| | | |
|---|---|---|
| IBAL SIG | **ANÁLISIS DE PRECIO DE MERCADO**<br>**SISTEMA INTEGRADO DE GESTIÓN** | **CÓDIGO:** GJ-R-002<br>**FECHA VIGENCIA:** 2022-01-12<br>**VERSIÓN: 04**<br>**Página 1 de 1** |

**CIUDAD Y FECHA: 10 DE MARZO DE 2022**

**DEPENDENCIA QUE REALIZA EL ANÁLISIS DE PRECIO DE MERCADO: GESTIÒN TECNOLOGICA**

**OBJETO CONTRACTUAL: CONTRATAR LA ADQUISICION DE UNA SOLUCIÓN DE FIREWALL CON SU RESPECTIVO LICENCIAMIENTO POR 24 MESES**

**MODALIDAD DE CONSULTA: Se solicito cotización de manera verbal a las empresas GMS , ITSEC y INFORTEC , quienes allegaron cotización al correo sistemas@ibal.gov.co**

| ITEM | DETALLE DEL SERVICIO | CPC | | CANTIDAD | GMS | | | ITSEC | | | INFORTEC | | | PROMEDIO |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | CODIGO | DESCRIPCION | | VALOR UNITARIO | IVA (SI APLICA) | VALOR TOTAL | VALOR UNITARIO | IVA (SI APLICA) | VALOR TOTAL | VALOR UNITARIO | IVA (SI APLICA) | VALOR TOTAL | |
| 1 | CONTRATAR LA ADQUISICION DE UNA SOLUCIÓN DE FIREWALL CON SU RESPECTIVO LICENCIAMIENTO POR 24 MESES | 45240 | Máquinas de procesamiento automático de datos presentadas en forma de sistemas | 1 | $45.500.000 | $ 8.645.000 | $54.145.000 | $50.400.000 | $9.576.000 | $59.976.000 | $39.410.000 | $7.487.900 | $46.897.900 | **$53.672.966** |
| VALOR PRESUPUESTO OFICIAL | | | | | | | | | | | | | | **$53.672.966** |

**CARLOS ANDRES CAMACHO ACUÑA**
Profesional Especializado 03 Gestión Tecnológica

INFORTEC
Especialistas en Ciberseguridad

20 AÑOS

Pereira, Febrero 22 de 2022

Señores:
**EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO - BAL**
Atte. Ing. **CARLOS CAMACHO**
Dirección de TI
Ibagué

Cordial Saludo:

Es muy grato para nosotros, poner a su entera disposición nuestra organización.

**INFORTEC** es una compañía especializada en brindar soluciones de ciberseguridad para la protección de la información y la optimización de los recursos informáticos.

20 años de experiencia y un equipo humano especializado, nos permiten aportar a la construcción de las mejores alternativas para la protección de la información en los puntos críticos donde es accedida, mitigando el riesgo de que esta sea vulnerada.

Las soluciones de **INFORTEC** están pensadas en una estrategia de seguridad completa y continua, ajustada a las necesidades de cada cliente, a la manera como fluye la información en el desarrollo de sus actividades y que sea fácilmente adaptable a las nuevas tendencias y riesgos que continuamente aparecen ya sea por la identificación de nuevas amenazas o por la implementación de nuevos servicios propios de la dinámica del negocio.

Agradecemos la oportunidad brindada permitiéndonos aportar, con nuestra experiencia, a la estrategia de su organización.

Atentamente,

**FEDERICO GIRALDO R.**
Gerente
3162548018

## JUSTIFICACION

Internet es sin lugar a duda el mayor factor de cambio en la sociedad actual, casi todo lo que interactúa alrededor del mundo posee un componente derivado de la web y su presencia es indispensable en el ejercicio de cualquier actividad ya sea en menor o mayor proporción, brindando a todas las organizaciones y personas, infinidad de herramientas para estar "conectados".

