

	MUNICIPIO DE CANDELARIA COMUNICACIONES OFICIALES	Código: 54-PGQ-FT-55
		Fecha: 17-Diciembre-2024
		Versión: 8
		Página 1 de 1

250.10.01

AVISO DE SOLICITUD A PRESENTAR COTIZACIÓN

El Municipio de Candelaria a través de la SECRETARÍA DE SEGURIDAD Y CONVIVENCIA, se encuentra interesada en conocer las actuales condiciones económicas de mercado que a la fecha existen de para ADQUISICIÓN DE ANTENAS STARLINK MINI Y SERVICIO DE INTERNET SATELITAL PARA LAS UNIDADES DEL EJERCITO NACIONAL, para lo cual invita a todos los interesados que se encuentran habilitados para la comercialización de este tipo de bienes a cotizar el valor unitario de cada uno de los ítems establecidos en la ficha técnica, que se presenta como archivo anexo del presente documento.

La ficha técnica ha sido elaborada de acuerdo con las especificaciones exigidas por el Ejército Nacional y se encuentran detalladas en el documento anexo.

La presentación de la respectiva cotización es un insumo de carácter informativo para la entidad territorial con el fin de presentar precios ajustados a la realidad de las necesidades de la entidad territorial y, por lo tanto, no genera obligación alguna con los particulares que decidan presentarla.

Es importante que para la estimación del valor total de la cotización deban tener en cuenta impuestos, tasas, contribuciones y/o retenciones e IVA que apliquen a la correspondiente presentación, así como los gastos asociados que considere necesarios para su operación.


EBERTO RIVEROS RINCÓN
 Secretario de Seguridad y Convivencia

Gestión Documental
Original Destinatario
Copia Archivo

	Nombre	Cargo	Firma
Proyectó	Paola Andrea Manrique Caicedo	Profesional Especializada	
Elaboró	Paola Andrea Manrique Caicedo	Profesional Especializada	
Revisó	Eberto Riveros Rincón	Secretario de Seguridad y Convivencia	
Aprobó	Eberto Riveros Rincón	Secretario de Seguridad y Convivencia	
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes, por lo tanto, bajo nuestra responsabilidad lo presentamos para firma.			



