

Oferta Técnica y Comercial

Soluciones Digitales AWS

MINCIT MINISTERIO DE COMERCIO INDUSTRIA Y TURISMO

business.tigo.com

tigo business

Bogotá, 22 de septiembre de 2025

Señores

Ciudad

Ref. Servicios AWS

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,

Ejecutivo de Cuenta

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.

Tabla de Contenido

AWS (Amazon Web Services) 4

1. GENERALES 4

1.1. Características y Beneficios 5

1.2. Propuesta de Valor 6

2. DESCRIPCIÓN DE LA PROPUESTA 7

2.1. Objetivo 7

2.2. Alcance 8

2.3. Ampliación de nuestra oferta 9

2.4. Servicios Administrados 9

2.4.1. Servicios administrados de Infraestructura 9

2.4.2. Servicios administrados de Bases de Datos 14

2.4.2.1. Gestión de bases de datos en instancias EC2 15

2.4.2.2. Gestión de bases de datos en AWS RDS 16

2.4.3. Alcance Servicios de Seguridad AWS 18

2.4.4. Requerimientos mínimos para administración de cuentas AWS 24

2.4.5. Consideraciones Servicios Administrados 25

2.5. Servicios Profesionales 26

2.5.1 Servicios Profesionales Cloud de Estrategia, Evaluación, Planeación y Diseño: ... 26

2.6. Antecedentes 27

2.7. Descripción General 27

2.8. Supuestos y Restricciones 27

2.9. Implementación y/o transición 28

2.10.1 Metodología de aprovisionamiento 28

2.10.2 Tiempo de aprovisionamiento 29

2.10.3 Entregables 30

2.10. Acuerdos de Niveles de Servicio 31

3. ROLES Y RESPONSABILIDADESDES 32

3.1 Modelo de Responsabilidad Compartida Amazon Web Services (AWS) 32

4. ACUERDO DE CONFIDENCIALIDAD 39

5. Condiciones Comerciales Tigo Cloud AWS Colombia 40

5.1. Propuesta Económica 40

5.2. Condiciones Comerciales: 40

AWS (Amazon Web Services)

1. GENERALES

Amazon Web Services (AWS) es la plataforma en la nube más adoptada[1] 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.

[1] 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 hibrido. 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.

1.1. 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.

1.2. 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.

2. DESCRIPCIÓN DE LA PROPUESTA

Tigo Business presenta al MINISTERIO DE COMERCIO INDUSTRIA Y TURISMO (MINCIT), de ahora en adelante el cliente, 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

2.1. Objetivo

El objetivo principal es presentar al cliente 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.

2.2. 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.

2.3. 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:

2.4. Servicios Administrados

En la siguiente tabla se describen el alcance del Plan de Servicios Administrado de Tigo Business (**VIP**), se indican las actividades que abarcan los diferentes tipos de Plan, especificando el alcance que se realizan sobre cada uno de ellos.

2.4.1. 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**	Tigo 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.

Categoría	ítem	Enterprise
		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: ✓ Administración de alarmas ✓ Etiquetas de recursos ✓ Líneas base de actualizaciones de seguridad y ventanas de mantenimiento ✓ Planificador de ejecución de recursos ✓ Planes de respaldo ✓ 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

Categoría	ítem	Enterprise
		* 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 Manager * Creación 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: ○ Amazon Linux 2 ○ CentOS 7.x ○ Oracle Linux 7: versiones menores 7.5 y superiores. Oracle Linux 8: versiones menores 8.3. ○ Red Hat Enterprise Linux (RHEL) 8.x, 7.x ○ SUSE Linux Enterprise Server 15 SP3, SP4 ○ Ubuntu Linux 18.04 and 20.04 ○ 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)

Categoría	ítem	Enterprise
	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

Alcance de los servicios administrados infraestructura AWS		
Categoría	ítem	
Administración y soporte del sistema operativo	Administración de Sistema Operativo	Tigo 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: ✓ Administración de alarmas ✓ Etiquetas de recursos ✓ Líneas base de actualizaciones de seguridad y ventanas de mantenimiento ✓ Planificador de ejecución de recursos ✓ Planes de respaldo ✓ 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.

Alcance de los servicios administrados infraestructura AWS		
Categoría	**ítem**	
		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 Manager * Creación 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: ○ Amazon Linux 2 ○ CentOS 7.x ○ Oracle Linux 7: versiones menores 7.5 y superiores. Oracle Linux 8: versiones menores 8.3. ○ Red Hat Enterprise Linux (RHEL) 8.x, 7.x ○ SUSE Linux Enterprise Server 15 SP3, SP4 ○ Ubuntu Linux 18.04 and 20.04 ○ 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	Trimestral
Aseguramiento de la cuenta y mejora continua	**Refuerzo de controles**	Implementación de biblioteca seleccionada de reglas de AWS Config. (Notificación, Remediación por caso o automática)
	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,)**	**Mensual (Responsable país)**
	Reportes de servicio (ejecución de respaldos, métricas de infraestructura para los servicios contratados)	**A demanda** **Mensual programado**

Alcance de los servicios administrados infraestructura AWS		
Categoría	**ítem**	
	Informe de aseguramiento (Gestión de Identidad, Assessment infraestructura y recomendaciones para optimización de costos)	Trimestral

2.4.2. 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
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

ítem	Enterprise
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

2.4.2.1. Gestión de bases de datos en instancias EC2

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 EC2 SQL Server
- Amazon EC2 MySQL
- Amazon EC2 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.