Las empresas actuales encuentran en la web, las redes sociales, el e-mail, los dispositivos móviles, la nube, la virtualización y muchos aspectos más, las herramientas necesarias para el manejo eficaz de las actividades y el contacto permanente con los clientes y aliados estratégicos, expandiendo las operaciones y llegando a nuevos mercados.

¿Pero...y que pasa con la información?

Internet ofrece grandes beneficios, pero también plantea grandes retos; uno de los más importantes es el manejo y el cuidado de la información, tarea nada fácil para las gerencias de TI mas aun cuando la tendencia es movilidad y los datos deben contar con completa accesibilidad, aumentando el riesgo de que la información privilegiada caiga en manos equivocadas. Entonces....que hacer al respecto?

## PALO ALTO NEXT GENERATION FIREWALL

Las mejores prácticas de seguridad determinan que las decisiones que tome con respecto a las políticas, su habilidad para informar la actividad de la red y la capacidad de análisis forense se basan en el contexto. El contexto de la aplicación en uso, la página visitada, las cargas asociadas y el usuario son todos datos específicos valiosos en su esfuerzo por proteger su red. Cuando sabe exactamente qué aplicaciones atraviesan su gateway de Internet, operan dentro de su centro de datos o entorno de la nube, o son usadas por usuarios remotos, se pueden aplicar políticas específicas a esas aplicaciones y completar con protección de amenazas coordinada.

Las soluciones de nueva generación de Palo Alto Networks, permite a las organizaciones abordar un amplio espectro de requisitos de seguridad basados en la premisa de aplicación, usuario y contenido combinada con una postura balanceada de seguridad de redes, inteligencia de amenazas globales y protección de endpoints; permitiendo a las empresas enfocarse en las iniciativas de negocios mientras mejoran significativamente la postura de seguridad y reducen la respuesta ante incidentes.

Lo anterior sumado a nuestro excelente servicio postventa que le asiste en el diseño, planeación, implementación y soporte técnico a nivel local, convierte a Infortec en la mejor alternativa al momento de adquirir una solución para la protección de la información en toda la plataforma tecnológica.

INFORTEC
Especialistas en Ciberseguridad

20 AÑOS

## COMPONENTES DE LA SOLUCION

| DETALLE |
|---|
| • **Threat Prevention:** Miles de aplicaciones de visibilidad y control; capacidad para crear aplicaciones personalizadas y para gestionar el tráfico desconocido en función de políticas u Identificación y control de usuarios: VPN, controladores de WLAN, portal cautivo, proxies, Active Directory, eDirectory, Exchange, servicios de terminal, análisis de syslog y XML API u Inspección y descifrado SSL exhaustivos (entrante y saliente); control SSH por política (entrante y saliente) ü Redes: enrutamiento dinámico, DHCP, DNS, NAT, redistribución de rutas, ECMP, LLDP, BFD e inspección de contenido de túnel y QoS: instancias lógicas de cortafuegos de gestión independiente en un solo cortafuegos físico, con separación del tráfico de cada sistema virtual ü Segmentación de red basada en zonas y protección de estas últimas; protección DoS frente a la saturación de nuevas sesiones.<br>• **Url Filtering:** Prevención automática de ataques basados en la web, incluidos los enlaces de phishing incorporados en mensajes de correo electrónico, los sitios de phishing, los ataques de comando y control basados en HTTP y las páginas portadoras de kits de exploits y Detención de ataques de phishing de credenciales en proceso y Categorías de URL, alertas y páginas de notificación personalizadas.<br>• **WildFired:** Detección de malware de día cero y de exploits con técnicas de análisis complementario por capas y prevención automatizada en la red, los endpoints y la nube en tan solo cinco minutos y Aprovechamiento de los datos procedentes de la comunidad (con más de 50.000 suscriptores) para la protección.<br>• **DNS Security:** Ejecucion de analisis predictivo para interrumpir los ataques que utilizan DNS para comando y control y robo de datos; predice y bloquea nuevos dominios maliciosos con aprendizaje automatico; neutraliza amenazas ocultas en tuneles DNS y aplica automatizacion para encontrar y contener dispositivos infectados, todo sin necesidad de herraminetas independientes.<br>• **Global Protect**: Extensión del perímetro mas allá de la LAN. Global Protect permite llevar las características y políticas de seguridad a los usuarios móviles.<br>• **IoT Security**: Detección y prevención de amenazas y ataques conocidos y desconocidos, dirigidos a los dispositivos IoT, IoMT y OT, con aprendizaje automático y telemetría colaborativa que brindan visibilidad amplia de todos los dispositivos.<br>• **Reportes**: Incluye gran variedad de reportes detallados que permiten ver en tiempo real el trafico, actividades y demas.<br>• **Premium Support**: Soporte directamente con fabrica y garantia de maquina.<br>• **Garantía del hardware hasta 5 años.** |

## PROPUESTA ECONÓMICA DE INVERSION A 2 AÑOS

| DETALLE | V/TOTAL |
|---|---|
| PALO ALTO PA-440 – SEGURIDAD DEL PERIMETRO | $30.000.000 |
| SERVICIOS DE IMPLEMENTACION | $2.690.000 |
| SERVICIOS DE SOPORTE TECNICO – 70 HORAS | $6.720.000 |
| T O T A L | $39.410.000 |
| I V A | $7.487.900 |
| N E T O | $46.897.900 |

| DETALLE |
|---|
| **ALCANCE DE LOS SERVICIOS** |
| Todos nuestros servicios son prestados por personal certificado y con amplia experiencia en el manejo de las soluciones.<br>**Implementación**: Diseño, configuración, implementación, transferencia de conocimiento de 8 horas para máximo 4 personas, entrega del proyecto y garantía de 30 días.<br>**Servicios de Soporte**: Servicios profesionales de soporte técnico bajo demanda en horario 5*11 vía mesa de ayuda, telefónica, e-mail o presencial (si aplica); las horas de servicio tienen vigencia durante el tiempo de licenciamiento adquirido.<br>**Sesiones de Aseguramiento**: Cada 3 meses realizamos un análisis de la consola de gestión, identificamos riesgos y oportunidades de mejora, construimos y socializamos el debido informe con las recomendaciones y reforzamos transferencia de conocimiento de 1 hora.<br>**Formación**: Acceso a la plataforma de formación de Palo Alto para 3 personas y apoyo en procesos de presentación de exámenes de certificación. |

INFORTEC
Especialistas en Ciberseguridad

20 AÑOS

## CONDICIONES COMERCIALES

- Valores en Pesos.
- Tiempo de entrega, 30 días hábiles.
- Vigencia de la propuesta, 30 días.
- Forma de pago, Contado.

## REQUERIMIENTOS TECNICOS Y CONDICIONES DE LOS SERVICIOS

Las soluciones de Palo Alto Networks incluyen actualizaciones (firmas y módulos), nuevas versiones de producto por el tiempo de vigencia de la licencia y soporte técnico en horario 7*24 con el fabricante.

**Implementacion**: Una vez legalizado el contrato, **INFORTEC** coordinará de inmediato los trabajos de implementación (en un plazo no mayor a 30 dias), este proceso se efectuará entre técnicos de **INFORTEC** y la persona idonea que la empresa designe como líder del proyecto, quien en adelante será el encargado de gestionar la plataforma.

