OBJETO: *Entregar e implementar los componentes digitales que brinden una solución para garantizar la autenticidad, integridad y validez legal de los documentos electrónicos de archivo para la Comisión Nacional del Servicio Civil, de acuerdo con las especificaciones técnicas.*

CONDICIONES TÉCNICAS EXIGIDAS.

1	**Nombre del producto y/o servicio:**	**Mecanismo de Firma Digital (Certificado de Titular de Función Pública Certificado de Persona Jurídica)**
Requerimientos generales		• **Emitir y asignar 57 Certificados de firma digital de Titular de Función Pública compatible con el SGDEA OnBase.** • **Emitir un (1) Certificado de firma digital de Persona Jurídica a nombre de la Comisión Nacional del Servicio Civil compatible con el SGDEA OnBase.** • Firmado de documentos mediante el uso de servicios web, incluyendo el servicio de firma con OTP. • El mecanismo de firma digital debe tener incluido el estampado de tiempo. • El proveedor debe entregar los certificados de firma digital integrados con el SGDEA OnBase de la Comisión y en funcionamiento. • Los certificados deben cumplir con los requisitos exigidos en artículo 35 de la Ley 527 de 1999, y dar cumplimiento de los estándares vigentes RFC 5280 - internet X.509, ITU X-509 y lo establecido en el Decreto Ley 0019 de 2012, el Decreto 333 de 2014, el Decreto 1471 de 2014, el CEA-4.1-10 Versión 01, Anexo A. y los reglamentos que los modifiquen o complementen. • Los Certificados de firma digital deben ser emitidos y activados en dispositivos criptográficos HSM (módulo de seguridad hardware) de la entidad certificadora. • El servicio de dispositivo criptográfico HSM de la entidad certificadora o contratista debe contar con alta disponibilidad y estar alojado en diferentes data center tipo TIER III, cuya ubicación debe ser en el territorio colombiano con una disponibilidad de 7x24x365, 99.9% *uptime* por año.
Vigencia		Un (1) año a partir de la fecha de emisión del certificado.
Renovación o reposición		La reposición es el mecanismo por el cual se emite un certificado digital a un usuario posterior a la revocación del certificado digital de un funcionario. Renovación o reposición del Certificado de firma digital emitido para la CNSC, se dará por los siguientes casos: – Pérdida del número de identificación personal (PIN) de acceso al certificado digital – Compromiso de la llave privada – Bloqueo del certificado digital – Fallecimiento, incapacidad sobrevenida total o parcial del titular del certificado – Por renuncia o retiro del titular del certificado

1	Nombre del producto y/o servicio:	Mecanismo de Firma Digital (Certificado de Titular de Función Pública Certificado de Persona Jurídica)
		– Por situaciones de carácter administrativo, como vacaciones o licencias del titular En estos casos la Entidad Certificadora emitirá un nuevo Certificado de firma digital de Titular de Función Pública por el tiempo restante de su vigencia sin costo adicional para la Comisión, hasta dos (2) emisiones de certificados digitales no simultaneas durante la vigencia del contrato. El tiempo máximo para renovación o reposición es de dos (2) días hábiles una vez solicitado el trámite. En estos casos la Entidad Certificadora emitirá un Certificado de firma digital de Persona Juridica de modo que se pueda consumir por presidencia, y si se requiere también, que se pueda consumir su capacidad gradualmente, por usuarios que lo requieran por situaciones de carácter administrativo, como vacaciones o licencias del titular, a medida que se utiliza para firmar electrónicamente documentos durante su periodo de validez, según lo dispuesto por el ordenamiento jurídico vigente, y hasta por un número ilimitado de consumo. El tiempo máximo para la renovación o reposición es de cinco (5) días hábiles una vez solicitado el trámite. Para esto el representante legal, -presidencia-, emitirá comunicación de autorización para cuando sea necesario delegar el uso del certificado de firma digital de persona jurídica a los usuarios que lo necesiten, además de la presidencia.
Características técnicas del certificado	Se aclara que frente a cada ITEM (Requisito técnico) se debe cumplir con el estándar técnico y/o normativo mínimo indicado y descrito frente a cada característica.	
	Algoritmo de firma	– Función hash y RSA – RSA 2048 o superior SHA-256 Tamaño de clave mínimo 2048 bits (agosto 2002)
	Contenido del Certificado Digital	– RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and CRL Profile, o más recientes. – ITU-T Recommendation X.509 | ISO/IEC 9594-8, Information technology - Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks. (octubre 2016) Los certificados deben cumplir con los requisitos exigidos en artículo 35 de la ley 527 de 1999, deben contener los requisitos del estándar ITU X-509 y como mínimo lo siguiente: – Nombre, cargo, dirección y domicilio del suscriptor. – Una Identificación única del suscriptor nombrado en el certificado – El nombre y el lugar donde realiza actividades la CA. – Llave pública del certificado.

