PROPUESTA ECONÓMICA

ECONOMIC PROPOSAL

INSTITUTO NACIONAL DE SALUD

Plataforma de Seguridad Palo Alto

bha_cybersecurity

bha - black hat archetype

www.desmantelandoalhacker.net

+57 1 8053207 Bogotà D.C.

+57 4 2315524 Medellìn

ISO 14001: 2015
ISO 9001: 2015
OHSAS 18001: 2007
BUREAU VERITAS Certification

CONTENIDO / CONTENT

¿QUIENES SOMOS? / ABOUT US 2
SERVICIOS DE BHA / BHA SERVICES 4
CONDICIONES GENERALES / TERMS 7
OBJETO / OBJECT 7
DESCRIPCIÓN DE LA SOLUCIÓN / PRODUCTS OR SERVICES 7
DESCRIPCIÓN DEL SOPORTE / SUPPORT DESCRIPTION 11
SISTEMA DE TICKETS / TICKETS SYSTEM 11
MATRIZ DE ESCALAMIENTO / ESCALATION MATRIX 11
UBICACIÓN / LOCATION 13
PROPUESTA ECONÓMICA / ECONOMIC PROPOSAL 14
CONTACTOS / CONTACTS 16

¿QUIENES SOMOS? / ABOUT US

BLACK HAT ARCHETYPE
Desmantelando al Hacker

Somos una compañía con más de 14 años de experiencia en la implementación y el soporte de proyectos de seguridad informática, seguridad de la información, ciberseguridad y ciberdefensa, contamos con un laboratorio de investigación y desarrollo el cual ayuda a soportar los procesos de innovación de la empresa, esto nos ha permitido superar los diferentes retos propuestos por nuestros clientes; gracias a al trabajo y el compromiso de los funcionarios de la empresa contamos con las certificaciones **ISO 14000, ISO 9001, OHSAS 18001** lo que nos permite ofrecer un servicio diferencial y personalizado.

BHA como una empresa comprometida con el ambiente y gracias al departamento de investigación y desarrollo utiliza la **energía solar** para su operación tecnológica y con el apoyo del departamento del Sistema de Gestión estamos en el proceso continuo de conversión a: trabajo con cero emisiones, trabajo social y familiarmente responsable y entrega de **servicios y soluciones innovadoras, limpias, de calidad y seguras**.

COT. 555657

Bogotá, 17 de julio de 2023

Señores
INSTITUTO NACIONAL DE SALUD
Atn: Johanna Barragán
Colombia
La Ciudad
REF: Propuesta Económica: Plataforma de seguridad Palo Alto

A continuación, relacionamos los valores de los servicios o de las soluciones según sea el caso basados en los requerimientos presentados por ustedes, las instalaciones, configuraciones, capacitaciones, mantenimientos y los soportes son realizados por personal certificado en las diferentes soluciones, utilizando procesos normalizados, con ello garantizamos un excelente, eficiente y eficaz desarrollo de actividades, esperamos sean de interés para ustedes.

Atentamente,

Revisada por:

Esperanza Jiménez Espinel
Consultora de Negocios en Seguridad de la Información
(57) 317 853 4200
(571) 805 9229

Realizada por:

Mónica Acevedo
Asistente de Dirección Comercial Seguridad Digital
(571) 805 3207

SERVICIOS DE BHA / BHA SERVICES

Relacionamos brevemente nuestra oferta de servicios a fin que puedan tenerla en consideración para posibles desarrollos futuros.

Analizando las necesidades del mercado sobre la administración de plataformas de seguridad y el control de los eventos de las mismas, pudimos identificar que los servicios actuales no eran altamente competentes para suministrar a nuestros clientes un servicio completo y profesional, de esta forma **BHA** decide crear el **C.A.R (Centro de Acceso Remoto)** el cual fortalece a sistemas como el SOC que consideramos no brindaban una protección completa frente al entorno cibernético actual.



