



**tigo** business

**Oferta Técnica y Comercial  
Servicios de Internet,  
Ciberseguridad en Premisas  
Soluciones Digitales AWS  
Y UCaaS Webex Calling**

**COLEGIO MAYOR DE ANTIOQUIA**



Medellín, 13 de abril de 2026

Señores

COLEGIO MAYOR DE ANTIOQUIA

Ciudad

En Tigo Business entregamos diferentes servicios y soluciones tecnológicas que buscan acompañarlo en la evolución tecnológica de su empresa. Por esta razón y con el objeto de brindar una experiencia de comunicación memorable y a su medida hoy le presentamos, para su evaluación, una propuesta pensada en sus necesidades y acorde al crecimiento de su negocio y su operación.

Ponemos a su disposición todo nuestro capital humano y tecnológico para entregarle el mejor servicio que le permita una adecuada y mejor utilización de los productos que actualmente tiene de nuestro portafolio.

Gracias por su confianza.

Cordial saludo,

  
**Víctor Andrés Trujillo Mestra**

Ejecutivo de Cuenta

**Teléfono celular:** 300 774 3163

**Correo electrónico:** victor.trujillo@tigo.com.co

*El contenido de esta oferta, presentada por UNE EPM Telecomunicaciones S.A., en adelante Tigo Business, es meramente enunciativo y no es vinculante. Esta propuesta estará vigente por 30 días calendario contados a partir de la fecha de presentación, y anula otras propuestas presentadas con anterioridad al cliente en este mismo sentido. En todo caso, los términos de esta podrán modificarse por parte de UNE de acuerdo con las condiciones del mercado, cuando haya cambios en la legislación que afecten a la Compañía, cuando sea exigido por una autoridad judicial o administrativa, o cuando el tráfico cursado por el cliente con UNE registre modificaciones importantes; sin perjuicio de los incrementos tarifarios previstos de manera explícita en el Contrato de Prestación de los Servicios Fijos de Comunicaciones.*



**Nuestro propósito: conectar cada vez a más colombianos**

Tigo es uno de los operadores de telecomunicación más grandes de Colombia

Tenemos cerca de **12M** de usuarios en nuestros negocios de hogares, móvil y B2B

Generamos más de **25mil** empleos directos e indirectos

La **Innovación** está en nuestro ADN, trabajamos para transformar Colombia hacia lo digital

**Oferta diferenciada para segmentos B2C y B2B**



**Somos una empresa industrial y comercial de Estado con mayoría pública**

**Reconocimientos**





Presentes en 9 países de Latinoamérica

## La mejor red móvil de Colombia

Validado por **OPENSIGNAL**  
**MEJOR EN:** Experiencia de video - Juegos Móviles  
 • Aplicaciones de Voz - Velocidad de Carga  
 • Velocidad de Descarga - Disponibilidad 4G

Validado por **OOKLA**  
 en velocidad

### Conectividad Velocidad Seguridad

La mejor integración de fibra submarina y terrestre de Centroamérica, con cuatro estaciones de aterrizaje de fibra.

Múltiples canales de conectividad con Carriers Tier 1 en el NAP de Las Américas.

11 Data Centers en toda la región con las principales certificaciones estandarizadas del mercado



DC EPM Medellín

DC Titanium Bogotá

### La red submarina más robusta a tu servicio

- Cuatro sistemas diferentes de cable submarino
- Un volumen de datos de +1.800 Gbps



### Soluciones diseñadas para clientes en todos los Segmentos

#### Servicios Core

- Portafolio móvil
- Datos e internet
- Voz
- Televisión

#### Servicios Digitales

- Cloud
- Seguridad
- Conectividad Inteligente
- Comunicaciones Unificadas
- IoT
- Big Data
- Servicios Administrados

### Nuestra experiencia

**154M**

Clientes en el segmento emprendedores

**2.3M**

Clientes de empresas medianas

**471**

Multi nacionales en Colombia

**1.5K**

Multi nacionales a nivel regional

**414**

Clientes corporaciones

**841**

Clientes del segmento gobierno

### ¿Por qué Tigo Business?

Adaptamos nuestros servicios en función de las necesidades reales de nuestros clientes. Somos sus aliados estratégicos.

Dotamos a nuestros clientes de atención especializada y adaptada, independientemente de su tamaño.



1	OFERTA TÉCNICA GENERAL	8
1.2	DISEÑO	8
2	OFERTA TÉCNICA CIBERSEGURIDAD ON-PREMISES Y SMART WIFI	9
2.1	CIBERSEGURIDAD EN PREMISAS SEDE PRINCIPAL	9
2.1.1	ALCANCE DE LA SOLUCIÓN	9
2.2	CIBERSEGURIDAD EN PREMISAS Y SMART WIFI PARA COLEGIO SAN JUAN EUDES	9
2.2.1	ALCANCE DE LA SOLUCIÓN	9
2.3	CIBERSEGURIDAD EN PREMISAS PARA INSTITUCIÓN EDUCATIVA NUEVO HORIZONTE 1	10
2.3.1	ALCANCE DE LA SOLUCIÓN	10
2.4	SEGURIDAD EN PREMISAS	11
2.4.1	Funcionalidades técnicas:	12
2.4.2	<b>Requerimientos eléctricos para Instalación de Equipos</b>	13
2.4.3	<b>Servicios Administrados De Ciberseguridad</b>	14
2.4.4	<b>Topología de la solución</b>	16
2.4.5	<b>Características de CiberSeguridad a Implementar en los equipos FortiGate</b>	18
2.4.6	<b>Consideraciones Técnicas Ciberseguridad</b>	19
2.4.7	<b>Reportes FortiAnalyzer</b>	20
2.4.8	<b>FortiPortal</b>	21
2.4.9	<b>Consideraciones administración sede principal</b>	24
2.4.9.1	Administración de Equipos	24
2.4.9.2	Implicaciones para Cliente	24
2.4.9.3	Responsabilidad del Cliente	25
2.4.9.4	Limitantes y Exclusiones	25
2.5	SUPUESTOS	28
3	AWS (Amazon Web Services)	30
3.1	GENERALES	30
3.2	CARACTERÍSTICAS Y BENEFICIOS	31
3.3	PROPUESTA DE VALOR	32
3.4	DESCRIPCIÓN DE LA PROPUESTA	32
3.5	OBJETIVO	33
3.6	ALCANCE	34
3.7	AMPLIACIÓN DE NUESTRA OFERTA	35
3.7.1	IaaS o Infrastructure As a Service	35



3.8	SERVICIOS ADMINISTRADOS .....	35
3.8.1	<b>Servicios administrados de Infraestructura</b> .....	35
3.8.2	<b>Servicios administrados de Bases de Datos</b> .....	37
3.8.2.1	<b>Gestión de bases de datos en AWS RDS</b> .....	38
3.8.3	<b>Requerimientos mínimos para administración de cuentas AWS</b> .....	40
3.8.4	<b>Consideraciones Servicios Administrados</b> .....	41
3.8.5	<b>Requerimientos mínimos para administración de cuentas AWS</b> .....	41
3.9	SERVICIOS PROFESIONALES.....	41
3.10	ANTECEDENTES .....	42
3.11	DESCRIPCIÓN GENERAL.....	43
3.11.1	<b>Alcance de los Servicios Ofertados</b> .....	43
3.11.2	<b>Arquitectura propuesta</b> .....	46
3.12	SUPUESTOS Y RESTRICCIONES .....	46
3.12.1	<b>Acuerdos de Niveles de Servicio</b> .....	47
3.13	ROLES Y RESPONSABILIDADES.....	48
3.13.1	<b>Modelo de Responsabilidad Compartida Amazon Web Services (AWS)</b> .....	48
3.14	RECOMENDACIONES DE SEGURIDAD EN CLOUD .....	52
4	COMUNICACIONES UNIFICADAS .....	54
4.1	CARACTERÍSTICAS Y BENEFICIOS.....	54
4.2	PROPUESTA DE VALOR .....	55
4.3	DESCRIPCIÓN DEL SERVICIO/SOLUCIÓN .....	56
4.4	CARACTERÍSTICAS DEL SERVICIO DE CISCO WEBEX CALLING .....	57
4.5	OFERTA – COMPONENTES .....	58
4.6	CALL CENTER BÁSICO .....	59
4.7	LICENCIAMIENTO WEBEX CALLING .....	60
4.8	ATRIBUTOS CONFIGURABLES ADICIONALES / OPCIONALES .....	60
4.8.1	Grabación de Llamadas .....	60
4.9	DESCRIPCION DE LA PROPUESTA .....	61
4.9.1	Objetivo .....	61
4.9.2	Elementos Ofrecidos .....	61
4.9.3	Alcance .....	62
4.9.4	Especificaciones técnicas - Arquitectura y Diseño. ....	62
4.9.5	Topología General de la Solución.....	62
4.9.6	Topología Lógica.....	63



4.9.7	Analíticas y Reportes Estándar .....	64
4.10	PORTAL AUTO CUIDADO CLIENTE FINAL.....	73
4.11	CONDICIONES TÉCNICAS ESPECÍFICAS .....	74
4.12	PUERTOS Y SERVICIOS DE COMUNICACIÓN REQUERIDOS .....	74
4.13	SUPUESTOS Y RESTRICCIONES .....	75
5	IMPLEMENTACIÓN DE LA SOLUCIÓN .....	76
5.1	METODOLOGÍA DE APROVISIONAMIENTO .....	76
5.1.1	<b>Tiempo de despliegue de los servicios</b> .....	76
5.1.2	<b>Entregables</b> .....	79
5.1.3	<b>Responsabilidades del Cliente</b> .....	79
5.1.4	<b>Ofertas de Servicio</b> .....	79
6	OFERTA ECONÓMICA .....	80
6.1	OFERTA RENOVACIÓN CIBERSEGURIDAD EN PREMISAS Y SMART WIFI.....	80
6.2	OFERTA RENOVACIÓN NUBE PÚBLICA AWS .....	82
6.3	OFERTA RENOVACIÓN UCaaS WEBEX CALLING .....	84
6.4	RESUMEN OFERTA DE SERVICIOS.....	86
6.5	FORMA DE PAGO.....	86
6.6	VALIDEZ DE LA OFERTA .....	86
6.7	IMPUESTOS Y ESTAMPILLAS.....	86
7	ACUERDO DE CONFIDENCIALIDAD .....	86



# 1 OFERTA TÉCNICA GENERAL

## 1.2 DISEÑO

### Alcance de la Solución

**COLEGIO MAYOR DE ANTIOQUIA** solicita la cotización de varios servicios de portafolio fijo que permitan atender sus requerimientos a corto plazo.

El plazo solicitado para esta cotización es de 6 meses o hasta agotar los recursos, lo primero que ocurra.

Nota: En todo caso, el anterior alcance se circunscribe únicamente a lo ofertado en el presente documento y sujeto a las condiciones de este.

### Componentes

Se consideran los componentes que hacen parte de la renovación de la oferta:

- Ciber seguridad On premises para sede principal
  - Equipos FortiGate 400F en HA
  - Un (1) servicio de Internet Dedicado de 500 Mbps
  - Un (1) servicio de Internet Banda Ancha de 500 Mbps
  
- Ciber seguridad On premises para el Colegio San Juan Eudes
  - Un (1) Equipo FortiGate 60F
  - Un (1) servicio de Internet Dedicado de 60 Mbps
  - Un (1) servicio de Internet Empresarial de 120 Mbps
  
- Servicio de Smart Wifi para el Colegio San Juan Eudes
  - Servicio de cuatro (4) dispositivos Access Point
  
- Ciber seguridad On premises para Institución Educativa Nuevo Horizonte 1
  - Un (1) Equipo FortiGate 60F
  - Un (1) servicio de Internet Dedicado de 60 Mbps
  - Un (1) servicio de Internet Empresarial de 120 Mbps
  
- Nube Pública AWS
  - 6 cuentas existentes:
    - Log Archive
    - Tigo Business Colegio Mayor MGMT
    - MIBIENESTAR-COLMAYOR
    - Audit
    - sicma\_colmayor
    - COLEGIO MAYOR DE ANTIOQUIA



- UCaaS Webex Calling
  - Licencias Webex Calling Professional
  - Licencias Webex Calling Workspace
  - Troncal SIP Fija Centralizada en Data Center Tigo
  - Servicios Administrados Plan Básico

## 2 OFERTA TÉCNICA CIBERSEGURIDAD ON-PREMISES Y SMART WIFI

### 2.1 CIBERSEGURIDAD EN PREMISAS SEDE PRINCIPAL

#### 2.1.1 ALCANCE DE LA SOLUCIÓN

De acuerdo con los requerimientos de seguridad del cliente **COLEGIO MAYOR DE ANTIOQUIA**, se ofrece la solución de ciber seguridad on-premises compuesta por equipos FortiGate 400F en un esquema de HA, (1) servicio de Internet dedicado de 500 MB y (1) servicio de Internet BA de 500MB los cuales pueden ser utilizados simultáneamente evitando asignación de recursos ociosos, esto permitirá aumenta la experiencia de los usuarios.

**NOTA:** Los servicios administrados no se incluyen, ya que la administración de la solución la realiza el cliente.

La propuesta presentada por TIGO BUSINESS consiste en el servicio de Ciberseguridad en Premisas por 6 meses o hasta agotar los recursos, lo primero que ocurra.

Dirección	Ciberseguridad	Internet	Adicionales
CR 78 Nro. 65-46 Bloque Patrimonial	On premises compuesta por (2) FortiGate 400F en HA	*1 Internet Dedicado de 500 Mbps * 1 Internet Banda Ancha de 500 Mbps	3 pool de direcciones IP Públicas.

Los Servicios de Ciber Seguridad en Premisas están basados en tecnología Fortinet, se tienen los equipos FortiGate con licenciamiento UTP.

### 2.2 CIBERSEGURIDAD EN PREMISAS Y SMART WIFI PARA COLEGIO SAN JUAN EUDES

#### 2.2.1 ALCANCE DE LA SOLUCIÓN

De acuerdo con los requerimientos de seguridad del cliente **COLEGIO MAYOR DE ANTIOQUIA**, se ofrece la solución de ciber seguridad on-premises compuesta por un (1) equipo FortiGate 60, (1) servicio de Internet dedicado de 60 MB y (1) servicio de Internet BA de 120 MB los cuales pueden



ser utilizados simultáneamente evitando asignación de recursos ociosos, esto permitirá aumenta la experiencia de los usuarios.

**NOTA:** Los servicios administrados para Ciberseguridad en Premisas y Smart Wifi para esta sede son prestados por Tigo.

La propuesta presentada por TIGO BUSINESS consiste en el servicio de Ciberseguridad en Premisas por 6 meses o hasta agotar los recursos, lo primero que ocurra.

Servicio	Dirección	BW Acceso	Tecnología Acceso	Cantidad Equipos	Tipo
Ciberseguridad en Premisas	Colegio San Juan Eudes Calle 77E #79B-36	Internet Dedicado 60 Mbps Internet Empresarial Ultra Banda Ancha 120 Mbps	Fibra óptica GPON	1	FG-60F

Servicio	Dirección	Alcance
Smart Wifi	Colegio San Juan Eudes Calle 77E #79B-36	Smart Wifi (4 equipos Ruckus)

## 2.3 CIBERSEGURIDAD EN PREMISAS PARA INSTITUCIÓN EDUCATIVA NUEVO HORIZONTE 1

### 2.3.1 ALCANCE DE LA SOLUCIÓN

De acuerdo con los requerimientos de seguridad del cliente **COLEGIO MAYOR DE ANTIOQUIA**, se ofrece la solución de ciber seguridad on-premises compuesta por un (1) equipo FortiGate 60, (1) servicio de Internet dedicado de 60 MB y (1) servicio de Internet BA de 120 MB los cuales pueden ser utilizados simultáneamente evitando asignación de recursos ociosos, esto permitirá aumenta la experiencia de los usuarios.

**NOTA:** Los servicios administrados para Ciberseguridad en Premisas para esta sede son prestados por Tigo.

La propuesta presentada por TIGO BUSINESS consiste en el servicio de Ciberseguridad en Premisas por 6 meses o hasta agotar los recursos, lo primero que ocurra.



Servicio	Dirección	BW Acceso	Tecnología Acceso	Cantidad Equipos	Tipo
Ciberseguridad en Premisas	Institución Educativa Nuevo Horizonte 1 CARRERA 37 #109-24	Internet Dedicado 60 Mbps Internet Empresarial Ultra Banda Ancha 120 Mbps	Fibra óptica GPON	1	FG-60F

## 2.4 SEGURIDAD EN PREMISAS

El servicio de Ciberseguridad en Premisas Tigo (Cybersecurity On Premise) provee protección perimetral a la información y recursos informáticos de las empresas alojados en sus premisas, empleando para ello plataformas tecnológicas de Ciberseguridad ubicadas en una o más sedes del cliente según su necesidad.

La protección perimetral mitiga aquellas amenazas y ataques presentes en Internet. El servicio es un excelente complemento de protección los servicios de Internet.

El servicio ofrecido se fundamenta en funcionalidades de seguridad requeridas y habilitadas, las herramientas de gestión y administración, el seguimiento de estándares y mejores prácticas útiles para empresas de cualquier sector y tamaño en escenarios como:

- Clientes Tigo con internet Dedicado.
- Empresas que ofrecen servicios a clientes, empleados o aliados a través de Internet, en cualquiera de las siguientes arquitecturas:
  - ✓ Sus aplicaciones de servicios están alojadas en una granja de servidores o datacenter en una o varias sedes de la compañía.
  - ✓ Híbrida, en la que sus aplicaciones de servicios están distribuidas simultáneamente en Datacenter propio y en Datacenter de Tigo.
  - ✓ Privada, en la que sus aplicaciones de servicios se encuentran en el Datacenter propio.
- Empresas que requieren hacer uso del Internet de forma más productiva y segura previniendo a sus empleados y usuarios internos de acceder a uno o varios tipos de contenidos como:
  - ✓ De alto consumo de ancho de banda.
  - ✓ Redes sociales.
  - ✓ De alto riesgo de seguridad.
  - ✓ No deseables (terrorismo, contenido para adultos, etc).
- Empresas con diferentes sedes cada con su propia conexión a Internet.
- Empresas que tienen contratado con un tercero su solución de conectividad a Internet.
- Empresas que requieren respaldar sus servicios digitales a través de un operador alterno.



### 2.4.1 Funcionalidades técnicas:

#### **Firewall**

- Protección a nivel de control puertos TCP/UDP basado en redes IP.
- El servicio es dimensionado de acuerdo con el Ancho de Banda del servicio de Internet y al número de usuarios de la red a proteger (Throughput).

#### **VPN Site-to-Site (S2S)**

Protege la información que viaja entre dos sedes remotas conectadas a través de una red pública como Internet, permitiendo que dicha información sea entendible solo para los usuarios al interior de las sedes que conecta la VPN. En caso de que un tercero no autorizado intercepte los paquetes de datos que viajan por la VPN, este encontrará que los datos están cifrados y por lo tanto se mantendrá la información confidencial.

- La VPN Site-to-Site se configura entre el equipo de Ciberseguridad en Premisas instalado por Tigo y un enrutador del cliente conectado a Internet en una sede remota que soporte esta funcionalidad.
- Este servicio se configura con un dispositivo remoto que soporte protocolo IPsec, creando un túnel cifrado para la comunicación.
- El servicio se dimensiona de acuerdo con el número de túneles requeridos, el ancho de banda estimado que utilizará la conexión VPN y al número de usuarios de la red a proteger.

#### **VPN Client-to-Site (C2S):**

- Protección del tráfico que cursa por Internet entre clientes VPN (dispositivos de usuario) y una sede central
- El dispositivo de usuario cliente VPN requiere estar conectado a Internet.
- Este servicio es una funcionalidad adicional al componente de Firewall y se configura empleando L2TP con cifrado IPsec soportados de forma nativa en los sistemas operativos Windows, OS X y iOS.
- El servicio es dimensionado de acuerdo con la cantidad de usuarios y el ancho de banda que concurrentemente consumen los usuarios conectados al terminador VPN en la sede central.
- Los tiempos de entrega de la implementación del servicio VPN Client-to-Site están basados en la entrega del cliente VPN para Sistemas Operativos Windows de 32 y 64 Bits.

#### **Antivirus Gateway (Malware Protection)**

- Se fundamenta en una Base de Datos de definiciones de firmas de virus que son actualizadas periódicamente por el fabricante.
- Esta protección se aplica al tráfico entrante y saliente (navegación y publicación) de tráfico no cifrado.
- El servicio es dimensionado de acuerdo con el ancho de banda del tráfico de la conexión a Internet contratada por el cliente y al número de usuarios de la red a proteger.



- Este servicio complementa el Antivirus de Host que se instala en dispositivos de usuario y servidores, por lo cual se recomienda siempre mantener activo y actualizado el Antivirus en estos dispositivos.

### **Application Control (Firewall Capa 7)**

El servicio es dimensionado de acuerdo con el ancho de banda del tráfico de la conexión a Internet contratada por el cliente y al número de usuarios de la red a proteger.

#### **IDS/IPS:**

- Esta protección se aplica para el tráfico entrante, es decir tráfico de publicación.
- El servicio es dimensionado de acuerdo con el ancho de banda del tráfico de la conexión a Internet contratada por el cliente y al número de usuarios de la red a proteger.
- PCI-compliant.

### **WCF (Filtrado de Contenidos)**

- La Protección de Control de Contenido está basado en la categorización de millones de sitios Web. Restricción de sitios maliciosos y no deseados.
- El servicio es dimensionado de acuerdo con el ancho de banda del tráfico de la conexión a Internet contratada por el cliente y al número de usuarios de la red a proteger.
- CIPA-compliance.

### **Full UTM (Unified Threat Management)**

- Las consideradas en cada uno de los servicios que lo componen.

## **2.4.2 Requerimientos eléctricos para Instalación de Equipos**

### **Instalación eléctrica**

- Niveles nominales de tensión Regulada AC a través de UPS.
- Fase – Neutro = 120 VAC (+5%, -10%)
- Fase – Tierra = 120 VAC (+5%, -10%)
- Neutro Tierra. = 0 (máximo 1.5) VAC
- Se debe tomar la energía del mismo tableros regulado (misma UPS) que alimenta los equipos de datos y comunicaciones del cliente.
- Distribución de la red eléctrica.
- La alimentación eléctrica para los equipos de datos se tomará del tablero de distribución a la salida de la UPS, se deberá proteger con un Breaker apropiado (1 x 15 A) para los equipos y se instalará la acometida eléctrica hasta el rack de equipos usando un cable encauchetado formado por tres conductores de cobre en calibres AWG apropiados (No. 12). (fase, neutro y tierra) y aislamiento THW. En el rack se instalará un multitoma.



- Cuando la instalación lo requiere se instala un multitoma independiente para los equipos de datos y otra para los de radio, siguiendo el concepto anterior.
- Capacidades de las protecciones (breakers).
- La acometida eléctrica se debe proteger y dimensionar en forma adecuada según la carga.
- Los elementos de protección y seccionamiento de circuitos sólo deberán instalarse sobre las fases, los conductores de neutro y tierra deberán correr en forma continua, sin ningún elemento que pueda provocar su desconexión accidental.
- En la instalación de equipos el primer conductor que se conecta es el de tierra, y es el desmonte éste es el último que se desconecta.

