ADENDA No. 001
PROCESO DE SELECCIÓN MÍNIMA CUANTÍA No. IPMC-CNE-003-2026

OBJETO DEL PROCESO: *"*Adquirir certificados digitales para interactuar con plataformas tecnológicas para el Consejo Nacional Electoral."

CONSIDERANDO

Que el CONSEJO NACIONAL ELECTORAL a través del Grupo Interno de trabajo de Gestión Financiera estructuró los estudios y demás documentos previos requeridos para el inicio del proceso de **MÍNIMA CUANTÍA** el cual tiene por objeto: "*"*Adquirir certificados digitales para interactuar con plataformas tecnológicas para el Consejo Nacional Electoral."

Que, el **Consejo Nacional Electoral** con el fin de dar cumplimiento a lo establecido en el artículo 2.2.1.1.1.7.1 del Decreto 1082 de 2015, procedió a la publicación de los documentos precontractuales en desarrollo del proceso de selección en el Sistema Electrónico para la Contratación Pública –SECOP II, a través del Portal Único de Contratación cuyo sito web es: https://www.colombiacompra.gov.co/secop-ii a partir del **23 de abril de 2026**, de conformidad con el cronograma del proceso.

Que, el CNE otorgó hasta el 24 de abril de 2026 para presentar observaciones y fijando el 27 de abril de 2026 a las 07:00 PM como fecha límite para dar respuesta a las mismas y expedir adendas.

Que, atendiendo las observaciones formuladas por Gestión de Seguridad Electrónica S.A. y CAMERFIRMA a la Invitación Pública en la plataforma SECOP II, se hace necesario modificar lo descrito en el presente documento.

Que, en aras de garantizar los principios de publicidad, transparencia y libre concurrencia, y en consideración del interés general, la Entidad se encuentra legalmente habilitada para modificar los pliegos de condiciones a través de adendas expedidas antes del vencimiento del plazo de presentación de ofertas, de conformidad con lo dispuesto en el artículo 2.2.1.1.2.2.1 del Decreto 1082 de 2015.

DECISIÓN

PRIMERO: Modificar el numeral 6.1.2., de la Invitación Pública el cual quedará de la siguiente manera:

6.1.2. Certificados Digitales de Función Pública expedidos por Entidades de Certificación Abierta homologadas por la Administración del 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.
3. Los certificados de función pública a utilizar en el SIIF Nación que estén almacenados en Token Criptográficos, 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) 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.
9. Cualquier cambio de alguno de estos datos debe ser informado previamente por la

entidad de certificación abierta a la administración SIIF Nación.

10. Una vez la Administración SIIF Nación informe que dichos cambios fueron aplicados, podrán ser utilizados en el aplicativo SIIF Nación.
11. 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.
12. 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.
13. 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:
14. Soporte Nivel 1 de “Mesa de ayuda”: Este es el nivel de soporte inicial, responsable de atender y solucionar los requerimientos y las incidencias básicas del usuario. Esto incluye resolución de problemas de usuario, contraseña, funcionamiento, asistencia mediante la navegación de menús y aplicación de guías y procedimientos, según corresponda. La mesa con una disponibilidad 7 x 24 x 365 días.
15. Soporte Nivel 2 “Ingeniero Especialista”: Son los encargados de realizar soporte con base al nivel de conocimiento especializado. Las funciones del nivel 2 son: Atender los casos escalados por el nivel 1. Documentar los casos y las soluciones proporcionadas. Verificar que el caso escalado corresponda a una falla en la funcionalidad del certificado y dar una solución definitiva a la falla reportada.
16. 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 supervisor del contrato 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.
17. 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.
18. La entidad de certificación abierta debe contar con al menos una de las garantías a que hace referencia el artículo 9 del Decreto 333 de 2014 la vigencia de la misma y que cumple con los requisitos señalados en la norma. Adicionalmente, adjuntar copia de la garantía.
19. El proponente deberá prestar el servicio de técnico a los usuarios de los certificados digitales durante la vigencia del token.
20. La vigencia de los certificados debe ser de dos (2) años a partir de la fecha de su activación.
21. Los certificados digitales emitidos deben estar completamente ajustados a la Ley 527 de 1999, el Decreto 1747 de 2000 y demás disposiciones legales inherentes a entidades de certificación digital.
22. Los cupos de certificados digitales podrán ser solicitados por el Consejo Nacional Electoral hasta dieciocho (18) meses después contados a partir de la fecha de

terminación del contrato.

SEGUNDO: Modificar el numeral 6.1.4., de la Invitación Pública el cual quedará de la siguiente manera:

6.1.4. Certificados digitales en formato de firma digital con Token (dispositivo criptográfico), para los funcionarios del CNE.

1. Entregar los certificados digitales entre un (1) día hábil hasta tres (3) días hábiles, siguientes a la solicitud, los cuales deben estar en buen estado de acuerdo con las especificaciones técnicas requeridas.
2. Proporcionar vía correo electrónico o a través de la página web de la entidad certificadora, las instrucciones o tutoriales para instalación de los certificados digitales incluyendo la llave privada.
3. Los certificados digitales deben tener una vigencia de dos (2) años a partir de la fecha de emisión
4. Los cupos de certificados digitales podrán ser solicitados por el Consejo Nacional Electoral hasta dieciocho (18) meses después contados a partir de la fecha de terminación del contrato.
5. El contratista debe enviar la certificación en idioma español donde se indique todas las características de los certificados digitales en el presente proceso.
6. Otorgar mínimo una (1) revocación o reposición por cada uno de los certificados digitales emitidos, sin costo adicional para la Entidad. Cada una de las revocaciones tendrá una vigencia correspondiente a la que le reste al certificado anteriormente emitido.

TERCERO: Modificar el numeral 6.1.5., de la Invitación Pública el cual quedará de la siguiente manera:

6.1.4. Condiciones de los certificados digitales

Ítem	Concepto	Descripción de lo ofrecido (*)
1.	Validez del certificado	La validez de los certificados corresponderá a 24 meses a partir de su activación.
2.	Formato del Token	Token – Virtuales
3.	Cantidad Requerida de certificados digitales en formato Token Virtual	Se requiere proveer 50 certificados en formato Token Virtual.

4.	Acreditación de certificados digitales	Los certificados emitidos deben estar completamente ajustados: A la Ley 527 de 1999 y los estándares técnicos internacionales. Los certificados de firma digital deberán ser generados o expedidos a través de una entidad certificada ante el Organismo Nacional de Acreditación de Colombia (ONAC) Los servicios de Certificación Digital deben estar soportados en la tecnología PKI (son las siglas de Public Key Infrastructure (infraestructura de clave pública), o lo que es lo mismo, todo lo necesario, tanto de hardware como de software, para las comunicaciones seguras mediante el uso de certificadas digitales y firmas digitales.
5.	Tipo de plataforma	Web y/o escritorio para poder generar las firmas digitales
6.	Emisión de Certificados de Firma Digital Seguros y Multiplataforma	Se solicita la emisión de los certificados de firma digital que permitan la autenticación y firma electrónica avanzada de documentos desde equipos de cómputo y dispositivos móviles. El certificado deberá cumplir con los estándares vigentes de seguridad y criptografía, garantizando la integridad, autenticidad y no repudio de la información firmada, así como compatibilidad con sistemas operativos Windows, macOS, Android e iOS. Asimismo, deberá ser emitido por una entidad certificadora acreditada y permitir su utilización en plataformas institucionales y aplicaciones de gestión documental.
7.	Características de los servicios	**Integridad:** En cualquier momento posterior a la firma se podrá demostrar que el documento es el original que se firmó o fue alterado o modificado. **Autenticidad:** Al firmarse directamente por una persona que porta un certificado digital, se puede determinar que el documento es auténtico. **No Repudio:** El firmante del documento no puede repudiar la firma del documento, debido a que es el único custodio del certificado digital o es el único que tiene acceso a él.
8.	Reemisión sin costo durante la vigencia del certificado	El servicio de reemisión ilimitada del certificado Digitales de Función Pública, durante vigencia del mismo, en caso de presentarse los siguientes escenarios: Cambio del funcionario (Por no tener vínculo laboral con el CNE y/o por estar en periodo de vacaciones y/o renuncia al cargo y/o inhabilidad y/o cambio de funciones) y/o cualquier otra circunstancia presentada, la cual será previamente comunicada

		por el supervisor del contrato.
9.	Soporte General	El proponente deberá brindar el soporte necesario en caso de presentarse incidencias en el uso de los certificados de firma digital en formato de Token virtual, o en caso de presentarse caídas del sistema o plataforma dispuesta por el proveedor.
10.	Soporte Técnico	El soporte Técnico debe incluir. Instalación del certificado Digital. Configuración del certificado Digital
11.	Tiempo de emisión del certificado	Mínimo un (1) día hábil, máximo tres (3) días hábiles.
12.	Sensibilización	El proponente deberá incluir dentro del servicio dos (2) sensibilizaciones para Veinticinco (25) personas cada una, de mínimo tres (3) horas, las cuales se podrán hacer de manera virtual en donde se sensibilicen a los diferentes usuarios en las funcionalidades y métodos para utilización de los certificados de firma digital.

CUARTO: Modificar el numeral 8.1.2., de la Invitación Pública el cual quedará de la siguiente manera:

8.1.2 OBLIGACIONES ESPECIFICAS

En la ejecución del contrato, el contratista debe cumplir con las siguientes obligaciones:

1. Entregar cuarenta y nueve (49) certificados digitales de función pública para ingresar al SIIF y un (1) certificado de firma digital de persona jurídica para facturación electrónica de conformidad con las especificaciones técnicas descritas en el presente estudio previo, que cumplan con su correcta operatividad para el cumplimiento del objeto y acorde con la necesidad a satisfacer.
2. Implementar y mantener los sistemas de seguridad que resulten razonables en función del servicio prestado y en general la infraestructura necesaria para la prestación del servicio de certificación digital.
3. Dar cumplimiento a lo previsto en la Declaración de Prácticas de certificación digital de la entidad de certificación digital que se encuentre publicada en su página web, reconocido jurídicamente por el Decreto 333 de 2014.
4. Garantizar la trazabilidad de la utilización de todos y cada uno de los certificados digitales centralizados, en la plataforma establecida.

5. Ofrecer el derecho a una (1) reposición sobre el mismo dispositivo, por el tiempo restante de vigencia de los certificados digitales centralizados, en los casos que se presenten de cambio de titularidad, bloqueo u olvido de contraseña, sin costo adicional, con el mismo soporte y cumplimiento de lo requerido para el normal funcionamiento en SIIF Nación.
6. Advertir, sobre las medidas de seguridad que deben observar los suscriptores de firmas y certificados digitales para la utilización de estos mecanismos.
7. Los certificados de firma digital deben tener vigencia de dos (02) años, a partir de su activación. Durante este período de vigencia, el contratista deberá prestar todos los servicios conexos al objeto descrito en el presente documento.
8. Acreditar el cabal cumplimiento de las obligaciones relativas al Sistema de Seguridad Social Integral atendiendo lo establecido en el artículo 23 de la Ley 1150 de 2007.
9. La entidad de certificación digital 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.
10. La entidad de certificación digital 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.
11. La entidad de certificación digital deberá disponer de la infraestructura de operación, servicio y soporte a sus usuarios, durante 7 x 24 x 365 días.
12. La entidad de certificación digital deberá notificar al usuario y al coordinador SIIF de la entidad por lo menos con un mes de anticipación a 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 la Entidad.
13. La entidad de certificación digital deberá presentar la Acreditación de Servicios emitida por el Organismo Nacional de Acreditación de Colombia – ONAC, que le permite prestar los servicios de emisión de certificados digitales de función pública y emisión de certificados digitales en formato centralizado y/o virtual.
14. Dar a conocer y capacitar al coordinador SIIF Nación o a quienes se designe, sobre los procedimientos de instalación y funcionamiento de los certificados digitales.
15. La entidad de certificación digital deberá disponer de una línea telefónica de contacto donde tenga un agente disponible, para resolver casos de soporte que involucren las dos partes, durante 7 x 24 x 365 días.
16. La entidad de certificación digital deberá presentar como requisito de suscripción del acta de inicio alguna de las garantías establecidas en el Artículo 9 del Decreto 333 de 2014, con el cual se reglamenta el artículo 160 del Decreto-Ley 19 de 2012.
17. La entidad de certificación digital deberá prestar el servicio de dos (2) sensibilizaciones para Veinticinco (25) personas cada una, de mínimo tres (3) horas, las cuales se podrán hacer de manera virtual en donde se sensibilicen a los diferentes usuarios en las funcionalidades y métodos para utilización de los certificados de firma digital.
18. Las demás que sean necesarias para el debido cumplimiento del objeto de la Contratación.

QUINTO: Las demás condiciones de los documentos de la Invitación Pública IPMC-CNE-003-2026, no son modificados o suprimidos mediante la presente adenda continúan vigentes y su exigibilidad permanece para las personas interesadas en participar del proceso de selección.

La presente adenda podrá ser consultada en la página web: https://community.secop.gov.co

Dada en Bogotá a los veintisiete (27) días del mes de abril de 2026.

FIN DE LA ADENDA No. 001

CRISTINA RICARDO QUIROZ ROMERO
Presidente
Consejo Nacional Electoral

POR PRESIDENCIA
Revisó: Mayra Alexandra Montoya Villamizar – Abogada contratista

POR DIRECCION DE GESION CORPORATIVA

Proyectó: Jhon Fredy Páez González – DGC.
Revisó: Jonatan Andres Avendaño Giraldo.

Aprobó: Martha Margarita Salazar Alonso- Directora de Gestión Corporativa