

Oferta Técnica y Comercial

Soluciones Digitales AWS

INSTITUCIÓN UNIVERSITARIA DIGITAL DE ANTIOQUIA - IU DIGITAL

business.tigo.com

tigo business

Medellín, 19 de Octubre

Señores
INSTITUCIÓN UNIVERSITARIA DIGITAL DE ANTIOQUIA - IU DIGITAL
Medellín

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,

tigo
Esteban Ríos Ángel
Ejecutivo de cuenta
Dirección Comercial Gobierno
Vp. de Empresas y Gobierno
esteban.riosa@tigo.com.co • (57) 310 461 60 98
Carrera 48 # 20-45 • Sede Principal • Piso 17 • Medellín - Colombia

AWS (Amazon Web Services) *4*

1. GENERALES 4

1.1. Propuesta de Valor 4

2. DESCRIPCIÓN DE LA PROPUESTA 5

2.1. Antecedentes 5

2.2. Descripción General de la Solución 5

2.3. Características destacadas: 6

2.4. Casos de uso: 6

2.5. Protección de servicios en AWS 7

2.5.1. Protección de instancias EC2 7

2.5.2. Protección de bases de datos RDS 7

2.5.3. Protección de Amazon DynamoDB 7

2.5.4. Protección de Amazon EFS 7

2.5.5. Protección de Amazon FSx 7

2.5.6. Protección de configuraciones VPC 8

2.6. Componentes de la solución 8

2.7. Topología General de la Solución 11

2.8. Consideraciones Técnicas del Servicio 11

2.9. Servicios Administrados 13

2.10. Servicios Profesionales 17

2.11. Acuerdos de Niveles de Servicio 18

2.13. Implementación y/o transición 19

3. ROLES Y RESPONSABILIDADES 21

4. ACUERDO DE CONFIDENCIALIDAD 24

5. OFERTA ECONOMICA 25

5.1. Servicios recurrentes: Tarifas mensuales de operación del servicio en AWS 25

5.2. Servicios por demanda: Tarifas mensuales de operación del servicio en AWS. 25

5.3. Servicios no recurrentes o de único pago 26

5.4. Condiciones Comerciales Tigo Cloud AWS Colombia 26

6. RECOMENDACIONES DE SEGURIDAD EN CLOUD 28

AWS (Amazon Web Services)

1. GENERALES

Amazon Web Services (AWS) es la plataforma en la nube más adoptada y completa en el mundo, que ofrece más de 230 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.

1.1. 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, Analítica, Asesoría en la migración de sus cargas de trabajo hacia la nube, gestión centralizada, entre otros. Además de ofrecer servicios profesionales y administrados con el objetivo de dar valor a nuestros Clientes y que ellos puedan centrarse en sus proyectos y crecimiento. Delegando a Tigo 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 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.

BaaS para AWS es la oferta de protección de datos de Tigo Business que permite a los clientes proteger sus cargas de trabajo en AWS con una solución diseñada específicamente para la nube, sin agentes en las instancias, integración nativa con los servicios de AWS, con respaldo por políticas, recuperación granular y capacidades de inmutabilidad para protección contra ransomware o recuperación ante desastres.

2.1. Antecedentes

El cliente **INSTITUCIÓN UNIVERSITARIA DIGITAL DE ANTIOQUIA, IU DIGITAL,** cuenta con infraestructura tecnológica desplegada en Amazon Web Services (AWS), compuesta por trece (13) instancias Amazon EC2, cuatro (4) instancias Amazon RDS con motor MySQL, con una capacidad total de almacenamiento productivo estimada de 2 TB.

Con el propósito de fortalecer la protección y disponibilidad de la información, así como reducir el riesgo de pérdida de datos ante fallas operativas, eliminación accidental, incidentes de seguridad u otros eventos que puedan afectar la continuidad del servicio, **IU DIGITAL** requiere implementar una solución de Backup, para la protección de sus cargas de trabajo alojadas en AWS.

Presentamos una solución de respaldo basada en Veeam Backup for AWS, complementada con servicios nativos de AWS para la protección de los buckets Amazon S3. La solución permitirá centralizar y automatizar la ejecución de los respaldos, administrar las políticas de retención, monitorear su correcta ejecución y facilitar la recuperación de la información y de los recursos protegidos.

2.2. Descripción General de la Solución

BaaS para AWS es una oferta integral de Tigo Business para la protección de datos en Amazon Web Services (AWS), que permite a los clientes proteger, gestionar y recuperar sus recursos de forma centralizada y automatizada.

La solución cubre el ciclo completo de respaldo, gestión y restauración de los principales servicios de AWS, proporcionando una estrategia de protección de datos consistente y simplificada.

Adicionalmente, BaaS para AWS permite unificar la protección de datos de entornos híbridos, integrando en una misma plataforma la protección de las cargas de trabajo on-premise y de nube pública AWS. Esto facilita la administración mediante políticas centralizadas, una gestión unificada y mayor flexibilidad para recuperar y restaurar los datos según las necesidades del negocio.

La solución está basada en Veeam, plataforma líder en gestión y protección de datos, y se complementa con las capacidades y experiencia de Tigo como Veeam Cloud Service Provider. De esta manera, Tigo Business impulsa una estrategia de protección de datos unificada, brindando a sus clientes una solución integral para sus entornos híbridos y de nube.

