RESOLUCIÓN Nro. 027
03-02-2025

# RESOLUCIÓN POR MEDIO DE LA CUAL SE JUSTIFICA UNA CONTRATACIÓN DIRECTA PARA LA CELEBRACIÓN DE UN CONTRATO INTERADMINISTRATIVO

El Director Jurídico de la Institución Universitaria Colegio Mayor de Antioquia en uso de sus facultades legales, y en especial de las otorgadas por la Resolución No. 428 del 20 de diciembre de 2022, expedida por el Rector de la Institución, mediante la cual se le delega la firma de los contratos derivados de la modalidad de contratación directa y los demás actos precontractuales, contractuales y postcontractuales asociados a las mismas, y,

## CONSIDERANDO

**1.** Que en cumplimiento de los principios de transparencia, economía y responsabilidad que rigen la contratación pública, la Ley 1150 de 2007, en su artículo 2, numeral 4, literal c), prevé dentro de las modalidades de selección, la contratación directa para la celebración de contratos interadministrativo " *siempre que las obligaciones derivadas del mismo tengan relación directa con el objeto de la entidad ejecutora (...)"*.

**2.** Que el artículo 73, capítulo VI, del Decreto 1510 de 2013 y el Decreto 1082 de 2015 artículo 2.2.1.2.1.4.1**,** determina que en los casos de contratación directa se debe expedir un acto administrativo de justificación, entre los que se encuentra, los contratos interadminstrativos.

**3.** Que la Institución Universitaria Colegio Mayor de Antioquia según la necesidad, consignó en el estudio previo, lo siguiente:

**a)** Que La Institución Universitaria Colegio Mayor de Antioquia en aras de responder de manera óptima a los procesos de Telecomunicaciones, requiere contratar la prestación de servicios de internet y ciberseguridad. Específicamente, se necesita un servicio de internet con dos canales de 500 Mbps cada uno (uno dedicado y otro de banda ancha), un alto nivel de seguridad con servicios administrados de ciberseguridad en las instalaciones utilizando equipos Fortigate 400F en HA (activo-pasivo), servicios en la nube pública de AWS donde actualmente se encuentran todos los servidores Web institucionales, y un sistema de comunicaciones unificadas administradas.

**b)** Que la contratación de estos servicios es esencial para el funcionamiento de la Institución, ya que garantizan la conectividad y seguridad necesarias para las operaciones académicas y administrativas. Además, la implementación de soluciones de ciberseguridad avanzadas es crucial para proteger la infraestructura tecnológica de la Institución contra amenazas cibernéticas.

**c)** Que Dado la gran cantidad de amenazas y la celeridad en que debemos responder a estas, se requiere que la ciberseguridad institucional sea con dispositivos de firewall de nueva generación (NGFW) desarrollados por Fortinet, diseñados para ofrecer una protección robusta y eficiente contra amenazas cibernéticas a través de capacidades avanzadas de inteligencia artificial y aprendizaje automático, proporcionando una protección de extremo a extremo, incluyendo seguridad web, filtrado de contenido y protección de dispositivos, lo que reduce la complejidad en redes híbridas, integra múltiples funciones de seguridad en una sola plataforma, mejorando la visibilidad y control sobre aplicaciones, usuarios y dispositivos antes de que se conviertan en amenazas, mediante la interfaz intuitiva del sistema operativo FortiOS que permite una gestión ágil y eficiente de la seguridad

**d)** Que la Institución requiere el servicio de servidores en la nube, continuando con los requerimientos del Ministerio de las Tecnologías de la Información y las Comunicaciones (MINTIC), entidad que solicita que todas las instituciones públicas migren a la nube. Teniendo en cuenta este requerimiento, desde el área de tecnología de la Institución elaboró los cálculos de necesidades de almacenamiento, memoria RAM, Core de procesadores y todos los recursos técnicos proyectados en máquinas virtuales necesarias para darle funcionamiento determinado a las diferentes plataformas de la Institución, como son los sistemas de ACCADEMIA de Naonsoft, DOCUMENTAL de Gmas, Moodle, PAGINA WEB Institucional, MIU VIRTUAL. Cada sistema requiere máquinas virtuales con especificaciones diferentes por los volúmenes de información que manejan y su grado de complejidad, los recursos en cada caso se ajustan a la necesidad, por lo que cada máquina tendrá un costo diferente. Adicionalmente, la Institución cuenta con algunos servicios en la nube plenamente configurados y funcionales en AWS, por lo que se requiere darle continuidad ya que se realizaron las migraciones y configuraciones respectivas y actualmente están siendo ejecutadas.

**e)** Que adicionalmente, se requiere de un servicio o cuenta adicional en AWS para alojar nuevas instancias desarrolladas durante el año 2024, específicamente para los sistemas Lacma y SICMA que se alojaron en los servidores en la nube de AWS. Así estas instancias alojarán las bases de datos, los softwares asociados y las copias de seguridad, lo que garantiza la continuidad y operatividad de estas plataformas en el año 2025. Estas nuevas instancias deben incluir los recursos técnicos necesarios para su correcto funcionamiento, asegurando la capacidad de almacenamiento y procesamiento requerida por los sistemas institucionales.

**f)** Que por otra parte, el servidor físico de telefonía, de propiedad de UNE Telecomunicaciones, ubicado en el datacenter de la Institución, ha cumplido su vida útil tras más de 10 años de servicio y actualmente no cuenta con soporte debido a su obsolescencia. Este servidor incluye la consola de control e informes, y además opera la troncal que conecta más de 140 extensiones de la red interna de telefonía institucional, la cual también depende del mismo proveedor. Ante esta situación, es necesario contratar un servicio avanzado de comunicación empresarial en la nube

para garantizar la continuidad de las operaciones.

**g)** Que el servicio de comunicaciones unificadas ha permitido aumentar la capacidad del sistema PBX, integrando dispositivos móviles, computadoras y tabletas, además de facilitar llamadas grupales, compartir archivos e imágenes, y mejorar el control y la seguridad de las llamadas mediante la generación de informes detallados. Este sistema también ofrece grabación de llamadas y control del consumo de llamadas a celulares y de larga distancia desde una consola administrativa, asegurando que no existan gastos no planificados. Asimismo, este servicio elimina la dependencia del servidor físico, ya que las operaciones de telefonía ahora se alojan en la nube de Azure de Microsoft, proporcionada por el mismo proveedor, lo que garantiza mayor estabilidad, seguridad y eficiencia operativa, por lo cual se hace necesario asegurar la continuidad de este servicio.

