



Superintendencia de Notariado y Registro

MEMORANDO No.

DAF-530

Bogotá, D.C., 15 de abril de 2026

PARA: Doctor DAVID FELIPE SANCHEZ MORA, Director de Contratos

DE: **ARCENIO DE JESUS PERALTA VALBUENA**
Director de Superintendencia 0105-20

Asunto: COTIZACIÓN EN EL PROCESO DE CONTRATACIÓN DE SUMINISTRO DE CERTIFICADOS DE FIRMA DIGITAL DE FUNCIÓN PÚBLICA JUNTO CON LOS SERVICIOS ASOCIADOS DE LA SUPERINTENDENCIA DE NOTARIADO Y REGISTRO.

Cordial saludo.

En cumplimiento de lo dispuesto en la Ley 527 de 1999 y en concordancia con la Circular Externa No. 020 del 16 de mayo de 2023 expedida por el Ministerio de Hacienda y Crédito Público, mediante la cual se establece la implementación obligatoria del uso de certificados digitales en el Sistema Integrado de Información Financiera – SIIF Nación, me permito informar la necesidad de adelantar el proceso de cotización para la contratación del suministro de certificados de firma digital de función pública, junto con los servicios asociados para la Vigencia 2026.

Estos certificados digitales son requeridos para el registro y la firma de transacciones presupuestales y contables en los aplicativos SIIF Nación II – Sistema Integrado de Información Financiera y CETIL – Certificación Electrónica de Tiempos Laborados, garantizando el cargue de información en tiempo real, la continuidad del servicio y el cumplimiento de los lineamientos establecidos por el Ministerio de Hacienda y Crédito Público.

En este sentido, respetuosamente solicito se adelanten las gestiones administrativas y presupuestales correspondientes para la solicitud de cotizaciones en el SECOP y posterior contratación del suministro de certificados de firma digital de función pública, junto con los servicios asociados.



Superintendencia de Notariado y Registro

OBJETO: Contratar el suministro de certificados de firma digital de función pública, junto con los servicios asociados para su emisión, activación, custodia, administración, soporte, reasignación y renovación, requeridos para la autenticación y la firma digital de transacciones y operaciones en el Sistema Integrado de Información Financiera – SIIF Nación II y en el aplicativo CETIL – Certificación Electrónica de Tiempos Laborados.

Agradezco la atención prestada y quedo atenta a cualquier información adicional que se requiera para adelantar el trámite correspondiente.

ARCENIO DE JESUS PERALTA VALBUENA

Director de Superintendencia 0105-20

Dirección Administrativa y Financiera

Documento Firmado Electrónicamente

Anexo: Si

Copia JUAN MARTINEZ; KATERIN GOMEZ

Elaboró: DINA VANESA GUERRA RAMIREZ / DAF

Revisó: Ingeniero Oscar Corredor - Juan Pablo Martinez. YOLANDA RODRIGUEZ ROLDAN / DAF

Aprobó: Yolanda Rodríguez Roldán. KATERIN GOMEZ OLAYA / DAF



Superintendencia de Notariado y Registro



COTIZACIÓN EN EL PROCESO DE CONTRATACIÓN DE SUMINISTRO DE CERTIFICADOS DE FIRMA DIGITAL DE FUNCIÓN PÚBLICA JUNTO CON LOS SERVICIOS ASOCIADOS DE LA SUPERINTENDENCIA DE NOTARIADO Y REGISTRO.

OBJETO: Contratar el suministro de certificados de firma digital de función pública, junto con los servicios asociados para su emisión, activación, custodia, administración, soporte, reasignación y renovación, requeridos para la autenticación y la firma digital de transacciones y operaciones en el Sistema Integrado de Información Financiera – SIIF Nación II y en el aplicativo CETIL – Certificación Electrónica de Tiempos Laborados.

ALCANCE DEL OBJETO

Se requiere el suministro de certificados de firma digital de función pública, junto con los servicios asociados, con el fin de garantizar la continuidad en el registro de la información contable y financiera en el Sistema Integrado de Información Financiera SIIF Nación II, así como en el aplicativo CETIL - Certificación Electrónica de Tiempos Laborados.

El certificado digital es un archivo electrónico que contiene la información de identificación de un funcionario y permite vincular de manera segura una clave pública con una persona natural o jurídica. Este mecanismo posibilita la autenticación del usuario, la firma de transacciones electrónicas y la validación de su identidad en los sistemas de información, garantizando la integridad, autenticidad y no repudio de la información, así como la prevención de suplantación de identidad.

Los certificados de firma digital de función pública podrán estar almacenados en dispositivos criptográficos (token), en servidores seguros (HSM) u otras tecnologías equivalentes debidamente certificadas, garantizando la interoperabilidad con los aplicativos SIIF Nación II y CETIL.

Los certificados de firma digital de función pública serán utilizados para el acceso, autenticación y firma de operaciones dentro del aplicativo SIIF Nación II y del aplicativo CETIL, en cumplimiento de los lineamientos establecidos por el Ministerio de Hacienda y Crédito Público.

Los certificados de firma digital de función pública permanecerán bajo custodia de la entidad de certificación contratista, con el fin de que la Superintendencia de Notariado y Registro pueda solicitarlos y consumirlos a demanda permaneciendo en custodia de la entidad, los certificados deberán mantenerse disponibles para su entrega cuando la entidad así lo requiera.