Los motores de base de datos deberán estar configurados bajo las buenas prácticas. 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 para configuración de availability group y/o always on.
- 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 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 plan
- Análisis de métricas y datos
- Acompañamiento en la actualización del motor de base de 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.

2.4.2.2. 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.

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.

2.4.3. Alcance Servicios de Seguridad AWS

El servicio administrado de Tigo ofrece las siguientes características, las cuales estarán disponibles para el cliente según el plan de servicios administrados contratado, y aplican cuando adquiere alguno de los servicios de seguridad que se mencionan en la siguiente tabla: WAF, Security Hub, GuardDuty e Inspector.

Categoría	ítem	Enterprise
Protección de redes y aplicaciones	Administración de WAF Nota: Depende de la integración de servicios ELB, CloudFront, AppSync y API Gateway* Capacidad = WCU* Se incluyen reglas para control de listas negras/IP Block.	Configuración y gestión de las reglas administradas por AWS, Custom y de terceros. Monitoreo con CloudWatch de 12 métricas.
	Administración de Network Firewall Nota: Para arquitecturas con tráfico East-West o entre VPCs se debe considerar un plan Enterprise o VIP* Capacidades de acuerdo con el tráfico Stateless y Stateful*	Configuración y gestión de controles de seguridad para la inspección en el tráfico de salida y entrada de la VPC. Configuración de 16 rule groups o reglas de FW (6 Firewall Policy). Nota: El Firewall puede necesitar un certificado público para descifrar el tráfico TLS* Monitoreo con CloudWatch de 10 métricas
	Administración Shield Advanced Nota: Es necesario tener soporte Business o Enterprise de AWS para acceder al equipo de respuesta (AWS SRT Support). Acceso al panel de entorno de amenazas globales.	Configuración y gestión de los recursos protegidos (CloudFront, EIP, WAF). Gestión de Route 53 Health Check y monitoreo del panel de eventos. Proactive engagement y comunicación con el SRT Support para manejo de mitigaciones.
Detección y respuesta	Security Hub	Integración del CSPM con GuardDuty para manejo centralizado de Findings y proceso de gestión de eventos con RSOC.

Categoría	ítem	Enterprise
	(CSPM)	8 Sugerencias o recomendaciones para mejorar la postura de seguridad* Automatizaciones con ASR AWS: Reglas de SG. Reglas de NACL. Políticas de Buckets S3.
	GuardDuty Nota: Depende de la activación de otros servicios como: CloudTrail (Management and Event logs), VPC Flow logs y DNS logs*.	Configuración y gestión de inteligencia de amenazas para 4 planes de protección. S3 Protection (logs) RDS Protection (login logs) EKS Protection (Audit logs) Lambda Protection (Network activity logs)
	Inspector Nota: RSOC no realiza proceso de remediación en servicios del cliente.	Servicio de administración automatizada de vulnerabilidades que analiza continuamente las cargas de trabajo de AWS. Gestión de Findings críticos.

Alcance servicios de detección y respuesta:

Los servicios de detección y respuesta de AWS le ayudan a mejorar su postura de seguridad y a optimizar las operaciones de seguridad en todo su entorno de AWS al identificar y priorizar continuamente los riesgos de seguridad, así como supervisar los desvíos que se pueden presentar a nivel Conformidad como el cumplimiento de los estándares establecidos por: el Centro para la Seguridad de Internet CIS (Center for Internet Security), el Marco de Seguridad en la Nube (CSF) del Instituto Nacional de Estándares y Tecnología (NIST), la Ley de Portabilidad y Responsabilidad de Seguros Médicos (HIPAA y el Estándar de Seguridad de Datos (DSS) de la Industria de Tarjetas de Pago (PCI).

Amazon GuardDuty: Es un servicio de detección de amenazas que supervisa de manera continua sus cargas de trabajo y cuentas de AWS para detectar actividades maliciosas y envía hallazgos detallados de seguridad para su visibilidad y corrección.

Actividades y alcance del RSOC servicio GuardDuty:

- Monitoreo general de amenazas de acuerdo con los planes de protección: eventos en S3 Protection, EKS Protection, Malware Protection en EC2 y contenedores, RDS Protection y Lambda Protection.
- Ejecución de escaneos de malware bajo demanda para cuentas especificas o instancias EC2.
- Gestión de findings o hallazgos de acuerdo con su severidad y notificación al cliente de hallazgos de seguridad con severidad Alta.
- Configuración de listas blancas o negras de direcciones IP en formatos CSV, STIX o texto plano.

- Recomendaciones y buenas prácticas de seguridad de acuerdo con los findings o hallazgos identificados que puedan dar al cliente la visibilidad y mejora continua de su postura de seguridad.

