ANEXO II

CARTA DE PRESENTACION DE LA PROPUESTA

Pitalito, _____ de ____ de 2026.

Señores
INSTITUTO DE TRANSITO DE PITALITO - INTRAPITALITO –
Calle 1 N° 11-45 este – Barrio Paraíso.
Teléfono: 8369520.
Email: contactenos@intrapitalito-huila.gov.co
Pitalito.

Asunto: Invitación Pública No. 016 de 2026.

Objeto: *"El Suministro, instalación, configuración y puesta en funcionamiento de una solución de seguridad perimetral tipo firewall con licenciamiento, para el Instituto de Tránsito y Transporte de Pitalito – INTRAPITALITO".*

Respetados señores:

El suscrito (nombre de la persona natural o representante legal de la persona jurídica), en mi calidad de (Persona natural o Representante legal de la empresa xxxxxxx); identificado (a) con (la cédula de ciudadanía o NIT de la empresa) N° indicar el N° de cédula de ciudadanía o el N° del NIT de la empresa), actuando como proponente en el proceso de contratación de asunto y de conformidad con las condiciones que en este proceso de contratación se estipulan, presento propuesta que si es aceptada, me comprometo a dar cumplimiento a lo establecido en el respectivo contrato.

La propuesta es la siguiente:

Exponer o describir la propuesta, indicando como mínimo el producto, cantidad y valor.

El valor de la propuesta o cada uno de los ítems no podrá exceder el valor de la invitación o los indicados a continuación.

DESCRIPCION	CANT.	VALOR
Equipo con Solución Perimetral Firewall de Próxima Generación (NGFW), que incluya: 1. Licencia del firewall. 2. Licenciamiento de Seguridad Avanzada para 50 Estaciones de Trabajo, 3. Licenciamiento de Seguridad Avanzada para 3 servidores 4. Solución de Seguridad Avanzada para 50 Correos Electrónicos Institucional. 5. Instalación, configuración y puesta en marcha de la solución de seguridad, por ingeniero certificado por el fabricante.	1	$33.769.188

6. Mínimo 50 Horas de soporte técnico posventa por ingeniero certificado por el fabricante. 7. Capacitación y transferencia de conocimiento por ingeniero certificado por el fabricante. 8. Un voucher para certificación del fabricante de la solución de seguridad perimetral firewall, presencial dentro del departamento del Huila. 9. Mínimo dos (02) revisiones del estado de la consola.		
VALOR TOTAL		**$33.769.188**
IVA		**$6.416.146**
VALOR TOTAL IVA INCLUIDO		**$40.185.334**

EL VALOR DE LA OFERTA ES LA SUMA DE:

Indicar el Valor en Letras (de la sumatoria de los valores unitarios) .

Las condiciones técnicas ofertadas corresponden con las siguientes:

Suministro, instalación, configuración y puesta en funcionamiento una solución integral de seguridad perimetral y seguridad informática de categoría empresarial, orientada a ambientes corporativos e institucionales, diseñada para garantizar altos niveles de disponibilidad, protección, interoperabilidad, administración y mitigación de amenazas cibernéticas avanzadas sobre la infraestructura tecnológica del Instituto de Tránsito y Transporte de Pitalito – INTRAPITALITO.

La solución ofertada cumple con las especificaciones técnicas descritas a continuación:

1. SOLUCIÓN DE SEGURIDAD PERIMETRAL FIREWALL DE PRÓXIMA GENERACIÓN (NGFW), QUE INCLUYA:

El equipo con la solución ofertado cuenta con una plataforma de seguridad perimetral de categoría empresarial, orientada a ambientes corporativos e institucionales, diseñada para garantizar altos niveles de disponibilidad, protección, interoperabilidad, administración y mitigación de amenazas avanzadas de seguridad informática.

La solución es nueva, original, no remanufacturada, no reacondicionada y no se encuentra en estado de obsolescencia, fin de soporte (End of Support), fin de vida útil (End of Life – EOL) o descontinuación por parte del fabricante durante la vigencia contractual y del licenciamiento suministrado.

La solución cumple con mínimo con las siguientes características técnicas:

1.1. Arquitectura y Hardware.

- Equipo físico de seguridad perimetral de categoría empresarial rackeable.
- Arquitectura multinúcleo de doble procesador dedicado:
  - un procesador principal x86,

- y un coprocesador o procesador especializado para aceleración de tráfico y procesamiento de seguridad.

