Alcaldía de
MONTERÍA

SECRETARÍA GENERAL

FICHAS TÉCNICAS

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.

FICHA TÉCNICA DE PRODUCTO
CLASIFICACIÓN DEL BIEN O SERVICIO SEGÚN CLASIFICACIÓN UNSPSC
43222500 – 43222600 – 43233200 – 81111500
DENOMINACIÓN TÉCNICA DEL SERVICIO
SOLUCIONES DE SEGURIDAD PERIMETRAL TIPO FIREWALL DE NUEVA GENERACIÓN
UNIDAD DE MEDIDA
UNIDAD
CALIDAD MÍNIMA Y LOS PATRONES DE DESEMPEÑO MÍNIMOS

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 SFP+ SR con sus respectivos cables de F.O.) 8 interfaces de 1 GE SFP (se deben incluir en la oferta ocho (02) transceivers SFP SR con sus respectivos cables de F.O.) 16 interfaces de 1 GE RJ45 **Funcionalidades generales firewall (Core)** **Capacidades de NAT (Network Address Translation)** Las plataformas deben soportar lo siguientes tipos de traducción de direcciones: NAT y PAT NAT estático NAT: destino, origen NAT, NAT64 persistente **Funciones básicas de Firewall** Las reglas de firewall deben analizar las conexiones que pasen por el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs. La solución debe integrarse con el directorio activo y soportar políticas basadas en identidad. Esto significa que podrán definirse políticas de seguridad de acuerdo con el grupo de pertenencia de los usuarios. Debe tener la capacidad de generar una advertencia al administrador cuando este configure una política duplicada Debe estar en la capacidad de integrase con plataforma Cloud IaaS como: AWS,Azure,Google etc. Con el fin de generar y actualizar objetos de direcciones de manera automática basado en los parámetros de red (IP, TAG, etc) de las instancias desplegadas en la nube y estas ser usadas como objetos de reglas o políticas de firewall Debe soportar reglas de firewall en IPv6 configurables tanto por CLI (Command Line	UNIDAD	4