### **Sistema de puesta a tierra**

- El sistema de puesta a tierra deberá cumplir con lo exigido por las normas ICONTEC (NTC 2050) y NFPA 70 (National Electric Code) garantizando las medidas de resistencia de puesta a tierra y las características constructivas del sistema.
- Los equipos de datos se deberán conectar a la misma barra de tierra de los equipos de comunicaciones y sistemas del cliente. Esto para evitar diferentes referencias de tierra, que causan errores en los datos transmitidos o ponen en riesgo estos equipos instalados. Esta barra de tierra deberá estar conectada la malla cumpliendo las exigencias de las mencionadas normas.
- Si se debe instalar un equipo de radio en algún sitio, las antenas deberán instalarse cumpliendo lo exigido por la norma ICONTEC (NTC 452) e IEC.
- Las antenas deben tener su sistema de tierra y protección adecuado, las cuales se instalarán según las indicaciones del fabricante, siguiendo la exigencia de la norma

### **Condiciones Ambientales**

El sitio de instalación debe garantizar las siguientes condiciones ambientales para los equipos:

- Temperatura máxima 22 ° C,
- Humedad relativa no condensante del 55%.
- Libre de polvo y suciedad.
- Los equipos deben instalarse siguiendo las recomendaciones del fabricante, respecto a las distancias de seguridad, ventilación y mantenimiento que requiera el equipo.

## **2.4.3 Servicios Administrados De Ciberseguridad**

Este alcance aplica para las sedes San Juan Eudes y la Institución Educativa Horizonte 1

### **Beneficios**

A continuación, se describen los beneficios más relevantes de los servicios administrados de Seguridad.

- Disminución de carga operativa delegando en especialistas y experiencia de TIGO la administración de la seguridad perimetral.
- Planeación predecible de costos de administración de Ciber Seguridad sin inversiones asociadas y que estén alineados con las expectativas del negocio.
- Visibilidad y control de las políticas de seguridad para facilitar la toma de decisiones en los gastos en infraestructura de TI.



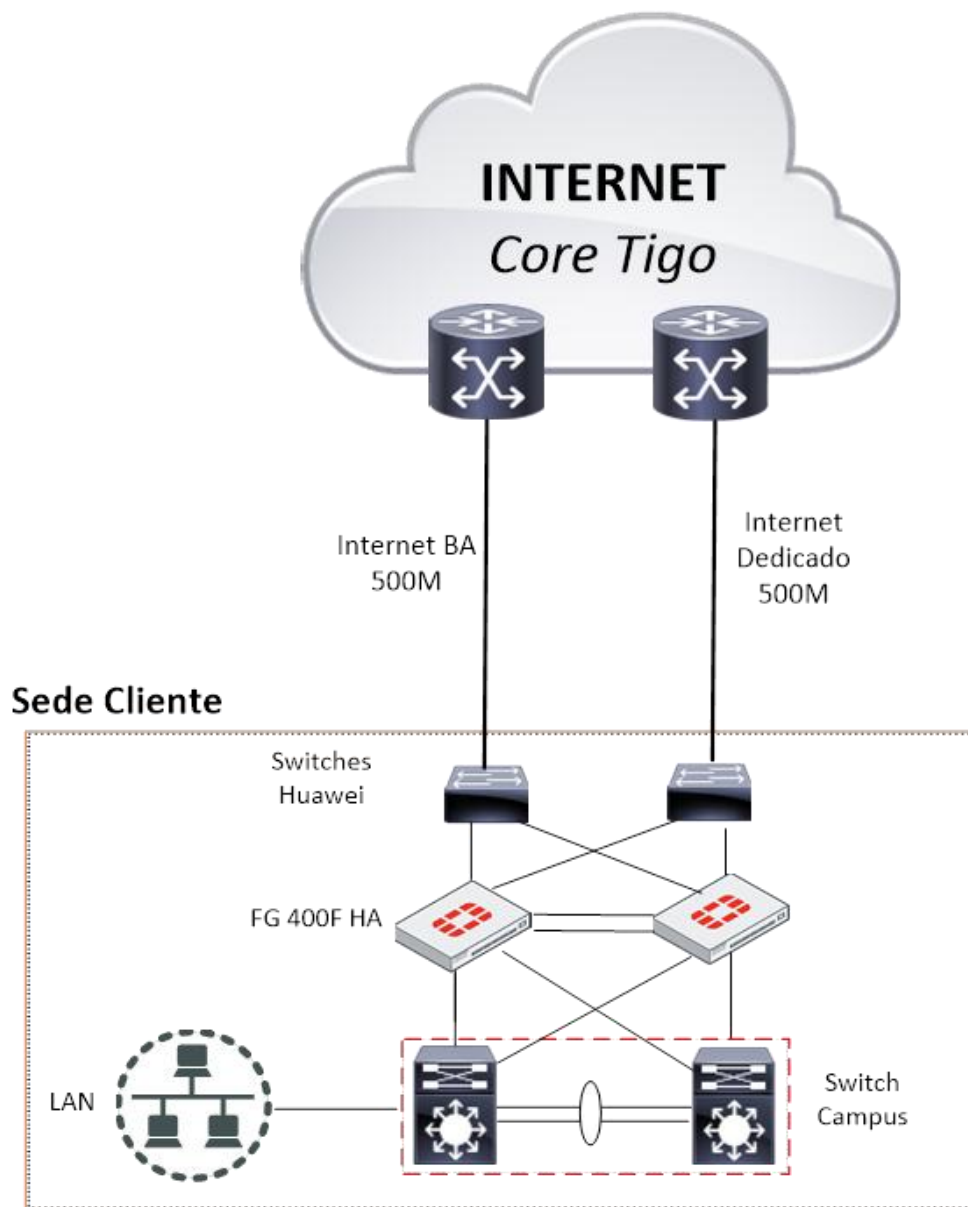
- Flexibilidad para realizar cambios sobre políticas de seguridad a través de un equipo experto que realiza la gestión completa de los servicios de Ciber Seguridad
- Disminución de riesgos operativos con la notificación proactiva y correlación de eventos de Ciber seguridad.

Los servicios de Ciberseguridad en Premisas incluyen los siguientes Servicios Administrados:

- **Instalación y puesta en marcha:** dentro de los tiempos pactados en los ANS y una vez entregada por parte del cliente la información requerida.
- **Informes:** entrega del informe de incidentes de disponibilidad ante incidentes críticos presentados (afectación total del servicio) y por solicitud del cliente. Basado en plantillas estándar definidas por TigoUne. Incluye el almacenamiento de los logs de los servicios de Ciberseguridad. Retención de los logs por 1 mes.
- **Cambios:**
  - ✓ Ilimitados dentro del periodo de estabilización (sujetos al alcance del servicio contratado).
  - ✓ Ilimitados después del periodo de Estabilización. Cada cambio se asocia a un requerimiento del cliente y cuenta por cada servicio contratado, siempre que el cambio solicitado esté dentro del alcance del servicio contratado.
  - ✓ Cambios Estándar: comprende aquellas actividades que conlleven a la creación, modificación y/o eliminación de políticas, usuarios o configuraciones de los servicios operativos del cliente.
  - ✓ Cambios de Emergencia: están relacionados con la creación, modificación, o eliminación de usuarios, políticas o configuraciones que requieren ser implementados para mitigar un incidente sobre uno o varios servicios operativos del cliente.
  - ✓ NO incluye Reingeniería de Políticas, es decir análisis ni rediseño de la estructura de políticas de seguridad.
- Atención 7x24x365 para incidentes en los equipos (nivel 1).
- Soporte con especialistas del SOC (nivel 2).
- Monitoreo de Infraestructura de prestación de servicios de Ciberseguridad: consiste en monitoreo de la disponibilidad del equipo en que se soportan los servicios de Ciberseguridad.

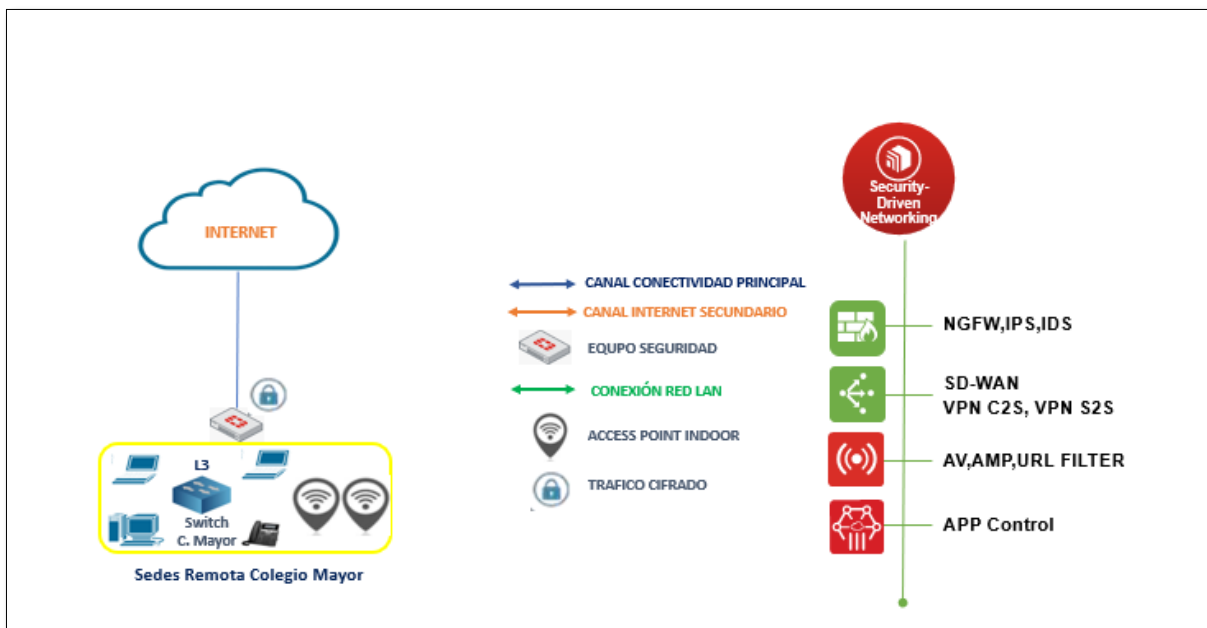
## 2.4.4 Topología de la solución

### Topología Sede Principal



## Topología Colegio San Juan Eudes y la Institución Educativa Horizonte 1

La siguiente topología incluye los ítems de seguridad en premisas para la sede del cliente a través de los equipos FortiGate y los servicios administrados de Ciberseguridad.



### Consideraciones Técnicas

- ✓ En la sede de COLEGIO MAYOR ANTIOQUIA se destinará un equipo FortiGate, que recibirán el canal de Internet que brindarán protección perimetral para la sede incluye (FULL UTM). Las especificaciones del equipo de acuerdo con el siguiente datasheet <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-100f-series.pdf>
- ✓ No se incluyen integraciones a otras plataformas del cliente
- ✓ El cliente COLEGIO MAYOR ANTIOQUIA debe suministrar los puertos disponibles en sus equipos de acceso para la recepción de la conectividad de la nueva infraestructura. Así como también los puertos para la conexión a los equipos firewall FortiGate objeto de esta oferta
- ✓ COLEGIO MAYOR ANTIOQUIA debe garantizar las conexiones de energía y potencia en sus racks de acuerdo al tipo de especificaciones que vienen con los equipos.
- ✓ En caso de que haya un cambio que por su complejidad se salga del alcance de los Administradores de Tigo, se validara la configuración con personal del fabricante en una nueva factibilidad que tendrá costo para COLEGIO MAYOR ANTIOQUIA en su puesta en funcionamiento. Igualmente, las migraciones de configuraciones existentes que no tengan el alcance de funcionalidades cubiertas en el anexo técnico estarán sujetos a factibilidad y tendrá costo para COLEGIO MAYOR ANTIOQUIA



- ✓ Tigo es el administrador de la solución y los cambios y modificaciones deben realizarse a través del centro de soporte de acuerdo con los ANS establecidos en la oferta.
- ✓ No se incluye la integración al directorio activo.
- ✓ Se incluye servicios administrados para informes de ciberseguridad mensual automatizado por la plataforma (informe de filtrado, informe de firewall e informe de IPS, adicional el informe de disponibilidad)
- ✓ Todas las interconexiones a los equipos de última milla se realizarán en puerto 1 Gbps eléctricos, no se incluyen SFP para conexiones de Fibra.

#### 2.4.5 Características de CiberSeguridad a Implementar en los equipos FortiGate

Se presentan los features de seguridad ofrecidos para implementar en la solución de CiberSeguridad en Premisas:

##### **Sede Principal**

- Firewall Capa 3, 4 y 7
- Web Filtering (El servicio incluye 3 perfiles de este tipo)
- Inspección SSL
- 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)
- Integración con AD (Opcional)

##### **NOTAS:**

- En caso de requerirse la configuración de una funcionalidad adicional de Seguridad se deberá validar su viabilidad en una nueva factibilidad
- Se tomará como base la configuración que se tiene en la VDOM (ciberseguridad cloud) actualmente operativo
- En caso de requerirse, dentro de la fase de implementación se definirá en conjunto con el cliente las políticas de seguridad a configurar en los dispositivos
- 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

##### **Sedes San Juan Eudes y la Institución Educativa Horizonte 1**

- 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 C2S: (Se incluyen 5)

Referencia del equipo UTM	FG-60F
Número de sedes del cliente con la configuración	2

Componentes	Valores
Desempeño (Mbps)	300
Número de Reglas	10
Número de Usuarios	50
Número de Túneles Site to Site	2
Número de Túneles Client to Site	5
Throughput VPN-SSL	12 Mbps

#### NOTAS:

- En caso de requerirse la configuración de una funcionalidad adicional de seguridad se deberá validar su viabilidad en una nueva factibilidad
- En caso de requerirse, dentro de la fase de implementación se definirá en conjunto con el cliente las políticas de seguridad a configurar en los dispositivos

#### 2.4.6 Consideraciones Técnicas Ciberseguridad

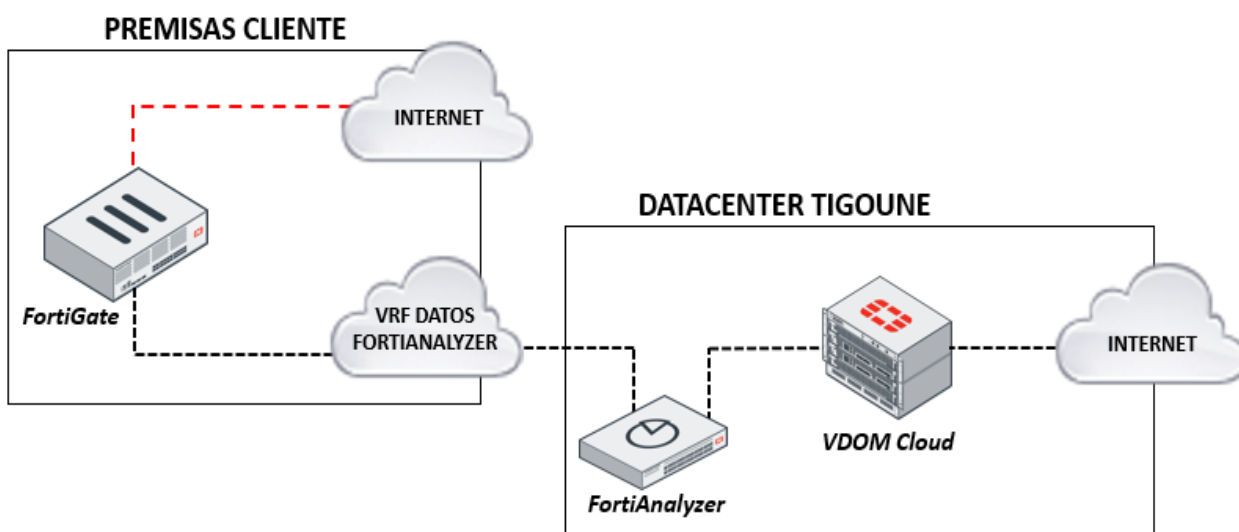
- El equipo Fortigate será la capa de seguridad perimetral de la solución
- El cliente debe disponer de espacio en Rack para los equipos
- El cliente debe asegurar las condiciones eléctricas para el buen funcionamiento del equipo
- En caso de requerirse, es responsabilidad del cliente configurar los diferentes endpoint o servidores de la organización
- La administración y soporte de la solución de ciberseguridad estará a cargo de Tigo, aplica para la Sede San Juan Eudes y la Institución Educativa Horizonte 1. Para la sede principal no aplica los servicios administrados Tigo.
- Se definirá en conjunto con el cliente el LLD para esta solución
- El cliente debe asegurar las condiciones eléctricas para el buen funcionamiento de los equipos
- En caso de requerirse, es responsabilidad del cliente configurar los diferentes endpoint o servidores de la organización

- Debido a que se instalarán servicios de Internet nuevos, el direccionamiento público también será nuevo, este cambio trae un impacto en los servicios que estén utilizando el direccionamiento público del DC Tigo como lo son las VPN y publicaciones
- El cliente deberá realizar los cambios pertinentes en sus DNS o en la gestión con sus proveedores con los cuales tenga establecidas VPN, el cambio de direccionamiento y su impacto

#### 2.4.7 Reportes FortiAnalyzer

El feature de FortiAnalyzer puede ser adquirido tanto para soluciones OnPremise o Cloud, en los cuales se tengan equipos Fortinet.

Esta es una herramienta centralizada de gestión y análisis de Logs de soluciones Fortinet, genera de manera automatizada informes de desempeño/seguridad de las soluciones perimetrales Fortinet aprovisionadas.



#### Entregables FAZ

Se entregarán los siguientes reportes:

- 360 Security Report
- Application Risk and Control

#### Restricciones

- Los informes del FAZ pueden ser modificados según el caso de uso o actualización de la plataforma
- Los reportes presentados mensualmente al cliente ya están preestablecidos, para una personalización esta debe pasar por factibilidad al grupo Soporte DataCenter y esto podría tener costos adicionales



- Para este proyecto se considera una capacidad de almacenamiento de Logs de 220GB
- El tiempo de retención de Logs es proporcional a la capacidad de Almacenamiento, por lo tanto, TIGO no se compromete con tiempos de retención sino con capacidad de Almacenamiento.

#### 2.4.8 FortiPortal

El Fortiportal permite gestionar y monitorear redes de seguridad de manera centralizada y fácil. Está diseñada para facilitar la administración de servicios de seguridad por parte de empresas y proveedores de servicios, permitiéndoles manejar múltiples clientes desde una sola interfaz.

Nota: FortiPortal es una plataforma de administración de seguridad basada en la nube que ofrece una disponibilidad diferente a los accesos de internet de la presente oferta.

##### El cliente puede:

1. Monitorear el tráfico de la red en tiempo real, obteniendo una visión general del uso de ancho de banda y de las amenazas.
2. Configurar políticas de seguridad en dispositivos de la red, como firewalls.
3. Gestionar usuarios y accesos a la red, aplicando políticas personalizadas según el perfil de cada usuario.
4. Generar reportes detallados sobre el rendimiento de la red y la seguridad, lo cual ayuda en la toma de decisiones y cumplimiento de normativas

El impacto determina la prioridad del incidente, dependiendo de cuánto afecta sus procesos clave de negocio y/o número de usuarios afectados. A continuación, encuentra los criterios que se analizarán para definir el impacto del incidente sobre el servicio:

Impacto	Criterio
<b>Significativo</b>	Caída total del servicio / Degradación de los servicios hasta el punto de que no puedan ser utilizados
<b>Moderado</b>	2 o más Intermittencias de servicio, en dónde el período de afectación acumulado sea superior o igual a 30 minutos, en un día / Degradación de los servicios sin afectación total del mismo.
<b>Menor</b>	No afecta ni degrada la prestación del servicio, se incluyen eventos en monitoreo, en caso de que el cliente cuente con este servicio / Intermittencias esporádicas con periodicidad de uno o más días y con duración menor a 5 minutos.

Para la atención presencial se definen los siguientes tipos de sede de acuerdo con la ubicación geográfica del servicio y la cobertura de Tigo:

Tipo Ciudad	Descripción
<b>Principal</b>	Ciudades principales y área metropolitana.
<b>Secundaria</b>	Otras ciudades/municipios del departamento.



<b>Terciaria</b>	Otras ciudades/municipios donde no se cuenta con cobertura de Tigo y se presta el servicio a través de terceros.
------------------	--

**Tiempos de Atención y Solución**

Con el fin de darle siempre el mejor servicio, nuestro Tiempo de Atención, tanto para incidentes o fallas como para cualquier otro tipo de solicitud es de 30 minutos. Una vez atendido su requerimiento, los siguientes son los tiempos de solución (tiempos dados en horas corrientes):

PRIORIDAD	Solución Centralizada	Solución en Sede del Cliente		
		Ciudad Principal	Ciudad Secundaria	Ciudad Terciaria
<b>Significativo</b>	4	10	16	120
<b>Moderado</b>	8	36	42	120
<b>Menor</b>	48	96	120	120

Disponibilidad del Servicio		ANS	Descripción
<b>Ciber Seguridad</b>	Disponibilidad del Servicio	99.7%	La disponibilidad está basada en las condiciones de la Infraestructura del DC y el equipo Propiedad de Tigo Business. Los límites de desempeño de cada equipo son entregados en la oferta comercial controlados por Sesiones Concurrentes y desempeño en Mbps de cada equipo particular
	Instalación de Equipo Ciber Seguridad	Definidos de acuerdo al número de equipos y servicios requeridos.	Una vez firmado el contrato se procede a la reserva de equipos y programación de la instalación y configuración.
	Levantamiento información Política de Seguridad	2 días hábiles	Sujeto a la disponibilidad y respuesta del cliente para brindar la información.
	Configuración	4 días	Este tiempo empieza a contar una vez el cliente ha suministrado toda la información necesaria para configurar los servicios de seguridad (Ejemplo: redes IP,



		políticas, equipos, topología de red, entre otros). . Una vez configurado el servicio se procede a la facturación del servicio.
Estabilización	15 días máximo.	Pruebas y ajustes de las reglas de seguridad dentro del alcance de lo contratado.
<b>Comunicación Mantenimientos Preventivos y Correctivos con afectación</b>		Tiempo de anticipación con que será comunicada la realización del mantenimiento.
Mantenimiento Preventivo	5 días hábiles	
Mantenimiento Correctivo Programado	2 días hábiles	
<b>Comunicación Mantenimientos Preventivos y Correctivos sin afectación</b>		
Mantenimiento Preventivo	2 días hábiles	
Mantenimiento Correctivo Programado	0.5 días hábiles	
Cambios en Configuración de Políticas	Cambio Estándar: 5x8, respuesta en 24 horas	
	Cambio de Emergencia: 5x8, respuesta en 8 horas	No incluye el tiempo de atención a incidentes.
Monitoreo	7x24	De acuerdo con el alcance especificado en “Servicios Administrados Incluidos”
Informes	48 horas después de solicitado	De acuerdo con el alcance especificado en “Servicios Administrados Incluidos”  Basados en plantillas estándar definidas por Tigo Business



## 2.4.9 Consideraciones administración sede principal

### 2.4.9.1 Administración de Equipos

La administración y soporte de los equipos de red quedara bajo la responsabilidad de COLEGIO MAYOR DE ANTIOQUIA.

De acuerdo con las políticas de seguridad y soporte de la empresa, el cliente COLEGIO MAYOR DE ANTIOQUIA se hace responsable por la configuración y posterior soporte de la solución de seguridad, malas políticas de seguridad, configuraciones inadecuadas y desconocimiento de la tecnología que atenten contra el buen desempeño de la solución de comunicaciones son responsabilidad total del cliente.

El cliente se hace responsable del uso y cuidado de los equipos que pudiere llegar a entregarle TIGO a título de comodato o arrendamiento, con base en esto el cliente se obliga a cumplir con la cláusula documentada en el contrato de prestación de servicios referente a la utilización y cuidado de los equipos.

Observación: El cliente debe de firmar la carta de aceptación de que la administración es de el por tanto el soporte es su responsabilidad.

