ESTUDIO PREVIO

Puerto Gaitán, 11 de marzo de 2026

1- DESCRIPCIÓN DE LA NECESIDAD

La Constitución Política de Colombia, en su artículo 2°, establece los fines esenciales del Estado, entre los cuales se encuentran servir a la comunidad, promover la prosperidad general y garantizar la efectividad de los principios, derechos y deberes consagrados en la Constitución. Asimismo, se resalta la importancia de facilitar la participación ciudadana y asegurar la convivencia pacífica y la vigencia de un orden justo. En este contexto, las autoridades tienen la responsabilidad de proteger a las personas en su vida, honra, bienes y libertades, así como de asegurar el cumplimiento de sus deberes sociales.

El artículo 287 de la Constitución Política reconoce que las entidades territoriales gozan de autonomía para la gestión de sus intereses, incluyendo la administración de recursos y el establecimiento de medidas necesarias para el cumplimiento de sus funciones. Esta autonomía permite a los municipios tomar decisiones orientadas al fortalecimiento de su infraestructura y capacidades institucionales, dentro del marco constitucional y legal vigente.

En este sentido, el artículo 91, literal d, numeral 1 de la Ley 136 de 1994, establece como atribución del alcalde municipal dirigir la acción administrativa del municipio, asegurar el cumplimiento de sus funciones, garantizar la prestación de los servicios a su cargo y ejercer la ordenación del gasto. Esto implica la responsabilidad de adoptar medidas que aseguren el acceso a herramientas tecnológicas que permitan una gestión pública eficiente.

La Oficina de Tecnologías de la Información y las Comunicaciones (TIC), conforme a lo establecido en el artículo 7°, numeral 14 del Decreto N.° 0124 de 2025 expedido por la Alcaldía Municipal de Puerto Gaitán, desarrolla funciones orientadas a la administración integral de la infraestructura tecnológica institucional. En cumplimiento de esta responsabilidad, la Oficina gestiona la infraestructura de red y los sistemas corporativos existentes, así como aquellos que se incorporen en la administración central, lo que permite asegurar un funcionamiento coordinado, eficiente y alineado con las necesidades operativas de la Administración Municipal.

De igual manera, la Oficina TIC impulsa acciones dirigidas a fortalecer la disponibilidad de los servicios tecnológicos, promover la integridad de los datos institucionales y proteger la confidencialidad de la información procesada por las diversas dependencias. Con este propósito, implementa políticas, procedimientos y lineamientos técnicos que consolidan un entorno digital confiable, apoyado en mecanismos de monitoreo continuo, gestión de incidentes, administración de accesos, actualización permanente de componentes tecnológicos y controles de seguridad tanto perimetrales como internos.

En complemento a estas acciones, la Oficina orienta su labor al fortalecimiento progresivo de la **Política de Seguridad Digital de la entidad**, integrando estándares y buenas prácticas internacionales, entre ellos los lineamientos de la **Norma *ISO 27001***, que constituyen una guía esencial para el establecimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI). Este enfoque permite elevar la madurez institucional en materia de seguridad digital y facilita la adopción de procesos que respaldan la gestión del riesgo tecnológico en todos los niveles de operación.

Asimismo, la gestión de la Oficina TIC incorpora medidas específicas para la **salvaguarda de la información que se maneja en las zonas WiFi públicas del municipio**, dado que estos espacios amplían el acceso ciudadano a los servicios digitales y requieren esquemas robustos de protección que garanticen la integridad del tráfico, la protección de los usuarios y la continuidad del servicio. La administración adecuada de estas zonas fortalece la confianza digital y contribuye a un uso seguro de la infraestructura tecnológica dispuesta para la comunidad.

En conjunto, estas acciones consolidan a la Oficina TIC como un actor estratégico dentro de la Administración Municipal, ya que garantiza un funcionamiento tecnológico eficiente, seguro y confiable, elementos esenciales para el desarrollo de los procesos administrativos, misionales y de atención a la ciudadanía que dependen de la operación de los sistemas de información del Municipio de Puerto Gaitán.

La Alcaldía Municipal de Puerto Gaitán, actualmente cuenta con una (1) licencia para firewall físico de marca Hillstone Network referencia A2800. El firewall Hillstone A2800 actúa como la primera línea de defensa ante ciberamenazas. Actualmente, el dispositivo cuenta con un conjunto de servicios de seguridad (Cloud Sandbox, IPS, Antivirus, Antispam, etc.) cuya vigencia está programada para finalizar el 30 de marzo de 2026.

