ESTUDIOS PREVIOS DE CONVENIENCIA Y OPORTUNIDAD Decreto 1082 de 2015 Artículo 2.2.1.2.1.5.1.	
FECHA:	AGOSTO DE 2026
DEPENDENCIA:	SECRETARÍA GENERAL
OBJETO:	ADQUISICIÓN, INSTALACIÓN Y/O CONFIGURACIÓN Y PUESTA EN FUNCIONAMIENTO DE INFRAESTRUCTURA DE SEGURIDAD PERIMETRAL PARA EL FORTALECIMIENTO DE LA RED Y CONECTIVIDAD LAN/WLAN DE LA ALCALDIA DE MONTERÍA.

1. DESCRIPCIÓN DE LA NECESIDAD QUE LA ENTIDAD ESTATAL PRETENDE SATISFACER CON EL PROCESO DE CONTRATACIÓN.

Que conforme lo dispone el artículo 2º de la Constitución Política de 1991, el Estado tiene como fin esencial, entre otros, servir a la comunidad, garantizar la efectividad de los principios, derechos y deberes consagrados en la Constitución y facilitar la participación de todos en las decisiones que los afectan, siendo un deber de todas las autoridades públicas, asegurar la convivencia pacífica, la vigencia de un orden justo y proteger a todas las personas residentes en Colombia, en su vida, honra, bienes, creencias y demás derechos y libertades.

Que el Artículo 311 de la Constitución Política de Colombia señala que a los *"municipios, como entidad fundamental de la división político-administrativa del Estado le corresponde prestar los servicios públicos que determine la Ley, construir las obras que demande el progreso local, ordenar el desarrollo de su territorio, promover la participación comunitaria, el mejoramiento social y cultural de sus habitantes y cumplir las demás funciones que le asignen la Constitución y las leyes".*

De conformidad con el artículo 311 de la Constitución Política de Colombia, corresponde al municipio como entidad fundamental de la división político-administrativa del Estado, la prestación de los servicios públicos que determine la ley, la construcción de obras que impulsen el progreso local, la ordenación del desarrollo territorial, la promoción de la participación comunitaria y el mejoramiento social y cultural de sus habitantes. En cumplimiento de este mandato constitucional, la Alcaldía de Montería debe garantizar la prestación eficiente, segura y accesible de sus servicios públicos, incluyendo aquellos que se ofrecen a través de medios digitales.

Dentro de los principios de la contratación estatal señalados en el Artículo 3 de la Ley 80 de 1993, se indica que 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 administradores que colaboran con ellas en la consecución de dichos fines. Asimismo, dentro de las facultades que concede la ley al Alcalde Municipal, está la de contratar la adquisición de los diferentes bienes y servicios requeridos para el cumplimiento de los fines descritos.

Por su parte, la Ley 1341 de 2009 "*Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones —TIC, se crea la Agenda Nacional de Espectro y se dictan otras disposiciones",* en su artículo 2º establece lo siguiente:

"PRINCIPIOS ORIENTADORES. La investigación, el fomento, la promoción y el desarrollo de las Tecnologías de la Información y las Comunicaciones son una política de Estado que involucra a todos los sectores y niveles de la administración pública y de la sociedad, para contribuir al desarrollo educativo, cultural, económico, social y político e incrementar la productividad, la competitividad, el respeto a los Derechos Humanos inherentes y la inclusión social.

Las Tecnologías de la Información y las Comunicaciones deben servir al interés general y es deber del Estado promover su acceso eficiente y en igualdad de oportunidades, a todos los habitantes del territorio nacional."

Que, el artículo 230 de la Ley 1450 de 2011, modificado por el artículo 148 de la Ley 1955 de 2019 señala que *"Todas las entidades de la administración pública deberán adelantar las acciones que señale el Gobierno nacional a través del Ministerio de Tecnologías de la información y las Comunicaciones para la implementación de la política de Gobierno Digital"*. Dentro de las acciones

prioritarias se encuentra el cumplimiento de los lineamientos y estándares para el incremento de la confianza y la seguridad digital.

Que el Decreto 767 de 2022 “Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones” establece en el artículo 2.2.9.1.2.1. el habilitador de Seguridad y Privacidad de la Información:

“*3. Habilitadores: Los sujetos obligados desarrollarán las capacidades que les permitan ejecutar las Líneas de Acción de la Política de Gobierno Digital, mediante la implementación de los siguientes habilitadores:*

3.2. Seguridad y Privacidad de la Información: Este habilitador busca que los sujetos obligados desarrollen 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 los datos.”

Que, el Ministerio de Tecnologías de la información y las Comunicaciones estableció, a través de la Resolución 500 de 2021 los lineamientos y estándares para la estrategia de seguridad digital, y la adopción del Modelo de Seguridad y Privacidad de la Información - MSPI, como habilitador de la política de Gobierno Digital., el cual conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

Que, el Conpes 3995 de 2020, Política Nacional de Confianza y Seguridad digital, señala el objetivo de establecer medidas para desarrollar la confianza digital a través de la mejora en la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías.

Por su parte, el Modelo Integrado de Planeación y Gestión – MIPG, reglamentado mediante el Decreto 1499 de 2017, establece un marco obligatorio para las entidades de la Rama Ejecutiva del orden nacional y territorial, incluyendo entidades descentralizadas. Este modelo permite planear, gestionar, evaluar, controlar y mejorar el desempeño institucional bajo criterios de calidad, orientando la gestión pública hacia resultados con valores. Dentro de las 18 políticas de gestión y desempeño institucional que conforman el MIPG, se destaca la Política de Gobierno Digital, la cual busca impactar positivamente en la calidad de vida de los ciudadanos y en la competitividad del país, mediante el uso estratégico de las Tecnologías de la Información y las Comunicaciones – TIC, promoviendo la generación de valor público en un entorno de confianza digital.

Desde el enfoque territorial, el Plan de Desarrollo Municipal 2024–2027 “Una Sola Montería”, contempla dentro del eje estratégico “Montería vive con un gobierno sólido”, el fortalecimiento de la gestión y dirección de la administración pública territorial. Este lineamiento implica la modernización de la infraestructura tecnológica y la implementación de medidas de seguridad informática que garanticen la continuidad operativa, la protección de datos sensibles y la confianza ciudadana en los servicios digitales ofrecidos por la entidad; la cual está a cargo de la Secretaría General.

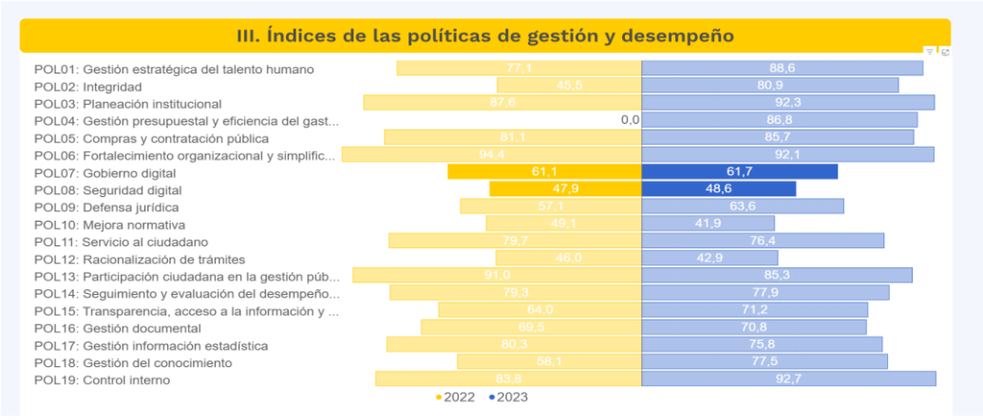
Programa 32. Montería vive con un gobierno sólido

Este es el programa de fortalecimiento institucional para ampliar y mejorar bienes y servicios públicos del Estado local. Para este programa se impulsará:

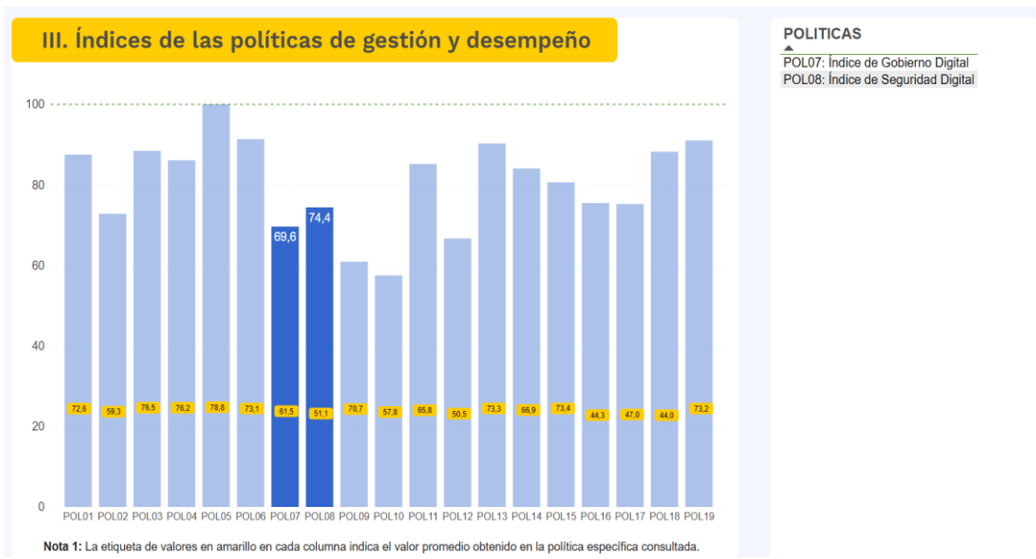
1. Programa de saneamiento fiscal y financiero ejecutado
2. Sistema de facturación para el Impuesto Predial Unificado implementado
3. Implementar el sistema de gestión documental incluyendo la planificación, manejo, organización de la información y dotación, adecuación y/o arriendo del espacio físico donde se integren las tecnologías de la información para almacenamiento en la nube de los archivos
4. Fortalecimiento a la gestión y dirección de la administración pública territorial en el municipio de Montería
5. Nuevo estatuto tributaria diseñado
6. Creación de las Secretarías de Desarrollo Económico y Competitividad y Cultura
7. Empresas descentralizadas
8. Interoperabilidad entre el sistema de información tributario y financiero para la simplificación de procesos de conciliación, la generación más ágil de ejecuciones presupuestales y de Informes financieros a entidades nacionales y órganos de control
9. Campañas anual de gestión tributaria diseñada y realizada
10. Programa Hacienda a la Calle por Una Sola Montería implementada
11. Formulación de Política de Atención al Ciudadano y Política social del cuidado (incluyendo a los adultos mayores)
12. Dotación de sedes de la Alcaldía de Montería
13. Dotación de Infraestructura Tecnológica (Hardware - Software) y Seguridad Informática
14. Información para el registro administrativo del SISBEN

Fuente: Plan de Desarrollo "Una Sola Montería"

En el marco del Modelo Integrado de Planeación y Gestión – MIPG, y en concordancia con las Políticas de Gobierno Digital y Seguridad Digital, la Alcaldía de Montería reconoce la urgencia de seguir fortaleciendo sus capacidades institucionales en materia de ciberseguridad toda vez que los resultados de la Medicación de Desempeño Institucional de las Vigencias 2023 y 2024 aplicada a través del Formulario Único de Reporte de Avances de la Gestión (FURAG), fueron los siguiente



Fuente: Resultados FURAG 2022, 2023



Fuente: Resultados FURAG 2024

Con base en los resultados, el Departamento Administrativo de la Función Pública estableció recomendaciones para la Alcaldía de Montería entre las que se destacan:

- Contar con un firewall licenciado y con soporte para los temas de seguridad perimetral de la infraestructura on premise.
- Analizar los incidentes de seguridad digital (Ciberseguridad) que se presentaron y adoptar medidas técnicas, administrativas y de talento humano para garantizar que la seguridad digital se incorpore al plan de seguridad y privacidad de la información y así mitigar riesgos relacionados con la protección y la privacidad de la información e incidentes de seguridad digital.

Función Pública

mipg | modelo integrado de planeación y gestión

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA
RECOMENDACIONES FURAG VIGENCIA 2024

Entidad		
431	ALCALDIA DE MONTERIA	CORDOBA
Recomendaciones	242	

Política	Recomendación	Índice
Seguridad Digital	Realizar pruebas de respaldo a las copias de seguridad de la información de los aplicativos misionales, estratégicos, soporte y de mejora, de m	POL09
Seguridad Digital	Contar con un Plan de Recuperación de Desastres -DRP-, que esté definido, documentado e implementado para todos los procesos.	POL09
Seguridad Digital	Contar con un Plan de Continuidad del Negocio -BCP-, que esté definido, documentado e implementado para los procesos críticos y misionale	POL09
Seguridad Digital	Contar con un firewall licenciado y con soporte para los temas de seguridad perimetral de la infraestructura on premise.	POL09
Seguridad Digital	Verificar y asegurar que los proveedores y contratistas de la entidad cumplan con las políticas de ciberseguridad internas.	POL09
Seguridad Digital	Implementar un sistema para dar el cumplimiento a la Ley de protección de datos personales (ley 1581 de 2012)	POL09
Seguridad Digital	Analizar los incidentes de seguridad digital (Ciberseguridad) que se presentaron y adoptar medidas técnicas, administrativas y de talento huma	POL09

Fuente: Función Publica - Recomendaciones MDI 2024

Que, en compañía del Centro de Investigación y Desarrollo en Tecnologías de la Información y las Comunicaciones (**CINTEL**), en mayo 2025 se aplicó el Instrumento de Medición de Nivel de Madurez Organizacional en Seguridad de la Información, basado en estándares internacionales como ISO/IEC 27001, ISO 22301, Cyber Resiliency Engineering Framework (CREF), NIST Cybersecurity Framework (NIST CSF) y CIS Controls.

El diagnóstico abarcó dimensiones esenciales, como gestión estratégica, gestión de riesgos, protección informática, continuidad del negocio, cumplimiento normativo, cultura de seguridad y respuesta a incidentes. Cada dimensión ha sido analizada con base en una escala de madurez que va desde un estado "Inexistente" (0), en el que no existen prácticas formales, hasta un nivel "Líder" (5), donde se aplican estrategias avanzadas de mejora continua. Esta metodología permite identificar fortalezas y áreas de oportunidad dentro de la organización, proporcionando información clave para la toma de decisiones y la planificación estratégica en seguridad de la información.

A partir del autodiagnóstico realizado, se ha determinado el nivel de madurez general de la Alcaldía de Montería en seguridad de la información. Este resultado es el reflejo del estado actual de las prácticas, procesos y controles implementados en cada una de las dimensiones analizadas:

Resultados: 0.86 NIVEL: 1 INCIPIENTE



A través de esta evaluación, las organizaciones pueden optimizar recursos, fortalecer la toma de decisiones y mejorar su capacidad de enfrentar amenazas, avanzando hacia una cultura de seguridad más robusta.

Actualmente, la Alcaldía de Montería enfrenta desafíos críticos en la gestión de sus servicios digitales, derivados de la ausencia de controles de seguridad y protección de la información. Esta situación ha generado vulnerabilidades que exponen los sistemas institucionales a riesgos como:

- Accesos no autorizados a plataformas y bases de datos
- Filtración de información confidencial
- Ataques cibernéticos que comprometen la continuidad operativa
- Dificultades en la protección de datos personales y sensibles

Sumado a lo anterior, el Grupo de Respuesta a Emergencias Cibernéticas de Colombia (COLCERT), entidad responsable de coordinar, apoyar y asesorar la gestión de incidentes de ciberseguridad en el sector público y privado del país, ha compartido recientemente el informe técnico de análisis de seguridad correspondiente a la evaluación del dominio institucional y sus subdominios asociados a la Alcaldía de Montería.

Este informe presenta los hallazgos identificados durante el proceso de revisión, así como recomendaciones generales y técnicas orientadas a mitigar riesgos, fortalecer la postura de ciberseguridad de la entidad y promover el cumplimiento de buenas prácticas en la gestión de activos digitales. El informe dio como resultado lo siguiente:

Consolidado de vulnerabilidades detectadas sobre el dominio monteria.gov.co y sus subdominios

No	Dominio/IP	Críticas	Altas	Medias	Bajas	Total
1	arem.mc	0	2	2	0	4
2	comisior	0	2	2	0	4
3	formtest.	0	2	2	0	4
4	todosala	0	2	2	0	4
5	tamias.n	0	2	1	0	3
6	www.mo	0	2	1	0	3
7	monteria	0	2	1	0	3
8	forms.m	0	1	2	0	3
Total		0	15	13	0	28

Vulnerabilidades Críticas Detectadas

La siguiente tabla resume los principales riesgos críticos identificados durante el análisis, su severidad y la mitigación recomendada:

Tipo de Riesgo	Severidad	Mitigación Propuesta
Subdominios huérfanos	Media	Monitorear cambios en DNS y auditoría periódica de subdominios.
Carencia de registros SPF, DKIM y DMARC	Alta	Implementar políticas de DMARC con reportes.
Software expuesto	Alta	Utilizar WAF o proxy inverso que filtre headers.
Exposición de puertos de administración	Alta	Implementar firewalls y listas blancas de IP.
Ausencia de encabezados de seguridad HTTP esenciales	Media	Revisar configuración de web server y WAF.
Cifrados débiles	Media	Usar suites modernas (AES-GCM, ChaCha20).

Fuente: INFORME COLCERT 2025

Además, el 16 de diciembre de 2025, la entidad fue víctima de un ataque de Phishing (técnica de ingeniería social en la que los ciberdelincuentes suplantan la identidad de personas o empresas de confianza). Su objetivo es engañarlo para que revele información confidencial (como contraseñas o tarjetas de crédito) o descargue archivos maliciosos) y Malware, que consiste en la instalación de un programa malicioso que permite a los delincuentes llevar a cabo este tipo de operaciones indebidas. Como consecuencia, esta situación permitió la alteración de la información durante el proceso de un

pago y la manipulación indebida de dichas credenciales dando como resultado movimientos no reconocidos en una cuenta bancaria del municipio. Esto deja en evidencia las debilidades significativas en los controles de ciberseguridad existentes.

Este incidente constituye un riesgo materializado, demostrando que las amenazas cibernéticas no son hipotéticas, sino reales y con capacidad de generar impactos directos sobre los recursos públicos.

A raíz de lo sucedido, la entidad bancaria con la que el municipio tiene vinculo ha condicionado futuros análisis de riesgo a la implementación estricta de medidas de seguridad remitidas a través de Oficio de la Oficina de Tesorería No.TGM-0103-2026 cuyo asunto es: Remisión de respuesta Davivienda Rad. 1-57585444301 y solicitud de implementación de medidas de seguridad informática.

Con base en el incidente ocurrido, se hace imperativo fortalecer la infraestructura tecnológica de la Alcaldía mediante la adquisición e implementación de una solución integral de seguridad perimetral, que permita:

- Prevenir ataques de Phishing mediante:
    - Inspección de tráfico.
    - Filtrado de contenido.
    - Control de aplicaciones.
- Detectar y bloquear malware antes de que afecte los sistemas internos.
- Proteger los procesos críticos de áreas sensibles como Tesorería.
- Aplicar políticas de seguridad unificadas para todos los usuarios y sedes.
- Monitorear en tiempo real los eventos de seguridad.
- Reducir la probabilidad de fraudes electrónicos y accesos no autorizados.

La implementación de firewalls de seguridad perimetral de nueva generación, junto con el fortalecimiento de la red LAN/WLAN y la administración centralizada, constituye una medida correctiva y preventiva esencial para evitar la repetición de incidentes que comprometan los recursos públicos.

Actualmente, la dirección IP pública asociada a la infraestructura tecnológica de la Alcaldía se encuentra incluida en listas negras (blacklists) utilizadas por proveedores de servicios de correo electrónico, plataformas en la nube y sistemas de reputación en internet, como consecuencia de tráfico malicioso, intentos de envío de spam o actividades anómalas originadas o canalizadas desde la red institucional.

Esta situación evidencia la existencia de debilidades en los controles de seguridad perimetral, así como la falta de mecanismos robustos de prevención, detección y respuesta frente a incidentes de ciberseguridad.

La inclusión de la IP institucional en listas negras genera múltiples impactos negativos, entre los cuales se destacan:

1. Afectación a los Servicios de Correo Electrónico Institucional

- Bloqueo o rechazo de correos electrónicos enviados desde dominios institucionales.
- Clasificación de mensajes como spam por destinatarios externos.
- Dificultades en la comunicación con:
    - Otras entidades del Estado.
    - Proveedores.
    - Ciudadanía.
- Riesgo de incumplimiento de trámites administrativos que dependen del correo electrónico.

2. Riesgos para la Continuidad del Servicio

- Restricciones en el acceso a plataformas externas.
- Limitaciones para la interoperabilidad con servicios digitales.

- Posibles bloqueos por parte de proveedores de internet o servicios en la nube.

3. Riesgos de Seguridad de la Información

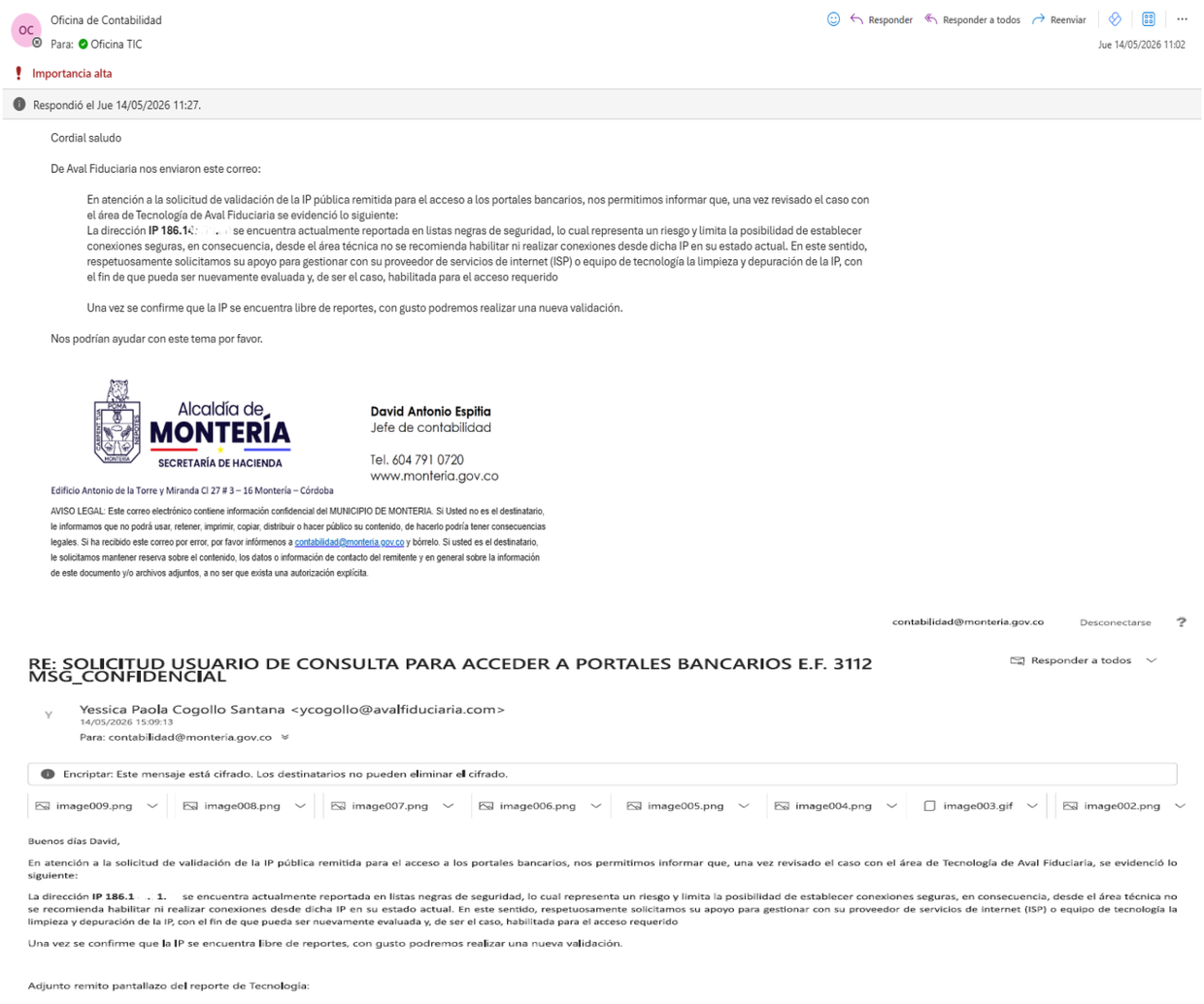
- Evidencia de posibles:
  - Infecciones de malware.
  - Equipos comprometidos.
  - Uso indebido de la red institucional.

- Incremento del riesgo de:
  - Pérdida de información.
  - Accesos no autorizados.
  - Fugas de datos personales o sensibles.