### 2.4.9.2 Implicaciones para Cliente

A continuación, se establecen las implicaciones e impactos que asumiría el cliente, bajo este esquema de administración:

- Caídas o indisponibilidades del servicio, derivados de las configuraciones o modificaciones a las que el cliente tenga acceso.
- Impacto en los niveles de servicio, derivados de las configuraciones o modificaciones a las que el cliente tenga acceso.
- 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.
- 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 (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.

#### *2.4.9.3 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.

#### *2.4.9.4 Limitantes y Exclusiones*

- Los Acuerdos niveles de servicio 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 responsabilidades; independiente de las Notificaciones que brinde el cliente sobre los cambios que ejecute.
- Cuando el cliente requiera apoyo de Tigo en alguna responsabilidad, 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.
- 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.

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 BUSSINESS 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 BUSINESS.
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 BUSSINESS, 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 BUSINESS en aras de cumplir con el alcance de los servicios ofrecidos. En caso de que éstas no sean debidamente implementadas en su totalidad, TIGO BUSINESS 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 BUSSINESS no garantiza estado 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 BUSSINESS 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 BUSSINESS 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 BUSSINESS 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 BUSINESS 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 pérdida pecuniaria o de otro tipo)], que se deriven o de otro modo este relacionados con la materialización de un incidente de seguridad. Tigo BUSINESS 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.

## 2.5 SUPUESTOS

- La implementación de soluciones en sedes distintas a las mencionadas anteriormente no se encuentra contemplada en el alcance de esta propuesta.
- Cualquier servicio o solicitud que no estén claramente especificados en este documento se encuentran por fuera del alcance.
- 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, COLEGIO MAYOR ANTIOQUIA gestionará dichos permisos
- COLEGIO MAYOR ANTIOQUIA es responsable de asegurar el espacio físico para los equipos en cada Sede.
- 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 Ciberseguridad y que cualquier otra falla en el servicio derivada de la red LAN, o condiciones físicas o eléctricas en cada sitio será soportada y asumida por el cliente.
- En caso de requerirse trabajos adicionales, esto se cotizará por separado, en común acuerdo con TIGO
- En caso de requerirse trabajos adicionales, esto se cotizará por separado, en común acuerdo con TIGO.
- Tanto Tigo Business como COLEGIO MAYOR ANTIOQUIA serán responsables en conjunto a la adherencia a los alcances del trabajo y a los tiempos establecidos para el proyecto que se especifican en este documento.
- Sobre cualquier situación inesperada que pueda presentarse durante el proyecto, Tigo Business e COLEGIO MAYOR ANTIOQUIA aplicarán el buen juicio y sentido común cuando se determinen roles, costos y responsabilidades requeridas para la resolución.
- COLEGIO MAYOR ANTIOQUIA 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 se considerarán aceptados por resultados y entregables definidos.
- Entre Tigo Business y COLEGIO MAYOR ANTIOQUIA 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.
- En caso de requerirse traslado o modificaciones de los servicios ofrecidos, se realizará un análisis previo de factibilidad por parte de Tigo Business y se cobrarán tarifas por derechos de conexión y obras civiles (cuando apliquen) de acuerdo con las tarifas establecidas para sedes nuevas en el portafolio de clientes corporativos vigente.
- Los servicios serán facturados de acuerdo con la fecha de entrega individual.
- Es responsabilidad de COLEGIO MAYOR ANTIOQUIA suministrar el espacio físico con condiciones ambientales y eléctricas adecuadas para el alojamiento de los diferentes equipos que hacen parte de esta solución.
- Tigo actúa como el integrador del sistema y se encarga de la implementación y configuración de los equipos. Sin embargo, en caso de fallas o defectos inherentes al fabricante, Tigo no asume responsabilidad alguna. Estas situaciones serán gestionadas directamente con el fabricante, ya que Tigo no tiene control sobre la calidad o el funcionamiento interno de los productos suministrados.



## 3 AWS (Amazon Web Services)

### 3.1 GENERALES

Amazon Web Services (AWS) es la plataforma en la nube más adoptada<sup>1</sup> y completa en el mundo, que ofrece más de 220 servicios integrales de centros de datos a nivel global. Millones de clientes, incluso las empresas emergentes que crecen más rápido, las compañías más grandes y los organismos gubernamentales líderes, están usando AWS para reducir los costos, aumentar su agilidad e innovar de forma más rápida.

#### ¿Cómo opera AWS?

AWS cuenta con una infraestructura de nube distribuida a nivel mundial, ofrece en las regiones múltiples zonas de disponibilidad conectadas por redes de baja latencia, alto rendimiento y altamente redundantes. AWS ofrece 99 zonas de disponibilidad en 31 regiones geográficas de todo el mundo brindando baja latencia, alto rendimiento y alta disponibilidad a través de 450 puntos de presencia.

**Regiones:** Cada región de AWS proporciona niveles de redundancia y conectividad plenos a la red. A diferencia de otros proveedores de nube, que definen una región como un centro de datos único, en AWS las regiones consisten en múltiples zonas de disponibilidad (normalmente 3), cada una de las cuales es una partición completamente aislada de la infraestructura de AWS que consta de centros de datos independientes, cada uno con capacidad energética, de red y conectividad, redundante, y ubicado en instalaciones separadas.

**Zonas de Disponibilidad:** Cada zona de disponibilidad (Availability Zone -AZ, por su sigla en inglés) puede estar conformada por varios centros de datos (normalmente 3) y, a escala completa, por cientos de miles de servidores. Son particiones totalmente aisladas de la infraestructura global de AWS. Las zonas, que cuentan con su propia infraestructura de energía, están físicamente separadas entre sí por una distancia significativa de muchos kilómetros, aunque todas están dentro de un rango de 100 km. Todas las zonas están interconectadas con redes de alto ancho de banda y baja latencia, a través de una fibra metropolitana exclusiva totalmente redundante que proporciona una red de alto rendimiento y baja latencia entre las zonas. El rendimiento de la red es suficiente como para llevar a cabo la replicación sincrónica entre las zonas de disponibilidad. Las zonas de disponibilidad de AWS también son herramientas poderosas para ayudar a desarrollar aplicaciones de alta disponibilidad. Las AZ hacen que el particionamiento de aplicaciones sea tan fácil como sea posible. Si una aplicación se divide en las AZ, las empresas están mejor aisladas y protegidas de problemas como rayos, tornados, terremotos y más.

---

<sup>1</sup> Fuente: Gartner, Magic Quadrant for Cloud Infrastructure and Platform Services, 2022. Disponible en: <https://www.gartner.com/doc/reprints?id=1-2AOZQAQL&ct=220728&st=sb>



Regiones de AWS a nivel mundial (Fuente: AWS)

Las Soluciones AWS (Amazon Web Services) de Tigo Business constituyen para las empresas y entidades una forma ágil, flexible y segura de usar plataformas digitales como servicio (as a Service) para apalancar sus estrategias de negocio y proyectos de Transformación Digital, haciendo uso de capacidades de la nube pública de AWS, así como de los Servicios Profesionales y Administrados Cloud de Tigo Business.

La estrategia de Nube de Tigo Business está orientada a ser un prestador de servicios administrados multicloud híbrido. En este sentido, Tigo Business está en capacidad de entregar soluciones multicloud, integrando servicios de AWS y de la nube privada Tigo Cloud (o Cloud 360), para aquellos clientes que requieren de alta disponibilidad y/o de uso de ambientes diferentes para sus aplicaciones.

### 3.2 CARACTERÍSTICAS Y BENEFICIOS

AWS tiene varias características y beneficios que la hacen una plataforma en la nube ideal entre las empresas, entidades y organizaciones. A continuación, se detallan algunos de los principales:



**Optimización de Costos:** les permite no solo disminuir o eliminar su CAPEX (presupuesto de inversión) asociado a la infraestructura TI para soportar los servicios digitales que requiere el negocio, sino también optimizar los costos de operación y mantenimiento de dicha infraestructura. Gracias al modelo “as a Service” complementado con los servicios profesionales y administrados Tigo Business, las empresas y entidades pueden delegar en Tigo Business aspectos operativos de su negocio o actividad, mientras que focaliza los esfuerzos de sus departamentos de TI y Seguridad en apoyar la estrategia de estos.



**Continuidad del negocio:** les permite soportar sus servicios digitales en plataformas de alta disponibilidad y con esquemas de redundancia entre los Data Center de Tigo Business, así como con la nube AWS®, de esta manera la información, aplicaciones y servidores se mantienen disponibles para el negocio y sus clientes.



**Crecimiento responsable del negocio:** El modelo “as a Service” de Tigo Business flexibiliza la forma como se contratan y consumen los recursos que soportan los servicios digitales del negocio, configurando solo las capacidades que requiere el negocio y creciendo dichas capacidades ágil y de forma flexible solo cuando el negocio así lo requiere.

### 3.3 PROPUESTA DE VALOR

En Tigo Business, entendemos que la transformación digital es esencial para el éxito continuo de las empresas y entidades en la era moderna. Como socio estratégico de confianza en soluciones en la nube de Amazon Web Services (AWS), nuestra propuesta de valor se centra en empoderar a nuestros clientes para que logren una innovación ágil, una escalabilidad sin límites y una eficiencia operativa superior.

Tigo Business busca acelerar la transformación digital de todas las empresas y entidades de la región poniendo a disposición de sus clientes servicios como IaaS, Backups, Disaster Recovery, Asesoría en la migración de sus cargas de trabajo hacia la nube, gestión centralizada, conectividad privada y dedicada a través del servicio AWS Direct Connect con el cual se consigue una conexión con anchos de banda según sus necesidades, es segura y de muy baja latencia aprovechando la extensa red de fibra óptica de Tigo Business en toda la región, además de ofrecer servicios profesionales y administrados con el objetivo de dar más valor a nuestros clientes y que ellos puedan centrarse únicamente en sus proyectos y en su crecimiento delegándonos la responsabilidad del mantenimiento y supervisión de sus cargas de trabajo, soluciones e infraestructura en la nube de Amazon Web Services.

Todo esto diseñado, implementado y supervisado por nuestro equipo de expertos cualificados, con una extensa experiencia en la nube y certificados en Amazon Web Services.

### 3.4 DESCRIPCIÓN DE LA PROPUESTA

Tigo Business presenta a COLEGIO MAYOR DE ANTIOQUIA una solución de Tigo Cloud escalable, flexible y segura, que le ayudara a impulsar la transformación digital de su empresa, cubriendo los componentes: Servicios Tigo AWS la implementación, el soporte, el mantenimiento, la operación, el monitoreo y el cumplimiento de ANS, a través del recurso humano, las herramientas, la seguridad y los procesos del ciclo de vida de servicios enmarcados en ITIL y COBIT. Con esta solución Tigo Business ofrece los siguientes diferenciadores:

- Rápido proceso de implementación tecnológica y operativa
- Escalabilidad de la solución a brindar considerando el crecimiento del negocio
- Flexibilidad para el cambio y modificación de recursos
- Confidencialidad sobre la información y documentación procesada
- Oportunidad en la inclusión de nuevos servicios y/o funcionalidades que apoyen el negocio



### 3.5 OBJETIVO

El objetivo principal es presentar al cliente COLEGIO MAYOR DE ANTIOQUIA una solución con las siguientes características.

- **Optimización de costos:** Nuestra solución Tigo Cloud AWS está diseñada para potenciar la eficiencia operativa de su empresa. Al migrar a AWS, elimina la dependencia de inversiones en infraestructura física, lo que le permite adoptar un modelo de pago por uso. Esto significa que solo pagará por los recursos que realmente necesita, lo que resulta en una reducción significativa de costos innecesarios y una optimización absoluta de su presupuesto de TI.
- **Escalabilidad y flexibilidad:** Con Tigo Cloud AWS, su empresa obtendrá la capacidad de escalar sus recursos de TI de forma rápida y eficiente, en línea con las demandas cambiantes del mercado. AWS ofrece la flexibilidad necesaria para aumentar o disminuir la capacidad de procesamiento y almacenamiento según sus necesidades operativas, lo que le permite mantener un rendimiento óptimo en todo momento y adaptarse ágilmente a cualquier situación.
- **Alta disponibilidad y confiabilidad:** La infraestructura de Tigo Cloud AWS se basa en una arquitectura altamente confiable que garantiza la máxima disponibilidad de sus aplicaciones y servicios. Esto se traduce en una reducción significativa del tiempo de inactividad, asegurando la continuidad de su negocio y brindando una experiencia de usuario excepcional para sus clientes.
- **Seguridad avanzada:** Con Tigo Cloud AWS, su empresa puede aprovechar las medidas avanzadas de seguridad ofrecidas por AWS, que incluyen cifrado de datos, autenticación de múltiples factores y monitoreo continuo. Cumplimos con los más altos estándares de seguridad para proteger su información y garantizar el cumplimiento de regulaciones y normativas relevantes.
- **Soporte técnico y asesoramiento especializado:** Nuestro equipo de expertos en Tigo Cloud AWS estará a su disposición para brindarle un soporte técnico de primera clase. Desde el inicio de la implementación hasta la optimización continua, contará con el respaldo de profesionales altamente capacitados que lo guiarán en todo el proceso, asegurando una migración fluida y una gestión eficiente de sus recursos en la nube a través de nuestros servicios administrados y profesionales.
- **Integración con servicios existentes:** La implementación de Tigo Cloud AWS se llevará a cabo de forma transparente y sin interrupciones en sus operaciones actuales. AWS se integra perfectamente con las soluciones y aplicaciones que ya utiliza su empresa, lo que le permite aprovechar al máximo sus inversiones previas. Garantizamos una transición sin complicaciones hacia la nube, así como la integración de nubes híbridas, para una experiencia de migración fluida y eficiente.
- **Innovación y actualización tecnológica:** Con Tigo Cloud AWS, su empresa estará a la vanguardia de la innovación tecnológica, accediendo a las últimas herramientas y tecnologías para mantenerse competitiva en un entorno empresarial en constante evolución. Estaremos a su lado para asegurarnos de que su infraestructura en la nube esté siempre actualizada y optimizada.



- **Análisis y optimización de recursos:** En Tigo, creemos en la importancia de la eficiencia operativa. Con Tigo Cloud AWS, tendrá acceso a herramientas avanzadas de análisis y monitoreo que le permitirán optimizar el uso de sus recursos en la nube. Esto se traducirá en una mayor eficiencia operativa, reducción de costos y una toma de decisiones más informada y estratégica para el crecimiento de su negocio.
- **Cumplimiento normas de calidad:** La seguridad y la calidad son fundamentales en nuestra oferta. Tigo Cloud AWS cumple con los más altos estándares y certificaciones internacionales, asegurando que sus datos y aplicaciones estén protegidos y que los servicios que ofrecemos sean de la más alta calidad. Podrá tener la tranquilidad de que su empresa opera dentro de un entorno seguro y confiable.

### 3.6 ALCANCE

Tigo Cloud AWS, consiste en una solución integral que combina los servicios de AWS, junto con Servicios Administrados y Servicios Profesionales proporcionados por Tigo Business.

Tigo Business agrega valor a la oferta de AWS, al proporcionar Servicios Administrados que realizan la gestión y supervisión continua de la infraestructura y de los servicios en la nube de AWS, por parte de expertos técnicos de Tigo Business. Estos servicios garantizan un monitoreo proactivo, mantenimiento, actualizaciones, solución de problemas y optimización de los recursos en la nube, permitiendo a las organizaciones centrarse en su negocio principal sin preocuparse por la gestión técnica de AWS.

Además de los Servicios Administrados, Tigo Business también ofrece Servicios Profesionales, que se refieren a la consultoría, diseño, implementación y personalización de soluciones basadas en AWS. Estos servicios están respaldados por un equipo de profesionales capacitados y certificados en AWS, quienes trabajan en estrecha colaboración con los clientes para comprender sus necesidades y ofrecer soluciones a medida que maximicen los beneficios de AWS y optimicen la eficiencia operativa.

En resumen, el producto de Tigo Business combina los servicios de AWS con Servicios Administrados y Servicios Profesionales, brindando a las organizaciones una solución completa y personalizada en la nube. Esto les permite aprovechar al máximo las capacidades de AWS, garantizar un rendimiento óptimo, minimizar los riesgos y mejorar la eficiencia operativa, todo respaldado por la experiencia y el apoyo de Tigo Business.

A continuación, se listan las condiciones comerciales, técnicas y de servicio que se aplican a cada oferta o plan habilitado en el portafolio Tigo Cloud AWS.



### 3.7 AMPLIACIÓN DE NUESTRA OFERTA

AWS ofrece una amplia gama de servicios como solución para distintos contextos, para ser presentados al cliente y aplicados según la necesidad. A continuación, se detallan el alcance comercial y las especificaciones técnicas de cada escenario:

#### 3.7.1 IaaS o Infrastructure As a Service

En este escenario (IaaS) entran muchos servicios de AWS fundamentales en toda infraestructura, los cuales están divididos en subcategorías como lo son redes, computo, almacenamiento y bases de datos.

### 3.8 SERVICIOS ADMINISTRADOS

En la siguiente tabla se describen el alcance del Plan de Servicios Administrado de Tigo Business “SA Tigo” Enterprise, se indican las actividades que abarca dicho Plan, especificando el alcance que se realiza sobre cada ítem.

#### 3.8.1 Servicios administrados de Infraestructura

El alcance de los servicios administrados para infraestructura que se encuentren desplegadas en la nube pública de AWS se encuentra en la siguiente tabla:

Categoría	Ítem	Enterprise
Administración y soporte del sistema operativo	Administración de Sistema Operativo	<p>Tigo solo realiza cambios para los fines y situaciones específicos que se describen a continuación:</p> <ul style="list-style-type: none"> <li>Se realizan cambios solo a nivel de infraestructura, utilizando la consola, CLI o las APIs</li> <li>Nunca se realizan cambios en la aplicación del cliente o en aplicaciones de terceros.</li> </ul> <p>A través de Servicios Administrados, Tigo despliega o actualiza recursos únicamente en los siguientes escenarios:</p> <ul style="list-style-type: none"> <li>* Implementación y actualización de herramientas y recursos requeridos para la operación del servicio administrado de Tigo Business.</li> <li>* Implementación como parte de monitoreo, respuesta a eventos y alarmas de la infraestructura.</li> <li>* Para remediar los problemas de seguridad según las mejores prácticas de seguridad.</li> <li>* Durante la remediación y restauración como parte de la respuesta a un incidente.</li> <li>* Solicitudes de clientes con características tales como: <ul style="list-style-type: none"> <li>✓ Administración de alarmas</li> <li>✓ Etiquetas de recursos</li> <li>✓ Líneas base de actualizaciones de seguridad y ventanas de mantenimiento</li> <li>✓ Planificador de ejecución de recursos</li> <li>✓ Planes de respaldo</li> </ul> </li> </ul>



Categoría	Ítem	Enterprise
		<p>✓ Recursos para soportar la carga de trabajo que no requieran ser revisados por el equipo de preventa (ej. Despliegue de recursos que no impliquen la modificación a la arquitectura implementada)</p> <p>Configuraciones de sistema operativo: El equipo de soporte de TIGO puede realizar cambios en el sistema operativo durante situaciones de indisponibilidad y para solución de incidentes.</p> <p>Las siguientes son las actividades contempladas en la administración del sistema operativo:</p> <ul style="list-style-type: none"> <li>* Restauración de instancia EC2 ante fallas siempre que se cuente con un esquema de backup (AWS Backup)</li> <li>* Acompañamiento en Creación de usuarios en Sistema Operativo</li> <li>* Acompañamiento en asignación de permisos a usuarios de Sistema Operativo</li> <li>* Cambio de clave de usuarios</li> <li>* Habilitar/Deshabilitar de usuario de Sistema Operativo</li> <li>* Creación de carpeta con permisos específicos solicitados por el cliente</li> <li>* Revisión de permisos sobre carpetas del Sistema Operativo</li> <li>* Análisis de consumo de recursos del Sistema Operativo</li> <li>* Revisión y cierre de sesiones abiertas en el Sistema Operativo</li> <li>* Instalación y configuración del agente de CloudWatch y AWS Systems Manager</li> <li>* Creación de discos y/o volúmenes para sistema operativo.</li> </ul> <p>Configuración del Sistema Operativo soportadas: SA TIGO soporta las siguientes configuraciones:</p> <ul style="list-style-type: none"> <li>* Arquitectura del sistema operativo (x86-64 o ARM64) cualquiera sistema operativo soportado tanto por SSM (Systems Manager) como por CloudWatch.</li> <li>* Sistemas operativos compatibles: <ul style="list-style-type: none"> <li>○ Amazon Linux 2</li> <li>○ CentOS 7.x</li> <li>○ Oracle Linux 7: versiones menores 7.5 y superiores. Oracle Linux 8: versiones menores 8.3.</li> <li>○ Red Hat Enterprise Linux (RHEL) 8.x, 7.x</li> <li>○ SUSE Linux Enterprise Server 15 SP3, SP4</li> <li>○ Ubuntu Linux 18.04 and 20.04</li> <li>○ Microsoft Windows Server 2022, 2019, 2016, 2012 R2, 2012</li> </ul> </li> </ul> <p>Nota: Para los clientes que cuenten con sistemas operativos licenciados como RedHat, SUSE Linux, y Windows, todo soporte requerido sobre el sistema operativo con el fabricante lo deberá escalar el cliente directamente, si cuenta con soporte de AWS (Developer en adelante) Tigo podrá crear un caso de soporte con AWS para las AMI con licenciamiento incluido.</p>
	Gestión de actualizaciones de seguridad - Periodicidad	Semestral



Categoría	Ítem	Enterprise
Aseguramiento de la cuenta y mejora continua	Refuerzo de controles	Implementación de biblioteca seleccionada de reglas de AWS Config. (Notificación)
	Gestión de accesos y usuarios	Si, siempre y cuando el IdP sea gestionado por Tigo
Gestión de servicio	Respaldo y restauración	Configuración de respaldos y restauración (AWS Backup) de acuerdo con la línea base. En caso de negativa por parte del cliente entregara la correspondiente carta de riesgo
	Administración de bases de datos	Revisar numeral 3.8.2
Registros operacionales, Monitoreo, y Reportes	Reportes de gestión (incidentes/requerimientos,)	A demanda (Responsable país)
	Reportes de servicio (ejecución de respaldos, métricas de infraestructura para los servicios contratados)	Bimestral programado
	Informe de aseguramiento (Gestión de Identidad, Assessment infraestructura y recomendaciones para optimización de costos)	Semestral

### 3.8.2 Servicios administrados de Bases de Datos

El alcance de los servicios administrados para las bases de datos que se encuentren desplegadas en la nube pública de AWS se encuentra en la siguiente tabla:

Ítem	Enterprise
Cantidad de motores de Base de Datos a gestionar	5
Tamaño Base Datos	200GB - 1 TB
Pruebas de restauración Backup	1 semestral
Entrega de reporte	1 mensual
Ajuste de recursos	Aplica
Ajustes o cambios esquema de Backup	Aplica
Ampliación de recursos	Aplica
Análisis de métricas y registros	Aplica
Cambio de plan (aplica para cambio de capacidad en el servicio)	Aplica
Cancelación de Bloqueos	Aplica
Configuración de alertas	Aplica
Configurar políticas de copia de seguridad automatizadas para realizar copias de seguridad regulares y programadas	Aplica
Configurar y monitorear alta disponibilidad y replicación	Aplica
Acompañamiento en Creación de BD	Aplica
Creación de puntos de restauración	Aplica



ítem	Enterprise
Creación y monitoreo de cuentas y roles de bases de datos	Aplica
Creación, modificación o borrado de Jobs	Aplica
Definición de índices y estadísticas adecuadas	limitado a 1 BD
Ejecución Scripts a demanda	Aplica
Establecer directivas de fragmentación de tablas	Aplica
Establecer umbrales de rendimiento	Aplica
Habilitación de accesos	Aplica
Acompañamiento <b>configuración</b> servicios redundancia	Aplica
Reinicio de servicios de Base de datos	Aplica
Restauración de bases de datos	Aplica
Revisión Planes de Ejecución	Aplica
Revisión y ejecución migración de ambientes de pruebas a producción	Aplica

### 3.8.2.1 Gestión de bases de datos en AWS RDS

Este servicio le ofrece al Cliente la posibilidad de delegar la administración de sus motores de bases de datos al Especialista de Tigo.

