Nombre Comercial del Bien o Servicio	SERVICIO DE CONECTIVIDAD WAN-LAN
Calidad	El servicio debe cumplir con todos los requisitos establecidos en el presente ANEXO TÉCNICO. NTC2050 – Norma Retie para instalaciones eléctricas. Registro TIC RFC 8200 y 2460 Resolución 1126 de 2021. **Eficiencia energética y requisitos ambientales de los equipos de conectividad.** El CONTRATISTA deberá garantizar que los equipos activos que suministre e instale para la prestación del servicio de conectividad cumplan la certificación ENERGY STAR® vigente o una certificación ambiental equivalente, como EPEAT, TCO Certified u otra expedida por un organismo reconocido internacionalmente con criterios de eficiencia energética iguales o superiores. Esto incluye equipos SD-WAN, enrutadores, conmutadores (switches), puntos de acceso inalámbrico, equipos terminales satelitales, sistemas de alimentación ininterrumpida (UPS) y demás componentes. Las fuentes de alimentación de los equipos de centro de datos y de los cuartos de telecomunicaciones deberán contar con certificación 80 PLUS o equivalente. Para los equipos cuya categoría no esté cubierta por las certificaciones mencionadas, el CONTRATISTA deberá acreditar el cumplimiento mediante una declaración del fabricante. Dicha declaración deberá venir acompañada de la ficha técnica en la que consten el consumo de energía en operación y en reposo y las funciones de ahorro de energía disponibles, como el estándar IEEE 802.3az (Energy Efficient Ethernet) o el apagado de puertos sin uso. El cumplimiento se acreditará con la entrega de los certificados, registros o declaraciones vigentes de cada modelo ofertado, los cuales serán verificados por la supervisión o la interventoría antes de la aceptación de los equipos. Esta exigencia se enmarca en la política de Compra Pública Sostenible y en los lineamientos de la Agencia Nacional de Contratación Pública – Colombia Compra Eficiente.
Generalidades	Se requiere la prestación del servicio de conectividad corporativa WAN□LAN, con soporte para IPv4 e IPv6, a nivel nacional para la Fiscalía General de la Nación, en todas las sedes y nodos descritos en el Anexo Técnico 1.1. Dado que la FGN adquiere un servicio integral, se verificará la capacidad técnica de todos los dispositivos y componentes utilizados por el /PROVEEDOR, con el fin de garantizar el cumplimiento de los parámetros exigidos y la viabilidad del objeto contractual. Cuando en el presente Anexo Técnico se utilice la expresión “sin costo adicional”, se entenderá que el valor de la obligación deberá estar incluido en el precio ofertado y no dará lugar a un pago separado durante la ejecución. Esta expresión no implica que la Entidad pueda exigir prestaciones ilimitadas, diferentes o adicionales al alcance definido en los documentos del proceso. Las actividades inherentes a la prestación integral del servicio, necesarias para cumplir las especificaciones, la continuidad, la interoperabilidad, el soporte y los ANS, deberán estar comprendidas en el valor ofertado, dentro de las cantidades, capacidades y límites establecidos en los anexos técnicos y en el Formato de Oferta Económica. Cuando una necesidad exceda dichas cantidades, capacidades o límites, su reconocimiento solo procederá si existe una unidad y un precio contractual aplicable, o mediante el trámite de modificación correspondiente, previa justificación, autorización de la FGN y disponibilidad presupuestal. La interventoría verificará que la facturación corresponda a servicios efectivamente prestados y a valores contractualmente pactados.

El PROVEEDOR deberá implementar y configurar los protocolos de enrutamiento necesarios para el underlay y la superposición SD-WAN, asegurando estabilidad operativa, convergencia eficiente y comportamiento predecible de los servicios. La solución deberá integrarse con las herramientas de Observabilidad de la FGN, exponiendo métricas de desempeño tales como: latencia, jitter, pérdida, disponibilidad, SLA por enlace, calidad de ruta y selección basada en políticas y las demás métricas que la FGN requiera.

La red operará en modo ACTIVO□ACTIVO entre los nodos primarios Categoría 1 (Bogotá y Cali). La FGN definirá la distribución del tráfico por aplicación y servicio, mientras que las políticas de balanceo y conmutación automática se aplicarán conforme a los ANS de desempeño establecidos por la Entidad.

Todo el tráfico se transportará mediante un overlay SD-WAN cifrado (IPsec/AES□256), con priorización por clase y por aplicación, y selección dinámica de ruta basada en métricas de desempeño (latencia, pérdida, jitter/MOS y retenibilidad). Esta arquitectura deberá garantizar continuidad operativa incluso ante degradación o falla severa de uno de los nodos Categoría 1, permitiendo que el nodo restante asuma la carga total mediante balanceo geográfico, sin intervención manual ni afectación del servicio.

Se mantendrá la independencia operativa entre la conectividad provista por el PROVEEDOR y la LAN interna de la FGN. El acceso del PROVEEDOR deberá finalizar en interfaces definidas (hand□off), mientras que la administración de los recursos LAN (switches, impresoras, cámaras, CCTV, entre otros) permanecerá bajo los lineamientos, herramientas y controles de la FGN. Esta separación aplica a las seis (6) categorías y deberá quedar documentada en el diseño integral de la solución.

El PROVEEDOR deberá suministrar comunicaciones desde todas las sedes de la Entidad en las Categorías 2, 3, 4 y, cuando aplique categoría 6 hacia los nodos Categoría 1 (Datacenter Bogotá, Datacenter Cali y nubes públicas Azure y OCI), mediante canales dedicados, VPN B2B o mecanismos de interconexión cloud según la categoría y necesidad de la FGN. Todos estos enlaces deberán integrarse al overlay SD-WAN cifrado y operar en modo activo□activo, aplicando políticas de QoS y priorización por clase y aplicación definidas por la FGN.

El presente Anexo Técnico aborda exclusivamente los componentes propios del dominio de Conectividad. Los requerimientos de seguridad perimetral, inspección, Sandboxing, SSE/SASE, prevención de fuga de información, criptografía avanzada y demás controles de ciberseguridad se desarrollan en el ANEXO TECNICO 2. SEGURIDAD DIGITAL Y CIBERSEGURIDAD (Ficha Técnica de Seguridad), la cual deberá leerse en conjunto con este documento. La integración entre ambos dominios será responsabilidad del PROVEEDOR conforme al diseño aprobado por la FGN.

Para verificar este requerimiento, el proveedor deberá presentar a la firma del acta de inicio el certificado del fabricante donde acredite que los equipos son nuevos, no remanufacturados y no se encuentran fuera de venta (“end of sale”) durante toda la ejecución del contrato, así como, que cuenta con soporte técnico, disponibilidad de repuestos y garantía durante el tiempo de ejecución del contrato. Adicionalmente, se deben adjuntar las órdenes de compra de proveedor al fabricante de los equipos a instalar en las sedes con fecha posterior a la adjudicación del presente proceso.

Posterior a la nacionalización de los equipos el proveedor deberá entregar a la supervisión los certificados de importación de los equipos a instalar en las sedes con fecha posterior a la adjudicación del presente proceso.
Los documentos relacionados con órdenes de compra al fabricante, seriales de los equipos, documentos de importación, manifiestos, certificados de nacionalización y registros de garantía podrán ser presentados de manera progresiva, conforme al cronograma de suministro e instalación aprobado para la ejecución del contrato y dentro de los plazos que establezca la supervisión, respecto de los equipos efectivamente adquiridos, nacionalizados e instalados por fase o sede. Lo anterior no

<table>
<tr><td></td><td>elimina los requisitos documentales exigidos por la Entidad, los cuales deberán acreditarse en las etapas de recepción, verificación, instalación y aceptación de los bienes, garantizando la trazabilidad, la legal procedencia y la condición de equipos nuevos. El certificado del fabricante señalado en el presente numeral deberá presentarse, en todo caso, a la firma del acta de inicio.</td></tr>
<tr><td>Requisitos generales</td><td>Adquirir los servicios de telecomunicaciones de red corporativa WAN-LAN integrada a la seguridad informática y videoconferencia para la Fiscalía General de la Nación.

Requerimientos generales de la solución

<table>
<tr><th>ITEM</th></tr>
<tr><td>C1. Requerimientos generales de la solución</td></tr>
<tr><td>C2. Requerimientos de Cobertura</td></tr>
<tr><td>C3. Requerimientos tecnológicos y Perfiles de las sedes de la FGN</td></tr>
<tr><td>C4. Requerimientos de Instalaciones</td></tr>
<tr><td>C5. Requerimientos de Aprovisionamiento</td></tr>
<tr><td>C6. Adiciones, Cancelaciones, Suspensiones, Ampliaciones temporales y traslados del servicio durante la ejecución del contrato</td></tr>
<tr><td>C7. Clases de servicio requeridos</td></tr>
<tr><td>C8. Requerimientos de Topología</td></tr>
<tr><td>C9. Requerimientos de Gestión de Red (Operación)</td></tr>
<tr><td>C10. Servicio de Internet Requerido</td></tr>
<tr><td>C11. Servicio de Obras de adecuación</td></tr>
<tr><td>C12. Requerimientos de Mantenimiento</td></tr>
<tr><td>C13. Análisis de Ingeniería de Tráfico</td></tr>
<tr><td>C14. Inventario de los servicios prestados.</td></tr>
<tr><td>C15. Pruebas de Aceptación del Servicio</td></tr>
<tr><td>C16. Acuerdos de Niveles de Servicios (ANS)</td></tr>
<tr><td>C17. Requerimientos de Gestión de Tráfico de Internet mediante Plataforma SD-WAN</td></tr>
<tr><td>C18. Requerimiento de equipos del contrato</td></tr>
<tr><td>C19. Requerimientos de switching (core)</td></tr>
<tr><td>C20. Requerimiento a eventos jornadas de descongestión</td></tr>
</table></td></tr>
<tr><td>Requisitos específicos</td><td>
<table>
<tr><th>ITEM</th><th></th></tr>
<tr><td>C1. Requerimientos generales de la solución</td><td>La FISCALÍA GENERAL DE LA NACIÓN (FGN) requiere la prestación del servicio de la red nacional corporativa de telecomunicaciones de amplia cobertura (WAN) y de red local (LAN), soportada en una arquitectura SD-WAN de última generación la cual debe consistir en una red definida por software, gestionada de forma centralizada mediante un controlador , que permita la transmisión de datos, voz y video de forma segura, eficiente y con priorización por aplicación, cumpliendo con los Acuerdos de Niveles de Servicio descritos en el ANEXO TECNICO 5. ACUERDO NIVELES DE SERVICIO - ANS
.</td></tr>
</table></td></tr>
</table>

		La solución SD-WAN deberá utilizar un overlay cifrado, soportado en múltiples tecnologías de acceso (fibra, Internet satelital de orbita baja Empresarial), y permitir la selección dinámica de rutas conforme a parámetros de desempeño (latencia, ancho de banda, perdida de paquetes, jitter, disponibilidad), garantizando la continuidad y calidad de los servicios misionales de la FGN, implementada en una arquitectura SASE (Secure Access Service Edge). Para este efecto el PROVEEDOR debe: C1.1. A la firma del acta de inicio se debe presentar el diseño integral de la solución SD-WAN, incluyendo: C1.1.1. Descripción del modelo de operación en modo activo-activo entre los Centros de Datos de Bogotá y Cali. C1.1.2. Infraestructura requerida para el overlay SD-WAN, políticas de seguridad, segmentación por VRF/VLAN, y gestión de tráfico por aplicación de acuerdo con la priorización solicitada por la Fiscalía General de la Nación. C1.1.3. Especificaciones técnicas completas de los CPE SD-WAN, equipos de seguridad, equipos de borde y elementos de conectividad utilizados para soportar el servicio.- C1.1.4. Arquitectura hub and- -spoke, malla parcial o total, según perfil de las sedes. C1.1.5. Topología de acceso por categoría de sede en línea con lo establecido en el anexo técnico 1.1. Entregar completamente diligenciados dentro de su propuesta los anexos solicitados, garantizando que toda la información refleja la nueva arquitectura de la solución ofertada, sus capacidades, dependencias y configuración requerida por la FGN. C1.2. En el valor total de su propuesta, el PROVEEDOR debe incluir: C1.2.1. Hardware y software licenciados necesarios para la implementación de la solución ofertada, en todas las sedes, incluyendo para las conexiones a las nubes públicas que utiliza la entidad. C1.2.2. Personal con experiencia y certificación del fabricante de cada uno de los componentes que integran la solución ofertada, garantizando que dicho personal esté técnicamente calificado para ejecutar los procesos de instalación, configuración, puesta en producción y operación de la plataforma. *El equipo humano del PROVEEDOR para la prestación de los servicios de Conectividad se describe en el Anexo Técnico 6 Perfiles Profesionales, numerales P1 (Roles estratégicos transversales), P2 (Perfiles técnicos de Conectividad), P4 (Perfiles técnicos de Servicios - Mesa de Ayuda) y P9 (Reglas generales del personal). La disponibilidad operativa de cada perfil se rige por el régimen indicado en su respectiva ficha.* C1.2.3. Se debe suministrar la totalidad los cables, herrajes, tornillos, bases y accesorios necesarios para su correcta instalación, integración y funcionamiento con los equipos existentes de la FGN.

		C1.2.4. Gestión unificada de la solución, incluyendo administración centralizada y telemetría avanzada la cual debe ser integrada a la herramienta de Observabilidad de la fiscalía General de la Nación. C1.2.5. La tecnología ofrecida deberá soportar IPv4 e IPv6 en modalidad dual stack en todos sus componentes. Asimismo, el proveedor deberá implementar IPv6 conforme a la Resolución 1126 de 2021, realizar la adquisición de un pool IPv6 /44 y un ASN a nombre de la Fiscalía General de la Nación, y garantizar su renovación durante toda la vigencia del contrato. De igual manera, deberá elaborar la documentación técnica requerida por la guía correspondiente y realizar la transferencia de conocimiento asociada a la implementación. C1.2.6. En caso de que la implementación requiera componentes activos y pasivos adicionales para soportar los servicios de transmisión de voz, datos, video o segmentación, el PROVEEDOR deberá suministrarlos, configurarlos e instalarlos como parte integral de la solución y la red MPLS, sin costos adicionales. Asi mismo la solución debe permitir conectar los Datacenter de Bogotá y Cali como puntos de agregación nacional y a las nubes públicas (Oracle Cloud y Microsoft Azure existentes a la fecha), con políticas de segmentación, QoS y seguridades aprobadas por la FGN. C1.2.7. Todos los dispositivos de comunicaciones deberán permitir administración y monitoreo bajo la plataforma de Observabilidad seguro mediante: □ SSH versión 2 con cifrado (AES 256), □ SNMP v2/v3, □ Netftlow □ Syslog seguro (TLS V1.3 o su equivalente), □ Exposición de métricas SD-WAN: SLA por enlace, jitter, latencia, pérdida, disponibilidad, calidad de ruta y selección por aplicación, anchos de banda. □ Instalación de sintéticos de observabilidad de la plataforma de la Fiscalía General de la Nación. C1.2.8. Los dispositivos de conectividad, seguridad, control y los CPE SD-WAN deberán sincronizarse con el servicio NTP de la FGN (hora legal colombiana), asegurando sincronización consistente para efectos de auditoría, correlación de eventos y funcionamiento correcto de la plataforma de administración. C1.2.9. La solución deberá contar con componentes de última milla deberán ser dedicados exclusivamente para la red de la FGN, evitando cualquier arquitectura multitenant que comprometa el aislamiento, confidencialidad o desempeño requerido para los servicios misionales. C1.2.10. El PROVEEDOR deberá suministrar un acceso de lectura a todos los equipos que hacen parte de la solución, en línea con lo establecido en el anexo técnico de Seguridad. C1.2.11. En aquellos casos en que la actualización de la plataforma o de alguno de sus componentes requiera ajustes que impliquen cambios en el entorno tecnológico de la Entidad, deberá adelantarse previamente el proceso de Gestión del Cambio, conforme a los lineamientos establecidos por la fiscalía

		general de la Nación. El incumplimiento de dicho procedimiento dará lugar a la aplicación de los Acuerdos de Niveles de Servicio (ANS) correspondientes.
	C2. Requerimientos de Cobertura	C2.1. Se requiere proveer la interconexión de todos los nodos de la FGN (relacionados en el ANEXO TÉCNICO 1.1.) distribuidos a nivel nacional, mediante una arquitectura propuesta en dicho anexo, que permita el transporte seguro y priorizado de datos, voz y videoconferencia, soportada en un overlay cifrado (IPsec/AES256) y políticas de selección dinámica de ruta basadas en niveles de desempeño (latencia, pérdida, jitter, retenibilidad). Los nodos se clasificarán de la siguiente manera: C2.1.1. Nodos Completos Tipo 1: Sedes a las cuales se les deberá proveer acceso mediante enlaces de comunicaciones dedicados, integrados a la arquitectura SD-WAN, asegurando:- □ Transmisión de datos, voz y videoconferencia. □ Conexión simultánea hacia los Centros de Datos de la FGN (Bogotá y Cali), en modo activo activo. □ Segmentación por VRF/VLAN y políticas de aplicación. □ Alta disponibilidad en la solución completa en la sede. □ Redundancia de ultimo kilometro por proveedor y ruta geográfica de acceso diferente. □ Priorización de tráfico mediante QoS. □ Variación de retardo: la solución deberá cumplir los parámetros de variación de retardo de paquetes, IPDV o jitter establecidos en el Anexo Técnico 5 – Acuerdo Niveles de Servicio, de acuerdo con el tipo de trayecto, categoría y tecnología aplicable. Estos parámetros constituirán la referencia para la medición y evaluación contractual del desempeño de la red. □ Políticas de tráfico definidas extremos a extremo. □ Seguridad inherente por la red privada. □ Capacidad estable y simétrica para que los anchos de banda sean consistentes. □ SD-WAN cifrado, incluyendo conectividad a las nubes públicas de la entidad. □ Debe realizar local internet breakout con inspección y filtrado (Firewall, Antivirus, IPS, Control de Aplicaciones, sandboxing) local en la sede para brindar seguridad a los usuarios. □ Estabilidad en las rutas. □ Redundancia lógica permitiendo failover instantáneo. □ Control sobre BGP, DHCP y direcciones fijas. C2.1.2. Nodos Datos Tipo 2: Sedes que requieren transmisión de datos, mediante enlaces dedicados integrados a la capa SD-WAN, garantizando:- □Conectividad cifrada hacia los Centros de Datos de la FGN. □Priorización por aplicación y clase de servicio (QoS).

		- Políticas de tráfico definidas extremos a extremo. - Seguridad inherente por la red privada. - Capacidad estable y simétrica para que los anchos de banda sean consistentes. - SD-WAN cifrado, incluyendo conectividad a las nubes públicas de la entidad. - Estabilidad en las rutas. - Redundancia lógica permitiendo failover instantáneo. En ambos tipos de nodos, la solución SD-WAN deberá permitir operación simultánea con múltiples tecnologías de acceso, incluyendo fibra óptica, solución satelital del orbita baja empresarial como respaldo, según disponibilidad. C2.1.3. Escalabilidad y crecimiento El PROVEEDOR deberá considerar la escalabilidad completa de la red SD-WAN, garantizando: - Ampliación de ancho de banda por demanda en cualquier nodo, sin afectar la operación del resto de la red. - El throughput mínimo exigible a cada CPE SD-WAN es el definido por categoría en el Cuadro C5.3, medido en condiciones operativas con los túneles cifrados (IPsec/AES-256) y las funcionalidades inherentes a la solución habilitadas, no sobre tráfico plano. - Inclusión, traslado o eliminación de nodos dentro de cualquier región del país, mediante procesos de provisión automática (Zero-Touch Provisioning). Capacidad para soportar crecimiento futuro en las categorías de sedes, incluyendo incrementos en tráfico de voz, video, aplicaciones misionales, servicios colaborativos y servicios expuestos vía Internet. C2.1.4. Soporte a VoIP (HCS) y servicios de comunicaciones unificadas La solución deberá permitir la implementación completa del servicio de VoIP (HCS) de la FGN, garantizando que: - Todo tráfico de voz viaje por el servicio, con el QoS adecuada y priorización por aplicación/clase definida en las políticas centrales. - El servicio de telefonía IP funcione independientemente del proveedor saliente o entrante, manteniendo la integración con las sedes y plataformas centrales. - En caso de que la FGN cambie de operador del servicio HCS, el PROVEEDOR deberá realizar las configuraciones requeridas sobre los CPE SD - Voz, datos y videoconferencia se encuentren totalmente integrados dentro de la solución ofertada. C2.1.5. Cobertura nacional y categorización Las ubicaciones geográficas de todas las sedes y su clasificación por categorías se encuentran descritas en el Anexo Técnico 1.1.

		La solución deberá garantizar: Cobertura nacional completa, en todas las sedes listadas. Tecnología de acceso adecuada por ubicación Fibra donde exista disponibilidad. Solución satelital del Orbita baja empresarial donde no exista fibra de cualquier proveedor de última milla y capacidad de conexión. Cuando en una ubicación no exista disponibilidad de fibra óptica u oferta terrestre que cumpla los requisitos exigidos, dicha condición podrá acreditarse mediante certificación de uno o varios operadores de telecomunicaciones habilitados, estudios de cobertura o de factibilidad, conceptos técnicos de cobertura u otros documentos equivalentes, los cuales serán validados por la FGN. Conectividad priorizada hacia los Centros de Datos y hacia Internet, según políticas de la FGN.
	C3. Requerimientos tecnológicos y Perfiles de las sedes de la FGN	La FGN ha clasificado sus sedes con base en los requerimientos de comunicaciones, la ubicación geográfica y el número de usuarios a interconectar, según las siguientes categorías de perfiles, tal como se indica a continuación: El universo de sedes objeto del presente proceso es de ochocientas setenta y seis (876) sedes, distribuidas así: Categoría 1, dos (2) nodos alojados en dos (2) sedes físicas (Búnker Salitre — Nivel Central Bogotá y Búnker Cali), correspondientes a cuatro (4) registros del Anexo Técnico 1.1 (ID 51, 118, 127 y 820); Categoría 2, setecientas sesenta y una (761) sedes; Categoría 3, ochenta y seis (86) sedes; y Categoría 4, veinticinco (25) sedes. A ello se suman cuatro (4) canales de Categoría 5 (interconexión a nubes públicas) y cuatro (4) canales de Categoría 6 (complementarios). La relación detallada por sede, con su categoría, esquema de acceso, capacidad y servicios asociados, es la contenida en el Anexo Técnico 1.1 Requerimiento de sedes a conectar, que establece la clasificación definitiva sede por sede, con el ID Nodo como identificador, y constituye la referencia para determinar la categoría, capacidades, medios de acceso, redundancia y demás servicios requeridos. En caso de diferencias entre referencias históricas, estudios previos o versiones anteriores y los documentos técnicos actualizados, prevalecerá la clasificación definitiva publicada por la FGN. C3.1. Red Categoría 1 (Datacenter / Núcleo SD-WAN): Núcleo de la red conformado por los nodos primarios del PROVEEDOR ENTRANTE que soportan el servicio: Datacenter de Bogotá (Nivel Central) y Datacenter de Cali, operando en modo activo-activo y constituyendo los puntos de agregación nacional del overlay SD-WAN. Cada nodo Cat 1 dispone de dos (2) canales de Internet de mínimo 5 Gbps (uno por nodo), dos (2) canales de datos de mínimo 5 Gbps para el transporte entre nodos y entre las sedes hacia los nodos, y dos (2) canales de interconexión dedicada por cada nube pública de la entidad. Los Cat 1 alojan la totalidad de los componentes de control, gestión, orquestación y seguridad perimetral de acuerdo con lo establecido en el ANEXO TECNICO 2. SEGURIDAD DIGITAL Y CIBERSEGURIDAD, estos canales proveen las salidas de Internet con políticas de balanceo geográfico y se integran con la plataforma de Observabilidad de la FGN. Soportan la totalidad del tráfico de datos, voz (HCS) y videoconferencia. Los canales de Categoría 1 corresponden a los registros identificados con los ID 51, 118, 127 y 820 del Anexo Técnico 1.1 – Sedes, los cuales deberán considerarse para el dimensionamiento de la conectividad asociada a los nodos principales de la Entidad. Los canales de interconexión con

		las nubes públicas Azure y OCI (Categoría 5) son independientes de los anteriores y deberán dimensionarse conforme a las características técnicas, capacidades, redundancia y esquemas de interconexión definidos para el componente de nube, sin que puedan interpretarse como canales adicionales de Categoría 1. C3.2. Red Categoría 2 (Sedes principales por ciudad): Conectividad operativa entre las sedes principales de la FGN ubicadas en ciudades capitales y los nodos Cat 1 (Bogotá, Cali y Nubes públicas) a través del overlay SD-WAN cifrado. Categoría que consolida la antigua Cat 2 y Cat 2.1 (sedes con atención a usuarios). Se atiende mediante enlaces dedicados de fibra óptica con redundancia 1:1, doble proveedor de última milla, rutas geográficas distintas y nodos/PoP diferentes; sin reuso, conforme al procedimiento de excepción por imposibilidad técnica o comercial previsto en el numeral C3.8.5. Cada sede dispone de CPE SD-WAN, integración a las VRF/VLAN definidas por la FGN, priorización por aplicación y clase (QoS), local Internet breakout con inspección y filtrado, conexión simultánea hacia Bogotá, Cali y nubes en modo activo-activo, alta disponibilidad de la solución completa y baja variación de retardo (jitter) entre nodos. Comprende el Nivel Central, las sedes de Bogotá y las sedes principales en capitales departamentales. Concentra la mayoría de la planta de la FGN. C3.3. Red Categoría 3 (Redes metropolitanas / Ciudades intermedias): Conectividad dentro de los límites de una ciudad ciudades intermedias y municipios que integra sedes de la FGN a su sede principal local (Cat 2) y a los nodos Cat 1 (Bogotá, Cali y Nubes públicas) a través del overlay SD-WAN. Acceso provisto típicamente por fibra óptica dedicada con redundancia lógica y failover instantáneo. Cada sede dispone de un (1) canal WAN terrestre dedicado integrado al overlay SD-WAN y de un mecanismo de respaldo (segunda vía terrestre donde exista cobertura, o enlace satelital LEO empresarial donde no la haya), con conmutación automática gestionada por el CPE SD-WAN. Integra los servicios de voz, datos y videoconferencia bajo el mismo esquema de QoS; mantiene control de BGP, DHCP y direcciones fijas, y opera bajo las mismas políticas de seguridad y observabilidad de la red. Cubre las sedes seccionales en ciudades intermedias del territorio nacional. C3.4. Red Categoría 4 (Resto nacional Satelital órbita baja empresarial): Conectividad para los municipios y demás sedes no incluidas en las categorías anteriores, prestada mediante tecnología satelital de órbita baja (LEO) empresarial como medio de acceso WAN, totalmente integrada al overlay SD-WAN cifrado. No se permiten tecnologías MEO, GEO, radio spread spectrum ni radio no licenciado. Podrá emplearse cualquier servicio satelital LEO empresarial disponible en el mercado, incluidos los que surjan durante la ejecución del contrato, siempre que cumpla los requisitos de desempeño establecidos en el presente Anexo Técnico. La sede mantiene su direccionamiento interno y segmentación VLAN definidos por la FGN; el CPE SD-WAN administra el local breakout y permite la administración de los recursos LAN (switches, impresoras, CCTV, etc.). El servicio opera bajo planes empresariales con priorización de tráfico mediante QoS, integración a la observabilidad de la FGN y conexión hacia Bogotá, Cali y nubes públicas. Concentra las sedes de baja densidad geográfica. C3.5. Red Categoría 5 (Nubes públicas): Categoría reservada exclusivamente para garantizar la comunicación con las nubes públicas de la Entidad. Se atiende mediante dos (2) canales de interconexión dedicada por proveedor cloud , terminados sobre los nodos Cat 1 de Bogotá y Cali, con capacidad mínima

definida por la FGN, modo activo-activo, segmentación por VRF/VLAN y políticas de seguridad alineadas con la arquitectura SD-WAN. La conectividad cloud queda incluida en el overlay cifrado, sujeta a las mismas políticas de QoS, ruteo y priorización por aplicación. Esta categoría no incluye sedes físicas de la FGN.

C3.6. Red Categoría 6 (Canales complementarios): Categoría destinada a los canales adicionales que complementan o respaldan la operación de la red corporativa de la FGN y que no hacen parte del overlay SD-WAN principal, tales como canales de Internet dedicados empresariales y enlaces de contingencia. Estos canales deberán ofrecer capacidad mínima de 100 Mbps simétricos, sin reuso, sobre fibra óptica, con disponibilidad mínima del 99,8 %, redundancia hasta el punto de entrega, canal de respaldo activo-pasivo, routers empresariales, pool mínimo de veinticinco (25) direcciones IP públicas IPv4/IPv6, y contar con monitoreo proactivo 7×24 y soporte técnico especializado. El PROVEEDOR podrá presentar, para aprobación de la FGN, alternativas de uso optimizado del direccionamiento IPv4 (traducción de direcciones, segmentación o reasignación), siempre que se garantice la operación de los servicios publicados. Los canales de esta categoría mantendrán visibilidad y capacidades de observabilidad cuando aplique, y estarán exentos de la integración y aplicación de la solución de seguridad de la Entidad dentro del presente proceso contractual.

C3.7. Disposiciones comunes a todas las categorías de red: La solución SD-WAN debe cubrir las seis (6) categorías del contrato (Cat 1 Datacenter, Cat 2 Ciudades principales, Cat 3 Ciudades intermedias / metropolitanas, Cat 4 Resto nacional, Cat 5 Nubes públicas y Cat 6 Canales complementarios), garantizando para todas:

C3.7.1. Tráfico cifrado por overlay SD-WAN (IPsec/AES256), con priorización por aplicación/clase y selección dinámica de ruta basada en métricas de desempeño (latencia, pérdida, jitter/MOS, retenibilidad).
C3.7.2. Independencia entre la conexión del PROVEEDOR y la LAN interna de la FGN: el acceso del PROVEEDOR terminará en interfaces definidas (hand-off) y la administración de los recursos LAN (switches, impresoras, cámaras, CCTV, etc.) seguirá bajo lineamientos y herramientas de la FGN.
C3.7.3. Conectividad de cada sede hacia los nodos Categoría 1 (Datacenter Bogotá, Datacenter Cali y Nubes públicas) en modo activo-activo, con balanceo y conmutación automática.
C3.7.4. Direccionamiento LAN interno y segmentación (VLAN por sede) preservados según los lineamientos de la FGN.
C3.7.5. Visibilidad y telemetría expuestas en la plataforma de Observabilidad de la entidad y en el orquestador SD-WAN.-
C3.7.6. La condición "sin reuso" se refiere a la no sobreasignación de la capacidad contratada por sede (relación 1:1 entre capacidad contratada y capacidad disponible), sin que ello implique exclusividad física de la red de transporte del operador más allá del segmento de acceso de última milla dedicado.

C3.8. Categorías 1 y 2 Doble vía terrestre dedicada: Cada sede de las Categorías 1 y 2 deberá contar con un (1) canal WAN dedicado y un (1) canal de Internet dedicado, ambos en modo activo-activo sobre el overlay SD-WAN, cumpliendo estrictamente:

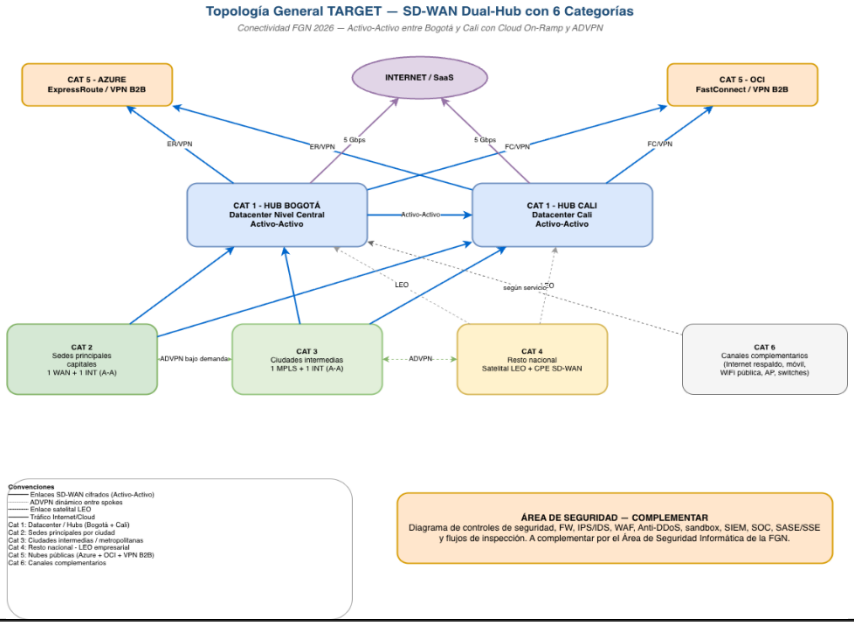
		C3.8.1. Cada canal debe cursar por nodo/PoP diferente del PROVEEDOR. C3.8.2. Fibras y rutas completamente distintas; no se aceptan hilos o pares de la misma fibra. C3.8.3. Equipos de último kilómetro independientes por cada camino. C3.8.4. El PROVEEDOR documentará la diversidad (planos, rutas, OTDR/trazabilidad de fibra o equivalente y rutas de transporte) y ejecutará pruebas de conmutación y balanceo activo-activo. Entregará por cada sede los planos de rutas y copia de configuraciones al momento de la entrega, incluyendo sedes en traslado o ampliación. C3.8.5. Procedimiento de excepción por imposibilidad técnica o comercial (sedes Categoría 2): cuando el PROVEEDOR evidencie de manera objetiva y documentada la imposibilidad técnica o comercial de implementar la totalidad de las condiciones de diversidad física requeridas en una sede, mediante estudios de cobertura, certificaciones de operadores, análisis de factibilidad o documentos equivalentes, la FGN podrá evaluar soluciones alternativas técnicamente equivalentes que permitan cumplir los Acuerdos de Niveles de Servicio y los objetivos de disponibilidad definidos en el proceso. La aceptación de dichas alternativas será evaluada por la Entidad caso por caso y no constituirá exoneración de los requisitos de disponibilidad y continuidad establecidos en el pliego de condiciones. C3.8.6. Categoría 3 Vía única terrestre dedicada con respaldo: Cada sede de la Categoría 3 deberá contar con un (1) canal WAN terrestre dedicado integrado al overlay SD-WAN cifrado y con un mecanismo de respaldo que garantice la continuidad del servicio ante falla del canal principal. El respaldo podrá proveerse mediante una segunda vía terrestre donde exista cobertura acreditada, o mediante enlace satelital LEO empresarial donde no la haya, conforme al esquema registrado para cada sede en el Anexo Técnico 1.1. La conmutación entre el canal principal y el de respaldo deberá ser automática, gestionada por el CPE SD-WAN y verificable en las pruebas de aceptación. Las condiciones de diversidad de nodo, fibra y ruta exigidas para las Categorías 1 y 2 no aplican a la Categoría 3. C3.9. Categoría 4 Acceso satelital de órbita baja: Se garantizará el servicio mediante tecnología satelital LEO empresarial, integrada al CPE SD-WAN. No se permiten tecnologías MEO, GEO, radio spread spectrum ni radio no licenciado. Podrá emplearse cualquier servicio satelital LEO empresarial disponible en el mercado, incluidos los que surjan durante la ejecución del contrato, siempre que cumpla los requisitos de desempeño establecidos en el presente Anexo Técnico. La sede operará bajo planes empresariales con priorización de tráfico (QoS) y exposición de métricas SD-WAN. El CPE permitirá la administración local de los recursos tecnológicos de la FGN (switches, impresoras, cámaras, CCTV, etc.). Cuando exista alternativa terrestre, podrá habilitarse como respaldo del LEO, con conmutación automática hacia el overlay SD-WAN.- C3.10. Categoría 5 Interconexión a Nubes públicas: Se proveerán dos (2) canales de interconexión dedicada por cada nube publica, uno terminando en cada nodo Cat 1 (Bogotá y Cali) en modo activo-activo, con capacidad simétrica acorde a los servicios productivos de la FGN. La conectividad cloud queda incluida en el overlay SD-WAN cifrado y operará bajo las mismas políticas de QoS, segmentación por VRF/VLAN, ruteo y priorización por aplicación que aplican a las sedes físicas. --

C3.11. Categoría 6 Canales complementarios: Agrupa los servicios y canales adicionales que complementan o respaldan la operación de la red corporativa de la FGN y que no hacen parte del overlay SD-WAN principal, tales como canales de Internet dedicados empresariales y enlaces de contingencia. Estos canales deberán ofrecer capacidad mínima de 100 Mbps simétricos, sin reuso, sobre fibra óptica, con disponibilidad mínima del 99,8 %, redundancia hasta el punto de entrega, canal de respaldo activo-pasivo, routers empresariales, pool mínimo de veinticinco (25) direcciones IP públicas IPv4/IPv6, y contar con monitoreo proactivo 7×24 y soporte técnico especializado. El PROVEEDOR podrá presentar, para aprobación de la FGN, alternativas de uso optimizado del direccionamiento IPv4 (traducción de direcciones, segmentación o reasignación), siempre que se garantice la operación de los servicios publicados. Los canales de esta categoría mantendrán visibilidad y capacidades de observabilidad cuando aplique, y estarán exentos de la integración y aplicación de la solución de seguridad de la Entidad dentro del presente proceso contractual.

Nota: La FGN ha definido una arquitectura de referencia que sirve como insumo orientador y establece el mínimo requerido para el presente proceso. Esta arquitectura expresa la expectativa técnica de la Entidad frente a la solución a implementar y deberá ser tenida en cuenta por el PROVEEDOR/PROVEEDOR durante la elaboración de su propuesta.

La arquitectura de referencia podrá ser ajustada, optimizada o ampliada con base en los comentarios de diseño, recomendaciones y mejoras que presenten los OFERENTES/PROVEEDOR, siempre que dichas propuestas contribuyan a fortalecer la solución y mantengan el cumplimiento de los requisitos funcionales, técnicos y de desempeño definidos por la FGN.

Se aclara que el desglose detallado del diseño, así como su consistencia técnica, viabilidad, integración, documentación y gestión, son responsabilidad exclusiva del PROVEEDOR/PROVEEDOR, quien deberá garantizar que la solución final cumpla con los lineamientos de la FGN y soporte adecuadamente la operación institucional.



	C4. Requerimientos de Instalaciones	Para la instalación del servicio El PROVEEDOR deberá: C4.1. El PROVEEDOR deberá designar personal calificado y certificado para la instalación, configuración y puesta en producción de la solución. C4.2. En el momento de inicio del contrato, se debe detallar en el cronograma las fechas de instalación del servicio en las sedes, para coordinar con los analistas de las regionales, la autorización de ingreso de los implantadores. *El equipo humano del PROVEEDOR para la prestación de los servicios de Conectividad se describe en el Anexo Técnico 6 Perfiles Profesionales, numerales P1 (Roles estratégicos transversales), P2 (Perfiles técnicos de Conectividad), P4 (Perfiles técnicos de Servicios - Mesa de Ayuda) y P9 (Reglas generales del personal). La disponibilidad operativa de cada perfil se rige por el régimen indicado en su respectiva ficha.* C4.3. Instalar, configurar y poner en funcionamiento los CPE SD-WAN, así como los equipos activos requeridos para su integración con el cableado estructurado de cada sede, garantizando el funcionamiento de los dos enlaces WAN en activo-activo-- C4.4. Identificar y desarrollar los requisitos que se encuentran detallados en el “Anexo Tecnico 7.1 - Lista_Chequeo_Entrega_Servicio”. C4.5. El PROVEEDOR deberá suministrar, instalar y mantener en operación un servidor SFTP central, debidamente licenciado, alojado en los nodos de Categoría 1, con estructura de carpetas por sede y categoría, control de acceso por perfiles y retención durante toda la vigencia del contrato. En dicho servidor se publicarán los registros fotográficos, los planos de rutas, las configuraciones y las evidencias de las pruebas de aceptación de cada sede. El pago correspondiente al servicio de conectividad SD-WAN y la aceptación final de cada sede solo procederán cuando la FGN verifique el cumplimiento del Anexo Tecnico 7.1 - Lista_Chequeo_Entrega_Servicio.
	C5. Requerimientos de Aprovisionamiento	Para atender las necesidades que surjan durante la ejecución del contrato, se requieren implementar los siguientes procedimientos de logística de aprovisionamiento para la red de la FGN: C5.1. Administración del ancho de banda: la solución propuesta debe permitir la gestión de cambios en el ancho de banda en todos los puntos de la red, en cualquiera de los sectores en que se haya definido; también deberá permitir la gestión anticipada de recursos de red necesarios para soportar el ancho de banda requerido, por un intervalo predefinido de tiempo específico, para satisfacer las necesidades puntuales y de emergencia, que demanden los usuarios. C5.2. Cambios permanentes en el ancho de banda: Los cambios deberán ser realizados por el proveedor en un tiempo máximo de siete (7) días calendario,

contados a partir de la solicitud que realizará la FGN a través de los supervisores del contrato y viabilidad técnica positiva. Para lo cual el proveedor debe:

C5.2.1. Presentar la viabilidad técnica contados desde la fecha de la solicitud de la siguiente manera:

Categoría	Descripción	Tiempo de viabilidad	Justificación
Categoría1	Datacenter / Núcleo SD-WAN (Bogotá, Cali, Nubes)	2 días calendario	Recursos del PROVEEDOR ya desplegados en sus DC.
Categoría 2	Sedes principales por ciudad (consolida Cat 2.1)	10 días calendario	Disponibilidad típica de fibra dedicada con redundancia.
Categoría 3	Ciudades intermedias / redes metropolitanas	12 días calendario	Ampliación o instalación de fibra puede requerir gestión de permisos.
Categoría 4	Resto nacional satelital LEO empresarial	15 días calendario	Activación, alineación de antenas y validación de cobertura LEO.
Categoría 5	Nubes públicas	5 días calendario	Activación de circuito ExpressRoute / FastConnect coordinada con el cloud provider. VPN B2B
Categoría 6	Canales complementarios (Internet respaldo, móvil, WiFi públicas, AP, switches, etc.)	3 días calendario (el plazo aplica al servicio activado; se ajusta a tiempos del catálogo de servicios complementarios cuando éste sea menor)	Diversidad de servicios; tiempo medio de mercado.

C5.2.2. Contemplar la proyección de crecimiento que estime la FGN y/o recomendaciones del mismo proveedor, previa validación y aprobación de la supervisión del contrato.

C5.2.3. En todos los casos, evidenciar y documentar el trámite de viabilidad técnica y de permisos para la conexión de sedes.

C5.3. Requerimientos Mínimos de los enrutadores por categorías:

Categoría	Throughput mínimo exigido	Procesamiento (pps)	Alta Disponibilidad	Puertos Ethernet mínimos	RAM mínima	Otros requerimientos
Categoría 1 Datacenter	10 Gbps	Capacidad de procesamiento acorde con el throughput exigido, acreditada por el fabricante	Requerida (HA fault-tolerant en pareja)	Mínimo 8 puertos 1GE y 4 puertos 10GE con operación simultánea a velocidad nominal	≥ 8 GB	Operación activo-activo entre Bogotá y Cali; soporte multicast; integración con ADVPN o mecanismo equivalente, FW, IPS.
Categoría 2 Ciudades principales	1 Gbps	Capacidad de procesamiento acorde con el throughput exigido	Opcional	4 GE RJ-45/SFP + 2×10GE SFP+	≥ 2 GB	DHCP en sede dimensionado según el número de usuarios registrado en el Anexo Técnico 1.1, con mínimo 4.000 direcciones y 20 % de crecimiento; soporte multicast; SD-WAN dual-link.
Categoría 3 Ciudades intermedias	100 Mbps	≥ 500 Kpps	Opcional	4 GE RJ-45 + 1 GE SFP	≥ 512 MB	DHCP en sede dimensionado según el número de

							usuarios registrado en el Anexo Técnico 1.1, con mínimo 4.000 direccion es y 20 % de crecimien to; soporte multicast; SD-WAN MPLS+Int ernet.
		Categoría 4 Resto nacional (LEO)	40 Mbp s	≥ 500 Kpps	Opciona l	4 GE RJ-45	≥ 512 MB	DHCP local en CPE; soporte multicast; integració n con terminal LEO; respaldo terrestre cuando aplique.
		Categoría 5 Nubes públicas (Azure ExpressRo ute, OCI FastConne ct, VPN B2B)	5 Gbps por canal dedic ado (o el contr atad o si supe ra 5 Gbps); VPN B2B segú n ficha del servi cio	N/A interco nexión gestion ada por cloud provide r o por túnel cifrado en el caso de VPN B2B	Requeri da: 2 canales por nube en activo-activo (1 Bogotá + 1 Cali) para Expres sRoute y FastCo nnect; VPN B2B redund ante con	Hand-off según oferta cloud (Express Route / FastCon nect) o interfaz física disponibl e para VPN B2B	N/A (servicio gestion ado)	Segmenta ción VRF/VLA N; cifrado overlay; políticas QoS y ruteo iguales a sedes físicas; VPN B2B con IPsec AES-256, IKEv2, PFS y protecció n contra replay.

			dos extremos				
Categoría 6 Canales complementarios	≥ 100 Mbps simétricos (escalable)	≥ 250.000 pps	Sí – Redundancia hasta el punto de entrega y respaldo activo-pasivo-	Mínimo 2 puertos Ethernet Gigabit (WAN/LAN)	4 GB	Router empresarial (no SOHO), soporte IPv4/IPv6, pool mínimo de 25 IP públicas, monitoreo proactivo 7×24, soporte técnico especializado, herramienta de visibilidad y optimización de ancho de banda	

C5.4. Los equipos CPE SD-WAN objeto del presente proceso deberán soportar protocolos multicast para servicios de videoconferencia y transmisión en vivo.

C5.5. El servicio DHCP del Nivel Central (Salitre) está excluido de este requerimiento. Para todas las demás sedes, la solución SD-WAN deberá proveer DHCP directamente desde el CPE instalado en cada sede, conforme a los volúmenes mínimos por categoría definidos en C5.3 y a la asignación por sede del Anexo Técnico 1.1.

C5.6. Capacidades de orquestación y agregación

C5.6.1. Los equipos propuestos deberán soportar la inclusión o agregación de interfaces lógicas o físicas para conformar un enlace SD-WAN virtual, con el número mínimo de interfaces por categoría definido en C5.3.

C5.6.2. El sistema deberá soportar ajustes de SLA de rendimiento (Health Checks) para supervisar la calidad de los enlaces WAN y detectar fallos. Los ajustes deberán incluir, como mínimo:

-
- Capacidad para definir y aplicar perfiles de SLA (*health-check*) por aplicación, destino o grupo de destinos.
- Health-check probes mediante IPv4/IPv6 Ping y HTTP.
- Selección de varios destinos o servidores para sondear.
- Asociación de perfiles SLA a interfaces específicas.
- Mecanismos de monitoreo y validación compatibles con IPv4 e IPv6, o funcionalidades equivalentes soportadas por el fabricante ofertado.
-

		C5.6.3. La solución deberá permitir crear objetivos SLA que actúen como restricciones para las reglas, configurables al menos por: - Umbral de latencia. - Umbral de jitter. - Umbral de pérdida de paquetes. C5.6.4. La solución deberá permitir definir reglas que controlen la distribución de sesiones a las interfaces, con criterios mínimos de: - Origen: dirección IP y/o grupo de usuarios. - Destino: dirección IP, aplicación y/o base de datos dinámica de servicios comunes de Internet. - Estrategias de control de rutas (mejor calidad, menor costo, manual, etc.). C5.7. Optimización de transporte - La solución deberá soportar equilibrio de carga por paquete entre túneles IPSec. - La solución deberá soportar corrección de errores de reenvío (FEC) en redes superpuestas VPN, con activación selectiva por aplicación o ruta. - La solución deberá soportar reglas SD-WAN con rutas aprendidas vía BGP como destinos dinámicos. C5.8. Continuidad operativa local (resiliencia ante falla de la plataforma de administración) Los dispositivos que componen la solución deberán conservar de manera autónoma las capacidades de inteligencia, reenvío y redirección del tráfico, así como las políticas de enrutamiento previamente configuradas, de modo que la operación de la red no dependa de la disponibilidad permanente del controlador o de la plataforma de administración. En caso de falla de la plataforma de administración o de pérdida de conectividad con esta, los equipos CPE deberán continuar operando normalmente, garantizando la continuidad de los servicios y el procesamiento del tráfico conforme a las configuraciones vigentes. Las soluciones admitirán arquitecturas con plano de control y administración centralizado y descentralizada, siempre que se garantice que una contingencia sobre la plataforma de administración no afecte la operación de la red, de tal forma que no se comprometa la administración y continuidad del servicio. C5.9. Continuidad de la conectividad SD-WAN para sedes Categoría 2, 3, 4 y 5 Considerando la arquitectura híbrida de la entidad y que las sedes Categorías 2, 3 y 4 podrán conectarse directamente desde la sede a servicios SaaS y a las nubes públicas (Categoría 5: Azure ExpressRoute, OCI FastConnect y VPN B2B), la solución deberá: C5.9.1. Realizar local Internet breakout desde el CPE de la sede para tráfico autorizado por la FGN, sin requerir tránsito obligatorio por los nodos Categoría 1 ni por nodos SSE en nube cuando el usuario está dentro de la red corporativa. C5.9.2. Mantener inspección y aplicación de políticas sobre ese breakout local. Las políticas y los componentes de seguridad asociados (FW, IPS, Antimalware, Sandboxing, Filtrado Web, etc.) serán los definidos en la Ficha Técnica de Seguridad. C5.9.3. Integrarse con la solución SASE/SSE de la entidad de manera tal que: cuando el usuario esté dentro de la red corporativa, el tráfico curse por la red SD-WAN con la inspección local definida; cuando el usuario esté fuera de la red corporativa, el tráfico curse por SASE/SSE conforme a la Ficha Técnica de

		Seguridad. La especificación de cómo opera SASE/SSE corresponde a dicho Anexo de Seguridad. C5.10. Identidad y políticas basadas en usuario C5.10.1. La solución deberá integrarse con el Directorio Activo (Active Directory) y soportar políticas basadas en identidad para efectos de enrutamiento y asignación de calidad de servicio, permitiendo seleccionar rutas SD-WAN, asignar QoS y aplicar traffic shaping en función del usuario o grupo de pertenencia. C5.10.2. La solución deberá soportar autenticación local y remota integrándose con servidores RADIUS, LDAP o TACACS+ para la administración de los CPE. C5.10.3. La solución deberá integrarse con el servicio de directorio institucional para la identificación de usuarios y grupos con fines de enrutamiento y calidad de servicio, mediante los mecanismos estándar soportados por el fabricante ofertado, sin exigir un método de autenticación propietario ni un producto de directorio específico. C5.11. Calidad de servicio (QoS) y modelado de tráfico C5.11.1. Capacidad para asignar parámetros de traffic shaping mediante reglas de manera independiente. C5.11.2. Capacidad para aplicar parámetros de traffic shaping diferenciados para el tráfico en distintos sentidos de una misma conexión. C5.11.3. Capacidad para definir parámetros de traffic shaping por dirección IP en forma independiente, así como para todo el tráfico hacia una aplicación específica. C5.11.4. Capacidad para definir límites de ancho de banda máximo por tipo de tráfico, según las necesidades de la FGN. C5.11.5. Capacidad para crecimiento escalable de niveles de QoS (100 Mbps, 1 Gbps, 5 Gbps o superiores) sin reemplazo de hardware en los nodos Categoría 1. C5.12. Conectividad a Nubes Públicas (Categoría 5) C5.12.1. . La solución deberá soportar el establecimiento de túneles IPsec/IKEv2 hacia nubes públicas y entornos externos, incluyendo capacidades de NAT-Traversal (NAT-T) y mecanismos que permitan la operación mediante puertos alternativos cuando las condiciones de conectividad así lo requieran, o funcionalidades equivalentes soportadas por el fabricante ofertado. C5.12.2. Los dispositivos deberán integrarse con plataformas de nube pública (IaaS) para descubrir y actualizar dinámicamente objetos de red o direccionamiento con base en atributos, etiquetas o metadatos de los recursos cloud, mediante conectores nativos, APIs o mecanismos equivalentes soportados por el fabricante ofertado." C5.12.3. C5.13. Soporte IPv4/IPv6 e interoperabilidad C5.13.1. Los CPE deberán operar en dual-stack IPv4/IPv6 nativo en el underlay y en el overlay SD-WAN, conforme a la Resolución 1126 de 2021 del MinTIC. C5.13.2. Los CPE deberán soportar definición de objetos y reglas de enrutamiento SD-WAN tanto por CLI como por GUI, en IPv4 e IPv6. C5.14. Cifrado del transporte Todo el tráfico transportado entre sedes y nodos Categoría 1, así como entre sedes y Categoría 5, viajará cifrado en el overlay SD-WAN (IPsec/AES-256, IKEv2). El cumplimiento de los requisitos de criptografía avanzada o post-cuántica, manejo de certificados y rotación de llaves se desarrolla en la Ficha Técnica de Seguridad

	C6. Adiciones, Cancelaciones, Suspensiones, Ampliaciones temporales y traslados del servicio durante la ejecución del contrato	Durante la ejecución del contrato y para atender las necesidades operativas, de reubicación o de continuidad del servicio que surjan en cualquiera de las seis (6) categorías de red de la FGN, el PROVEEDOR deberá implementar y atender, sin costo adicional, los procedimientos descritos en este numeral, sobre las sedes y servicios listados en el Anexo Técnico 1.1 Requerimiento de sedes a conectar. Los tiempos máximos por categoría aplicables a cada procedimiento son los definidos en el Cuadro C5.2.1 del numeral C5 (Aprovisionamiento). C6.1. Suspensiones temporales C6.1.1. Cuando la FGN requiera suspender el servicio en una sede de manera temporal por adecuaciones de infraestructura, novedades de personal, mantenimientos mayores, reorganizaciones internas o causas fortuitas debidamente justificadas el PROVEEDOR deberá: C6.1.2. Suspender el cobro y la facturación de la sede durante el período suspendido, conservando la asignación de recursos (hardware en sede, configuraciones, direccionamiento IP/IPv6 y licencias) para su reactivación. C6.1.3. Mantener documentado el período de suspensión (fecha de inicio y de fin estimado) en la herramienta de gestión. C6.1.4. Reactivar el servicio en los plazos máximos definidos en el Cuadro C5.2.1 desde la solicitud de la FGN, sin requerir nueva instalación. C6.1.5. No se considerará suspensión la indisponibilidad atribuible al PROVEEDOR; ésta se gestiona bajo los Acuerdos de Niveles de Servicio. C6.2. Ampliaciones temporales Cuando la FGN requiera incrementar de manera temporal el ancho de banda u otros recursos asociados (por ejemplo, durante eventos, jornadas especiales, contingencias o picos operativos), el PROVEEDOR deberá: C6.2.1. Atender la solicitud y poner en servicio la ampliación dentro del tiempo máximo de cambio temporal definido en el Cuadro C5.2.1 por categoría. C6.2.2. Mantener inalterados los demás parámetros del servicio (QoS, segmentación, ANS). C6.2.3. Retornar al estado original al término del período solicitado, sin afectación del servicio ni nueva facturación. C6.3. Traslados del servicio Cuando la FGN requiera trasladar una sede a una nueva ubicación dentro del territorio nacional por reubicación, emergencia, crecimiento, cambio de personal o reorganización institucional —, el PROVEEDOR deberá: C6.3.1. Ejecutar el traslado conservando la categoría asignada o reclasificándola con base en la nueva ubicación, lo cual deberá quedar reflejado en el Anexo Técnico 1.1 actualizado. C6.3.2. Realizar las pruebas de aceptación técnica (PAT) según el Anexo Técnico 7 Protocolo de Transición. C6.3.3. Atender los tiempos máximos por categoría definidos en el Cuadro C5.2.1 (instalación / activación) desde la viabilidad técnica positiva. C6.3.4. Garantizar la continuidad operativa de la sede en su ubicación original hasta el corte de servicio en la nueva ubicación, en los términos del Anexo Técnico 7.

		C6.3.5. Hasta el veinte por ciento (20 %) del total de sedes registradas en el Anexo Técnico 1.1 a la firma del contrato podrá ser objeto de traslado durante la vigencia del contrato, sin generar costos adicionales para la FGN. C6.4. Cancelaciones definitivas Cuando la FGN requiera cancelar definitivamente el servicio en una sede por cierre, fusión, reestructuración o decisión institucional —, el PROVEEDOR deberá: C6.4.1. Atender la cancelación dentro del tiempo máximo definido en el Cuadro C5.2.1. C6.4.2. Suspender la facturación a partir de la fecha efectiva de cancelación. C6.4.3. Retirar los equipos y elementos de su propiedad de la sede dentro de los plazos del Anexo Técnico 7 Protocolo de Transición (numeral T8, Retirada y Desmonte). C6.4.4. Liberar las direcciones IP públicas asignadas a la FGN y entregar la documentación final del servicio cancelado. C6.5. Adiciones (incorporación de nuevas sedes) Para la incorporación de nuevas sedes durante la ejecución del contrato, el PROVEEDOR deberá: C6.5.1. Atender los plazos definidos en el Cuadro C5.2.1 (viabilidad técnica) y Cuadro C5.3 (capacidades mínimas) según la categoría asignada a la nueva sede. C6.5.2. Cobrar exclusivamente por los servicios efectivamente activados a partir de la fecha de aceptación de cada nueva sede. C6.5.3. Actualizar el Anexo Técnico 1.1 con los datos de la nueva sede y su categoría. C6.6. Trazabilidad y reporte C6.6.1. En todos los casos del presente numeral, el PROVEEDOR deberá evidenciar y documentar el trámite de viabilidad técnica, la gestión de permisos, las ventanas de mantenimiento y los resultados, en la herramienta de monitoreo y gestión definida en el numeral C9 del presente Anexo. Los reportes mensuales de cumplimiento incluirán el detalle de suspensiones, ampliaciones, traslados, cancelaciones y adiciones del período.
	C7. Clases de servicio requeridos	La Red Categoría 1 (C3.1 – Datacenter / Núcleo SD-WAN) presenta los menores niveles de retardo, al concentrar los núcleos activos activos ubicados en los datacenters de Bogotá, Cali y las interconexiones con nubes públicas. En esta categoría, el retardo intradatacenter es prácticamente despreciable (hasta 1 ms), mientras que el retardo entre datacenters a nivel nacional se mantiene dentro de los 20 ms. Las interconexiones dedicadas con nubes públicas presentan retardos de hasta 30 ms y las salidas a Internet nacional e internacional cercano alcanzan valores máximos de 40 ms y 80 ms respectivamente, con una variación de retardo controlada para soportar servicios de datos, voz y videoconferencia. La Red Categoría 2 (C3.2 – Sedes principales en ciudades capitales) ofrece conectividad de alta calidad entre las sedes estratégicas de la entidad y los nodos Cat 1, mediante enlaces dedicados redundantes sobre fibra óptica y operación activo-activo del overlay SD-WAN. En esta categoría, el retardo intraciudad se mantiene por debajo de 5 ms y el retardo entre las sedes Cat 2 y los núcleos Cat 1 no supera los 30 ms, permitiendo una baja variación de retardo y garantizando la prestación estable de los servicios misionales con atención a usuarios.

Por su parte, la Red Categoría 3 (C3.3 – Redes metropolitanas y ciudades intermedias) está diseñada para integrar las sedes seccionales a su sede principal local y a los nodos Cat 1, combinando enlaces MPLS e Internet en modo activo-activo dentro del SD-WAN. En esta categoría, los retardos intraciudad y metropolitanos oscilan entre 10 y 15 ms, mientras que el retardo hacia los núcleos nacionales Cat 1 puede llegar hasta 50 ms y hacia las nubes públicas hasta 60 ms. La variación de retardo se mantiene controlada hasta 30 ms, incluso durante eventos de conmutación o failover, garantizando continuidad operativa.---

Tabla No.5. Requerimientos de máximo retardo

Categoría de red	Tipo de trayecto	Escenario típico	IPTD máximo	IPDV máximo
C3.1 – Cat 1 Datacenter / Núcleo SD-	Intra-datacenter / campus	Dentro del mismo DC o campus	≤ 1 ms	≤ 5 ms
C3.1 – Cat 1	Inter-datacenter	Bogotá ↔ Cali (activo-activo)-	≤ 20 ms	≤ 10 ms
C3.1 – Cat 1	Cat 1 ↔ Nube pública	Interconexión dedicada	≤ 30 ms	≤ 15 ms
C3.2 – Cat 2 Sedes principales (	Intra-ciudad	Sede ↔ nodo del proveedor	≤ 5 ms	≤ 10 ms
C3.2 – Cat 2	Cat 2 ↔ Cat 1	Enlaces redundantes activo-activo-	≤ 30 ms	≤ 20 ms
C3.3 – Cat 3 Redes	Intra-ciudad / metropolitano	Sede ↔ sede principal local (Cat 2)	≤ 10 ms	≤ 15 ms
C3.3 – Cat 3	Cat 3 ↔ Cat 2	Fibra dedicada metropolitana	≤ 15 ms	≤ 20 ms
C3.3 – Cat 3	Cat 3 ↔ Cat 1	SD-WAN activo-activo (MPLS + Internet)--	≤ 50 ms	≤ 30 ms
C3.3 – Cat 3	Cat 3 ↔ Nube pública	Tránsito vía Cat 1	≤ 60 ms	≤ 30 ms

Para las sedes conectadas mediante tecnología satelital de Órbita Baja (LEO), el proveedor deberá garantizar un retardo extremo a extremo (IPTD) promedio no superior a 100 milisegundos, pudiendo alcanzar hasta 150 milisegundos en escenarios de congestión o condiciones atmosféricas adversas, manteniendo valores de variación de retardo (IPDV) acordes con la prestación de servicios de datos, voz y videoconferencia.

CLASE	IPTD máximo recomendado para soluciones de orbita baja LEO.
Soluciones de orbita baja / empresarial	≤ 100 ms

	Soluciones de Orbita baja LEOen condiciones degradadas (clima, handover satelital)	≤ 150 ms

Fuente: Subdirección de TIC FGN

Nota: Los valores de IPDV o variación de retardo establecidos en la Tabla No. 5 deberán interpretarse y aplicarse de conformidad con el Anexo Técnico 5 – Acuerdo Niveles de Servicio, según el trayecto, categoría y tecnología correspondiente. En caso de diferencia, para efectos de medición, cumplimiento y aplicación de descuentos prevalecerán los parámetros establecidos en el Anexo Técnico 5.

Los routers objeto del presente proceso deberán cumplir con la funcionalidad para definir diferentes calidades de red, para los diferentes servicios asociados, acorde con las necesidades de los usuarios y servicios.

En síntesis, el PROVEEDOR deberá garantizar la prestación de servicios de voz, datos y videoconferencia; éste último con equipos multimedia gestionados en esta solución.

C8. Requerimientos de Topología

C8.1. Tipo de topología

La FGN adopta una topología híbrida SD-WAN tipo Dual-Hub Activo-Activo con Cloud On-Ramp y ADVPN bajo demanda.

La referencia a ADVPN constituye una funcionalidad de referencia y no la exigencia de una tecnología o fabricante específico. Se aceptarán tecnologías o mecanismos equivalentes que proporcionen capacidades funcionales iguales o superiores para el establecimiento dinámico y automático de túneles entre sedes (spoke-to-spoke), bajo demanda y sin intervención manual, con selección inteligente de rutas, cifrado, control centralizado y operación integrada dentro de la arquitectura SD-WAN. Toda mención a ADVPN en el presente Anexo Técnico se entenderá referida a dicha capacidad funcional.

Las características fundamentales son:

C8.1.1. Dual-Hub Activo-Activo: dos nodos primarios Categoría 1 ubicados en el Datacenter Nivel Central (Bogotá) y el Datacenter Cali, operando simultáneamente con políticas de balanceo y conmutación automática definidas por la FGN.

C8.1.2. Multi-Cloud edge (Categoría 5): las nubes públicas Microsoft Azure y Oracle Cloud Infrastructure se integran como hubs adicionales a través de Azure ExpressRoute, OCI FastConnect y/o VPN B2B, con doble homing a Bogotá y Cali.

C8.1.3. Spokes dual-link: las sedes Categoría 2 y 3 se conectan a ambos hubs Categoría 1 mediante dos enlaces independientes (WAN dedicado + Internet o MPLS + Internet, según la categoría).

C8.1.4. Spokes single-link satelital: las sedes Categoría 4 se conectan mediante un enlace LEO empresarial integrado al CPE SD-WAN, con respaldo terrestre cuando exista cobertura.

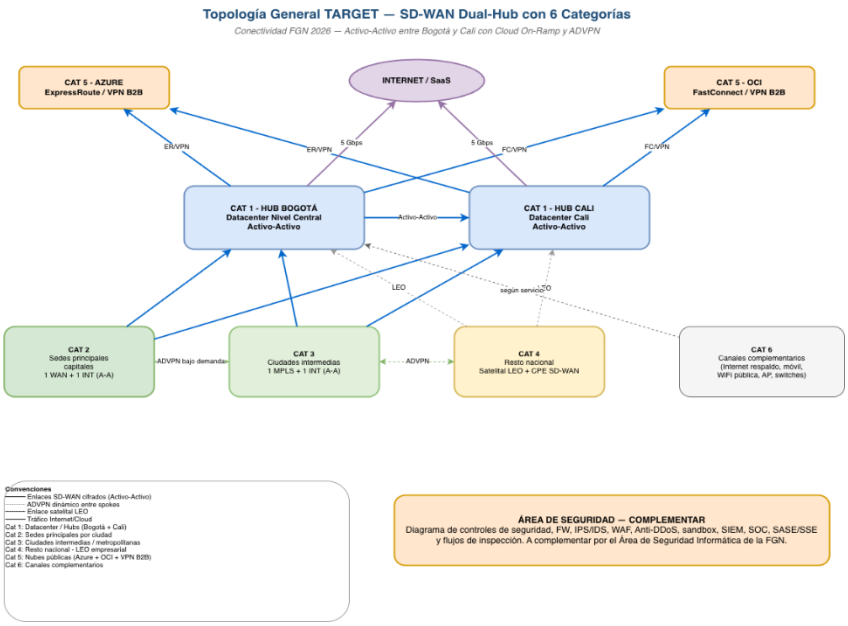
C8.1.5. La solución deberá soportar mecanismos dinámicos de establecimiento de túneles VPN entre sedes (*spoke-to-spoke*), bajo demanda y sin intervención manual, permitiendo la comunicación directa entre nodos cuando las condiciones

operativas lo requieran. Se aceptarán tecnologías o mecanismos equivalentes soportados por el fabricante ofertado, siempre que proporcionen capacidades funcionales iguales o superiores para el establecimiento dinámico de túneles dentro de la arquitectura SD-WAN.

C8.1.6. Local Internet breakout: cada CPE permite salida directa a Internet/SaaS desde la sede según política aprobada por la FGN, sin tránsito obligatorio por DC.

C8.1.7. Categoría 6 canales complementarios: se integran al overlay SD-WAN cuando el servicio activado lo permita; los demás se gestionan bajo los ANS específicos del catálogo de servicios complementarios.

Diagrama 1 - Topología General TARGET (6 Categorías)



Vista completa de la arquitectura objetivo: dos hubs Categoría 1 en Bogotá y Cali operando activo-activo, conexión a las nubes Categoría 5 (Azure y OCI, Canal dedicado, VPN B2B), spokes Categoría 2/3/4 con sus enlaces correspondientes, ADVPN dinámico entre sedes y placeholder para los componentes que aporta el Anexo de Seguridad.

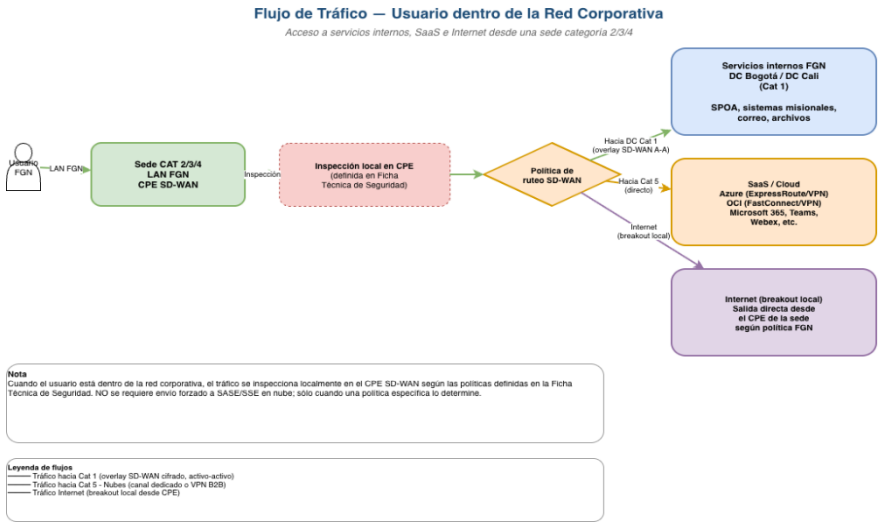
C8.2. Esquema de contingencia y resiliencia

Entre la red del PROVEEDOR y los centros de comunicaciones de la FGN se instalarán los enlaces que soporten las Categorías 1, 2, 3, 4 y 5 con los esquemas de contingencia necesarios para garantizar el cumplimiento de los ANS exigidos en el numeral C16 del presente Anexo. Para las sedes Categoría 4 que requieran conexión específica con la ciudad capital (Categoría 2 más cercana), el PROVEEDOR deberá garantizar la conmutación automática vía SD-WAN. En caso de degradación o falla severa de uno de los hubs Categoría 1, el otro asumirá la carga total mediante balanceo geográfico, sin intervención manual y sin afectación del servicio.

C8.3. Categorías de priorización (QoS)

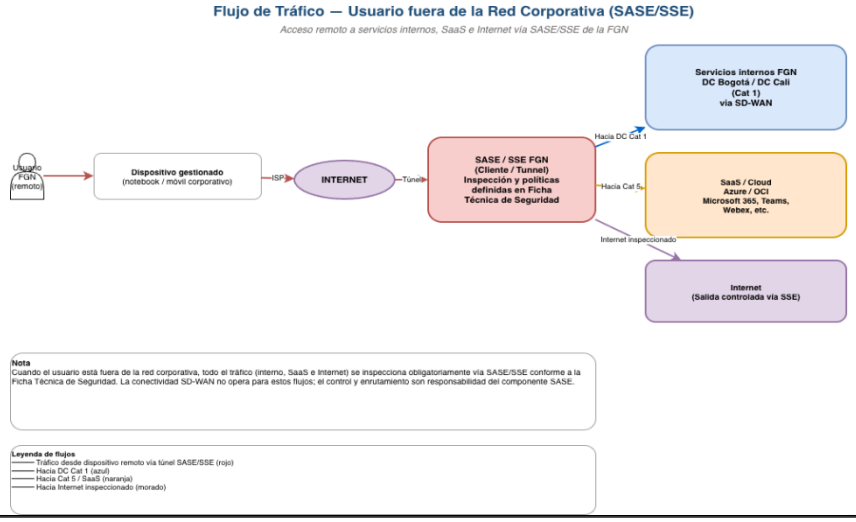
Se requiere implementar como mínimo cinco (5) categorías de priorización de tráfico (clases de servicio) configurables por sede. Para asociar las aplicaciones de software de la FGN a dichas categorías, el PROVEEDOR acordará la distribución con la supervisión del contrato durante el período de transición.

Diagrama 2 Flujo de tráfico: usuario en red corporativa



Cuando un usuario de la FGN se encuentre conectado a la red corporativa en una sede Categoría 2, 3 o 4 y trate de acceder a servicios internos, SaaS o Internet, el flujo será: el tráfico parte del usuario hacia el CPE SD-WAN de la sede, el CPE aplica las políticas de inspección locales (las cuales se complementan en la Ficha Técnica de Seguridad), y la política de ruteo SD-WAN determina el destino: servicios internos hacia los hubs Categoría 1 (overlay cifrado activo-activo Bogotá/Cali), SaaS y nube de la entidad por canal directo Categoría 5 (canales dedicados o VPN B2B), o Internet general por breakout local desde el CPE de la sede.

Diagrama 3 Flujo de tráfico: usuario fuera de la red corporativa (SASE/SSE)



		Cuando un usuario se encuentre fuera de la red corporativa de la FGN (teletrabajo, viaje, sede ajena), el dispositivo gestionado establecerá un túnel hacia la solución SASE/SSE de la entidad. Todo el tráfico (interno, SaaS e Internet) se inspeccionará obligatoriamente conforme a la Ficha Técnica de Seguridad, y desde el SASE se enrutará a servicios internos (Categoría 1), SaaS y nubes (Categoría 5), o Internet inspeccionado. La conectividad SD-WAN no opera para estos flujos remotos; la responsabilidad de inspección y enrutamiento corresponde al componente SASE/SSE descrito en el Anexo de Seguridad. C8.4. Diseño detallado del PROVEEDOR La arquitectura aquí descrita y los diagramas son insumo orientador y mínimo requerido. El PROVEEDOR podrá ajustarla, optimizarla o ampliarla en su diseño detallado, conservando la operación dual-hub activo-activo, la categorización de las sedes del Anexo Técnico 1.1, los ANS del numeral C16 y la integración con el Anexo de Seguridad. Toda variación deberá ser aprobada por la FGN dentro del Plan Detallado de Transición (Anexo Técnico 7).
	C9. Requerimientos de Gestión de Red (Operación)	C9.1. Durante la ejecución del contrato, el PROVEEDOR deberá suministrar, configurar y operar una plataforma de monitoreo que actuará como punto de contraste frente a la herramienta de Observabilidad institucional, la cual constituye el sistema oficial de verificación del cumplimiento de los Acuerdos de Niveles de Servicio (ANS). La modalidad de despliegue de la plataforma del PROVEEDOR (on-premise, nube o híbrida) queda a su discreción, siempre que cumpla con: (i) soberanía del dato (Ley 1581 de 2012 y Circular Externa 008 de 2017 SIC), (ii) alta disponibilidad equivalente a los ANS exigidos, (iii) integración técnica con la herramienta de Observabilidad mediante los conectores y protocolos que esa plataforma defina, y (iv) acceso permanente para mínimo diez (10) funcionarios de la Subdirección de TIC. En caso de discrepancia entre la plataforma del PROVEEDOR y la herramienta de Observabilidad, prevalecerá esta última como fuente oficial. C9.2. La plataforma de monitoreo debe permitir a la Subdirección de TIC de la FGN contar con una herramienta de seguimiento y verificación del cumplimiento de los Acuerdos de Niveles de Servicio (ANS) y apoyarse en ésta para actividades de monitoreo, diagnóstico y verificación del cumplimiento de las configuraciones y el funcionamiento de todos los equipos de conectividad y seguridad suministrados por el proveedor en los nodos instalados en las sedes de la FGN, está información será contrastada con la herramienta de observabilidad de la FGN. C9.3. Esta plataforma deberá garantizar mediante un aplicativo especializado o un browser que la FGN utilice para acceder en línea a las herramientas debidamente licenciadas, consultar su información estadística y otras funciones de la plataforma suministrada. Para mínimo diez (10) funcionarios de la entidad, los cuales realizarán funciones de seguimiento, monitoreo, aprobación de disponibilidad de acuerdo con los perfiles solicitados por el supervisor del contrato. C9.4. La plataforma debe proveer mapas del estado de la red, verificación de las configuraciones, análisis remoto de tráfico, utilizando los protocolos SNMP v2, v2c y v3, RMON, http, https y SSH v2.

		C9.5. El monitoreo y generación de estadísticas de cada una de las sedes de la red, en tiempo real, debe incluir como mínimo: • Despliegue de la topología de la red, donde se muestre la disponibilidad de todas las sedes conectadas. • El consumo por aplicación, el tipo de protocolo, el puerto y la dirección IP. • Agrupamiento por Seccionales o departamentos. • Configuración de diferentes roles y perfiles de gestión. • Captura y visualización de fallas detectadas en el monitoreo de los equipos • Restauración de las configuraciones de los dispositivos (realizar Backup de la configuración de los dispositivos y en caso de falla la misma herramienta restaurar la configuración correspondiente) • Monitoreo de CPU y memoria de los dispositivos • Monitoreo de Colas y políticas de servicio aplicados en los Dispositivos • Monitoreo de disponibilidad de los equipos • Monitoreo de tiempos de respuesta desde el punto central hacia c/u de los equipos • Monitoreo de ancho de banda o 'throughtput' de las interfaces • Monitoreo de Errores de las interfaces • Monitoreo de tráfico Broadcast de las interfaces • Monitoreo de tráfico Multicast de las interfaces • Monitoreo de calidad de servicio aplicada en los dispositivos • Monitoreo de perdida de paquetes desde c/u de los equipos hasta los puntos centrales en Bogotá. • Monitoreo de Retenibilidad del servicio. • El PROVEEDOR deberá presentar, dentro del diseño detallado de la solución, la metodología de medición del MOS y de la retenibilidad del servicio (herramienta, fórmula de cálculo, fuentes de datos, periodicidad, tamaños de muestra, umbrales de referencia y responsables), la cual deberá ser aprobada por la FGN antes de su aplicación en la operación y en los ANS. • Monitoreo y generación de alertas de las sedes sobre las clases de servicios RETARDO IPTD para conexiones terrestres y satelitales. • Análisis de tráfico por direcciones IP y/o Aplicativos por Sede (Protocolos, Puerto TCP/IP y Direcciones IP). • Notificaciones de Umbrales de CPU, Memoria, numero de Errores detectados en las interfaces, latencia de medición desde c/u de los dispositivos hacia los puntos centrales. • Notificación de degradación de latencia de los dispositivos • En los reportes de todas las mediciones realizadas se debe tener: • Histórico de la ejecución del contrato. • Generación de reporte especificando el periodo de tiempo que puede ser desde 1 hora hasta al menos el tiempo de ejecución del contrato. • Generación de Reportes en Excel y PDF • Medición de la disponibilidad exigida con la posibilidad de acceso en línea para la validación de las sedes por Seccional • Registro y seguimiento de los incidentes reportados en el grupo de gestión del contrato del contrato. • Registro de Tickets asociados al servicio de conectividad ofrecido

		• Notificación al momento de aprobar la disponibilidad de todos los sitios para cada zona por parte de los analistas de sistemas de la FGN. • Registro y reportes de los servicios DHCP de cada uno de los CPEs SD-WAN gestionados en el contrato. • Registro, monitoreo y reportes de disponibilidad de servicio de videoconferencia • Monitoreo y reportes de disponibilidad de equipos plataforma de seguridad • Envío de alertas por medio correo electrónico y mensajes SNMP o SMS • La aplicación debe contar niveles de seguridad (agrupamiento, roles y permisos). • El software debe ser licenciado. • La base de datos de la solución debe contar con seguridad y auditoría; o en su defecto, integrarse con el motor de base de datos de la fiscalía general de la Nación, conforme a las especificaciones técnicas que la entidad provea. • Se requiere que la herramienta de monitoreo registre los eventos de indisponibilidad de manera automática y almacene los logs de eventos de sistema de los enrutadores durante el periodo del contrato y por 12 meses más. C9.6. Todos los anteriores parámetros requerirán el almacenamiento de las estadísticas, durante el tiempo de ejecución del contrato y garantizar tanto la realización de backups como su almacenamiento en los equipos incluidos en la solución de conectividad, seguridad y videoconferencia; por lo tanto, el proveedor deberá suministrar los medios necesarios para dicho almacenamiento y entregarlos a solicitud de la FGN sin pérdida de información. C9.7. Estas funcionalidades, podrán ser provistas por una o varias herramientas integradas en una o más plataformas. El PROVEEDOR deberá incluir todo el hardware de uso exclusivo para este servicio, el software, soporte preventivo, soporte correctivo y el licenciamiento para su correcta operación. C9.8. Los datos utilizados para la generación de informes de gestión y análisis dentro del servicio prestado en el marco de la ejecución del contrato deberán entregarse como mínimo en archivos planos debidamente documentados y de forma periódica en medio magnético a la FGN. NOTA: La herramienta deberá implementarse y ponerse en funcionamiento, dentro de los 60 días calendario, siguientes a la suscripción el acta de inicio.
	C10. Servicio de Internet Requerido	La solución de internet requerida para los Datacenter de Bogotá y Cali es la siguiente: La solución a implementar requerida es de dos (2) servicios de internet, para lo cual se requiere que los dos (2) servicios estén integrados en la solución para permitir la distribución de tráfico de la siguiente manera: C10.1. Un (1) canal de internet de mínimo 5 Gbps de ancho de banda, provista en solución ofrecida, el cual deberá soportar los servicios de la entidad y el tráfico de internet a nivel nacional instalado en el Nivel Central de la ciudad de Bogotá.