4. Impacto Reputacional e Institucional

- Deterioro de la imagen institucional frente a ciudadanos y entidades externas.
- Pérdida de confianza en los canales digitales oficiales.
- Riesgo de observaciones por parte de organismos de control.

Lo anterior, se evidencia en correo de la oficina de contabilidad donde nos reportan los correos enviados por Aval Fiduciaria indicando que la IP del Municipio se encuentra actualmente reportada en listas negras de seguridad, lo cual representa un riesgo y limita la posibilidad de establecer conexiones seguras con la entidad. Esta situación ha dificultado las validaciones y conexiones con los portales de Aval Fiduciaria:



Oficina de Contabilidad
Para: Oficina TIC
Responder | Responder a todos | Reenviar
Jue 14/05/2026 11:02

Importancia alta

Respondió el Jue 14/05/2026 11:27.

Cordial saludo

De Aval Fiduciaria nos enviaron este correo:

En atención a la solicitud de validación de la IP pública remitida para el acceso a los portales bancarios, nos permitimos informar que, una vez revisado el caso con el área de Tecnología de Aval Fiduciaria se evidenció lo siguiente:
La dirección **IP 186.1** se encuentra actualmente reportada en listas negras de seguridad, lo cual representa un riesgo y limita la posibilidad de establecer conexiones seguras, en consecuencia, desde el área técnica no se recomienda habilitar ni realizar conexiones desde dicha IP en su estado actual. En este sentido, respetuosamente solicitamos su apoyo para gestionar con su proveedor de servicios de internet (ISP) o equipo de tecnología la limpieza y depuración de la IP, con el fin de que pueda ser nuevamente evaluada y, de ser el caso, habilitada para el acceso requerido

Una vez se confirme que la IP se encuentra libre de reportes, con gusto podremos realizar una nueva validación.

Nos podrían ayudar con este tema por favor.

Alcaldía de MONTERÍA
SECRETARÍA DE HACIENDA

David Antonio Espitia
Jefe de contabilidad

Tel. 604 791 0720
www.monteria.gov.co

Edificio Antonio de la Torre y Miranda Cl 27 # 3 – 16 Montería – Córdoba

AVISO LEGAL: Este correo electrónico contiene información confidencial del MUNICIPIO DE MONTERIA. Si Usted no es el destinatario, le informamos que no podrá usar, retener, imprimir, copiar, distribuir o hacer público su contenido, de hacerlo podría tener consecuencias legales. Si ha recibido este correo por error, por favor infórmenos a contabilidad@monteria.gov.co y bórrelo. Si usted es el destinatario, le solicitamos mantener reserva sobre el contenido, los datos o información de contacto del remitente y en general sobre la información de este documento y/o archivos adjuntos, a no ser que exista una autorización explícita.

contabilidad@monteria.gov.co Desconectarse

RE: SOLICITUD USUARIO DE CONSULTA PARA ACCEDER A PORTALES BANCARIOS E.F. 3112 MSG_CONFIDENCIAL

Responder a todos

Yessica Paola Cogollo Santana <ycogollo@avalfiduciaria.com>
14/05/2026 15:09:13
Para: contabilidad@monteria.gov.co

Encriptar: Este mensaje está cifrado. Los destinatarios no pueden eliminar el cifrado.

image009.png | image008.png | image007.png | image006.png | image005.png | image004.png | image003.gif | image002.png

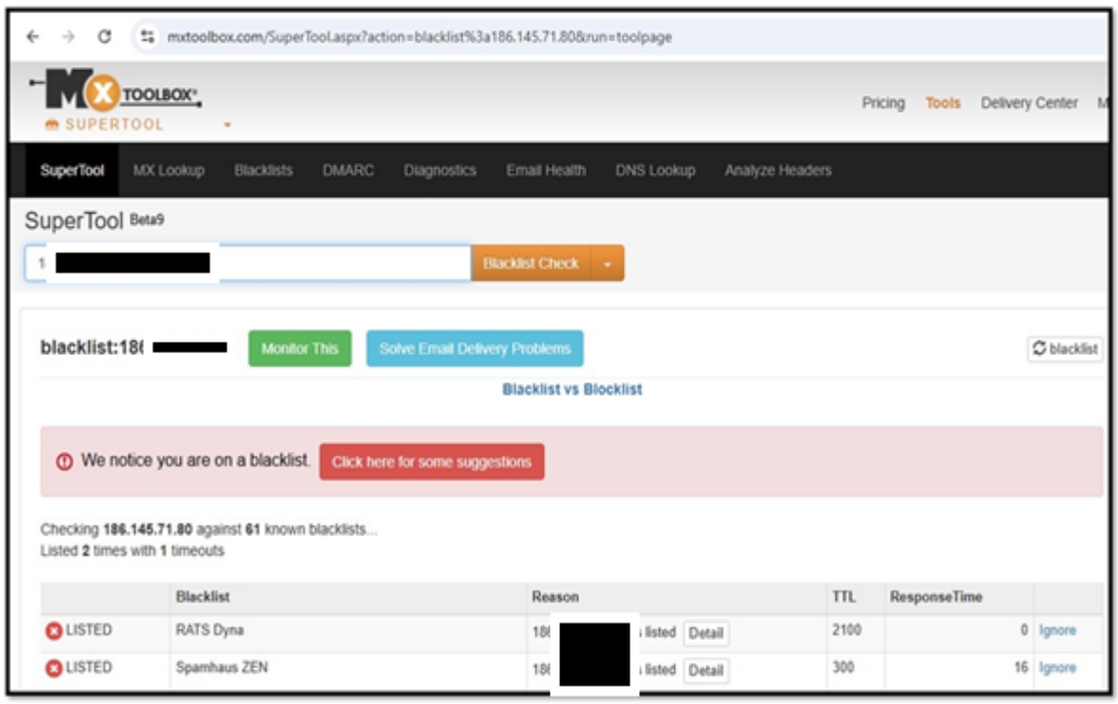
Buenos días David,

En atención a la solicitud de validación de la IP pública remitida para el acceso a los portales bancarios, nos permitimos informar que, una vez revisado el caso con el área de Tecnología de Aval Fiduciaria, se evidenció lo siguiente:

La dirección **IP 186.1 . 1.** se encuentra actualmente reportada en listas negras de seguridad, lo cual representa un riesgo y limita la posibilidad de establecer conexiones seguras, en consecuencia, desde el área técnica no se recomienda habilitar ni realizar conexiones desde dicha IP en su estado actual. En este sentido, respetuosamente solicitamos su apoyo para gestionar con su proveedor de servicios de internet (ISP) o equipo de tecnología la limpieza y depuración de la IP, con el fin de que pueda ser nuevamente evaluada y, de ser el caso, habilitada para el acceso requerido

Una vez se confirme que la IP se encuentra libre de reportes, con gusto podremos realizar una nueva validación.

Adjunto remito pantallazo del reporte de Tecnología:



Los incidentes de ciberseguridad ocurridos en la Alcaldía evidencian la materialización de riesgos críticos asociados a debilidades en la infraestructura de red y en los controles de seguridad perimetral. Estos hechos demuestran que la Entidad enfrenta amenazas avanzadas que no pueden ser mitigadas de manera efectiva mediante soluciones básicas, fragmentadas o de bajo nivel de madurez tecnológica.

Estas debilidades no solo afectan la integridad de la infraestructura tecnológica, sino que también debilitan la confianza ciudadana en los servicios públicos digitales. En un contexto donde la transformación digital es un eje estratégico para mejorar la eficiencia, transparencia y accesibilidad de la gestión pública, resulta imperativo implementar soluciones técnicas y estratégicas que garanticen la seguridad de la información y la resiliencia institucional.

En este contexto, resulta técnicamente necesario que la solución a implementar corresponda a tecnologías empresariales de alto nivel, con capacidades comprobadas de prevención, detección y respuesta frente a amenazas sofisticadas, así como de operación estable en entornos distribuidos y críticos como los del sector público. Por tal razón, la Entidad requiere que los componentes de seguridad perimetral (Hybrid Mesh Firewall y SD-WAN) y de infraestructura LAN/WLAN provengan de fabricantes que, en los dos últimos reportes publicado por Gartner, se encuentren ubicados en el cuadrante de Líderes de los respectivos Magic Quadrant.

El Cuadrante Mágico de Gartner es un reporte elaborado por Gartner, una firma internacional e independiente de análisis y consultoría, reconocida a nivel mundial por evaluar tecnologías y proveedores de servicios. Este reporte analiza y compara a los principales fabricantes del mercado en una determinada categoría tecnológica, con base en criterios objetivos como la calidad de la solución, su nivel de innovación, la capacidad de respuesta ante incidentes, la solidez del fabricante y su visión de largo plazo.

Desde el punto de vista técnico, las soluciones clasificadas como Líderes por Gartner se caracterizan por contar con capacidades avanzadas de seguridad integrada, tales como inspección profunda de tráfico, prevención de intrusiones, protección contra malware, control de aplicaciones, visibilidad centralizada y respuesta automatizada a incidentes, funcionalidades indispensables para prevenir ataques como los ya sufridos por la Entidad. Asimismo, estas soluciones ofrecen arquitecturas consolidadas y probadas, que reducen el riesgo de configuraciones débiles o fallos operativos que puedan ser explotados por actores maliciosos.

Así las cosas, se requiere una solución integral de infraestructura y ciberseguridad, para fortalecer la conectividad LAN y WLAN mediante la adquisición e implementación de firewalls de seguridad perimetral, switches y access points, complementados con servicios profesionales especializados para su diseño, instalación, configuración y puesta en operación, con el fin de garantizar la continuidad del servicio, la protección de la información y la mitigación de riesgos. Esta solución se requiere para el cubrimiento de las sedes o dependencias administrativas que han sido identificadas con servicios de internet:

SEDE O DEPENDENCIA ADMINISTRATIVA	DIRECCION
CENTRO VERDE EDIFICIO 1 – PRINCIPAL	Cra. 1W # 32A - 49
CENTRO VERDE EDIFICIO 2	Cra. 1W # 32A - 49
ANTONIO DE LA TORRE Y MIRANDA – 27	Calle 27 # 3-16
SECRETARÍA DE EDUCACIÓN	a 22a-196, Cra. 15 #22a BARRIO COSTA DE ORO
CASA DE JUSTICIA	CRA 14#1SUR-43 MZ 25 LOTE 1 BARRIO LOS ARAUJOS
SECRETARIA TRANSITO	Calle 56 No. 6-174 BARRIO LA CASTELLANA
CASA DE LA MUJER EMPODERADA	Carrera 19 # 27 - 88 BARRIO PASATIEMPO
ADULTO MAYOR - CENTRO DE VIDA ESPIRITU DE DIOS	CALLA 11 D # 12-22 BARRIO SAMARIA
UNIDAD DE VICTIMAS	Calle 10 #8e-20 Barrio La Granja
COMISARIA PRIMERA DE FAMILIA	Calle 20 Carrera 32 CANTA CLARO
INSPECCION PRIMERA URBANA	MONTECENTRO
INSPECCION TERCERA URBANA	Calle 20 Carrera 2w #2-40, BARRIO RIO DE JANEIRO
INSPECCIÓN DE POLICÍA ESPECIALIZADA EN URBANISMO	Carrera 3 # 22 - 08
COMISARIA TERCERA DE FAMILIA	CARRERA 3W #24A - 05

No obstante, teniendo en cuenta las restricciones presupuestales actuales, la Entidad ha definido la ejecución del proyecto bajo un enfoque por fases, priorizando en una primera fase aquellas sedes que concentran:

- Mayor número de funcionarios y usuarios.
- Infraestructura tecnológica crítica.
- Servicios administrativos y misionales estratégicos.
- Mayor exposición a riesgos de seguridad de la información.

En consecuencia, la primera fase del proyecto se desarrollará en las siguientes sedes:

- Centro Verde Edificio 1 - Principal
- Centro Verde Edificio 2
- Palacio de la Torre y Miranda - 27
- Educación
- Casa de justicia

Esta estrategia permitirá a la Entidad:

- Iniciar de manera inmediata el fortalecimiento de su infraestructura tecnológica.
- Obtener beneficios operativos y de seguridad desde la primera fase.
- Garantizar la sostenibilidad financiera del proyecto.
- Contar con una base tecnológica escalable para las siguientes fases.

Tratándose de una implementación por fases, iniciando en las sedes principales, la adopción de soluciones líderes garantiza que la infraestructura de red LAN/WLAN y de seguridad perimetral cuente con escalabilidad, interoperabilidad y sostenibilidad a largo plazo, permitiendo la incorporación progresiva de nuevas sedes sin necesidad de rediseños estructurales ni dependencia tecnológica indebida. Esto es particularmente relevante para asegurar una administración centralizada, políticas de seguridad homogéneas y una gestión eficiente del crecimiento futuro.

En aras de fortalecer la infraestructura de red, se requiere contratar la “ADQUISICIÓN, INSTALACIÓN Y/O CONFIGURACIÓN Y PUESTA EN FUNCIONAMIENTO DE INFRAESTRUCTURA DE

SEGURIDAD PERIMETRAL PARA EL FORTALECIMIENTO DE LA RED Y CONECTIVIDAD LAN/WLAN DE LA ALCALDIA DE MONTERÍA"

El objeto del presente proceso se encuentra incluido en el Plan Anual de Bienes, Obras y Servicios del Municipio de Montería – vigencia 2026, tal y como consta en el Certificado N° P.C 1640, expedido el 28 de Mayo de 2026 por la Coordinadora del Área de Compras del Municipio de Montería, el cual hará parte integral de este estudio previo.

Por lo anterior, se hace necesaria la presente contratación.

2. OBJETO A CONTRATAR, CON SUS ESPECIFICACIONES, LAS AUTORIZACIONES, PERMISOS Y LICENCIAS REQUERIDOS PARA SU EJECUCIÓN.

2.1. OBJETO A CONTRATAR: ADQUISICIÓN, INSTALACIÓN Y/O CONFIGURACIÓN Y PUESTA EN FUNCIONAMIENTO DE INFRAESTRUCTURA DE SEGURIDAD PERIMETRAL PARA EL FORTALECIMIENTO DE LA RED Y CONECTIVIDAD LAN/WLAN DE LA ALCALDIA DE MONTERÍA.

2.2. IDENTIFICACIÓN DEL OBJETO CONTRACTUAL DE ACUERDO AL CLASIFICADOR DE BIENES Y SERVICIOS: De acuerdo al Clasificador de Bienes y Servicios de las Naciones Unidas, el proceso de selección se clasifica de la siguiente manera:

CÓDIGO UNSPSC	GRUPO	SEGMENTO	FAMILIA	CLASE
43222500	(E). PRODUCTOS DE USO FINAL	(43) Difusión de Tecnologías de Información y Telecomunicaciones	(22) Equipos o plataformas y accesorios de redes multimedia o de voz y datos	(25) Equipo de seguridad de red
43222600	(E). PRODUCTOS DE USO FINAL	(43) Difusión de Tecnologías de Información y Telecomunicaciones	(22) Equipos o plataformas y accesorios de redes multimedia o de voz y datos	(26) Equipo de servicio de red
43233200	(E). PRODUCTOS DE USO FINAL	(43) Difusión de Tecnologías de Información y Telecomunicaciones	(23) Software	(32) Software de seguridad y protección
81111500	(F). SERVICIOS	(81) Servicios Basados en Ingeniería, Investigación y Tecnología	(11) Servicios informáticos	(15) Ingeniería de software o hardware

2.3. ESPECIFICACIONES TÉCNICAS DEL OBJETO:

El objeto contractual se ejecutará teniendo en cuenta las especificaciones que a continuación se describen:

El proyecto comprende la implementación de la solución en las siguientes sedes administrativas priorizadas:

1. Centro Verde – Edificio 1
2. Centro Verde – Edificio 2
3. Palacio de la Torre y Miranda – 27
4. Educación
5. Casa de Justicia

La solución deberá quedar completamente implementada, configurada, afinada y en operación, sirviendo como base para su ampliación progresiva a las demás sedes de la Entidad.

ETAPA 1. PLANEACIÓN, DISEÑO Y ALISTAMIENTO DE LA SOLUCIÓN

Definir y preparar la solución técnica de infraestructura LAN/WLAN y seguridad perimetral que será implementada en la Fase 1, garantizando alineación con las políticas de la Entidad, escalabilidad y control del riesgo. Debe contemplar como mínimo y sin limitarse las siguientes actividades:

1. Levantamiento de información técnica por sede.
2. Inventario y diagnóstico de infraestructura existente.
3. Identificación de riesgos de seguridad y puntos críticos.
4. Diseño de la arquitectura técnica:

    - Segmentación
    - Esquema
    - Políticas de seguridad perimetral.
    - Integración de infraestructura

5. Planeación detallada de actividades

ETAPA 2. SUMINISTRO, INSTALACIÓN Y CONFIGURACIÓN DE LA INFRAESTRUCTURA

Implementar física y lógicamente la solución integral, por personal certificado asegurando su correcta configuración, integración y afinamiento conforme a buenas prácticas y lineamientos del fabricante. Debe contemplar como mínimo y sin limitarse las siguientes actividades:

1. Suministro de equipos y licencias.
2. Verificación de equipos nuevos, originales y con garantía.
3. Instalación física en las sedes priorizadas:

- Montaje en racks.
- Conexiones eléctricas y de red.

4. Configuración y alistamiento de las plataformas:

- Políticas de seguridad perimetral.
- Configuración LAN/WLAN.
- Administración centralizada.

5. Licenciamiento y puesta en funcionamiento en equipos

6. Configuración sobre las últimas versiones estables de firmware y software aprobadas por el fabricante.

7. Afinamiento y estabilización de las plataformas.

ETAPA 3. PRUEBAS, PUESTA EN OPERACIÓN Y ACEPTACIÓN DEL SERVICIO

Verificar el correcto funcionamiento de la solución y dejarla operativa a satisfacción de la Entidad. Debe contemplar como mínimo y sin limitarse las siguientes actividades:

1. Pruebas de:

    - Conectividad LAN y WLAN.
    - Seguridad perimetral.
    - Rendimiento y estabilidad.

2. Pruebas / muestras que evidencien:

    - Correcta configuración.

- Afinamiento de las plataformas.

3. Corrección de incidencias detectadas.

4. Puesta en operación oficial de la solución en la Fase 1.

5. Entrega formal a satisfacción de la Entidad.

ETAPA 4. TRANSFERENCIA DE CONOCIMIENTO, SOPORTE Y MANTENIMIENTO

Garantizar la continuidad, estabilidad y sostenibilidad de la solución implementada, así como el fortalecimiento de capacidades del personal de la Oficina TIC. Debe contemplar como mínimo y sin limitarse las siguientes actividades:

1. Transferencia de conocimiento

- Transferencia de conocimiento mínima de 24 horas.
- Capacitación a tres (3) funcionarios designados por la Entidad.
- Entrega de documentación técnica final.

2. Soporte y mantenimiento

- Soporte técnico 7x24 por doce (12) meses.
- Atención remota y en sitio según requerimiento.
- Mantenimiento preventivo y correctivo sin costo adicional.
- Actualización de firmware conforme a versiones estables del fabricante.
- Cumplimiento de los SLA.

Las especificaciones técnicas de las etapas antes descritas son las siguientes:

ITEM	DESCRIPCIÓN GENERAL	UNIDAD MEDIDA	CANTIDAD
SOLUCIONES DE SEGURIDAD PERIMETRAL TIPO FIREWALL DE NUEVA GENERACIÓN			
1	**SUMINISTRO, INSTALACIÓN Y PUESTA EN FUNCIONAMIENTO DE FIREWALL DE SEGURIDAD PERIMETRAL CORE** **GENERALIDADES** Los equipos deben cumplir con las siguientes características mínimas de desempeño activas y funcionales en la puesta en marcha de las plataformas. Los equipos deben ser Appliances físicos (nuevos en su empaque original y sellados de fabrica) (No se aceptarán equipos remanufacturados y/o reparados y/o reformados). Los equipos deben ser de propósito específico tipo Firewall. Los equipos deben contar con tecnología ASIC para permitir acelerar los procesos (no solo por CPU) y de esta manera permita mejorar el rendimiento del procesamiento de tráfico. La solución debe pertenecer al cuadrante de líder de Gartner para Hybrid Mesh Firewall y SD-WAN en su último reporte publicado. **Capacidades operativas mínimas de cada equipo:** NGFW Throughput: 3.1 Gbps o superior	UNIDAD	4

	Firewall Throughput: 37 Gbps o superior IPS Throughput: 5 Gbps o superior Threat Protection Throughput: 2.8 Gbps o superior VPN SSL Throughput: 1.5 Gbps o superior Inspección SSL Throughput: 3 Gbps o superior Sesiones Concurrentes: 3.000.000 o superior Disco Interno 480 GB SSD o superior IPsec VPN Throughput: 33 Gbps o superior 4 interfaces de 10 GE SFP+ (se deben incluir en la oferta ocho (08) transceivers SFP+ SR con sus respectivos cables de F.O.) 8 interfaces de 1 GE SFP (se deben incluir en la oferta ocho (02) transceivers SFP SR con sus respectivos cables de F.O.) 16 interfaces de 1 GE RJ45 **Funcionalidades generales firewall (Core)** **Capacidades de NAT (Network Address Translation)** Las plataformas deben soportar lo siguientes tipos de traducción de direcciones: NAT y PAT NAT estático NAT: destino, origen NAT, NAT64 persistente **Funciones básicas de Firewall** Las reglas de firewall deben analizar las conexiones que pasen por el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs. La solución debe integrarse con el directorio activo y soportar políticas basadas en identidad. Esto significa que podrán definirse políticas de seguridad de acuerdo con el grupo de pertenencia de los usuarios. Debe tener la capacidad de generar una advertencia al administrador cuando este configure una política duplicada Debe estar en la capacidad de integrase con plataforma Cloud IaaS como: AWS,Azure,Google etc. Con el fin de generar y actualizar objetos de direcciones de manera automática basado en los parámetros de red (IP, TAG, etc) de las instancias desplegadas en la nube y estas ser usadas como objetos de reglas o políticas de firewall Debe soportar reglas de firewall en IPv6 configurables tanto por CLI (Command Line Interfaz) como por GUI (Graphical User Interfaz). La solución tendrá la capacidad de hacer captura de paquetes por política de seguridad implementada para luego ser exportado en formato PCAP. El dispositivo será capaz de crear e integrar políticas contra ataques DoS (Denial of service) las cuales se deben poder aplicar por interfaces. El dispositivo será capaz de ejecutar inspección de tráfico SSL en todos los puertos y seleccionar bajo que certificado será válido este tráfico. Tendrá la capacidad de hacer escaneo a profundidad de tráfico tipo SSH dentro de todos o cierto rango de puertos configurados para este análisis. **Conectividad y enrutamiento** Funcionalidad de DHCP: como Cliente DHCP, Servidor DHCP y reenvío (Relay) de solicitudes DHCP.		

