multisoft

Soluciones en Movimiento

Industria y Comercio

SUPERINTENDENCIA

BOGOTÁ:

(601) 644 3300 Av. 15 No 100-69, Piso 7

Edificio Vanguardia, Bogotá D.C., Colombia.

Multisoft Soluciones en Movimiento Multisoft S.A.S @Multisoft_SAS

www.multisoft.com.co

Bogotá, 15 de mayo de 2023

INGENIERA
NATALIA SALVADOR RODRIGUEZ
ASESOR PROYECTOS TIC
OFICINA DE TECNOLOGIA E INFORMATICA
SIC – SUPERINTENDENCIA INDUSTRIA Y COMERCIO
CUIDAD.

REF: Propuesta de valor para renovación de soluciones de Trellix – Endpoint, Siem , IPS

Multisoft es una compañía con más de 30 años de experiencia y presencia regional con amplia experiencia en servicios gestionados de Ciberseguridad e infraestructura, contando con más de 800 proyectos ejecutados en la región.

Analizando el alcance de su proyecto, Multisoft en calidad de Partner Collaborate (Platinum) de Trellix adjunta la propuesta de valor respectiva.

Esperamos que nuestra oferta se ajuste a sus necesidades, responda sus inquietudes y constituya una oportunidad para el crecimiento y la madurez en la estrategia de seguridad y tecnología de su organización.

Atentamente,

MARIO ALARCON OLAYA
mario.alarcon@multisoft.com.co
STRATEGIC ACCOUNT MANAGER
Cel. 317 6397126

¿Qué hacemos para transformar su negocio?

Con la ciberseguridad, logramos que las empresas de Latino América adopten y evolucionen rápidamente los nuevos retos en un mundo tan dinámico, hacemos que las soluciones de seguridad de la información, Ciber-Seguridad e Infraestructura Tecnológica permitan fortalecer sus estrategias de una manera ágil y asertiva.

Nuestras ventajas

- **Representamos fabricantes líderes** en tecnología e innovación.
- **Flexibilidad en soluciones:** Servicios, Administrados (MSP), SaaS, Leasing.
- **Ingeniería especializada** y certificada.
- **Enfoque consultivo** en las necesidades del cliente.
- **Servicios de principio a fin:** Diseño, Implementación y Mantenimiento.
- Aplicamos metodologías **ágiles y mejores prácticas** para garantizar el éxito.

¿A qué se enfrentan hoy las empresas?

- Riesgos
- Cultura – Awareness
- Auditoría
- Cumplimiento
- Reputación

¿Qué deben proteger?

- Endpoint
- Móviles
- Usuarios remotos
- Cloud
- Workload
- Aplicaciones

¿Cómo podemos llegar juntos al éxito?

Proteja adecuadamente la información de su empresa con **soluciones robustas que se adapten a los ciberataques más avanzados,** prevenga los ataques cibernéticos de manera proactiva con soluciones que le permitan aumentar la **visibilidad**, el **monitoreo** y el análisis del **comportamiento**.

Deje en nuestras manos la ciberseguridad de su compañía, desde el endpoint hasta la nube de forma automatizada, sin invertir recursos adicionales ni crecer sus áreas de operación.

Ciberseguridad

Proactivo

- Vulnerability Management
- Security Information & Events Management - SIEM
- Inteligencia de Amanazas
- Endpoint/Network /Cloud Monitoring
- Comportamiento XBA
- Cifrado de dispositivos

Protección

- Anti-Malware
- Antiphishing (Protección de correo)
- Proxy Web - Filtrado Web
- NG-Firewall
- Gestión de accesos privilegiados (PAM)
- Prevención de fuga de información (DLP)
- Sistemas de prevention intrusos (IPS)
- Web Isolation (RBI)

Detección

- Security Orchestration Automation & Response (SOAR)
- Extended Detect and Response (XDR)
- SandBoxing
- Investigación
- Incident Management



Servicios Gestionados

Proceso de gestión de plataforma tecnológica de seguridad con personal especializado en sitio.

Servicios Profesionales

- Implementación
- Mantenimiento
- Administración
- Transferencia de conocimiento
- Soporte

Consultoría

- Respuesta de incidentes Consultoría en Sistemas de Gestión de Seguridad de la Información (SGSI)
- Ethical Hacking (Caja Blanca, Gris y Negra)
- Informática Forense Concientización de usuarios.

Capacitaciones

Nuestra área de capacitaciones ofrece diferentes tipos de entrenamientos que le permitirán preparar al personal y desarrollar sus capacidades técnicas en las diferentes plataformas de CiberSeguridad.

NG SOC



MULTISOFT - MSSP

Managed Security Service Provider

Nuestros servicios de seguridad gestionada prestada por nuestro Centro de Operaciones de Seguridad (SOC), le permitirá desarrollar una estrategia de ciberseguridad integral, involucrando tecnologías, personas y procesos. Contamos con experiencia, certificaciones internacionales y personal experto para ser parte de su estrategia de ciberdefensa.

SOM



Security Operation Management

- Correlación de eventos (SIEM).
- Automatización / Playbooks (SOAR).
- Atención y respuesta a incidentes (RI).

SPM



Security Platform Management

- Gestión de plataformas de seguridad.
- Monitoreo y análisis de ciberamenazas.

CTI



Cyber Threat Intelligence

- Inteligencia de amenazas (Threat intelligence)
- Boletines de seguridad.
- Protección digital de marca.

SECaaS



Security as a Service

- Seguridad gestionada 7x24.
- Gestión de incidentes de seguridad.

MDR



Managed Detection & Response

- Investigación de amenazas.
- Caza de amenazas (Threat Hunting)

RT

Red Team Services



- Web app Scan.
- Ethical Hacking.
- Análisis de código.
- Análisis de vulnerabilidades.
- Programa de sensibilización.
- Ingeniería social.

Infraestructura Tecnológica

Para garantizar la disponibilidad de los servicios y aplicaciones críticas de su negocio. Multisoft ofrece soluciones de infraestructura que cubren sus necesidades de licenciamiento, equipos, servidores, comunicaciones, almacenamiento, ambientes virtualizados y herramientas para gestionar de manera optimizada la infraestructura tecnológica de su organización sea on-premise, nube o híbrida.

