ANEXO - FICHA TÉCNICA

1. **OBJETO:** ADQUIRIR EL CERTIFICADO DE SEGURIDAD PARA LAS APLICACIONES DE LA AUTORIDAD NACIONAL DE LICENCIAS AMBIENTALES ANLA.

2. **CLASIFICACIÓN DE BIENES Y SERVICIOS A ADQUIRIR:**

Con base en el clasificador de bienes y servicios de las Naciones Unidas, a continuación, se establece el sector económico al que pertenece el servicio a contratar:

CLASIFICACIÓN UNSPSC	SEGMENTO	FAMILIA	CLASE
81111800	Servicios Basados en Ingeniería, Investigación y Tecnología	Servicios informáticos	Servicios de sistemas y administración de componentes de sistemas
43232200	Difusión de Tecnologías de Información y Telecomunicaciones	Software	Software de gestión de contenidos

3. **DESCRIPCIÓN DE LOS CERTIFICADOS A ADQUIRIR:**

La Oficina de Tecnologías de la Información (OTI) requiere la adquisición del certificado SSL por un (1) año así:

- Un (1) certificado de Servidor Seguro **(certificado SSL sitio seguro OV WILCARD, con sello de seguridad de reconocimiento SAN)** con Numero de SAN ilimitados para asegurar el dominio *anla.gov.co, es decir Este certificado permite la inclusión de un número ilimitado de nombres de dominio y subdominios bajo el dominio principal *anla.gov.co.

La Vigencia de Certificado de Servidor Seguro (SSL OV WILDCARD con sello de seguridad de reconocimiento SAN), ser de un (1) año a partir de su activación teniendo en cuenta la vigencia del certificado actual, esto es contado desde el **03 de noviembre de 2026 a las 19:00 horas.**

La vigencia del certificado de Servidor Seguro (SSL OV WILDCARD con sello de seguridad de reconocimiento SAN) solicitado deberá corresponder a **un (1) año**, comprendido entre el **03 de noviembre de 2026 a las 19:00 horas** y el **03 de noviembre de 2027 a las 18:59 horas**.

Nota: El proveedor deberá emitir y entregar el certificado con una antelación mínima de **tres (3) días calendario** al inicio de su vigencia, permitiendo a la ANLA realizar las actividades necesarias para su implementación y puesta en producción sin afectar la disponibilidad de los servicios.

La adquisición del certificado SSL es necesaria para garantizar la autenticidad, confidencialidad e integridad de las comunicaciones entre los usuarios y los servicios digitales de la ANLA. Asimismo, permite mantener la protección de los dominios y subdominios institucionales bajo ***.anla.gov.co**, cumpliendo con las buenas prácticas de seguridad de la información y asegurando la continuidad operativa de los servicios publicados por la entidad.

A continuación, se indican las especificaciones de cada Certificado:

3.1. CERTIFICADO SSL SITIO SEGURO OV WILCARD

- Certificado SSL/TLS tipo OV (Organization Validation) Wildcard.
- Protección del dominio principal*.anla.gov.co y sus subdominios asociados.
- Inclusión de SAN (Subject Alternative Names) para la protección de nombres de dominio y subdominios adicionales requeridos por la Entidad.
- Compatibilidad con algoritmos criptográficos RSA de 2048 bits o superior.
- Compatibilidad con algoritmos criptográficos ECC (Elliptic Curve Cryptography) P-256 o superior.

- Compatibilidad con algoritmos de firma digital SHA-256 o superiores.
- Compatibilidad en los protocolos TLS 1.2 o superior
- Monitoreo de registros de transparencia de certificados (Certificate Transparency Logs - CT Logs) para la detección de certificados emitidos sobre el dominio protegido.
- Inclusión de sello de seguridad (Trust Seal) visible para los usuarios del portal web protegido.
- Anti-suplantación de sitio suplantación de sitio) y con escaneos de seguridad (malware y vulnerabilidades) o equivalente
- Compatible con cifrado PQC y monitoreo de log CT
- Compatible con algoritmo ECC: Acrónimo del inglés Elliptic Curve Cryptography
- Reemisión (sin costo) ilimitada del certificado TLS durante vigencia del contrato.
- Instalación del certificado SSL/TLS OV versión 1.1 o superior:
- Configuración del certificado TLS.
- Validación del correcto funcionamiento del certificado TLS en cada uno de los servicios que se implemente.
- Respuesta frente a fallas técnicas del certificado TLS durante su vigencia.
- Debe mostrar el portal web asegurado con el certificado SSL/TLS un sello de seguridad.
- Asistencia técnica de seguridad ilimitada con el certificado SSL/TLS, durante la vigencia del certificado.
- Compatibilidad con los actuales navegadores del mercado y con dispositivos móviles.
- La clave de los algoritmos de cifrado debe ser para RSA (Rivest, Shamir y Adleman) mínimo de 2048 bits o superior y para ECC (Elliptic Curve Cryptography) mínimo de 224 bits.
- Extensiones requeridas:

  - ✓ PFX
  - ✓ KEY
  - ✓ .CRT
  - ✓ .CER
  - ✓ .PEM
- El certificado deberá ser emitido por una Autoridad de Certificación (CA) reconocida y confiable para los principales navegadores web, sistemas operativos y dispositivos móviles del mercado. Para lo anterior el oferente deberá presentar **una certificación expedida directamente por la Autoridad Certificadora (CA), en la que se indique expresamente su condición de partner, distribuidor, reseller o canal autorizado para la comercialización y suministro de certificados SSL/TLS**. La certificación deberá tener una fecha de expedición no superior a sesenta (60) días calendario anteriores a la fecha de presentación de la oferta.

NOTA 1: El proponente con la firma del presente documento se compromete a cumplir con todos los requerimientos técnicos descritos en los estudios previos y el pliego de condiciones y así mismo manifiesta expresamente que cumple con la totalidad de los requerimientos técnicos diseñados y solicitados por la Entidad.

NOMBRE DEL PROPONENTE: _____

FIRMA DEL REPRESENTANTE LEGAL: _____

Nombre del Representante Legal: _____

C.C.: _____

Autorizo la notificación electrónica a la dirección de correo electrónico_____