Las características principales del **CAR** son:

- **Prevención:**



- Análisis de amenazas globales.
- Prevención de amenazas globales.
- Blindaje de amenazas superadas.
- Reportes de procesos de seguridad.
- Inteligencia de archivos.

- **Administración:**



- Implementación de políticas o reglas de seguridad de manera controlada.
- Actualizar plataformas, instalar o migrar plataformas.
- Dar soporte inmediato a los operadores ante incidentes de seguridad.
- Contactar de manera directa al usuario final con el fin de obtener evidencias o dar seguimiento a eventos de seguridad.
- Generar reportes ejecutivos o técnicos ante incidentes de seguridad.
- Centralizar los eventos de seguridad en un punto de contacto y dar seguimiento de los mismos.

- **Respaldo y Acompañamiento en Procesos de Seguridad:**



- Diseño de las estrategias de seguridad.
- Diseño de las arquitecturas de seguridad.
- Generación de políticas de seguridad.
- Grupo de seguridad para las reuniones interdisciplinarias.

- **Monitoreo:**



- Monitoreo de amenazas avanzadas.
- Monitoreo de marca.
- Monitoreo y correlación de eventos (SIEM).
- Monitoreo y auditoría de bases de datos.
- Monitoreo de integridad de archivos -Sandboxing –
- Reportes de procesos de seguridad.

- **Mesa de ayuda:**



- Central telefónica 24/7.
- Atención personalizada frente a eventos de seguridad.
- Personal capacitado en seguridad.
- Respaldo de productos directamente con fábrica.
- Portal de seguimiento de casos

Servicios Especializados

Las pruebas de seguridad ayudan a detectar debilidades de seguridad que puedan tener los productos a los cuales tiene acceso el público o que manejan información sensible de la compañía.

Las pruebas de seguridad se dividen en:

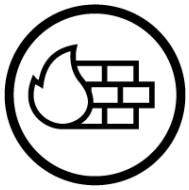
- **Diagnóstico de Seguridad:** Con este diagnóstico, se hace una exploración en el sistema y se identifican las diferentes vulnerabilidades que este puede llegar a tener, una vez el estudio concluye brindamos las herramientas más efectivas del mercado para ponerle fin a las deficiencias de seguridad.



- **Prueba de Penetración de Seguridad:** Esta prueba pretende verificar que tan difícil es acceder a los servidores de la compañía, a través de un ataque directo a la infraestructura del servidor o la red desde un punto externo o interno que intentará realizar cambios, denegaciones o extracciones de información.



- **Ponderación de Seguridad:** La ponderación permite saber si las medidas de control implementadas en la RED (Firewall, WAF, ADS, Antivirus, etc.) están actuando de forma coordinada y correcta frente a posibles amenazas externas, de esta forma podemos saber cuantitativamente el nivel de seguridad de la infraestructura.



CONDICIONES GENERALES / TERMS

OBJETO / OBJECT

Presentar pre-cotización de plataformas Palo Alto con el fin de mejorar los procesos diseñados para proteger los sistemas informáticos, software, redes, aplicaciones y usuarios fortaleciendo el modelo de ciberseguridad de la Información de la entidad, el cual implica un manejo estructurado y sistemático que utilice métodos adecuados para la revisión y control de los sistemas garantizando la confidencialidad, disponibilidad e integridad de la Información en la entidad.

DESCRIPCIÓN DE LA SOLUCIÓN / PRODUCTS OR SERVICES

El firewall de nueva generación protege con una arquitectura enfocada en la prevención e innovaciones integradas que son fáciles de implementar y utilizar. En la arquitectura de Palo Alto (figura 1), se puede observar el tráfico de la red, donde permite políticas con detalles granulares para la configuración requerida por la entidad.

El firewall detecta amenazas conocidas y desconocidas, incluso en el tráfico cifrado, mediante la inteligencia generada a través de miles de implementaciones de los clientes. Esto significa que reducen los riesgos y previenen una gran cantidad de ataques. Por ejemplo, permiten que los usuarios accedan a datos y aplicaciones en función de los requerimientos comerciales como también impiden el robo de credenciales y la capacidad del atacante de utilizar credenciales robadas.