**h)** Que para la ejecución del presente contrato, se requiere de una entidad pública que preste este tipo de servicios, teniendo en cuenta lo dispuesto en el artículo 2°, numeral 4°, literal c) de la Ley 1150 de 2007, que dispone: “La modalidad de selección de contratación directa, solamente procederá en los siguientes casos: […] c) Contratos interadministrativos, siempre que las obligaciones derivadas del mismo tengan relación directa con el objeto de la entidad ejecutora señalado en la ley o en sus reglamentos”.

**I)** Que la sociedad UNE EPM TELECOMUNICACIONES S.A. tiene dentro de su objeto social la prestación de servicios de telecomunicaciones, tecnologías de la información y las comunicaciones, servicios de información y las actividades complementarias relacionadas y / o conexas con ellos, por esta razón, cumple con los requerimientos normativos para suscribir el contrato interadministrativo para la prestación de los servicios objeto del presente estudio previo y la norma que regula este tipo de contratos.

**4.**Que de acuerdo a lo anterior la Institución Universitaria requiere la ejecución de un contrato cuyo objeto y obligaciones específicas se describen a continuación:

**OBJETO:** El contratista, de manera independiente, por su propia cuenta y riesgo se obliga con la Institución Universitaria Colegio Mayor de Antioquia a prestar los servicios de Tecnologías de la Información y/o Comunicaciones que se detallan en las especificaciones del objeto.

**Especificaciones del Objeto**

Para la ejecución del objeto contractual, el proveedor prestará los siguientes servicios y actividades:

1. INTERNET DEDICADO Y CIBERSEGURIDAD CLOUD:

Requerimos por parte del proveedor nos suministre 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, para aumentar la experiencia de los usuarios.

| 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<br>* 1 Internet Banda Ancha de 500 Mbps | 3 pool de direcciones IP Públicas. |

- Disponer de direcciones de IP fijas que lo identificarán en el mundo de Internet para aplicaciones como cámaras IP, servidores propios de archivos y de correo, equipos de videoconferencia, telefonía IP, entre otros.
- Alta disponibilidad, gracias a que contamos con tecnología de punta con red de acceso en fibra, soportado de la mano de un recurso humano capacitado, para ofrecer un servicio de excelente calidad y desempeño.
- Mantener una conexión efectiva y confiable en Internet de forma simétrica y sin reúso, para realizar negociaciones en línea y transacciones con el mundo.
- Ejecutivos altamente capacitados en las diferentes ciudades para brindarle asesoría permanente y personalizada
- Integración con todo el portafolio de servicios y complemento de la conectividad de su empresa, a través de diferentes medios y tecnologías a escala nacional: Voz, Conectividad Nacional, Data Center, entre otros.
- Con (6) nodos de Internet que se encuentran ubicados en sitios geográficamente diferentes con salida internacional hacia los cinco (5) cables submarinos (Arcos, Maya, Emergía, GlobeNet y CFX) y diferentes proveedores de contenido en Estados Unidos (USA), que nos permite manejar de una manera distribuida las conexiones con nuestros usuarios y proveedores, brindando una mayor disponibilidad y confiabilidad a sus servicios.
- Red de transmisión nacional e internacional en fibra óptica, totalmente respaldada y con rutas internacionales a través de los cables submarinos más importantes.

2. CIBERSEGURIDAD ON PREMISES:

El servicio de Ciber Seguridad en Premisas TIGO (Cyber Security On Premise) debe proveer protección perimetral a la información y recursos informáticos de la institución que debe estar alojada en sus premisas, empleando para ello plataformas tecnológicas de Ciber Seguridad ubicadas en una o más sedes la IU 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 que nos entreguen debe fundamentarse 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 Banda Ancha o 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 adulto, etc).
- Los Servicios de Ciber Seguridad en Premisas están basados en tecnología Fortinet, se instalará un (2) equipos Fortigate con licenciamiento UTP.

Componentes del servicio de Ciberseguridad On premises
Los servicios de Ciber Seguridad en Premisas se configuran según sus necesidades con una o varias de las siguientes funcionalidades de seguridad:

Firewall: este servicio provee un primer nivel de seguridad que permite filtrar el tráfico de entrada y salida a la red de acuerdo con una lista de reglas definida.

El Firewall es un servicio básico que suele complementarse con otros servicios de seguridad para

ayudar a prevenir eventos que impacten la confidencialidad, integridad y disponibilidad de la información y servicios de la compañía.

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

- 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.

VPN: las Redes Privadas Virtuales (VPN, por sus siglas en inglés) evita que terceros no autorizados puedan interceptar la información que está viajando de entre dos nodos de la red a través de Internet. El servicio VPN permite ingresar de manera segura a redes privadas y/o servicios del cliente hospedados en los Data Center Tigo Business.

Las VPN ayudan a mantener la confidencialidad de la información que viaja entre diferentes puntos de la red.

VPN Site o Site:

- Protege la información que viaja entre dos sedes remotas conectadas a través de 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 manteniendo la información confidencial.
- La VPN Site to Site se configura entre el equipo de Ciber Seguridad en Premisas instalado por Tigo Business 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:
- 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 encriptación 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.

1. Antivirus Gateway (Malware Protection): Proporciona una protección de red contra descargas de archivos maliciosos (malware). Ejemplo de este tipo de ataques son Wannacry o Petya.

Este servicio proporciona una primera protección frente a ataques externos que pueden poner en riesgo la integridad o disponibilidad de la información y servicios críticos del negocio.

- 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 al ancho de banda del tráfico de la conexión a Internet contratada por La IU 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: Ofrece visibilidad del uso de aplicaciones en tiempo real. Esta protección es usada para controlar aplicaciones maliciosas, riesgosas y no deseadas en la red. A través de este servicio se puede tener control sobre funcionalidades específicas de ciertas aplicaciones, por ejemplo, permitir Facebook, pero bloqueando el tráfico de chat o video de esta aplicación. Esta funcionalidad es un complemento que disminuye el riesgo de ataques que afecten la confidencialidad, integridad o disponibilidad de la información.

- Se soporta en una Base de Datos firmas (aplicaciones) que son actualizadas periódicamente por el fabricante
- Este servicio es una funcionalidad adicional al componente de Firewall.
- El servicio es dimensionado de acuerdo con el número de perfiles de protección que corresponden al tipo de aplicaciones a proteger.

IDS/IPS: Proporciona protección ante amenazas a nivel de red empleando una Base de Datos de firmas que periódicamente son actualizadas por el fabricante de acuerdo con las nuevas amenazas. El servicio IDS/IPS previene ataques que pongan en riesgo principalmente la integridad y disponibilidad de información y servicios críticos de la Compañía.

- Esta protección se aplica para el tráfico entrante, es decir tráfico de publicación.
- El servicio es dimensionado de acuerdo con el número de perfiles de protección que corresponden al tipo de publicación a proteger. Para cada perfil se debe especificar cuáles son los Sistemas Operativos y Aplicaciones a proteger.
- PCI-compliance.