	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	UNIDAD	1

	Funcionalidades generales firewall (Multigiga) **Capacidades de NAT (Network Address Translation)** Las plataformas deben soportar lo siguientes tipos de traducción de direcciones: NAT y PAT NAT estático NAT: destino, origen NAT, NAT64 persistente **Funciones básicas de Firewall** Las reglas de firewall deben analizar las conexiones que pasen por el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs. La solución debe integrarse con el directorio activo y soportar políticas basadas en identidad. Esto significa que podrán definirse políticas de seguridad de acuerdo con el grupo de pertenencia de los usuarios. Debe tener la capacidad de generar una advertencia al administrador cuando este configure una política duplicada Debe estar en la capacidad de integrase con plataforma Cloud IaaS como: AWS,Azure,Google etc. Con el fin de generar y actualizar objetos de direcciones de manera automática basado en los parámetros de red (IP, TAG, etc) de las instancias desplegadas en la nube y estas ser usadas como objetos de reglas o políticas de firewall Debe soportar reglas de firewall en IPv6 configurables tanto por CLI (Command Line Interfaz) como por GUI (Graphical User Interfaz). La solución tendrá la capacidad de hacer captura de paquetes por política de seguridad implementada para luego ser exportado en formato PCAP. El dispositivo será capaz de crear e integrar políticas contra ataques DoS (Denial of service) las cuales se deben poder aplicar por interfaces. El dispositivo será capaz de ejecutar inspección de tráfico SSL en todos los puertos y seleccionar bajo que certificado será válido este tráfico. Tendrá la capacidad de hacer escaneo a profundidad de tráfico tipo SSH dentro de todos o cierto rango de puertos configurados para este análisis. **Conectividad y enrutamiento** Funcionalidad de DHCP: como Cliente DHCP, Servidor DHCP y reenvío (Relay) de solicitudes DHCP. Soporte de enrutamiento estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas. Soporte a enrutamiento dinámico RIP V1, V2, OSPF y BGP. La solución podrá habilitar políticas de enrutamiento en IPv6. La solución deberá ser capaz de habilitar enrutamiento estático para cada interfaz en IPv6. **VPN IPsec** Los equipos deben soportar las siguientes características: Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site). Soporte para IKEv2 y IKE Configuration Method. Soporte de VPNs con algoritmos de cifrado: AES, DES, 3DES Se debe soportar longitudes de llave para AES de 128, 192 y 256 bits **Autenticación** Los dispositivos deben manejar los siguientes tipos de autenticación: Capacidad de soporta autenticación local y remota integrándose con Servidores de Autenticación RADIUS, LDAP o TACACS+. Capacidad incluida, al integrarse con Microsoft Windows Active Directory o Novell eDirectory, de autenticar transparentemente usuarios sin preguntarles username o password. Esto es aprovechar las credenciales del dominio de Windows bajo un concepto “Single-Sign-On”. Soporte de Token Físicos o Mobile sobre Smartphone basado en IOS o Android, token de SMS, email o con plataformas de terceros como RSA SecurID. Capacidad de soportar autenticación de acceso de usuario a través de 802.1x y portal cautivo. **Manejo de tráfico y calidad de servicio** La solución debe soportar balanceo de enlaces WAN inteligente (SD-WAN Seguro) sin licencia adicional basado en: Aplicaciones cloud, SLA y Mejor calidad de enlace basado en (Jitter, latencia, ancho de banda, perdida de paquetes). Capacidad de poder asignar parámetros de traffic shapping atreves de reglas de manera independiente. Capacidad de poder asignar parámetros de traffic shaping diferenciadas para el tráfico en distintos sentidos de una misma sesión. Capacidad de definir parámetros de traffic shaping que apliquen para cada dirección IP en forma independiente, en contraste con la aplicación y categoría URL de las mismas para la regla en general. Capacidad de poder definir límite de ancho de banda (ancho de banda máximo) en Kilobits por segundo. **Antimalware** Debe ser capaz de analizar, establecer control de acceso y detener ataques y hacer Antivirus en tiempo real en al menos los siguientes protocolos aplicativos: HTTP, SMTP, IMAP, POP3, FTP.MAPI El módulo de antimalware debe haber sido desarrollado por el mismo fabricante de la solución de firewall, así como las firmas deben ser de su propiedad y no por medio de licenciamiento o concesiones de un tercero, esto con el fin de garantizar la idoneidad de la protección, así como los tiempos de respuesta del soporte de la misma. Debe soportar la inspección de archivos comprimidos como los son: GZIP,RAR,LZH,IHA,CAB,ARJ;ZIP entre otros con el fin de proteger contra estas técnicas de evasión. El Antivirus debe integrarse de forma nativa con una solución Sandbox del mismo fabricante, de tal manera que envíen muestras de archivos a dicho dispositivo para su análisis.		

