ANEXO TECNICO

INSTITUTO DE MOVILIDAD DE PEREIRA

SD-WAN SEGURO FORTINET
Y SERVICIOS MOVILES

tigo business

INFORMACIÓN DEL DOCUMENTO			
ID del Requerimiento		02899512	
Tipo de Requerimiento		Colaboración	
Fecha	**Versión**	**Comentarios**	**Elaborado Por**
24/07/2026	1	Diseño Inicial	Jorge Alberto Jaramillo
06/08/2026	2	Actualización oferta	Jorge Alberto Jaramillo

Tabla de contenido

1 OFERTA TECNICA 5

1.1 ESTRATEGIA 5

1.2 SOLUCION SDWAN TIGO 5

1.2.1 Alcance de la solución 5

1.2.1 Componentes de la solución propuesta 6

1.2.2 Servicio SDWAN TIGO 6

1.2.2.1 Necesidad de aprovisionar SDWAN 6

1.2.2.2 Descripción General 7

1.2.2.3 Características Técnicas Solución SD-WAN 8

1.2.2.3.1 Conocimiento de la aplicación: 8

1.2.2.3.2 Control de múltiples rutas: 9

1.2.2.3.3 Rendimiento 10

1.2.2.3.4 Balanceo de todo tipo de líneas 10

1.2.2.3.5 Monitoreo inteligente de enlaces WAN 10

1.2.2.3.6 VPN Inteligente 11

1.2.2.3.7 Inspección SSL y prevención de amenazas 11

1.2.2.3.8 Funcionalidades de Seguridad 11

1.2.2.3.9 Single pane of glass 11

1.2.2.3.10 Branch Office in a box 12

1.2.2.3.11 Beneficios Clave SDWAN Segura 13

1.3 ARQUITECTURA Y DISEÑO SDWAN 13

1.3.1 Dimensionamiento de la Solución 14

1.3.2 Topología General de la Solución SD-WAN 15

1.3.3 SD-WAN Topología Lógica 16

1.3.4 Descripción de los componentes 16

1.3.4.1 FortiGate: Next Generation Firewall 16

1.3.4.2 FortiManager: Gestión centralizada para todos los dispositivos FortiGate en una sola consola. 17

1.3.4.3 FortiAnalyzer: Analítica y Gestión de logs enfocado a Seguridad. 17

1.3.4.4 Analítica y reportes sd-wan 18

1.3.4.5 FortiGuard Labs: Servicios de Seguridad. 20

1.3.1 Equipos propuestos en la solución 20

1.3.2 SD-WAN Segura (SD-WAN + Internet Seguro Avanzado) 21

1.3.3 Características de Seguridad a Implementar para el DIA 23

1.3.4 Red de Transporte Sdwan 23

1.3.4.1 Internet 24

1.4 SERVICIOS ADMINISTRADOS SDWAN 25

1.4.1 Enterprise 25

1.5 MODELO DE ADMINISTRACIÓN COMPARTIDA SDWAN (*FortiPortal*) 27

1.6 SUPUESTOS, RESTRICCIONES Y RESPONSABILIDADES 31

1.6.1 Consideraciones generales: 32

1.7 IMPLEMENTACIÓN Y/O TRANSICIÓN 35
1.7.1 Metodología de Aprovisionamiento 35
1.7.2 Tiempo de Aprovisionamiento 35
1.7.3 Entregables 36
1.7.4 Roles y responsabilidades 36
1.7.5 Responsabilidades del Cliente 37
2 COMPROMISOS DEL CLIENTE 40
1.8 ACUERDO DE CONFIDENCIALIDAD 40
1.9 USO DE LOS SERVICIOS 40

1 OFERTA TECNICA

1.1 ESTRATEGIA

Tigo presenta al INSTITUTO DE MOVILIDAD DE PEREIRA una solución de SDWAN Segura para las sedes en modalidad de Servicios que cubren los componentes tales como: SERVICIOS DE TELECOMUNICACIONES (Servicios, Internet, equipos SDWAN, Seguridad), y a su vez, el equipamiento, instalación, soporte proactivo, mantenimiento, operación, monitoreo y cumplimiento de ANS a través del recurso humano, herramientas, seguridad y procesos del ciclo de vida de servicios enmarcados en ITIL y COBIT. Con esta solución TIGO ofrece una solución con los siguientes diferenciadores:

- ✓ Simplicidad en la operación
- ✓ Rápido proceso de implementación tecnológica y operativa.
- ✓ Escalabilidad de la solución a brindar considerando el crecimiento del cliente.
- ✓ Confidencialidad sobre la información y documentación procesada
- ✓ Flexibilidad en adiciones, cambios y modificaciones
- ✓ Oportunidad en la inclusión de nuevos servicios y/o funcionalidades que apoyen el negocio.

1.2 SOLUCION SDWAN TIGO

1.2.1 Alcance de la solución

Presentar al cliente INSTITUTO DE MOVILIDAD DE PEREIRA una solución de SD WAN con Tecnología Fortinet la cual proporciona una plataforma de red de área amplia (WAN) de superposición definida por software que le permitirá al cliente implementar una WAN híbrida escalable, segura y enfocada en los objetivos de Negocio.

El presente diseño corresponde al HLD, la elaboración del LLD se realizará en conjunto con el cliente, para definir detalles de alcance y modos de operación de la infraestructura de red en las diferentes fases propuestas para la Implementación.
La oferta contiene los siguientes servicios de Telecomunicaciones:

- ✓ Solución SDWAN Segura
- ✓ Instalación, Configuración, Afinación, Administración, Soporte HW
- ✓ Firewall Nueva Generación + Licenciamiento UTP
- ✓ Plataforma de Gestion Sdwan
  - Fortimanager
  - Fortianalyzer
  - FortiPortal
- ✓ Enlaces Internet

1.2.1 Componentes de la solución propuesta

En Tigo estamos convencidos que la base para la transformación digital del CLIENTE es a través de las tecnologías SD-WAN y la seguridad integrada, lo que le permite resolver los problemas de la WAN de hoy y prepararse para la creciente adopción de más cloud y servicios digitales.
Los siguientes componentes están incluidos en la propuesta:

1. Topología Redundante Internet – Internet
2. Mejor utilización de los canales
3. Seguridad del tráfico en cualquier tipo de medio mediante el uso de VPNs dinámicas.
4. Completa utilización de enlaces redundantes.
5. Visibilidad y monitoreo de aplicaciones y usuarios.
6. Flexibilidad y escalabilidad de la solución y la infraestructura.
7. Servicio administrado SD-WAN
8. Mejora en el transporte de las App.
9. Enrutamiento inteligente que considera los requerimientos de las aplicaciones que corran dentro de la red del cliente
10. Calidad de servicio basado en el tipo de aplicación que correrá sobre los enlaces de retorno hacia las sucursales
11. Diseño basado en disponibilidad, escalabilidad y flexibilidad.
12. Reducción de tiempos de implementación.

Nota: en todo caso, el anterior alcance se circunscribe únicamente a lo ofertado en el presente documento.

1.2.2 Servicio SDWAN TIGO

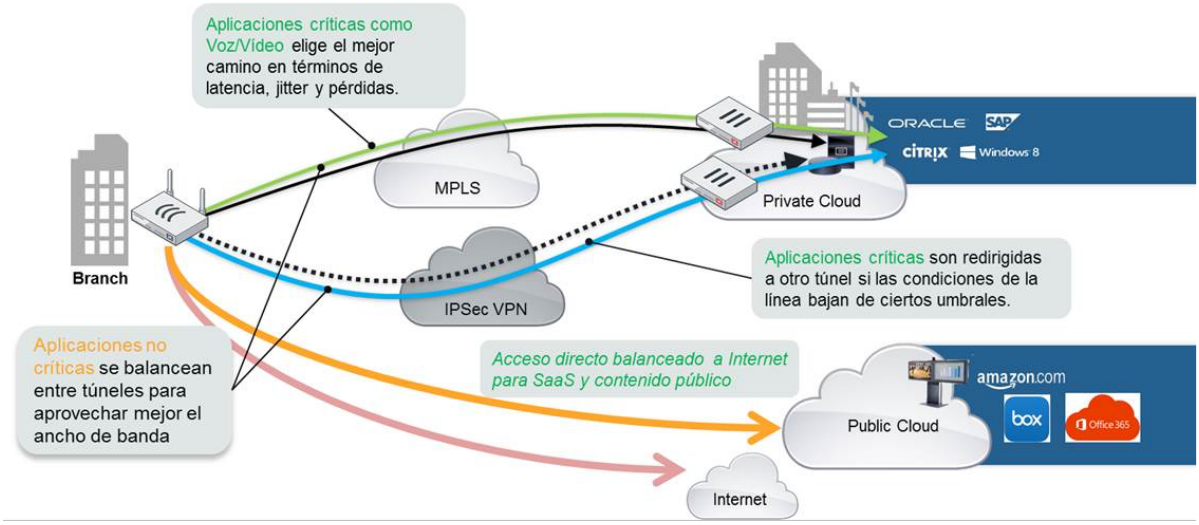
1.2.2.1 Necesidad de aprovisionar SDWAN

El aumento de servicios en la nube requiere infraestructuras WAN que puedan conectar, de forma fiable y eficiente, las diferentes ubicaciones de los clientes a los recursos corporativos. Las empresas demandan soluciones SD-WAN que les permitan superar la limitación de la escalabilidad, los altos costes y la complejidad creciente de las arquitecturas WAN tradicionales, sin dejar de lado la seguridad al permitir acceso directo a servicios y datos sensibles SaaS, además del aumento de amenazas como el malware cifrado SSL, ransomware y un volumen cada vez mayor de intentos de intrusión avanzada.

Gartner define SD-WAN (Software Defined WAN) como una solución que provee un reemplazo para los routers WAN tradicionales, es agnóstica para las tecnologías de transporte WAN, proporciona una selección de rutas de aplicaciones dinámicas basadas en políticas a través de varias conexiones WAN y soporta servicios adicionales como la optimización de WAN y funciones de firewall.

1.2.2.2 Descripción General

La tecnología SD-WAN propuesta ofrece opciones de conectividad flexible, funciones de calidad de servicio, servicios de conexión de red automatizada y despliegue simplificado para adaptarse a los cambios de uso del tráfico empresarial. Los beneficios y capacidades de SD-WAN ofrecen una solución que simplifica la transición de los clientes a una infraestructura de red definida por software flexible, escalable y segura

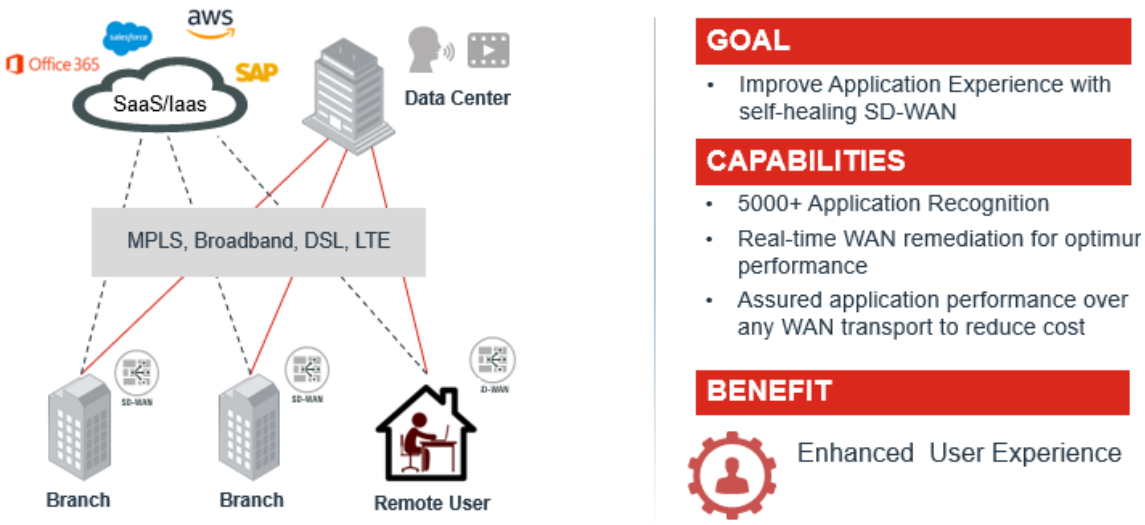


Este servicio permite consolidar varios canales (Internet/MPLS o Internet/Internet) del cliente en una interfaz de tipo SD-WAN y distribuir el tráfico del cliente a través de estos basados en algoritmos de balanceo (Volumen, Sesiones, Spillover, IP Origen-Destino, IP Origen). FortiOS emplea diversos protocolos como Ping, HTTP Echo o TWAMP para obtener detalles de latencia, jitter y perdida de paquetes para cada enlace. De tal forma, si el monitoreo de un enlace específico no cumple con los mínimos exigidos a la conectividad, se eliminará del grupo de enlace virtual y cualquier tráfico futuro se otorgará a otros enlaces saludables.