2.3. Características destacadas:

- **Servicio administrado:** Operación, monitoreo y gestión de la solución a cargo de Tigo Business.
- **Servicios profesionales:** Diseño, implementación, configuración y acompañamiento especializado.
- **Escalabilidad:** Crecimiento flexible de la capacidad de protección de acuerdo con las necesidades del cliente.
- **Protección contra ransomware:** Respaldos inmutables mediante **S3 Object Lock**, evitando su modificación o eliminación durante el periodo definido.
- **Protección basada en SLA:** Políticas de respaldo orientadas al **RPO**, con monitoreo y alertas para asegurar el cumplimiento de los objetivos definidos.
- **Integración con Veeam:** Gestión y visibilidad centralizada de los respaldos AWS, permitiendo copias adicionales, restauraciones y administración desde una consola unificada.
- **Optimización de costos**: Utiliza instancias de trabajo temporales que se activan solo durante las operaciones de copia de seguridad y se apagan inmediatamente después, minimizando así los costos de computación.
- **Retención flexible:** Permite el archivado a largo plazo mediante la estratificación de los datos de copia de seguridad en Amazon S3 Glacier y S3 Glacier Deep Archive.

2.4. Casos de uso:

La oferta BaaS para AWS de Tigo Business se basa en Veeam Data platform, desplegado como un appliance nativo dentro de la cuenta AWS del cliente. La solución permite gestionar y proteger de forma centralizada los principales servicios de AWS, incluyendo Amazon EC2, RDS, DynamoDB, EFS y FSx.

Tigo Business ofrece esta solución en dos modalidades, dependiendo de la infraestructura de respaldo existente y de las necesidades de gestión del cliente:

- ✓ **Standalone**

El appliance se despliega como una instancia independiente dentro de la cuenta AWS del cliente y es administrado por Tigo Business. Cuenta con su propia interfaz de gestión y permite configurar y administrar de forma autónoma las políticas de respaldo y recuperación.

Ideal para: clientes que no cuentan actualmente con infraestructura Veeam o que requieren una solución de protección para AWS independiente.

2.5. Protección de servicios en AWS

2.5.1. Protección de instancias EC2

Veeam Backup for AWS protege instancias EC2 mediante dos niveles complementarios:

- Snapshots en la nube: Copia a nivel de volumen EBS usando las APIs nativas de AWS. Rápido, sin intervención de workers, ideal como primera línea de protección con RPO corto.
- Image-level backups: Respaldo completo de la imagen de la instancia (todos los volúmenes EBS) en formato Veeam almacenado en un bucket S3. Permite recuperación granular, retención larga, compresión y deduplicación.

Para instancias con aplicaciones que requieren consistencia en caliente (SQL Server, Oracle, Exchange), Veeam soporta Application-Aware Processing (validación de la aplicación vía VSS/scripts) y Guest Scripting. Esto requiere conectividad SSH/WinRM entre el Worker y la instancia EC2.

Changed Block Tracking (CBT): Para los image-level backups incrementales, Veeam utiliza CBT basado en snapshots de EBS. Solo se transfieren al repositorio S3 los bloques que cambiaron desde el último respaldo, reduciendo el tiempo de backup y el costo de transferencia.

2.5.2. Protección de bases de datos RDS

Veeam Backup for AWS protege instancias RDS (MySQL, PostgreSQL, Oracle, SQL Server, MariaDB, Aurora) y Aurora Serverless mediante snapshots nativos RDS cross-account o cross-region, e image-level backups a S3 independientes del ciclo de vida de los snapshots nativos de AWS. Soporta restauración de instancia completa y de base de datos individual.

2.5.3. Protección de Amazon DynamoDB

Veeam Backup for AWS realiza backups de tablas DynamoDB exportando su contenido a S3 en formato Parquet. Permite backup programado por políticas, retención configurable independiente de los backups nativos de DynamoDB, y restauración de tabla completa o en nueva tabla.

2.5.4. Protección de Amazon EFS

Backup de sistemas de archivos EFS mediante copia de datos al repositorio S3, con indexación del contenido para recuperación a nivel de archivo, políticas de programación y retención configurables, y soporte de copia cross-region.

2.5.5. Protección de Amazon FSx

Soporte para FSx for Windows File Server, FSx for NetApp ONTAP, FSx for OpenZFS y FSx for Lustre. Backup mediante snapshot nativo y exportación al repositorio S3 de Veeam.

2.5.6. Protección de configuraciones VPC

Veeam Backup for AWS captura y almacena la configuración de red completa de las VPCs protegidas: subnets, route tables, security groups, NACLs, Internet Gateways, NAT Gateways, VPN connections, peering connections. Permite restaurar la configuración completa o elementos individuales, y comparar estados de configuración entre puntos de restauración para auditoría y troubleshooting.

2.6. Componentes de la solución

A continuación, se describen los principales componentes de la solución BaaS para AWS:

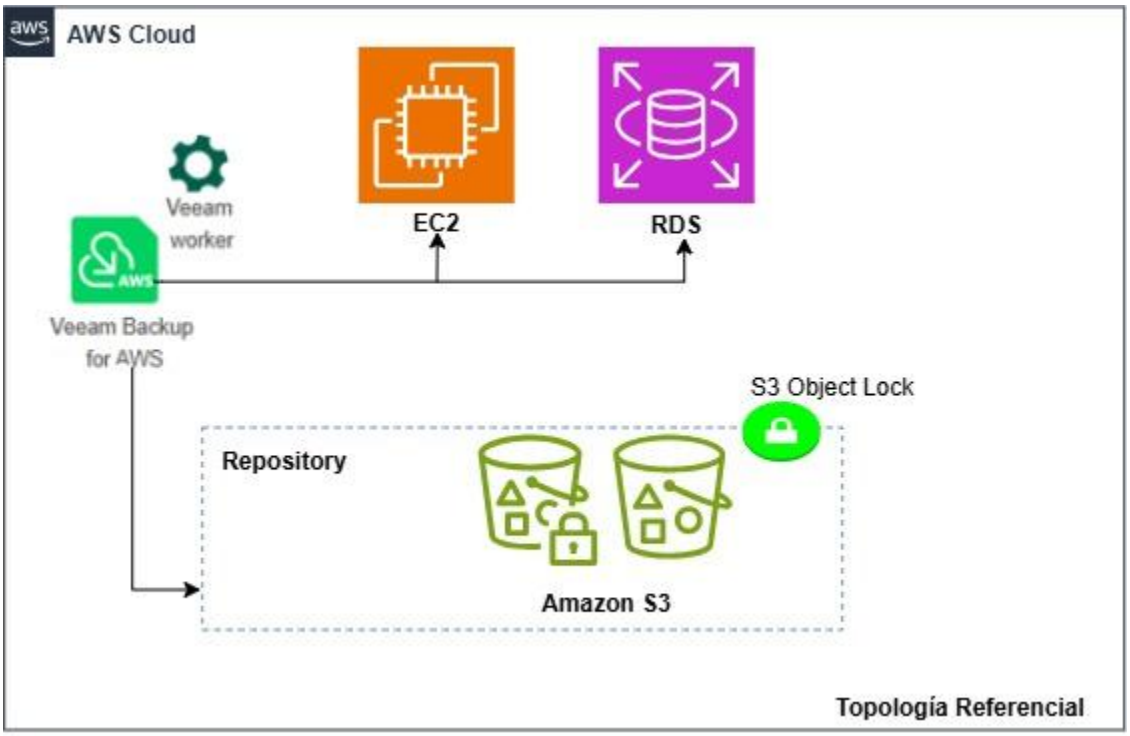
Servicio	Descripción Propuesta	Resumen de la configuración
Data Transfer	Servicio que facilita la transferencia segura y eficiente de datos entre entornos on-premises e infraestructura AWS, así como entre regiones y servicios cloud. Proporciona múltiples métodos de ingesta incluyendo conexiones de red, dispositivos físicos y APIs, optimizando la migración de cargas de trabajo y garantizando integridad de datos durante el proceso. **Para más información ingresar al siguiente enlace:** https://aws.amazon.com/es/datasync/	• Descripcion: Data Transfer Out • DT Inbound: Internet (1 TB per month) • DT Outbound: Internet (5 TB per month) • DT Intra-Region: (0 TB per month)
Amazon EC2	Servicio de computación en la nube que proporciona capacidad de procesamiento escalable bajo demanda. Permite provisionar instancias virtuales configurables con diferentes características de CPU, memoria y almacenamiento. Ofrece flexibilidad en sistemas operativos, modelos de pago y opciones de red. Integrable con otros servicios AWS para construir arquitecturas robustas y resilientes en entornos empresariales. **Para más información ingresar al siguiente enlace:** https://aws.amazon.com/es/ec2/	• Descripcion: Appliance de Veeam Backup for AWS • Tenencia (Instancias compartidas) • Sistema operativo (Linux) • Workload (Consistent • Number of instances: 1) • Instancia EC2 por adelantado (t3.medium) • Pricing strategy (On-Demand Utilization: 100 %Utilized/Month) • Habilitar la monitorización (enabled) • EBS Cantidad de almacenamiento (200 GB) • DT Inbound: Not selected (0 TB per month) • DT Outbound: Not selected (0 TB per month) • DT Intra-Region: (0 TB per month) • vCPU: 2 • RAM: 4 GiB
S3 Standard	Servicio de almacenamiento de objetos altamente disponible y duradero diseñado para casos de uso general. Proporciona acceso inmediato a datos con redundancia automática en múltiples zonas de disponibilidad. Ideal para aplicaciones web, análisis de datos, respaldo y recuperación ante desastres. Ofrece durabilidad excepcional, escalabilidad sin límites y control granular de acceso mediante políticas de seguridad. **Para más información ingresar al siguiente enlace:** https://aws.amazon.com/es/s3/	• Descripcion: Bucket para almacenamiento • Almacenamiento de S3 Estándar (5 TB por mes) • Solicitudes PUT • COPY • POST y LIST a S3 Standard (10000) • Solicitudes GET • SELECT y todas las demás desde S3 Estándar (10000) • Datos devueltos por S3 Select (10 GB por mes) • Datos escaneados por S3 Select (10 GB por mes)