	Soporte de enrutamiento estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas. Soporte a enrutamiento dinámico RIP V1, V2, OSPF y BGP. La solución podrá habilitar políticas de enrutamiento en IPv6. La solución deberá ser capaz de habilitar enrutamiento estático para cada interfaz en IPv6. **VPN IPsec** Los equipos deben soportar las siguientes características: Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site). Soporte para IKEv2 y IKE Configuration Method. Soporte de VPNs con algoritmos de cifrado: AES, DES, 3DES Se debe soportar longitudes de llave para AES de 128, 192 y 256 bits **Autenticación** Los dispositivos deben manejar los siguientes tipos de autenticación: Capacidad de soporta autenticación local y remota integrándose con Servidores de Autenticación RADIUS, LDAP o TACACS+. Capacidad incluida, al integrarse con Microsoft Windows Active Directory o Novell eDirectory, de autenticar transparentemente usuarios sin preguntarles username o password. Esto es aprovechar las credenciales del dominio de Windows bajo un concepto “Single-Sign-On”. Soporte de Token Físicos o Mobile sobre Smartphone basado en IOS o Android, token de SMS, email o con plataformas de terceros como RSA SecurID. Capacidad de soportar autenticación de acceso de usuario a través de 802.1x y portal cautivo. **Manejo de tráfico y calidad de servicio** La solución debe soportar balanceo de enlaces WAN inteligente (SD-WAN Seguro) sin licencia adicional basado en: Aplicaciones cloud, SLA y Mejor calidad de enlace basado en (Jitter, latencia, ancho de banda, perdida de paquetes). Capacidad de poder asignar parámetros de traffic shapping atreves de reglas de manera independiente. Capacidad de poder asignar parámetros de traffic shaping diferenciadas para el tráfico en distintos sentidos de una misma sesión. Capacidad de definir parámetros de traffic shaping que apliquen para cada dirección IP en forma independiente, en contraste con la aplicación y categoría URL de las mismas para la regla en general. Capacidad de poder definir límite de ancho de banda (ancho de banda máximo) en Kilobits por segundo. **Antimalware** Debe ser capaz de analizar, establecer control de acceso y detener ataques y hacer Antivirus en tiempo real en al menos los siguientes protocolos aplicativos: HTTP, SMTP, IMAP, POP3, FTP.MAPI El módulo de antimalware debe haber sido desarrollado por el mismo fabricante de la solución de firewall, así como las firmas deben ser de su propiedad y no por medio de licenciamiento o concesiones de un tercero, esto con el fin de garantizar la idoneidad de la protección, así como los tiempos de respuesta del soporte de la misma. Debe soportar la inspección de archivos comprimidos como los son: GZIP,RAR,LZH,IHA,CAB,ARJ;ZIP entre otros con el fin de proteger contra estas técnicas de evasión. El Antivirus debe integrarse de forma nativa con una solución		

	Sandbox del mismo fabricante, de tal manera que envíen muestras de archivos a dicho dispositivo para su análisis. **Filtrado Web** Facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías. Por flexibilidad, el filtro de URLs debe tener por lo menos 78 categorías y por lo menos 47 millones de sitios web en la base de datos. Debe poder categorizar contenido Web requerido mediante IPv6. Será posible exceptuar la inspección de HTTPS por categoría. Debe contar con la capacidad de bloquear contenido de YouTube usando el Channel ID El filtrado debe ser sobre tráfico http y https. **Protección contra intrusos (IPS)** El sistema de detección y prevención de intrusos deben poder implementarse tanto en línea como fuera de línea. En línea, el tráfico a ser inspeccionado pasará a través del equipo. Fuera de línea, el equipo recibirá el tráfico a inspeccionar desde un switch con un puerto configurado en span o mirror. Debe ser posible definir políticas de detección y prevención de intrusiones para tráfico IPv6. A través de sensores. Capacidad de detección de más de 7000 ataques. El sistema de detección y prevención de intrusos debe estar integrado a la plataforma de seguridad “appliance”. Sin necesidad de instalar un servidor o appliance externo, La interfaz de administración del sistema de detección y prevención de intrusos deberá de estar perfectamente integrada a la interfaz de administración del dispositivo de seguridad appliance, sin necesidad de integrar otro tipo de consola para poder administrar este servicio. Esta deberá permitir la protección de este servicio por política de control de acceso. Debe ofrecerse la posibilidad de guardar información sobre el paquete de red que detonó la detección del ataque, así como al menos los 5 paquetes sucesivos. Estos paquetes deben poder ser visualizados por una herramienta que soporte el formato PCAP. **Control de aplicaciones** La solución debe soportar la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo. La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico. La solución debe tener un listado de al menos 3000 aplicaciones ya definidas por el fabricante. Para aplicaciones identificadas deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log y resetear conexión **Inspección de Contenido SSL/SSH** La solución debe soportar inspeccionar tráfico que esté siendo encriptado mediante SSL al menos para los siguientes protocolos: HTTP, IMAP, SMTP, POP3 y FTP en su versión segura. Debe ser posible definir perfiles de inspección SSL donde se definan los protocolos a inspeccionar y el certificado usado, estos perfiles deben poder ser escogidos una vez se defina la política de seguridad. La inspección debe realizarse: mediante la técnica conocida como Hombre en el Medio (MITM – Man In The Middle) para una inspección completa o solo inspeccionando el certificado sin necesidad de hacer full inspection. **Alta disponibilidad** El dispositivo deberá soportar Alta Disponibilidad transparente, es decir, sin pérdida de conexiones en caso de que un nodo falle		

	tanto para IPV4 como para IPV6 Alta Disponibilidad en modo Activo-Activo de forma automática sin requerir hacer políticas de enrutamiento basado en orígenes y destino para poder hacer la distribución del tráfico. El equipo debe soportar hasta 2 equipos en esquema de HA. **Visibilidad** La solución debe estar en la capacidad de visualizar el tráfico de usuario, aplicaciones, navegación y niveles de riesgo en tiempo real, esto deberá ser sobre la misma plataforma sin necesidad de software o licenciamiento adicional. Deber tener la capacidad de poder validar con que política la sesión se está coincidiendo y un link hacia la misma. **Características de Administración** Interfaz gráfica de usuario (GUI), vía Web por HTTP y HTTPS para hacer administración de las políticas de seguridad y que forme parte de la arquitectura nativa de la solución para administrar la solución localmente. Por seguridad la interfaz debe soportar SSL sobre HTTP (HTTPS) Soporte de al menos 3 servidores syslog para poder enviar bitácoras a servidores de SYSLOG remotos Debe tener la capacidad de gestionar todas las políticas de seguridad, además de poder gestionar Switches y APs dentro de una única consola de gestión. **Licenciamiento y actualizaciones** El licenciamiento de todas las funcionalidades debe ser ILIMITADO en cuanto a usuarios, conexiones, VPNs equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo. La vigencia de las actualizaciones para los servicios de Antivirus, AntiSpam, IPS, Application Control y URL Filtering debe proveerse por al menos doce (12) meses a partir de su activación en el portal del fabricante. La plataforma es requerida por un periodo de doce (12) meses en un esquema de soporte 7x24 ante el fabricante a partir de su activación en el portal del fabricante. Garantía y licenciamiento de los equipos y software ofertados, con Servicio de soporte 7x24 de 12 meses a partir de su activación en el portal de fabricante, que incluya Soporte Telefónico y repuestos (estos repuestos deberán ser gestionados por el contratista en caso tal de requerirse un en tiempo no mayor a (08) días calendario).		
SUMINISTRO, INSTALACIÓN Y PUESTA EN FUNCIONAMIENTO DE FIREWALL DE SEGURIDAD PERIMETRAL MULTIGIGA			
2	**GENERALIDADES** Los equipos deben cumplir con las siguientes características mínimas de desempeño activas y funcionales en la puesta en marcha de las plataformas. Los equipos deben ser Appliances físicos (nuevos en su empaque original y sellados de fabrica) (No se aceptarán equipos remanufacturados y/o reparados y/o reformados). Los equipos deben ser de propósito específico tipo Firewall. Los equipos deben contar con tecnología ASIC para permitir acelerar los procesos (no solo por CPU) y de esta manera permita mejorar el rendimiento del procesamiento de tráfico. La solución debe pertenecer al cuadrante de líder de Gartner para Hybrid Mesh Firewall y SD-WAN en su último reporte publicado. **Capacidades operativas mínimas de cada equipo:** NGFW Throughput: 2.5 Gbps o superior	UNIDAD	1

	Firewall Throughput: 27 Gbps o superior IPS Throughput: 4.5 Gbps o superior Threat Protection Throughput: 2.1 Gbps o superior VPN SSL Throughput: 1.3 Gbps o superior Inspección SSL Throughput: 2.6 Gbps o superior Sesiones Concurrentes: 3.000.000 o superior Disco Interno 120 GB SSD o superior IPsec VPN Throughput: 25 Gbps o superior 2 interfaces de 10 GE SFP+ (se deben incluir en la oferta seis (06) transceivers SFP+ SR con sus respectivos cables de F.O.) 2 interfaces multigiga 10/5/2.5 GE RJ45 8 interfaces de 1 GE RJ45 **Funcionalidades generales firewall (Multigiga)** **Capacidades de NAT (Network Address Translation)** Las plataformas deben soportar lo siguientes tipos de traducción de direcciones: NAT y PAT NAT estático NAT: destino, origen NAT, NAT64 persistente **Funciones básicas de Firewall** Las reglas de firewall deben analizar las conexiones que pasen por el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs. La solución debe integrarse con el directorio activo y soportar políticas basadas en identidad. Esto significa que podrán definirse políticas de seguridad de acuerdo con el grupo de pertenencia de los usuarios. Debe tener la capacidad de generar una advertencia al administrador cuando este configure una política duplicada Debe estar en la capacidad de integrase con plataforma Cloud IaaS como: AWS,Azure,Google etc. Con el fin de generar y actualizar objetos de direcciones de manera automática basado en los parámetros de red (IP, TAG, etc) de las instancias desplegadas en la nube y estas ser usadas como objetos de reglas o políticas de firewall Debe soportar reglas de firewall en IPv6 configurables tanto por CLI (Command Line Interfaz) como por GUI (Graphical User Interfaz). La solución tendrá la capacidad de hacer captura de paquetes por política de seguridad implementada para luego ser exportado en formato PCAP. El dispositivo será capaz de crear e integrar políticas contra ataques DoS (Denial of service) las cuales se deben poder aplicar por interfaces. El dispositivo será capaz de ejecutar inspección de tráfico SSL en todos los puertos y seleccionar bajo que certificado será válido este tráfico. Tendrá la capacidad de hacer escaneo a profundidad de tráfico tipo SSH dentro de todos o cierto rango de puertos configurados para este análisis. **Conectividad y enrutamiento** Funcionalidad de DHCP: como Cliente DHCP, Servidor DHCP y reenvío (Relay) de solicitudes DHCP. Soporte de enrutamiento estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas.		

	Soporte a enrutamiento dinámico RIP V1, V2, OSPF y BGP. La solución podrá habilitar políticas de enrutamiento en IPv6. La solución deberá ser capaz de habilitar enrutamiento estático para cada interfaz en IPv6. **VPN IPsec** Los equipos deben soportar las siguientes características: Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site). Soporte para IKEv2 y IKE Configuration Method. Soporte de VPNs con algoritmos de cifrado: AES, DES, 3DES Se debe soportar longitudes de llave para AES de 128, 192 y 256 bits **Autenticación** Los dispositivos deben manejar los siguientes tipos de autenticación: Capacidad de soporta autenticación local y remota integrándose con Servidores de Autenticación RADIUS, LDAP o TACACS+. Capacidad incluida, al integrarse con Microsoft Windows Active Directory o Novell eDirectory, de autenticar transparentemente usuarios sin preguntarles username o password. Esto es aprovechar las credenciales del dominio de Windows bajo un concepto “Single-Sign-On”. Soporte de Token Físicos o Mobile sobre Smartphone basado en IOS o Android, token de SMS, email o con plataformas de terceros como RSA SecurID. Capacidad de soportar autenticación de acceso de usuario a través de 802.1x y portal cautivo. **Manejo de tráfico y calidad de servicio** La solución debe soportar balanceo de enlaces WAN inteligente (SD-WAN Seguro) sin licencia adicional basado en: Aplicaciones cloud, SLA y Mejor calidad de enlace basado en (Jitter, latencia, ancho de banda, perdida de paquetes). Capacidad de poder asignar parámetros de traffic shapping atreves de reglas de manera independiente. Capacidad de poder asignar parámetros de traffic shaping diferenciadas para el tráfico en distintos sentidos de una misma sesión. Capacidad de definir parámetros de traffic shaping que apliquen para cada dirección IP en forma independiente, en contraste con la aplicación y categoría URL de las mismas para la regla en general. Capacidad de poder definir límite de ancho de banda (ancho de banda máximo) en Kilobits por segundo. **Antimalware** Debe ser capaz de analizar, establecer control de acceso y detener ataques y hacer Antivirus en tiempo real en al menos los siguientes protocolos aplicativos: HTTP, SMTP, IMAP, POP3, FTP.MAPI El módulo de antimalware debe haber sido desarrollado por el mismo fabricante de la solución de firewall, así como las firmas deben ser de su propiedad y no por medio de licenciamiento o concesiones de un tercero, esto con el fin de garantizar la idoneidad de la protección, así como los tiempos de respuesta del soporte de la misma. Debe soportar la inspección de archivos comprimidos como los son: GZIP,RAR,LZH,IHA,CAB,ARJ;ZIP entre otros con el fin de proteger contra estas técnicas de evasión. El Antivirus debe integrarse de forma nativa con una solución Sandbox del mismo fabricante, de tal manera que envíen muestras de archivos a dicho dispositivo para su análisis.		

	Filtrado Web Facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías. Por flexibilidad, el filtro de URLs debe tener por lo menos 78 categorías y por lo menos 47 millones de sitios web en la base de datos. Debe poder categorizar contenido Web requerido mediante IPv6. Será posible exceptuar la inspección de HTTPS por categoría. Debe contar con la capacidad de bloquear contenido de YouTube usando el Channel ID El filtrado debe ser sobre tráfico http y https. **Protección contra intrusos (IPS)** El sistema de detección y prevención de intrusos deben poder implementarse tanto en línea como fuera de línea. En línea, el tráfico a ser inspeccionado pasará a través del equipo. Fuera de línea, el equipo recibirá el tráfico a inspeccionar desde un switch con un puerto configurado en span o mirror. Debe ser posible definir políticas de detección y prevención de intrusiones para tráfico IPv6. A través de sensores. Capacidad de detección de más de 7000 ataques. El sistema de detección y prevención de intrusos debe estar integrado a la plataforma de seguridad “appliance”. Sin necesidad de instalar un servidor o appliance externo, La interfaz de administración del sistema de detección y prevención de intrusos deberá de estar perfectamente integrada a la interfaz de administración del dispositivo de seguridad appliance, sin necesidad de integrar otro tipo de consola para poder administrar este servicio. Esta deberá permitir la protección de este servicio por política de control de acceso. Debe ofrecerse la posibilidad de guardar información sobre el paquete de red que detonó la detección del ataque, así como al menos los 5 paquetes sucesivos. Estos paquetes deben poder ser visualizados por una herramienta que soporte el formato PCAP. **Control de aplicaciones** La solución debe soportar la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo. La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico. La solución debe tener un listado de al menos 3000 aplicaciones ya definidas por el fabricante. Para aplicaciones identificadas deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log y resetear conexión **Inspección de Contenido SSL/SSH** La solución debe soportar inspeccionar tráfico que esté siendo encriptado mediante SSL al menos para los siguientes protocolos: HTTP, IMAP, SMTP, POP3 y FTP en su versión segura. Debe ser posible definir perfiles de inspección SSL donde se definan los protocolos a inspeccionar y el certificado usado, estos perfiles deben poder ser escogidos una vez se defina la política de seguridad. La inspección debe realizarse: mediante la técnica conocida como Hombre en el Medio (MITM – Man In The Middle) para una inspección completa o solo inspeccionando el certificado sin necesidad de hacer full inspection. **Alta disponibilidad** El dispositivo deberá soportar Alta Disponibilidad transparente, es decir, sin pérdida de conexiones en caso de que un nodo falle tanto para IPV4 como para IPV6 Alta Disponibilidad en modo Activo-Activo de forma automática sin		

	requerir hacer políticas de enrutamiento basado en orígenes y destino para poder hacer la distribución del tráfico. El equipo debe soportar hasta 2 equipos en esquema de HA. **Visibilidad** La solución debe estar en la capacidad de visualizar el tráfico de usuario, aplicaciones, navegación y niveles de riesgo en tiempo real, esto deberá ser sobre la misma plataforma sin necesidad de software o licenciamiento adicional. Deber tener la capacidad de poder validar con que política la sesión se está coincidiendo y un link hacia la misma. **Características de Administración** Interfaz gráfica de usuario (GUI), vía Web por HTTP y HTTPS para hacer administración de las políticas de seguridad y que forme parte de la arquitectura nativa de la solución para administrar la solución localmente. Por seguridad la interfaz debe soportar SSL sobre HTTP (HTTPS) Soporte de al menos 3 servidores syslog para poder enviar bitácoras a servidores de SYSLOG remotos Debe tener la capacidad de gestionar todas las políticas de seguridad, además de poder gestionar Switches y APs dentro de una única consola de gestión. **Licenciamiento y actualizaciones** El licenciamiento de todas las funcionalidades debe ser ILIMITADO en cuanto a usuarios, conexiones, VPNs equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo. La vigencia de las actualizaciones para los servicios de Antivirus, AntiSpam, IPS, Application Control y URL Filtering debe proveerse por al menos doce (12) meses a partir de su activación en el portal del fabricante. La plataforma es requerida por un periodo de doce (12) meses en un esquema de soporte 7x24 ante el fabricante a partir de su activación en el portal del fabricante. Garantía y licenciamiento de los equipos y software ofertados, con Servicio de soporte 7x24 de 12 meses a partir de su activación en el portal de fabricante, que incluya Soporte Telefónico y repuestos (estos repuestos deberán ser gestionados por el contratista en caso tal de requerirse un en tiempo no mayor a (08) días calendario).		
SUMINISTRO, INSTALACIÓN Y PUESTA EN FUNCIONAMIENTO DE FIREWALL DE SEGURIDAD PERIMETRAL BASICO			
3	**GENERALIDADES** Los equipos deben cumplir con las siguientes características mínimas de desempeño activas y funcionales en la puesta en marcha de las plataformas. Los equipos deben ser Appliances físicos (nuevos en su empaque original y sellados de fabrica) (No se aceptarán equipos remanufacturados y/o reparados y/o reformados). Los equipos deben ser de propósito específico tipo Firewall. Los equipos deben contar con tecnología ASIC para permitir acelerar los procesos (no solo por CPU) y de esta manera permita mejorar el rendimiento del procesamiento de tráfico. La solución debe pertenecer al cuadrante de líder de Gartner para Hybrid Mesh Firewall y SD-WAN en su último reporte publicado. **Capacidades operativas mínimas de cada equipo:** NGFW Throughput: 1.2 Gbps o superior Firewall Throughput: 5 Gbps o superior IPS Throughput: 2.2 Gbps o superior	UNIDAD	1

	Threat Protection Throughput: 1.1 Gbps o superior Inspección SSL Throughput: 1.3 Gbps o superior Sesiones Concurrentes: 720000 o superior Disco Interno 64 GB SSD o superior IPsec VPN Throughput: 4.5 Gbps o superior 5 interfaces de 1 GE RJ45 1 puerto de consola RJ45 **Funcionalidades generales firewall (Basico)** **Capacidades de NAT (Network Address Translation)** Las plataformas deben soportar lo siguientes tipos de traducción de direcciones: NAT y PAT NAT estático NAT: destino, origen NAT, NAT64 persistente **Funciones básicas de Firewall** Las reglas de firewall deben analizar las conexiones que pasen por el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs. La solución debe integrarse con el directorio activo y soportar políticas basadas en identidad. Esto significa que podrán definirse políticas de seguridad de acuerdo con el grupo de pertenencia de los usuarios. Debe tener la capacidad de generar una advertencia al administrador cuando este configure una política duplicada Debe estar en la capacidad de integrase con plataforma Cloud IaaS como: AWS,Azure,Google etc. Con el fin de generar y actualizar objetos de direcciones de manera automática basado en los parámetros de red (IP, TAG, etc) de las instancias desplegadas en la nube y estas ser usadas como objetos de reglas o políticas de firewall Debe soportar reglas de firewall en IPv6 configurables tanto por CLI (Command Line Interfaz) como por GUI (Graphical User Interfaz). La solución tendrá la capacidad de hacer captura de paquetes por política de seguridad implementada para luego ser exportado en formato PCAP. El dispositivo será capaz de crear e integrar políticas contra ataques DoS (Denial of service) las cuales se deben poder aplicar por interfaces. El dispositivo será capaz de ejecutar inspección de tráfico SSL en todos los puertos y seleccionar bajo que certificado será válido este tráfico. Tendrá la capacidad de hacer escaneo a profundidad de tráfico tipo SSH dentro de todos o cierto rango de puertos configurados para este análisis. **Conectividad y enrutamiento** Funcionalidad de DHCP: como Cliente DHCP, Servidor DHCP y reenvío (Relay) de solicitudes DHCP. Soporte de enrutamiento estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas. Soporte a enrutamiento dinámico RIP V1, V2, OSPF y BGP. La solución podrá habilitar políticas de enrutamiento en IPv6. La solución deberá ser capaz de habilitar enrutamiento estático para cada interfaz en IPv6. **VPN IPsec**		

	Los equipos deben soportar las siguientes características: Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site). Soporte para IKEv2 y IKE Configuration Method. Soporte de VPNs con algoritmos de cifrado: AES, DES, 3DES Se debe soportar longitudes de llave para AES de 128, 192 y 256 bits **Autenticación** Los dispositivos deben manejar los siguientes tipos de autenticación: Capacidad de soporta autenticación local y remota integrándose con Servidores de Autenticación RADIUS, LDAP o TACACS+. Capacidad incluida, al integrarse con Microsoft Windows Active Directory o Novell eDirectory, de autenticar transparentemente usuarios sin preguntarles username o password. Esto es aprovechar las credenciales del dominio de Windows bajo un concepto “Single-Sign-On”. Soporte de Token Físicos o Mobile sobre Smartphone basado en IOS o Android, token de SMS, email o con plataformas de terceros como RSA SecurID. Capacidad de soportar autenticación de acceso de usuario a través de 802.1x y portal cautivo. **Manejo de tráfico y calidad de servicio** La solución debe soportar balanceo de enlaces WAN inteligente (SD-WAN Seguro) sin licencia adicional basado en: Aplicaciones cloud, SLA y Mejor calidad de enlace basado en (Jitter, latencia, ancho de banda, perdida de paquetes). Capacidad de poder asignar parámetros de traffic shapping atreves de reglas de manera independiente. Capacidad de poder asignar parámetros de traffic shaping diferenciadas para el tráfico en distintos sentidos de una misma sesión. Capacidad de definir parámetros de traffic shaping que apliquen para cada dirección IP en forma independiente, en contraste con la aplicación y categoría URL de las mismas para la regla en general. Capacidad de poder definir límite de ancho de banda (ancho de banda máximo) en Kilobits por segundo. **Antimalware** Debe ser capaz de analizar, establecer control de acceso y detener ataques y hacer Antivirus en tiempo real en al menos los siguientes protocolos aplicativos: HTTP, SMTP, IMAP, POP3, FTP.MAPI El módulo de antimalware debe haber sido desarrollado por el mismo fabricante de la solución de firewall, así como las firmas deben ser de su propiedad y no por medio de licenciamiento o concesiones de un tercero, esto con el fin de garantizar la idoneidad de la protección, así como los tiempos de respuesta del soporte de la misma. Debe soportar la inspección de archivos comprimidos como los son: GZIP,RAR,LZH,IHA,CAB,ARJ;ZIP entre otros con el fin de proteger contra estas técnicas de evasión. El Antivirus debe integrarse de forma nativa con una solución Sandbox del mismo fabricante, de tal manera que envíen muestras de archivos a dicho dispositivo para su análisis. **Filtrado Web** Facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías. Por flexibilidad, el filtro de URLs debe tener por lo menos 78 categorías y por lo menos 47 millones de sitios web en la base de datos.		