Servicio de Licencia actual	**Importancia para la Entidad**
Cloud Sandbox	Analiza archivos sospechosos en un entorno aislado en la nube antes de permitir su descarga. Bloquea ataques de "Día Cero" que aún no tienen una firma conocida.
APP Signature	Permite identificar y controlar qué aplicaciones (Facebook, WhatsApp, herramientas de gestión pública, etc.) circulan por la red, evitando el uso de aplicaciones no autorizadas.
URL DB (Filtrado Web)	Bloquea el acceso a sitios web maliciosos, de phishing o de contenido no productivo, protegiendo al personal de sitios que intentan robar credenciales.
IP Reputation	Mantiene una base de datos de direcciones IP que han sido identificadas como fuentes de ataques, bloqueando el tráfico desde o hacia estas antes de que interactúen con tu red.
Antispam	Filtra correos electrónicos maliciosos, evitando ataques de suplantación (phishing) que suelen llegar a los funcionarios por correo.
Botnet C&C Prevention	Detecta si un dispositivo dentro de la alcaldía ha sido infectado y está intentando comunicarse con un servidor externo (servidor de comando y control) para recibir instrucciones maliciosas.
IPS (Prevención de Intrusiones)	Es el corazón de la defensa. Escanea el tráfico en busca de patrones de ataque conocidos contra vulnerabilidades de software.
Anti-Virus	Inspecciona los archivos que atraviesan la red en busca de virus, troyanos y malware conocido, deteniéndolos antes de que lleguen a los equipos finales.

La no renovación de estos servicios implica un riesgo crítico para la entidad, debido a que:

- Obsolescencia de la base de datos de amenazas: Sin la suscripción, el firewall dejará de recibir firmas actualizadas contra virus, exploits y nuevas variantes de malware, quedando la red expuesta a vectores de ataque modernos.
- Incapacidad de análisis avanzado: La pérdida de servicios como Cloud Sandbox y Botnet C&C Prevention deja a la red desprotegida frente a ataques de día cero y comunicaciones maliciosas que intentan exfiltrar información institucional.
- Incumplimiento de estándares de seguridad: La falta de un sistema de protección activo contraviene las políticas de seguridad de la información y normativas vigentes sobre la protección de activos digitales del Estado.

La actualización de los servicios de suscripción y el soporte técnico especializado son requisitos transversales e ineludibles para la operatividad de la seguridad perimetral de la Alcaldía. Dado que la arquitectura de amenazas cibernéticas evoluciona de manera exponencial, el componente de hardware por sí solo resulta insuficiente si no cuenta con las actualizaciones de firmas y motores de análisis que proporcionan las licencias vigentes. Así mismo, la administración, parametrización de políticas, gestión de VPN y segmentación de red deben ser ejecutadas por personal certificado por el fabricante, garantizando que el despliegue técnico cumpla con las mejores prácticas internacionales de ciberseguridad y asegure la continuidad del servicio público sin interrupciones por malas configuraciones.

Así mismo se hace necesario la actualización de conocimientos con el fin de garantizar que el personal de la administración pueda desarrollar de forma autónoma actividades de configuración y parametrización de politicas de seguridad, y analizar las diferentes amenazas que se encuentran en el medio.

Actividades de transferencia de conocimiento a realizar:

Actividad	Descripción Técnica	Objetivo	Cantidad	Intensidad horaria
Taller de Configuración	Sesión práctica donde el experto configura una política real (ej. segmentación de red o VPN) bajo supervisión.	Aprender a operar el firewall en entorno controlado.	1	4 horas
Verificación y actualización de Firmware	Verificación actual y actualización del firmware llegado el caso que no se cuente con la última versión.	Conocer en donde se verifica el firmware, donde descargarlo y como instalarlo.	1	2 horas (programar ventana en caso de realizar actualización)
Simulación de Incidentes y como detectarlas	Ejercicio de "falla controlada" (ej. simular un ataque o caída de enlace) para probar la respuesta del firewall.	Asegurar que saben responder ante una emergencia.	2	2 horas
Elaboración de "Runbooks" (SOPs)	Creación de manuales paso a paso de procedimientos comunes (ej. "Cómo bloquear una IP" o "Cómo crear un usuario VPN").	Tener una guía de consulta rápida para el día a día.	1	Documento tipo manual

Evaluación de Competencias	Examen teórico-práctico al finalizar la transferencia para validar que el personal adquirió las habilidades.	Certificar la transferencia de conocimiento.	1	4 horas

Para la transferencia se debe cubrir obligatoriamente los siguientes temas en el acta de capacitación:

- **Gestión de Políticas y Objetos:** Cómo crear, modificar y eliminar reglas de firewall sin comprometer la seguridad.
- **Administración de VPN (SSL/IPSec):** Configuración de acceso remoto para funcionarios, gestión de certificados y autenticación de doble factor (MFA).
- **Monitoreo y Análisis de Logs:** Identificación de patrones sospechosos en el panel *Monitor* y uso de dashboard para reportes.
- **Gestión de Vulnerabilidades:** Cómo interpretar alertas del *Intrusion Prevention System (IPS)* y aplicar parches o excepciones.
- **Mantenimiento Preventivo:** Backup de archivos de configuración, actualización de firmas y gestión de licencias.