Amazon EC2	Servicio de computación en la nube que proporciona capacidad de procesamiento escalable bajo demanda. Permite provisionar instancias virtuales configurables con diferentes características de CPU, memoria y almacenamiento. Ofrece flexibilidad en sistemas operativos, modelos de pago y opciones de red. Integrable con otros servicios AWS para construir arquitecturas robustas y resilientes en entornos empresariales. **Para más información ingresar al siguiente enlace:** https://aws.amazon.com/es/ec2/	• Descripcion: Worker • Tenencia (Instancias compartidas) • Sistema operativo (Linux) • Carga de trabajo (Consistent • Cantidad de instancias: 1) • Instancia EC2 por adelantado (m5.large) • Pricing strategy (On-Demand Utilization: 10 Hours/Month) • Habilitar la monitorización (habilitado) • EBS Cantidad de almacenamiento (200 GB) • DT Entrada: Not selected (0 TB al mes) • DT Salida: Not selected (0 TB al mes) • DT Intra-región: (0 TB al mes) • vCPU: 2 • RAM: 8 GiB
Amazon CloudWatch	Servicio de observabilidad y monitoreo completamente administrado que recopila, visualiza y analiza métricas, registros y eventos desde recursos e infraestructura en AWS. Proporciona dashboards personalizables, alarmas inteligentes y capacidades de troubleshooting para optimizar rendimiento, disponibilidad y salud operacional de aplicaciones y sistemas distribuidos. **Para más información ingresar al siguiente enlace:** https://aws.amazon.com/es/cloudwatch/	• Descripcion: CloudWatch • Número de eventos de OTEL móvil y spans • o spans por visita (70) • Frecuencia de muestreo móvil (1) • Cantidad de métricas (incluye las métricas personalizadas y detalladas) (30) • GetMetricData: cantidad de métricas solicitadas (10) • GetMetricWidgetImage: cantidad de métricas solicitadas (10) • Cantidad de otras solicitudes de API (10)
AWS CloudTrail	Servicio de auditoría y registro que captura llamadas API realizadas en una cuenta AWS. Proporciona visibilidad completa sobre acciones de usuarios, aplicaciones e integración de servicios. Genera logs detallados con información de quién, qué, cuándo y dónde se ejecutaron operaciones. Facilita cumplimiento normativo, investigación de seguridad y análisis forense en infraestructuras cloud. **Para más información ingresar al siguiente enlace:** https://docs.aws.amazon.com/es_es/awscloudtrail/latest/userguide/cloudtrail-user-guide.html	• Descripcion: CloudTrail • Unidades de eventos de administración (millones) • Registros de eventos de administración (1) • Registros de seguimiento de administración de lectura (1) • Unidades de eventos de datos (millones) • Registros de seguimiento de S3 (1) • Registros de seguimiento de Lambda (1) • Unidades de eventos de actividad de red (millones) • Rutas de eventos de actividad en la red (1)

		• Unidades de eventos de Insights (millones) • Número de rutas o almacenes de datos de eventos en los que están activados los eventos de Insights (1) • Número de eventos de administración (10 por mes) • Eventos de administración de lectura (10 por mes) • Operaciones de S3 (10 por mes)
AWS Config	Servicio de gobernanza que proporciona visibilidad continua sobre la configuración de recursos en tu infraestructura cloud. Permite auditar cambios, evaluar cumplimiento normativo mediante reglas personalizables y mantener un inventario detallado de activos. Facilita la detección de desviaciones de configuración y genera reportes para asegurar conformidad con políticas organizacionales y estándares de seguridad. **Para más información ingresar al siguiente enlace:** https://docs.aws.amazon.com/es_es/config/latest/developerguide/	• Descripcion: Config • Número de elementos de configuración continua registrados (10) • Número de elementos de configuración periódica registrados (10) • Número de evaluaciones de las reglas de configuración (10) • Número de evaluaciones del paquete de conformidad (10000)

Nota: El alcance definido en el presente documento se limita estrictamente a lo expresamente ofertado y descrito en esta propuesta.

2.7. Topología General de la Solución



El diseño presentado es una arquitectura de alto nivel que tiene como objetivo reflejar el alcance general de la solución propuesta. Este diseño puede estar sujeto a modificaciones en función de las soluciones y requisitos específicos.

2.8. Consideraciones Técnicas del Servicio

- La integración con VBR es opcional. Veeam Backup for AWS funciona de forma completamente autónoma a través de su propia interfaz web.

- Principio de privilegio mínimo: Los roles IAM del Appliance, Workers y repositorios deben seguir el principio de menor privilegio. Veeam proporciona plantillas de políticas IAM predefinidas para cada función.

- Los Worker Instances son instancias EC2 temporales que Veeam Backup for AWS despliega automáticamente al inicio de cada operación de respaldo o restauración, y termina al finalizar el trabajo. Su función principal es ejecutar el procesamiento de datos, leen los snapshots de EBS adjuntos a la instancia EC2 de origen, realizan compresión y deduplicación de bloques, y transfieren los datos procesados al repositorio de respaldo (bucket S3).

- Por defecto, los Workers se comunican con S3 y otros servicios AWS a través de internet. Para entornos con restricciones de red:
    - Configurar VPC Interface Endpoints para los servicios consumidos por Veeam: s3, ec2, sts, ssm, secretsmanager

- Configurar VPC Peering entre la VPC de la Cuenta de Backup y las VPCs de las cuentas de producción para que los Workers accedan al repositorio S3 sin salir a internet
- Activar la opción Private Network Deployment en el Appliance para que Veeam no intente usar IPs públicas.

- Cifrado en reposo: Los repositorios S3 deben usar SSE-KMS con claves CMK administradas por el cliente (no claves AWS-managed). Esto permite control explícito sobre rotación y acceso a las claves.

- Antes de comenzar a utilizar el complemento Veeam para AWS, tenga en cuenta los siguientes requisitos: https://helpcenter.veeam.com/docs/vbr/userguide/aws_planning_and_preparation.html?ver=13

- Los dispositivos de copia de seguridad utilizan los permisos de los roles de IAM para acceder a los servicios y recursos de AWS, y para realizar las operaciones de copia de seguridad y restauración.

- Solo se pueden implementar dispositivos de respaldo dentro de una única zona de disponibilidad.

- El tipo de instancia EC2 mínimo recomendado para el dispositivo de copia de seguridad es t3.medium , y la arquitectura AMI compatible es x86_64. Para ver la lista de todos los tipos de instancia existentes.

- Para acceder a la interfaz web del dispositivo de copia de seguridad, utilice Microsoft Edge (última versión), Mozilla Firefox (última versión) o Google Chrome (última versión). Internet Explorer no es compatible.