Posteriormente, se crea una capa "*overlay* segura" de túneles VPN encima de la conectividad provista ("*underlay*"), lo cual permite que se puedan utilizar de forma simultánea múltiples enlaces de múltiple naturaleza, pudiendo combinar a conveniencia múltiples circuitos MPLS, de Internet dedicado, de Internet banda ancha, redes 3G/4G o enlaces satelitales en las combinaciones requeridas para ampliar el ancho de banda disponible y así mismo maximizando las inversiones y los medios disponibles para poder aplicar políticas cuando se combinan conexiones de múltiples calidades y costos.

Las reglas de SD-WAN permiten definir para flujos de tráfico específico, basado en direcciones IP, puertos, servicio de internet a consultar definir el canal o los canales por los cuales se enviará el tráfico.

De forma adicional este servicio permite configurar perfiles de seguridad (Antivirus, IPS, control de aplicaciones, filtrado web) para los flujos de tráfico que el cliente considere necesario.



Una solución SD-WAN conecta a los usuarios donde sea que se encuentren a la nube para la utilización de cualquier aplicación. SD-WAN determina de forma inteligente qué ruta satisface mejor los requerimientos de rendimiento ideales para una aplicación específica. Luego enruta el tráfico a la ruta ideal de la WAN.

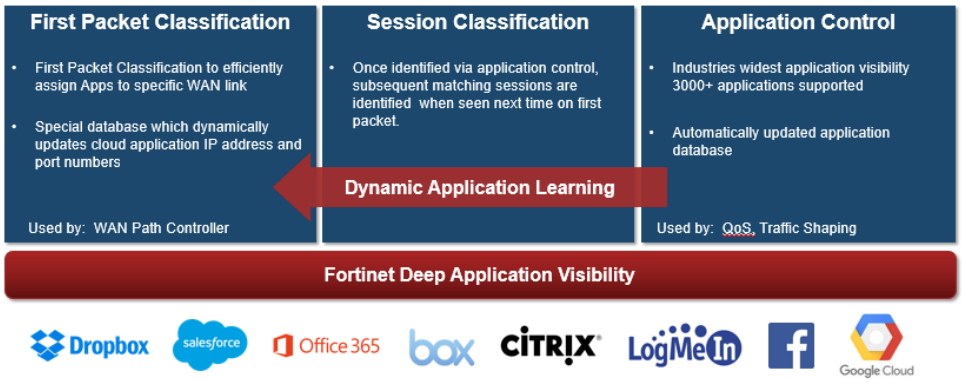
A continuación, se presentan algunas características que definen cómo funciona una solución de SD-WAN, la solucion presentada puede tener una o varias de las siguientes funcionalidades según el caso de uso planteado:

1.2.2.3 Características Técnicas Solución SD-WAN

1.2.2.3.1 Conocimiento de la aplicación:

Con las soluciones de WAN tradicionales, las organizaciones presentan una calidad de experiencia menos que ideal y les resulta difícil ofrecer un ancho de banda de alto rendimiento para aplicaciones críticas. Debido a que las arquitecturas de WAN heredadas dependen del enrutamiento de paquete, carecen de una visibilidad detallada de la aplicación. Sin embargo, las soluciones de SD-WAN identifican de manera inteligente las aplicaciones desde el primer paquete de tráfico de datos. Los equipos de red obtienen la visibilidad que necesitan sobre qué aplicaciones se utilizan más ampliamente en toda la organización, lo que les ayuda a aplicar políticas y tomar decisiones más inteligentes y mejor informadas.
La solución de SDWAN Segura con conocimiento de las aplicaciones, admite una amplia gama de más de 3,000 aplicaciones, así como visibilidad granular en las subaplicaciones.

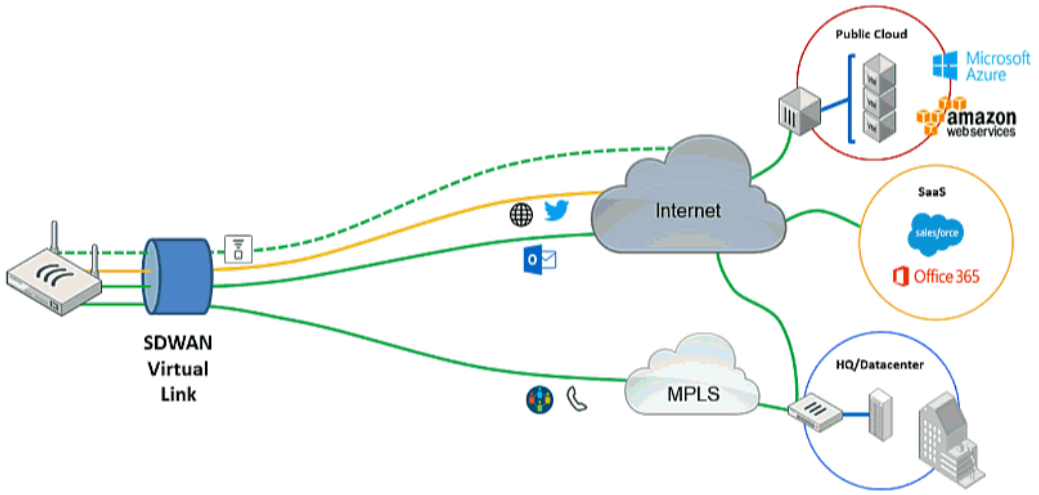
Permite Inteligencia de reconocimiento de ruta para monitorear transacciones a nivel de aplicación y conmutación por error dinámica a la mejor ruta disponible



1.2.2.3.2 Control de múltiples rutas:

La solución SD-WAN segura debe ser capaz de distinguir entre aplicaciones para aprovechar toda la funcionalidad de la solución. Al distinguir las aplicaciones y controlar los entornos de múltiples rutas, SD-WAN proporciona una dirección dinámica de las aplicaciones a través de paquetes o sesiones para recorrer las rutas disponibles hacia la WAN corporativa o los entornos multi-cloud.

La solución SD-WAN puede identificar de manera inteligente las aplicaciones y determinar la mejor ruta que debe tomar para maximizar la funcionalidad. Además, la tecnología de múltiples rutas enruta automáticamente el tráfico al siguiente mejor enlace disponible en caso de una interrupción del enlace principal. Esta capacidad automatizada no solo reduce la complejidad dentro de la red, sino que ofrece una experiencia de usuario mejorada y mejora el rendimiento de las aplicaciones.



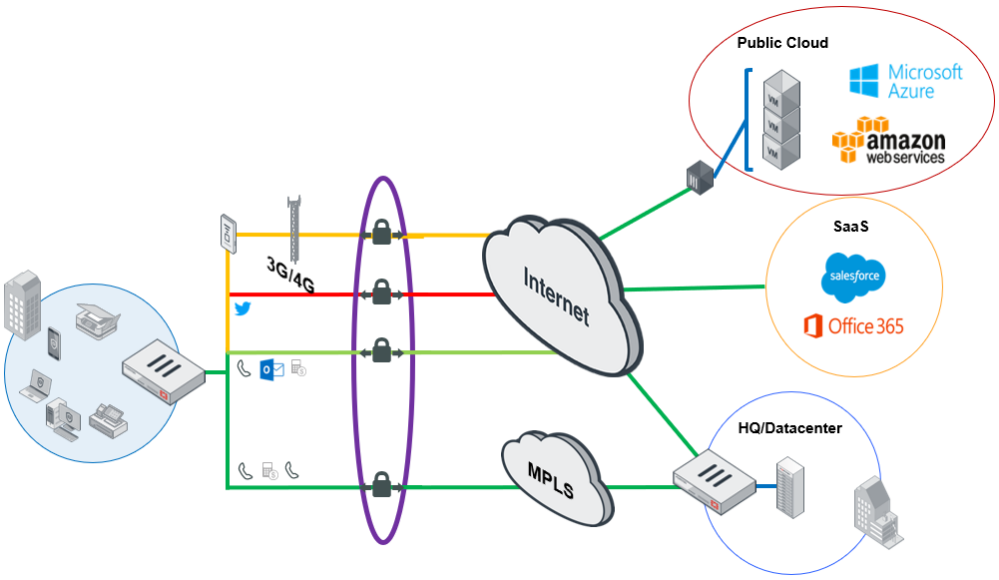
1.2.2.3.3 Rendimiento

Gracias a los procesadores de seguridad SPU (procesamiento hardware), la solución puede ofrecer un gran rendimiento a todo tipo de sedes realizando tareas de red, seguridad e inspección.

1.2.2.3.4 Balanceo de todo tipo de líneas

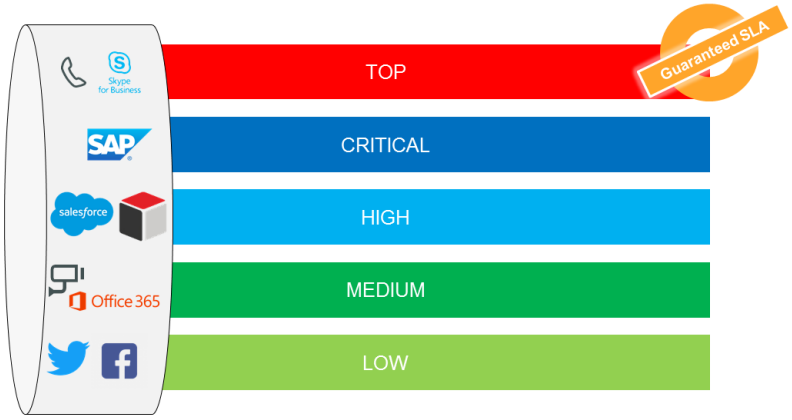
Fortigate permite configurar todos sus puertos como líneas WAN y crear múltiples túneles IPSec en cada una. Además,según el modelo permite conectar canales 3G/4G para redes de backup.
Fortigate puede balancear tráfico de Internet, aplicaciones SaaS y aplicaciones corporativas de forma inteligente mediante umbrales de latencia, jitter, ancho de banda disponible para asegurar que la VoIP o videoconferencia y las aplicaciones críticas siempre vayan por la línea óptima en cada momento.

Una de las ventajas de sdwan es el poder llevar a todos los enlaces contratados a un esquema de Activo-Activo, de tal manera que desaparecen las capacidades ociosas



1.2.2.3.5 Monitoreo inteligente de enlaces WAN

Desde FortiOS 5.6 integra la funcionalidad SD-WAN para el balanceo de carga WAN Link para que los clientes puedan elegir el mejor enlace para aplicaciones críticas de negocio. Sin embargo, si la degradación de la salud de enlace falla, este simplemente utiliza próximo enlace con mejor SLA para las aplicaciones. FortiOS también soporta TWMAP (medir el rendimiento de la red de ida y vuelta entre dos dispositivos) y otros protocolos para que los clientes puedan obtener una vista detallada de aplicaciones y servicios sensibles, como jitter, pérdida de paquetes, latencia, etc.