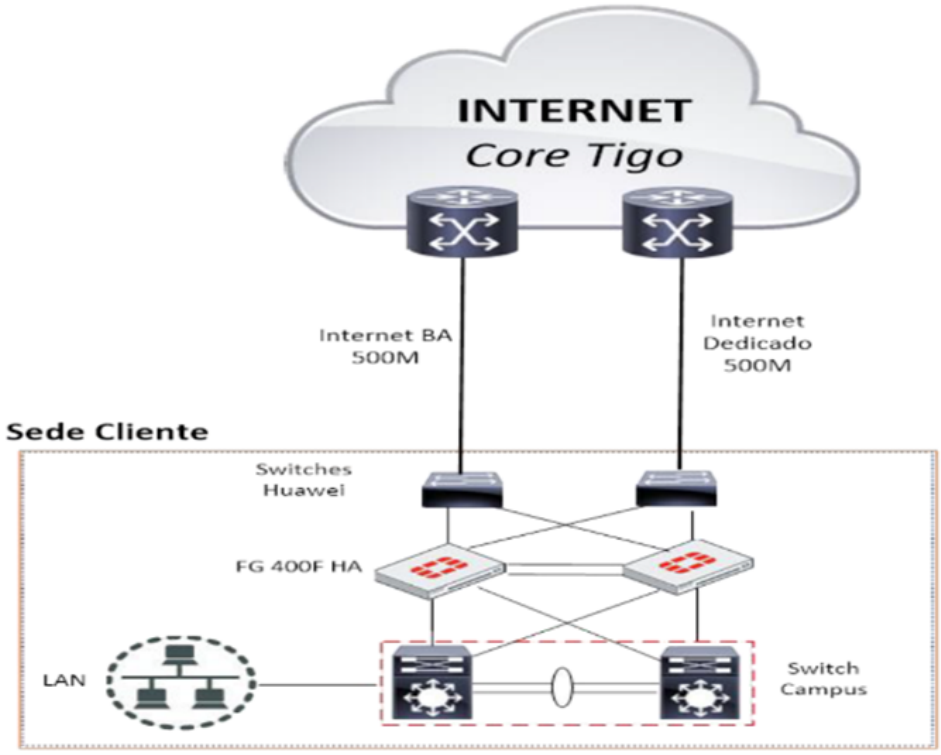
WCF (Web Content Filtering): El filtrado de contenido es un método que permite controlar la información que un usuario de Internet puede ver.

A través de este servicio el proveedor puede lograr que la navegación a Internet sea más productiva y segura para sus colaboradores, evitando el acceso a páginas de contenidos no deseados como Pornografía, Drogas, Juegos, Entretenimiento, Racismo, entre otros.

- 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 número de perfiles de protección que corresponden a las categorías de sitios de web a restringir.
- Full UTM (Unified Threat ManagementIncluye): los servicios de Firewall, VPN Client to Site, VPN Site to Site, WCF, IDS/IPS, Application Control, Antivirus Gateway.

La topología que el proveedor debe suministrar será la siguiente:

Topología Lógica de la Solución




El equipo de Seguridad para la solución en el Datacenter Principal debe ser con las siguientes características:

Para la solución se Instalará 2 UTM Fortigate 400F en el DC de la sede principal donde se encuentran los servicios de Internet.

Dimensionamiento del Equipo:

| Ref de Equipo | Cantidad | Licenciamiento | Sede |
|---|---|---|---|
| FG-400F | 2 | UTP | Principal |

FortiGate 400F

| IPS | NGFW | Threat Protection | Interfaces |
|---|---|---|---|
| 12 Gbps | 10 Gbps | 9 Gbps | Multiple GE RJ45, 10GE SFP+ Slots, GE SFP Slots |

El rendimiento y escalabilidad está limitada al hardware y licenciamiento del equipo según la hoja de datos del fabricante

Características de Seguridad disponibles

Se presentan los features de seguridad disponibles en la ciberseguridad para la sede ppal:

- 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)

**Consideraciones Técnicas Ciberseguridad:**

- Los equipos Fortigate será la capa de seguridad perimetral de la sede principal
- La institucion debe disponer de espacio en Rack para los equipos
- Se definirá en conjunto con La IU el LLD para esta solución
- La insititucion debe asegurar las condiciones eléctricas para el buen funcionamiento de los equipos
- En caso de requerirse, es responsabilidad de la institucion configurar los diferentes endpoint o servidores de la organización
- La Administración y soporte de la solución de ciberseguridad estará a cargo de la institucion, opcionalmente si La IU requiere la administración de Tigo se puede continuar con los servicios

administrados de ciberseguridad.
- En los equipos Fortigate se instalarán los servicios de internet dedicado y BA de 500M
- Se continua con la línea base de configuración del servicio actual de ciberseguridad Cloud
- Se realizará la migración de las configuraciones de seguridad que se tienen en la VDOM en DC Tigo hacia los equipos Fortigate en premisas
- Debido a que se instalaran 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
- La institución 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.

**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, La IU 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 de la IU.

La IU 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 La IU 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: La IU debe de firmar la carta de aceptación de que la administración es de el por tanto el soporte es su responsabilidad.

**La institución se hará cargo adicionalmente de:**

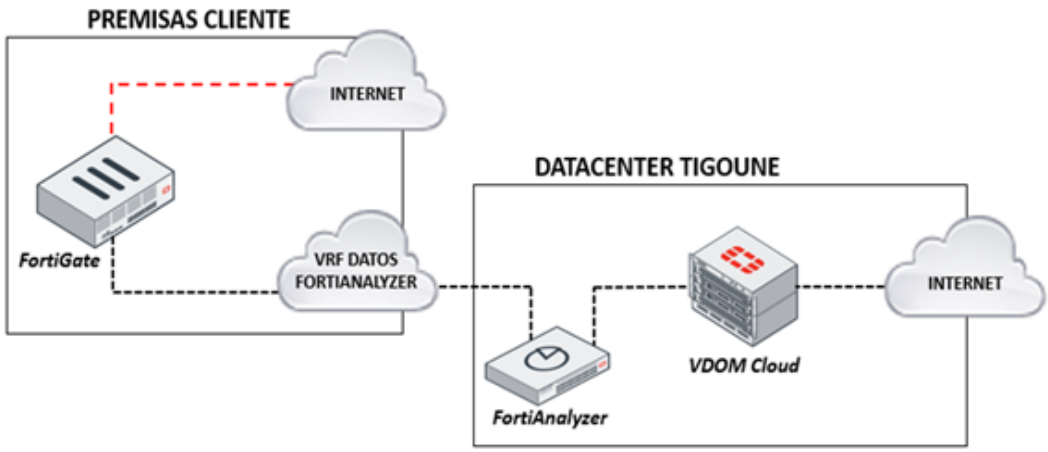
- Caídas o indisponibilidades del servicio, derivados de las configuraciones modificaciones a las que la IU tenga acceso.
- Impacto en los niveles de servicio, derivados de las configuraciones o modificaciones a las que la IU tenga acceso.
- Modificar parámetros sensibles de auditorías.
- Costos adicionales, derivados de servicios profesionales para la normalización del servicio; para resolver los incidentes ocasionados por configuraciones en las que la IU 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 de la IU a través de VPN (Virtual Private Network) Client to Site.
- Cualquier riesgo, exposición o vulnerabilidad que se derive de una configuración desde el perfil de la IU, queda bajo responsabilidad de este.
- La IU 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.
- 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 de la IU 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.