Superintendencia de Notariado y Registro



Así mismo, la entidad contratista deberá realizar la reasignación de los certificados de firma digital de función pública adquiridos en los casos en que se presente cambio de suscriptor, bloqueo del certificado o cualquier otra situación que implique modificaciones en los datos originales del certificado. Esta reasignación deberá efectuarse sin costo adicional para la Superintendencia de Notariado y Registro. Realizar la activación de los Certificados Digitales, cuando el supervisor del Contrato haga la solicitud acompañada de los documentos requeridos. Dichos certificados deberán tener una vigencia de dos (2) años, contados a partir de la fecha de activación del certificado.

Realizar la activación de los certificados de firma digital de función pública, cuando el supervisor del Contrato haga la solicitud acompañada de los documentos requeridos. Dichos certificados deberán tener una vigencia de dos (2) años, contados a partir de la fecha de activación del certificado.

Nota técnica aclaratoria:

Para efectos del presente proceso contractual, el certificado de firma digital de función pública es el mecanismo que habilita la autenticación y la firma digital en los aplicativos SIIF Nación II y CETIL.

Dicho certificado podrá estar almacenado en token criptográfico o en servidor seguro (HSM) provisto por la entidad de certificación digital, según la modalidad ofrecida, sin que ello implique la contratación independiente de dispositivos físicos, software de firma o marcas específicas.

DESCRIPCIÓN DE LA NECESIDAD

Con el propósito de garantizar la confiabilidad de la información financiera para atender lo establecido por el Gobierno Nacional, conforme al Decreto Reglamentario 1068 del 26 de Mayo de 2015 y el Decreto 2674 de 2012 que los artículos 2 y 4 disponen lo siguiente:

Decreto 2674 de 2012

Artículo 2. “El Sistema Integrado de Información Financiera (SIIF) Nación es un sistema que coordina, integra, centraliza y estandariza la gestión financiera pública nacional, con el fin de propiciar una mayor eficiencia en el uso de los recursos de la Nación y de sus entidades descentralizadas, y de brindar información oportuna y confiable.”

Decreto Reglamentario 1068 del 26 de Mayo de 2015



Superintendencia de Notariado y Registro

Artículo 2.9.1.1.5 *“Los órganos ejecutores del Presupuesto General de la Nación, las Direcciones Generales del Presupuesto Público Nacional y de Crédito Público y del Tesoro Nacional del Ministerio de Hacienda y Crédito Público, y la Contaduría General de la Nación, o quien haga sus veces, deberán registrar en línea las transacciones en el SIIF Nación asociadas con su área de negocio, dentro del horario establecido, conforme con los instructivos que para el efecto expida el Administrador del Sistema...”*

La Superintendencia debe dar un adecuado uso y administración de su información presupuestal, debe registrar en el sistema SIIF Nación las diferentes transacciones de conformidad con los instructivos que para el efecto expide el administrador del Sistema SIIF, en el cual se realiza el cargue de información presupuestal y contable en tiempo real.

Para tales efectos, con el propósito de adelantar y continuar con las acciones necesarias para el cargue de la información financiera de la Superintendencia de Notariado y Registro en el SIIF y de acuerdo lo establecido en la circular No. 05 de febrero de 2015, “A partir del 1 de abril de 2016 será obligatorio para el ingreso al sistema de todos los usuarios del SIIF Nación, el certificado digital almacenado en token criptográfico”.

La Superintendencia debe asegurar el registro confiable de información financiera y laboral de conformidad con:

- Ley 527 de 1999
- Decreto 2674 de 2012, artículos 2 y 4
- Decreto Reglamentario 1068 de 2015
- Circulares del Ministerio de Hacienda y Crédito Público

SIIF Nación II: Sistema que centraliza y estandariza la gestión financiera nacional, obligando a que todos los usuarios utilicen certificados digitales de función pública homologados para registrar transacciones.

CETIL: Aplicativo para certificación de tiempos laborados, que también requiere certificados de firma digital de función pública para autenticar usuarios y registrar información laboral.

Se busca garantizar continuidad operativa, evitar interrupciones en los servicios y asegurar cumplimiento normativo.



Superintendencia de Notariado y Registro

Así mismo, mediante la Circular Externa N. 014 del 28 de marzo 2025 expedida por el Ministerio de Hacienda, estableció las condiciones para operar con entidades de certificación digital abiertas homologadas en el SIIF Nación.

El Sistema Integrado de Información Financiera SIIF Nación con base a la ley 527 de 1999 implementa la firma digital de registros realizados por los usuarios en el aplicativo, con certificados digitales de función pública expedidos por Entidades de Certificación Digital Abiertas acreditadas por la ONAC y homologadas por la Administración del SIIF Nación, dentro del marco establecido en la circular externa N. 002 del 25 de enero de 2021 expedida por la Administración del SIIF Nación.

Las Entidades de certificación abiertas cuyos certificados de función pública pueden ser utilizadas en el aplicativo SIIF Nación.

1. ANDES SERVICIO DE CERTIFICACION DIGITAL S. A.
En token criptográfico y/o servidor seguro (HSM) provisto por ANDES SCD. S.A.
2. CAMERFIRMA COLOMBIA SAS.
En token criptográfico y/o servidor seguro (HSM) provisto por CAMERFIRMA SAS.
3. GESTIÓN DE SEGURIDAD ELECTRÓNICA S.A. – GSE.
En token criptográfico y/o servidor seguro (HSM) provisto por GSE S.A.
4. LLEIDA SAS
En token criptográfico y/o servidor seguro (HSM) provisto por Lleida SAS
5. OLIMPIA IT S.A.S
En token criptográfico y/o servidor seguro (HSM) provisto por OLIMPIA IT S.A.S.
6. SOCIEDAD CAMERAL DE CERTIFICACION DIGITAL - CERTICAMARA S.A.