Guarantee SLA for Business Critical Apps

1.2.2.3.6 VPN Inteligente

Fortigate dispone de ADVPN (*) para realizar túneles IPSec automáticos entre sedes. Esto permite optimizar las redes SD-WAN, crear caminos de baja latencia y mantener todas las ventajas de una red unificada bajo entorno IPSec centralizado, especialmente interesante en entornos internacionales.

1.2.2.3.7 Inspección SSL y prevención de amenazas

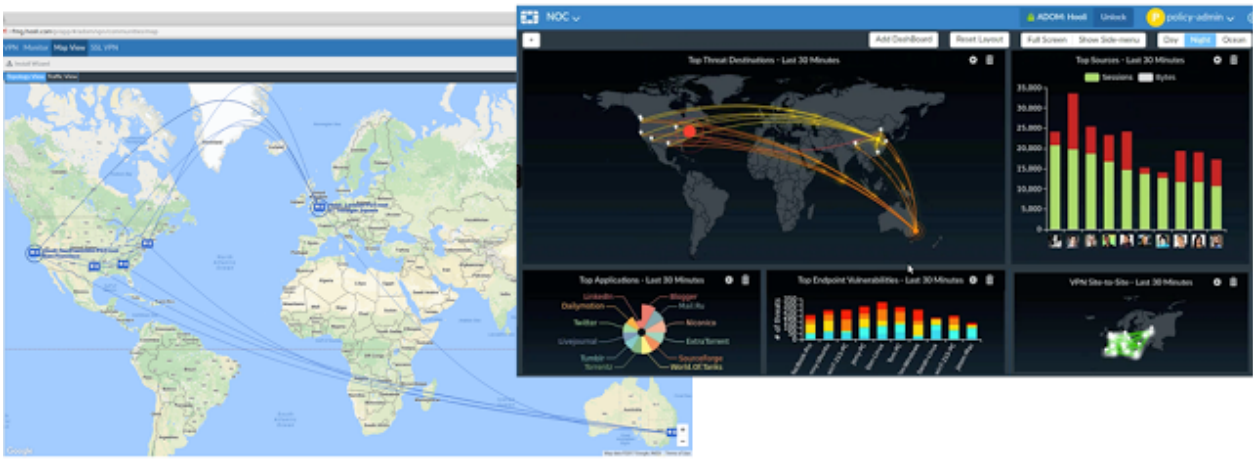
Las organizaciones no deberían tener que elegir entre el rendimiento y la protección. Sin embargo, debido a que cada vez más datos pasan por la red en forma cifrada, muchas soluciones de seguridad se convierten en un cuello de botella cuando intentan abrir e inspeccionar el tráfico. Las soluciones de Fortinet no solo admiten cifrados que impone la industria, sino que los firewalls de Fortigate proporcionan el mayor rendimiento de inspección SSL de la industria.

1.2.2.3.8 Funcionalidades de Seguridad

El equipo Fortigate procesa el tráfico a nivel 7 para realizar funciones adicionales de seguridad tales como: Antivirus, Filtrado web, control de aplicaciones e IPS.

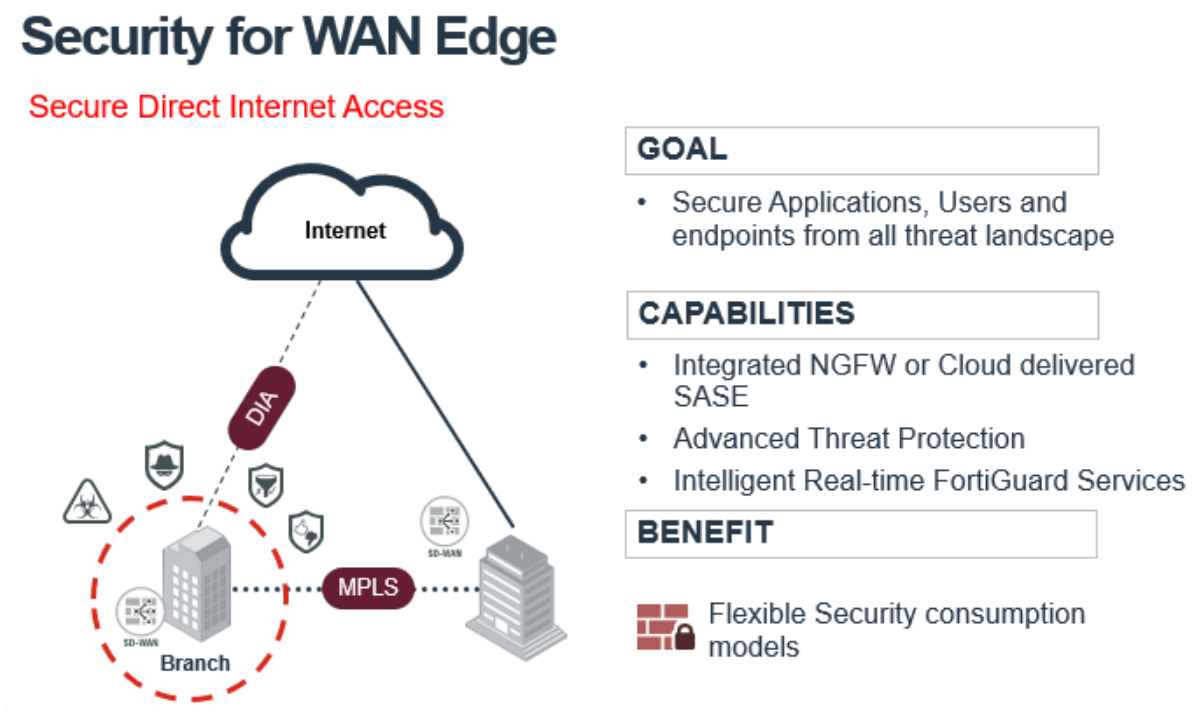
1.2.2.3.9 Single pane of glass

A través de la plataforma FortiManager es posible gestionar todo el entorno SD-WAN desde un único punto, pudiendo controlar los túneles IPSec, el estado de todas las líneas, amenazas, incidencias de red. Además ofrece una completa visibilidad en tiempo real e informes personalizados desde un único punto central.



1.2.2.3.10 Branch Office in a box

No se necesitan equipos adicionales para dar servicio a una oficina remota. El diseño propuesto para el servicio de SD-WAN se basa en equipos físicos que realizan las tareas de SD-WAN y red (Gestiona VLANS, routing dinámico, IPSec, QoS, ADVPN, DNS, DHCP) y las funciones de Seguridad (IPS, AppCtrl, AV, Filtrado web, autenticación con AD).



1.2.2.3.11 Beneficios Clave SDWAN Segura



1.3 ARQUITECTURA Y DISEÑO SDWAN

los siguientes criterios de diseño aplican para la solución de conectividad sdwan:

- ✓ **Modelo de Red**: Solución sdwan con Arquitectura Redundante Internet-Internet, Topología Lógica Hub and spoke

  Componentes SD-WAN
  - **FortiGate** – Next Generation Firewall con Funcionalidades de SD-WAN
  - **FortiManager** – Gestión Centralizada de múltiples FortiGates
  - **FortiAnalyzer** – Analítica y Reporteria de los equipos Fortigate
- ✓ **Atributos Clave SD-WAN:**
  - Administración y gestión centralizada
  - Control y visualización de aplicaciones
  - Enrutamiento basado en aplicaciones
  - Balanceo Dinámico
  - DIA (direct internet access)
  - Forward Error correction (FEC)
  - Conectividad segura Cifrada
  - Optimización aplicaciones SaaS basado en SLA +
  - Packet cloning para tráfico RTP +

  + Se deben tener mínimo dos enlaces WAN contratados para SD-WAN
- ✓ **Alta disponibilidad:**
  - Full utilización de enlaces WAN redundantes.

- A nivel WAN (Underlay) las sedes con doble canal tendrán un esquema de alta disponibilidad de acceso físico y lógico, este esquema de enlaces redundantes permite tener una ruta alterna en caso de que el enlace principal falle aumentando de forma significativa la disponibilidad de los servicios corporativos.
- La solución de SDWAN segura permite un balanceo de carga avanzado que tiene como fin utilizar la capacidad de la red de transporte al 100%
- Con la red de transporte todo Internet se evitan problemas de fallas cruzadas

✓ **Escalabilidad:**
- Se contempla un modelo de crecimiento soportado en los UTM dimensionados
- Fortimanager Centralizado en modalidad Virtual que permite escalar a nivel de licenciamiento y crecimiento en demanda
- Fortianalyzer Centralizado en modalidad Virtual que permite crecimiento en demanda

✓ **Seguridad:**
- Licenciamiento UTP para todos los equipos.
- Trafico cifrado entre sedes

✓ **Experiencia de usuario:** la implementación contempla perfilamiento de las aplicaciones de INSTITUTO DE MOVILIDAD DE PEREIRA para hacerlas parte de las políticas enrutamiento SD-WAN.

✓ **Salida a Internet:**
- El tráfico de navegación saldrá de forma local a través del DIA por los equipos Sdwan (NGFW Fortigate) de manera segura.

✓ **Consideraciones Técnicas:**
- Publicaciones, VPN S2S o VPN C2S se deben establecer desde el equipo de seguridad de la sede Torre Central
- El cliente debe suministrar las políticas de seguridad actualmente configurada en sus equipos Fortigate 200E
- El cliente debe asegurar espacio en la sede principal para los equipos SDWAN
- Se definirá en conjunto con el cliente las políticas de seguridad y sdwan en los Edge sdwan
- Se Instalará un servicio de Internet nuevo en la sede ppal como TX sdwan y navegación, no se reemplazarán canales de Internet sobre los cuales se tenga direccionamiento publico posicionado

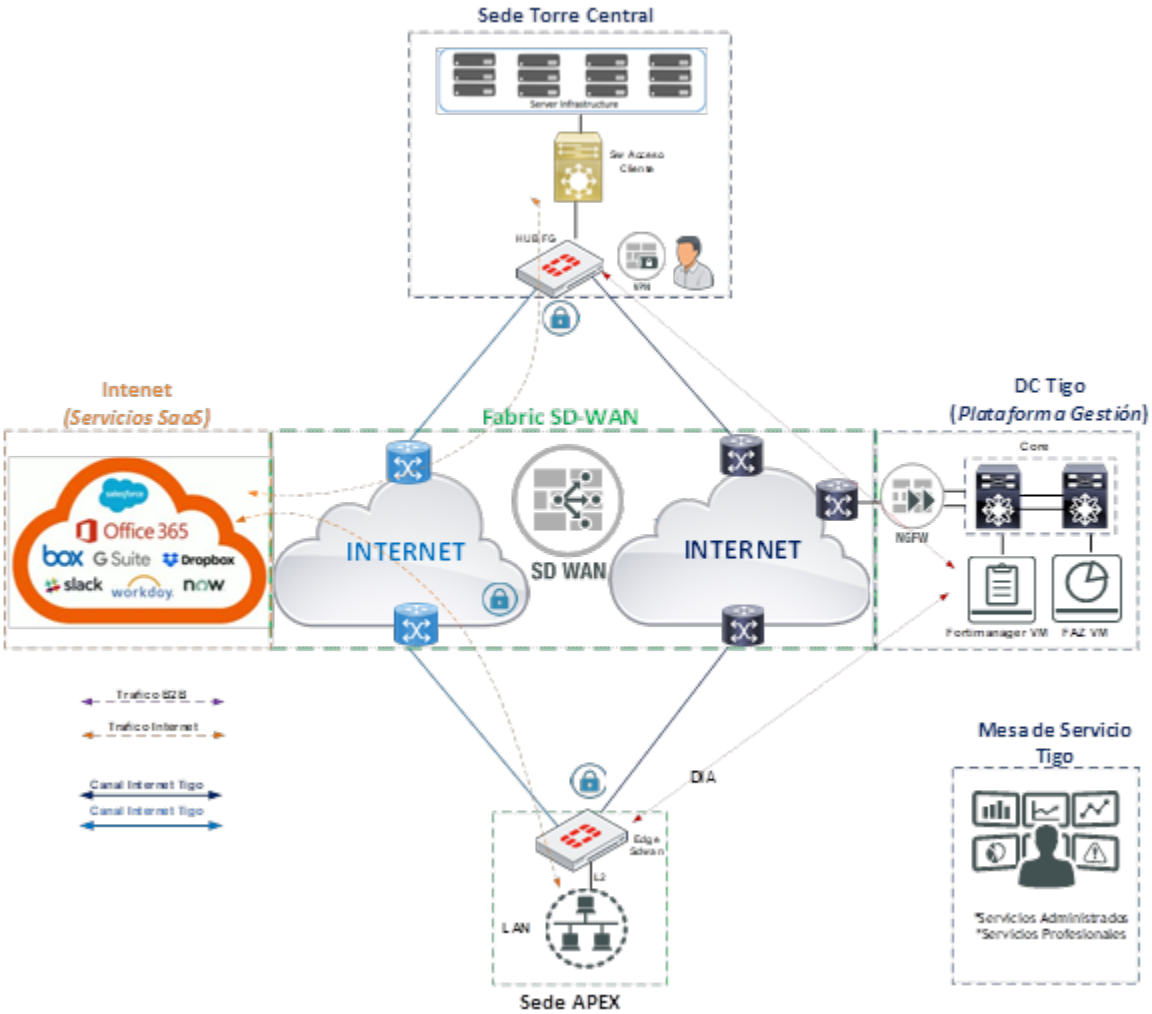
1.3.1 Dimensionamiento de la Solución

A continuación, se definen las sedes a interconectar, anchos de banda ofrecidos, tecnologías de acceso y cantidad de Equipos.