MUNICIPIO DE CANDELARIA
COMUNICACIONES OFICIALES

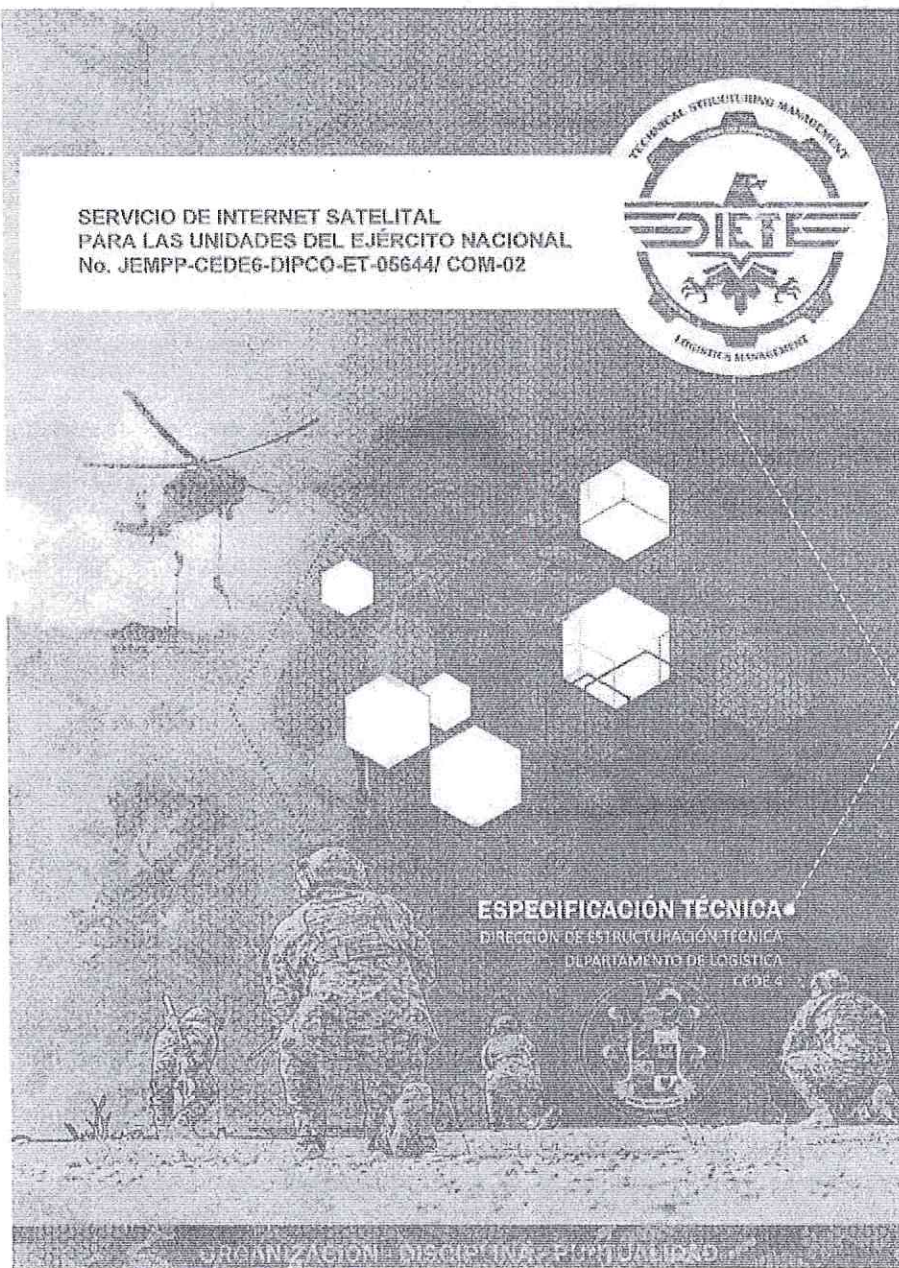
Código: 54-PGQ-FT-55

Fecha: 17-Diciembre-2024

Versión: 8

Página 1 de 1

SERVICIO DE INTERNET SATELITAL
PARA LAS UNIDADES DEL EJÉRCITO NACIONAL
No. JEMPP-CEDE6-DIPCO-ET-05644/ COM-02



ESPECIFICACIÓN TÉCNICA

DIRECCIÓN DE ESTRUCTURACIÓN TÉCNICA
DEPARTAMENTO DE LOGÍSTICA
CEDE 6



ORGANIZACIÓN DISCIPLINADA PORTUGUESA



MUNICIPIO DE CANDELARIA
COMUNICACIONES OFICIALES

Código: 54-PGQ-FT-55

Fecha: 17-Diciembre-2024

Versión: 8

Página 1 de 1

3.1. REQUISITOS GENERALES

No.	REQUISITO
1	Se deberá suministrar el hardware y/o el servicio, para brindar servicios de internet satelital a las unidades del Ejército Nacional.
2	Todos los servicios de internet satelital para las unidades del ejército nacional deben ser nuevos. No se debe hacer reutilización de ningún material.
3	Se deberá tener en cuenta que esta especificación técnica está estructurada para satisfacer las necesidades de una infraestructura catalogada como "Infraestructura Critica".
4	Se deberá configurar y entregar en completo funcionamiento los bienes y servicios adquiridos; todas las actividades adicionales, deberán ser cubiertas y soportadas sin generar costos adicionales para el Ejército Nacional.
5	HOMOLOGACIÓN DE EQUIPOS PARA IPV6 POR MEDIO LACNIC. A fin de asegurar la comunicación de los servicios informáticos del Ejército Nacional por medio del protocolo IPV6, los equipos deben ser compatibles y permitir la comunicación en Dual Stack.

3.2 REQUISITOS ESPECÍFICOS

ITEM	ESPECIFICACIÓN
ITEM 1	KIT MINI
1	Debe estar compuesto por los siguientes elementos así: • Antena • Base • Adaptador de tubo y soporte plano • Fuente de alimentación • Cable de alimentación (corriente continua) de 15 metros
2	ANTENA Antena: matriz de fase electrónica Router: integrado a la antena Campo de visión: 110 ° Orientación: manual asistida por software Clasificación ambiental: IP67 Tipo 4 Temperatura de funcionamiento: -30 °C a 50 °C (-22 °F a 122 °F) Capacidad para derretir nieve: hasta 25 mm/hora (1 pulg./hora) Consumo de energía: promedio 25-40 W Clasificación de entrada: 12 a 48 V, 60 W Tecnología wifi: 802.11a/b/g/n/ac Generación: wifi 5 Radio: banda dual 3 x 3 MU-MIMO Puertos Ethernet: un (1) puerto LAN Ethernet Cobertura wifi: hasta 112 m² (1200 pies²) Seguridad: WPA2 Compatibilidad de malla: compatible con todos los sistemas de malla Starlink. Dispositivos: deberá permitir conectar hasta 128 dispositivos
3	FUENTE DE ALIMENTACIÓN Calificación ambiental: IP66 Tipo 4 Temperatura de funcionamiento: -30°C a 50°C (-22°F a 122°F) Especificaciones de potencia: 100-240V – 1,6A 50 a 60Hz

ITEM 4	SERVICIO DE INTERNET
1	Se deberá suministrar el SERVICIO DE INTERNET SATELITAL de alta velocidad, con tarifas basadas en una facturación mensual, ajustada al plan elegido y en consonancia con los requerimientos específicos de consumo de datos de las unidades militares. Así mismo debe garantizar una conectividad de navegación a una velocidad mínima de carga de 10 Mbps y descarga de 100 Mbps dentro de la capacidad del plan activado, una vez consumida la capacidad de navegación deberá pasar a internet ilimitado con velocidades de descarga de hasta 1Mb/s y de carga de 0,5 Mb/s, con cobertura en todo el territorio nacional, cobertura en territorio continental (incluidos lagos y ríos); no para uso global o en altamar.
4	Plan fijo datos ilimitados



MUNICIPIO DE CANDELARIA
COMUNICACIONES OFICIALES

Código: 54-PGQ-FT-55

Fecha: 17-Diciembre-2024

Versión: 8

Página 1 de 1

ITEM 5	SOLUCIÓN DE COMUNICACIÓN PARA SEGURIDAD Y CONTROL
1	INTERCONEXIÓN: Los equipos deberán estar interconectados física y lógicamente con la red de datos de área local del Ejército Nacional por medio de canales Ethernet, los cuales se deben integrar de forma óptima y deberá garantizar el completo enrutamiento entre las redes LAN de los sitios remotos y las diferentes VLANs que las componen, integrando totalmente la WAN del Ejército.
2	SEDES REMOTAS • Capacidad de ancho de banda bidireccional: 500Mbps • Conexiones simultáneas: 250Kbps • Optimización WAN: 200Mbps Número de interfaces: 4 RJ45
3	SEDE CENTRAL Capacidad de ancho de banda bidireccional: 5Gbps Conexiones simultáneas: 2Mbps Optimización WAN: 1Gbps Número de interfaces: 8 RJ45 + 4 1Gbps/10Gbps
4	La solución debe contar con la opción de virtualizar el CPE SD-WAN (equipos ofertados según la descripción de la solución) sobre alguno de los siguientes hipervisores: vmware, hyper-v, xenserver o KVM (Kernel-based Virtual Machine).
5	La solución debe contar con la opción de virtualizar el appliance CPE SD-WAN sobre al menos 3 proveedores de nube pública (AWS (amazon web services), Azure, GCP, y OCI) Sacando ventaja de todas las características que ofrece la solución de SD-WAN hacia la infraestructura como servicio contratado y debe poder ser desplegada desde el gestor centralizado.
6	Aseguramiento del mejor path para consumo con avanzada medidas del estado y rendimiento de la red y resolución de DNS Local hacia los servicios ofimáticos con los que cuenta la fuerza.
7	Con el objetivo de soportar la conectividad hacia los servicios ofimáticos con los que cuenta la fuerza, la solución debe detectar la aplicación al primer paquete de ingreso al SD-WAN CPE.
8	La solución debe contar con integración CLOUD hacia Transit Gateway AWS.
9	La solución debe contar con integración CLOUD hacia los servicios



