

ANEXO No. 1
CONDICIONES TÉCNICAS

Bogotá,

Señores:

AGENCIA NACIONAL DIGITAL

Ciudad

REF: Proceso de Selección de Mínima Cuantía No. **IP-AND-001-2022**

[Nombre del representante legal], identificado como aparece al pie de mi firma, *[obrando en mi calidad de representante legal de]* *[nombre del Proponente]*, manifiesto que, me comprometo a cumplir con las especificaciones que se señalan a continuación:

A continuación, se describen las condiciones técnicas del servicio que será entregado por el Proponente y/o Proveedor, de acuerdo con la normatividad vigente así:

A continuación, se describen las condiciones técnicas del servicio que será entregado por el Proponente y/o Proveedor, de acuerdo con la normatividad vigente así:

a. Autenticación de identidad.

La firma digital puede utilizarse para identificar a una persona física o jurídica como quien dices ser en el ámbito de su actividad.

b. Certificado Digital.

Los Certificados digitales ofrecen los medios de respaldo para garantizar la autenticidad del origen, la integridad de los datos firmados y el no repudio.

- **Autenticidad del origen:** En una comunicación electrónica el suscriptor puede acreditar válidamente su identidad y su condición ante otra persona demostrando la posesión de la clave privada asociada con la respectiva clave pública contenida en el certificado.

- **Integridad del documento:** La utilización del certificado garantiza que el documento es íntegro, es decir, existe la garantía de que el documento no fue alterado o modificado después de firmado por el suscriptor. Además certifica que el mensaje recibido por el usuario es el mismo emitido por el suscriptor.

- **No repudio:** Evita que el emisor del documento firmado pueda negar en un determinado momento la autoría o la integridad del documento, puesto que la firma a

través del certificado digital puede demostrar la identidad del emisor sin que este pueda repudiarlo.

c. Cifrado de información.

Es el proceso de transformar la información para hacerla incomprensible para todos excepto para el receptor a quien va dirigida.

d. La entidad de certificación abierta debe estar autorizada por el organismo Nacional de acreditación de Colombia ONAC, para expedir certificados digitales de Función Pública.

e. Los certificados de función pública a utilizar en la AND deben estar almacenados en Token Criptográficos, los cuales debe cumplir con los estándares tecnológicos y de seguridad exigidos por el ONAC.

f. La Entidad de certificación abierta debe proveer a sus suscriptores los controladores o drivers para el Token criptográfico en los sistemas operativos utilizados por la entidad usuaria y el soporte para su instalación.

g. Los certificados de firma digital a utilizar por la entidad para sus usuarios son certificados de Función Pública los cuales deben cumplir como mínimo con los estándares definidos por el ONAC y por ende con los requisitos exigidos en el artículo 35 de la Ley 527 de 1999.

h. Los certificados digitales de función pública se deben poder utilizar para:

i. Firmar digitalmente archivos para ser utilizados en cargas masivas en aplicativo. La entidad de certificación debe proveer el soporte para el uso de los certificados digitales para la firma de archivos o documentos electrónicos.

j. La entidad de certificación abierta debe garantizar, la actualización de la CRL, siendo su responsabilidad que sea oportuna y que esté disponible para consulta durante 7x24x365 días.

k. La entidad de certificación abierta deberá notificar por lo menos con un mes de anticipación la fecha de vencimiento del certificado digital, así mismo ofrecer a la CGR 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.

l. La entidad certificadora abierta deberá disponer de un contacto directo de soporte para la entidad para resolver casos de soporte de involucren las dos partes.

m. La entidad certificadora abierta y la entidad usuaria acordarán lo referente a las garantías que hace referencia el artículo 9 del Decreto 333 de 2014.

n. Entregar el Certificado de Firma Digital Función Pública a la Corporación Agencia Nacional de Gobierno Digital de forma personal a través de un operador logístico dentro y fuera de Bogotá D.C.

o. Suministrar el dispositivo criptográfico con el Certificados de Firma Digital Función Pública para la Corporación Agencia Nacional de Gobierno Digital, con una vigencia de un (01) año, contados a partir de la fecha de emisión de cada firma digital almacenada en dispositivo criptográfico.

p. El PIN de protección del certificado digital es único, de uso personal e intransferible, el conocimiento del mismo está solo en el suscriptor o usuario final.

En constancia de lo anterior, y como manifestación de la aceptación de los compromisos incorporados en el presente documento, se firma el mismo en la ciudad de _____, a los _____ (fecha en letras y números).

Firma

C.C.

SUSCRIBIRÁN EL DOCUMENTO TODOS LOS INTEGRANTES DEL PROPONENTE SI ES PLURAL, A TRAVÉS DE LOS REPRESENTANTES LEGALES ACREDITADOS DENTRO DE LOS DOCUMENTOS DE EXISTENCIA Y REPRESENTACIÓN LEGAL Y/O PODERES CONFERIDOS Y ALLEGADOS AL PRESENTE PROCESO.