Dirección	Municipio	Producto 1	Medio	Nuevo BW Mbps	Producto 2	Medio	BW Mbps	Equipo Sdwan	Cantidad Equipos
Torre Central	Pereira	Internet	FO	500	Internet	FO	300	FG120G	1
APEX	Pereira	Internet	FO	500	Internet	FO	300	FG50G	1

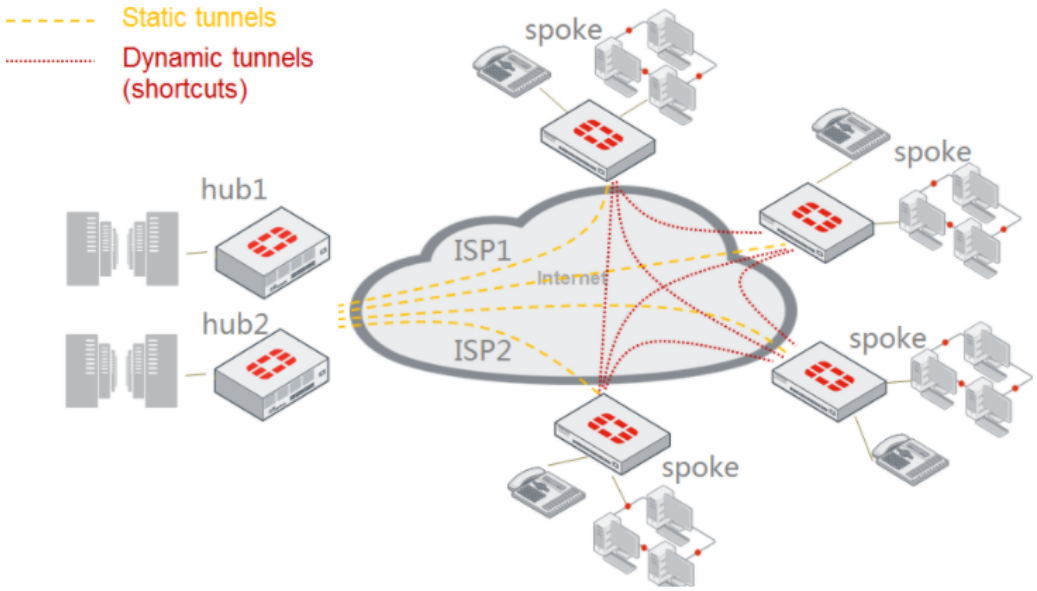
Nota: las factibilidades para los servicios nuevos son por cobertura y están sujetos a visita en terreno en el momento de la implementación.

1.3.2 Topología General de la Solución SD-WAN



1.3.3 SD-WAN Topología Lógica

La topología lógica propuesta para el cliente es Hub and Spoke con túneles estáticos, las reglas del servicio SD-WAN pueden utilizar la VPN de acceso directo (túneles dinámicos) para reenviar el tráfico entre las sucursales sin pasar por el HUB



NOTA:

- El HUB principal de la solución estará ubicado en el DC Ppal, el cual estará compuesto por el Fortigate 120G
- El HUB de contingencia para manejar el plano de control estará en la sede remota con FG50G

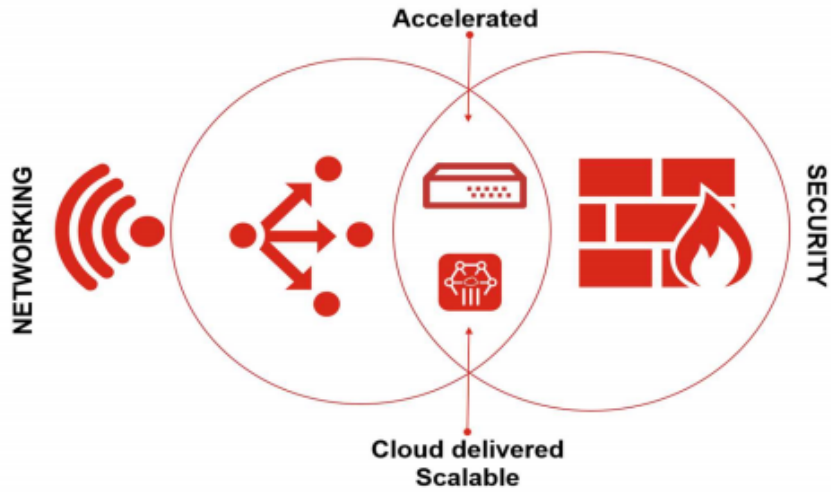
1.3.4 Descripción de los componentes

1.3.4.1 FortiGate: Next Generation Firewall

FortiGate proporciona funcionalidades de NGFW con un rendimiento excepcional, ultra baja latencia y protección de amenazas multi vector. Las plataformas NGFW FortiGate incluyen un sistema de prevención de intrusiones (IPS) con un escaneado del paquete en profundidad, capacidad para identificar y controlar las aplicaciones ejecutadas en la red y la posibilidad de verificar la identidad del usuario y cumplir con las políticas de acceso.

FortiGate ofrece implementaciones flexibles del borde de la red hasta el Core, el centro de datos, el segmento interno y la nube. Los FortiGate aprovechan los procesadores de seguridad (SPU) que son específicamente diseñados para brindar un rendimiento escalable de servicios de seguridad avanzados,

como protección contra amenazas, inspección de SSL y latencia ultra baja y así proteger segmentos internos y entornos de misión crítica.
El SD-Wan embebido en FortiGate le permite distribuir el tráfico en múltiples conexiones para permitir la transformación digital y acceso rápido a la nube. Ayuda a mejorar la productividad y permite el acceso directo a Internet para el uso de las aplicaciones SaaS.



Concepto de Redes enfocadas en Seguridad de Fortinet

1.3.4.2 FortiManager: Gestión centralizada para todos los dispositivos FortiGate en una sola consola.

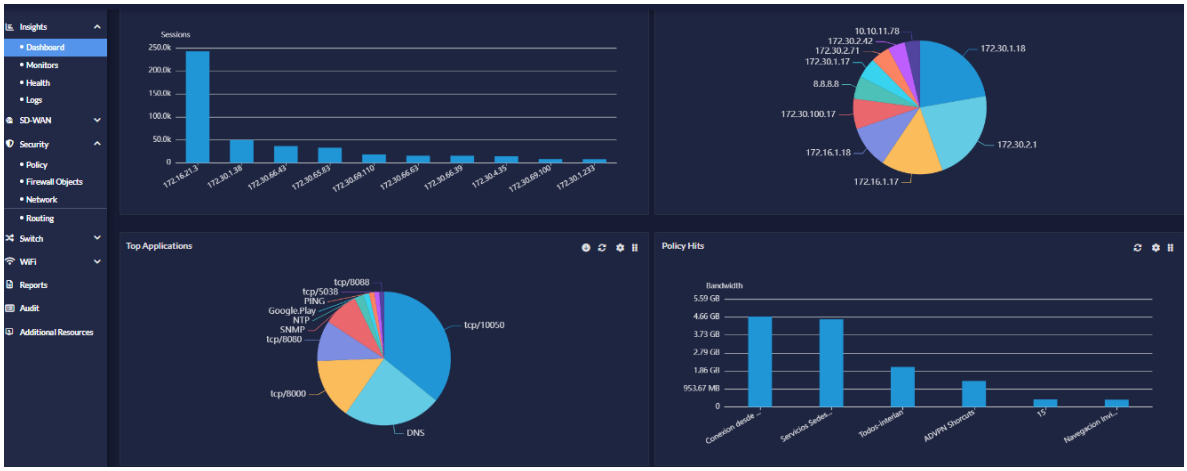
Plataforma de gestión que permite la centralización de las acciones que se han de llevar a cabo en los equipos FortiGate permitiendo un rápido despliegue de los proyectos de SD-WAN, el mantenimiento y actualización de los distintos dispositivos y su monitoreo en tiempo real.

1.3.4.3 FortiAnalyzer: Analítica y Gestión de logs enfocado a Seguridad.

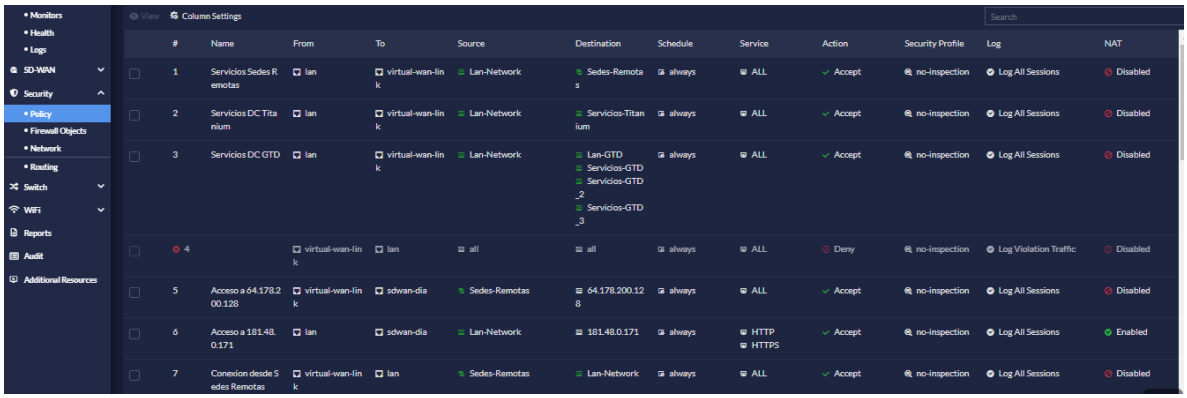
Plataforma dedicada al registro centralizado de logs, la gestión y tratamiento de los mismos y la generación de reportes. FortiAnalyzer posee la capacidad de generar gráficas e informes diferentes que aportan información detallada sobre los eventos registrados a nivel de los equipos FortiGate. FortiAnalyzer es parte del servicio brindado en la nube por Tigo, pero también puede implementarse de forma adicional un equipo en las premisas del cliente.