- Los buckets de Amazon S3 con S3 Object Lock y S3 Versioning habilitados solo se pueden usar para crear repositorios de copias de seguridad con la configuración de inmutabilidad habilitada.

- Si habilita el bloqueo de objetos S3 para un bucket que ya se utiliza como ubicación de destino para copias de seguridad a nivel de imagen, el dispositivo de copia de seguridad no podrá seguir creando copias de seguridad ni almacenándolas en un repositorio de copias de seguridad existente.

- Todos los servicios protegidos por Veeam Backup para AWS requieren de una licencia por carga de trabajo protegidas, a continuación, se muestran las unidades de puntos por carga para el licenciamiento: https://helpcenter.veeam.com/docs/vcsp/refguide/public_cloud_workloads.html

- De acuerdo con el servicio a proteger en AWS se sugiere revisar los siguiente restricciones y limitaciones:https://helpcenter.veeam.com/docs/vbr/userguide/aws_limitations.html?ver=13

- No se pueden mezclar licencia del cliente en modalidad VUL (Veeam Universal License) en premisas con licencias licencias de alquiler (Rental) de VCSP (Veeam Cloud & Service Provider (VCSP) de Tigo en un mismo Veeam Backup and Replication console. Esto para el caso en el cual se quiera realizar una integración del VBR local con el appliance de Veeam for AWS.

2.9. Servicios Administrados

Tigo Business agrega valor a la oferta de AWS, al proporcionar Servicios Administrados de Tigo Business (SATIGO) que realizan gestión y supervisión continua de la infraestructura y de los servicios en la nube de AWS, por parte de expertos técnicos de Tigo Business. Operan bajo un modelo colaborativo en el que Tigo aporta experiencia técnica, procesos y herramientas, mientras el Cliente aporta el contexto de negocio, las decisiones y la propiedad de sus aplicaciones y datos.

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

Estos servicios en sus diferentes planes 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.

Gestión de Incidentes: SATIGO detecta, clasifica y acompaña la resolución de incidentes sobre la infraestructura AWS del Cliente. El equipo responde de forma proactiva y trabaja junto al Cliente para restablecer la operación en el menor tiempo posible. Los ingenieros especialistas están disponibles 24x7 a través del canal de soporte.

Monitoreo: SATIGO realiza seguimiento continuo a los recursos AWS del Cliente. Las cuentas incorporadas al servicio son configuradas con una línea base de alertas y gestión de eventos en AWS CloudWatch, optimizada para notificar únicamente las alertas de mayor relevancia operativa. Ante una alerta, el equipo actúa mediante notificaciones al Cliente, remediaciones automáticas preaprobadas y/o intervención de ingenieros de soporte, con el objetivo de restablecer los recursos dentro de los umbrales establecidos.

Gobierno de nube: Las cuentas AWS del Cliente son incorporadas en una organización, propia o multicliente, bajo la supervisión de AWS Control Tower, donde se establecen controles preventivos y de detección (GuardRails) basados en las políticas de seguridad del Centro de Excelencia de Tigo (CCoE).

Aseguramiento: SATIGO evalúa, audita y supervisa continuamente las cuentas AWS del Cliente para comprobar si cumplen las mejores prácticas de seguridad, a través de un proceso estructurado. Se

realizan análisis técnicos periódicos sobre la infraestructura desplegada, identificando oportunidades de mejora alineadas a las mejores prácticas publicadas por AWS. Como resultado SATIGO entrega un informe de evaluación de postura de seguridad, que identifica desviaciones frente a las mejores prácticas y estándares de seguridad reconocidos en la industria, acompañado de recomendaciones priorizadas y planes de remediación.

Gestión de actualizaciones de seguridad: TIGO y el Cliente definen los procedimientos, calendarios y periodicidad de actualizaciones, aportando las mejores prácticas para una instalación controlada que minimice riesgos y garantice la posibilidad de rollback. El alcance de la gestión de actualizaciones se realiza a través de la consola de AWS Patch Manager, este acompañamiento cubre únicamente parches de seguridad clasificados como críticos y altos. y está sujeta a las siguientes condiciones:

- Las instancias deben ejecutar sistemas operativos soportados por AWS, con actualizaciones vigentes disponibles directamente desde el fabricante del sistema operativo.
- El agente de AWS Systems Manager (SSM) debe estar instalado y operativo en cada instancia a gestionar.

Gestión de copias de seguridad: Se crean, monitorizan y almacenan copias de respaldo para los servicios de AWS compatibles con AWS Backup. El Cliente es responsable de definir los programas de respaldos, la frecuencia y el periodo de retención mediante la creación de planes de AWS Backup en el momento de la incorporación de la cuenta.

Para los procesos de parchado, monitoreo, copias de seguridad y gestión de incidentes, es necesario que el Cliente cuente con el etiquetado de recursos y la instalación de los agentes de SSM y CloudWatch en cada una de las instancias EC2, así como, un IAM Instance Profile que autorice la interacción con estos servicios.

Recomendaciones para Optimización de costos: SATIGO puede ayudar a reducir los costos operativos, automatizando el inicio y la detención de instancias de Amazon Elastic Compute Cloud (Amazon EC2), instancias de Amazon Relational Database Service (Amazon RDS) y grupos de Amazon EC2 Auto Scaling, según las necesidades del Cliente, quien es responsable de indicar los periodos en los que se deben detener e iniciar los servicios.

