Regional Security Operations Center (R-SOC) de Tigo Business

Oferta técnico comercial

Renovación Servicios SIEM/SOC con Integración plataformas

INSTITUCIÓN UNIVERSITARIA DIGITAL DE ANTIOQUIA - IU DIGITAL

Los servicios de CiberSeguridad son prestados por UNE EPM Telecomunicaciones S.A. Este documento contiene información confidencial perteneciente a Tigo Business, constituyendo secreto empresarial; por tanto, la información aquí consignada no deberá ser utilizada, parcial o totalmente, para fines diferentes al propósito de este documento; excepto en aquellos casos aprobados previamente por Tigo Business.

Medellín, 20 de agosto de 2026

Señores
INSTITUCIÓN UNIVERSITARIA DIGITAL DE ANTIOQUIA - IU DIGITAL
Medellín

ASUNTO: PROPUESTA COMERCIAL RENOVACIÓN R-SOC

En Tigo Business, trabajamos día a día por ofrecer mejores soluciones de tecnologías de información y comunicaciones a nuestros clientes. Contamos con una moderna y robusta infraestructura para ofrecer a su compañía/entidad servicios de alta calidad y confiabilidad.

En esta propuesta se describe el alcance de la solución ofrecida por Tigo Business con el propósito de escanear su sitio web, para lograr identificar las vulnerabilidades que apoyan la eficiencia, productividad y comunicación en (nombre empresa o entidad).

Agradecemos la confianza depositada en Tigo Business para la ejecución de esta actividad

Cualquier inquietud o aclaración adicional al respecto, estaremos atentos para responderle a la mayor brevedad.

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

ACUERDO DE CONFIDENCIALIDAD (verificar según el producto/solución)
Este documento contiene información confidencial perteneciente a Tigo Business. y constituye secreto industrial y comercial. Esta información se entrega con el entendimiento de que será manejada bajo la más estricta confidencialidad. La información no deberá ser revelada, duplicada o usada en su totalidad ni en parte, para ningún otro propósito que no sea la evaluación de este material. De ninguna manera los asuntos descritos en este documento pueden ser revelados a otras personas, sólo a aquellas personas que sean aprobadas por Tigo Business

REGIONAL SECURITY OPERATIONS CENTER (R-SOC) de TIGO BUSINESS

1 INTRODUCCIÓN

El portafolio de soluciones de los servicios de ciberseguridad de TIGO Business se enfoca en el resguardo y la protección de la confidencialidad de integridad de los datos de las empresas, bajo el estricto cumplimiento de estándares internacionales y con certificaciones que garantizan la continuidad del negocio y la seguridad de la información. El Regional SOC de Tigo Business es el único que tiene las certificaciones ISO 27001, ISO 20000-1 entre otras, confirmando así el compromiso de implementar las mejores prácticas, medidas, controles y políticas de ciberseguridad y de entrega de servicios.

1.1 Principales Beneficios

- Envío notificaciones y alertas de eventos de seguridad.
- Detección de eventos de seguridad críticos y recomendaciones de buenas prácticas utilizando procedimientos basados en normas y estándares internacionales para la atención de estos.
- La reducción de riesgos tecnológicos mediante alertas de eventos de seguridad.
- Respuesta a incidentes en alineación con los estándares ISO y NIST.
- Mejora continua en los procesos tecnológicos con una asesoría constante sobre sus plataformas tecnológicas.
- Equipo de profesionales altamente especializados y con certificaciones en ciberseguridad, dedicados a vigilar la seguridad de su red las 24 horas del día durante los 365 días del año.
- Oportunidad de focalizar su atención a los procesos directamente relacionados con su negocio.
- Presencia y capacidad de gestión a nivel regional.

1.2 Propuesta de valor

Nuestro equipo de SOC Regional de Tigo Business está dedicado a brindar soluciones completas de ciberseguridad para nuestros clientes B2B. A través de nuestros servicios de monitoreo, gestión y soporte, ofrecemos:

- **Protección continua y proactiva:** Supervisamos y analizamos constantemente su infraestructura de TI para identificar cualquier actividad maliciosa y amenaza potencial. Utilizamos tecnologías avanzadas de detección y análisis de amenazas para garantizar una protección continua y proactiva.
- **Respuesta inmediata y eficiente a incidentes:** En caso de un incidente de seguridad, nuestro equipo actúa rápidamente para mitigar el impacto y minimizar el tiempo de inactividad. Contamos con procedimientos establecidos y expertos capacitados que están preparados para responder de manera eficiente y efectiva ante cualquier amenaza o intrusión.
- **Análisis y recomendaciones de mejora:** En situaciones de incidentes de seguridad, realizamos un análisis forense exhaustivo para comprender las causas raíz y tomar medidas correctivas.

Además, proporcionamos recomendaciones de mejora basadas en las lecciones aprendidas, con el objetivo de fortalecer su infraestructura de seguridad y prevenir futuros incidentes.

- **Soporte técnico especializado las 24/7:** Nuestro equipo del SOC Regional está disponible las 24 horas, los 7 días de la semana, para brindarle soporte técnico especializado. Ya sea que necesite asesoramiento sobre políticas de seguridad, asistencia en tiempo real durante una situación crítica o consultas generales, estamos aquí para ayudarle en todo momento.

2 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

3 LIMITACIONES DE RESPONSABILIDADES

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.
5. 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.