Multisoft Cloud Services

Análisis y Diseño de Arquitecturas de virtualización en una nube propia autogestionada.

Soluciones de Respaldo:

Ajustadas a su necesidad, flexibles y escalables, con pagos únicos o mensualizados con crecimiento.

Datacenter:

Servidores, almacenamiento y equipos de red de última generación entregados y soportados por un equipo experto.

Cloud Computing

Ambientes remotos confiables, para teletrabajo con seguridad.

Partners

Contamos con personal certificado por nuestros socios de negocios en las soluciones que ofrecemos a nuestros clientes.

Contenido

1. RENOVACION SOLUCIONES 7
1.1. TRELLIX COMPLETE ENDPOINT PROTECTION 7
1.1.1. ALCANCE DE RENOVACION 8
1.2. TRELLIX DATA LOSS PREVENTION ENDPOINT 8
1.2.1. ALCANCE DE RENOVACIÓN 10
1.3. TRELLIX NETWORK SECURITY PLATFORM 10
1.3.1. APPLIANCE TRELLIX NS7500 10
1.3.2. ALCANCE DE RENOVACION 11
1.4. TRELLIX SIEM 12
1.4.1. ALCANCE DE RENOVACION 12
1.5. ARQUITECTURA GENERAL. 13
2. ALCANCE DEL PROYECTO 14
2.1. HEALTH CHECK DE LOS COMPONENTES ACTUALES 15
2.2. TIEMPO DE IMPLEMENTACIÓN 15
2.3. REQUISITOS DE IMPLEMENTACIÓN 15
3. SERVICIOS DE MANTENIMIENTO Y SOPORTE DE LAS SOLUCIONES 16
3.1. MANTENIMIENTO PREVENTIVO 16
3.2. SOPORTE CORRECTIVO 7X24 16
3.2.1. HORARIO DE ATENCIÓN 17
3.2.2. SERVICIO TELEFÓNICO 17
3.2.3. CORREO ELECTRÓNICO 17
3.2.4. SOPORTE REMOTO 17
3.2.5. SOPORTE EN SITIO 18
3.2.6. TIPOS DE ESCALAMIENTO 18
3.2.7. TIEMPOS DE RESPUESTA 18
3.2.8. PROCESO PARA ATENCIÓN DE UN REQUERIMIENTO 19
3.2.9. EXCLUSIONES 19
3.2.10. ENTREGABLES 19
4. OFERTA ECONOMICA 21
5. CONDICIONES COMERCIALES 21

1. RENOVACION SOLUCIONES

Propuesta Renovación del licenciamiento y upgrade de las distintas soluciones de Trellix , tales como Endpoint Protection, protección de fuga de información (DLP), IPS , SIEM entre otras, dentro de cada una de las suit ofertadas encontramos los siguientes productos:

1.1. TRELLIX COMPLETE ENDPOINT PROTECTION

Trellix Comple Endpoint Protection le permite tomar las riendas con amplias protecciones, controles de cumplimiento de normativas y administración unificada. Se trata de una solución integral con la combinación perfecta de funciones y ahorro de costes para mantener a raya tanto a virus como a piratas informáticos, a remitentes de spam, a ladrones de datos y a auditores.

Características:

Función	Por qué es imprescindible
Administración integrada unificada	El software Trellix ePO proporciona visibilidad instantánea de los eventos y del estado de seguridad, y facilita el acceso directo a la administración para controlar de manera centralizada todas sus herramientas de seguridad y de cumplimiento de normativas
Multiplataforma	Protege la amplia gama de endpoints que necesitan los usuarios avanzados y móviles, incluidos los sistemas Mac, Linux y Microsoft Windows.
Control de dispositivos	Le permite supervisar y restringir los datos que se copian en dispositivos y soportes de almacenamiento extraíbles para impedir que escapen al control de la empresa
Prevención de intrusiones en host y firewall para equipos de escritorio	Proporciona protección de tipo zero-day frente a las nuevas vulnerabilidades, lo que disminuye la urgencia de aplicar parches y controla las aplicaciones que pueden acceder a la red para detener los ataques propagados por esta vía.
Antimalware	Bloquea virus, troyanos, gusanos, adware, spyware y otros programas potencialmente no deseados que roban datos confidenciales y sabotean la productividad de los usuarios.
Antispam	Ayuda a eliminar el spam, que puede inducir a usuarios desprevenidos a visitar sitios que distribuyen malware y utilizan técnicas de phishing
Búsqueda y navegación seguras	Contribuye a garantizar el cumplimiento de las normativas y a reducir los riesgos asociados a la navegación por Internet. Para ello, alerta a los usuarios sobre los sitios web maliciosos antes de que los visiten, dejando que sean los administradores los que decidan autorizar o bloquear el acceso a los sitios web.
Filtrado web (host)	Controla la actividad de los usuarios, ya estén navegando por Internet desde dentro o fuera de la red de la empresa, mediante filtrado de contenidos y regulando el acceso a la Web por parte de usuarios y grupos.
Seguridad de servidores de correo electrónico	Protege el servidor del correo electrónico e intercepta el malware antes de que llegue al buzón de entrada del usuario
Auditoría de directivas	Facilita la elaboración de informes plenamente integrados sobre cumplimiento para normas como HIPAA, PCI, etc.