Alcance Centralización /integración de AWS GuardDuty a CSPM (Security Hub) a una cuenta delegada regional

- Para los modelos ECAM/SPAM, se realiza la integración de AWS GuardDuty a través del servicio de AWS Organizations o por invitación al CSPM Security Hub. De esta forma el equipo de Seguridad SOC y equipo regional de soporte pueden monitorear a las cuentas de los clientes que tengan el servicio habilitado, y éste enviando findings a un CSPM, y a su vez, asociado a una cuenta maestra de Security Hub.

Nota: Este alcance está dirigido a la iniciativa de tener un CSPM como Oferta comercial de seguridad con sus planes adecuados.

Inspector: Es un servicio de gestión de vulnerabilidades que analiza continuamente las cargas de trabajo en busca de vulnerabilidades de software y exposición no deseada de la red. Amazon Inspector descubre y analiza automáticamente las instancias de Amazon EC2 en ejecución, las imágenes de los contenedores del Amazon Elastic Container Registry (Amazon ECR) y AWS Lambda las funciones para detectar vulnerabilidades de software conocidas y exponer la red de forma involuntaria.

Actividades y alcance del RSOC servicio Inspector:

- Analizar continuamente el entorno en busca de vulnerabilidades en instancias EC2 y contenedores (Aplican costos por ejecución*).
- Identificar hallazgos de impacto crítico con el panel de control de Inspector.
- Entrega de Informe con los findings o hallazgos.
- Dar seguimiento a las remediaciones de acuerdo con la clasificación de activos y responsables del servicio y/o las cargas de trabajo en nube.

Alcance Centralización /integración de AWS Inspector al CSPM (Security Hub) a una cuenta delegada regional

- Para los modelos ECAM / SPAM, se realiza la integración de AWS Inspector a través del servicio de AWS Organizations o por invitación al Security Hub. De esta forma el equipo de Seguridad SOC y equipo regional de soporte pueden monitorear a las cuentas de los clientes que tengan el servicio habilitado, y éste enviando hallazgos a un CSPM, y a su vez, asociado a una cuenta maestra de Security Hub.

Nota: Este alcance está dirigido a la iniciativa de tener un CSPM como Oferta comercial de seguridad con sus planes adecuados.

Security Hub

Actividades y alcance del RSOC Security Hub:

- Gestión de findings centralizados de servicios como: GuardDuty, Inspector, AWS Config y Detective.
- Gestión de conformidad de acuerdo con frameworks de seguridad como: NIST, CIS, AWS Foundational y PCI DSS.
- Verificación de las posibles desviaciones en la línea base o lineamientos de seguridad de las cargas de trabajo.
- Análisis de insights de acuerdo con los findings reportados por los servicios de seguridad integrados.

Nota: Security Hub permite la integración de findings de terceros como Barracuda, Alert Logic, Aqua Security, Check Point CloudGuard, FortiCNP, etc.

Alcance CSPM Centralización de AWS Security Hub (ECAM/ SPAM C/País)

- Es necesario la centralización de dichos servicios habilitados de AWS Security Hub en una única consola por país para los modelos ECAM/SPAM, de esta forma el equipo de Seguridad SOC y equipo regional de soporte pueden monitorear a las cuentas de los clientes que tengan el servicio habilitado, y estas estar asociados a una cuenta maestra de AWS Security Hub.

Servicios nativos de AWS que soportan el CSPM para la ingesta:

Servicio seguridad AWS (Nativo)	CSPM (Producto)
Security Hub	**SI**
Amazon Detective	**SI**
Amazon GuardDuty	**SI**
Amazon Inspector	**SI**
Amazon Macie	**SI**
Firewall Manager	**SI**
AWS Shield	**NO**

Nota: Este alcance está dirigido a la iniciativa de tener un CSPM como Oferta comercial de seguridad con sus planes adecuados.

AWS CloudTrail: Realiza un seguimiento de la actividad de los usuarios y del uso de la API en AWS y en entornos híbridos y multinube. Este servicio monitorea y registra la actividad de la cuenta en

toda la infraestructura de AWS, lo que le permite controlar las acciones de configuración y acceso sobre los servicios de nube AWS.

Actividades y alcance del RSOC AWS CloudTrail:

- Investigar eventos de seguridad para dar respuesta a eventos o incidentes de seguridad (Por defecto CloudTrail almacena los últimos 90 días, si el cliente requiere mayor tiempo de almacenamiento es necesario considerar los costos adicionales*).
- Detección de actividades inusuales a nivel de llamados al API y notificación de eventos usando servicios como SNS o EventBridge (La inclusión de estos servicios puede generar costos adicionales al cliente*).

Alcance servicios de protección de redes y aplicaciones:

Los servicios de protección de redes y aplicaciones lo ayudan a aplicar políticas de seguridad precisas en los puntos de control de red de toda su organización. Los servicios de AWS lo ayudan a inspeccionar y filtrar el tráfico para impedir el acceso no autorizado a los recursos en los límites a nivel de host, red y aplicación.

AWS Firewall Manager: Este servicio simplifica las tareas de administración y mantenimiento en varias cuentas y recursos para una variedad de protecciones de AWS WAF y Shield Advanced*, incluidos los grupos de seguridad de Amazon VPC y el firewall DNS Amazon Route 53 Resolver.

Adicionalmente con Network Firewall y Firewall Manager, se agregan las protecciones solo una vez y el servicio las aplica automáticamente en todas las cuentas y recursos, incluso cuando se agregan cuentas y recursos.