Es fundamental que el personal que realizará esta transferencia tenga **certificaciones vigentes de Hillstone** (ej. *HCNP* - Hillstone Certified Network Professional o superior), y uno de los ingenieros deberá aportar obligatoriamente carta de residencia del municipio de Puerto Gaitán - Meta, expedida conforme al documento establecido por la entidad territorial para acreditar dicha condición, con el fin de promover la generación de empleo local y contribuir a la dinamización de la economía del municipio.

La licencia asociada al dispositivo ofrece acceso continuo a motores especializados de análisis, bases de datos actualizadas de firmas de amenazas, reglas avanzadas de inspección, parches de seguridad y soporte técnico profesional del fabricante. Dado que esta licencia se encuentra programada para finalizar en marzo de 2026, su renovación promueve la continuidad de la protección perimetral, la evolución de los mecanismos de defensa y la estabilidad del sistema de seguridad que respalda los servicios institucionales.

Además, la licencia permite que el firewall incorpore capacidades actualizadas frente al panorama cambiante de ciberamenazas, fortaleciendo los procesos de detección temprana, respuesta oportuna, análisis forense y trazabilidad de eventos. Con ello, la infraestructura tecnológica del municipio mantiene un comportamiento estable ante la aparición de vulnerabilidades críticas, variantes de malware, ataques automatizados y nuevas técnicas de intrusión. Asimismo, la asistencia oficial del fabricante facilita la aplicación de actualizaciones, correcciones especializadas, optimización de rendimiento y soporte frente a incidentes que requieran intervención técnica avanzada.

En consecuencia, se hace necesario adelantar el proceso contractual correspondiente, bajo las especificaciones técnicas definidas por la Oficina de Tecnologías de la Información y las Comunicaciones, garantizando la protección de la infraestructura tecnológica institucional, en cumplimiento de la meta PDM0024: Implementar estrategias para fortalecer las Tecnologías de la Información y las Comunicaciones (TIC) del municipio de Puerto Gaitan, establecida en el Plan de Desarrollo Municipal "Juntos Lo Hacemos Posible 2024-2027", código del producto: Servicio de Información implementado 2301075, indicador del producto: Sistemas de información implementados 230107500.

Lo anterior, se encuentra incluido dentro del Plan Anual de Adquisiciones de la Oficina de Tecnologías de la Información y las Comunicaciones - vigencia 2026, conforme se observa en el certificado de plan de compras No. 2026000770 expedido el 10 de marzo de 2026, y los recursos se encuentran amparados por el rubro presupuestal del cual se derivan estos recursos, así: RUBRO PRESUPUESTAL: 1-AC-1-2301-0400-2301075, fuente 1.2.1.0.00-I.C.L.D.

Este proceso cuenta así mismo cuenta con el certificado de disponibilidad presupuestal No. 2026000954 expedido el día 10 de marzo de 2026, por valor de **OCHENTA MILLONES DE PESOS ($80.000.000) M/CTE.**

2- DESCRIPCIÓN DEL OBJETO A CONTRATAR, ESPECIFICACIONES ESENCIALES E IDENTIFICACION DEL CONTRATO A CELEBRAR

OBJETO: "RENOVACIÓN, REPARAMETRIZACIÓN, SOPORTE Y PUESTA EN MARCHA DEL LICENCIAMIENTO FIREWALL PARA LA INFRAESTRUCTURA TECNOLÓGICA DE LA ALCALDÍA MUNICIPAL DE PUERTO GAITÁN - META".

Se requiere la contratación de los siguientes ítems:

ÍTEM	CÓDIGO U.N.S.P.S.C.	DESCRIPCIÓN	CANT.
1	43233200	Software de seguridad y protección	1
2	43232800	Software de administración de redes	

Fuente: https://operaciones.colombiacompra.gov.co/clasificador-de-bienes-y-servicios

A. IDENTIFICACIÓN O CLASE DE CONTRATO A CELEBRAR:

Contrato de suministro.

3- CONDICIONES TÉCNICAS EXIGIDAS

3.1 ESPECIFICACIONES TÉCNICAS

ÍTEM	TIPO	DESCRIPCIÓN	CANTIDAD
1	LICENCIA FIREWALL Licencia del dispositivo Firewall	LICENCIA FIREWALL A2800 por 3 años, con las siguientes características: • Type: Effective License • ZTNA • VSYS • QoS • SSL VPN • Cloud sandbox • APP signature • URL DB • IP Reputation • Antispam • Botnet C&C Prevention	1

		• Intrusion Prevention System • Anti-Virus • Platform	
2	SOPORTE Y TRANSFERENCIA DE CONOCIMIENTO	- Realizar trasferencia de conocimiento por mínimo 12 horas, con personal certificado, y entrega de un documento paso a paso de actividades recurrentes que se implementan en el firewall.	1
3	REPARAMETRIZACIÓN DE POLITICAS Y CONFIGURACIONES	- **Gestión de Políticas y Objetos** - **Administración de VPN (SSL/IPSec)** - **Monitoreo y Análisis de Logs** - **Gestión de Vulnerabilidades** - **Mantenimiento Preventivo**	1

3.2 EXPERIENCIA MÍNIMA DEL PROPONENTE

El proponente deberá anexar a su oferta una (1) certificación de contrato debidamente iniciado o ejecutado, con el que acredite la experiencia en objeto similar al del presente proceso de contratación, expedida por entidades públicas, privadas o particulares, cuyo valor sea igual o superior al presupuesto oficial expresado en SMLMV (45,69 SMLMV) y que haya sido suscrito dentro de los tres (3) años anteriores a la fecha del cierre del presente proceso.