Registros y Reportes: SATIGO pone a disposición del cliente los registros generados como resultado de operaciones en CloudWatch y CloudTrail hasta por 90 días, de acuerdo con la configuración por defecto de cada uno de estos servicios. Información relevante para resolver incidentes y auditorías del sistema. SATIGO proporciona un informe de servicio, de acuerdo con el plan contratado de Servicios Administrados, que resume las métricas de rendimiento clave, métricas operativas, recursos administrados e informes de aseguramiento con optimización de costos, ahorros y recomendaciones técnicas relevantes.

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

Para Esta oferta se incluye el servicio administrado ENTERPRISE:

	Enterprise
Gestión de Servicio	* Gestión de incidentes y requerimientos * Respaldo y restauración con el servicio de AWS Backup * Reporte de Cumplimiento y Respaldo: Actualizaciones y parches pendientes de seguridad en Sistema operativos soportados en AWS System Manager. Reporte de Recursos (EC2, RDS) sin Copias de Respaldo * Informe de Aseguramiento: Seguridad y Costos Periodicidad: Semestral
Monitoreo	* Reportes de servicio del (ejecución de respaldos, incidentes/requerimientos, métricas de infraestructura para los servicios contratados) * Gestión proactiva de alarmas y eventos (CloudWatch, Personal Health Dashboard, Cost Anomaly Detection)
Aseguramiento de la cuenta y Mejora Continua	* Gestión de usuarios (Identity Center Gestionado por Tigo) * Socialización de Hallazgos en Seguridad y acompañamiento en la remediación * Socialización de Hallazgos de Optimización de Costos y acompañamiento en la aplicación
Seguridad - Gestión de Identidades y Accesos	* Gestion de AWS IAM * Aplicación de SCPs estándar * Gestión de AWS Identity Center
Seguridad - Detección de Amenazas y Monitoreo	* Gestión de GuardDuty * Gestión de Security Hub * Gestión de estándares de seguridad en Security Hub * Gestión de Inspector v2 * Priorización y gestión de hallazgos por severidad * Notificación de hallazgos críticos y de alta severidad
Seguridad - Protección de Datos y Cifrado	* Verificación de cifrado en reposo (S3, EBS, RDS, etc.) – Semestral * Verificación de cifrado en tránsito (TLS/HTTPS) - Semestral * Gestión de certificados con AWS ACM

Seguridad - Cumplimiento, Auditoría y Gobernanza	* Configuración básica de AWS Config multi-cuenta * Configuración organizacional de CloudTrail multi-cuenta * Verificación de integridad y cobertura de CloudTrail * Biblioteca estándar de reglas de AWS Config * Supervisión de cumplimiento de reglas Config baseline * Notificación de infracciones críticas de Config * Supervisión de Control Tower y Landing Zone
Seguridad - Respuesta a Incidentes y Automatización	* Notificaciones de incidentes de seguridad * Contención básica reactiva con aprobación del cliente * Coordinación de restauración con AWS Support * Reporte post-incidente (RCA básico) * RCA completo con recomendaciones de mejora * Runbooks/Playbooks de respuesta documentados

Soporte AWS (fábrica)

Tigo incluye como parte del servicio administrado el manejo de tickets de AWS Support en nombre del cliente. El cliente puede solicitar Business Support o Enterprise Support según necesidad, sumándose al costo base del servicio Tigo (No incluido en esta propuesta).

2.10. Servicios Profesionales

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.
- 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.

Servicio	Alcance	Actividad
AWS Backup	Configuración de respaldos de acuerdo con la necesidad del Cliente teniendo en cuenta el alcance del servicio: instancias de Amazon Elastic Compute Cloud (EC2), los volúmenes de Amazon Elastic Block Store (EBS), las bases de datos de Amazon Relational Database Service (RDS), las tablas de Amazon DynamoDB, los sistemas de archivos de Amazon Elastic File System (EFS), los sistemas de archivos de Amazon FSX y los volúmenes de AWS Storage Gateway.	Configuración plataforma
S3	Creación de bucket de S3 de acuerdo con la solicitud del Cliente.	Configuración plataforma
VPC	Creación de un VPC con el direccionamiento indicado (o el sugerido) y las subredes respectivas requeridas para la aplicación.	Configuración plataforma
AWS CloudWatch	Configuración de servicio AWS CloudWatch para monitoreo de servicios de cómputo (CPU, Memoria, Discos), redes (Data transfer, estado VPN, Estado Direct-Connect), entre otros.	Configuración plataforma
	Configuración de Alarmas de notificación mediante SNS para los monitoreos anteriormente mencionados.	Configuración plataforma
	Configuración de Alarmas para integrar con los servicios de Auto-Scaling, Lambda	Configuración plataforma
AWS CloudTrail	Habilitación del servicio de CloudTrail sobre la cuenta del Cliente para tener trazabilidad de eventos y configuraciones que se ejecuten sobre está.	Configuración plataforma
AWS Config	Habilitación del servicio de Config sobre la cuenta del Cliente para tener trazabilidad del inventario y cambios en la infraestructura en servicio.	Configuración plataforma

2.11. 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

Las solicitudes de cambios o requerimientos de información ingresados fuera del horario hábil serán gestionadas a partir del inicio del siguiente día hábil. Solo los Incidentes Altos y requerimientos Altos y Críticos (Afectación total del servicio productivo) activarán el protocolo de disponibilidad 7x24.

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/

Los Ans por indisponibilidad los aplica Amazon automáticamente de acuerdo con el ANS comprometido con cada servicio.

2.12. 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.

2.13. Implementación y/o transición

Para llevar a cabo el proceso de entrega de la solución contratada por el Cliente, Tigo Business asignará 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, liderará 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.

