ADENDA No. 2

UNIDAD ADMINISTRATIVA ESPECIAL –
DIRECCIÓN NACIONAL DE DERECHO DE AUTOR

Mínima Cuantía No. DNDA-029-2026

Me permito comunicar a los oferentes, a las veedurías ciudadanas y a la ciudadanía en general, dentro del proceso de Mínima Cuantía **No. DNDA-029-2026** cuyo objeto es **"Adquisición de certificados digitales TOKEN para los usuarios que ejecutan el aplicativo SIIF NACIÓN y funcionarios que requieren firma digital en PDF, de la Dirección Nacional de Derechos de Autor"**, que teniendo en cuenta las observaciones presentadas por los posibles oferentes, se requiere modificar la invitación pública en los numerales que a continuación se relacionan:

Modificar en la invitación pública el numeral 5. Especificaciones Técnicas.

El requerimiento de especificaciones técnicas queda así:

5. ESPECIFICACIONES TÉCNICAS MÍNIMAS EXIGIDAS.

Los proponentes deberán presentar con su oferta el formato de compromiso de cumplimiento de especificaciones técnicas, el contratista deberá cumplir con la totalidad de las especificaciones técnicas que se indican a continuación:

CERTIFICADOS FUNCIÓN PÚBLICA SIIF NACIÓN
FORMATO: Firma Centralizada
VIGENCIA: 1 año

Ítem	Condiciones Técnicas Mínimas
1	Certificado Digital de Función Pública emitido por una entidad acreditada ante el Organismo Nacional de Acreditación (ONAC), de acuerdo con los Criterios Específicos de Acreditación CEA, para prestar el servicio de emisión de certificados digitales de función pública.
2	El Certificado Digital debe ser alojado en dispositivos criptográficos HSM (Hardware Security Module) que cumplan con el estándar FIPS 140-2 Level 3 o superior.
3	Algoritmo de firma SHA256 with RSA.
4	El servicio de certificados centralizados debe disponer de un punto de entrada vía servicio web seguro, utilizando el estándar TLS (Transport Layer Security).
5	El Certificado Digital debe Contar con una clave pública RSA (2048 bits).
6	El servicio de certificados digitales de firma centralizada debe permitir al suscriptor del modificar la contraseña de acceso a su certificado en múltiples oportunidades. En caso de requerirse interoperabilidad con las plataformas o sistemas de información en la que se utilizará la firma, la Entidad Certificadora suministra un API y las credenciales de consumo.

7	Debe permitir firmado PADES con validación a largo plazo.
8	La Entidad de Certificación Digital Abierta debe garantizar la prestación del servicio en su infraestructura.
9	Con derecho a una (1) reposición sobre el mismo dispositivo.
10	La Entidad de Certificación Digital debe suministrar un componente de software que garantice la integración con el sistema operativo Windows en las versiones 7, 8 y 10, y su almacén de certificados.
11	El componente software que garantiza la integración con el sistema operativo Windows debe tener habilitados el doble factor de autenticación, mediante el algoritmo TOTP. (Time-based Onetime Password).
12	El mecanismo de doble factor autenticación debe permitirse sobre dispositivos móviles (Android o IOS) para cumplir el principio de "algo que tengo" + "algo que se" y garantizar autenticación fuerte.
13	Garantizar que los certificados digitales a utilizar en el aplicativo SIIF Nación, son certificados de Función Pública con estándar X.509.V3, según las siguientes características: • Nombre • Correo electrónico • Ciudad • Entidad • Cédula de Ciudadanía • NIT de la entidad usuaria. • Área= SIIF NACIÓN.
14	Los certificados digitales deben ser 100% compatibles con el aplicativo SIIF (Sistema Integrado de información Financiera del Ministerio de Hacienda y Crédito Público).