- El servicio contratado debe tener 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 como son:

- Reportes de navegación, reporte de Firewall, Reporte IPs, Faz, y que permita ajustar los informes según las necesidades y en los tiempos programados.

La topología del servicio debe ser con la siguiente arquitectura:




Debe permitir el almacenamiento de LOGs hasta 220GB y superado este tope se reescriba.

El servicio ofrecido debe tener los siguientes alcances:

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.

Los proveedores no serán responsables de:

1. Cuando las interrupciones, caídas, problemas o deficiencias en los servicios o afectación de indicadores tengan origen en la infraestructura física y tecnológica de la IU
2. En los eventos de errores, decisiones, cambios en procesos y procedimientos por parte de la IU que no hayan sido oportunamente informados al SOC.
3. En aquellos casos en los cuales los sistemas, plataformas y aplicativos de la IU 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 el proveedor.
4. Por fuerza mayor o caso fortuito.
5. En caso de presentarse suspensión o afectación del servicio por cualquiera de los eventos señalados en los numerales 1 ,2 y 3 la IU asumirá los costos en los que incurrió el proveedor, por la no prestación del servicio, durante el período de tiempo que dure la suspensión o afectación del mismo.

La institución será responsable de:

- LA IU deberá realizar copias de seguridad de su información en el medio que considere pertinente.
- LA IU 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.
- La IU 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 la IU 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 a la IU, 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 a la IU o a terceros; (d) por fraude cometido por La IU 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 a la IU o a terceros; (f) en caso de ataques informáticos a los PBX por causas imputables a la IU. En caso de que en la Orden de Compra y/o Servicio se incluya la entrega a la IU de cuentas administradoras de cualquier servicio, LA IU exime a TIGO BUSSINESS de cualquier evento de indisponibilidad, seguridad y confidencialidad que pueda ocurrir. Adicionalmente, en los casos en que LA IU solicite deshabilitar y/o desinstalar las herramientas de Antivirus implementadas por TIGO BUSSINESS o por un tercero para proteger los servicios, la IU 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 perdida 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 de la IU en un momento determinado, ya sea por causas técnicas, tareas de mantenimiento del sistema no notificadas al SOC, falla eléctrica en las instalaciones de la IU y todas aquellas que estén bajo su control y gestión.

Servicios de nube publica AWS (Amazon Web Services)

La institución requiere una solución de en la nube escalable, flexible y segura, que le ayude a impulsar la transformación digital de la IU, donde el proveedor cubra 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 el fin de tener unos servicios administrados y profesionales para:

- 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
- Optimización de costos
- Escalabilidad y flexibilidad
- Innovación y actualización tecnológica
- Cumplimiento de normas de calidad

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 | Item | Enterprise |
|---|---|---|
| **Administración y soporte del sistema operativo** | **Administración de Sistema Operativo** | Tigo une solo realiza cambios para los fines y situaciones específicos que se describen a continuación:· Se realizan cambios solo a nivel de infraestructura, utilizando la consola, CLI o las APIs· Nunca se realizan cambios en la aplicación del cliente o en aplicaciones de terceros.· A través de Servicios Administrados, Tigo despliega o actualiza recursos únicamente en los siguientes escenarios:* Implementación y actualización de herramientas y recursos requeridos para la operación del servicio administrado de Tigo Business.* Implementación como parte de monitoreo, respuesta a eventos y |

| | | |
|---|---|---|
| | | alarmas de la infraestructura.* Para remediar los problemas de seguridad según las mejores prácticas de seguridad.* Durante la remediación y restauración como parte de la respuesta a un incidente.* Solicitudes de clientes con características tales como:ü Administración de alarmasü Etiquetas de recursosü Líneas base de actualizaciones de seguridad y ventanas de mantenimientoü Planificador de ejecución de recursosü Planes de respaldoü 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) 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. Las siguientes son las actividades contempladas en la administración del sistema operativo:* Restauración de instancia EC2 ante fallas siempre que se cuente con un esquema de backup (AWS Backup)* Acompañamiento en Creación de usuarios en Sistema Operativo* Acompañamiento en asignación de permisos a usuarios de Sistema Operativo* Cambio de clave de usuarios* Habilitar/Deshabilitar de usuario de Sistema Operativo* |

| | | |
|---|---|---|
| | | Creación de carpeta con permisos específicos solicitados por el cliente* Revisión de permisos sobre carpetas del Sistema Operativo* Análisis de consumo de recursos del Sistema Operativo* Revisión y cierre de sesiones abiertas en el Sistema Operativo* Instalación y configuración del agente de CloudWatch y AWS Systems ManagerCreación de discos y/o volúmenes para sistema operativo. Configuración del Sistema Operativo soportadas: SA TIGO soporta las siguientes configuraciones:* Arquitectura del sistema operativo (x86-64 o ARM64) cualquiera sistema operativo soportado tanto por SSM (Systems Manager) como por CloudWatch.* Sistemas operativos compatibles:o Amazon Linux 2o CentOS 7.xo Oracle Linux 7: versiones menores 7.5 y superiores. Oracle Linux 8: versiones menores 8.3.o Red Hat Enterprise Linux (RHEL) 8.x, 7.xo SUSE Linux Enterprise Server 15 SP3, SP4o Ubuntu Linux 18.04 and 20.04o Microsoft Windows Server 2022, 2019, 2016, 2012 R2, 2012 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. |
| | Gestión de actualizaciones de seguridad - Periodicidad | Semestral |
| **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 2.4.2 |
| **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 |
| **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 |

**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** |
| 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 **configuración** 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** |

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.

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.

