DIRIGIDO A	**MAYELY GALAN BAUTISTA** Secretaria Administrativa
SECRETARÍA Y/O OFICINAS GESTORAS	**FREDDY ALEXANDER LEON NEIRA** Asesor TIC Proceso de Gestión de las TIC
FECHA DE ELABORACIÓN	julio 28 de 2026

1. JUSTIFICACION DE LA NECESIDAD

La Constitución Política en su artículo 311 establece que el Municipio como entidad fundamental de la división político-administrativa del estado le corresponde prestar los servicios públicos que determine la ley, así mismo en su artículo 354, establece que los servicios son inherentes a la finalidad social del Estado y que es deber del Estado asegurar su prestación eficiente a todos los habitantes del territorio nacional.

Por otra parte, el artículo 2° de nuestra Carta Magna, señala que son fines esenciales del Estado, entre otros: "… servir a la comunidad, promover la prosperidad general y garantizar la efectividad de los principios, derechos y deberes consagrados en la Constitución; facilitar la participación de todos en las decisiones que los afectan y en la vida económica, política, administrativa y cultural de la Nación; defender la independencia nacional, mantener la integridad territorial y asegurar la convivencia pacífica y la vigencia de un orden justo.(…)".

En concordancia con lo anterior, el artículo 209 superior advierte que la función administrativa está al servicio de los intereses generales y que "…Las autoridades administrativas deben coordinar sus actuaciones para el adecuado cumplimiento de los fines del Estado. La administración pública, en todos sus órdenes, tendrá un control interno que se ejercerá en los términos que señale la ley".

De acuerdo con esto y en lo que respecta a la contratación estatal, la ley 80 de 1993 "Por la cual se expide el Estatuto General de Contratación de la Administración Pública" en su artículo 3, dispuso:
"*ARTÍCULO 3o. DE LOS FINES DE LA CONTRATACIÓN ESTATAL. Los servidores públicos tendrán en consideración que al celebrar contratos y con la ejecución de los mismos, las entidades buscan el cumplimiento de los fines estatales, la continua y eficiente prestación de los servicios públicos y la efectividad de los derechos e intereses de los administrados que colaboran con ellas en la consecución de dichos fines.*
Los particulares, por su parte, tendrán en cuenta al celebrar y ejecutar contratos con las entidades estatales que colaboran con ellas en el logro de sus fines y cumplen una función social que, como tal, implica obligaciones."

De otra parte, a la Secretaría Administrativa del Municipio de Bucaramanga, en cumplimiento de la facultad residual delegada mediante Decreto 0041 de fecha 20 de febrero de 2025, le corresponde específicamente: "
"ARTÍCULO 4°. DELEGACIONES ESPECÍFICAS AL SECRETARIO (A) ADMINISTRATIVO. Celebrar todos los contratos y convenios imputables a gastos de funcionamiento. Además, le corresponde la facultad residual, entendiéndose por tal, la celebración de contratos y convenios que no correspondan a ningún de los casos que sean expresamente designados o delegados a otros despachos.

PARÁGRAFO. Sin perjuicio de las delegaciones que en materia de contratación de Obra Pública se confían al Secretario (a) de Infraestructura, le corresponderá al Secretario (a) Administrativo o quien haga sus veces, la competencia para adelantar y celebrar los contratos que impliquen actividades de mantenimiento, conservación, reparación o instalación en los bienes inmuebles destinados para el funcionamiento de la Alcaldía Municipal."

En tal sentido el proceso de Gestión de las TIC tiene como objetivo principal liderar la gestión estratégica de las tecnologías de la información y las comunicaciones en la Administración Municipal mediante la definición, implementación y mantenimiento de un modelo de arquitectura de TI integrando las estrategias de gobierno electrónico y normatividad vigente asociada al sector TIC, para el beneficio de la gestión institucional y la ciudadanía. Así mismo, el Asesor asignado

al referido proceso tiene la obligación de desarrollar y cumplir las funciones que se encuentran consignadas en el manual de funciones del Municipio de Bucaramanga adoptado mediante Decreto 066 de 2018 modificado por el Decreto 025 de fecha 20 de enero de 2020, que se relacionan a continuación:

"1. Liderar la gestión estratégica de las tecnologías de la información y las comunicaciones en la Administración Municipal mediante la definición, implementación y mantenimiento de un modelo de arquitectura de TI, conforme a normas y procedimientos establecidos.
2. Establecer estudios técnicos de implementación de TIC con su respectivo presupuesto y el manejo de la información siguiendo especificaciones técnicas.
3. Definir políticas de seguridad informática según estándares internacionales y políticas institucionales.
4. Realizar análisis de riesgos de seguridad informática, definiendo el plan de mitigación para los mismos.
5. Administrar la infraestructura de seguridad y custodia de la información, según procedimientos establecidos.
6. Participar en la elaboración y seguimiento del presupuesto anual de inversiones en TIC, teniendo en cuenta las directrices institucionales y los recursos disponibles."

De acuerdo con lo anterior y con el ánimo de garantizar una gestión estratégica de las Tecnologías de la Información en el Municipio, el Proceso de Gestión de las TIC observando su deber funcional y misional, diseñó e implementó un Plan Estratégico de Tecnologías de la Información -PETI- que está alineado con el mapa de procesos y el Modelo Integrado de Planeación y Gestión del Municipio de Bucaramanga con un enfoque de generación de valor público, que agrupa las oportunidades de mejoramiento de los interesados en lo relacionado con la gestión de TI para apoyar la estrategia y el modelo operativo de la organización apoyados en los lineamientos de la Política de Gobierno la cual de acuerdo al decreto 767 de 2022 se basa en una estrategia de gobernanza fundamentada en cinco (5) aspectos como son: sector privado, academia civil, ciudadanos, sociedad civil y entidades públicas. Este modelo de gobernanza esta apalancado por un concepto de innovación pública que incluye además de las líneas de acción e iniciativas dinamizadoras, cuatro (4) habilitadores que enuncian las capacidades que permiten ejecutar las Líneas de Acción de la Política de Gobierno Digital, los cuales son: Arquitectura, Cultura y apropiación, **seguridad y privacidad** de la información y servicios ciudadanos digitales, bajo ese marco se contempla como servicio TI la ***Seguridad de la Información*** que permite la identificación de parámetros de seguridad y realización de proceso que garanticen la seguridad, disponibilidad y confiabilidad de la información de la Entidad, así mismo contempla en el catálogo de servicios de infraestructura de TI la ***Seguridad de la información*** como el servicio consistente en ***Brindar la administración y operación de la seguridad de la información para los servicios TI acorde a las necesidades definidas en política de seguridad de la información de la Alcaldía de Bucaramanga***.

Los procesos funcionales de cada área requieren que la oficina TIC cuente con capacidades técnicas, operativas y estratégicas, que le permitan asegurar el uso continuo de herramientas, soluciones, plataformas e insumos tecnológicos. Todo ello con el fin de garantizar el funcionamiento normal de la Entidad y el cumplimiento de sus fines esenciales. En ese sentido, se han definido las siguientes estrategias:

1. *Aumentar la capacidad de soporte requerida por la plataforma tecnológica (hardware y software) para atender la demanda de solicitudes por parte de funcionarios y ciudadanos con la conformación de un equipo interdisciplinario.*
2. *Lograr con el uso de las TIC una administración, eficiente, transparente y participativa.*
3. *Mejorar sustancialmente el proceso de planeación para garantizar el cumplimiento de las metas del plan de desarrollo.*
4. *Ampliar el alcance estratégico de la oficina TIC mediante el soporte, gestión e implementación de la plataforma tecnológica en beneficio de los usuarios internos y los ciudadanos.*
5. *Fomentar la apropiación tecnológica en la Administración central y los ciudadanos.*
6. *Generar estrategias de apropiación tecnológicas de acuerdo a las tendencias del sector de TI.*

Adicionalmente, es importante destacar que a través del Decreto 767 de 2022 *"Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital (...)"*, se generó un nuevo enfoque, no sólo del Estado, sino también de los diferentes actores de la sociedad, fundamentales para un desarrollo integral del Gobierno Digital en Colombia, y en donde las necesidades y problemáticas del contexto determinan el uso de la tecnología y la forma como ésta puede aportar en la generación de valor público. Ahora bien, en lo que respecta en el habilitador de la **"Seguridad y privacidad de la información"** este busca "*(...) desarrollar capacidades a través de la implementación de los lineamientos de seguridad y privacidad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de datos.*"

En el marco de la economía digital, el Municipio de Bucaramanga enfrenta desafíos significativos en materia de atención ciudadana, resolución de problemáticas sociales y garantía de derechos fundamentales. Estos retos requieren decisiones estratégicas sustentadas en el uso efectivo de las Tecnologías de la Información y las Comunicaciones (TIC), siendo prioritario implementar medidas que mitiguen amenazas como virus informáticos, accesos no autorizados y otros riesgos cibernéticos.