		C10.2. Un (1) canal de internet de mínimo 5 Gbps de ancho de banda, provista en la solución ofrecida, para publicar los servicios de la entidad y soportar el acceso de internet a nivel nacional instalado en la Sede Bunker Cali. C10.3. Cada uno de los canales de internet requeridos en la solución provista sin re uso 1:1 simétrico; Full Dúplex simétrico. C10.4.El ISP del proveedor deberá acreditar interconexión con al menos un punto neutro de intercambio de tráfico (IXP) de presencia nacional, con capacidad suficiente para garantizar los niveles de servicio requeridos. Deberá presentar documentación técnica que acredite dicha conectividad, emitida por la entidad competente, en el momento de suscribir el acta de inicio del contrato y cuando la FGN lo requiera. C10.5.Para la salida de los canales exclusivos se acordará con los supervisores del contrato, las sedes que saldrán por cada una de ellas, con el fin de generar un balanceo adecuado de los canales. C10.6.La conexión será usada para el consumo de todos los servicios y sistemas de información de la FGN que están públicos hacía Internet, uso de herramientas colaborativas, navegación general de acuerdo los perfiles y lineamientos de seguridad de la Entidad. C10.7.El PROVEEDOR deberá incluir en su oferta los costos asociados a la entrega de un pool de direcciones IPv4 públicas /25 para uso de la FGN. Asimismo, deberá garantizar la adquisición de un pool IPv6 /44 ante LACNIC, en cumplimiento de la Resolución 1126 de 2021 del MinTIC, requisito necesario para dar cumplimiento al soporte dual-stack IPv4/IPv6 exigido en los Requerimientos generales de la solución del presente documento. C10.8.El monitoreo del acceso a Internet, la medición del ancho de banda, el diagnóstico e inventario de direcciones IP deberán estar incluidos en la gestión de la red mencionada mediante una IPAM dando cumplimiento también a los requerimientos expuestos en el numeral C9.
	C11. Servicio de Obras de adecuación	Son el conjunto de instalaciones que el proveedor debe realizar para garantizar la correcta operación de los equipos y medios de transmisión (del proveedor) en las sedes, sin costo adicional para la FGN, para lo cual el proveedor debe: Proveer, como mínimo, las tomas eléctricas, cableado eléctrico, canalizaciones, soportes, gabinetes o racks de comunicaciones, sistemas de puesta a tierra con sus respectivas mediciones, UPS de mínimo un (1) kVA con baterías internas selladas y libres de mantenimiento, así como las obras civiles que se requieran (canalizaciones, perforaciones, fijaciones, bases y adecuaciones) para la instalación y operación de los equipos en todas las sedes descritas en el Anexo Técnico N.° 1.1 ; adicionalmente, deberá suministrar e instalar los soportes, torres, mástiles, bases en concreto y demás obras civiles necesarias para la instalación de soluciones satelitales, garantizando su estabilidad, seguridad y correcta operación, sin costo adicional para la Fiscalía General de la Nación, con el fin de asegurar la disponibilidad y continuidad de la conexión requerida.

		C11.1. La FGN gestionará los permisos de ingreso a las sedes de la entidad, la FGN no estará obligada a gestionar permisos de instalación, realizar contratos de arrendamiento, ni solicitar autorizaciones ante terceros para la instalación. C11.2. El PROVEEDOR deberá suministrar, transportar, instalar, configurar y dejar en operación los racks de Datacenter requeridos para los nodos de Nivel Central (Datacenter Bogotá) y Cali (Datacenter), de conformidad con las especificaciones técnicas de los racks, cuando sean necesarios para el alojamiento de la plataforma de gestión, orquestación y seguridad de la solución. Dichos racks deberán cumplir, como mínimo, con las siguientes características: 42 unidades de altura (42U), ancho estándar de 19 pulgadas, profundidad mínima de 1000 mm, fabricados en acero de alta resistencia, con capacidad de carga mínima de 1.000 kg, puertas frontal y posterior perforadas con sistema de cerradura, paneles laterales desmontables, sistemas de gestión térmica y de cableado de alta densidad, barra interna de puesta a tierra, y compatibilidad con PDU, UPS y equipos activos de centro de datos. El PROVEEDOR deberá incluir, sin costo adicional para la Fiscalía General de la Nación, todas las adecuaciones eléctricas, de cableado estructurado y de energía, así como los materiales, tomas, accesorios y elementos necesarios para garantizar el correcto funcionamiento, operación continua y segura de los equipos instalados. C11.3. Es de obligatorio cumplimiento en las implementaciones eléctricas que haga el proveedor, la norma RETIE, los ductos eléctricos y de telecomunicaciones que sean necesarios instalar, deben cumplir las normas ICONTEC 1630 y aquellas vigentes relacionadas con este requerimiento. C11.4. El PROVEEDOR deberá suministrar e instalar, cuando aplique, un gabinete rack de pared con tapas laterales removibles, de capacidad mínima de catorce (14) Unidades de Rack (14U), el cual deberá incluir Unidad de Distribución de Energía (PDU) adecuada para la conexión segura de todos los equipos que conforman la solución ofertada (CPE SD-WAN, equipos de último kilómetro, dispositivos de seguridad y demás elementos requeridos). El gabinete deberá permitir la ubicación ordenada, ventilación adecuada, acceso para mantenimiento y crecimiento de la solución, e implementarse con todos sus accesorios, incluyendo sistema de puesta a tierra debidamente instalado, barra de tierra, conductores, herrajes y elementos necesarios, cumpliendo con las normas técnicas y eléctricas vigentes (RETIE y normas aplicables). Todos los racks suministrados deberán ser nuevos, no remanufacturados ni usados, y deberán entregarse con sus accesorios completos de montaje, gestión de cableado y puesta a tierra, sin generar costos adicionales para la Fiscalía General de la Nación. Nota: En el caso que el proveedor dentro de su diseño justifique técnicamente que no requiere instalar y/o suministrar rack para los equipos WAN (router, equipos de ultimo kilometro) haciendo uso de los que actualmente están instalados de propiedad de la Fiscalía General de la Nación, la entidad descontará el valor por la no instalación del rack del primer pago del servicio de la sede (una vez se garantice la aceptación de las pruebas), de la siguiente manera: se descontará el mayor valor de 3 cotizaciones, Una (1) será suministrada por el oferente, una (1) suministrada por la entidad y una (1) cotización con el valor de referencia del mercado.

		Lo anterior previa autorización de la supervisión del contrato.
	C12. Requerimientos de Mantenimiento	En el caso de requerirse por parte del proveedor un plan de mantenimiento preventivo de la Red Nacional de Telecomunicaciones, debe ser comunicado para aprobación por parte de la supervisión, con al menos un (1) mes de anticipación y tendrá que ser realizado en horarios a convenir, sin que esto implique costos adicionales para la FGN. El proveedor debe convenir el cronograma de mantenimientos, detallando tanto fechas como sedes a visitar y deberá suscribir un Acta por cada sede, en donde se consigne las actividades realizadas en el mantenimiento, la cual deberá ser entregada a los supervisores del contrato. C12.1. Alcance del mantenimiento El mantenimiento prestado por el PROVEEDOR cubrirá la totalidad de los componentes del servicio (CPE SD-WAN, equipos de borde, routers, switches core y de acceso, firewalls, antenas LEO empresariales, módems, racks, fuentes de poder, UPS, cableado estructurado, conexiones de fibra y demás elementos pasivos y activos descritos en el Anexo Técnico 1.1) en las seis (6) Categorías de red del contrato (Categoría 1 Datacenter, Categoría 2 Sedes principales, Categoría 3 Ciudades intermedias, Categoría 4 Resto nacional / LEO, Categoría 5 Nubes públicas y Categoría 6 Canales complementarios). C12.2. Mantenimiento preventivo C12.2.1. Frecuencia mínima: cuatro (4) jornadas anuales por sede o componente, sin perjuicio de actualizaciones urgentes adicionales. C12.2.2. Actividades mínimas por jornada: actualización de firmware/software a la última versión estable liberada por el fabricante; revisión y limpieza física; validación de logs, alertas y métricas SD-WAN; verificación y respaldo de configuraciones; inspección de cableado, etiquetado, polos a tierra, UPS y temperatura; pruebas de conmutación activo-activo y rendimiento sobre el overlay SD-WAN. C12.2.3. Coordinación: plan de mantenimiento entregado y aprobado por la supervisión con mínimo un (1) mes de anticipación, calendario por Categoría y sede. C12.2.4. Documentación: acta por sede o bloque de sedes con actividades realizadas, evidencias y observaciones, entregada a la supervisión dentro de los cinco (5) días hábiles siguientes a la jornada. C12.2.5. Reconocimiento ANS: las interrupciones de servicio previamente acordadas para mantenimientos preventivos no se contabilizarán en la medición de los ANS del Anexo Técnico 5. C12.3. Mantenimiento correctivo C12.3.1. Atención de incidentes: el PROVEEDOR atenderá los incidentes reportados por cualquiera de los canales de soporte (telefónico, correo, chat, portal) con la efectividad de atención y dentro de los tiempos establecidos en el Anexo Técnico 5 – Acuerdo Niveles de Servicio (ANS).

		C12.3.2. Tiempos máximos de resolución. Los tiempos máximos de resolución de incidentes y solicitudes, de acuerdo con la categoría y prioridad P1, P2 y P3, serán los establecidos en el Anexo Técnico 5 – Acuerdo Niveles de Servicio (ANS). Para efectos de medición, seguimiento, evaluación del cumplimiento y aplicación de descuentos, se aplicarán los parámetros, tiempos, rangos y demás condiciones definidos en dicho Anexo. C12.3.3. Indicadores asociados: los valores y condiciones aplicables a disponibilidad, tiempos de resolución, RTO, MTBF, interrupciones máximas, retrasos y demás indicadores sujetos a Acuerdos de Niveles de Servicio serán los establecidos en el Anexo Técnico 5 – Acuerdo Niveles de Servicio (ANS), el cual constituye la fuente aplicable para su medición contractual, evaluación de cumplimiento y aplicación de descuentos. C12.3.4. Reemplazo de equipos: los equipos defectuosos serán reemplazados con repuestos del mismo modelo o superior y la configuración restaurada desde el respaldo más reciente, sin costo adicional para la FGN. El plazo máximo de reemplazo será el establecido en el Anexo Técnico 5 – Acuerdo Niveles de Servicio (ANS) por Categoría. C12.3.5. Escalamiento: se aplicará el modelo de niveles N1-N4 definido en el Anexo Técnico 7 Protocolo de Transición (numeral T6.2) cuando ocurran fallos persistentes, rollbacks consecutivos o caídas que excedan el ANS. C12.3.6. Informe de causa raíz: entregado a la FGN dentro de los cinco (5) días hábiles siguientes al cierre de cualquier incidente clasificado como P1 o de afectación generalizada. C12.4. Actualizaciones urgentes y gestión de vulnerabilidades Cuando se identifiquen vulnerabilidades de seguridad, alertas críticas del fabricante, riesgos operacionales o cuando lo requiera la Entidad por hallazgos en su gestión de ciberseguridad, el PROVEEDOR ejecutará actualizaciones urgentes sobre los equipos afectados con notificación previa al Supervisor (severidad, alcance y ventana propuesta), procedimiento de rollback documentado y probado en laboratorio, aplicación en horarios de baja demanda (preferentemente 22:00–05:00) salvo cuando la criticidad exija intervención inmediata, verificación post-cambio y entrega de evidencia a la FGN en plazo no superior a 48 horas. Estas actualizaciones no afectarán la continuidad del servicio ni los ANS. C12.5. Reportes y trazabilidad de mantenimiento El PROVEEDOR consolidará en su informe mensual de cumplimiento de ANS (numeral C16) la siguiente información del mantenimiento del período: jornadas preventivas ejecutadas (sedes, fechas, hallazgos) clasificadas por Categoría, incidentes atendidos (cantidad, prioridad, Categoría, tiempo de resolución), reemplazos de hardware, actualizaciones urgentes aplicadas, indicadores de RTO/MTBF/disponibilidad por Categoría y plan de acción correctivo cuando aplique. Toda la información de mantenimiento se sincronizará con el sistema de CMDB del numeral C14 y con la plataforma de gestión del numeral C9.
	C13. Análisis de	El PROVEEDOR suministrará a la FGN la capacidad de observar, analizar, dimensionar y proyectar el comportamiento del tráfico de red sobre la solución contratada, con visibilidad en tiempo real e histórica, segmentada por Categoría,

	Ingeniería de Tráfico	sede, túnel SD-WAN, aplicación y usuario, integrada al ecosistema de gestión y observabilidad de la entidad y al sistema IPAM. C13.1. Modelo de análisis: continuo + estudios formales El análisis opera en dos planos: C13.2. Plano continuo (always-on): la plataforma expone telemetría, métricas y dashboards en línea para toda la red durante toda la vigencia del contrato, sin períodos ciegos. Este plano alimenta a la plataforma de gestión de C9, al sistema IPAM (numeral C10 Sistema de gestión de direcciones IP (IPAM)) y a la plataforma de Observabilidad de la FGN. C13.3. Plano de estudios formales: el PROVEEDOR consolida y entrega informes con periodicidad mínima: - Línea base inicial al cumplirse tres (3) meses desde el cierre del Período de Transición (Anexo Técnico 7). - Estudio anual durante toda la vigencia del contrato. - Estudios a demanda cuando la FGN lo requiera (incidentes recurrentes, planeación de capacidad, hallazgos de ciberseguridad, cambios de cloud provider, masivos de sedes). - Estudios post-evento después de hitos relevantes: incorporación masiva de sedes, traslados, cambios de proveedor cloud o reestructuración de aplicaciones. C13.4. Capacidades mínimas exigibles a la solución La plataforma del PROVEEDOR deberá exponer, sin costo adicional: - Identificación L7 / DPI de aplicaciones, con catálogo de aplicaciones empresariales (SaaS, voz, video, almacenamiento, mensajería, P2P) y reconocimiento de tráfico cifrado por metadatos cuando la inspección SSL no esté habilitada. - Métricas operativas por enlace y por túnel: throughput, ancho de banda consumido, picos, promedios, variaciones, latencia, jitter, pérdida, retenibilidad y disponibilidad. - Métricas de los CPE: uso de CPU, memoria, sesiones concurrentes, estado de túneles SLA, eventos de conmutación / failover. - - Telemetría de túneles VPN dinámicos sede a sede (spoke-to-spoke): identificación de origen y destino, estado del túnel, duración, volumen de tráfico cursado, utilización y condiciones de establecimiento o activación automática.Telemetría de Categoría 5 (Cloud On-Ramp): comportamiento de los canales Azure ExpressRoute, OCI FastConnect y VPN B2B; latencia, throughput y errores hacia las nubes. - Telemetría del breakout local en los CPE: tráfico salido directamente a Internet, top de aplicaciones SaaS por sede. - Identificación por usuario y grupo mediante integración con Active Directory para los flujos donde aplique. - Detección automática de anomalías y alertas (cambios bruscos de patrón, aplicaciones no autorizadas, sedes con saturación).