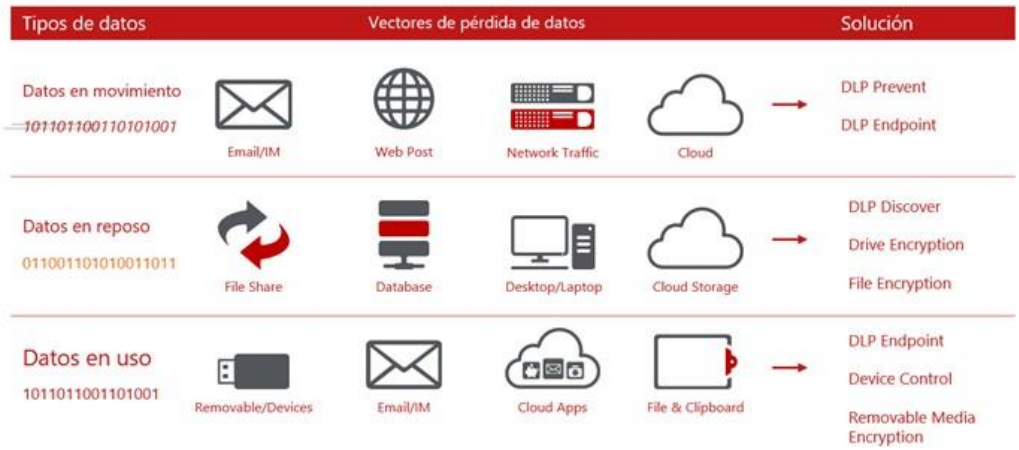
1.1.1. ALCANCE DE RENOVACION

- Renovación de Licenciamiento Trellix Complete EndPoint Protection para 2020 Nodos de la entidad, por 1 año.
- Renovación Soporte Trellix para 2020 nodos, por 1 año.
- Soporte local correctivo de Multisoft, en esquema 7x24 por 1 año. (Opcional)
- Mantenimiento Preventivo de la solución, por 1 año. (Opcional)
- Presentar los servicios especializados de Multisoft para todas las inquietudes, y posibles incidentes que llegasen a presentarse.
- Presentar los servicios especializados de Multisoft para llevar a cabo las sesiones de mantenimientos preventivos sobre la plataforma de seguridad.

1.2. TRELLIX DATA LOSS PREVENTION ENDPOINT

La protección de datos siempre ha sido objeto de gran atención por parte de los ejecutivos de seguridad de la empresa y los oficiales de cumplimiento, pero las recientes leyes de privacidad indudablemente elevarán la protección de datos a la sala de juntas debido a las posibles consecuencias graves del incumplimiento. Lo que lo hace aún más desafiante es que las empresas de todos los tamaños están adoptando servicios basados en la nube, como Microsoft Office 365, para dar a sus empleados una mayor flexibilidad y un acceso más fácil a las aplicaciones empresariales principales.

Como las regulaciones y las necesidades corporativas imponen cada vez más exigencias a las áreas TI para garantizar el manejo seguro de los datos, la implementación de las soluciones de protección necesarias puede parecer desalentadora. Algunos productos de prevención de pérdida de datos requieren un esfuerzo sustancial de implementación y, por lo general, tienen grandes costos de consultoría en curso.



Trellix® Total Protection for DLP ayuda a garantizar el cumplimiento y protege los datos confidenciales dondequiera que se encuentren: en los puntos finales, en la red, en los sistemas de almacenamiento o en la nube. La solución ofrece el mismo motor de políticas y clasificación de DLP en múltiples entornos. No es necesario volver a crear políticas para proteger la misma pieza de datos

en diferentes entornos. Esta capacidad común de política de protección de datos se logra a través del software Trellix® ePolicy Orchestrator® (Trellix ePO ™) y su estrecha integración con Trellix MVISION Cloud.

TRELLIX DATA-LOSS-PREVENTION ENDPOINT

Con Trellix DLP Endpoint puede supervisar de manera rápida y fácil las actividades de los usuarios finales en tiempo real, y aplicar directivas de seguridad administradas de manera centralizada con el fin de regular y restringir, cómo transfieren los empleados los datos confidenciales o sensibles sin que se vea afectada su productividad.

Funcionalidades

Trellix DLP Endpoint proporciona protección integral para todos los canales potenciales de fugas, como los dispositivos de almacenamiento extraíbles, la nube, el correo electrónico, la mensajería instantánea, la Web, el material impreso, el Portapapeles, las capturas de pantalla, las aplicaciones para compartir archivos, etc.; a continuación, algunas de sus características:

- Clasificación manual que permite a los usuarios finales clasificar manualmente los documentos, incrementando la concienciación sobre la protección de datos de los empleados y reduciendo la carga administrativa.
- Funcionalidades de análisis y reparación que permiten a los usuarios finales ejecutar análisis de descubrimiento de Endpoints y tomar medidas de reparación de forma autónoma.
- Mayor compatibilidad con Mac OS aumentando la protección según el contenido para Mac OS en dispositivos de almacenamiento extraíbles, el acceso a archivos de aplicaciones y los recursos compartidos de la red.
- Clasificación flexible, incluidos diccionarios, expresiones regulares y algoritmos de validación, documentos registrados y compatibilidad con soluciones de clasificación de usuarios finales de terceros.
- Exclusiva tecnología de etiquetado para identificar los documentos según su origen.
- Varias directivas y conjuntos de reglas reutilizables que ofrecen la capacidad de definir distintas directivas de prevención de la fuga de datos en toda la empresa, crear directivas por oficina, departamento, normativa, etc.
- Gestión de incidentes más pormenorizada que permite realizar consultas/filtrar/ver por propiedades de incidentes (por ejemplo, número de serie del dispositivo, nombre del archivo de prueba y grupos).
- Supervisión de eventos y funciones de auditoría centralizadas.
- Control de acceso basado en funciones (también conocido como separación de funciones) mejorado para la administración de directivas, así como para revisar los incidentes.

1.2.1. ALCANCE DE RENOVACIÓN

- Renovación de licenciamiento Trellix Data Loss Prevention Endpoint Software para 1620 Nodos de la entidad, por 1 año.
- Renovación Soporte Trellix para 1620 nodos, por 1 año.
- Soporte local correctivo Multisoft, en esquema 7x24 por 1 año. (Opcional)
- Mantenimiento Preventivo de la solución. (Opcional)
- Presentar los servicios especializados de Multisoft para todas las inquietudes, y posibles incidentes que llegasen a presentarse.
- Presentar los servicios especializados de Multisoft para llevar a cabo las sesiones de mantenimientos preventivos sobre la plataforma de seguridad.

1.3. TRELLIX NETWORK SECURITY PLATFORM

Trellix® Network Security Platform (Trellix NSP) es un sistema de prevención de intrusiones (IPS) de próxima generación que descubre y bloquea amenazas de malware sofisticadas en la red. Emplea técnicas avanzadas de detección y emulación, y va más allá de la comparación con patrones para ofrecer protección contra los ataques ocultos con un alto grado de precisión. Para satisfacer las necesidades de las redes más exigentes, la plataforma puede adaptarse hasta 40 Gbit/s con un solo dispositivo.