Las características principales de AWS Firewall Manager incluyen:

- **Gestión centralizada de políticas**: Permite a los administradores definir y aplicar políticas de seguridad de manera centralizada, asegurando que todas las aplicaciones y cuentas estén protegidas por las mismas reglas de seguridad, lo cual facilita el cumplimiento de los requisitos de seguridad y reduce el riesgo de configuraciones incorrectas.

- **Automatización**: Automatiza la aplicación de políticas de seguridad a todos los recursos existentes y futuros en la organización, lo que ayuda a garantizar una cobertura de seguridad completa sin la necesidad de intervención manual cada vez que se agregan nuevos recursos o servicios.

- **Integración con servicios de AWS**: Funciona de manera integrada con otros servicios de seguridad de AWS como AWS WAF (Web Application Firewall), AWS Shield para protección contra DDoS, y Amazon VPC (Virtual Private Cloud) Security Groups, permitiendo a los administradores aplicar un amplio rango de políticas de seguridad a través de diferentes capas de su infraestructura.

- **Gestión de cumplimiento**: Ayuda a las organizaciones a cumplir con sus políticas de seguridad internas y requisitos de cumplimiento externos, proporcionando visibilidad sobre las políticas aplicadas y permitiendo la detección de recursos no conformes.

- **Simplicidad y escalabilidad**: Ofrece una solución simplificada para la gestión de la seguridad a escala, eliminando la necesidad de gestionar múltiples herramientas o políticas de seguridad de forma individual en cada cuenta o servicio de AWS.

Integración con SCPM Security Hub: AWS Firewall Manager se integra con AWS Security Hub para proporcionar una visión centralizada de las alertas y hallazgos de seguridad relacionados con las políticas de firewall en tus cuentas de AWS.

AWS Firewall Manager es útil para organizaciones con múltiples cuentas de AWS y muchos recursos en la nube, ya que facilita la gestión de la seguridad a gran escala y asegura una postura de seguridad consistente en la organización.

Actividades y alcance del RSOC AWS Firewall Manager:
Gestionar de manera centralizada reglas de firewall, ACLs de AWS WAF, Shield Advanced*, grupos de seguridad, y reglas de DNS.

AWS Shield Standard : Todos los clientes de AWS se benefician de las protecciones automáticas de AWS Shield Standard* sin cargo adicional. AWS Shield Standard protege contra los ataques DDoS más comunes y frecuentes de la capa de transporte y de red que tienen como objetivo las aplicaciones web. Cuando utiliza AWS Shield Standard con Amazon CloudFront y Amazon Route 53, recibe protección de disponibilidad integral contra todos los ataques conocidos a la infraestructura (capas 3 y 4).

AWS Shield Advanced: Proporciona protección contra una amplia gama de vectores de ataque DDoS conocidos y vectores de ataque de día cero. La detección y mitigación están diseñadas para brindar cobertura contra las amenazas, incluso si el servicio no las conoce explícitamente en el momento de la detección.

Las características clave de AWS Shield Advanced incluyen:

Protección contra ataques DDoS de gran escala: AWS Shield Advanced está diseñado para mitigar incluso los ataques DDoS más grandes y complejos, asegurando que las aplicaciones sigan siendo accesibles para los usuarios legítimos.

- Soporte 24/7 de un equipo de respuesta a incidentes DDoS (DRT): Los suscriptores de Shield Advanced tienen acceso al equipo de respuesta a incidentes DDoS de AWS, que puede proporcionar asistencia experta en tiempo real para mitigar ataques.

- Costos de escalabilidad protegidos: AWS Shield Advanced ofrece protección contra los costos de escalabilidad que pueden resultar de un ataque DDoS, ayudando a los clientes a evitar gastos inesperados debido al tráfico de ataques.

- Visibilidad y reportes de ataques: Los clientes reciben notificaciones y reportes detallados sobre ataques DDoS, lo que les permite entender mejor la naturaleza de los ataques y cómo están siendo mitigados.

- Integración con AWS WAF: Shield Advanced se integra estrechamente con AWS WAF (Web Application Firewall), permitiendo a los usuarios crear reglas personalizadas para mitigar ataques complejos y adaptarse a vectores de ataque específicos.

- Protección para aplicaciones en premisa: Además de proteger las aplicaciones hospedadas en AWS, Shield Advanced también puede proteger aplicaciones en instalaciones físicas mediante el uso de AWS Global Accelerator.

- Tarifa fija: A diferencia de AWS Shield Standard, que es gratuito para todos los usuarios de AWS, Shield Advanced tiene una tarifa fija mensual, además de posibles cargos adicionales basados en el uso de servicios complementarios como AWS WAF y AWS Global Accelerator.

AWS Shield Advanced está diseñado para organizaciones con necesidades de seguridad críticas, que requieren el más alto nivel de protección y soporte contra ataques DDoS.

2.4.4. 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): Línea base de alertas - monitoreo SA TIGO.xlsx (sharepoint.com)
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.