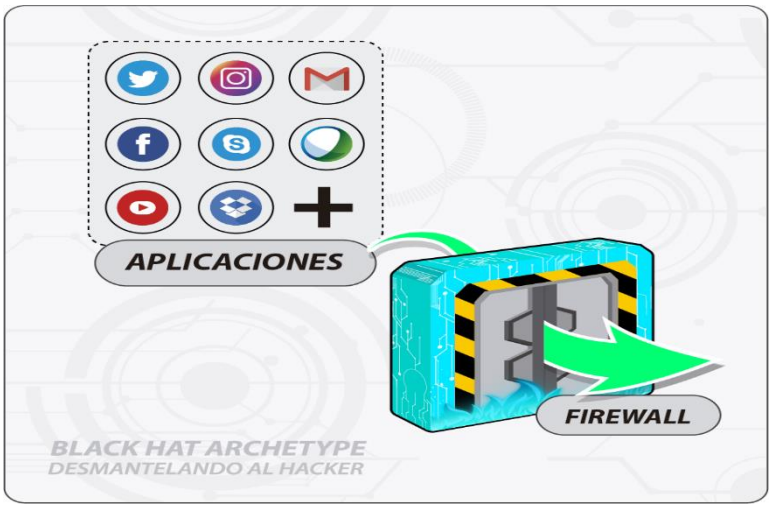


Figura 1. Arquitectura Palo Alto.

Con el firewall se logran crear reglas de seguridad rápidamente que repliquen su política de negocios: son fáciles de mantener y adaptar a su entorno dinámico. Reducen los tiempos de respuesta con medidas automatizadas basadas en políticas, y le permiten automatizar los flujos de trabajo a través de la integración con herramientas administrativas como servicios de registros.

En la figura 1, vemos la conexión del firewall como una barrera con filtrado a la red interna y el internet. Con esto se permite monitorear el tráfico de red entrante y saliente, también decidir si permite o bloquea el tráfico específico en función de un conjunto definido de reglas de seguridad. El firewall establece una barrera entre las redes internas protegidas y controladas en las que se puede confiar y redes externas que no son de confianza, como Internet.

La arquitectura de Palo Alto (figura 2) está basada en un procesamiento paralelo donde se manejan 3 factores principales:

- App-id (identificación de aplicación).
- Content-id (escanear el contenido).
- User-id (identificación de usuario).

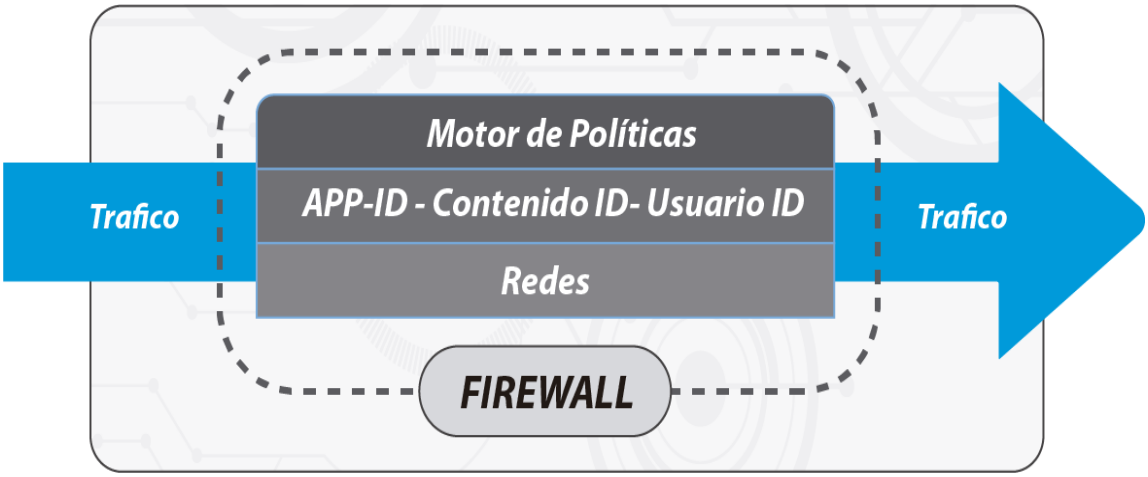


Figura 2. Arquitectura Palo Alto.

