada, generada bajo su exclusivo control.

V. El Certificado de software CASEFIN debe ser instalado únicamente en las computadoras de la SEFIN.

Artículo 15. Principios

La FIEL deberá cumplir con los siguientes principios:

I. **Autenticidad:** da certeza de que el documento, acto, actuación electrónica o mensaje de datos ha sido emitido por el firmante de manera tal que su contenido le es atribuible al igual que las consecuencias jurídicas que de el deriven;

II. **Confidencialidad:** consiste en que la FIEL en un documento, acto, actuación electrónica o mensaje de datos, garantiza que sólo pueda ser cifrado por el remitente con la llave privada y verificado por el receptor con la llave pública;

III. **Equivalencia Funcional:** consiste en que la FIEL contenida en un documento, acto, actuación electrónica o en su caso, en un mensaje de datos, satisface el requisito de firma del mismo modo que la firma manuscrita en los documentos impresos;

IV. **Integridad:** da certeza de que el documento, acto, actuación electrónica 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:** consiste en que la tecnología utilizada para la emisión de certificados

digitales y para la prestación de los servicios relacionados con la FIEL será aplicada de modo tal que no excluya, restrinja o favorezca la utilización de alguna marca en particular; y,

VI. **No Repudio:** consiste en que la FIEL contenida en un documento, acto, actuación electrónica o mensaje de datos garantiza la autoría e integridad de los mismos y que dicha firma corresponde exclusivamente al firmante.

CAPÍTULO III.

DE LOS DOCUMENTOS Y DE LOS MENSAJES DE DATOS

Artículo 16. Uso de la Firma en las Comunicaciones
En las comunicaciones entre los sujetos obligados y, en su caso, los actos jurídicos que realicen entre los mismos, se hará uso de mensajes de datos y aceptarán la presentación de documentos electrónicos, los cuales deberán contar, cuando así se requiera, con la FIEL del usuario habilitado para esos efectos.

Artículo 17. Notificación de recepción
Los documentos digitales firmados con la FIEL se considerarán como notificados con la recepción de la "Notificación de Entrega" del correo electrónico institucional por lo que el uso de estos medios implicará la aceptación para las comunicaciones internas.
Estos medios deberán registrar fecha y hora de entrega.

Artículo 18. Acuse de Recibido Electrónicamente
El acuse de recibo electrónico (Notificación de Lectura de correo electrónico) deberá contener la información que permita dar plena certeza sobre la fecha y hora de recepción de las actuaciones electrónicas, actos, mensajes de datos o documentos electrónicos asociados a dicho acuse de recibo para las comunicaciones internas.

Artículo 19. Privacidad de la información
La información contenida en los mensajes de datos y en los documentos será pública, salvo que la misma esté clasificada como reservada o confidencial en términos de la normatividad aplicable a la materia de transparencia y acceso a la información pública. Las actuaciones electrónicas, actos, mensajes de datos y los documentos que contengan datos personales estarán sujetos a las disposiciones previstas en materia de protección de datos personales.

Artículo 20. Almacenamiento de las Actuaciones con la Firma Electrónica
Los sujetos obligados deberán conservar en medios electrónicos, las actuaciones electrónicas, actos, mensajes de datos y los documentos con la FIEL derivados del intercambio de información a que se refiere este Reglamento, así como los plazos de conservación previstos en los ordenamientos aplicables, según la naturaleza de la información.

Artículo 21. Digitalización de Documentos firmados físicamente
Toda la recepción de documentos que sea de forma física, es decir impresa y con firma manuscrita podrá ser digitalizada para continuar con su debido proceso en la Secretaría, conservando el documento original impreso con el fin de cumplir con lo establecido por los entes reguladores. Tal requisito se considerará satisfecho si la copia se genera en un documento electrónico y se cumple con lo siguiente:

I. Que la información contenida en el documento electrónico se mantenga íntegra e inalterada a partir del momento en que se recibió por primera vez en su forma original y sea accesible para su posterior consulta tanto física como electrónicamente;

II. Que el documento electrónico permita conservar el formato del documento impreso y reproducirlo con exactitud (escaneo en formato PDF); ,y

III. Que se observe lo previsto en las disposiciones generales en materia de conservación de mensajes

Artículo 22. Validez de los Documentos Firmados Digitalmente

Los documentos generados y firmados electrónicamente no requerirán de un documento de certificación respecto de su originalidad emitido por la Secretaría General, ya que la naturaleza de la FIEL produce los mismos efectos que los presentados con firma autógrafa, por lo que se considerará como un documento fidedigno y con certeza jurídica.

La validación de los documentos firmados electrónicamente será potestad del destinatario y/o receptor.

CAPÍTULO IV.

INVOLUCRADOS EN LA OPERACIÓN Y USO DE LA FIEL DE LA SEFIN

Artículo 23. Ente Certificador

La Secretaría de Finanzas es el Ente Certificador quien delega a un Agente Certificador quien coordinará el enrolamiento con la FIEL y una Autoridad de Certificación para la generación de Certificados por medio de la CA-SEFIN según solicitud del Agente Certificador. Que en su primera fase la función de Agente Certificador fue realizada por la UDEM, pero posteriormente estará a cargo de la Subgerencia de Recursos Humanos quien otorgue los mismos.

Artículo 24. Responsabilidades del Ente Certificador y el Agente Certificador

Las atribuciones del Ente Certificador y del Agente Certificador, serán las siguientes:

A. La Secretaría de Finanzas como Ente Certificador es responsable de:

- Designar las responsabilidades de Agente Certificador y la Autoridad de Certificación sobre la dependencia que presente las características técnicas y administrativas para cumplir con dicha labor.
- Designar al Agente de Certificación la generación de los mismos, una vez validada la documentación por el Agente Certificador.
- Instruir la revocación de los certificados de la FIEL, cuando se cumpla alguno de los supuestos de revocación especificados en el presente Reglamento;
- Adoptar las medidas necesarias para difundir el uso correcto de los certificados digitales, así como de los servicios relacionados con la FIEL;
- Habilitar el uso de la FIEL, con todas sus características, emitiendo la documentación legal y los certificados digitales correspondientes;
- Fomentar y difundir el uso de la FIEL, y otros medios electrónicos, para agilizar el desarrollo de las actividades sustantivas de los sujetos obligados de acuerdo a sus facultades o atribuciones; así como propiciar la eliminación del uso del papel de manera paulatina en las comunicaciones e intercambio de información que se lleve a cabo entre las unidades responsables;
- Adoptar e implementar las medidas necesarias, para disuadir el uso indebido de certificados digitales;
- Preservar la confidencialidad, integridad y seguridad de los datos personales de los titulares de los certificados digitales observando las disposiciones aplicables en

materia de protección de datos personales y/o datos sensibles; así como aquellas en materia de transparencia y acceso a la información pública;

- Presupuestar los recursos necesarios para el uso y operación de la FIEL de acuerdo al ámbito de su competencia;

- Realizar o llevar a cabo auditorías internas y externas en materia de seguridad informática; en el caso de las externas, estas deberán ser autorizadas por la Máxima Autoridad de la Institución, conforme con la disponibilidad presupuestal del ejercicio que corresponda, que permitan identificar riesgos y vulnerabilidades potenciales en la infraestructura que soporta los procesos operativos asociados al sistema de registro y certificación (internos y externos), así como ejecutar los procesos de remediación que se consideren adecuados,

- Las que se deriven de las disposiciones del presente Reglamento, y demás normatividad aplicable.

B. La Subgerencia de Recursos Humanos fungirá como el Agente Certificador siendo responsable de:

I. Recibir y revisar que las solicitudes y documentación que presenten los sujetos obligados de manera física o electrónica para la emisión de certificados digitales cumplan con los requisitos que al efecto establezca este Reglamento;

II. Registrar a los sujetos obligados que se les haya expedido el certificado para la utilización de la FIEL; llevando un control de los certificados digitales que se emitan y de los que se revoquen;

III. Atender los requerimientos relacionados con las solicitudes de emisión de certificados digitales en sus respectivos ámbitos de competencia;

IV. Realizar las altas, bajas, revocaciones o modificaciones de los titulares que repercutan en los certificados digitales;

V. Notificar al solicitante respecto de inconsistencias o duplicidades en la documentación física o electrónica que presente.

VI. Autenticar que la información que se incorpora a la solicitud de certificado digital corresponda efectivamente a la identidad del solicitante;

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

VIII. Habilitar un cuadro conteniendo la “lista blanca” y “lista negra” siendo ambas de duración directamente relacionadas a la duración del certificado de la CASEFIN para consulta de los sujetos obligados en el sitio de colaboración de la SEFIN;

Artículo 25. Responsabilidades de la UIT

La UIT será la encargada de:

A. Coordinar la administración de la infraestructura tecnológica necesaria para la operación de la FIEL CA-SEFIN;

B. Brindar la asesoría técnica que requiera el Ente Certificador para operar el sistema de registro y certificación;

C. Diseñar las medidas de seguridad técnicas para la gestión de la FIEL;

D. Establecer y operar los esquemas de monitoreo para garantizar la disponibilidad

de la infraestructura que soporta los procesos operativos asociados al sistema de gestión de firmas, para aquellos procesos aplicables, de la FIEL;

E. Habilitar el uso de la FIEL, con todas sus características, emitiendo los certificados digitales correspondientes;

F. Las que se deriven de las disposiciones del presente Reglamento y demás normatividad aplicable.

Artículo 26. Obligaciones de la UDEM

La Unidad de Modernización en conjunto con el Ente Certificador deberá:

I. Realizar Análisis y Diseño de los procesos para la implementación gradual de la FIEL en la Secretaría de Finanzas;

II. Definición de las Fases de la implementación gradual de la FIEL;

III. Brindar las capacitaciones y soporte necesario a los servidores públicos que cuenten con la FIEL;

IV. En base a las mejoras o nuevas prácticas realizar las propuestas de actualización al presente Reglamento cuando un evento lo amerite. Dicho Reglamento estará bajo la custodia de la Secretaría General de la SEFIN;

V. Capacitar y asesorar a los usuarios internos de la SEFIN para el uso de la herramienta que permita generar el requerimiento de certificado digital, que la SEFIN determine;

VI. Diseñar las medidas de seguridad administrativas para la gestión de la FIEL.

VII. Control Temporal, por lo 6 meses de la primera etapa de la entrega de los Tokens. Esta función será asumida en la segunda etapa por el agente certificador.

VIII. Las demás que se deriven de las disposiciones del presente Reglamento y normatividad aplicable.

CAPÍTULO V.

DEL CERTIFICADO DIGITAL

Artículo 27. Solicitud del Certificado

Para obtener un certificado digital, los sujetos deberán dirigir la solicitud correspondiente con la firma de la Dirección, mediante la cual se manifestará que se convalidan todos aquellos actos que se celebren con la FIEL, como si hubieran sido firmados en manuscrito por su suscriptor y será enviada a la cuenta de correo electrónico institucional indicado por el usuario.

Con la finalidad de dar certeza y seguridad para el otorgamiento del certificado digital, los sujetos obligados deberán:

1. Realizar el trámite a través de la modalidad a distancia o con el uso de herramientas tecnológicas que la Autoridad Certificadora determine para el Método I.

2. Presentarse en el domicilio que señale la Autoridad Certificadora en los casos que se requiera la aplicación del Método II.

Los usuarios deberán realizar el requerimiento del certificado digital dirigido al Agente Certificador, así mismo, deberán presentar o remitir en medios electrónicos los siguientes documentos:

1. ***Formulario de Solicitud de Firma Electrónica Avanzada SEFIN*** debidamente requisitada para obtener el mismo independientemente del método que aplique, la cual debe contener al menos los siguientes datos:

   A. Nombre completo;

   B. Domicilio laboral;

   C. Correo electrónico institucional, teléfono y extensión de contacto;

   D. Área de adscripción;

   E. Cargo que desempeña,

   F. Firma del Director(a) o Encargado del área

   G. Fecha de solicitud.

2. Política de Términos y Condiciones, tiene por objeto regular el uso de la firma electrónica avanzada sea este provisto por la Secretaría de Finanzas o por un tercero, generando un acuerdo entre la SEFIN y el Servidor Público el cual firmará aceptando estar de acuerdo con lo descrito en el mismo (Ver Anexo 4).