	Debe poder categorizar contenido Web requerido mediante IPv6. Será posible exceptuar la inspección de HTTPS por categoría. Debe contar con la capacidad de bloquear contenido de YouTube usando el Channel ID El filtrado debe ser sobre tráfico http y https. **Protección contra intrusos (IPS)** El sistema de detección y prevención de intrusos deben poder implementarse tanto en línea como fuera de línea. En línea, el tráfico a ser inspeccionado pasará a través del equipo. Fuera de línea, el equipo recibirá el tráfico a inspeccionar desde un switch con un puerto configurado en span o mirror. Debe ser posible definir políticas de detección y prevención de intrusiones para tráfico IPv6. A través de sensores. Capacidad de detección de más de 7000 ataques. El sistema de detección y prevención de intrusos debe estar integrado a la plataforma de seguridad “appliance”. Sin necesidad de instalar un servidor o appliance externo, La interfaz de administración del sistema de detección y prevención de intrusos deberá de estar perfectamente integrada a la interfaz de administración del dispositivo de seguridad appliance, sin necesidad de integrar otro tipo de consola para poder administrar este servicio. Esta deberá permitir la protección de este servicio por política de control de acceso. Debe ofrecerse la posibilidad de guardar información sobre el paquete de red que detonó la detección del ataque, así como al menos los 5 paquetes sucesivos. Estos paquetes deben poder ser visualizados por una herramienta que soporte el formato PCAP. **Control de aplicaciones** La solución debe soportar la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo. La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico. La solución debe tener un listado de al menos 3000 aplicaciones ya definidas por el fabricante. Para aplicaciones identificadas deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log y resetear conexión **Inspección de Contenido SSL/SSH** La solución debe soportar inspeccionar tráfico que esté siendo encriptado mediante SSL al menos para los siguientes protocolos: HTTP, IMAP, SMTP, POP3 y FTP en su versión segura. Debe ser posible definir perfiles de inspección SSL donde se definan los protocolos a inspeccionar y el certificado usado, estos perfiles deben poder ser escogidos una vez se defina la política de seguridad. La inspección debe realizarse: mediante la técnica conocida como Hombre en el Medio (MITM – Man In The Middle) para una inspección completa o solo inspeccionando el certificado sin necesidad de hacer full inspection. **Alta disponibilidad** El dispositivo deberá soportar Alta Disponibilidad transparente, es decir, sin pérdida de conexiones en caso de que un nodo falle tanto para IPV4 como para IPV6 Alta Disponibilidad en modo Activo-Activo de forma automática sin requerir hacer políticas de enrutamiento basado en orígenes y destino para poder hacer la distribución del tráfico. El equipo debe soportar hasta 2 equipos en esquema de HA. **Visibilidad** La solución debe estar en la capacidad de visualizar el tráfico de		

	usuario, aplicaciones, navegación y niveles de riesgo en tiempo real, esto deberá ser sobre la misma plataforma sin necesidad de software o licenciamiento adicional. Deber tener la capacidad de poder validar con que política la sesión se está coincidiendo y un link hacia la misma. **Características de Administración** Interfaz gráfica de usuario (GUI), vía Web por HTTP y HTTPS para hacer administración de las políticas de seguridad y que forme parte de la arquitectura nativa de la solución para administrar la solución localmente. Por seguridad la interfaz debe soportar SSL sobre HTTP (HTTPS) Soporte de al menos 3 servidores syslog para poder enviar bitácoras a servidores de SYSLOG remotos Debe tener la capacidad de gestionar todas las políticas de seguridad, además de poder gestionar Switches y APs dentro de una única consola de gestión. **Licenciamiento y actualizaciones** El licenciamiento de todas las funcionalidades debe ser ILIMITADO en cuanto a usuarios, conexiones, VPNs equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo. La vigencia de las actualizaciones para los servicios de Antivirus, AntiSpam, IPS, Application Control y URL Filtering debe proveerse por al menos doce (12) meses a partir de su activación en el portal del fabricante. La plataforma es requerida por un periodo de doce (12) meses en un esquema de soporte 7x24 ante el fabricante a partir de su activación en el portal del fabricante. Garantía y licenciamiento de los equipos y software ofertados, con Servicio de soporte 7x24 de 12 meses a partir de su activación en el portal de fabricante, que incluya Soporte Telefónico y repuestos (estos repuestos deberán ser gestionados por el contratista en caso tal de requerirse un en tiempo no mayor a (08) días calendario).		
4	**INSTALACIÓN, RENOVACIÓN DE LICENCIA, Y PUESTA EN FUNCIONAMIENTO DE FIREWALL** Renovación de una plataforma FG 120G por 12 meses a partir de la suscripción del acta de inicio con licenciamiento UTP. El No. Serial del equipo a renovar es el siguiente: FG120GTK24003019 El licenciamiento de todas las funcionalidades debe ser ILIMITADO en cuanto a usuarios, conexiones, VPNs equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo. La vigencia de las actualizaciones para los servicios de Antivirus, AntiSpam, IPS, Application Control y URL Filtering debe proveerse por al menos doce (12) meses a partir de su activación en el portal del fabricante. La plataforma es requerida por un periodo de doce (12) meses en un esquema de soporte 7x24 ante el fabricante a partir de su activación en el portal del fabricante. Garantía y licenciamiento de los equipos y software ofertados, con Servicio de soporte 7x24 de 12 meses a partir de su activación en el portal de fabricante, que incluya Soporte Telefónico y repuestos (estos repuestos deberán ser gestionados por el contratista en caso tal de requerirse un en tiempo no mayor a (08) días calendario). El equipo renovado debe integrarse nativamente con la plataforma	UNIDAD	1

	de administración centralizada a adquirir por parte la entidad.		
SOLUCIONES DE ACCESO SEGURO PARA REDES LAN/WLAN			
5	**SUMINISTRO, INSTALACIÓN Y PUESTA EN FUNCIONAMIENTO DE ACCESS POINTS** **GENERALIDADES** Los equipos deben ser Appliances físicos (nuevos en su empaque original y sellados de fabrica) (No se aceptarán equipos remanufacturados y/o reparados y/o reformados). El fabricante debe estar en el cuadrante de lideres de Gartner para soluciones empresariales LAN/WLAN en al menos uno (01) los dos (02) últimos reportes publicados. La instalación de los equipos Access Point se realizará punto por punto, el oferente no deberá incluir servicios de cableado estructurado. Los APs deben incluir al menos: 1 interfaz RJ45 100M/1000M/2.5G/5G 1 interfaz RS-232 o un puerto RJ45 Serial SSID Simultáneos hasta 8 Debe permitir la conexión de dispositivos inalámbricos que soporten los estándares 802.11a/b/g/n/ac/ax de forma simultánea Debe poseer capacidad de conexión en tres bandas (2.4 GHz, 5 GHz y 6 Ghz) operando simultáneamente, además de permitir configuraciones independientes para cada radio Debe contar con un radio BLE (Bluetooth Low Energy) integrado e interno en el dispositivo Numero de radios 3 Wi-Fi+BLE La solución debe permitir la conexión de por lo menos 512 (quinientos doce) clientes inalámbricos simultáneamente por radio Debe soportar agregación de enlaces de acuerdo con el estándar IEEE 802.3ad El sistema operativo debe incluir la última versión completa liberada por el fabricante a la fecha de la compra Debe soportar su alimentación a través de Power Over Ethernet (PoE) conforme a los estándares 802.3af, 802.3at, 802.11bt. Adicionalmente debe poseer una entrada de alimentación de DC. El flujo de tráfico de los dispositivos conectados a la red inalámbrica debe ocurrir de forma centralizada a través del túnel establecido entre el punto de acceso y el controlador inalámbrico. En este modo todos los paquetes enviados en un SSID determinado deben ser enviados a través del túnel hasta el controlador inalámbrico. Cada dispositivo ofertado debe incluir su respectivo Power Injector POE, 802.3at up to 30W for Gigabit PoE Injector Servicio de Soporte Técnico y garantía Premium con Servicio de asistencia técnica continua con cobertura 24/7 ante el fabricante a partir de su activación en el portal del fabricante, atención prioritaria ante incidentes críticos y reemplazo de hardware en caso de fallas (con un máximo de 8 días calendario). Incluye actualizaciones de software y firmware. Los puntos de acceso (APs) deben ser administrables a través de la misma solución de seguridad perimetral tipo firewall (por adquirir) sin requerir licenciamientos adicionales permitiendo así su operatividad, y la extensión del perímetro de seguridad hasta la capa de acceso Wi-Fi. Integrarse de manera nativa con la infraestructura de seguridad perimetral Firewall (por adquirir), de forma que actúen como una extensión lógica del firewall corporativo, permitiendo que éste	UNIDAD	13

	gestione directamente las funcionalidades de los Access Point, incluyendo su configuración, monitoreo y la aplicación de políticas de seguridad en el acceso. **Estándares y certificaciones Access Points** Los APs deben soportar al menos los siguientes estándares de la industria: - 802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h, 802.11i,802.11j, 802.11k, 802.11n, 802.11r, 802.11u, 802.11v, 802.11ac, 802.11ax (Wi-Fi 6), 802.1Q, 802.1X, 802.3ad, 802.3af, 802.3at, 802.3az, 802.3bz - WiFi Certified a,b,g,n,ac,ax, passpoint - WAP2, WPA3 - UL2043 - ROHS **Seguridad inalámbrica Access Point** - Algoritmo de cifrado: AES, TLS, EAP, TTLS, TKIP, WPA, WPA2 y WPA3. - La controladora debe incluir un control y filtro de más de 3000 aplicaciones de aplicaciones de uso común, y permita aplicar políticas granulares de seguridad, QoS, control de ancho de banda y filtrado web. El punto de acceso debe soportar encaminamiento de trafico de los clientes Wireless de manera tunelada, garantizando integridad de los datos a través de túneles IPSec. Cuando se tuneliza el tráfico de los clientes inalámbricos hacia la controladora inalámbrica, para garantizar un mejor uso de los recursos, la solución debe permitir una función conocida como Split Tunneling que se configurará en el SSID. Con esta característica, el AP debe soportar la creación de listas de excepción con direcciones de servicio de la red local que no deben enviar los paquetes a través del túnel al concentrador, es decir, todos los paquetes deben ser tunelizados excepto aquellos destinados a direcciones especificadas locales en las listas de excepciones. El punto de acceso debe soportar encaminamiento de trafico de tipo Modo Bridge o conmutación local. En este modo todo el tráfico de los dispositivos conectados en un determinaod SSID deberá ser conmutado localmente en la interfaz ethernet del punto de acceso y no deberán ser tunelados hasta la controladora inalámbrica El punto de acceso deberá soportar mecanismos de identificación y protección de ataques a la infraestructura inalámbrica (WIPS/WIDS). El punto de acceso deberá soportar la funcionalidad de análisis de espectro con un radio exclusivo que monitoree la red 7x24, que permita la identificación de interferencias no Wi-Fi y que operen en las frecuencias de 2.4GHz, 5GHz y 6 GHz Capacidad de manejar roles por usuario y políticas basadas en identidad. Coexistencias Avanzada Celular (Advanced Cellular Coexistence ACC) Radio dedicado para funciones de WIPS/WIDS y analizador de espectro. No se aceptan Access point adicionales para cumplir este requerimiento		
6	**INSTALACIÓN, RENOVACIÓN DE LICENCIA, Y PUESTA EN FUNCIONAMIENTO DE ACCESS POINT** Renovación de soporte y garantía de fabrica por 12 meses a partir		

	de la suscripción del acta de inicio para los siguientes equipos Access Point. El No. Serial de los equipos a renovar son los siguientes: FP231GTF24062110 FP231GTF24018641 FP231GTF24062108 FP231GTF24062109 FP231GTF24018767 FP231GTF24062124 FP231GTF24062117 FP231GTF24062116 El oferente debe garantizar servicio de Soporte Técnico y garantía Premium con Servicio de asistencia técnica continua con cobertura 24/7 ante el fabricante a partir de la suscripción del acta de inicio, atención prioritaria ante incidentes críticos y reemplazo de hardware en caso de fallas (con un máximo de 8 días calendario). Incluye actualizaciones de software y firmware. Los puntos de acceso (APs) deben ser administrables a través de la misma solución de seguridad perimetral tipo firewall (por adquirir) sin requerir licenciamientos adicionales permitiendo así su operatividad, y la extensión del perímetro de seguridad hasta la capa de acceso Wi-Fi. Integrarse de manera nativa con la infraestructura de seguridad perimetral Firewall (por adquirir), de forma que actúen como una extensión lógica del firewall corporativo, permitiendo que éste gestione directamente las funcionalidades de los Access Point, incluyendo su configuración, monitoreo y la aplicación de políticas de seguridad en el acceso.	UNIDAD	**8**
7	**SUMINISTRO, INSTALACIÓN Y PUESTA EN FUNCIONAMIENTO DE SWITCHES DE ACCESO 48 PUERTOS** La solución de switches ofertada debe ser de la misma marca de la solución de acceso inalámbrico y la controladora de red de este proceso de contratación para garantizar el SD-LAN o SD-BRANCH de la Entidad. Los switches deben permitir descargar políticas de seguridad desde el firewall perimetral de la Entidad. Se debe poder administrar Switches, Access Point, SD-BRANCH, SD-WAN y Firewalls desde la misma consola de Administración (No se requieren consolas en la nube, la administración debe ser local). El fabricante debe estar en el cuadrante de lideres de Gartner para soluciones empresariales LAN/WLAN en al menos uno (01) los dos (02) últimos reportes publicados. Debe estar en capacidad de detectar Dispositivos IoT Debe permitir la autenticación y autorización Local RADIUS y TACACS+ Debe soportar SSH Debe soportar DHCP snooping, Dynamic ARP Debe soportar una funcionalidad de ahorro de Energía que bajé consumo si no hay tráfico y si llega tráfico hacia el dispositivo conectado se envié un mensaje de encendido (Wake-On-Lan - WOL) Debe soportar IEEE 802.1X (Port Based Network Access Control) MTBF minimo de 10 Años (87600 horas) STP Root Guard, STP (802,1d), RSTP (IEEE 802.1w), MSTP (IEEE 802.1s), RPVST (Rapid per Vlan Spanning Tree) Todas las funcionalidades que soporte el equipo deben estar	UNIDAD	9

	incluidas y soportadas a perpetuidad. No se acepta funcionalidades por suscripción. Certificaciones: FCC, CE, RCM, VCCI, BSMI, UL, CB, RoHS2 Incluir 24 Transceiver 10GE SFP+ transceiver module, short range 300m LC connector, MMF, 850nm, 0°C to 70°C, for systems with SFP+ slots para todos los switches. **Capacidades específicas para los switches de 48 puertos** Los equipos deben ser Appliances físicos (nuevos en su empaque original y sellados de fabrica) (No se aceptarán equipos remanufacturados y/o reparados y/o reformados). Interfaces Red Totales: 48x GE RJ45 and 4x 10GE SFP+ Puerto de Consola: 1 RJ-45 Tráfico: IPV4/IPV6 Switch Capacity: Mayor o igual a 176 GB Packets Per Second: Mayor o igual a 260 Mpps VLANs: Mayor o igual a 4K Packet Buffers: Mayor o igual a 2 MB Memory: 512 MB ACL: 640		
8	**SUMINISTRO, INSTALACIÓN Y PUESTA EN FUNCIONAMIENTO DE SWITCHES DE ACCESO BÁSICO DE 24 PUERTOS** La solución de switches ofertada debe ser de la misma marca de la solución de acceso inalámbrico y la controladora de red de este proceso de contratación para garantizar el SD-LAN o SD-BRANCH de la Entidad. Los switches deben permitir descargar políticas de seguridad desde el firewall perimetral de la Entidad. Se debe poder administrar Switches, Access Point, SD-BRANCH, SD-WAN y Firewalls desde la misma consola de Administración (No se requieren consolas en la nube, la administración debe ser local). Debe estar en capacidad de detectar Dispositivos IoT Debe permitir la autenticación y autorización Local RADIUS y TACACS+ Debe soportar SSH Debe soportar DHCP snooping, Dynamic ARP Debe soportar una funcionalidad de ahorro de Energía que bajé consumo si no hay tráfico y si llega tráfico hacia el dispositivo conectado se envié un mensaje de encendido (Wake-On-Lan - WOL) Debe soportar IEEE 802.1X (Port Based Network Access Control) MTBF minimo de 10 Años (87600 horas) STP Root Guard, STP (802,1d), RSTP (IEEE 802.1w), MSTP (IEEE 802.1s), RPVST (Rapid per Vlan Spanning Tree) Todas las funcionalidades que soporte el equipo deben estar incluidas y soportadas a perpetuidad. No se acepta funcionalidades por suscripción. Certificaciones: FCC, CE, RCM, VCCI, BSMI, UL, CB, RoHS2 **Capacidades específicas para los switches de 24 puertos** Los equipos deben ser Appliances físicos (nuevos en su empaque original y sellados de fabrica) (No se aceptarán equipos remanufacturados y/o reparados y/o reformados). Interfaces Red Totales: 24x GE RJ45 and 4x 10GE SFP+ Puerto de Consola: 1 RJ-45 Tráfico: IPV4/IPV6 Switch Capacity: Mayor o igual a 128 GB	UNIDAD	3

	Packets Per Second: Mayor o igual a 190 Mpps VLANs: Mayor o igual a 4K Packet Buffers: Mayor o igual a 2 MB Memory: 512 MB ACL: 640		
	SUMINISTRO, INSTALACIÓN Y PUESTA EN FUNCIONAMIENTO DE SWITCH DE ACCESO MULTIGIGA 24 PUERTOS	UNIDAD	1
9	La solución de switches ofertada debe ser de la misma marca de la solución de acceso inalámbrico y la controladora de red de este proceso de contratación para garantizar el SD-LAN o SD-BRANCH de la Entidad. Los switches deben permitir descargar políticas de seguridad desde el firewall perimetral de la Entidad. Se debe poder administrar Switches, Access Point, SD-BRANCH, SD-WAN y Firewalls desde la misma consola de Administración (No se requieren consolas en la nube, la administración debe ser local). Debe estar en capacidad de detectar Dispositivos IoT Debe permitir la autenticación y autorización Local RADIUS y TACACS+ Debe soportar SSH Debe soportar DHCP snooping, Dynamic ARP Debe soportar una funcionalidad de ahorro de Energía que bajé consumo si no hay tráfico y si llega tráfico hacia el dispositivo conectado se envié un mensaje de encendido (Wake-On-Lan - WOL) Debe soportar IEEE 802.1X (Port Based Network Access Control) MTBF minimo de 10 Años (87600 horas) STP Root Guard, STP (802,1d), RSTP (IEEE 802.1w), MSTP (IEEE 802.1s), RPVST (Rapid per Vlan Spanning Tree) Todas las funcionalidades que soporte el equipo deben estar incluidas y soportadas a perpetuidad. No se acepta funcionalidades por suscripción. Certificaciones: FCC, CE, RCM, VCCI, BSMI, UL, CB, RoHS2 **Capacidades específicas para los switches de 24 puertos MULTIGIGA** Los equipos deben ser Appliances físicos (nuevos en su empaque original y sellados de fabrica) (No se aceptarán equipos remanufacturados y/o reparados y/o reformados). Interfaces Red Totales: 24x 2.5G/1G/100M RJ45 and 6x 10G/1G SFP+/SFP ports Puerto de Consola: 1 RJ-45 Tráfico: IPV4/IPV6 Switch Capacity: Mayor o igual a 240 GB Packets Per Second: Mayor o igual a 355 Mpps VLANs: Mayor o igual a 4K Packet Buffers: Mayor o igual a 2 MB Memory: 1 GB		
	INSTALACIÓN, RENOVACIÓN DE LICENCIA, Y PUESTA EN FUNCIONAMIENTO DE SWITCHES NO POE		
	Renovación de soporte y garantía de fabrica por 12 meses a partir de la suscripción del acta de inicio para los siguientes equipos FS 124F. El No. Serial de los equipos a renovar son los siguientes: S124FPTF24002200 S124FNTF24001962		

10	S124FNTF24001988 El oferente debe garantizar servicio de Soporte Técnico y garantía Premium con Servicio de asistencia técnica continua con cobertura 24/7 ante el fabricante a partir de la suscripción del acta de inicio, atención prioritaria ante incidentes críticos y reemplazo de hardware en caso de fallas (con un máximo de 8 días calendario). Incluye actualizaciones de software y firmware. Los switches deben permitir descargar políticas de seguridad desde el firewall perimetral de la Entidad. Se debe poder administrar Switches, Access Point, SD-BRANCH, SD-WAN y Firewalls desde la misma consola de Administración (No se requieren consolas en la nube, la administración debe ser local).	UNIDAD	1
11	**INSTALACIÓN, RENOVACIÓN DE LICENCIA, Y PUESTA EN FUNCIONAMIENTO DE SWITCH POE** Renovación de soporte y garantía de fabrica por 12 meses a partir de la suscripción del acta de inicio para el siguiente equipo FS 124F-POE. El No. Serial del equipo a renovar es el siguiente: S124FPTF230005065 El oferente debe garantizar servicio de Soporte Técnico y garantía Premium con Servicio de asistencia técnica continua con cobertura 24/7 ante el fabricante a partir de la suscripción del acta de inicio, atención prioritaria ante incidentes críticos y reemplazo de hardware en caso de fallas (con un máximo de 8 días calendario). Incluye actualizaciones de software y firmware. Los switches deben permitir descargar políticas de seguridad desde el firewall perimetral de la Entidad. Se debe poder administrar Switches, Access Point, SD-BRANCH, SD-WAN y Firewalls desde la misma consola de Administración (No se requieren consolas en la nube, la administración debe ser local).	UNIDAD	3
SOLUCIÓN DE ADMINISTRACIÓN CENTRALIZADA			
12	**PLATAFORMA DE ADMINISTRACIÓN CENTRALIZADA DE FIREWALL DE SEGURIDAD PERIMETRAL** Se debe entregar una plataforma o sistema de administración centralizada de dispositivos de seguridad perimetral que cuente con las siguientes características: Se requiere un equipo tipo appliance físico que permita Centralización de Configuración y monitoreo de todos los firewalls de nueva generación, así como todas sus funciones de protección de red y de SD-WAN (nuevo en su empaque original y sellado de fabrica) (No se aceptarán un equipo remanufacturado y/o reparado y/o reformado). **LA SOLUCIÓN DE ADMINISTRACIÓN CENTRALIZADA DEBE DAR SOPORTE A LAS SIGUIENTES CARACTERÍSTICAS:** Administrar mínimo 30 equipos Capacidad de Almacenamiento de hasta 8 Terabytes. Debe permitir Creación e implementación automatizada de configuraciones de dispositivos Permitir tener un solo repositorio de almacenamiento centralizado y administración de configuraciones, para simplificar las tareas de administración de una gran cantidad de dispositivos de seguridad con protección completa de contenido. Deberá tener integración nativa con la solución de seguridad	UNIDAD	1

	perimetral tipo Firewall. **FUNCIONALIDADES DE GESTION DE UTM/NGFW** La gestión debe permitir la creación y administración de políticas de firewall y control de aplicación. La gestión debe permitir la creación y administración de políticas de IPS, Antivírus y Anti-Spyware. La gestión debe permitir la creación y administración de políticas de Filtro de URL. Permitir buscar cuáles reglas un objeto está siendo utilizado. Debe atribuir secuencialmente un número a cada regla de firewall. Permitir la creación de reglas que permanezcan activas en horario definido. Permitir backup de las configuraciones y rollback de configuración para la última configuración. Debe tener mecanismos de validación de políticas avisando cuando haya reglas que ofusquen o conflictúen con otras (shadowing). Debe posibilitar la visualización y comparación de configuraciones actuales, configuraciones previas y configuraciones antiguas. Debe posibilitar que todos los firewalls sean controlados de manera centralizada utilizando solo un servidor de gestión. Cada servidor de gestión debe ser hospedado en un equipo independiente, no ejecutando función de firewall. La solución debe incluir una herramienta para gestionar centralmente las licencias de todos los aparatos controlados por estaciones de gestión, permitiendo al administrador actualizar licencias en los aparatos a través de esta herramienta. La solución debe permitir la distribución e instalación remota, de manera centralizada, de nuevas versiones de software de los aparatos. Debe ser capaz de generar reportes o presentar comparativos entre dos secciones distintas, resumiendo todos los cambios efectuados. Debe permitir crear flujos de aprobación en la solución de gestión, donde un administrador pueda crear todas las reglas, pero estas mismas solamente sean aplicadas después de la aprobación de otro administrador. Tener "wizard" en la solución de gestión para agregar los dispositivos por interfaz gráfica utilizando IP, login y clave de los mismos. Permitir que las políticas y los objetos ya presentes en los dispositivos sean importados cuando el mismo es agregado a la solución de gestión; Permitir la visualización, a partir de la estación de gestión centralizada, informaciones detalladas de los dispositivos gerenciados, tales como hostname, serial, IP de gestión, licencias, horario de lo sistema y firmware. Tener "wizard" en la solución de gestión para instalación de políticas y configuraciones de los dispositivos. Permitir crear en la solución de gestión templates de configuración de los dispositivos con informaciones de DNS, SNMP, configuraciones de LOG y administración. Permitir crear scripts customizados, que sean ejecutados de forma centralizada en un o más dispositivos gestionados con comandos de CLI de los mismos. Tener histórico de los scripts ejecutados en los dispositivos gestionados pela solución de gestión. Permitir configurar y visualizar balanceo de enlaces en los		

	dispositivos gestionados de forma centralizada. Permitir crear varios paquetes de políticas que serán aplicados/asociados a los dispositivos o grupos de dispositivos. Debe permitir crear reglas de NAT64 y NAT46 de forma centralizada. Permitir la creación de reglas anti DoS de forma centralizada. Permitir la creación de objetos que serán utilizados en las políticas de forma centralizada. Permitir crear a partir de la solución de gestión, VPNs entre los dispositivos gestionados de forma centralizada, incluyendo topología (hub, spoke, dial-up) autenticaciones, claves y métodos de criptografía. Garantía y licenciamiento del equipo y software ofertado, con servicio de soporte 7x24 de 12 meses a partir de su activación en el portal de fabricante, que incluya soporte telefónico y repuestos (estos repuestos deberán ser gestionados por el contratista en caso tal de requerirse un en tiempo no mayor a (08) días calendario).		
PRESTACIÓN DE SERVICIOS			
13	**Generalidades del Servicio:** El oferente debe contemplar en su oferta todos los costos o gastos asociados a la logística (desplazamiento, transporte, parqueaderos, equipos y herramientas de trabajo, refrigerios, entre otros) requerida para que el personal asignado al proyecto pueda cumplir sus funciones. **IMPLEMENTACIÓN:** Se debe dar cumplimento a la etapa del proyecto y entregar implementada y funcionando las soluciones completas, de acuerdo con los requerimientos y políticas establecidas por la entidad. Planeación de cada una de las actividades, validadas en conjunto con la entidad. Configuración y alistamiento del software a la última versión estable aprobada por el fabricante para la plataforma. Afinamiento y estabilización de las plataformas. Pruebas de Servicio de las plataformas. Entrega de las plataformas a satisfacción de la entidad Las actividades de implementación y/o afinamiento de las plataformas deben ser realizadas por personal certificado por el fabricante (se deben presentar las certificaciones del personal previo a la implementación de las plataformas). Se deberán realizar pruebas / muestras de las plataformas donde se evidencie la correcta configuración y afinamiento de cada plataforma. **SOPORTE Y/O MANTENIMIENTO:** El servicio de soporte debe incluir atención de incidentes sobre las plataformas ofertadas. Se debe garantizar soporte y garantía para las plataformas ofertadas en un esquema 7x24 por doce (12) meses a partir de la activación de las plataformas en el portal del fabricante, con soporte remoto o en sitio en caso de requerirse. El oferente debe contar con certificación vigente del Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO/IEC 27001:2022, expedida por un organismo de certificación acreditado en Colombia. La certificación debe estar vigente a la fecha de cierre del proceso y cubrir los servicios	-	-

asociados a la solución ofertada.
El oferente debe contar con certificación vigente del Sistema de Gestión de Servicios de TI conforme a la norma ISO/IEC 20000-1:2018, expedida por un organismo de certificación acreditado en Colombia. La certificación debe estar vigente a la fecha de cierre del proceso y cubrir la prestación y gestión de los servicios de tecnología de la información relacionados con la solución ofertada.
Realizar y documentar entre otras, las siguientes actividades previa coordinación con el supervisor del contrato en desarrollo:
Configurar los reportes / logs de las plataformas.
Mantener actualizados los niveles de Firmware de los componentes ofertados de acuerdo con las últimas versiones estables liberadas por el fabricante.
El horario de atención para el mantenimiento correctivo y preventivo debe ser de 7x24, sin costo adicional para la entidad.
Se deben incluir en la oferta dos (02) actividades de mantenimiento preventivo y afinamiento con el fin de minimizar problemas y mantener los sistemas actualizados, estas actividades deberán ser con previa aprobación del responsable TI de la entidad.
Al finalizar cada visita correctiva y/o preventiva el contratista deberá:
Generar un informe de servicio en el que se realice un resumen de las actividades realizadas (actualización, soporte y mantenimiento), problemas presentados, soluciones utilizadas y recomendaciones.
Consignar en la misma acta o informe de servicio si hubo cambio de software y/o en la configuración.
El soporte deberá contemplar:

El servicio de soporte debe incluir atención de incidentes sobre las plataformas ofertadas.
Consultas a través de llamadas telefónicas, correo electrónico
Sesiones remotas y atención en sitio (En caso de requerirse) en horario Hábil y No Hábil.

