Outlook

Solicitud de cotizacion proceso Seguridad perimetral

Desde Secretaria General <secretariageneral@monteria.gov.co>
Fecha Jue 18/06/2026 14:40
Para aescobar@ingeniumcolombia.com <aescobar@ingeniumcolombia.com>; sergio.diaz@datasec.com.co <sergio.diaz@datasec.com.co>; felipe.munoz@growdata.com.co <felipe.munoz@growdata.com.co>
CC Kátherin Ramos Licona <kramos.tic@monteria.gov.co>

2 archivos adjuntos (1 MB)
SOLICITUD DE COTIZACION SEGURIDAD (1).pdf; ANEXO 1 SOLICITUD DE COTIZACION SEGURIDAD.pdf;

Cordial saludo,

Por medio del presente, se permite hacer envio de solicitud de cotizacion 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.

Agradecemos el envio de diha cotizacion junto con la camara de comercio de la entidad.

Alcaldía de MONTERÍA

SECRETARÍA GENERAL

SOLICITUD DE COTIZACIÓN	
LEY 80 DE 1993 ARTICULO 25 Nº 7 Y 12, LEY 1150 ARTICULO 2º PARÁGRAFO 1 Y DECRETO 1082 DE 2015 SECCIÓN 2 SUBSECCIÓN 1 ARTÍCULO 2.2.1.1.2.1.1	
FECHA	JUNIO DE 2026
DEPENDENCIA SOLICITANTE	SECRETARÍA GENERAL

ADVERTENCIA	La cotización que aquí se solicita servirá de base para la elaboración de un estudio de mercado y para la proyección de los respectivos estudios previos de la contratación a realizar y, por tanto, no constituye en sí misma una oferta vinculante, motivo por el cual no se genera obligación alguna para la entidad pública o para el respectivo proveedor.	
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.	
VALIDEZ DE LA COTIZACIÓN	La cotización que se emita como consecuencia de esta solicitud deberá tener una vigencia de tres (3) meses, contados a partir de la fecha de expedición.	
ESPECIFICACIONES TÉCNICAS	**VER ANEXO 1**	
CONDICIONES DE CONTRATACIÓN	**PLAZO**	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.
	OBLIGACIONES DEL CONTRATISTA	**1.** Presentar dentro los cinco (5) días calendario contados a partir de la firma del acta de inicio del contrato, un plan de ejecución, equipo de trabajo y cronograma de actividades. **2.** Mantener el personal mínimo requerido durante la ejecución del contrato el cual solo podrá ser cambiado por situaciones de fuerza mayor o caso fortuito, evento en el cual deberá ser justificado y soportado ante el supervisor designado por la entidad, y para tal efecto, el que lo reemplace o sustituya debe cumplir como mínimo, los mismos o mejores requisitos del profesional aprobado por la entidad, de acuerdo con lo señalado en el pliego de condiciones. **3.** Presentar dentro de los quince (15), días calendario contados a partir de la firma del acta de inicio del contrato, topología o arquitectura de la solución diseñada. **4.** Entregar a la Coordinación de la Oficina de Gestión de Servicios Administrativos, en los horarios de atención previstos por esa dependencia, los bienes objeto del contrato de acuerdo con los requerimientos que haga la Administración. **5.** Hacer entrega de los equipos y/o licencias y/o bienes y/o elementos nuevos de última generación del fabricante de acuerdo con las especificaciones técnicas, para ello se tendrá un plazo no mayor a 60 días para entrega, contados a partir de la suscripción del acta de inicio. **6.** Entregar a la entidad los documentos (licenciamiento legal y de uso) de la renovación de soporte y garantía donde se

		especifique el detalle de los productos objeto de renovación de su licenciamiento y que están descritos en las especificaciones técnicas. **7.** Prestar los servicios de instalación, configuración, implementación, parametrización, pruebas de funcionamiento, puesta en marcha y soporte por 1 año a partir de la activación en el portal del fabricante. **8.** Presentar certificación emitida directamente del fabricante de las soluciones ofertadas dirigida a la Entidad donde se evidencie que los equipos y/o soluciones suministradas no se encuentran en fin de venta y/o fin de vida y/o fin de soporte y que se contaran con mínimo 5 años de garantía y repuestos por parte del fabricante. **9.** Brindar soporte técnico nivel 1 y 2 definidos en el ANEXO FICHA DE CONDICIONES TÉCNICAS. **10.** Realizar los dos (02) mantenimiento correctivo y preventivo a que haya lugar y garantizar la reposición de los equipos y repuestos necesarios, así como su reinstalación si hay lugar a ello, sin que ello genere costo adicional para la entidad. **11.** Realizar transferencia de conocimiento de mínimo veinticuatro (24) Horas conforme se programe con la Supervisión, para tres (3) ingenieros de la entidad, la cual debe incluir como mínimo temas de administración, configuración y afinamiento de las plataformas puestas a disposición en el marco de la ejecución del contrato. **12.** Mantener durante la vigencia del contrato la certificación de distribuidor autorizado del fabricante donde se evidencie que tiene el nivel de membresía más alta (Platinum, Gold o Expert o su equivalente), para ello en la entrega de los equipos adquiridos por la entidad, el contratista debe allegar la certificación de aval del fabricante para su remisión en la Oficina de Gestión de Servicios Administrativos. **13.** Todos los equipos y/o accesorios deben ser del mismo fabricante, no se aceptan elementos complementarios y/o de referencias distintas, lo anterior, con el fin de garantizar la compatibilidad entre todos los equipos a adquirir. **14.** Entregar documentación e informes de la arquitectura implementada, así como de las pruebas de funcionamiento, configuración e implementación de la solución contratada. **15.** Las demás que se deriven y que garanticen su cabal y oportuna ejecución, acorde con el anexo técnico
	FORMA DE PAGO	El valor de este contrato se pagará así: Mediante pagos parciales, previa entrega de los bienes solicitados por la entidad, presentando el informe de ejecución, la factura y/o cuenta de cobro, expedido el certificado de ingreso al almacén, el certificado de cumplimiento por parte del supervisor, el acta final de ejecución y el acta de liquidación. PARÁGRAFO PRIMERO. Para cada pago, deberá presentarse acta parcial de ejecución en donde se anoten todas y cada una de las actividades ejecutadas

		a la fecha de cohorte del acta y el certificado de cumplimiento suscrito por el SUPERVISOR del contrato. PARÁGRAFO SEGUNDO. Para el caso del último pago, EL CONTRATISTA deberá presentar informe final de ejecución y acta de liquidación, el cual dará cuenta de todas y cada una de las actividades ejecutadas en desarrollo del objeto contractual durante la vigencia del mismo y la certificación del SUPERVISOR donde conste el cumplimiento de todas y cada una de sus obligaciones derivadas de este contrato. PARÁGRAFO TERCERO. Para cada pago deberá acompañarse el pago de la seguridad social y riesgos profesionales, con el fin de darle cumplimiento al artículo 23 de la Ley 1150 de 2007 y acreditarse de conformidad con la Ley y los conceptos emitidos por el Ministerio de Protección Social al respecto. 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
	RIESGOS DE LA CONTRATACIÓN	**Riesgos Económicos:** Se recomienda que por regla general y bajo la premisa de contar con información suficiente y con las condiciones necesarias para llevar a cabo el objeto contractual, el riesgo se traslade al contratista en atención a su experticia en el manejo y posibilidad de administración efectiva de los riesgos económicos. **Riesgos Sociales o Políticos:** Se recomienda que por regla general el riesgo previsible de esta naturaleza lo asuma la entidad contratante que en atención a su condición, se presume que cuenta con un manejo y posibilidad de administración efectiva del mismo. **Riesgo Operacional:** Por regla general y bajo la premisa de contar con información suficiente, los riesgos operacionales se transfieren al contratista, en la medida en que cuenta con mayor experiencia y conocimiento de las variables que determinan el valor de la inversión y tendrá a su cargo las actividades propias del contrato. **Riesgos Financieros:** Se recomienda que el riesgo se traslade al contratista por regla general y bajo la premisa de contar con información suficiente. En atención a su experticia en la consecución y estructuración de los recursos necesarios, se presume que cuenta con un manejo y posibilidad de administración efectiva de los riesgos financieros. **Riesgos Regulatorios:** Se recomienda que, por regla general, el

<table>
<tr><td></td><td></td><td>riesgo lo asuma la parte que cuenta con un manejo y posibilidad de administración efectiva de los riesgos regulatorios por su naturaleza y en virtud de las normas propias de cada regulación.
Riesgos de la naturaleza: Siempre y cuando existan formas de mitigación al alcance del contratista, los riesgos de la naturaleza deben ser trasladados al mismo.

