ANEXO TÉCNICO PARA LA ADQUISICIÓN DE CERTIFICADOS DIGITALES

1. OBJETO:

Adquisición de certificados de firma digital con token virtual centralizado y componente API para integración con la plataforma SIGA, bolsa de correos certificados electrónicos para garantizar la trazabilidad de comunicaciones oficiales y certificado SSL para la seguridad del sitio web institucional"

2. ESPECIFICACIONES Y/O CONDICIONES TÉCNICAS REQUERIDAS

La solución ofertada deberá garantizar la interoperabilidad con la plataforma SIGA, permitiendo la integración de sus diferentes componentes mediante mecanismos seguros de intercambio de información, sin afectar la operación normal del sistema ni requerir desarrollos adicionales diferentes a las actividades propias de integración.

Como mínimo, el contratista deberá suministrar los siguientes componentes tecnológicos:

1. **Bolsa de correos electrónicos certificados**

   Suministro de una bolsa de seis mil (6.000) correos electrónicos certificados, que permita el envío de comunicaciones oficiales electrónicas desde la plataforma SIGA, garantizando el registro de la fecha y hora de envío, entrega al servidor del destinatario, trazabilidad completa del mensaje, integridad del contenido y generación de evidencias electrónicas con validez probatoria

2. **Certificados de Firma Digital Función Pública**

   Activación de diez (10) certificados de Firma Digital Función Pública con token virtual centralizado para los funcionarios que determine el supervisor del contrato por vigencia de 1 año.

3. API para integración de firma digital

El certificado digital deberá incluir una API (Application Programming Interface) que permita la integración de los certificados de firma digital con la plataforma SIGA mediante servicios web (Web Services) en modalidad SaaS.

ESPECIFICACIONES CERTIFICADOS DE FIRMA DIGITAL - (TOKEN VIRTUAL)	
Descripción	La entidad requiere diez (10) certificados de firma digital con token virtual centralizado que garantice la validación de identidad y responsabilidad del autor de documentos en transacciones electrónicas y firmas digitales para los funcionarios responsables del manejo de recursos públicos. Adicional los certificados de firma digital deben incluir un componente API (Application Programmer Interface) para el uso de las firmas que permita sea invocado/integrado en cualquier sistema de información vía Web Service. EL CONTRATISTA deberá activar los certificados de firma digital a criterio de la entidad y conforme a las instrucciones del Supervisor.
Vigencia	1 año
Tipo	Firma Digital Función Pública – Token Virtual Centralizado
Exposición del API	Se requiere que el proveedor incluya el API para que vía WS en modalidad SaaS pueda consumirse y realizarse el proceso de firmado.
Compatibilidad con sistemas operativos	Garantizar que el servicio es compatible con los sistemas operativos Windows, versiones Win 8, Win 10 y MAC OS; los certificados deberán ser compatibles con sistemas de 32 y 64 bits.
Compatibilidad con estándares de seguridad	Garantizar que el servicio es compatible con los estándares de seguridad: • PKCS (Public Key Cryptography Standards) 7 ó superior. • ITU X509, las disposiciones de campos mínimos requeridos definidas por la Ley 527 de 1999, el Decreto 333 de 2014 y 019 de 2012.

Firma digital Función Pública	Acreditar certificación del servicio Certificado de Firma Digital-Función Pública (o equivalente) ante ONAC, garantizando así, el cumplimiento con la normatividad vigente.
Llaves criptográficas	El tamaño de la llave de los certificados digitales de Función Pública debe ser de 2048 bits o tamaño superior con base en tecnología PKI (Public Key Infrastructure). El RSA con longitud de clave no inferior a 2048 para CA, No se permiten Claves inferiores a 2048.
Soporte	La adquisición de los certificados de firma digital debe incluir como servicio conexo, el soporte que se describe a continuación: a. Realizar la atención de los requerimientos y/o incidentes en el horario de atención de 8:00 am a 5:00 pm de lunes a viernes y los sábados en jornada de la mañana b. Asistencia para la instalación, configuración y atención de incidentes. c. Brindar soporte técnico durante toda la vigencia de los certificados digitales

1. *Certificado SSL Wildcard*

ITEM	REQUISITO TECNICO
Tipo de certificado	SSL/TLS tipo OV —Organization Validation— Wildcard
Dominio principal	idep.edu.co
Dominio Wildcard	*.idep.edu.co
Vigencia	1 año
SAN requerido	Debe incluir como mínimo idep.edu.co y *.idep.edu.co
Cobertura	Protección del dominio principal y subdominios de primer nivel bajo idep.edu.co

Período de Soporte

El proveedor deberá garantizar el soporte durante la vigencia de los certificados digitales.