Las características principales de Palo Alto son:

- Identificar y controlar las aplicaciones en cualquier puerto.
- Identificar y controlar la evasión.
- Descifrar el tráfico SSL saliente y controlar el SSH.
- Proporcionar control funcional de las aplicaciones.
- Administrar sistemáticamente el tráfico desconocido.
- Explorar en busca de virus y malware todas las aplicaciones y todos los puertos.
- Permitir la misma visibilidad de aplicaciones y el mismo control para todos los usuarios y dispositivos.
- Simplificar la seguridad de redes en lugar de hacerla más compleja, añadiendo el control de aplicaciones.
- Ofrecer la misma capacidad y rendimiento con un control total de aplicaciones.
- Soportar las mismas funciones de firewall, tanto en formato hardware como virtual.

PALO ALTO VM-SERIES

Protege aplicaciones y datos implementados a través de una amplia variedad de entornos de nube pública, de virtualización y NFV (Network Functions Virtualization).

Es compatible con un amplio rango de entornos de nube y virtualización, incluso VMware NSX, ESXi, vCloud Air, Citrix Netscaler SDX, Microsoft Azure e Hyper-V, Amazon Web Services, Google Cloud y KVM, con soporte opcional para el complemento OpenStack.

Sus principales características son:

- Identificar y controlar las aplicaciones en sus entornos de nube o virtualizados, limitando el acceso basado en usuarios y prevenir amenazas conocidas y desconocidas.
- Segmentar aplicaciones y datos críticos según los principios de Zero Trust para mejorar su postura de seguridad y lograr el cumplimiento.
- Gestionar las políticas de manera centralizada a través de firewalls tanto físicos como virtualizados para garantizar una postura de seguridad consistente.
- Agilizar la automatización de los flujos de trabajo para garantizar que la seguridad mantenga el ritmo de la tasa de cambio en su nube.

DESCRIPCIÓN DEL SOPORTE / SUPPORT DESCRIPTION

SISTEMA DE TICKETS / TICKETS SYSTEM

El sistema de gestión de ticket hace parte de nuestro sistema de respuesta para nuestros clientes, funciona directamente desde nuestro sitio web www.bhamesadeayuda.net, ingresando en esta página nuestros clientes podrán encontrar diferentes medios para solucionar las dudas que tengan sobre las soluciones adquiridas.

MATRIZ DE ESCALAMIENTO / ESCALATION MATRIX

Matriz de Escalamiento Técnico / Technical Escalation Matrix					
Nivel/ Level	**Tipo de contacto/ Type of contact**	**Contacto/ Contact**	**Responsable/ Responsible**	**Horario/ Schedule**	**Predecesora/ Predecessor**
I	Soporte vía correo electronico/ Email support	mesadeayuda@bhamesadeayuda.net	Mesa de Ayuda/ Help Desk	7 x 24	**N/A**
	Soporte vía Skype/ Skype support	bhamesadeayuda	Mesa de Ayuda/ Help Desk	7 x 24	
	Soporte vía Web Ticket/ Web Ticket Support	http://bhamesadeayuda.net/mantis/login_page.php	Mesa de Ayuda/ Help Desk	7 x 24	
	Soporte Telefónico Local/ Local Phone Support	805 41 98	Mesa de Ayuda/ Help Desk	7 x 24	
	Soporte Telefónico Nacional/ National Phone Support	018000 180129	Mesa de Ayuda/ Help Desk	7 x 24	
II	Soporte Técnico especializado/ Specialized Technical Support	805 41 98	Mesa de Ayuda/ Help Desk	7 x 24	**I**

En la siguiente imagen **(figura 1)** podemos observar el flujograma cuando se registra un requerimiento o un incidente en la mesa de ayuda.