6. Cuando TIGO BUSSINESS hizo la respectiva recomendación para la remediación de la vulnerabilidad y el cliente no la ejecutó.
7. TIGO no será responsable de remediar los eventos de seguridad, intervención de hardware, aplicaciones o servicios pertenecientes al cliente.
8. La captura y correlación de datos, alertas, alarmas y reportes que resulten del monitoreo no implica per-se la resolución de incidentes de seguridad. En cada caso el SOC de TIGO requerirá comunicarse con los responsables designados por el cliente para consultar, evaluar y acordar la respuesta apropiada para mitigar cada incidente detectado.
9. Las notificaciones o alertas, independientes a las de seguridad, que el cliente desea recibir estarán limitadas, única y exclusivamente, a los casos de uso que se definan en el FortiSIEM previo acuerdo con el cliente y que se definen en la etapa de implementación.
10. TIGO entregará al cliente un (1) usuario de lectura para el acceso en el FortiSIEM.
11. La presente oferta NO incluye SOAR.

3.1 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. (No aplica plan de Monitoreo)

3.2 Régimen 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.

4 DESCRIPCIÓN DEL SERVICIO

Los servicios certificados del RSOC (Regional Security Operations Center) de TIGO Business brindan el monitoreo y gestión de sus sistemas informáticos para prevenir incidentes de seguridad las 24 horas de los 365 días del año.

El RSOC es operado por un equipo de profesionales certificados y especializados en la atención de problemas técnicos, operativos y de mantenimiento distribuidos en toda la región. El equipo asignado para la resolución de casos contará con conocimientos previos sobre la arquitectura e instalación de la solución de los servicios y plataformas del Cliente, con el fin de resolver de manera efectiva cualquier problema que se presente según los niveles de severidad y tiempos de respuesta descritos en el presente documento.

5 ALCANCE DEL SERVICIO DE R-SOC

Tigo Business ofrece el siguiente plan de la renovación del servicio de Monitoreo R-SOC

Atributos	R-SOC Monitoreo
Implementación de dashboards y reportes autogestionados para monitoreo.	✅
Notificación de alertas de alto riesgo para evento de seguridad.	✅
Recomendación de buenas prácticas de seguridad basadas en las plataformas monitoreadas (cuando aplique).	✅

5.1 Alcance Plan R-SOC Monitoreo

El sistema de monitoreo de TIGO Business es una avanzada plataforma que ofrece la disminución de los riesgos tecnológicos al detectar de manera temprana y notificar rápidamente los eventos de seguridad. Para lograrlo, es necesario configurar un túnel VPN hacia el colector de eventos en el Centro de Datos de Tigo Business, lo que permite colectar y transmitir información de manera segura, trasladándola luego a la plataforma central.

Uno de los aspectos más destacados de esta plataforma es su completa integración, que abarca múltiples marcas y plataformas, permitiendo centralizar todas las soluciones del Cliente en un solo lugar.

5.1.1 Alcance herramienta FortiSIEM

Detalle del servicio ofertado (Línea Base)

SKU	FC1-10-FSM98-180-02-12- Cantidad:50
Descripción	FC1-10-FSM98-180-02-12 FortiSIEM All-In-One Subscription License 1 Year Per Device Subscription License that manages minimum 50 devices, 10 EPS/Device. Does not include Maintenance & Support
SKU	FC1-10-FSM98-182-02-12- Cantidad:50
Descripción	FortiSIEM Subscription License for Advanced Agents 1 Year Per Agent Subscription License - Log & FIM - minimum 50 Advanced Agents. Does not include Maintenance & Support.
SKU	FC2-10-FSM97-248-02-12- Cantidad:1
Descripción	FortiCare Support for Software based FortiSIEM deployments 1 Year FortiCare Premium Support (1 - 100 points) for FortiSIEM Software deployments. 1 "Device" or 2 "End points" or 3 "Advanced Agents - Log & FIM" or 10 “Advanced Agents - UEBA Telemetry" equals 1 point.

Arquitectura DC TIGO

Se mantendrá la plataforma dimensionada para el SIEM la cual consta de lo siguiente, un VDC en DC Tigo con el FortiSIEM virtual all-in-one, la capa de seguridad estará compuesta por una VDOM dedicada con los módulos de FW, VPN S2S e IPS habilitados, a esta VDOM se conectará un servicio de internet dedicado de 30M para terminar los túneles Ipsec y recibir los logs de las diferentes fuentes de información

Detalle de los Servicios de Ciberseguridad (VDOM Dedicada)

A continuación, se presentan los valores de los atributos de ciberseguridad que hacen parte de la presente oferta:

Características del servicio

Firewall Cloud	Especificación de las Variables
Tipo de Arquitectura	Dedicada
Desempeño (Mbps)	30
Número de Sesiones Concurrentes	6000
Número de Reglas	10
Alta Disponibilidad	Si
ID del Servicio de Internet a impactar	Internet DC 30M

