

Oferta Técnica y Comercial

Soluciones Digitales AWS

INSTITUCIÓN UNIVERSITARIA DIGITAL DE ANTIOQUIA - IU DIGITAL

Renovación Acta 27

business.tigo.com

tigo business

Medellín, 18 de junio de 2026

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,

Andrés Trujillo Mestra
Ejecutivo de Cuenta
Dirección Comercial Gobierno
Vp. De Negocio de Empresas y Gobierno
victor.trujillo@tigo.com.co • (57) 300 774 31 63
Carrera 48 # 20-45 • Sede Principal • Piso 15 • Medellín - Colombia

AWS (Amazon Web Services)

1. GENERALES

Amazon Web Services (AWS) es la plataforma en la nube más adoptada1 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.

[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 cliente **INSTITUCIÓN UNIVERSITARIA DIGITAL DE ANTIOQUIA - IU DIGITAL** 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 una solución con las siguientes características.

- **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.
- **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.

- **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. 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.

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.

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:

2.3.1 IaaS o Infrastructure As a Service:

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

2.3.2 DRaaS o Disaster Recovery As a Service

AWS Elastic Disaster Recovery es un servicio de recuperación de desastres escalable y rentable el cual se utiliza para ayudar a mantener la continuidad del negocio en caso de un desastre natural o humano a nuestros Clientes. Este servicio ofrece una amplia gama de escenarios y dominios de falla para garantizar que las empresas puedan recuperar sus aplicaciones y datos en caso de un desastre.

Además, AWS Elastic Disaster Recovery es escalable y rentable, lo que significa que solo pagan por el sitio de recuperación de desastres cuando es necesario. Esto con el fin de optimizar costos al eliminar los recursos inactivos del sitio de recuperación de desastres.

AWS Elastic Disaster Recovery admite la replicación de datos a través de una variedad de canales, incluidos Amazon S3, Amazon EBS y Amazon RDS. La elección del canal de datos adecuado dependerá de las necesidades específicas de la empresa y de la aplicación en cuestión.

2.4. Servicios Administrados

2.5. Servicios administrados de Infraestructura

La presente incluye la renovación de los servicios administrados **Enterprise**, los cuales se encuentran actualmente contemplados en el contrato *AT_2026_06_Renovacion_Acta_27_AWS_Actas_Anteriores_Contrato_AM-044539-65_Jul_2026_Jul_2027*

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. 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

Categoría	ítem	Enterprise
		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 * Habilitación / Deshabilitación 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. Configuraciones 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

Categoría	ítem	Enterprise
		caso de soporte con AWS para las AMI con licenciamiento incluido.
	Gestión de actualizaciones de seguridad - Periodicidad	Semestral
Aseguramiento de la cuenta y mejora continua	Refuerzo de controles	Implementación de biblioteca seleccionada de reglas de AWS Config. (Notificación)
	Gestión de accesos y usuarios	Si, siempre y cuando el IdP sea gestionado por Tigo
Gestión de servicio	Respaldo y restauración	Configuración de respaldos y restauración (AWS Backup) de acuerdo con la línea base. En caso de negativa por parte del Cliente entregara la correspondiente carta de riesgo
Registros operacionales, Monitoreo, y Reportes	Reportes de gestión (incidentes/requerimientos,)	A demanda
	Administración de bases de datos	Revisar numeral 2.4.1
	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

2.4.1 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

ítem	Enterprise
Pruebas de restauración Backup	1 semestral
Entrega de reporte	1 mensual
Ajuste de recursos	Aplica
Ajustes o cambios esquema de Backup	Aplica
Ampliación de recursos	Aplica
Análisis de métricas y registros	Aplica
Cambio de plan (aplica para cambio de capacidad en el servicio)	Aplica
Cancelación de Bloqueos	Aplica
Configuración de alertas	Aplica
Configurar políticas de copia de seguridad automatizadas para realizar copias de seguridad regulares y programadas	Aplica
Configurar y monitorear alta disponibilidad y replicación	Aplica
Acompañamiento en Creación de BD	Aplica
Creación de puntos de restauración	Aplica
Creación y monitoreo de cuentas y roles de bases de datos	Aplica
Creación, modificación o borrado de Jobs	Aplica
Definición de índices y estadísticas adecuadas	limitado a 1 BD
Ejecución Scripts a demanda	Aplica
Establecer directivas de fragmentación de tablas	Aplica
Establecer umbrales de rendimiento	Aplica
Habilitación de accesos	Aplica
Acompañamiento configuración servicios redundancia	Aplica
Reinicio de servicios de Base de datos	Aplica
Restauración de bases de datos	Aplica
Revisión Planes de Ejecución	Aplica
Revisión y ejecución migración de ambientes de pruebas a producción	Aplica