Dicha experiencia se deberá acreditar con la respectiva copia del contrato y copia del acta de liquidación o certificación expedida por el contratante, la cual deberá estar debidamente suscrita por el contratante, en el evento de que en alguno o algunos de los contratos no se acredite con los soportes antes solicitados estos contratos no se tendrán en cuenta para la habilitación.

La experiencia deberá ser demostrada por medio de una certificación (expedida por el representante legal o funcionario competente) o copia del contrato debidamente acompañado del acta de liquidación, documentos que deberán contener lo siguiente:

- Número de contrato
- Objeto del contrato
- Datos del Contratante y del Contratista
- Identificación
- Dirección
- Teléfono
- Correo electrónico de quien certifica
- Nombre e identificación de quien es certificado
- Valor final del contrato
- Fecha de inicio y finalización

Si el contrato se suscribió en Consorcio o Unión Temporal, se deberá indicar el porcentaje de participación y acreditarlo mediante copia del acuerdo consorcial o el acuerdo de unión temporal o con la certificación correspondiente.

El contrato que incumpla el requisito anterior no será tenido en cuenta para la evaluación.

Experiencia entre particulares: Para efectos de acreditación de experiencia entre particulares, el Proponente deberá adicionalmente aportar los documentos que se describen a continuación:

- Certificación del contrato celebrado entre las partes, el cual deberá estar suscrito por el revisor fiscal o contador público del Proponente que acredita la experiencia, con la copia de la tarjeta profesional del contador público o revisor fiscal (según corresponda) y certificado de antecedente disciplinarios vigente, expedido por la Junta Central de Contadores, o los documentos equivalentes que hagan sus veces en el país donde se expide el documento del profesional.
- El proveedor de servicios o bienes que se encuentre obligado a facturar electrónicamente deberá aportar la(s) factura(s) expedida(s) con cargo al contrato que acredita la experiencia.

3.3 ESPECIFICACIONES TÉCNICAS DE CARÁCTER OBLIGATORIO PARA LA TRANSFERENCIA DE CONOCIMIENTO

El oferente deberá acreditar que cuenta con el siguiente personal idóneo:

1. Ingeniero Especialista:

Requisito	Detalle Mínimo
Formación Académica	• Título profesional en Ingeniería de Sistemas, Electrónica, Telecomunicaciones o afines. • Título en especialización de la seguridad de la información y Certificación de Estándares: ISO/IEC 27001:2022 Foundation vigente.
Experiencia General	Mínimo cinco (5) años de experiencia certificada en el área de infraestructura tecnológica, redes o sistemas.
Experiencia Específica	Mínimo tres (3) años en administración o implementación de soluciones de seguridad perimetral.
Certificaciones.	HCSA-NGFW (Hillstone Certified Security Associate) e ISO/IEC 27001:2022 Foundation, vigentes a la fecha.
Documental	- Copia de la cédula de ciudadanía. - Acreditación de estudios (diploma y acta de grado) cuando aplique. - Tarjeta profesional (si aplica). - Certificado vigencia de matrícula y antecedentes profesionales (si aplica). - Certificado de antecedentes judiciales, disciplinarios y fiscales, medidas correctivas, REDAM e inhabilidad de delitos sexuales. - Acreditación de Experiencia Laboral.

	- Acreditación de Experiencia Específica.

2. Ingeniero Especialista:

Requisito	Detalle Mínimo
Formación Académica	• Título profesional en Ingeniería de Sistemas, Electrónica, Telecomunicaciones o afines. • Título de especialización en Gerencia de Proyectos.
Experiencia General	Mínimo cinco (5) años de experiencia certificada en el área de infraestructura tecnológica, redes o sistemas.
Documental	- Copia de la cédula de ciudadanía. - Acreditación de estudios (diploma y acta de grado) cuando aplique. - Tarjeta profesional (si aplica). - Certificado vigencia de matrícula y antecedentes profesionales (si aplica). - Certificado de antecedentes judiciales, disciplinarios y fiscales, medidas correctivas, REDAM e inhabilidad de delitos sexuales. - Acreditación de Experiencia Laboral.