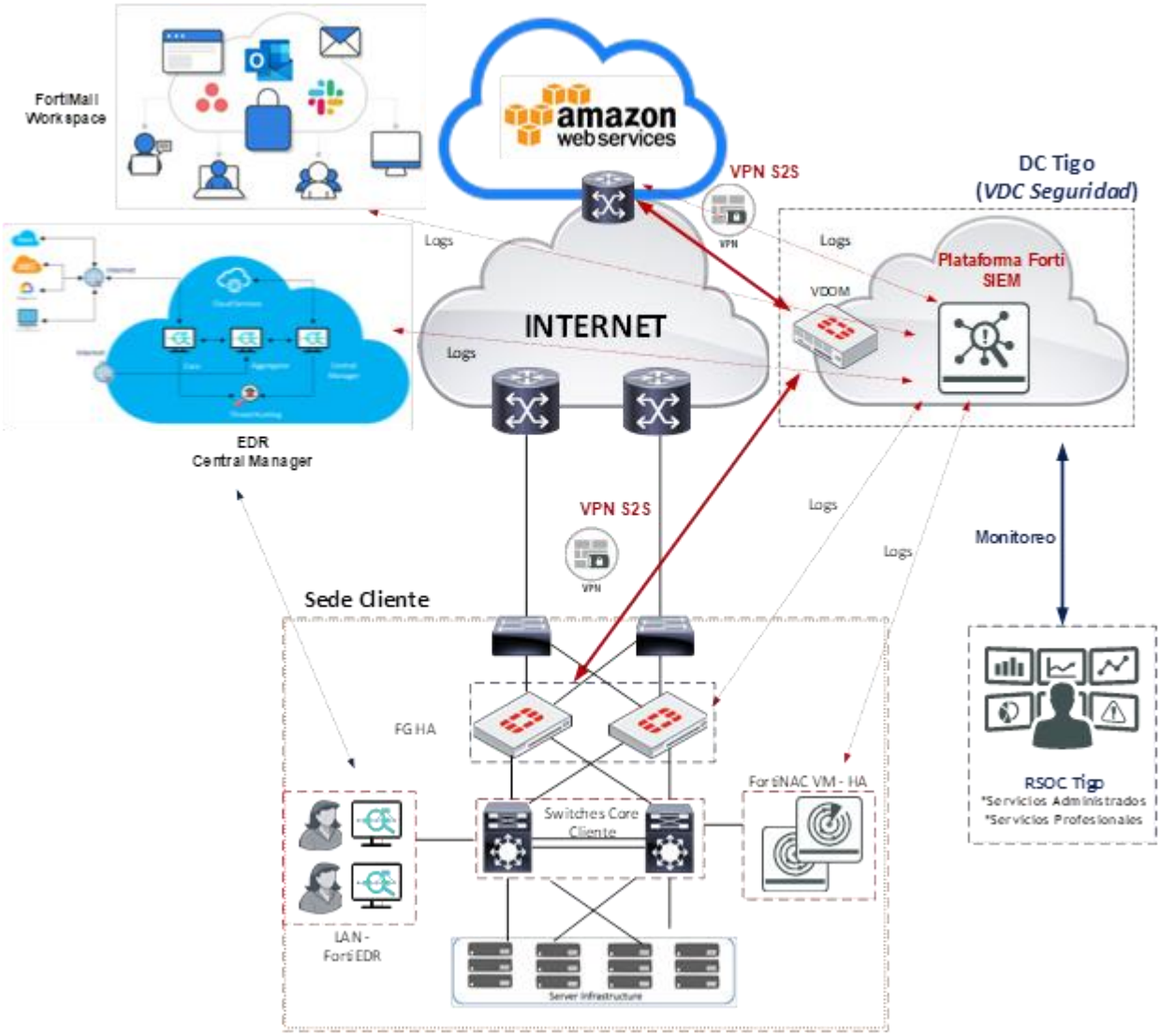
IDS/IPS Cloud	Especificación de las Variables
Tipo de Arquitectura	Dedicada
Desempeño (Mbps)	30
Número de Sesiones Concurrentes	6000
Alta Disponibilidad	SI
Número de Perfiles	2
ID del Servicio de Internet a impactar	Internet DC 30M

VPN Client to Site IPSec Cloud	Especificación de las Variables
Tipo de Arquitectura	Dedicada
Desempeño (Mbps)	30
Número de Usuarios	2
Número de Sesiones Concurrentes	6000
Alta Disponibilidad	Si
Recuperación de Desastres (Si o No)	NO
ID del Servicio de Internet a impactar	Internet DC 30M

VPN Site to Site Cloud	Especificación de las Variables
Tipo de Arquitectura	Dedicada
Desempeño (Mbps)	30
Número de Sesiones Concurrentes	6000
Número de Túneles Site to Site	2
Alta Disponibilidad	Si

Recuperación de Desastres (Si o No)	NO
ID del Servicio de Internet a impactar	Internet DC 30M

5.1.2 Arquitectura



*Arquitectura de Referencia

5.1.3 Consideraciones Técnicas

- No se incluyen elementos o componentes diferentes a los ofertados en este anexo
- Según la necesidad particular del cliente, en caso de requerirse algún componente adicional que no esté contemplado en esta oferta, se validara con el cliente en una nueva factibilidad
- El alcance tecnológico y de funcionalidades de la solución de (FortiSIEM) está delimitado al licenciamiento del SKU ofertado.

- En el Monitoreo SIEM se soporta un número máximo de 10 EPS (Eventos por Segundo, por sus siglas en inglés) por dispositivo, es decir, que cada dispositivo monitoreado con el SIEM puede configurarse con un número máximo de 10 logs que generen mensajes o eventos hacia el SIEM.
- La plataforma FortiSIEM actualmente soporta actualmente hasta 500 EPS
- Se incluyen servicios profesionales para la configuración de la solución
- TIGO propone reglas preestablecidas para el monitoreo de dispositivos del cliente, no obstante, el cliente puede solicitar la configuración de máximo tres (3) reglas particulares para el monitoreo de dispositivos (servidores, aplicaciones, equipos de red) propiedad del cliente. Las reglas particulares solicitadas por el cliente son evaluadas por TIGO para determinar la viabilidad de su implementación. No se garantiza que toda regla particular pueda ser implementada.
- Los dispositivos a monitorear deben tener capacidad Syslog o poder soportar la instalación de un Agente Syslog
- Las fuentes que se van a monitorear deben ser compatibles con alguno de los protocolos o métodos que se describen en la tabla recursos a monitorear y en la columna protocolos soportados
- El hecho de que el FortiSIEM soporte tráfico Syslog de un dispositivo no garantiza que soporte tráfico SNMP (Traps) de dicho dispositivo. Se deberá validar previamente si el dispositivo es soportado.
- Es necesario que el SOC TIGO valide previamente la información y clasificación de los logs enviados por los dispositivos del cliente para determinar si dicha información puede procesarse y ser útil. Esto aplica principalmente cuando los dispositivos utilizan variaciones de Syslog y SNMP.
- El cliente se hace responsable de la instalación de los agentes en aquellos componentes a monitorear que no tienen la capacidad de enviar syslog ejem servidores.
- Tigo incluye el computo necesario para el aprovisionamiento de los sku ofertados de FortiSIEM.