Para atender esta necesidad, el Municipio cuenta actualmente con una solución tecnológica avanzada en materia de seguridad perimetral, basada en la implementación de un sistema de firewall de próxima generación (Next-Generation Firewall - NGFW) configurado en alta disponibilidad (HA) y con esquemas de redundancia del fabricante Palo Alto. Esta infraestructura tiene como objetivo principal asegurar comunicaciones seguras entre la Alcaldía, otras entidades públicas, entidades bancarias y la ciudadanía en general, garantizando además el cumplimiento de la normativa legal vigente en materia de protección de datos personales, como lo establece la Ley 1581 de 2012 y la Resolución No. 746 de 2022.

La Entidad administra una plataforma tecnológica compuesta por aproximadamente 104 servidores (entre físicos y virtuales), 750 estaciones de trabajo, 60 bases de datos y 649 accesos VPN, que soportan sistemas críticos como el portal de impuestos, la gestión de nómina, la planeación institucional, la gestión documental y el tratamiento de datos sensibles de la ciudadanía. Estos sistemas requieren una infraestructura de hardware y software robusta, capaz de protegerlos frente a amenazas informáticas y garantizar su operación continua y segura.

En este contexto, el Proceso de Gestión de las TIC de la Alcaldía tiene como responsabilidad garantizar la seguridad de la información en todos los procesos internos, en cumplimiento del habilitador transversal **"Seguridad y Privacidad de la Información"**, definido en la política nacional de Gobierno Digital. Uno de los principales mecanismos para cumplir este habilitador es el **Firewall**, una herramienta tecnológica que permite monitorear, controlar, auditar y facilitar de manera segura las conexiones entre usuarios (internos y externos) y los servicios digitales de la Entidad.

Actualmente, la Alcaldía de Bucaramanga opera una plataforma de seguridad perimetral basada en dispositivos **Palo Alto Networks** PA-850, configurados en alta disponibilidad (HA). Estos equipos están clasificados como **Firewalls** de próxima generación (NGFW) y se integran en una arquitectura escalable y robusta. La solución ofrece funcionalidades avanzadas como:

1. Filtrado inteligente de paquetes
2. Control de aplicaciones y visibilidad del tráfico
3. Gestión de ancho de banda (QoS)
4. VPN con protocolos IPSec y SSL
5. Sistema de prevención de intrusos (IPS)
6. Protección contra amenazas (virus, malware, spyware)
7. Control de tráfico y políticas de acceso a Internet

Estas capacidades permiten a la Entidad contar con un entorno seguro, conforme a los estándares internacionales de ciberseguridad, garantizando tanto la integridad como la disponibilidad de la información institucional.

Dado que esta solución no es de carácter perpetuo, se requiere la renovación tanto de los equipos como del licenciamiento, así como la extensión de la garantía de fábrica y del soporte técnico oficial del fabricante. Esto es esencial para mantener la plataforma actualizada con las últimas versiones de software, definiciones de seguridad y capacidades de respuesta ante amenazas emergentes.

En cumplimiento de los lineamientos en materia de seguridad de la información y con el fin de proteger los servicios ofrecidos a los funcionarios y ciudadanos, es indispensable mantener políticas de control y restricción de alto nivel sobre el acceso a la red institucional. La plataforma de seguridad **Palo Alto Networks Inc** permite ejercer este control de manera continua, filtrando y monitoreando el tráfico entrante y saliente 24/7, los 365 días del año, constituyéndose así en la primera línea de defensa ante cualquier intento de ataque o vulneración a la infraestructura tecnológica del Municipio de Bucaramanga.