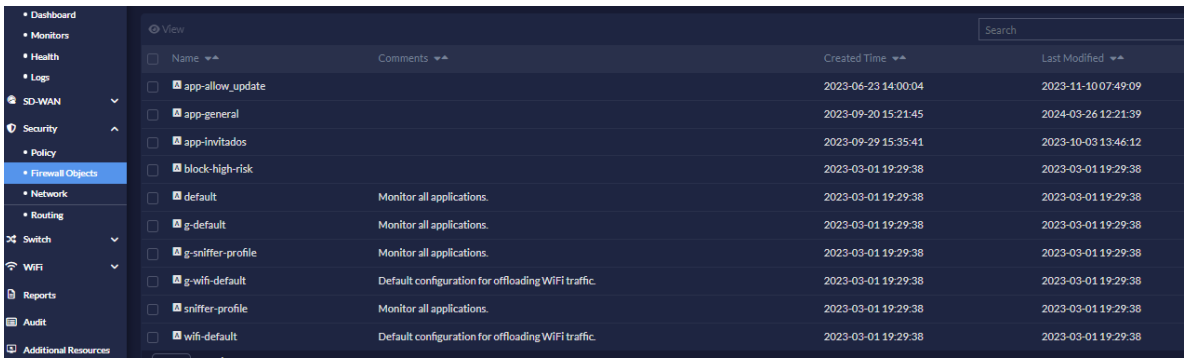
1.3.4.4 Analítica y reportes sd-wan

- **Visualización detallada de:** utilización de ancho de banda, disponibilidad, estado de los enlaces, top de consumo de ancho de banda por direcciones ip, top de aplicaciones, mapa de salud general, módulo de seguridad.











*Las imágenes son referenciales de la plataforma FortiPortal

Alcance FortiAnalyzer

Como parte de la solución se implementará la solución de FortiAnalyzer en modalidad virtual Centralizado en el DC Tigo, el cual permitirá analizar los Logs de los diferentes dispositivos Fortigate que hacen parte de la solución SDWAN Segura, a través de esta herramienta se sacaran los reportes sdwan, se tiene la posibilidad de entregar al cliente un usuario de gestión.

1.3.4.5 *FortiGuard Labs: Servicios de Seguridad.*

FortiGuard, la organización de Inteligencia e investigación de amenazas de Fortinet, constantemente desarrollan, innovan y mantienen uno de los sistemas de Inteligencia Artificial y Machine Learning más reconocidos y galardonados de la industria.

FortiGuard está integrado en todas las plataformas de seguridad de Fortinet (FortiGate, FortiClient, FortiNAC, FortiAnalyzer, etc) para entregar la mejor protección, visibilidad, y continuidad del negocio en todo el Security Fabric, protegiendo a los clientes de las amenazas cada vez más cambiantes y sofisticadas.

La plataforma de FortiGuard procesa más de 100.000 Millones de eventos diarios en promedio, para entregar más de 1.000 Millones de actualizaciones de seguridad a diario sobre todas las plataformas de Fortinet.

FortiGuard se ha acreditado más de 841 descubrimientos de Malware de día cero, un récord inigualable por cualquier otra marca de Ciberseguridad.

1.3.1 Equipos propuestos en la solución

Los siguientes son los equipos propuestos para la solución en las sedes:

Sedes Remota

FortiGate 50G



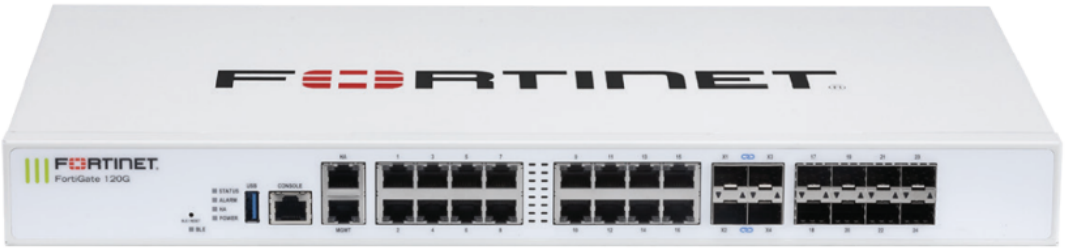
IPS	NGFW	Threat Protection	Interfaces
2.25 Gbps	1.25 Gbps	1.1 Gbps	Multiple GE RJ45 | Variants with 5G, PoE, DSL, SFP, WiFi, and/or storage

Ficha Técnica General:

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-fortiwifi-50g-series.pdf

Sede Ppal

FortiGate 120G



IPS	NGFW	Threat Protection	Interfaces
5 Gbps	3.5 Gbps	3 Gbps	Multiple GE RJ45, GE SFP, and 10 GE SFP+ slots

Ficha Técnica General:
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-120g-series.pdf

NOTA:

- En caso de no contar con estas referencias en el momento de implementar los servicios, se podrán utilizar equipos de similares características técnicas que cumplan con los requerimientos de la solución.
- El rendimiento y escalabilidad está limitada al hardware y licenciamiento del equipo según la hoja de datos del fabricante

1.3.2 SD-WAN Segura (SD-WAN + Internet Seguro Avanzado)

Este servicio permite consolidar varios canales (Internet/Internet) del cliente en una interfaz de tipo SD-WAN y distribuir el tráfico del cliente a través de estos basados en algoritmos de balanceo (Volumen, Sesiones, Spillover, IP Origen-Destino, IP Origen). Es posible monitorear la salud de los canales basados en parámetros de latencia, Jitter y pérdidas de paquetes y en base a esta información hacer la distribución del tráfico.
Las reglas de SD-WAN permiten definir para flujos de tráfico específico, basado en direcciones IP, puertos, aplicaciones o servicio de internet a consultar definir el canal o los canales por los cuales se enviará el tráfico.
Este servicio además de incluir reglas de firewall basadas en Capa 4 (Puertos TCP/UDP) y en Capa 7 (por aplicaciones), permite configurar los siguientes perfiles avanzados de seguridad: Antivirus/Antimalware, IPS, control de aplicaciones, filtrado web para los flujos de tráfico que el cliente considere necesario. Las reglas de seguridad pueden ser configuradas basadas en direcciones IP o en usuarios a través de la integración con el directorio activo del cliente.

- **Firewall**: este servicio provee un primer nivel de seguridad que permite filtrar el tráfico de entrada y salida a la red de acuerdo con una lista de reglas definida.
  El Firewall es un servicio básico que suele complementarse con otros servicios de seguridad para ayudar a prevenir eventos que impacten la confidencialidad, integridad y disponibilidad de la información y servicios de la compañía.

A través de esta funcionalidad se protege el acceso a segmentos de red de importancia para la compañía, así como a puertos TCP/UDP de servicios críticos para el negocio.

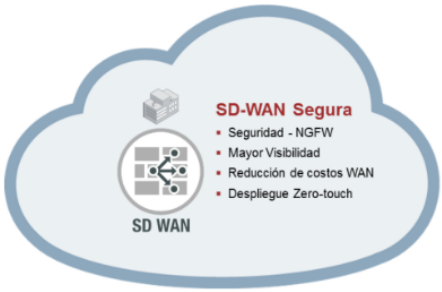
- **Antivirus / AntiMalware:** con esta funcionalidad, la solución permite detectar la existencia de un archivo infectado en una transmisión y sustituirlo por un mensaje de alerta, también es capaz de bloquear ficheros de un tipo específico (.bat, .exe, etc) que potencialmente sean contenedores de virus o bien bloquear ficheros con un determinado patrón en el nombre. El servicio incluye 3 perfiles de este tipo.

- **Detección y prevención de Intrusos (IDS/IPS):** esta funcionalidad constituye un sensor de red en tiempo real que utiliza definiciones de firmas de ataques y detección de comportamientos anómalos para detectar y prevenir tráfico sospechoso y ataques de red. La funcionalidad de IPS detecta y previene los siguientes tipos de ataques: ataques de denegación de servicio (DoS), ataques de reconocimiento, exploits, ataques de evasión de sondas IDS y botnets. El servicio incluye 3 perfiles de este tipo.

- **Control de Aplicaciones**: con esta funcionalidad, la solución permite detectar y tomar medidas contra el tráfico de red en función de la aplicación. El control de aplicaciones utiliza los decodificadores IPS que pueden analizar el tráfico de red para detectar el tráfico de aplicaciones, incluso si el tráfico utiliza los puertos o protocolos no estándar. Esta funcionalidad permite Ir más allá del control tradicional de nivel 4 de los firewalls convencionales, pudiendo así controlar aplicaciones evasivas o que cambien de puerto con frecuencia y obtener una mayor visibilidad de la red, de forma que sea posible conocer en profundidad y con detalle el uso que se hace de este recurso por parte de cada usuario de la organización. El servicio incluye 3 perfiles de este tipo.

- **Filtrado Web:** esta funcionalidad permite el monitoreo y el control del uso que los funcionarios hacen de los accesos a Internet y la prevención de visualización de contenidos web inapropiados, o no autorizados**.** La solución puede ser configurada para escanear toda la cadena del contenido del protocolo http permitiéndonos filtrar direcciones URL potencialmente no asociadas al desarrollo de la normal actividad laboral, contenidos embebidos en las propias páginas web o scripts basados en java, activeX o cookies, contenidos potencialmente peligrosos. El servicio de filtrado de contenidos web posee una clasificación actualizada de forma continua que engloba más de dos mil millones de URL´s distribuidas en un abanico de 77 categorías. El servicio incluye 3 perfiles de este tipo.

Este servicio incluye también de conexiones remotas de VPN (cliente a sitio) que permiten a los usuarios remotos acceder de forma segura a los archivos, aplicaciones y servicios disponibles y conexiones remotas de VPN (sitio a sitio) que permiten establecer conexiones seguras centre oficinas o terceros IPsec sobre redes WAN públicas.



1.3.3 Características de Seguridad a Implementar para el DIA

Se presentan los features de seguridad disponibles en la solución para las sedes en las cuales se desea que la navegación sea de manera segura a través del equipo sdwan:

- Firewall Capa 3, 4 y 7
- Web Filtering (El servicio incluye 3 perfiles de este tipo)
- App Control (El servicio incluye 3 perfiles de este tipo)
- Antivirus Perimetral (El servicio incluye 3 perfiles de este tipo)
- IPS/IDS (El servicio incluye 3 perfiles de este tipo)
- VPN S2S/C2S
- Integración con Directorio Activo
- Inspección Certificado SSL

NOTAS:

- En caso de requerirse una funcionalidad adicional de Seguridad se deberá validar su viabilidad en una nueva factibilidad
- Dentro de la fase de implementación se definirá en conjunto con el cliente las políticas de seguridad a configurar en los dispositivos
- Se mantendrá la línea base de seguridad configurada actualmente en la sede ppal
- (En caso de requerirse) Para la implementación de SSL Decryption es necesario que el cliente distribuya e instale el certificado emitido por Fortinet en los navegadores de usuarios
- Dependiendo de la cantidad de usuarios que tenga la organización se podría necesitar para la integración con AD de un componente adicional (FortiAuthenticator), esto se valida en una nueva factibilidad

1.3.4 Red de Transporte Sdwan

1.3.4.1 Internet

Con el fin de brindar una mayor seguridad, privacidad, flexibilidad y disponibilidad en los accesos de internet que son usados para construir el overlay de SD-WAN SEGURO y navegar hacia SaaS; a continuación, se muestran las características técnicas del servicio a ofertar las cuales se adecuan perfectamente a las necesidades del cliente:

Beneficios

- **Dispone de direcciones de IP fijas** (aplica dependiendo del producto) que lo identificarán en el mundo de Internet para aplicaciones como cámaras IP, servidores propios de archivos y de correo, equipos de videoconferencia, telefonía IP, entre otros.
- **Alta disponibilidad**, gracias a que contamos con tecnología de punta y personal capacitado, para garantizar un servicio de excelente calidad y desempeño.
- **Mantener una conexión permanente** y confiable en Internet, para que realice negociaciones en línea y transacciones con el mundo.
- **Soporte 7x24 durante todo el año**, con personal calificado y tiempos de respuesta adecuados a las necesidades de su Empresa.
- **Ejecutivos altamente capacitados** en las diferentes ciudades para brindarle asesoría permanente y personalizada.
- **Integración con todo el portafolio de servicios** y complemento de la conectividad de su empresa, a través de diferentes medios y tecnologías a escala nacional: Voz, Conectividad Nacional, Data Center, entre otros.