1	Nombre del producto y/o servicio:	Mecanismo de Firma Digital (Certificado de Titular de Función Pública Certificado de Persona Jurídica)
		– La metodología para verificar la firma digital del suscriptor impuesta en el mensaje de datos. – El número de serie (único) del certificado. – Fecha de emisión y expiración del certificado
	Ciclo de vida de los certificados	– RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. (junio 2006) – ETSI TS 102 042 - Policy requirements for certification authorities issuing public key certificate (febrero 2013)
	LDAP repositorio de Certificados	– RFC 4523 - Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates (junio 2006)
	Generación de claves	– Los requisitos de seguridad deben ser de alto nivel de forma que generen confianza, además de cumplir con requisitos certificado FIPS 140-2 level 3 o superior.
	Formatos de Firma digital contemplados para el servicio	– RFC 5126 CMS Advanced Electronic Signatures (CAdES) – RFC 5652 Cryptographic Message Syntax (CMS). – ETSI TS 101 733 CMS Advanced Electronic Signatures (CAdES) – W3C XML Advanced Electronic Signatures (XAdES) – ETSI TS (EN) 101 903 XML Advanced Electronic Signatures (XAdES) – ETSI TS(EN) 102 778 PDF Advanced Electronic Signature Profiles (PAdES) PDF/A
	Mecanismos de validación del estado del certificado - Lista de Certificados Revocados	– RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and CRL Profile. – ITU-T Recommendation X.509 ISO/IEC 9594-8 Information technology – Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.
	Mecanismos de validación del estado del certificado - Servicio del estado del certificado en línea	– RFC 6960 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP – RFC 2560 Protocolo OCSP (Protocolo de Estado de Certificado en Línea) – X.509 Internet PKI Online Certificate Status Protocol – OCSP – RFC 6960, de junio de 2013

2	Nombre del producto y/o servicio	Mecanismo de Firma Electrónica (cupo de 1000 firmas)
Requerimientos generales		• El mecanismo de Firma Electrónica debe vincular la identidad de una persona y su relación con el contenido de un documento electrónico producido en el SGDEA OnBase de la CNSC, obteniendo un documento PDF integro y firmado electrónicamente desde la plataforma del proveedor

2	Nombre del producto y/o servicio	Mecanismo de Firma Electrónica (cupo de 1000 firmas)	
		del servicio el cual contiene estampa del tiempo y toda la trazabilidad de la transacción. • El mecanismo de Firma Electrónica debe contar con métodos de validación tales como, códigos, contraseñas o datos biométricos que permiten identificar a una persona en relación con un mensaje de datos, en los términos del Decreto 2364 de 2012. • La plataforma de Firma Electrónica debe contar con mecanismos para realizar la trazabilidad de la transacción. • La plataforma de Firma Electrónica debe contar con la funcionalidad de validacion de credenciales de usuario en línea. • La gestión de la firma electrónica debe realizarse desde la plataforma del proveedor del servicio. • Los servicios ofertados deberán contar los respectivos API o SDK con el fin de llevar a cabo la integración con el SGDEA OnBase de la Entidad. • El proveedor del servicio debe entregar al supervisor del contrato un reporte mensual del consumo de firmas electrónicas y cupos de OTP dentro de los primeros cinco (5) días hábiles de cada mes o proporcionar una disponibilidad de consulta en línea o servicio web. O en su defecto sumistrar a la CNSC una herramienta web donde se pueda llevar el control sobre la disponibilidad de las firmas electronicas y el cupo usado para OTP.	
Vigencia		El cupo de firmas electrónicas estará vigente por un tiempo de hasta veinticuatro (24) meses a partir del recibo a satisfacción del producto.	
Características técnicas		Se aclara que frente a cada ITEM (Requisito técnico) se debe cumplir con el estándar técnico y/o normativo mínimo indicado y descrito frente a cada requisito.	
		Sistema operativo	Compatible con los sistemas operativos, Windows 8.1 (32 y 64 bits), Windows 10 (32 y 64 bits) y Windows 11 (32 y 64 bits).
		Dispositivos móviles	Debe ser compatible con cualquier tipo de dispositivo móvil con SO Windows, Windows Mobile, Android, iOS, dependiendo de la tecnología ofertada por el contratista.
		Confiabilidad de la firma electrónica	Decreto 2364 de 2012, Articulo 4. La firma electrónica se considerará confiable para el propósito por el cual el mensaje de datos fue generado o comunicado si: – Los datos de creación de la firma, en el contexto en que son utilizados, corresponden exclusivamente al firmante. – Es posible detectar cualquier alteración no autorizada del mensaje de datos, hecha después del momento de la firma.
		Métodos de validación / firmado electrónico	Firma electrónica Certificada con el servicio de validación de identidad, que dentro de su caracterización permite la firma a través de SMS (OTP)