En token criptográfico.
7. THOMAS SIGNE

Servidor seguro (HSM) provisto por THOMAS SIGNE

Teniendo en cuenta que se debe garantizar el adecuado uso y administración de la información presupuestal, se debe registrar en el sistema SIIF Nación las diferentes transacciones de conformidad con los instructivos que para el efecto expide el administrador del Sistema SIIF, en el cual se realiza el cargue de información presupuestal y contable en tiempo real, se requiere la adquisición - renovación de los certificados de



Superintendencia de Notariado y Registro



firma digital de función pública cuales son una herramienta necesaria para trabajar en SIIF II y CETIL, de acuerdo requerimiento del Ministerio de Hacienda y Crédito Público, con el fin de obtener el servicio sin interrupción, disminuyendo los tiempos de trámite y entrega y no perder días de vigencia ya que los certificados digitales tienen una vigencia de uno (1) o dos (2) años. Igualmente dar cumplimiento a los requisitos exigidos por el Ministerio de Hacienda y Crédito Público.

Por lo anterior se requiere que la SNR adelante la presente contratación de suministro de certificados de firma digital de función pública para continuar con el ingreso y registro de la información financiera de la Superintendencia de Notariado y Registro en el Sistema Integrado de Información Financiera SIIF Nación II y en el aplicativo CETIL.

En concordancia con lo anterior, nos permitimos relacionar el listado de la necesidad que se requieren contratar para satisfacer la necesidad de la entidad, los cuales se señalan a continuación:

No.	ELEMENTO	UNIDAD DE MEDIDA	CANTIDAD
1	Certificados de firma digital de función pública	Unidad	250

El presente proceso está codificado en el clasificador de bienes y servicios UNSPSC como se indica en la siguiente tabla.

El objeto contractual se enmarca en los siguientes códigos del Clasificador de bienes y servicios:

Grupo	Segmento	Familia	Clase	Producto	Código UNPSC	Descripción
Productos de uso final	Difusión de Tecnologías de Información y Telecomunicaciones	Software	Software de seguridad y protección	Software de servidor de autenticación	43233201	Certificados de firma digital de función pública de conformidad con las condiciones técnicas de acuerdo con la Circular Externa N. 002 del 25 de enero 2021 del Ministerio de Hacienda.
Servicios	Servicios basados en ingeniería, investigación y tecnología	Entrega de servicios de tecnología de información	Servicios de administración de acceso	Servicios de administración de aplicaciones de software	81161501	Certificados de firma digital de función pública de conformidad con las condiciones técnicas de acuerdo con la Circular Externa N. 002 del 25 de enero 2021 del Ministerio de Hacienda
Servicios	Servicios basados en ingeniería, investigación y tecnología	Servicios informáticos	Ingeniería de software o hardware	Servicios de programación de aplicaciones	81111504	Certificados de firma digital de función pública de conformidad con las condiciones técnicas de acuerdo con la Circular Externa N. 002 del 25 de enero 2021 del Ministerio de Hacienda

En atención a lo expuesto, se requiere el suministro de certificados de firma digital de función pública para los usuarios que tengan asignados los perfiles definidos por el Ministerio de Hacienda y Crédito Público, tales como Pagador, Gastos, Contable, PAC, Modificación Presupuestal e Ingresos, entre otros.



Superintendencia de Notariado y Registro



Se precisa que, si bien los certificados digitales de función pública serán utilizados tanto para el acceso y operación en el aplicativo SIIF Nación II como en el aplicativo CETIL - Certificación Electrónica de Tiempos Laborados, la mayor demanda de certificados se concentra en el SIIF Nación II, en razón al volumen de usuarios y a la frecuencia de las transacciones financieras que allí se registran.

Cuando los certificados de firmas digitales de función pública sean almacenados en dispositivos criptográficos físicos (token), el proveedor deberá asegurar la entrega oportuna y segura de los mismos en las sedes y dependencias que determine la Superintendencia de Notariado y Registro, incluyendo las Oficinas de Registros de Instrumentos Públicos a Nivel Nacional y Nivel Central.

Se precisa que los certificados digitales destinados al ingreso al aplicativo CETIL son pocos para la Entidad

No obstante, se garantiza que la solución contratada cubra de manera integral las necesidades de ambos aplicativos, asegurando la disponibilidad de certificados de firma digital de función pública para los usuarios que requieran acceso y operación en SIIF y en CETIL.

El aplicativo CETIL – Certificación Electrónica de Tiempos Laborados sirve principalmente para gestionar y certificar electrónicamente el tiempo trabajado de los empleados públicos de manera oficial y segura. Su función es digitalizar y centralizar la información sobre tiempos laborados, lo que permite a las entidades del sector público cumplir con normativas laborales y administrativas.

El aplicativo CETIL es utilizado por la Dirección de Talento Humano de la SNR para Certificar los tiempos laborados de los funcionarios y exfuncionarios que pertenecen (o pertenecieron) a la planta de la entidad; lo anterior, para dar respuesta a los requerimientos a título personal o de fondos de pensiones.

El aplicativo CETIL es utilizado para el Fondo de Vivienda para atender las peticiones que envían los Fondos de Pensiones y particulares para certificar los tiempos laborados de trabajadores de Fonprenor, por lo que cuando llegan peticiones, las atiende Dirección Administrativa y Financiera de acuerdo con un acto administrativo.

