Upgrade de Hardware Firewall de próxima generación

Palo Alto Networks PA-1410

Presentado a:

Alcaldía de Bucaramanga

Bogotá, 13 de mayo de 2026

Estimado Cliente:

Alcaldía de Bucaramanga

CARTA DE PRESENTACIÓN

GMS Seguridad de la Información agradece la oportunidad de presentarle esta oferta de refrescamiento de hardware firewall de próxima generación.

Hemos estructurado nuestra oferta con acompañamiento de Palo alto Networks para brindar las mejores soluciones enfocadas a Seguridad de la Información, que se complementan con servicios de consultoría en estrategias, normas de TI y servicios de desarrollo de aplicaciones.

Somos una empresa de Seguridad de la Información con más de 40 años de experiencia, durante los cuales hemos podido atender a muchas de las compañías más importantes de la región. Nuestras soluciones cubren las más altas exigencias de nuestros clientes, y nos caracterizamos por cumplir proyectos de alta complejidad. Asumimos el papel de socio estratégico para establecer relaciones exitosas a largo plazo.

Esperamos que esta propuesta sea de su conveniencia y quedo a su disposición para atender cualquier inquietud o comentario que pudiera surgir respecto a la misma.

Cordialmente,

Erika Mazo

Gerente de Cuentas Estratégicas

Erika.mazo@gmsseguridad.com

Celular: +57 313 6359576

Declaratoria de Confidencialidad

El presente documento y todo su contenido es de carácter confidencial. Todos sus derechos son reservados por su autor, GMS. GMS autoriza expresamente a los funcionarios de la **Alcaldía de Bucaramanga** que tengan injerencia directa en la evaluación de proyectos tecnológicos, como también a los miembros activos de su Comité de Seguridad, a acceder al contenido de este documento con el propósito exclusivo de la evaluar la oferta planteada por GMS. Las personas que accedan al contenido del presente documento aplicarán al menos las mismas buenas prácticas de cuidado de información confidencial que mantienen para la información confidencial de sus propias organizaciones, comprometiéndose a no usar el documento ni su contenido para ningún otro propósito que el establecido en esta declaratoria, ni compartirlo de forma completa ni parcial con personas no autorizadas.

1 Presentación corporativa.

Fundada en 1978, GMS Seguridad de la Información es una de las empresas de seguridad informática de mayor trayectoria en la región. Nuestra visión es ser el aliado predilecto de las principales organizaciones de la región para proteger su información, sumando a sus negocios con la efectiva mitigación de ciber riesgos. Tenemos la misión de Aportar a la mejora continua en la mitigación de ciber riesgos en empresas e instituciones de la región andina que tienen como imperativo a la protección de su información. Lo hacemos con un equipo humano altamente especializado que aplica metodologías, servicios y tecnologías de clase mundial.

Hemos estructurado nuestra oferta para brindar las mejores soluciones enfocadas a Seguridad de la Información, que se complementan con servicios de consultoría en estrategias, normas de TI y servicios de desarrollo de aplicaciones. Con nuestro apoyo, su empresa puede dejar en el pasado preocupaciones como incompatibilidad entre herramientas o rendición de cuentas con diversos proveedores que no logran responsabilizarse de la operación global de su red empresarial.

Datos de la Empresa:

- Razón Social: Grupo Microsistemas Colombia S.A.S
- NIT: 900418656-1
- Dirección: Transversal 22 # 98 – 82 OF 502 - Bogotá, Colombia
- Teléfono: 3213396584

Sistemas de Gestión

Para asegurar los niveles de servicio que requieren las empresas más exigentes, GMS opera con un sistema de gestión de tickets para el control de actividades y requerimientos. En el mismo, hemos habilitado un portal web que permite a nuestros clientes revisar el historial y estado de los tickets creador, ingresar nuevas solicitudes. El sistema también permite registrar los niveles de satisfacción ante los soportes entregados, con lo cual mantenemos un control para asegurar un mejoramiento continuo.

