

ANEXO TÉCNICO

Objeto: Adquirir certificados digitales (token) para el Ministerio de las Culturas, las Artes y los Saberes.

Elementos a contratar:

Ítem	Descripción	cantidad	Vigencia
1	Certificado Digital (Token físico y/o virtual) para personas naturales -Función Pública – SIIF Nación	50	1 año
2	Certificado Digital personas jurídica	1	1 año

REQUERIMIENTOS:

- Certificado digital en formato token físico tipo USB.
- Acceder al certificado a través de las claves de acceso: como PIN.
- Firmas ilimitadas en plataformas y documentos.
- Compatibilidad con sistemas operativos Windows 7, 8, 10 o superior, en arquitecturas de 32 y 64 bits.y Mac iOS.
- Desbloqueo del dispositivo TOKEN FISICO a través del Código PUCK .
- Esta almacenada en un Token (FIPS 140-2).
- Llave privada de 2048bits.
- Algoritmo de firma de certificado con hash SHA256.
- Canal de comunicación cifrado con protocolo HTTPS y TLS 1.2 y certificado de validación extendida.
- Cifrado realizado mediante dispositivos criptográficos que cumplen el estándar FIPS 140 2 Nivel 3.
- Compatibilidad con APIs: Microsoft PC/SC con drivers asociados.
- Interfaz de host: Plug and Play – USB 2.0 de alta velocidad.
- Indicador visual led
- Interfaz humana: LED de un solo color.
- Diseño robusto, a prueba de manipulaciones, con ensamble único de tarjeta SIM.
- Operación ambiental: entre 0°C y 70°C (32°F a 158°F), resistente al agua.
- Vigencia mínima de 1 año para el token físico y/o virtual.
- Se debe garantizar la autenticación OTP (One-Time Password) es un código

"Se consideran copias controladas los documentos que se encuentran vigentes en ISOLUCIÓN".

Ministerio de las Culturas, las Artes y los Saberes

Dirección: Calle 9 No.8 - 31, Bogotá D.C., Colombia

Conmutador: (+57) 601 342 4100

Línea Gratuita: (+57) 01 8000 938081

www.mincultura.gov.co

Sede Correspondencia

Palacio Echeverry Calle 9 # 8 - 31

Ext. 4073 – 4074 - 4076

servicioalciudadano@mincultura.gov.co

de uso único que se utiliza para reforzar la seguridad de una contraseña o método de acceso. Este tipo de código proporciona un nivel adicional de seguridad al requerir un código único para validar acciones específicas, como iniciar sesión en una cuenta o autorizar una transacción financiera.

- Realizar firmas masivas mediante KSI y cargues con archivos planos.
- Compatibilidad con el estándar PKCS (Public Key Cryptography Standards) vigente.
- Funcionamiento garantizado en sistemas operativos Windows 10 y superiores, para certificados digitales personas jurídicas.
- Garantizar la compatibilidad con los sistemas de gestión documental, con el fin de garantizar la firma masiva de documentos.
- Operación Ambiental: 0°C ~ 70°C (32°F ~ 158°F) - A prueba de agua.
- Diseño robusto a prueba de manipulación, Ensamble único de tarjeta SIM.
- Operación Ambiental: 0°C ~ 70°C (32°F ~ 158°F) - A prueba de agua.
- Interfaz de Host: Plug and Play - USB 2.0 de alta velocidad.
- Los certificados digitales deben ser compatibles con el Gestor Documental AZ Digital, toda vez que a través de esta plataforma se realiza la firma masiva de documentos tales como Certificados de Disponibilidad Presupuestal (CDP), Registros Presupuestales (RP) y Obligaciones.

Como referencia del alcance de las actuaciones administrativas que se adelantan a través del Certificado Digital (Token físico y/o virtual) para personas naturales - Función Pública – SIIF Nación, se establece una relación de documentos emitidos en la vigencia 2025 en SIIF nación con procesos de firma en gestor documental AZ DIGITAL:

OPERACIONES REALIZADA EN SIIF NACIÓN CON TOKEN FUNCIÓN PÚBLICA VIGENCIA 2025

MES	CDP	COMP	COMP RES	OB	OB RES	OP	OP RES	TOTAL
1	1.033	767	2.388	305	1.582	279	1.086	7.440
2	201	1.409		1.043	555	694	518	4.420
3	1.054	594		1.461	205	1.150	615	5.079
4	211	2.464		1.197	114	1.676	100	5.762
5	134	1.031		2.285	67	2.242	81	5.840
6	36	1.637		3.242	57	3.271	47	8.290
7	97	753		2.321	92	2.270	63	5.596
8	49	914		2.488	42	2.419	59	5.971
9	58	903		2.350	66	2.253	44	5.674
10	40	915		2.218	39	2.143	51	5.406
11	29	1.741		2.207	28	2.134	38	6.177
12	16	3.580		3.934	32	3.889	35	11.486
Total general	2.958	16.708	2.388	25.051	2.879	24.420	2.737	77.141

*Información extraída de listados de operaciones en SIIF Nación vigencia 2025.

