

Soluciones Digitales AWS
Capa de Seguridad AWS

Anexo Técnico

INSTITUCIÓN UNIVERSITARIA DIGITAL DE ANTIOQUIA
IU DIGITAL

tigo business

Medellín, 7 de septiembre de 2026

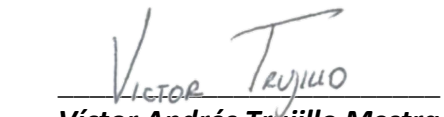
Señores
INSTITUCIÓN UNIVERSITARIA DIGITAL DE ANTIOQUIA - IU DIGITAL
Medellín

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

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

Gracias por su confianza.

Cordial saludo,



Víctor Andrés Trujillo Mestra
Ejecutivo de Cuenta
Teléfono celular: 300 774 3163
Correo electrónico: *victor.trujillo@tigo.com.co*

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

Contenido

1 Diseño 5
1.1 Alcance de la solución 5
2 Solución Digital AWS 5
2.1 Generales: AWS (Amazon Web Services) 5
2.2 Propuesta de Valor 5
2.3 Descripción de la Propuesta 6
2.3.1 Servicios Administrados 6
2.3.2 Servicios Profesionales 9
2.3.3 Descripción General de la Solución 9
2.3.4 Descripción de servicios de AWS 10
2.3.5 Topología de alto Nivel AWS 13
2.3.6 Requerimientos mínimos para administración de cuentas AWS 14
2.3.7 Roles y Responsabilidades 14
2.3.8 Supuestos y Restricciones AWS 17
2.3.9 Acuerdos de Niveles de Servicio en AWS 18
3 Capa de Seguridad AWS 19
3.1 Servicios de Seguridad Perimetral (FortiGate Virtual) 19
3.1.1 Topología General 20
3.1.2 Descripción de los componentes 20
FWaaS AWS (FG Virtual) 20
3.1.3 Instancias NGFW propuestas en la solución 21
3.1.4 Detalle de los servicios ofertados 22
3.1.5 Características de Seguridad disponibles Fortigate VM 23
3.1.6 Consideraciones Técnicas Ciberseguridad: 23
3.1.7 Requerimiento para desplegar FWaaS en AWS 23
3.1.8 Planes FWaaS 24
3.1.9 Plan Premium (Unified Threat Protection) 26
3.1.10 Servicio administrado incluido 28
3.1.11 FortiPortal usuario lectura y escritura (Coadministración - Opcional) 29
3.2 Servicio WAF y AntiDDoS (Opción 1 – CloudFlare) 33
3.2.1 Propuesta de valor 33
3.2.2 Características y beneficios 34
3.2.3 Alcance de la implementación 35
3.2.4 Arquitectura 35
3.2.5 Atributos de seguridad WAF 36
3.2.6 Atributos de seguridad AntiDDoS 37
3.2.7 Argo Smart Routing 37
3.2.8 Alcance del servicio WAF y Anti DDoS 38
3.2.9 Portales a proteger con el servicio de WAF 39
3.2.10 ADD-Ons: 40
4 Implementación y/o Transición 41
4.1 Metodología de Aprovisionamiento 41
4.2 Tiempo de Aprovisionamiento 41
4.3 Entregables 42

tigo business

5 Condiciones de Servicio 42
5.1 Niveles de servicio y atención al cliente 42
5.2 Tiempo de atención y prestación del soporte en fallas 43
5.3 Delimitaciones 43
5.4 Escala de clasificación prioridades 44
5.5 Facturación del servicio y PQRs 45
5.5.1 Peticiones, Quejas y Reclamos 45
6 Oferta Comercial 46
6.1 Servicios recurrentes: Tarifas mensuales de operación del servicio en AWS – WAF y AntiDDoS Cloudflare 46
6.2 Servicios no recurrentes o de único pago 46
6.2.1 Consideraciones comerciales 46
6.2.2 Consideraciones Entrega de Servicio 50
6.3 Condiciones económicas 50
6.4 Compromisos del cliente 51
6.4.1 Responsabilidades del cliente 51
6.5 Recomendaciones de seguridad 51
6.6 Acuerdo de Confidencialidad 52
6.7 Consideraciones generales 52
6.8 Recomendaciones de seguridad en Cloud 54
7 Compromisos del Cliente 57
ACUERDO DE CONFIDENCIALIDAD 57
USO DE LOS SERVICIOS 57
8 ACUERDO DE CONFIDENCIALIDAD 58

1 Diseño

1.1 Alcance de la solución

La presente oferta contempla una solución que integra los servicios existentes en AWS con nuevos componentes nativos de la plataforma, los cuales se incorporan mediante un esquema de seguridad perimetral robusto. Este diseño permite asegurar la comunicación entre servicios, así como la transmisión de datos, mediante mecanismos de control, inspección y protección del tráfico, garantizando su confidencialidad, integridad y disponibilidad.

Dicha propuesta contempla dentro del alcance los siguientes componentes:

- Solución Digital AWS
- Capa de Seguridad AWS
    - FortiGate Virtual
        - Servicio de WAF y AntiDDoS con Cloudflare

2 Solución Digital AWS

2.1 Generales: AWS (Amazon Web Services)

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

2.2 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.

2.3 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.

2.3.1 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.

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:

	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
Administración de parches y soporte al SO (Sistema operativo)	* Soporte a cambios sobre el SO: Asesoramiento general, apoyo para creación de respaldo previo al cambio o restauración en caso de rollback. * Los cambios a nivel de SO siempre deben ser ejecutados por el cliente * Soporte de SO compatibles con System Manager de AWS. https://docs.aws.amazon.com/es_es/systems-manager/latest/userguide/operating-systems-and-machine-types.html
Seguridad - Gestión de Identidades y Accesos	* Gestion de AWS IAM * Aplicación de SCPs estándar * Gestión de AWS Identity Center
Seguridad - Protección de Infraestructura y Red	* Protección DDoS estándar – Shield Standard * Gestión VPC y configuración de red
Seguridad - Detección de Amenazas y Monitoreo	* Gestión de GuardDuty * 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

2.3.2 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.

2.3.3 Descripción General de la Solución

La INSTITUCIÓN UNIVERSITARIA DIGITAL DE ANTIOQUIA - IU DIGITAL requiere una solución que centralice la gestión de redes y seguridad para todas las cuentas dentro de la organización en AWS.

Actualmente se encuentran en operación las siguientes cuentas:

- 537124947679 (Tigo Business IU Digital MGMT).
- 961341535234 (Log Archive).
- 084828557880 (Audit).
- 116762722850 (Institucion Universitaria Digital de Antioquia).
- 782431258628 (CO_SPAM_IU_DIGITAL).
- 905418445086 (CO_SPAM_IU_DIGITAL_2).
- 980921719474 (CO_SPAM_IU_DIGITAL_DRAAS).
- 891377262723 (CO_SPAM_IU_DIGITAL_APPSTREAM).
- 065502538856 (Connect IU Digital).
- 488453321823 (Analitica IUDigital).
- 705557196784 (CO_SPAM_IU_DIGITAL_BEDROCK)____POC.
- 199702507972 (CO_ECAM_IU_DIGITAL_KIRO)____POC.

Para lograr el objetivo, se plantea una arquitectura multicuenta donde se crea una nueva cuenta llamada Redes y Seguridad que a través de un TransitGateway permitirá la conexión con las demás cuentas. Se deben tener en cuenta las siguientes consideraciones:

- Se deben reconfigurar los servicios de salida y entrada de datos desde internet y dese otras cuentas para que pasen a través del TG hacia y desde la cuenta de Redes y Seguridad.

- Suspender los servicios de Internet, VPN, WAF de todas las cuentas para que estos servicios sean gestionados únicamente desde la cuenta de Redes y Seguridad
- Los servicios de Firewall serán desplegados en la cuenta de Redes y Seguridad con Fortinet mientras que el WAF y AntiDDoS serán desplegados en la nube de CloudFlare.

2.3.4 Descripción de servicios de AWS

Servicio	Descripcion Propuesta	Resumen de la configuracion
Amazon GuardDuty	Servicio de detección de amenazas que utiliza aprendizaje automático e inteligencia de amenazas para identificar actividades maliciosas y comportamientos anómalos en entornos AWS. Analiza logs de VPC Flow, eventos de CloudTrail y DNS para proteger cuentas, cargas de trabajo y datos. Proporciona hallazgos priorizados que facilitan la respuesta a incidentes y fortalecen la postura de seguridad. Para más información ingresar al siguiente enlace: https://aws.amazon.com/es/guardduty/	• Análisis de eventos de administración de AWS CloudTrail (100000 por mes) • Análisis de registros de flujo de VPC de EC2 (10 GB per mes)
Amazon Inspector	Servicio de evaluación automatizada de seguridad que identifica vulnerabilidades, exposiciones de red y desviaciones de mejores prácticas en instancias EC2, contenedores y aplicaciones. Realiza análisis continuo mediante agentes, detectando amenazas potenciales y generando reportes detallados con recomendaciones de remediación priorizadas por severidad. Para más información ingresar al siguiente enlace: https://aws.amazon.com/es/inspector/	• Número medio* de instancias de EC2 analizadas al mes (50) • Cantidad promedio de funciones de Lambda analizadas al mes (30)
Transit Gateway	Servicio de conectividad centralizada que simplifica la interconexión de múltiples redes virtuales, redes locales y conexiones remotas. Actúa como hub de enrutamiento, eliminando la necesidad de configurar conexiones punto a punto complejas. Facilita la administración de tráfico, implementación de políticas de seguridad y escalabilidad en arquitecturas híbridas y multi-cuenta. Para más información ingresar al siguiente enlace: https://aws.amazon.com/es/ec2/transit-gateway/	• Número de asociaciones de gateway de tránsito (15) • Número de receptores de multidifusión (0)
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/	• DT Inbound: Internet (2 TB per month) • DT Outbound: Internet (2 TB per month) • DT Intra-Region: (2 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/	• Tenencia (Instancias compartidas) • Sistema operativo (Linux) • Carga de trabajo (Consistent • Cantidad de instancias: 2) • Instancia EC2 por adelantado (c6in.2xlarge) • Pricing strategy (On-Demand Utilization: 100 %Utilized/Month) • Habilitar la monitorización (habilitado) • EBS Cantidad de almacenamiento (256 GB) • DT Entrada: Not selected (0 TB al mes) • DT Salida: Not selected (0 TB al mes) • DT Intra-región: (0 TB al mes)