1.1 Nivel de Partner Palo Alto Networks

January 26, 2026

To Whom It May Concern:

On Behalf of the Global NextWave Partner Program team at Palo Alto Networks, this is to inform you the partnership between Palo Alto Networks, Inc. and:

Grupo Microsistemas Colombia Sas

Bogota, Bogota

Colombia

At the time of this communication, **Grupo Microsistemas Colombia Sas** is classified as a Solution Provider at the **Diamond Innovator** level partner respectively in the Palo Alto Networks NextWave Partner Program and is in good standing.

Grupo Microsistemas Colombia Sas is also currently set with the following Specializations : **Hardware Firewall;Software Firewall;Prisma SASE;Cortex XDR;Cortex XSOAR;Cortex XSIAM**

Thank you,

Michael Khoury
VP, Global Channel Programs
Palo Alto Networks

2 Propuesta técnica

2.1 Antecedentes

La Alcaldía de Bucaramanga, actualmente posee equipos PA850 de tercera generación, los cuales ya no se encuentran en ciclo de venta y se propone realizar su refrescamiento de hardware, permitiendo tener las capacidades de las nuevas versiones que no son soportadas por los dispositivos actuales y adicionando mayores características que permiten mejorar y fortalecer la seguridad de los dispositivos perimetrales.

2.2 Componentes de la solución

Dentro de la presente propuesta se detalla su alcance y sus características:

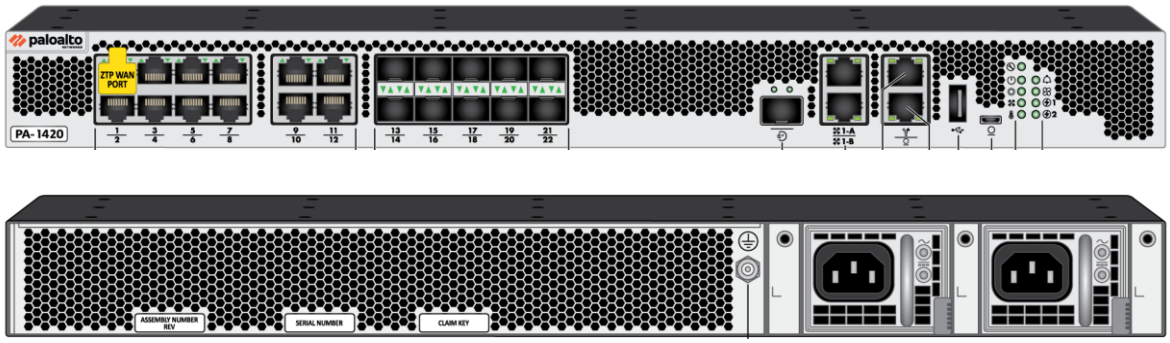
2.2.1 Listado de componentes

Adquisición, activación, migración, configuración, implementación, puesta en marcha, estabilización y soporte de los siguientes componentes que hacen parte del NGFW de Palo Alto networks **para la Alcaldía de Bucaramanga**.

Componente	Cantidad
Palo Alto Networks PA-1410	2
PA-1410, Precision AI Network Security Subscription Bundle.	2
PA-1410, Premium support	2
Spare Power Supply 450w	2
SFP+ form factor, 10Gb direct attach twin-ax passive cable	1

2.2.2 Palo Alto Networks PA-1410

Dispositivo de seguridad perimetral de capa de aplicación de cuarta generación que reemplazara los dispositivos PA-850.



PA1410 y PA1420 front & back panel

Se adjunta hoja de datos con las especificaciones del equipo.

2.2.3 Precision AI Network Security Subscription Bundle.

El Precision AI Security Subscription Bundle de Palo Alto Networks es un paquete de suscripción avanzado que combina tecnologías de inteligencia artificial (IA) y aprendizaje automático (ML) para mejorar la seguridad en los firewalls de próxima generación (NGFW) de Palo Alto.