Para la configuración de los planes de AWS Backup en los recursos soportados, SA Tigo propone el esquema básico de la siguiente tabla:

Plan de respaldo AWS Backup mínimo requerido		
Plan	**Frecuencia**	**Retención**
Respaldo diario	Diario - 05:00 UTC	7 días
Respaldo semanal	Domingo - 03:00 UTC	3 semanas
Respaldo mensual	1er día del mes - 03:00 UTC	2 meses

Las zonas horarias y frecuencia de los planes de backups descritas en la tabla son sugeridas por el equipo de SA TIGO y se deben validar con el cliente en las etapas de preventa y/o implementación.

2.4.5. 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.

2.5. 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.

2.5.1 Servicios Profesionales Cloud de Estrategia, Evaluación, Planeación y Diseño:

Involucra aquellas actividades necesarias para identificar las necesidades del cliente, la definición de una estrategia de despliegue, crecimiento, diseño de arquitectura y políticas de administración, consumo y seguridad asociadas a los servicios que componen la solución y la planeación integral de

las actividades necesarias para la implementación que impliquen el menor impacto para el cliente durante la migración. podemos apoyar a migrar sus cargas de trabajo utilizando servicios como Application Discovery Service para el descubrimiento de las cargas de trabajo, aplicaciones y dependencias.

2.6. Antecedentes

El Cliente requiere una propuesta de servicios AWS, los cuales ya están desplegados en AWS.

2.7. Descripción General

Nuestro objetivo es simplificar y optimizar la gestión de sus servicios en AWS. Ofrecemos un acompañamiento integral para realizar la transferencia de su cuenta actual a nuestra organización, garantizando la continuidad operacional de sus cargas de trabajo. Este proceso no solo asegura una transición sin interrupciones, sino que también le permitirá acceder a beneficios exclusivos, como tarifas competitivas, soporte especializado en español, y asesoramiento constante para maximizar el valor de sus servicios en la nube. Nuestro equipo de expertos está comprometido a trabajar de la mano con su organización para desarrollar estrategias que impulsen su innovación y eficiencia en AWS.

2.8. 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.

2.9. Implementación y/o transición

2.10.1 Metodología de aprovisionamiento

Para llevar a cabo el proceso de entrega de la solución contratada por el cliente, Tigo Business asignara la solicitud al Order Manager u Rol que sea designado como responsable de canalizar las necesidades y comunicación con el cliente, además de la integración de proveedores y aliados clave para el desarrollo de dicha solución.

El Order Manager u Rol designado harán uso de metodologías y herramientas de gestión de proyectos para el aprovisionamiento y seguimiento del desarrollo de la solución. Liderara la planificación de aprovisionamiento, revisión de alcances, identificación de riesgos, solicitud de recursos tanto internos como externos y todo lo consecuente a la construcción y ejecución de un plan de trabajo.

Dara inicio al proyecto con una Kick-off meeting con el cliente, áreas internas y externas como proveedores y aliados clave con el fin de mantenerse alineados, se realizarán reuniones periódicas de seguimiento y monitoreo a la ejecución del plan de trabajo según sea necesario.

A la finalización y cierre del proyecto se llevará a cabo una entrega formal de la solución al cliente, la cual incluye entrega de topología actualizada, entrega de la operación y el soporte.



2.10.2 Tiempo de aprovisionamiento

Apartado de descripción de las fases de desarrollo del proyecto con alto detalle, incluidas observaciones obtenidas al inicio, durante o al final de cada fase.

A continuación, se muestra los hitos principales de la implementación:

	Hito	Días
1	Aceptación de la oferta por parte del Cliente	1
2	Asignación de Gerente de Proyecto	2
3	Revisar Documentación Interna	3
4	Realizar Empalme Interno	5
5	Realizar presentación KickOff interno	7
6	Solicitar requerimientos internos	9
7	Realizar presentación KickOff externo	10
8	Creación de la Cuenta, Despliegue de Servicios de conectividad, cómputo y base de datos	11 y 12
9	Entrega Cliente	12
10	Facturación de los Servicios	13
11	Entrega servicio	14

Cronograma de Alto Nivel	Dia 1	Dia 2	Dia 3	Dia 4	Dia 5	Dia 6	Dia 7	Dia 8	Dia 9	Dia 10	Dia 11	Dia 12	Dia 13	Dia 14
Implementación														
Aceptación de la oferta por parte del Cliente														
Asignación de Gerente de Proyecto														
Revisar Documentación MF - EDT - Matriz de interesados- riesgos- Factibilidades- SOW														
Realizar Empalme Interno														

Realizar presentación KickOff interno														
Solicitar requerimientos internos														
Realizar presentación KickOff externo														
- Revisión Requerimientos y/o Levantamiento de información de Redes y Diseño de Bajo Nivel (LLD)														
Creación de Cuenta en AWS y Despliegue de Servicios														
Entrega Cliente														
Facturación de los Servicios														
Entrega servicio														

La duración del proyecto se estima en 14 días hábiles a partir de la firma de contrato y ejecución de Kick-off con el cliente y áreas involucradas. Este tiempo aplica únicamente para aprovisionamiento de infraestructura.