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 de 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	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

Categoría	ítem	Enterprise
	acuerdo con el tráfico Stateless y Stateful	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 (CSPM)	Integración del CSPM con GuardDuty para manejo centralizado de Findings y proceso de gestión de eventos con RSOC. 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

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.

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.

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.

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

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

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 Servicios Administrados para DRaaS

Tigo Business ha diseñado varios específicos para Clientes que adquieran servicios de DRaaS on AWS, su descripción y alcance es el siguiente:

- **Enterprise (DRaaS asistido)**: si prefiere mantener la responsabilidad de algunos aspectos de su plan de recuperación ante desastres, o si tiene aplicaciones únicas o personalizadas que pueden ser un desafío para que un tercero se haga cargo, DRaaS asistido podría ser una mejor opción. En este modelo, Tigo ofrece su experiencia para optimizar los procedimientos de recuperación ante desastres y acompaña y ejecuta algunas tareas, sin embargo, el Cliente es responsable de ejecutar parte del plan de recuperación ante desastres.

A continuación, se plantea el plan propuesto para usted:

Categoría	Enterprise DRaaS AWS
Monitoreo de la replicación	Tigo acuerdo a la sección “Monitoreo solución DRS”

Asistencia, comprobación y ensayo de lanzamiento de eventos Failover y Failback	Tigo Frecuencia: Anual
Reportes	Trimestral • Estado de la replicación • Jobs de recuperación • Recomendaciones tipos de instancia
Procedimiento de Failover	Tigo, en conjunto con el Cliente de acuerdo con alcance definido en etapa de implementación
Procedimiento de Failback	Tigo, en conjunto con el Cliente de acuerdo con alcance definido en etapa de implementación

2.4.5 Requerimientos mínimos para administración de cuentas AWS

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

El no contar con alguna de estas configuraciones limitará el alcance del equipo de soporte y la posibilidad de monitorear y/o restaurar un recurso que sea parte de la infraestructura desplegada, lo cual debe ser aceptado por el cliente firmando la carta de aceptación de riesgos.

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

Componente	Descripción
Reglas de AWS Config	Despliegue de la línea base de reglas de AWS Config
Nat Gateway	Salida internet para actualizaciones de seguridad en subredes privadas
Alertas	Despliegue de la línea base de alertas de monitoreo, Budget de presupuesto diario y notificaciones del PHD (Personal Health Dashboard):
Agente del agente de Systems Manager y CloudWatch	En todas las instancias EC2, se debe contar con la instalación de los agentes de SSM y CloudWatch para realizar tareas administrativas y tener acceso a las métricas de monitoreo requeridas
RDS Performance Insights	Para los Clientes que tengan desplegadas instancias de RDS es requerido habilitar esta herramienta para troubleshooting

Habilitación de logs de AWS System Manager Session Manager	Configuración de logs hacia S3 para las sesiones creadas a través del administrador de sesiones de AWS Systems Manager
AWS Backup	Backup para todas las instancias EC2 de la cuenta
AWS Security Hub	Servicio de administración de la posición de seguridad en la nube (CSPM) que realiza revisiones de las prácticas recomendadas de seguridad.

Para la configuración de los planes de AWS Backup en los recursos soportados, Servicios Administrados 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 se acordarán con el Cliente en las etapas de preventa y/o implementación.

2.4.6 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.

2.5.2 Detalle técnico por servicio profesional

No se contempla bolsa de horas de servicios profesionales para esta renovación.