REQUISITOS DEL PROVEEDOR

El proveedor deberá cumplir con los siguientes requisitos:

Mediante la Circular Externa N. 014 del 28 de Marzo 2025, expedida por el Ministerio de Hacienda, Entidades de certificación digital abiertas homologadas en el SIIF



Superintendencia de Notariado y Registro



Nación, con base en la ley 527 de 1999 implementa la firma digital de registros realizados por los usuarios en el aplicativo, con certificados de función pública expedidos por Entidades de Certificación Digital Abiertas acreditadas por LA ONAC y homologadas por la Administración del SIIF Nación dentro del marco establecido en la Circular Externa N. 002 de 25 de enero de 2021 expedida por la Administración SIIF Nación.

De acuerdo con la Circular Externa N. 002 del 25 de enero de 2021 – Firmas digital en el aplicativo SIIF Nación.

La Administración SIIF Nación implementó el uso de la firma digital con base en la ley 527 de 1999, para el registro por parte de los usuarios del aplicativo de transacciones en el SIIF Nación desde el año 2005, utilizando certificados digitales de función pública expedidos por Entidades de Certificación Digital Abierta.

Considerando que el Ministerio de Hacienda - SIIF Nación no es el responsable de la emisión de los certificados digitales, a continuación, se establecen las condiciones para operar con entidades certificadoras digitales abiertas de confianza para el SIIF Nación:

1. La entidad de certificación digital abierta debe estar autorizada por el Organismo Nacional de Acreditación de Colombia – ONAC, para expedir certificados digitales de Función Pública.
2. La entidad de certificación digital abierta debe estar autorizada por la Administración SIIF Nación para utilizar sus certificados digitales de función pública en el aplicativo SIIF Nación almacenados en token criptográfico o almacenados en un servidor seguro (HSM) provisto por la entidad de certificación digital.

Dicha autorización se emitirá por la Administración SIIF Nación, previa solicitud del representante legal a la administración SIIF Nación en la cual se manifieste el cumplimiento de lo establecido en el documento y adjuntando los respectivos soportes y una vez realizadas las pruebas técnicas de funcionamiento de los certificados digitales con el aplicativo SIIF Nación.

La lista de entidades de certificación digital abierta autorizadas y el tipo de almacenamiento utilizado para el certificado digital autorizado por la Administración del SIIF Nación, puede ser consultada en la página WEB del Ministerio de Hacienda y Crédito Público en www.minhacienda.gov.co/ SIIF Sistema Integrado de Información Financiera/ Ciclo de negocios/ Administración de seguridad.

3. Los certificados de función pública a utilizar en el SIIF Nación que estén almacenados en Token Criptográficos, estos deben soportar interfaz PKCS11 y cumplir mínimo con el



Superintendencia de Notariado y Registro



estándar 140-2 Nivel 3 de aseguramiento criptográfico.

4. La entidad de certificación digital abierta debe proveer a sus suscriptores que utilicen token criptográfico, los controladores o drivers para el token criptográfico en los sistemas operativos utilizados por la entidad usuaria y el soporte para su instalación.
5. Para los certificados de función pública que estén almacenados en un servidor seguro (HSM) provisto por la entidad de certificación digital, la entidad de certificación digital debe proveer a sus suscriptores los controladores o driver para acceder al certificado digital del suscriptor. Este controlador o driver debe cumplir mínimo con:
 - a. Integrarse con el terminador de VPN para acceso al SIIF Nación y con el componente cliente de firma digital del SIIF Nación.
 - b. Implementar doble factor de autenticación del usuario para acceder al certificado digital almacenado en el servidor seguro (HSM) provisto por la entidad.
6. Los certificados digitales a utilizar en el aplicativo SIIF Nación para sus usuarios, son certificados de Función Pública con estándar X.509.V3, Los certificados deben cumplir con los requisitos exigidos en artículo 35 de la ley 527 de 1999, teniendo en cuenta las siguientes características del certificado digital requeridos en el SIIF Nación:
 - a) Nombre
 - b) Correo electrónico
 - c) Ciudad
 - d) Entidad
 - e) Cédula de Ciudadanía
 - f) NIT de la entidad usuaria
 - g) Título o cargo del usuario.
 - h) El certificado digital debe utilizar algoritmo de firma: SHA2RSA
7. Los certificados digitales de función pública se deben poder utilizar en el SIIF Nación para:
 - a) Autenticación, utilizando un terminador de VPN para acceso al SIIF Nación, el cual verifica la información del certificado y la autorización del SIIF Nación de la entidad de certificación.
 - b) Firmar digitalmente transacciones.
 - c) Firmar digitalmente archivos para ser utilizados en cargas masivas en el SIIF Nación.
 - d) El aplicativo SIIF Nación no provee la herramienta para la firma de archivos. La entidad de certificación debe proveer el soporte para el uso de los certificados digitales para la firma de archivos o documentos electrónicos.



Superintendencia de Notariado y Registro



8. La entidad de certificación digital abierta deberá proveer a la Administración SIIF Nación, para la validación del estado de revocación del certificado, la publicación de la CRL, adicionalmente el SIIF Nación utilizará el método de verificación del estado del certificado llamado OCSP, para la cual la entidad de certificación digital abierta deberá proveer una URL de acceso a este servicio.

Cualquier cambio de alguno de estos datos debe ser informado previamente por la entidad de certificación abierta a la administración SIIF Nación.

Una vez la Administración SIIF Nación informe que dichos cambios fueron aplicados, podrán ser utilizados en el aplicativo SIIF Nación.

9. La entidad de certificación digital abierta debe garantizar, la actualización de la CRL, siendo su responsabilidad que sea oportuna y que esté disponible para consulta durante 7 x 24 x 365 días.

La administración SIIF Nación no se hace responsable por los perjuicios que pueda ocasionar al usuario del aplicativo que no pueda realizar registros oportunamente por fallas en la actualización o disponibilidad de la CRL, dicha responsabilidad recae directamente sobre la entidad certificadora digital abierta.

10. La entidad de certificación digital abierta debe garantizar la disponibilidad del servicio OCSP, siendo su responsabilidad que sea oportuno y que esté disponible para consulta durante 7 x 24 x 365 días.

La administración SIIF Nación no se hace responsable por los perjuicios que pueda ocasionar al usuario del aplicativo que no pueda realizar registros oportunamente por fallas en la disponibilidad del servicio OCSP, dicha responsabilidad recae directamente sobre la entidad de certificación digital abierta.

11. La entidad de certificación digital abierta deberá disponer de la infraestructura de operación, servicio y soporte a sus usuarios, según los acuerdos de niveles de servicio que tenga con la entidad usuaria.

La administración SIIF Nación no se hace responsable por los perjuicios que pueda ocasionar al usuario del aplicativo las posibles fallas que afecten la operación, servicio o soporte de los usuarios de la entidad de certificación digital abierta.

12. La entidad de certificación digital abierta deberá notificar por lo menos con un mes de anticipación la fecha de vencimiento del certificado digital, así mismo ofrecer al coordinador SIIF Nación de la entidad las herramientas para la gestión (fechas de emisión, fechas de caducidad, cupo utilizado) para una oportuna gestión por parte de



Superintendencia de Notariado y Registro



este de los certificados digitales. Así mismo, de dar a conocer y capacitar a los Coordinadores y usuarios del SIIF Nación sobre los procedimientos y trámites administrativos para el manejo del ciclo de vida del certificado digital.

13. La entidad de certificación digital abierta deberá disponer de un contacto directo de soporte de la entidad certificadora con el soporte del SIIF Nación para resolver casos de soporte que involucren las dos partes.
14. La entidad de certificación abierta y la entidad usuaria deberán acordar lo referente a las garantías a que hace referencia el artículo 9 del Decreto 333 de 2014.

OBLIGACIONES ESPECIFICAS

1. Suministrar y activar los certificados de firma digital de función pública en coordinación con la Superintendencia de Notariado y Registro (SNR), de manera paulatina y conforme a las necesidades de la entidad, asegurando su entrega en sincronía con la implementación de los macroprocesos del Sistema Integrado de Información Financiera SIIF Nación II y CETIL.
Con el fin de optimizar el uso de los certificados digitales, el contratista deberá indicar la fecha de asignación de cada certificado a los funcionarios de las Oficinas de Registro Principales, sus Seccionales y el Nivel Central, garantizando que los certificados no sean revocados sin haber sido utilizados por los funcionarios de la Superintendencia de Notariado y Registro.
2. Garantizar el adecuado funcionamiento de los certificados de firma digital de función pública en los computadores en los cuales se instalen, asegurando que la capacitación proporcionada sea avalada por los funcionarios que la reciban. Lo anterior deberá constar por escrito mediante certificación del supervisor designado, dejando constancia del recibo a satisfacción.
3. Cumplir con las condiciones técnicas descritas en la oferta, que forma parte integral del contrato, relativas al suministro, instalación y funcionamiento de los certificados de firma digital de función pública.
4. Efectuar el reemplazo inmediato de los certificados de firma digital de función pública que presenten defectos o que no cumplan con las condiciones necesarias para que los usuarios del SIIF Nación puedan realizar sus actividades de manera adecuada, en un plazo máximo de cinco (5) días hábiles.



Superintendencia de Notariado y Registro



5. Disponer de la infraestructura necesaria para la operación, servicio y soporte de los certificados de firma digital de función pública a los usuarios.
6. Brindar acompañamiento telefónico constante para que los funcionarios y contratistas puedan resolver sus inquietudes, garantizando el servicio de Call Center o mensajería instantánea, con el fin de coordinar citas para la entrega personalizada de los certificados de firma digital de función pública a los suscriptores.
7. Entregar el certificado de firma digital de función pública directamente al suscriptor, previa verificación de su identidad, de manera personal e intransferible. En casos excepcionales, se podrá efectuar la entrega a un tercero que actúe como apoderado del suscriptor, siempre que el poder correspondiente haya sido otorgado ante Notario.
8. Entregar los certificados de firma digital de función pública y todos los elementos relacionados, asegurando que sean de óptima calidad.
9. Suministrar certificados de firma digital de función pública de acuerdo con las necesidades de los usuarios SIIF Nación.
10. Proporcionar la renovación y/o reposición de certificados de firma digital de función pública, asegurando que sean compatibles con la tecnología de la Superintendencia de Notariado y Registro donde se encuentren en funcionamiento los certificados actuales.
11. Incluir la entrega de manuales de usuario y medios de instalación para los certificados de firma digital de función pública.
12. Cumplir con los lineamientos de compatibilidad tecnológica exigidos por el Sistema Integrado de Información Financiera SIIF Nación y CETIL para el correcto funcionamiento de los certificados de firma digital de función pública
13. Prestar soporte estándar durante la vigencia del respectivo certificado digital de conformidad con lo establecido en la oferta. Este soporte será prestado a través de acceso telefónico en horario de 8:00 am a 5:00 pm de lunes a viernes.
14. Prestar soporte relacionado con los certificados de firma digital de función pública a través de la página web del oferente, incluyendo los servicios de chat, preguntas y respuestas frecuentes, y la documentación técnica de soporte.