Una vez validada la información contenida en la solicitud presentada o remitida por el solicitante y Firmado el documento de Políticas de Términos y Condiciones, la Autoridad Certificadora, emitirá el certificado digital correspondiente por medio del Agente Certificador. (Ver Formatos Anexo 1 y Anexo 4)

Artículo 28. Inconsistencias en la Solicitud

En caso de que el Agente Certificador detecte inconsistencias o duplicidad en los datos y elementos de identificación, se deberá rechazar el trámite del certificado digital, notificando mediante correo electrónico al solicitante; y sólo en los casos en los que las incidencias sean subsanables deberá informar a éste para que acuda o remita a través de medios electrónicos a la Autoridad correspondiente, para subsanar la inconsistencia o duplicidad.

En caso de no subsanar las inconsistencias en un plazo de 5 días hábiles posteriores a la entrega de la solicitud, se entenderá como rechazado el trámite por lo que el usuario deberá iniciar nuevamente el proceso.

Artículo 29. Derechos del poseedor del Certificado

El titular de un certificado digital tendrá derecho a:

I. Que los datos personales que proporcione para la obtención de la FIEL de la SEFIN sean tratados confidencialmente, observando las disposiciones aplicables en materia de protección de datos personales; así como aquellas en materia de transparencia y acceso a la información pública;

II. Recibir información sobre el procedimiento de solicitud y/o trámite de la FIEL de la SEFIN mediante correo electrónico institucional a la cuenta de correo proporcionada en la solicitud de certificado;

III. Las demás que establezca el presente Reglamento, y demás normatividad aplicable.

Artículo 30. Obligaciones del poseedor del Certificado

El titular de un certificado digital tendrá las siguientes obligaciones:

I. Usar bajo su única y exclusiva responsabilidad la FIEL;

II. Proporcionar a la Autoridad Certificadora información, datos y documentación veraces, completos y exactos al momento de solicitar su certificado;

III. Custodiar adecuadamente sus datos de creación de firma, la contraseña y la llave privada vinculada con ellos, a fin de mantenerlos en secreto;

IV. Actualizar los datos proporcionados para la tramitación del certificado digital;

V. Solicitar a la Autoridad Certificadora la revocación de su certificado digital en caso de que la integridad o confidencialidad de sus datos de creación de firma o contraseña hayan sido comprometidos y presuma que su llave privada pudiera ser utilizada indebidamente;

VI. Dar aviso al Agente Certificador cuando requiera realizar cualquier modificación a sus datos de identificación personal, a fin de que éste incorpore las modificaciones en los registros correspondientes y emita un nuevo certificado digital;

VII. Hacer uso de los certificados digitales sólo para los fines autorizados, en términos de los procesos que para tal efecto sean implementados por la SEFIN considerando los Métodos descritos en el Artículo 9;

VIII. Las demás que establezca el presente Reglamento y la normatividad aplicable.

CAPÍTULO VI.

DE LA REVOCACIÓN DEL CERTIFICADO DIGITAL

Artículo 31. Revocación del Certificado Digital

El certificado digital quedará sin efectos o será revocado por la Autoridad Certificadora, cuando se cumpla alguno de los supuestos siguientes:

I. Por expiración de su vigencia;

II. Cuando se acredite que los documentos presentados por el titular del certificado digital para verificar su identidad son apócrifos;

III. Cuando así lo solicite el titular del certificado digital a la Autoridad Certificadora;

IV. Por fallecimiento del titular del certificado digital;

V. Cuando se ponga en riesgo la confidencialidad o integridad de los datos de creación de la FIEL;

VI. Por resolución de Autoridad Judicial o Administrativa que así lo determine;

VII. Cuando el usuario interno haya sufrido un movimiento de personal en nómina en el Secretaría, la solicitud para la revocación del certificado digital deberá llevarse cuando se haya realizado el movimiento del puesto de manera formal y se podrá solicitar de manera directa por el usuario interno, a través de la Dirección, según corresponda, o bien, la Sub Gerencia de Recursos Humanos de oficio podrá solicitarlo al Agente Certificador de la Unidad Responsable a la que se encuentre adscrito el usuario interno.

VIII. Cuando el titular haga del conocimiento a la autoridad certificadora del extravío o inutilización por daños del medio electrónico que contenga el certificado digital o la llave privada; o bien, en caso de pérdida, robo o destrucción del medio electrónico que contiene la FIEL, o cualquier otro evento que ponga en riesgo la confidencialidad del certificado digital o la llave que conforma al mismo, los sujetos obligados, bajo su absoluta responsabilidad, deberán proceder a solicitar su

inmediata revocación o reposición ante la autoridad correspondiente, sujetándose a los procesos que este último determine.

Artículo 32. Solicitud de Revocación de la FIEL

Los sujetos obligados que requieran revocar su FIEL, que haya extraviado el mismo, que haya sido desvinculado de la SEFIN o que haya tenido un cambio de puesto deberá ser notificado a través de un comunicarlo vía correo electrónico institucional por parte de la Subgerencia de Recursos Humanos al Agente Certificador correspondiente. Para el caso de la CASEFIN a la UIT, adjuntando los siguientes requisitos:

I. Solicitud debidamente autorizada en la que se solicite la revocación del certificado digital, señalada en el *Anexo 3 Solicitud de Revocación del Certificado Digital*.

II. Señalar nombre completo del solicitante y adjuntar identificación oficial.

III. En el caso de revocación de la FIEL de un servidor público por solicitud de una autoridad competente, este deberá de comunicar al servidor público dicha revocación y adjuntar constancia de la comunicación.

IV. Deberá ser actualizada la Lista Blanca y Lista Negra de los usuarios de la CASEFIN

Para la revocación de la FIEL PSC al Prestador de Servicio a través de la UDEM.

Todo proceso de Revocación el usuario tiene los datos necesarios (información anotada en el proceso de emisión en el Trifolio negro entregado) para poder realizarla personalmente, ingresar a la página web del Prestador de Servicio y completar la información solicitada en dicha dirección electrónica.

Si fuera el caso y que los usuarios no tienen la información para **revocación** con una nota por parte de SEFIN debidamente firmada y sellada solicitando dicha gestión se realizará directamente en la agencia con el número de Ticket que genera la solicitud de creación.

En específico:

- Ya no labora en la SEFIN y debe devolver el token: revocación por medio de las 2 opciones antes mencionadas (realizada por el usuario directamente o en oficinas de del PSC) y para poder reutilizar el dispositivo Token el usuario deberá brindarle a SEFIN el pin de uso de la firma y el puk (información confidencial generada por cada usuario) para hacer un barrido de la información registrada en ese dispositivo y poder instalar un nuevo certificado digital.

- Extravío el Token: revocación por medio de las 2 opciones antes mencionadas (realizada por el usuario directamente o en oficinas del PSC)

- Olvidó la contraseña: Si el usuario olvidó la contraseña Pin de uso y no cuenta con la información anotada en el trifolio negro que se les brinda en la emisión o alguna foto o documento de respaldo **NO** podrá recuperar su Certificado Digital ni reutilizar el dispositivo TOKEN, por lo que deberá adquirir uno nuevo. **(para desbloquear y cambiar pin de acceso de requiere el PUK)**

Nota Importante: La empresa No conoce las contraseñas generadas por los usuarios y No quedan registradas en sus sistemas.

La falta de cumplimiento en la entrega del dispositivo, PIN y/o PUK ocasionará que los gastos ocasionados para recuperar dicho instrumento sean imputados al funcionario público. El costo de la renovación de un token por reasignación del funcionario público o su desvinculación correrán por parte de la SEFIN, siempre y cuando el mismo cumpla con el requisito de la entrega del dispositivo, PIN y PUK.

CAPÍTULO VII.