- Procesamiento dedicado para funciones de:
  - Inspección profunda de paquetes.
  - Inspección SSL/TLS.
  - Aceleración de tráfico.
  - FastPath,
  - Procesamiento criptográfico.
  - y procesamiento de amenazas en tiempo real.

- Almacenamiento interno mínimo de 64 GB SSD tipo M.2 destinado a:
  - almacenamiento de logs,
  - reportes,
  - cuarentena,
  - firmware,
  - y funciones de análisis de seguridad.

- Operación continua 7x24.
- Arquitectura diseñada para ambientes empresariales o institucionales.
- Fuente de alimentación compatible con infraestructura institucional.

1.2. Rendimiento Mínimo

La solución cumple con mínimo con los siguientes niveles de rendimiento:

- Rendimiento del firewall: 19.100 Mbps
- Rendimiento IPS: 5.850 Mbps
- Rendimiento de protección contra amenazas: 4750 Mbps
- Rendimiento de inspección SSL/TLS de Xstream: 1700 Mbps
- Conexiones simultáneas: 6.550.000
- Nuevas conexiones por segundo:105.000
- Consumo de energía: 33 W (en reposo), 51 W (máx.)
- Conexiones Simultáneas Xstream SSL/TLS 18.432

1.3. Interfaces y Conectividad.

La solución cumple mínimo con:

Interfaces Ethernet

- Mínimo cuatro (4) puertos RJ45 Ethernet 10/100/1000 Mbps.
- Mínimo dos (2) puertos RJ45 2.5 GbE con soporte PoE+ bajo estándar IEEE 802.3at. Puertos de cobre de 2,5 GE
- Mínimo dos (2) puertos Fibra SFP+ con soporte para conectividad 1 GbE y 10 GbE.

Interfaces de Administración

- Mínimo un (1) puerto consola RJ45.
- Mínimo un (1) puerto Micro USB de administración.

Interfaces Adicionales
- Mínimo un (1) puerto USB 2.0 frontal.
- Mínimo un (1) puerto USB 3.0 posterior.

Expansión
- Mínimo una (1) bahía o ranura de expansión para conectividad celular LTE/5G.

1.4. Funcionalidades de Seguridad

La solución cumple mínimo con:

- Firewall Stateful Inspection.
- Deep Packet Inspection (DPI).
- Sistema IPS/IDS.
- Inspección TLS 1.3.
- Filtrado web avanzado por categorías.
- Control de aplicaciones Layer 7.
- Protección antimalware.
- Protección anti ransomware.
- Protección frente a amenazas Zero-Day.
- Sandboxing .
- Inteligencia de amenazas en tiempo real.
- Protección contra phishing.
- Protección contra botnets.
- Protección contra command & control.
- Protección frente a exploits.
- Seguridad sincronizada con endpoints.
- Respuesta automática frente a amenazas.
- Detección y aislamiento automático de dispositivos comprometidos.
- Segmentación de red mediante VLAN.
- Soporte IPv4/IPv6.
- NAT/PAT.
- SD-WAN.
- Balanceo de enlaces WAN.
- QoS.
- VPN SSL.
- VPN IPsec.
- VPN cliente HTML5.
- Administración cloud centralizada.
- Consola web de administración.
- Generación de logs y reportes.
- Alertamiento automático.
- Integración con Active Directory o LDAP.
- Integración con servicios de directorio y autenticación.
- Capacidad de gestión centralizada de seguridad.

NOTA 1: La solución permite crecimiento, escalabilidad y expansión futura sin requerir reemplazo inmediato de la plataforma principal.

NOTA 2: La solución garantiza la interoperabilidad y compatibilidad con la infraestructura tecnológica, servicios de red, plataformas institucionales y sistemas de información actualmente implementados por la entidad

2. LICENCIA DEL FIREWALL

La solución incluye licenciamiento mínimo por doce (12) meses la cual contempla como mínimo:

A. Reducción de la Superficie de amenazas

- Protección contra virus de nueva generación.
- Protección web
- Control web
- Reputación de descargas
- Control de aplicaciones
- Control de periféricos
- Prevención de pérdida de datos
- Bloqueo de servidor (lista de aplicaciones permitidas)