"Se consideran copias controladas los documentos que se encuentran vigentes en ISOLUCIÓN".

Ministerio de las Culturas, las Artes y los Saberes

Dirección: Calle 9 No.8 - 31, Bogotá D.C., Colombia

Conmutador: (+57) 601 342 4100

Línea Gratuita: (+57) 01 8000 938081

www.mincultura.gov.co

Sede Correspondencia

Palacio Echeverry Calle 9 # 8 - 31

Ext. 4073 – 4074 - 4076

servicioalcidudano@mincultura.gov.co

Características para la interoperabilidad con los sistemas de información de gestión documental:

API:

Debe permitir el llamado e integración en aplicativo de .NET, Java, PHP Python con las siguientes características técnicas.

- Componente de Firma, con las funcionalidades necesarias para firmar digitalmente un documento en formato PADES XADES y CADES, el mismo se ejecuta en dos capas capa de servicios Web y Capa cliente.
- No applets y Jnlp para no generar huecos de seguridad ni dependencia en actualizaciones del browser que generen impactos en la operación.
- El firmado se debe realizar siempre en línea desde los portales web de la entidad, no debe admitir el cargue de documentos. Debe ser integrado en la interfaz de los sistemas sin que el usuario identifique que está en otro sistema.
- El componente siempre será desplegado con capa de servicios REST lo cual permite solo enviar el HASH y retornar el HASH de Firma en la capa Backend.
- Capacidad de firma digital concurrentes hasta 200 transacciones (depende de las características del servidor a ser desplegado)
- Despliegue de servicios en sistemas operativos Windows y Linux mediante Apache e IIS dependiendo del caso.
- El componente debe soportar los siguientes exploradores WEB Vigentes:

Google Chrome	84.0.4147.94 +
Mozilla Firefox	79.0 +
Edge	Edge
Safari	14. 0 +

- Ejecución en sistemas operativos: Windows 10/8.1/8/7 de 64 bits y 32 Bits, Mac OS Catalina 10.15.6, Mojave 10.14.6
- Ejecución en Token criptográfico o Remoto con el certificado de firma y su clave privada, mediante el almacén de certificados del sistema operativo.
- La aplicación cliente se encargará de generar el documento en PDF en línea e integrarse por servicio web para tener la capacidad de enviar a firmar digitalmente el documento al componente y recibir el documento firmado, generando el ID de transacción, el componente debe tener la capacidad de recibir el documento levantar la invocación del almacén de certificados del sistema operativo del cliente y realizar la firma digital y dejarlo a uso de la aplicación para que pueda ser tomado en base de datos o File System.
- Para firmar los documentos, el Componente de Firma listará los certificados almacenados en los siguientes repositorios:

"Se consideran copias controladas los documentos que se encuentran vigentes en ISOLUCIÓN".