Superintendencia de Notariado y Registro



15. Prestar soporte relacionado con los certificados de firma digital de función pública a través del correo electrónico que el oferente determine.
16. Informar por escrito cualquier cambio en las condiciones establecidas en este contrato durante su ejecución. Obrar con lealtad y buena fe en todas las etapas contractuales, evitando dilaciones o trabas. El soporte relacionado con los certificados digitales se prestará en los siguientes niveles de servicio: primer nivel, con respuesta máxima de dos (2) horas; y segundo nivel, para casos que requieran un proceso de investigación específico, los cuales contarán con un registro y diagnóstico que permitirá al usuario conocer el tiempo estimado de respuesta y realizar seguimiento a su solicitud a través de la aplicación proporcionada.
17. Cumplir con las condiciones técnicas de los certificados digitales, de acuerdo con lo establecido en la Circular Externa N.º 002 del 25 de enero de 2021, expedida por la Administración SIIF Nación del Ministerio de Hacienda.
18. Cumplir con la Circular Externa N. 014 del 28 de marzo 2025 expedida por el Ministerio de Hacienda, estableció las condiciones para operar con entidades de certificación digital abiertas homologadas en el SIIF Nación.
19. Los certificados de firma digital de función pública permanecerán bajo custodia de la entidad de certificación contratista, con el fin de que la Superintendencia de Notariado y Registro pueda solicitarlos y consumirlos a demanda permaneciendo en custodia de la entidad, los certificados deberán mantenerse disponibles para su entrega cuando la entidad así lo requiera.
20. La entidad contratista deberá realizar la reasignación de los certificados de firma digital de función pública adquiridos en los casos en que se presente cambio de suscriptor, bloqueo del certificado o cualquier otra situación que implique modificaciones en los datos originales del certificado. Esta reasignación deberá efectuarse sin costo adicional para la Superintendencia de Notariado y Registro. Realizar la activación de los Certificados Digitales, cuando el supervisor del Contrato haga la solicitud acompañada de los documentos requeridos. Dichos certificados deberán tener una vigencia de dos (2) años, contados a partir de la fecha de activación del certificado.
21. Realizar la activación de los certificados de firma digital de función pública, cuando el supervisor del Contrato haga la solicitud acompañada de los documentos requeridos. Dichos certificados deberán tener una vigencia de dos (2) años, contados a partir de la fecha de activación del certificado.



Superintendencia de Notariado y Registro



22. Entregar los certificados de firma digital de función pública a nivel nacional, conforme a los requerimientos que la Superintendencia de Notariado y Registro determine; teniendo en cuenta las fechas de vencimiento y las solicitudes que realiza el Registrador de Usuarios de la Entidad.
23. Presentar mensualmente un informe sobre la cantidad de certificados digitales que están próximos a vencerse y de los ya entregados, remitiéndolo a la Registradora de Usuarios de la entidad en formato digital. Asimismo, informar el saldo de certificados en custodia que aún están pendientes de entrega.
24. Presentar un informe final detallado de todos los certificados digitales entregados a la entidad, indicando cantidades, destinatarios y estado de cada uno.
25. Contar con la información precisa y repositorio de controladores y programas requeridos por la entidad certificadora que sea seleccionada con acompañamiento formativo para los técnicos de la mesa de ayuda que se encargarán de hacer las respectivas instalaciones y configuraciones en los equipos de cómputo.
26. Los certificados de firma digital de función pública a contratar deberán tener una vigencia de dos (2) años, contados a partir del día de su entrega al usuario.
27. Cuando los certificados de firmas digitales de función pública sean almacenados en dispositivos criptográficos físicos (token), el proveedor deberá asegurar la entrega oportuna y segura de los mismos en las sedes y dependencias que determine la Superintendencia de Notariado y Registro, incluyendo las Oficinas de Registros de Instrumentos Públicos a Nivel Nacional y Nivel Central.
28. El certificado de firma digital de función pública objeto del presente proceso deberá ser utilizado para el ingreso y gestión en los sistemas SIIF y CETIL, conforme a las necesidades y requerimiento previamente definidos por la Superintendencia de Notariado y Registro (SNR).

Ficha Técnica - Especificaciones mínimas de los elementos a contratar

ITEM	Descripción del bien	Unidad de medida	Material	Tamaño	Utilidad	Características Físicas
1	Certificados de firma digital de función pública junto con los servicios asociados para su emisión, activación, custodia, administración, soporte, reasignación y renovación, requeridos para la autenticación y la firma digital de transacciones y operaciones en el Sistema Integrado de Información Financiera SIIF Nación y en el aplicativo CETIL – Certificación Electrónica de Tiempos Laborados	Unidad			Certificados de firma digital de función pública, junto con los servicios asociados para su emisión, activación, custodia, administración, soporte, reasignación y renovación, requeridos para la autenticación y la firma digital de transacciones y operaciones en el Sistema Integrado de Información Financiera – SIIF Nación II y en el aplicativo CETIL – Certificación Electrónica de Tiempos Laborados. Los certificados de firma digital de función pública permanecerán bajo custodia de la entidad de certificación contratista, con el fin de que la Superintendencia de Notariado y Registro pueda solicitarlos y consumirlos a demanda permaneciendo en custodia de la entidad, los certificados deberán mantenerse disponibles para su entrega cuando la entidad así lo requiera. Así mismo, la entidad contratista deberá realizar la reasignación de los certificados de firma digital de función pública adquiridos en los casos en que se presente cambio de suscriptor, bloqueo del certificado o cualquier otra situación que implique modificaciones en los datos originales del certificado. Esta reasignación deberá efectuarse sin costo adicional para la Superintendencia de Notariado y Registro. Realizar la activación de los Certificados Digitales, cuando el supervisor del Contrato haga la solicitud acompañada de los documentos requeridos. Dichos certificados deberán tener una vigencia de dos (2) años, contados a partir de la fecha de activación del certificado. Realizar la activación de los certificados de firma digital de función pública, cuando el supervisor del Contrato haga la solicitud acompañada de los documentos requeridos. Dichos certificados deberán tener una vigencia de dos (2) años, contados a partir de la fecha de activación del certificado. La Empresa debe cumplir las condiciones técnicas de las firmas (certificados) digitales relacionadas en la Circular N. 002 del 25 de enero 2021 Asunto: Firma digital en el aplicativo SIIF Nación del Ministerio de Hacienda y la Circular Externa N. 014 del 28 de marzo 2025: Entidades de Certificación abiertas homologadas en el SIIF Nación; Externa N. 014 del 28 de marzo 2025; Las Entidades de certificación digital abiertas homologadas en el SIIF Nación 1. ANDES SERVICIO DE CERTIFICACION DIGITAL S. A. En token criptográfico y/o servidor seguro (HSM) provisto por ANDES SCD. S.A. 2. CAMERFIRMA COLOMBIA SAS. En token criptográfico y/o servidor seguro (HSM) provisto por CAMERFIRMA SAS. 3. GESTIÓN DE SEGURIDAD ELECTRÓNICA S.A. – GSE. En token criptográfico y/o servidor seguro (HSM) provisto por GSE S.A. 4. LLEIDA SAS En token criptográfico y/o servidor seguro (HSM) provisto por Lleida SAS 5. OLIMPIA IT S.A.S En token criptográfico y/o servidor seguro (HSM) provisto por OLIMPIA IT S.A.S. 6. SOCIEDAD CAMERAL DE CERTIFICACION DIGITAL - CERTICAMARA S.A. En token criptográfico. 7. THOMAS SIGNE Servidor seguro (HSM) provisto por THOMAS SIGNE	Certificados de Firma digital de función pública, junto con los servicios asociados