B. Prevención de amenazas

- Advertencias de ataques críticos en toda la infraestructura Windows
- Prevención de malware basada en IA con Deep Learning
- Escaneado de archivos antimalware
- Bloqueo de aplicaciones no deseadas (PUA)
- Búsquedas en la nube de Live Protection
- Análisis de comportamientos
- Antiexploits (+60 mitigaciones)
- Bloqueo de aplicaciones
- Interfaz de escaneado antimalware (AMSI)
- Detección de tráfico malicioso
- Sistema de prevención de intrusiones (IPS)
- Monitorización de integridad de archivos (servidores)
- Agente ZTNA integrado

C. Detección Investigación y respuesta

- Datos detallados en el dispositivo para obtener información clave en tiempo real
- Detecciones de eventos sospechosos
- Priorización de detecciones basada en IA
- Asignación automática a la plataforma MITRE
- Detecciones de comportamientos y exploits en contenedores Linux
- Exposición de dispositivos
- Genere detecciones basadas en datos de productos de terceros integrados
- Correlación y análisis de eventos entre productos
- Gráficos de amenazas de RCA
- Limpieza automática de malware
- Reversión automática del cifrado de archivos del ransomware
- Finalización automática de procesos

- Protección de archivos contra ransomware (CryptoGuard)
- Protección contra el ransomware remoto (CryptoGuard)
- Protección contra el ransomware que ataca el registro de arranque maestro (MBR)
- Adaptive Attack Protection
- Datos exhaustivos en el dispositivo y en la nube
- Antimalware avanzado.
- Deep Learning.
- Inteligencia artificial.
- Protección anti ransomware.
- Rollback automático.
- Protección MBR.
- Mitigación de exploits.
- Protección fileless.
- Protección contra robo de credenciales.
- Control web.
- Control de aplicaciones.
- Control de dispositivos USB.
- DLP básico.
- EDR/XDR.
- Consola cloud centralizada.
- Monitoreo en tiempo real.
- Aislamiento automático de equipos comprometidos.
- Integración con firewall.
- Compatibilidad con sistemas operativos Windows de entorno empresarial. (Windows , Apple, Linux)
- Vigencia mínima de doce (12) meses.
- Gestion de reportes en Nube.

3. LICENCIAMIENTO DE SEGURIDAD AVANZADA PARA ESTACIONES DE TRABAJO

La solución incluye cincuenta (50) licencias para estaciones de trabajo y cumple mínimo con:

- Antivirus de nueva generación.
- Antimalware avanzado.
- Deep Learning.
- Inteligencia artificial.
- Protección anti ransomware.
- Rollback automático.
- Protección MBR.
- Mitigación de exploits.
- Protección fileless.
- Protección contra robo de credenciales.
- Control web.
- Control de aplicaciones.
- Control de dispositivos USB.
- DLP básico.

- EDR/XDR.
- Consola cloud centralizada.
- Monitoreo en tiempo real.
- Aislamiento automático de equipos comprometidos.
- Integración con firewall.
- Compatibilidad con sistemas operativos Windows de entorno empresarial.
- Vigencia mínima de doce (12) meses.

4. LICENCIAMIENTO DE SEGURIDAD AVANZADA PARA SERVIDORES

La solución incluye tres (3) licencias para servidores y cuenta mínimo con:

- Protección antimalware para servidores.
- Protección anti ransomware.
- Detección avanzada de amenazas.
- EDR/XDR para servidores.
- Protección de procesos críticos.
- Protección fileless.
- Mitigación de exploits.
- Consola cloud centralizada.
- Integración con firewall.
- Monitoreo y alertamiento.
- Compatibilidad con sistemas operativos servidor.
- Vigencia mínima de doce (12) meses.

5. SOLUCIÓN DE SEGURIDAD AVANZADA PARA CORREO ELECTRÓNICO

La solución incluye cincuenta (50) cuentas de correo electrónico institucional y cuenta mínimo con:

- Protección antispam.
- Protección anti phishing.
- Protección malware.
- Protección Business Email Compromise (BEC).
- Protección spoofing.
- Sandboxing de adjuntos.
- Análisis de URLs maliciosas.
- Validación SPF, DKIM y DMARC.
- Filtrado correo entrante y saliente.
- Consola centralizada.
- Reportes y alertas.
- Escaneo de archivos adjuntos.
- Protección dominios maliciosos.
- Actualización automática.
- Vigencia mínima de doce (12) meses.
- Integración y compatibilidad con plataformas de correo corporativo en entornos cloud, incluyendo servicios tipo Google Workspace o equivalentes.

