Anexo técnico 1 Ficha de Requerimientos Técnicos Mínimos

Ítem	Descripción
1	**Correo Electrónico Certificado** **Cantidad:** 10.000
1.1	Prestar servicio de correo electrónico certificado con estampa cronológica de tiempo con la hora legal colombiana del Instituto Nacional de Metrología.
1.2	Proveer el registro del envío y de la recepción del mensaje de datos por cada destinatario, en el cual se pueda identificar: (i) la fecha y hora de envío del correo electrónico certificado, (ii) la fecha y hora de entrega del mensaje al destinatario, y (iii) la fecha y hora de apertura del mensaje, siempre que el destinatario realice dicha acción. Nota: De no ser posible la entrega, informar la razón por la cual no llegó el mensaje al destinatario, generando alerta en casos como: el dominio de la cuenta no existe, la cuenta de correo está llena, la cuenta de correo no existe, la cuenta esta inactiva, problema en la entrega al servidor de destino.
1.3	Poner a disposición de la entidad copias de respaldo (backup) de la información asociada, con periodicidad mensual, en formato descargable (por ejemplo, Excel o CSV), con información por envío de entrega y apertura de los mensajes de datos.
1.4	Garantizar envío cuando trate de uno o varios destinatarios en un mismo mensaje de datos.
1.5	Tamaño máximo de envío: 20 MB.
1.6	Garantizar la capacidad técnica para el funcionamiento del servicio, en términos de volumen, velocidad y capacidad de correos electrónicos enviados simultáneamente a diferentes destinatarios.
1.7	Vigencia: 1 año.
1.8	Contar con la infraestructura tecnológica y de seguridad necesaria para la utilización adecuada de los correos electrónicos certificados.
2	**Certificados de firmas digitales de función pública** Cantidad: 80 certificados, distribuidos de la siguiente manera: • **18 certificados de firma digital con connotación de función pública**, para uso en el Sistema Integrado de Información Financiera – SIIF Nación, respecto de los cuales el proveedor deberá estar homologado como operador por la Administración de SIIF Nación del Ministerio de Hacienda y Crédito Público, así: 17 certificados de persona natural de función pública. 1 certificado de persona jurídica para facturación electrónica con autenticación previa y generación de documento soporte para no obligados a facturar para la realización de transacciones en el SIIF Nación • **62 certificados de firma digital de persona natural con connotación de función pública**, para funcionarios públicos y contratistas, destinados a la firma de

	mensajes de datos y/o documentos en el ejercicio de sus funciones u obligaciones contractuales.
2.1	**17 certificados digitales de Función Pública para persona natural en SIIF Nación – vigencia: 1 año a partir de su activación.**
2.1.1	Los certificados deberán cumplir con las condiciones técnicas requeridas para su uso en SIIF Nación, pudiendo ser suministrados mediante token criptográfico o a través de infraestructura segura tipo HSM provisto por la entidad de certificación digital, garantizando en ambos casos el cumplimiento de los estándares de seguridad, autenticación y compatibilidad exigidos por dicho sistema.
2.1.2	Compatibilidad con el Sistema Integrado de Información Financiera – SIIF Nación y permitir: a) Autenticación mediante los mecanismos definidos por SIIF Nación, incluyendo el uso de infraestructura de acceso seguro (VPN), garantizando la validación del certificado y la autorización por parte del sistema. b) Firma digital de transacciones dentro del aplicativo. c) Firma digital de archivos para procesos de carga masiva en SIIF Nación. d) Uso en la firma de documentos electrónicos, para lo cual el proveedor deberá garantizar el soporte técnico requerido.
2.1.3	Garantizar los mecanismos de validación del estado del certificado, incluyendo: • Publicación de Listas de Certificados Revocados (CRL). • Disponibilidad del servicio de validación en línea (OCSP), incluyendo la provisión de la URL correspondiente.
2.1.4	Cualquier modificación en estos servicios deberá ser informada oportunamente y cumplir con los lineamientos definidos para su uso en SIIF Nación
2.1.5	La disponibilidad de los servicios CRL y OCSP deberá ser continua (7x24x365), garantizando su actualización y consulta oportuna.
2.1.6	Garantizar la disponibilidad de soporte técnico bajo los siguientes niveles: **Nivel 1 – Mesa de ayuda:** Atención de requerimientos básicos (acceso, autenticación, uso del certificado), con disponibilidad siete 7 días a la semana, durante veinticuatro 24 horas al día los 365 días al año. **Nivel 2 – Soporte especializado:** Atención de incidentes escalados, análisis técnico y solución definitiva de fallas relacionadas con los certificados digitales.
2.1.7	Garantizar: • Notificar con al menos un (1) mes de anticipación la fecha de vencimiento de los certificados. • Disponer de herramientas de gestión que permitan consultar información como fechas de emisión, vencimiento y estado de los certificados. • Brindar orientación a los usuarios sobre el ciclo de vida del certificado digital. • Contar con un canal de contacto para la articulación con el soporte de SIIF Nación en caso de incidentes
2.1.8	Garantizar la reposición sin costo en los siguientes casos:

	• Cambio de titular. • Bloqueo de clave, siempre que la solicitud se realice dentro de los seis (6) meses siguientes a su emisión. • Modificación de atributos del certificado debidamente reportados. Nota: La reposición se realizará por el tiempo restante del certificado original.
2.2	**1 certificado Digital de Función Pública para persona jurídica en SIIF Nación – vigencia: 1 año a partir de su activación**
2.2.1	El certificado podrá ser suministrado mediante token criptográfico o a través de infraestructura segura tipo HSM, garantizando en todo caso el cumplimiento de los requisitos técnicos exigidos por SIIF Nación.
2.2.2	El certificado deberá cumplir con el estándar X.509 versión 3.
2.2.3	Deberá contar con un par de claves criptográficas con longitud mínima de 2048 bits, utilizando algoritmos de firma seguros basados en SHA-2 (por ejemplo, SHA-256 con RSA).
2.2.4	En caso de que el certificado sea suministrado mediante token criptográfico, deberá garantizar: • La provisión de los controladores (drivers) necesarios para su funcionamiento en los sistemas operativos de la entidad. • El soporte técnico para su instalación y uso.
2.2.5	Garantizar el soporte técnico durante toda la vigencia del certificado, incluyendo asistencia a los usuarios para su correcta utilización
2.2.6	Garantizar la reposición sin costo en los siguientes casos: • Cambio de titular. • Bloqueo de clave, siempre que la solicitud se realice dentro de los seis (6) meses siguientes a su emisión. • Modificación de atributos del certificado debidamente reportados. Nota: La reposición se realizará por el tiempo restante del certificado original.
2.3	**62 certificados digitales de Función Pública para persona natural – vigencia: 1 año a partir de su activación**
2.3.1	Los certificados deben ser emitidos y almacenados en infraestructura segura tipo HSM (Hardware Security Module), cumpliendo con el estándar FIPS 140-2 nivel 3 o superior, con longitud de clave RSA de 2048 bits o superior, y en concordancia con los criterios técnicos vigentes establecidos por el documento de Criterios Específicos de Acreditación (CEA) expedido por el Organismo Nacional de Acreditación de Colombia.
2.3.2	Los certificados deberán permitir ser utilizados en diferentes dispositivos (computador de escritorio, portátil, tablet o teléfono móvil), garantizando su acceso mediante mecanismos de autenticación segura.
2.3.3	Suministrar los componentes de software necesarios para la configuración y uso de los certificados digitales en sistemas operativos Windows 10 o superiores y macOS, incluyendo las herramientas de acceso, autenticaciones requeridas para su operación
2.3.4	Garantizar que el servicio es compatible con el estándar de seguridad PKCS (Public Key Cryptography Standards) vigente y apropiado para la emisión y administración de los certificados de seguridad.
2.3.5	Garantizar la reposición sin costo en los siguientes casos:

	• Cambio de titular. • Bloqueo de clave, siempre que la solicitud se realice dentro de los seis (6) meses siguientes a su emisión. • Modificación de atributos del certificado debidamente reportados. Nota: La reposición se realizará por el tiempo restante del certificado original.
2.3.6	Brindar solución a los incidentes reportados, de acuerdo con la prioridad de los incidentes que se puedan presentar y resolver en los tiempos indicados a continuación - **Prioridad 1**: Perdida total del servicio Efectividad de resolución: 4 horas hábiles - **Prioridad 2:** Perdida parcial del servicio Efectividad de resolución: 8 horas hábiles

Características generales para ambos servicios:

- La entidad de certificación digital abierta deberá estar acreditada por el Organismo Nacional de Acreditación de Colombia – ONAC para la expedición de certificados digitales, conforme a la normatividad vigente
- Acompañamiento técnico y funcional en la implementación de correo electrónico certificado y firmas digitales hasta su operación.
- Disponer de mesa de servicio y/o canales atención necesarios para atender incidentes y requerimientos durante la operatividad del servicio.
- Entregar documento técnico o manual equivalente para el consumo de los servicios en la entidad.
- Garantizar la custodia del servicio de correo electrónico certificado y certificados de firmas digitales (servicio cupo custodia), que se adquieran en la presente vigencia pero que no se utilicen dentro de esta inclusive.