3. Ingeniero:

Requisito	Detalle mínimo
Formación Académica	• Título profesional en Ingeniería de Sistemas, Electrónica, Software, Telecomunicaciones o afines. • Título de tecnólogo en desarrollo de sistemas de información y redes.
Certificaciones	Certificado de residencia del municipio de Puerto Gaitán - Meta, vigente.
Documental	- Copia de la cédula de ciudadanía. - Acreditación de estudios (diploma y acta de grado) cuando aplique. - Tarjeta profesional (si aplica). - Certificado vigencia de matrícula y antecedentes profesionales (si aplica). - Certificado de antecedentes judiciales, disciplinarios y fiscales, medidas correctivas, REDAM e inhabilidad de delitos sexuales.

Actividades Técnicas de Renovación: Los profesionales serán responsables de ejecutar las siguientes tareas para asegurar la continuidad de la protección:

- Gestión de Licenciamiento: Realizar la carga, activación y verificación de las suscripciones de seguridad (IPS, AV, URL Filtering, Cloud Sandboxing) en el chasis del Firewall.
- Actualización de Firmas y Software: Ejecutar la actualización del sistema operativo a la versión recomendada por el fabricante para habilitar las últimas protecciones contra amenazas.
- Auditoría de Políticas (Compliance): Revisar la matriz de reglas de acceso para asegurar que se alineen con los controles del Sistema de Gestión de Seguridad de la Información (SGSI) bajo la norma ISO 27001.

- Optimización de Rendimiento: Ajustar los parámetros de inspección de tráfico y seguridadpara maximizar la eficiencia del hardware actual.
- Pruebas de Conectividad y Seguridad: Validar que los servicios críticos de la entidad (ej. conexiones 10GbE SFP+ o 2.5GbE) mantengan su operatividad tras la aplicación de las nuevas licencias.
- Informe Técnico de Cierre: Entrega de un documento que detalle el estado final de las suscripciones, fechas de vencimiento y recomendaciones de seguridad para el próximo periodo.
- Protección Avanzada: Socializar las mejoras en la detección de Ransomware y el uso de Snapshots o herramientas de recuperación integradas en la solución.

Actividades de transferencia de conocimiento a realizar:

Actividad	Descripción Técnica	Objetivo	Cantidad	Intensidad horaria
Taller de Configuración	Sesión práctica donde el experto configura una política real (ej. segmentación de red o VPN) bajo supervisión.	Aprender a operar el firewall en entorno controlado.	1	12 horas
Verificación y actualización de Firmware	Verificación actual y actualización del firmware llegado el caso que no se cuente con la última versión	Conocer en donde se verifica el firmware, donde descargarlo y como instalarlo.	1	6 horas (programar ventana en caso de realizar actualización)
Simulación de Incidentes y como detectarlas	Ejercicio de "falla controlada" (ej. simular un ataque o caída de enlace) para probar la respuesta del firewall.	Asegurar que saben responder ante una emergencia.	2	6 horas
Elaboración de "Runbooks" (SOPs)	Creación de manuales paso a paso de procedimientos comunes (ej. "Cómo bloquear una IP" o "Cómo crear un usuario VPN").	Tener una guía de consulta rápida para el día a día.	1	Documento tipo manual
Evaluación de Competencias	Examen teórico-práctico al finalizar la transferencia para validar que el personal adquirió las habilidades.	Certificar la transferencia de conocimiento.	1	4 horas

Para la transferencia se debe cubrir obligatoriamente los siguientes temas en el acta de capacitación:

- **Gestión de Políticas y Objetos:** Cómo crear, modificar y eliminar reglas de firewall sin comprometer la seguridad.

- **Administración de VPN (SSL/IPSec):** Configuración de acceso remoto para funcionarios, gestión de certificados y autenticación de doble factor (MFA).

- **Monitoreo y Análisis de Logs:** Identificación de patrones sospechosos en el panel *Monitor* y uso de dashboard para reportes.

- **Gestión de Vulnerabilidades:** Cómo interpretar alertas del *Intrusion Prevention System (IPS)* y aplicar parches o excepciones.

- **Mantenimiento Preventivo:** Backup de archivos de configuración, actualización de firmas y gestión de licencias.

Es fundamental que el personal que realizará esta transferencia tenga **certificaciones vigentes de Hillstone** (ej. *HCNP* - Hillstone Certified Network Professional o superior).