6. SOPORTE TÉCNICO ESPECIALIZADO

Se brindará mínimo cincuenta (50) horas de soporte técnico especializado, el cual incluye como mínimo:

- Atención remota en horario mínimo 5x8.
- Diagnóstico de incidentes.
- Solución de fallas.
- Ajustes de configuración.
- Soporte sobre firewall, endpoints y correo.
- Escalamiento técnico especializado.
- Atención por personal certificado por fabricante.

7. INSTALACIÓN, CONFIGURACIÓN Y PUESTA EN FUNCIONAMIENTO

Durante la ejecución del contrato se realizará:

- Instalación física y lógica.
- Configuración inicial.
- Configuración de políticas.
- Configuración VPN.
- Configuración IPS.
- Configuración filtrado web.
- Configuración control aplicaciones.
- Integración con infraestructura existente.
- Activación de licencias.
- Pruebas funcionales.
- Puesta en producción.

8. CAPACITACIÓN Y TRANSFERENCIA DE CONOCIMIENTO

Durante la ejecución del contrato se realizará capacitación técnica sobre:

- Administración básica.
- Gestión de políticas.
- Monitoreo.
- Gestión de incidentes.
- Buenas prácticas de seguridad.

La capacitación deberá tener duración mínima de cuatro (4) horas y estar dirigida al personal designado por la entidad.

9. UN (1) VOUCHER, CUPO O MECANISMO EQUIVALENTE DE CERTIFICACIÓN DEL FABRICANTE DE LA SOLUCIÓN DE SEGURIDAD PERIMETRAL FIREWALL

La solución ofertada incluye un (1) voucher, cupo, entrenamiento técnico, examen de certificación o mecanismo equivalente orientado al fortalecimiento de capacidades técnicas del personal designado por la entidad, relacionado con administración de soluciones firewall o seguridad perimetral.

La capacitación, entrenamiento técnico o proceso de certificación presencial se realizará dentro del departamento del Huila. En consecuencia, el contratista deberá tener en cuenta dentro de la propuesta económica todos los costos requeridos para garantizar el desarrollo integral de dicha actividad, incluyendo, cuando haya lugar a ello:

- desplazamiento,
- alojamiento,
- alimentación,
- inscripción,
- capacitación,
- material técnico o didáctico,
- derecho de presentación de pruebas o evaluaciones,
- certificación,
- y demás costos asociados.

La actividad deberá ser impartida o avalada por el fabricante de la solución ofertada o por un centro autorizado por este.

10. REVISIONES TÉCNICAS DEL ESTADO DE SEGURIDAD DE LA CONSOLA DE ADMINISTRACIÓN

Durante la vigencia del contrato se realizará mínimo dos (2) revisiones técnicas del estado de seguridad y funcionamiento de la consola centralizada de administración de la solución implementada.

Las revisiones incluir como mínimo:

- validación del estado general de seguridad,
- revisión de eventos e incidentes,
- análisis de alertas,
- validación de políticas de seguridad,
- revisión de amenazas detectadas,
- identificación de vulnerabilidades,
- validación del estado de licenciamiento,
- y análisis general del estado operativo de la plataforma.

Cada revisión incluye:

- clasificación de riesgos,
- categorización de criticidad,
- recomendaciones técnicas de mitigación,
- y buenas prácticas de fortalecimiento de seguridad.

Al finalizar las revisiones se entregará informe técnico de cada revisión realizada.

11. GARANTÍA Y SOPORTE

- Garantía oficial fabricante.
- Soporte oficial fabricante durante la vigencia del licenciamiento.
- En caso de daño

- Acceso a actualizaciones de seguridad.
- Acceso a firmware.
- Acceso a parches de seguridad.
- No se aceptarán soluciones OEM, clonadas, reacondicionadas o sin respaldo oficial fabricante.
- El licenciamiento suministrado deberá quedar registrado oficialmente a nombre del Instituto de Tránsito y Transporte de Pitalito – INTRAPITALITO.
- Garantizar el soporte y restablecimiento del Firewall, realizando la reparación o reposición del equipo en un término no mayor a setenta y dos (72) horas, contadas a partir del reporte realizado por la entidad.