**SISTEMA INTEGRADO DE INFORMACION FINANCIERA SIIF NACION
CIRCULAR EXTERNA No. 002**

2.0.0.1

Bogotá D. C., 25 de enero de 2021

PARA: COORDINADORES DEL SIIF NACION

ASUNTO: Firma digital en el aplicativo SIIF Nación

La Administración SIIF Nación implementó el uso de la firma digital con base en la ley 527 de 1999, para el registro por parte de los usuarios del aplicativo de transacciones en el SIIF Nación desde el año 2005, utilizando certificados digitales de función pública expedidos por Entidades de Certificación Digital Abierta.

Considerando que el Ministerio de Hacienda - SIIF Nación no es el responsable de la emisión de los certificados digitales, a continuación, se establecen las condiciones para operar con entidades certificadoras digitales abiertas de confianza para el SIIF Nación:

1. La entidad de certificación digital abierta debe estar autorizada por el Organismo Nacional de Acreditación de Colombia – ONAC, para expedir certificados digitales de Función Pública.
2. La entidad de certificación digital abierta debe estar autorizada por la Administración SIIF Nación para utilizar sus certificados digitales de función pública en el aplicativo SIIF Nación almacenados en token criptográfico o almacenados en un servidor seguro (HSM) provisto por la entidad de certificación digital.

Dicha autorización se emitirá por la Administración SIIF Nación, previa solicitud del representante legal a la administración SIIF Nación en la cual se manifieste el cumplimiento de lo establecido en este documento y adjuntando los respectivos documentos soporte y una vez realizadas las pruebas técnicas de funcionamiento de los certificados digitales con el aplicativo SIIF Nación.

La lista de entidades de certificación digital abierta autorizadas y el tipo de almacenamiento utilizado para el certificado digital autorizado por la Administración del SIIF Nación, puede ser consultada en la página WEB del Ministerio de Hacienda y Crédito Público en www.minhacienda.gov.co / SIIF Sistema Integrado de Información Financiera / Ciclo de Negocios / Administración de seguridad.



3. Los certificados de función pública a utilizar en el SIIF Nación que estén almacenados en Token Criptográficos, estos deben soportar interfaz PKCS11 y cumplir mínimo con el estándar 140-2 Nivel 3 de aseguramiento criptográfico.
4. La entidad de certificación digital abierta debe proveer a sus suscriptores que utilicen token criptográfico, los controladores o drivers para el token criptográfico en los sistemas operativos utilizados por la entidad usuaria y el soporte para su instalación.
5. Para los certificados de función pública que estén almacenados en un servidor seguro (HSM) provisto por la entidad de certificación digital, la entidad de certificación digital debe proveer a sus suscriptores los controladores o driver para acceder al certificado digital del suscriptor. Este controlador o driver debe cumplir mínimo con:
 - a. Integrarse con el terminador de VPN para acceso al SIIF Nación y con el componente cliente de firma digital del SIIF Nación.
 - b. Implementar doble factor de autenticación del usuario para acceder al certificado digital almacenado en el servidor seguro (HSM) provisto por la entidad.
6. Los certificados digitales a utilizar en el aplicativo SIIF Nación para sus usuarios, son certificados de Función Pública con estándar X.509.V3, Los certificados deben cumplir con los requisitos exigidos en artículo 35 de la ley 527 de 1999, teniendo en cuenta las siguientes características del certificado digital requeridos en el SIIF Nación:
 - a) Nombre
 - b) Correo electrónico
 - c) Ciudad
 - d) Entidad
 - e) Cédula de Ciudadanía
 - f) NIT de la entidad usuaria
 - g) Título o cargo del usuario.
 - h) El certificado digital debe utilizar algoritmo de firma: SHA2RSA
7. Los certificados digitales de función pública se deben poder utilizar en el SIIF Nación para:
 - a) Autenticación, utilizando un terminador de VPN para acceso al SIIF Nación, el cual verifica la información del certificado y la autorización del SIIF Nación de la entidad de certificación.
 - b) Firmar digitalmente transacciones.
 - c) Firmar digitalmente archivos para ser utilizados en cargas masivas en el SIIF Nación.



d) El aplicativo SIIF Nación no provee la herramienta para la firma de archivos. La entidad de certificación debe proveer el soporte para el uso de los certificados digitales para la firma de archivos o documentos electrónicos.