Culturas

- Lectura de Tokens USB conectadas y con drivers instalados (Firma tipo PKCS) emitidos por las entidades de certificación digital acreditadas por el ONAC que deberán estar soportados en los dispositivos token y/o token virtual, que deberá ser accedido por el almacén de certificados de los sistemas operativos, no se permite acceder a los certificados digitales en la nube o remotos por medio de servicios web o API.
- Verificar la validez de este certificado digital al momento de la firma.
- Tomar los bytes de un documento y firmarlos digitalmente a partir del uso de un certificado digital.
- Relacionar a la firma digital un grafo de la firma del firmante mediante la incorporación de la imagen cargándola en formato jpg.
- Permite varias firmas digitales de diferentes usuarios siempre manteniendo la integridad del documento.
- El componente es capaz de recibir el documento en base64 para realizar la firma, la lógica de estado en pendientes de firma y firmado son estados que se deben manejar desde las aplicaciones. El componente realiza la firma del documento en base64 y retorna el mismo documento firmado digitalmente en base 64 para que sea alojado en la aplicación, los flujos de secuencias de firma también deben ser manejados desde la lógica de aplicaciones con tablas paramétricas que lleve control en los mismos de pendientes de firma, firmados o circuito de firma terminada.
- El componente debe tener un mecanismo que permita validar las entidades de certificación digital acreditadas en Colombia, que permita en el momento que exista una nueva entidad acreditada se adicione en este mecanismo de validación y la aceptación de la misma.
- El componente realiza la validación del estado del certificado por medio de CRL o OCSP.
- Debe contar con mecanismo de firma en PADES y/o CADES e integrado servicio de stampa cronológica de tiempo TSA, y que funcione mediante el estándar RFC 3161, accediendo por URL usuario + password debe ser parametrizable y modificable.
- Debe permitir firmar masivamente documentos de forma desatendida.
- El componente permite al gestor documental implementar la lógica necesaria para la funcionalidad de un usuario en flujo (preparador, revisor, aprobador y firmante) o identificar si es interno o externo.
- El componente permite implementar lógica para las notificaciones pertinentes con los datos establecidos de este.
- En cuanto el límite de fecha máxima, el componente permite implementar la lógica necesaria para el vencimiento del flujo de firma.
- Para usuarios que necesiten firmas en dispositivos Móviles el gestor documental mediante la integración con la API, permite implementar flujos de firma según sea el caso específico para esta funcionalidad.

"Se consideran copias controladas los documentos que se encuentran vigentes en ISOLUCIÓN".

Ministerio de las Culturas, las Artes y los Saberes

Dirección: Calle 9 No.8 - 31, Bogotá D.C., Colombia

Conmutador: (+57) 601 342 4100

Línea Gratuita: (+57) 01 8000 938081

www.mincultura.gov.co

Sede Correspondencia

Palacio Echeverry Calle 9 # 8 - 31

Ext. 4073 – 4074 - 4076

servicioalcudadano@mincultura.gov.co

OBLIGACIONES DE LA ENTIDAD

1. Aprobar las garantías allegadas por el proveedor para el inicio de la ejecución del contrato.
2. Poner a disposición del proveedor los comprobantes de descuentos y retenciones efectuados al pagar las facturas de acuerdo con lo dispuesto en el artículo 28 del Decreto Ley 019 de 2012.
3. Designar a la persona y esta, su tiempo, para recibir la capacitación del certificado digital de persona jurídica.
4. Contar con la disponibilidad presupuestal antes de publicar el proceso y realizar el correspondiente registro presupuestal antes del inicio de la ejecución del contrato.
5. Hacer el registro presupuestal del contrato de acuerdo con la normativa aplicable.
6. Poner a disposición de los Proveedores, cuando estos lo soliciten, el registro presupuestal.
7. Poner a disposición del proveedor cuando por la naturaleza de la adquisición aplique, los datos del ordenador del gasto, supervisor o persona designada por la entidad para realizar las descargas correspondientes.
8. Las demás que se encuentran consignadas para el desarrollo del presente contrato.

OBLIGACIONES GENERALES DEL CONTRATISTA:

1. Cumplir a cabalidad con el objeto del presente contrato, con plena autonomía técnica y administrativa, en la forma, tiempo, características técnicas, cantidad, calidad y cumplimiento pactadas, de acuerdo con los requisitos y especificaciones técnicas solicitadas por el Ministerio de las Culturas, las Artes y los Saberes y la propuesta presentada por el proponente, la cual forma parte integral del contrato.
2. Comunicar por escrito al Supervisor, cuando durante la ejecución del contrato se presenten situaciones no previstas, ajenas al control del Contratista, para que se tomen las medidas del caso.
3. Constituir la garantía única de cumplimiento que se exija en el contrato.
4. Mantener la debida confidencialidad de la información que pueda llegar a conocer durante la ejecución del contrato.
5. El proveedor se obliga a cumplir con la totalidad de requisitos de la política de Teletrabajo establecidos por el Gobierno Nacional.
6. Garantizar que los datos personales entregados por la Entidad sean manejados de acuerdo con la normatividad aplicable a la protección de datos personales.
7. Conocer y dar cumplimiento a las POLÍTICAS ESPECÍFICAS DE SEGURIDAD

"Se consideran copias controladas los documentos que se encuentran vigentes en ISOLUCIÓN".

Y PRIVACIDAD DE LA INFORMACIÓN y a los procedimientos, guías y lineamientos derivados de ella, así como a la política de tratamiento de datos personales y al MANUAL PARA TRATAMIENTO DE LA INFORMACIÓN PERSONAL – LEY HABEAS DATA (M-GAC-001) publicada en el aplicativo del Sistema Integrado de Gestión Institucional (ISOLUCION) del MINISTERIO.