**Servicios de Soporte**: Los servicios de soporte técnico posventa serán atendidos desde la ciudad de Pereira con el siguiente escalamiento: telefónicamente, vía e-mail o de manera remota. Las solicitudes de servicio deben ser solicitadas a través de la plataforma Helpdesk o al correo técnico@infortec.co. La atención de casos se atenderá según la siguiente tabla de SLA.

| IMPACTO | TIEMPO DE ATENCION Y SOLUCION | | | | | |
|---|---|---|---|---|---|---|
| | NIVEL 1 - INFORTEC | | NIVEL 2 - MAYORISTA | | NIVEL 3 - FABRICANTE | |
| | Atención | Solución | Atención | Solución | Atención | Solución |
| P1-Critico | 1 Hora | 4 Horas | 1 Hora | 8 Horas | 1 Hora | |
| P2-Alto | 2 Horas | 8 Horas | 2 Horas | 16 Horas | 2 Horas | |
| P4-Medio | 4 Horas | 12 Horas | 4 Horas | 24 Horas | 4 Horas | |
| P5-Bajo | 8 Horas | 16 Horas | 8 Horas | 32 Horas | 8 Horas | |
| IMPACTO | DESCRIPCION | | | | | |
| P1-Critico | Afectación completa del servicio - Perdida total | | | | | |
| P2-Alto | Afectación parcial del servicio - A un grupo de usuarios | | | | | |
| P4-Medio | Degradación del servicio - Sin afectación | | | | | |
| P5-Bajo | Servicios complementarios - Consultas, actualizaciones, mejoras. | | | | | |

## CONSIDERACIONES ADICIONALES DEL SERVICIO

Averías mayores y críticas (ej. daño de maquinas) deben ser abiertas vía telefónica. Los casos serán abiertos por el cliente y atendidos según tabla de SLAs.

Lo anterior solo aplica a problemas reportados que pueden ser totalmente neutralizados en forma remota. Si es necesaria una intervención en sitio para la neutralización de un problema crítico de soporte técnico, este se debe cotizar por concepto de soporte en sitio el cual se cotiza a parte, el tiempo de arribo al sitio debe ser agregado al tiempo de neutralización, con un tiempo máximo de intervención en sitio de NBD para todos los casos.

Exclusiones y neutralización de TMR (tiempos medios de reparación) por fallas que requieran RMAs (cambio de partes), por problemas generados por elementos externos y ajenos a la solución tales como, fallas y fluctuaciones eléctricas, ambientales, manipulación de terceros, ataques de hackers fuera del perímetro, desastres naturales, revueltas y todo lo que sea externo a la solución. Si la falla es determinada por uno de lo casos mencionados y el hardware/software es dañado, el cliente debe responder con la reposición o compra de este.

gms

seguridad de
la información

# PROPUESTA DE SEGURIDAD PERIMETRAL - PALOALTO

**Preparada para:**

**EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO**

**25 febrero de 2022**

Bogotá, 25 febrero de 2022

Ingeniero
**Carlos Camacho**
Director de TI
Ibagué

Apreciado Ingeniero:

GMS agradece la oportunidad de presentarle esta oferta de soluciones informáticas. Somos una empresa de consultoría de TI con más de 30 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.

Atentamente,

Laura Navarro Franco
Gerente de Cuenta
laura.navarro@gmsseguridad.com
Oficina: +601 7433559
Celular: 3209197148
www.gmscolombia.com

# I. Información sobre GMS

## Perfil empresarial

Fundada en 1978, GMS es una de las empresas de consultoría informática de mayor trayectoria en la región. Nuestra misión es potenciar la habilidad empresarial de nuestros clientes hacia la excelencia, a través de tecnología de vanguardia, sistemas y servicios de alta calidad. Medimos nuestros resultados según los que obtienen nuestros clientes, ya que nos consideramos sus socios de negocio para asegurar el mejor retorno sobre las inversiones que realizan con nosotros.

Nuestro principal diferenciador es nuestro personal, a base de los equipos de trabajo que formamos con nuestros clientes. Profesionales altamente capacitados de GMS participan de la mano con sus contrapartes en las empresas que apoyamos para entender a fondo sus requerimientos y definir las soluciones más inteligentes a cada entorno particular. Esta cooperación es la base sobre la cual construimos relaciones a largo plazo que permiten lograr los mejores resultados.

A partir de nuestro personal, hemos formado un portafolio de productos y servicios que nos permite ofrecer soluciones integradas de seguridad informática, telecomunicaciones, administración de infraestructura TI y cloud services. Estas soluciones se complementan con servicios de consultoría en estrategias y normas de TI y seguridad, 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.

## Sistemas de gestión

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

Todos nuestros servicios cuentan con esquemas de escalamiento. Estos aseguran redundancia en canales de comunicación para que los clientes puedan aprovechar del soporte 7x24 ofrecido por GMS. Adicionalmente establecen tiempos de respuesta para distintos tipos de requerimientos, incluyendo los mecanismos de apoyo por parte de fabricantes internacionales, según el caso. La combinación de estos elementos permite a GMS otorgar niveles de atención y apoyo que marcan la diferencia.

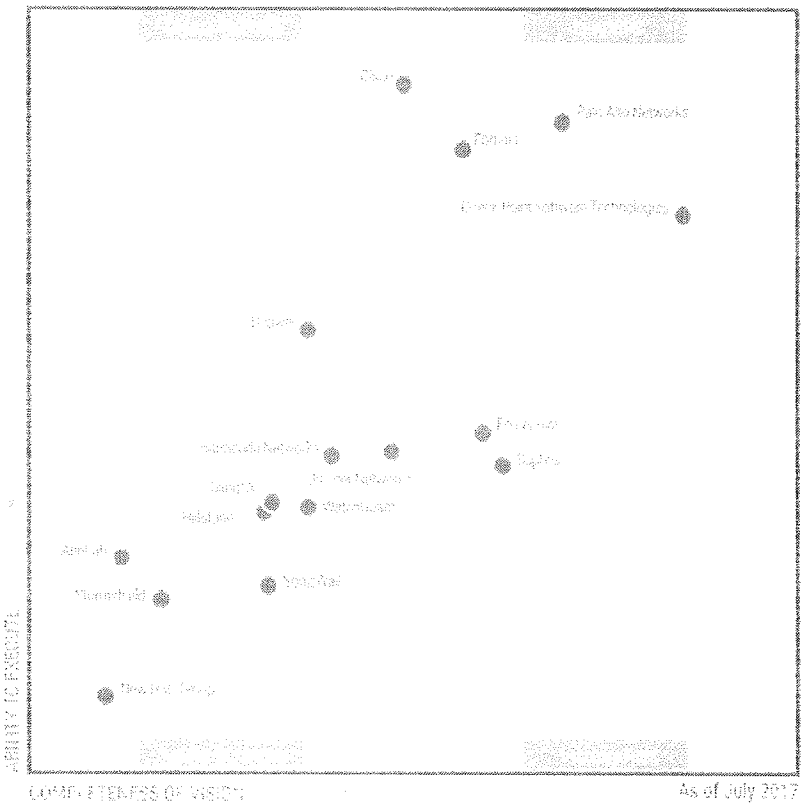
## PALO ALTO

PALOALTO es líder en una nueva etapa en ciberseguridad protegiendo a miles de redes de empresas, gobiernos y proveedores de servicios contra las amenazas cibernéticas. Gracias a nuestra amplia experiencia, nuestro compromiso con la innovación y a una plataforma de seguridad que cambiará las reglas del juego, miles de clientes nos han elegido a PaloAlto como su solución de seguridad y es la empresa de seguridad de más rápido crecimiento del mercado.

La plataforma de seguridad une de forma nativa todas las funciones claves de seguridad de redes, incluyendo la protección contra amenazas avanzadas, firewall, IDS/IPS y filtrado de URL. Debido a que estas funciones se construyen en la plataforma de forma nativa y comparten información importante a lo largo de sus respectivas disciplinas, garantizamos una mejor seguridad que las versiones anteriores de los firewalls, la gestión unificada de amenazas (UTM, por sus siglas en inglés) o productos de detección de puntos de amenaza.

Con la plataforma, las organizaciones pueden permitir de forma segura el uso de todas las aplicaciones, mantener un control y una visibilidad totales, adquirir con confianza iniciativas de nuevas tecnologías, tales como en la nube y en movilidad, y proteger a la organización de ciberataques, tanto conocidos como desconocidos.