2.6. Antecedentes

El cliente **INSTITUCIÓN UNIVERSITARIA DIGITAL DE ANTIOQUIA - IU DIGITAL** solicita renovar los servicios de AWS que tiene bajo las cuentas:980921719474 (Servicio DRaaS), 116762722850 (Servicios varios AWS) 782431258628 (Servicios Portal Web) por un periodo de 12 Meses.

#	Cuenta AWS	ID
1	Servicio DRaaS	980921719474
2	Servicios varios AWS	116762722850
3	Servicios Portal Web	782431258628

2.7. Descripción General

De acuerdo con la información obtenida de la cuenta de AWS, se ofrece la renovación de servicios cloud sobre una nube pública alojada en AWS (Amazon Web Services) que estará dimensionada para soportar las siguientes cargas de trabajo, entre otras.

La siguiente estimación de servicios se realiza con base en la facturación del mes de Mayo de 2026:

Alcance de los Servicios Ofertados

- ✓ **116762722850 (Servicios varios AWS)**

Cuenta 116762722850
Elastic Compute Cloud
Virtual Private Cloud
Relational Database Service
CloudWatch
Elastic Load Balancing
Data Transfer
Simple Storage Service
Config
Backup
Key Management Service
Elastic File System

Systems Manager
Route 53
Cost Explorer
CloudWatch Events
Secrets Manager
CloudFormation
CloudTrail
Glue
Simple Notification Service
Simple Queue Service

✓ **980921719474 (Servicio DRaaS)**

Cuenta 980921719474
AWS Cost Explorer
AmazonCloudWatch
AWS Systems Manager
Amazon Simple Notification Service
Amazon Simple Queue Service
Amazon Elastic Compute Cloud
AWS Elastic Disaster Recovery
AWS CloudFormation
AWS Data Transfer
AWS CloudTrail
AWS Config
AWS Secrets Manager
AWS Key Management Service
Amazon Virtual Private Cloud
AWS Glue
Amazon Simple Storage Service

INSTANCIAS DRAAS	PLANTILLAS
SRV-DCMED01	t3a.xlarge
SRV-BMSMED01	c6a.xlarge
SRV-FSMED01	m5a.xlarge

✓ **782431258628 (Servicios Portal Web)**

Cuenta 782431258628
AWS Systems Manager
Elastic Load Balancing

AWS Key Management Service
AmazonCloudWatch
Amazon Simple Storage Service
Amazon QuickSight
AWS WAF
AWS Security Hub
Amazon GuardDuty
Amazon Simple Notification Service
Amazon Virtual Private Cloud
Amazon CloudFront
AWS CloudFormation
Amazon Simple Queue Service
AWS Config
Amazon Inspector
AWS Lambda
Amazon Elastic Compute Cloud
Amazon Relational Database Service
CloudWatch Events
AWS Support (Business)
AWS Certificate Manager
AWS CloudTrail
AWS Secrets Manager

Notas:

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

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.
- 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

2.9.1 Metodología de aprovisionamiento

Para llevar a cabo el proceso de entrega de la solución contratada por el cliente **INSTITUCIÓN UNIVERSITARIA DIGITAL DE ANTIOQUIA - IU DIGITAL** Se 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 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.



2.9.2 Tiempo de aprovisionamiento

No se contemplan tiempos de aprovisionamiento, dado a que los servicios AWS se encuentran operando. No se incluyen servicios nuevos.