MUNICIPIO DE CANDELARIA
COMUNICACIONES OFICIALES

Código: 54-PGQ-FT-55

Fecha: 17-Diciembre-2024

Versión: 8

Página 1 de 1

	ofimáticos con los que cuenta la fuerza
10	Por medio del software de administración centralizado, la solución debe permitir la Optimización SaaS.
11	El software de administración centralizado debe brindar actualizaciones diarias automatizadas con las últimas definiciones de aplicaciones e información de IP a los dispositivos SD-WAN, lo que permite que las sucursales siempre envíen tráfico al destino SAAS de forma óptima.
12	La solución debe tener la capacidad de monitorear el performance hacia las aplicaciones SaaS basados en jitter, latencia, loss y Mos con el fin de detectar cual es el mejor enlace o path antes de realizar cualquier envío de tráfico.
13	La solución debe contar con actualizaciones diarias de aplicaciones y actualización de la tabla de direccionamiento permitiendo visibilidad y steering inteligente.
14	La solución debe estar en la capacidad de reconocer mínimo 10000 aplicaciones, debe utilizar algoritmos de machine learning para identificación de estas.
15	La solución debe tener visibilidad y control de la aplicación desde el primer paquete enviado con el fin de clasificar el paquete de forma rápida y óptima.
16	La identificación de aplicaciones debe ser lo suficientemente robusta y flexible hasta tal punto de determinar si el paquete cuenta con los siguientes TAGs: Dominio, DSCP (Punto de Código de Servicios Diferenciados), segmento IP, Puerto.
17	Cada dispositivo SD-WAN debe soportar enrutamiento de tráfico por aplicativo basado en políticas eligiendo la mejor ruta en todo momento de acuerdo a varios KPIs medidos extremo-extremo, aplicando políticas de seguridad y calidad de servicio.
18	Los equipos CPE (Customer Premises Equipment) SD-WAN y vCPE (Virtual Customer Premises Equipment) SD-WAN debe permitir la creación de túneles IPSEC (Protocolo de Seguridad de Internet), Túneles GRE (Generic Routing Encapsulation), Túneles UDP (Protocolo de Datagramas de Usuario), VRRP (Protocolo de Redundancia de Enrutador Virtual), WCCP (Web Cache Communication Protocol).
19	Cada dispositivo CPE o vCPE debe soportar balanceo de tráfico por segmentos por diferentes canales a nivel WAN (Internet, MPLS o banda ancha, etc).
20	Cada dispositivo CPE o vCPE debe soportar balanceo de tráfico por aplicativo por diferentes canales a nivel WAN diferentes (Internet, MPLS, banda ancha, etc).
21	La solución debe proporcionar distintas opciones de balanceo entre los



MUNICIPIO DE CANDELARIA
COMUNICACIONES OFICIALES

Código: 54-PGQ-FT-55

Fecha: 17-Diciembre-2024

Versión: 8

Página 1 de 1

	transportes utilizados en la arquitectura: Balanceo por calidad del transporte Por latencia Por Jitter Por Loss Balanceo por capacidad local Balanceo por capacidad local y remota
22	La solución debe poder customizar los tipos de balanceo por calidad del transporte y por BW disponible de los transportes Local, exclusión de transportes por fallas en el underlay u overlay y configuración del tiempo de espera a nivel de FEC.
23	La solución debe poder garantizar que un grupo de aplicaciones utilice un tipo de transporte específico y se conmute hacia otro transporte en caso de no cumplir con los KPIs de la aplicación a nivel de Jitter, Loss, Latencia entre los extremos de fábrica o hacia Internet (internet secure breakout). Para otro grupo de aplicaciones, la solución debe poder garantizar que se utilice otro tipo de transporte como principal y que conmute el tráfico en caso de no cumplir con los KPIs de la aplicación a nivel de Jitter, Loss, Latencia entre los extremos del fabricante o hacia internet (internet secure breakout).
24	Cada dispositivo SD-WAN deben poder interconectarse simultáneamente con sitios de sedes no SD-WAN estableciendo protocolos de enrutamiento dinámico fuera de la nube SD-WAN.
25	La solución debe poder detectar tráfico y enviarlo hacia internet para consumo de tráfico SaaS y WEB de acuerdo a políticas configuradas (Intelligent Local Breakout)
26	La solución debe tener la capacidad de manejar los siguientes tipos de redundancia a nivel WAN sin la necesidad de incluir dispositivos adicionales. - Activo/Activo (por segmentos o por aplicaciones) - Activo / Stand By (por segmentos o por aplicaciones) - Load balance
27	La solución debe tener la capacidad de conmutar el tráfico entre canales a nivel WAN de acuerdo con los siguientes criterios de disponibilidad del canal sobre la nube de SD-WAN. Canal Down Loss Latencia Jitter KPIs de Loss, latencia y Jitter deben poder especificarse con valores de



MUNICIPIO DE CANDELARIA
COMUNICACIONES OFICIALES

Código: 54-PGQ-FT-55

Fecha: 17-Diciembre-2024

Versión: 8

Página 1 de 1

	acuerdo con el caso de uso del cliente, es decir, no es posible tener una solución con valores ya prediseñados de fábrica que no se pueda modificar.
28	La solución ofertada debe tener la capacidad de tener opciones de topologías regionales en Mesh o regionales para hub and Spoke con el fin de reducir sobre procesamiento en el establecimiento de túneles full Mesh por grupo de aplicaciones y para manejo de tráfico de forma diferente por cada región (topología, transporte, KPIs de medición, tipo de balanceo) la comunicación entre las regiones debe ser viables a través de los HUB sobre cada una de ellas. Las topologías deben ser definidas por software.
29	Los equipos de la solución (físicos y virtuales) debe ser compatibles con protocolos estándar de recopilación de datos como Netflow y/o homólogos.
30	Appliance CPE SD-WAN debe soportar los siguientes servicios adicionales: DHCP (Protocolo de Configuración Dinámica de Host), NAT (Traducción de Direcciones de Red), NTP (Protocolo de Tiempo de Red), PPPoE (Protocolo Punto a Punto sobre Ethernet), autodescubrimiento de MTU (Unidad de Transmisión Máxima) para formación de túneles.
31	La solución debe soportar políticas de corrección adaptativa. La relación entre los paquetes de paridad para recuperación automática debe estar asociado a las mediciones dinámicas sobre la red (FEC adaptativo) sin sacrificar alguna característica de performance sobre el equipo SD-WAN.
32	La solución debe tener la capacidad modificar el parámetro FEC de acuerdo con las necesidades del negocio por conjunto de aplicaciones; dentro de las opciones mandatarias se debe definir lo siguiente: - FEC estático - FEC adaptativo - Sin FEC
33	La solución SD-WAN debe soportar el agrupamiento lógico de canales WAN en un solo túnel o bonding y llevar a cabo balanceo de carga por paquete. Esta agregación de canales debe ser soportada, aunque los enlaces WAN tengan anchos de banda diferentes
34	La solución debe monitorear continuamente el estado de los túneles, así como la medición de los parámetros de delay, jitter, packetloss para toma de decisiones de enrutamiento inteligente del tráfico o flujos.
35	La solución debe monitorear continuamente el estado de los túneles a nivel de MOS (Mean Opinion Score)
36	Los dispositivos CPE SD-WAN deben seguir funcionando a nivel de flujo de tráfico incluso si se pierde la conectividad con el sistema de gestión o