<table>
<tr><th>RIESGOS</th><th>PROBABILIDAD</th><th>IMPACTO</th><th>ASIGNACIÓN</th></tr>
<tr><td>SOCIALES O POLITICOS</td><td>MEDIA - BAJA</td><td>MEDIA - BAJA</td><td>ENTIDAD</td></tr>
<tr><td>OPERACIONALES</td><td>MEDIA - BAJA</td><td>MEDIA - BAJA</td><td>CONTRATISTA</td></tr>
<tr><td>FINANCIEROS</td><td>MEDIA - BAJA</td><td>MEDIA - BAJA</td><td>CONTRATISTA</td></tr>
<tr><td>REGULATORIOS</td><td>MEDIA - BAJA</td><td>MEDIA - BAJA</td><td>CONTRATISTA</td></tr>
</table></td></tr>
<tr><td>VALOR OFRECIDO</td><td colspan="2">Al cotizar debe tener en cuenta que los impuestos que se causen correrán por cuenta del futuro 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, Municipal o Municipal. Así:

<table>
<tr><th>ESTAMPILLA</th><th>PORCENTAJE SOBRE EL VALOR DEL CONTRATO</th></tr>
<tr><td>Pro Universidad</td><td>2%</td></tr>
<tr><td>Pro Cultura</td><td>1%</td></tr>
<tr><td>Retefuente</td><td>0,1%</td></tr>
<tr><td>Inducom</td><td>Máximo 1% conforme a la actividad o servicio contratado según Estatuto de Rentas del Municipio.</td></tr>
<tr><td>Pro Adulto Mayor</td><td>3% siempre que el valor del contrato supere 3.850 UVT</td></tr>
<tr><td>Pro Deporte</td><td>1%</td></tr>
<tr><td>Justicia Familiar</td><td>2%</td></tr>
</table></td></tr>
<tr><td>PLAZO Y LUGAR PARA PRESENTAR COTIZACIÓN</td><td colspan="2">Los interesados deberán presentar la respectiva cotización a más tardar 5 días posteriores a la fecha de recibido del presente documento, en las Instalaciones de la Secretaría General del Municipio de Montería – Córdoba, o en su defecto en el siguiente e-mail: secretariageneral@monteria.gov.co</td></tr>
</table>

Agradecemos adjuntar certificados de existencia y representación legal o certificados de matrícula mercantil sean enviadas al correo secretariageneral@monteria.gov.co, o en físico en la Calle 27 N° 3-16 Piso 2, Oficina Secretaría General.

Cordialmente,

DANIEL EDUARDO PATRON PÉREZ
SECRETARIO GENERAL
MUNICIPIO DE MONTERÍA

Proyectó: Luis Miguel Tarrá Lozano – Profesional Universitario TIC

Revisó: Kátherin Ramos Licona – Profesional Especializado TIC Firmado digitalmente por KATHERIN RAMOS LICONA

Revisó: Eduardo Estrada C. – Abogado contratista

Alcaldía de MONTERÍA

SECRETARÍA GENERAL

ANEXO 1 – ESPECIFICACIONES TÉCNICAS

El proyecto comprende la implementación de la solución integral de infraestructura y ciberseguridad, para fortalecer la conectividad LAN y WLAN 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 YMANTENIMIENTO

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 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 10GE SFP+ con sus respectivos cables de F.O.) 8 interfaces de 1 GE SFP (se deben incluir en la oferta dos	UNIDAD	4

	(02) transceivers 1GE SFP 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 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 10GE SFP+ 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	UNIDAD	1

	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 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	UNIDAD	1

	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 de administración centralizada a adquirir por parte la entidad.	UNIDAD	1
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 256	UNIDAD	13

	(doscientos cincuenta y seis) clientes inalámbricos simultáneamente por radio Debe soportar agregación de enlaces de acuerdo con el estándar IEEE 802.3at 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, 802.11b. 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, 802.11be, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11k, 802.11n, 802.11r, 802.11v, 802.11ac, 802.11ax, 802.11mc, 802.1X, 802.3af, 802.3at, 802.3bt, 802.3az, 802.1Q, 802.11u, 802.11w, 802.3bz - 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	UNIDAD	**8**

	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.		
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 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.	UNIDAD	9

	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 Packets Per Second: Mayor o igual a 190 Mpps	UNIDAD	3

	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		
10	**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: S124FNTF24002200 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	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: S124FPTF23005065 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 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,	UNIDAD	1

	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 las etapas 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.		

Proyectó: Luis Miguel Tarrá Lozano – Profesional Universitario ~~TIC~~

Revisó: Pablo Ballut Rubio – Contratista TIC

Revisó: Kátherin Ramos Licona – Profesional Especializado TIC

Outlook

RE: [EXTERNAL]Solicitud de cotizacion proceso Seguridad perimetral

Desde Sergio Daniel Diaz Jimenez <sergio.diaz@datasec.com.co>
Fecha Jue 25/06/2026 17:36
Para Secretaria General <secretariageneral@monteria.gov.co>
CC Kátherin Ramos Licona <kramos.tic@monteria.gov.co>

7 archivos adjuntos (25 MB)

CCIO DATASEC JUNIO.pdf; ET DATASEC.pdf; fortigate-90g-series.pdf; fortigate-120g-series.pdf; fortigate-fortiwifi-50g-series.pdf; fortimanager.pdf; fortiswitch-secure-access-series.pdf;

Buenas tardes estimados,

Me dirijo cordialmente, por medio del presente remitimos nuestra propuesta para el proyecto de 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.

Quedo atento a comentarios e inquietudes, muchas gracias.

DataSec
Sergio Diaz J.
Gerente De Cuenta
+57 321 318 4645
sergio.diaz@datasec.com.co
Cra 14a # 101 - 11 OF 201, Bogotá
www.datasec.com.co
DataSec SAS

De: Sergio Daniel Diaz Jimenez <sergio.diaz@datasec.com.co>
Enviado: jueves, 25 de junio de 2026 5:27 p. m.
Para: Secretaria General <secretariageneral@monteria.gov.co>
Cc: Kátherin Ramos Licona <kramos.tic@monteria.gov.co>
Asunto: RE: [EXTERNAL]Solicitud de cotizacion proceso Seguridad perimetral

Buenas tardes estimados,

Me dirijo cordialmente, por medio del presente remitimos nuestra propuesta para el proyecto de 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.

Quedo atento a comentarios e inquietudes, muchas gracias.

De: Secretaria General <secretariageneral@monteria.gov.co>
Enviado: jueves, 18 de junio de 2026 2:40 p. m.
Para: aescobar@ingeniumcolombia.com <aescobar@ingeniumcolombia.com>; Sergio Daniel Diaz Jimenez <sergio.diaz@datasec.com.co>; felipe.munoz@growdata.com.co <felipe.munoz@growdata.com.co>
Cc: Kátherin Ramos Licona <kramos.tic@monteria.gov.co>
Asunto: [EXTERNAL]Solicitud de cotizacion proceso Seguridad perimetral

Cordial saludo,

Por medio del presente, se permite hacer envio de solicitud de cotizacion 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.

Agradecemos el envio de diha cotizacion junto con la camara de comercio de la entidad.

ANEXO 1 – ESPECIFICACIONES TÉCNICAS

El proyecto comprende la implementación de la solución integral de infraestructura y ciberseguridad, para fortalecer la conectividad LAN y WLAN 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 YMANTENIMIENTO

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	VALOR UNITARIO	VALOR TOTAL
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 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.)	UNIDAD	4	$ 58.963.988	$ 235.855.952

	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 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.	UNIDAD	1	$ 13.591.898	$ 13.591.898

	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.	UNIDAD	1	$ 8.362.318	$ 8.362.318

	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 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 de administración centralizada a adquirir por parte la entidad.	UNIDAD	1	$ 14.677.430	$ 14.677.430
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.	UNIDAD	13	$ 6.060.505	$ 78.786.565

	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 - 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**	$ 366.936	$ 2.935.488
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)	UNIDAD	9	$ 9.021.372	$ 81.192.348

	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				
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	UNIDAD	3	$ 4.889.195	$ 14.667.585

	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 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				
9	**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	UNIDAD	1	$ 9.816.531	$ 9.816.531

	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				
10	**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	$ 2.935.486	$ 8.806.458
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	1	$ 2.935.486	$ 2.935.486

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 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,	UNIDAD	1	$ 60.637.180	$ 60.637.180

	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 las etapas 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.	UNIDAD	1	$ 118.903.582	$ 118.903.582

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.				

CERTIFICADO DE EXISTENCIA Y REPRESENTACIÓN LEGAL

Fecha Expedición: 3 de junio de 2026 Hora: 09:28:26
Recibo No. AB26075639
Valor: $ 12,100

CÓDIGO DE VERIFICACIÓN B26075639EA7D5

Verifique el contenido y confiabilidad de este certificado, ingresando a www.ccb.org.co/certificadoselectronicos y digite el respectivo código, para que visualice la imagen generada al momento de su expedición. La verificación se puede realizar de manera ilimitada, durante 60 días calendario contados a partir de la fecha de su expedición.

CON FUNDAMENTO EN LA MATRÍCULA E INSCRIPCIONES EFECTUADAS EN EL REGISTRO MERCANTIL, LA CÁMARA DE COMERCIO CERTIFICA:

NOMBRE, IDENTIFICACIÓN Y DOMICILIO

Razón social: DATASEC S.A.S
Nit: 901223827 1 Administración : Direccion Seccional De Impuestos De Bogota
Domicilio principal: Bogotá D.C.

MATRÍCULA

Matrícula No.	03027356
Fecha de matrícula:	19 de octubre de 2018
Último año renovado:	2026
Fecha de renovación:	24 de marzo de 2026
Grupo NIIF:	Grupo II.

UBICACIÓN

Dirección del domicilio principal:	Cr 14 A # 101 - 11 Of 201
Municipio:	Bogotá D.C.
Correo electrónico:	miguel.caicedo@datasec.com.co
Teléfono comercial 1:	3232901254
Teléfono comercial 2:	No reportó.
Teléfono comercial 3:	No reportó.

Dirección para notificación judicial:	Cr 14 A # 101 - 11 Of 201
Municipio:	Bogotá D.C.
Correo electrónico de notificación:	miguel.caicedo@datasec.com.co
Teléfono para notificación 1:	3232901254
Teléfono para notificación 2:	No reportó.
Teléfono para notificación 3:	No reportó.

La persona jurídica SI autorizó para recibir notificaciones personales a través de correo electrónico, de conformidad con lo establecido en los artículos 291 del Código General del Procesos y 67 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo.

Mario Fernando Avila Cristancho

CERTIFICADO DE EXISTENCIA Y REPRESENTACIÓN LEGAL

Fecha Expedición: 3 de junio de 2026 Hora: 09:28:26
Recibo No. AB26075639
Valor: $ 12,100

CÓDIGO DE VERIFICACIÓN B26075639EA7D5

Verifique el contenido y confiabilidad de este certificado, ingresando a www.ccb.org.co/certificadoselectronicos y digite el respectivo código, para que visualice la imagen generada al momento de su expedición. La verificación se puede realizar de manera ilimitada, durante 60 días calendario contados a partir de la fecha de su expedición.