Para corresponder a las exigencias de su Empresa ponemos a su disposición las siguientes características en el servicio de Internet Dedicado sobre tecnología Fibra Óptica:

- Contamos con seis (6) grandes nodos de Internet que se encuentran ubicados en sitios geográficamente diferentes con salida internacional hacia los cinco (5) cables submarinos y diferentes proveedores de contenido en Estados Unidos (USA), que nos permite manejar de una manera distribuida las conexiones con nuestros usuarios y proveedores, brindando una mayor disponibilidad y confiabilidad a sus servicios.
- Una Red de transmisión nacional e internacional con anillos de fibra óptica, totalmente respaldada en configuraciones redundantes con balanceo de tráfico hacia el Backbone de Internet (columna vertebral de Internet), donde están concentrados los principales nodos y proveedores Tier1 de Internet con los que estamos interconectados en el NAP de Las Américas, principal punto de interconexión de las redes internacionales de Latinoamérica y el resto del mundo.
- Puntos de presencia en las principales ciudades del país.
- Enrutadores tipo Carrier Class, en un esquema de máxima disponibilidad: fuente y procesador redundantes y múltiples conexiones.

- Conexión directa con el NAP Colombia, el cual es el punto de conexión nacional de las redes de las empresas que proveen el servicio de acceso a Internet en nuestro país.
- Esquemas de configuración y diferenciación del servicio, realizando balanceo de redes, enlaces y tráfico.
- Alta disponibilidad con esquemas de resarcimiento y excelentes tiempos de respuesta.
- Amplia variedad de velocidades de acceso que permiten ajustarse a sus necesidades de conectividad.

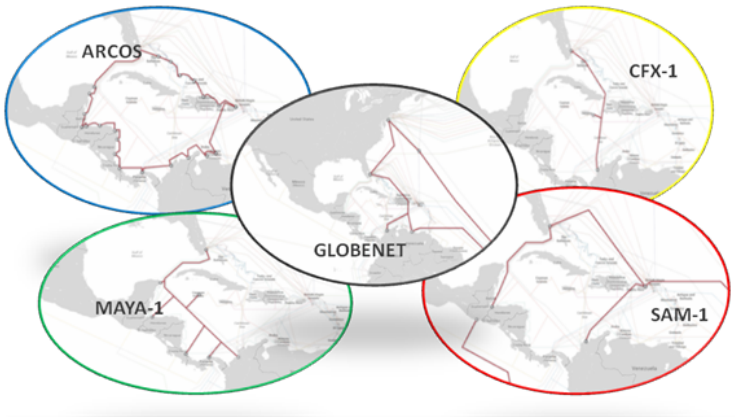


Ilustración - Cables Submarinos

Servicios Incluidos:

- **Direcciones IPv4:** Se entregan según el medio de acceso

1.4 SERVICIOS ADMINISTRADOS SDWAN

1.4.1 Enterprise

Este reporte se entregará de manera mensualizada por cliente, con la siguiente información:

SD-WAN

Rendimiento de SD-WAN:

- Resumen del Dispositivo
- Disponibilidad de SD-WAN
- Latencia
- Jitter
- Pérdida de Paquetes
- Estado de Salud de Enlace SD-WAN
- Calidad del Enlace SD-WAN

Utilización de SD-WAN:

- Utilización de Tráfico por Regla de SD-WAN
- Distribución de Tráfico
- Utilización de Tráfico por Miembros de SD-WAN a lo Largo del Tiempo

- Aplicaciones de SD-WAN
- Distribución de Tráfico por Aplicación
- Principales Aplicaciones de SD-WAN por Volumen de Tráfico y Sesión
- Distribución de Tráfico del Dispositivo SD-WAN por Interfaz y Aplicación

Usuarios de SD-WAN:

- Principal Fuente de SD-WAN por Volumen de Tráfico
- Principal Fuente de SD-WAN por Aplicación y Volumen de Tráfico

Seguridad

- **Top 10 categorías URL:** consumo de ancho de banda promedio por categoría.
- **Top 10 Source Address:** consumo de ancho de banda promedio por IP origen.
- **Top 10 Destination Address:** consumo de ancho de banda promedio por IP destino.

Notas importantes:

- El detalle a nivel del reporte dependerá del Plan contratado para cada sede, pues cada plan tiene un alcance definido por funcionalidades.
- Los reportes contarán con data histórica de un (1) mes.

Monitoreo y Autogestión

Nuestro equipo de especialistas de servicios administrados estará monitoreando el desempeño de la red y aplicando las acciones necesarias para mitigar afectaciones en la experiencia de usuario final. Accediendo a la plataforma SD-WAN podrá monitorear sus servicios ya sea con visualizaciones en tiempo real o histórica de un (1) mes.

Nota importante:

- El acceso al portal debe ser solicitado de forma explícita por el cliente y puede solicitar hasta dos (2) usuarios máximos.
- El acceso de portal cliente será Forti Portal.

Adicionalmente el cliente podrá solicitar los siguientes cambios mensuales:

Número de Solicitudes	**Tiempo de gestión**
hasta 10 por mes de los siguientes componentes	**Hasta 24 horas (hábiles)**
Solicitud de información	X
Cambios en políticas de enrutamiento inteligente SD-WAN	X
Configuración del DIA (acceso directo a internet) *	X
Cambios en reglas de firewall **	X
Segmentación de tráfico***	X
Cambio en las políticas de control de aplicaciones**	X

Recategorización de las políticas de filtrado de contenido**	X
Cambios en las políticas actuales en la integración con el directorio activo**	X
Modificación en políticas existentes de Antivirus	X
Crear y modificación de usuario para acceder al portal cliente*****	X
Creación y modificación de VPN IPSEC S2S****	Max 5 dominios de encripción

Consideraciones:
Los cambios sobre configuraciones existentes o habilitación de nuevas características que no estén descritas en la tabla anterior deben ser gestionadas a través del ejecutivo comercial para ejecutarlas a través de servicios profesionales.
(*) Si es habilitar o modificar políticas sobre el DIA ya configurado se gestiona a través de soporte, si la solicitud es implementar un nuevo canal para activar el DIA, se debe gestionar a través del ejecutivo comercial.
(**) En algunos casos estas actividades podrían llegar a tomar hasta 36 horas hábiles.
(***) El equipo de soporte factibilizará si está dentro de su alcance o si es necesario que se gestione a través del ejecutivo comercial.
(****) Max 5 dominios de encripción (previo formato diligenciado y socializado) 5 VPN IPSEC. Si se requiere VPN SSL será necesario agregar un equipo adicional.
(*****) Max 2 usuarios por cliente
Las solicitudes serán evaluadas por el equipo de soporte centralizado, se analizará si se requiere un proyecto para factibilizarlo, vía ejecutivo comercial y el costo adicional.

1.5 MODELO DE ADMINISTRACIÓN COMPARTIDA SDWAN (*FortiPortal)*

Roles y responsabilidades (*)	Tigo	Cliente
Disponibilidad de acceso a portales de plataformas	X	
Configuración/creación cliente en plataforma	X	
Creación de usuario/cliente en plataforma con el perfil acordado	X	
Atención de incidentes asociados a plataformas	X	
Atención de incidentes asociados a configuraciones realizadas sobre el servicio y asociadas a los permisos otorgados en el perfil de usuario/cliente		X
Insights	X	
SD-WAN		
Configuration		X
Security		
Policy		
Security Policy		X
Central SNAT		X
Central DNAT		X
IPv6 Central DNAT		X
NAT64-NAT46 Policy		X

Roles y responsabilidades (*)	Tigo	Cliente
Proxy Policy		X
Authentication Policy		X
IPv4-IPv6 Multicast/ Local in / DoS / Interface Policy		X
Traffic Shaping Policy		X
Firewall Policy		X
Firewall Objects		
Address		X
Schedule		X
Service		X
Virtual IP		X
Antivirus Profile		X
Application Control		X
File Filter Profile		X
Intrusion Prevention Profile		X
Web Filter Profile		X
Local Category		X
Web Rating Overrides		X
Video Filter		X
SSL/SSH Inspection		X
User		X
User Groups		X
Network		
IPSec Phase 1	X	
IPSec Phase 2	X	
Static Route	X	
DHCP Server	X	
Certificate	X	
Routing	X	
Switch		
Configuration		X
WiFi		
Configuration		X
Reports		X

FWaaS= Aplica única y exclusivamente para el siguiente caso de uso:

- Caso de uso: Navegación segura on-premises.

(*) Los anteriores roles y responsabilidades intentan dar claridad del alcance para cada una de las partes y las tareas con relación a los servicios de SD-WAN/FWaaS y ayudan a guiar a los clientes sobre cuándo y cómo se deben realizar ciertos servicios operativos, que se definen a continuación:

- Disponibilidad de acceso a portales de plataformas: Se refiere a mantener la disponibilidad de los portales entregados al cliente para su gestión del servicio.
- Configuración/creación cliente en plataforma: refiere al aprovisionamiento inicial del servicio contratado por el cliente.
- Creación de usuario/cliente en plataforma con el perfil acordado: refiere a la generación de los accesos que serán entregados al cliente para su posterior gestión del servicio según los perfiles

respetivos. Este servicio no permitirá la creación de usuario genéricos, con el fin de garantizar la trazabilidad de la administración por ambas partes.

- Configuración de reglas de firewall: refiere a la capacidad de poder crear reglas y objetos a nivel de seguridad de firewall como apertura de puertos de origen/destino, salida y/o entrada de tráfico desde y hacia la red local, además de traducciones de red NAT
- Configuración de reglas de filtrado de contenido: refiere a la capacidad de poder crear reglas a nivel de filtrado de tráfico basados en patrones o tipos de categoría de conexiones desde y hacia la red local y así controlar la información que un usuario de internet puede ver
- Configuración de reglas de aplicaciones de control (APP Control): refiere a la capacidad de poder crear reglas de aplicación para el análisis de tráfico hasta la capa 7 de aplicaciones. Esta protección es usada para controlar aplicaciones riesgosas y no deseadas en la red
- Creación/Modificación/Eliminación de usuarios para la conexión a través de VPN IPSEC Client to Site: refiere al privilegio de crear, modificar o eliminar usuarios que podrán tener acceso a la red del cliente a través de una VPN IPSEC (Virtual Private Network) Client to Site.
- Consumo y manejo de la seguridad de los datos: refiere al adecuado consumo de los datos de las aplicaciones que fluyen por la red, velando por su correcto aseguramiento basado en las políticas de reglas de firewall, filtrado de contenido y aplicaciones de control del tráfico definidas
- Manejo de las credenciales de acceso usuario/cliente al portal e identidad de los accesos: refiere al adecuado uso y manejo de los accesos a los portales de gestión del servicio entregados al cliente según los perfiles respetivos
- Atención de incidentes asociados a plataformas: refiere al soporte y atención de los incidentes asociados a las plataformas principales que estén afectando el servicio final contratado por el cliente
- Atención de incidentes asociados a configuraciones realizadas sobre el servicio y asociadas a los permisos otorgados en el perfil de usuario/cliente: refiere al soporte y atención de los incidentes sobre las configuraciones realizadas por el cliente

Implicaciones para Cliente

A continuación, se establecen las implicaciones e impactos que asumiría el cliente, bajo este esquema de administración y conforme a los roles y responsabilidades, anteriormente descritos:

- Caídas o indisponibilidades del servicio, derivados de las configuraciones o modificaciones a las que el cliente tenga acceso establecidas en la tabla 1 de responsabilidades.
- Impacto en los niveles de servicio, derivados de las configuraciones o modificaciones a las que el cliente tenga acceso establecidas en la tabla 1 de responsabilidades.
- Modificar parámetros sensibles de auditorías.
- Costos adicionales, derivados de servicios profesionales para la normalización del servicio; para resolver los incidentes ocasionados por configuraciones en las que el cliente tenga acceso establecidas en la tabla 1 de responsabilidades.