- Histórico mínimo de un (1) año en línea consultable desde la consola, con respaldo de datos crudos durante toda la vigencia del contrato y entregables al cierre.

C13.5. Cobertura mínima por Categoría

Los estudios formales analizarán como mínimo las siguientes muestras, sin perjuicio de la observabilidad continua que cubre el 100 % de la red:

Categoría	Cobertura mínima del estudio formal
Categoría 1 Datacenter / Núcleo SD-WAN	100 % de los nodos (Bogotá + Cali, incluidos los canales hacia las nubes públicas).
Categoría 2 Sedes principales por ciudad	Mínimo 25 sedes representativas de las ciudades capitales.
Categoría 3 Ciudades intermedias	Mínimo 15 sedes distribuidas geográficamente.
Categoría 4 Resto nacional / LEO empresarial	Mínimo 10 sedes, incluyendo al menos 3 con cobertura LEO única.
Categoría 5 Nubes públicas	100 % de los canales activos (Azure ExpressRoute, OCI FastConnect y VPN B2B).
Categoría 6 Canales complementarios	Mínimo 10 servicios o enlaces activos al momento del estudio.

C13.6. Productos del estudio formal

Cada estudio formal entregará a la supervisión:

- Caracterización del tráfico por Categoría, sede, aplicación y usuario.
- Curvas de utilización y proyección (próximos 6, 12 y 24 meses) por enlace y por nodo Categoría 1.
- Mapa de tráfico hacia Categoría 5 (Azure / OCI / VPN B2B): cuánto va a cada nube, por qué canal y con qué QoS.
- Análisis de *breakout* local y de los mecanismos dinámicos de establecimiento de túneles VPN *spoke-to-spoke*, identificando cuánto tráfico evita el tránsito por nodos centrales y bajo qué condiciones se activan dichas comunicaciones.
- Identificación de las diez (10) aplicaciones críticas con mayor consumo de ancho de banda por sede.
- Detección de patrones anómalos: subutilización, saturación, aplicaciones no autorizadas y tráfico hacia destinos sospechosos (esta última coordinada con la Ficha Técnica de Seguridad).
- Recomendaciones de optimización por Categoría y por sede: ajustes de QoS, ampliaciones, reasignaciones de canales, optimización de mecanismos dinámicos de comunicación entre sedes, *traffic shaping* y ajustes de políticas de *breakout* local.
- Insumo para C6 Adiciones, Cancelaciones, Suspensiones, Ampliaciones temporales y Traslados.
- Formatos de entrega: Excel, PDF y exportación vía API; datos crudos disponibles para auditoría.

C13.7. Provisión de herramientas e infraestructura

		El PROVEEDOR suministrará sin costo adicional para la FGN durante toda la vigencia del contrato el hardware, el software y el licenciamiento necesarios para habilitar estas capacidades: consolas SD-WAN, módulos analíticos, motores DPI, dashboards, herramientas de generación de reportes y APIs de integración. No se aceptan herramientas externas dedicadas para suplir estas funciones; toda la analítica se entregará desde la propia plataforma SD-WAN integrada con las plataformas de la entidad. Mínimo diez (10) cuentas de acceso para funcionarios de la FGN con perfiles diferenciados (consulta, análisis, administración). C13.8. Compromiso de mejora continua A partir del segundo año de operación, los estudios anuales incluirán un componente de comparativa interanual y un roadmap de optimización propuesto por el PROVEEDOR, alineado con la evolución de la entidad, la incorporación de nuevas aplicaciones misionales y los lineamientos de eficiencia operacional definidos por la Subdirección de TIC.
	C14. Inventario de los servicios prestados.	El proveedor deberá mantener actualizado el inventario de los equipos suministrados en los servicios requeridos en el contrato en la CMDB de la Entidad. Nota: El proveedor deberá suministrar el inventario después del periodo de transición, el cual deberá ser entregado a la FGN finalizado este periodo.
	C15. Pruebas de Aceptación del Servicio	Certificar, sede por sede y por Categoría, que el servicio entregado por el PROVEEDOR cumple las especificaciones técnicas, los Acuerdos de Niveles de Servicio del numeral C16, las políticas de seguridad definidas en la Ficha Técnica de Seguridad y las configuraciones de administración acordadas, antes de ser puesto en operación productiva. C15.1. Plan de Pruebas instrumento único El plan de pruebas de aceptación se materializa en la FASE 4 del Anexo Técnico 7.1 Lista de Chequeo de Entrega del Servicio, con los siguientes 15 puntos de control mínimos por sede:

#	Punto de control	Referencia
4.1	Notificación al Supervisor con ≥ 72 horas (correo + tickets).	Anexo 7, T10.1 paso 1
4.2	Ventana de mantenimiento programada (preferente 22:00–05:00).	Anexo 7, T10.1 paso 3
4.3	Backup de configuración del equipo o enlace anterior entregado a FGN TIC.	Anexo 7, T10.1 paso 4
4.4	PAT Disponibilidad ≥ 99,9 % (ping continuo, 15 minutos).	Anexo 7, T11
4.5	PAT Latencia (RTT) e IPDV dentro de los umbrales por categoría y trayecto definidos en la Tabla No. 5 del numeral C7 y, para Categoría 4, en el cuadro de soluciones de órbita baja del mismo numeral.	Anexo 7, T11

		4.6	PAT Verificación de variación de retardo, IPDV o jitter (iPerf3 UDP, 10 minutos): el resultado deberá cumplir el umbral establecido en el Anexo Técnico 5 – Acuerdo Niveles de Servicio, de acuerdo con la categoría de la sede, el tipo de trayecto y la tecnología del enlace evaluado. La prueba se considerará satisfactoria cuando el valor medido sea igual o inferior al umbral aplicable.
		4.7	PAT Pérdida de paquetes ≤ 0,5 % (iPerf3 UDP, 10 minutos).
		4.8	PAT Ancho de banda ≥ 90 % del contratado (iPerf3 TCP, 5 minutos).
		4.9	PAT 100 % de aplicaciones críticas FGN accesibles (manual, 30 minutos).
		4.10	PAT Políticas de seguridad activas (FW, segmentación VLAN, cifrado overlay).
		4.11	PAT Sede gestionable desde consola SD-WAN central.
		4.12	Acta de Activación de Sede suscrita (analista de sistemas seccional o regional).
		4.13	Registros fotográficos, planos de ruta y configuraciones publicados en SFTP central.
		4.14	Registros fotográficos por sede cargados al SFTP central del PROVEEDOR.
		4.15	Verificación del cumplimiento de umbrales por Categoría asignada a la sede.

			Anexo 7, T11
			Anexo 7, T11
			Anexo 7, T11
			Anexo 7, T11
			Anexo 7, T11 / Ficha Técnica de Seguridad
			Anexo 7, T11
			C4 / Anexo 7, T7
			C4 (Requerimientos de Instalaciones)
			C4
			C16 / Anexo 7, T11

C15.2. Criterios de aceptación por Categoría

Los umbrales mínimos exigidos durante la PAT se calibran por la Categoría asignada a la sede en el Anexo Técnico 1.1, con los valores establecidos en C16 (ANS). Los parámetros se miden con las herramientas indicadas en C9. La FGN podrá ampliar los criterios cuando la sede sea crítica o cuando, por su perfil, requiera pruebas funcionales adicionales (voz / videoconferencia / aplicaciones misionales).

C15.3. Ejecución y herramientas

- Herramientas: las pruebas se realizan con las herramientas que provee el PROVEEDOR (consolas SD-WAN, módulos analíticos, iPerf3, generadores de tráfico, scripts ICMP, sondas) sin costo adicional para la FGN, durante todo el período de aceptación y posteriormente cuando la entidad las requiera.
- Participación: la ejecución requiere la presencia y participación del personal técnico de la Subdirección de TIC de la FGN y/o del analista de sistemas seccional / regional autorizado.
- Plazo máximo de ejecución de las PAT: dos (2) horas desde el inicio del corte conforme al Anexo 7, T10.1 paso 6.

- Notificación de no conformidades: la FGN comunicará por escrito (sistema de tickets) al PROVEEDOR los cambios, no conformidades o detalles a cambiar.

C15.4. Resultado: declaración go / no-go y firma del Acta

Al concluir las PAT en una sede:

- Go: si la totalidad de los puntos de control de la FASE 4 están en estado "Cumplido" y el resultado se ajusta a la Categoría de la sede, se firma el Acta de Activación de Sede (Anexo 7, T7). No se aceptan actas de instalación ni de recibo a satisfacción como sustituto del Acta de Activación.
- No-go: si uno o más puntos fallan, se activa el Protocolo de Rollback (Anexo 7, T12) el servicio anterior se restablece y el corte se reprograma con al menos cinco (5) días hábiles de antelación, previa corrección documentada.

C15.5. Segunda ronda de pruebas

Para los puntos no cumplidos en la primera ronda, el PROVEEDOR cuenta con siete (7) días calendario para perfeccionar la instalación. Posteriormente se ejecuta una segunda ronda restringida exclusivamente a los puntos pendientes. Si la segunda ronda tampoco supera los criterios, la FGN podrá aplicar las penalidades del numeral C16 y/o reclasificar la sede para reprogramación bajo el procedimiento del numeral C6 (Adiciones, Cancelaciones, Suspensiones, Ampliaciones temporales y Traslados).

C15.6. Trazabilidad y publicación

- Evidencia: todas las mediciones, capturas de pantalla, logs, planos, registros fotográficos y configuraciones de cada sede deberán publicarse en el servidor SFTP central descrito en el numeral C4 (Requerimientos de Instalaciones), con clasificación por sede y por Categoría.
- Acta digital: el Acta de Activación, sus evidencias y los resultados de la Lista de Chequeo se conservan en la herramienta de gestión documental de la FGN para auditoría, durante toda la vigencia del contrato y los plazos de retención aplicables.
- Reporte mensual: los resultados consolidados de las PAT del período se incluyen en el reporte mensual de cumplimiento de ANS (numeral C16).

C15.7. Pruebas específicas por Categoría

Para reflejar la diversidad de la red SD-WAN, las PAT incluyen pruebas particulares según la Categoría:

- Categoría 1 (Datacenter / Núcleo): prueba de operación activo-activo Bogotá ↔ Cali; conmutación geográfica ante falla de un hub; pruebas de los canales hacia Categoría 5; pruebas de switching core con HA.
- Categoría 2 y 3 (sedes terrestres): prueba de conmutación entre los dos enlaces (WAN + Internet o MPLS + Internet) en activo-activo; verificación de diversidad de fibra y nodo; pruebas QoS por aplicación.

		- Categoría 4 (LEO empresarial): pruebas de estabilidad satelital bajo condiciones meteorológicas distintas (cuando sea factible programarlas); validación del CPE SD-WAN integrando el terminal LEO; pruebas de respaldo terrestre cuando exista. - Categoría 5 (Nubes públicas): pruebas de los dos canales (ExpressRoute / FastConnect / VPN B2B) en activo-activo terminados en Bogotá y Cali; latencia y throughput contra los servicios productivos en Azure y OCI. - Categoría 6 (Canales complementarios): pruebas según la ficha del servicio activado.
	C16. Acuerdos de Niveles de Servicios (ANS)	Remitirse al 5. ANEXO TECNICO 5. ACUERDO NIVELES DE SERVICIO
	C17. Requerimientos de Gestión de Tráfico de Internet mediante Plataforma SD-WAN	C17.1. Gestión integrada de ancho de banda La solución deberá incluir de manera nativa la administración del ancho de banda en todos los enlaces de Internet de los nodos Categoría 1 (Bogotá y Cali) y de las sedes Categorías 2, 3, 4, 5 y 6. Como mínimo: - Optimización automática mediante traffic shaping, policing, colas inteligentes y algoritmos dinámicos de priorización. - Asignación de ancho de banda por aplicación, categoría de tráfico, usuario, grupo (Active Directory para identificación, no para autorización de seguridad), VLAN, VRF o dirección IP. - Balanceo de carga y selección dinámica de ruta basada en mediciones continuas de SLA (latencia, jitter, pérdida, disponibilidad, retenibilidad). - Soporte mínimo de 10 Gbps de tráfico legítimo gestionado en cada nodo Categoría 1, con margen de crecimiento del 50 %. - Direcciones IP gestionables por sede conforme al dimensionamiento del Cuadro C5.3 y al Anexo Técnico 1.1, y 4.000 servidores publicados entre los nodos Categoría 1. - Mínimo 512 políticas de QoS activas por nodo / sede. - Funcionamiento en alta disponibilidad y administración centralizada vía controlador SD-WAN. - Soporte para múltiples tecnologías de transporte: MPLS, Ethernet, Internet dedicado, fibra, banda ancha empresarial, LEO satelital, móvil 4G/5G y cualquier otro medio aprobado por la FGN. C17.2. Identificación y clasificación del tráfico para QoS - La solución deberá implementar capacidades de inspección, identificación y clasificación de aplicaciones y flujo de trafico en capas L4 – L7 mediante tecnología de inspección profunda de trafico soportados por el fabricante, con propósito de clasificación de tráfico y aplicación de QoS.. priorización, selección de rutas, traffic shaping y generación de reportes de capacidad. Esta funcionalidad se utilizará exclusivamente para fines de operación y optimización de la red WAN y no para inspección de seguridad, firewall de capa 7 ni control de

contenido, los cuales corresponden a los componentes definidos en la Ficha Técnica de Seguridad.

- Catálogo de aplicaciones empresariales con identificación de mínimo:
  - Protocolos P2P: BitTorrent, eDonkey, Ares, similares.
  - VoIP y colaboración: SIP, RTP, H.323, Microsoft Teams, Webex, Zoom.
  - Streaming: Netflix, YouTube, Spotify, RTSP, MMS y similares.
  - Aplicaciones empresariales: HTTP, HTTPS, FTP, SMTP, IMAP, POP3, DNS, SSH, Office 365 y equivalentes.
  - Aplicaciones cloud: Azure, AWS, Google Cloud, OCI, Salesforce, ServiceNow.
- Actualización del catálogo / firmas de aplicaciones con periodicidad mínima semanal, sin afectación del servicio. Deberá contemplar aplicaciones colombianas (entidades del Estado, banca) y misionales de la FGN cuando éstas se integren.
- Categorías predefinidas de tráfico seleccionables por la FGN: productividad, navegación general, streaming, P2P, colaboración, almacenamiento, redes sociales, gaming, criptominería y demás del catálogo del fabricante.
- Reconocimiento de tráfico cifrado por metadatos (cabeceras, hostname SNI, tamaño y patrón) cuando la inspección SSL no esté habilitada. La inspección SSL/TLS misma se desarrolla en la Ficha Técnica de Seguridad.