Este Bundle este compuesto por las siguientes suscripciones:

2.2.3.1 Advanced WildFire

Advanced Wildfire es la suscripción que permite tener una detección proactiva de malware desconocido (zero-day) y ransomware mediante análisis sandboxing en la nube. El cual permite:

- ✓ Sandboxing en la nube: Analiza archivos sospechosos (PDF, Office, ejecutables, etc.) en un entorno seguro.
- ✓ Detección basada en IA: Usa machine learning para identificar variantes de malware nunca vistas.
- ✓ Informes de análisis: Proporciona detalles sobre el comportamiento del malware (C2 callbacks, exploits, etc.).
- ✓ Soporte para múltiples formatos: Incluye análisis de archivos, correos electrónicos y tráfico web.

2.2.3.2 Advanced Threat Prevention

Advanced Threat Prevention permite proteger contra exploits, ataques dirigidos y evasión de técnicas de seguridad, brindando la capa IPS e IDS para todo el tráfico que fluye sobre la red, esto demostrando características clave como:

- ✓ Protección contra vulnerabilidades (CVEs): Mitiga exploits conocidos (ej. Log4j, ProxyShell).
- ✓ Anti-evasión: Detecta técnicas que intentan evadir firewalls (fragmentación de paquetes, cifrado engañoso, etc.).
- ✓ Inspección SSL/TLS: Descifra y analiza tráfico cifrado para detectar amenazas ocultas.

2.2.3.3 Advanced URL Filtering

Advanced URL Filtering permite realizar un Filtrado inteligente de URLs para bloquear phishing, malware y sitios de riesgo con funcionalidades como:

- ✓ Categorización en tiempo real: Usa IA para clasificar sitios web no catalogados previamente.
- ✓ Protección contra phishing/ransomware: Bloquea dominios maliciosos incluso si son nuevos.
- ✓ Controles granulares: Permite políticas por usuario, aplicación o horario.

- ✓ Soporte para HTTPS: Filtra URLs incluso en tráfico cifrado.
- ✓ Protección de credenciales corporativas: evita que los usuarios usen las mismas credenciales corporativas en sitios Web de categorías previamente definidas.

2.2.3.4 Advanced DNS Security

Advanced DNS Security Previene ataques basados en DNS (exfiltración de datos, tunneling, etc.)., protegiendo a los usuarios con las siguientes características:

- ✓ Bloqueo de dominios maliciosos: Listas actualizadas de sitios asociados a malware, botnets o C2.
- ✓ Protección contra DNS tunneling: Detecta tráfico DNS anómalo usado para evadir firewalls.
- ✓ Enforcement de políticas: Restringe consultas DNS a servidores no autorizados.
- ✓ Prevención de exfiltración: Previene y protege frente a la exfiltración de datos a través de goteo mediante el uso indebido del protocolo DNS.

2.2.3.5 Advanced SDWAN

El Advanced SD-WAN de Palo Alto Networks integra capacidades de red definida por software (SD-WAN) directamente en sus firewalls de próxima generación (NGFW), combinando seguridad avanzada con una gestión optimizada del tráfico de red.

Esto permite que el tráfico que fluye a través de estos canales SDWAN realicen una optimización inteligente del tráfico basado en la aplicación, monitoreando la calidad de los enlaces garantizando la mejor experiencia para la aplicación

Permitiendo una redundancia no solo basada en métricas como Jitter, PacketLoss y ping, sino que realizando un análisis eficiente del flujo y respuesta las aplicaciones, mejorando la experiencia de uso de estas.

2.2.3.6 Premium Support for NGFW

El licenciamiento de Premium Support para los firewalls de próxima generación (NGFW) de Palo Alto Networks ofrece un nivel superior de soporte técnico y servicios proactivos diseñados para maximizar la disponibilidad, el rendimiento y la seguridad de tus dispositivos, esto puede constar de:

Soporte Técnico Prioritario 24x7x365 Acceso rápido a expertos:

- Respuesta en menos de 30 minutos para casos críticos (severidad 1).
- Canales de contacto: Teléfono, portal en línea y correo electrónico.

Actualizaciones de software y parches:

- Acceso prioritario a las últimas versiones de PAN-OS y parches de seguridad.

Garantía de Hardware

- Se tiene acceso a cambio de equipos en caso de fallas posterior al diagnóstico del fabricante.