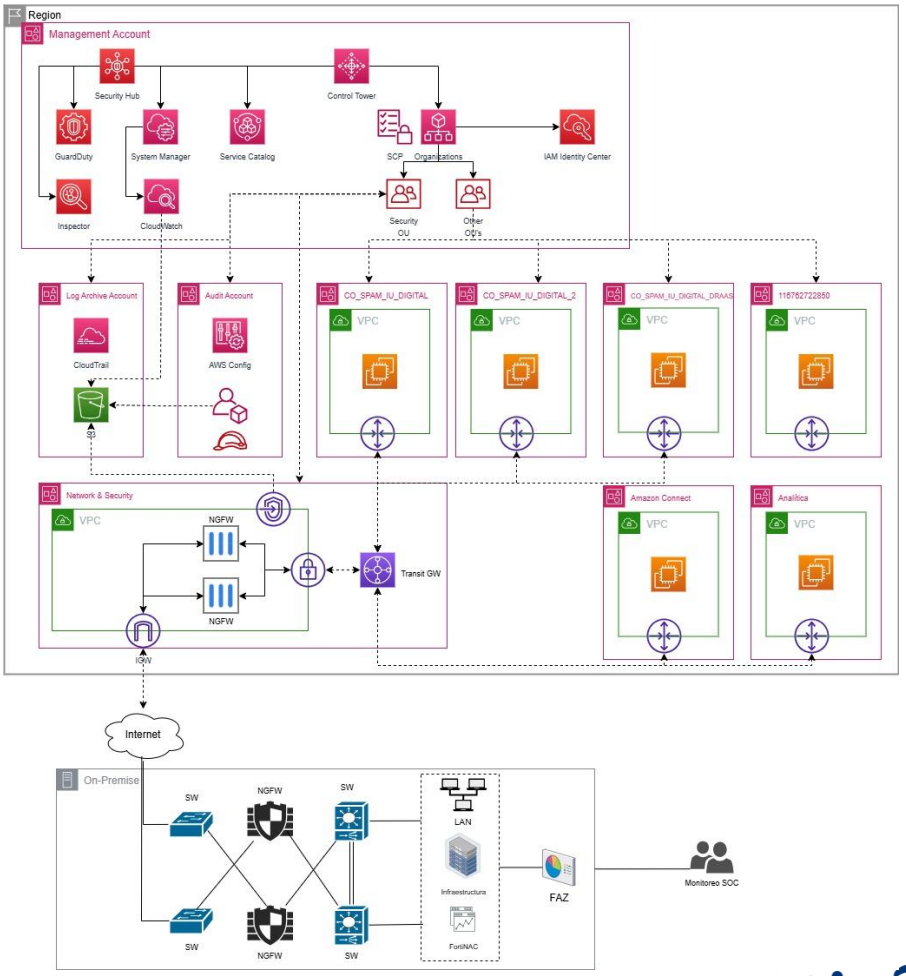
		• vCPU: 8 • RAM: 16 GiB
Network Load Balancer	Servicio de distribución de tráfico de capa 4 (transporte) optimizado para aplicaciones de ultra-alto rendimiento y baja latencia. Maneja millones de solicitudes por segundo con throughput extremadamente alto. Ideal para protocolos TCP/UDP, IoT, gaming y sistemas en tiempo real. Ofrece rendimiento predecible y gestión eficiente de conexiones concurrentes. Para más información ingresar al siguiente enlace: https://docs.aws.amazon.com/es_es/elasticloadbalancing/latest/network/	• Número de balanceadores de carga de red (1) • Bytes procesados por NLB para TCP (3 TB per mes) • Número promedio de conexiones TCP nuevas (100 por segundo) • Duración promedio de conexión TCP (60 segundos) • Bytes procesados por cada NLB para UDP (3 TB per mes) • Cantidad promedio de flujos de UDP nuevos (100 por segundo) • Duración promedio del flujo de UDP (60 segundos)
Public IPv4 Address	Servicio que asigna direcciones IPv4 públicas enrutables en Internet a instancias EC2 y recursos de red dentro de VPC. Facilita conectividad bidireccional desde y hacia Internet, permitiendo acceso remoto, comunicaciones externas y exposición de aplicaciones. Se gestiona automáticamente o manualmente según configuración de subnets y políticas de red. Para más información ingresar al siguiente enlace: https://docs.aws.amazon.com/es_es/AWSEC2/latest/UserGuide/using-instance-addressing.html	• Cantidad de direcciones IPv4 públicas en uso (4)
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	• 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 (1 por mes) • Eventos de administración de lectura (10 por mes) • Operaciones de S3 (1 por mes) • Eventos de datos Lambda (1 por

		mes) • Número total de llamadas a la API de administración (tanto de lectura como de escritura) que se analizarán para detectar actividades inusuales (2 por mes)
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/	• 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)
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/	• Número de elementos de configuración continua registrados (2000) • Número de evaluaciones de las reglas de configuración (2000)
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/	• Almacenamiento de S3 Estándar (512 GB 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 (1000 GB por mes) • Datos escaneados por S3 Select (1000 GB por mes)
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/	• nan

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/	• Almacenamiento de S3 Estándar (80 GB 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 (1000 GB por mes)
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/	• nan

https://calculator.aws/#/estimate?id=1b480c961649c172084129a82a8751b409f33d74

2.3.5 Topología de alto Nivel AWS



2.3.6 Requerimientos mínimos para administración de cuentas AWS

En la siguiente tabla se encuentran cada uno de los requerimientos mínimos que deben contar las cargas de trabajo de AWS 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:

Componente	Descripción
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 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. Sistemas Operativos compatibles: https://docs.aws.amazon.com/es_es/systems-manager/latest/userguide/operating-systems-and-machine-types.html
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.
Roles IAM	Se desplegarán roles IAM dedicados para la ejecución de operaciones dentro del servicio administrado de AWS.

El Cliente acepta que el no contar con alguna de estas configuraciones limitará el alcance del equipo de soporte y la posibilidad de monitorear y/o restaurar un recurso que sea parte de la infraestructura desplegada, por lo tanto, Tigo no puede garantizar la disponibilidad ni el cumplimiento de SLA.

2.3.7 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: https://aws.amazon.com/es/compliance/shared-responsibility-model/

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 es el único responsable de los contenidos, productos, servicios e información que ofrezca, publique o transmita mediante 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.

- 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 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.

2.3.8 Supuestos y Restricciones AWS

- 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.
- 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.
- 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.
- 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

- 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.

2.3.9 Acuerdos de Niveles de Servicio en AWS

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 con el ANS comprometido con cada servicio.

3 Capa de Seguridad AWS

Se oferta una solución de ciberseguridad perimetral para proteger las cargas de trabajo en AWS.

La oferta contiene los siguientes servicios de Telecomunicaciones, la protección perimetral en AWS está acotada a la tecnología ofertada y sus limitantes:

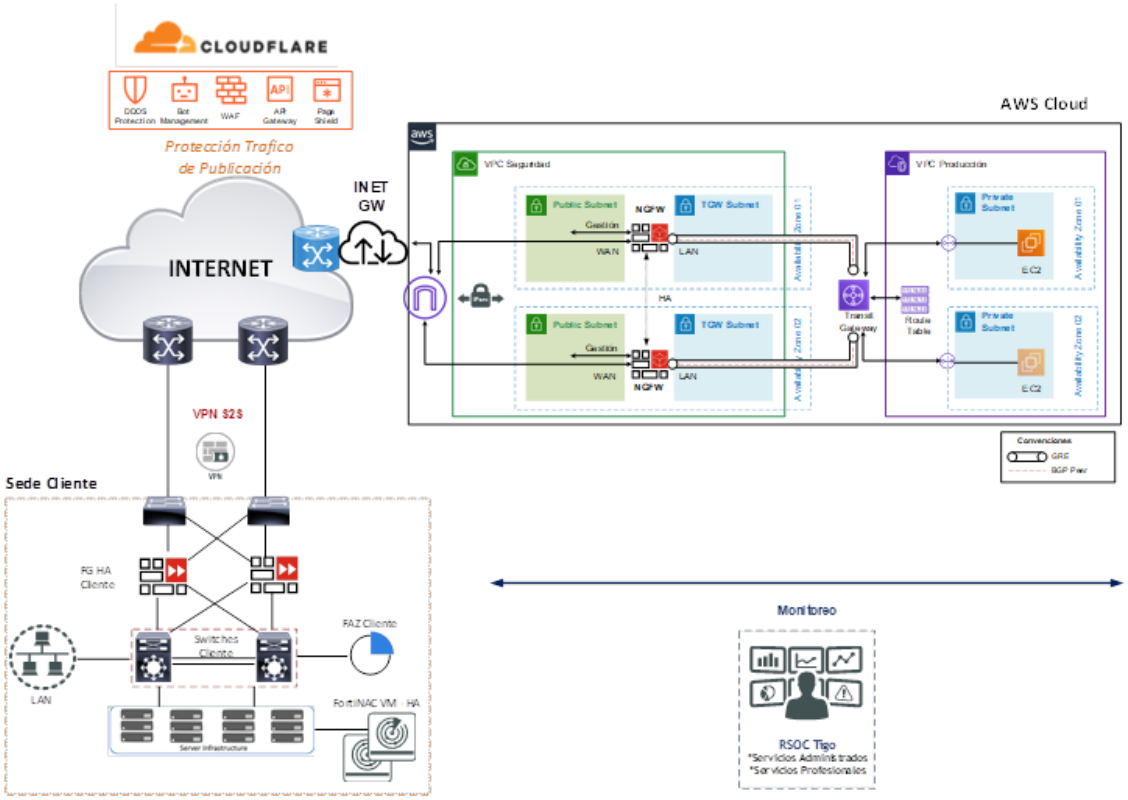
- Servicio de Seguridad Perimetral compuesta por (2) FortiGate Virtual
- Servicio de WAF y AntiDDoS

3.1 Servicios de Seguridad Perimetral (FortiGate Virtual)

Para la solución de ciberseguridad en nube publica se aprovisionará un VPC exclusivo para la capa de seguridad en AWS, este VPC tendrá rol de HUB Security donde se instalarán 2 firewall virtuales en modalidad HA en zonas de disponibilidad independientes, este VPC se conectará a un Transit Gateway y de esa forma el VPC de Seguridad tendrá conectividad contra los diferentes VCP de producción del cliente.

Con esta arquitectura todo el tráfico destinado hacia las cargas de AWS será procesada por el VPC de Seguridad permitiendo al cliente tener una capa de seguridad flexible y alto rendimiento para controlar el flujo de datos de la nube.

3.1.1 Topología General

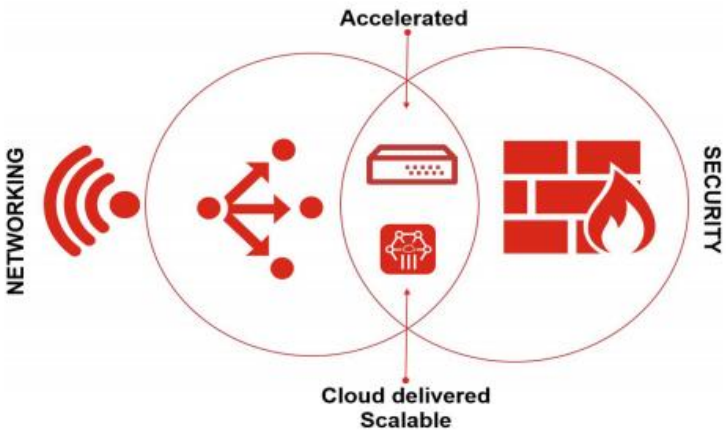


3.1.2 Descripción de los componentes

FWaaS AWS (FG Virtual)

- **Alcance FortiGate Virtual:** como perímetro de la red en AWS se aprovisionará (2) Fortigate modalidad virtual el cual tendrá licenciamiento FortiGuard Unified Threat Protection (UTP). Estos Firewall controlaran el tráfico proveniente desde Internet hacia las instancias de AWS del cliente.
- **FortiGate: Next Generation Firewall:** FortiGate proporciona funcionalidades de NGFW con un rendimiento excepcional, ultra baja latencia y protección de amenazas multi vector. Las plataformas NGFW FortiGate incluyen un sistema de prevención de intrusiones (IPS) con un escaneado del paquete en profundidad, capacidad para identificar y controlar las aplicaciones ejecutadas en la red y la posibilidad de verificar la identidad del usuario y cumplir con las políticas de acceso.

FortiGate ofrece implementaciones flexibles del borde de la red hasta el Core, el centro de datos, el segmento interno y la nube.



Concepto de Redes enfocadas en Seguridad de Fortinet

3.1.3 Instancias NGFW propuestas en la solución

Para la solución del IU DIGITAL se oferta (2) NGFW Fortigate en modalidad virtual en AWS.

Dimensionamiento del Firewall:

Ref de Equipo	Cantidad	Licenciamiento	Nube
FortiGate-VM (8 CPU)	2	UTP	AWS

	VM-01/01S	VM-02/02S		VM-04/04S		VM-08/08S	
System Requirement							
vCPU (Minimum / Maximum)	1 / 1	1 / 2		1 / 4		1 / 8	
Technical Specifications							
Network Interface Support (Minimum / Maximum) [1]	1 / 24	1 / 24		1 / 24		1 / 24	
Virtual Domains (Default / Maximum) [2]	10 / 10	10 / 25		10 / 50		10 / 500	
Firewall Policies	10 000	10 000		10 000		200 000	
System Performance		ENA Driver - Yes		ENA Driver - Yes		ENA Driver - Yes	
Instance Shape to be Measured		C6in.LARGE		C6in.XLARGE		C6in.2XLARGE	
AWS Bandwidth [3]		Up to 25 Gbps		Up to 30 Gbps		Up to 40 Gbps	
		Native	IPSEC	Native	IPSEC	Native	IPSEC
Firewall Throughput (UDP Packets) in Mbps - 1518 bytes*		16 960	2020	21 200	3370	31 600	5350
Firewall Throughput (UDP Packets) in Mbps - 512 bytes*		5760	1020	9900	1630	10 900	2640
Firewall Throughput (UDP Packets) in Mbps - 64 bytes*		720	170	1200	270	1420	450
New Sessions / Second (TCP)		140 000	-	216 000	-	240 000	-
HTTP Throughput w/ Application profile (64K size) [4] in Mbps		10 700	-	15 800	-	29 000	-
HTTP Throughput w/ IPS profile (44K size) in Mbps		10 500	-	15 700	-	28 800	-
HTTP Throughput w/ IPS profile (1M size) [5] in Mbps		10 800	-	15 800	-	29 000	-
NGFW Throughput [6] in Mbps		790	-	1420	-	2790	-
Threat Protection Throughput [7] in Mbps		780	-	1380	-	2740	-
SSL Inspection Throughput in Mbps [8]		1810	-	3350	-	6540	-

NOTA:

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

3.1.4 Detalle de los servicios ofertados

Presentamos la solución tecnológica de protección perimetral en AWS para **IU DIGITAL**

Detalle de los Servicios ofertados

SKU	FC4-10-FGVVS-990-02-12 **Cantidad:**1
Descripción	Subscriptions license for FortiGate-VM (8 CPU) with UTP Bundle included.

Ficha Técnica General:
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_VM_AWS.pdf

3.1.5 Características de Seguridad disponibles Fortigate VM

Se presenta a continuación los features de seguridad disponibles en el NGFW delimitado al licenciamiento propuesto, información suministrada de la plataforma y de las necesidades del proyecto:

- Firewall Capa 3, 4 y 7
- Web Filtering
- App Control
- Antivirus Perimetral
- IPS
- VPN C2S
- VPN S2S

NOTAS:

- En caso de requerirse la configuración de una funcionalidad adicional de Seguridad se deberá validar su viabilidad en una nueva factibilidad ya que podría cambiar el licenciamiento.

3.1.6 Consideraciones Técnicas Ciberseguridad:

- Las Instancias Fortigate virtual será la capa de seguridad perimetral de la solución AWS
- Dentro de la fase de implementación se definirá en conjunto con el cliente las políticas de seguridad a configurar en el FG virtual
- Se definirá en conjunto con el cliente el LLD para esta solución
- Se debe tener una ventana de mantenimiento para ejecutar las actividades

3.1.7 Requerimiento para desplegar FWaaS en AWS

Las siguientes son las características de referencia para el despliegue de las VM en AWS, estos elementos deben ser considerados por el cliente:

Tipo de Característica	Característica y Cantidades
Licencia	FG VM 08
Tipo de Instancia	C6in.2XLARGE
RAM	16GB

Almacenamiento Minimo	60GB
Red Virtual	1 VPC
Salida a Internet	1 Public Gateway asignado a subnet public
Enrutamiento	**2 Routing Tables**: *Internal:como ruta por defecto apra el VPC *Open: para las subnets - Public - Managment y Heartbeat
Balanceo HA	**4 Floating IP/failover**: *2 Floating IP estatica permanente para produccion y servicios * 2 Floating IP temporales para gestion en ambos firewalls durante la implementacion
Subnets	4 (Public,Internal, Management, Heartbeat)
API Keys	API Key con SDN Connector con permisos administrativos a nivel de VPC, compute y asignacion de recursos a Instancias

3.1.8 Planes FWaaS

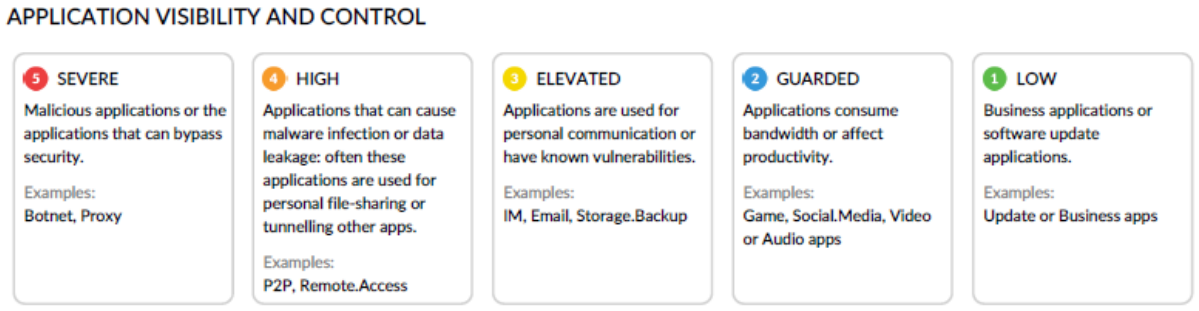
Estos son los diferentes planes con los que se cuenta en la oferta de FWaaS. De acuerdo con la necesidad de su Empresa el plan ofertado es **PREMIUM:**

Atributos	Estandar (Web filtering)	Avanzado (UTP)	Premium (UTP)
Filtrado de contenido basado en categorías	•	•	•
Filtrado web	•	•	•
VPN Site to Site ipsec	5 max	10 max	10 max
VPN client to Site ipsec	5 max	10 max	10 max
Firewall capa 3, 4	x	•	•
Control de aplicaciones	•	•	•
Enrutamiento basado en aplicaciones	x	•	•
Conectividad segura Cifrada	•	•	•
Balanceo Dinámico	•	•	•
Administración	Centralizada	Centralizada	Con posibilidad de Coadministración (Hasta 3 usuarios por cliente)
DIA (direct internet access)	•	•	•

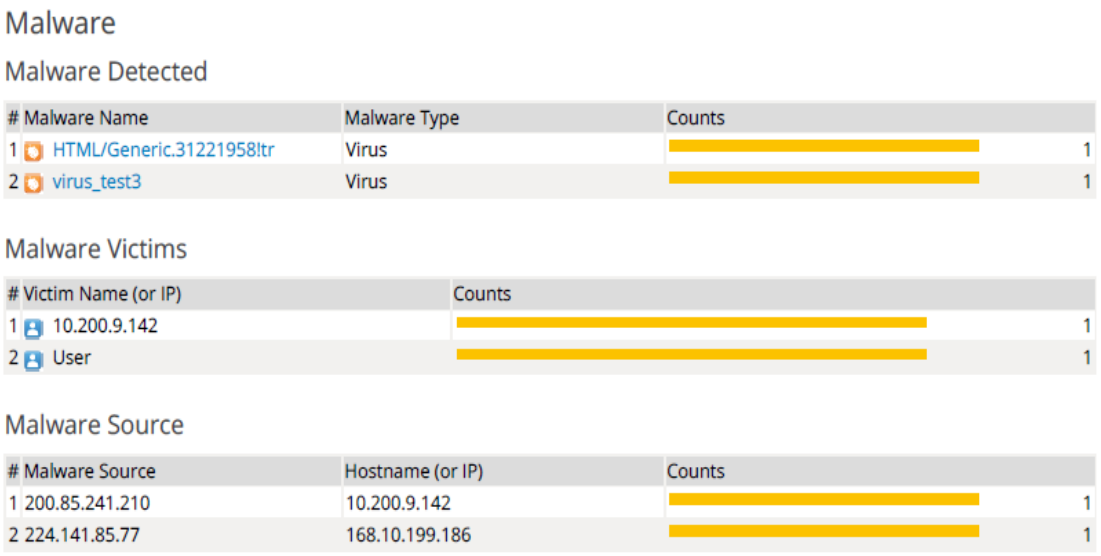
Optimización aplicaciones SaaS basado en SLA +	•	•	•
Reporteria	x	•	•
Firewall capa 7	x	•	•
Integración a Directorio Activo*	x	•	•
Antivirus perimetral	x	•	•
IPS/IDS	x	•	•
File filtering	x	•	•

Reportes automáticos* que se entregarán son los siguientes tanto para el plan avanzado como para el plan Premium son los siguientes:

Nombre del reporte: 360 Security Report
Descripción: Resumen mensual de incidentes y eventos de seguridad



Nombre del reporte: Threat Report
Descripción: Es un reporte que logra mostrar los malware detectados y las victimas de estos malware



Malware

Malware Detected

#	Malware Name	Malware Type	Counts
1	HTML/Generic.31221958!tr	Virus	1
2	virus_test3	Virus	1

Malware Victims

#	Victim Name (or IP)	Counts
1	10.200.9.142	1
2	User	1

Malware Source

#	Malware Source	Hostname (or IP)	Counts
1	200.85.241.210	10.200.9.142	1
2	224.141.85.77	168.10.199.186	1

NOTA: Estos reportes automáticos estarán disponibles durante el mes para su descarga o envío, con la información correspondiente al mes anterior. Si el cliente requiere ampliar el periodo de visualización de sus reportes, podrá solicitarlo a través de su ejecutivo comercial o de servicio asignado.

En caso de que el cliente exceda el volumen de logs establecido para la generación de estos informes, Tigo Business podrá contactarlo para revisar las condiciones vigentes de su oferta comercial, con el propósito de garantizar la continuidad y eficiencia del servicio.

Definición de los Perfiles de navegación (filtrado Web y control de aplicaciones)

Navegación Alta: Alta restricción
Navegación Media: Acceso limitado
Navegación Baja: Acceso a todo

3.1.9 Plan Premium (Unified Threat Protection)

- **Firewall:** Esta característica provee un primer nivel de seguridad que permite filtrar el tráfico de entrada y salida a la red de acuerdo con una lista de reglas definidas. El Firewall es un servicio básico que suele complementarse con otros servicios de seguridad para ayudar a prevenir eventos que impacten la confidencialidad, integridad y disponibilidad de la información y servicios de la compañía. A través de esta funcionalidad se protege el acceso a segmentos de red de importancia para la compañía, así como a puertos TCP/UDP de servicios críticos para el negocio. Protección a nivel de control de puertos TCP/UDP basado en redes IP. El equipo y la capacidad de protección es dimensionado de acuerdo con el Ancho de Banda que tenga el

servicio de Internet que se vaya a proteger y el total de sesiones concurrentes (entrantes y salientes).

- **VPN:** Las Redes Privadas Virtuales (VPN), por sus siglas en inglés, están dispuestas para controlar y evitar que terceros no autorizados puedan interceptar la información que está viajando de entre dos nodos de la red a través de una red insegura como Internet. El servicio VPN permite ingresar de manera segura a redes privadas y/o servicios del cliente hospedados en los **DataCenter** Tigo. Las VPN ayudan a mantener la confidencialidad de la información que viaja entre diferentes puntos de la red.

- **Antivirus Gateway:** Proporciona una protección de red contra una variedad de amenazas incluyendo códigos maliciosos conocidos y desconocidos (malware), Advanced Target Attacks (ATA) y Advanced Persistent Threats (APT). Este servicio proporciona una primera protección frente a ataques externos que pueden poner en riesgo la integridad o disponibilidad de la información y servicios críticos del negocio. Se fundamenta en una Base de Datos de definiciones de firmas de malware que son actualizadas periódicamente por el fabricante. La funcionalidad cuenta con un motor de inspección basado en comportamiento identificando amenazas desconocidas en los laboratorios del fabricante. Esta protección se aplica al tráfico entrante y saliente (navegación y publicación) de tráfico no cifrado. Este servicio es una funcionalidad adicional al componente de Firewall. Se recomienda siempre complementar con un Antivirus de Host ya que el Antivirus de Red no reemplaza el Antivirus que se instala en dispositivos de usuario y servidores.

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

- **IDS / IPS:** IDS (Intrusion Detection System) o sistema de detección de intrusiones e IPS (Intrusion Prevention System) proporcionan protección ante amenazas a nivel de red empleando una Base de Datos de firmas que periódicamente son actualizadas por el fabricante de acuerdo con las nuevas amenazas. El servicio IDS/IPS previene ataques que pongan en riesgo principalmente la integridad y disponibilidad de información y servicios críticos de la Compañía. Esta protección se aplica para el tráfico entrante, es decir tráfico de publicación.

- **Filtrado Web:** esta funcionalidad permite el monitoreo y el control del uso que los funcionarios hacen de los accesos a Internet y la prevención de visualización de contenidos web inapropiados, o no autorizados. La solución puede ser configurada para escanear toda la cadena

del contenido del protocolo http permitiéndonos filtrar direcciones URL potencialmente no asociadas al desarrollo de la normal actividad laboral, contenidos embebidos en las propias páginas web o scripts basados en java, activeX o cookies, contenidos potencialmente peligrosos.

3.1.10 Servicio administrado incluido

A continuación, se detallan los servicios administrados incluidos en todas las etapas del servicio Tigo FWaaS contratado por el cliente:

- Los cambios solicitados debido a una emergencia donde se el cliente haya identificado un evento o incidente de seguridad, los tiempos de respuesta son los expuestos en la tabla 1
- Si el cliente requiere un servicio de monitoreo proactivo, que tenga notificación de eventos y/o incidentes debe contratar servicio de SOC como un Add On.
- No se incluye reingeniería de políticas, análisis o rediseño del esquema de seguridad configurado a petición del cliente.
- Atención 7x24x365 para eventos en los equipos (nivel 1).
- Si el cliente va a realizar cualquier actividad programada al interior de su red y que deba tener impacto sobre lo configurado previamente en el servicio de FWaaS prestado por Tigo Business esta solicitud deberá hacerse con anterioridad, teniendo en cuenta los siguientes tiempos expuestos en la tabla 1.

Estas solicitudes deberán hacerse a través de los canales oficinales de Tigo Business que se mencionan en la sesión ANS y servicio al cliente

Tabla 1

Actividad	Tiempos de Atención		
	Hasta 2 horas	Hasta 24 horas	Análisis Preventa
Gestión de políticas		x	
Cambio de correo electrónico para el envío de los reportes en el caso que aplique			
Gestión de cambios de enrutamiento		x	
Gestión de políticas		x	
Creación y modificación de políticas		x	
Apertura de tickets en base a criticidad de alarmas o alertas		x	
Parche o Fix de plataforma		x	

3.1.11 FortiPortal usuario lectura y escritura (Coadministración - Opcional)

FortiPortal

Es una herramienta que se accede a través de la web que entrega TigoBusiness sin costo adicional que permite monitorear, visualizar y/o cambiar las políticas de seguridad de los equipos que protegen el perímetro.

Tipos de Usuarios
Con el rol ROP-Basic tiene perfil de solo lectura del FortiPortal que ofrece visualización de políticas de seguridad en la nube, Es indispensable que el Cliente use de manera correcta este usuario, asegurando el control en el uso, acceso de contraseñas frente a lo cual Tigo no se hará responsable.

Con el usuario RWP-Basic-Security de lectura y escritura del fortiportal que entrega Tigo Business sin costo adicional que permite tener una COADMINISTRACION entendiéndose está como una facilidad o permiso que se otorga al cliente que permite realizar cambios sobre la configuración inicial de sus equipos.

La plataforma FortiPortal le permite al cliente acceder a las siguientes funcionalidades, las cuales requieren el cumplimiento de parámetros de manejo de accesos, contraseñas y perfiles que deben ser asignados, manejados y controlados por el Cliente en aras de garantizar la reserva, confidencialidad a la información y datos alojados. En este sentido el cliente es el responsable del acceso y manejo del “usuario“ asignado. Tigo no será responsable del uso, manejo, disposición de este perfil y el cliente asume toda la responsabilidad derivada del uso dado al mismo.

Alcance y funcionalidades que le permite la plataforma al Cliente de manera directa

- Monitorear el tráfico de la red en tiempo real, obteniendo una visión general del uso de ancho de banda y de las amenazas.
- Configurar políticas de seguridad en dispositivos de la red, como firewalls.
- Gestionar usuarios y accesos a la red del cliente, aplicando políticas personalizadas según el perfil de cada usuario.

Alcance de actividades de la Coadministración

El entorno de la nube es dinámico y requiere cambios constantes y alineación con las tendencias y requisitos emergentes. Los proveedores de servicios gestionados en la nube deben llevar a cabo todos los aspectos de la gestión del ciclo de vida y los clientes, a través del modelo de administración compartida establecido en este documento, deberán asumir las responsabilidades tal y como se indica a continuación:

Alcance con Perfil Usuario RWP-Basic-Security	Tigo	Cliente
Disponibilidad de acceso a portales de plataformas	X	
Configuración/creación cliente en plataforma	X	
Creación de usuario/cliente en plataforma con el perfil acordado	X	
Atención de incidentes asociados a plataformas	X	
Atención de incidentes asociados a configuraciones realizadas sobre el servicio y asociadas a los permisos otorgados en el perfil de usuario/cliente Tigo Business prestará apoyo		X
Insights	X	
Security		
Policy		x
Security Policy		X
Central SNAT		X
Central DNAT		X
IPv6 Central DNAT		X
NAT64-NAT46 Policy		X
Proxy Policy		X
Authentication Policy		X
IPv4-IPv6 Multicast/ Local in / DoS / Interface Policy		X
Traffic Shaping Policy		X
Firewall Policy		X
Firewall Objects		
Address		X
Schedule		X
Service		X
Virtual IP		X
Antivirus Profile		X
Application Control		X
File Filter Profile		X
Intrusion Prevention Profile		X
Web Filter Profile		X
Local Category		X
Web Rating Overrides		X
Video Filter		X
SSL/SSH Inspection		X
User		X
User Groups		X
Network		
IPSec Phase 1	X	
IPSec Phase 2	X	
Static Route	X	

DHCP Server	X	
Certificate	X	
Routing	X	
Switch		
Configuration		X

Descripción:

- **Disponibilidad de acceso a portales de plataformas:** Se refiere a mantener la disponibilidad de los portales entregados al cliente para su gestión del servicio.
- **Configuración/creación cliente en plataforma:** refiere al aprovisionamiento inicial del servicio contratado por el cliente.
- **Creación de usuario/cliente en plataforma con el perfil acordado:** refiere a la generación de los accesos que serán entregados al cliente para su posterior gestión del servicio según los perfiles respectivos. Este servicio no permitirá la creación de usuario genéricos, con el fin de garantizar la trazabilidad de la administración por ambas partes.
- **Configuración de reglas de firewall:** refiere a la capacidad de poder crear reglas y objetos a nivel de seguridad de firewall como apertura de puertos de origen/destino, salida y/o entrada de tráfico desde y hacia la red local, además de traducciones de red NAT
- **Configuración de reglas de filtrado de contenido:** refiere a la capacidad de poder crear reglas a nivel de filtrado de tráfico basados en patrones o tipos de categoría de conexiones desde y hacia la red local y así controlar la información que un usuario de internet puede ver
- **Configuración de reglas de aplicaciones de control (APP Control):** refiere a la capacidad de poder crear reglas de aplicación para el análisis de tráfico hasta la capa 7 de aplicaciones. Esta protección es usada para controlar aplicaciones riesgosas y no deseadas en la red
- **Creación/Modificación/Eliminación de usuarios para la conexión a través de VPN Client to Site:** refiere al privilegio de crear, modificar o eliminar usuarios que podrán tener acceso a la red del cliente a través de una VPN (Virtual Private Network) Client to Site.
- **Consumo y manejo de la seguridad de los datos:** refiere al adecuado consumo de los datos de las aplicaciones que fluyen por la red, velando por su correcto aseguramiento basado en las políticas de reglas de firewall, filtrado de contenido y aplicaciones de control del tráfico definidas
- **Manejo de las credenciales de acceso usuario/cliente al portal e identidad de los accesos:** refiere al adecuado uso y manejo de los accesos a los portales de gestión del servicio entregados al cliente según los perfiles respetivos
- **Atención de incidentes asociados a plataformas:** refiere al soporte y atención de los incidentes asociados a las plataformas principales que estén afectando el servicio final contratado por el cliente
- **Atención de incidentes asociados a configuraciones realizadas sobre el servicio y asociadas a los permisos otorgados en el perfil de usuario/cliente:** refiere al soporte y atención de los incidentes sobre las configuraciones realizadas por el cliente

Responsabilidad para el cliente con la Coadministración

A continuación, se establecen las implicaciones e impactos que asumiría el cliente, bajo este esquema de administración y conforme a los roles y responsabilidades, anteriormente descritos. En ese sentido es responsabilidad del cliente lo siguiente:

- Caídas o indisponibilidades del servicio, derivados de las configuraciones o modificaciones que son asignadas al cliente y a las que éste tiene acceso establecidas en la tabla de responsabilidades.
- Impacto en los niveles de servicio, derivados de las configuraciones o modificaciones a las que el cliente tenga acceso establecidas en la tabla de responsabilidades.
- Modificar parámetros sensibles de auditorías.
- Costos adicionales, derivados de servicios profesionales para la normalización del servicio; para resolver los incidentes ocasionados por configuraciones en las que el cliente tenga acceso establecidas en la tabla de responsabilidades.
- Cualquier riesgo, exposición o vulnerabilidad que se derive de una configuración desde el perfil del cliente, queda bajo responsabilidad de este.