PRIORIDAD		DESCRIPCION
1	CRITICA	De manera remota (2) horas de atención y (3) horas de traslado a sitio
2	ALTA	De manera remota (3) horas de atención y (4) horas de traslado a sitio.
3	MEDIA	De manera remota (8) horas y de ser necesario traslado a sitio.
4	BAJA	De manera remota (24) horas y de ser necesario traslado a sitio.

TRANSFERENCIA DE CONOCIMIENTO

Realizar transferencia de conocimientos de 24 Horas para 3 funcionarios de la entidad, la cual debe incluir como mínimo temas de administración, configuración y afinamiento de las plataformas.

CERTIFICACIONES DEL PROPONENTE

El oferente debe presentar certificación de distribuidor autorizado del fabricante donde se evidencie que tiene el nivel de membresía más alto del fabricante (gold, premium, expert o platinum (según aplique el fabricante), esta certificación debe estar dirigida a la entidad y debe no ser mayor a 30 días calendario a la fecha de

	presentación de la propuesta. Lo anterior con el fin de garantizar por parte de la entidad el respaldo en la calidad en canal autorizado para la reventa y/o distribución de las soluciones que requiere la entidad. El oferente debe presentar al menos cinco (05) especialidades técnicas del mismo fabricante con el cual se está presentando, dentro de la cuales son obligatorias las siguientes (SD-WAN, Secure Networking Firewall, Secure Networking LAN). El oferente debe entregar junto con la propuesta una certificación emitida directamente del fabricante de las soluciones ofertadas donde se evidencie que los equipos suministrados no se encuentran en fin de venta y/o fin de vida y/o fin de soporte por un periodo mínimo de cinco (05) años contados a partir de la fecha de presentación de la propuesta, esta certificación debe ser dirigida a la Entidad, especificando el objeto y número de proceso público. **CAPACIDAD TÉCNICA** El contratista debe disponer dentro de su equipo de trabajo, con el siguiente personal mínimo, requerido por la Entidad para el desarrollo y ejecución del contrato, así como las certificaciones y experiencia descritas. **Un (1) Ingeniero - Gerente del Proyecto** Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones, industrial o carreras afines. Tarjeta Profesional con expedición mínimo de diez (10) años. Posgrado en Gerencia de Proyectos y/o certificación PMP Certificaciones vigentes ITILFoundation v3 o superior, ITIL Managing Professional y ITIL 4 Strategist Direct, Plan and Improve Certificate Experiencia mínima 5 proyectos gerenciando y/o coordinando proyectos de TI y/o Seguridad Informática. **Un (1) Ingeniero - Líder Técnico** Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones o carreras afines. ● Especialización o maestría en Seguridad de la Información ó informática ó Ciberseguridad. ● Certificación vigente en SCRUM Foundations Professional (SFPC). ● Certificación vigente en AUDITOR INTERNO en la norma ISO/IEC 20000-1:2018. ● Certificación vigente en AUDITOR LÍDER en la norma ISO/IEC 27001:2022. ● Certificación vigente en LÍDER GESTOR CIBERSEGURIDAD en la norma ISO/IEC 27032:2023. ● Certificación vigente como especialista en seguridad en redes. Emitida por el fabricante con el cual se esté presentado el proponente. Experiencia general de diez (10) años a partir de la expedición de la tarjeta profesional certificar mínimo de cinco (5) años de experiencia como líder o coordinador o gerente de servicios de TI.		

	Un (1) Ingeniero - Implementador Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones o carreras afines. ● Especialización o maestría en Seguridad de la Información ó informática ó Ciberseguridad. ● Certificación en AUDITOR INTERNO en la norma ISO/IEC 20000-1:2018. ● Certificación vigente en AUDITOR INTERNO en la norma ISO/IEC 27001:2022. ● Certificación vigente como profesional de seguridad en redes ● Certificación vigente como especialista en seguridad en redes Experiencia general de diez (10) años a partir de la expedición de la tarjeta profesional, debe certificar mínimo de cinco (5) años en implementación, soporte y/o monitoreo de soluciones de seguridad. **Un (01) Ingeniero de soporte Nivel 2** Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones o carreras afines. ● Especialización o maestría en Seguridad de la Información ó informática ó Ciberseguridad. ● Certificación vigente en AUDITOR INTERNO en la norma ISO/IEC 27001:2022. ● Certificación vigente como profesional de seguridad en redes ● Certificación vigente como especialista en seguridad en redes Experiencia general de siete (7) años a partir de la expedición de la tarjeta profesional, de los cuales debe certificar mínimo cinco (5) años en implementación, soporte y/o monitoreo de soluciones de seguridad. Nota: Cada uno de los perfiles debe presentarse por separado (ninguno podrá repetir cargo o rol), El oferente debe aportar en conjunto con la presentación de la propuesta la hoja de vida actualizada, certificaciones y contrato laborales de vinculación a la empresa o proponente participante (evitando figuras de tercerización) (a la fecha de presentación de la propuesta) evidenciando el cumplimiento de cada especificación solicitada.		

FICHAS TÉCNICAS: De acuerdo a lo preceptuado por el artículo 2.2.1.2.1.2.1. del Decreto 1082 de 2015, las fichas técnicas se indicarán en el pliego de condiciones del respectivo proceso de contratación, las cuales se entienden incorporadas a este documento, como las especificaciones técnicas del objeto a contratar.

2.4. OBLIGACIONES DE LAS PARTES.

2.4.1. OBLIGACIONES GENERALES DEL CONTRATISTA:

1. Garantizar la calidad de los bienes a suministrar de acuerdo con las especificaciones técnicas consignadas.
2. Acatar las órdenes que durante el desarrollo del contrato imparta el municipio y de manera general obrar con lealtad y buena fe en las distintas etapas contractuales.
3. Realizar el informe de ejecución, parciales y final, de acuerdo con lo pactado con el supervisor del contrato, dando estricto cumplimiento a las especificaciones técnicas del proyecto.

4. Mantener la confidencialidad de la información entregada por la entidad, en reserva o secreto, dándole a la misma el carácter estrictamente confidencial, y mantenerla debidamente protegida de accesos no autorizados a terceros, con el fin de no permitir su conocimiento o manejo por parte de tales terceros no autorizados. Así mismo, a no permitir la copia o reproducción total o parcial de la misma y devolverla una vez utilizadas para los fines estrictamente necesarios para la consultoría objeto del contrato.
5. Prestar las garantías exigidas por la entidad contratante en los términos y condiciones establecidas en el contrato.
6. Suscribir la correspondiente acta de inicio y la correspondiente acta de liquidación.
7. Pagar mensualmente la seguridad social y acreditarla durante la vigencia del contrato, de acuerdo a los lineamientos fijados por la Ley y el Ministerio de Protección Social, hasta que entre en vigencia el Decreto 1273 de 2018 que obliga a las entidades públicas a hacer las deducciones directamente.
8. No acceder a peticiones o amenazas de quienes actúen por fuera de la ley con el fin de obligarlos hacer u omitir algún acto o hecho. Cuando se presenten tales ocurrencias a la entidad contratante y a las demás autoridades competentes para que ellas adopten las medidas u correctivos que fueren necesarios. El incumplimiento de esta obligación y la celebración de pactos o acuerdos prohibidos dará lugar a la caducidad del contrato Art. 5 numeral 5 Ley 80 de 1993.
9. Las demás actividades necesarias para cumplir con el objeto contractual y que sean establecidas por el supervisor del contrato.

2.4.2. OBLIGACIONES ESPECÍFICAS DEL CONTRATISTA:

1. El contratista efectuará la entrega de lo solicitado en la ficha de especificaciones técnicas estipulada en los estudios previos, dentro del plazo establecidos.
2. El contratista deberá hacer entrega oportuna de los bienes, en las condiciones señaladas por la entidad, los cuales deben ser nuevos, originales, no usados ni remanufacturados y de excelente calidad.
3. El contratista es responsable de todos los costos por concepto de empaque, embalaje, transporte, traslado y demás costos operativos o logísticos necesarios para entregar los bienes objeto del contrato. En consecuencia, el contratista deberá empacar y embalar debidamente los bienes objeto del contrato, en materiales reciclables o reutilizables que garanticen su conservación durante el transporte al lugar de destino y su entrega en perfecto estado, sin rayones, golpes o deterioro, si aplica
4. El contratista deberá coordinar con el supervisor del contrato la fecha, hora y lugar de entrega de los bienes objeto del contrato, para coordinar con la Oficina TIC de la Alcaldía de Montería la revisión técnica de los elementos o dispositivos que se le van a entregar, permitiendo avalar los elementos adquiridos de acuerdo con las características y especificaciones solicitadas por un funcionario especializado en el tema.
5. Otorgar la garantía técnica de los productos adquiridos.
6. El contratista por la totalidad de los dispositivos entregados dará una capacitación (Transferencia de conocimiento) al personal requerido por parte beneficiario, es decir, la Alcaldía de Montería, tal y como se indica en la ficha técnica. La capacitación será dada por el personal idóneo y certificado en el área y manejo de estos dispositivos, allegando la hoja de vida y certificaciones que acrediten la idoneidad en el tema de capacitación antes de iniciar con las respectivas capacitaciones.
7. El proveedor deberá otorgar la garantía del fabricante, la cual no podrá ser inferior a tres (3) años como lo indica la ficha técnica.
8. Cambiar sin costo los bienes que no cumplan con las características y especificaciones definidas en la ficha técnica y que le sean solicitadas por la supervisión del contrato; dicho cambio se debe garantizar que llegue al sitio de entrega del elemento dentro de los cinco (5) días hábiles siguiente a la fecha de la solicitud.
9. El contratista deberá cambiar sin costo alguno los bienes defectuosos. Se entiende por bienes defectuosos, aquellos que, habiéndose recibido a satisfacción por la entidad contratante, a través de la supervisión, presente defectos con posterioridad a su entrega una vez se vaya a hacer uso de los mismo.
10. El contratista para garantizar el correcto funcionamiento del equipo, se compromete a realizar dos (2) visitas de revisión técnica por año dentro del término de garantía.
11. Disponer de un profesional en la materia 24/7 para recibir consultas, durante un plazo de doce (12) meses. Donde en primer lugar se realizará soporte técnico vía telefónica, en segundo lugar, se

realizará de manera remota (virtual) y como tercer modo, se realizará el soporte de manera presencial en caso de no solucionar previamente el requerimiento.
12. Informar oportunamente a la entidad, cuando exista o sobrevenga alguna de las inhabilidades e incompatibilidades previstas en la constitución y la ley.
13. Asumir los daños que se presenten durante el transporte de los bienes, entregando un nuevo producto de iguales o mejores especificaciones sin generarle algún costo a la entidad por cualquier concepto.
14. Los elementos deberán ingresar al Almacén de la entidad y cumplir con los procedimientos establecidos para tales fines.

2.4.4. OBLIGACIONES DEL MUNICIPIO:

1. Ejercer el respectivo control de ejecución y supervisión del Contrato.
2. Recibir de parte del CONTRATISTA los informes relacionados con la ejecución del contrato.
3. Expedir el cumplido correspondiente.
4. Suscribir con el CONTRATISTA las actas de iniciación, recibo y liquidación.
5. Cancelar el valor del presente contrato, en la forma prevista en los presentes estudios previos.
6. Adelantar las gestiones necesarias para hacer efectiva la garantía constituida por el contratista si a ello hubiere lugar.
7. Requerir al contratista para que adopte las medidas pertinentes cuando surjan faltas en el cumplimiento del contrato.

2.5. IDENTIFICACIÓN DEL CONTRATO A CELEBRAR:

La entidad prevé celebrar un contrato de compraventa, el cual se encuentra previsto dentro del artículo 1849 del Código Civil, el cual dispone: *"ARTICULO 1849. <CONCEPTO DE COMPRAVENTA>. La compraventa es un contrato en que una de las partes se obliga a dar una cosa y la otra a pagarla en dinero. Aquélla se dice vender y ésta comprar. El dinero que el comprador da por la cosa vendida se llama precio."*

2.6. PLAZO DE EJECUCIÓN: El plazo de ejecución será de **TRES (3) MESES.** Dicho plazo se contabilizará a partir de la suscripción del acta de inicio y previo cumplimiento de los requisitos de perfeccionamiento y ejecución contractual.

2.7. LUGAR Y EJECUCIÓN DEL CONTRATO: El contrato se desarrollará en el municipio de Montería - Departamento de Córdoba.

3. MODALIDAD DE SELECCIÓN DEL CONTRATISTA Y SU JUSTIFICACIÓN, INCLUYENDO LOS FUNDAMENTOS JURÍDICOS.

3.1. LA MODALIDAD DE SELECCIÓN DEL CONTRATISTA: La modalidad de selección del contratista previsto para adelantar este proceso es la de Selección Abreviada – Subasta Inversa.

3.2. JUSTIFICACIÓN Y FUNDAMENTO JURÍDICO DE LA MODALIDAD DE SELECCIÓN PREVISTA PARA LA CONTRATACIÓN:

Que de conformidad con lo dispuesto en el Decreto 310 del 2021[1], expedido por el Departamento Nacional de Planeación, las Entidades Estatales sometidas al Estatuto General de Contratación de la Administración Pública, están obligadas a adquirir Bienes y Servicios de Características Técnicas Uniformes de Común Utilización a través de los Acuerdos Marco de Precios previamente justificados, diseñados, organizados y celebrados por la Agencia Nacional de Contratación Pública -Colombia Compra Eficiente.

Que el uso obligatorio de los Acuerdos Marco de Precios organizados y celebrados por la Agencia Nacional de Contratación Pública -Colombia Compra Eficiente- por parte de las Entidades Estatales sometidas al Estatuto General de Contratación de la Administración Pública, se concibió de manera

[1] "Por el cual se reglamenta el artículo 41 de la Ley 1955 de 2019, sobre las condiciones para implementar la obligatoriedad y aplicación de los Acuerdos Marco de Precios y se modifican los artículos 2.2.1.2.1.2.7. y 2.2.1.2.1.2.12. del Decreto 1082 de 2015, Único Reglamentario del Sector Administrativo de Planeación Nacional"

gradual y en ese entendido la Agencia dispuso mediante la Circular 004-2021, un plan operativo de despliegue detallado para el ingreso gradual de las entidades, indicándose que a más tardar el 7 de octubre del 2021 y previo un programa de capacitación, los entes territoriales que sean capitales de departamento, como es el caso del Municipio de Montería, deberían ingresar a la Tienda Virtual del Estado Colombiano – TVEC.

Que por todo lo anterior, el Municipio de Montería, siguiendo los lineamientos de la Agencia Nacional de Contratación Pública – Colombia Compra Eficiente -, validó si el servicio de **"ADQUISICIÓN, INSTALACIÓN Y/O CONFIGURACIÓN Y PUESTA EN FUNCIONAMIENTO DE INFRAESTRUCTURA DE SEGURIDAD PERIMETRAL PARA EL FORTALECIMIENTO DE LA RED Y CONECTIVIDAD LAN/WLAN DE LA ALCALDIA DE MONTERÍA",** existía en la página web de la Tienda Virtual del Estado Colombiano[2] constatando que existe el acuerdo marco denominado *"Servicios de Conectividad IV (CCE-SNG-AMP-003-2024 – Proceso No. CCENEG-074-01-2024)"* donde se concluye que no es posible adquirir la solución a través de este acuerdo toda vez que el proyecto requerido contempla una solución integral de infraestructura y ciberseguridad, que incluye la adquisición e implementación de switches, access points, firewall de seguridad perimetral, además de servicios profesionales especializados para su diseño, implementación, configuración y puesta en operación.

Posteriormente, la Entidad validó la búsqueda en la Bolsa de Productos[3] que tiene disponible Bolsa Mercantil Colombiana en su página WEB, de conformidad con el Articulo 2.2.1.2.1.2.12. del decreto 310 de 2021 el cual establece: *"Planeación de una adquisición en la bolsa de productos; cuando no exista un Acuerdo Marco de Precios, para el bien o servicio requerido, es deber de las entidades de estudiar, comparar e identificar las ventajas de utilizar la bolsa de productos frente a la subasta inversa, análisis basado en el proceso de selección del comisionista, los costos asociados de selección, el valor de la comisión y las garantías, entre otros"*.

De igual forma, y con el objetivo de agotar el ejercicio comparativo entre las modalidades de selección, se consultó en la página institucional de la Bolsa Mercantil de Colombia las tarifas operacionales por concepto de gastos de operación y comisionistas de bolsa, así mismo en fecha 18 de junio de 2026 se solicitó a través de correo electrónico enviado al servicio al cliente de la Bolsa Mercantil de Colombia "servicioalcliente@bolsamercantil.com.co", indicara si era posible contratar el suministro de elementos papelería y útiles de escritorio y oficina con todas las condiciones técnicas descritas para el presente proceso, además nos remitiera un análisis del proceso de selección del comisionista, los costos asociados a dicha selección, el valor de la comisión y las garantías respectivas.



Outlook

Solicitud viabilidad seguridad perimetral

Desde Secretaria General <secretariageneral@monteria.gov.co>
Fecha Jue 18/06/2026 11:01
Para Marcelo Lopez Zuleta <marcelo.lopez@bolsamercantil.com.co>; servicioalcliente <servicioalcliente@bolsamercantil.com.co>
CC Kátherin Ramos Licona <kramos.tic@monteria.gov.co>

1 archivo adjunto (789 KB)
SOLICITUD DE VIABILIDAD SEGURIDAD.pdf;

Cordial saludo,

Por medio de la presente, se permite enviar solicitud de viabilidad del proceso cuyo objeto es ADQUISICIÓN, INSTALACIÓN Y/O CONFIGURACIÓN Y PUESTA EN FUNCIONAMIENTO DE INFRAESTRUCTURA DE SEGURIDAD PERIMETRAL PARA EL FORTALECIMIENTO DE LA RED Y CONECTIVIDAD LAN/WLAN DE LA ALCALDIA DE MONTERÍA.

Alcaldía de MONTERÍA
SECRETARÍA GENERAL
Edificio Antonio de la Torre y Miranda Cl 27 # 3 – 16 Montería – Córdoba

Secretaría General
www.monteria.gov.co

No imprima este correo de no ser necesario

De lo anterior no ha sido posible obtener respuesta por parte de BMC, por lo que la Entidad no ha podido realizar el análisis de costo – beneficio de que trata el articulo el Articulo 2.2.1.2.1.2.12. del Decreto 310 de 2021, puesto que no fue posible detallar en bolsa mercantil, las especificaciones

[2] https://colombiacompra.gov.co/content/tienda-virtual
[3] Hará parte integral de este estudio previo, la trazabilidad que da cuenta de la verificación efectuada en la Bolsa de Productos.

técnicas descritas en este documento, así como tampoco se conocen los costos asociados a la compra por BMC.

Que la trazabilidad de todo lo anterior se encuentra consignado en el documento denominado "*DOCUMENTO PARA LA TRAZABILIDAD DE VERIFICACIÓN DE BIENES Y SERVICIOS CON CARACTERÍSTICAS TÉCNICAS UNIFORMES EN LA TIENDA VIRTUAL DEL ESTADO COLOMBIANO Y BOLSA MERCANTIL DE COLOMBIA",* el cual hace parte integral del presente estudio previo.

Lo anterior de conformidad con lo previsto en el artículo 2 numeral 2 literal a) de la Ley 1150 de 2007 a saber:

> ***"2) Selección Abreviada.*** *La selección abreviada corresponde a la modalidad de selección objetiva prevista para aquellos casos en que, por las características del objeto a contratar, las circunstancias de la contratación o la cuantía o destinación del bien, obra o servicios, pueden adelantarse procesos simplificados para garantizar la eficiencia de la gestión contractual.*
>
> *Serán causales de selección abreviada las siguientes:*
>
> *a) La adquisición o suministro de bienes y servicios de características técnicas uniformes y de común utilización por parte de las entidades, que corresponden a aquellos que poseen las mismas especificaciones técnicas, con independencia de su diseño o de sus características descriptivas, y comparten patrones de desempeño y calidad objetivamente definidos.*
>
> *Para la adquisición de estos bienes y servicios las entidades deberán, siempre que el reglamento así lo señale, hacer uso de procedimientos de subasta inversa o de instrumentos de compra por catálogo derivados de la celebración de acuerdos marco de precios o de procedimientos de adquisición en bolsas de productos."*

Por lo anterior, se utilizará el proceso de selección abreviada en la modalidad de subasta inversa de acuerdo al Decreto 1082 de 2015.

4. EL VALOR ESTIMADO DEL CONTRATO Y LA JUSTIFICACIÓN DEL MISMO.

4.1. VALOR ESTIMADO DEL CONTRATO: El valor de la presente contratación no podrá superar la suma de **SEISCIENTOS SESENTA Y UN MILLONES CUATROCIENTOS NOVENTA MIL SEISCIENTOS DIECISIETE PESOS M/CTE. ($661.490.617 M/CTE.),** incluidos todos los costos directos e indirectos e impuestos que se puedan generar con la celebración del contrato.

Los impuestos que se causen correrán por cuenta del contratista y se consideraran incluidos como parte del precio todos los derechos, tasas y contribuciones que se originen en el desarrollo del contrato, sean estos de carácter Nacional, Departamental o Municipal.

Los valores antes descritos incluyen todos los costos directos e indirectos.