- Infiltración y materialización de cualquier tipo de amenaza o ataque de seguridad al realizar una configuración inadecuada en las reglas de firewall.
- Materialización de un ataque de DoS o DDoS al realizar publicaciones de servicios en las reglas de firewall.
- Infiltración y materialización de cualquier tipo de amenaza o ataque de seguridad al realizar publicaciones de servicios (NAT) en las reglas de firewall
- Infiltración y materialización de cualquier tipo de amenazas o ataque de seguridad al permitir aplicaciones, URLs o dominios.
- Infiltración y materialización de cualquier tipo de amenaza o ataque de seguridad en la conexión de los usuarios a la red del cliente a través de VPN IPSEC (Virtual Private Network) Client to Site.
- Cualquier riesgo, exposición o vulnerabilidad que se derive de una configuración desde el perfil del cliente, queda bajo responsabilidad de este.

Responsabilidad del Cliente

- El cliente deberá notificar al canal de comunicación que le corresponda de acuerdo con su oferta de servicio, cualquier cambio sobre el alcance establecido en este documento que esté asociado a su rol o responsabilidad.

Limitantes y Exclusiones

- Los SLA asociados a cambios realizados por incorrectas configuraciones de perfil usuario/cliente no serán impactados, ni aplicarán resarcimientos.
- Tigo no es responsable de la configuración, soporte y monitoreo de los roles y responsabilidades del cliente, ni las consecuencias que estas conlleven ante una configuración inadecuada.
- El cliente acepta y comprende que en caso de materialización de los riesgos descritos en el presente anexo y que sean de su competencia, exime al proveedor de cualquier responsabilidad y consecuencias a que estas conlleven.
- Tigo no es responsable de las indisponibilidades del servicio que surjan por cambios efectuados por el cliente bajo sus roles o responsabilidades; independiente de las Notificaciones que brinde el cliente sobre los cambios que ejecute.
- Cuando el cliente requiera apoyo de Tigo en alguno de sus roles y responsabilidades, deberá evaluarse el requerimiento como un nuevo proyecto y definir si el apoyo requiere servicios profesionales, los cuales deberán ser cotizados con base a la necesidad o casuística específica.
- En caso de presentarse una falla y, como medida correctiva, se deba aplicar la configuración inicial, el SOC aplicará la plantilla con la que se implementaron los servicios inicialmente. Por ende, el cliente será el responsable de volver a actualizar los cambios de su rol o responsabilidad.

1.6 SUPUESTOS, RESTRICCIONES Y RESPONSABILIDADES

- ✓ La implementación de soluciones en sedes distintas a las mencionadas anteriormente no se encuentra contemplada en el alcance de esta propuesta.
- ✓ Todas las adecuaciones o instalaciones de cableado, rack, energía y demás necesarias para el funcionamiento en el centro de datos o el lugar asignado por el cliente en sus empresas y sitios involucrados en el servicio ofrecido son responsabilidad total de este, en cumplimiento de las especificaciones del fabricante necesarias para la instalación y funcionamiento adecuado de la solución ofrecida.
- ✓ Se asume que se cuentan con los permisos a cada una de las sedes o Data Centers para la instalación de los equipos de comunicaciones, en caso de no tener previamente los permisos a las sedes en las cuales se instalará el servicio, el CLIENTE gestionará dichos permisos
- ✓ Se asume que el cliente tendrá configurado sus equipos intermedios (switch) para la recepción de la conectividad.
- ✓ Se asume que el cliente tendrá puertos disponibles en sus equipos de acceso para la recepción de la conectividad desde los CPE
- ✓ No se incluye suministro de racks, cableados, accesorios, hardware /software, etc diferentes a los incluidos en esta oferta
- ✓ No se incluye configuración de equipos no incluidos en esta oferta.
- ✓ No se incluye toda actividad no incluida en los alcances del servicio.
- ✓ El cliente dispondrá del personal propio o de sus terceros necesario durante el desarrollo del proyecto para poder garantizar los tiempos de entrega y calidad del servicio.
- ✓ Se asume que el cliente proporcionará los parámetros e información necesaria para la configuración de los equipos.
- ✓ Se asume que el soporte aplica para los dispositivos y cableado suministrados por Tigo para proveer su solución de conectividad SDWAN.
- ✓ En caso de requerirse trabajos adicionales, esto se cotizará por separado, en común acuerdo con Tigo
- ✓ En caso de que se presente un incidente de seguridad, será responsabilidad del CLIENTE establecer la denuncia con la entidad pertinente, posterior a esto es responsabilidad del CLIENTE solicitar a través de un caso de soporte técnico, las evidencias digitales como logs, de los diferentes dispositivos, para contribuir a la investigación en el caso en el que la entidad pertinente lo considere.
- ✓ Los servicios se considerarán aceptados por resultados y entregables definidos.
- ✓ Entre Tigo y el CLIENTE acuerdan que la terminación exitosa del proyecto requiere de una mutua buena fe de cooperación. Los acuerdos, aprobaciones, aceptaciones, consentimientos o acciones similares de cualquier parte se requieren para cualquier producto de este servicio, tal acción no será retardada o retenida sin razón.

- ✓ Es responsabilidad del CLIENTE suministrar el espacio físico con condiciones ambientales y eléctricas adecuadas para el alojamiento de los diferentes equipos que hacen parte de esta solución.
- ✓ La referencia de los equipos para las sedes se especificó de acuerdo con el requerimiento del cliente por lo tanto el rendimiento y escalabilidad está limitada al hardware y licenciamiento del equipo según la hoja de datos del fabricante.
- ✓ Cualquier servicio o solicitud que no estén claramente especificados en este documento se encuentran por fuera del alcance.
- ✓ Tanto Tigo como el CLIENTE serán responsables en conjunto de definir el alcance de la configuración y los tiempos establecidos para el proyecto que se especifican en este documento.
- ✓ Sobre cualquier situación inesperada que pueda presentarse durante el proyecto, Tigo y el CLIENTE aplicarán el buen juicio y sentido común cuando se determinen roles, costos y responsabilidades requeridas para la resolución.
- ✓ El CLIENTE será responsable por los retrasos generados por imprevistos causados por trabajos de terceros y/o del cliente que se encuentran fuera del alcance del presente servicio y que puedan tener alto impacto sobre el éxito del proyecto.
- ✓ **Los servicios del proponente: "Tigo" de la propuesta se entregan así:**
  - **Direcciones IPv4: El servicio se entrega configurado con un (1) bloque de ocho (8) IP de las cuales cinco (5) podrán ser usadas en las configuraciones que usted requiera en su servicio.**
  - **Red de direcciones IPv6: En la modalidad de Dual Stack cuando sean requeridas por el cliente**
- ✓ **Los servicios de SDWAN del proponente: "Tigo" se prestarán desde el primer día por un servicio de internet dedicado para evitar interrupciones a la operación y afectaciones al servicio del cliente Instituto de Movilidad de Pereira; una vez legalizado el contrato con el cliente y con el acta de inicio se organizará un cronograma para la implementación de los servicios de SDWAN en las 2 sedes del cliente, donde se implementaran los enlaces configurados para la prestación del servicio oferta en esta propuesta.**

1.6.1 Consideraciones generales:

Hace parte de la presente oferta las siguientes consideraciones a efectos de establecer el alcance de las actividades y compromisos de las partes para la adecuada prestación de los servicios contratados:

1.Definiciones:

Incidente de seguridad digital: Ocurrencia de una situación que pone en peligro la confidencialidad, integridad o disponibilidad de un sistema de información o la información que el sistema procesa, almacena o transmite; o que constituye una violación a las políticas de seguridad, procedimientos de seguridad o políticas de uso aceptable.

Infraestructura crítica cibernética: Sistemas y activos, físicos o virtuales, soportados por Tecnologías la Seguridad de la Información, cuya afectación significativa tendría un impacto grave en el bienestar social o económico de los ciudadanos, o en el funcionamiento efectivo del gobierno o la economía.

Ciberseguridad: Es el proceso de proteger los activos de información por medio del tratamiento de las amenazas a la información que es procesada, almacenada y/o transportada a través de sistemas de información interconectados.

Incidente de Seguridad: Es un evento inesperado y no deseado que compromete la Seguridad de la Información.

Evento de seguridad: Un evento de seguridad de la información indica que el sistema, la seguridad o los servicios de red y de infraestructura han sido comprometidos o vulnerados. Esto indica que los controles implementados han fallado y/o que no se ha seguido la política de seguridad de la información de la organización

Cualquier ocurrencia relacionada con los activos o el entorno que indique un posible compromiso de las políticas o la falla de los controles, o incluso una situación no asignada que pueda afectar a la seguridad.

LIMITACIONES DE RESPONSABILIDAD:

Tigo no será responsable por la prestación del servicio en los siguientes eventos:

1. Cuando las interrupciones, caídas, problemas o deficiencias en los servicios o afectación de indicadores tengan origen en la infraestructura física y tecnológica del CLIENTE.

2. En los eventos de errores, decisiones, cambios en procesos y procedimientos por parte de EL CLIENTE que no hayan sido oportunamente informados al SOC.

3. En aquellos casos en los cuales los sistemas, plataformas y aplicativos del CLIENTE que no hagan parte de los sistemas, servicios o componentes de los servicios Ciberseguridad contratados, y éstos tengan falencias de seguridad que faciliten eventos de fraudes, hayan sido o no detectadas y/o advertidas por Tigo.

4. Por fuerza mayor o caso fortuito.

En caso de presentarse suspensión o afectación del servicio por cualquiera de los eventos señalados en los numerales 1 ,2 y 3 el cliente asumirá los costos en los que incurrió Tigo, por la no prestación del servicio, durante el período de tiempo que dure la suspensión o afectación del mismo.

OBLIGACIONES ADICIONALES DEL CLIENTE:

EL CLIENTE deberá realizar copias de seguridad de su información en el medio que considere pertinente.

EL CLIENTE es el directo responsable de la Información que se ingrese procese, genere y mantenga en relación del uso de sus equipos y servicios de CIBERSEGURIDAD y deberá garantizar el cumplimiento adecuado y oportuno de la implementación de las mejores prácticas que el equipo de SOC, NOC remoto le informe.

El cliente será responsable de implementar las configuraciones y demás recomendaciones que le entregue Tigo en aras de cumplir con el alcance de los servicios ofrecidos. En caso que éstas no sean debidamente implementadas en su totalidad, Tigo no será responsable de los efectos, vulnerabilidad, amenazas o efecto adverso que se derive de esta situación.

Es responsable de autorizar la contención de los riesgos detectados y notificados; de no autorizar la contención, Tigo no será responsable de los riesgos o la posible materialización de un evento de seguridad.

REGIMEN DE RESPONSABILIDAD

Igualmente y tratándose de Servicios Administrados de Ofimática, Conectividad, Voz y Colaboración, Movilidad, Infraestructura de TI, Cloud, Data Center, Servicios Administrados y Seguridad, Tigo no garantiza resultado alguno por los usos y/o aplicaciones específicos que realice EL CLIENTE y de manera particular por: (a) Interrupciones de los servicios originadas en causas ajenas a su control, tales como: mal funcionamiento de Internet, problemas satelitales, interrupción o insuficiencia de energía eléctrica, huelgas, desastres naturales, conflictos bélicos, actos de la autoridad, etc.; (b) pérdida de datos almacenados en el servidor, ya sea por causas imputables al CLIENTE, por fallas en el sistema, por eventos o incidentes de seguridad perpetuados por terceros (por ejemplo ataques de denegación de servicio, virus, malware, ransomware, entre otros) que comprometan la integridad, confidencialidad o la disponibilidad de la información o por actualización de los servidores; (c) demoras en los trámites de Registro de Dominio y transferencias de DNS por causas imputables al CLIENTE o a terceros; (d) por fraude cometido por El CLIENTE o por terceros; (e) por fallas de tipo técnico tales como la seguridad informática de los ambientes en hosting, cloud y de soluciones de terceros atribuibles al CLIENTE o a terceros; (f) en caso de ataques informáticos a los PBX por causas imputables al CLIENTE. En caso de que en la Orden de Compra y/o Servicio se incluya la entrega al CLIENTE de cuentas administradoras de cualquier servicio, EL CLIENTE exime a Tigo de cualquier evento de indisponibilidad, seguridad y confidencialidad que pueda ocurrir. Adicionalmente, en los casos en que EL CLIENTE solicite deshabilitar y/o desinstalar las herramientas de Antivirus implementadas por Tigo o por un tercero para proteger los servicios, EL CLIENTE exime a Tigo BUSSINESS de cualquier evento de indisponibilidad, seguridad, confidencialidad, virus, malware, ransomware o cualquier otro software malicioso que pueda generar algún tipo de afectación durante la prestación del servicio. Esto aplica para cualquier servicio que se pueda afectar con la deshabilitación solicitada. Parágrafo: Cuando se trate de servicios de Cloud para distribuidores o revendedores, Tigo no será responsable de la prestación o suministro de servicios (venta, aprovisionamiento, soporte técnico, licenciamiento y demás) frente al cliente final.