CONSTITUCIÓN

Por Documento Privado del 7 de junio de 2018 de Asamblea de Accionistas, inscrito en esta Cámara de Comercio el 19 de octubre de 2018, con el No. 02387316 del Libro IX, se constituyó la sociedad de naturaleza Comercial denominada DATASEC S.A.S.

TÉRMINO DE DURACIÓN

La persona jurídica no se encuentra disuelta y su duración es indefinida.

OBJETO SOCIAL

Objeto social: la sociedad tendrá como objeto la realización de cualquier actividad comercial o civil lícita tanto en el territorio nacional como en el exterior, en especial mas no limitada a: a) la compra, venta, fabricación, distribución, representación, comercialización, importación, exportación, mantenimiento, asesoramiento, promoción, implementación, soporte, reparaciones, manejo de información, servicios profesionales de consultoría y asesoramiento gerencial de empresas en temas relacionados con el manejo de la información, soluciones de seguridad informática, manual de funciones, sistemas y computación, software y aplicativos para internet, comercio electrónico y demás aplicaciones de software para redes de computadores e internet, servicio de entrenamiento y enseñanza en general, prestación de servicios de soporte, mantenimiento y monitoreo en línea a través de internet, todo en el ámbito nacional e internacional. B) suscribir acuerdos comerciales con compañías extranjeras, representar o agenciar personas naturales o jurídica, nacionales o extranjeras. C) exportar e importar, agenciar, distribuir, comercializar, comprar o vender a comisión o consignación, o de cualesquiera otra forma o modalidad a otros en la misma forma, toda clase de bienes y servicios, al por mayor o al detal. D) inversión a título oneroso, de sus dineros en otras compañías, así semejantes, complementarias o accesorias de la empresa. E). Inversión de sus dineros, a título oneroso, en toda clase de bienes muebles o inmuebles, así como la administración,

CERTIFICADO DE EXISTENCIA Y REPRESENTACIÓN LEGAL

Fecha Expedición: 3 de junio de 2026 Hora: 09:28:26
Recibo No. AB26075639
Valor: $ 12,100

CÓDIGO DE VERIFICACIÓN B26075639EA7D5

Verifique el contenido y confiabilidad de este certificado, ingresando a www.ccb.org.co/certificadoselectronicos y digite el respectivo código, para que visualice la imagen generada al momento de su expedición. La verificación se puede realizar de manera ilimitada, durante 60 días calendario contados a partir de la fecha de su expedición.

---

construcción, enajenación, constitución de gravámenes, recibir o dar en arrendamiento tales bienes en desarrollo de este objeto, la sociedad podrá ejecutar y celebrara toda clase de operaciones, actos y contratos y en especial: a intervenir ante terceros o antes los accionistas como acreedora o como deudora en toda clase de operaciones de crédito, dando o recibiendo las garantías del caso, cuando haya lugar a ellas; b. Efectuar cualquier clase de operaciones de crédito activo ó pasivo, tales como constituir depósitos, efectuar prestamos, otorgar o recibir documentos negociables, girar aceptar, endosar, asegurar y negociar en general títulos valores y recibirlos en pago; c. Celebrar contratos de cuentas en participación, sea como participe activa o como participe inactiva, d. Adquirir marcas, patentes, procedimientos de fabricación, explotadas en cualquier forma, ya sea utilizándolos directamente o permitiendo su explotación por otras personas naturales o jurídicas contra el pago de regalías o participaciones; f) celebrar así mismo operaciones relacionadas con la protección de sus bienes, negocios y personas a su servicio; g) en general, celebrar toda clase de actos y contratos lícitos que necesarios para el desarrollo de su objeto social.

CAPITAL

* CAPITAL AUTORIZADO *

Valor : $800.000.000,00
No. de acciones : 800.000,00
Valor nominal : $1.000,00

* CAPITAL SUSCRITO *

Valor : $500.000.000,00
No. de acciones : 500.000,00
Valor nominal : $1.000,00

* CAPITAL PAGADO *

Valor : $500.000.000,00
No. de acciones : 500.000,00
Valor nominal : $1.000,00

CERTIFICADO DE EXISTENCIA Y REPRESENTACIÓN LEGAL

Fecha Expedición: 3 de junio de 2026 Hora: 09:28:26
Recibo No. AB26075639
Valor: $ 12,100

CÓDIGO DE VERIFICACIÓN B26075639EA7D5

Verifique el contenido y confiabilidad de este certificado, ingresando a www.ccb.org.co/certificadoselectronicos y digite el respectivo código, para que visualice la imagen generada al momento de su expedición. La verificación se puede realizar de manera ilimitada, durante 60 días calendario contados a partir de la fecha de su expedición.

REPRESENTACIÓN LEGAL

La representación legal de la sociedad por acciones simplificada S.A.S., estará a cargo de una persona natural o jurídica, accionista o no, quien podrá tener un (1) suplente que lo reemplazará en sus faltas temporales, transitorias o absolutas o en los casos en que aquel estuviere impedido para actual por razones de orden legal.

FACULTADES Y LIMITACIONES DEL REPRESENTANTE LEGAL

El Representante Legal ejercerá todas las funciones propias de la naturaleza de su cargo, y en especial las siguientes: 1) Representar a la sociedad y los socios ante terceros y ante toda clase de autoridades del orden administrativo o jurisdiccional; 2) Ejecutar todos los actos u operaciones comprendidas dentro del objeto social o que se relacionen con la existencia y el funcionamiento de la sociedad o las que sean impartidas por la Asamblea General de Accionistas; 3) Autorizar con su firma todos los documentos, públicos o privados que deban otorgarse en desarrollo de las actividades sociales o en interés de la compañía; 4) Presentar a la Asamblea General de Accionistas en su primera reunión ordinaria del año, un balance general de fin de ejercicio, con un inventario general, un informe escrito sobre la situación de la sociedad, un detalle completo de la cuenta de pérdidas y ganancias y un proyecto de distribución de utilidades; 5) Presentar a la Asamblea General de Accionistas, cada mes, el balance de prueba del mes anterior y suministrarle los informes que ésta le solicite en relación con la compañía y las actividades sociales; 6) Con autorización previa del Gerente General, nombrar y remover los empleados de la sociedad cuyo nombramiento y remoción no corresponda a la Asamblea general. Todos los empleados de la compañía, con excepción de los elegidos por la Asamblea General de Accionistas, estarán sometidos al Gerente General en el desempeño de sus cargos; 7) Tomar las medidas que reclame la conservación de los bienes sociales, vigilar la actividad de los empleados de la sociedad e impartir las órdenes e instrucciones que exija la buena marcha de la compañía; 8) Convocar a la Asamblea General de Accionistas a las reuniones ordinarias y extraordinarias cuando lo juzgue necesario; 9) Cumplir oportunamente los requisitos y exigencias legales que se relacionen con el funcionamiento y las actividades de la sociedad; 10) Manejar los fondos sociales, girar, cancelar, recibir, firmar letras, pagarés, cheques, giros, libranzas

CERTIFICADO DE EXISTENCIA Y REPRESENTACIÓN LEGAL

Fecha Expedición: 3 de junio de 2026 Hora: 09:28:26
Recibo No. AB26075639
Valor: $ 12,100

CÓDIGO DE VERIFICACIÓN B26075639EA7D5

Verifique el contenido y confiabilidad de este certificado, ingresando a www.ccb.org.co/certificadoselectronicos y digite el respectivo código, para que visualice la imagen generada al momento de su expedición. La verificación se puede realizar de manera ilimitada, durante 60 días calendario contados a partir de la fecha de su expedición.

---

y cualesquiera otros títulos valores, así como negociarlos, tomarlos, pagarlos y descontarlos.; 11) Celebrar todos los actos y contratos para el normal desarrollo de la sociedad, sin límite de cuantía 12) En los procesos de contratación pública podrá presentar propuestas, firmar, ejecutar y liquidar el contrato en caso de resultar adjudicatario. Al igual que podrá delegar estas funciones en caso de necesitar unirse con otras empresas bajo las modalidades de Consorcios o Uniones Temporales. 13) Le está prohibido al representante legal y a los demás administradores de la sociedad, por sí o por interpuesta persona, obtener bajo cualquier forma o modalidad jurídica préstamos por parte de la sociedad u obtener de parte de la sociedad aval, fianza o cualquier otro tipo de garantía de sus obligaciones personales, 14) Cumplir las demás funciones que le señalen la Asamblea General de Accionistas y aquellas que le sean propias de acuerdo con la ley y los Estatutos, como órgano ejecutivo de la sociedad.
PARAGRAFO: FUNCIONES DELREPRESENTANTE LEGAL SUPLENTE: El Representante Legal Suplente tendrá las siguientes atribuciones a nivel de autorizaciones y firmas: 1. Celebrar y ejecutar todos los actos relacionados con ofertas, contratos, órdenes de compra y de servicio del cliente, extensiones o prórrogas de contratos y cartas de solicitud de extensiones, aprobación de contratos en SECOP II, actas de inicio y liquidación de contratos, acuerdos de unión temporal, en montos iguales o inferiores a Mil Millones de pesos moneda corriente ($1.000.000.000.). 2. Aprobación de observaciones en etapa de prepliegos, pliegos definitivos y subsanaciones en procesos públicos. Una vez sometida a votación la propuesta de modificación de estatutos, esta es aprobada por el 100% de las acciones presentes en la asamblea. El señor Miguel Caicedo Ambuila, quien, estando presente en la asamblea, manifiesta que acepta la designación.