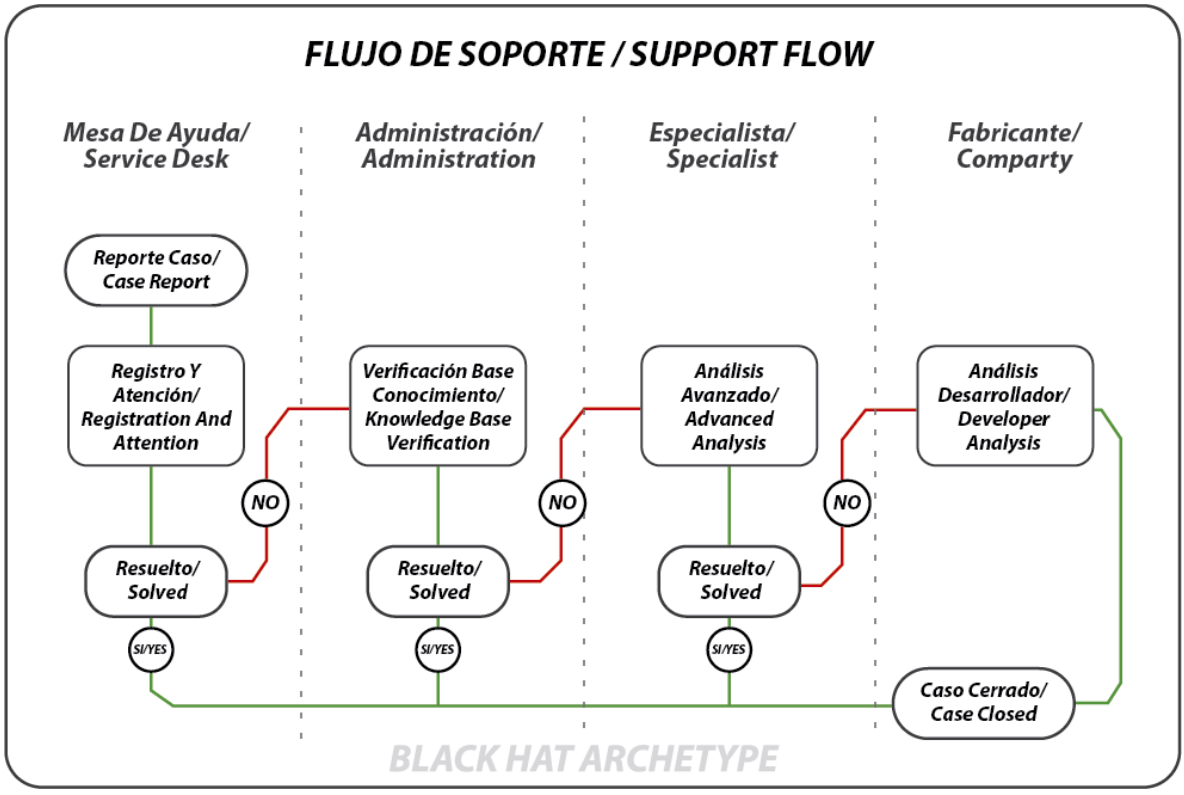