Delimitación de responsabilidad para el cliente bajo la Coadministración

- Los SLA asociados a cambios realizados por incorrectas configuraciones de perfil usuario/cliente no serán impactados, ni aplicarán resarcimientos.
- Tigo no es responsable de la configuración, soporte y monitoreo de los roles y responsabilidades del cliente, ni las consecuencias que estas conlleven ante una configuración inadecuada.
- El cliente acepta y comprende que en caso de materialización de los riesgos descritos en el presente anexo y que sean de su competencia, exime al proveedor de cualquier responsabilidad y consecuencias a que estas conlleven.
- Tigo no es responsable de las indisponibilidades del servicio que surjan por cambios efectuados por el cliente bajo sus roles o responsabilidades; independiente de las Notificaciones que brinde el cliente sobre los cambios que ejecute.
- Cuando el cliente requiera apoyo de Tigo en alguno de sus roles y responsabilidades, deberá evaluarse el requerimiento como un nuevo proyecto y definir si el apoyo requiere servicios profesionales, los cuales deberán ser cotizados con base a la necesidad o casuística específica.
- En caso de presentarse una falla y, como medida correctiva, se deba aplicar la configuración inicial, el SOC B2B aplicará la plantilla con la que se implementaron los servicios inicialmente, aclarando que este apoyo no genera responsabilidad de Tigo. Por ende, el cliente será el responsable de volver a actualizar los cambios de su rol o responsabilidad.

3.2 Servicio WAF y AntiDDoS (Opción 1 – CloudFlare)

Web Application Firewall (WAF) es una solución de ciberseguridad enfocada en la protección de aplicaciones WEB y las APIs1 que incluye servicios basados en la nube para la protección integral de los ataques maliciosos sobre este tipo de aplicaciones.

La implementación de un WAF ayuda a las organizaciones a proteger sus sitios web y Apis de servicios para aplicaciones móviles frente a las amenazas de hackers, bots y hacer frente a las vulnerabilidades forma proactiva.

Entre algunas de las características de protección que incluyen los WAAP/WAF tenemos las siguientes:

- Firmas
- Heurística
- Detección de anomalías
- Protección contra denegación de servicio distribuida (DDoS)
- Violaciones de acceso
- Manipulaciones de API

Tigo Business, en alianza con Cloudflare proveedor líder mundial en el mercado en soluciones de protección de aplicaciones, ofrece una propuesta de valor excepcional con nuestro servicio de WAF y AntiDDoS.

3.2.1 Propuesta de valor

El servicio de WAF y AntiDDoS está soportada sobre una plataforma de seguridad global en nube en modalidad “as a Service” para proteger las aplicaciones web y móviles en Internet de empresas contra ataques de Denegación de Servicio (DDoS Attacks), ataques de Aplicación Web (Capa 7) y bots, además de proporcionar la aceleración de contenido haciendo Cache y optimización de entrega en nuestra CDN. Es una solución de gran escalabilidad y fácil de usar a través de un panel único de control desde donde se configuran las todas las funcionalidades y se pueden integrar otros servicios SSE de Cloudflare.

[1] Requiere un add-on que se compra por separado del paquete base.

3.2.2 Características y beneficios

- Plataforma de Nube Global que permite una mayor disponibilidad del servicio del 100 % teórico al contar con más de 300 puntos de presencia (PoP) distribuidos a nivel mundial. https://www.cloudflare.com/network/
- **WAF con defensa por capas:**
    - Las reglas administradas ofrecen protección contra vulnerabilidades de día cero.
    - Las reglas OWASP que atienden el top 10 publicado más recientemente https://developers.cloudflare.com/waf/managed-rules/reference/owasp-core-ruleset/
    - Los conjuntos de reglas personalizadas ofrecen protección a medida para bloquear cualquier ataque.
    - Las comprobaciones de credenciales expuestas supervisan y bloquean el uso de credenciales robadas/expuestas para la apropiación de cuentas.
    - La detección de datos confidenciales alerta acerca de las respuestas que contienen datos confidenciales.
    - La limitación de conexiones avanzada impide los intentos de utilización abusiva y los ataques DDoS y por fuerza bruta junto con los controles centrados en API.
    - Las opciones de respuesta flexibles permiten el bloqueo, el registro, la limitación de velocidad o las pruebas de verificación.
    - Page Shield[2]: Protección del lado del cliente con validación de scripts relevante para páginas de pagos o formas.
- **Panel de administración unificado:** La plataforma de administración del servicio de WAF y antiDDoS también consolida la gestión de otros servicios de Ciberseguridad Cloudflare dentro del marco de SSE como lo son Zero Trust Network Access (ZTNA), Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Data Loss Prevention (DLP) y Remote Browser Isolation (RBI), entre otros.
- **Visibilidad de Aplicaciones y Analítica de Red**, para saber en tiempo real o mediante un histórico cuál es o ha sido el desempeño de la red en general o vista por aplicaciones, lo que ayudará a la toma de decisiones con datos y hechos que lo soporten, haciendo un uso más eficiente de sus recursos permitiendo hacer las inversiones a nivel de conectividad realmente necesarias.
- **Seguridad de aplicaciones:** a través de las capacidades de protección de aplicaciones en capa **3**, 4 y 7, protecciones por capas contra los ataques OWASP y los exploits emergentes, detección de evasiones y nuevos ataques, aprendizaje automático, protección AntiDDoS, bloquea la toma de control de cuentas, detecta la pérdida de datos y mucho más.
- Administración y Gestión Centralizada desde una única interfaz donde podrá visualizar el comportamiento de la red de su empresa. Tigo Business realiza el servicio gestionado de su ambiente.
- Soporte técnico 24/7/365

[2] Requiere un add-on que se compra por separado del paquete base.

3.2.3 Alcance de la implementación

Configuración de Web Application Firewall (WAF)

- Creación y gestión de cuentas administrativas en el ambiente
- Implementación de la línea base de seguridad para la protección de las aplicaciones Web
    - Activación y actualización de las reglas administradas: Reglas del WAF por defecto recomendadas por Cloudflare y el top ten de OWASP.
- Creación de Custom Rules: creación de reglas de bloqueo geográfico, reglas de bloqueo de acceso a portales administrativos, reglas de lista blanca para administradores de sitios web, reglas de excepción de monitoreo sobre paths específicos.

Configuración del Content Delivery Network

- Configuración de las reglas de caché y las políticas de expiración para maximizar la eficiencia del CDN
- Implementación de reglas para la optimización del contenido estático.

Configuración del DNS

- Implementación de los registros DNS en la plataforma según el caso de uso
- Implementación de uno de los escenarios soportados:
    - Migración completa de el o los dominios a la plataforma
    - Migración parcial de los dominios/subdominos basados en CNAME en la plataforma

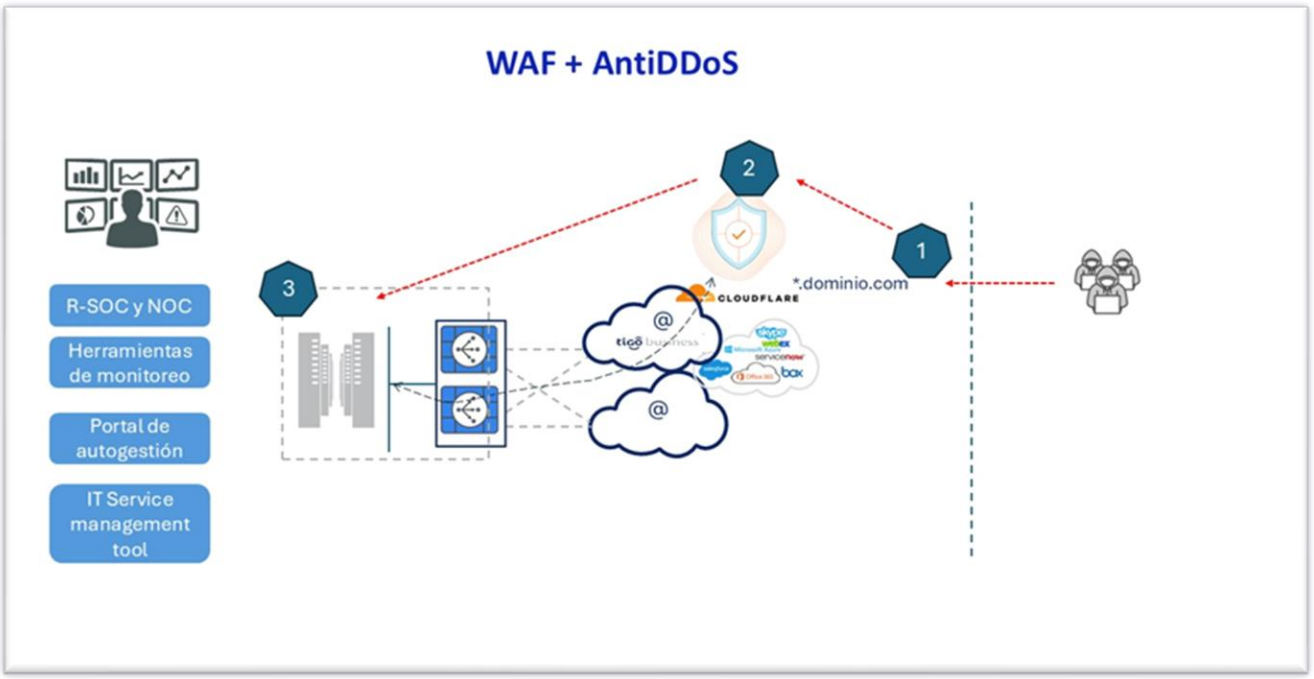
Configuración de protección contra DDoS

- Implementación de medidas de mitigación de ataques DDoS en capa de aplicación en la plataforma
- Ajuste de políticas de protección según el comportamiento del tráfico y las amenazas detectadas.