4- VALOR ESTIMADO DEL CONTRATO

El presupuesto oficial estimado para la presente contratación es de **OCHENTA MILLONES DE PESOS ($80.000.000) M/CTE.**

Los precios unitarios promedio obtenidos del estudio de mercados son los siguientes:

ITEM	DESCRIPCION	CANT	CONVIEST S.A.S.				ITT SUPPLIES S.A.S.				SDT S.A.S.				PROMEDIO			
			VALOR UNITARIO ANTES DE IVA	IVA	VALOR UNITARIO INCLUIDO IVA	VALOR PARCIAL	VALOR UNITARIO ANTES DE IVA	IVA	VALOR UNITARIO INCLUIDO IVA	VALOR PARCIAL	VALOR UNITARIO ANTES DE IVA	IVA	VALOR UNITARIO INCLUIDO IVA	VALOR PARCIAL	VALOR UNITARIO ANTES DE IVA	IVA	VALOR UNITARIO INCLUIDO IVA	VALOR PARCIAL
FIREWALL	Suministro e instalación de LICENCIA para FIREWALL A2800 por 3 años, con las siguientes caracteristicas: -Type: Effective License -ZTNA -VSYS -QoS -SSL VPN -Cloud sandbox -APP signature -URL DB -IP Reputation -Antispam -Botnet C&C Prevention -Intrusion Prevention System -Anti-Virus -Platform	1	$ 40.300.000,00	$ 7.657.000,00	$ 47.957.000,00	$ 47.957 000,00	$ 40.200.000,00	$ 7.638.000,00	$ 47.838.000,00	$ 47.838 000,00	$ 39.800.000,00	$ 7.562.000,00	$ 47.362.000,00	$ 47.362.000,00	$ 40.100.000,00	$ 7.619.000,00	$ 47.719.000,00	$ 47.719.000,00
SOPORTE Y TRANSFERENCIA DE CONOCIMIENTO	transferencia de conocimiento por mínimo 12 horas, con personal certificado, y entrega de un documento paso a paso de actividades recurrentes que se implementan en el firewall	1	$ 17.000.000,00	$ 3.230.000,00	$ 20.230.000,00	$ 20.230 000,00	$ 17.100.000,00	$ 3.249.000,00	$ 20.349.000,00	$ 20.349 000,00	$ 17.200.000,00	$ 3.268.000,00	$ 20.468.000,00	$ 20.468.000,00	$ 17 100 000,00	$ 3.249.000,00	$ 20.349.000,00	$ 20.349 000,00
REPARAMETRIZACION DE POLITICAS Y CONFIGURACIONES	-Gestión de Políticas y Objetos -Administración de VPN (SSL/IPSec) -Monitoreo y Análisis de Logs -Gestión de Vulnerabilidades -Mantenimiento Preventivo	1	$ 10.090.672,27	$ 1.917.227,73	$ 12.007.900,00	$ 12.007 900,00	$ 10.090.000,00	$ 1.917.100,00	$ 12.007.100,00	$ 12.007 100,00	$ 9.900.000,00	$ 1.881.000,00	$ 11.781.000,00	$ 11 781 000,00	$ 10 026 890,76	$ 1.905 109,24	$ 11 932.000,00	$ 11 932.000,00
TOTAL VALOR ANTES DE IVA						$ 67 390 672,27	TOTAL VALOR ANTES DE IVA			$ 67 390 000,00	TOTAL VALOR ANTES DE IVA			$ 66 900 000,00	TOTAL VALOR ANTES DE IVA			$ 67 226 890,76
IVA						$ 12 804 227 73	IVA			$ 12 804 100,00	IVA			$ 12 711 000,00	IVA			$ 12 773 109,24
VALOR TOTAL						$ 80 194 900,00	VALOR TOTAL			$ 80 194 100,00	VALOR TOTAL			$ 79 611 000,00	VALOR TOTAL			$ 80 000 000,00

VALOR TOTAL DEL PROCESO: OCHENTA MILLONES DE PESOS ($80.000.000) M/CTE.

4.1. FORMA DE PAGO: El Municipio se compromete a efectuar DOS (2) PAGOS parciales mensuales al contratista, de acuerdo con el valor efectivamente ejecutado, conforme a los bienes y servicios suministrados, y recibidos a satisfacción por parte del supervisor del contrato. Dicho pago se realizará con base en los precios unitarios ofertados por el contratista en su propuesta económica, previa presentación de la factura de venta o cuenta de cobro si le aplica, certificación de recibo a satisfacción por parte del supervisor, soportes de ingreso a

almacén de los elementos suministrados, certificación de cumplimiento, informe del contratista, informe del supervisor y soporte de pago de obligaciones de salud y parafiscales cuando corresponda.

Los proponentes y los contratistas deberán acreditar que se encuentran al día en el pago de aportes parafiscales relativos al Sistema de Seguridad Social Integral, así como los propios del Sena, ICBF y Cajas de Compensación Familiar, teniendo en cuenta el régimen tributario y legal que le aplique al contratista, con relación a estos sistemas.

5. INDICAR SI APLICA O NO LA CONVOCATORIA PARA LIMITACIÓN A MIPYMES.

De conformidad con lo establecido en el parágrafo 1° del artículo 30 y el artículo 34 de la Ley 2069 de 2020, en concordancia con el artículo 2.2.1.2.4.2.2 y ss. del Decreto 1082 de 2015, la presente convocatoria será limitada a mipymes colombianas que acrediten como mínimo un (1) año de existencia, teniendo en cuenta que el valor del proceso de Contratación es menor a ciento veinticinco mil dólares de los Estados Unidos de América (US$125.000).