El **Firewall** se cataloga como un dispositivo realmente importante para procesos interno/externos tales como:

1. Canales VPN P2P previamente configurados con el sector Bancario y otras entidades.
2. Controles de seguridad exigidos dentro del cumplimiento de la Ley 1581 de 2012 y definidos en la Guía de Responsabilidad Demostrada creada por la SIC para todas las entidades públicas y privadas de Colombia.
3. El FIREWALL actual maneja las siguientes utilidades o controles de seguridad: Sistema de detección de intrusos, Antivirus, filtrado de contenido, protección por geolocalización, sistema avanzado de reportes, visualización del tráfico de la red, protección de vulnerabilidades, permite establecer las VPN (conexiones privadas a través de la red).
4. Informa y bloquea incidentes cibernéticos que motiven un mal tratamiento de datos personales, como por ejemplo secuestro de información o RANSOMWARE.
5. Brinda herramientas tecnológicas que permiten proteger sitios e infraestructura web con medidas de seguridad fuertes.
6. La conexión SEGURA que brinda este sistema de licenciamiento hacia otras entidades públicas o sector Bancario permite que dichas conexiones no se vean comprometidas, y minimiza riesgos de fallas o problemas en las transacciones.
7. Los equipos de cómputo adscritos a la Alcaldía de Bucaramanga cuentan con controles de peticiones hacia INTERNET, es decir, los errores o malas prácticas de usuarios son detectados en aras de evitar pérdida de información valiosa de la Entidad.
8. Brinda herramientas en relación a la seguridad de la información en la figura de TELETRABAJO. Ver página 38 del Libro Blanco del Teletrabajo https://teletrabajo.gov.co/622/articles8228_archivo_pdf_libro_blanco.pd
9. El licenciamiento permitirá a la Oficina TIC obtener herramientas para monitorear y controlar la actividad de la red hacia INTERNET haciendo este tráfico más seguro y confiable, minimizando las probabilidades de ataques y asegurando de una mejor manera la información generada por dicha actividad.

Dada la creciente exposición a amenazas informáticas y riesgos de ciberseguridad que comprometen la integridad, disponibilidad y confidencialidad de los sistemas de información incluidas las aplicaciones web institucionales, tanto de uso interno como orientadas a servicios ciudadanos, se hace indispensable garantizar la continuidad operativa y la robustez de los mecanismos de protección implementados. En este contexto, resulta crítico mantener actualizada la infraestructura de seguridad perimetral, lo cual, implica la renovación de los dispositivos físicos y la garantía extendida del licenciamiento vigente, así como la suscripción activa del software y soporte asociado a dicha plataforma.

El Municipio de Bucaramanga cuenta con el dispositivo tipo **Firewall** del fabricante **Palo Alto Networks Inc.** para garantizar altos niveles de seguridad perimetral en la red de la Entidad. La solución tecnológica con que se cuenta tiene como referencia equipos físicos PA-850 y está

conformada por dos dispositivos en Alta Disponibilidad (HA) los cuales dependen de su licenciamiento (uno para cada dispositivo) para que la solución cumpla su funcionalidad en debida forma y se configuren las reglas y condiciones de accesibilidad que permiten monitorear y ofrecer alto nivel de seguridad a las conexiones de red y a los diferentes dispositivos de conectividad utilizados en la Alcaldía. Dichos equipos y licenciamientos por estar asociados al fabricante del producto, como sucede con este tipo de dispositivos, se encuentra licenciado única y exclusivamente por **Palo Alto Networks Inc.,** motivo por el cual se hace necesario la adquisición de la renovación de equipos y licencias para mantener su actualización y correcto funcionamiento, controlar ciberamenazas de todo tipo y dar cumplimiento a las normas de derechos de autor y de protección y privacidad de la información de la Alcaldía Municipal de Bucaramanga, aunado al hecho que las especificaciones técnicas aseguran la eficacia de los bienes a contratar a través de este proceso en pro de la continuidad e interoperabilidad necesaria para el normal funcionamiento del sistema de la Entidad.