Consideraciones Entrega de servicio

1. El tiempo de entrega de un proyecto es variable con dependencia de la cantidad de servicios contratados, complejidad de aprovisionamiento, conectividad y acuerdos realizados con el cliente. Si el plazo estipulado se ve afectado independientemente si se trata de factores internos o externos, ambas partes deben reunirse y realizar las actualizaciones necesarias sobre lo pactado inicialmente.

2. Las actividades en cada fase pueden ser susceptibles a cambios, en la reunión inicial o Kick-off, el cliente, el equipo de implementaciones y el Order Manager u Rol asignado como responsable definirán un calendario de actividades, así como una fecha de finalización del proyecto.

3. En todos los casos, se realizará el mejor esfuerzo posible para la implementación de la solución en el menor tiempo posible.

4. 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.

2.10.3 Entregables

En el actual espacio deberá incluir entregables correspondientes a cada una de las fases que hacen parte del desarrollo del proyecto.

Entregable	Descripción de alcance
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.

Nota: Las entregas parciales deben realizarse acorde a lo estipulado dentro del cronograma, cada entregable debe detallar nombre del entregable, fecha de inicio/fin y fase a la que pertenece.

2.10. 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	
HIGH	El negocio del cliente tiene una pérdida o degradación significativa de los servicios y requiere atención prioritaria.		HIGH	Solicitudes que el cliente requiere con prioridad media en un entorno productivo.	
MODERATE	El negocio del cliente tiene una pérdida o degradación moderada de los servicios, pero el trabajo puede continuar razonablemente 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

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:

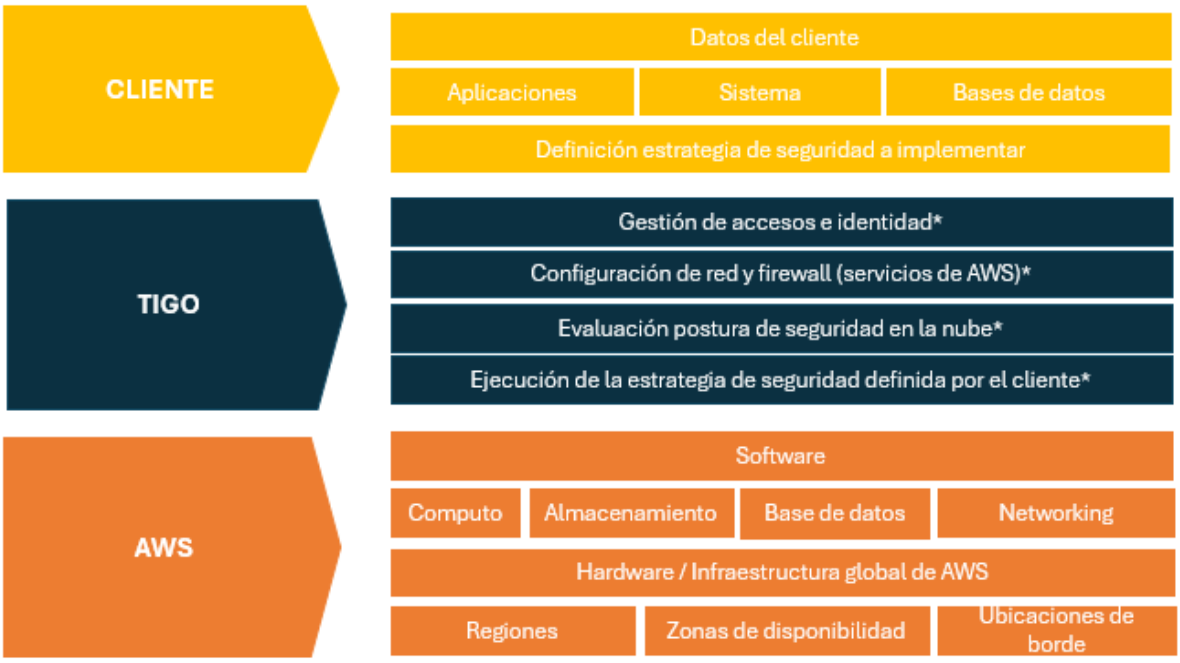
https://aws.amazon.com/es/legal/service-level-agreements/

3. ROLES Y RESPONSABILIDADESDES

3.1 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:

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 en base a 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 perdida 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. Ver términos y condiciones: <<url>>.
- 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 aprovisionados acorde a los requerimientos entregados por el cliente.

Condiciones Comerciales Tigo Cloud AWS

- El cliente se obliga a pagar por el consumo de servicios en la nube de AWS, además de los servicios profesionales y administrados brindados por Tigo Business. Según lo estipulado y aceptado en el contrato firmado por el cliente y Tigo Business.
- En casos en los que el cliente posea accesos con permisos de adición y modificación en su infraestructura en la nube de AWS, este deberá asumir total responsabilidad del uso e implicaciones resultantes de sus acciones. Implicaciones que podrían tener consecuencias en aumento de costos por consumo y problemas de rendimiento en servicios de AWS o sistemas propios del cliente.
- La aplicación de cambios o nuevos requerimientos solicitados por el cliente a Tigo Business, una vez, estos se han implementados, se verán reflejados en el consumo de AWS y la facturación propia de Tigo Business.
- El consumo se calcula desde el momento en que un servicio es aprovisionado (creado) hasta que este se ha dado de baja (eliminado).
- Tigo Business proporcionara reportes de consumo en AWS al cliente acorde al plan de servicios administrados contratado.
- El valor mensual agregado en la oferta comercial es de referencia, dado que puede incluir muchos servicios AWS y posiblemente otros servicios complementarios basados en el consumo, por lo tanto, el valor de facturación variara mes a mes. De acuerdo con lo antes mencionado, el valor mensual por servicios administrados Cloud también podría variar.
- Las ofertas presentadas en dólares americanos se facturarán mensualmente usando la moneda local.