Tigo Business está en capacidad de administrar los motores de bases de datos relacionados a continuación:

- Amazon RDS Aurora
- Amazon RDS SQL Server
- Amazon RDS MySQL
- Amazon RDS MariaDB

Prerrequisitos de administración de base de datos

- Licenciamiento de Base de Datos
- Soporte activo con fabricante
- Respaldo de datos

Si la base de datos ya está instalada y operativa es necesaria la siguiente información para conocer el estado de salud:

- Descripción de los usuarios creados en la BD y sus roles.
- Actividades periódicas y la transferencia de conocimiento sobre los procesos realizados en la base de datos.
- Políticas de respaldo de la base de datos y sus retenciones.
- Funcionamiento de los Jobs creados en la base de datos.



Si la base de datos va a ser migrada de una infraestructura on premises a una as a service se deberá realizar un chequeo previo de compatibilidad para el correcto proceso de migración y estabilización de la base de datos.

Los motores de base de datos deberán estar configurados bajo las buenas prácticas de acuerdo con la documentación de AWS, las cuales pueden encontrar en el siguiente enlace:

[https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP\\_BestPractices.html](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_BestPractices.html).

Después de realizar el análisis del estado de salud, Tigo podrá realizar recomendaciones de ajustes/mejoras previo a la recepción de la base de datos para su administración. Es responsabilidad del Cliente ejecutar las recomendaciones antes de la entrega a Tigo o contratar servicios profesionales.

Las actividades de administración de bases de datos son las siguientes:

- Ajuste de recursos
- Habilitación redundancia
- Habilitación de accesos
- Definición de índices y estadísticas adecuadas
- Establecer directivas de fragmentación de tablas
- Ajustes o cambios esquema de Backup
- Restauración de bases de datos
- Configurar políticas de copia de seguridad automatizadas para realizar copias de seguridad regulares y programadas
- Creación de puntos de restauración
- Análisis de métricas y registros
- establecer umbrales de rendimiento
- configuración de roles adicionales (en caso de ser necesario)
- Configuración de alertas
- Configurar y monitorear alta disponibilidad, replicación y configuración de grupos de conmutación por error
- Creación y monitoreo de cuentas y roles de bases de datos
- Ejecución Scripts a demanda
- Creación, modificación o borrado de Jobs
- Revisión Planes de Ejecución
- Reinicio de servicios de Base de datos
- Cancelación de Bloqueos
- Revisión y ejecución migración de ambientes de pruebas a producción
- Ampliación de recursos
- Cambio de tipo de instancia (EC2 o RDS)
- Análisis de métricas y datos

Configuraciones y gestiones que impliquen cualquier tipo de manipulación de datos, inserción de datos, eliminación de datos, replicación de datos, etc. Se excluyen de los alcances de servicios administrados. Estas configuraciones serán responsabilidad del cliente.



### 3.8.3 Requerimientos mínimos para administración de cuentas AWS

Para operar las cargas de trabajo en AWS de nuestros clientes, el equipo de SA Tigo ha establecido requisitos mínimos para garantizar el monitoreo del estado de salud de los recursos, la respuesta ante las fallas y las actividades proactivas contempladas en el servicio administrado.

El no contar con alguna de estas configuraciones limitará el alcance del equipo de soporte y la posibilidad de monitorear y/o restaurar un recurso que sea parte de la infraestructura desplegada, por lo tanto, en caso de recibir una carga de trabajo de AWS sin estos componentes, se debe gestionar con el cliente la correspondiente carta de aceptación de riesgos la cual se puede consultar en el siguiente documento:

[Acta de aceptación de riesgos SA Tigo \(sharepoint.com\)](#)

En la siguiente tabla se encuentran cada uno de los requerimientos mínimos que deben contar las cargas de trabajo de AWS para ser operadas por el equipo de soporte con algún plan de SA Tigo:

Componente	Descripción
Reglas de AWS Config	Despliegue de la línea base de reglas de AWS Config que se encuentra en el siguiente documento:  Reglas de Config SA TIGO.xlsx (sharepoint.com)
Nat Gateway	Salida internet para actualizaciones de seguridad en subredes privadas
Alertas	Despliegue de la línea base de alertas de monitoreo, Budget de presupuesto diario y notificaciones del PHD (Personal Health Dashboard):  <u><a href="#">Línea base de alertas - monitoreo SA TIGO.xlsx (sharepoint.com)</a></u>
Agente del agente de Systems Manager y CloudWatch	En todas las instancias EC2, se debe contar con la instalación de los agentes de SSM y CloudWatch para realizar tareas administrativas y tener acceso a las métricas de monitoreo requeridas
RDS Performance Insights	Para los clientes que tengan desplegadas instancias de RDS es requerido habilitar esta herramienta para troubleshooting
Habilitación de logs de AWS System Manager Session Manager	Configuración de logs hacia S3 para las sesiones creadas a través del administrador de sesiones de AWS Systems Manager
AWS Backup	Backup para todas las instancias EC2 de la cuenta
AWS Security Hub	Servicio de administración de la posición de seguridad en la nube (CSPM) que realiza revisiones de las prácticas recomendadas de seguridad.



#### 3.8.4 Consideraciones Servicios Administrados

- Todas las solicitudes de servicios administrados deberán ser gestionadas por el cliente por medio de los canales de soporte de Tigo Business.
- Si el cliente requiere una consulta o gestión de servicio sobre un ambiente virtual o recursos para los cuales no fue contratado el servicio administrado, podrá escalar la solicitud a través del ejecutivo comercial/ejecutivo servicio o rol asociado como un servicio profesional., para que este sea factibilizado y se le presente propuesta comercial al cliente para su aceptación.
- El Cliente será responsable de cualquier instalación o gestión sobre los aplicativos que se encuentren desplegados en los recursos virtuales. El Cliente será responsable del aprovisionamiento / configuración / de cualquier componente de red y seguridad que no se encuentre dentro de la organización de recursos virtuales de cliente.
- Los alcances diferentes a los indicados en el presente documento están sujetos a factibilidad técnica y económica por parte de Tigo, y la presentación y eventual posterior aceptación de la respectiva oferta técnico comercial.
- Toda solicitud realizada por cliente deberá ser sobre servicios contratados con Tigo Business.
- En caso de que el cliente tenga acceso a la consola AWS con Usuario Administrador no puede ser garantizada la disponibilidad ni el cumplimiento de SLA y se deberá firmar la carta de riesgo de administración compartida.
- Para garantizar alta disponibilidad en los servicios críticos del cliente, se recomienda usar diferentes zonas de disponibilidad o región según corresponda.

#### 3.8.5 Requerimientos mínimos para administración de cuentas AWS

Para operar las cargas de trabajo en AWS de nuestros Clientes, Tigo ha establecido requisitos mínimos para garantizar el monitoreo del estado de salud de los recursos, la respuesta ante las fallas y las actividades proactivas contempladas en el servicio administrado.

El no contar con alguna de estas configuraciones limitará el alcance del equipo de soporte y la posibilidad de monitorear y/o restaurar un recurso que sea parte de la infraestructura desplegada, por lo tanto, en caso de recibir una carga de trabajo de AWS sin estos componentes, se debe gestionar con el cliente la correspondiente carta de aceptación de riesgos.

En la siguiente tabla se encuentran cada uno de los requerimientos mínimos que deben contar las cargas de trabajo de AWS para ser operadas por el equipo de soporte con algún plan de Servicios Administrados Tigo:

### 3.9 SERVICIOS PROFESIONALES

Los Servicios Profesionales es el nivel especializado que ofrece Tigo Business a sus clientes con relación a las líneas de TI como Cloud, Data Center, Seguridad, Networking, entre otras. Estos



servicios aplican para ejecutarse en actividades específicas en un periodo corto definido. Son necesarios para diseñar, migrar o implementar servicios en la nube.

A través de los Servicios Profesionales Cloud de Tigo Business, las empresas pueden coordinar la implementación de soluciones en la nube, desde la planificación y diseño hasta la puesta en marcha. La cantidad de horas de trabajo hábiles y no hábiles requeridas para cada proyecto varía según los Servicios Cloud de Tigo Business que se incluyen en la solución y su complejidad.

La prestación de los Servicios Profesionales Cloud Tigo Business, tienen las siguientes condiciones:

- Los Servicios Profesionales por defecto se brindan de forma remota los días hábiles de lunes a viernes, en horario de 5x8 horas locales (de 8:00 am a 5:00 pm). El precio de este servicio se basa en un pago único por hora o en la compra de una bolsa de horas.
- Los Servicios Profesionales se desarrollan según el plan de trabajo previamente acordado con el Cliente, incluyendo si es necesario los casos de Ventanas de Mantenimiento, en horarios nocturnos o fines de semana con una tarifa diferente. Si se requieren horas adicionales de Servicios Profesionales, se factibilizará con el Cliente, requiriendo una adición y/o anexo de servicio nuevo, según aplique para poder contratar dichos servicios, de esta manera Tigo facturará estas horas adicionales. Es responsabilidad del Cliente contar con los recursos necesarios para cumplir con los pagos adicionales relacionados con los Servicios Profesionales.
- Las horas de servicios profesionales adquiridas tendrán una validez de 12 meses desde la fecha de la firma del anexo de servicio, después de este período, las horas no utilizadas expirarán. Es importante que el Cliente tenga en cuenta este plazo máximo de tiempo, para poder planificar y aprovechar la totalidad de horas de servicios profesionales contratadas.

### 3.10 ANTECEDENTES

COLEGIO MAYOR DE ANTIOQUIA, cuenta con infraestructura bajo un esquema de nube pública (sobre AWS) donde aloja varias de sus aplicaciones principales: Documental G+, Accademia, Moodle, Página Web, Miuvirtual, entre otras.

De acuerdo con la facturación del COLEGIO MAYOR DE ANTIOQUIA, y con el fin de dar continuidad a cada una de las seis cuentas existentes detalladas a continuación, se presenta la oferta de renovación en la nube de AWS bajo la modalidad de servicio, calculada con base en el promedio de consumo de los últimos cuatro meses:

#	ID Cuenta	Nombre
1	148761682741,00	Log Archive
2	495599752380,00	Tigo Business Colegio Mayor MGMT
3	615529218654,00	MIBIENESTAR-COLMAYOR
4	664418986274,00	Audit
5	812369156857,00	sicma_colmayor
6	944776520710,00	COLEGIO MAYOR DE ANTIOQUIA



### 3.11 DESCRIPCIÓN GENERAL

De acuerdo con las necesidades del Cliente, se diseñó una solución que consta de los siguientes nuevos componentes en la nube de AWS que se agregaron a las cuentas existentes en modalidad servicio:

#### 3.11.1 Alcance de los Servicios Ofertados

- **Log Archive**

<b>Log Archive</b>
AWS Glue
AmazonCloudWatch
AWS Config
Amazon Simple Queue Service
Amazon Simple Storage Service
AWS Systems Manager
Amazon Simple Notification Service
AWS Data Transfer
AWS Key Management Service
AWS Secrets Manager
AWS CloudTrail
AWS Lambda

#### Tigo Business Colegio Mayor MGMT

<b>Tigo Business Colegio Mayor MGMT</b>
AWS CloudTrail
AWS Glue
CloudWatch Events
AWS Lambda
AWS Secrets Manager
Amazon Simple Queue Service
Amazon Simple Storage Service
AWS Data Transfer
AWS Cost Explorer
AWS Key Management Service
Amazon Simple Notification Service
AWS Support (Business)



## MIBIENESTAR-COLMAYOR

MIBIENESTAR-COLMAYOR
AWS Glue
AmazonCloudWatch
AWS Systems Manager
Amazon Simple Storage Service
Amazon Simple Notification Service
AWS Data Transfer
AWS Key Management Service
Amazon Relational Database Service
Amazon Simple Queue Service
AWS Secrets Manager
Amazon API Gateway
AWS CloudTrail
AWS Config
Amazon Elastic Compute Cloud
Amazon Virtual Private Cloud

## Audit

Audit
Amazon Simple Storage Service
AWS Glue
Amazon Simple Queue Service
AWS Data Transfer
AWS Systems Manager
AWS Config
Amazon Simple Notification Service
AWS Key Management ServiceAWS Key Management Service
AWS Secrets Manager
AWS CloudTrail

## sicma\_colmayor

sicma_colmayor
AWS Config
AmazonCloudWatch
Elastic Load Balancing
Amazon Simple Storage Service



AWS Secrets Manager
Amazon Virtual Private Cloud
AWS Glue
Amazon Simple Queue Service
Amazon Simple Notification Service
CloudWatch Events
AWS Key Management Service
Amazon Elastic Compute Cloud
AWS CloudTrail
AWS Data Transfer
Amazon Relational Database Service
AWS Systems Manager
AWS Backup

#### COLEGIO MAYOR DE ANTIOQUIA

<b>COLEGIO MAYOR DE ANTIOQUIA</b>
Amazon CloudFront
AWS Secrets Manager
Amazon DynamoDB
Amazon Simple Notification Service
AWS CloudTrail
AWS Backup
AWS Security Hub
Amazon Simple Storage Service
CloudWatch Events
AWS Glue
Elastic Load Balancing
AWS WAF
Amazon Elastic File System
AWS Service Catalog
AWS Data Transfer
AWS X-Ray
Amazon Relational Database Service
Amazon Elastic Compute Cloud
AWS Systems Manager
AWS Config
Amazon Simple Queue Service
AWS Key Management Service
AWS Lambda

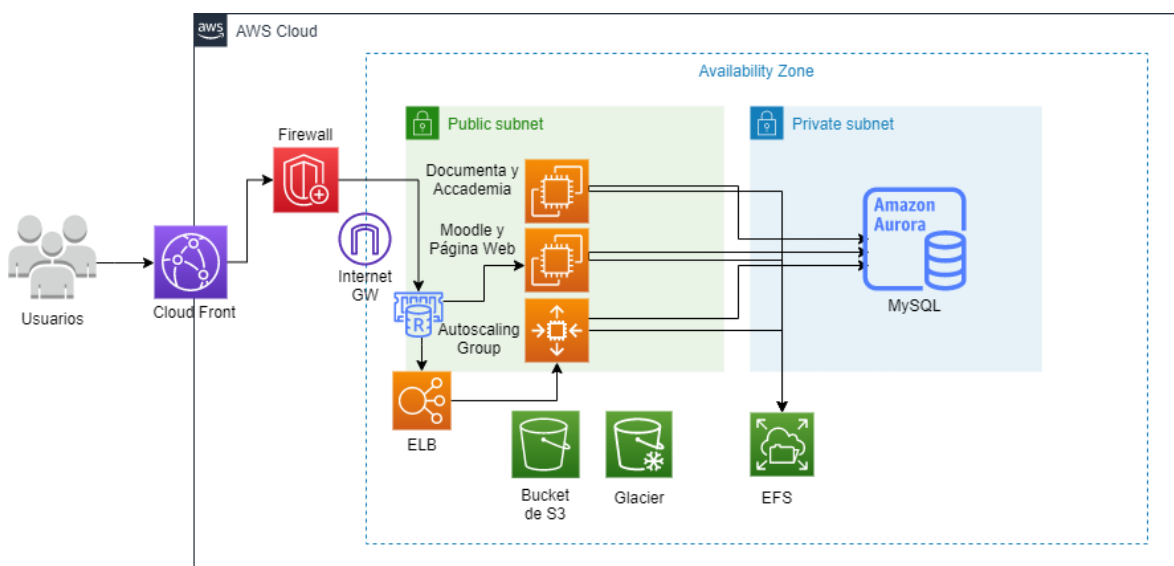
Amazon GuardDuty
AmazonCloudWatch
Amazon Virtual Private Cloud
Amazon ElastiCache

#### Notas

- ✓ En todo caso, el anterior alcance se circunscribe únicamente a lo ofertado en el presente documento.
- ✓ No se incluyen servicios adicionales.

### 3.1.1.2 Arquitectura propuesta

A continuación, se muestra la arquitectura propuesta para la solución:



**Nota:** El diseño presentado es una arquitectura de alto nivel que tiene como único objetivo plasmar el alcance general de la solución ofrecida. Es posible que sufra cambios durante el despliegue de los servicios.

### 3.12 SUPUESTOS Y RESTRICCIONES

- La presente oferta supone que El Cliente ha estimado el dimensionamiento de los recursos necesarios para la correcta ejecución de sus cargas de trabajo, por lo tanto, cualquier inconveniente con el desempeño resultante de la asignación de estos recursos no podrá ser imputable a Tigo.



- Las políticas de respaldo ofertadas por Tigo en la presente oferta se ha dimensionado bajo la consideración que es suficiente para el resguardo de la información, toda vez que hacen parte del paquete de políticas estándar que Tigo ha definido con base en su experiencia y que El Cliente acepta en la medida que no entregó detalle adicional u otros requerimientos acerca de sus necesidades.
- No se contemplan esquemas de coadministración de los servicios, por lo tanto, Tigo no tendrá impacto de configuración en los servicios del Cliente en los casos que el Cliente sea el administrador de la infraestructura.
- Los resultados de la evaluación de infraestructura constituyen una recomendación basada en las condiciones particulares al momento de su realización, por lo cual, los recursos objeto de la presente Oferta y que se implementarán en la nube serán los acordados con El Cliente según las recomendaciones de los fabricantes de las aplicaciones y de su propio conocimiento del desempeño de las cargas de trabajo.
- La arquitectura base ofrecida en esta oferta es susceptible de cambios a nivel de capacidades y/o servicios con el fin de garantizar el desempeño de las cargas de trabajo. Dichas modificaciones se pueden realizar durante las fases de despliegue u operación de las cargas de trabajo.

#### Generales

- Los servicios se considerarán aceptados por resultados y entregables definidos.
- El Cliente acuerda que si, por alguna razón, no tiene capacidad de cumplir con sus responsabilidades y esto genera afectaciones, fallas, inconvenientes, fracasos o retrasos por parte de Tigo en el cumplimiento de sus obligaciones, Tigo no será responsable de dicho incumplimiento o demora.
- El Cliente garantizará la disponibilidad de un contacto válido para coordinar pruebas de funcionalidad de acuerdo con lo requerido por Tigo.
- El dimensionamiento de los recursos ofertados está sujeto a la información entregada por El Cliente. Cualquier cambio adicional sobre el dimensionamiento de la solución está sujeto a viabilidad técnica y económica durante la fase de Implementación.
- Cualquier servicio o solicitud que no esté claramente especificado en este documento se encuentran por fuera del alcance.
- El estado, alcance e integridad de la información alojada es responsabilidad del Cliente.

#### 3.12.1 Acuerdos de Niveles de Servicio

Un acuerdo de nivel de servicio (SLA) define el nivel de servicio que se espera de un proveedor y establece las métricas sobre las cuales se mide el servicio, los siguientes son los tiempos de atención que Tigo Business ofrece a sus clientes para el servicio administrado en AWS:

TIEMPOS DE ATENCIÓN	
HORARIO DE ATENCIÓN	7x24x365



TIEMPO DE ATENCIÓN INICIAL		30 min	
INCIDENTES		SOLICITUDES	
SEVERIDAD	CRITERIOS	SEVERIDAD	CRITERIOS
<b>HIGH</b>	El negocio del cliente tiene una pérdida o degradación significativa de los servicios y requiere atención prioritaria.	<b>HIGH</b>	Solicitudes que el cliente requiere con prioridad media en un entorno productivo.
<b>MODERATE</b>	El negocio del cliente tiene una pérdida o degradación moderada de los servicios, pero el trabajo puede continuar razonablemente de manera deteriorada.	<b>MODERATE</b>	Solicitudes que el cliente requiere con prioridad baja en un entorno productivo o no productivo.
<b>LOW</b>	Para entornos de producción, hay un impacto medio-bajo, o no hay impacto, en la operación o en el desempeño o funcionalidad del sistema. Para entornos de desarrollo, tiene un impacto medio-bajo sobre su negocio, pero este puede continuar funcionando.	<b>LOW</b>	Es una consulta general, solicitud o aclaración de un informe, error en documentación.
TIEMPOS DE ATENCIÓN DE INCIDENTES		TIEMPOS DE ATENCIÓN DE SOLICITUDES	
SEVERIDAD	ATENCIÓN	SEVERIDAD	ATENCIÓN
<b>HIGH</b>	2 horas	<b>HIGH</b>	8 horas
<b>MODERATE</b>	4 horas	<b>MODERATE</b>	16 horas
<b>LOW</b>	24 horas	<b>LOW</b>	24 horas

Tigo se compromete a cumplir con estos SLAs de atención y a proporcionar a sus clientes un servicio de atención al cliente de alta calidad, sin embargo, no se compromete con SLAs de solución, se prestará apoyo y acompañamiento durante la incidencia, no se asegura un tiempo de resolución. El Acuerdo de Nivel de Servicio (SLA) para la infraestructura contratada será el ofrecido por AWS. Los SLAs para cada uno de los servicios de AWS se pueden encontrar en el siguiente enlace:

<https://aws.amazon.com/es/legal/service-level-agreements/>

### 3.13 ROLES Y RESPONSABILIDADES

#### 3.13.1 Modelo de Responsabilidad Compartida Amazon Web Services (AWS)

AWS solo provee seguridad en la infraestructura y servicios, mientras que el Cliente es el responsable por la seguridad en los sistemas operativos, plataformas y datos. En consecuencia, EL Cliente no podrá presentar reclamación en caso de afectaciones o indisponibilidad derivadas de actividades o medidas a su cargo. Para asegurar la seguridad global de la solución, AWS provee servicios y funcionalidades que el Cliente podrá ampliar la seguridad, solicitando servicios adicionales, tales como IAM (Identity and Access Management).

Es importante entender el modelo de responsabilidad compartida en la nube, para identificar las responsabilidades y funciones de seguridad que son administradas por el proveedor de la nube y las



del cliente. Las responsabilidades sobre las cargas de trabajo son diferentes dependiendo del modelo de servicio en nube que elija el cliente para sus servicios, si sus cargas están alojadas en software como servicio (SaaS), plataforma como servicio (PaaS), infraestructura como servicio (IaaS) o en su centro de datos local:



\*Depende del plan de servicios administrados contratado

Esquema basado en el modelo de responsabilidad compartida de AWS:  
<https://aws.amazon.com/es/compliance/shared-responsibility-model/>

### Responsabilidad de Tigo Business

- Habilitar recursos de infraestructura contratados por el cliente.
- Habilitar / configurar servicios adicionales solicitados por el cliente, el contrato y la propuesta deberán ser actualizados.
- Validar que los servicios aprovisionados estén activos y que funcionen correctamente.
- Proporcionar enlaces, usuarios y contraseñas a cliente para el acceso a servicios habilitados.
- Verificar y mantener la disponibilidad del soporte, servicios, accesos y recursos contratados por el cliente.
- Tigo Business es responsable de proporcionar información sobre los canales de comunicación habilitados para gestión y soporte.
- Tigo Business es responsable de garantizar la disponibilidad de un centro de gestión a incidentes.