1.3.1. APPLIANCE TRELLIX NS7500



Los sensores de la serie NS son una plataforma de hardware de tercera generación para Trellix® Network Security Sensor (Sensor) diseñada para enlaces de alto ancho de banda, para proporcionar la capacidad IPS de próxima generación (NGIPS), proporcionando un alto rendimiento agregado en varios modelos de sensores. El sensor NS7350 es una unidad de 1RU que proporciona un rendimiento agregado de hasta 10 Gbps.

ESPECIFICACIONES TECNICAS

Performance	
Aggregate Performance	3 Gb/s - 5 Gb/s – 7,5 Gb/s
Maximum Throughput (UDP 1512-byte packets)	Up to 6 Gbps - Up to 9 Gbps - Up to 12 Gbps
Maximum Concurrent Connections	4.000.000 - 7.000.000 -10.000.000
Connections per Second	225.000
HTTP Connections per Second	135.000
Throughput with SSL Decryption (based on 10% SSL traffic)	2,7 Gbit/s - 4,5 Gbit/s - 6,7 Gbit/s
Maximum SSL Flow Count	500.000
SSL Keys Imported	1.024
Typical Latency	Less than 100 µs

Number of Virtual IPS Systems	1.000
Maximum DoS Profiles	5.000
ACL Rules	5.000
Ports	
Fixed Gigabit Ethernet—Copper Ports (internal fail-open)	8
Fixed 10 GigE/1 GigE (SFP+) Ports	2
Fixed 40 Gigabit Ethernet	-
Network I/O Slots	2
Network I/O Modules (six options)	4-port 10 GigE/1 GigE SR Optical 50 micron with fail-open, 4-port 10 GigE/1 GigE SR Optical 62.5 micron with fail-open, 4-port 10 GigE/1 GigE LR Optical with fail-open, 8-port (SFP+/SFP) 10 GigE/1 GigE, 6-port (RJ45) 1 GigE with internal fail-open, or 4-port (RJ45) 10 GigE/1 GigE/100 Mbps (with internal fail-open)
10 Gigabit Ethernet	Up to 18
40 Gigabit Ethernet	-
Dedicated Response Ports (RJ45)	1 (10G/1G)
Dedicated Management Ports (RJ45)	1 (10G/1G)
Dedicated Storage Ports (RJ45)	-
Physical	
Dimensions	17.31” (W) x 1.75” (H) x 29.13” (D)
Weight	28 lbs
Storage	Solid State 240 GB
Maximum Power Consumption	300W
DC Power Available	Optional
Redundant Power Supply	Included
Power	100–240 VAC (50/60Hz)
Temperature	0° C to 35° C (operating) -40° C to 70° C (non-operating)
Relative Humidity (non-condensing)	Operational: 10% to 90% Non-operational: 5% to 95%

1.3.2. ALCANCE DE RENOVACION

- Adquisición y soporte de fábrica de (1) IPS NS7500 de red del fabricante Trellix junto con sus componentes adicionales como Trellix Network Security Starter Manager.
- (2) Fuente de Alimentación AC para alta redundancia
- Soporte local correctivo, en esquema 7x24 por 1 años.
- Soporte local correctivo Multisoft, en esquema 7x24 por 1 año.(Opcional)
- Mantenimiento Preventivo de la solución.(Opcional)
- Presentar los servicios especializados de Multisoft para todas las inquietudes, y posibles incidentes que llegasen a presentarse.
- Presentar los servicios especializados de Multisoft para llevar a cabo las sesiones de mantenimientos preventivos sobre la plataforma de seguridad.

1.4. TRELLIX SIEM

Trellix Enterprise Security Manager Priorizar. Investigar. Responder. La seguridad más eficaz empieza por la visibilidad de toda la actividad que ocurre en sistemas, redes, bases de datos, aplicaciones y la nube. Una solución de administración de información y eventos de seguridad (SIEM) es el pilar fundamental de una infraestructura de seguridad eficaz. Trellix® Enterprise Security Manager, núcleo de Trellix SIEM, ofrece rendimiento, inteligencia procesable e integración de soluciones a la velocidad y capacidad de adaptación requeridas por los departamentos de seguridad. Esta solución permite priorizar, investigar y responder rápidamente a las amenazas ocultas, así como cumplir los requisitos normativos.

Principales ventajas:

- Inteligente: los análisis avanzados y el amplio contexto le ayudan a detectar y priorizar amenazas.
- Práctica: los datos que necesita se presentan en vistas dinámicas que incluyen la opción de tomar medidas para investigar, contener y corregir, así como adaptar lo necesario cuando se reciben alertas y patrones importantes.
- Integrada: la solución supervisa y analiza datos desde una infraestructura de seguridad amplia y heterogénea, y ofrece integración bidireccional a través de interfaces abiertas. Asimismo, permite automatizar muchas respuestas iniciales.
- Despliegue flexible: se puede desplegar como hardware o máquina virtual según los requisitos, necesidades

A continuación mostramos los componentes actuales de solución SIEM dentro de la SIC.

Enterprise Security, Enterprise Log Manager and Event Receiver 5700 Combination

- **Enterprise Security, Enterprise Log Manager and Event Receiver 5700 Combination**: Proporciona SIEM, Log Management, y Network Analysis functions. Incluye Event Receiver. Proporciona gestión de registros compatible y recopila datos para su correlación y análisis por parte de Enterprise Security Manager. Incluye almacenamiento local SSD de 32 TB + 800 GB. (La retención de registros sin procesar requiere almacenamiento externo. La tarjeta SAN opcional se vende por separado). Dispositivo de 2U.
- **Global Threat Intelligence (Module for ESM) - Combination 5700 Appliance:** Integra Global Threat Intelligence (GTI) para mejorar el conocimiento de la situación local, lo que permite a los administradores de seguridad identificar qué hosts se comunican con direcciones IP sospechosas o maliciosas, al tiempo que resalta los eventos, los hosts y los usuarios involucrados en transacciones potencialmente maliciosas. Disponible como un complemento opcional para un dispositivo independiente o un dispositivo combinado de Enterprise Security Manager; seleccione los modelos de máquina virtual de ESM y el dispositivo Event Reporter.