El presupuesto estimado para la contratación es el siguiente:

SUMINISTRO, INSTALACIÓN Y PUESTA EN FUNCIONAMIENTO DE FIREWALL DE SEGURIDAD PERIMETRAL CORE	UNIDAD	CANTIDAD	PROMEDIO	
			VALOR UNITARIO	VALOR TOTAL
GENERALIDADES Los equipos deben cumplir con las siguientes características mínimas de desempeño activas y funcionales en la puesta en marcha de las plataformas. Los equipos deben ser Appliances físicos (nuevos en su empaque original y sellados de fabrica) (No se aceptarán equipos remanufacturados y/o reparados y/o reformados). Los equipos deben ser de propósito específico tipo Firewall. Los equipos deben contar con tecnología ASIC para permitir acelerar los procesos (no solo por CPU) y de esta manera permita mejorar el rendimiento del procesamiento de tráfico. La solución debe pertenecer al cuadrante de líder de Gartner para Hybrid Mesh Firewall y SD-WAN en su último reporte publicado. **Capacidades operativas mínimas de cada equipo:** NGFW Throughput: 3.1 Gbps o superior Firewall Throughput: 37 Gbps o superior IPS Throughput: 5 Gbps o superior Threat Protection Throughput: 2.8 Gbps o superior	UNIDAD	4	$ 60.507.750	$ 242.031.001

VPN SSL Throughput: 1.5 Gbps o superior Inspección SSL Throughput: 3 Gbps o superior Sesiones Concurrentes: 3.000.000 o superior Disco Interno 480 GB SSD o superior IPsec VPN Throughput: 33 Gbps o superior 4 interfaces de 10 GE SFP+ (se deben incluir en la oferta ocho (08) transceivers SFP+ SR con sus respectivos cables de F.O.) 8 interfaces de 1 GE SFP (se deben incluir en la oferta ocho (02) transceivers SFP SR con sus respectivos cables de F.O.) 16 interfaces de 1 GE RJ45 **Funcionalidades generales firewall (Core)** **Capacidades de NAT (Network Address Translation)** Las plataformas deben soportar lo siguientes tipos de traducción de direcciones: NAT y PAT NAT estático NAT: destino, origen NAT, NAT64 persistente **Funciones básicas de Firewall** Las reglas de firewall deben analizar las conexiones que pasen por el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs. La solución debe integrarse con el directorio activo y soportar políticas basadas en identidad. Esto significa que podrán definirse políticas de seguridad de acuerdo con el grupo de pertenencia de los usuarios. Debe tener la capacidad de generar una advertencia al administrador cuando este configure una política duplicada Debe estar en la capacidad de integrase con plataforma Cloud IaaS como: AWS,Azure,Google etc. Con el fin de generar y actualizar objetos de direcciones de manera automática basado en los parámetros de red (IP, TAG, etc) de las instancias desplegadas en la nube y estas ser usadas como objetos de reglas o políticas de firewall Debe soportar reglas de firewall en IPv6 configurables tanto por CLI (Command Line Interfaz) como por GUI (Graphical User Interfaz). La solución tendrá la capacidad de hacer captura de paquetes por política de seguridad implementada para luego ser exportado en formato PCAP. El dispositivo será capaz de crear e integrar políticas contra ataques DoS (Denial of service) las cuales se deben poder aplicar por interfaces. El dispositivo será capaz de ejecutar inspección de tráfico SSL en todos los puertos y seleccionar bajo que certificado será válido este tráfico. Tendrá la capacidad de hacer escaneo a profundidad de tráfico tipo SSH dentro de todos o cierto rango de puertos configurados para este análisis. **Conectividad y enrutamiento** Funcionalidad de DHCP: como Cliente DHCP, Servidor DHCP y reenvío (Relay) de solicitudes DHCP. Soporte de enrutamiento estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas. Soporte a enrutamiento dinámico RIP V1, V2, OSPF y BGP. La solución podrá habilitar políticas de enrutamiento en IPv6. La solución deberá ser capaz de habilitar enrutamiento estático para cada interfaz en IPv6. **VPN IPsec** Los equipos deben soportar las siguientes características: Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site). Soporte para IKEv2 y IKE Configuration Method. Soporte de VPNs con algoritmos de cifrado: AES, DES, 3DES Se debe soportar longitudes de llave para AES de 128, 192 y 256 bits **Autenticación** Los dispositivos deben manejar los siguientes tipos de autenticación: Capacidad de soporta autenticación local y remota integrándose con Servidores de Autenticación RADIUS, LDAP o TACACS+. Capacidad incluida, al integrarse con Microsoft Windows Active Directory o Novell eDirectory, de autenticar transparentemente usuarios sin preguntarles username o password. Esto es aprovechar las credenciales del dominio de Windows bajo un concepto “Single-Sign-On”. Soporte de Token Físicos o Mobile sobre Smartphone basado en IOS o Android, token de SMS, email o con plataformas de terceros como RSA SecurID. Capacidad de soportar autenticación de acceso de usuario a través de 802.1x y portal cautivo. **Manejo de tráfico y calidad de servicio** La solución debe soportar balanceo de enlaces WAN inteligente (SD-WAN Seguro) sin licencia adicional basado en: Aplicaciones cloud, SLA y Mejor calidad de enlace basado en (Jitter, latencia, ancho de banda, perdida de paquetes). Capacidad de poder asignar parámetros de traffic shapping atreves de reglas de manera independiente. Capacidad de poder asignar parámetros de traffic shaping diferenciadas para el tráfico en distintos sentidos de una misma sesión. Capacidad de definir parámetros de traffic shaping que apliquen para cada dirección IP en forma independiente, en contraste con la aplicación y categoría URL de las mismas para la regla en general. Capacidad de poder definir límite de ancho de banda (ancho de banda máximo) en Kilobits por segundo. **Antimalware** Debe ser capaz de analizar, establecer control de acceso y detener ataques y hacer Antivirus en tiempo real en al menos los siguientes protocolos aplicativos: HTTP, SMTP, IMAP, POP3, FTP.MAPI El módulo de antimalware debe haber sido desarrollado por el mismo fabricante de la solución de firewall, así como las firmas deben ser de su propiedad y no por medio de licenciamiento o concesiones de un tercero, esto con el fin de garantizar la idoneidad de la protección, así como los tiempos de respuesta del soporte de la misma. Debe soportar la inspección de archivos comprimidos como los son: GZIP,RAR,LZH,IHA,CAB,ARJ;ZIP entre otros con el fin de proteger contra estas técnicas de evasión. El Antivirus debe integrarse de forma nativa con una solución Sandbox del mismo fabricante, de tal manera que envíen muestras de archivos a dicho dispositivo para su análisis. **Filtrado Web** Facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías. Por flexibilidad, el filtro de URLs debe tener por lo menos 78 categorías y por lo menos 47 millones de sitios web en la base de datos. Debe poder categorizar contenido Web requerido mediante IPv6. Será posible exceptuar la inspección de HTTPS por categoría. Debe contar con la capacidad de bloquear contenido de YouTube usando el Channel ID El filtrado debe ser sobre tráfico http y https. **Protección contra intrusos (IPS)** El sistema de detección y prevención de intrusos deben poder implementarse tanto en línea como fuera de línea. En línea, el tráfico a ser inspeccionado pasará a través del equipo. Fuera de línea, el equipo recibirá el tráfico a inspeccionar desde un switch con un puerto configurado en span o mirror. Debe ser posible definir políticas de detección y prevención de intrusiones para tráfico IPv6. A través de sensores. Capacidad de detección de más de 7000 ataques. El sistema de detección y prevención de intrusos debe estar integrado a la plataforma de seguridad “appliance”. Sin necesidad de instalar un servidor o appliance externo, La interfaz de administración del sistema de detección y prevención de intrusos deberá de estar perfectamente integrada a la interfaz de administración del dispositivo de seguridad appliance, sin necesidad de integrar otro tipo de consola para poder administrar este servicio. Esta deberá permitir la protección de este servicio por política de control de acceso. Debe ofrecerse la posibilidad de guardar información sobre el paquete de red que detonó la detección del ataque, así como al menos los 5 paquetes sucesivos. Estos paquetes deben poder ser visualizados por una herramienta que soporte el formato PCAP. **Control de aplicaciones** La solución debe soportar la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo. La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico.				

La solución debe tener un listado de al menos 3000 aplicaciones ya definidas por el fabricante. Para aplicaciones identificadas deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log y resetear conexión **Inspección de Contenido SSL/SSH** La solución debe soportar inspeccionar tráfico que esté siendo encriptado mediante SSL al menos para los siguientes protocolos: HTTP, IMAP, SMTP, POP3 y FTP en su versión segura. Debe ser posible definir perfiles de inspección SSL donde se definan los protocolos a inspeccionar y el certificado usado, estos perfiles deben poder ser escogidos una vez se defina la política de seguridad. La inspección debe realizarse: mediante la técnica conocida como Hombre en el Medio (MITM – Man In The Middle) para una inspección completa o solo inspeccionando el certificado sin necesidad de hacer full inspection. **Alta disponibilidad** El dispositivo deberá soportar Alta Disponibilidad transparente, es decir, sin pérdida de conexiones en caso de que un nodo falle tanto para IPV4 como para IPV6 Alta Disponibilidad en modo Activo-Activo de forma automática sin requerir hacer políticas de enrutamiento basado en orígenes y destino para poder hacer la distribución del tráfico. El equipo debe soportar hasta 2 equipos en esquema de HA. **Visibilidad** La solución debe estar en la capacidad de visualizar el tráfico de usuario, aplicaciones, navegación y niveles de riesgo en tiempo real, esto deberá ser sobre la misma plataforma sin necesidad de software o licenciamiento adicional. Deber tener la capacidad de poder validar con que política la sesión se está coincidiendo y un link hacia la misma. **Características de Administración** Interfaz gráfica de usuario (GUI), vía Web por HTTP y HTTPS para hacer administración de las políticas de seguridad y que forme parte de la arquitectura nativa de la solución para administrar la solución localmente. Por seguridad la interfaz debe soportar SSL sobre HTTP (HTTPS) Soporte de al menos 3 servidores syslog para poder enviar bitácoras a servidores de SYSLOG remotos Debe tener la capacidad de gestionar todas las políticas de seguridad, además de poder gestionar Switches y APs dentro de una única consola de gestión. **Licenciamiento y actualizaciones** El licenciamiento de todas las funcionalidades debe ser ILIMITADO en cuanto a usuarios, conexiones, VPNs equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo. La vigencia de las actualizaciones para los servicios de Antivirus, AntiSpam, IPS, Application Control y URL Filtering debe proveerse por al menos doce (12) meses a partir de su activación en el portal del fabricante. La plataforma es requerida por un periodo de doce (12) meses en un esquema de soporte 7x24 ante el fabricante a partir de su activación en el portal del fabricante. Garantía y licenciamiento de los equipos y software ofertados, con Servicio de soporte 7x24 de 12 meses a partir de su activación en el portal de fabricante, que incluya Soporte Telefónico y repuestos (estos repuestos deberán ser gestionados por el contratista en caso tal de requerirse un en tiempo no mayor a (08) días calendario).				
SUMINISTRO, INSTALACIÓN Y PUESTA EN FUNCIONAMIENTO DE FIREWALL DE SEGURIDAD PERIMETRAL MULTIGIGA				
Los equipos deben cumplir con las siguientes características mínimas de desempeño activas y funcionales en la puesta en marcha de las plataformas. Los equipos deben ser Appliances físicos (nuevos en su empaque original y sellados de fabrica) (No se aceptarán equipos remanufacturados y/o reparados y/o reformados). Los equipos deben ser de propósito específico tipo Firewall. Los equipos deben contar con tecnología ASIC para permitir acelerar los procesos (no solo por CPU) y de esta manera permita mejorar el rendimiento del procesamiento de tráfico. La solución debe pertenecer al cuadrante de líder de Gartner para Hybrid Mesh Firewall y SD-WAN en su último reporte publicado. **Capacidades operativas mínimas de cada equipo:** NGFW Throughput: 2.5 Gbps o superior Firewall Throughput: 27 Gbps o superior IPS Throughput: 4.5 Gbps o superior Threat Protection Throughput: 2.1 Gbps o superior VPN SSL Throughput: 1.3 Gbps o superior Inspección SSL Throughput: 2.6 Gbps o superior Sesiones Concurrentes: 3.000.000 o superior Disco Interno 120 GB SSD o superior IPsec VPN Throughput: 25 Gbps o superior 2 interfaces de 10 GE SFP+ (se deben incluir en la oferta seis (06) transceivers SFP+ SR con sus respectivos cables de F.O.) 2 interfaces multigiga 10/5/2.5 GE RJ45 8 interfaces de 1 GE RJ45 **Funcionalidades generales firewall (Multigiga)** **Capacidades de NAT (Network Address Translation)** Las plataformas deben soportar lo siguientes tipos de traducción de direcciones: NAT y PAT NAT estático NAT: destino, origen NAT, NAT64 persistente **Funciones básicas de Firewall** Las reglas de firewall deben analizar las conexiones que pasen por el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs. La solución debe integrarse con el directorio activo y soportar políticas basadas en identidad. Esto significa que podrán definirse políticas de seguridad de acuerdo con el grupo de pertenencia de los usuarios. Debe tener la capacidad de generar una advertencia al administrador cuando este configure una política duplicada Debe estar en la capacidad de integrase con plataforma Cloud IaaS como: AWS,Azure,Google etc. Con el fin de generar y actualizar objetos de direcciones de manera automática basado en los parámetros de red (IP, TAG, etc) de las instancias desplegadas en la nube y estas ser usadas como objetos de reglas o políticas de firewall Debe soportar reglas de firewall en IPv6 configurables tanto por CLI (Command Line Interfaz) como por GUI (Graphical User Interfaz). La solución tendrá la capacidad de hacer captura de paquetes por política de seguridad implementada para luego ser exportado en formato PCAP. El dispositivo será capaz de crear e integrar políticas contra ataques DoS (Denial of service) las cuales se deben poder aplicar por interfaces. El dispositivo será capaz de ejecutar inspección de tráfico SSL en todos los puertos y seleccionar bajo que certificado será válido este tráfico. Tendrá la capacidad de hacer escaneo a profundidad de tráfico tipo SSH dentro de todos o cierto rango de puertos configurados para este análisis. **Conectividad y enrutamiento** Funcionalidad de DHCP: como Cliente DHCP, Servidor DHCP y reenvío (Relay) de solicitudes DHCP. Soporte de enrutamiento estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas. Soporte a enrutamiento dinámico RIP V1, V2, OSPF y BGP. La solución podrá habilitar políticas de enrutamiento en IPv6. La solución deberá ser capaz de habilitar enrutamiento estático para cada interfaz en IPv6. **VPN IPsec** Los equipos deben soportar las siguientes características: Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site). Soporte para IKEv2 y IKE Configuration Method. Soporte de VPNs con algoritmos de cifrado: AES, DES, 3DES Se debe soportar longitudes de llave para AES de 128, 192 y 256 bits **Autenticación** Los dispositivos deben manejar los siguientes tipos de autenticación:	**UNIDAD**	**1**	$ 14.578.897	$ 14.578.897

Capacidad de soporta autenticación local y remota integrándose con Servidores de Autenticación RADIUS, LDAP o TACACS+. Capacidad incluida, al integrarse con Microsoft Windows Active Directory o Novell eDirectory, de autenticar transparentemente usuarios sin preguntarles username o password. Esto es aprovechar las credenciales del dominio de Windows bajo un concepto "Single-Sign-On". Soporte de Token Físicos o Mobile sobre Smartphone basado en IOS o Android, token de SMS, email o con plataformas de terceros como RSA SecurID. Capacidad de soportar autenticación de acceso de usuario a través de 802.1x y portal cautivo. **Manejo de tráfico y calidad de servicio** La solución debe soportar balanceo de enlaces WAN inteligente (SD-WAN Seguro) sin licencia adicional basado en: Aplicaciones cloud, SLA y Mejor calidad de enlace basado en (Jitter, latencia, ancho de banda, perdida de paquetes). Capacidad de poder asignar parámetros de traffic shapping atreves de reglas de manera independiente. Capacidad de poder asignar parámetros de traffic shaping diferenciadas para el tráfico en distintos sentidos de una misma sesión. Capacidad de definir parámetros de traffic shaping que apliquen para cada dirección IP en forma independiente, en contraste con la aplicación y categoría URL de las mismas para la regla en general. Capacidad de poder definir límite de ancho de banda (ancho de banda máximo) en Kilobits por segundo. **Antimalware** Debe ser capaz de analizar, establecer control de acceso y detener ataques y hacer Antivirus en tiempo real en al menos los siguientes protocolos aplicativos: HTTP, SMTP, IMAP, POP3, FTP.MAPI El módulo de antimalware debe haber sido desarrollado por el mismo fabricante de la solución de firewall, así como las firmas deben ser de su propiedad y no por medio de licenciamiento o concesiones de un tercero, esto con el fin de garantizar la idoneidad de la protección, así como los tiempos de respuesta del soporte de la misma. Debe soportar la inspección de archivos comprimidos como los son: GZIP,RAR,LZH,IHA,CAB,ARJ;ZIP entre otros con el fin de proteger contra estas técnicas de evasión. El Antivirus debe integrarse de forma nativa con una solución Sandbox del mismo fabricante, de tal manera que envíen muestras de archivos a dicho dispositivo para su análisis. **Filtrado Web** Facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías. Por flexibilidad, el filtro de URLs debe tener por lo menos 78 categorías y por lo menos 47 millones de sitios web en la base de datos. Debe poder categorizar contenido Web requerido mediante IPv6. Será posible exceptuar la inspección de HTTPS por categoría. Debe contar con la capacidad de bloquear contenido de YouTube usando el Channel ID El filtrado debe ser sobre tráfico http y https. **Protección contra intrusos (IPS)** El sistema de detección y prevención de intrusos deben poder implementarse tanto en línea como fuera de línea. En línea, el tráfico a ser inspeccionado pasará a través del equipo. Fuera de línea, el equipo recibirá el tráfico a inspeccionar desde un switch con un puerto configurado en span o mirror. Debe ser posible definir políticas de detección y prevención de intrusiones para tráfico IPv6. A través de sensores. Capacidad de detección de más de 7000 ataques. El sistema de detección y prevención de intrusos debe estar integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o appliance externo, La interfaz de administración del sistema de detección y prevención de intrusos deberá de estar perfectamente integrada a la interfaz de administración del dispositivo de seguridad appliance, sin necesidad de integrar otro tipo de consola para poder administrar este servicio. Esta deberá permitir la protección de este servicio por política de control de acceso. Debe ofrecerse la posibilidad de guardar información sobre el paquete de red que detonó la detección del ataque, así como al menos los 5 paquetes sucesivos. Estos paquetes deben poder ser visualizados por una herramienta que soporte el formato PCAP. **Control de aplicaciones** La solución debe soportar la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo. La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico. La solución debe tener un listado de al menos 3000 aplicaciones ya definidas por el fabricante. Para aplicaciones identificadas deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log y resetear conexión **Inspección de Contenido SSL/SSH** La solución debe soportar inspeccionar tráfico que esté siendo encriptado mediante SSL al menos para los siguientes protocolos: HTTP, IMAP, SMTP, POP3 y FTP en su versión segura. Debe ser posible definir perfiles de inspección SSL donde se definan los protocolos a inspeccionar y el certificado usado, estos perfiles deben poder ser escogidos una vez se defina la política de seguridad. La inspección debe realizarse: mediante la técnica conocida como Hombre en el Medio (MITM – Man In The Middle) para una inspección completa o solo inspeccionando el certificado sin necesidad de hacer full inspection. **Alta disponibilidad** El dispositivo deberá soportar Alta Disponibilidad transparente, es decir, sin pérdida de conexiones en caso de que un nodo falle tanto para IPV4 como para IPV6 Alta Disponibilidad en modo Activo-Activo de forma automática sin requerir hacer políticas de enrutamiento basado en orígenes y destino para poder hacer la distribución del tráfico. El equipo debe soportar hasta 2 equipos en esquema de HA. **Visibilidad** La solución debe estar en la capacidad de visualizar el tráfico de usuario, aplicaciones, navegación y niveles de riesgo en tiempo real, esto deberá ser sobre la misma plataforma sin necesidad de software o licenciamiento adicional. Deber tener la capacidad de poder validar con que política la sesión se está coincidiendo y un link hacia la misma. **Características de Administración** Interfaz gráfica de usuario (GUI), vía Web por HTTP y HTTPS para hacer administración de las políticas de seguridad y que forme parte de la arquitectura nativa de la solución para administrar la solución localmente. Por seguridad la interfaz debe soportar SSL sobre HTTP (HTTPS) Soporte de al menos 3 servidores syslog para poder enviar bitácoras a servidores de SYSLOG remotos Debe tener la capacidad de gestionar todas las políticas de seguridad, además de poder gestionar Switches y APs dentro de una única consola de gestión. **Licenciamiento y actualizaciones** El licenciamiento de todas las funcionalidades debe ser ILIMITADO en cuanto a usuarios, conexiones, VPNs equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo. La vigencia de las actualizaciones para los servicios de Antivirus, AntiSpam, IPS, Application Control y URL Filtering debe proveerse por al menos doce (12) meses a partir de su activación en el portal del fabricante. La plataforma es requerida por un periodo de doce (12) meses en un esquema de soporte 7x24 ante el fabricante a partir de su activación en el portal del fabricante. Garantía y licenciamiento de los equipos y software ofertados, con Servicio de soporte 7x24 de 12 meses a partir de su activación en el portal de fabricante, que incluya Soporte Telefónico y repuestos (estos repuestos deberán ser gestionados por el contratista en caso tal de requerirse un en tiempo no mayor a (08) días calendario).				
SUMINISTRO, INSTALACIÓN Y PUESTA EN FUNCIONAMIENTO DE FIREWALL DE SEGURIDAD PERIMETRAL BASICO				
GENERALIDADES Los equipos deben cumplir con las siguientes características mínimas de desempeño activas y funcionales en la puesta en marcha de las plataformas. Los equipos deben ser Appliances físicos (nuevos en su empaque original y sellados de fabrica) (No se aceptarán equipos remanufacturados y/o reparados y/o reformados). Los equipos deben ser de propósito específico tipo Firewall. Los equipos deben contar con tecnología ASIC para permitir acelerar los procesos (no solo por CPU) y de esta manera permita mejorar el rendimiento del procesamiento de tráfico. La solución debe pertenecer al cuadrante de líder de Gartner para Hybrid Mesh Firewall y SD-WAN en su último reporte publicado. **Capacidades operativas mínimas de cada equipo:**	**UNIDAD**	**1**	$ 8.161.850	$ 8.161.850

NGFW Throughput: 1.2 Gbps o superior Firewall Throughput: 5 Gbps o superior IPS Throughput: 2.2 Gbps o superior Threat Protection Throughput: 1.1 Gbps o superior Inspección SSL Throughput: 1.3 Gbps o superior Sesiones Concurrentes: 720000 o superior Disco Interno 64 GB SSD o superior IPsec VPN Throughput: 4.5 Gbps o superior 5 interfaces de 1 GE RJ45 1 puerto de consola RJ45 **Funcionalidades generales firewall (Basico)** **Capacidades de NAT (Network Address Translation)** Las plataformas deben soportar lo siguientes tipos de traducción de direcciones: NAT y PAT NAT estático NAT: destino, origen NAT, NAT64 persistente **Funciones básicas de Firewall** Las reglas de firewall deben analizar las conexiones que pasen por el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs. La solución debe integrarse con el directorio activo y soportar políticas basadas en identidad. Esto significa que podrán definirse políticas de seguridad de acuerdo con el grupo de pertenencia de los usuarios. Debe tener la capacidad de generar una advertencia al administrador cuando este configure una política duplicada Debe estar en la capacidad de integrase con plataforma Cloud IaaS como: AWS,Azure,Google etc. Con el fin de generar y actualizar objetos de direcciones de manera automática basado en los parámetros de red (IP, TAG, etc) de las instancias desplegadas en la nube y estas ser usadas como objetos de reglas o políticas de firewall Debe soportar reglas de firewall en IPv6 configurables tanto por CLI (Command Line Interfaz) como por GUI (Graphical User Interfaz). La solución tendrá la capacidad de hacer captura de paquetes por política de seguridad implementada para luego ser exportado en formato PCAP. El dispositivo será capaz de crear e integrar políticas contra ataques DoS (Denial of service) las cuales se deben poder aplicar por interfaces. El dispositivo será capaz de ejecutar inspección de tráfico SSL en todos los puertos y seleccionar bajo que certificado será válido este tráfico. Tendrá la capacidad de hacer escaneo a profundidad de tráfico tipo SSH dentro de todos o cierto rango de puertos configurados para este análisis. **Conectividad y enrutamiento** Funcionalidad de DHCP: como Cliente DHCP, Servidor DHCP y reenvío (Relay) de solicitudes DHCP. Soporte de enrutamiento estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas. Soporte a enrutamiento dinámico RIP V1, V2, OSPF y BGP. La solución podrá habilitar políticas de enrutamiento en IPv6. La solución deberá ser capaz de habilitar enrutamiento estático para cada interfaz en IPv6. **VPN IPsec** Los equipos deben soportar las siguientes características: Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site). Soporte para IKEv2 y IKE Configuration Method. Soporte de VPNs con algoritmos de cifrado: AES, DES, 3DES Se debe soportar longitudes de llave para AES de 128, 192 y 256 bits **Autenticación** Los dispositivos deben manejar los siguientes tipos de autenticación: Capacidad de soporta autenticación local y remota integrándose con Servidores de Autenticación RADIUS, LDAP o TACACS+. Capacidad incluida, al integrarse con Microsoft Windows Active Directory o Novell eDirectory, de autenticar transparentemente usuarios sin preguntarles username o password. Esto es aprovechar las credenciales del dominio de Windows bajo un concepto “Single-Sign-On”. Soporte de Token Físicos o Mobile sobre Smartphone basado en IOS o Android, token de SMS, email o con plataformas de terceros como RSA SecurID. Capacidad de soportar autenticación de acceso de usuario a través de 802.1x y portal cautivo. **Manejo de tráfico y calidad de servicio** La solución debe soportar balanceo de enlaces WAN inteligente (SD-WAN Seguro) sin licencia adicional basado en: Aplicaciones cloud, SLA y Mejor calidad de enlace basado en (Jitter, latencia, ancho de banda, perdida de paquetes). Capacidad de poder asignar parámetros de traffic shapping atreves de reglas de manera independiente. Capacidad de poder asignar parámetros de traffic shaping diferenciadas para el tráfico en distintos sentidos de una misma sesión. Capacidad de definir parámetros de traffic shaping que apliquen para cada dirección IP en forma independiente, en contraste con la aplicación y categoría URL de las mismas para la regla en general. Capacidad de poder definir límite de ancho de banda (ancho de banda máximo) en Kilobits por segundo. **Antimalware** Debe ser capaz de analizar, establecer control de acceso y detener ataques y hacer Antivirus en tiempo real en al menos los siguientes protocolos aplicativos: HTTP, SMTP, IMAP, POP3, FTP.MAPI El módulo de antimalware debe haber sido desarrollado por el mismo fabricante de la solución de firewall, así como las firmas deben ser de su propiedad y no por medio de licenciamiento o concesiones de un tercero, esto con el fin de garantizar la idoneidad de la protección, así como los tiempos de respuesta del soporte de la misma. Debe soportar la inspección de archivos comprimidos como los son: GZIP,RAR,LZH,IHA,CAB,ARJ;ZIP entre otros con el fin de proteger contra estas técnicas de evasión. El Antivirus debe integrarse de forma nativa con una solución Sandbox del mismo fabricante, de tal manera que envíen muestras de archivos a dicho dispositivo para su análisis. **Filtrado Web** Facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías. Por flexibilidad, el filtro de URLs debe tener por lo menos 78 categorías y por lo menos 47 millones de sitios web en la base de datos. Debe poder categorizar contenido Web requerido mediante IPv6. Será posible exceptuar la inspección de HTTPS por categoría. Debe contar con la capacidad de bloquear contenido de YouTube usando el Channel ID El filtrado debe ser sobre tráfico http y https. **Protección contra intrusos (IPS)** El sistema de detección y prevención de intrusos deben poder implementarse tanto en línea como fuera de línea. En línea, el tráfico a ser inspeccionado pasará a través del equipo. Fuera de línea, el equipo recibirá el tráfico a inspeccionar desde un switch con un puerto configurado en span o mirror. Debe ser posible definir políticas de detección y prevención de intrusiones para tráfico IPv6. A través de sensores. Capacidad de detección de más de 7000 ataques. El sistema de detección y prevención de intrusos debe estar integrado a la plataforma de seguridad “appliance”. Sin necesidad de instalar un servidor o appliance externo, La interfaz de administración del sistema de detección y prevención de intrusos deberá de estar perfectamente integrada a la interfaz de administración del dispositivo de seguridad appliance, sin necesidad de integrar otro tipo de consola para poder administrar este servicio. Esta deberá permitir la protección de este servicio por política de control de acceso. Debe ofrecerse la posibilidad de guardar información sobre el paquete de red que detonó la detección del ataque, así como al menos los 5 paquetes sucesivos. Estos paquetes deben poder ser visualizados por una herramienta que soporte el formato PCAP. **Control de aplicaciones** La solución debe soportar la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo. La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico.				