	Filtrado Web Facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías. Por flexibilidad, el filtro de URLs debe tener por lo menos 78 categorías y por lo menos 47 millones de sitios web en la base de datos. Debe poder categorizar contenido Web requerido mediante IPv6. Será posible exceptuar la inspección de HTTPS por categoría. Debe contar con la capacidad de bloquear contenido de YouTube usando el Channel ID El filtrado debe ser sobre tráfico http y https. **Protección contra intrusos (IPS)** El sistema de detección y prevención de intrusos deben poder implementarse tanto en línea como fuera de línea. En línea, el tráfico a ser inspeccionado pasará a través del equipo. Fuera de línea, el equipo recibirá el tráfico a inspeccionar desde un switch con un puerto configurado en span o mirror. Debe ser posible definir políticas de detección y prevención de intrusiones para tráfico IPv6. A través de sensores. Capacidad de detección de más de 7000 ataques. El sistema de detección y prevención de intrusos debe estar integrado a la plataforma de seguridad “appliance”. Sin necesidad de instalar un servidor o appliance externo, La interfaz de administración del sistema de detección y prevención de intrusos deberá de estar perfectamente integrada a la interfaz de administración del dispositivo de seguridad appliance, sin necesidad de integrar otro tipo de consola para poder administrar este servicio. Esta deberá permitir la protección de este servicio por política de control de acceso. Debe ofrecerse la posibilidad de guardar información sobre el paquete de red que detonó la detección del ataque, así como al menos los 5 paquetes sucesivos. Estos paquetes deben poder ser visualizados por una herramienta que soporte el formato PCAP. **Control de aplicaciones** La solución debe soportar la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo. La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico. La solución debe tener un listado de al menos 3000 aplicaciones ya definidas por el fabricante. Para aplicaciones identificadas deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log y resetear conexión **Inspección de Contenido SSL/SSH** La solución debe soportar inspeccionar tráfico que esté siendo encriptado mediante SSL al menos para los siguientes protocolos: HTTP, IMAP, SMTP, POP3 y FTP en su versión segura. Debe ser posible definir perfiles de inspección SSL donde se definan los protocolos a inspeccionar y el certificado usado, estos perfiles deben poder ser escogidos una vez se defina la política de seguridad. La inspección debe realizarse: mediante la técnica conocida como Hombre en el Medio (MITM – Man In The Middle) para una inspección completa o solo inspeccionando el certificado sin necesidad de hacer full inspection. **Alta disponibilidad** El dispositivo deberá soportar Alta Disponibilidad transparente, es decir, sin pérdida de conexiones en caso de que un nodo falle tanto para IPV4 como para IPV6 Alta Disponibilidad en modo Activo-Activo de forma automática sin requerir hacer políticas de enrutamiento basado en orígenes y destino para poder hacer la distribución del tráfico. El equipo debe soportar hasta 2 equipos en esquema de HA. **Visibilidad** La solución debe estar en la capacidad de visualizar el tráfico de usuario, aplicaciones, navegación y niveles de riesgo en tiempo real, esto deberá ser sobre la misma plataforma sin necesidad de software o licenciamiento adicional. Deber tener la capacidad de poder validar con que política la sesión se está coincidiendo y un link hacia la misma. **Características de Administración** Interfaz gráfica de usuario (GUI), vía Web por HTTP y HTTPS para hacer administración de las políticas de seguridad y que forme parte de la arquitectura nativa de la solución para administrar la solución localmente. Por seguridad la interfaz debe soportar SSL sobre HTTP (HTTPS) Soporte de al menos 3 servidores syslog para poder enviar bitácoras a servidores de SYSLOG remotos Debe tener la capacidad de gestionar todas las políticas de seguridad, además de poder gestionar Switches y APs dentro de una única consola de gestión. **Licenciamiento y actualizaciones** El licenciamiento de todas las funcionalidades debe ser ILIMITADO en cuanto a usuarios, conexiones, VPNs equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo. La vigencia de las actualizaciones para los servicios de Antivirus, AntiSpam, IPS, Application Control y URL Filtering debe proveerse por al menos doce (12) meses a partir de su activación en el portal del fabricante. La plataforma es requerida por un periodo de doce (12) meses en un esquema de soporte 7x24 ante el fabricante a partir de su activación en el portal del fabricante. Garantía y licenciamiento de los equipos y software ofertados, con Servicio de soporte 7x24 de 12 meses a partir de su activación en el portal de fabricante, que incluya Soporte Telefónico y repuestos (estos repuestos deberán ser gestionados por el contratista en caso tal de requerirse un en tiempo no mayor a (08) días calendario).		
SUMINISTRO, INSTALACIÓN Y PUESTA EN FUNCIONAMIENTO DE FIREWALL DE SEGURIDAD PERIMETRAL BASICO			1

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 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).	UNIDAD	

	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 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	UNIDAD	13