Dará 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.

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

	Hito
1	Aceptación de la oferta por parte del Cliente
2	Asignación de Gerente de Proyecto
3	Revisar Documentación MF - EDT - Matriz de interesados- riesgos- Factibilidades- SOW
4	Realizar Empalme Ing. Preventa
5	Realizar presentación KickOff interno
6	Solicitar requerimientos internos
7	Realizar presentación KickOff externo
8	Configuración Solución Cloud AWS
9	Entrega Cliente
10	Facturación de los Servicios
11	Entrega servicio

La duración del proyecto se estima 30 días hábiles a partir de la firma de contrato y ejecución de Kick-off con el Cliente y áreas involucradas.

Consideraciones Entrega de servicio

- 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.
- 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.
- En todos los casos, se realizará el mejor esfuerzo posible para la implementación de la solución en el menor tiempo posible.
- No se consideran los tiempos imputables a las adecuaciones internas o aspectos técnicos o de servicio bajo la responsabilidad del Cliente en sus sedes o Data Center.
- El Cliente en la reunión de inicio debe indicar a Tigo, si el email de acceso a la cuenta root va a pertenecer al cliente o si se puede usar un email con dominio de Tigo. En caso de ser cuenta con dominio del Cliente (123@cliente.com) debe proporcionar los correos electrónicos para la creación de las cuentas enlazadas.

3. ROLES Y RESPONSABILIDADES

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).

A continuación, se presenta 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) o infraestructura como servicio (IaaS):



**Depende del plan de servicios administrados contratado*

Esquema basado en el modelo de responsabilidad compartida de AWS:

Responsabilidad de Tigo Business

- Habilitar / configurar recursos de infraestructura y servicios contratados por el Cliente.
- Validar que los servicios aprovisionados estén activos y 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.

Responsabilidades del Cliente

- Garantizar el suministro, exactitud y veracidad de 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.
- Tigo Business proporcionará accesos a la infraestructura de nube y el Cliente será responsable de su uso y protección y asumir la responsabilidad ante la perdida, robo o mal uso de accesos brindados
- En caso de filtración o perdida de accesos, el Cliente es responsable de solicitar la eliminación o actualización de credenciales.
- EL CLIENTE deberá informar formalmente a Tigo Business las personas autorizadas para acceder a los servicios contratados y para solicitar soporte técnico, cambios o requerimientos asociados a estos. Asimismo, será responsable de notificar oportunamente cualquier modificación de dicho personal. Tigo Business se reserva el derecho de revocar o restringir accesos cuando identifique usos indebidos o situaciones que representen un riesgo para los servicios prestados, la infraestructura administrada o cualquier entidad perteneciente a su grupo empresarial.
- 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).
- Verificar la correcta aplicación de configuraciones que Tigo Business aplique a los servicios aprovisionados acorde a los requerimientos entregados por el Cliente.
- El Cliente es el único responsable de sus equipos informáticos y conexión necesarios para conectarse o acceder a sus servicios en la nube de AWS, si el Cliente cuenta con servicios de datos o internet adquiridos a través de Tigo Business, estos serán contratos totalmente independientes.
- Es responsabilidad del Cliente garantizar que los sistemas se encuentren libres de virus, spam o cualquier otro programa malicioso. El Cliente deberá contar con mecanismos adecuados de protección, detección y mitigación de amenazas de seguridad informática. En caso de no disponer de dichas herramientas, podrá contratar los servicios correspondientes con Tigo Business. 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.
- El Cliente debe declarar y garantizar que es titular del nombre de dominio de internet que utiliza, 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 declara y garantiza que es titular o cuenta con las licencias, autorizaciones y derechos necesarios para el uso del software, bases de datos y demás contenidos que incorpore a los servicios contratados.
- 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.
- 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 será el único responsable de garantizar no 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 es el único responsable ante Tigo Business y sus empresas afiliadas y se compromete a indemnizarle por todos los daños y perjuicios, intereses y denuncias en las que Tigo Business o sus empresas afiliadas o los terceros contratados pudieran verse afectadas por demandas, o reclamación de un tercero interpuesta como consecuencia de una infracción del Cliente de las obligaciones que contrae.

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

5. OFERTA ECONOMICA

Esta propuesta estará vigente por treinta (30) días calendario contados a partir de la fecha de presentación, y anula otras propuestas presentadas con anterioridad al Cliente en este mismo sentido.

5.1. Servicios recurrentes: Tarifas mensuales de operación del servicio en AWS

El valor recurrente mensual de la Solución AWS de Tigo Cloud y Servicios Administrados Tigo es un valor de referencial, el cual puede variar en proporción de los consumos reales de cada mes.

Servicio	Tarifa Mensual Sin IVA	IVA (19%)	Tarifa Mensual Con IVA
Servicios AWS	$ 2.875.560	$ 0	$ 2.875.560
Servicios Administrados Tigo (Enterprise)	$ 431.334	$ 81.953	$ 513.287
Licencias Veeam (17)	$ 575.385	$ 0	$ 575.385
Total	**$ 3.882.279**	**$ 81.953**	**$ 3.964.232**

* La facturación del **Servicios Administrado AWS Enterprise** es el **15%** del consumo mensual de servicios en AWS, por lo cual puede variar mensualmente.

** El valor mensual en COP es un valor referencial y no corresponde al valor de facturación, debido a que la facturación se realizará con la TRM correspondiente cada mes y el consumo real del servicio.