MUNICIPIO DE CANDELARIA
COMUNICACIONES OFICIALES

Código: 54-PGQ-FT-55

Fecha: 17-Diciembre-2024

Versión: 8

Página 1 de 1

	capa de control.
37	La solución debe tener la capacidad de re-ordenar los paquetes que están fuera de orden antes de entrega al destino final.
38	Cpe SD-WAN y vcpe SD-WAN deben contar y ser compatibles con protocolos estándar de QoS (Shaping - Rate Limit - queuing) para delimitar tráfico de ingreso o egreso de acuerdo con el flujo de conectividad por segmento o aplicativo
39	La solución debe garantizar un BW mínimo o BW máximo de acuerdo con el flujo u overlay.
40	El QoS debe tener la capacidad de asignarlo a los flujos de tráfico identificados y/o overlays.
41	La solución SD-WAN debe respetar la marcación de QoS presentes, la solución debe proporcionar soporte nativo para QoS avanzada, incluida la lógica de clasificación sofisticada, una variedad de técnicas de marcación de paquetes, y el encolamiento y el modelaje de tráfico.
42	Los equipos CPE SD-WAN tipo appliance deben permitir su aprovisionamiento ZTP (Zero Touch Provisioning). No se debe requerir configuraciones previas sobre ellos para desplegarla solución. Es mandatorio que el ZTP se despliegue desde la misma consola de administración centralizada, en esta misma consola se debe garantizar reportería, analítica avanzada, aceleración, troubleshooting, orquestación y automatización).
43	La solución debe tener la capacidad de desplegar configuraciones de forma centralizada mediante plantillas o templates para todas las funcionalidades descritas en este documento.
44	El orquestador debe ofrecer soporte de IP SLA y, con base en violación de los umbrales definidos, soportar varias acciones como: habilitar túnel, deshabilitar túnel, anunciar rutas, modificar una métrica la métrica, cambiar prioridad de VRRP y generar alarmas.
45	La solución debe suministra seguridad tanto en la capa de datos como en la capa de control entre la conexión del CPE SD-WAN y el sistema de gestión u orquestación.
46	Cada Overlay (cifrado de red) debe ser protegido a través de túneles encriptados AES de 256 bits.
47	Los túneles a nivel de underlay deben ser construidos por default por el protocolo IPSEC UDP entre los CPEs dentro del fabrica SD-WAN.
48	La solución debe garantizar segmentación de red end-to-end por intermedio de instancias virtuales
49	La solución debe soportar 2000 VRFs, los cuales deben ser orquestadas centralmente. Cada dispositivo debe soportar al menos 64 instancias virtuales o Vrf's.



MUNICIPIO DE CANDELARIA
COMUNICACIONES OFICIALES

Código: 54-PGQ-FT-55

Fecha: 17-Diciembre-2024

Versión: 8

Página 1 de 1

50	La solución debe soportar encriptación de disco AES de 128 bits para propósito de duplicación.
51	Statefull Firewall, Antispoofing, Attack detection & protection, Secure syslog
52	IPS/IDS
53	DDoS detection and prevention
54	Best-of-Breed SASE integration
55	La solución de SD-WAN debe poder integrarse hacia SPLUNK para fines de análisis de seguridad.
56	Mitigación de inundaciones
57	Encriptación de data sensible: IPsec, IPsec Suite B, IKEv1/v2 (múltiples opciones de SHA & AES)
58	OAuth/SAML SSO debe contar con inicio de sesión único OAuth/SAML SSO.
59	El controlador sso debe realizar la integración entre Sisense y la plataforma de inicio de sesión del usuario determinado.
60	Debe cumplir con la validación del hardware criptográfico.
61	El sistema de gestión debe ser una plataforma única, que pueda realizar la administración de todos los dispositivos de la solución a nivel de SDN y gestión de todas las funcionalidades descritas en este documento en nube o premisas sin la necesidad de ejecutar comandos vía CLI para activación de alguna funcionalidad, es decir en un mismo gestor se debe asegurar: Orquestación, automatización, analítica avanzada, Optimización y aceleración, ZTP, reportería, administración, monitoreo, eventos y troubleshooting)
62	La plataforma de gestión /orquestación debe poder ser desplegada de forma flexible: instalada en nube pública, SaaS, nube privada o premisas del cliente final.
63	La plataforma de gestión / orquestación debe contar con administración de dispositivos basado en roles RBAC (Control de Acceso Basado en Roles).
64	Plataforma debe contar con interfaz web (GUI) para la administración de los dispositivos, actualizaciones remotas, y configuración masiva mediante templates o scripts que permita la configuración de equipos sobre todas las funcionalidades indicadas en el documento.
65	La plataforma de gestión y/o orquestación debe permitir integración con API's hacia sistemas o equipos de terceros
66	La plataforma de administración debe tener implementado una herramienta de medición de ancho de banda end-to-end de los canales. Monitoreo de red centralizado, visibilidad global y configuración de políticas centralizadas.
67	La plataforma de gestión debe administrar toda la solución de SD-WAN