	Access Point, incluyendo su configuración, monitoreo y la aplicación de políticas de seguridad en el acceso. **Estándares y certificaciones Access Points** Los APs deben soportar al menos los siguientes estándares de la industria: - 802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h, 802.11i,802.11j, 802.11k, 802.11n, 802.11r, 802.11u, 802.11v, 802.11ac, 802.11ax (Wi-Fi 6), 802.1Q, 802.1X, 802.3ad, 802.3af, 802.3at, 802.3az, 802.3bz - WiFi Certified a,b,g,n,ac,ax, passpoint - WAP2, WPA3 - UL2043 - ROHS **Seguridad inalámbrica Access Point** - Algoritmo de cifrado: AES, TLS, EAP, TTLS, TKIP, WPA, WPA2 y WPA3. - La controladora debe incluir un control y filtro de más de 3000 aplicaciones de aplicaciones de uso común, y permita aplicar políticas granulares de seguridad, QoS, control de ancho de banda y filtrado web. El punto de acceso debe soportar encaminamiento de trafico de los clientes Wireless de manera tunelada, garantizando integridad de los datos a través de túneles IPSec. Cuando se tuneliza el tráfico de los clientes inalámbricos hacia la controladora inalámbrica, para garantizar un mejor uso de los recursos, la solución debe permitir una función conocida como Split Tunneling que se configurará en el SSID. Con esta característica, el AP debe soportar la creación de listas de excepción con direcciones de servicio de la red local que no deben enviar los paquetes a través del túnel al concentrador, es decir, todos los paquetes deben ser tunelizados excepto aquellos destinados a direcciones especificadas locales en las listas de excepciones. El punto de acceso debe soportar encaminamiento de trafico de tipo Modo Bridge o conmutación local. En este modo todo el tráfico de los dispositivos conectados en un determinaod SSID deberá ser conmutado localmente en la interfaz ethernet del punto de acceso y no deberán ser tunelados hasta la controladora inalámbrica El punto de acceso deberá soportar mecanismos de identificación y protección de ataques a la infraestructura inalámbrica (WIPS/WIDS). El punto de acceso deberá soportar la funcionalidad de análisis de espectro con un radio exclusivo que monitoree la red 7x24, que permita la identificación de interferencias no Wi-Fi y que operen en las frecuencias de 2.4GHz, 5GHz y 6 GHz Capacidad de manejar roles por usuario y políticas basadas en identidad. Coexistencias Avanzada Celular (Advanced Cellular Coexistence ACC) Radio dedicado para funciones de WIPS/WIDS y analizador de espectro. No se aceptan Access point adicionales para cumplir este requerimiento		
6	**INSTALACIÓN, RENOVACIÓN DE LICENCIA, Y PUESTA EN FUNCIONAMIENTO DE ACCESS POINT** Renovación de soporte y garantía de fabrica por 12 meses a partir de la suscripción del acta de inicio para los siguientes equipos Access Point. El No. Serial de los equipos a renovar son los siguientes: FP231GTF24062110 FP231GTF24018641 FP231GTF24062108 FP231GTF24062109 FP231GTF24018767 FP231GTF24062124 FP231GTF24062117 FP231GTF24062116 El oferente debe garantizar servicio de Soporte Técnico y garantía Premium con Servicio de asistencia técnica continua con cobertura 24/7 ante el fabricante a partir de la suscripción del acta de inicio, atención prioritaria ante incidentes críticos y reemplazo de hardware en caso de fallas (con un máximo de 8 días calendario). Incluye actualizaciones de software y firmware. Los puntos de acceso (APs) deben ser administrables a través de la misma solución de seguridad perimetral tipo firewall (por adquirir) sin requerir licenciamientos adicionales permitiendo así su operatividad, y la extensión del perímetro de seguridad hasta la capa de acceso Wi-Fi. Integrarse de manera nativa con la infraestructura de seguridad perimetral Firewall (por adquirir), de forma que actúen como una extensión lógica del firewall corporativo, permitiendo que éste gestione directamente las funcionalidades de los Access Point, incluyendo su configuración, monitoreo y la aplicación de políticas de seguridad en el acceso.	UNIDAD	**8**
7	**SUMINISTRO, INSTALACIÓN Y PUESTA EN FUNCIONAMIENTO DE SWITCHES DE ACCESO 48 PUERTOS** La solución de switches ofertada debe ser de la misma marca de la solución de acceso inalámbrico y la controladora de red de este proceso de contratación para garantizar el SD-LAN o SD-BRANCH de la Entidad. Los switches deben permitir descargar políticas de seguridad desde el firewall perimetral de la Entidad. Se debe poder administrar Switches, Access Point, SD-BRANCH, SD-WAN y Firewalls desde la misma consola de Administración (No se requieren consolas en la nube, la administración debe ser local). El fabricante debe estar en el cuadrante de lideres de Gartner para soluciones empresariales LAN/WLAN en al menos uno (01) los dos (02) últimos reportes publicados. Debe estar en capacidad de detectar Dispositivos IoT Debe permitir la autenticación y autorización Local RADIUS y TACACS+ Debe soportar SSH Debe soportar DHCP snooping, Dynamic ARP	UNIDAD	9