### Responsabilidades del Cliente

- Brindar la información solicitada por Tigo Business para el seguimiento y desarrollo del proyecto. Esto incluye información sobre las necesidades / requerimientos dentro de la empresa e información de personal designado como punto de contacto.
- Realizar una evaluación de necesidades latentes dentro de la empresa.



- Garantizar el suministro, exactitud y veracidad de toda la información solicitada por Tigo Business.
- En casos en que se entregue información incorrecta, incompleta, con retraso o requisitos adicionales será tratado como una solicitud de cambio por parte del Cliente a los alcances del servicio, por lo tanto, estará sujeto a un control de cambios y a una nueva factibilidad con nuevos costos y la generación de ordenes de servicio adicionales.
- Creación de una lista de requerimientos técnicos y no técnicos de sus necesidades.
- Tigo Business estará a disposición de brindar asesoría en base al plan de servicios administrados contratado y el Cliente será responsable de la toma de las decisiones finales.
- Tigo Business proporcionará accesos a la infraestructura de nube y el Cliente será responsable de su uso y protección.
- En caso de filtración o pérdida de accesos, el Cliente es responsable de solicitar la eliminación o actualización de credenciales.
- El Cliente deberá cumplir con los términos y condiciones establecidos por Tigo Business.
- Es obligación del Cliente proteger información confidencial e información sensible.
- El Cliente debe notificar a Tigo Business ante cualquier cambio relevante en sus necesidades o por problemas que podría enfrentar en relación con los servicios en la nube de AWS, esto puede incluir requisitos de capacidad, problemas de rendimiento o cualquier otro problema o necesidad latente.
- Es responsabilidad del Cliente realizar backups de su información. Tigo Business está a disposición para apoyar en esta u otras tareas aplicando a uno de nuestros planes de servicios administrados (Business, Enterprise y VIP).
- El Cliente debe cumplir con los acuerdos de pago y medios de pago de servicios profesionales y administrados, esto puede incluir pagos iniciales, mensuales, anuales o cualquier otro pago adicional acordado en el contrato.
- Verificar la correcta aplicación de configuraciones que Tigo Business aplique a los servicios provisionados acorde a los requerimientos entregados por el Cliente.
- El Cliente es el único responsable de sus equipos informáticos y conexión necesarios para conectarse o acceder a sus servicios en la nube de AWS, si el Cliente cuenta con servicios de datos o internet adquiridos a través de Tigo Business, estos serán contratos totalmente independientes.
- Mantener protegidos accesos a servidores u otros servicios incluidos en los servicios contratados.
- Es responsabilidad del Cliente contar con sistemas libres de virus, spam o programas maliciosos. El Cliente habilitara su propio sistema de detección de virus, software malicioso entre otros, en caso de no poseer un sistema para tal propósito, debe contratar el servicio a Tigo Business con



el único propósito de mantener seguros sus sistemas, información y contenidos alojados en el espacio o servicios contratados. Si la red se ve afectada debido a software malicioso en la infraestructura, plataforma o sistemas del Cliente, Tigo Business podrá desconectar los servicios de la infraestructura de red y conectividad para proteger a los demás Clientes.

- Asumir la responsabilidad ante la pérdida, robo o mal uso de accesos brindados por Tigo Business.
- El Cliente declara y garantiza que es titular del nombre de dominio de internet que utiliza, dicha afirmación será incluida dentro del contrato y en caso de cualquier demanda, acción judicial, arbitral o administrativa que sea en su contra, razón, origen de dominio infringiendo derechos de propiedad intelectual o por falta de pagos respectivos al registrador de este. El Cliente acepta total responsabilidad, liberando a Tigo Business de toda responsabilidad derivada de daños o perjuicios.
- El Cliente debe declarar y garantizar a Tigo Business que es legítimo titular o propietario de la información alojada en los servicios contratados
- El Cliente debe declarar y garantizar a Tigo Business que es titular o estar legalmente autorizado mediante licencias o contratos correspondientes al incorporar en los servicios contratados: software y sus propias bases de datos.
- El Cliente asume toda la responsabilidad derivada de la titularidad, legitimidad y uso que efectúe de los datos y software, mediante este acto libera a Tigo Business de toda responsabilidad y nos exonera ante una demanda, acción judicial o administrativa resultado de sus propias acciones.
- El Cliente es responsable del manejo de su información, por lo tanto, en todo caso de terminación de contrato independientemente de la causa, entiende y acepta que toda información será destruida o borrada, sin posibilidad de ser recuperada una vez superados los plazos definidos a partir de la notificación que anuncia la baja del sistema y remoción de la información.
- El Cliente acepta que es el único responsable de los contenidos, servicios o bienes ofrecidos a través de los servicios contratados. Si Tigo Business determina que la conducta del Cliente, productos, servicios u contenidos violan la ley aplicable y que dañan la reputación de Tigo Business y ponen en riesgo los sistemas, equipos, procesos o derechos de propiedad intelectual de Tigo Business, nos reservamos el derecho de suspender de forma definitiva e inmediata los servicios brindados en el presente contrato.
- Los negocios de internet que constituyan contenido para adultos, pornografía, instrucciones para el desarrollo de armas de fuego o bombas, contenido que promuevan el racismo, el odio, son negocios denominados restringidos e inaceptables.
- El Cliente será el único responsable del contenido usado y publicación de las informaciones y comunicaciones transmitidas mediante los servicios contratados y de la violación o incumplimiento por su parte de cualquier norma que sea aplicable en relación con la utilización del servicio, incluyendo, entre otras, las disposiciones de códigos de autorregulación en materia de protección de datos, protección de consumidores y usuarios, derecho de propiedad industrial y derecho de autor, actos de competencia desleal, vigentes en cada momento.



- EL Cliente es el único responsable ante Tigo Business y sus empresas afiliadas y se compromete a indemnizarle por todos los daños y perjuicios, intereses y denuncias en las que Tigo Business o sus empresas afiliadas o los terceros contratados pudieran verse afectadas por demandas, o reclamación de un tercero interpuesta como consecuencia de una infracción del Cliente de las obligaciones que contrae.
- El Cliente es el único responsable de los servicios que le presta a sus propios Clientes y del soporte técnico que les brinda, así como de la administración no delegada de los servicios contratados.
- El Cliente es el responsable del uso que le dé él y sus Clientes a los servicios contratados, de administrar su espacio no delegado y de realizar copias de seguridad de los servicios contratados o de contratar a Tigo Business en la realización con copias de respaldo.
- El Cliente garantiza por este medio a Tigo Business que el contenido en o los sitios no infringen o violan leyes y regulaciones aplicables, o causan daños a terceros, incluyendo, pero no limitándose a la pornografía, contenido para adultos, desarrollo o venta de armas de fuego, municiones o bombas, contenido que incite a la violencia y racismo. Ante cualquier caso, Tigo Business se reserva el derecho de aceptar, rechazar o en última instancia eliminar contenido publicado por el Cliente dentro de los servicios contratados sin derecho a reclamo alguno ni compensación de ninguna naturaleza, siendo aceptado expresamente por el Cliente desde el momento de la firma del contrato.

### 3.14 RECOMENDACIONES DE SEGURIDAD EN CLOUD

Estimado cliente, en TIGO su seguridad es nuestra prioridad. Por ello, queremos recordarle la importancia de proteger sus servicios y datos, evitando la exposición directa de ciertos servicios a Internet. Esta práctica puede aumentar el riesgo de accesos no autorizados, explotación de vulnerabilidades y pérdida de información.

Los siguientes son algunos servicios que no deben estar expuestos a Internet

#### **Servicios de Gestión de Infraestructura:**

- Telnet y FTP: Transmiten datos sin cifrado y son altamente vulnerables.
- Remote Desktop Protocol (RDP): Frecuente objetivo de ataques. Úselo solo a través de una VPN segura y/o debe restringirse con listas de control (ACL). Ejemplo, gateway (IP) de su organización.
- Secure Shell (SSH): Aunque seguro, debe restringirse con listas de control (ACL). Ejemplo, gateway (IP) de su organización.

#### **Servicios de Bases de Datos:**

MySQL, PostgreSQL, MongoDB, etc.: No deben ser accesibles desde Internet. Use conexiones internas o túneles cifrados como VPN (de preferencia IPSec) o SSH (con listas de control ACLs).



### **Servicios de Correo y Mensajería:**

SMTP, IMAP y POP sin cifrar: Asegúrese de utilizar SSL/TLS en todo el tráfico de correo. Consolas de gestión de servidores de correo: Proteja accesos administrativos con autenticación segura.

### **Servicios de Monitoreo y Almacenamiento:**

SNMP, Nagios, Zabbix, Grafana, Prometheus: No deben estar abiertos a Internet. Manténgalos en redes privadas o túneles seguros.

Compartimos un listado de buenas prácticas para un entorno seguro

- ✓ Autenticación multifactor (MFA): Actívela siempre que sea posible.
- ✓ Reglas de firewall y acceso restringido a solo su organización: Defina listas blancas de IP y aplique controles de seguridad estrictos.
- ✓ Cifrado obligatorio: Asegure que todas las conexiones usen TLS/SSL.
- ✓ Auditorías periódicas: Identifique y corrija vulnerabilidades antes de que sean un problema.
- ✓ Antivirus/EDR: Ayuda significativamente a la continuidad operativa al prevenir secuestros de datos (ransomware) y ataques a nivel SO, ayuda a proteger la integridad de su información crítica, asegurando el cumplimiento legal y evitando pérdidas financieras por fugas de datos.

### **Importancia de los Respaldos Periódicos:**

Contar con respaldos actualizados de su información y máquinas virtuales, es una medida esencial para garantizar la continuidad del negocio ante incidentes como ataques cibernéticos, fallos en el hardware o errores humanos. Recomendamos establecer políticas de respaldo con la siguiente frecuencia:

- ✓ Respaldo diario: Para datos críticos que cambian constantemente con retención de al menos 1 semana.
- ✓ Respaldo semanal o mensual: Para máquinas virtuales y configuraciones del sistema, con retención de al menos 3 semanas o 3 meses respectivamente.

Asegúrese de que los respaldos se almacenen en ubicaciones seguras, preferiblemente fuera de línea o en soluciones de almacenamiento en la nube cifradas. Además, pruebe regularmente la restauración de respaldos para garantizar su integridad y disponibilidad en caso de necesidad.

Recuerde de concientizar a sus usuarios privilegiados sobre el uso correcto de los accesos y la importancia de usar claves seguras.

Si necesita asesoría para fortalecer la seguridad de su infraestructura, nuestro equipo está listo para ayudarle. Contáctenos y proteja su negocio.



## 4 COMUNICACIONES UNIFICADAS

### Simplifique la comunicación de su Organización

Trabajo Híbrido consiste en poder contar con un espacio de trabajo digital en el cual los participantes puedan estar en diferentes lugares, usando diferentes dispositivos, con diferentes medios de acceso, pero que al final todos puedan experimentar la misma experiencia de comunicación. Para adaptarse a este modelo de trabajo híbrido, las organizaciones ahora necesitan una solución de comunicaciones unificadas confiable para sus empleados y usuarios finales, que trabajen desde casa, desde oficinas y sucursales, o desde cualquier lado. Sus usuarios necesitan acceso a las herramientas adecuadas para ser productivos: herramientas que sean flexibles, seguras y diseñadas específicamente para impulsar la colaboración remota. Todas estas necesidades son abordadas por el producto de comunicaciones unificadas sobre Cisco Webex Calling que provee Tigo Business

#### 4.1 CARACTERÍSTICAS Y BENEFICIOS

Dentro de las características y beneficios que se encuentran al usar la solución de (Cisco Webex Calling)

- **Mejor experiencia del usuario:** Utiliza una sola aplicación para llamar, enviar mensajes, compartir archivos y reunirse. Esto proporciona una experiencia coherente e intuitiva para el usuario final. Así mismo, hace más fácil y manejable el soporte de las áreas de TI.
- **Capacidades de (PBX) para llamadas empresariales:** La solución de comunicaciones unificadas (Cisco Webex Calling) cuenta con características de PBX empresarial como:
  - Operadora Automática
  - Colas de Llamadas.
  - Grupos de búsqueda y captura
  - Líneas compartidas y/o buzones de correo de voz personalizados
  - Números de extensión, números de marcación interna directa
  - Marcación basada en directorio.
  - Funciones de mitad de llamada, MoH, reanudar, reenviar, transferir y conferencia.
- **Dispositivos para cada usuario y oficina:** Además de poder responder su extensión independiente de su ubicación geográfica, los usuarios también podrían elegir múltiples dispositivos para manejar llamadas. Entre los cuales están:
  - Computadora
  - Dispositivo móvil
  - Teléfonos de escritorio habilitados para Webex Calling (Cisco 6800, 7800, 8800)
  - Equipos habilitados para dispositivos de sala de conferencias
- **Análisis e información:** Webex Calling proporciona análisis para ayudar a los clientes a obtener información sobre sus implementaciones de llamadas. Los administradores pueden monitorear fácilmente la información del estado del dispositivo, obtener información sobre la participación de las llamadas y análisis de la calidad de los medios a través del Control Hub.



- **Solución de Colaboración Integrada:** La solución de Webex Calling está disponible en una única aplicación modular, segura y fácil de usar. También puede emparejar/compartir de forma inalámbrica con sus dispositivos de video de Cisco para unirse a reuniones o compartir contenido en la pantalla y en las reuniones.
- **Seguridad:** todos los servicios de Webex, incluidas las llamadas, tienen configuraciones predeterminadas seguras listas para usar que garantizan que sus usuarios obtengan acceso seguro y protección de datos confidenciales, desde el centro de datos hasta las aplicaciones y los dispositivos. Webex Calling se basa en el ciclo de vida de desarrollo seguro (CSDL) de Cisco con los siguientes principios de seguridad: privacidad, seguridad y transparencia.
- **Administración centralizada:** Control Hub es la interfaz web que le brinda al cliente una visión excepcional sobre su entorno de nube. A través de un único panel de control, puede implementar, administrar y admitir la aplicación de llamadas, con aprovisionamiento a través de códigos de activación e importaciones o sincronización de usuarios de plataformas externas como Azure en O365. Adicionalmente, la solución cuenta con un portal de autocuidado para que los usuarios finales pueden manejar configuraciones y preferencias básicas por sí mismos.
- **Redundancia y recuperación ante desastres:** Proporciona servicios de llamadas en la nube a través de centros de datos geográficamente distribuidos y redundantes. Cada centro de datos está diseñado de tal manera que, si un centro de datos deja de estar disponible, el tráfico es redirigido y procesado por otro centro de datos. Todos los elementos de control y servicios de voz migran automáticamente (conmutación por error) casi en tiempo real de un centro de datos a otro, si un centro de datos deja de estar disponible. Todos los elementos del servicio operativo, como las interfaces web de aprovisionamiento y configuración, están diseñados en una arquitectura activa/en espera y se pueden migrar de un centro de datos a otro, cuando surja la necesidad.

## 4.2 PROPUESTA DE VALOR

Con Comunicaciones Unificadas Cisco Webex Calling se podrán simplificar los mecanismos de comunicación a través de la integración de nuestros servicios de telefonía con la plataforma de Cisco Webex Calling, obteniendo las mejores herramientas de comunicación para que su empresa simplifique su trabajo, permitiéndole alcanzar fácil y ágilmente sus objetivos.

Su empresa podrá incrementar la eficiencia de sus comunicaciones, sin grandes inversiones y generando ahorros en tiempo y costos. Desde Tigo acompañamos la transición o actualización de su empresa de la telefonía tradicional a un sistema avanzado de comunicación empresarial en la nube, un paso imprescindible para aumentar la productividad de su empresa.

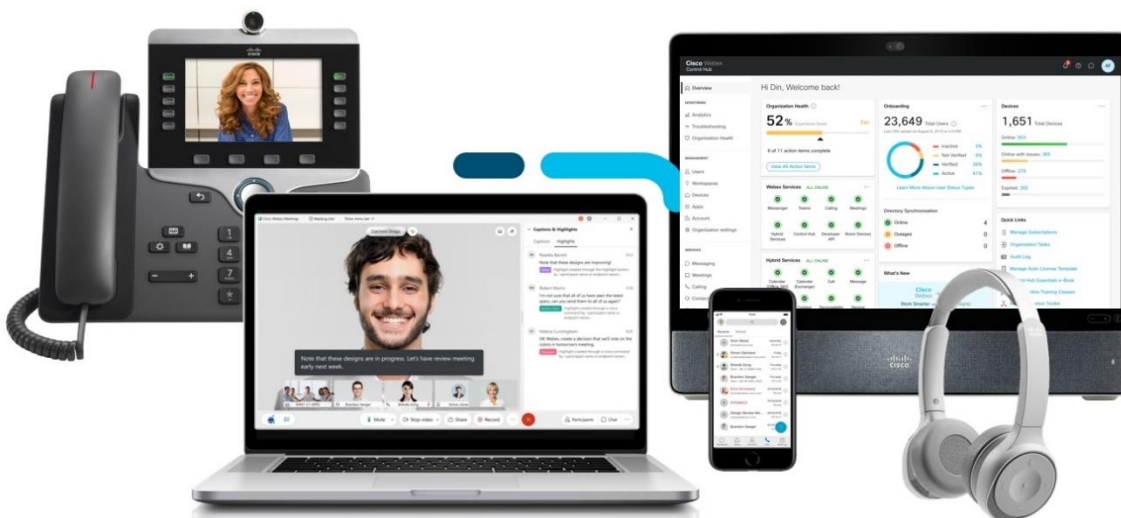
Nuestra experiencia nos permite poner a su disposición un excelente equipo comercial y de ingeniería para acelerar el crecimiento de su negocio.



### 4.3 DESCRIPCIÓN DEL SERVICIO/SOLUCIÓN

Tigo presenta a COLEGIO MAYOR DE ANTIOQUIA una solución de Comunicaciones Unificadas Webex Calling. El equipamiento, la instalación, el soporte, el mantenimiento, la operación, el monitoreo y el cumplimiento de ANS, a través del recurso humano, las herramientas, la seguridad y los procesos del ciclo de vida de servicios enmarcados en ITIL y COBIT. Con esta solución Tigo ofrece los siguientes diferenciadores:

- Rápido proceso de implementación tecnológica y operativa
- Simplicidad en la operación
- Escalabilidad de la solución a brindar considerando el crecimiento del negocio
- 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



Comunicaciones Unificadas sobre Cisco Webex Calling es una solución comprobada de colaboración en equipo y llamadas basada en la nube y de nivel empresarial que combina llamadas, reuniones,



mensajería, centro de contacto y dispositivos integrados en una sola experiencia de usuario, lo que brinda a su compañía todo lo que su fuerza laboral necesita para sea productivo desde cualquier lugar.

Webex Calling trabaja con las herramientas de sus empleados y contratistas; ya está en uso y está diseñado para garantizar que las comunicaciones y los datos de su empresa estén protegidos. Puede trabajar desde cualquier lugar con capacidades completas de control de llamadas que son fáciles de adquirir, incorporar y administrar a través de un portal de administración central.

Con Cisco Webex Calling, permite que se reemplace su sistema actual de telefonía (PBX) local por una solución de llamadas en una nube confiable a nivel mundial. Webex Calling ofrece el acceso a la PSTN de Tigo de manera centralizada optimizando los costos de conexión a la red pública de telefonía.

Como parte de la solución de Cisco Webex Calling se tiene la aplicación modular, Webex App, la cual permitirá elegir los servicios que se van a tener para cada usuario incluyendo telefonía, mensajería y reuniones. Para este último punto se tiene en las licencias de telefonía de la solución de Webex Calling la solución de reuniones de Webex en su forma básica en donde cada usuario puede hacer reuniones con usuarios internos o externos de su compañía teniendo 100 participantes por un tiempo de 40 minutos.

La solución de Webex Calling tiene características básicas de un sistema de telefonía como el establecimiento de llamadas internas, externas, reenvío de llamadas, llamada en espera, buzón de voz, permisos de llamadas, acceso a la red pública telefónica de Tigo, así como características avanzadas como encolamiento de llamadas con roles de supervisor, agente, reportería, grupos de llamadas, cliente recepcionista, paging, etc que hacen esta solución en nube la más completa del mercado.

#### 4.4 CARACTERÍSTICAS DEL SERVICIO DE CISCO WEBEX CALLING

Las siguientes son las características específicas de la solución presentada, funcionalidades del servicio:

##### Características de la plataforma de telefonía en Nube Cisco Webex Calling

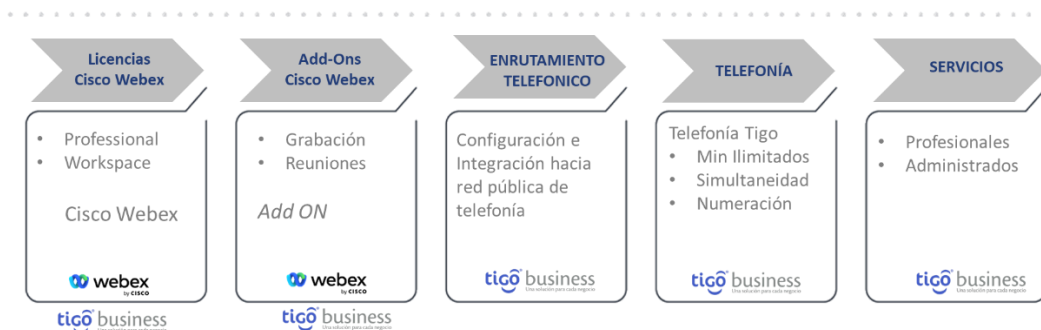
Carcterísticas de Sitio		
Auto Attendant	Music on Hold	Call Park Group
Call Pick Up	Call Queue	Receptionist Client
Group Paging	Hunt Group	Intercept Group
Intercept User	Voice Portal	

Características de Usuario		
Voicemail	Anonymous Call Rejection	Barge-In Exempt



Visual Voicemail	Busy Lamp Monitoring	Call Forwarding: Always/Busy/No Answer/Selective
Call History	Call Hold & Resume	Call Logs w/ Click to Dial
Call Notify	Call Queue Agent	Call Redial
Call Return	Call Transfer (Attended & Blind)	Call Waiting
User Web Portal	Video (Point to Point)	Convenience Call Recording*
Directed Call Pickup	Directed Call Pickup with Barge In	Do Not Disturb
Enterprise Phone Directory	Executive / Executive Assistant	Sequential Ring
Feature Access Codes	Hoteling: Host & Guest	Inbound Caller ID (Name & Number)
Unified Messaging	Three-Way Calling	Multiple Line Appearance
N-Way Calling (6)	Office Anywhere	Outbound Caller ID Blocking
Personal Phone Directory	Priority Alert	Privacy
Simultaneous Ring	Remote Office	Shared Call Appearance

#### 4.5 OFERTA – COMPONENTES



#### Partner Regional Cisco

Dentro de los componentes que Tigo puede entregar como parte de su oferta se encuentran los siguientes, los cuales serán facturados de manera independiente:

**Licenciamiento Webex:** Tigo como partner de Cisco suministra las licencias que sean requeridas para la prestación de los servicios contratados, para este caso el licenciamiento de llamadas o de componentes adicionales como reuniones avanzadas y grabación.



**Interconexión Telefónica – Local Gateway:** Corresponde a la comunicación que se debe establecer entre el servicio de Telefonía que se ofrece desde el Datacenter de Tigo y la nube de Cisco Webex través de Internet.

**Telefonía:** Corresponde al servicio para habilitar llamadas telefónicas entrantes y salientes hacia o desde la red de telefonía pública, usando números telefónicos de Tigo.