Exclusión de responsabilidad por daños indirectos y otros. Sin perjuicio de los casos en que la ley aplicable prohíba la limitación de responsabilidad por daños, Tigo no se responsabilizará en ningún caso de daños directos e indirectos, cualquiera que sea su naturaleza u origen incluidos, entre otros los daños por lucro cesante, pérdida de la información confidencial o de otro tipo, interrupción de negocios, pérdida de privacidad, incumplimiento de obligaciones (ya sea de buena fe o con diligencia razonable, negligencia y cualquier perdida pecuniaria o de otro tipo)], que se deriven o de otro modo este relacionados con la materialización de un incidente de seguridad. Tigo se excluye expresamente cualquier responsabilidad por falta de disponibilidad del servicio y/o de equipos del CLIENTE en un momento determinado, ya sea por causas técnicas, tareas de mantenimiento del sistema no notificadas al SOC, falla eléctrica en las instalaciones del CLIENTE y todas aquellas que estén bajo su control y gestión.

1.7 IMPLEMENTACIÓN Y/O TRANSICIÓN

1.7.1 Metodología de Aprovisionamiento

Para llevar a cabo la entrega de una solución operativa al cliente, Tigo asigna un **Ingeniero de Desarrollo de Soluciones** responsable de canalizar las necesidades y comunicaciones del cliente e integrar tecnológicamente los proveedores y aliados requeridos para ello.

El **Ingeniero de Desarrollo de Soluciones** utiliza metodologías y herramientas de gestión de proyectos para realizar el aprovisionamiento de la solución. En el inicio y planificación del proyecto, analiza el alcance de la solución, identifica los riesgos y controles del proyecto, solicita los recursos requeridos y construye el plan de trabajo asociado. En la ejecución realiza reuniones de inicio y empalme con el cliente y las áreas, proveedores y aliados involucrados, realiza monitoreo y seguimiento al plan de trabajo y los riesgos del proyecto, interventoría, recepción y pruebas de servicios y equipos que componen la solución. Para el cierre del proyecto se realiza la entrega formal al cliente, se actualiza la topología de la solución, se realiza la entrega para su operación y soporte, se aprueba el pago a proveedores y/o aliados involucrados y se realiza el cierre y soporte documental del proyecto en los sistemas de información pertinentes.



1.7.2 Tiempo de Aprovisionamiento

La duración del aprovisionamiento es de **5** días calendario, a partir del perfeccionamiento del contrato y de la reunión de inicio
Debido a que la factibilidad de acceso es dada por cobertura, el proveedor, el medio, el tiempo de implementación y el precio está sujeto a factibilidad en sitio una vez perfeccionado el contrato.

CONSIDERACIONES

- En todo caso se realizará el mejor esfuerzo para tener implementado el servicio en el menor tiempo posible.
- Para la instalación de enlaces nuevos no se consideran los tiempos imputables a permisos con entidades municipales, entre otras.

- Se cuenta con equipos en stock para realizar la implementación de SDWAN, en caso de que no haya equipos en el momento de la contratación, se debe contar con los tiempos de importación vigentes al momento de la contratación.
- No se consideran los tiempos imputables a las adecuaciones internas por parte del cliente en sus sedes.
- Los plazos para las distintas fases de aprovisionamiento se establecerán de mutuo acuerdo con el cliente, sin embargo, en caso de presentarse situaciones de fuerza mayor o caso fortuito, o situaciones que estén fuera del contrato del proveedor, dicho plazo se podrá modificar dando aviso previo al cliente, sin que esto implique incumplimiento alguno por parte del proveedor

1.7.3 Entregables

Entregable	Descripción
Acta de entrega	Documento donde se realiza verificación y entrega de cantidad, calidad y operatividad de la solución de acuerdo a lo establecido en la oferta técnica.

1.7.4 Roles y responsabilidades

Se relacionan los roles y responsabilidades de Tigo y del cliente requerido durante el aprovisionamiento de la solución:

Actividad	Tigo	Cliente
Obras civiles externas necesarias para ampliación de red	X	
Condiciones ambientales adecuadas		X
Condiciones eléctricas		X
Adecuaciones en las premisas del cliente		X
Permisos de acceso en las premisas del cliente		X
Custodia de equipos		X
Aprovisionamiento de recursos	X	X
Análisis funcional	X	X
Diseño técnico	X	
Pruebas cualitativas funcionales y de servicio	X	X
Actividades de despliegue y puesta en marcha	X	X
Capacitación de 1 a 3 usuarios definido por el cliente – Aprox. 2 Horas	X	
Gestión del cambio	X	X
Acompañamiento post puesto en marcha	X	
Soporte y garantía	X	

1.7.5 Responsabilidades del Cliente

Garantizar el suministro, exactitud y completitud de toda la información requerida por Tigo. Si la información es incompleta o incorrecta, cualquier retardo o requisito adicional que pueda generarse para corregir los problemas originados por el uso de tal información incompleta o inexacta será tratado como una solicitud de cambio del Cliente al alcance del servicio, por lo tanto, estará sujeta al proceso de control de cambios lo que implicará una nueva factibilidad y posibles costos adicionales.

2 OFERTA ECONÓMICA

2.1 TARIFAS

Oferta económica.

Datos	Cantidad	Valor mensual antes de IVA	Valor mensual con IVA	Valor 4,5 meses con IVA
Sede 1 FIBRA 500 Mb + GPON 300 Mb	1	$ 2.463.303	$ 2.931.331	$ 13.190.990
Sede 2 FIBRA 500 Mb + GPON 300 Mb	1	$ 2.463.303	$ 2.931.331	$ 13.190.990
Paquete Voz y Datos Corporativo 4.5 Plus 85 GB	110	$ 5.285.238	$ 6.500.843	$ 29.253.794
Conectividad gestionada Individual Fijo 25 GB	10	$ 758.643	$ 933.131	$ 4.199.090
Total			$ 13.296.636	$ 59.834.864

NOTA: En todo caso, las partes podrán discriminar el pago de acuerdo con los servicios y/o bienes prestados o provistos por Tigo.

CONSIDERACIONES:

La aprobación es sobre la conformación del 100% de esta oferta.
Servicio a 4.5 meses o desde el acta de inicio hasta el 31 diciembre del 2026
Se deben activar todos los servicios relacionados para la entrega de los beneficios, no aplica para órdenes de compra parciales.
Los beneficios y/o características de los planes aplican durante la vigencia del contrato.
Oferta valida por 15 días y anula otras propuestas presentadas con anterioridad en este mismo sentido.
En caso de que se presenten cambios en la oferta se deberá realizar una nueva factibilidad.
No es compatible con otras promociones.
Tarifas sujetas a la Ley 1819 de 2016, IVA del 19% e impuesto al consumo del 4% sobre los servicios de datos móviles que superen la facturación de 1.5 UVT – Unidad de Valor Tributario.
La oferta infinita no aplica para usuarios que se encuentran en Roaming internacional.
Los paquetes de Whatsapp, Mail y Facebook Infinito permiten que los clientes puedan tener acceso a Whatsapp, Mail y Facebook hasta la fecha de corte, aun después de consumidos los recursos del paquete.

Los recursos infinitos están habilitados únicamente para necesidades de consumo del cliente empresarial, no aplica para actividades comerciales de reventa del servicio. Si se detecta el uso no autorizado (entre los que se encuentra la reventa) de este servicio será causal de cancelación de servicio.
Los recursos no utilizados de los paquetes y combos de los Planes Business se vencen cada mes y no serán acumulables.
Los Plan Business aplica con cobro vencido mes corriente.
Para las líneas que requieran servicio de Roaming, el cliente empresarial podrá adquirir el plan abierto de Plan Business. Las líneas en este plan solo podrán estar a nombre de la empresa. Los cobros de los consumos por Voz y Datos en Roaming se harán como cargo adicional a su factura del mes y no se generará descuento del plan básico. Aplican términos y condiciones del plan y del servicio de Roaming.
El plan abierto de Plan Business solo aplica para líneas que sean matriculadas en el portafolio de servicios de Planes Business.
El cliente empresarial podrá comprar en cualquier momento paquetes por demanda para asignarle recursos a una o más líneas que lo requieran, estos recursos asignados no tienen renovación automática y otorgan recursos de minutos, mensajes de texto, navegación y funcionan desde el momento de la compra hasta el próximo ciclo o corte de facturación del cliente empresarial.
Los productos y/o servicios que no se encuentren relacionados dentro de la oferta, no hacen parte de esta.
Tigo no maneja el concepto de prefactura.

2.2 FORMA DE PAGO

El pago se realizará mensualmente bajo contrato entre el cliente y COLOMBIA MOVIL SA ESP con un plazo de 60 días, se ofrece de posibilidad de inmunizar la cuenta para evitar suspensiones del servicio en caso de presentarte eventualidades con la facturación.

2.3 VALIDEZ DE LA OFERTA

Esta propuesta estará vigente durante 30 días calendario a partir de la fecha de la presente oferta, y anula otras propuestas presentadas con anterioridad en este mismo sentido. En caso de que se presenten cambios en la oferta se deberá realizar una nueva factibilidad técnica y económica.

3 COMPROMISOS DEL CLIENTE

Adicional a lo indicado en la oferta técnica y económica, el cliente se compromete a:

3.1 ACUERDO DE CONFIDENCIALIDAD

La información oral, escrita, gráfica, en lenguaje de máquina, o en cualquier otra forma conocida o no, incluyendo, pero sin limitarse a documentos, catálogos, cartas, correos electrónicos, memorandos, fórmulas, estadísticas, presentaciones que Tigo ponga en conocimiento del cliente en esta oferta se entiende que tiene un carácter eminentemente confidencial, en consecuencia, el cliente tendrá las siguientes obligaciones frente a la misma:

- Mantener la reserva de la información, y tomar todas las medidas razonables para protegerla, incluyendo, pero sin limitarse, todas las precauciones que el cliente utiliza respecto de su información confidencial.
- Abstenerse de usar, facilitar, divulgar o revelar, sin causa justificada y sin consentimiento de Tigo, cualquier información entregada o derivada de la misma, a cualquier tercero, o ponerla a su disposición o para su beneficio.

Propiedad intelectual e industrial
Toda invención, modelo de utilidad o diseño industrial creado por Tigo en cumplimiento de esta oferta será propiedad de Tigo conforme al Decreto 2591 de 2000, que reglamenta los Títulos II, III y V de la Decisión 486 de la Comisión de la Comunidad Andina. Por ende, el derecho a la patente de invención o de modelo de utilidad, o del registro del diseño industrial será titularidad de Tigo

3.2 USO DE LOS SERVICIOS

EL CLIENTE se obliga a acatar el régimen nacional e internacional sobre protección de terceros y derechos de propiedad intelectual, en especial las disposiciones establecidas en los tratados internaciones que vinculan a Colombia. Así mismo se compromete a cumplir las disposiciones de la Ley 679 de 2001 y sus decretos reglamentarios, teniendo en cuenta que su incumplimiento le acarreará las sanciones administrativas y penales allí contempladas impuestas por la autoridad competente; en tal sentido, deberá abstenerse de enviar, recibir, distribuir, transportar, almacenar y utilizar o archivar material pornográfico o de contenido sexual con utilización de menores de edad, así como de usar las redes globales de información para divulgación de material ilegal con menores de edad