6. TIPIFICACIÓN, ESTIMACIÓN Y ASIGNACIÓN DE RIESGOS PREVISIBLES

No.	Riesgo	Etapa del proceso	Descripción	Causa	Consecuencia	Probabilidad	Impacto	Nivel de riesgo	Tratamiento / Medidas de manejo	Responsable
1	Incompatibilidad del licenciamiento	Ejecución	El licenciamiento del firewall no es compatible con la infraestructura tecnológica existente	Falta de validación técnica previa	No se logra la puesta en marcha del firewall	Media	Alta	Alto	Validación técnica previa, fichas técnicas y aprobación del supervisor	Contratista
2	Configuración incorrecta del firewall	Ejecución	La reparametrización del firewall es deficiente	Falta de idoneidad del personal técnico	Vulnerabilidades de seguridad informática	Media	Alta	Alto	Exigir personal certificado y pruebas de funcionamiento	Contratista
3	Interrupción del servicio tecnológico	Ejecución	Suspensión temporal de servicios durante la puesta en marcha	Mala planeación de la implementación	Afectación de servicios institucionales	Media	Media	Medio	Implementación en ventanas de mantenimiento y plan de	Compartido

									contingencia	
4	Persistencia de vulnerabilidades	Ejecución	El firewall no mitiga adecuadamente los riesgos de seguridad	Configuración incompleta o licencias limitadas	Riesgo de ataques y pérdida de información	Media	Alta	Alto	Pruebas de seguridad y acta de aceptación técnica	Contratista
5	Incumplimiento contractual	Ejecución	El contratista no cumple las obligaciones pactadas	Desconocimiento del alcance contractual	Retrasos o terminación anticipada	Baja	Media	Medio	Supervisión permanente y control del cronograma	Contratista
6	Deficiente estructuración del proceso	Planeación	Errores en el análisis previo del contrato	Documentación incompleta	Observaciones de entes de control	Baja	Alta	Medio	Aplicación estricta del Decreto 1082 y lineamientos CCE	Entidad

7. PLAZO DE EJECUCIÓN DEL CONTRATO

El plazo de ejecución del contrato será de DOS (2) MESES, contados a partir de la firma del acta de inicio la cual se suscribirá cuando se haya expedido el registro presupuestal y se hayan aprobado las garantías.

El lugar de ejecución del contrato será en la Alcaldía Municipal de Puerto Gaitán – Meta.

8. DISPONIBILIDAD PRESUPUESTAL

El Municipio de Puerto Gaitán cuenta con la disponibilidad presupuestal No. 2026000954 expedido el día 10 de marzo de 2026, por valor de **OCHENTA MILLONES DE PESOS ($80.000.000) M/CTE.**

9. GENERALIDADES DEL CONTRATO

A. EXIGENCIA DE GARANTÍAS

De acuerdo con lo anterior y en cumplimiento a lo señalado en el Decreto 1082 de 2015, el contratista favorecido con la futura contratación deberá constituir una garantía única a favor del municipio de Puerto Gaitán con los siguientes amparos:

GARANTÍA	VALOR (%)	DURACIÓN
Seriedad de la	Diez por ciento (10%) del	Desde la presentación de la oferta y hasta la aprobación de la

oferta	valor total del contrato.	garantía de cumplimiento del contrato (según artículo 2.2.1.2.3.1.9 del Decreto 1082 de 2015).
Cumplimiento	Diez por ciento (10%) del valor total del contrato.	La del contrato y hasta su liquidación; (según artículo 2.2.1.2.3.1.7. del decreto 1082 de 2015) hasta por cuatro (4) meses más.
Calidad del bien o servicio.	Veinte por ciento (20%) del valor total del contrato.	Por el término de duración del contrato (según artículo 2.2.1.2.3.1.1.6. del decreto 1082 de 2015) y dos (02) años más.
Pago de salarios y prestaciones sociales	Cinco por ciento (5%) del valor total del contrato.	Por el término de duración del contrato y tres (3) años más, según artículo 2.2.1.2.3.1.13 del Decreto 1082 de 2015)

Requisitos de la póliza o garantía:

a. Asegurado o beneficiario: MUNICIPIO DE PUERTO GAITÁN.
b. Tomador / Afianzado: Sí el proponente es una persona jurídica, la póliza o garantía deberá tomarse con el nombre o razón social que figura en el Certificado de Existencia y Representación Legal expedido por la Cámara de Comercio respectiva, y no sólo con su sigla, a no ser que en el referido documento se exprese que la sociedad podrá denominarse de esa manera.
c. Cuando la propuesta se presente en consorcio o unión temporal, la póliza deberá tomarse a nombre de todos y cada uno de sus integrantes, y no a nombre de los representantes legales, ni a nombre del consorcio o unión temporal.
d. Firmas: La póliza ineludiblemente deberá estar firmada por el representante legal o autorizado de la Compañía o Entidad Bancaria que la expide y por el tomador.
e. Acompañarse del Recibo de pago o Constancia de Ley.
f. No se aceptan pólizas expedidas por Aseguradoras que hayan sido intervenidas.