**Servicios Administrados:** Tigo cuenta con planes para realizar la gestión y administración de la plataforma de Cisco Webex atendiendo las peticiones de servicio postventa acorde con sus necesidades, para esta propuesta se ofrecen los servicios administrados básicos:

- **Básico:** Asesoría en el alcance en el licenciamiento de los servicios, sesión remota para traslado de conocimiento, soporte en función de la licencia contratada con Tigo, escalamiento funcional hacia Cisco de licencias contratadas con Tigo, un (1) cambio al mes en configuración de Cisco Webex Calling por extensión, componente de Telefonía, sobre un (1) elemento (IVR, Cola, Usuario o DIDs).

El dimensionamiento de la cantidad de horas requeridas para el servicio será validado y acordado con el cliente en el levantamiento de la necesidad y plasmado en el formato de Tigo para su estimación de la oferta.

## 4.6 CALL CENTER BÁSICO

Call Center Básico es una capacidad avanzada de encolamiento de llamadas que hace que sea fácil y asequible administrar un alto volumen de llamadas en el servicio de Webex Calling. Esta funcionalidad agrega características claves que brindan capacidades de supervisor, mejora las políticas de cola para determinar el enrutamiento de llamadas según el horario comercial, proporciona enrutamiento basado en habilidades e informes y análisis para administradores. Call Center Básico es una funcionalidad incluida en el licenciamiento de llamadas de Webex Calling.

Call Center Básico refiere a una colección de funciones diseñadas para trabajar en conjunto que permiten apoyar la gestión de alto volumen de llamadas dirigidas a equipos de soporte y/o ventas:

### Características:

- Encolamiento de llamadas entrantes.
- Enrutamiento basado en habilidades
- Enrutamiento (Circular, Top-down, inactivo durante más tiempo, ponderado, repique simultaneo)
- Mensaje de Bienvenida (aviso predeterminado o personalizado)
- Mensaje de tranquilidad/Anuncios.
- Mensaje de espera en cola (posición en cola o tiempo de espera).
- Políticas de cola mejoradas para servicio nocturno, servicio de vacaciones, reenvío forzado, llamadas bloqueadas.
- Inicio/cierre de sesión del agente en las colas de llamadas
- Gestión del estado del agente
- Operación del agente en múltiples colas de llamadas



- Asignar supervisores a agentes
- Funcionalidades para supervisores (mentoría, monitoreo silencioso, irrupción)
- Informes de colas de llamadas y paneles de análisis
- Limitación de cantidad de llamadas en cola
- Tratamiento de desbordamiento (Tono de línea ocupado, transferencia a otro número)

Call center básico se apoya en el portal de administración del servicio (Webex Control Hub) para entregar un amplio compendio de informes y estadísticas predefinidas brindan a los administradores acceso a visualizaciones de datos interactivos que muestran información importante.

#### 4.7 LICENCIAMIENTO WEBEX CALLING

Licenciamiento Webex Calling	Workspace	Professional
Numero de dispositivos	56	100
Licencia de sesión SIP hacia PSTN 1 licencia / Por cada 2 Licencias de Telefonía.	✓	✓
Grabación Personal Dubber Go (Ilimitado, retención 30 días)	✓	✓
Aplicación de Webex	x	✓
Buzón de Voz	x	✓
Call Center Básico	✓	✓
IVR	✓	✓
Reuniones de Webex Básicas	x	✓

#### 4.8 ATRIBUTOS CONFIGURABLES ADICIONALES / OPCIONALES

##### 4.8.1 Grabación de Llamadas

Grabación de Llamadas	Incluido	Tiene Costo Adicional
Dubber Go	SI	NO
Dubber Personal Recording	NO	SI
Dubber Unified Capture	NO	SI
Dubber Insights	NO	SI

## Dispositivos Telefónicos

### Teléfonos IP Cisco Multiplataforma Serie 6800



Los teléfonos multiplataforma Cisco IP Phone 6800 Series están diseñados para ser asequibles. Ofrecen audio confiable de nivel empresarial, con integración Gigabit Ethernet y bajo consumo de energía.

Ideal para clientes con necesidades de VoIP de moderadas a activas, los teléfonos de la serie 6800 son compatibles con proveedores de comunicaciones unificadas como servicio (UCaaS) de terceros aprobados por Cisco.

La marca y referencia de los equipos mencionados en esta oferta puede variar dependiendo de la disponibilidad, sin embargo, las características técnicas se mantienen.

## 4.9 DESCRIPCIÓN DE LA PROPUESTA

### 4.9.1 Objetivo

El objetivo principal es presentar al cliente COLEGIO MAYOR DE ANTIOQUIA una solución basada en la nube de colaboración de Cisco, la cual proporciona la habilitación de los servicios de telefonía y colaboración sobre la plataforma de Cisco Webex Calling, que le permitirá disponer de un servicio de comunicaciones unificadas (voz, video, chat, reuniones) capaz de comunicarse con la telefonía pública a través de la interconexión a la red voz de Tigo.

### 4.9.2 Elementos Ofrecidos

Para cubrir el requerimiento de COLEGIO MAYOR DE ANTIOQUIA en el proceso de migración, Tigo Business se permite presentar una oferta con los siguientes elementos y servicios:



Sede CL 65 CR 77 -126 Medellín

- Licencias Webex Calling Professional
  - 100 Extensiones
- Licencias Webex Calling Workspace
  - 56 Extensiones
- Troncal SIP Fija Centralizada en Data Center Tigo
  - 30 canales de simultaneidad
  - Plan de Minutos Ilimitado Nacional Fijo
- Servicios Administrados Plan **Básico**

#### Detalle de cantidades:

OFERTA WEBEX CALLING	Cantidad
NU Webex Calling Professional	100
NU Webex Calling Workspace	56
Enrutamiento Telefónico Estandar-P1MM	30
Servicio Administrado Basico-P1MM	156
Teléfonos Cisco 6851	140
TSIP_Dedicada_Sin Minutos	3
TSIP_Dedicada_Acceso_Adicional	27
ILIMITADO ENTRE 30 Y 59 TRC	1

#### 4.9.3 Alcance

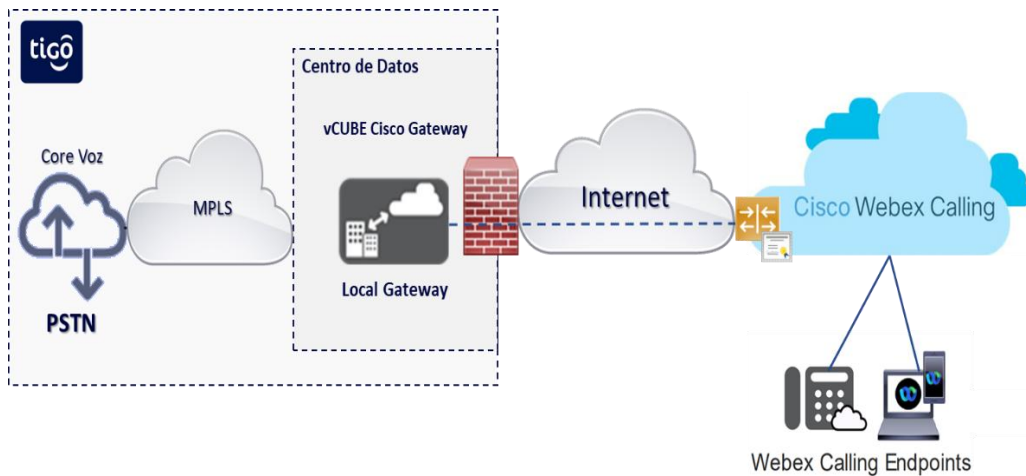
El diseño contenido en este documento contempla el alcance general del servicio, las funcionalidades incluidas, los componentes ofertados y las cantidades consideradas de cada uno de sus componentes para la elaboración de la presente propuesta.

#### 4.9.4 Especificaciones técnicas - Arquitectura y Diseño.

A continuación, describiremos de manera general los componentes técnicos del servicio, su interacción y la forma de operación para que el servicio pueda funcionar de manera integral.

#### 4.9.5 Topología General de la Solución.

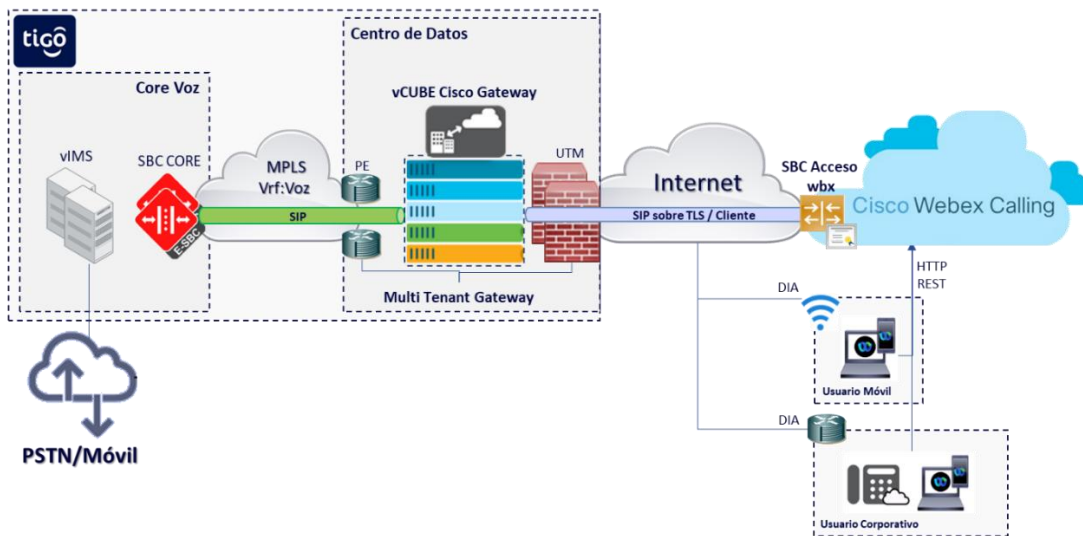
La solución de Webex Calling es una solución en la nube pública de Webex en donde el acceso se hace por Internet. Cada dispositivo telefónico o la aplicación de Webex se registrará en el servicio de Webex Calling usando el canal de internet y accederá a la PSTN a través del DC de Tigo usando Local Gateways que permiten la conectividad hacia la red pública de telefonía.



La topología general del servicio comprende:

- Servicios de Telefonía de acuerdo con las capacidades contratadas.
- Servicio de Interconexión telefónica a través de un Local Gateway Cisco Centralizado en el Centro de Datos de Tigo UNE Certificado.
- Seguridad Perimetral en Datacenter Tigo para el Interconexión telefónica.
- Conexión a internet centralizada para los servicios de interconexión telefónico en el Datacenter de Tigo con la Nube de Cisco Webex Calling.
- Certificado digital en los SBC de Webex Calling firmado por una CA Publica para establecimiento de SIP trunks Cifrados por cada tenant.

#### 4.9.6 Topología Lógica



La arquitectura general de operación del servicio comprende:

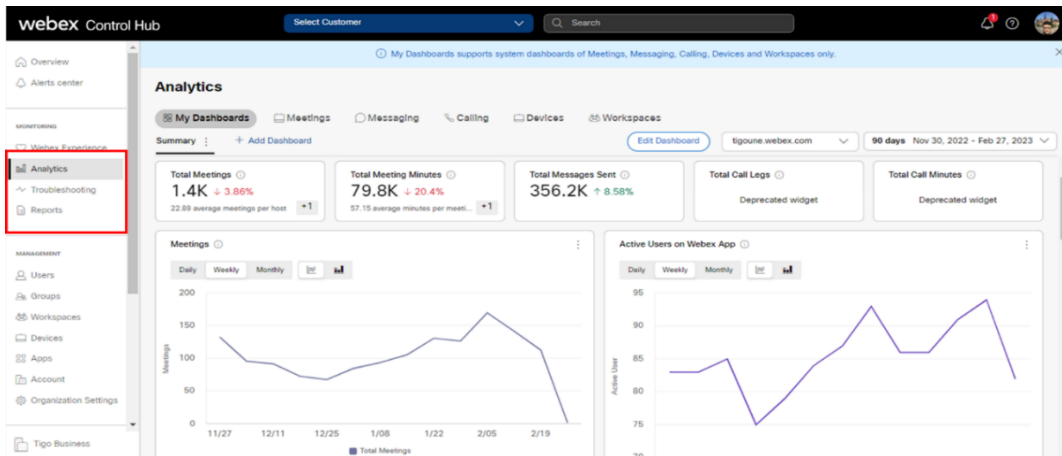
- Core de Voz - Tigo
  - SBC de Core en Alta disponibilidad que normalizan los servicios y protegen toda la arquitectura de voz de Tigo.
  - IMS en Alta disponibilidad que gestiona y administra los abonados de voz.



- Conexiones con la PSTN y Redes móviles propias o de otros Service Providers.
- MPLS - Tigo
  - Red Nacional de Tigo con múltiples conexiones redundantes.
  - Red privada virtual (vrf) exclusiva para los servicios de voz y conexión SIP entre los SBC de Core y SBC Certificados.
- Centro de datos - Tigo
  - Conexiones redundantes hacia la red MPLS por medio de 2 PE o equipos de enrutamiento con soporte para alto volumen de tráfico.
  - Gateway Cisco para la habilitación de la interconexión telefónica entre la nube de Webex Calling y el Core de voz de Tigo, con posibilidad de habilitación de geo redundancia en Datacenter de Tigo distinto.
  - Seguridad Perimetral mediante UTM desplegados en Alta Disponibilidad.
  - Acceso de Internet centralizado y redundante para la interconexión telefónica con la nube de Cisco Webex Calling.
  - Conexión segura con la nube de Webex Calling mediante SIP sobre TLS.
  - Certificado digital del SBC de acceso de Cisco para el establecimiento del SIP sobre TLS por cada Tenant de cliente.
- Nube de Cisco Webex Calling
  - Sistema de telefonía en nube para habilitar el control de llamadas y las capacidades de Private Branch Exchange (PBX).
  - Monitoreo de llamadas disponible en el centro de administración de Cisco Webex Control Hub.
  - Análisis e informes telefonía disponible en el centro de administración de Cisco Webex Control Hub.
- Usuarios móviles - Cliente
  - Acceso a Internet Directo (DIA) fijo o móvil, suministrado por el usuario final.
  - Aplicativo Cisco Webex instalada en dispositivo tipo pc o móvil.
- Usuarios Corporativos - Cliente
  - Acceso a Internet Directo (DIA) cableado o inalámbrico suministrado por el cliente en la sede corporativa.
  - Aplicativo Cisco Webex instalada en dispositivo tipo pc o móvil.

#### 4.9.7 Analíticas y Reportes Estándar

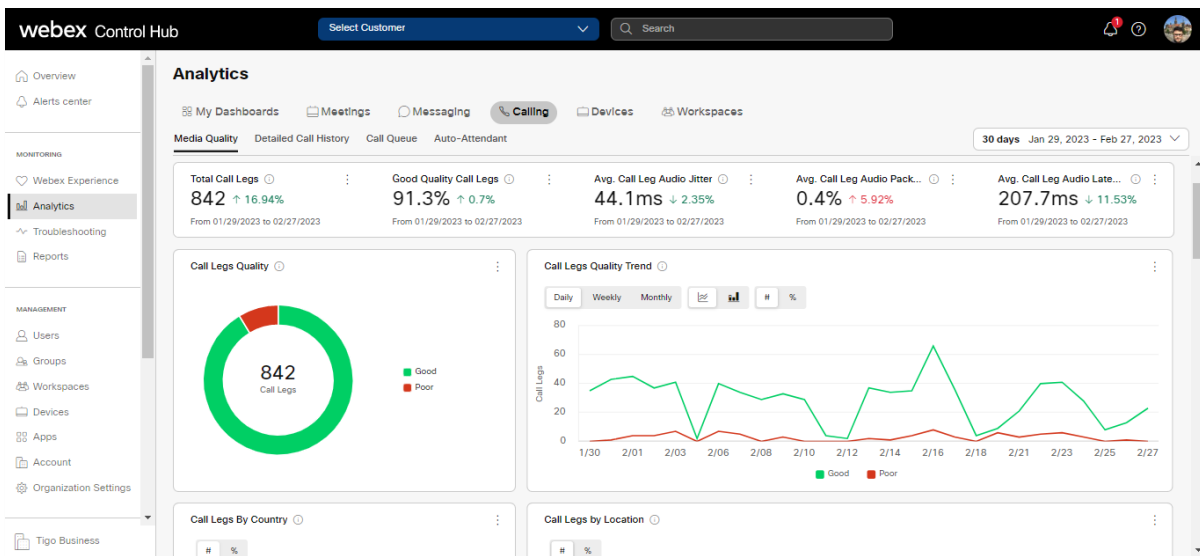
El portal de administración del servicio, Cisco Webex Control Hub, permite visualizar tableros de Analíticas, Resolución de problemas y Reportes desde una interfaz gráfica amigable e intuitiva.



**Analíticas:** En la sección de Analíticas, se cuentan con tableros predefinidos para visualizar estadísticas de Reuniones, Mensajería, Llamadas, Dispositivos, espacios de trabaja. También, se cuenta con un tablero que resume los reportes de consumo de los distintos servicios activados hasta por un histórico de 90 días.

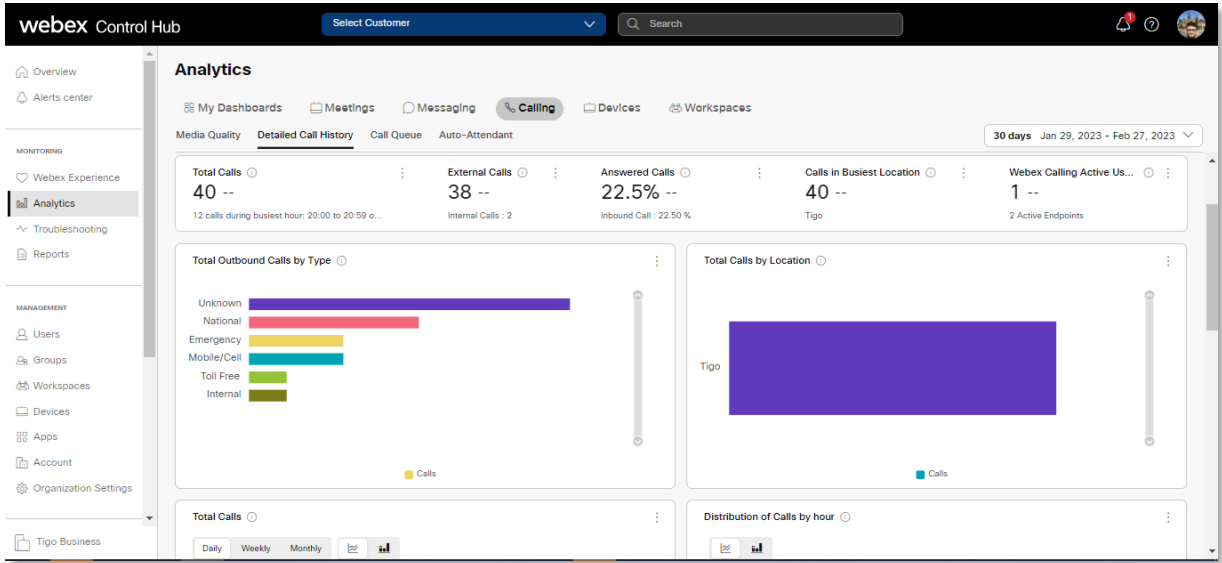
La sección de analítica de llamadas. Permite visualizar estadísticas de la Calidad de las Llamadas, Histórico detallado de llamadas, estadísticas de colas de llamadas y Auto Attendants.

## Calidad de la media

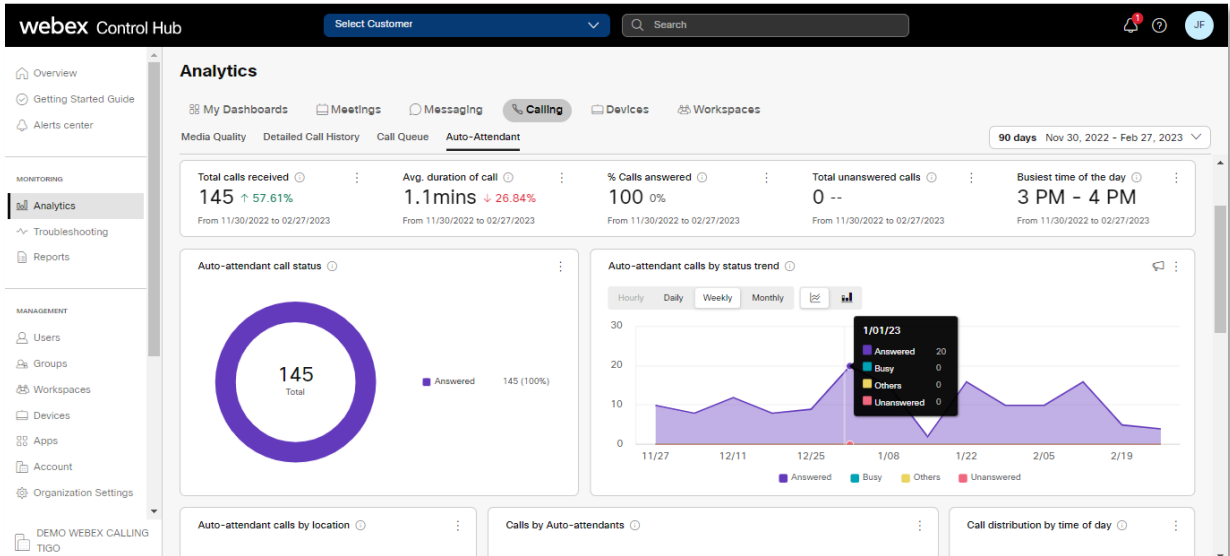




## Histórico detallado de llamadas

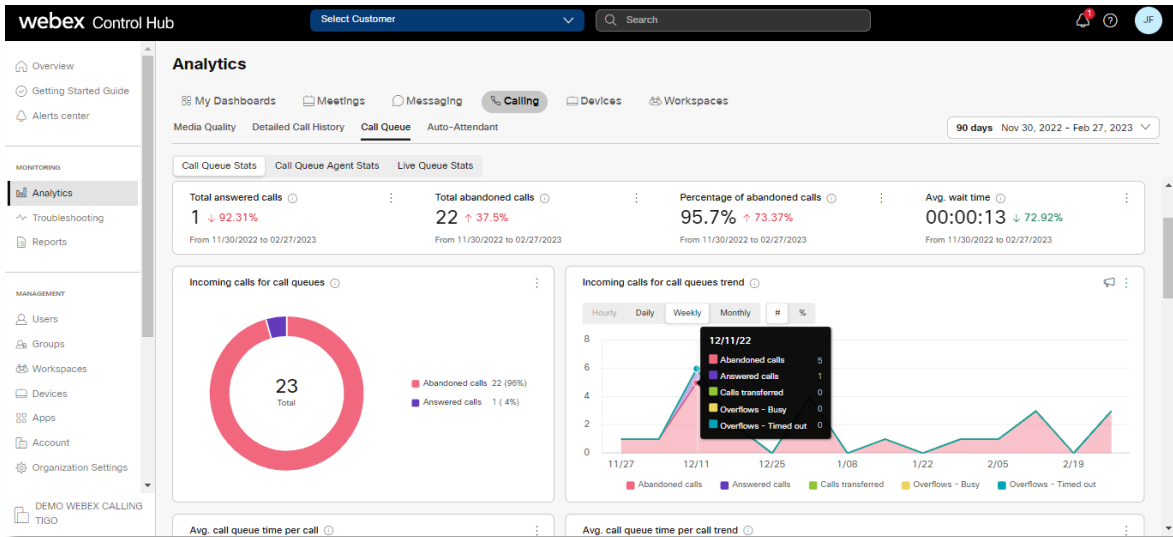


## Estadísticas Auto Attendant





## Estadísticas Cola de Llamadas



### KPI's de desempeño de Cola de Llamadas

- **Total de Llamadas contestadas:** Número total de llamadas que contestan los agentes
- **Total de Llamadas abandonadas:** Número total de llamadas donde el llamante cuelga antes de que un agente esté disponible
- **Porcentaje de llamadas abandonadas:** Porcentaje de llamadas donde el llamante cuelga antes de que un agente esté disponible.
- **Tiempo promedio de espera en cola:** Tiempo promedio que esperan los llamantes a que un agente este disponible para contestar la llamada



### Tendencias para llamadas entrantes a la cola

Este gráfico muestra un desglose de las estadísticas de la cola de llamadas para llamadas entrantes. Este gráfico permite ver cómo las colas de llamadas manejan todas las llamadas entrantes a su organización.