CERTIFICADOS FIRMA ELECTRÓNICA PARA FACTURA ELECTRÓNICA

FORMATO: Firma Centralizada

VIGENCIA: 1 año

Ítem	Condiciones Técnicas Mínimas
1	Certificado Digital de Función Pública emitido por una entidad acreditada ante el Organismo Nacional de Acreditación (ONAC), de acuerdo con los Criterios Específicos de Acreditación CEA, para prestar el servicio de emisión de certificados digitales de función pública.
2	El Certificado Digital debe ser alojado en dispositivos criptográficos HSM (Hardware Security Module) que cumplan con el estándar FIPS 140-2 Level 3 o superior.
3	Algoritmo de firma SHA256 with RSA.
4	El servicio de certificados centralizados debe disponer de un punto de entrada vía servicio web seguro, utilizando el estándar TLS (Transport Layer Security).
5	El Certificado Digital debe Contar con una clave pública RSA (2048 bits).
6	El servicio de certificados digitales de firma centralizada debe permitir al suscriptor del modificar la contraseña de acceso a su certificado en múltiples oportunidades.

	En caso de requerirse interoperabilidad con las plataformas o sistemas de información en la que se utilizará la firma, la Entidad Certificadora suministra un API y las credenciales de consumo.
7	Debe permitir firmado PADES con validación a largo plazo.
8	La Entidad de Certificación Digital Abierta debe garantizar la prestación del servicio en su infraestructura.
9	Con derecho a una (1) reposición sobre el mismo dispositivo.
10	La Entidad de Certificación Digital debe suministrar un componente de software que garantice la integración con el sistema operativo Windows en las versiones 7, 8 y 10, y su almacén de certificados.
11	El componente software que garantiza la integración con el sistema operativo Windows debe tener habilitados el doble factor de autenticación, mediante el algoritmo TOTP. (Time-based Onetime Password).
12	El mecanismo de doble factor autenticación debe permitirse sobre dispositivos móviles (Android o IOS) para cumplir el principio de "algo que tengo" + "algo que se" y garantizar autenticación fuerte.
13	Garantizar que los certificados digitales a utilizar en el aplicativo SIIF Nación, son certificados de Función Pública con estándar X.509.V3, según las siguientes características: • Nombre • Correo electrónico • Ciudad • Entidad • Cédula de Ciudadanía • NIT de la entidad usuaria. • Área= SIIF NACIÓN.
14	Los certificados digitales deben ser 100% compatibles con el aplicativo SIIF (Sistema Integrado de información Financiera del Ministerio de Hacienda y Crédito Público).

CERTIFICADOS FUNCIÓN PÚBLICA COMPATIBLE ADOBE SIGN
FORMATO: FIRMA CENTRALIZADA
VIGENCIA: 1 año

Ítem	Condiciones Técnicas Mínimas
1	Certificado Digital de Función Pública emitido por una entidad acreditada ante el Organismo Nacional de Acreditación (ONAC), de acuerdo con los Criterios Específicos de Acreditación CEA, para prestar el servicio de emisión de certificados digitales de función pública.
2	El Certificado Digital debe ser alojado en dispositivos criptográficos HSM (Hardware Security Module) que cumplan con el estándar FIPS 140-2 Level 3 o superior.
3	Algoritmo de firma SHA256 with RSA.
4	El servicio de certificados centralizados debe disponer de un punto de entrada vía servicio web seguro, utilizando el estándar TLS (Transport Layer Security).
5	El Certificado Digital debe Contar con una clave pública RSA (2048 bits).

6	El servicio de certificados digitales de firma centralizada debe permitir al suscriptor del modificar la contraseña de acceso a su certificado en múltiples oportunidades.
7	En caso de requerirse interoperabilidad con las plataformas o sistemas de información en la que se utilizará la firma, la Entidad Certificadora suministra un API y las credenciales de consumo.
8	Debe permitir firmado PADES con validación a largo plazo.
9	La Entidad de Certificación Digital Abierta debe garantizar la prestación del servicio en su infraestructura.
10	Con derecho a una (1) reposición sobre el mismo dispositivo.
11	La Entidad de Certificación Digital debe suministrar un componente de software que garantice la integración con el sistema operativo Windows en las versiones 7, 8 y 10, y su almacén de certificados.
12	El componente software que garantiza la integración con el sistema operativo Windows debe tener habilitados el doble factor de autenticación, mediante el algoritmo TOTP. (Time-based Onetime Password).
13	El mecanismo de doble factor autenticación debe permitirse sobre dispositivos móviles (Android o IOS) para cumplir el principio de "algo que tengo" + "algo que se" y garantizar autenticación fuerte.
14	Emisión con estándar X.509.V3, según las siguientes características: • Nombre • Correo electrónico • Ciudad • Entidad • Cédula de Ciudadanía • NIT de la entidad usuaria.