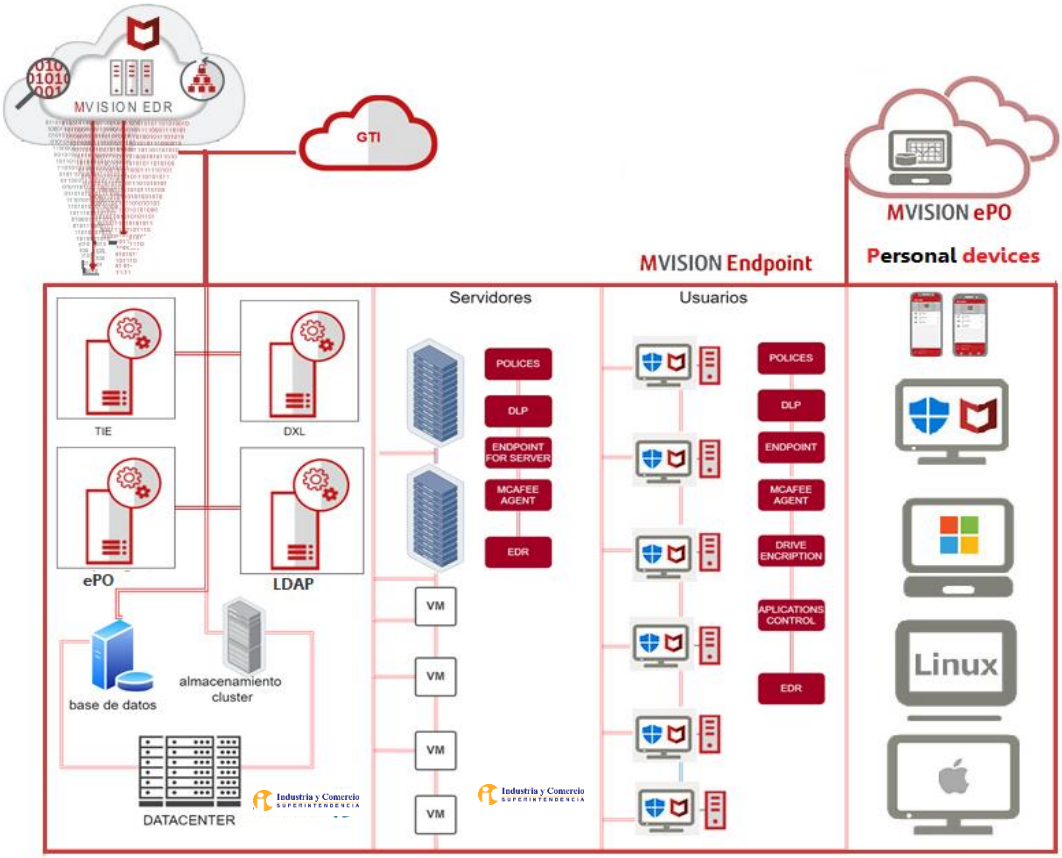
1.4.1. ALCANCE DE RENOVACION

- Renovación de soporte de fábrica de un (1) Enterprise Security, Enterprise Log Manager and Event Receiver 5700 Combination del fabricante Trellix junto con sus componentes adicionales, por un año.

- Renovación de soporte de fábrica de un (1) Global Threat Intelligence (Module for ESM) - Combination 5700 Appliance del fabricante Trellix junto con sus componentes adicionales, por un año.
- Soporte local correctivo, en esquema 7x24 por un año (Opcional).
- Mantenimiento Preventivo de la solución, (Opcional)
- Presentar los servicios especializados de Multisoft para todas las inquietudes, y posibles incidentes que llegasen a presentarse.
- Presentar los servicios especializados de Multisoft para llevar a cabo las sesiones de mantenimientos preventivos sobre la plataforma de seguridad.

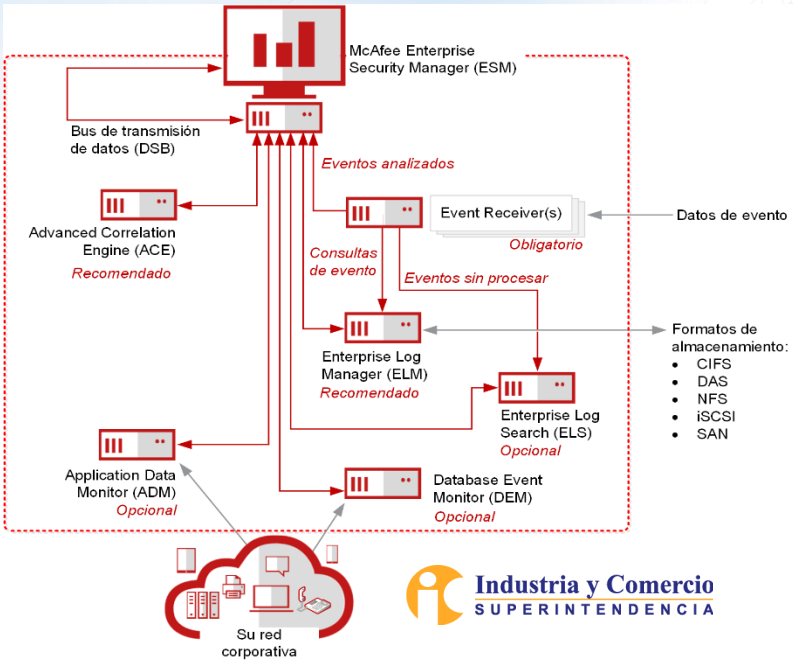
1.5. ARQUITECTURA GENERAL.

A continuación se presenta una arquitectura general de la solucion Trellix EPO , con sus componentes (DLP, EDR)



Nota: Se recomienda como buenas prácticas la migración de la base de datos a una instancia propia ya que la SQL Express está muy limitada y los eventos relacionados con DLP congestionan la base de datos.