Es fundamental señalar que:

1. Actualmente el Municipio de Bucaramanga tiene 2 equipos Palo Alto PA850 en HA como Firewall de protección, actualmente esta referencia de equipos está en fin de ciclo de ventas y el fabricante emitió la última versión de OS; con lo cual se hace necesario hacer upgrade a la última versión en este caso Palo Alto PA-1410 la cual ofrece mejoras en rendimiento, capacidad de procesamiento, eficiencia energética y funcionalidades de conectividad, incluyendo puertos Ethernet compatibles con velocidades de 10 Mbps, 100 Mbps, 1 Gbps, 2,5 Gbps y 5 Gbps.
2. Los equipos firewall de Palo Alto han funcionado de forma óptima durante más de 8 años en la Alcaldía de Bucaramanga, protegiendo adecuadamente a nivel perimetral a la Entidad y el equipo de ingeniería ha usado y adoptado la solución tecnológica garantizando la protección frente a amenazas de piratas informáticos.
3. Realizar migración con equipos de la misma marca, reduce el impacto en la migración de políticas de la referencia actual a la nueva, propiciando que la migración se realice de forma transparente y rápida sin afectación a las conexiones o la red con la que cuenta la Entidad.
4. De no llevarse a cabo la renovación de las licencias del firewall perimetral del Municipio, los módulos de filtrado y protección dejarán de operar, comprometiendo seriamente la seguridad de la red institucional. En consecuencia, resulta esencial garantizar la renovación oportuna de dichas licencias, a fin de mantener la integridad de los mecanismos de defensa perimetral y mitigar el riesgo de accesos no autorizados, intrusiones o vulnerabilidades que puedan afectar la infraestructura tecnológica de la Entidad.
5. En caso de que el Municipio de Bucaramanga decidiera cambiar el fabricante y/o la marca del licenciamiento del firewall actualmente implementado, se generarían afectaciones críticas durante la fase de transición o migración hacia la nueva solución tecnológica, estimada en un periodo de aproximadamente cinco (5) a siete (7) meses. Durante este tiempo, se comprometería la continuidad operativa, así como la seguridad y privacidad de la información administrada por la Alcaldía de Bucaramanga, lo que conllevaría a un posible incumplimiento del modelo institucional de seguridad de la información. Lo anterior, considerando la curva de aprendizaje del equipo de ingeniería interno de la oficina TIC del Municipio. Adicionalmente, dicho cambio implicaría la adquisición de equipos que posiblemente no se integren de forma nativa con los actuales para realizar la migración, además de servicios de implementación, configuración y capacitación especializada con mayor alcance, lo que representaría un incremento significativo en los costos operativos y presupuestales para la Entidad.

2. OBJETO PROPUESTO

RENOVACIÓN CON UPGRADE DE EQUIPOS Y LICENCIAMIENTO PARA EL FIREWALL MARCA PALO ALTO DE CONFORMIDAD CON LAS ESPECIFICACIONES TÉCNICAS REQUERIDAS POR LA ENTIDAD.

3. ALCANCE DEL OBJETO / ESPECIFICACIONES TECNICAS

En concordancia con lo anterior, y con el fin de asegurar la cobertura funcional y el soporte técnico requerido, la Entidad debe proceder con la renovación de los equipos físicos y el licenciamiento durante la vigencia actual. Esta acción es esencial para la sostenibilidad del entorno de ciberseguridad institucional, al ser la plataforma de seguridad perimetral un componente estratégico dentro del esquema de gestión integral de la Seguridad de la Información.

ITEM	DESCRIPCIÓN	CANTIDAD
1	Upgrade de equipos PA850 a Palo Alto Networks PA-1410	2
2	Upgrade a PA-1410, Precision AI Network Security Subscription Bundle (Advanced Threat Prevention, Advanced URL Filtering, Advanced Wildfire, Advanced DNS Security and Advanced SD-WAN), 1 year (12 months) term.	2
3	PA-1410, Premium Support, 1 year (12 months) term.	2
4	Soporte ilimitado del proveedor por 1 año vía web, correo electrónico o telefónico 7*24 ilimitado. Incluye: Migración de equipos actuales PA850 a los PA1410 y capacitación.	1

Acorde con lo anterior, la Entidad requiere realizar la adquisición de la renovación de los equipos físicos y licenciamiento en la presente vigencia, con el fin de mantener la plataforma con este control, que constituye una de las partes que apoya el proceso de la Seguridad de la Información.