3. 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/

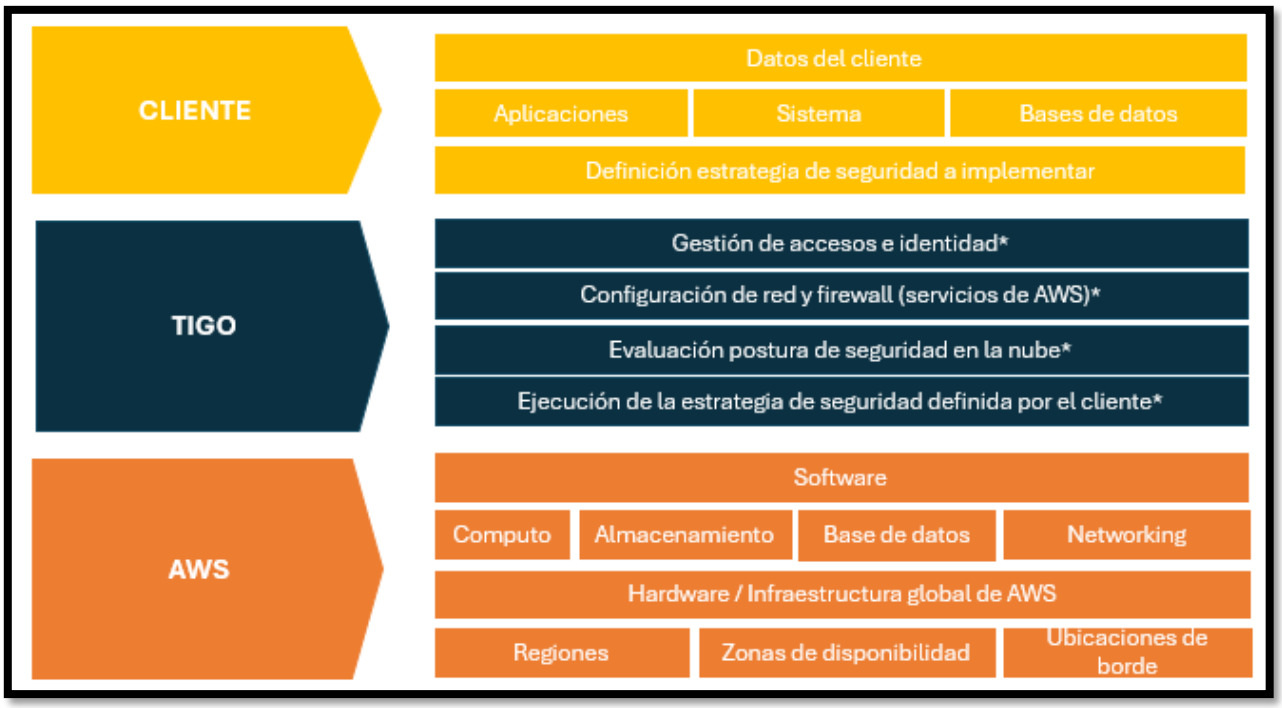
Los Ans por indisponibilidad los aplica Amazon automáticamente de acuerdo al ANS comprometido con cada servicio.

4. ROLES Y RESPONSABILIDADES

4.1 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.

- El Cliente es el único responsable de sus equipos informáticos y conexión necesarios para conectarse o acceder a sus servicios en la nube de AWS, si el Cliente cuenta con servicios de datos o internet adquiridos a través de Tigo Business, estos serán contratos totalmente independientes.

- Mantener protegidos accesos a servidores u otros servicios incluidos en los servicios contratados.

- Es responsabilidad del Cliente contar con sistemas libres de virus, spam o programas maliciosos. El Cliente habilitara su propio sistema de detección de virus, software malicioso entre otros, en caso de no poseer un sistema para tal propósito, debe contratar el servicio a Tigo Business con el único propósito de mantener seguros sus sistemas, información y contenidos alojados en el espacio o servicios contratados. Si la red se ve afectada debido a software malicioso en la infraestructura, plataforma o sistemas del Cliente, Tigo Business podrá desconectar los servicios de la infraestructura de red y conectividad para proteger a los demás Clientes.

- Asumir la responsabilidad ante la 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.

- 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.

- 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.

5. 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.

6. OFERTA COMERCIAL

6.1 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.