3.2.4 Arquitectura

- El servicio de WAF y Anti DDoS está basado en la tecnología del fabricante Cloudflare.
- El tráfico debe pasar por la nube (PoP) de Cloudflare
- Se debe realizar el registro DNS de los dominios a proteger con Clouflare
- Rate Limit (límite de conexiones o Control de conexiones). Se aplican reglas que consideran escenarios diferentes como país de origen, valores de campos, parámetros de HTTP como headers, cookies, campos JSON. Las capacidades de rate limit están limitadas a 100 reglas. los rate limits Incluye API rate limit.
- API shield: Se protegen los API de los dominios dados de alta con una identificación de los endpoints, métodos y rutas usan, así como secuencias esperadas y Lectura mediante esquemas e identificadores de sesión.
    - Consideraciones para API Shield:
        - Se recomienda tener una sincronía con los responsables del servicio de API.

- Límite y disponibilidad de un API: se recomienda limitar por rate limit debido a los posibles abusos automatizados (intencionales o accidentales).
- Licenciamiento: se requiere el add-on de API Shield.
- API shield aplica únicamente para REST API.



Esquema general de protección del servicio WAF y Anti DDoS

3.2.5 Atributos de seguridad WAF

Protección WAF

OWASP

- Broken access control
- cryptographic failure flaw
- Injection attacks
- Insecure design
- Misconfiguration vulnerabilities
- “vulnerable” or “outdated”
- Identification and authentication failures
- Software and data integrity failures
- Logging and monitoring failures
- Server Side Request Forgery (SSRF)

3.2.6 Atributos de seguridad AntiDDoS

- Tipos de ataques soportados por la protección AntiDDoS:
- UDP Fragment
- SNMPv2 XMAS flood Payload
- DNS
- ACK GRE Payload
- NTP
- RPC RIP SPSS
- CLDAP
- RESET QOTD QUIC
- Memcached
- ICMP IPMI Dahua
- OpenVPN
- FIN WS-DISCOVERY VxWorks
- UDP
- NetBIOS
- Teeworlds XDisplayManager
- CharGEN
- MSSQL VSE BitTorrent
- SYN
- TFTP
- LOIC Ubiquity
- SSDP
- MDNS Teamspeak CoAP
- SYN/ACK
- Amplificación DNS

3.2.7 Argo Smart Routing

La congestión de la red en Internet puede ralentizar los tiempos de carga de páginas. Argo Smart Routing detecta y enruta los puntos de congestión de la red en tiempo real para acelerar hasta más de un 30 % de media el rendimiento de las aplicaciones web.

Tiempos de Carga más Rápidos: Distribuye el tráfico web a través de las rutas de red más rápidas disponibles para acelerar notablemente el rendimiento de las aplicaciones y mejorar las experiencias de los usuarios.

Mayor Fiabilidad: Evita los puntos de congestión y utiliza las rutas más fiables para mejorar el tiempo activo.

Costes Reducidos: Minimiza las solicitudes de contenido al servidor de origen para reducir la latencia, la carga del servidor y el uso de ancho de banda.

Seguridad Integrada: Encripta el tráfico de extremo a extremo a través de la red de Cloudflare para proteger el tráfico web de los atacantes.

La red de Cloudflare enruta una media de 60 millones de solicitudes HTTP por segundo, lo que nos proporciona una visión única del flujo de tráfico en Internet. Argo Smart Routing utiliza esta información para detectar las rutas de red más rápidas y, a continuación, dirige de forma inteligente el tráfico web del cliente por esas rutas.

Argo Smart Routing entrega tráfico web y de otros protocolos, a través de los enlaces más rápidos disponibles, aumentando notablemente (más de 30%) la velocidad de los activos y mejorando la experiencia del usuario final.

3.2.8 Alcance del servicio WAF y Anti DDoS

Oferta		
Descripción del servicio	**Unidades de medida por Mes**	**Cantidad**
Managed DNS - DNS Queries	Millones de solicitudes	50
CDN - Total Data Transfer	TB	2
CDN - Requests	Millones de solicitudes	50
Primary Domains	Dominios	1
Advanced Manager Certification	Dominios	1
Bot Management	Millones de solicitudes	50
Argo	Incluído	
DDOs	Incluído	
Content Scanning	Incluído	
WAF	Incluido	
Soporte Telefónico 7/24	Incluido	
Success Plan	Standard Success	Enterprise

3.2.9 Portales a proteger con el servicio de WAF

Los siguientes son los portales web a proteger con el servicio de WAF y AntiDDoS según la información suministrada por el cliente, la oferta cubre un dominio principal y sus respectivos subdominios:

Nombre de la aplicación	Ambiente	DNS
Portal Insitucional Producción	Producción	iudigital.edu.co
Alistamiento Backend	Producción	backendsigpte.iudigital.edu.co
Alistamiento Frontend	Producción	sigpte.iudigital.edu.co
Certificados Estudiantes Backend	Producción	backcertiestudiantes.iudigital.edu.co
Certificados Estudiantes Frontend	Producción	certiestudiantes.iudigital.edu.co
Gestión Certificados Backend	Producción	backgestionadmin.iudigital.edu.co
Gestión Certificados Frontend	Producción	gestioncertificados.iudigital.edu.co
Daci Frontend	Producción	fronttransicion.iudigital.edu.co
Daci Backend	Producción	backtransicion.iudigital.edu.co
Carnetizacion Frontend	Producción	credenciales.iudigital.edu.co
Carnetizacion Backend	Producción	backcredenciales.iudigital.edu.co
Enlace Imagenes Portal Desarrollo	Desarrollo	test.iudigital.edu.co
Firmas Automáticas	Desarrollo	back1.iudigital.edu.co
Portal Joomla Desarrollo	Desarrollo	front1.iudigital.edu.co
Alistamiento Backend	Desarrollo	back2.iudigital.edu.co
Alistamiento Frontend	Desarrollo	front2.iudigital.edu.co
Dspace Backend	Desarrollo	back3.iudigital.edu.co
Dspace Frontend	Desarrollo	front3.iudigital.edu.co
Gestión Certificados Backend	Desarrollo	back4.iudigital.edu.co
Gestión Certificados Frontend	Desarrollo	front4.iudigital.edu.co
GLPI Actualizado	Desarrollo	back5.iudigital.edu.co
Carnetizacion Frontend	Desarrollo	back6.iudigital.edu.co
Carnetizacion Backend	Desarrollo	front6.iudigital.edu.co
DACI Backend	Desarrollo	back7.iudigital.edu.co
DACI Frontend	Desarrollo	front7.iudigital.edu.co
Subcuentas Backend	Desarrollo	back8.iudigital.edu.co
GLPI Infraestructura	Desarrollo	front8.iudigital.edu.co
Cartas	Desarrollo	back9.iudigital.edu.co
Plantillas Crea	Desarrollo	front9.iudigital.edu.co
Control Asistencia Backend	Desarrollo	back10.iudigital.edu.co
Control Asistencia Frontend	Desarrollo	front10.iudigital.edu.co

Insignias Backend	Desarrollo	back11.iudigital.edu.co
Insignias Frontend	Desarrollo	front11.iudigital.edu.co
Formulario Prácticas Backend	Desarrollo	back12.iudigital.edu.co
Formulario Prácticas Frontend	Desarrollo	front12.iudigital.edu.co
Certificados Estudiantes Backend	Desarrollo	back13.iudigital.edu.co
Certificados Estudiantes Frontend	Desarrollo	front13.iudigital.edu.co
n8n (Automatización)	Producción	n8n.iudigital.edu.co
OpenProject	Producción	project.iudigital.edu.co
Portal Desarrollo	Producción	portaldesarrollo.iudigital.edu.co
GitLab	Producción	gitlab.iudigital.edu.co
GLPI Servicios	Producción	servicios.iudigital.edu.co
Stack Monitoreo (Prometheus+Grafana)	Producción	monitoreo.iudigital.edu.co

NOTA: En caso de que se requieran agregar a la protección de WAF más dominios principales esto se debe validar en una nueva factibilidad ya que impactaría la oferta comercial

3.2.10 ADD-Ons:

- **API Shield:** protección y detección de APIs, convirtiendo la solución en un WAAP (Web Application and API Protection).
- **Bot Management:** La posibilidad de limitar tráfico de bots y poder insertar "retos" (challenges) automáticos o manuales con interacción del usuario. Este tráfico es constantemente cambiante y Cloudflare actualiza las detecciones con su servicio de Inteligencia.
- **Page Shield:** Un elemento importante que revisa ataques del lado del cliente, es decir, los scripts que puedan existir en las aplicaciones, sus interacciones (conexiones a sitios maliciosos o scripts identificados como maliciosos por la inteligencia de Cloudflare) y las interacciones con las cookies.
- **Load Balancing:** Es la capacidad distribuir cargas entre los servicios que se tienen protegidos con Cloudflare, pudiendo hacer distribuciones locales o globales. El balanceo tiene diferentes métodos para satisfacer necesidades de carga diferentes.

NOTA: La oferta contempla addon Bot Management y Smart Argo Routing

4 Implementación y/o Transición

4.1 Metodología de Aprovisionamiento

Para llevar a cabo la entrega de una solución operativa al cliente, Tigo asigna un Project Manager responsable de canalizar las necesidades y comunicaciones del cliente e integrar tecnológicamente los proveedores y aliados requeridos.

El Project Manager utiliza metodologías y herramientas de gestión de proyectos para realizar el aprovisionamiento de la solución. En el inicio y planificación del proyecto, analiza el alcance de la solución, identifica los riesgos y controles del proyecto, solicita los recursos requeridos y construye el plan de trabajo asociado.



4.2 Tiempo de Aprovisionamiento

La implementación del servicio tendrá una duración estimada de 60 días calendario, sujeta a la entrega oportuna de la documentación requerida y a la realización de las configuraciones necesarias por parte de ambas Entidades. Estas actividades se coordinarán en las mesas de trabajo técnicas que se realicen una vez legalizado el contrato.

Para el caso de la Coadministración los accesos a los diferentes aplicativos se entregarán durante el acta de entrega del cierre del proyecto.

El cliente podrá hacer ajustes necesarios de configuración durante el proceso de implementación con acompañamiento del PM que esté ajustado en el alcance del proyecto inicial.

CONSIDERACIONES TIEMPO DE IMPLEMENTACION

- En todo caso se realizará el mejor esfuerzo para tener implementado el servicio en el menor tiempo posible.

- No se consideran los tiempos imputables a configuraciones internas por parte del cliente en AWS.
- 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.