2.3 Migración y puesta en marcha de la solución propuesta

2.3.1 Supuestos

Como fase exploratoria de proyecto se listan los principales supuestos en el marco del anterior alcance:

Supuestos a cargo de Grupo Microsistemas Colombia S.A.S:

- Disponer de personal idóneo para el desarrollo de las actividades de las tecnologías a implementar.
- Otorgar a los ingenieros y consultores las herramientas y recursos necesarios para la realización de las actividades técnicas definidas en el alcance.
- Entrega en tiempos estimados de equipos con su correspondiente licenciamiento a nombre de la **Alcaldía de Bucaramanga**.
- Coordinación del equipo técnico multidisciplinario para la implementación (Especialistas en cada tecnología a implementar).

Supuestos a cargo de la Alcaldía de Bucaramanga.

- Asegurar la participación del personal clave relacionado en las diferentes actividades planificadas.
- Garantizar los prerrequisitos solicitados para la implementación.
- Preparar el sitio de instalación y operación de los firewalls en niveles de temperatura y humedad estándar, proveer rack o lugar apropiado para el tamaño y peso de los equipos, así como la identificación de puertos para el cableado y disponibilidad de conexiones para la energización de los dispositivos PA-1410.
- Entregar la información requerida para cada una de las fases del proyecto de forma oportuna.
- Revisar y aprobar los entregables del proyecto en los tiempos acordados en el cronograma del proyecto.
- Suministrar accesos remotos para verificar configuraciones de la solución actual.
- Suministrar copia de seguridad de las configuraciones de los dispositivos actuales.
- Suministrar las conexiones remotas necesarias para las actividades.

2.3.2 Restricciones

Las restricciones que hasta el momento se han podido evidenciar en el marco inicial del proyecto son las siguientes:

- Asociadas a las funcionalidades de cada una de las herramientas según el licenciamiento a contratar, en este apartado deberá dirigirse al numeral de la propuesta comercial en donde se lista cada uno de los licenciamientos a contratar y la arquitectura técnica de instalación.
- Restricciones de recursos, Grupo Microsistemas Colombia S.A, en el marco del proyecto de implementación asigna recursos tanto humanos como técnicos según las estimaciones de tiempo, lo anterior en un marco de tareas programadas con anticipación y no a demanda del cliente; dicho equipo de trabajo se detallará más adelante en el presente documento.
- Las actividades objeto del contrato se coordinarán previamente en horario laboral, en días y horas no hábiles o en fines de semana o días festivos, tanto en horario diurno como nocturno, es decir 7x24.
- Las actividades desarrolladas por expertos o especialista no deben superar más de doce (12) horas continuas.

2.3.3 Alcance de migración

Dentro del proceso de refrescamiento de hardware de seguridad perimetral se tienen presente el siguiente alcance:

- Activación de dispositivos y licenciamiento dispositivos nuevos PA-1410
- Definición de prerrequisitos el diseño de arquitectura a detalle, la cual será informada en la fase de levantamiento de información a detalle.
- Migración de configuraciones de los dispositivos PA-850 a los dispositivo PA-1410
- Verificación de configuraciones migradas.
- Integración con Strata Cloud Manager Essentials, para envío de telemetría y salud del dispositivo.
- Los servicios de puesta en marcha de los dispositivos PA-1410 se realizaran en sitio por parte de un especialista de GMS.
- Configuración y puesta en marcha de HA en modo activo pasivo.
- Los dispositivos NGFW estarán en la última versión recomendada por fabrica.
- Adopción del uso de buenas prácticas desde el momento de la configuración inicial de los dispositivos.
- Documentación respectiva de la migración del equipo.

2.3.4 Alcance Post Implementación

Posterior a la puesta en marcha se tiene el siguiente alcance durante el desarrollo del contrato:

- Un periodo de estabilización de la solución durante un día posterior a su puesta en marcha.
- Soporte 7/24/365 directamente con especialistas de GMS.
- Apoyo y gestión de casos escalados a fabricante.
- Apoyo en la actualizacion de nuevas versiones de firmware de los dispositivos NGFW.

- Gestion y apoyo de RMAs.
- 1 BPA (Best practice Assessment) por año del dispositivo, mencionando las mejoras a realizar.
- 2 mantenimientos por años, ejecutados de manera semestral sobre los dispositivos PA-1410 ejecutados remotamente
- Transferencia de conocimiento de la solución.