Magic Quadrant



- Visibilidad sobre sus aplicaciones, tráfico web, amenazas y patrones de datos.
- Visibilidad basada en usuarios y grupos, no en direcciones IP.
- Vista comparada de patrones de tráfico y amenazas.
- Análisis exhaustivo de todas las actividades relacionadas con su tráfico y dispositivos.
- Elaboración de informes sobre todas las actividades de tráfico y de dispositivos.
- Visibilidad de la actividad del usuario en la aplicación.
- Control de políticas en función del usuario.
- Análisis, generación de informes e investigación en función de los usuarios
- Integración con cualquier repositorio de usuarios.
- Análisis de amenazas desconocidas en un espacio aislado (sandbox).
- Firmas de botnet basadas en DNS.
- Informe de comportamiento de botnets.
- Active una completa protección IPS sin que ello afecte al rendimiento.
- Bloquea una amplia variedad de exploits de vulnerabilidad, tanto conocidos como desconocidos.
- Protección contra ataques de denegación de servicio (DoS) y de denegación distribuida de servicio (DDoS).
- Liderazgo en el mercado en detección e investigación de amenazas.
- Autorizar aplicaciones y bloquear archivos por tipo no aprobados o peligrosos.
- Permitir o denegar el uso de funciones de transferencia de archivos.
- Evite la pérdida de datos con la identificación de contenidos basada en modelos.
- Intégrese en cualquier arquitectura con nuestra arquitectura flexible de conexión a la red.
- Participación en el enrutamiento de tráfico Multicast.
- Equilibrio entre la protección y la habilitación mediante el cumplimiento de una política perfectamente delimitada.
- Filtre de forma selectiva las aplicaciones para crear rápidamente listas de control.
- Detenga las amenazas y las transferencias de archivos/datos no autorizadas.
- La clasificación del tráfico asegura que las aplicaciones de la empresa cuenten con suficiente ancho de banda.
- Control flexible y basado en políticas del uso de la web.
- Identifique y controle de forma sistemática el tráfico desconocido.
- Alta disponibilidad en modos activo/activo o activo/pasivo
- RESISTENCIA integrada y redundancia de los componentes.
- La base de datos de URL integrada maximiza el rendimiento y la flexibilidad.
- Base de datos y categorías de URL personalizables.
- Notificaciones personalizables para el usuario final.
- Control flexible y basado en políticas del uso de la web.

## 1. Propuesta Economica

**ADQUISICION PALO ALTO PA-440 A 2 AÑOS**

| Cantidad | Descripción | Valor Unitario ($COP) | Valor Total ($COP) |
|---|---|---|---|
| 1 | Palo Alto Strata PA-440 | $ 45.500.000 | $ 45.500.000 |
| 1 | Licenciamiento a 2 años de:<br>Threat prevention.<br>Url Filtering.<br>WildFire.<br>DNS Security.<br>IoT Security. | | |
| 1 | Garantía de hardware y soporte directo de fabrica por 2 años en horario 7*24 | | |
| 1 | Bolsa de 50 horas de servicios por año. | | |

| | |
|---|---|
| Total | $ 45.500.000 |
| IVA | $ 8.645.000 |
| **TOTAL IVA INCLUIDO** | **$ 54.145.000** |

## 2. Condiciones Comerciales

1. **Los precios** se encuentran en Pesos Colombianos
2. **Forma de Pago:** a 30 días después de radicación de la factura.

   Factura a nombre de GRUPO MICROSISTEMAS COLOMBIA S.A.S.

   NIT: 900.418.656-1
3. **Validez oferta:** La presente oferta tiene una validez de 30 días calendario.
4. Tiempo de entrega 30 días hábiles.
5. IVA corresponde al 19%

En caso de presentarse alguna inquietud o querer ampliación de la información, no duden en contactarnos.