NOMBRAMIENTOS

REPRESENTANTES LEGALES

Por Acta No. 014 del 3 de junio de 2025, de Asamblea de Accionistas, inscrita en esta Cámara de Comercio el 6 de junio de 2025 con el No. 03263808 del Libro IX, se designó a:

CARGO	NOMBRE	IDENTIFICACIÓN

CERTIFICADO DE EXISTENCIA Y REPRESENTACIÓN LEGAL

Fecha Expedición: 3 de junio de 2026 Hora: 09:28:26
Recibo No. AB26075639
Valor: $ 12,100

CÓDIGO DE VERIFICACIÓN B26075639EA7D5

Verifique el contenido y confiabilidad de este certificado, ingresando a www.ccb.org.co/certificadoselectronicos y digite el respectivo código, para que visualice la imagen generada al momento de su expedición. La verificación se puede realizar de manera ilimitada, durante 60 días calendario contados a partir de la fecha de su expedición.

Representante Legal	Miguel Caicedo Ambuila	C.C. No. 4655022

CARGO	NOMBRE	IDENTIFICACIÓN
Representante Legal Suplente	Raiza Del Valle Benitez Ramos	C.E. No. 563777

REVISORES FISCALES

Por Acta No. 007 del 10 de febrero de 2023, de Asamblea de Accionistas, inscrita en esta Cámara de Comercio el 22 de febrero de 2023 con el No. 02936945 del Libro IX, se designó a:

CARGO	NOMBRE	IDENTIFICACIÓN
Revisor Fiscal Persona Juridica	CR FINANCIAL & LEGAL SERVICES COLOMBIA S A S	N.I.T. No. 900179223 1

Por Documento Privado del 3 de enero de 2025, de Revisor Fiscal, inscrita en esta Cámara de Comercio el 3 de enero de 2025 con el No. 03193890 del Libro IX, se designó a:

CARGO	NOMBRE	IDENTIFICACIÓN
Revisor Fiscal Principal	Sandra Yaneth Gil Moreno	C.C. No. 1016019034 T.P. No. 301138-T

Por Documento Privado del 15 de febrero de 2023, de Revisor Fiscal, inscrita en esta Cámara de Comercio el 22 de febrero de 2023 con el No. 02936946 del Libro IX, se designó a:

CARGO	NOMBRE	IDENTIFICACIÓN
Revisor Fiscal Suplente	Rosa Daisy Amaya De Reyes	C.C. No. 41483476 T.P. No. 6664-T

REFORMAS DE ESTATUTOS

CERTIFICADO DE EXISTENCIA Y REPRESENTACIÓN LEGAL

Fecha Expedición: 3 de junio de 2026 Hora: 09:28:26
Recibo No. AB26075639
Valor: $ 12,100

CÓDIGO DE VERIFICACIÓN B26075639EA7D5

Verifique el contenido y confiabilidad de este certificado, ingresando a www.ccb.org.co/certificadoselectronicos y digite el respectivo código, para que visualice la imagen generada al momento de su expedición. La verificación se puede realizar de manera ilimitada, durante 60 días calendario contados a partir de la fecha de su expedición.

Los estatutos de la sociedad han sido reformados así:

DOCUMENTO	INSCRIPCIÓN
Acta No. 006 del 17 de noviembre de 2022 de la Asamblea de Accionistas	02909208 del 14 de diciembre de 2022 del Libro IX
Acta No. 11 del 6 de noviembre de 2024 de la Asamblea de Accionistas	03186893 del 12 de diciembre de 2024 del Libro IX
Acta No. 014 del 3 de junio de 2025 de la Asamblea de Accionistas	03263809 del 6 de junio de 2025 del Libro IX

RECURSOS CONTRA LOS ACTOS DE INSCRIPCIÓN

De conformidad con lo establecido en el Código de Procedimiento Administrativo y de lo Contencioso Administrativo y la Ley 962 de 2005, los actos administrativos de registro, quedan en firme dentro de los diez (10) días hábiles siguientes a la fecha de inscripción, siempre que no sean objeto de recursos. Para estos efectos, se informa que para la Cámara de Comercio de Bogotá, los sábados NO son días hábiles.

Una vez interpuestos los recursos, los actos administrativos recurridos quedan en efecto suspensivo, hasta tanto los mismos sean resueltos, conforme lo prevé el artículo 79 del Código de Procedimiento Administrativo y de los Contencioso Administrativo.

A la fecha y hora de expedición de este certificado, NO se encuentra en curso ningún recurso.

CLASIFICACIÓN DE ACTIVIDADES ECONÓMICAS - CIIU

Actividad principal Código CIIU: 4741
Actividad secundaria Código CIIU: 9511
Otras actividades Código CIIU: 6209, 6202

TAMAÑO EMPRESARIAL

CERTIFICADO DE EXISTENCIA Y REPRESENTACIÓN LEGAL

Fecha Expedición: 3 de junio de 2026 Hora: 09:28:26
Recibo No. AB26075639
Valor: $ 12,100

CÓDIGO DE VERIFICACIÓN B26075639EA7D5

Verifique el contenido y confiabilidad de este certificado, ingresando a www.ccb.org.co/certificadoselectronicos y digite el respectivo código, para que visualice la imagen generada al momento de su expedición. La verificación se puede realizar de manera ilimitada, durante 60 días calendario contados a partir de la fecha de su expedición.

De conformidad con lo previsto en el artículo 2.2.1.13.2.1 del Decreto 1074 de 2015 y la Resolución 2225 de 2019 del DANE el tamaño de la empresa es Mediana

Lo anterior de acuerdo a la información reportada por el matriculado o inscrito en el formulario RUES:

Ingresos por actividad ordinaria $ 34.210.985.000
Actividad económica por la que percibió mayores ingresos en el período - CIIU : 4741

INFORMACIÓN COMPLEMENTARIA

Que, los datos del empresario y/o el establecimiento de comercio han sido puestos a disposición de la Policía Nacional a través de la consulta a la base de datos del RUES.

Los siguientes datos sobre RIT y Planeación son informativos: Contribuyente inscrito en el registro RIT de la Dirección de Impuestos, fecha de inscripción : 26 de marzo de 2022. Fecha de envío de información a Planeación : 12 de abril de 2026. \n \n Señor empresario, si su empresa tiene activos inferiores a 30.000 SMLMV y una planta de personal de menos de 200 trabajadores, usted tiene derecho a recibir un descuento en el pago de los parafiscales de 75% en el primer año de constitución de su empresa, de 50% en el segundo año y de 25% en el tercer año. Ley 590 de 2000 y Decreto 525 de 2009. Recuerde ingresar a www.supersociedades.gov.co para verificar si su empresa está obligada a remitir estados financieros. Evite sanciones.

El presente certificado no constituye permiso de funcionamiento en ningún caso.

****

Este certificado refleja la situación jurídica registral de la sociedad, a la fecha y hora de su expedición.

****

Este certificado fue generado electrónicamente con firma digital y cuenta con plena validez jurídica conforme a la Ley 527 de 1999.

CERTIFICADO DE EXISTENCIA Y REPRESENTACIÓN LEGAL

Fecha Expedición: 3 de junio de 2026 Hora: 09:28:26
Recibo No. AB26075639
Valor: $ 12,100

CÓDIGO DE VERIFICACIÓN B26075639EA7D5

Verifique el contenido y confiabilidad de este certificado, ingresando a www.ccb.org.co/certificadoselectronicos y digite el respectivo código, para que visualice la imagen generada al momento de su expedición. La verificación se puede realizar de manera ilimitada, durante 60 días calendario contados a partir de la fecha de su expedición.

****

Firma mecánica de conformidad con el Decreto 2150 de 1995 y la autorización impartida por la Superintendencia de Industria y Comercio, mediante el oficio del 18 de noviembre de 1996.

Outlook

Cotización Infraestructura de seguridad perimetral

Desde Adriana Escobar <aescobar@ingeniumcolombia.com>
Fecha Jue 25/06/2026 19:15
Para Secretaria General <secretariageneral@monteria.gov.co>

2 archivos adjuntos (6 MB)
CCB 110626.pdf; INGENIUM MONTERIA.zip;

Cordial saludo,

Adjunto nos permitimos enviar cotización al proceso "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".

Gracias por la atención y quedo atenta a sus comentarios,

INGENIUM

ANEXO 1 – ESPECIFICACIONES TÉCNICAS

El proyecto comprende la implementación de la solución integral de infraestructura y ciberseguridad, para fortalecer la conectividad LAN y WLAN 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 YMANTENIMIENTO

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	VALOR UNITARIO	VALOR TOTAL
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 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.)	UNIDAD	4	$ 62.319.528	$ 249.278.111

	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 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.	UNIDAD	1	$ 14.095.403	$ 14.095.403

	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.	UNIDAD	1	$ 7.938.448	$ 7.938.448

	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 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 de administración centralizada a adquirir por parte la entidad.	UNIDAD	1	$ 16.469.745	$ 16.469.745
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.	UNIDAD	13	$ 6.079.604	$ 79.034.849

	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 - 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**	$ 411.744	$ 3.293.949
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)	UNIDAD	9	$ 9.536.721	$ 85.830.493

	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				
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	UNIDAD	3	$ 5.646.164	$ 16.938.493

	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 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				
9	**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	UNIDAD	1	$ 10.349.832	$ 10.349.832

	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				
10	**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	$ 3.293.949	$ 9.881.847
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	1	$ 3.293.949	$ 3.293.949

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 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,	UNIDAD	1	$ 58.039.482	$ 58.039.482

	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 las etapas 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.	UNIDAD	1	$ 120.293.839	$ 120.293.839

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.				