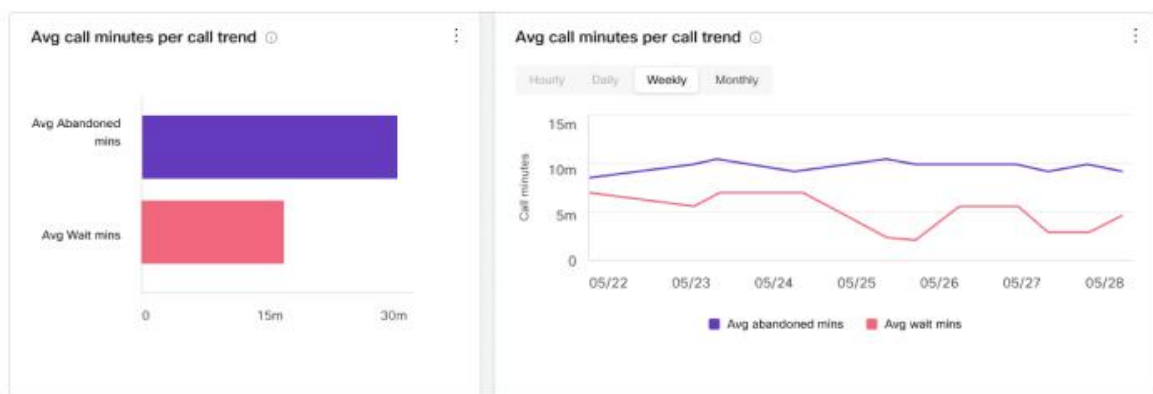




### Promedio de minutos de cola de llamadas por llamada y tendencia

Este gráfico muestra un desglose entre el promedio de minutos abandonados y el promedio de espera de las llamadas entrantes. Puede usar este gráfico para ver cuánto tiempo tuvieron que esperar las personas que llamaron antes de colgar la llamada o ser transferidos a un agente. Los minutos promedio se calculan como:

- Promedio de minutos abandonados: promedio de minutos de llamada que las personas que llamaron esperaron a un agente antes de colgar o seleccionar la opción para dejar un mensaje.
- Minutos de espera promedio: tiempo promedio que las personas que llaman pasan esperando que el siguiente agente disponible responda la llamada.



### Top 25 principales colas de llamadas por estado de las llamadas

Esta tabla muestra el Top 25 colas de llamadas principales con la mayor cantidad de llamadas por estado específico. Los estados de las llamadas disponibles son:

- Llamadas respondidas: número de llamadas respondidas por los agentes.
- % de llamadas respondidas: porcentaje de llamadas respondidas por agentes.
- Llamadas abandonadas: número de llamadas en las que la persona que llamó colgó o dejó un mensaje antes de que un agente estuviera disponible.
- % de llamadas abandonadas: porcentaje de llamadas en las que la persona que llamó colgó o dejó un mensaje antes de que un agente estuviera disponible.
- Desbordamientos - Ocupado: número de llamadas que se desbordaron a una cola de llamadas diferente porque se alcanzó el límite de la cola.
- Desbordamientos - tiempo de espera agotado: número de llamadas que se desbordaron a una cola de llamadas diferente porque el tiempo de espera superó el límite máximo configurado.
- Llamadas transferidas - número de llamadas que se transfirieron fuera de la cola.



Call Queue	answered Calls	answered Calls
Call Queue 33	% of answered calls	1.3%
Call Queue 12	abandoned calls	1.5%
Call Queue 12	% of abandoned calls	1.5%
Call Queue45 abcdefghj...	overflows - busy	1.7%
CQ_Main_HQ_3536	overflows - timed out	1.3%
Queue_Rec_23	calls transferred	1.1%
Call Queue 3	Number of calls	0.7%
Call Queue 32	Washington D.C.	83.7%

### Estadísticas Cola de Llamadas

Esta tabla muestra los detalles de las colas de llamadas que se han configurado en su organización. Puede usar esta tabla para ver la cantidad de llamadas entrantes a las colas de llamadas y el estado de esas llamadas. También puede buscar colas de llamadas, ubicaciones, números de teléfono y extensiones específicas utilizando la barra de búsqueda en la tabla. Los detalles disponibles son:

- Cola de llamadas: nombre de la cola de llamadas.
- Ubicación: ubicación asignada a la cola de llamadas.
- Número de teléfono: número de teléfono asignado a la cola de llamadas.
- Extensión: número de extensión asignado a la cola de llamadas.
- Total, de minutos en espera: número total de minutos que los agentes pusieron las llamadas en espera.
- Promedio de minutos en espera: número promedio de minutos que los agentes pusieron las llamadas en espera.
- Minutos totales de conversación: cantidad total de minutos que los agentes estuvieron hablando activamente en las llamadas.
- Promedio de minutos de conversación: promedio de minutos que los agentes estuvieron hablando activamente en las llamadas.
- Minutos totales de atención: número total de minutos que los agentes dedicaron a atender llamadas. Los minutos de atención se calculan como Minutos totales de conversación + Minutos totales de espera = Minutos totales de atención.
- Promedio de minutos de atención: número promedio de minutos que los agentes dedicaron a atender llamadas.
- Minutos de espera totales: cantidad total de minutos que las personas que llamaron esperaron a que el siguiente agente disponible respondiera la llamada.
- Minutos de espera promedio: número promedio de minutos que las personas que llamaron esperaron a que el siguiente agente disponible respondiera la llamada.
- Llamadas respondidas: número de llamadas respondidas por los agentes.
- % de llamadas respondidas: porcentaje de llamadas respondidas por agentes.
- Llamadas abandonadas: número de llamadas en las que la persona que llamó colgó o dejó un mensaje antes de que un agente estuviera disponible.
- % de llamadas abandonadas: porcentaje de llamadas en las que la persona que llamó colgó o dejó un mensaje antes de que un agente estuviera disponible.



- Promedio de minutos abandonados: promedio de minutos en los que las personas que llamaron colgaron o dejaron un mensaje antes de que un agente estuviera disponible.
- Minutos abandonados: cantidad de minutos en los que las personas que llamaron colgaron o dejaron un mensaje antes de que un agente estuviera disponible.
- Total de llamadas: número total de llamadas entrantes.
- Desbordamiento - Ocupado: número de llamadas que se desbordaron porque se alcanzó el límite de la cola.
- Desbordamiento - Tiempo agotado: número de llamadas que se desbordaron porque el tiempo de espera superó el límite máximo.
- Llamadas transferidas: número de llamadas que se transfirieron fuera de la cola.
- Cantidad promedio de agentes asignados: cantidad promedio de agentes asignados a las colas de llamadas.
- Número promedio de agentes que manejan llamadas: número promedio de agentes que manejan llamadas activamente.

Call queue stats

Search by Call queue name, Extension, Location, Phone no....

Call queue	Location	↑ Extension	Phone no.	Total hold time	Avg. hold time	Total talk time
CQ_Soporte	IDC Med	9980		00:00:00	00:00:00	00:00:02
CQ_Ventas	IDC Med	9981		00:00:00	00:00:00	00:00:00
CQ_Implementacion	IDC Med	9982		00:00:00	00:00:00	00:00:00

### KPI's de cola de llamada en vivo.

Los KPI están disponibles en la parte superior de la página para mostrarle todas las llamadas entrantes actuales y cuáles son sus estados para ayudarlo a monitorear las colas de llamadas en tiempo real. Los KPI disponibles son:

- Llamadas activas: muestra la cantidad de llamadas en las que los agentes están hablando con las personas que llaman. El porcentaje muestra el cambio de valor a lo largo del tiempo comparándolo con los últimos datos actualizados hace 30 segundos.
- Llamadas en espera: muestra la cantidad de llamadas que están esperando a que responda el siguiente agente disponible. El porcentaje muestra el cambio de valor a lo largo del tiempo comparándolo con los últimos datos actualizados hace 30 segundos.
- Llamadas en espera: muestra la cantidad de llamadas que los agentes pusieron en espera. El porcentaje muestra el cambio de valor a lo largo del tiempo comparándolo con los últimos datos actualizados hace 30 segundos.

Active calls	Calls Waiting	Held calls
23K ↑ 13% +1	10K ↑ 5% +1	20K ↑ 13% +1

### Estadísticas de cola de llamada en vivo.

Esta tabla muestra los detalles de todas las colas de llamadas que se han configurado en su organización. Puede usar esta tabla para ver qué cola de llamadas recibe la mayor cantidad de llamadas y ajustar la cantidad de agentes según sea necesario. También puede buscar colas de



llamadas, ubicaciones, números de teléfono y extensiones específicas utilizando la barra de búsqueda en la tabla. Los detalles disponibles son:

- Cola de llamadas: el nombre de la cola de llamadas.
- Ubicación: la ubicación asignada a la cola de llamadas.
- Número de teléfono: el número de teléfono asignado a la cola de llamadas.
- Extensión: la extensión asignada a la cola de llamadas.
- Llamadas activas: la cantidad de llamadas en las que los agentes están hablando con las personas que llaman.
- Llamadas retenidas: la cantidad de llamadas que los agentes han puesto en espera.
- Llamadas en espera: la cantidad de llamadas que están esperando al siguiente agente disponible.
- Marca de tiempo (UTC): la hora en que se capturaron los datos.

**Resolución de Problemas:** En la sección de resolución de problemas, se puede visualizar la actividad de un usuario y como se comportó ésta durante la interacción con una llamada o una reunión. Estas estadísticas son enfocadas a la resolución de problemas y están disponibles por un rango de 21 días.

Quality	Service	Start Time	Meeting / Caller ...	Name	Host / Caller	Particip...	Duration	Site / Loc...	Conference / Call ID
None		2023-02-25 11:43:37 ...	317916687	Sala personal de Howard C...	howard cardo...	2	1:15:47	tigoune	253128160819818320
None		2023-02-22 06:30:59 ...	317916687	Sala personal de Howard C...	howard cardo...	1	32:46	tigoune	253125761737698687
None		2023-02-22 05:50:44 ...	317916687	Sala personal de Howard C...	howard cardo...	1	34:53	tigoune	252642170060680528
None		2023-02-17 10:14:46 ...	317916687	Sala personal de Howard C...	howard cardo...	1	04:22	tigoune	251688826729148274
Good		2023-02-17 10:06:16 ...	1987	Howard Cardona → 601743...	Howard Card...	2	00:10	Tigo	SSE150616730170223174...
Good		2023-02-17 10:06:06 ...	1987	Howard Cardona → 018000...	Howard Card...	2	00:06	Tigo	SSE150606082170223-19...
Good		2023-02-16 03:44:35 ...	+5760448092...	+576044809292 → Howard ...	+5760448092...	2	00:06	Tigo	BW2044357341602235457...
Good		2023-02-16 03:44:15 ...	1987	Howard Cardona → 601743...	Howard Card...	2	00:07	Tigo	SSE204414926160223184...
Poor		2023-02-16 03:43:50 ...	1987	Howard Cardona → 018000...	Howard Card...	2	00:08	Tigo	SSE204349851160223101...
Good		2023-02-16 03:43:30 ...	1987	Howard Cardona → 123	Howard Card...	2	00:04	Tigo	SSE204330485160223133...
Good		2023-02-16 03:43:23 ...	1987	Howard Cardona → +57601...	Howard Card...	2	00:04	Tigo	SSE204323352160223140...
Good		2023-02-16 03:43:01 ...	1987	Howard Cardona → 302329...	Howard Card...	2	00:13	Tigo	SSE204301390160223136...
Good		2023-02-16 01:46:21 ...	+5760448092...	+576044809292 → Howard ...	+5760448092...	2	00:07	Tigo	BW184621472160223-227...



**webex Control Hub** | Select Customer | Search

Meetings & Calls > Howard Cardona > +573022296084

### Hop Detail

Howard Cardona (1987 User) — Good —> Cloud —> +573022296084 (3022296084 Local Gateway) — Good —> Cloud —> +573022296084 (3022296084 Local Gateway) — Poor —> Cloud —> +573022296084 (3022296084 Local Gateway)

Howard Cardona	Metric	+573022296084
Webex App (Windows)	Endpoint	-
-	Hardware	-
Tigo	Location	-
-	MAC address	-
192.168.1.12	Local IP	-
181.135.185.228	Public IP	-
Medellin, CO	Geolocation	-
epm telecomunicaciones s.a. e.s.p.	ISP	-
Wi-Fi	Connection	-
PCMA	Audio Codec	-
@tigo.com.co	Email ID	-
SSE2043013901602231361169581@10.71.1...	Call ID	-

**Call Details**

- Calling Date: 02/16/2023
- Calling Time: 03:43 pm - 03:43 pm (13 seconds) (GMT -05:00) America/Bogota
- Session Type: Webex Call
- Participants: 2
- Caller Name: Howard Cardona
- Caller Number: 1987
- Audio: VoIP
- Video: No
- Path Optimization: No Optimization
- Calling Type: Mobile Call
- Call Ended by: +573022296084
- Dialed Digits: 3022296084

**Chart Legend**

- Signal Quality
- Good
- Poor
- Not Available

**Reportes:** En la sección de reportes, se cuenta con una serie de reportes predefinidos por cada tipo de servicio Reuniones, Mensajería, Llamadas, Dispositivos, los cuales se pueden generar por demanda o de forma periódica. Estos informes se pueden generar hasta por un periodo de 90 días de información histórica.

## Reportes de Llamadas

**webex Control Hub** | Select Customer | Search

Reports

Templates | Report list | Scheduled Jobs | Classic reports

Meetings

Messaging

Calling

Usage | Quality

Template name	Description	Start date(UTC)
Calling Engagement Report	One entry for every call made or received using Cisco Webex App, Webex Calling App or Clo...	11/29/2022
Calling Detailed Call History	Detailed Call Records for all calls made using Webex Calling.	11/29/2022
Call Queue Stats	Report for Call Queue	11/30/2022
Call Queue Agent Stats	Report for Call Queue	11/30/2022
Auto-Attendant Stats Summary	Report for Auto Attendant	11/30/2022
Auto-Attendant Business Hours Key Details	Report for Auto-Attendant Business Hours Key Details	11/30/2022
Auto-Attendant After Hours Key Details	Report for Auto-Attendant After Hours Key Details	11/30/2022



## Reportes Periódicos

Name	Site / Org	Frequency	Generates on	Last generated	Status	Notification	Actions
Call Queue Agent Stats	DEMO WEBEX CALLING TIGO	Weekly	Monday	-	Active	Subscribed	...
Calling Detailed Call History	DEMO WEBEX CALLING TIGO	Monthly	First day	-	Active	Subscribed	...
Auto-Attendant Stats Summary	DEMO WEBEX CALLING TIGO	Monthly	First day	-	Active	Subscribed	...

Todos los reportes y analíticas se consultan a través del portal de autogestión del servicio Cisco Webex Control Hub el cual se accede mediante la cuenta de administración (email) aprovisionado en la plataforma en el momento de la instalación.

## 4.10 PORTAL AUTO CUIDADO CLIENTE FINAL

El portal de Auto Cuidado le permite al usuario final interactuar con las funcionalidades telefónicas de su cuenta de usuario. En este portal puede activar o desactivar facilidades como (No molestar, Desvió de Llamadas, Repique simultaneo, Llamadas en espera, listas blancas, listas negras), consultar histórico de llamadas, Buzón de Voz, Directorio Telefónico, Contactos.

**Cisco Webex Calling** Jhon Fredy Ballesteros Fernandez Extension: 1010

**Incoming Calls** Schedules Additional Features

- Anonymous Call Rejection**  Reject incoming calls with blocked caller IDs.
- Call Forwarding**  Forward incoming calls to personal phone number.
- Call Notify**  Receive an email when an incoming call meets criteria such as phone number or date/time.
- Simultaneous Ring**  Ring personal numbers at the same time for incoming calls.

Cancel Save

El portal de autocuidado puede ser accedido con las credenciales del usuario final en la URL <https://settings.webex.com/login>



## 4.11 CONDICIONES TÉCNICAS ESPECÍFICAS

Las siguientes son las condiciones específicas de la solución presentada:

- El cliente es responsable de suministrar cuenta de correo electrónico para el usuario administrador del portal y para cada uno de los usuarios que requieran ser dados de alta en el servicio
- Los equipos que posea el usuario contarán con hardware y sistemas operativos actualizados y compatibles de acuerdo con las especificaciones de Cisco Webex durante la duración del contrato, las cuales se encuentran en el siguiente link <https://help.webex.com/en-us/article/fz1e4b/System-requirements-for-Webex-services>
- Tigo es responsable del diseño y arquitectura de bajo y alto nivel (LLD y HLD) de la solución de Cisco Webex Calling integrada con los servicios de telefonía de Tigo.
- El cliente debe suministrar el plan de numeración existente y diligenciarlo en el formato establecido por Tigo con acompañamiento del equipo de Tigo.
- Tigo es responsable de la configuración de los planes de numeración y enrutamiento de llamadas, así como de la configuración de las extensiones de usuario en el portal Webex Control Hub.
- Tigo habilitará las configuraciones requeridas para la realización de llamadas a la red pública de telefonía que se requieran para este fin acorde con lo contratado por el cliente y previamente definido en el formato de levantamiento de información de Tigo.

Nota: Todos los prerequisites anteriormente listados y que están bajo responsabilidad del cliente, son obligatorios para cumplir con los tiempos y condiciones de instalación, soporte y postventas descritos en la oferta.

## 4.12 PUERTOS Y SERVICIOS DE COMUNICACIÓN REQUERIDOS

A continuación, se describe la lista de puertos y protocolos usados para conectar dispositivos telefónicos y/o la aplicación de Webex al servicio de Webex Calling.

Dispositivo	Protocolo	Aplicación	Puerto Origen	Puerto Destino
Desktop / Móvil - Aplicación Wbx	TCP	HTTP/HTTPS	Efímero	80, 443, 8443
	TLS	SIP TLS	Efímero	8934
	UDP	sRTP/sRTCP	Efímero	19560-65535
	TCP	Outlook Add-in	Efímero	5000-5010
	TCP/UDP	DNS	Efímero	53
	UDP	NTP	123	123
Teléfono	TLS	SIP TLS	5060-5060	8934
	UDP	sRTP/sRTCP	19560-19660	19560-65535
	TCP	Cscan	Efímero	80, 443, 8443, 19560-19570
	UDP	NTP	514494	123
	TCP	Device Config	Efímero	80, 443
	TP/UDP	DNS	Efímero	53

Para mayor detalle sobre los puertos, protocolos y listado de direcciones IP que se deben habilitar en la red corporativo consultar el siguiente link <https://help.webex.com/en-us/article/b2exve/Port-Reference-Information-for-Cisco-Webex-Calling>



#### 4.13 SUPUESTOS Y RESTRICCIONES

- ✓ No se contemplan cambios o ajustes sobre equipos actuales propiedad del cliente para el correcto funcionamiento de los servicios.
- ✓ Esta oferta únicamente contempla minutos de telefonía todo destino nacional en Colombia, no está contemplado la opción de minutos internacionales
- ✓ Para minutos internacionales se debe contemplar un producto adicional de troncal sip que permita la tasación de minutos independiente.
- ✓ La numeración que se asignara en la presente oferta será usando los prefijos 60x – xxxxxxx según la región que el cliente elija.
- ✓ Se podrá mantener la numeración que se tiene actualmente con el Conmutador Virtual, sin embargo, es importante validar los números que se desean conservar para optimizar el proceso de implementación.
- ✓ No se contemplan actualizaciones de software en dispositivos del cliente.
- ✓ Las fallas del servicio atribuibles a Cisco no representarán una indisponibilidad para Tigo.
- ✓ Se asume que el cliente tendrá configurado sus equipos de red o dispositivos de usuario final para acceder al servicio en nube de Cisco Webex <https://help.webex.com/en-us/article/b2exve/Port-Reference-Information-for-Cisco-Webex-Calling>
- ✓ 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, racks, 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 del cliente, en cumplimiento de las especificaciones del fabricante necesarias para la instalación y funcionamiento adecuado de la solución ofrecida.
- ✓ Se asume que se cuenta con los permisos de acceso a cada una de las sedes o Data Centers para la instalación y/o mantenimiento de los equipos de comunicaciones e ingreso de fibra en los casos que aplique, en caso de no tener previamente los permisos a las sedes en las cuales se instalará el servicio, EL CLIENTE gestionará dichos permisos.
- ✓ EL CLIENTE es responsable de asegurar el suministro de los Facilities continuos (espacio, aire y energía) para los equipos en cada sede.
- ✓ Se asume que el cliente tendrá configurado sus equipos intermedios (switches) 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 el suministro de racks, cableados, accesorios, hardware/software diferente 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 el alcance 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 demás componentes suministrados por Tigo para proveer su solución de Comunicaciones Unificadas y que cualquier otra falla en el servicio derivada de la red LAN, o condiciones físicas o eléctricas en cada sitio será soportada y asumida por el cliente.
- ✓ En caso de requerirse trabajos adicionales, esto se cotizará por separado, en común acuerdo con Tigo.

## 5 IMPLEMENTACIÓN DE LA SOLUCIÓN

### 5.1 METODOLOGÍA DE APROVISIONAMIENTO

Para llevar a cabo la entrega de la solución contratada por el Cliente, Tigo Business asignará la solicitud, al equipo de Order Manager responsable de canalizar las necesidades y comunicaciones del Cliente e integrar tecnológicamente los proveedores y aliados requeridos.

El Order Manager utiliza metodologías y herramientas de gestión de proyectos para realizar el aprovisionamiento de la solución. Lidera el inicio y planificación del aprovisionamiento, revisa el alcance de la solución, identifica los riesgos y controles de la solicitud, solicita los recursos requeridos internos o externos y construye el plan de trabajo asociado.

Durante la implementación del servicio, realiza reuniones de inicio y empalme con el Cliente, áreas internas, proveedores y aliados involucrados según necesidad; realiza monitoreo y seguimiento al plan de trabajo, incluyendo todos los servicios que componen la solución tales como: los Servicios AWS, Servicios Profesionales, Servicios Administrados y otros. Realiza también el monitoreo y seguimiento de los riesgos del proyecto, interventoría y recepción. De ser requeridos y previa coordinación para ello podrá realizar pruebas de servicios y equipos que podrían componer la solución.

Para el cierre del proyecto y entrega formal al Cliente, en caso de ser necesario, se actualiza la topología de la solución. Así mismo se realiza la entrega del servicio implementado para la operación y soporte.



#### 5.1.1 Tiempo de despliegue de los servicios

La duración del aprovisionamiento la siguiente:

- Para los servicios no aplica tiempo de aprovisionamiento, dado a que ya están operativos, si el cliente no renueva a tiempo, el tiempo de implementación es de 60 días calendario.