8. Las demás que sean inherentes al objeto contractual.

OBLIGACIONES ESPECÍFICAS DEL CONTRATISTA:

1. Entregar al supervisor del contrato para su correspondiente entrada a almacén en caso de que aplique, la carta de custodia de los certificados digitales, en la cual conste que la vigencia de cada uno será de 12 meses, a partir de la activación de cada uno de ellos.
2. Entregar al supervisor del contrato al supervisor del contrato, para su correspondiente entrada a almacén en caso de que aplique, un (1) certificado digital de persona jurídica (token físico o virtual) de vigencia de un (1) año, con el mecanismo para la identificación y autenticación que se requiera.
3. Entregar 50 certificados digitales para persona natural, en formato de token criptográfico o Certificado Digital almacenado en un servidor seguro (HSM), solicitados cuya vigencia será de un (1) año contado a partir de la activación del certificado.
4. Coordinar con la empresa de mensajería, si es el caso, la entrega del certificado y/o firma digital, al supervisor del contrato, dentro del tiempo establecido (2 días hábiles).
5. Garantizar la instalación y configuración de los certificados y firmas digitales, en los equipos asignados a los usuarios designados para el uso de los dispositivos, a través de soporte técnico remoto, así como suministrar los drivers necesarios para su correcto funcionamiento.
6. Informar a los usuarios de cada uno de los dispositivos (tokens y certificados digitales), el procedimiento para la utilización de los certificados digitales para la firma de documentos.
7. Contar y mantener la acreditación dada por el Organismo Nacional de Acreditación de Colombia – ONAC, para expedir certificados digitales de Función Pública.
8. Garantizar el 100% compatibilidad de los certificados y firmas digitales con el aplicativo SIIF Nación II del Ministerio de Hacienda y Crédito Público y el cumplimiento de las garantías de seguridad: Autenticidad, Integridad, No Repudio y Confidencialidad.
9. Garantizar la compatibilidad del certificado digital de persona jurídica con el estándar PKCS (Public Key Cryptography Standards) vigente, apropiado para la emisión y administración de certificados.

"Se consideran copias controladas los documentos que se encuentran vigentes en ISOLUCIÓN".



Culturas

10. Suministrar al supervisor del contrato los Drivers necesarios para la configuración y uso del certificado digital de persona jurídica garantizando su funcionamiento en sistemas operativos Windows 10 y superiores.
11. Capacitar a la persona designada por la supervisión del contrato el uso del certificado digital de persona jurídica.
12. Garantizar el correcto funcionamiento del dispositivo. En caso de ser necesario, este será remplazado sin costo alguno.
13. Realizar la validación de identidad de los suscriptores del certificado y la firma digital, de acuerdo con las solicitudes realizadas por la entidad.
14. Garantizar que los certificados en token o digitales que no se activen durante la vigencia del contrato entraran en custodia por parte del proveedor y serán activados cuando la entidad lo requiera.
15. Garantizar la reposición de los certificados y firmas digitales hasta dos meses antes de su vencimiento, en caso de presentarse las siguientes situaciones:
 - Por daño de token físico: entiéndase daño como avería, ruptura, deterioro, desperfecto del token físico o daño lógico NO atribuible al suscriptor y que no pueda ser reparado.
 - Por olvido de clave del token virtual, siempre y cuando no pueda llevarse a cabo la recuperación de clave con la metodología dispuesta para tal fin, cuando aplique y el Proveedor lo tenga definido en sus procedimientos.
 - Por retiro definitivo o parcial del suscriptor del cargo o de la Entidad Compradora, siempre que se mantenga la necesidad funcional que dio origen a la expedición del certificado digital.

Para constancia firmo, en la ciudad de Bogotá a los _____

NOMBRE Y FIRMA REPRESENTANTE LEGAL

C.C.

Representante Legal

Empresa:

NIT:

"Se consideran copias controladas los documentos que se encuentran vigentes en ISOLUCIÓN".

Ministerio de las Culturas, las Artes y los Saberes

Dirección: Calle 9 No.8 - 31, Bogotá D.C., Colombia

Conmutador: (+57) 601 342 4100

Línea Gratuita: (+57) 01 8000 938081

www.mincultura.gov.co

Sede Correspondencia

Palacio Echeverry Calle 9 # 8 - 31

Ext. 4073 – 4074 - 4076

servicioalciudadano@mincultura.gov.co