5.1.4 Requisitos por parte del cliente

- El cliente se compromete a definir y mantener matrices de comunicación en tres niveles: técnico-operativo, seguridad y responsable del servicio. Estas matrices deben incluir información de contacto actualizada, roles y responsabilidades de las partes involucradas, y los canales de comunicación preferidos.
- El cliente se compromete a transferir el acceso administrativo en caso de ser necesario a las soluciones aportadas por el RSOC. Esto implica proporcionar los permisos y credenciales necesarios para que el equipo del RSOC pueda llevar a cabo la gestión completa de las soluciones de seguridad. El cliente mantendrá un acceso de lectura y reportes autogestionados y de acuerdo con el plan contratado en cada una de las soluciones, con el fin de supervisar y obtener información sobre el estado de seguridad de sus sistemas.
- El cliente deberá colaborar activamente con el equipo del RSOC en la identificación y respuesta a incidentes de seguridad. Esto incluye la provisión oportuna de información detallada sobre posibles amenazas o incidentes de seguridad, así como la implementación de las recomendaciones y medidas correctivas propuestas por el equipo de Tigo Business, de acuerdo con el plan contratado.
- El cliente se compromete a mantener actualizada la información de contactos de emergencia y notificación de alertas de eventos de seguridad. Además, se espera que el cliente notifique de

manera inmediata al RSOC sobre cualquier evento de seguridad que pueda afectar la operación normal de la red o los sistemas críticos.

- El cliente ante eventos de pruebas, verificaciones, deberá informar a Tigo Business para la gestión de falsos positivos.
- El cliente es responsable de gestionar el ciclo de vida de licenciamiento de sus equipos y plataformas asociadas.

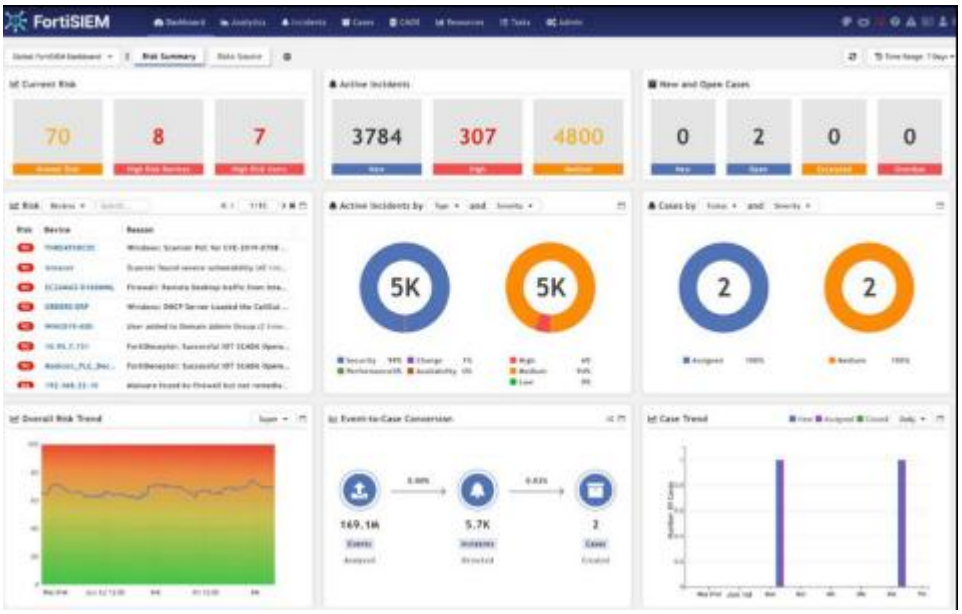
5.2 Recursos a Monitorear con el SIEM

Cantidad	Ubicación
Fuentes de información: • Equipos Fortigate Cliente (Plan: Monitoreo) • Servidores: On premises: Virtuales – físicos:15, AWS: 2 VM (Solo Monitoreo) • Servicio FortiNAC, Servicio FortiMail y Servicio FortiEDR	Sede cliente – Plataformas nube (FortiMail - EDR)

5.3 Entregables

5.3.1 Tableros de Monitoreo

Dentro del sistema de monitoreo utilizado por el RSOC para mantener niveles de seguridad altos y riesgos bajos, se ha desarrollado una interfaz de acceso que permite a nuestros clientes tener una visión en tiempo real del comportamiento de sus eventos de seguridad. Esta interfaz cuenta con tableros de monitoreo los cuales le permiten descargar reportes existentes o bien realizar vistas personalizadas de información, lo que brinda a nuestros clientes la visibilidad completa de la gestión de la seguridad de los recursos que administran. Al dar de alta el servicio, se proporcionará a nuestros clientes acceso a su consola de monitoreo, para que puedan visualizar sus tableros de forma autónoma.



5.3.2 Reporte Automatizado

Se realizará el envío de un (1) Reporte automatizado de manera mensual. Este reporte esta diseñados para ofrecer una visión detallada de las actividades relevantes en materia de eventos de seguridad, con el objetivo de mantenerlos informados y protegidos. Este reporte será enviado al contacto descrito para recibir notificaciones.

- El reporte incluido en el servicio será descargado directamente de la plataforma.