NOTA 1: La solución ofertada es nueva, original, no remanufacturada, no reacondicionada y no encontrarse en estado de obsolescencia, fin de soporte (End of Support), fin de vida útil (End of Life – EOL) o descontinuación por parte del fabricante durante la vigencia del contrato y del licenciamiento suministrado.

NOTA 2: Cuando en las especificaciones técnicas se indiquen capacidades, arquitecturas, funcionalidades, estándares, tecnologías o características técnicas específicas, se entenderán como requisitos mínimos equivalentes requeridos por la entidad para garantizar el adecuado funcionamiento, interoperabilidad, seguridad y desempeño de la solución tecnológica ofertada.

12. PERSONAL TÉCNICO MÍNIMO REQUERIDO

Para la ejecución de las actividades de instalación, configuración, implementación, soporte técnico y capacitación de la solución tecnológica, como contratista manifiesto que cuento con personal profesional calificado.

Para tal efecto, adjunto a la propuesto acredito la disponibilidad de dos (2) profesionales en ingeniería de sistemas, telecomunicaciones o áreas afines. Los cuales relaciono a continuación:

1. **Indicar el Nombre, numero de documento de identificación y título profesional que ostenta el Profesional 1.**

---

2. **Indicar el Nombre, numero de documento de identificación y título profesional que ostenta el Profesional 2.**

Declaro así mismo:

1. Que esta propuesta solo compromete a los firmantes de esta carta.
2. Que conocemos y aceptamos los documentos de la invitación pública, en especial las condiciones técnicas establecidas.
3. Que para calcular el precio ofrecido, hemos calculado todos los gastos, costos, derechos, impuestos, tasas y demás contribuciones que se causen con ocasión de la presentación de la oferta, suscripción y ejecución del contrato, de acuerdo con las

normas legales vigentes, ya que los mismos se entienden y se asumen por cuenta nuestra.

4. Declaro bajo la gravedad de juramento de manera clara e inequívoca, que ni el proponente, ni su representante legal, ni su apoderado, ni sus socios, nos encontramos incursos en las causales de inhabilidad e incompatibilidad previstas en la Constitución y en la Ley, en especial las contempladas en el artículo 8 de la Ley 80 de 1993, en la Ley 1150 de 2007 y en la Ley 1474 del 12 de Julio de 2011.
5. Autorizo expresamente para recibir notificaciones en el correo electrónico.
6. Declaro bajo la gravedad de juramento de manera clara e inequívoca, que como proponente estoy a paz y salvo con mis obligaciones laborales frente al sistema de seguridad social integral y demás aportes relacionados con las obligaciones laborales.
7. Declaro bajo la gravedad de juramento que se entiende prestado por la mera suscripción de la presente carta, que los recursos obtenidos para la presentación de la oferta y en caso de resultar adjudicatario, para la ejecución del contrato resultante del presente proceso, no se han obtenido de la celebración de ofertas de cesión de derechos económicos o de beneficiario con pacto de readquisición u operaciones de captación o recaudo masivo no autorizado de dineros del público o de entrega masiva de dineros a personas naturales o jurídicas directamente o través de intermediarios, mediante la operación de captación o recaudo en operaciones no autorizados tales como, pirámides, tarjetas prepago, venta de servicios y otras operaciones semejantes a cambio de bienes, servicios o rendimientos sin explicación financiera razonable. La suscripción del presente documento constituye prueba de nuestro compromiso de no participar en hechos que configuren los supuestos del recaudo no autorizado de dineros del público al tenor de lo dispuesto en el Decreto 1981 de 1988. En caso de Uniones Temporales o Consorcios, se entiende que con la suscripción de esta carta, todos y cada uno de sus miembros o integrantes efectuarán esta declaración.

Nuestra Dirección Comercial, a donde se puede remitir o enviar por correo, notificaciones o citaciones es la siguiente:

Persona de contacto	[Nombre]
Dirección	[Dirección de la compañía]
Teléfono	[Teléfono de la compañía]
e-mail	[Dirección de correo electrónico de la compañía]

[Firma representante legal del Proponente o del Proponente persona natural] Nombre: [Insertar información]
Cargo: [Insertar información]
Documento de Identidad: [Insertar información]
NIT: [Persona Jurídica]
Teléfono contacto: [insertar número telefónico o celular]
Dirección: [insertar dirección de notificación]
Email: [insertar correo electrónico de contacto].