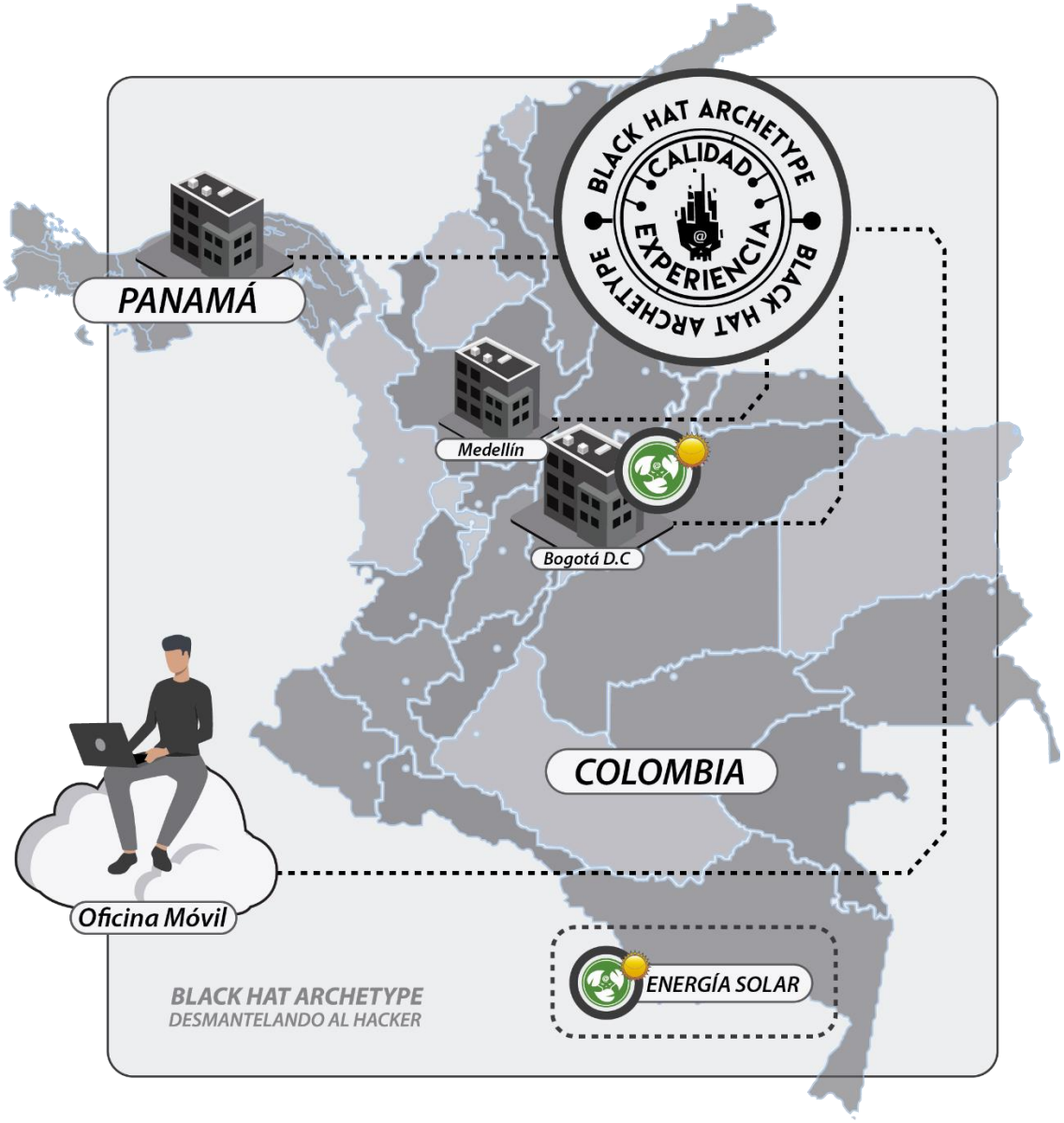