A continuación, se presenta una arquitectura a alto nivel de solución de SIEM



2. ALCANCE DEL PROYECTO

Como parte de mejores prácticas y que la entidad pueda tener las últimas versiones de productos A continuación, se describen los requerimientos recomendados para la actualización de las distintas soluciones de Trellix.

- Las máquinas virtuales requeridas para implementación en caso tal de ser requerido deberán ser suministradas por el cliente.
- Se realizará la actualización de las soluciones de TRELLIX según la arquitectura final que se seleccione.
- Multisoft SAS realizará la actualización de la consola de administración y dependerá de la información y conectividad que deberá brindar el cliente para su funcionamiento.
- Se realizarán actas del trabajo técnico realizado.
- Multisoft SAS no realizará manuales personalizados o guías de implementación de los elementos, en caso de requerir este tipo de información el cliente deberá tomarla de la creada directamente por el fabricante.
- Multisoft hará el acompañamiento de instalación de agente en 50% de las máquinas las demás serán a cargo de la entidad
- Las sesiones de implementación del proyecto serán asignadas en común acuerdo según la disponibilidad del cliente y de la agenda de Multisoft con relación a sus ingenieros.
- El cliente deberá exigir a los ingenieros asistentes al proyecto la entrega de las actas de servicio, donde se describe las actividades realizadas.

- Multisoft no es responsable de las claves de productos ingresadas dentro del proceso de implementación. El cliente deberá administrar y almacenar dichas claves según sus procesos internos lo definan.
- Como se encuentra una solución de DLP la propuesta no cuenta con la consultoría previa que se realiza para la puesta en punto de DLP por la información que suministra la entidad ya está realizada según la cantidad de nodos instalados
- Se realizará la actualización de las soluciones de Trellix DLP según la arquitectura final que se seleccione.
- Se realizará cambio de la solución de IPS 7500 según la arquitectura final que se seleccione.
- El cronograma de implementación debe iniciar en un tiempo máximo de 1 mes y si por causas atribuibles al cliente dicho cronograma se extiende a más del doble del tiempo programado, se procederá a liberar los recursos asignados al proyecto y reevaluar el costo de las horas de implementación

2.1. HEALTH CHECK DE LOS COMPONENTES ACTUALES

Multisoft realizara Health Check al inicio del contrato de la solución ofertada en la cual se revisará el estado actual de los productos implementados así como las mejoras que se podrán hacer a los mismos, por medio de un informe de gestión donde se compartirán con las partes dolientes los resultados de lo encontrado en los diferentes productos desplegados. Se plantea una semana de health check sobre la arquitectura actual implementada en la SIC.

2.2. TIEMPO DE IMPLEMENTACIÓN

Durante el tiempo los ingenieros implementadores proporcionados por Multisoft S.A.S prestará los servicios de instalación, configuración, afinamiento y transferencia de conocimientos de la solución.

El tiempo de ejecución de la implementación de la solución es de 3 semanas a partir que el cliente entregue la totalidad la infraestructura y requerimientos solicitados por nuestro personal calificado

2.3. REQUISITOS DE IMPLEMENTACIÓN

Para facilitar la implementación de la solución, SIC debe proporcionar la siguiente información:

Fase I: Inicio de Proyecto	
* Reunión de Inicio (Objetivos, alcances, levantamiento información). * Verificar los requisitos de instalación * Análisis de infraestructura actual	Multisoft / Cliente
Fase II: Instalación	
* Configuración consolas ePo, IPS, SIEM * Incorporación de productos nuevos * Incorporación extensiones de los productos	Multisoft

Fase III: Configuración Herramienta	
* Configuración tareas clientes en compañía del ingeniero encargado de la entidad. * Configuración tareas de servidor en compañía del ingeniero encargado de la entidad. * Configuración de políticas para clientes en compañía del ingeniero encargado de la entidad. * Configuración de tareas de depuración de eventos de clientes y servidor.	Multisoft
Fase IV: Despliegue de productos	
* Despliegue de Link de descarga de aplicación Trellix para endpoint en acompañamiento con el Ingeniero encargado de la entidad. * * Ajustar directivas de acuerdo a resultados obtenidos	Multisoft
Fase V: Pruebas Funcionales	
* Ejecutar checkList de aplicaciones internas y uso de las maquinas cliente	Multisoft / Cliente

3. SERVICIOS DE MANTENIMIENTO Y SOPORTE DE LAS SOLUCIONES

3.1. MANTENIMIENTO PREVENTIVO

A continuación, presentamos el alcance y programación de las visitas de mantenimiento preventivo sobre las soluciones cubiertas en la presente oferta:
Actividades para desarrollar:

- Revisión de la utilización de la herramienta.
- Mantenimiento (creación, modificación y/o Configuración de políticas y/o tareas).
- Solución de inconvenientes.
- Revisión de Políticas creadas.
- Informe de las acciones realizadas.
- Formulación de recomendaciones concretas sobre acciones.
- Seguimiento y evaluación sobre recomendaciones formuladas en la visita anterior.
- Transferencia de Conocimiento.

Duración de la Visita: 4 horas

Periodicidad de las visitas:

DESCRIPCIÓN DEL PRODUCTO	PERIODICIDAD
Trellix Data Loss Prevention Endpoint y Device Control	Mensual
Trellix IPS - SIEM	Mensual

3.2. SOPORTE CORRECTIVO 7X24

Nuestra Mesa de Ayuda está en capacidad de atender consultas y solicitudes de soporte técnico referente a los productos adquiridos con Multisoft S.A.S.

Contamos con 3 puntos de contacto para comunicarse con nuestra Mesa de Ayuda donde nuestros ingenieros atenderán sus requerimientos.

3.2.1. HORARIO DE ATENCIÓN

Lunes a viernes de 8:00 AM – 6:00 PM, horario continuo – No Incluye festivos.

Para atención de requerimientos fuera de este horario, es decir, de lunes a viernes de 18:01 a las 07:59, sábados, domingos y festivos de 00:00 a 23:59 estará disponible el número **320 3495790** donde un ingeniero dará trámite a su requerimiento.