8. La entidad de certificación digital abierta deberá proveer a la Administración SIIF Nación, para la validación del estado de revocación del certificado, la publicación de la CRL, adicionalmente el SIIF Nación utilizará el método de verificación del estado del certificado llamado OCSP, para la cual la entidad de certificación digital abierta deberá proveer una URL de acceso a este servicio.

Cualquier cambio de alguno de estos datos debe ser informado previamente por la entidad de certificación abierta a la administración SIIF Nación.

Una vez la Administración SIIF Nación informe que dichos cambios fueron aplicados, podrán ser utilizados en el aplicativo SIIF Nación.

9. La entidad de certificación digital abierta debe garantizar, la actualización de la CRL, siendo su responsabilidad que sea oportuna y que esté disponible para consulta durante 7 x 24 x 365 días.

La administración SIIF Nación no se hace responsable por los perjuicios que pueda ocasionar al usuario del aplicativo que no pueda realizar registros oportunamente por fallas en la actualización o disponibilidad de la CRL, dicha responsabilidad recae directamente sobre la entidad certificadora digital abierta.

10. La entidad de certificación digital abierta debe garantizar la disponibilidad del servicio OCSP, siendo su responsabilidad que sea oportuno y que esté disponible para consulta durante 7 x 24 x 365 días.

La administración SIIF Nación no se hace responsable por los perjuicios que pueda ocasionar al usuario del aplicativo que no pueda realizar registros oportunamente por fallas en la disponibilidad del servicio OCSP, dicha responsabilidad recae directamente sobre la entidad de certificación digital abierta.

11. La entidad de certificación digital abierta deberá disponer de la infraestructura de operación, servicio y soporte a sus usuarios, según los acuerdos de niveles de servicio que tenga con la entidad usuaria.

La administración SIIF Nación no se hace responsable por los perjuicios que pueda ocasionar al usuario del aplicativo las posibles fallas que afecten la operación, servicio o soporte de los usuarios de la entidad de certificación digital abierta.



12. La entidad de certificación digital abierta deberá notificar por lo menos con un mes de anticipación la fecha de vencimiento del certificado digital, así mismo ofrecer al coordinador SIIF Nación de la entidad las herramientas para la gestión (fechas de emisión, fechas de caducidad, cupo utilizado) para una oportuna gestión por parte de este de los certificados digitales. Así mismo, de dar a conocer y capacitar a los Coordinadores y usuarios del SIIF Nación sobre los procedimientos y trámites administrativos para el manejo del ciclo de vida del certificado digital.
13. La entidad de certificación digital abierta deberá disponer de un contacto directo de soporte de la entidad certificadora con el soporte del SIIF Nación para resolver casos de soporte que involucren las dos partes.
14. La entidad de certificación abierta y la entidad usuaria deberán acordar lo referente a las garantías a que hace referencia el artículo 9 del Decreto 333 de 2014.

DAVID FERNANDO MORALES DOMINGUEZ
Administrador del SIIF Nación
Viceministerio General de Hacienda

APROBÓ: David Morales
ELABORÓ: Jesús Rodríguez



**SISTEMA INTEGRADO DE INFORMACION FINANCIERA SIIF NACION
CIRCULAR EXTERNA No. 014**

2.0.0.1

Bogotá D. C., 28 de marzo de 2025

PARA Coordinadores, delegados, usuarios del SIIF Nación

ASUNTO Entidades de certificación digital abiertas homologadas en el SIIF Nación

El Sistema Integrado de Información Financiera SIIF Nación con base en la ley 527 de 1999, implementa la firma digital de registros realizados por los usuarios en el aplicativo, con certificados digitales de función pública expedidos por Entidades de Certificación Digital Abiertas acreditadas por la ONAC y homologadas por la Administración del SIIF Nación, dentro del marco establecido en la circular externa No. 002 del 25 de enero de 2021 expedida por la Administración del SIIF Nación.

A continuación, se lista las Entidades de Certificación Abierta cuyos certificados de función pública pueden ser utilizados en el aplicativo SIIF Nación:

1. ANDES SERVICIO DE CERTIFICACION DIGITAL S. A.
En token criptográfico y/o servidor seguro (HSM) provisto por ANDES SCD. S.A.
2. CAMERFIRMA COLOMBIA SAS.
En token criptográfico y/o servidor seguro (HSM) provisto por CAMERFIRMA SAS.
3. GESTIÓN DE SEGURIDAD ELECTRÓNICA S.A. – GSE.
En token criptográfico y/o servidor seguro (HSM) provisto por GSE S.A.
4. LLEIDA SAS
En token criptográfico y/o servidor seguro (HSM) provisto por Lleida SAS
5. OLIMPIA IT S.A.S
En token criptográfico y/o servidor seguro (HSM) provisto por OLIMPIA IT S.A.S.
6. SOCIEDAD CAMERAL DE CERTIFICACION DIGITAL - CERTICAMARA S.A.
En token criptográfico.



7. THOMAS SIGNE

Servidor seguro (HSM) provisto por THOMAS SIGNE.

Cordialmente,



DAVID FERNANDO MORALES DOMÍNGUEZ
Administrador del SIIF Nación
Viceministerio General de Hacienda