4.3 Entregables

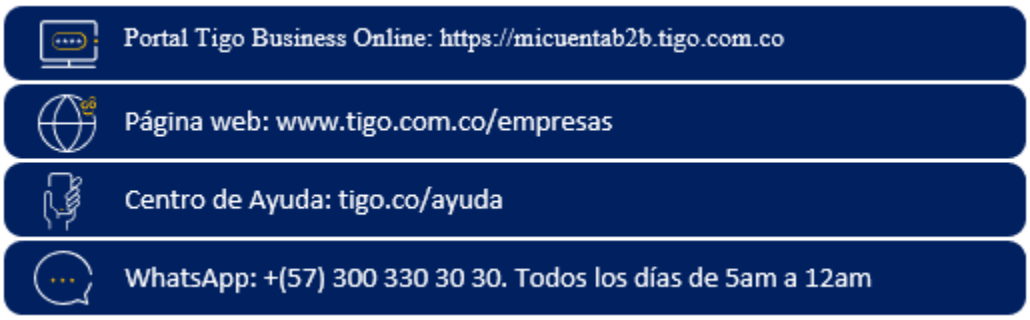
Entregable	Descripción
Acta de entrega	Documento donde se realiza verificación y entrega de cantidad, calidad y operatividad de la solución de acuerdo a lo establecido en la oferta técnica.

5 Condiciones de Servicio

5.1 Niveles de servicio y atención al cliente

En Tigo Business estamos comprometidos con el buen servicio y la calidad en la atención. Le presentamos a continuación nuestra Oferta de Servicio Posventa:
Canales de Atención.

Para brindarle una solución y orientación oportuna, contamos con diferentes canales digitales, en los cuales usted podrá autogestionar sus servicios, reportar fallas de sus productos, consultar y pagar su factura, radicar y consultar quejas sobre los valores facturados e incluso modificar su portafolio actual:



Si desea contactarnos telefónicamente, también hemos puesto a su disposición:

Línea gratuita nacional: + (57) 01 8000 513 287
Desde su celular Tigo: #513

5.2 Tiempo de atención y prestación del soporte en fallas

Impacto	Inicio de la solución	Tiempo objetivo de resolución	Tipo de Atención	Horario de Atención
Significativo	Inmediato	4 horas	Conexión remota, telefónica, correo	Lunes a domingo de 00:00 a 23:59 horas.
Moderado	Inmediato	10 horas	Conexión remota, telefónica, correo	Lunes a domingo de 00:00 a 23:59 horas.
Menor	4 horas	24 horas	Conexión remota, telefónica, correo	Lunes a domingo de 00:00 a 23:59 horas.

5.3 Delimitaciones

- No se considera tiempo on-hold cuando el cliente no ha entregado la información adecuada.
- Tiempos se consideran a partir de la apertura de tiquete de falla.
- Tiempo aplica únicamente para soporte remoto
- En los casos donde las vulnerabilidades, fallas o comportamientos no esperados de la solución prestada por Tigo sean atribuibles al sistema operativo del fabricante por

vulnerabilidades o bugs, Tigo queda exento de penalizaciones y los tiempos de atención y resolución pueden variar de acuerdo con los tiempos de respuesta y solución del fabricante.

- En cualquier caso, Tigo se compromete a buscar alternativas de solución viables y acordadas con el cliente final.

5.4 Escala de clasificación prioridades

A continuación, se describen las prioridades (impacto) y los criterios que se utiliza en el esquema operativo para clasificar las alertas y el tiempo de respuesta frente a ellas:

Impacto	Criterio
Significativo	• Problema mayor o incidente muy serio que compromete o detiene al negocio • 2 o más Intermitencias de servicio en dónde el período de afectación acumulado sea superior o igual a 30 minutos, en un día. • Caída total del servicio • Degradación de los servicios hasta el punto de que no puedan ser utilizados.
Moderado	• Problema significativo que ocasiona que los servicios estén degradados, genera un impacto limitado al negocio y afecta la productividad seriamente. • 2 o más Intermitencias de servicio en donde el período de afectación acumulado en un día sea menor a 30 minutos • Degradación de los servicios sin afectación total del mismo.
Menor	• Problema que causa ineficiencias en los procesos normales del negocio y no tienen un impacto cuantificable o significativo • No afecta ni degrada la prestación del servicio, se incluyen eventos en monitoreo • Intermitencias esporádicas con periodicidad de uno o más días y con duración menor a 5 minutos • Gestión de cambios en políticas, nuevas políticas, solicitud de información. • Solicitud de reconfiguración de policías • Solicitud de envío reporte automatizados descritos en la sección de reportes. • Resolución de consultas.

5.5 Facturación del servicio y PQRs

5.5.1 Peticiones, Quejas y Reclamos

Para la atención de sus PQRs y con el compromiso de brindar una atención oportuna y eficiente, los tiempos de respuesta son de 15 días hábiles. En Tigo Business trabajamos para que este tiempo sea menor, en función de la complejidad de la PQR. Para el registro de sus requerimientos es importante tener en cuenta las siguientes definiciones:

Petición:

- Requerimientos adicionales a los servicios contratados o modificaciones en los mismos
- Queja por Facturación: Cualquier manifestación de inconformidad asociada a los valores facturados.
- Queja por Servicio: Cualquier manifestación de inconformidad asociada a las condiciones y calidad en que se ha presentado o dejando de prestar los servicios.

Le invitamos a nuestros canales de atención para poder radicar su PQR y con gusto comenzaremos las validaciones y acciones a las que haya lugar.

Amparados en la ley 1341 de 2009, en donde se señalan las condiciones que rigen las relaciones entre los Usuarios y las Empresas Prestadoras de Servicios de Tecnologías de la Información y las Comunicaciones, aplica lo concerniente a los derechos descritos en el artículo 53 Ibídem; en este sentido al contrato que se suscriba no le es aplicable lo dispuesto por la CRC en materia del Régimen Integral de Protección de los Derechos de los Usuarios de los Servicios de Comunicaciones-.s, como también excluyendo la revisión de PQR´s (Peticiones, Quejas de Servicios, Quejas de Factura, Quejas de Daños o Sugerencias) por parte de la Superintendencia de Industria y Comercio.

Lo anterior, por cuanto la solución de los servicios ofrecidos no hace parte de la competencia de la mencionada entidad de control y vigilancia, dado que todas las características de red y de servicio y las condiciones técnicas, económicas y jurídicas serán negociadas y pactadas por mutuo acuerdo entre las partes del contrato.

6 Oferta Comercial

A continuación, se especifica el valor de la propuesta o solución a implementar:

6.1 Servicios recurrentes: Tarifas mensuales de operación del servicio en AWS – WAF y AntiDDoS Cloudflare

Servicio	Tarifa Mensual (Antes de IVA)	IVA (19%)	Total, Recurrente Mensual
AWS Cloud	$ 7.177.760	$ 0	$ 7.177.760
Soporte AWS	$ 0	$ 0	$ 0
Servicios Administrados Tigo	$ 1.076.664	$ 204.566	$ 1.281.230
Ciberseguridad Fortinet	$ 5.123.120	$ 0	$ 5.123.120
Ciberseguridad CloudFlare	$ 9.948.199	$ 0	$ 9.948.199
Total	**$ 23.325.743**	**$ 204.566**	**$ 23.530.309**

* 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 expresado en COP es únicamente de carácter referencial y no corresponde al valor final de facturación. La facturación se realizará mensualmente con base en la TRM aplicable en el mes de emisión de la factura y en el consumo real del servicio durante el período correspondiente.

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 soporte técnico y orientación de arquitectura de sus casos de uso específicos, directamente con AWS (No se incluye en esta propuesta).

6.2 Servicios no recurrentes o de único pago

Servicio	Pago Único	IVA (19%)	Total, Pago Único
Despliegue Servicios AWS	$ 10.402.500	$ 1.976.475	$ 12.378.975

6.2.1 Consideraciones comerciales

- El servicio se ofrece por un periodo mínimo de 12 meses.
- 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 del Sector Gobierno se facturará a la TRM de $ XXXX 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.

- Al adquirir Soluciones cloudflare y firmar la Orden de Compra y/o Servicio o el contrato entre las partes, el Cliente autorizará a TIGO a abrir una cuenta cloudflare a nombre del Cliente empleando una dirección de email válida de este, en. 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 cloudflare publicados en el siguiente enlace: https://www.cloudflare.com/es-es/privacypolicy/
- El cliente acepta que Tigo Business no tiene control directo sobre la infraestructura que soporta los servicios de cloudflare 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 cloudflare.
- El cliente acepta las políticas de cumplimiento de cloudflare plasmado en el siguiente enlace: https://www.cloudflare.com/es-es/enterpriseterms/
- Una vez el cliente tenga la cuenta activada en el dashboard, creará los usuarios administradores para TIGO business. Tigo Business tendrá acceso de administrador del portal del cliente para gestionar el servicio.
- Durante el periodo del contrato Tigo puede realizar Business Reviews para identificar si las capacidades dimensionadas inicialmente de transferencia de tráfico, dominios principales a proteger y add ons, entre otras, requieren revisión y ajuste del servicio contratado.
- En los casos donde las vulnerabilidades, fallas o comportamientos no esperados de la solución prestada por Tigo sean atribuibles al sistema operativo o hardware del fabricante por vulnerabilidades o bugs, Tigo queda exento de penalizaciones y los tiempos de atención y resolución pueden variar de acuerdo con los tiempos de respuesta y solución del fabricante. En cualquier caso, Tigo se compromete a buscar alternativas de solución viables y acordadas con el cliente final.
- Las reglas que se configurarán se basarán en la información recolectada en el SoW y los requisitos funcionales del proyecto.
- 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.
- 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.
- 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.

6.2.2 Consideraciones Entrega de Servicio

- 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.
- No se consideran los tiempos imputables a aspectos técnicos o de servicio bajo la responsabilidad del Cliente.
- Es necesario realizar la activación del licenciamiento para dar inicio al proceso de implementación, posterior a la reunión de kick-off, en la cual se alinea el alcance del proyecto. Esto implica que el paso a facturación se efectuará una vez se active el licenciamiento. Desde el día 1 de la implementación El PM (Order Manager) enviará el cronograma de implementación y, a partir de la primera sesión, se dará inicio al proceso de facturación, el cual se realizará a mes vencido.

6.3 Condiciones económicas

Tigo Business, podrá realizar facturas parciales, de acuerdo con las etapas de instalación o aprovisionamiento acordadas con el cliente. Igualmente, el cliente deberá realizar pagos relacionados con los saldos de las facturas presentadas bajo la conformidad de las tareas realizadas.

El contenido de esta propuesta es considerado por Tigo Business como información de uso exclusivo, y no debe ser reproducido sin la autorización previa y por escrito de Tigo Business. El material, ideas, enfoques y conceptos incluidos deben utilizarse única y exclusivamente con la finalidad de evaluar la idoneidad de la propuesta.

6.4 Compromisos del cliente

6.4.1 Responsabilidades del cliente

Como cliente se compromete a garantizar el suministro, exactitud y completitud de toda la información requerida por Tigo Business. Si la información es incompleta o incorrecta, cualquier retardo o requisito adicional que pueda generarse para corregir los problemas originados por el uso de tal información incompleta o inexacta será tratado como una solicitud de cambio del cliente al alcance del servicio, por lo tanto, estará sujeta al proceso de control de cambios, lo que implica una nueva factibilidad y posibles costos adicionales.