CERTIFICADO DE EXISTENCIA Y REPRESENTACIÓN LEGAL

Fecha Expedición: 11 de junio de 2026 Hora: 11:21:50
Recibo No. AB26126347
Valor: $ 12,100

CÓDIGO DE VERIFICACIÓN B26126347DFE76

Verifique el contenido y confiabilidad de este certificado, ingresando a www.ccb.org.co/certificadoselectronicos y digite el respectivo código, para que visualice la imagen generada al momento de su expedición. La verificación se puede realizar de manera ilimitada, durante 60 días calendario contados a partir de la fecha de su expedición.

CON FUNDAMENTO EN LA MATRÍCULA E INSCRIPCIONES EFECTUADAS EN EL REGISTRO MERCANTIL, LA CÁMARA DE COMERCIO CERTIFICA:

NOMBRE, IDENTIFICACIÓN Y DOMICILIO

Razón social: INGENIUM COLOMBIA SAS
Nit: 900500876 5 Administración : Girardot, Regimen Comun
Domicilio principal: Bogotá D.C.

MATRÍCULA

Matrícula No.	02184150
Fecha de matrícula:	21 de febrero de 2012
Último año renovado:	2026
Fecha de renovación:	16 de marzo de 2026
Grupo NIIF:	Grupo II.

El empresario se acogió al beneficio que establece el artículo 7 de la Ley 1429 del 29 de diciembre de 2010, y que al realizar la renovación de la matrícula mercantil informó bajo gravedad de juramento los siguientes datos:
El empresario INGENIUM COLOMBIA SAS realizó la renovación en la fecha: 16 de marzo de 2026.
El número de trabajadores ocupados reportado por el empresario en su última renovación es de: 30.

UBICACIÓN

Dirección del domicilio principal:	Carrera 19 #95-20 Oficina 704
Municipio:	Bogotá D.C.
Correo electrónico:	info@ingeniumcolombia.com
Teléfono comercial 1:	3202909525
Teléfono comercial 2:	3005695329
Teléfono comercial 3:	No reportó.

Dirección para notificación judicial:	Carrera 19 #95-20 Oficina 704
Municipio:	Bogotá D.C.
Correo electrónico de notificación:	info@ingeniumcolombia.com

Mario Fernando Avila Cristancho

CERTIFICADO DE EXISTENCIA Y REPRESENTACIÓN LEGAL

Fecha Expedición: 11 de junio de 2026 Hora: 11:21:50
Recibo No. AB26126347
Valor: $ 12,100

CÓDIGO DE VERIFICACIÓN B26126347DFE76

Verifique el contenido y confiabilidad de este certificado, ingresando a www.ccb.org.co/certificadoselectronicos y digite el respectivo código, para que visualice la imagen generada al momento de su expedición. La verificación se puede realizar de manera ilimitada, durante 60 días calendario contados a partir de la fecha de su expedición.

Teléfono para notificación 1: 3202909525
Teléfono para notificación 2: 3143845903
Teléfono para notificación 3: No reportó.

La persona jurídica SI autorizó para recibir notificaciones personales a través de correo electrónico, de conformidad con lo establecido en los artículos 291 del Código General del Procesos y 67 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo.

CONSTITUCIÓN

Por Documento Privado del 17 de febrero de 2012 de Asamblea de Accionistas, inscrito en esta Cámara de Comercio el 21 de febrero de 2012, con el No. 01609036 del Libro IX, se constituyó la sociedad de naturaleza Comercial denominada INGENIUM COLOMBIA SAS.

TÉRMINO DE DURACIÓN

La persona jurídica no se encuentra disuelta y su duración es indefinida.

OBJETO SOCIAL

Consultoría e implementación de soluciones integrales para la transformación digital, incluido arquitectura empresarial, seguridad de la información, gobierno y calidad de datos, además de la venta de licencias de software de herramientas de arquitectura, seguridad de la información, software de gobierno de datos y soluciones de nube e inteligencia artificial.

CAPITAL

* CAPITAL AUTORIZADO *

Valor : $7.900.000,00
No. de acciones : 7.900,00

CERTIFICADO DE EXISTENCIA Y REPRESENTACIÓN LEGAL

Fecha Expedición: 11 de junio de 2026 Hora: 11:21:50
Recibo No. AB26126347
Valor: $ 12,100

CÓDIGO DE VERIFICACIÓN B26126347DFE76

Verifique el contenido y confiabilidad de este certificado, ingresando a www.ccb.org.co/certificadoselectronicos y digite el respectivo código, para que visualice la imagen generada al momento de su expedición. La verificación se puede realizar de manera ilimitada, durante 60 días calendario contados a partir de la fecha de su expedición.

Valor nominal : $1.000,00

* CAPITAL SUSCRITO *

Valor : $7.900.000,00
No. de acciones : 7.900,00
Valor nominal : $1.000,00

* CAPITAL PAGADO *

Valor : $7.900.000,00
No. de acciones : 7.900,00
Valor nominal : $1.000,00

REPRESENTACIÓN LEGAL

La representación legal de la Sociedad Por Acciones Simplificadas estará a cargo de una Persona Natural o Jurídica, Accionista o no, quien tendrá suplentes, designado para un término de un año por la Asamblea General de Accionistas.

FACULTADES Y LIMITACIONES DEL REPRESENTANTE LEGAL

Son funciones del Representante. a) Constituir, para propósitos concretos, los apoderados especiales que considere necesarios para representar judicial o extrajudicialmente a la sociedad. b) Certificar conjuntamente con el contador y el Revisor Fiscal de la compañía los estados financieros en el caso de ser exigido por las normas legales. c) Celebrar los contratos que de acuerdo con las circunstancias sean convenientes. d) Celebrar los actos y contratos comprendidos en el objeto social de la empresa y los necesarios para que esta desarrolle plenamente los fines para los cuales ha sido constituida. e) Cumplir las demás funciones que le correspondan según lo previsto en las normas legales, en estos estatutos y las que sean compatibles con el cargo. Parágrafo: El representante legal queda facultado para celebrar actos y contratos, en desarrollo del objeto de la sociedad, con entidades públicas, privadas y mixtas, sin límite de cuantía.

CERTIFICADO DE EXISTENCIA Y REPRESENTACIÓN LEGAL

Fecha Expedición: 11 de junio de 2026 Hora: 11:21:50
Recibo No. AB26126347
Valor: $ 12,100

CÓDIGO DE VERIFICACIÓN B26126347DFE76

Verifique el contenido y confiabilidad de este certificado, ingresando a www.ccb.org.co/certificadoselectronicos y digite el respectivo código, para que visualice la imagen generada al momento de su expedición. La verificación se puede realizar de manera ilimitada, durante 60 días calendario contados a partir de la fecha de su expedición.

NOMBRAMIENTOS

REPRESENTANTES LEGALES

Por Acta No. 21 del 1 de abril de 2025, de Asamblea de Accionistas, inscrita en esta Cámara de Comercio el 2 de abril de 2025 con el No. 03226831 del Libro IX, se designó a:

CARGO	NOMBRE	IDENTIFICACIÓN
Gerente General	Adriana Lucia Escobar Castañeda	C.C. No. 1069734144

CARGO	NOMBRE	IDENTIFICACIÓN
Suplente	Andres Felipe Mendez Antolinez	C.C. No. 1019005663

REVISORES FISCALES

Por Acta No. 5 del 4 de enero de 2023, de Asamblea de Accionistas, inscrita en esta Cámara de Comercio el 31 de enero de 2023 con el No. 02928327 del Libro IX, se designó a:

CARGO	NOMBRE	IDENTIFICACIÓN
Revisor Fiscal	Jorge Eduardo Molina Jimenez	C.C. No. 1072894364 T.P. No. 190330-T

REFORMAS DE ESTATUTOS

Los estatutos de la sociedad han sido reformados así:

DOCUMENTO	INSCRIPCIÓN
Acta No. 020 del 15 de septiembre de 2024 de la Asamblea de Accionistas	03171527 del 25 de octubre de 2024 del Libro IX

CERTIFICADO DE EXISTENCIA Y REPRESENTACIÓN LEGAL

Fecha Expedición: 11 de junio de 2026 Hora: 11:21:50
Recibo No. AB26126347
Valor: $ 12,100

CÓDIGO DE VERIFICACIÓN B26126347DFE76

Verifique el contenido y confiabilidad de este certificado, ingresando a www.ccb.org.co/certificadoselectronicos y digite el respectivo código, para que visualice la imagen generada al momento de su expedición. La verificación se puede realizar de manera ilimitada, durante 60 días calendario contados a partir de la fecha de su expedición.

RECURSOS CONTRA LOS ACTOS DE INSCRIPCIÓN

De conformidad con lo establecido en el Código de Procedimiento Administrativo y de lo Contencioso Administrativo y la Ley 962 de 2005, los actos administrativos de registro, quedan en firme dentro de los diez (10) días hábiles siguientes a la fecha de inscripción, siempre que no sean objeto de recursos. Para estos efectos, se informa que para la Cámara de Comercio de Bogotá, los sábados NO son días hábiles.

Una vez interpuestos los recursos, los actos administrativos recurridos quedan en efecto suspensivo, hasta tanto los mismos sean resueltos, conforme lo prevé el artículo 79 del Código de Procedimiento Administrativo y de los Contencioso Administrativo.

A la fecha y hora de expedición de este certificado, NO se encuentra en curso ningún recurso.