**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): |
| 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. |

**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.

SERVICIOS PROFESIONALES

Los Servicios Profesionales de Tigo Business representan un nivel especializado que ofrece a sus

clientes soluciones en el ámbito de las tecnologías de la información, incluyendo Cloud, Data Center, Seguridad y Networking, entre otros. Estos servicios están diseñados para llevar a cabo tareas específicas dentro de un periodo corto y definido, siendo esenciales para el diseño, migración o implementación de servicios en la nube. Mediante los Servicios Profesionales Cloud de Tigo Business, las empresas pueden gestionar la implementación de soluciones en la nube, abarcando desde la planificación y el diseño hasta la ejecución final. La cantidad de horas requeridas, tanto hábiles como no hábiles, para cada proyecto varía en función de los Servicios Cloud incluidos en la solución y su nivel de 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 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

Detalle técnico de servicios profesionales

| Servicio | Alcance | Actividad |
|---|---|---|
| **RDS** | Despliegue de un servicio de PaaS de acuerdo con los requerimientos del cliente:<br>o Amazon Aurora con compatibilidad con MySQL,<br>o Amazon Aurora con compatibilidad con PostgreSQL,<br>o MySQL, MariaDB,<br>o PostgreSQL,<br>o Oracle y<br>o SQL Server, e<br>o Amazon RDS en AWS Outposts. | Configuración plataforma |
| **EC2** | Despliegue de instancias de EC2 en la nube. Dependiendo del servicio contratado se ofrece administración del sistema operativo. | Configuración por máquina |

ANTECEDENTES INFRAESTRUCTURA INSTITUCIÓN

De acuerdo con la facturación de COLEGIO MAYOR DE ANTIOQUIA y para dar continuidad a cada una de las 3 cuentas existentes detalladas a continuación, se diseña la oferta de Renovación en la nube de AWS en modalidad servicio acorde a los consumos obtenidos del mes de octubre de 2024:

**Cuenta 944776520710 COLEGIO MAYOR**
+ Nuevo Balanceador para la protección del dominio

**Cuenta 812369156857 SICMA**
+ Nuevo Balanceador para la protección de dominio
+ EC2 y RDS más servicios complementarios de redes y monitoreo

**Cuenta 615529218654 MI BIENESTAR**
No se le agregan servicios nuevos

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:

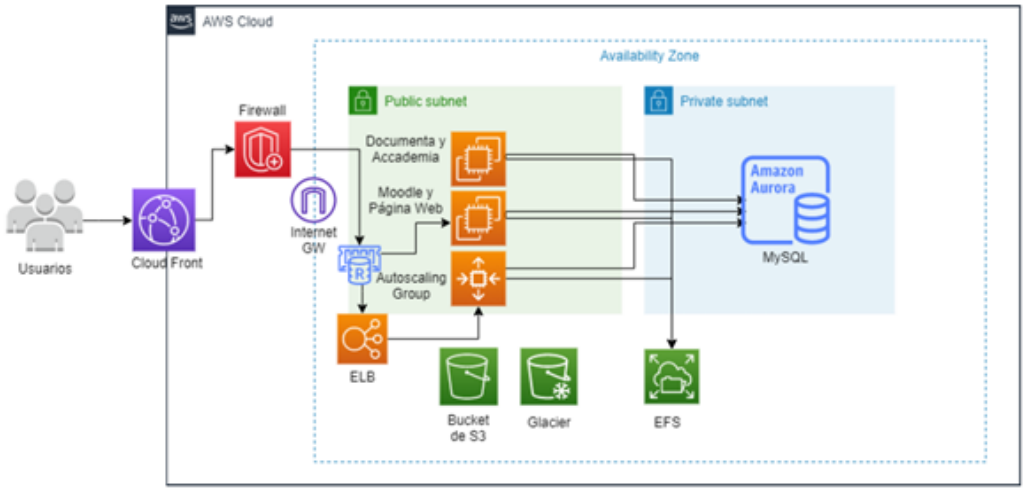
| Item | Servicio | Descripción |
|---|---|---|
| lacma y 2 elb > Lacma | Amazon EC2 | Tenencia (Instancias compartidas), Sistema operativo (Ubuntu Pro), Carga de trabajo (Consistent, Cantidad de instancias: 1), Instancia EC2 por adelantado (t4g.nano), Pricing strategy (On-Demand Utilization: 100 %Utilized/Month), Habilitar la monitorización (desactivado), EBS Cantidad de almacenamiento |

| | | |
|---|---|---|
| | | (50 GB), DT Entrada: Not selected (0 TBal mes), DT Salida: Not selected (0 TB al mes), DT Intra-región: (0 TB al mes) |
| lacma y 2 elb > Lacma | Amazon RDS for MySQL | Cantidad de almacenamiento (20 GB), Almacenamiento para cada instancia RDS (SSD de uso general (gp3)), Nodos (1), Tipo de instancia (db.m1.large), Utilización (solo bajo demanda) (100 %Utilized/Month), Opción de implementación (Single-AZ), Modelo de precios(OnDemand) |
| lacma y 2 elb > Lacma > Redes y monitoreo | Data Transfer | DT Entrada: Internet (1 TB al mes), DT Salida: Internet (100 GB al mes), DT Intra-región: (0 TB al mes), Costo por transferencia de datos (9) |
| lacma y 2 elb > Lacma > Redes y monitoreo | AWS Config | Número de elementos de configuración continua registrados (200), Número de elementos de configuración periódica registrados (200), Número de evaluaciones de las reglas de configuración (1000), Número de evaluaciones del paquete de conformidad (1000) |
| lacma y 2 elb > Lacma > Redes ymonitoreo | Amazon CloudWatch | Número de métricas (incluye las métricas personalizadas y detalladas) (50) |
| lacma y 2 elb > Lacma > Redes y monitoreo | AWS CloudTrail | Unidades de eventos de administración (millones), Registros de seguimiento de administración de escritura (1), Registros de seguimiento de administración de lectura (1), Unidades de eventos de datos (millones), Registros de seguimiento de S3 (1), Registros de seguimiento de Lambda (1), Unidades de eventos de Insights (millones), Registros de seguimiento con eventos de Insights (1), Eventos de administración de escritura (1 por segundo), Eventos de administración de lectura (1 por mes), Operaciones de S3 (1 por mes), Eventos de datos Lambda (1 por mes), Número de eventos de administración de escritura analizados (1 por mes) |
| lacma y 2 elb > Lacma > Redes ymonitoreo | AWS Key ManagementService | Número de claves maestras del cliente (CMK) administradas por el cliente (5), Número de solicitudes simétricas (2000000) |
| lacma y 2 elb > Sicma | Application Load Balancer | Número de balanceadores de carga de aplicaciones (1) |
| lacma y 2 elb >Colmayor | ApplicationLoad Balancer | Número de balanceadores de carga de aplicaciones (1) |