La solución debe tener un listado de al menos 3000 aplicaciones ya definidas por el fabricante. Para aplicaciones identificadas deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log y resetear conexión **Inspección de Contenido SSL/SSH** La solución debe soportar inspeccionar tráfico que esté siendo encriptado mediante SSL al menos para los siguientes protocolos: HTTP, IMAP, SMTP, POP3 y FTP en su versión segura. Debe ser posible definir perfiles de inspección SSL donde se definan los protocolos a inspeccionar y el certificado usado, estos perfiles deben poder ser escogidos una vez se defina la política de seguridad. La inspección debe realizarse: mediante la técnica conocida como Hombre en el Medio (MITM – Man In The Middle) para una inspección completa o solo inspeccionando el certificado sin necesidad de hacer full inspection. **Alta disponibilidad** El dispositivo deberá soportar Alta Disponibilidad transparente, es decir, sin pérdida de conexiones en caso de que un nodo falle tanto para IPV4 como para IPV6 Alta Disponibilidad en modo Activo-Activo de forma automática sin requerir hacer políticas de enrutamiento basado en orígenes y destino para poder hacer la distribución del tráfico. El equipo debe soportar hasta 2 equipos en esquema de HA. **Visibilidad** La solución debe estar en la capacidad de visualizar el tráfico de usuario, aplicaciones, navegación y niveles de riesgo en tiempo real, esto deberá ser sobre la misma plataforma sin necesidad de software o licenciamiento adicional. Deber tener la capacidad de poder validar con que política la sesión se está coincidiendo y un link hacia la misma. **Características de Administración** Interfaz gráfica de usuario (GUI), vía Web por HTTP y HTTPS para hacer administración de las políticas de seguridad y que forme parte de la arquitectura nativa de la solución para administrar la solución localmente. Por seguridad la interfaz debe soportar SSL sobre HTTP (HTTPS) Soporte de al menos 3 servidores syslog para poder enviar bitácoras a servidores de SYSLOG remotos Debe tener la capacidad de gestionar todas las políticas de seguridad, además de poder gestionar Switches y APs dentro de una única consola de gestión. **Licenciamiento y actualizaciones** El licenciamiento de todas las funcionalidades debe ser ILIMITADO en cuanto a usuarios, conexiones, VPNs equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo. La vigencia de las actualizaciones para los servicios de Antivirus, AntiSpam, IPS, Application Control y URL Filtering debe proveerse por al menos doce (12) meses a partir de su activación en el portal del fabricante. La plataforma es requerida por un periodo de doce (12) meses en un esquema de soporte 7x24 ante el fabricante a partir de su activación en el portal del fabricante. Garantía y licenciamiento de los equipos y software ofertados, con Servicio de soporte 7x24 de 12 meses a partir de su activación en el portal de fabricante, que incluya Soporte Telefónico y repuestos (estos repuestos deberán ser gestionados por el contratista en caso tal de requerirse un en tiempo no mayor a (08) días calendario).				
INSTALACIÓN, RENOVACIÓN DE LICENCIA, Y PUESTA EN FUNCIONAMIENTO DE FIREWALL				
Renovación de una plataforma FG 120G por 12 meses a partir de la suscripción del acta de inicio con licenciamiento UTP. El No. Serial del equipo a renovar es el siguiente: FG120GTK24003019 El licenciamiento de todas las funcionalidades debe ser ILIMITADO en cuanto a usuarios, conexiones, VPNs equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo. La vigencia de las actualizaciones para los servicios de Antivirus, AntiSpam, IPS, Application Control y URL Filtering debe proveerse por al menos doce (12) meses a partir de su activación en el portal del fabricante. La plataforma es requerida por un periodo de doce (12) meses en un esquema de soporte 7x24 ante el fabricante a partir de su activación en el portal del fabricante. Garantía y licenciamiento de los equipos y software ofertados, con Servicio de soporte 7x24 de 12 meses a partir de su activación en el portal de fabricante, que incluya Soporte Telefónico y repuestos (estos repuestos deberán ser gestionados por el contratista en caso tal de requerirse un en tiempo no mayor a (08) días calendario). El equipo renovado debe integrarse nativamente con la plataforma de administración centralizada a adquirir por parte la entidad.	UNIDAD	1	$ 15.231.522	$ 15.231.522
SUMINISTRO, INSTALACIÓN Y PUESTA EN FUNCIONAMIENTO DE ACCESS POINTS				
GENERALIDADES Los equipos deben ser Appliances físicos (nuevos en su empaque original y sellados de fabrica) (No se aceptarán equipos remanufacturados y/o reparados y/o reformados). El fabricante debe estar en el cuadrante de lideres de Gartner para soluciones empresariales LAN/WLAN en al menos uno (01) los dos (02) últimos reportes publicados. La instalación de los equipos Access Point se realizará punto por punto, el oferente no deberá incluir servicios de cableado estructurado. Los APs deben incluir al menos: 1 interfaz RJ45 100M/1000M/2.5G/5G 1 interfaz RS-232 o un puerto RJ45 Serial SSID Simultáneos hasta 8 Debe permitir la conexión de dispositivos inalámbricos que soporten los estándares 802.11a/b/g/n/ac/ax de forma simultánea Debe poseer capacidad de conexión en tres bandas (2.4 GHz, 5 GHz y 6 Ghz) operando simultáneamente, además de permitir configuraciones independientes para cada radio Debe contar con un radio BLE (Bluetooth Low Energy) integrado e interno en el dispositivo Numero de radios 3 Wi-Fi+BLE La solución debe permitir la conexión de por lo menos 512 (quinientos doce) clientes inalámbricos simultáneamente por radio Debe soportar agregación de enlaces de acuerdo con el estándar IEEE 802.3ad El sistema operativo debe incluir la última versión completa liberada por el fabricante a la fecha de la compra Debe soportar su alimentación a través de Power Over Ethernet (PoE) conforme a los estándares 802.3af, 802.3at, 802.11bt. Adicionalmente debe poseer una entrada de alimentación de DC. El flujo de tráfico de los dispositivos conectados a la red inalámbrica debe ocurrir de forma centralizada a través del túnel establecido entre el punto de acceso y el controlador inalámbrico. En este modo todos los paquetes enviados en un SSID determinado deben ser enviados a través del túnel hasta el controlador inalámbrico. Cada dispositivo ofertado debe incluir su respectivo Power Injector POE, 802.3at up to 30W for Gigabit PoE Injector Servicio de Soporte Técnico y garantía Premium con Servicio de asistencia técnica continua con cobertura 24/7 ante el fabricante a partir de su activación en el portal del fabricante, atención prioritaria ante incidentes críticos y reemplazo de hardware en caso de fallas (con un máximo de 8 días calendario). Incluye actualizaciones de software y firmware. Los puntos de acceso (APs) deben ser administrables a través de la misma solución de seguridad perimetral tipo firewall (por adquirir) sin requerir licenciamientos adicionales permitiendo así su operatividad, y la extensión del perímetro de seguridad hasta la capa de acceso Wi-Fi. Integrarse de manera nativa con la infraestructura de seguridad perimetral Firewall (por adquirir), de forma que actúen como una extensión lógica del firewall corporativo, permitiendo que éste gestione directamente las funcionalidades de los Access Point, incluyendo su configuración, monitoreo y la aplicación de políticas de seguridad en el acceso. **Estándares y certificaciones Access Points** Los APs deben soportar al menos los siguientes estándares de la industria: - 802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h, 802.11i,802.11j, 802.11k, 802.11n, 802.11r, 802.11u, 802.11v, 802.11ac, 802.11ax (Wi-Fi 6), 802.1Q, 802.1X, 802.3ad, 802.3af, 802.3at, 802.3az, 802.3bz - WiFi Certified a,b,g,n,ac,ax, passpoint - WAP2, WPA3 0 - ROHS **Seguridad inalámbrica Access Point** - Algoritmo de cifrado: AES, TLS, EAP, TTLS, TKIP, WPA, WPA2 y WPA3. - La controladora debe incluir un control y filtro de más de 3000 aplicaciones de aplicaciones de uso común, y	UNIDAD	13	$ 5.993.610	$ 77.916.934

permita aplicar políticas granulares de seguridad, QoS, control de ancho de banda y filtrado web. El punto de acceso debe soportar encaminamiento de trafico de los clientes Wireless de manera tunelada, garantizando integridad de los datos a través de túneles IPSec. Cuando se tuneliza el tráfico de los clientes inalámbricos hacia la controladora inalámbrica, para garantizar un mejor uso de los recursos, la solución debe permitir una función conocida como Split Tunneling que se configurará en el SSID. Con esta característica, el AP debe soportar la creación de listas de excepción con direcciones de servicio de la red local que no deben enviar los paquetes a través del túnel al concentrador, es decir, todos los paquetes deben ser tunelizados excepto aquellos destinados a direcciones especificadas locales en las listas de excepciones. El punto de acceso debe soportar encaminamiento de trafico de tipo Modo Bridge o conmutación local. En este modo todo el tráfico de los dispositivos conectados en un determinaod SSID deberá ser conmutado localmente en la interfaz ethernet del punto de acceso y no deberán ser tunelados hasta la controladora inalámbrica El punto de acceso deberá soportar mecanismos de identificación y protección de ataques a la infraestructura inalámbrica (WIPS/WIDS). El punto de acceso deberá soportar la funcionalidad de análisis de espectro con un radio exclusivo que monitoree la red 7x24, que permita la identificación de interferencias no Wi-Fi y que operen en las frecuencias de 2.4GHz, 5GHz y 6 GHz Capacidad de manejar roles por usuario y políticas basadas en identidad. Coexistencias Avanzada Celular (Advanced Cellular Coexistence ACC) Radio dedicado para funciones de WIPS/WIDS y analizador de espectro. No se aceptan Access point adicionales para cumplir este requerimiento				
INSTALACIÓN, RENOVACIÓN DE LICENCIA, Y PUESTA EN FUNCIONAMIENTO DE ACCESS POINT				
Renovación de soporte y garantía de fabrica por 12 meses a partir de la suscripción del acta de inicio para los siguientes equipos Access Point. El No. Serial de los equipos a renovar son los siguientes: FP231GTF24062110 FP231GTF24018641 FP231GTF24062108 FP231GTF24062109 FP231GTF24018767 FP231GTF24062124 FP231GTF24062117 FP231GTF24062116 El oferente debe garantizar servicio de Soporte Técnico y garantía Premium con Servicio de asistencia técnica continua con cobertura 24/7 ante el fabricante a partir de la suscripción del acta de inicio, atención prioritaria ante incidentes críticos y reemplazo de hardware en caso de fallas (con un máximo de 8 días calendario). Incluye actualizaciones de software y firmware. Los puntos de acceso (APs) deben ser administrables a través de la misma solución de seguridad perimetral tipo firewall (por adquirir) sin requerir licenciamientos adicionales permitiendo así su operatividad, y la extensión del perímetro de seguridad hasta la capa de acceso Wi-Fi. Integrarse de manera nativa con la infraestructura de seguridad perimetral Firewall (por adquirir), de forma que actúen como una extensión lógica del firewall corporativo, permitiendo que éste gestione directamente las funcionalidades de los Access Point, incluyendo su configuración, monitoreo y la aplicación de políticas de seguridad en el acceso.	UNIDAD	8	$ 380.788	$ 3.046.307
SUMINISTRO, INSTALACIÓN Y PUESTA EN FUNCIONAMIENTO DE SWITCHES DE ACCESO 48 PUERTOS				
La solución de switches ofertada debe ser de la misma marca de la solución de acceso inalámbrico y la controladora de red de este proceso de contratación para garantizar el SD-LAN o SD-BRANCH de la Entidad. Los switches deben permitir descargar políticas de seguridad desde el firewall perimetral de la Entidad. Se debe poder administrar Switches, Access Point, SD-BRANCH, SD-WAN y Firewalls desde la misma consola de Administración (No se requieren consolas en la nube, la administración debe ser local). El fabricante debe estar en el cuadrante de lideres de Gartner para soluciones empresariales LAN/WLAN en al menos uno (01) los dos (02) últimos reportes publicados. Debe estar en capacidad de detectar Dispositivos IoT Debe permitir la autenticación y autorización Local RADIUS y TACACS+ Debe soportar SSH Debe soportar DHCP snooping, Dynamic ARP Debe soportar una funcionalidad de ahorro de Energía que bajé consumo si no hay tráfico y si llega tráfico hacia el dispositivo conectado se envié un mensaje de encendido (Wake-On-Lan - WOL) Debe soportar IEEE 802.1X (Port Based Network Access Control) MTBF minimo de 10 Años (87600 horas) STP Root Guard, STP (802,1d), RSTP (IEEE 802.1w), MSTP (IEEE 802.1s), RPVST (Rapid per Vlan Spanning Tree) Todas las funcionalidades que soporte el equipo deben estar incluidas y soportadas a perpetuidad. No se acepta funcionalidades por suscripción. Certificaciones: FCC, CE, RCM, VCCI, BSMI, UL, CB, RoHS2 Incluir 24 Transceiver 10GE SFP+ transceiver module, short range 300m LC connector, MMF, 850nm, 0°C to 70°C, for systems with SFP+ slots para todos los switches. **Capacidades específicas para los switches de 48 puertos** Los equipos deben ser Appliances físicos (nuevos en su empaque original y sellados de fabrica) (No se aceptarán equipos remanufacturados y/o reparados y/o reformados). Interfaces Red Totales: 48x GE RJ45 and 4x 10GE SFP+ Puerto de Consola: 1 RJ-45 Tráfico: IPV4/IPV6 Switch Capacity: Mayor o igual a 176 GB Packets Per Second: Mayor o igual a 260 Mpps VLANs: Mayor o igual a 4K Packet Buffers: Mayor o igual a 2 MB Memory: 512 MB ACL: 640	UNIDAD	9	$ 9.166.881	$ 82.501.926
SUMINISTRO, INSTALACIÓN Y PUESTA EN FUNCIONAMIENTO DE SWITCHES DE ACCESO BÁSICO DE 24 PUERTOS				
La solución de switches ofertada debe ser de la misma marca de la solución de acceso inalámbrico y la controladora de red de este proceso de contratación para garantizar el SD-LAN o SD-BRANCH de la Entidad. Los switches deben permitir descargar políticas de seguridad desde el firewall perimetral de la Entidad. Se debe poder administrar Switches, Access Point, SD-BRANCH, SD-WAN y Firewalls desde la misma consola de Administración (No se requieren consolas en la nube, la administración debe ser local). Debe estar en capacidad de detectar Dispositivos IoT Debe permitir la autenticación y autorización Local RADIUS y TACACS+ Debe soportar SSH Debe soportar DHCP snooping, Dynamic ARP Debe soportar una funcionalidad de ahorro de Energía que bajé consumo si no hay tráfico y si llega tráfico hacia el dispositivo conectado se envié un mensaje de encendido (Wake-On-Lan - WOL) Debe soportar IEEE 802.1X (Port Based Network Access Control) MTBF minimo de 10 Años (87600 horas) STP Root Guard, STP (802,1d), RSTP (IEEE 802.1w), MSTP (IEEE 802.1s), RPVST (Rapid per Vlan Spanning Tree) Todas las funcionalidades que soporte el equipo deben estar incluidas y soportadas a perpetuidad. No se acepta funcionalidades por suscripción. Certificaciones: FCC, CE, RCM, VCCI, BSMI, UL, CB, RoHS2 **Capacidades específicas para los switches de 24 puertos** Los equipos deben ser Appliances físicos (nuevos en su empaque original y sellados de fabrica) (No se aceptarán equipos remanufacturados y/o reparados y/o reformados). Interfaces Red Totales: 24x GE RJ45 and 4x 10GE SFP+ Puerto de Consola: 1 RJ-45 Tráfico: IPV4/IPV6 Switch Capacity: Mayor o igual a 128 GB	UNIDAD	3	$ 5.522.273	$ 16.566.820

Packets Per Second: Mayor o igual a 190 Mpps VLANs: Mayor o igual a 4K Packet Buffers: Mayor o igual a 2 MB Memory: 512 MB ACL: 640				
SUMINISTRO, INSTALACIÓN Y PUESTA EN FUNCIONAMIENTO DE SWITCH DE ACCESO MULTIGIGA 24 PUERTOS				
La solución de switches ofertada debe ser de la misma marca de la solución de acceso inalámbrico y la controladora de red de este proceso de contratación para garantizar el SD-LAN o SD-BRANCH de la Entidad. Los switches deben permitir descargar políticas de seguridad desde el firewall perimetral de la Entidad. Se debe poder administrar Switches, Access Point, SD-BRANCH, SD-WAN y Firewalls desde la misma consola de Administración (No se requieren consolas en la nube, la administración debe ser local). Debe estar en capacidad de detectar Dispositivos IoT Debe permitir la autenticación y autorización Local RADIUS y TACACS+ Debe soportar SSH Debe soportar DHCP snooping, Dynamic ARP Debe soportar una funcionalidad de ahorro de Energía que bajé consumo si no hay tráfico y si llega tráfico hacia el dispositivo conectado se envié un mensaje de encendido (Wake-On-Lan - WOL) Debe soportar IEEE 802.1X (Port Based Network Access Control) MTBF minimo de 10 Años (87600 horas) STP Root Guard, STP (802,1d), RSTP (IEEE 802.1w), MSTP (IEEE 802.1s), RPVST (Rapid per Vlan Spanning Tree) Todas las funcionalidades que soporte el equipo deben estar incluidas y soportadas a perpetuidad. No se acepta funcionalidades por suscripción. Certificaciones: FCC, CE, RCM, VCCI, BSMI, UL, CB, RoHS2 **Capacidades específicas para los switches de 24 puertos MULTIGIGA** Los equipos deben ser Appliances físicos (nuevos en su empaque original y sellados de fabrica) (No se aceptarán equipos remanufacturados y/o reparados y/o reformados). Interfaces Red Totales: 24x 2.5G/1G/100M RJ45 and 6x 10G/1G SFP+/SFP ports Puerto de Consola: 1 RJ-45 Tráfico: IPV4/IPV6 Switch Capacity: Mayor o igual a 240 GB Packets Per Second: Mayor o igual a 355 Mpps VLANs: Mayor o igual a 4K Packet Buffers: Mayor o igual a 2 MB Memory: 1 GB	UNIDAD	1	$ 10.404.919	$ 10.404.919
INSTALACIÓN, RENOVACIÓN DE LICENCIA, Y PUESTA EN FUNCIONAMIENTO DE SWITCHES NO POE				
Renovación de soporte y garantía de fabrica por 12 meses a partir de la suscripción del acta de inicio para los siguientes equipos FS 124F. El No. Serial de los equipos a renovar son los siguientes: S124FPTF24002200 S124FNTF24001962 S124FNTF24001988 El oferente debe garantizar servicio de Soporte Técnico y garantía Premium con Servicio de asistencia técnica continua con cobertura 24/7 ante el fabricante a partir de la suscripción del acta de inicio, atención prioritaria ante incidentes críticos y reemplazo de hardware en caso de fallas (con un máximo de 8 días calendario). Incluye actualizaciones de software y firmware. Los switches deben permitir descargar políticas de seguridad desde el firewall perimetral de la Entidad. Se debe poder administrar Switches, Access Point, SD-BRANCH, SD-WAN y Firewalls desde la misma consola de Administración (No se requieren consolas en la nube, la administración debe ser local).	UNIDAD	3	$ 3.046.304	$ 9.138.913
INSTALACIÓN, RENOVACIÓN DE LICENCIA, Y PUESTA EN FUNCIONAMIENTO DE SWITCH POE				
Renovación de soporte y garantía de fabrica por 12 meses a partir de la suscripción del acta de inicio para el siguiente equipo FS 124F-POE. El No. Serial del equipo a renovar es el siguiente: S124FPTF230005065 El oferente debe garantizar servicio de Soporte Técnico y garantía Premium con Servicio de asistencia técnica continua con cobertura 24/7 ante el fabricante a partir de la suscripción del acta de inicio, atención prioritaria ante incidentes críticos y reemplazo de hardware en caso de fallas (con un máximo de 8 días calendario). Incluye actualizaciones de software y firmware. Los switches deben permitir descargar políticas de seguridad desde el firewall perimetral de la Entidad. Se debe poder administrar Switches, Access Point, SD-BRANCH, SD-WAN y Firewalls desde la misma consola de Administración (No se requieren consolas en la nube, la administración debe ser local).	UNIDAD	1	$ 3.046.304	$ 3.046.304
PLATAFORMA DE ADMINISTRACIÓN CENTRALIZADA DE FIREWALL DE SEGURIDAD PERIMETRAL				
Se debe entregar una plataforma o sistema de administración centralizada de dispositivos de seguridad perimetral que cuente con las siguientes características: Se requiere un equipo tipo appliance físico que permita Centralización de Configuración y monitoreo de todos los firewalls de nueva generación, así como todas sus funciones de protección de red y de SD-WAN (nuevo en su empaque original y sellado de fabrica) (No se aceptarán un equipo remanufacturado y/o reparado y/o reformado). **LA SOLUCIÓN DE ADMINISTRACIÓN CENTRALIZADA DEBE DAR SOPORTE A LAS SIGUIENTES CARACTERÍSTICAS:** Administrar mínimo 30 equipos Capacidad de Almacenamiento de hasta 8 Terabytes. Debe permitir Creación e implementación automatizada de configuraciones de dispositivos Permitir tener un solo repositorio de almacenamiento centralizado y administración de configuraciones, para simplificar las tareas de administración de una gran cantidad de dispositivos de seguridad con protección completa de contenido. Deberá tener integración nativa con la solución de seguridad perimetral tipo Firewall. **FUNCIONALIDADES DE GESTION DE UTM/NGFW** La gestión debe permitir la creación y administración de políticas de firewall y control de aplicación. La gestión debe permitir la creación y administración de políticas de IPS, Antivírus y Anti-Spyware. La gestión debe permitir la creación y administración de políticas de Filtro de URL. Permitir buscar cuáles reglas un objeto está siendo utilizado. Debe atribuir secuencialmente un número a cada regla de firewall. Permitir la creación de reglas que permanezcan activas en horario definido. Permitir backup de las configuraciones y rollback de configuración para la última configuración. Debe tener mecanismos de validación de políticas avisando cuando haya reglas que ofusquen o conflictúen con otras (shadowing). Debe posibilitar la visualización y comparación de configuraciones actuales, configuraciones previas y configuraciones antiguas. Debe posibilitar que todos los firewalls sean controlados de manera centralizada utilizando solo un servidor de gestión. Cada servidor de gestión debe ser hospedado en un equipo independiente, no ejecutando función de firewall. La solución debe incluir una herramienta para gestionar centralmente las licencias de todos los aparatos controlados por estaciones de gestión, permitiendo al administrador actualizar licencias en los aparatos a través de esta herramienta. La solución debe permitir la distribución e instalación remota, de manera centralizada, de nuevas versiones de software de los aparatos. Debe ser capaz de generar reportes o presentar comparativos entre dos secciones distintas, resumiendo todos los cambios efectuados. Debe permitir crear flujos de aprobación en la solución de gestión, donde un administrador pueda crear todas las reglas, pero estas mismas solamente sean aplicadas después de la aprobación de otro administrador. Tener "wizard" en la solución de gestión para agregar los dispositivos por interfaz gráfica utilizando IP, login y clave de los mismos. Permitir que las políticas y los objetos ya presentes en los dispositivos sean importados cuando el mismo es	UNIDAD	1	$ 59.871.718	$ 59.871.718