	Debe soportar una funcionalidad de ahorro de Energía que bajé consumo si no hay tráfico y si llega tráfico hacia el dispositivo conectado se envié un mensaje de encendido (Wake-On-Lan - WOL) Debe soportar IEEE 802.1X (Port Based Network Access Control) MTBF minimo de 10 Años (87600 horas) STP Root Guard, STP (802,1d), RSTP (IEEE 802.1w), MSTP (IEEE 802.1s), RPVST (Rapid per Vlan Spanning Tree) Todas las funcionalidades que soporte el equipo deben estar incluidas y soportadas a perpetuidad. No se acepta funcionalidades por suscripción. Certificaciones: FCC, CE, RCM, VCCI, BSMI, UL, CB, RoHS2 Incluir 24 Transceiver 10GE SFP+ transceiver module, short range 300m LC connector, MMF, 850nm, 0°C to 70°C, for systems with SFP+ slots para todos los switches. **Capacidades específicas para los switches de 48 puertos** Los equipos deben ser Appliances físicos (nuevos en su empaque original y sellados de fabrica) (No se aceptarán equipos remanufacturados y/o reparados y/o reformados). Interfaces Red Totales: 48x GE RJ45 and 4x 10GE SFP+ Puerto de Consola: 1 RJ-45 Tráfico: IPV4/IPV6 Switch Capacity: Mayor o igual a 176 GB Packets Per Second: Mayor o igual a 260 Mpps VLANs: Mayor o igual a 4K Packet Buffers: Mayor o igual a 2 MB Memory: 512 MB ACL: 640		
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 VLANs: Mayor o igual a 4K Packet Buffers: Mayor o igual a 2 MB Memory: 512 MB ACL: 640	UNIDAD	3
	SUMINISTRO, INSTALACIÓN Y PUESTA EN FUNCIONAMIENTO DE SWITCH DE ACCESO MULTIGIGA 24 PUERTOS		
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	UNIDAD	1