CLASIFICACIÓN DE ACTIVIDADES ECONÓMICAS - CIIU

Actividad principal Código CIIU: 7112
Actividad secundaria Código CIIU: 6209

TAMAÑO EMPRESARIAL

De conformidad con lo previsto en el artículo 2.2.1.13.2.1 del Decreto 1074 de 2015 y la Resolución 2225 de 2019 del DANE el tamaño de la empresa es Mediana

Lo anterior de acuerdo a la información reportada por el matriculado o inscrito en el formulario RUES:

Ingresos por actividad ordinaria $ 12.286.050.132
Actividad económica por la que percibió mayores ingresos en el período - CIIU : 7112

INFORMACIÓN COMPLEMENTARIA

Que, los datos del empresario y/o el establecimiento de comercio han

CERTIFICADO DE EXISTENCIA Y REPRESENTACIÓN LEGAL

Fecha Expedición: 11 de junio de 2026 Hora: 11:21:50
Recibo No. AB26126347
Valor: $ 12,100

CÓDIGO DE VERIFICACIÓN B26126347DFE76

Verifique el contenido y confiabilidad de este certificado, ingresando a www.ccb.org.co/certificadoselectronicos y digite el respectivo código, para que visualice la imagen generada al momento de su expedición. La verificación se puede realizar de manera ilimitada, durante 60 días calendario contados a partir de la fecha de su expedición.

---

sido puestos a disposición de la Policía Nacional a través de la consulta a la base de datos del RUES.

Los siguientes datos sobre RIT y Planeación son informativos: Contribuyente inscrito en el registro RIT de la Dirección de Impuestos, fecha de inscripción : 27 de marzo de 2023. Fecha de envío de información a Planeación : 17 de marzo de 2026. \n \n Señor empresario, si su empresa tiene activos inferiores a 30.000 SMLMV y una planta de personal de menos de 200 trabajadores, usted tiene derecho a recibir un descuento en el pago de los parafiscales de 75% en el primer año de constitución de su empresa, de 50% en el segundo año y de 25% en el tercer año. Ley 590 de 2000 y Decreto 525 de 2009. Recuerde ingresar a www.supersociedades.gov.co para verificar si su empresa está obligada a remitir estados financieros. Evite sanciones.

El presente certificado no constituye permiso de funcionamiento en ningún caso.

****
Este certificado refleja la situación jurídica registral de la sociedad, a la fecha y hora de su expedición.

****
Este certificado fue generado electrónicamente con firma digital y cuenta con plena validez jurídica conforme a la Ley 527 de 1999.
****
****
****
****
****
****
****
****
****
****
****
****

CERTIFICADO DE EXISTENCIA Y REPRESENTACIÓN LEGAL

Fecha Expedición: 11 de junio de 2026 Hora: 11:21:50
Recibo No. AB26126347
Valor: $ 12,100

CÓDIGO DE VERIFICACIÓN B26126347DFE76

Verifique el contenido y confiabilidad de este certificado, ingresando a www.ccb.org.co/certificadoselectronicos y digite el respectivo código, para que visualice la imagen generada al momento de su expedición. La verificación se puede realizar de manera ilimitada, durante 60 días calendario contados a partir de la fecha de su expedición.

****

Firma mecánica de conformidad con el Decreto 2150 de 1995 y la autorización impartida por la Superintendencia de Industria y Comercio, mediante el oficio del 18 de noviembre de 1996.

Outlook

Oferta Económica Solución Fortinet

Desde FELIPE MUNOZ MUNOZ <felipe.munoz@growdata.com.co>
Fecha Jue 25/06/2026 17:59
Para Kátherin Ramos Licona <kramos.tic@monteria.gov.co>; Secretaria General <secretariageneral@monteria.gov.co>

1 archivo adjunto (7 MB)
GROWDATA.zip;

Cordial saludo,

Acorde a la invitación recibida nos permitimos remitir oferta económica para el suministro de equipos de seguridad del fabricante Fortinet.

Quedamos atentos a resolver cualquier inquietud.

Cordialmente,

ANEXO 1 – ESPECIFICACIONES TÉCNICAS

El proyecto comprende la implementación de la solución integral de infraestructura y ciberseguridad, para fortalecer la conectividad LAN y WLAN 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 YMANTENIMIENTO

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	VALOR UNITARIO	VALOR TOTAL
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 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.)	UNIDAD	4	$ 60.239.735	$ 240.958.939

	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 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.	UNIDAD	1	$ 16.049.389	$ 16.049.389

	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.	UNIDAD	1	$ 8.184.783	$ 8.184.783

	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 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 de administración centralizada a adquirir por parte la entidad.	UNIDAD	1	$ 14.547.392	$ 14.547.392
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.	UNIDAD	13	$ 5.840.722	$ 75.929.383

	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 - 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**	$ 363.685	$ 2.909.478
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)	UNIDAD	9	$ 8.942.549	$ 80.482.938

	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				
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	UNIDAD	3	$ 6.031.461	$ 18.094.383

	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 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				
9	**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	UNIDAD	1	$ 11.048.395	$ 11.048.395

	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				
10	**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	$ 2.909.478	$ 8.728.435
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	1	$ 2.909.478	$ 2.909.478

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 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,	UNIDAD	1	$ 60.938.493	$ 60.938.493

	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 las etapas 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.	UNIDAD	1	$ 117.783.094	$ 117.783.094

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.				

CERTIFICADO DE EXISTENCIA Y REPRESENTACIÓN LEGAL

Fecha Expedición: 4 de junio de 2026 Hora: 15:00:23
Recibo No. AB26088679
Valor: $ 12,100

CÓDIGO DE VERIFICACIÓN B26088679B0DA4

Verifique el contenido y confiabilidad de este certificado, ingresando a www.ccb.org.co/certificadoselectronicos y digite el respectivo código, para que visualice la imagen generada al momento de su expedición. La verificación se puede realizar de manera ilimitada, durante 60 días calendario contados a partir de la fecha de su expedición.

CON FUNDAMENTO EN LA MATRÍCULA E INSCRIPCIONES EFECTUADAS EN EL REGISTRO MERCANTIL, LA CÁMARA DE COMERCIO CERTIFICA:

NOMBRE, IDENTIFICACIÓN Y DOMICILIO

Razón social: GROW DATA SAS
Nit: 900238438 1
Domicilio principal: Bogotá D.C.

MATRÍCULA

Matrícula No.	01833379
Fecha de matrícula:	3 de septiembre de 2008
Último año renovado:	2026
Fecha de renovación:	17 de marzo de 2026

UBICACIÓN

Dirección del domicilio principal:	Cl 93 # 11 A -11
Municipio:	Bogotá D.C.
Correo electrónico:	comunicados@growdata.com.co
Teléfono comercial 1:	6017465659
Teléfono comercial 2:	3212052325
Teléfono comercial 3:	No reportó.
Página web:	HTTPS://GROWDATA.COM.CO

Dirección para notificación judicial:	Cl 93 # 11 A -11
Municipio:	Bogotá D.C.
Correo electrónico de notificación:	comunicados@growdata.com.co
Teléfono para notificación 1:	6017465659
Teléfono para notificación 2:	3212052325
Teléfono para notificación 3:	No reportó.

La persona jurídica NO autorizó para recibir notificaciones personales a través de correo electrónico, de conformidad con lo establecido en los artículos 291 del Código General del Procesos y 67 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo.

Mario Fernando Avila Cristancho

CERTIFICADO DE EXISTENCIA Y REPRESENTACIÓN LEGAL

Fecha Expedición: 4 de junio de 2026 Hora: 15:00:23
Recibo No. AB26088679
Valor: $ 12,100

CÓDIGO DE VERIFICACIÓN B26088679B0DA4

Verifique el contenido y confiabilidad de este certificado, ingresando a www.ccb.org.co/certificadoselectronicos y digite el respectivo código, para que visualice la imagen generada al momento de su expedición. La verificación se puede realizar de manera ilimitada, durante 60 días calendario contados a partir de la fecha de su expedición.

CONSTITUCIÓN

Por Escritura Pública No. 0005941 del 14 de agosto de 2008 de Notaría 24 de Bogotá D.C., inscrito en esta Cámara de Comercio el 3 de septiembre de 2008, con el No. 01239540 del Libro IX, se constituyó la sociedad de naturaleza Comercial denominada GREENSCO LTDA.

REFORMAS ESPECIALES

Por Acta No. 03 de la junta de socios, del 29 de agosto de 2009, inscrita el 09 de octubre de 2009 bajo el número 01333102 del libro IX, la sociedad de la referencia se transformó de sociedad limitada a sociedad por acciones simplificada bajo el nombre de: GREENSCO S.A.S.

Por Acta del 29 de agosto de 2009 de Junta de Socios, inscrito en esta Cámara de Comercio el 9 de octubre de 2009, con el No. 01333102 del Libro IX, la sociedad cambió su denominación o razón social de GREENSCO LTDA a GREENSCO S A S.

Por Acta No. 14 del 4 de mayo de 2015 de Asamblea de Accionistas, inscrito en esta Cámara de Comercio el 26 de mayo de 2015, con el No. 01942706 del Libro IX, la sociedad cambió su denominación o razón social de GREENSCO S A S a GROW DATA SAS.

TÉRMINO DE DURACIÓN

La persona jurídica no se encuentra disuelta y su duración es indefinida.

La persona jurídica se disolvió y entró en estado de liquidación mediante Acta No. 10 del 17 de octubre de 2013 de Asamblea de Accionistas , inscrita en esta Cámara de Comercio el 19 de noviembre de 2013 con el No. 01782017 del Libro IX y por Acta No. 11 del 29 de noviembre de 2013 de Asamblea de Accionistas , inscrita en esta Cámara de Comercio el 2 de diciembre de 2013 con el No. 01785969 del Libro IX, la persona jurídica de la referencia se reactivó.

CERTIFICADO DE EXISTENCIA Y REPRESENTACIÓN LEGAL

Fecha Expedición: 4 de junio de 2026 Hora: 15:00:23
Recibo No. AB26088679
Valor: $ 12,100

CÓDIGO DE VERIFICACIÓN B26088679B0DA4

Verifique el contenido y confiabilidad de este certificado, ingresando a www.ccb.org.co/certificadoselectronicos y digite el respectivo código, para que visualice la imagen generada al momento de su expedición. La verificación se puede realizar de manera ilimitada, durante 60 días calendario contados a partir de la fecha de su expedición.