MUNICIPIO DE CANDELARIA
COMUNICACIONES OFICIALES

Código: 54-PGQ-FT-55

Fecha: 17-Diciembre-2024

Versión: 8

Página 1 de 1

	(orquestración, automatización, analítica avanzada, optimización y aceleración, ZTP, reportería, administración, monitoreo, eventos y troubleshooting), debe poder diferenciar la capa de Underlay y la capa Overlay a nivel de Loss, latencia, Jitter, MOS y topologías).
68	La plataforma de gestión debe contar con la capacidad de debe permitir la realización de backup de la configuración del orquestador y de los gateways que conforman la plataforma SD-WAN.
69	La plataforma de gestión debe visualizar a nivel real e históricos las principales aplicaciones en uso.
70	La plataforma de gestión debe visualizar a nivel real e históricos: consumo de ancho de banda por aplicativo.
71	La plataforma de gestión debe visualizar a nivel real e históricos: utilización de ancho de banda: presentar la cantidad total de ancho de banda que está siendo utilizada tanto para tráfico optimizado como el no optimizado.
72	La plataforma de gestión debe visualizar a nivel real e históricos: Desempeño de red. A nivel de paquetes por segundo del desempeño que está siendo alcanzado a nivel de WAN para tráfico optimizado y no optimizado.
73	La plataforma de gestión debe visualizar a nivel real e históricos: Conteo de flujos. Seguimiento del número de flujos generados a través de la WAN para tráfico optimizado y no optimizado.
74	La plataforma de gestión debe visualizar a nivel real e históricos: Latencia: componentes de la solución con mayor latencia.
75	La plataforma de gestión debe visualizar a nivel real e históricos: • Pérdida de paquetes. • Medición de la pérdida máxima de paquetes como un conjunto y como conexiones WAN individuales.
76	La plataforma de gestión debe estar en la capacidad de generar reportes programados y a demanda.
77	Los reportes deben poder ser extraídos desde la plataforma de gestión
78	Se debe monitorear la corrección de errores (FEC) extremo - extremo dentro del fabric SD-WAN.
79	La solución debe proveer mecanismos de aceleración en las aplicaciones detectadas que mitigue la latencia de los enlaces, disminución de requerimientos de ancho de banda en la red y que mejore los tiempos de respuestas a estas sin necesidad de desplegar "service Chaining".
80	Técnicas de reducción de datos que incluyen mecanismos de compresión y de duplicación de datos para reducir la cantidad de datos que atraviesan enlaces WAN.

	MUNICIPIO DE CANDELARIA COMUNICACIONES OFICIALES	Código: 54-PGQ-FT-55
		Fecha: 17-Diciembre-2024
		Versión: 8
		Página 1 de 1

81	La solución SD-WAN debe inspeccionar el tráfico que se envía entre clientes y servidores, almacenando información localmente en los dispositivos SD-WAN. técnicas avanzadas de detección de patrones repetitivos, lo que minimiza la interacción a través de la WAN para mejorar el rendimiento de las aplicaciones y maximizar la utilización de la WAN.
82	La solución SD-WAN debe utilizar la fusión de paquetes para agrupar varios paquetes más pequeños en un solo paquete más grande (Paquet Coalescing).
83	La solución debe proveer mecanismos de compresión y de duplicación que elimina la transmisión de datos repetitivo sobre los enlaces WAN. Esta puede ser aplicada para todos los protocolos basados en IP incluyendo TCP (Protocolo de Control de Transmisión) y UDP (Protocolo de Datagramas de Usuario).
84	La solución debe proveer mecanismos que asegure la aceleración a nivel de TCP: Window Scaling Selective Ack Round Trip Time Measurement
85	Los equipos SD-WAN deben estar en la capacidad de soportar en la misma caja funcionalidades de aceleración sin la necesidad de hacer un upgrade/ adición de hardware.
86	El mismo sistema de gestión / orquestación debe tener la capacidad de orquestar, administrar y monitorear funcionalidades de aceleración sin la necesidad de contar con otro sistema de gestión diferente. Es mandatorio que el gestor sea el mismo para reportes, analítica, troubleshooting, automatización, centralización de políticas, visibilidad.

Numeral 3.5 REQUISITOS DE EMPAQUE Y ROTULADO.

3.5.1. Empaque

La antena, modem y accesorios deberán estar perfectamente empacados con el fin que se puedan transportar a todos los sitios que se requieran. Además, los elementos deberán estar almacenados en una caja robusta para que brinde seguridad y conservación de los elementos en el transporte.

3.5.2. Rotulado

Los elementos deberán contar con su debida marcación con serial o número de identificación, número de contrato y proveedor, a fin de establecer en caso de fallas a donde se debe tomar contacto.

4. TOMA DE MUESTRAS Y CRITERIO DE ACEPTACIÓN O RECHAZO:

4.1. TOMA DE MUESTRAS Y CRITERIO DE ACEPTACIÓN O RECHAZO PARA EVALUAR LOS REQUISITOS ESPECÍFICOS GENERALES Y REQUISITOS DE EMPAQUE Y ROTULADO

4.1.1. Muestreo

Se realizará la comprobación del ancho de banda en cuanto a descarga de datos mediante aplicación de testeo de velocidad.

FICHA TÉCNICA

SERVICIO DE INTERNET SATELITAL
PARA LAS UNIDADES DEL EJÉRCITO NACIONAL
No. JEMPP-CEDE6-DIPCO-ET-05644/ COM-02



ESPECIFICACIÓN TÉCNICA

DIRECCIÓN DE ESTRUCTURACIÓN TÉCNICA
DEPARTAMENTO DE LOGÍSTICA
CEDE 4



ORGANIZACIÓN DISCIPLINA PLURALIDAD

3.1. REQUISITOS GENERALES

No.	REQUISITO
1	Se deberá suministrar el hardware y/o el servicio, para brindar servicios de internet satelital a las unidades del Ejército Nacional.
2	Todos los servicios de internet satelital para las unidades del ejército nacional deben ser nuevos. No se debe hacer reutilización de ningún material.
3	Se deberá tener en cuenta que esta especificación técnica está estructurada para satisfacer las necesidades de una infraestructura catalogada como "Infraestructura Crítica".
4	Se deberá configurar y entregar en completo funcionamiento los bienes y servicios adquiridos; todas las actividades adicionales, deberán ser cubiertas y soportadas sin generar costos adicionales para el Ejército Nacional.
5	HOMOLOGACIÓN DE EQUIPOS PARA IPV6 POR MEDIO LACNIC. A fin de asegurar la comunicación de los servicios informáticos del Ejército Nacional por medio del protocolo IPV6, los equipos deben ser compatibles y permitir la comunicación en Dual Stack.

3.2 REQUISITOS ESPECÍFICOS

ÍTEM	ESPECIFICACIÓN
ITEM 1	KIT MINI
1	Debe estar compuesto por los siguientes elementos así: • Antena • Base • Adaptador de tubo y soporte plano • Fuente de alimentación • Cable de alimentación (corriente continua) de 15 metros
2	ANTENA Antena: matriz de fase electrónica Router: integrado a la antena Campo de visión: 110 ° Orientación: manual asistida por software Clasificación ambiental: IP67 Tipo 4 Temperatura de funcionamiento: -30 °C a 50 °C (-22 °F a 122 °F) Capacidad para derretir nieve: hasta 25 mm/hora (1 pulg./hora) Consumo de energía: promedio 25-40 W Clasificación de entrada: 12 a 48 V, 60 W Tecnología wifi: 802.11a/b/g/n/ac Generación: wifi 5 Radio: banda dual 3 x 3 MU-MIMO Puertos Ethernet: un (1) puerto LAN Ethernet Cobertura wifi: hasta 112 m² (1200 pies²) Seguridad: WPA2 Compatibilidad de malla: compatible con todos los sistemas de malla Starlink. Dispositivos: deberá permitir conectar hasta 128 dispositivos
3	FUENTE DE ALIMENTACIÓN Calificación ambiental: IP66 Tipo 4 Temperatura de funcionamiento: -30°C a 50°C (-22°F a 122°F) Especificaciones de potencia: 100-240V – 1,6A 50 a 60Hz