- En caso de que el Cliente no formalice en el plazo establecido la renovación de la Orden de Compra y/o Servicio o del contrato suscrito entre las partes, Tigo Prorrogará automáticamente por un período igual al contratado inicialmente.
- 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.
- 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.
- Administración de la información, sitio en internet o cualquier contenido que sea habilitado en él o como parte del servicio.
- 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.
- Asumir la responsabilidad ante la perdida, robo o mal uso de accesos brindados por Tigo Business.
- El cliente declara y garantizara 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 recuperar 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 daña 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.
- Tigo Business no está en la obligación de monitorear el contenido alojado por el cliente en el espacio o servicios contratados, a excepción de cuando es un punto acordado directamente con el cliente. Además, el cliente indemnizará y mantendrá a Tigo Business exento de todo daño provocado por cualquier razón ilegal del lado del cliente.
- 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.
- 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.

- Tigo Business no es responsable de ataques a servidores, perdida de información o la caída de sistemas del cliente derivado de ataques a los servicios del cliente por la ausencia o mala configuración de las plataformas de seguridad del cliente.
- Los servicios contratados por el Cliente no le otorgan derecho a efectuar despachos masivos de correos electrónicos o a efectuar envíos de correos a casillas de receptores que no lo han autorizado y que dan a entender que el Cliente está llevando a cabo SPAM. El incumplimiento de lo anterior, faculta a Tigo Business a dar por terminado el contrato sin responsabilidad de su parte y sin perjuicio de la responsabilidad del Cliente por el uso indebido.
- El Cliente será el único responsable del contenido uso 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 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.
- Esta en las obligaciones del cliente presentar de manera formal que personas de su empresa u institución recibirán accesos y tendrán permitido solicitar asistencias técnicas o requerimientos sobre los servicios contratados. También es responsable de informar el cambio de personal designado a tales funciones. Sin perjuicio alguno Tigo Business podrá revocar el acceso remoto a los servicios contratados por el cliente, derivado del mal uso o que representen un riesgo a los servicios prestados por Tigo Business o cualquier otra entidad que haga parte del grupo comercial.

- Las licencias, programas y software utilizado por el Cliente que no sea contratado y administrado por Tigo Business, serán de su entera y exclusiva responsabilidad, por lo que desde el inicio del contrato exonera a Tigo Business de responsabilidad alguna que se derive de las instalaciones, licencias de software que el Cliente realice sin los debidos soportes de licenciamiento o derechos de uso de software u aplicaciones de terceros. Tigo Business queda facultado para trasladar cualquier multa o sanción que le sea impuesta por el proveedor, quedando el Cliente obligado a cancelar la misma y liberando a Tigo Business de toda responsabilidad con relación a dicho incumplimiento.
- Tigo Business puede a requerimiento del Cliente, activar soluciones de seguridad básicas y avanzadas en la parte de Firewall y de IPS, servicios que se adhieren a las soluciones adquiridas por el Cliente y están sujetas a la configuración que el Cliente utilice en los equipos, lo cual es responsabilidad exclusiva del Cliente por lo que, consecuentemente libera a Tigo Business de la configuración, parámetros y compatibilidad de éstos, y cualquier otro aspecto que se encuentre relacionado y/o se derive del mismo.
- El Cliente, acepta que todo Derecho de titularidad y propiedad intelectual e industrial sobre los servicios prestados (y los componentes de estos, incluidos, entre otros, imágenes, fotografías, animaciones, video, audio, música, texto y “applets” incorporados en los servicios) son propiedad de AWS o de sus proveedores. Los servicios están protegidos por leyes de propiedad intelectual y tratados de propiedad intelectual internacionales, así como por otras leyes y tratados de propiedad intelectual e industrial. Su posesión, acceso o uso de los servicios (productos de AWS) no le transmite ninguna propiedad sobre éstos, como tampoco ningún derecho de propiedad intelectual e industrial.

4. 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.

Glosario

Assessment: proceso de evaluación que permite realizar un diagnóstico inicial de una situación o contexto.

Direct Connect: es la posibilidad de entregar conectividad expresa hacia la nube. Un canal dedicado como el Direct Connect que permite que se haga una conexión privada y segura prestada a través del Carrier (operador Telco.

DRaaS (Disaster Recovery As a Service): «Recuperación de desastres como servicio», se trata de una tecnología de cloud que ofrece una alternativa de recuperación ante desastres, en el cual las organizaciones pueden tercerizar las configuraciones, equipamiento y las operaciones de sus métodos de recuperación de emergencia a empresas que cuentan con infraestructura y procesos mucho más optimizados.

Migración: es el proceso de mover aplicaciones y/o datos desde una ubicación (usualmente servidores privados del cliente) hacia otra (usualmente a la nube).