Dentro de los cinco (5) días siguientes a la suscripción del contrato, el CONTRATISTA se compromete a constituir a favor del MUNICIPIO DE PUERTO GAITAN y a satisfacción de este, la Garantía de Cumplimiento de las obligaciones requerida para la ejecución del contrato.

El Contratista deberá aportar las pólizas debidamente suscritas y en original y su correspondiente recibo de pago deberá ser aportado en original, so pena de que la misma no sea aprobada por el Municipio y suscrita por el Representante legal de la persona jurídica o el proponente plural o persona natural según sea el caso (Contratista).

B. OBLIGACIONES DE LAS PARTES:

DEL CONTRATISTA:

1. Renovar la licencia del dispositivo de seguridad perimetral (Firewall) conforme a las especificaciones técnicas definidas por la Oficina de Tecnologías de la Información y las Comunicaciones.
2. Garantizar la continuidad de los servicios asociados al firewall, incluyendo:
   - Actualizaciones de firmware.
   - Actualizaciones de bases de datos de seguridad.

- Servicios de prevención de intrusiones (IPS), filtrado web, control de aplicaciones y demás funcionalidades licenciadas.
- Type: Effective License
- ZTNA
- VSYS
- QoS
- SSL VPN
- Cloud sandbox
- APP signature
- URL DB
- IP Reputation
- Antispam
- Botnet C&C Prevention
- Intrusion Prevention System
- Anti-Virus
- Platform

3. Asegurar que no exista interrupción en la protección perimetral durante el proceso de renovación.
4. Realizar la activación, validación y verificación del correcto licenciamiento del equipo.
5. Brindar acompañamiento técnico remoto o presencial (si aplica) para la verificación del correcto funcionamiento posterior a la renovación.
6. Entregar certificado de vigencia y soporte oficial expedido por el fabricante durante el período requerido de la licencia (3 años).
7. Realizar la transferencia de conocimiento al personal de la Oficina de Tecnologías de la Información y las Comunicaciones de la Alcaldía Municipal de Puerto Gaitán, atendiendo los ejes temáticos e intensidad horaria dispuesta, y expidiendo el acta respectiva.
8. Crear el documento tipo manual de Elaboración de "Runbooks" (SOPs), donde se describa el paso a paso de procedimientos comunes (ej. "Cómo bloquear una IP" o "Cómo crear un usuario VPN").
9. Ejecutar la reparametrizacion de políticas y configuraciones en el dispositivo de seguridad perimetral firewall con su mantenimiento preventivo.

DEL MUNICIPIO:

1. Suministrar oportunamente la información necesaria para el óptimo desarrollo del contrato.
2. Constituir el registro presupuestal que garantice el giro de los recursos de contrato.
3. Cancelar el valor pactado en el contrato en las condiciones establecidas siempre y cuando el supervisor certifique el cumplimiento del objeto contractual.
4. Designar un funcionario para que supervise la ejecución del contrato.
5. Revisar cada uno de los informes de actividades realizados durante la ejecución del contrato.
6. Exigir al contratista ejercer cada una de sus actividades aplicando los valores de transparencia, responsabilidad, celeridad y lealtad.
7. Exigir al contratista cumplir con la totalidad de las obligaciones con el sistema de seguridad social integral, de acuerdo con la normatividad vigente.
8. Exigir al contratista que para el pago se deberá anexar soporte del cumplimiento de sus obligaciones con el Sistema de Seguridad Social Integral., en la forma establecida en el ordenamiento jurídico.

Requerir al contratista, para que adopte las medidas correctivas pertinentes cuando surjan falla en el cumplimiento del objeto contractual.

C. SUPERVISIÒN:

Teniendo en cuenta las características del servicio a contratar y dado que el mismo atañe a las funciones propias de la Oficina de Tecnologías de la Información y las Comunicaciones se sugiere que la supervisión del contrato sea efectuada por el Jefe de Oficina de Tecnologías de la Información y las Comunicaciones, o en su defecto quien el ordenador del gasto o su delegado designe para tal fin. El supervisor deberá cumplir los roles señalados en la ley 1474 de 2011 y en el Manual de Contratación del Municipio de Puerto Gaitán, así como los señalados en los pliegos de condiciones del proceso de selección.

JOHN FERNEY FONTECHA MENDOZA
Jefe de Oficina de Tecnologías de la Información y las Comunicaciones

Elaboró: Maryori Stefan Silva Arevalo	Revisó: John Ferney Fontecha Mendoza	Aprobó: John Ferney Fontecha Mendoza
Cargo: Profesional Especializado CPS 0090 de 2026	Cargo Jefe Oficina de Tecnologías de la Información y las Comunicaciones	Cargo: Jefe Oficina de Tecnologías de la Información y las Comunicaciones