2.3.5 Prerrequisitos de implementación NGFW

Dentro del proceso de la implementación se requiere:

- Personal por parte de la **Alcaldía de Bucaramanga** con la información de Canales, Vlans, segmentos de red, enrutamientos y demás relacionados.
- Backup de configuración de dispositivos actuales.
- Diagrama de arquitectura a detalle de la solución actual.
- Disponibilidad de dos unidades en rack de centro de datos para la ubicación de los dispositivos PA-1410.
- Disponibilidad de 4 tomas de corriente eléctrica para la alimentación eléctrica de los dispositivos PA-1410.
- Acceso a portal de soporte palo alto networks para el registro y activación de licencias.
- Identificación de puertos de conectividad de redes.
- En caso de tener VPN's Sitio a Sitio, se requiere de los administradores del peer remoto en caso de que se requiera repisar las PSK.
- En caso de tener publicaciones, se debe tener al administrador del servicio para su verificación pre y post migración.

2.3.6 Plan de migración

A continuación, se define un plan de migración **estimado** de los dispositivos a alto nivel. Este iniciará una vez se firme el contrato y se tengan disponibles los equipos nuevos, la migración se definirá en conjunto con la **Alcaldía de Bucaramanga** para así minimizar el impacto en la operación.

Actividad	Responsables
Kick Off Inicial	GMS/Alcaldía
Activación y alistamiento de dispositivos Nuevos	GMS
Configuración de dispositivos	GMS/Alcaldía
Verificación de configuraciones	GMS/Alcaldía
Envío de equipos	GMS
Montaje y energización de dispositivos	GMS/Alcaldía
Identificación de conexiones físicas	Alcaldía
Diseño de plan de pruebas	Alcaldía/GMS

Ejecución Plan de pruebas previo a la puesta en marcha	Alcaldía
Puesta en Marcha	GMS/ Alcaldía
Ejecución de plan de pruebas post puesta en marcha	Alcaldía
Configuración y levantamiento HA Activo/pasivo	GMS
Afinamiento y Estabilización	GMS
Creacion y envío de documentación	GMS
Cierre de migración NGFW	GMS/ Alcaldía
Transferencia de conocimiento	GMS
Paso a modelo de soporte y servicios de seguimiento	GMS

Durante la ejecución del plan estimado se debe tener en cuenta que las actividades serán desarrolladas secuencialmente y en el momento en que se confirmen el éxito de cada una.

2.3.7 Soporte y mantenimientos

Una vez finalizado con éxito el proceso de migración y estabilización de los dispositivos NGFW PA-1410 de Palo Alto Networks se llevará a cabo la transferencia de conocimiento y el paso a soporte de la solución.

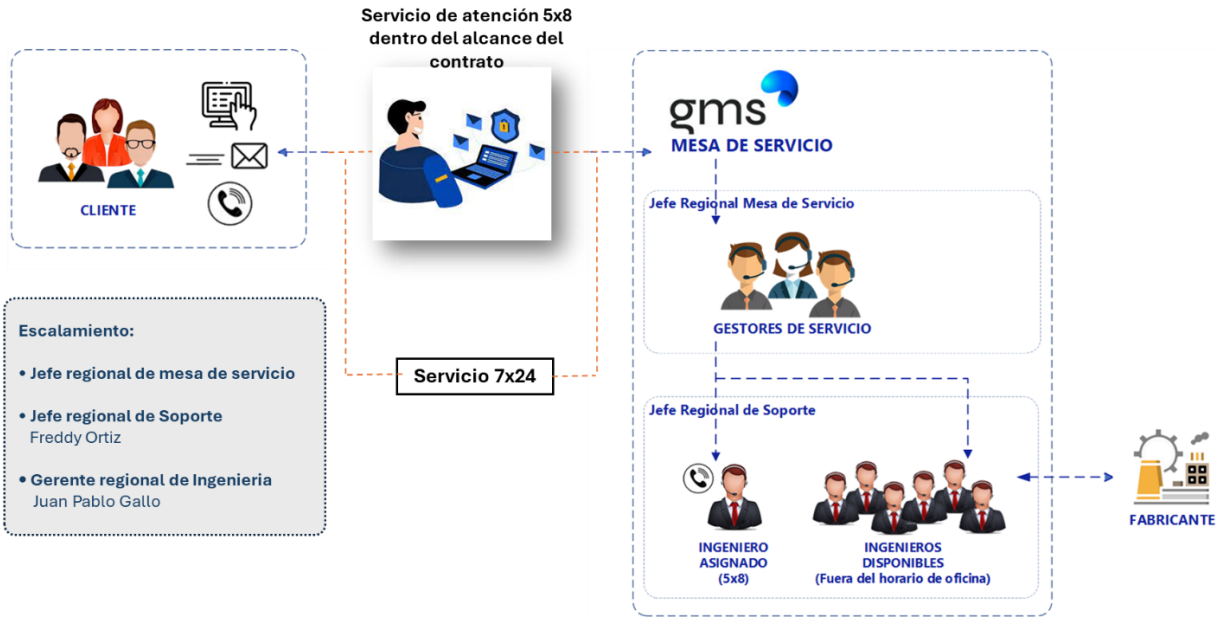
Dentro del alcance del soporte con GMS únicamente se limitará al licenciamiento adquirido mencionado en los componentes de la solución