La presente solicitud comprende la renovación con upgrade de equipos de la garantía y licencias, soporte y actualización de la plataforma de seguridad perimetral de **Palo Alto Networks Inc.,** conforme a las condiciones y obligaciones que se detallan a continuación:

1. **Personal Mínimo requerido:**

Perfil	Cant	Formación académica	Experiencia
Ingeniero Certificado en la solución de firewall de Palo Alto Networks.	2	Deberá acreditar formación académica en: Ingeniería de sistemas, electrónica, de telecomunicaciones o afines.	Deberá acreditar: Mínimo tres (3) años de experiencia profesional a partir de la tarjeta profesional y acreditar participación en por lo menos un proyecto de objeto similar, en el que incluye instalación de equipos firewall de Palo Alto.

El futuro CONTRATISTA a quien se le adjudica el contrato deberá presentar, dentro de los dos (2) días siguientes a la comunicación de aceptación de la oferta, las hojas de vida con los respectivos soportes del personal solicitado (digital o física) del personal propuesto.

NOTA 1: Si bien el tipo de contrato que se desprende del presente proceso de selección corresponde a una compraventa, el objeto a contratar no se limita a la simple adquisición y entrega de equipos y licenciamiento, toda vez que comprende actividades especializadas de migración, instalación, configuración, puesta en funcionamiento, soporte técnico y capacitación de la solución Firewall Palo Alto Networks.

En este sentido, se requiere contar con dos (2) profesionales técnicos especializados, teniendo en cuenta que la solución está conformada por dos equipos que operarán bajo un esquema de alta disponibilidad (HA) y que su intervención requiere garantizar la continuidad operativa y la seguridad de la red institucional. La exigencia de este personal mínimo busca asegurar la correcta ejecución de las actividades técnicas, mitigar los riesgos asociados a la migración y configuración de la plataforma y garantizar el soporte especializado durante la ejecución contractual.

NOTA 2: El representante legal del proponente deberá suscribir carta de compromiso en la que manifieste que, en caso de resultar adjudicatario, garantizará la disponibilidad y permanencia del personal mínimo requerido durante la ejecución del contrato, de conformidad con las necesidades y actividades técnicas establecidas por la Entidad.

2. **Soporte técnico.** La prestación del soporte de la plataforma Palo Alto deberá cumplir con lo siguiente:

- Presentar cronograma que debe ser aprobado por el supervisor para realizar el upgrade de equipos físicos.
- Prestar el servicio de soporte y solución de problemas asociados a la plataforma todas las veces que lo requiera la entidad, de forma remota, durante el tiempo de vigencia de la suscripción al servicio de soporte y actualización.
- Presentar al supervisor del contrato el procedimiento para el reporte y atención de los casos generados relacionados con plataforma Palo Alto.
- Prestar el servicio de soporte vía web, correo electrónico o telefónico 7 x 24 por 1 año para las soluciones Palo Alto, acorde a los niveles de servicio.
- Emplear la siguiente metodología para el escalamiento de los casos de soporte:
    - Tiempos de atención para incidentes de primer nivel: 1 hora
    - Tiempos de atención para incidentes de segundo nivel (escalados al fabricante): 48 horas.
    - Presentar informes de los mantenimientos correctivos y preventivos cada seis meses.
    - El contratista debe prestar soporte técnico para la reconfiguración del equipo o nuevas implementaciones que surjan durante el tiempo de garantía (1 año), según las necesidades de la Entidad.

3. **Condiciones técnicas mínimas:**

- Migrar la configuración del hardware actual al hardware nuevo, asegurándose de transferir todas las configuraciones, redes privadas y ajustes pertinentes a la nueva arquitectura. Esto incluye, pero no se limita a, políticas de seguridad, reglas de firewall, configuraciones de red, y cualquier otra configuración específica de la plataforma Palo Alto. La migración debe realizarse de manera que garantice la continuidad operativa y la seguridad de la red durante el proceso de transición.
- Entregar los dos nuevos equipos PA-1410 configurados en alta disponibilidad y conectados en la red interna de la Alcaldía de Bucaramanga.
- Presentar para el caso de las actualizaciones que se realicen, una ficha con la descripción de las actividades a realizar, instalación, configuración y pruebas.