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

	Debe posibilitar la visualización y comparación de configuraciones actuales, configuraciones previas y configuraciones antiguas. Debe posibilitar que todos los firewalls sean controlados de manera centralizada utilizando solo un servidor de gestión. Cada servidor de gestión debe ser hospedado en un equipo independiente, no ejecutando función de firewall. La solución debe incluir una herramienta para gestionar centralmente las licencias de todos los aparatos controlados por estaciones de gestión, permitiendo al administrador actualizar licencias en los aparatos a través de esta herramienta. La solución debe permitir la distribución e instalación remota, de manera centralizada, de nuevas versiones de software de los aparatos. Debe ser capaz de generar reportes o presentar comparativos entre dos secciones distintas, resumiendo todos los cambios efectuados. Debe permitir crear flujos de aprobación en la solución de gestión, donde un administrador pueda crear todas las reglas, pero estas mismas solamente sean aplicadas después de la aprobación de otro administrador. Tener "wizard" en la solución de gestión para agregar los dispositivos por interfaz gráfica utilizando IP, login y clave de los mismos. Permitir que las políticas y los objetos ya presentes en los dispositivos sean importados cuando el mismo es agregado a la solución de gestión; Permitir la visualización, a partir de la estación de gestión centralizada, informaciones detalladas de los dispositivos gerenciados, tales como hostname, serial, IP de gestión, licencias, horario de lo sistema y firmware. Tener "wizard" en la solución de gestión para instalación de políticas y configuraciones de los dispositivos. Permitir crear en la solución de gestión templates de configuración de los dispositivos con informaciones de DNS, SNMP, configuraciones de LOG y administración. Permitir crear scripts customizados, que sean ejecutados de forma centralizada en un o más dispositivos gestionados con comandos de CLI de los mismos. Tener histórico de los scripts ejecutados en los dispositivos gestionados pela solución de gestión. Permitir configurar y visualizar balanceo de enlaces en los dispositivos gestionados de forma centralizada. Permitir crear varios paquetes de políticas que serán aplicados/asociados a los dispositivos o grupos de dispositivos. Debe permitir crear reglas de NAT64 y NAT46 de forma centralizada. Permitir la creación de reglas anti DoS de forma centralizada. Permitir la creación de objetos que serán utilizados en las políticas de forma centralizada. Permitir crear a partir de la solución de gestión, VPNs entre los dispositivos gestionados de forma centralizada, incluyendo topología (hub, spoke, dial-up) autenticaciones, claves y métodos de criptografía. Garantía y licenciamiento del equipo y software ofertado, con servicio de soporte 7x24 de 12 meses a partir de su activación en el portal de fabricante, que incluya soporte telefónico y repuestos (estos repuestos deberán ser gestionados por el contratista en caso tal de requerirse un en tiempo no mayor a (08) días calendario).		
PRESTACIÓN DE SERVICIOS			
13	**Generalidades del Servicio:** El oferente debe contemplar en su oferta todos los costos o gastos asociados a la logística (desplazamiento, transporte, parqueaderos, equipos y herramientas de trabajo, refrigerios, entre otros) requerida para que el personal asignado al proyecto pueda cumplir sus funciones. **IMPLEMENTACIÓN:** Se debe dar cumplimento a las etapa del proyecto y entregar implementada y funcionando las soluciones completas, de acuerdo con los requerimientos y políticas establecidas por la entidad. Planeación de cada una de las actividades, validadas en conjunto con la entidad. Configuración y alistamiento del software a la última versión estable aprobada por el fabricante para la plataforma. Afinamiento y estabilización de las plataformas. Pruebas de Servicio de las plataformas. Entrega de las plataformas a satisfacción de la entidad Las actividades de implementación y/o afinamiento de las plataformas deben ser realizadas por personal certificado por el fabricante (se deben presentar las certificaciones del personal previo a la implementación de las plataformas). Se deberán realizar pruebas / muestras de las plataformas donde se evidencie la correcta configuración y afinamiento de cada plataforma. **SOPORTE Y/O MANTENIMIENTO:** El servicio de soporte debe incluir atención de incidentes sobre las plataformas ofertadas. Se debe garantizar soporte y garantía para las plataformas ofertadas en un esquema 7x24 por doce (12) meses a partir de la activación de las plataformas en el portal del fabricante, con soporte remoto o en sitio en caso de requerirse. El oferente debe contar con certificación vigente del Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO/IEC 27001:2022, expedida por un organismo de certificación acreditado en Colombia. La certificación debe estar vigente a la fecha de cierre del proceso y cubrir los servicios asociados a la solución ofertada. El oferente debe contar con certificación vigente del Sistema de Gestión de Servicios de TI conforme a la norma ISO/IEC 20000-1:2018, expedida por un organismo de certificación acreditado en Colombia. La certificación debe estar vigente a la fecha de cierre del proceso y cubrir la prestación y gestión de los servicios de tecnología de la información relacionados con la solución ofertada. Realizar y documentar entre otras, las siguientes actividades previa coordinación con		

el supervisor del contrato en desarrollo:
Configurar los reportes / logs de las plataformas.
Mantener actualizados los niveles de Firmware de los componentes ofertados de acuerdo con las últimas versiones estables liberadas por el fabricante.
El horario de atención para el mantenimiento correctivo y preventivo debe ser de 7x24, sin costo adicional para la entidad.
Se deben incluir en la oferta dos (02) actividades de mantenimiento preventivo y afinamiento con el fin de minimizar problemas y mantener los sistemas actualizados, estas actividades deberán ser con previa aprobación del responsable TI de la entidad.
Al finalizar cada visita correctiva y/o preventiva el contratista deberá:
Generar un informe de servicio en el que se realice un resumen de las actividades realizadas (actualización, soporte y mantenimiento), problemas presentados, soluciones utilizadas y recomendaciones.
Consignar en la misma acta o informe de servicio si hubo cambio de software y/o en la configuración.
El soporte deberá contemplar:

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

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.		

Katia CB. Firmado digitalmente por KATYA CABRALES BECHARA

KATIA CABRALES BECHARA
SECRETARIA GENERAL
MUNICIPIO DE MONTERÍA

Proyectó: Luis Miguel Tarrá- Profesional Universitario TIC - SGM Firmado digitalmente por Luis Miguel Tarra Lozano

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

Proyectó jurídicamente: Gabriel Corrales Daza – Contratista SGM