6.5 Recomendaciones de seguridad

En Tigo Business nos comprometemos con su seguridad, es por esto, que entregamos las siguientes recomendaciones:

Servicios que no deben estar expuestos directamente:

Gestión de infraestructura

- Telnet y FTP: transmiten credenciales sin cifrado.
- RDP (Remote Desktop): uno de los principales vectores de ransomware.
- SSH: debe restringirse por IP y no exponerse abiertamente

Bases de datos

MySQL, PostgreSQL, MongoDB, entre otras. El acceso público a bases de datos es una de las causas más frecuentes de fugas masivas de información.

Consolas administrativas

Protocolos de correo sin cifrar (SMTP, POP, IMAP). Consolas de administración accesibles desde Internet.

Monitoreo y almacenamiento Herramientas como Zabbix, Grafana, Prometheus o SNMP deben operar únicamente en redes privadas.

Buenas prácticas internacionales indican que estos servicios deben accederse **exclusivamente mediante VPN, redes privadas y controles de acceso estrictos.** En Tigo Business le ayudamos a **cerrar estas superficies de ataque sin afectar la operación,** mediante conectividad segura, segmentación y monitoreo continuo.

Las empresas que sufren menos incidentes no son las que tienen más herramientas, sino las que **aplican consistentemente buenas prácticas de seguridad.**

Basados en marcos como **Zero Trust y CIS Controls,** estas son las medidas que más impacto tienen en la protección de su entorno:

1. **Autenticación multifactor (MFA):** Reduce drásticamente el uso indebido de credenciales robadas
2. **Accesos restringidos por IP y firewall:** Solo su organización debe poder administrar sistemas críticos
3. **Cifrado obligatorio (TLS/SSL):** Toda comunicación debe viajar cifrada, sin excepciones.
4. **Auditorías y revisiones periódicas:** Las vulnerabilidades no detectadas son el principal riesgo oculto.
5. **Antivirus avanzado y EDR:** No solo previenen ransomware, también garantizan:
    - Continuidad operativa
    - Integridad de la información
    - Cumplimiento normativo
    - Protección financiera ante incidentes

La evidencia demuestra que aplicar estas prácticas reduce de forma significativa los tiempos de recuperación y el impacto económico de un ataque.

6.6 Acuerdo de Confidencialidad

Las partes, se comprometen a mantener en reserva la información que obtenga, conozca y desarrolle con ocasión de los servicios objeto de este contrato

6.7 Consideraciones generales

Hace parte de la presente oferta las siguientes consideraciones a efectos de establecer el alcance de las actividades y compromisos de las partes para la adecuada prestación de los servicios contratados:

1.Definiciones:

Incidente de seguridad digital: Ocurrencia de una situación que pone en peligro la confidencialidad, integridad o disponibilidad de un sistema de información o la información que el sistema procesa, almacena o transmite; o que constituye una violación a las políticas de seguridad, procedimientos de seguridad o políticas de uso aceptable.
Infraestructura crítica cibernética: Sistemas y activos, físicos o virtuales, soportados por Tecnologías la Seguridad de la Información, cuya afectación significativa tendría un impacto grave en el bienestar social o económico de los ciudadanos, o en el funcionamiento efectivo del gobierno o la economía.
Ciberseguridad: Es el proceso de proteger los activos de información por medio del tratamiento de las amenazas a la información que es procesada, almacenada y/o transportada a través de sistemas de información interconectados.
Incidente de Seguridad: Es un evento inesperado y no deseado que compromete la Seguridad de la Información.
Evento de seguridad: Un evento de seguridad de la información indica que el sistema, la seguridad o los servicios de red y de infraestructura han sido comprometidos o vulnerados. Esto indica que los controles implementados han fallado y/o que no se ha seguido la política de seguridad de la información de la organización
Cualquier ocurrencia relacionada con los activos o el entorno que indique un posible compromiso de las políticas o la falla de los controles, o incluso una situación no asignada que pueda afectar a la seguridad.

LIMITACIONES DE RESPONSABILIDAD: TIGO BUSSINESS no será responsable por la prestación del servicio en los siguientes eventos:
1. Cuando las interrupciones, caídas, problemas o deficiencias en los servicios o afectación de indicadores tengan origen en la infraestructura física y tecnológica del CLIENTE.
2. En los eventos de errores, decisiones, cambios en procesos y procedimientos por parte de EL CLIENTE que no hayan sido oportunamente informados al SOC.
3. En aquellos casos en los cuales los sistemas, plataformas y aplicativos del CLIENTE que no hagan parte de los sistemas, servicios o componentes de los servicios Ciberseguridad contratados, y éstos tengan falencias de seguridad que faciliten eventos de fraudes, hayan sido o no detectadas y/o advertidas por TIGO BUSINESS.
4. Por fuerza mayor o caso fortuito.
En caso de presentarse suspensión o afectación del servicio por cualquiera de los eventos señalados en los numerales 1 ,2 y 3 el cliente asumirá los costos en los que incurrió TIGO BUSSINESS, por la no prestación del servicio, durante el período de tiempo que dure la suspensión o afectación del mismo.

OBLIGACIONES ADICIONALES DEL CLIENTE: EL CLIENTE deberá realizar copias de seguridad de su información en el medio que considere pertinente.

EL CLIENTE es el directo responsable de la Información que se ingrese procese, genere y mantenga en relación del uso de sus equipos y servicios de CIBERSEGURIDAD y deberá garantizar el cumplimiento adecuado y oportuno de la implementación de las mejores prácticas que el equipo de SOC , NOC remoto le informe.

El cliente será responsable de implementar las configuraciones y demás recomendaciones que le entregue TIGO BUSINESS en aras de cumplir con el alcance de los servicios ofrecidos. En caso de que éstas no sean debidamente implementadas en su totalidad, TIGO BUSINESS no será responsable de los efectos, vulnerabilidad, amenazas o efecto adverso que se derive de esta situación.

Es responsable de autorizar la contención de los riesgos detectados y notificados; de no autorizar la contención, TIGO no será responsable de los riesgos o la posible materialización de un evento de seguridad.

6.8 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.

REGIMEN DE RESPONSABILIDAD

Igualmente y tratándose de Servicios Administrados de Ofimática, Conectividad, Voz y Colaboración, Movilidad, Infraestructura de TI, Cloud, Data Center, Servicios Administrados y Seguridad, TIGO BUSSINESS no garantiza resultado alguno por los usos y/o aplicaciones específicos que realice EL CLIENTE y de manera particular por: (a) Interrupciones de los servicios originadas en causas ajenas a su control, tales como: mal funcionamiento de Internet, problemas satelitales, interrupción o insuficiencia de energía eléctrica, huelgas, desastres naturales, conflictos bélicos, actos de la autoridad, etc.; (b) pérdida de datos almacenados en el servidor, ya sea por causas imputables al CLIENTE, por fallas en el sistema, por eventos o incidentes de seguridad perpetuados por terceros (por ejemplo ataques de denegación de servicio, virus, malware, ransomware, entre otros) que comprometan la integridad, confidencialidad o la disponibilidad de la información o por actualización de los servidores; (c) demoras en los trámites de Registro de Dominio y transferencias de DNS por causas imputables al CLIENTE o a terceros; (d) por fraude cometido por El CLIENTE o por terceros; (e) por fallas de tipo técnico tales como la seguridad informática de los ambientes en hosting, cloud y de soluciones de terceros atribuibles al CLIENTE o a terceros; (f) en caso de ataques informáticos a los PBX por causas imputables al CLIENTE. En caso de que en la Orden de Compra y/o Servicio se incluya la entrega al CLIENTE de cuentas administradoras de cualquier servicio, EL CLIENTE exime a TIGO BUSSINESS de cualquier evento de indisponibilidad, seguridad y confidencialidad que pueda ocurrir. Adicionalmente, en los casos en que EL CLIENTE solicite deshabilitar y/o desinstalar las herramientas de Antivirus implementadas por TIGO BUSSINESS o por un tercero para proteger los servicios, EL CLIENTE exime a TIGO BUSSINESS de cualquier evento de indisponibilidad, seguridad, confidencialidad, virus, malware, ransomware o cualquier otro software malicioso que pueda generar algún tipo de afectación durante la prestación del servicio. Esto aplica para cualquier servicio que se pueda afectar con la deshabilitación solicitada. Parágrafo: Cuando se trate de servicios de Cloud para distribuidores o revendedores, TIGO BUSSINESS no será responsable de la prestación o suministro de servicios (venta, aprovisionamiento, soporte técnico, licenciamiento y demás) frente al cliente final.

Exclusión de responsabilidad por daños indirectos y otros. Sin perjuicio de los casos en que la ley aplicable prohíba la limitación de responsabilidad por daños, TIGO BUSINESS no se responsabilizará en ningún caso de daños directos e indirectos, cualquiera que sea su naturaleza u origen incluidos, entre otros los daños por lucro cesante, pérdida de la información confidencial o de otro tipo, interrupción de negocios, pérdida de privacidad, incumplimiento de obligaciones (ya sea de buena fe o con diligencia razonable, negligencia y cualquier perdida pecuniaria o de otro tipo)], que se deriven o de otro modo este relacionados con la materialización de un incidente de seguridad. Tigo BUSINESS se excluye expresamente cualquier responsabilidad por falta de disponibilidad del servicio y/o de equipos del CLIENTE en un momento determinado, ya sea por causas técnicas, tareas de mantenimiento del sistema no notificadas al SOC, falla eléctrica en las instalaciones del CLIENTE y todas aquellas que estén bajo su control y gestión.

7 Compromisos del Cliente

Adicional a lo indicado en la oferta técnica y económica, el cliente se compromete a:

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 TigoUne 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.

Propiedad intelectual e industrial
Toda invención, modelo de utilidad o diseño industrial creado por TigoUne en cumplimiento de esta oferta será propiedad de Tigo conforme al Decreto 2591 de 2000, que reglamenta los Títulos II, III y V de la Decisión 486 de la Comisión de la Comunidad Andina. Por ende, el derecho a la patente de invención o de modelo de utilidad, o del registro del diseño industrial será titularidad de Tigo

USO DE LOS SERVICIOS

EL CLIENTE se obliga a acatar el régimen nacional e internacional sobre protección de terceros y derechos de propiedad intelectual, en especial las disposiciones establecidas en los tratados internaciones que vinculan a Colombia. Así mismo se compromete a cumplir las disposiciones de la Ley 679 de 2001 y sus decretos reglamentarios, teniendo en cuenta que su incumplimiento le acarreará las sanciones administrativas y penales allí contempladas impuestas por la autoridad competente; en tal sentido, deberá abstenerse de enviar, recibir, distribuir, transportar, almacenar y utilizar o archivar material pornográfico o de contenido sexual con utilización de menores de edad, así como de usar las redes globales de información para divulgación de material ilegal con menores de edad

8 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.