- ✓ **980921719474 (Servicio DRaaS)**

Producto	Nombre Producto	Detalle	Valor Mensual Sin IVA (COP)	Valor IVA (COP)	Valor Mensual Con IVA (COP)
Servicios AWS Cobro Fijo mensual	Servicios AWS Cuenta **980921719474**	Servicios AWS	$3.200.800	$0	$3.200.800
Servicios TIGO	Servicios Administrados Enterprise	Servicios Administrados TIGO	$480.120	$91.223	$571.343
VALOR MENSUAL TOTAL			**$3.680.920**	**$91.223**	**$3.772.143**

- ✓ **116762722850 (Servicios varios AWS)**

Producto	Nombre Producto	Detalle	Valor Mensual Sin IVA (COP)	Valor IVA (COP)	Valor Mensual Con IVA (COP)
Servicios AWS Cobro Fijo mensual	Servicios AWS Cuenta **116762722850**	Servicios AWS	$6.831.600	0	$6.831.600
Servicios TIGO	Servicios Administrados Enterprise	Servicios Administrados TIGO	$1.024.740	$194.701	$1.219.441
VALOR MENSUAL TOTAL			**$7.856.340**	**$194.701**	**$8.051.041**

✓ **782431258628 (Servicios Portal Web)**

Producto	Nombre Producto	Detalle	Valor Mensual Sin IVA (COP)	Valor IVA (COP)	Valor Mensual Con IVA (COP)
Servicios AWS Cobro Fijo mensual	Servicios AWS Cuenta **782431258628**	Servicios AWS	$3.056.800	$0	$3.056.800
Soporte AWS	Soporte Business	Soporte Business	$304.800	$57.912	$362.712
Servicios TIGO	Servicios Administrados Enterprise	Servicios Administrados TIGO	$458.520	$87.119	$ 545.639
VALOR MENSUAL TOTAL			**$3.820.120**	**$145.031**	**$ 3.965.151**

* 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).

Vigencia de la oferta: 10 días calendario.

6.2 Servicios por demanda: tarifas mensuales de operación del servicio en AWS

Las instancias EC2 contempladas en la presente solución, se modela bajo un esquema “On Demand”, lo cual indica que el cliente pagará exclusivamente por la cantidad de horas de uso durante un fail over (conmutación). El valor presentado a continuación es de referencia y corresponde al uso por hora de cada máquina:

Valores Recurrentes			
Producto	**Nombre Producto**	**Detalle**	**Valor x 24 horas sin IVA (COP)**
Servicios AWS Por Demanda Cuenta 980921719474	AWS EC2, VPC	Recovery Area	$ 801.616,00

VALOR MENSUAL TOTAL	$ 801.616,00

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 los consumos generados desde el momento en el que se aprovisionen los recursos, es decir, desde su creación en la plataforma de AWS hasta que se den de baja en la misma.
- 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.
- 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.
- El Cliente debe Indicar si la cuenta actualmente está bajo una organización AWS de un Partner o si está bajo contratación directa del Cliente con AWS y según sea el caso debe:

  Si la cuenta está con un Partner de AWS el cliente debe asegurar que el Partner de AWS estará presente en el momento que se haga el traslado de la cuenta a la Organización de Tigo y de igual forma el Cliente debe contar con un medio de pago autorizado el cual se usará por un lapso de 30 a 60 minutos mientras la cuenta se libera de la organización AWS del Partner y pasa a la Organización AWS de Tigo.

  Si la cuenta está contratada de forma directa entre el Cliente y AWS no se requiere de medio de pago autorizado temporal.
- El Cliente debe garantizar que para el momento del traslado de la cuenta no se tengan saldos pendientes con el proveedor actual, de haber saldos pendientes estos deben ser cubiertos por el cliente antes de que Tigo solicite el traslado de la cuenta.
- Para el traslado de los servicios, AWS maneja un calendario por mes con las fechas limite donde se puede hacer el traslado, estas fechas serán informadas en la reunión de inicio.
- 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.
- El **valor mensual** de la Oferta Comercial es de **referencia**, debido a que incluye **servicios Cloud AWS** y algunos servicios complementarios, cuya **facturación depende del consumo real** de los servicios, por lo tanto, el valor a facturar puede variar cada mes. De acuerdo con lo anterior, el valor mensual del Servicio Administrado Cloud también puede variar.
- Para Clientes del Sector Gobierno se facturará a la TRM de $ 4.000 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 mes, publicada por el Banco de la República, en el mes que se consumieron los servicios tiene una variación igual o mayor al 5% respecto a la TRM acordada, 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. En caso de requerir consumos mayores el Cliente es responsable de hacer la adición presupuestal requerida. 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.
- 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.
- 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.
- 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.

7. 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.