DEL RECONOCIMIENTO DE CERTIFICADOS DIGITALES EMITIDOS POR AUTORIDADES CERTIFICADORAS

Artículo 33. Reconocimiento de Certificados Digitales
La SEFIN podrá celebrar acuerdos o convenios de colaboración para el reconocimiento de certificados digitales con entidades que se identifiquen necesarias debido al tipo de documentos que se intercambien o con aquellas entidades que así lo requieran, expedidos de manera enunciativa más no limitativa por:

I. El Sistema Financiero;

II. Los Entes gubernamentales;

III. La Empresa Privada;

IV. La Ciudadanía en General

Los convenios de colaboración o coordinación que se suscriban deberán publicarse en el Diario Oficial La Gaceta o en el portal de internet de la SEFIN.

Artículo 34. En caso de pérdida
En caso de pérdida, robo o destrucción del medio electrónico que contiene la FIEL, o cualquier otro evento que ponga en riesgo la confidencialidad del certificado digital o la llave que conforma al mismo, los sujetos obligados, bajo su absoluta responsabilidad, deberán proceder a solicitar su inmediata revocación o reposición ante la Autoridad correspondiente, sujetándose a los procesos que este último determine.

Artículo 35. Vínculo entre la Firma y el Firmante
Una vez verificada la FIEL se tendrá por válido el vínculo entre el firmante y los datos que fueron utilizados para la creación de la respectiva FIEL, generándose el acceso y registro de la persona de que se trate como firmante de los sistemas de servicios informáticos.

CAPÍTULO VIII.

SISTEMAS O HERRAMIENTAS QUE UTILICEN LA FIEL

Artículo 36. Uso de los Sistemas Informáticos
La utilización de los sistemas de servicios informáticos en la SEFIN, así como de la información registrada en ellos, será de uso restringido y solamente los sujetos autorizados podrán hacer uso de los mismos para los fines que establezca la SEFIN.

Artículo 37. Responsabilidades de la UDEM
La Unidad de Modernización al implementar procesos y procedimientos a través de servicios informáticos con la funcionalidad de la FIEL deberá generar la guía de operación correspondiente y demás material de apoyo la cual tendrá que publicarse en el portal.

Artículo 38. Documentación de Procesos y Procedimientos
Por lo anterior, la Unidad de Modernización cuando incorpore el uso de la FIEL en los procesos y

procedimientos o servicios en donde se lleven a cabo las actuaciones electrónicas, actos, mensajes de datos o documentos deberán atender y cumplir con los puntos y las características especificadas en la guía de operación que, como mínimo, deberán establecer lo siguiente:

- Objetivo
- Definiciones, siglas y abreviaturas
- Área (s) involucradas
- Ingreso al Sistema o herramientas
- Operación del Sistema
- Otros pertinentes

Artículo 39. Solicitud de Implementar FIEL en Procesos

Las dependencias de la Secretaría que requieran implementar procesos y procedimientos con la funcionalidad de la FIEL, deberán:

I. Notificar dichas iniciativas a la UDEM, UIT y a la AUTORIDAD CERTIFICADORA para que sean consideradas en el ámbito de sus atribuciones señaladas en el presente Reglamento;

II. Implementar un mecanismo de acuse de recibo electrónico de los documentos con la FIEL enviados por los medios tecnológicos establecidos;

III. Custodiar toda la documentación digital que contenga la aplicación de la FIEL en su propia computadora o cualquier otro medio provisto por la Secretaría para dicho fin, con la debida estampa de tiempo del uso de la FIEL;

IV. Realizar, previamente a la firma de los documentos, la revisión del estado de validez y vigencia del certificado digital que se utilizará;

V. En su caso solicitar a la UIT que se realicen pruebas de seguridad a la aplicación y a los servidores que interactúen con la Infraestructura.

SEGUNDO.- El presente Acuerdo debe entrar en vigencia una vez transcurrido un (1) mes contado a partir del día siguiente hábil de la fecha de su publicación en el Diario Oficial "La Gaceta".

COMUNÍQUESE Y PUBLÍQUESE,

LUIS FERNANDO MATA ECHEVERRI
Secretario de Estado en el Despacho de Finanzas

FANNY LUCÍA MARADIAGA VALLECILLO
Secretaria General
Secretaría de Estado en el Despacho de Finanzas