| | | |
|---|---|---|
| SICMA>EC2 | Amazon EC2 | Tenencia (Instancias compartidas), Sistema operativo (Windows Server), Carga de trabajo (Consistent, Cantidad de instancias: 1), Instancia EC2 por adelantado (c6a.2xlarge), Pricing strategy (On- Demand Utilization: 100 %Utilized/Month), Habilitar la monitorización (desactivado), EBS Cantidad de almacenamiento (300 GB), DT Entrada: Not selected (0 TB al mes), DT Salida: Not selected (0 TB al mes), DTIntra-región: (0 TB al mes) |
| SICMA>Base de datos MySql | Amazon RDS for MySQL | Cantidad de almacenamiento (100 GB), Almacenamiento para cada instancia RDS (SSD de uso general (gp3)), Nodos (1), Tipo de instancia (db.r5.xlarge), Utilización (solo bajo demanda) (100 %Utilized/Month), Opción de implementación (Single-AZ), Modelo de precios(OnDemand) |

| Servicio Profesional | Horas hábiles | Horas no hábiles | Descripción |
|---|---|---|---|
| Configuración Organización Propia en AWS | 8 | 0 | Servicios Profesionales para la creación de organización propia en AWS |

La arquitectura del servicio que se recibirá debe tener la siguiente topología, y puede variar según las circunstancias de configuración final




**ACUERDOS DE NIVELES DE SERVICIO**

| TIEMPOS DE ATENCIÓN | | | |
|---|---|---|---|
| **HORARIO DE ATENCIÓN** | | **7x24x365** | |
| **TIEMPO DE ATENCIÓN INICIAL** | | **30 min** | |
| **INCIDENTES** | | **SOLICITUDES** | |
| **SEVERIDAD** | **CRITERIOS** | **SEVERIDAD** | **CRITERIOS** |
| **HIGH** | El negocio del cliente tiene una pérdida o degradación significativa de los servicios yrequiere atención prioritaria. | **HIGH** | Solicitudes que el cliente requiere con prioridad media en un entornoproductivo. |
| **MODERATE** | El negocio del cliente tiene una pérdida o degradación moderada de los servicios, pero el trabajo puede continuarrazonablemente de manera deteriorada. | **MODERATE** | Solicitudes que el cliente requiere con prioridad baja en un entorno productivo o no productivo. |
| **LOW** | 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 funcionado. | **LOW** | 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** |

| | | | |
|---|---|---|---|
| **HIGH** | 2 horas | **HIGH** | 8 horas |
| **MODERATE** | 4 horas | **MODERATE** | 16 horas |
| **LOW** | 24 horas | **LOW** | 24 horas |

**COMUNICACIONES UNIFICADAS**

Trabajo Hibrido 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.

Capacidades de (PBX) para llamadas empresariales: La solución de comunicaciones unificadas (Cisco Webex Calling) cuentas 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.

| 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 |

Dentro del servicio se encuentran otros componentes como:

**Licenciamiento Webex**
**Interconexión Telefónica – Local Gateway**
**Telefonía**
**Servicios Administrados:**

La institución requiere del plan Básico de comunicaciones consistente en 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).

Dado que en la contratación correspondiente al otro si de ampliación de enero de 2025, para el resto del año 2025 no se requieren los servicios profesionales de implementación, migración, integración, oporte Reactivo y capacitación de usuarios, ya que estos fueron realizados en el mes de enero de

2025.

El servicio requerido Call Center Básico nos debe brindar una colección de funciones diseñadas para trabajar en conjunto que permitan 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)
- In formes 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)

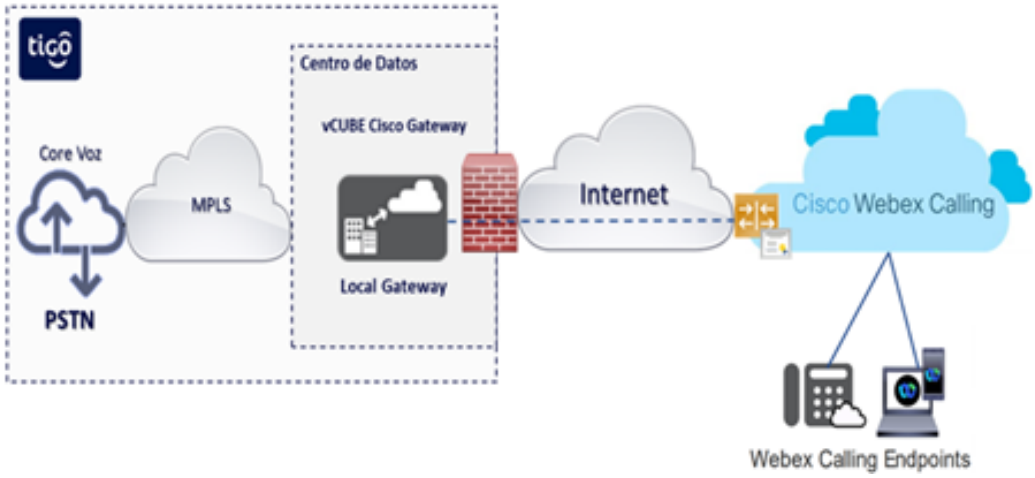
Call center básico se apoya en el portal de administración del servicio (Webex Control Hub) para entregar un amplio compendio de informes y estadísticas predefinidas brindan a los administradores acceso a visualizaciones de datos interactivos que muestran información importante.
Elementos requeridos:

- 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:**

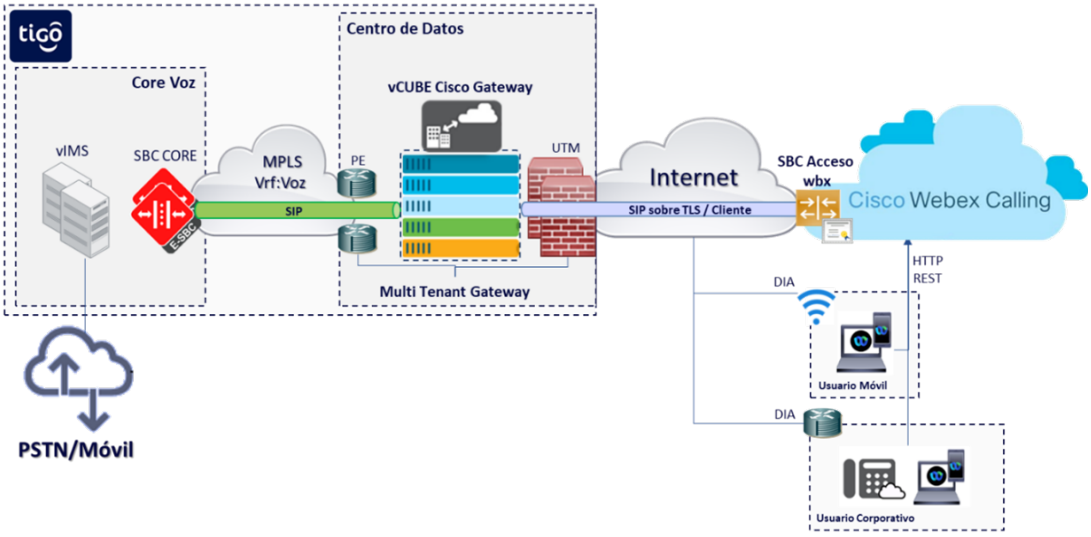
| OFERTA WEBEX CALLING | Cantidad |
|---|---|
| NU Webex Calling Professional | 100 |
| NU Webex Calling Workspace | 56 |
| Enrutamiento Telefonico Estandar-P1MM | 30 |
| Servicio  Administrado Basico-P1MM | 156 |
| Teléfonos Cisco 6851 | 140 |
| TSIP_Dedicada_Sin Minutos | 3 |
| TSIP_Dedicada_Acceso_Adicional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

La topología del servicio recibir y lo que contiene




- 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.
- Topología Lógica y compuesta por:




- 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.

Se requiere que esta solución permita revisar diferente tipo de informes:

Visualizar estadísticas de Reuniones, Mensajería, Llamadas, Dispositivos, espacios de trabaja, como mínimo por 90 días.

- Histórico de llamadas
- Informes de Cola de Llamadas, Total de Llamadas contestadas, Total de Llamadas abandonadas, llamadas donde el llamante cuelga antes de que un agente esté disponible, y sus porcentajes y demás informe de colas, y tendencias para llamadas entrantes a la cola.
- El portal debe permitir, 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 y acceder con las credenciales del usuario.

Responsabilidades de nosotros como clientes y del proveedor

- La Institución 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

- El proveedor 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 El proveedor.
- La Institución debe suministrar el plan de numeración existente y diligenciarlo en el formato establecido por El proveedor con acompañamiento del equipo de El proveedor.
- El proveedor 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.
- El proveedor 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 la Institución y previamente definido en el formato de levantamiento de información de El proveedor.

Restricciones al servicio recibido de Webex-Calling

- 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.

OFERTA ECONÓMICA

OFERTA RENOVACIÓN CIBERSEGURIDAD – INTERNET

| Producto | Cantidad | Ancho de Banda | Tarifa MensualSin IVA | Tarifa MensualCon IVA |
|---|---|---|---|---|
| Internet Dedicado Principal | 1 | 500 Mbps | $ 2.750.000 | $ 3.272.500 |
| Internet Banda Ancha Backup | 1 | 500 Mbps | $ 735.630 | $ 875.400 |
| Pool de IPs | 3 | No aplica | $ 0 | $ 0 |
| Servicio de Ciberseguridad en Premisas para 500 Mbps + FAZ | 1 | No aplica | $ 4.263.559 | $ 5.073.635 |

| | | |
|---|---|---|
| Tarifa Total Mensual por 11 meses | $ 7.749.189 | $ 9.221.535 |

Notas Importantes:

- Estos valores, hacen parte de una oferta integral, por lo tanto, si la oferta cambia, las tarifas pueden cambiar.
- Permanencia 11 Meses.
- 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.

OFERTA RENOVACIÓN NUBE PÚBLICA AWS

Facturación promedio de las cuentas Existentes y servicios nuevos

| | |
|---|---|
| Cuenta 944776520710 COLEGIO MAYOR | PROMEDIO CONSUMODe Sept2024 a Enero2025 |
| Total costs($) | USD 5.049,86 |
| Cuenta 615529218654 MI BIENESTAR | |
| Total costs($) | USD 55,77 |
| Cuenta 812369156857 SICMA | |
| Total costs($) | USD 79,94 |
| TOTAL SERVICIOS AWS | USD 5.185,56 |

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 TotalEstimado x mes |
|---|---|---|---|
| Servicios AWS | $ 22.038.646 | $ - | $ 22.038.646 |
| Servicios Administrados Tigo (Enterprise) | $ 3.305.797 | $ 628.101 | $ 3.933.898 |
| Tarifa Total Estimada por 11 meses | $ 25.344.443 | $ 628.101 | $ 25.972.544 |

- 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 de los servicios: 11 meses a partir de la activación de los mismos.

- Tarifa de Servicios Administrados Tigo: Equivale al 15% del consumo mensual de los Servicios AWS, manteniéndose esta tarifa para futuras adiciones.
- Obligaciones del Cliente: El Cliente debe abonar el consumo de servicios en AWS, así como los servicios profesionales y administrados, hasta el último día de actividad según lo estipulado en el contrato con Tigo Business.
- Responsabilidad del Cliente: Si el Cliente tiene permisos para realizar cambios en su infraestructura dentro de AWS, asumirá la total responsabilidad por las consecuencias que estos cambios puedan acarrear, tanto en rendimiento como en costos.
- Impacto de cambios solicitados: Los cambios y requerimientos solicitados por el Cliente a Tigo Business se reflejarán en el consumo en AWS y en la facturación correspondiente.
- Cálculo de facturación: La facturación al Cliente se basará en los consumos generados desde la provisión de recursos, es decir, desde su creación hasta su baja.
- Reportes de consumo: Tigo Business proporcionará al Cliente informes sobre el consumo dentro de AWS, conforme al alcance de los servicios administrados contratados.
- Valor mensual de la Oferta Comercial: Este valor es referencial, ya que incluye servicios Cloud AWS y complementarios, cuya facturación depende del consumo real. Por lo tanto, el monto a facturar puede variar mensualmente. En consecuencia, el costo mensual del Servicio Administrado Cloud también puede fluctuar.
- Facturación para clientes del Sector Gobierno: Se facturará a la TRM de $4.250 acordada entre las partes para la Orden de Compra o contrato respectivo. Sin embargo, si la TRM promedio oficial del mes en que se consumieron los servicios presenta una variación igual o mayor al 5% respecto a la TRM acordada o a la TRM utilizada para la facturación del mes anterior, esta se ajustará proporcionalmente a dicha variación para la facturación de los servicios consumidos.
- En los casos en que el cliente tenga autorización para realizar modificaciones en los servicios de AWS Cloud, será responsable de las consecuencias que dichos cambios puedan tener sobre el rendimiento y el costo de los recursos utilizados. Por lo tanto, podrá incrementar el consumo siempre que se mantenga dentro del presupuesto establecido y, en el caso del sector gubernamental, siempre que esté dentro del límite de su CDP. Si se requieren consumos adicionales, el cliente deberá realizar primero una adición presupuestaria. En cualquier circunstancia, la facturación se basará en el consumo real de los servicios de AWS asociados a la cuenta del cliente. Los registros de los cambios realizados por el cliente se considerarán parte de la orden de compra o del contrato correspondiente firmado entre las partes.
- Al adquirir soluciones de AWS Tigo Business, firmar la orden de compra y/o servicio o suscribir un contrato entre las partes implica que el cliente acepta los términos y condiciones de AWS y otras condiciones publicadas en su sitio oficial, como el “Contrato de AWS con el Cliente”, “Términos de servicio de AWS” y “Contratos de Nivel de Servicio de AWS”.
- Al contratar soluciones de AWS y firmar la orden de compra y/o servicio o el contrato