C17.3. Políticas de tráfico (QoS y enrutamiento)

La solución deberá permitir crear y aplicar políticas avanzadas de gestión de capacidad y enrutamiento, basadas en:

- Identificación de aplicaciones en Capa 7 (DPI o mecanismo funcionalmente equivalente, con fines operativos).
- Dirección IP origen / destino.
- Puerto y protocolo (L4).
- Categorías de tráfico predefinidas.
- Identidad de usuarios y grupos vía integración con Active Directory para fines de QoS y enrutamiento por usuario (la autorización de acceso, RBAC y autenticación de seguridad son responsabilidad de la Ficha Técnica de Seguridad).
- Horarios, fechas y ventanas operativas (políticas temporales programables).

Estas políticas permitirán limitar, priorizar, garantizar o redirigir el ancho de banda según los lineamientos definidos por la FGN. No incluyen acciones de bloqueo por contenido, restricción por categorías de seguridad, listas negras ni filtros antimalware esas funciones pertenecen a la Ficha Técnica de Seguridad.

C17.4. Cifrado del transporte

Todo el tráfico transportado entre sedes y nodos Categoría 1, así como entre sedes y la Categoría 5 (nubes públicas), viajará cifrado en el overlay SD-WAN mediante IPsec / AES-256 con IKEv2, con rendimiento mínimo de 5 Gbps de tráfico cifrado por nodo Categoría 1 y de la capacidad contratada por sede en las demás Categorías. Este cifrado es del transporte y forma parte del alcance de

Conectividad. La gestión de llaves, certificados, rotación, criptografía avanzada y verificación de integridad criptográfica corresponden a la Ficha Técnica de Seguridad.

C17.5. Capacidades analíticas y telemetría operativa

La solución deberá contar con capacidades analíticas dirigidas a la gestión operativa y de capacidad (no a detección de amenazas, que es de Seguridad), con:

- Procesamiento de múltiples flujos y volúmenes simultáneos en los nodos principales (mínimo 6 Gbps de tráfico legítimo en los nodos Categoría 1).
- Reportes históricos de mínimo doce (12) meses consultables en línea, con respaldo de datos crudos durante toda la vigencia del contrato.
- Análisis en tiempo real por aplicación, IP, usuario, túnel SD-WAN, sede y Categoría.
- Dashboards gráficos y administración centralizada por interfaz web responsive.
- Detección de anomalías de capacidad (saturación, sub-utilización, cambios bruscos de patrón de uso, sedes con consumo atípico). La detección de amenazas de seguridad (intrusión, exfiltración, malware, comportamiento anómalo malicioso) corresponde a la Ficha Técnica de Seguridad.
- Acceso restringido basado en roles (RBAC) integrado con Active Directory para mínimo diez (10) cuentas FGN.
- Continuidad analítica mediante replicación entre los nodos Categoría 1 (Bogotá y Cali).

C17.6. Reportes y periodicidad

El PROVEEDOR entregará reportes automáticos y bajo demanda con la siguiente periodicidad mínima:

- Diario: disponibilidad y eventos críticos de capacidad.
- Semanal: consumo por usuario, por sede, por Categoría y por aplicación.
- Mensual: consolidado para reporte de cumplimiento de ANS (numeral C16), incluyendo top de aplicaciones, top de usuarios y proyecciones de capacidad.
- A demanda: análisis solicitados por la supervisión.

Formatos: Excel, PDF y vía API REST. Los reportes de seguridad (incidentes, intentos de intrusión, eventos de FW, etc.) se entregan por separado conforme a la Ficha Técnica de Seguridad.

C17.7. Continuidad operativa de la solución

La solución deberá garantizar continuidad del tráfico hacia Internet incluso ante fallas locales mediante:

- Conmutación automática hacia rutas alternativas SD-WAN en cualquiera de las Categorías.
- Comportamiento equivalente al bypass operativo manteniendo la funcionalidad básica del enlace si la plataforma de gestión SD-WAN pierde conectividad temporal.
- Capacidad de operación local en el CPE conforme al numeral C5 (Aprovisionamiento) y al diseño detallado.

C17.8. Capacidades de gestión y automatización

La solución deberá ofrecer:

- Interfaz API REST para automatización (creación de políticas QoS, ajustes de QoS, generación de reportes operativos, integración con orquestadores de la FGN).
- Interfaz web para administración manual.
- CLI para tareas avanzadas.
- Modalidad de gestión seleccionable por la FGN: gestionada por el PROVEEDOR, gestionada por la FGN, o modelo compartido (cogestión).
- Integración con la plataforma de Observabilidad de la FGN y con el sistema IPAM (numeral C10).

C17.9. Funcionalidades adicionales

- Soportar niveles de QoS escalables para crecimiento futuro: 100 Mbps, 1 Gbps, 5 Gbps, 10 Gbps y superiores.
- Realizar descubrimiento, clasificación y agrupación de tráfico en capa 7 con fines operativos.
- Permitir programación temporal de políticas y perfiles (horarios, fechas, ventanas).
- Integrarse con la plataforma de monitoreo del numeral C9 y con la de Observabilidad de la FGN.
- Operar en dual-stack IPv4 / IPv6 nativo conforme al numeral C1 (Generalidades).

C17.10. Eliminación de dispositivos externos dedicados

Todas las funcionalidades operativas descritas en este numeral deberán ser provistas exclusivamente por la solución, sin requerir:

- Modeladores de tráfico adicionales.
- Administradores de ancho de banda externos.
- Equipos dedicados para clasificación operativa o control de tráfico.
- Aceleradores físicos independientes.

El PROVEEDOR garantizará que la solución cumpla integralmente con estas capacidades, sin costo adicional para la FGN durante toda la vigencia del contrato. Los appliances dedicados de seguridad (FW NGFW, IPS, WAF, DLP, etc.) son alcance de la Ficha Técnica de Seguridad y no se sustituyen por las capacidades aquí descritas.

		C17.11. Modalidad de prestación - Categoría 1 (Datacenter): modalidad físico-dedicada con HA fault-tolerant. - Categorías 2 y 3 (sedes terrestres): integrada al CPE SD-WAN de la sede. - Categoría 4 (LEO): integrada al CPE SD-WAN, considerando las restricciones del enlace satelital. - Categoría 5 (Nubes): virtualizada o gestionada por el cloud provider, con políticas equivalentes a las sedes físicas. - Categoría 6 (Complementarios): según la ficha del servicio activado.
	C18. Requerimiento de equipos del contrato	Durante la ejecución del contrato, el PROVEEDOR deberá asegurar la garantía integral y permanente de todos los equipos, componentes y software que conforman la solución SD-WAN, incluyendo: equipos de seguridad de la solución; equipos de comunicaciones de la solución; equipos de videoconferencia de la solución; y servidores de la solución. -Equipos de seguridad de la solución. -Equipos de comunicaciones de la solución. -Equipos de videoconferencia de la solución. -Servidores de la solución.
	C19. Requerimientos de switching (core)	El PROVEEDOR deberá contemplar, dentro de la topología de referencia y las mejoras propuestas, la inclusión de switches de core, los cuales deberán integrarse de manera nativa y compatible con la infraestructura LAN existente de la entidad. Actualmente, en el Datacenter de la ciudad de Bogotá, a nivel LAN, la Fiscalía General de la Nación dispone de dos (2) switches core operando en configuración de alta disponibilidad mediante tecnología IRF, de referencia HPE 7510X , los cuales soportan la operación actual del núcleo de red. Para la sede de Cali, la implementación de la capa core LAN se encuentra en proceso de contratación, por lo que el PROVEEDOR deberá diseñar e implementar la solución de switches core en coherencia con la arquitectura que sea definida para dicha sede, garantizando su escalabilidad, compatibilidad e integración futura con el modelo de red corporativa de la entidad. La referencia a IRF corresponde a la tecnología de la infraestructura actualmente instalada y no constituye exigencia de marca. Se aceptarán tecnologías equivalentes de virtualización o agregación de chasis (IRF, VSS, VSF, MLAG, M-LAG, apilamiento u otras) que provean capacidades funcionales iguales o superiores de alta disponibilidad, agregación de enlaces multichasis y administración unificada, y que garanticen la interoperabilidad con la infraestructura LAN existente mediante protocolos estándar (IEEE 802.3ad/LACP, IEEE 802.1Q, OSPF y BGP). C19.1. Suministrar, configurar poner en funcionamiento y administrar los switches con: - Alta disponibilidad para las interfaces de los Firewall ubicados en las sedes del Nivel Central Bogotá y Datacenter de la sede Cali, para lo cual debe proveer:

		- La conectividad en las interfaces de los firewalls en fibra. - La alta disponibilidad a nivel de hardware con el suministro de dos (2) equipos en alta disponibilidad en la sede de Nivel Central y (2) equipos en la Sede Cali. - La configuración mediante VLAN´s (802.1q), considerando las interfaces de firewall ofrecidas C19.2. Cumplir con las siguientes especificaciones para las sedes del Nivel Central Bogotá y el Datacenter de la sede Cali: - Mínimo 80 puertos de 1 Gigabit Ethernet autosense en cobre. - Mínimo cuarenta y ocho (48) puertos de 10 GigabitEhternet SFP+ (que no estén en combo o dual personality o doble propósito). En caso de ser requeridos por ocasión a la prestación del servicio, el proveedor deberá incluir los puertos adicionales necesarios para el cumplimiento del servicio contratado, garantizando que los puertos de las tarjetas o equipos adicionales, no estén en combo o dual personality o doble propósito. - Mínimo dieciséis (16) puertos de 1 GigabitEhternet SFP (que no estén en combo o dual personality o doble propósito) - Mínimo 4 puertos de 40 GE QSPF+ - Los switches deben ser administrables y de nivel 3 (con enrutamiento). - Switches de Nivel 3: Ruteo local entre VLANs, Rutas Estáticas, RIP, OSPF, OSPFv3 y BGP4 - Debe soportar la configuración de mínimo 4.000 Vlans (Estandar 802.1Q) - Facilidad para configurar Port Mirroring para análisis de tráfico. - Posibilidad de hacer Relay para Servidor DHCP - Protocolo de recuperación ante Loops - Matriz de Conmutación de Paquetes de 1.500 Mpps - Desempeño de switch de mínimo 1 Tbps por cada tarjeta manejadora. - Fuente redundante interna o externa. - Hacer trunking hasta con 8 puertos. - La tecnología aplicada a las unidades solicitadas deberá incluir el procesamiento de paquetes de IPv4 e IPv6, en hardware. - Suministrar los PATCH CORD de cobre y fibra multimodo y Tranceiver SFP y SFP+ para la totalidad de los puertos ofrecidos. (multimodo LC-LC OM4) - Funciones de Administración: - Por puerto de consola, sesión remota por SSH v2 con cifrado AES-256 y HTTPS (TLS 1.2 o superior). No se aceptan protocolos de administración en texto claro. - Soporte de protocolos SNMP V2C y V3 - Monitoreo de los puertos por estado de operación, estadísticas, errores generados y bitácora de eventos. - Funciones de seguridad: - Debe contar con protocolo de autenticación (Estandar 802.1x) - Manejar Listas de Control de Acceso (ACLs). - Protección contra ataques de Denegación de Servicio. - Limitar el número de direcciones MAC en cada uno de los puertos.
	C20. Requerimiento a	Suministro de veinte (20) soluciones móviles de conectividad satelital, destinadas a garantizar la prestación de servicios de conectividad para el desarrollo de

	eventos jornadas de descongestión	jornadas de descongestión, brigadas de fortalecimiento de justicia y eventos de videoconferencia en campo. Estas soluciones estarán diseñadas bajo tecnología satelital de órbita baja (LEO), que garantice velocidades de descarga de al menos 50 Mbps y de carga de al menos 10 Mbps, latencias reducidas aptas para videoconferencia (idealmente inferiores a 100 ms), cobertura nacional, capacidad de conexión simultánea de múltiples usuarios y planes de datos ilimitados. Cada solución deberá incluir terminal satelital portátil, antena de autoapuntamiento, router WiFi integrado o externo, accesorios de instalación y fuentes de alimentación, asegurando facilidad de transporte Las soluciones estarán centralizadas en la ciudad de Bogotá, desde donde se gestionará su despliegue hacia los distintos municipios del país de acuerdo con los requerimientos de la entidad. El proveedor será responsable de manera integral del servicio, incluyendo el transporte, instalación, configuración, puesta en operación, soporte técnico durante los eventos y retiro de los equipos, garantizando la disponibilidad, continuidad y adecuado funcionamiento del servicio bajo un esquema de atención bajo demanda. Asimismo, deberá asegurar que las soluciones soporten la operación de equipos de videoconferencia en campo, manteniendo niveles adecuados de estabilidad, calidad de servicio y desempeño en cualquier ubicación del territorio nacional.
Empaque y rotulado	Los gabinetes, CPE SD-WAN, equipos de seguridad, enrutadores, antenas de Órbita Baja, módems y demás elementos instalados por el CONTRATISTA deberán estar debidamente marquillados e identificados de forma permanente y visible en la parte frontal del hardware, incluyendo como mínimo el ID de la sede y el número del contrato, conforme a lo definido en el Anexo Técnico 1.1 – Requerimiento de Sedes a Conectar. Así mismo, los cables asociados a los equipos de último kilómetro, incluyendo cables de energía, red, fibra óptica y enlaces RF/IF, deberán estar marquillados en ambos extremos, indicando el ID de la sede, el equipo asociado, el número de contrato y el extremo correspondiente. El marquillado deberá ser legible, resistente y de carácter indeleble.- FGN – SEDE: [ID_SEDE] EQUIPO: [TIPO_EQUIPO] CONTRATO: [No_CONTRATO] Cableado de la solución: FGN – SEDE: [ID_SEDE] EQUIPO: [TIPO_EQUIPO] CONTRATO: [No_CONTRATO] EXTREMO: [ORIGEN / DESTINO] No aplica empaque físico por tratarse de un servicio gestionado de conectividad. Para los bienes que soportan el servicio (CPE SD-WAN, switches, equipos de seguridad y demás elementos activos) el PROVEEDOR debe entregarlos en su empaque original del fabricante, sellado y sin signos de apertura, con rotulado que identifique fabricante, modelo, número de serie y número de parte. El marcaje de inventario/activo fijo se aplicará conforme al procedimiento de activos de la FGN una vez instalados.	

Presentación y Unidad de Medida	Servicio continuo mensual durante la vigencia del contrato, prestado sobre la infraestructura SD-WAN a nivel nacional. Unidad de medida: servicio mes por sede, diferenciado por categoría (Categoría 1 Datacenter, Categoría 2 Ciudades principales, Categoría 3 Ciudades intermedias, Categoría 4 Resto nacional – satelital órbita baja, Categoría 5 Nubes públicas Azure y OCI, y Canales complementarios). Incluye anchos de banda, licenciamiento, soporte, monitoreo y gestión asociados a cada sede y categoría, conforme al ANEXO 1.1 – Requerimiento de Sedes.

Concepto	Nombre y apellidos	Rol	Firma
Aprobó	Eric Mauricio Vargas Forero	Jefe Departamento De Infraestructura	ERIC M VARGAS FORERO Firmado electrónicamente por ERIC M VARGAS FORERO Fecha: 2026.11.05 11:33:55 -05'00'
Elaboró	Carlos Alberto Pinto Chaparro	Estructurador	CARLOS ALBERTO PINTO CHAPARRO Firmado electrónicamente por carlos alberto pinto chaparro Fecha: 2026.11.04 14:41:59 -05'00'
Revisó	Joan Andres Perdomo Hernandez	Estructurador	JOAN ANDRES PERDOMO HERNANDEZ Firmado electrónicamente por JOAN ANDRES PERDOMO HERNANDEZ Fecha: 2026.11.04 17:11:23 -05'00'
Revisó	Jose Luis Daza Perez	Estructurador	JOSE LUIS DAZA PÉREZ Firmado electrónicamente por Jose Luis Daza Pérez Fecha: 2026.11.04 20:53:37 -05'00'
Revisó	Tania Milena Rozo Cortes	Estructurador	TANIA MILENA ROZO Firmado electrónicamente por TANIA MILENA ROZO Fecha: 2026.11.05 08:27:49 -05'00'