agregado a la solución de gestión; Permitir la visualización, a partir de la estación de gestión centralizada, informaciones detalladas de los dispositivos gerenciados, tales como hostname, serial, IP de gestión, licencias, horario de lo sistema y firmware. Tener "wizard" en la solución de gestión para instalación de políticas y configuraciones de los dispositivos. Permitir crear en la solución de gestión templates de configuración de los dispositivos con informaciones de DNS, SNMP, configuraciones de LOG y administración. Permitir crear scripts customizados, que sean ejecutados de forma centralizada en un o más dispositivos gestionados con comandos de CLI de los mismos. Tener histórico de los scripts ejecutados en los dispositivos gestionados pela solución de gestión. Permitir configurar y visualizar balanceo de enlaces en los dispositivos gestionados de forma centralizada. Permitir crear varios paquetes de políticas que serán aplicados/asociados a los dispositivos o grupos de dispositivos. Debe permitir crear reglas de NAT64 y NAT46 de forma centralizada. Permitir la creación de reglas anti DoS de forma centralizada. Permitir la creación de objetos que serán utilizados en las políticas de forma centralizada. Permitir crear a partir de la solución de gestión, VPNs entre los dispositivos gestionados de forma centralizada, incluyendo topología (hub, spoke, dial-up) autenticaciones, claves y métodos de criptografía. Garantía y licenciamiento del equipo y software ofertado, con servicio de soporte 7x24 de 12 meses a partir de su activación en el portal de fabricante, que incluya soporte telefónico y repuestos (estos repuestos deberán ser gestionados por el contratista en caso tal de requerirse un en tiempo no mayor a (08) días calendario).				
PRESTACION DE SERVICIOS				
Generalidades del Servicio: El oferente debe contemplar en su oferta todos los costos o gastos asociados a la logística (desplazamiento, transporte, parqueaderos, equipos y herramientas de trabajo, refrigerios, entre otros) requerida para que el personal asignado al proyecto pueda cumplir sus funciones. **IMPLEMENTACIÓN:** Se debe dar cumplimento a las etapa del proyecto y entregar implementada y funcionando las soluciones completas, de acuerdo con los requerimientos y políticas establecidas por la entidad. Planeación de cada una de las actividades, validadas en conjunto con la entidad. Configuración y alistamiento del software a la última versión estable aprobada por el fabricante para la plataforma. Afinamiento y estabilización de las plataformas. Pruebas de Servicio de las plataformas. Entrega de las plataformas a satisfacción de la entidad Las actividades de implementación y/o afinamiento de las plataformas deben ser realizadas por personal certificado por el fabricante (se deben presentar las certificaciones del personal previo a la implementación de las plataformas). Se deberán realizar pruebas / muestras de las plataformas donde se evidencie la correcta configuración y afinamiento de cada plataforma. **SOPORTE Y/O MANTENIMIENTO:** El servicio de soporte debe incluir atención de incidentes sobre las plataformas ofertadas. Se debe garantizar soporte y garantía para las plataformas ofertadas en un esquema 7x24 por doce (12) meses a partir de la activación de las plataformas en el portal del fabricante, con soporte remoto o en sitio en caso de requerirse. El oferente debe contar con certificación vigente del Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO/IEC 27001:2022, expedida por un organismo de certificación acreditado en Colombia. La certificación debe estar vigente a la fecha de cierre del proceso y cubrir los servicios asociados a la solución ofertada. El oferente debe contar con certificación vigente del Sistema de Gestión de Servicios de TI conforme a la norma ISO/IEC 20000-1:2018, expedida por un organismo de certificación acreditado en Colombia. La certificación debe estar vigente a la fecha de cierre del proceso y cubrir la prestación y gestión de los servicios de tecnología de la información relacionados con la solución ofertada. Realizar y documentar entre otras, las siguientes actividades previa coordinación con el supervisor del contrato en desarrollo: Configurar los reportes / logs de las plataformas. Mantener actualizados los niveles de Firmware de los componentes ofertados de acuerdo con las últimas versiones estables liberadas por el fabricante. El horario de atención para el mantenimiento correctivo y preventivo debe ser de 7x24, sin costo adicional para la entidad. Se deben incluir en la oferta dos (02) actividades de mantenimiento preventivo y afinamiento con el fin de minimizar problemas y mantener los sistemas actualizados, estas actividades deberán ser con previa aprobación del responsable TI de la entidad. Al finalizar cada visita correctiva y/o preventiva el contratista deberá: Generar un informe de servicio en el que se realice un resumen de las actividades realizadas (actualización, soporte y mantenimiento), problemas presentados, soluciones utilizadas y recomendaciones. Consignar en la misma acta o informe de servicio si hubo cambio de software y/o en la configuración. El soporte deberá contemplar: El servicio de soporte debe incluir atención de incidentes sobre las plataformas ofertadas. Consultas a través de llamadas telefónicas, correo electrónico Sesiones remotas y atención en sitio (En caso de requerirse) en horario Hábil y No Hábil.	UNIDAD	1	$ 118.993.505	$ 118.993.505

PRIORIDAD		DESCRIPCION
1	CRITICA	De manera remota (2) horas de atención y (3) horas de traslado a sitio
2	ALTA	De manera remota (3) horas de atención y (4) horas de traslado a sitio.
3	MEDIA	De manera remota (8) horas y de ser necesario traslado a sitio.
4	BAJA	De manera remota (24) horas y de ser necesario traslado a sitio.

TRANSFERENCIA DE CONOCIMIENTO

Realizar transferencia de conocimientos de 24 Horas para 3 funcionarios de la entidad, la cual debe incluir como mínimo temas de administración, configuración y afinamiento de las plataformas.

CERTIFICACIONES DEL PROPONENTE

El oferente debe presentar certificación de distribuidor autorizado del fabricante donde se evidencie que tiene el nivel de membresía más alto del fabricante (gold, premium, expert o platinum (según aplique el fabricante), esta certificación debe estar dirigida a la entidad y debe no ser mayor a 30 días calendario a la fecha de presentación de la propuesta. Lo anterior con el fin de garantizar por parte de la entidad el respaldo en la calidad en canal autorizado para la reventa y/o distribución de las soluciones que requiere la entidad.

El oferente debe presentar al menos cinco (05) especialidades técnicas del mismo fabricante con el cual se está presentando, dentro de la cuales son obligatorias las siguientes (SD-WAN, Secure Networking Firewall, Secure Networking LAN).

El oferente debe entregar junto con la propuesta una certificación emitida directamente del fabricante de las soluciones ofertadas donde se evidencie que los equipos suministrados no se encuentran en fin de venta y/o fin de vida y/o fin de soporte por un periodo mínimo de cinco (05) años contados a partir de la fecha de presentación de la propuesta, esta certificación debe ser dirigida a la Entidad, especificando el objeto y número de proceso público.

CAPACIDAD TÉCNICA

El contratista debe disponer dentro de su equipo de trabajo, con el siguiente personal mínimo, requerido por la Entidad para el desarrollo y ejecución del contrato, así como las certificaciones y experiencia descritas.

Un (1) Ingeniero - Gerente del Proyecto

Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones, industrial o carreras afines. Tarjeta Profesional con expedición mínimo de diez (10) años.

Posgrado en Gerencia de Proyectos y/o certificación PMP

Certificaciones vigentes ITILFoundation v3 o superior, ITIL Managing Professional y ITIL 4 Strategist Direct, Plan and Improve Certificate

Experiencia mínima 5 proyectos gerenciando y/o coordinando proyectos de TI y/o Seguridad Informática.

Un (1) Ingeniero - Líder Técnico

Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones o carreras afines.

● Especialización o maestría en Seguridad de la Información ó informática ó Ciberseguridad. ● Certificación vigente en SCRUM Foundations Professional (SFPC). ● Certificación vigente en AUDITOR INTERNO en la norma ISO/IEC 20000-1:2018. ● Certificación vigente en AUDITOR LÍDER en la norma ISO/IEC 27001:2022. ● Certificación vigente en LÍDER GESTOR CIBERSEGURIDAD en la norma ISO/IEC 27032:2023. ● Certificación vigente como especialista en seguridad en redes. Emitida por el fabricante con el cual se esté presentado el proponente. Experiencia general de diez (10) años a partir de la expedición de la tarjeta profesional certificar mínimo de cinco (5) años de experiencia como líder o coordinador o gerente de servicios de TI. **Un (1) Ingeniero - Implementador** Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones o carreras afines. ● Especialización o maestría en Seguridad de la Información ó informática ó Ciberseguridad. ● Certificación en AUDITOR INTERNO en la norma ISO/IEC 20000-1:2018. ● Certificación vigente en AUDITOR INTERNO en la norma ISO/IEC 27001:2022. ● Certificación vigente como profesional de seguridad en redes ● Certificación vigente como especialista en seguridad en redes Experiencia general de diez (10) años a partir de la expedición de la tarjeta profesional, debe certificar mínimo de cinco (5) años en implementación, soporte y/o monitoreo de soluciones de seguridad. **Un (01) Ingeniero de soporte Nivel 2** Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones o carreras afines. ● Especialización o maestría en Seguridad de la Información ó informática ó Ciberseguridad. ● Certificación vigente en AUDITOR INTERNO en la norma ISO/IEC 27001:2022. ● Certificación vigente como profesional de seguridad en redes ● Certificación vigente como especialista en seguridad en redes Experiencia general de siete (7) años a partir de la expedición de la tarjeta profesional, de los cuales debe certificar mínimo cinco (5) años en implementación, soporte y/o monitoreo de soluciones de seguridad. Nota: Cada uno de los perfiles debe presentarse por separado (ninguno podrá repetir cargo o rol), El oferente debe aportar en conjunto con la presentación de la propuesta la hoja de vida actualizada, certificaciones y contrato laborales de vinculación a la empresa o proponente participante (evitando figuras de tercerización) (a la fecha de presentación de la propuesta) evidenciando el cumplimiento de cada especificación solicitada.				
VALOR TOTAL				$ 661.490.617

4.2. JUSTIFICACIÓN DEL VALOR DEL CONTRATO:

Para el cálculo del Presupuesto de los bienes del objeto del presente proyecto, se tuvo en cuenta precios del mercado para obtener el valor, tres (3) empresas presentaron listados de precios unitarios, una vez, verificados y clasificados dichos valores se tomó el valor promedio, teniendo en cuenta que se cumpliera con las condiciones técnicas mínimas exigidas por la entidad. La definición de los factores de evaluación y costos del proyecto, se relacionan con la magnitud de la Adquisición, dando cumplimiento a los preceptos, de transparencia, economía, celeridad, responsabilidad, buena fe, contemplados en la ley 80 de 1993. Teniendo en cuenta lo dispuesto en el Decreto 1082 del 26 de mayo de 2015 y la Guía para la Elaboración de Estudios del Sector G-EES-02 emitida por Colombia Compra Eficiente el 31 de marzo de 2014, se procede a realizar un análisis del valor estimado del contrato y justificación de este.

El análisis de costos y precios del presente estudio se realizó en base a cotizaciones de empresas que representan el mercado, con las tres (3) cotizaciones que se detallan a continuación

EMPRESA COTIZADA	VALOR
INGENIUM COLOMBIA S.AS.	$ 674.738.446
GROWDATA	$ 658.564.595
DATA SEC S.AS.	$ 651.168.822
VALOR PROMEDIO	$ 661.490.621

Ítem	Descripción resumida	Unidad	Cantidad	DATASEC Unit.	DATASEC Total	INGENIUM Unit.	INGENIUM Total	GROWDATA Unit.	GROWDATA Total	Promedio unitario	Promedio total
1	Firewall de seguridad perimetral CORE	UNIDAD	4	$58.963.988	$235.855.952	$62.319.528	$249.278.111	$60.239.735	$240.958.939	$60.507.750	$242.031.001
2	Firewall de seguridad perimetral MULTIGIGA	UNIDAD	1	$13.591.898	$13.591.898	$14.095.403	$14.095.403	$16.049.389	$16.049.389	$14.578.897	$14.578.897
3	Firewall / solución de seguridad perimetral adicional	UNIDAD	1	$8.362.318	$8.362.318	$7.938.448	$7.938.448	$8.184.783	$8.184.783	$8.161.850	$8.161.850
4	Solución / componente de infraestructura de seguridad	UNIDAD	1	$14.677.430	$14.677.430	$16.469.745	$16.469.745	$14.547.392	$14.547.392	$15.231.522	$15.231.522
5	Puntos de acceso / componentes LAN-WLAN	UNIDAD	13	$6.060.505	$78.786.565	$6.079.604	$79.034.849	$5.840.722	$75.929.383	$5.993.610	$77.916.934
6	Renovación de soporte y garantía	UNIDAD	8	$366.936	$2.935.488	$411.744	$3.293.949	$363.685	$2.909.478	$380.788	$3.046.307
7	Switches de acceso 48 puertos	UNIDAD	9	$9.021.372	$81.192.348	$9.536.721	$85.830.493	$8.942.549	$80.482.938	$9.166.881	$82.501.926
8	Switches / dispositivos de acceso	UNIDAD	3	$4.889.195	$14.667.585	$5.646.164	$16.938.493	$6.031.461	$18.094.383	$5.522.273	$16.566.820
9	Switch / componente de acceso	UNIDAD	1	$9.816.531	$9.816.531	$10.349.832	$10.349.832	$11.048.395	$11.048.395	$10.404.919	$10.404.919
10	Equipos / componentes de conectividad	UNIDAD	3	$2.935.486	$8.806.458	$3.293.949	$9.881.847	$2.909.478	$8.728.435	$3.046.304	$9.138.913
11	Componente complementario LAN/WLAN	UNIDAD	1	$2.935.486	$2.935.486	$3.293.949	$3.293.949	$2.909.478	$2.909.478	$3.046.304	$3.046.304
12	Plataforma de administración centralizada	UNIDAD	1	$60.637.180	$60.637.180	$58.039.482	$58.039.482	$60.938.493	$60.938.493	$59.871.718	$59.871.718
13	Servicios de instalación, configuración, pruebas y puesta en funcionamiento	UNIDAD	1	$118.903.582	$118.903.582	$120.293.839	$120.293.839	$117.783.094	$117.783.094	$118.993.505	$118.993.505

TOTAL GENERAL				$651.168.821		$674.738.440		$658.564.580		$661.490.617

4.3. FORMA DE PAGO: El Municipio se compromete a realizar el pago de la siguiente manera: **A) UN ÚNICO PAGO,** una vez ejecutado totalmente el objeto contractual, para lo cual se deberá presentar cuenta de cobro, acompañada de las solicitudes realizadas por el supervisor del contrato, certificado de cumplimiento expedido por el Supervisor, en la que conste que las actividades se realizaron de acuerdo a los compromisos adquiridos, y liquidación del contrato. **PARÁGRAFO PRIMERO:** El pago se deberá acompañar de la seguridad social y riesgos profesionales, con el fin de darle cumplimiento al artículo 23 de la Ley 1150 de 2007 y acreditarse con la Ley y los conceptos emitidos por el Ministerio de Protección Social al respecto. **PARÁGRAFO SEGUNDO:** El contratista deberá en todo caso, a fin de tramitar el pago acatar en estricto rigor los requerimientos que para todos los efectos formule la entidad a través del supervisor. **NOTA:** El Municipio no se responsabilizará por la demora presentada en el pago al CONTRATISTA, cuando ella fuere provocada por encontrarse incompleta la documentación que sirve de soporte para el trámite y previa recepción de los elementos a satisfacción por parte del contratista o no se ajusta a cualquiera de las condiciones establecidas en el contrato. El termino para el pago solo empezara a contratarse desde la fecha en que se presenten en debida forma y adjuntándola totalidad de los documentos exigidos para tal efecto. Las demoras que se presenten por estos conceptos serán responsabilidad del CONTRATISTA elegido y no tendrá por ello derecho al pago de intereses o compensación de ninguna naturaleza.

5. LOS CRITERIOS PARA SELECCIONAR LA OFERTA MÁS FAVORABLE.

Atendiendo las disposiciones contempladas en el artículo 2.2.1.1.2.2.2 del Decreto 1082 de 2015, el ofrecimiento más favorable en el caso de la selección abreviada para la adquisición de bienes y servicios de características técnicas uniformes y de común utilización por el procedimiento de subasta inversa, será aquél con el MENOR PRECIO.

En tal sentido, el factor de selección que permite identificar la oferta más favorable a esta entidad es el MENOR PRECIO.

6. SOPORTE QUE PERMITA LA ESTIMACIÓN, TIPIFICACIÓN Y ASIGNACIÓN DE LOS RIESGOS PREVISIBLES QUE PUEDAN AFECTAR EL EQUILIBRIO ECONÓMICO DEL CONTRATO. El análisis de riesgo se encuentra en documento adjunto, que hace parte de este estudio previo.

7. GARANTÍAS QUE LA ENTIDAD ESTATAL CONTEMPLA EXIGIR EN EL PROCESO DE CONTRATACIÓN.

7.1. GARANTÍA DE LOS RIESGOS DERIVADOS DEL INCUMPLIMIENTO DE LA OFERTA.

El Proponente debe presentar con la propuesta una Garantía de seriedad de la oferta que cumpla con los parámetros, condiciones y requisitos que se indican en este numeral.

Cualquier error o imprecisión en el texto de la garantía presentada, será susceptible de aclaración por el Proponente hasta el término de traslado del informe de evaluación. Sin embargo, la no entrega de la garantía no es subsanable y se rechazará la oferta.

Las características de las garantías son las siguientes:

Característica	Condición
Clase	Cualquiera de las clases permitidas por el artículo 2.2.1.2.3.1.2 del Decreto 1082 de 2015, a saber: (i) Contrato de seguro contenido en una póliza, (ii) Patrimonio autónomo y (iii) Garantía Bancaria.
Asegurado/ beneficiario	Municipio de Montería
Amparos	Los perjuicios derivados del incumplimiento del ofrecimiento en los eventos señalados en el artículo 2.2.1.2.3.1.6 del Decreto 1082 de 2015.
Vigencia	**TRES (3) MESES,** contados a partir de la fecha de cierre del proceso de contratación.

Valor Asegurado	Diez por ciento (10%) del Presupuesto Oficial del presente Proceso de Selección
Tomador	• Para las personas jurídicas: la Garantía deberá tomarse con el nombre o razón social y tipo societario 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. • Para los Proponentes Plurales: la Garantía deberá ser otorgada por todos los integrantes del Proponente Plural, para lo cual se deberá relacionar claramente los integrantes, su identificación y porcentaje de participación, quienes para todos los efectos serán los otorgantes de la misma.

Si en desarrollo del proceso de selección se modifica el cronograma, el Proponente deberá ampliar la vigencia de la Garantía de seriedad de la oferta hasta tanto no se haya perfeccionado y cumplido los requisitos de ejecución del respectivo contrato.

La propuesta tendrá una validez igual al término de vigencia establecido para la garantía de seriedad de la oferta. Durante este período la propuesta será irrevocable, de tal manera que el Proponente no podrá retirar ni modificar los términos o condiciones de la misma, so pena de que la Entidad pueda hacer efectiva la garantía de seriedad de la oferta.

7.2. GARANTÍA DE OBLIGACIONES SURGIDAS CON OCASIÓN DEL CONTRATO: El contratista se obliga a constituir, a favor del Municipio de Montería, una garantía única contractual, de conformidad con las disposiciones del Decreto 1082 de 2015, que ampare:

CARACTERÍSTICA	CONDICIÓN
Clase	Cualquiera de las clases permitidas por el artículo 2.2.1.2.3.1.2 del Decreto 1082 de 2015, a saber: (i) Contrato de seguro contenido en una póliza para Entidades Estatales, (ii) Patrimonio autónomo, (iii) Garantía Bancaria.
Asegurado/beneficiario	Municipio de Montería, identificado con Nit. 800096734-1
Amparos, vigencia y valores asegurados	**a) CUMPLIMIENTO**: Para garantizar el cumplimiento general de las obligaciones del contratista, el pago de multas y demás sanciones, en cuantía equivalente al diez por ciento (10%) del valor del Contrato, y con una vigencia igual a la duración del mismo y seis (6) meses más. **b) CALIDAD DE LOS BIENES:** En cuantía igual al 10% del valor total del contrato, por el termino de ejecución del contrato y tres (3) años más, posteriores a la fecha del acta de finalización del contrato. **c) CALIDAD DEL SERVICIO**: Por una suma equivalente al 10% del valor total del contrato, por el término de ejecución del mismo y 6 meses más, posteriores a la fecha de finalización del contrato.
Tomador	• Para las personas jurídicas: la garantía deberá tomarse con el nombre o razón social y tipo societario 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. • No se aceptan garantías a nombre del representante legal o de alguno de los integrantes del consorcio. Cuando el contratista sea una Unión Temporal o Consorcio, se debe incluir razón social, NIT y porcentaje de participación de cada uno de los integrantes. • Para el Contratista conformado por una estructura plural (unión temporal, consorcio): la garantía deberá ser otorgada por todos los integrantes del Contratista, para lo cual se deberá relacionar claramente los integrantes, su identificación y porcentaje de participación, quienes para todos los efectos serán los otorgantes de la misma.
Información necesaria dentro de la póliza	• Número y año del contrato • Objeto del contrato • Firma del representante legal del Contratista • En caso de no usar centavos, los valores deben aproximarse al mayor.

	Ej. Cumplimiento si el valor a asegurar es $14.980.420,20 aproximar a $14.980.421

8. INDICACIÓN SI LA CONTRATACIÓN RESPECTIVA ESTÁ COBIJADA POR UN ACUERDO INTERNACIONAL O UN TRATADO DE LIBRE COMERCIO VIGENTE PARA EL ESTADO COLOMBIANO. De acuerdo a lo establecido en el Decreto 1082 de 2015 y el manual para el manejo de los acuerdos comerciales de procesos de contratación, se tiene:

ACUERDO		ENTIDAD ESTATAL INCLUIDA	PRESUPUESTO DEL PROCESO DE CONTRATACIÓN SUPERIOR AL UMBRAL DEL ACUERDO COMERCIAL	EXCEPCIÓN APLICABLE AL PROCESO DE CONTRATACIÓN	PROCESO DE CONTRATACIÓN CUBIERTO POR EL ACUERDO COMERCIAL
ALIANZA PACÍFICO	CHILE	SÍ	SI	NO	NO
	MEXICO	NO	-	-	NO
	PERÚ	SÍ	SI	NO	NO
CHILE		SÍ	SI	NO	NO
COSTA RICA		SÍ	SI	NO	SI
ESTADOS AELC		SÍ	SI	NO	SI
TRIÁNGULO NORTE	EL SALVADOR	NO	-	NO	NO
	GUATEMALA	SÍ	SÍ	NO	NO
	HONDURAS	NO	-	-	NO
UNIÓN EUROPEA		SI	SI	NO	SI

9. SUPERVISIÓN.

La supervisión de la ejecución del objeto contractual será ejercida por la Coordinadora de la Oficina TIC de la Alcaldía de Montería o por el funcionario que el ordenador del gasto designe; funcionario que vigilará el cumplimiento de las obligaciones emanadas del mismo, verificará el cabal cumplimiento de las obligaciones de EL CONTRATISTA y vigilará la correcta ejecución técnica, administrativa y financiera del contrato.

Para constancia se firma en Montería – Córdoba, a los doce (12) días mes de Agosto de 2026.

Katia Cabrales B.

Firmado digitalmente por KATYA CABRALES BECHARA

KATIA CABRALES BECHARA
SECRETARIA GENERAL
MUNICIPIO DE MONTERIA

Proyectó técnicamente: Luis Miguel Tarrá- Profesional Universitario TIC SGM

Firmado digitalmente por Luis Miguel Tarra Lozano

Revisó técnicamente: Kátherin Ramos – Profesional Especializado TIC SGM

Firmado digitalmente por KATHERIN RAMOS LICONA

Revisó jurídicamente: Gabriel Corrales Daza – Contratista SGM