SA TIGO: Servicios Administrados Tigo Business

5. Condiciones Comerciales Tigo Cloud AWS Colombia

5.1. Propuesta Económica

SERVICIO	VALOR ITEM	VALOR IVA	VALOR TOTAL ITEM
Valor Portal CSP (estimado de Consumo 9 Meses.	$ 1.172.515.883	$ 0	$ 1.172.515.883
Servicios Administrado TIGO	$ 194.281.457	$ 36.913.477	$ 231.194.934
		Valor Total Oferta	$ 1.403.710.816

Notas:

- El VALOR MENSUAL TOTAL de la Solución Tigo Cloud AWS es un valor referencial, el cual puede variar en proporción de los consumos reales de los servicios.
- El consumo mensual se toma con base en la siguiente calculadora:

  https://calculator.aws/#/estimate?id=63793c7f2d6fc7f5f65398d07b5a5d620d91e437
- En el siguiente link se encuentra las certificaciones que tiene Tigo.

  https://partners.amazonaws.com/partners/0010h00001aDSU6AAO/Tigo%20Business
- No incluye impuesto de estampillas.

5.2. Condiciones Comerciales:

- Plazo de ejecución inicial de los servicios: 9 meses contados a partir de la activación de los servicios.
- El plan de horas puede ser consumido durante un periodo de tiempo de 3 meses, contados a partir de la fecha de contratación.
- 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 Privados, las ofertas presentadas en dólares americanos (USD) se facturará mensualmente en pesos colombianos; la conversión se realizará a la **TRM promedio mes**, publicada por el Banco de la República el mes anterior, como línea de tiempo, se tendrá la TRM asociada al mes de consumo del cliente.
- Para clientes del Sector Gobierno se facturará a la TRM de $ XXXX 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.
- En caso de que el Cliente no formalice en el plazo establecido la renovación de la Orden de Compra y/o Servicio o del contrato suscrito entre las partes, Tigo Prorrogará automáticamente por un período igual al contratado inicialmente.
- 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.

CC VND 00408528 2025 TR

Amazon Web Services, Inc. ■ 410 Terry Avenue North, Seattle, WA 98109-5210, U.S.A.

Bogotá, 22 de Septiembre de 2025

Tigo Business
Cr 48 No 20-45 El Poblado
Medellín, Antioquia 111111
Colombia

Re: Carta de Apoyo

A quien corresponda:

Amazon Web Services, Inc. (AWS) se complace en apoyar a Tigo Business en sus esfuerzos para ayudar a Ministerio de Comercio, Industria y Turismo en La adquisición de servicio en la nube para plataforma tecnologica de la ventanilla unica de Comercio exterior VUCE utilizando recursos informáticos en la nube de AWS. Esta carta confirma que Tigo Business hace parte del AWS Partner Network (APN) y que actualmente es un AWS Advanced Partner.

Tigo Business también tiene la(s) siguiente(s) Competencia(s) de AWS: Education Consulting; Government Consulting; Migration -Consulting and Storage - Consulting.

Tigo Business participa en los siguientes Programas de socios de AWS: Amazon EC2 for Microsoft Windows and AWS Direct Connect.

AWS ofrece servicios de informática que ayudan a las organizaciones a evitar la mayoría de las dificultades típicamente asociada con el lanzamiento y crecimiento de aplicaciones exitosas. Estos servicios se basan en la infraestructura de la tecnología de Amazon e incorporan más de una década y media de experiencia en la construcción de una de las infraestructuras web más confiable, escalable y rentable del mundo. El uso de AWS ofrece a los clientes acceso a expertos en computación distribuida a gran escala y permite que las aplicaciones sean robustas y escalables.

AWS valora y aprecia la oportunidad de apoyar a Tigo Business y esperamos una colaboración larga y productiva. Si usted tiene alguna pregunta o necesita información adicional, póngase en contacto con nuestro Partner Sales Manager, Angela María Gómez L, a amgomezl@amazon.com o +57 3105731180.

Amazon Web Services, Inc. ■ 410 Terry Avenue North, Seattle, WA 98109-5210, U.S.A.

Atentamente,

Amazon Web Services, Inc.



_____

Shannon Lowther
Senior Manager, Worldwide Public Sector Contract Management



Amazon Web Services, Inc. ▪ 410 Terry Avenue N. ▪ Seattle, WA 98109

September 22, 2025

SENT VIA EMAIL

Ministerio de Comercio, Industria y Turismo
Calle 28 No. 13 A – 15
Bogotá, Cundinamarca 110311
Colombia

Re: AWS Partner Network Membership Confirmation

To whom it may concern:

This letter confirms that Tigo Business has been an AWS Partner in the AWS Partner Network since April 9, 2016. Please see the AWS Partner Solutions Finder for more information regarding Tigo Business's AWS Validated Qualifications:

https://partners.amazonaws.com/partners/0010h00001aDSU6AAO/Tigo%20Business

This letter does not certify or endorse the Partner's proposed solution, its abilities to provide the proposed solution, or its fitness to be selected. Please do not hesitate to contact us should you have any questions.

Sincerely,



Amazon Web Services, Inc.

September 22, 2025