5.3.3 Delimitaciones

1. El servicio no incluye la atención en las sedes del cliente.
2. No incluye la administración de otros productos que no estén mencionados en este servicio.
3. No incluye informes o reportes adicionales, sólo lo que está definido en la sección de entregables.
4. Todos los dispositivos gestionados por el equipo de R-SOC deberán contar con licenciamiento adecuado y legítimo, este licenciamiento deberá ser renovado en su debido momento por el cliente. El equipo de R-SOC no realizara notificaciones sobre estado de licenciamiento. En caso se tenga un evento de seguridad y el licenciamiento no esté disponible el equipo de R-SOC no tendrá responsabilidad alguna.
5. Es responsabilidad del cliente asegurar alimentación eléctrica, espacio y ambiente de los dispositivos, debido a que los SLA asociados al servicio de R-SOC no contemplan fallas o incidentes relacionados al hardware y/o ubicación de este.
6. La capacidad de corrección se centra en abordar la anomalía que generó la vulnerabilidad, aunque no abarca la recuperación de información que eventualmente pudo haberse perdido en este proceso.

5.4 Integraciones con FortiSIEM

La integración de las soluciones FortiNAC, FortiMail y FortiEDR con FortiSIEM, para la recepción, normalización y correlación de los logs y eventos de seguridad, con el fin de centralizar su monitoreo y facilitar la gestión y análisis de incidentes.

Esta integración significa conectar FortiNAC, FortiMail y FortiEDR con FortiSIEM para que FortiSIEM reciba y procese los eventos de seguridad generados por esas plataformas.

- **Configuración de comunicación:** establecer cómo cada solución enviará sus eventos a FortiSIEM.
- **Recepción de logs:** verificar que FortiSIEM esté recibiendo correctamente los eventos de FortiNAC, FortiMail y FortiEDR.
- **Normalización:** convertir los eventos de las diferentes plataformas a un formato que FortiSIEM pueda analizar.
- **Correlación**: crear o configurar reglas para relacionar eventos de diferentes soluciones y detectar posibles incidentes.
- **Validación**: realizar pruebas para confirmar que los eventos llegan, se interpretan y generan las alertas correspondientes.

5.4.1 FortiNAC

FortiNAC es la solución de control de acceso de Fortinet, que complementa la arquitectura Security Fabric con funcionalidades de visibilidad, control y respuesta automatizada, extendiendo el control a cualquier parte de la red de acceso, incluso en entornos multifabricante. Así, FortiNAC proporciona protección adicional contra las amenazas ligadas a la popularidad de los dispositivos IoT, y extiende la seguridad del Security Fabric a dispositivos de otros fabricantes, facilitando además la orquestación de respuestas automatizadas ante los eventos de red y seguridad que puedan ocurrir en la organización.

Dimensionamiento de Equipos

A continuación, se describen los SKU y cantidades ofertados para el servicio de NAC

Ref de Equipo	Cant	Descripción
FNC-CAX-VM	2	FortiNAC Control and Application next-gen VM Server (VMWare/Hyper-V/AWS/Azure/KVM).
FC-10-FNVXA-248-02-12	2	FortiCare Premium Support
FC6-10-FNAC1-209-01-12	1	FortiNAC Subscription PRO License for 1.000 concurrent endpoint devices. Pro license level provides the ultimate in visibility, control and response.

Integración 1: FortiNAC

ID Caso de Uso	Nombre del Caso de Uso	Descripción y Lógica FortiSIEM	Métrica de Valor / Resultado Esperado
UC-NAC-01	Detección de Dispositivo Desconocido o No Permitido en Red	Regla en FortiSIEM que detecta cuando FortiNAC registra un dispositivo en estado Unregistered o Rogue intentando asociarse a un puerto/VLAN.	Incidente generado con severidad Media. Permite identificar intentos de conexión no autorizados en capa de acceso.
UC-NAC-02	Aislamiento/Quarantine de Host por Incumplimiento de Postura	Regla basada en eventos de cambio de estado a Quarantine reportados por FortiNAC tras fallar chequeos de postura (Compliance Fail).	Incidente generado en FortiSIEM asociando la dirección IP/MAC del endpoint y la razón de aislamiento.
UC-NAC-03	Anomalía de Autenticación Masiva en Acceso de Red	Regla basada en umbral (Threshold Rule) que alerta si un puerto/switch registra más de X fallos de autenticación 802.1X reportados por FortiNAC en 5 minutos.	Detección temprana de ataques de fuerza bruta en capa 2 o fallos masivos en supplicants 802.1X.

5.4.1 FortiMAIL Workspace Protection

La solución Fortimail Workspace combina una plataforma de prevención de amenazas basada en la IA, que aprovecha los LLM o Modelos de Lenguaje de gran tamaño, reconocimiento de imágenes y la tecnología anti-evasión, con un servicio gestionado 24/7 de respuesta a incidentes

El servicio de Workspace Protection comprende el siguiente alcance:

- Workspace Security Bundle. Includes Cloud Email security SaaS + Internal Email + Google Drive Storage + Web Extension para 700 buzones de correo en google.

Fotimail Workspace Email Security + Web Security

SKU	FC2-10-PVMCL-1214-02-DD - Cantidad:700
Descripción	Workspace Security Bundle. Includes Cloud Email security SaaS + Internal Email + Google Drive Storage + Web Extension. 101-1,000 users. Includes FortiCare premium support.

Integración 2: FortiMail Workspace Security (700 Buzones)

ID Caso de Uso	Nombre del Caso de Uso	Descripción y Lógica FortiSIEM	Métrica de Valor / Resultado Esperado
UC-MAIL-01	Campaña Dirigida de Phishing / Spear Phishing	Regla de agrupación que detecta si FortiMail procesa un mismo indicador de correo malicioso o asunto catalogado como Phishing dirigido a más de N usuarios en un lapso de 15 min.	Identificación en tiempo real de ataques masivos o dirigidos por correo electrónico contra la organización.
UC-MAIL-02	Detección de Archivo Adjunto Malicioso / Sandbox Detection	Evento de FortiMail/FortiSandbox integrando la detección de un adjunto con carga útil maliciosa (Malware/Virus Found).	Incidente en FortiSIEM asociando al remitente externo, destinatario interno y el nombre del archivo adjunto malicioso.
UC-MAIL-03	Anomalía / Incremento Masivo de Fallos DMARC/SPF (Spoofing Attempt)	Regla basada en volumen que alerta cuando FortiMail registra un pico inusual de correos entrantes que fallan las validaciones SPF/DKIM/DMARC del dominio corporativo.	Detección de intentos de suplantación de identidad de marca o dominios ejecutados por terceros.