ITEM 4	SERVICIO DE INTERNET
1	Se deberá suministrar el SERVICIO DE INTERNET SATELITAL de alta velocidad, con tarifas basadas en una facturación mensual, ajustada al plan elegido y en consonancia con los requerimientos específicos de consumo de datos de las unidades militares. Así mismo debe garantizar una conectividad de navegación a una velocidad mínima de carga de 10 Mbps y descarga de 100 Mbps dentro de la capacidad del plan activado, una vez consumida la capacidad de navegación deberá pasar a internet ilimitado con velocidades de descarga de hasta 1Mb/s y de carga de 0,5 Mb/s, con cobertura en todo el territorio nacional. cobertura en territorio continental (incluidos lagos y ríos); no para uso global o en altamar.
4	Plan fijo datos ilimitados

ITEM 5	SOLUCIÓN DE COMUNICACIÓN PARA SEGURIDAD Y CONTROL
1	INTERCONEXIÓN: Los equipos deberán estar interconectados física y lógicamente con la red de datos de área local del Ejército Nacional por medio de canales Ethernet, los cuales se deben integrar de forma óptima y deberá garantizar el completo enrutamiento entre las redes LAN de los sitios remotos y las diferentes VLANs que las componen, integrando totalmente la WAN del Ejército.
2	SEDES REMOTAS • Capacidad de ancho de banda bidireccional: 500Mbps • Conexiones simultáneas: 250Kbps • Optimización WAN: 200Mbps Número de interfaces: 4 RJ45
3	SEDE CENTRAL Capacidad de ancho de banda bidireccional: 5Gbps Conexiones simultáneas: 2Mbps Optimización WAN: 1Gbps Número de interfaces: 8 RJ45 + 4 1Gbps/10Gbps
4	La solución debe contar con la opción de virtualizar el CPE SD-WAN (equipos ofertados según la descripción de la solución) sobre alguno de los siguientes hypervisores: vmware, hyper-v, xenserver o KVM (Kernel-based Virtual Machine).
5	La solución debe contar con la opción de virtualizar el appliance CPE SD-WAN sobre al menos 3 proveedores de nube pública (AWS (amazon web services), Azure, GCP, y OCI) Sacando ventaja de todas las características que ofrece la solución de SD-WAN hacia la infraestructura como servicio contratado y debe poder ser desplegada desde el gestor centralizado.
6	Aseguramiento del mejor path para consumo con avanzada medidas del estado y rendimiento de la red y resolución de DNS Local hacia los servicios ofimáticos con los que cuenta la fuerza.
7	Con el objetivo de soportar la conectividad hacia los servicios ofimáticos con los que cuenta la fuerza, la solución debe detectar la aplicación al primer paquete de ingreso al SD-WAN CPE.
8	La solución debe contar con integración CLOUD hacia Transit Gateway AWS.
9	La solución debe contar con integración CLOUD hacia los servicios

	ofimáticos con los que cuenta la fuerza
10	Por medio del software de administración centralizado, la solución debe permitir la Optimización SaaS.
11	El software de administración centralizado debe brindar actualizaciones diarias automatizadas con las últimas definiciones de aplicaciones e información de IP a los dispositivos SD-WAN, lo que permite que las sucursales siempre envíen tráfico al destino SAAS de forma óptima.
12	La solución debe tener la capacidad de monitorear el performance hacia las aplicaciones SaaS basados en jitter, latencia, loss y Mos con el fin de detectar cual es el mejor enlace o path antes de realizar cualquier envío de tráfico.
13	La solución debe contar con actualizaciones diarias de aplicaciones y actualización de la tabla de direccionamiento permitiendo visibilidad y steering inteligente.
14	La solución debe estar en la capacidad de reconocer mínimo 10000 aplicaciones, debe utilizar algoritmos de machine learning para identificación de estas.
15	La solución debe tener visibilidad y control de la aplicación desde el primer paquete enviado con el fin de clasificar el paquete de forma rápida y óptima.
16	La identificación de aplicaciones debe ser lo suficientemente robusta y flexible hasta tal punto de determinar si el paquete cuenta con los siguientes TAGs: Dominio, DSCP (Punto de Código de Servicios Diferenciados), segmento IP, Puerto.
17	Cada dispositivo SD-WAN debe soportar enrutamiento de tráfico por aplicativo basado en políticas eligiendo la mejor ruta en todo momento de acuerdo a varios KPIs medidos extremo-extremo, aplicando políticas de seguridad y calidad de servicio.
18	Los equipos CPE (Customer Premises Equipment) SD-WAN y vCPE (Virtual Customer Premises Equipment) SD-WAN debe permitir la creación de túneles IPSEC (Protocolo de Seguridad de Internet), Túneles GRE (Generic Routing Encapsulation), Túneles UDP (Protocolo de Datagramas de Usuario), VRRP (Protocolo de Redundancia de Enrutador Virtual), WCCP (Web Cache Communication Protocol).
19	Cada dispositivo CPE o vCPE debe soportar balanceo de tráfico por segmentos por diferentes canales a nivel WAN (Internet, MPLS o banda ancha, etc).
20	Cada dispositivo CPE o vCPE debe soportar balanceo de tráfico por aplicativo por diferentes canales a nivel WAN diferentes (Internet, MPLS, banda ancha, etc).
21	La solución debe proporcionar distintas opciones de balanceo entre los