Las actividades mencionadas en la tabla anterior comprenden, pero no se limitan a las siguientes:

- Instalación de los equipos en el rack.
- Levantamiento de información para la configuración y políticas.
- Configuración de las interfaces.
- Actualización a la última versión estable disponible.
- Creación de zonas de seguridad.
- Creación de salidas a internet.
- Creación de políticas de seguridad
- Creación de hasta 120 políticas de NAT
- Creación de hasta 4 políticas de enrutamiento.
- Migración de hasta 50 VPN cliente-sitio
- Creación de Alta Disponibilidad en activo-pasivo.
- Pruebas de funcionamiento de Alta disponibilidad.
- Pruebas de funcionamiento de controles de seguridad.
- Pruebas de funcionamiento de contingencia.
- Puesta en producción.
- Seguimiento.
- Configuración de la interfaz de conexión con los Firewalls de Nueva generación.
- Pruebas de generación de reportes.
- Pruebas de visualización en tiempo real.
- Entregar dentro la propuesta un plan de trabajo y cronograma aproximado el cual dentro de los cinco (5) días hábiles del inicio del contrato se debe ajustar a las fechas reales.
- Configuración de las funcionalidades del NGFW (Firewall, VPN, filtrado de contenido, antivirus e IPS).
- Configuración del clúster de Firewalls de Nueva Generación y de la plataforma de logs y reportes para el envió de eventos de disponibilidad con la que cuenta GMS.
- Transferencia de conocimiento para la Compañía, orientadas a explicar cómo quedó configurada la plataforma de seguridad y nociones básicas de administración. El proveedor debe indicar la cantidad de horas y el número de empleados
- Uso de las mejores prácticas para la gestión e implementación del proyecto.
- Análisis y gestión de riesgos para el proceso de implementación respecto a servicios críticos de la organización.
- Se incluye la utilización de gestión de cambios para la puesta en producción.
- Documentación de la situación inicial y final de la implementación, la cual incluya la topología de red, las políticas y los perfiles de seguridad configurados.

- **Transferencia de conocimiento (Capacitación):** Durante todo el despliegue se estará llevando a cabo un entrenamiento con la configuración que se esté implementando, y adicionalmente se hará una sesión de 3 días para 2 personas con el propósito de hacer una transferencia de conocimientos orientada a la configuración que se llevó a cabo durante las fases anteriores, esto asegura un nivel de aprendizaje que junto a experiencia de administración es suficiente para presentar la certificación PCNSE.
- **Inicio del ciclo de mejora continua:** Una vez aplicadas las configuraciones dimensionadas en la fase de implementación, se procederá a iniciar el ciclo de mejora continua para garantizar la optimización de la plataforma a través del monitoreo de nuestro centro de atención técnica.

**Bogotá D.C., 25 de febrero 2022**

Señores
**IBAL – IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO**
**Ibagué**

Atendiendo su solicitud, nos permitimos presentarle la propuesta técnica y económica de acuerdo con su requerimiento, estamos seguros representar la mejor alternativa de solución a sus necesidades. Es muy satisfactorio para nosotros encontrarnos entre sus proveedores, a lo cual estamos dispuestos a responder con seriedad, calidad y cumplimiento. Es por eso que contamos en la actualidad con la infraestructura adecuada y un excelente equipo de trabajo tanto interno como externo para ofrecer el mejor respaldo a sus necesidades.

Agradecemos de antemano su confianza en nuestra firma y es de nuestro interés hacer una presentación de esta oferta en donde podamos ampliar sobre las implicaciones y beneficios del alcance de la misma. Por tal razón extendemos desde ya nuestra cordial disposición para resolver cualquier inquietud que se presente durante su evaluación.

Esperamos poder seguir contando con ustedes como nuestros clientes y poder ofrecer nuestra experiencia y apoyo a este y a todos sus proyectos.

