## ANEXO ESTUDIO PREVIO

## ESPECIFICACIONES TÉCNICAS MÍNIMAS EXIGIDAS

**CERTIFICADOS FUNCIÓN PÚBLICA SIIF NACIÓN**
**FORMATO:** Firma Centralizada
**VIGENCIA**: 1 año desde su activación
**REASIGNACIÓN:** Posibilidad de reasignar 1 vez por cambio de titular

| ITEM | 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.<br>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 contar con Sello Web trust para garantizar la confiabilidad de sus procesos de ciclo de validación. |
| 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 | 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:<br>• Nombre<br>• Correo electrónico<br>• Ciudad<br>• Entidad<br>• Cédula de Ciudadanía<br>• NIT de la entidad usuaria. |

| | |
|---|---|
| | • Área= SIIF NACIÓN. |
| **15** | 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 desde su activación

| ITEM | 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.<br>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 contar con Sello Web trust para garantizar la confiabilidad de sus procesos de ciclo de validación. |
| **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** | 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:<br>• Nombre<br>• Correo electrónico<br>• Ciudad<br>• Entidad<br>• Cédula de Ciudadanía<br>• NIT de la entidad usuaria.<br>• Área= SIIF NACIÓN. |

| | |
|---|---|
| **15** | 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 desde su activación

**REASIGNACIÓN:** Posibilidad de reasignar 1 vez por cambio de titular

| ITEM | 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 contar con Sello Web trust para garantizar la confiabilidad de sus procesos de ciclo de validación. |
| **12** | 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. |
| **13** | 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). |
| **14** | 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. |
| **15** | Emisión con estándar X.509.V3, según las siguientes características:<br>• Nombre<br>• Correo electrónico<br>• Ciudad<br>• Entidad<br>• Cédula de Ciudadanía<br>• NIT de la entidad usuaria. |
| **16** | Los certificados deben compatibles con Adobe Sign utilizado en la entidad y AATL - CSC Cloud Signature Consortium (Certificados en Nube) |