Nota: La inclusión del servicio Soporte AWS es opcional y queda a discreción del Cliente, permitiéndole decidir si lo incluye o no en función de sus necesidades, sin embargo, Tigo Business recomienda su contratación para tener beneficios como acceso las 24 horas del día, los 7 días de la semana a soporte técnico y orientación arquitectónica de sus casos de uso específicos, directamente con AWS (No se incluye en esta propuesta).

5.2. Servicios por demanda: Tarifas mensuales de operación del servicio en AWS.

El componente Worker contemplado en la presente solución se implementa bajo un esquema de uso temporal (On Demand), activándose únicamente durante la ejecución de tareas de respaldo, restauración o mantenimiento programado. En consecuencia, el cliente pagará exclusivamente por el tiempo efectivo de utilización del recurso. El valor presentado a continuación corresponde a una

estimación referencial basada en un consumo promedio de 10 horas mensuales, el cual podrá variar de acuerdo con la frecuencia de ejecución de los trabajos y los requerimientos operativos de la plataforma.

Valores Recurrentes Mensual					
Producto	**Nombre Producto**	**Detalle**	**Valor Mensual sin IVA (COP)**	**Valor IVA (COP)**	**Valor Mensual con IVA (COP)**
Servicios AWS Por Demanda	Amazon EC2	Worker	$ 12.880	$ 0	$ 12.880

5.3. Servicios no recurrentes o de único pago

Servicio	Pago Único	IVA (19%)	Total
Despliegue servicios de AWS	$ 6.548.100	$ 1.244.139	$ 7.792.239

** El valor en COP es un valor referencial y no corresponde al valor de facturación. La facturación se realizará con la TRM correspondiente para cada mes.

5.4. Condiciones Comerciales Tigo Cloud AWS Colombia

- Plazo de ejecución inicial de los servicios: 12 meses contados a partir de la activación de los servicios.
- La facturación al Cliente se calculará con base en los consumos efectivamente generados desde el momento en que los recursos sean aprovisionados, es decir, desde su creación en la plataforma AWS - Tigo y hasta el desaprovisionamiento o eliminación de los servicios en AWS -Tigo, último día de actividad de acuerdo con lo establecido en el contrato suscrito con Tigo Business.
- El valor mensual indicado en la presente Oferta Comercial es referencial, dado que incluye servicios Cloud AWS y Servicios Administrados cuya facturación se basa en el consumo real registrado. En consecuencia, el valor facturado podrá variar mensualmente de acuerdo con dicho consumo.
- Para Clientes Privados, las ofertas comerciales se presentan en dólares estadounidenses (USD) y serán facturadas mensualmente en pesos colombianos (COP). La conversión se

efectuará utilizando la TRM promedio del mes anterior, publicada por el Banco de la República, la cual se aplicará a los consumos generados durante el período de facturación correspondiente

- Para Clientes del Sector Gobierno se facturará a la **TRM de $ 4.000 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 mensual publicada por el Banco de la República correspondiente al mes en que se hayan consumido los servicios presenta una variación igual o superior al cinco por ciento (5 %) con respecto a la TRM acordada, esta se ajustará proporcionalmente a dicha variación para efectos de la facturación de los servicios consumidos.
- Cuando EL CLIENTE cuente con permisos para realizar cambios sobre los Servicios Cloud AWS, será responsable de los impactos que dichos cambios generen en el desempeño, la disponibilidad y los costos asociados a los recursos consumidos. Cualquier incremento en el consumo o en los costos derivado de estos cambios será asumido por EL CLIENTE, quien deberá gestionar las aprobaciones presupuestales que resulten necesarias.
- 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.
- Tigo no será responsable por las modificaciones que AWS o terceros que comercialicen servicios a través de AWS realicen sobre sus productos o servicios, incluyendo cambios en alcance, precios, condiciones comerciales, disponibilidad, funcionalidades o cualquier otra característica. Dichas modificaciones se regirán por las políticas y condiciones aplicables a la comercialización o reventa de servicios de AWS o del proveedor correspondiente.
- Cualquier servicio o solicitud que no esté claramente especificado en este documento se encuentran por fuera del alcance.
- 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
- La presente oferta asume 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. Cualquier cambio adicional sobre el dimensionamiento de la solución está sujeto a viabilidad técnica y económica durante la fase de Implementación.
- 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.
- 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.

- Para el traslado de los servicios (on-boarding /off-boarding) del APN de Tigo, AWS maneja un calendario mes con fechas limite donde se puede hacer estas actividades dependiendo de si es una organización o cuenta individual. Por lo tanto, el cliente debe solicitar el retiro o no renovación del servicio de AWS al menos con una antelación de 30 días considerando las fechas o requisitos de AWS para el desarrollo de este proceso.
- 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.

6. RECOMENDACIONES DE SEGURIDAD EN CLOUD

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

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

Servicios de Gestión de Infraestructura:

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

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

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

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

Compartimos un listado de buenas prácticas para un entorno seguro

- ✓ Autenticación multifactor (MFA): Actívela siempre que sea posible.
- ✓ Reglas de firewall y acceso restringido a solo su organización: Defina listas blancas de IP y aplique controles de seguridad estrictos.

- ✓ Cifrado obligatorio: Asegure que todas las conexiones usen TLS/SSL.
- ✓ Auditorías periódicas: Identifique y corrija vulnerabilidades antes de que sean un problema.
- ✓ Antivirus/EDR: Ayuda significativamente a la continuidad operativa al prevenir secuestros de datos (ransomware) y ataques a nivel SO, ayuda a proteger la integridad de su información crítica, asegurando el cumplimiento legal y evitando pérdidas financieras por fugas de datos.

Importancia de los Respaldos Periódicos:

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

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

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

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

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