Obligaciones Específicas del Contratista:

1. Realizar el upgrade y la migración de las maquinas actuales PA850 a las nuevas PA1410.
2. Instalar los PA1410 incluyendo todos los accesorios, cables, conectores, adaptadores y/o accesorios necesarios para su correcto funcionamiento.
3. Presentar cronograma de migración de los equipos firewall al supervisor para su posterior aprobación e implementación.
4. Los equipos y accesorios para su instalación serán nuevos, de primera calidad y estarán libre de defectos e imperfecciones
5. Validar que la garantía y soporte de fábrica de los equipos esté registrada por el termino mínimo de un (1) año a nombre del Municipio de Bucaramanga.
6. Los equipos ofertados deben ser adquirido a través de los canales de distribución autorizados en Colombia y su introducción al país debe atender las normas aduaneras y cambiarias.
7. El futuro contratista deberá presentar, dentro de los dos (2) días siguientes a la suscripción del contrato, las hojas de vida del personal mínimo requerido, junto con los respectivos documentos soporte que acrediten el cumplimiento de los requisitos exigidos por la Entidad. La documentación podrá ser presentada en medio físico o digital.

8. Realizar los ajustes de versión necesarios durante la vigencia del contrato y al finalizar este, la entidad deberá contar con la última versión estable, "release" o actualización disponible de la plataforma Palo Alto.
9. Brindar el servicio de soporte y mantenimiento.
10. Garantizar la configuración y operatividad de la plataforma Palo Alto de acuerdo con las necesidades que surjan durante el tiempo de vigencia de la renovación del licenciamiento y la suscripción del servicio de soporte y actualización, propendiendo por la usabilidad y accesibilidad de esta.
11. Garantizar que después de realizar la instalación de nuevas versiones y/o atención de los incidentes y/o mantenimientos correctivos y/o mantenimientos preventivos, cada uno de los componentes de hardware, software y/o equipos o dispositivos que componen la solución de seguridad de red de datos (Firewall), queden 100% operativos de acuerdo a las necesidades de la Entidad.
12. Capacitar al personal designado por el supervisor sobre las nuevas características con las que cuentan los equipos instalados. La capacitación será virtual o presencial y tendrá una duración mínima de 4 horas.
13. Los componentes de hardware, software y/o equipos o dispositivos deben incluir todos los costos de operación, en los que se debe contemplar mano de obra, transporte y los repuestos.
14. Certificación o aval de Fábrica dirigido a la entidad, con el fin de que el fabricante PALOALTO NETWORKS certifique que es partner y que cuenta con condiciones aplicables a los servicios de instalación, soporte y mantenimiento de sus productos.

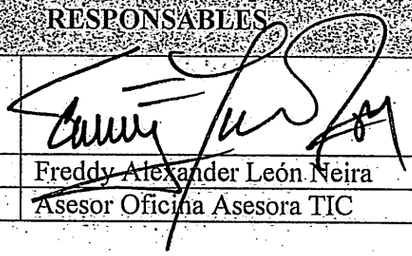
4. PLAZO TENTATIVO

El contrato tendrá un plazo de ejecución de **DOS (02) MESES** contados a partir de la suscripción del acta de inicio sin que exceda la vigencia fiscal 2026, previo cumplimiento de los requisitos legales establecidos en el artículo 23 de la Ley 1150 de 2007.

5. RELACION DE ASPECTOS PRESUPUESTALES

RUBRO PRESUPUESTAL	*2.1.2.02.01.004 Productos metálicos y paquetes de software*			
VALOR LIMITE DEL GASTO SEGÚN RUBRO PRESUPUESTAL	**DOSCIENTOS CUARENTA Y NUEVE MILLONES SETENTA Y SEIS MIL NOVECIENTOS NOVENTA Y SEIS PESOS M/CTE ($249.076.996) INCLUIDO IVA** y todos los gravámenes nacionales, departamentales y municipales vigentes que se generen con ocasión de la celebración, ejecución y liquidación del contrato.			
IMPUTACIÓN PRESUPUESTAL	FUNCIONAMIENTO	**X**	INVERSIÓN	
NOMBRE PROYECTO DE INVERSIÓN	N.A			
CÓDIGO BPIN	N.A			
LÍNEA ESTRATÉGICA	N.A			
PROGRAMA	N.A			
META	N.A			

6. ANEXOS
N.A

7. RESPONSABLES	
FIRMA	
NOMBRE	Freddy Alexander León Neira
CARGO O PROFESIÓN	Asesor Oficina Asesora TIC

COPIA CONTROLADA