La factibilidad de la conectividad está dada por cobertura, por lo tanto, 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 como CODENSA, Cens, ESSA, Emcali, entre otras.
- Se cuenta con equipos en stock para realizar la implementación de Comunicaciones Unificadas, 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.
- El tiempo de aprovisionamiento puede variar dependiendo de la cantidad de servicios contratados, el servicio de conectividad o de los acuerdos realizados con el Cliente. Si el plazo varía, las partes deben acordar y dejar establecido el cambio a través de una modificación en la orden de servicio.
- Las actividades dentro de cada fase pueden cambiar, en la reunión inicial con el equipo de implementación y el Order Manager, se definirá el calendario final de ejecución para la implementación de la solución.
- En todos los casos, se realizará el mejor esfuerzo para tener implementado el servicio en el menor tiempo posible.
- No se consideran los tiempos imputables a las adecuaciones internas o aspectos técnicos o de servicio bajo la responsabilidad del Cliente en sus sedes o Data Center.

## Supuestos

- Se asume que los equipos cotizados cumplen con la capacidad requerida por el cliente COLEGIO MAYOR DE ANTIOQUIA.
- No incluye actividades de reparación, afinación ni configuración de los sistemas no especificados en el alcance del proyecto.
- Toda la instalación y configuración se realiza en horarios previamente definidos en común acuerdo entre el Cliente y UNE.
- En caso de presentarse tiempos muertos por factores externos a UNE, serán cobrados previo acuerdo con el cliente.
- Los canales de comunicaciones los deberá proveer la Gerencia del proyecto del Cliente.
- Contar con espacio suficiente en el rack para la instalación de los equipos.
- El Cliente debe tener puertos disponibles en los switches y routers que interconectan las redes del CORE.
- El Cliente debe tener configurados los enrutamientos necesarios en los diferentes elementos de red que necesitan interactuar con CORE.
- El Cliente debe tener creadas en los switches de borde, las diferentes Vlans de las cuales, los segmentos del CORE, harían parte de la solución.
- Se asume que se cumplen las especificaciones físicas adecuadas para instalar los equipos.
- El cliente deberá entregar la topología de la red con su direccionamiento IP, los protocolos y servicios/aplicaciones, con el fin de hacer definiciones para el proceso de implementación. Las topologías mostradas en esta oferta son referenciales.
- Proporcionar un sistema de alimentación, con voltaje regulado y polo a tierra para la conexión.
- No se incluye configuración de equipos no especificados en esta oferta.



- En caso de requerirse trabajos adicionales, esto se cotizará por separado, en común acuerdo entre UNE y el Cliente.
- El alistamiento y entrega de los recursos que resulten de la etapa de diseño, son responsabilidad del Cliente. UNE no realizará ninguna tarea de alistamiento o aprovisionamiento de hardware y/o software diferente al que hace referencia en esta propuesta.
- Todas las adecuaciones o instalaciones de cableado, rack, energía, Internet, y demás necesarias para el funcionamiento en el centro de datos o el lugar asignado por el Cliente COLEGIO MAYOR DE ANTIOQUIA 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.
- UNE se encargará de escalar al fabricante las solicitudes de garantías que se puedan presentar.
- Esta oferta no incluye la modificación de la configuración de ninguno de los elementos previamente instalados por el cliente COLEGIO MAYOR DE ANTIOQUIA entre otros, y como ejemplo, mencionamos: de comunicaciones o de seguridad; o de aplicaciones desarrolladas o de red; o de sistemas operativos o cualquiera otro.
- El cliente COLEGIO MAYOR DE ANTIOQUIA entregará acceso a los recursos asignados a todas las áreas de trabajo que por definición del alcance sean requeridas, de acuerdo con un previo entendimiento entre las partes.
- El cliente COLEGIO MAYOR DE ANTIOQUIA 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.
- El cliente COLEGIO MAYOR DE ANTIOQUIA reconoce que el suministro oportuno de espacios de oficinas, instalaciones, equipos, asistencia, cooperación, información completa y exacta por parte de los directores, sus agentes y empleados es esencial para el desempeño de cualquiera de los servicios establecidos en esta propuesta.
- Se asume que la sede del cliente COLEGIO MAYOR DE ANTIOQUIA tiene condiciones físicas, ambientales y eléctricas bajo las cuales se garantiza el funcionamiento de los equipos de acceso.
- La implementación de soluciones en sedes distintas a las mencionadas anteriormente no se encuentra contemplada en el alcance de esta propuesta.
- Se asume que COLEGIO MAYOR DE ANTIOQUIA gestionará y garantizará las cross-conexiones y cables que sean necesarias para habilitar el servicio en los Datacenters y/o sedes.
- Se asume que el cliente COLEGIO MAYOR DE ANTIOQUIA tendrá configurado sus equipos intermedios (switch,router, etc ) para la recepción del Internet.
- Se asume que se cuentan con los permisos a cada una de sedes a nivel nacional para la instalación de los equipos de comunicaciones y de los servicios de canales de internet.
- No se incluye configuración de equipos no incluidos en esta oferta.
- No se incluye toda actividad no incluida en los alcances del servicio.
- En caso de requerirse trabajos adicionales, esto se cotizará por separado, en común acuerdo con UNE.
- No se incluye la configuración de interoperabilidad con otros servicios diferentes a los mencionados en este documento.
- Tener puertos disponibles en los switches de LAN de cada sede.



- El dimensionamiento de los recursos ofertados está sujeto a la información entregada por El Cliente, cualquier cambio adicional sobre el dimensionamiento de la solución está sujeto a viabilidad técnica y económica durante la fase de Implementación.
- Toda la instalación y configuración se realiza en horarios previamente definidos en común acuerdo entre el Cliente y UNE.
- Cualquier servicio o solicitud que no estén claramente especificados en este documento se encuentran por fuera del alcance.

#### 5.1.2 Entregables

Entregable	Descripción
Acta de entrega	Documento donde se realiza verificación y entrega de cantidad, calidad y operatividad de la solución de acuerdo con lo establecido en la oferta técnica. La entrega de este documento no condiciona el inicio de la facturación.
Delivery Kit	Documento con el inventario de los recursos implementados de acuerdo con lo establecido en la oferta técnica.

#### 5.1.3 Responsabilidades del Cliente

- Soportar los equipos que se instalarán en cada una de las sedes. En caso de que se presentan daños en los equipos por fallas asociadas al sistema eléctrico, el cliente deberá asumir todos los costos por reparación o cambio de éstos.
- Administrar de manera responsable los accesos que le sean concedidos por UNE a la infraestructura aprovisionada.

#### 5.1.4 Ofertas de Servicio

### AWS



Oferta%20de%20Se  
rvicio%20-%20Coleg



## 6 OFERTA ECONÓMICA

### 6.1 OFERTA RENOVACIÓN CIBERSEGURIDAD EN PREMISAS Y SMART WIFI

- Tarifas Sede Principal

Producto	Cantidad	Ancho de Banda	Tarifa Mensual Sin IVA	Tarifa Mensual Con IVA
Internet Dedicado Principal	1	500 Mbps	\$ 3.320.625	\$ 3.951.544
Internet Dedicado Principal	1	500 Mbps	\$ 888.273	\$ 1.057.045
Pool de IPs	3	No aplica	\$ 0	\$ 0
Servicio de Ciberseguridad en Premisas para 500 Mbps + FAZ	1	No aplica	\$ 5.148.247	\$ 6.126.414
<b>Tarifa Total Mensual</b>			<b>\$ 9.357.145</b>	<b>\$ 11.135.003</b>

#### Notas Importantes:

- ✓ Estos valores, hacen parte de una oferta integral, por lo tanto, si la oferta cambia, las tarifas pueden cambiar.
- ✓ El plazo solicitado para esta cotización es de 6 meses o hasta agotar los recursos, lo primero que ocurra.
- ✓ La propuesta está detallada en pesos colombianos (COP\$).
- ✓ El IVA a facturar será el vigente a la fecha de facturación de los servicios y equipos.
- ✓ No se incluyen costos de adecuaciones eléctricas, obras civiles, etc. Estos deberán ser asumidos por el cliente COLEGIO MAYOR DE ANTIOQUIA.
- ✓ Cualquier cambio que se requiera realizar a esta oferta deberá ser factibilizado nuevamente ya que puede afectar las tarifas contempladas.
- ✓ Todos los servicios se basan en equipos propiedad de TIGO BUSINESS, por lo que la responsabilidad del soporte físico, bodegaje, garantía y su obsolescencia tecnológica es de TIGO BUSINESS.
- ✓ No se incluye bolsa de horas adicionales, para configuraciones adicionales.
- ✓ Tarifas aplican para contratación global. Una vez firmado el contrato la totalidad de las cantidades definidas deberán ejecutarse.
- ✓ La oferta incluye Servicios Administrados Básicos que permite 1 cambio por extensión al mes.
- ✓ La oferta no incluye elementos ni equipos de red, es responsabilidad de COLEGIO MAYOR DE ANTIOQUIA suministrar los puntos de red necesarios para cada uno de los equipos telefónicos.
- ✓ Es responsabilidad del COLEGIO MAYOR DE ANTIOQUIA realizar los ajustes y configuraciones necesarios sobre los elementos de su red WAN y LAN para el debido funcionamiento de la solución.
- ✓ La oferta no incluye elementos de infraestructura de red eléctrica ni cableado estructurado, es responsabilidad de COLEGIO MAYOR DE ANTIOQUIA suministrar los puntos de red y de energía para cada uno de los equipos telefónicos.



- ✓ La oferta no incluye diademas para los softphone, es responsabilidad de COLEGIO MAYOR DE ANTIOQUIA suministrar los elementos necesarios para que los usuarios puedan hacer uso de los softphone aprovisionados.
- ✓ La oferta Webex Calling por el momento únicamente se entrega con Troncal SIP Fija para llamadas fijas.
- ✓ Las tarifas contempladas se basan en el alcance, supuestos y restricción que se establecen en el anexo técnico.
- ✓ Cualquier modificación en el alcance de la oferta deberá ser evaluada técnica y económicamente por TIGO.
- ✓ No se incluye llamadas Internacionales ni celular, si estas son requeridas, el alcance y los valores de la oferta pueden cambiar.

- **Tarifas Sede Colegio San Juan Eudes**

Servicios Recurrentes						
Sede	Descripción	Cantidad	Tarifa	Tarifa	Tarifa	Tarifa Mensual
			Mensual	Mensual	Mensual	Total
			Unitaria	Unitaria	Total	Con IVA
			Sin IVA	Con IVA	Sin IVA	
<b>Colegio San Juan Eudes</b> Dirección: Calle 77E #79B-36	Seguridad en Premisas 1 sede (1 equipo FG-60F)	1	\$ 1.014.300	\$ 1.207.017	\$ 1.014.300	\$ 1.207.017
	Internet Dedicado 60 Mbps (GPON o F.O)	1	\$ 724.500	\$ 862.155	\$ 724.500	\$ 862.155
	Internet Empresarial Ultra Banda Ancha 120 Mbps (GPON o F.O)	1	\$ 447.180	\$ 532.144	\$ 447.180	\$ 532.144
	Smart Wifi (4 equipos Ruckus)	4	\$ 255.990	\$ 304.628	\$ 1.023.960	\$ 1.218.512
	<b>Total, Mensual</b>					<b>\$ 3.209.940</b>

- **Sede Institución Educativa Nuevo Horizonte 1**

Servicios Recurrentes						
Sede	Descripción	Cantidad	Tarifa	Tarifa Mensual	Tarifa	Tarifa Mensual
			Mensual	Unitaria	Mensual	Total
			Unitaria	Con IVA	Total	Con IVA
			Sin IVA		Sin IVA	
<b>Institución Educativa Nuevo Horizonte 1</b> <b>CARRERA 37 #109-24</b>	Seguridad en Premisas 1 sede (1 equipo FG-60F)	1	\$ 1.014.300	\$ 1.207.017	\$ 1.014.300	\$ 1.207.017
	Internet Dedicado 60 Mbps (GPON o F.O)	1	\$ 724.500	\$ 862.155	\$ 724.500	\$ 862.155
	Internet Empresarial Ultra Banda Ancha 120 Mbps (GPON o F.O)	1	\$ 447.180	\$ 532.144	\$ 447.180	\$ 532.144
	<b>Total, Mensual</b>					<b>\$ 2.185.980</b>



## 6.2 OFERTA RENOVACIÓN NUBE PÚBLICA AWS

### Facturación promedio de las cuentas Existentes y servicios nuevos

A continuación, se presentan los componentes de la Solución AWS de Tigo Business. Tener presente que los valores para algunos de los componentes son tarifas de referencia con **TRM \$ 4.250** basados en los criterios de diseño expuestos en la Descripción de la Solución AWS de Tigo Business, sin embargo, el valor a facturar mensualmente dependerá del consumo real del periodo anterior.

Servicio	Mensual	IVA (19%)	Tarifa Total
			Estimado x mes
Servicios AWS	\$ 16.468.030	\$ -	\$ 16.468.030
Servicios Administrados Tigo ( <b>Enterprise</b> )	\$ 2.470.205	\$ 469.339	\$ 2.939.544

El **VALOR MENSUAL TOTAL en COP** de la Solución Tigo Cloud AWS es un valor referencial, el cual puede variar en proporción de los consumos reales de los servicios.

- Plazo de ejecución inicial de los servicios: **6 meses o hasta agotar los recursos, lo primero que ocurra.**
- La tarifa de Servicios Administrados Tigo corresponde al **15%** del consumo mensual de los Servicios AWS. Esta tarifa del **15%** se mantendrá para las futuras adiciones.
- El Cliente se obliga a pagar el consumo de servicios en AWS, además de los servicios profesionales y administrados hasta el último día de actividad de acuerdo con lo establecido en el contrato suscrito con Tigo Business.
- En los casos que el Cliente posea permisos que le permitan realizar cambios en su infraestructura dentro de AWS, deberá asumir la responsabilidad total por las implicaciones que dichos cambios puedan generar, en términos de rendimiento y costos de servicios consumidos.
- Los cambios y requerimientos que el Cliente solicite a Tigo Business, una vez implementados se verán reflejados en resultados de consumo en AWS y en la facturación con Tigo Business.
- La facturación al Cliente se calculará con base en los consumos generados desde el momento en el que se aprovisionen los recursos, es decir, desde su creación hasta que se den de baja.
- Tigo Business proveerá al Cliente reportes de consumo dentro AWS, según el alcance de los servicios administrados contratados.
- El valor mensual de la Oferta Comercial **es de referencia**, debido a que incluye servicios Cloud AWS y algunos servicios complementarios, cuya facturación depende del consumo



real de los servicios, por lo tanto, el valor a facturar puede variar cada mes. De acuerdo con lo anterior, el valor mensual del Servicio Administrado Cloud también puede variar,

- Para clientes del Sector Gobierno se facturará a la TRM de \$ 4.250 especificada en este documento y acordada entre las partes para la Orden de Compra y/o Servicio o el respectivo contrato suscrito entre las partes.

No obstante, si la TRM promedio oficial del mes en que se consumieron los servicios tiene una variación igual o mayor al 5% respecto a la TRM acordada/ informada o respecto a la TRM con que se facturó el mes anterior, la TRM se ajustará proporcionalmente a dicha variación para facturar los servicios consumidos.

En los casos en que EL CLIENTE tenga permisos para realizar cambios sobre los Servicios Cloud AWS, el cliente es responsable por las implicaciones que estos cambios generen a nivel de desempeño y el precio de los recursos consumidos. Por lo tanto, podrá aumentar consumos en la medida que estos se encuentren dentro del límite presupuestal y en el caso del Sector Gobierno, siempre que se encuentre dentro del límite de su CDP. En caso de requerir consumos mayores el cliente debe primero hacer una adición presupuestal. En cualquier caso, la facturación corresponderá al consumo real de los servicios AWS asociados a la cuenta de EL CLIENTE. Los registros de los cambios efectuados por EL CLIENTE se entenderán incorporados a la orden de compra/servicio o el respectivo contrato suscrito entre las partes.

- Al adquirir Soluciones AWS Tigo Business, firmar la Orden de Compra y/o Servicio o suscribir un contrato entre las partes, el Cliente acepta los términos y condiciones de AWS y demás condiciones de AWS publicados en <https://aws.amazon.com/es/legal/> en documentos como “Contrato de AWS con el Cliente”, “Términos de servicio de AWS”, “Contratos de Nivel de Servicio de AWS”, entre otros.
- Al adquirir Soluciones AWS y firmar la Orden de Compra y/o Servicio o el contrato entre las partes, el Cliente autorizará a TIGO a abrir una cuenta AWS a nombre de EL Cliente empleando una dirección de email válida de este, en caso de no tener aún una cuenta en AWS. En todo caso es responsabilidad del Cliente la entrega correcta de la información de la cuenta, su habilitación, así como acceder a las condiciones de AWS publicados en documentos como “Contrato de AWS con el Cliente”, “Términos de servicio de AWS”, “Contratos de Nivel de Servicio de AWS”, entre otros.
- El cliente acepta que Tigo Business no tiene control directo sobre la infraestructura que soporta los servicios de AWS por tanto, Tigo Business no asume ninguna responsabilidad por los errores, interrupciones, pérdidas de datos o cualquier otro problema que pueda surgir del uso de los servicios de AWS.



### 6.3 OFERTA RENOVACIÓN UCaaS WEBEX CALLING

- Tarifas mensuales servicio Webex Calling

Concepto	Cantidad	Valor Unitario Mensual Antes de IVA	Valor Total Mensual Antes de IVA	IVA	Valor Total Mensual Después de IVA
Webex Calling Professional	100	\$ 28.038	\$ 2.803.800	0%	\$ 2.803.800
Webex Calling Workspace	56	\$ 16.823	\$ 942.082	0%	\$ 942.088
Troncal SIP Base 3 (3 accesos y 10 DID)	1	\$ 85.706	\$ 85.706	19%	\$ 101.990
Accesos Adicionales	27	\$ 22.604	\$ 610.308	19%	\$ 726.267
Plan Minutos Ilimitado Fijo	1	\$ 351.690	\$ 351.690	19%	\$ 418.511
Enrutamiento Telefónico HA Georedundante	30	\$ 15.437	\$ 463.100	19%	\$ 551.101
Servicios Administrados Básico	156	\$ 0	\$ 0	19%	\$ 0
Teléfonos Cisco 6851	140	\$ 18.052	\$ 2.527.298	19%	\$ 3.007.463
<b>Total, Mensual COP\$</b>			<b>\$ 7.783.982</b>	<b>N/A</b>	<b>\$ 8.551.220</b>

- Tarifas opcionales mensuales llamadas a celular

Concepto	Cantidad	Valor Unitario Mensual Antes de IVA	Valor Unitario Mensual Después de IVA
Llamadas a celulares Tigo	1	\$ 50,98	\$ 62,7
Llamadas a celulares otros operadores	1	\$ 77,4	\$ 92,1

- Tarifas opcionales mensuales llamadas a larga distancia

GRUPO	PAÍS / TERRITORIO	TARIFA UNITARIA	
		FIJO	
	NOMBRE	SIN IVA	CON IVA
1	Estados Unidos, Puerto Rico, Canadá, Alaska (USA), Hawaii (USA), U.S.Virgin Islands	\$ 336	\$ 400
2	Argentina, Bolivia, Brasil, Chile, Ecuador, El Salvador, España, Guatemala, Honduras, México, Nicaragua, Panamá, Perú, Paraguay,	\$ 336	\$ 400



	Reino Unido, Uruguay, Venezuela, France, Italy, Singapore, Thailand, Japan, China, India, Luxembourg, Costa Rica, Hong Kong		
3	Remaining Countries	\$ 1.597	\$ 1.900
4	Cuba, Bahía de Guantánamo	\$ 1.597	\$ 1.900
5	Diego García, Afghanistan, Iraq, Barbados, North Korea, Inmarsat, Inmarsat - Atlantic East, Inmarsat - Pacific Ocean, Inmarsat - Indian Ocean, Inmarsat - Atlantic West, Iridium Satelite 1, Iridium Satelite 2, Global Mobile, Satelite, International Services, International Networks 1, International Networks 2, International Premium, International Shared, Universal Personal Tel	\$ 1.597	\$ 1.900

### Notas Importantes:

- Tarifas aplican para contratación global. Una vez firmado el contrato la totalidad de las cantidades definidas deberán ejecutarse.
- Se harán entregas parciales de las extensiones conforme se entreguen los equipos telefónicos. Los equipos serán facturados según la tarifa individual a partir de la entrega operativa de los mismos.
- La oferta incluye Servicios Administrados **Básicos** que permite 1 cambio por extensión al mes.
- En la migración del servicio de Conmutador Virtual a Webex Calling se requiere cambio de teléfono por temas de compatibilidad en la plataforma.
- La oferta no incluye elementos ni equipos de red, es responsabilidad de COLEGIO MAYOR DE ANTIOQUIA suministrar los puntos de red necesarios para cada uno de los equipos telefónicos.
- Es responsabilidad del COLEGIO MAYOR DE ANTIOQUIA realizar los ajustes y configuraciones necesarios sobre los elementos de su red WAN y LAN para el debido funcionamiento de la solución.
- La oferta no incluye elementos de infraestructura de red eléctrica ni cableado estructurado, es responsabilidad de COLEGIO MAYOR DE ANTIOQUIA suministrar los puntos de red y de energía para cada uno de los equipos telefónicos.
- La oferta no incluye servicios de conectividad a internet en ninguna de las sedes, es responsabilidad de COLEGIO MAYOR DE ANTIOQUIA suministrar los servicios de Internet para la debida comunicación de los equipos telefónicos y los softphone con la plataforma centralizada de Cisco Webex Calling. Para efectos de dimensionamiento de capacidad, se debe estimar un BW de 100 Kbps por cada usuario.
- La oferta no incluye diademas para los softphone, es responsabilidad de COLEGIO MAYOR DE ANTIOQUIA suministrar los elementos necesarios para que los usuarios puedan hacer uso de los softphone aprovisionados.
- Contratación de 6 meses o hasta agotar los recursos, lo primero que ocurra.
- La oferta Webex Calling por el momento únicamente se entrega con Troncal SIP Fija para llamadas fijas.
- Las tarifas contempladas se basan en el alcance, supuestos y restricción que se establecen en el anexo técnico.
- Cualquier modificación en el alcance de la oferta deberá ser evaluada técnica y económicamente por TIGO.



- No se incluye llamadas Internacionales ni celular, si estas son requeridas, el alcance y los valores de la oferta pueden cambiar. Se relacionan tarifas individuales en las páginas 72 y 73 de este documento, por tanto, el Cliente debe tener en cuenta estos valores de consumo en el presupuesto.
- El concepto asociado a Horas Servicios Profesionales está orientado para apoyar al cliente en el proceso de migración.

#### 6.4 RESUMEN OFERTA DE SERVICIOS

Servicios	Meses	Valor Mensual Antes de IVA	Valor Mensual incluido IVA
Servicios de Ciberseguridad y Smart Wifi	1	\$ 14.753.065	\$ 17.556.147
Servicios Nube Pública AWS	1	\$ 18.938.235	\$ 19.407.574
Servicios Comunicaciones Unificadas	1	\$ 7.783.982	\$ 8.551.220
<b>Total, Servicios Tarifa Mensual</b>		<b>\$ 41.475.282</b>	<b>\$ 45.514.941</b>

#### 6.5 FORMA DE PAGO

Pagos mensuales

#### 6.6 VALIDEZ DE LA OFERTA

Esta propuesta estará vigente hasta el **31-05-2026**, 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.

#### 6.7 IMPUESTOS Y ESTAMPILLAS

Los tributos del orden nacional, departamental y municipal que se generen con ocasión de la formalización y ejecución de la relación jurídica surgida de la oferta aceptada, estarán a cargo de quien determine la ley vigente.

## 7 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.