Durante el término del contrato se tendrán soporte premium ilimitado que tiene como cobertura todo soporte relacionado con los licenciamientos y dispositivo adquiridos disponibles durante el término del contrato.

Este soporte se desarrollará bajo los siguientes ANS:

	Prioridad	Incidentes		Solicitudes de servicio	
		Tiempo de respuesta	Actualización de estado	Tiempo de respuesta	Actualización de estado
Premium	Urgente	1 hora	2 horas		
	Alto	1 hora	4 horas		
	Medio	2 horas	24 horas	2 horas	hasta en 2 días
	Bajo	4 horas	48 horas	4 horas	hasta en 4 días

El flujo de escalamiento de soportes se desarrollar de la siguiente manera:



Durante la gestión y soporte del proyecto se definirán los canales de comunicación y la matriz de escalamientos entre GMS y la **Alcaldía de Bucaramanga**,

3 Propuesta económica

La siguiente propuesta económica se presenta como proyecto completo del refrescamiento de hardware de seguridad perimetral a dispositivos Palo Alto Networks PA-1410.

ITEM	DESCRIPCIÓN	CANT	VALOR UNITARIO	VALOR TOTAL
1	Upgrade de equipos PA850 a Palo Alto Networks PA-1410	2	46.575.300	93.150.600
2	Upgrade a PA-1410, Precision AI Network Security Subscription Bundle (Advanced Threat Prevention, Advanced URL Filtering, Advanced Wildfire, Advanced DNS Security and Advanced SD-WAN), 1 year (12 months) term.	2	40.500.600	81.001.200
3	PA-1410, Premium Support, 1 year (12 months) term.	2	10.500.000	21.000.000
4	Soporte ilimitado del proveedor por 1 año vía web, correo electrónico o telefónico 7*24 ilimitado. Incluye: Migración de equipos actuales PA850 a los PA1410 y capacitación.	1	14.080.000	14.080.000
SUBTOTAL				**209.231.800**
IVA				**39.754.042**
TOTAL				**248.985.842**

4 Condiciones comerciales

• Los valores indicados están en Pesos colombianos.

• Validez de la oferta –90 dias

• La Factura será emitirá por parte de Grupo Microsistemas Colombia SAS, NIT 900418656-1.

• La factura se emite una vez recibida la orden de compra la cual es un documento vinculante entre las partes, y se da por aceptado que el cliente conoce y acepta las condiciones comerciales.

• El valor de la factura emitida será por el valor total de la propuesta, dependiendo la opción que tome el cliente.

• Una vez emitida y radicada la factura, no se aceptan cancelaciones de la misma.

• Forma de pago: 30 días calendario contados luego de radicada la factura.

• Tiempo de entrega 40 días. Estos son tiempos estándar, pero podrán variar acorde a situaciones que no se puedan prever.