5.4.2 FortiEDR

EDR está diseñado para que cualquier tipo de empresa, sin importar su tamaño o la complejidad de sus necesidades, pueda contar con esquemas avanzados ante la protección contra ataques cibernéticos, aportando a la continuidad de negocio de las compañías y brindando el respaldo necesario para mantener su nivel de productividad. La seguridad de la información es uno de los pilares de la transformación digital de las compañías, por esta razón, es necesario contar con un aliado de negocios experto en materia de ciberseguridad. Las diferentes modalidades de Tigo EDR brindan niveles avanzados de protección contra amenazas a la confidencialidad, integridad y disponibilidad de la información de su negocio a través de la prevención, detección y respuesta a incidentes de seguridad, los cuales se complementan con Servicios Administrados de Seguridad que le permiten a su empresa contar con expertos capacitados para el diseño, configuración, monitoreo, pruebas y actualización de políticas y servicios de seguridad adquiridos.

- EDR es una solución con capacidades de protección, detección y respuesta automática a incidentes de ciberseguridad causados por software malicioso en los dispositivos terminales o endpoints brindando protección tanto antes(pre-infección) como después de que ocurre una infección (post-infección).

- EDR previene la infección de malware y de ransomware, detecta y desactiva posibles amenazas en tiempo real y automatiza procedimientos de respuesta y corrección con tareas programables y automatizables.

Descripción
• Suministro de (1000) licencias de FortiEDR • Servicios de gestión, monitoreo y notificación de alertas de seguridad 7*24 para (1000) agentes de FortiEDR por doce (12) meses.

5.4.3 Integración 2: FortiEDR - Discover, Protect and Respond

ID Caso de Uso	Nombre del Caso de Uso	Descripción y Lógica FortiSIEM	Métrica de Valor / Resultado Esperado
UC-EDR-01	Ejecución de Malware Bloqueada/Prevenida en Endpoint	Eventos de detección de amenazas de FortiEDR en política Prevent/Respond correlacionados en FortiSIEM con asignación de incremento en el Device/User Risk Score.	Incidente de alta severidad centralizado en la consola de FortiSIEM mostrando hash, proceso y máquina afectada.
UC-EDR-02	Detección de Intento de RANSOMWARE / Cifrado Inusual	Correlación de reglas de FortiEDR pertenecientes a las categorías de Exfiltration o File System Modification disparadas en un período corto.	Alerta inmediata de potencial infección de Ransomware en tiempo real para contención rápida.
UC-EDR-03	Endpoint Infectado / Amenaza Detectada Fuera de Red Corporativa	Identificación de eventos de amenazas generados por el agente FortiEDR cuando la IP de origen es una IP pública o fuera de los segmentos CMDB corporativos (Off-net Host).	Visibilidad sobre la salud de endpoints remotos/teletrabajadores sin conexión a la VPN corporativa.

5.5 Alcances De Servicios Profesionales de integración

La configuración e integración de FortiSIEM para incorporar FortiNAC, FortiEDR y FortiMail Workspace Security, habilitando ingesta de eventos, casos de uso, reglas de correlación, analítica y dashboards.

5.5.1 Configuración e Integración de FortiSIEM

Resumen Y Objetivo Del Proyecto

El presente documento define el alcance estricto de los servicios profesionales para la integración de tres (3) nuevas fuentes de datos sobre la infraestructura existente de FortiSIEM:

- FortiNAC: 1,000 Agentes/Dispositivos gestionados.

- FortiEDR: 1,000 Agentes (Discover, Protect and Respond).
- FortiMail Workspace Security: 700 Cuentas/Buzones.

El objetivo central es habilitar la ingesta, mapeo en la CMDB y habilitación de hasta nueve (9) casos de uso de seguridad (3 por tecnología) soportados por la arquitectura nativa de FortiSIEM.

Fases y Actividades del Proyecto

Fase 1: Planificación, Prerrequisitos y Registro en CMDB

- Sesión de kick-off con definición de contactos clave, revisión de alcances, roles y cronograma de hitos del proyecto.
- Levantamiento de prerrequisitos de red, puertos de comunicación (ej. Syslog UDP/TCP 514, HTTPS API 443) y credenciales de acceso.
- Configuración de credenciales de acceso y Discovery en el CMDB de FortiSIEM para registrar las consolas directivas (Management Appliances/Cloud Consoles) de FortiNAC, FortiEDR y FortiMail.
- Verificación de la salud general del clúster de FortiSIEM (Supervisor / Worker / Collector) para confirmar disponibilidad de EPS (Events Per Second) y capacidad de almacenamiento.

Fase 2: Integración e Ingesta de Eventos (Event Ingestion)

- Configuración del reenvío de eventos Syslog/API desde FortiNAC hacia el FortiSIEM Collector/Supervisor.
- Configuración de integración API / Webhook / Event Forwarding para FortiEDR hacia FortiSIEM.
- Configuración de integración Syslog/API desde FortiMail Workspace Security hacia FortiSIEM.
- Validación de la recepción, parsing y correcto mapeo de atributos de eventos (Parsed Event Attributes) en el módulo de Analytics.