3.2.2. SERVICIO TELEFÓNICO

Multisoft cuenta con una línea telefónica en la ciudad de Bogotá 01-8000-112-695 que lo comunicará con nuestra Mesa de Ayuda.

Al momento de contactarnos debe tener a mano la siguiente información:

- Nombre de la compañía.
- Nombre de la persona contacto.
- Dirección y Número telefónico.
- Dirección de correo electrónico.
- Descripción del servicio.

3.2.3. CORREO ELECTRÓNICO

A través de la cuenta de correo soporte@multisoft.com.co sus requerimientos o solicitudes también serán atendidos.

Al momento de contactarnos por este medio, debe suministrar la siguiente información:

- Nombre de la compañía.
- Nombre de la persona de contacto.
- Número telefónico.
- Dirección de correo electrónico.
- Descripción del servicio.

3.2.4. SOPORTE REMOTO

Nuestros ingenieros cuentan con una herramienta para tomar control remoto y así poder solucionar sus requerimientos. En caso de no ser permitido este tipo de acceso, está bajo su responsabilidad informar al ingeniero que lo está atendiendo, con el fin de tomar una medida alterna para atenderle.

Horario de Atención: lunes a domingo de 00:00 a 23:59.

3.2.5. SOPORTE EN SITIO

Si al efectuar la validación del servicio se requiere que un ingeniero se desplace a cliente, se programa una visita para ir a efectuar la atención del requerimiento.
Horario de Atención: lunes a Domingo de 00:00 a 23:59.

3.2.6. TIPOS DE ESCALAMIENTO

El modelo de escalamiento de requerimientos técnicos es:

- **Escalamiento Nivel 1:** Atención por ingeniero de Mesa de Ayuda Nivel 1.
- **Escalamiento Nivel 2:** Escalado a ingeniero de soporte de 2do. Nivel.
- **Escalamiento Nivel 3:** Se requiere programar una visita presencial para dar continuidad al servicio.
- **Escalamiento Nivel 4:** Se requiere intervención del fabricante.

3.2.7. TIEMPOS DE RESPUESTA

Dependiendo del nivel de criticidad de la falla encontrada, se darán los tiempos de respuesta y atención a la misma, estipulados a continuación:

NIVEL DE CRITICIDAD	DESCRIPCIÓN
Critica	• Paraliza la disponibilidad de algún servicio crítico del negocio. • Expone la confidencialidad de la información del negocio. • Afecta significativamente algún servicio crítico del negocio. • No hay funcionalidad del dispositivo en tu totalidad, o en una parte de él, que afecta uno o más servicios críticos del negocio.
Moderada	• Afecta la disponibilidad de uno o más servicios críticos del negocio. • El servicio está disponible de forma intermitente, y esta intermitencia permite ejecutar actividades relacionadas con el servicio. • La seguridad del servicio se encuentra afectada y es posible vulnerar el servicio, pero el servicio está activo para la organización
Baja	• No afecta la disponibilidad del servicio. • No pone en riesgo la confidencialidad de información del negocio. • Afecta un servicio, pero la organización puede continuar sin él. • Afecta la seguridad de un servicio, pero en caso de vulnerar el servicio, la organización puede continuar

Los tiempos de respuesta, están estipulados de acuerdo con el tipo de soporte adquirido y la criticidad definida para cada requerimiento de la siguiente forma:

Tipo de Soporte	Tiempos de Respuesta	Crítica	Moderada	Baja	Tipo de servicio	Horario de servicio	Boletines de seguridad	Telefónico	Correo	Remoto	Presencial
Platinum	Primer contacto	1 h	2 h	8 h	**7 X 24**	**00:00 a 23:59**	x	x	x	x	X

	Tiempo de atención	2 h	4 h	24 h							

3.2.8. PROCESO PARA ATENCIÓN DE UN REQUERIMIENTO

Este es el proceso que debe tener en cuenta al momento de colocar un requerimiento:

a) Contactar a nuestra mesa de ayuda para colocar su requerimiento por cualquier de los tres (2) puntos de contacto.
b) Una vez puesto su requerimiento, uno de nuestros ingenieros se pondrá en contacto en los tiempos de respuesta acordados de acuerdo con la criticidad asignada a su requerimiento.
c) La mesa de ayuda creará un ticket y dará gestión por medio de nuestra herramienta de gestión de incidentes.
d) Le llegará un correo electrónico con el número de ticket y la descripción del requerimiento (esta notificación se realizará a la persona de contacto suministrada al momento de suscribir sus servicios).
e) Sí el requerimiento no puede ser solucionado por teléfono y requiere de acceder a la plataforma afectada, el ingeniero de soporte realizará soporte remoto para avanzar en la atención y/o solución del requerimiento.
f) En caso de no ser posible dar solución remotamente, un ingeniero de soporte se desplazará a sitio para dar solución al requerimiento, de esta forma dar continuidad y solución a éste.
g) El ingeniero de soporte debe documentar el ticket con los procesos efectuados para dar solución a su requerimiento.
h) Se realiza cierre del ticket. Al cliente le llegará un correo electrónico con la descripción del cierre del ticket.

3.2.9. EXCLUSIONES

Multisoft no tendrá obligación de proporcionar el servicio contratado, cuando el daño haya sido ocasionado por:

- Los productos han sido instalados en equipos que están en condiciones ambientales, eléctricas y de temperatura no aptas, y/o no cumplen con las especificaciones técnicas indicadas por el fabricante.
- Inundaciones, incendio, terremoto, huelgas, motines, etc., es decir, casos de fuerza mayor.
- Daño por mantenimiento, reparación, modificación o reinstalación de los equipos y software donde se encuentran instalados los productos adquiridos a Multisoft.
- Por mal uso o maltrato de los equipos, o uso indebido de los equipos y software, o parte de ellos.

3.2.10. ENTREGABLES

Los servicios prestados tienen como definición diferente entregables que deberán estar en común acuerdo con el cliente para la generación de estos, presentación y seguimiento de la información allí contemplada.