OBJETO SOCIAL

La sociedad desarrollará su objeto social de forma principal con empresas del sector público y privado nacional e internacional, sus actividades comerciales serán principalmente las siguientes: A. Servicios de tecnología e información de las comunicaciones. B. Asesorías empresariales en gestión técnica, administrativa, financiera operativa y comercial en proyectos. C. Suministro e instalación en calidad de venta, arrendamiento, servicios administrados, leasing de equipos especializados de tecnología tales como: Equipos de cómputo de escritorio, equipos de cómputo portátiles, servidores, impresoras, escáner, accesorios, dispositivos móviles, equipos de comunicaciones y redes, telefonía IP, equipos de seguridad informática, equipos de conectividad y sus accesorios, equipos eléctricos, equipos de video, circuito cerrado de televisión, equipos de almacenamiento y monitoreo de cámaras, equipos de seguridad física, controles de acceso. D. Desarrollo de aplicaciones a la medida. E. Suministro en calidad de venta, arrendamiento, servicios administrados, leasing de aplicaciones y software. F. Desarrollo de aplicaciones a la medida. G. Mantenimiento de software y hardware, mantenimiento de equipos instalaciones. H. Instalaciones eléctricas. I. Servicios de datacenter, suministro y administración de cuentas de correo y conectividad. J. Soluciones en la nube. K. Soluciones de mesa de ayuda o help desk, mesa de servicios, outsourcing de TI, administración delegada de tecnología. L. Estructurar, gestionar, gerenciar y desarrollar proyectos relacionados con sistemas de información, gestión económica financiera, gestión comercial, gestión de personal, gestión de calidad y gestión de seguridad; así como la auditoría de estos. M. Prestar servicios de asesoramiento, diagnóstico, planeación y acompañamiento para la adopción e implementación de estrategias de sostenibilidad empresarial y ambiental. N. Desarrollo de estudios ambientales, estudios de impacto ambiental, Monitoreo ambiental, Gestión de residuos, Restauración ecológica y educación ambiental. O. Modelos de desarrollo sostenible que facilite o las entidades la incorporación estructurada de un buen gobierno. P. Elaboración de informes de sostenibilidad, implementación de estándares internacionales y capacitación en buenas prácticas. Q. Diseñar, desarrollar, implementar y mantener soluciones tecnológicas basadas en analítica avanzada e inteligencia artificial para dispositivos y

CERTIFICADO DE EXISTENCIA Y REPRESENTACIÓN LEGAL

Fecha Expedición: 4 de junio de 2026 Hora: 15:00:23
Recibo No. AB26088679
Valor: $ 12,100

CÓDIGO DE VERIFICACIÓN B26088679B0DA4

Verifique el contenido y confiabilidad de este certificado, ingresando a www.ccb.org.co/certificadoselectronicos y digite el respectivo código, para que visualice la imagen generada al momento de su expedición. La verificación se puede realizar de manera ilimitada, durante 60 días calendario contados a partir de la fecha de su expedición.

---

mejorar la toma de decisiones empresariales incluyendo la recolección, procesamiento y análisis de datos. R. Desarrollo de Capacidades y Transferencia de Conocimiento en liderazgo y habilidades en gerencia pública moderna. S. Implementación de modelos predictivos, sistemas de aprendizaje automático, automatización de procesos, integración de herramientas y algoritmos de inteligencia artificial generativa y desarrollo de aplicaciones personalizadas. T. Despliegue e integración de dispositivos lot en procesos de analítica descriptiva, predictiva, prescriptiva. U. Migración de Bases de Datos Qn premise y en nube. V. Despliegue e implementación de arquitecturas contenerizadas. W. Integración de Procesos y flujos en tiempo real. X. Ofrecer servicios de diseño, instalación, configuración y mantenimiento de redes de cableado estructurado para garantizar la conectividad y el óptimo desempeño de sistemas de telecomunicaciones, redes corporativas y soluciones tecnológicas. Y. Suministro e instalación de equipos y redes de comunicaciones. Z. Suministro e instalación de equipos y redes eléctricas. AB. Servicios de Contact Center. AC. Servicios de Outsourcing de Procesos de Negocio (BPO). AD. Servicios de monitoreo y gestión de infraestructura y plataformas informáticas (NOC). AE. Servicios de monitoreo y gestión de seguridad informática (SOC). AF. Servicios de seguridad informática y ciberseguridad. AG. Servicios de seguridad electrónica. AH. Formación profesional, entrenamiento y capacitación de trabajadores, empresarios y funcionarios. AI. La sociedad podrá ejecutar todos los actos o contratos que fueren convenientes para el cabal cumplimiento de su objeto social y que tengan relación directa con el objeto mencionado. AJ. Podrá firmar contratos de Joint Venture, colaboración empresarial, uniones temporales y consorcios, formar parte de otras sociedades que desarrollen uno o más de los objetos precedentes. AK. Participar en licitaciones y concursos públicos o privados de entidades estatales o particulares, suscribir y ejecutar los contratos adjudicados. AL. Suministro de mobiliario. AM. Prestar servicios de logística, ser licenciatario de marcas o representarlas bajo cualquier modalidad de casas nacionales o internacionales que guarden relación con el objeto de la compañía. AN. Importar y exportar bienes, servicios o tecnología que tengan que ver con el desarrollo del objeto social de la compañía. AO. Celebrar contratos bancarios, realizar toda clase de inversiones, aperturas de cuentas corrientes o de ahorros, en fin, cualquier clase de operación financiera nacional o internacional. AP. Constituir sociedades para el establecimiento de explotación de empresas destinadas a cualquiera de las actividades comprendidas en su objeto social y tomar interés

CERTIFICADO DE EXISTENCIA Y REPRESENTACIÓN LEGAL

Fecha Expedición: 4 de junio de 2026 Hora: 15:00:23
Recibo No. AB26088679
Valor: $ 12,100

CÓDIGO DE VERIFICACIÓN B26088679B0DA4

Verifique el contenido y confiabilidad de este certificado, ingresando a www.ccb.org.co/certificadoselectronicos y digite el respectivo código, para que visualice la imagen generada al momento de su expedición. La verificación se puede realizar de manera ilimitada, durante 60 días calendario contados a partir de la fecha de su expedición.

---

como participe, asociada o accionista en otras sociedades de objeto análogo o complementario al suyo. AQ. Adquirir patentes, nombres comerciales, marcas y demás derechos de propiedad intelectual o industrial, y adquirir u otorgar concesiones. AR. También podrá designar apoderados para que la representen en todos los actos o diligencias que celebre o sea citada. Sin perjuicio de lo anterior, la sociedad podrá realizar cualquier actividad comercial o civil, lícita, de conformidad con lo establecido en el numeral 5° del artículo 5° de la ley 1258, o la norma que sustituya la anotada disposición o haga sus veces.

CAPITAL

* CAPITAL AUTORIZADO *

Valor	: $2.000.000.000,00
No. de acciones	: 20.000,00
Valor nominal	: $100.000,00

* CAPITAL SUSCRITO *

Valor	: $800.000.000,00
No. de acciones	: 8.000,00
Valor nominal	: $100.000,00

* CAPITAL PAGADO *

Valor	: $800.000.000,00
No. de acciones	: 8.000,00
Valor nominal	: $100.000,00

REPRESENTACIÓN LEGAL

El representante legal de la sociedad podrá ser una persona natural o jurídica, tendrá un (01) suplente denominado "Representante legal primer suplente" o "Primer Suplente", cuya función será reemplazar al representante legal en sus faltas temporales o absolutas.

FACULTADES Y LIMITACIONES DEL REPRESENTANTE LEGAL

CERTIFICADO DE EXISTENCIA Y REPRESENTACIÓN LEGAL

Fecha Expedición: 4 de junio de 2026 Hora: 15:00:23
Recibo No. AB26088679
Valor: $ 12,100

CÓDIGO DE VERIFICACIÓN B26088679B0DA4

Verifique el contenido y confiabilidad de este certificado, ingresando a www.ccb.org.co/certificadoselectronicos y digite el respectivo código, para que visualice la imagen generada al momento de su expedición. La verificación se puede realizar de manera ilimitada, durante 60 días calendario contados a partir de la fecha de su expedición.

Son funciones del Representante Legal: A. Llevar la representación legal de la sociedad en todos los actos y contratos, judiciales y extrajudiciales en que ella intervenga. B. Dirigir la administración de la sociedad y la gestión de los negocios, conforme a las estipulaciones estatutarias y a las disposiciones de la Asamblea General de Accionistas. C. Presentar anua]mente a la Asamblea General de Accionistas en sus sesiones ordinarias, o en aquellas que hubieren de aprobar estados financieros, el Balance General de fin de ejercicio, con el informe sobre su gestión y rendirle cuentas cuando ésta lo pida o la Ley lo exija. En el informe se presentará la situación económica y financiera de la compañía y la gestión desempeñada durante el mandato del representante legal, acompañada de las recomendaciones pertinentes. D. Realizar libremente y sin limitación alguna todos los actos, operaciones, asociaciones y contratos comprendidos en el objeto social, que sean necesarios o convenientes para que la sociedad cumpla sus fines, a cabalidad. E. Nombrar apoderados para casos especiales y confiarles todas las funciones que la situación requiera. F. Otorgar préstamos a accionistas. G. Las demás funciones que la Ley o los estatutos le otorguen. El Representante Legal podrá celebrar cualquier tipo de negocio jurídico, enajenar o gravar activos correspondientes a bienes inmuebles de la sociedad, sin ninguna restricción. H. Presentar con el Oficial de Cumplimiento, para aprobación de la Asamblea General de Accionistas, la propuesta del ptee. I. Velar porque el ptee se articule con las Políticas de Cumplimiento adoptadas por la Asamblea General de Accionistas. J. Prestar efectivo, eficiente y oportuno apoyo al Oficial de Cumplimiento en el diseño, dirección, supervisión y monitoreo del ptee. K. Asegurar que las actividades que resulten del desarrollo del ptee se encuentran debidamente documentadas, de modo que se permita que la información responda a unos criterios de integridad, confiabilidad, disponibilidad, cumplimiento, efectividad, eficiencia y confidencialidad. Los soportes documentales deberán conservarse de acuerdo con lo previsto en el artículo 28 de la Ley 962 de 2005, o la norma que la modifique o sustituya.