Fig 1. Diagrama de Flujo Mesa de Ayuda.

UBICACIÓN / LOCATION

Los servicios se prestarán en la ciudad de Bogotá en las ventanas abiertas por el cliente, los servicios podrán ser según la necesidad prestados en sitio en las instalaciones del cliente o de maneta remota.

Los servicios prestados fuera de la ciudad de Bogotá tendrán valores adicionales.



PROPUESTA ECONÓMICA / ECONOMIC PROPOSAL

Fabricante de la Solución o Servicio: Palo Alto.

Duración o Tiempo del Soporte o del Licenciamiento: 12 meses

Cant.	Descripción	Valor Unitario	Valor Total
	PLATAFORMA PALO ALTO NUEVO		
	OPCION 3		
2	Equipo Palo Alto FIREWAL 1410	$ 70.588.235	**$141.176.471**
	• Threat Prevention		
	• URL Filtering		
	• Soporte		
1	Solución Seguridad en la Nube	$70.588.235	**$70.588.235**
	• Threat Prevention		
	• URL Filtering		
	• Global Protect		
	• Wildfire		
	• Soporte		
	SERVICIOS (1 año)		
1	Soporte 7*24x365 con:	$23.529.412	**$23.529.412**
	• Recomendaciones y mejores		
	prácticas		
	• Soporte mediante CHAT y FORO		
	• Llamadas y correos electrónicos		
	• Afinamiento de plataformas		
		SUBTOTAL	**$235.294.118**
		IVA	**$44.705.882**
		TOTAL	**$280.000.000**

Precios en Pesos Colombianos

NOTA:

1. Los precios presentados en los cuadros de costos se entienden en pesos colombianos
2. Los precios anteriormente relacionados incluyen impuestos.
3. De manera general se considera un solo pago.
4. De manera general se consideran pagos a 30 días.

Fabricante de la Solución o Servicio: Palo Alto.

Duración o Tiempo del Soporte o del Licenciamiento: 36 meses

Cant.	Descripción	Valor Unitario	Valor Total
	PLATAFORMA PALO ALTO NUEVO 3 AÑOS		
	OPCION 4		
2	Equipo Palo Alto FIREWAL 1410	$ 196.638.656	**$393.277.311**
	• Threat Prevention		
	• URL Filtering		
	• Soporte		
1	Solución Seguridad en la Nube	$ 196.638.656	**$196.638.656**
	• Threat Prevention		
	• URL Filtering		
	• Global Protect		
	• Wildfire		
	• Soporte		
	SERVICIOS (3 años)		
1	Soporte 7*24x365 con:	$65.546.219	**$65.546.219**
	• Recomendaciones y mejores		
	prácticas		
	• Soporte mediante CHAT y FORO		
	• Llamadas y correos electrónicos		
	• Afinamiento de plataformas		
		SUBTOTAL	**$655.462.186**
		IVA	**$124.537.814**
		TOTAL	**$780.000.000**

Precios en Pesos Colombianos

NOTA:

5. **Los precios presentados en los cuadros de costos se entienden en pesos colombianos**
6. **Los precios anteriormente relacionados incluyen impuestos.**
7. **De manera general se considera un solo pago.**
8. **De manera general se consideran pagos a 30 días.**

CONTACTOS / CONTACTS

Área Comercial / Business Area

Esperanza Jimenez Espinel.
Teléfono: 8059229.
Móvil: 317 853 42 00.

Área Administrativa / Administrative Area

Mónica Acevedo.
Teléfono: 8053207.
Móvil 318 600 59 18.
Dirección: Calle 37 # 28-38.
Nit: 900.034.395-5.

Área de Ingeniería / Support Area

David González.
Teléfono: 8054198.
Móvil 317 366 44 53.

BLACK HAT ARCHETYPE

Desmantelando al Hacker

PRESENTA

C.A.R

CENTRO DE ACCESO REMOTO

Analizando las necesidades del mercado sobre la administración de plataformas de seguridad y el control de los eventos de las mismas, pudimos identificar que los servicios actuales no eran altamente competentes para suministrar a nuestros clientes un servicio completo y profesional, de esta forma BHA decide crear el C.A.R (Centro de Acceso Remoto) el cual fortalece a sistemas como el SOC que consideramos no brindaban una protección completa frente al entorno cibernético actual.



EL ENEMIGO NUNCA DUERME Y NOSOTROS TAMPOCO



SERVICIO 24/7
CIBERSEGURIDAD

www.desmantelandoalhacker.net