- **Actualización:**
  - Cronograma de actividades
  - Documentación durante el proceso de actualización, a través de actas generadas en cada sesión

- **Implementación Nuevos Productos**
  - Cronograma de actividades
  - Documentación durante el proceso de implementación
  - Plantilla de configuración
  - Actas generadas por el implementador de cada sesión hecha

- **Gestión Diaria**
  - Informe Semanal de Actividades
  - Consolidado mensual de gestión
  - Avances y recomendaciones mensuales
  - Informe de productos de seguridad instalados y versiones de los mismas que se encuentra implementados en la entidad con sus respectivas recomendaciones (mensualmente)

- **Mantenimiento**
  - Documentación durante el proceso de mantenimiento, a través de actas generadas por cada sesión realizada, firmada por el cliente y el proveedor.

- **Soporte**
  - Informe de casos abiertos y cerrados de solicitudes de soporte (mensualmente)

4. OFERTA ECONOMICA

LICENCIAMIENTO ONE TIME - TRELLIX ENDPOINT - EDR - DLP - IPS - SIEM

CLIENTE SIC - Superintendencia de industria y comercio.
MONEDA **Pesos Col**
SAM Mario Alarcon

ITEM	DESCRIPCION PRODUCTO	SKU	CANTIDAD	VALOR UNITARIO PESOS COL	VALOR TOTAL PESOS COL
1	ProtectPLUS Business Software Support	DLPYFM-AA-EA	300	$ 44.555,94	$ 13.366.782,61
2	ProtectPLUS Business Software Support	DLPYFM-AA-GA	1320	$ 54.588,41	$ 72.056.695,65
3	ProtectPLUS Business Software Support	CEBYFM-AA-GI	1001	$ 72.071,45	$ 72.143.520,72
5	ProtectPLUS Business Software Support	CEBYFM-AA-EI	400	$ 71.260,00	$ 28.504.000,00
6	ProtectPLUS Business Software Support	CEBYFM-AA-EI	399	$ 52.965,51	$ 21.133.237,39
7	ProtectPLUS Business Software Support	CEBYFM-AA-DI	220	$ 72.071,45	$ 15.855.718,84
9	Advanced RMA (next business day ship) Hardware Support	IAC650ACARMAI	1	$ 1.940.101,45	$ 1.940.101,45
10	Advanced RMA (next business day ship) Hardware Support	IAC650ACARMAI	1	$ 1.940.101,45	$ 1.940.101,45
11	Trellix Network Security Manager Next Generation Appliance-Only for Standard, Global, Failover and Central manager	NSM-MAPL-NGI	1	$ 67.696.200,00	$ 67.696.200,00
12	Advanced RMA (next business day ship) Hardware Support	NYVMAPLNGARMAI	1	$ 10.581.741,16	$ 10.581.741,16
13	Advanced RMA (next business day ship) Hardware Support	NYVMAPLNGARMAI	1	$ 6.716.439,42	$ 6.716.439,42
14	Trellix Network Security IPS NS7500 Appliance	IPS-NS7500I	1	$ 128.685.208,70	$ 128.685.208,70
15	Business Software Support & 1yr Advance RMA (next business day ship) Hardware Support	IPSNS7150ARMAI	1	$ 45.518.837,25	$ 45.518.837,25
16	Advanced RMA (next business day ship) Hardware Support	RBIPSNS7500ARMAI	1	$ 26.726.409,71	$ 26.726.409,71
17	Advanced RMA (next business day ship) Hardware Support	RBIAC4P1GMM62MODI	1	$ 6.584.689,57	$ 6.584.689,57
18	Trellix IPS NS7500 - 3Gbps Software license (Throughput based entitlement)	NS75X03ECE-AT-AI	1	$ 79.423.401,01	$ 79.423.401,01
19	Trellix Network Security Manager Software Subscription Standard Edition	NMSECE-AA-AI	1	$ 16.846.645,94	$ 16.846.645,94
20	Trellix Network Security Manager Software Subscription Standard Edition	NMSECE-AA-AI	1	$ 10.596.494,78	$ 10.596.494,78
21	Global Threat Intelligence (Module for ESM) - Combination 5700 Appliance	GTE5700ELMGIEAD-AI	1	$ 39.022.448,12	$ 39.022.448,12
22	Business Software Support & 1yr Advance RMA (next business day ship) Hardware Support	ETM5700ELMARMAI	1	$ 97.790.924,20	$ 97.790.924,20
	SUBTOTAL COTIZACION			**$ 540.437.155,51**	**$ 763.129.597,97**
			IVA	**19%**	**$ 144.994.623,61**
				TOTAL COTIZACION	**$ 908.124.221,59**

SERVICIOS TRELLIX ENDPOINT - DLP - IPS - SIEM (OPCIONAL)

CLIENTE SIC - Superintendencia de industria y comercio.
MONEDA **Pesos Col**
SAM Mario Alarcon

ITEM	DESCRIPCION	CANTIDAD	CANT. MES	VALOR UNITARIO PESOS COL	VALOR UNITARIO PESOS COL
1	Servicios de Implementacion y Health Check	N/A	1	$ 24.475.000,00	$ 24.475.000,00
2	Soporte Mensual (Opcional)	N/A	12	$ 2.000.000,00	$ 24.000.000,00
3	Servicios de Matenimiento Preventivo (Opcional)	N/A	12	$ 520.000,00	$ 6.240.000,00
	SUBTOTAL COTIZACION			**$ 26.475.000,00**	**$ 54.715.000,00**
			IVA	**19%**	**$ 10.395.850,00**
				TOTAL COTIZACION	**$ 65.110.850,00**

5. CONDICIONES COMERCIALES

MONEDA DE COTIZACIÓN

Los valores incluidos en la propuesta económica en licenciamiento de la solución se encuentran expresados en Pesos. El pago del licenciamiento es One Time y debe pagarse a los 30 días después de la emisión de la factura.

Los valores incluidos en la propuesta económica en implementación (one time) y soporte platino se encuentran expresados en Pesos Col. Los servicios de soporte mensual y mantenimiento preventivo son opcionales a la oferta.

TIEMPO DE INICIO DE LOS SERVICIOS

30 días luego de formalizada la orden de compra / contrato

VALIDEZ DE LA OFERTA:

Esta oferta tiene una vigencia de sesenta (60) días a partir de la fecha de su presentación.