	transportes utilizados en la arquitectura: Balanceo por calidad del transporte Por latencia Por Jitter Por Loss Balanceo por capacidad local Balanceo por capacidad local y remota
22	La solución debe poder customizar los tipos de balanceo por calidad del transporte y por BW disponible de los transportes Local, exclusión de transportes por fallas en el underlay u overlay y configuración del tiempo de espera a nivel de FEC.
23	La solución debe poder garantizar que un grupo de aplicaciones utilice un tipo de transporte específico y se conmute hacia otro transporte en caso de no cumplir con los KPIs de la aplicación a nivel de Jitter, Loss, Latencia entre los extremos de fábrica o hacia Internet (internet secure breakout). Para otro grupo de aplicaciones, la solución debe poder garantizar que se utilice otro tipo de transporte como principal y que conmute el tráfico en caso de no cumplir con los KPIs de la aplicación a nivel de Jitter, Loss, Latencia entre los extremos del fabricante o hacia internet (internet secure breakout).
24	Cada dispositivo SD-WAN deben poder interconectarse simultáneamente con sitios de sedes no SD-WAN estableciendo protocolos de enrutamiento dinámico fuera de la nube SD-WAN.
25	La solución debe poder detectar tráfico y enviarlo hacia internet para consumo de tráfico SaaS y WEB de acuerdo a políticas configuradas (Intelligent Local Breakout)
26	La solución debe tener la capacidad de manejar los siguientes tipos de redundancia a nivel WAN sin la necesidad de incluir dispositivos adicionales. - Activo/Activo (por segmentos o por aplicaciones) - Activo / Stand By (por segmentos o por aplicaciones) - Load balance
27	La solución debe tener la capacidad de conmutar el tráfico entre canales a nivel WAN de acuerdo con los siguientes criterios de disponibilidad del canal sobre la nube de SD-WAN. - Canal Down - Loss - Latencia - Jitter KPIs de Loss, latencia y Jitter deben poder especificarse con valores de

	acuerdo con el caso de uso del cliente, es decir, no es posible tener una solución con valores ya prediseñados de fábrica que no se pueda modificar.
28	La solución ofertada debe tener la capacidad de tener opciones de topologías regionales en Mesh o regionales para hub and Spoke con el fin de reducir sobre procesamiento en el establecimiento de túneles full Mesh por grupo de aplicaciones y para manejo de tráfico de forma diferente por cada región (topología, transporte, KPIs de medición, tipo de balanceo) la comunicación entre las regiones debe ser viables a través de los HUB sobre cada una de ellas. Las topologías deben ser definidas por software.
29	Los equipos de la solución (físicos y virtuales) debe ser compatibles con protocolos estándar de recopilación de datos como Netflow y/o homólogos.
30	Appliance CPE SD-WAN debe soportar los siguientes servicios adicionales: DHCP (Protocolo de Configuración Dinámica de Host), NAT (Traducción de Direcciones de Red), NTP (Protocolo de Tiempo de Red), PPPoE (Protocolo Punto a Punto sobre Ethernet), autodescubrimiento de MTU (Unidad de Transmisión Máxima) para formación de túneles.
31	La solución debe soportar políticas de corrección adaptativa. La relación entre los paquetes de paridad para recuperación automática debe estar asociado a las mediciones dinámicas sobre la red (FEC adaptativo) sin sacrificar alguna característica de performance sobre el equipo SD-WAN.
32	La solución debe tener la capacidad modificar el parámetro FEC de acuerdo con las necesidades del negocio por conjunto de aplicaciones; dentro de las opciones mandatarias se debe definir lo siguiente: - FEC estático - FEC adaptativo - Sin FEC
33	La solución SD-WAN debe soportar el agrupamiento lógico de canales WAN en un solo túnel o bonding y llevar a cabo balanceo de carga por paquete. Esta agregación de canales debe ser soportada, aunque los enlaces WAN tengan anchos de banda diferentes
34	La solución debe monitorear continuamente el estado de los túneles, así como la medición de los parámetros de delay, jitter, packetloss para toma de decisiones de enrutamiento inteligente del tráfico o flujos.
35	La solución debe monitorear continuamente el estado de los túneles a nivel de MOS (Mean Opinion Score)
36	Los dispositivos CPE SD-WAN deben seguir funcionando a nivel de flujo de tráfico incluso si se pierde la conectividad con el sistema de gestión o

	capa de control.
37	La solución debe tener la capacidad de re-ordenar los paquetes que están fuera de orden antes de entrega al destino final.
38	Cpe SD-WAN y vcpe SD-WAN deben contar y ser compatibles con protocolos estándar de QoS (Shaping - Rate Limit - queuing) para delimitar tráfico de ingreso o egreso de acuerdo con el flujo de conectividad por segmento o aplicativo.
39	La solución debe garantizar un BW mínimo o BW máximo de acuerdo con el flujo u overlay.
40	El QoS debe tener la capacidad de asignarlo a los flujos de tráfico identificados y/o overlays.
41	La solución SD-WAN debe respetar la marcación de QoS presentes, la solución debe proporcionar soporte nativo para QoS avanzada, incluida la lógica de clasificación sofisticada, una variedad de técnicas de marcación de paquetes, y el encolamiento y el modelaje de tráfico.
42	Los equipos CPE SD-WAN tipo appliance deben permitir su aprovisionamiento ZTP (Zero Touch Provisioning). No se debe requerir configuraciones previas sobre ellos para desplegar la solución. Es mandatorio que el ZTP se despliegue desde la misma consola de administración centralizada, en esta misma consola se debe garantizar reportería, analítica avanzada, aceleración, troubleshooting, orquestación y automatización).
43	La solución debe tener la capacidad de desplegar configuraciones de forma centralizada mediante plantillas o templates para todas las funcionalidades descritas en este documento.
44	El orquestador debe ofrecer soporte de IP SLA y, con base en violación de los umbrales definidos, soportar varias acciones como: habilitar túnel, deshabilitar túnel, anunciar rutas, modificar una métrica la métrica, cambiar prioridad de VRRP y generar alarmas.
45	La solución debe suministrar seguridad tanto en la capa de datos como en la capa de control entre la conexión del CPE SD-WAN y el sistema de gestión u orquestación.
46	Cada Overlay (cifrado de red) debe ser protegido a través de túneles encriptados AES de 256 bits.
47	Los túneles a nivel de underlay deben ser construidos por default por el protocolo IPSEC UDP entre los CPEs dentro del fabrica SD-WAN.
48	La solución debe garantizar segmentación de red end-to-end por intermedio de instancias virtuales.
49	La solución debe soportar 2000 VRFs, los cuales deben ser orquestados centralmente. Cada dispositivo debe soportar al menos 64 instancias virtuales o Vrf's.