NOMBRAMIENTOS

REPRESENTANTES LEGALES

Por Acta No. 11 del 29 de noviembre de 2013, de Asamblea de

Accionistas, inscrita en esta Cámara de Comercio el 2 de diciembre de 2013 con el No. 01785971 del Libro IX, se designó a:

CARGO	NOMBRE	IDENTIFICACIÓN
Representante Legal	Zulma Dayfeny Urbano Buritica	C.C. No. 25286783

Por Acta No. 041 del 28 de noviembre de 2023, de Asamblea de Accionistas, inscrita en esta Cámara de Comercio el 4 de diciembre de 2023 con el No. 03041662 del Libro IX, se designó a:

CARGO	NOMBRE	IDENTIFICACIÓN
Primer Suplente Del Representante Legal	Diana Carolina Urbano Buritica	C.C. No. 34330933

REVISORES FISCALES

Por Acta No. 033 del 1 de noviembre de 2021, de Asamblea de Accionistas, inscrita en esta Cámara de Comercio el 11 de noviembre de 2021 con el No. 02761756 del Libro IX, se designó a:

CARGO	NOMBRE	IDENTIFICACIÓN
Revisor Fiscal	Cesar Augusto Rodriguez Gomez	C.C. No. 93399429 T.P. No. 140217-t

REFORMAS DE ESTATUTOS

Los estatutos de la sociedad han sido reformados así:

DOCUMENTO	INSCRIPCIÓN
Acta del 29 de agosto de 2009 de la Junta de Socios	01333102 del 9 de octubre de 2009 del Libro IX
Acta No. 7 del 27 de mayo de 2011 de la Asamblea de Accionistas	01487156 del 13 de junio de 2011 del Libro IX
Acta No. 09 del 23 de julio de	01703854 del 6 de febrero de

CERTIFICADO DE EXISTENCIA Y REPRESENTACIÓN LEGAL

Fecha Expedición: 4 de junio de 2026 Hora: 15:00:23
Recibo No. AB26088679
Valor: $ 12,100

CÓDIGO DE VERIFICACIÓN B26088679B0DA4

Verifique el contenido y confiabilidad de este certificado, ingresando a www.ccb.org.co/certificadoselectronicos y digite el respectivo código, para que visualice la imagen generada al momento de su expedición. La verificación se puede realizar de manera ilimitada, durante 60 días calendario contados a partir de la fecha de su expedición.

2012 de la Asamblea de Accionistas	2013 del Libro IX
Acta No. 11 del 29 de noviembre de 2013 de la Asamblea de Accionistas	01785969 del 2 de diciembre de 2013 del Libro IX
Acta No. 012 del 16 de diciembre de 2013 de la Asamblea de Accionistas	01792460 del 23 de diciembre de 2013 del Libro IX
Acta No. 14 del 4 de mayo de 2015 de la Asamblea de Accionistas	01942706 del 26 de mayo de 2015 del Libro IX
Acta No. 0020 del 19 de enero de 2017 de la Asamblea de Accionistas	02178833 del 24 de enero de 2017 del Libro IX
Acta No. 22 del 30 de enero de 2017 de la Asamblea de Accionistas	02220242 del 28 de abril de 2017 del Libro IX
Acta No. 029 del 7 de enero de 2021 de la Asamblea de Accionistas	02658109 del 2 de febrero de 2021 del Libro IX
Acta No. 030 del 1 de febrero de 2021 de la Asamblea de Accionistas	02660831 del 10 de febrero de 2021 del Libro IX
Acta No. 032 del 17 de marzo de 2021 de la Asamblea de Accionistas	02676486 del 24 de marzo de 2021 del Libro IX
Acta No. 036 del 14 de julio de 2022 de la Asamblea de Accionistas	02867424 del 10 de agosto de 2022 del Libro IX
Acta No. 038 del 20 de marzo de 2023 de la Asamblea de Accionistas	02983109 del 2 de junio de 2023 del Libro IX
Acta No. 041 del 28 de noviembre de 2023 de la Asamblea de Accionistas	03041661 del 4 de diciembre de 2023 del Libro IX
Acta No. 046 del 24 de diciembre de 2024 de la Asamblea de Accionistas	03191479 del 26 de diciembre de 2024 del Libro IX
Acta No. 049 del 23 de septiembre de 2025 de la Asamblea de Accionistas	03301112 del 26 de septiembre de 2025 del Libro IX

SITUACIÓN DE CONTROL Y/O GRUPO EMPRESARIAL

Por Documento Privado del 22 de septiembre de 2022 de Representante Legal, inscrito el 22 de septiembre de 2022 bajo el número 02882352 del libro IX, comunicó la sociedad matríz:

- C&L HOLDING S.A.S

Domicilio: Bogotá D.C.
Nacionalidad: Colombiana
Actividad: 6810 - La compra, venta, administración, alquiler

y/o arrendamiento de bienes inmuebles propios o arrendados, tales como: inmuebles residenciales e inmuebles no residenciales e incluso salas de exposiciones, salas cinematográficas, instalaciones para almacenamiento, centros comerciales y terrenos.

Presupuesto: Numeral 1 Artículo 261 del Código de Comercio

Que se ha configurado una situación de control con la sociedad de la referencia.

Fecha de configuración de la situación de control : 2021-02-03

RECURSOS CONTRA LOS ACTOS DE INSCRIPCIÓN

De conformidad con lo establecido en el Código de Procedimiento Administrativo y de lo Contencioso Administrativo y la Ley 962 de 2005, los actos administrativos de registro, quedan en firme dentro de los diez (10) días hábiles siguientes a la fecha de inscripción, siempre que no sean objeto de recursos. Para estos efectos, se informa que para la Cámara de Comercio de Bogotá, los sábados NO son días hábiles.

Una vez interpuestos los recursos, los actos administrativos recurridos quedan en efecto suspensivo, hasta tanto los mismos sean resueltos, conforme lo prevé el artículo 79 del Código de Procedimiento Administrativo y de los Contencioso Administrativo.

A la fecha y hora de expedición de este certificado, NO se encuentra en curso ningún recurso.

CLASIFICACIÓN DE ACTIVIDADES ECONÓMICAS - CIIU

Actividad principal Código CIIU: 6202
Actividad secundaria Código CIIU: 6201
Otras actividades Código CIIU: 6209

TAMAÑO EMPRESARIAL

De conformidad con lo previsto en el artículo 2.2.1.13.2.1 del Decreto 1074 de 2015 y la Resolución 2225 de 2019 del DANE el tamaño

CERTIFICADO DE EXISTENCIA Y REPRESENTACIÓN LEGAL

Fecha Expedición: 4 de junio de 2026 Hora: 15:00:23
Recibo No. AB26088679
Valor: $ 12,100

CÓDIGO DE VERIFICACIÓN B26088679B0DA4

Verifique el contenido y confiabilidad de este certificado, ingresando a www.ccb.org.co/certificadoselectronicos y digite el respectivo código, para que visualice la imagen generada al momento de su expedición. La verificación se puede realizar de manera ilimitada, durante 60 días calendario contados a partir de la fecha de su expedición.

---

de la empresa es Grande

Lo anterior de acuerdo a la información reportada por el matriculado o inscrito en el formulario RUES:

Ingresos por actividad ordinaria $ 156.029.761.000

Actividad económica por la que percibió mayores ingresos en el período - CIIU : 6202

INFORMACIÓN COMPLEMENTARIA

Que, los datos del empresario y/o el establecimiento de comercio han sido puestos a disposición de la Policía Nacional a través de la consulta a la base de datos del RUES.

Los siguientes datos sobre RIT y Planeación son informativos: Contribuyente inscrito en el registro RIT de la Dirección de Impuestos, fecha de inscripción : 11 de noviembre de 2021. Fecha de envío de información a Planeación : 19 de marzo de 2026. \n \n Señor empresario, si su empresa tiene activos inferiores a 30.000 SMLMV y una planta de personal de menos de 200 trabajadores, usted tiene derecho a recibir un descuento en el pago de los parafiscales de 75% en el primer año de constitución de su empresa, de 50% en el segundo año y de 25% en el tercer año. Ley 590 de 2000 y Decreto 525 de 2009. Recuerde ingresar a www.supersociedades.gov.co para verificar si su empresa está obligada a remitir estados financieros. Evite sanciones.

El presente certificado no constituye permiso de funcionamiento en ningún caso.

****

Este certificado refleja la situación jurídica registral de la sociedad, a la fecha y hora de su expedición.

****

Este certificado fue generado electrónicamente con firma digital y cuenta con plena validez jurídica conforme a la Ley 527 de 1999.

CERTIFICADO DE EXISTENCIA Y REPRESENTACIÓN LEGAL

Fecha Expedición: 4 de junio de 2026 Hora: 15:00:23
Recibo No. AB26088679
Valor: $ 12,100

CÓDIGO DE VERIFICACIÓN B26088679B0DA4

Verifique el contenido y confiabilidad de este certificado, ingresando a www.ccb.org.co/certificadoselectronicos y digite el respectivo código, para que visualice la imagen generada al momento de su expedición. La verificación se puede realizar de manera ilimitada, durante 60 días calendario contados a partir de la fecha de su expedición.

****

Firma mecánica de conformidad con el Decreto 2150 de 1995 y la autorización impartida por la Superintendencia de Industria y Comercio, mediante el oficio del 18 de noviembre de 1996.