Modificar el numeral 8 de la Invitación Pública así:

8. FORMA Y REQUISITOS DE PAGO DEL CONTRATO:

La DIRECCIÓN NACIONAL DE DERECHO DE AUTOR, cancelará el valor del contrato en un plazo de TREINTE (30) DÍAS calendario, contados a partir de del cumplimiento de los siguientes requisitos:

a) Una vez expedida la certificación de la disponibilidad de los 22 tokens en la cual además se indique que el proveedor garantiza la custodia y entrega bajo solicitud de estos por parte del supervisor del contrato, dentro del término de (01) un año a partir de la aprobación de la garantía, además de la entrega del primer token dentro de los (03) tres días siguientes a dicha aprobación.
b) Presentar la certificación de cumplimiento a satisfacción expedida por el supervisor del contrato.
c) Acreditar el correspondiente pago de los aportes parafiscales.
d) Presentar la respectiva factura electrónica de acuerdo con el Decreto 358 del 5 de marzo de 2020 expedido por el Ministerio de Hacienda y Crédito Público por el cual se reglamentan aspectos en materia tributaria y la Resolución No. 000042 del 5 de mayo de

2020 expedida por la Dirección de Impuestos y Aduanas Nacionales – DIAN y según indicación del supervisor del contrato.

Los pagos se efectuarán mediante transferencia a la cuenta bancaria informada por el proveedor que resulte seleccionado, previos los descuentos de ley.

Si la factura no ha sido correctamente elaborada o no se acompañan los documentos requeridos para el pago y/o se presentan de manera incorrecta, el término para este solo empezará a contarse desde la fecha en que se aporte el último documento y/o se presente en debida forma. Las demoras que se presenten por estos conceptos serán responsabilidad del contratista y no tendrán por ello derecho al pago de intereses o compensación de ninguna naturaleza.

En todo caso, el pago antes previsto se sujetará a los montos aprobados en el Programa Anual Mensualizado de Caja (PAC), de conformidad con lo dispuesto en los artículos 73 y 74 del Decreto 111 de 1996 y se realizarán los descuentos de Ley que deben corresponder al valor total del contrato, la propuesta presentada y los bienes y servicios suministrados.

NOTA: El pago se efectuará previa aprobación por parte del supervisor del contrato de los entregables o condiciones definidas en cada uno de ellos, diez (10) días hábiles después de presentada la factura con el lleno de los requisitos. Para efectos del pago, el CONTRATISTA deberá adjuntar factura y Certificación de los pagos de aportes al Sistema de Seguridad Social Integral en salud, pensiones, ARL y de aportes parafiscales a que haya lugar, o de la certificación respectiva expedida por el contador o Revisor Fiscal.

Modificar el numeral 10 de la Invitación Pública así:

10. OBLIGACIONES DE LAS PARTES:

OBLIGACIONES ESPECÍFICAS DEL CONTRATISTA:

1. Entregar certificados de firma digital con Token criptográfico bajo solicitud de la entidad durante el transcurso del contrato y estos con vigencia de un (1) año contado a partir de la entrega del token, de acuerdo con las condiciones especificaciones técnicas y garantizar la custodia y entrega bajo solicitud de estos por parte del supervisor del contrato y dentro del término de (01) un año a partir de la aprobación de la garantía.
2. Entregar el procedimiento para la ejecución del software para cambios de claves (o Personal Identification Number – PIN), y para la generación de llaves del certificado de firma digital.
3. Hacer entrega del protocolo de soporte durante un (1) año que le permita al Instituto la solicitud de soporte sin límite de casos.
4. Garantizar la calidad de los bienes objeto del presente contrato de acuerdo con las condiciones generales.
5. Todas las demás actividades inherentes a la ejecución del objeto.

Las demás condiciones establecidas en la Invitación Pública se mantienen.

NOTA: CON LA PRESENTE ADENDA SE PUBLICA ADJUNTO CON LOS FORMATOS SOLICITADOS EN LA INVITACIÓN PÚBLICA.

Bogotá D.C., cinco (05) días del mes de marzo de 2026.