Fase 3: Despliegue de Casos de Uso, Reglas de Correlación y Analítica

- Configuración de hasta nueve (9) reglas de correlación personalizadas en el Rule Engine distribuidas de acuerdo con los casos de uso definidos.
- Creación de tres (3) Reportes Analíticos personalizados (Custom Analytics Reports) orientados a visibilidad de telemetría e incidentes.
- Creación de un (1) Dashboard personalizado con nueve (9) Widgets para monitoreo operativo del SOC.
- Configuración de una (1) Política de Notificación de Incidentes (Incident Automation Policy) vía Email Gateway para alertas críticas.

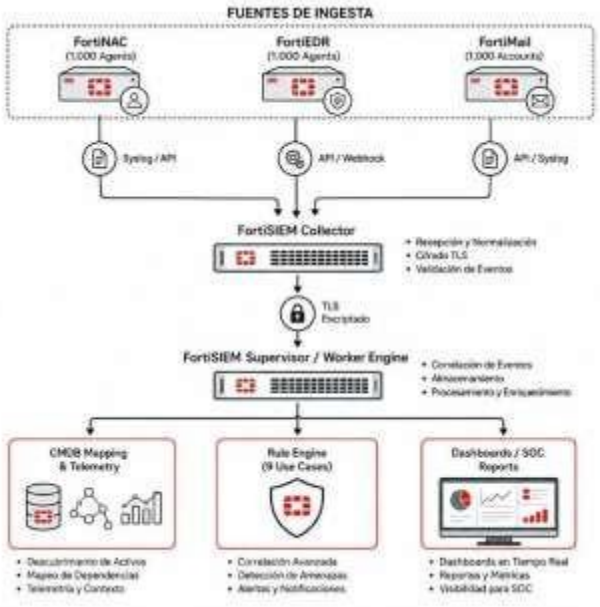
Fase 4: Validaciones, Afinamiento y Cierre

- Ejecución de pruebas de generación de eventos controlados para validar la activación de las reglas de correlación e incidentes.

- Afinamiento mediante la inclusión de excepciones o ajuste de umbrales (Thresholds) para minimizar falsos positivos.
- Sesión de transferencia de conocimiento operativa (máximo 2 horas) sobre la navegación de eventos y gestión de los nuevos incidentes generados.
- Acompañamiento remoto por hasta quince (15) días calendario posteriores a la salida a producción de las configuraciones realizadas.
- Documentación Low Level Design (LLD) del diagrama de las integraciones y de las configuraciones, políticas y casos de uso configurados.

Definición de Casos de Uso

Todos los casos de uso están delimitados sobre capacidades nativas de detección basada en reglas y perfilamiento (Rule Engine / Analytics) de FortiSIEM.



Matriz de Delimitación y Límites del Alcance

Para garantizar la correcta ejecución en tiempos, las actividades técnicas quedan estrictamente acotadas según los siguientes máximos configurables:

Elemento / Configurable	Cantidad Máxima Incluida	Notas / Exclusiones de Alcance
Consolas / Fuentes a Integrar	3 Fuentes	1 Clúster/Instancia de FortiNAC, 1 Tenant/Instancia de FortiEDR, 1 Tenant de FortiMail Workspace Security.
Agentes/ Entidades Ingestadas	2,700 en Total	1,000 FortiNAC, 1,000 FortiEDR, 700 Buzones FortiMail. No incluye despliegue de agentes propios de FortiSIEM (FortiSIEM Windows/Linux Agent) en servidores o

		endpoints.
Reglas de Correlación Personalizadas	9 Reglas	Exactamente 3 reglas por cada fuente de ingesta. Reglas adicionales requerirán un control de cambios.
CParsers Personalizados (Custom Parsers)	0 Parsers XML/JSON	Las fuentes requeridas (FortiNAC, FortiEDR, FortiMail) cuentan con soporte y parsers Out-Of-The-Box en FortiSIEM. No se contempla desarrollo de parsers desde cero.
Reportes Personalizados	3 Reportes	1 reporte tipo Analytics Query por tecnología integrada.
Dashboards Personalizados	1 Dashboard	Contendrá un máximo de 9 widgets consolidando la telemetría e incidentes de las 3 fuentes.
Políticas de Automatización/ Notificación	1 Política	Configuración de alerta por correo electrónico (Email Notification) dirigida a una lista de distribución del SOC.
Playbooks de Respuesta Automatizada / SOAR	0 Playbooks	No se incluye desarrollo ni ejecución de Playbooks o scripts de remediación remota (Remediation Scripts).
Sesiones de Tuning (Ajuste Fino)	2 Sesiones	Limitado a un máximo de 4 horas totales dentro de los primeros 15 días tras la activación.

Exclusiones del Alcance

Las siguientes actividades quedan fuera del alcance de esta bolsa de servicios profesionales y no serán ejecutadas por el equipo:

- Implementación o Configuración de Fuentes de Origen: No incluye la instalación, despliegue de agentes, actualización de firmware/políticas, endurecimiento (hardening) o remediación técnica sobre FortiNAC, FortiEDR ni FortiMail Workspace Security. Estas plataformas deben ser entregadas 100% operativas por el cliente.
- Despliegue de Agentes Propios de FortiSIEM: No se incluye la instalación o configuración del FortiSIEM Windows/Linux Agent en endpoints o servidores. La ingesta se realizará vía Syslog y/o conectores API nativos.
- Desarrollo de Parsers Personalizados (Custom Parsers): Excluye la creación desde cero de parsers XML, JSON o expresiones regulares (Regex), dado que las tres soluciones especificadas cuentan con soporte y parsers Out-Of-The-Box integrados en FortiSIEM.
- Playbooks y Respuesta Automatizada (SOAR): No se contempla el desarrollo de Playbooks, scripts de remediación (Remediation Scripts), ni acciones de bloqueo automatizado hacia las fuentes u otros elementos de red.
- Modificación de Arquitectura FortiSIEM: No incluye adición de nuevos nodos (Workers/Collectors), reestructuración del clúster, migración de motor de base de datos (p. ej., de EventDB a ClickHouse) ni actualización de versión del sistema operativo/FortiSIEM.
- Monitoreo y Operación Continuo (SOC): Excluye la gestión de incidentes en tiempo real, análisis triaje 24/7 o respuesta ante alertas generadas tras la entrega del proyecto.