50	La solución debe soportar encriptación de disco AES de 128 bits para propósito de duplicación.
51	Statefull Firewall, Antispoofing, Attack detection & protection, Secure syslog
52	IPS/IDS
53	DDoS detection and prevention
54	Best-of-Breed SASE integration
55	La solución de SD-WAN debe poder integrarse hacia SPLUNK para fines de análisis de seguridad.
56	Mitigación de inundaciones
57	Encriptación de data sensible: IPsec, IPsec Suite B, IKEv1/v2 (múltiples opciones de SHA & AES)
58	OAuth/SAML SSO debe contar con inicio de sesión único OAuth/SAML SSO.
59	El controlador sso debe realizar la integración entre Sisense y la plataforma de inicio de sesión del usuario determinado.
60	Debe cumplir con la validación del hardware criptográfico.
61	El sistema de gestión debe ser una plataforma única, que pueda realizar la administración de todos los dispositivos de la solución a nivel de SDN y gestión de todas las funcionalidades descritas en este documento en nube o premisas sin la necesidad de ejecutar comandos vía CLI para activación de alguna funcionalidad, es decir en un mismo gestor se debe asegurar: Orquestación, automatización, analítica avanzada, Optimización y aceleración, ZTP, reportería, administración, monitoreo, eventos y troubleshooting)
62	La plataforma de gestión /orquestación debe poder ser desplegada de forma flexible: instalada en nube pública, SaaS, nube privada o premisas del cliente final.
63	La plataforma de gestión / orquestación debe contar con administración de dispositivos basado en roles RBAC (Control de Acceso Basado en Roles).
64	Plataforma debe contar con interfaz web (GUI) para la administración de los dispositivos, actualizaciones remotas, y configuración masiva mediante templates o scripts que permita la configuración de equipos sobre todas las funcionalidades indicadas en el documento.
65	La plataforma de gestión y/o orquestación debe permitir integración con API's hacia sistemas o equipos de terceros
66	La plataforma de administración debe tener implementado una herramienta de medición de ancho de banda end-to-end de los canales Monitoreo de red centralizado, visibilidad global y configuración de políticas centralizadas.
67	La plataforma de gestión debe administrar toda la solución de SD-WAN

	(orquestación, automatización, analítica avanzada, optimización y aceleración, ZTP, reportería, administración, monitoreo, eventos y troubleshooting), debe poder diferenciar la capa de Underlay y la capa Overlay a nivel de Loss, latencia, Jitter, MOS y topologías).
68	La plataforma de gestión debe contar con la capacidad de debe permitir la realización de backup de la configuración del orquestador y de los gateways que conforman la plataforma SD-WAN.
69	La plataforma de gestión debe visualizar a nivel real e históricos las principales aplicaciones en uso.
70	La plataforma de gestión debe visualizar a nivel real e históricos: consumo de ancho de banda por aplicativo.
71	La plataforma de gestión debe visualizar a nivel real e históricos: utilización de ancho de banda: presentar la cantidad total de ancho de banda que está siendo utilizada tanto para tráfico optimizado como el no optimizado.
72	La plataforma de gestión debe visualizar a nivel real e históricos: Desempeño de red. A nivel de paquetes por segundo del desempeño que está siendo alcanzado a nivel de WAN para tráfico optimizado y no optimizado.
73	La plataforma de gestión debe visualizar a nivel real e históricos: Conteo de flujos. Seguimiento del número de flujos generados a través de la WAN para tráfico optimizado y no optimizado.
74	La plataforma de gestión debe visualizar a nivel real e históricos: Latencia: componentes de la solución con mayor latencia.
75	La plataforma de gestión debe visualizar a nivel real e históricos: • Pérdida de paquetes. • Medición de la pérdida máxima de paquetes como un conjunto y como conexiones WAN individuales.
76	La plataforma de gestión debe estar en la capacidad de generar reportes programadas y a demanda.
77	Los reportes deben poder ser extraídos desde la plataforma de gestión
78	Se debe monitorear la corrección de errores (FEC) extremo - extremo dentro del fabric SD-WAN.
79	La solución debe proveer mecanismos de aceleración en las aplicaciones detectadas que mitigue la latencia de los enlaces, disminución de requerimientos de ancho de banda en la red y que mejore los tiempos de respuestas a estas sin necesidad de desplegar "service Chaining".
80	Técnicas de reducción de datos que incluyen mecanismos de compresión y de duplicación de datos para reducir la cantidad de datos que atraviesan enlaces WAN.

81	La solución SD-WAN debe inspeccionar el tráfico que se envía entre clientes y servidores, almacenando información localmente en los dispositivos SD-WAN. técnicas avanzadas de detección de patrones repetitivos, lo que minimiza la interacción a través de la WAN para mejorar el rendimiento de las aplicaciones y maximizar la utilización de la WAN.
82	La solución SD-WAN debe utilizar la fusión de paquetes para agrupar varios paquetes más pequeños en un solo paquete más grande (Paquet Coalescing).
83	La solución debe proveer mecanismos de compresión y de duplicación que elimine la transmisión de datos repetitivo sobre los enlaces WAN. Esta puede ser aplicada para todos los protocolos basados en IP incluyendo TCP (Protocolo de Control de Transmisión) y UDP (Protocolo de Datagramas de Usuario).
84	La solución debe proveer mecanismos que asegure la aceleración a nivel de TCP: Window Scaling Selective Ack Round Trip Time Measurement
85	Los equipos SD-WAN deben estar en la capacidad de soportar en la misma caja funcionalidades de aceleración sin la necesidad de hacer un upgrade/ adición de hardware.
86	El mismo sistema de gestión / orquestación debe tener la capacidad de orquestar, administrar y monitorear funcionalidades de aceleración sin la necesidad de contar con otro sistema de gestión diferente. Es mandatorio que el gestor sea el mismo para reportes, analítica, troubleshooting, automatización, centralización de políticas, visibilidad.

Numeral 3.5 REQUISITOS DE EMPAQUE Y ROTULADO.

3.5.1. Empaque

La antena, modem y accesorios deberán estar perfectamente empacados con el fin que se puedan transportar a todos los sitios que se requieran. Además, los elementos deberán estar almacenados en una caja robusta para que brinde seguridad y conservación de los elementos en el transporte.

3.5.2. Rotulado

Los elementos deberán contar con su debida marcación con serial o número de identificación, número de contrato y proveedor, a fin de establecer en caso de fallas a donde se debe tomar contacto.

4. TOMA DE MUESTRAS Y CRITERIO DE ACEPTACIÓN O RECHAZO:

4.1. TOMA DE MUESTRAS Y CRITERIO DE ACEPTACIÓN O RECHAZO PARA EVALUAR LOS REQUISITOS ESPECÍFICOS GENERALES Y REQUISITOS DE EMPAQUE Y ROTULADO

4.1.1. Muestreo

Se realizará la comprobación del ancho de banda en cuanto a descarga de datos mediante aplicación de testeo de velocidad.