Cordialmente,

Mauricio Ospina
Gerente
Móvil: 3158523714
Correo: mauricio@itsec.net

itsec
PALO ALTO

**PALOALTO** es líder en una nueva etapa en ciberseguridad protegiendo a miles de redes de empresas, gobiernos y proveedores de servicios contra las amenazas cibernéticas. Gracias a nuestra amplia experiencia, nuestro compromiso con la innovación y a una plataforma de seguridad que cambiará las reglas del juego, miles de clientes nos han elegido a PaloAlto como su solución de seguridad y es la empresa de seguridad de más rápido crecimiento del mercado.

La plataforma de seguridad une de forma nativa todas las funciones claves de seguridad de redes, incluyendo la protección contra amenazas avanzadas, firewall, IDS/IPS y filtrado de URL. Debido a que estas funciones se construyen en la plataforma de forma nativa y comparten información importante a lo largo de sus respectivas disciplinas, garantizamos una mejor seguridad que las versiones anteriores de los firewalls, la gestión unificada de amenazas (UTM, por sus siglas en inglés) o productos de detección de puntos de amenaza.

## PALO ALTO NEXT GENERATION FIREWALL

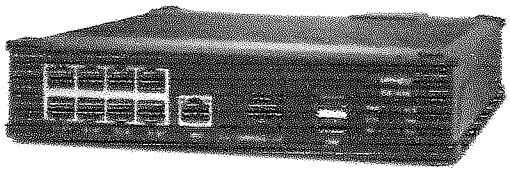
Las mejores prácticas de seguridad determinan que las decisiones que tome con respecto a las políticas, su habilidad para informar la actividad de la red y la capacidad de análisis forense se basan en el contexto. El contexto de la aplicación en uso, la página visitada, las cargas asociadas y el usuario son todos datos específicos valiosos en su esfuerzo por proteger su red. Cuando sabe exactamente qué aplicaciones atraviesan su gateway de Internet, operan dentro de su centro de datos o entorno de la nube, o son usadas por usuarios remotos, se pueden aplicar políticas específicas a esas aplicaciones y completar con protección de amenazas coordinada.

Las soluciones de nueva generación de Palo Alto Networks, permite a las organizaciones abordar un amplio espectro de requisitos de seguridad basados en la premisa de aplicación, usuario y contenido combinada con una postura balanceada de seguridad de redes, inteligencia de amenazas globales y protección de endpoints; permitiendo a las empresas enfocarse en las iniciativas de negocios mientras mejoran significativamente la postura de seguridad y reducen la respuesta ante incidentes.

**ITSEC S.A.S**
**NIT: 900.260.048-2**
· Transversal 72 D No. 82-07
PBX: 57-1- 7510713 / 7504480
Bogotá, Colombia
www.itsecsas.net

itsec

**PROPUESTA ECONÓMICA DE INVERSIÓN**



**PALO ALTO PA 440**

| Cantidad | Descripción | Vlr Unitario | Valor Total |
|---|---|---|---|
| 1 | Palo Alto Networks PA-440 seguridad perimetral. | $50.400.000 | $50.400.000 |
| 1 | Licenciamiento incluido a 2 años: Threat prevention, Url filtering, Wildfire, Global protect, IoT security, DNS security. | | |
| 1 | Garantía de hardware y soporte de fabrica 7*24 a 2 años. | | |
| 1 | Servicios de implementación y 50 horas de soporte técnico Remoto. | | |

| | |
|---|---|
| Sub Total | $50.400.000 |
| IVA | $9.576.000 |
| TOTAL | $59.976.000 |

## Condiciones Comerciales

- Forma de pago: 50% contra pedido, 50% contra entrega.
- Tiempo de entrega de equipos de 120 días calendario.
- Se factura el valor total contenido en esta propuesta.
- Los servicios profesionales que se requieran adicionales a lo contenido en esta oferta se deben cobrar de forma adicional.

**ITSEC S.A.S**
**NIT: 900.260.048-2**
Transversal 72 D No. 82-07
PBX: 57-1- 7510713 / 7504480
Bogotá, Colombia
www.itsecsas.net