5.6 Implementación de Servicio

5.6.1 Metodología de Aprovisionamiento

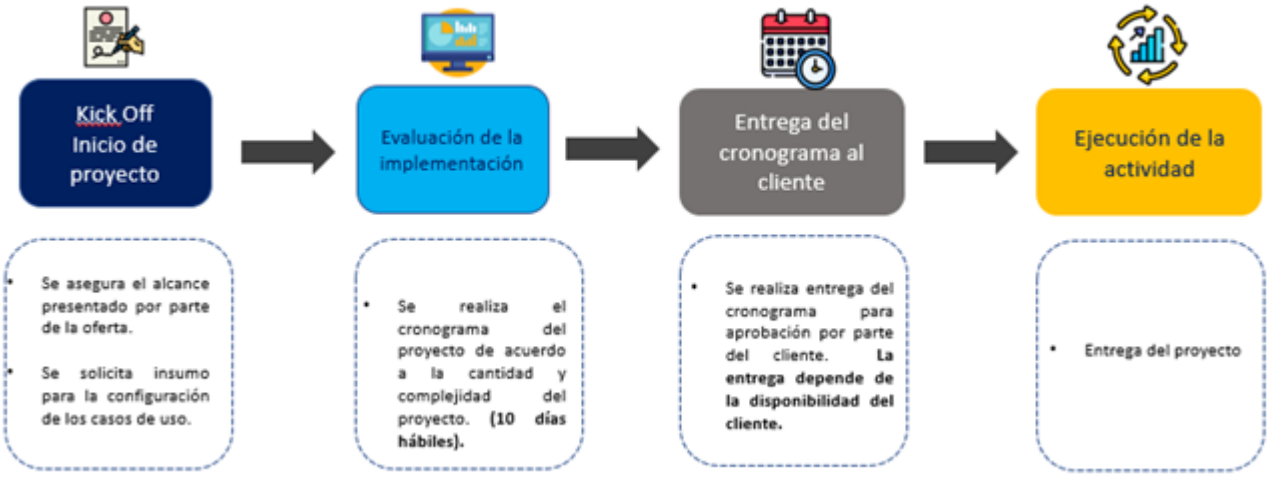
Para llevar a cabo la entrega de una solución operativa al cliente, Tigo asigna un Project Manager responsable de canalizar las necesidades y comunicaciones del cliente e integrar tecnológicamente los proveedores y aliados requeridos.

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.



5.6.2 Tiempo de Aprovisionamiento

Se estima un tiempo de implementación de 90 días, contados a partir de la firma del contrato, Este tiempo contempla la configuración, integración, validación de recepción de logs, ajustes de las correlaciones, así como las pruebas de funcionamiento de FortiNAC, FortiMail y FortiEDR con FortiSIEM.



CONSIDERACIONES

- En todo caso se realizará el mejor esfuerzo para tener implementado el servicio en el menor tiempo posible.
- Los plazos para las distintas fases de aprovisionamiento se establecerán de mutuo acuerdo con el cliente, sin embargo, en caso de presentarse situaciones de fuerza mayor o caso fortuito, o

situaciones que estén fuera del contrato del proveedor, dicho plazo se podrá modificar dando aviso previo al cliente, sin que esto implique incumplimiento alguno por parte del proveedor

5.6.3 Entregable Implementación del Proyecto

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

6 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.

6.1 Tiempo de notificación de alertas

	Riesgo	Tiempo de notificación de alerta
Alertas Ciberseguridad (RSOC)	Significativo	30 minutos
	Moderado	4 horas
	Menor	8 horas
	Información	En informe periódico (Información que no es contenida en los informes)

6.2 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.

6.3 Delimitaciones

1. No se considera tiempo on-hold por parte de cliente
2. Tiempos se consideran a partir de la apertura de tiquete de falla.
3. Tiempo aplica únicamente para soporte remoto, soporte de manos remota dependerá de la ubicación. El SLA comprometido para tipo de impacto significativo no incluye el tiempo de viaje del personal de TIGO Business y/o traslado de equipos o repuestos. Para esto, se ha definido un tiempo promedio de 2 horas de traslado de un punto a otro.
4. 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.

6.4 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.

7 PROPUESTA ECONÓMICA

Descripción	Cantidad	Meses	Tarifa Mensual Sin IVA	IVA	Tarifa Mensual Con IVA
Servicios avanzados de monitoreo de seguridad	1	12	$ 11.500.000	$ 2.185.000	**$ 13.685.000**
Servidor VM (Collector)	1	12	$ 1.150.000		**$ 1.150.000**
VPN S2S	1	12	$ 220.000	$ 41.800	**$ 261.800**
Internet DataCenter 30 MB	1	12	$ 218.000	$ 41.420	**$ 259.420**
Total Mensual			**$ 13.088.000**	**$ 2.268.220**	**$ 15.356.220**
Total 12 Meses			**$ 157.056.000**	**$ 27.218.640**	**$ 184.274.640**

7.1 Condiciones Económicas y Comerciales

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 para proveer los servicios profesionales.

Este cobro hará de manera mensual recurrente.

7.2 Validez de la Oferta

La vigencia de esta propuesta es de treinta (20) días calendario a partir de la entrega de la oferta