correspondiente, el cliente autoriza a TIGO a crear una cuenta de AWS a su nombre utilizando una dirección de correo electrónico válida, en caso de que aún no disponga de una cuenta en AWS. En todo momento, es responsabilidad del cliente proporcionar correctamente la información necesaria para la cuenta, su activación y acceder a las condiciones publicadas por AWS.

- El cliente reconoce que Tigo Business no tiene control directo sobre la infraestructura que sustenta los servicios de AWS, por lo tanto, Tigo Business no asume ninguna responsabilidad por errores, interrupciones, pérdidas de datos o cualquier otro inconveniente que pueda surgir del uso de los servicios proporcionados por AWS.

**OFERTA RENOVACIÓN UCaaS 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 | $ 23.220 | $ 2.322.000 | 0% | $ 2.322.000 |
| Webex Calling Workspace | 56 | $ 13.932 | $ 780.192 | 0% | $ 780.192 |
| Troncal SIP Base 3 (3 accesos y 10 DID) | 1 | $ 70.978 | $ 70.978 | 19% | $ 84.463 |
| Accesos Adicionales | 27 | $ 18.720 | $ 505.440 | 19% | $ 601.474 |
| Plan Minutos Ilimitado Fijo | 1 | $ 291.255 | $ 291.255 | 19% | $ 346.594 |
| Enrutamiento Telefónico HA Georedundante | 30 | $ 12.784 | $ 383.520 | 19% | $ 456.389 |
| Servicios Administrados Básico | 156 | $ 0 | $ 0 | 19% | $ 0 |
| Teléfonos Cisco 6851 | 140 | $ 14.950 | $ 2.093.000 | 19% | $ 2.490.670 |
| Total Mensual COP$ | | | $ 6.446.385 | N/A | $ 7.081.782 |

Notas Importantes:

- Las tarifas son aplicables para la contratación global. Una vez firmado el contrato, se deberá

ejecutar la totalidad de las cantidades definidas.

- Se realizarán entregas parciales de las extensiones conforme se vayan entregando los equipos telefónicos. La facturación de los equipos se realizará según la tarifa individual a partir de su entrega operativa.
- La oferta incluye Servicios Administrados Básicos, que permiten un cambio por extensión al mes.
- En el proceso de migración del servicio de Conmutador Virtual a Webex Calling, será necesario cambiar los teléfonos debido a cuestiones de compatibilidad con la plataforma.
- La oferta no contempla elementos ni equipos de red; es responsabilidad del Colegio Mayor de Antioquia proporcionar 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 11 meses.
- 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.
- El concepto asociado a Horas Servicios Profesionales está orientado para apoyar al cliente en el proceso de migración.

RESUMEN OFERTA DE SERVICIOS

| Servicios | Meses | Valor Mensual Antes de IVA | Valor Mensual incluido IVA |
|---|---|---|---|
| Servicios de Internet - Ciberseguridad | 11 | $ 7.749.189 | $ 9.221.535 |
| Servicios Nube Pública AWS | 11 | $ 25.344.443 | $ 5.972.545 |
| Servicios Comunicaciones Unificadas | 11 | $ 6.446.385 | $ 7.081.782 |
| Total Servicios Tarifa Mensual | | $ 39.540.018 | $ 42.275.861 |
| Total Presupuesto Contrato 11 Meses | | $ 434.940.194 | $ 465.034.471 |

Código UNSPSC 81112100 Clase: Servicios de internet.

**5.** Que la Institución Universitaria Colegio Mayor de Antioquia cuenta con un presupuesto estimado de **CUATROCIENTOS SESENTA Y CINCO MILLONES TREINTA Y CUATRO MIL CUATROCIENTOS SETENTA Y UN PESOS ($465.034.471)** para la realización de este contrato.

**6.** Que **UNE EPM TELECOMUNICACIONES S.A.** con NIT **900092385-9**, presentó propuesta económica y anexó los documentos requeridos para la contratación.

**7.** Que la Institución elaboró el correspondiente estudio y obtuvo los documentos previos esenciales para este tipo de contratación, y estos se podrán consultar en la plataforma transaccional SECOP II.

**8**. Que se cuenta con la Disponibilidad y Compromiso Presupuestal expedido por la Oficina de Presupuesto.

En mérito de lo expuesto,

**R E S U E L V E**

**ARTÍCULO PRIMERO:** Contratar directamente a **UNE EPM TELECOMUNICACIONES S.A.** con NIT **900092385-9** para la ejecución del siguiente objeto:*" El contratista, de manera independiente, por su propia cuenta y riesgo se obliga con la Institución Universitaria Colegio Mayor de Antioquia a prestar los servicios de Tecnologías de la Información y/o Comunicaciones que se detallan en las especificaciones del objeto.",* por un valor total de **CUATROCIENTOS SESENTA Y CINCO MILLONES TREINTA Y CUATRO MIL CUATROCIENTOS SETENTA Y UN PESOS ($465.034.471)** El plazo de duración del contrato será desde la firma del acta de inicio hasta el día 31 de diciembre de 2025.

**PARÁGRAFO:** El contrato sólo se suscribirá si el contratista cumple con todos los requisitos legales.

**ARTÍCULO SEGUNDO**: De acuerdo con lo dispuesto en el artículo 77 de la Ley 80 de 1993, contra el presente acto procede el recurso de reposición.

**ARTÍCULO TERCERO**: El presente acto administrativo rige a partir de la fecha de su publicación.

**PUBLÍQUESE Y CÚMPLASE**

JOSE LUIS BEDOYA CASTAÑEDA
DIRECTOR(A) TÉCNICO
DIRECCIÓN JURÍDICA

Proyectó: MANUELA OSORIO GALVIS
CONTRATISTA
DIRECCIÓN JURÍDICA

Revisó: LUISA FERNANDA YASSIN OSPINA
CONTRATISTA
DIRECCIÓN JURÍDICA