3	Nombre del producto y/o servicio	Servicios conexos (Soporte implementación y licencia o Renovación del servicio de suscripción)
	Soporte técnico	• Resolver los problemas técnicos que surjan en la generación o emisión, activación, implementación y utilización de los productos y servicios adquiridos por la CNSC y prestar soporte técnico durante el término de vigencia de los certificados emitidos y de cupo de firmas electrónicas. El servicio de soporte será, como mínimo de lunes a viernes de 8:00 a 18:00 horas. • Contar con un sistema web de administración de cupo de certificados de firmas digitales a través de la cual el funcionario designado por la CNSC pueda llevar a cabo la gestión y control del cupo. El módulo debe permitir: – Radicar las solicitudes de emisión de los certificados digitales y hacer el cargue de los documentos soporte. – Visualizar las aprobaciones de solicitudes de emisión de certificados – Solicitar revocación, reposición y reasignación de certificado digital – Realizar seguimiento a la emisión y asignación de certificados digitales – Controlar la cantidad de certificados digitales emitidos, activados, revocados, vigentes – Consultar la trazabilidad del proceso de emisión y entrega de certificados • Publicar y mantener la lista de revocados en la CRL con una disponibilidad de consulta en línea o servicio web 7X24X365, 99,9% *uptime* por año, conforme al documento Criterios Específicos de Acreditación CEA-4.1-10, versión 1. • Proveer el servicio de revocación de los certificados a través de una línea de atención a nivel nacional o servicio web con disponibilidad 7X24X365. • Contar con un centro de servicio que permita la atención y recepción de los requerimientos de la CNSC a través de: – Número telefónico de atención en Bogotá D.C. o línea telefónica con atributo de llamada local desde ciudad de Bogotá D.C. que cuente con un esquema de mesa de ayuda para la atención y solución de los requerimientos técnicos. – Chat en línea – Correo electrónico • Todo requerimiento o solicitud de soporte debe tener historial, desde su registro hasta la solución definitiva. El tiempo máximo para resolución de los casos de soporte debe ser de máximo dos (2) días hábiles en horario colombiano a partir de la radicacion del caso(incidente, requerimiento) de soporte.
	Instalación y configuración y/o renovación suscripción servicios firma	• Facilitar la instalación y configuración de todos los componentes necesarios de software y recursos humanos. • Garantizar el correcto funcionamiento de las firmas con el SGDEA OnBase. • Proporcionar, el servicio de integración del SGDEA (OnBase) de la CNSC con la plataforma del proveedor del servicio de firma digital y electrónica

3	Nombre del producto y/o servicio	Servicios conexos (Soporte implementación y licencia o Renovación del servicio de suscripción)
	electrónica, firma digital y estampado modalidad SaaS	se hará mediante interfaz de programación de aplicaciones que se ajuste a los límites de la arquitectura REST. • **El proveedor del servicio asumirá a cuenta y riesgo los costes de la integración del Sistema de Gestión Documental OnBase de la entidad con su plataforma de firma digital y electrónica.** • El contratista apoyará las actividades técnicas necesarias durante el proceso de transición de cambio de proveedor que se da por terminación del contrato e inicio de uno nuevo con un posible nuevo proveedor, lo anterior con el fin de mitigar cualquier riesgo de que la CNSC quede descubierto del servicio y esto afecta la operación. • En la actividad de transición el contratista debe mantener la disponibilidad de acceder a un certificado valido, este proceso puede tardar hasta máximo 2 meses.

FIRMA
NOMBRE DEL REPRESENTANTE LEGAL:
NOMBRE O RAZÓN SOCIAL:
NIT:
DOCUMENTO DE IDENTIDAD: