BLACK HAT ARCHETYPE®
Desmantelando al Hacker

PROPUESTA ECONÓMICA

ECONOMIC PROPOSAL

N.º 333527

CREG

AEGURIDAD DIGITAL

bha news
bha_cybersecurity
black-hat-archetype
bha - black hat archetype

V2024

¿QUIENES SOMOS? / ABOUT US

BLACK HAT ARCHETYPE
Desmantelando al Hacker

Somos una compañía con más de 17 años de experiencia en la implementación y el soporte de proyectos de seguridad informática, seguridad de la información, ciberseguridad y Seguridad Digital, 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 al trabajo y el compromiso de los funcionarios de la empresa contamos con las certificaciones **ISO 27001, ISO 14001, ISO 9001, ISO 45001** 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**.

ISO 9001:2015 BUREAU VERITAS Certification
ISO 14001:2015 BUREAU VERITAS Certification
ISO 27001:2013 BUREAU VERITAS Certification
ISO 45001:2018 BUREAU VERITAS Certification

COT. 333527

Bogotá, 29 de agosto de 2024
Señores
COMISION DE REGULACIÓN DE ENERGÍA Y GAS (CREG)
Atn: Luz Mary Vásquez
Teléfono: 601 5426241
Dirección: Ac 116 #7-15
NIT: 900-034-993-1

REF: Propuesta Económica

Recomendaciones y condiciones:

A continuación, relacionamos la propuesta económica referente a los servicios o soluciones según 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,

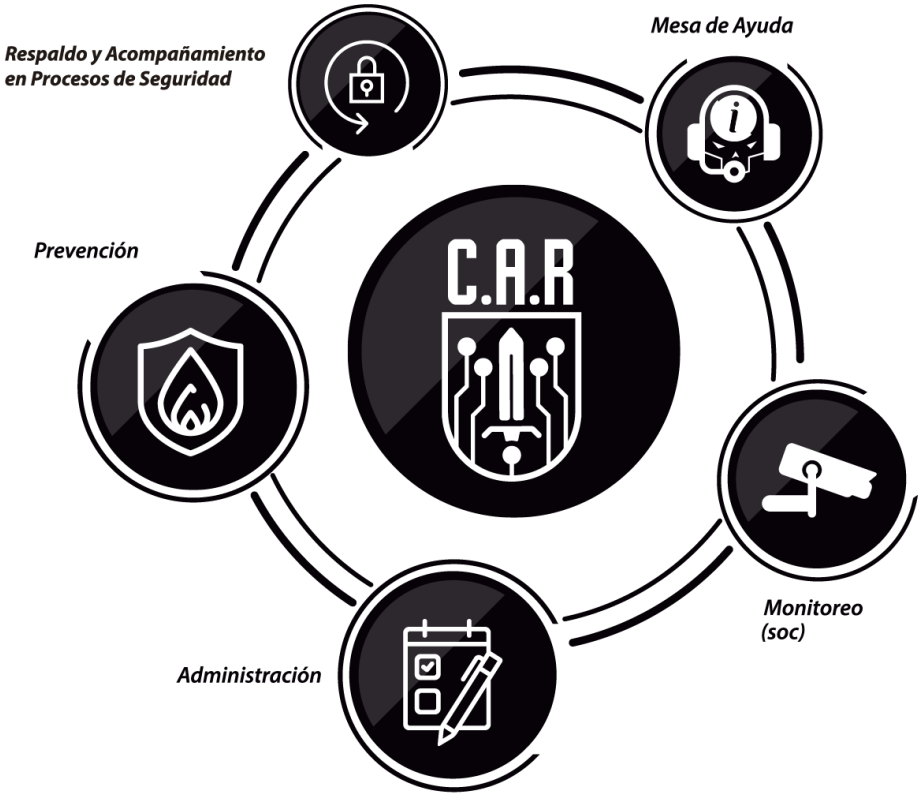
Revisada por:
Esperanza Jiménez Espinel
Consultora de Negocios en Seguridad de la Información
(57) 317 853 4200

Realizada por:
Alejandra Rojas
Asistente de Dirección Comercial Seguridad Digital
(571) 805 3207

1. 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.



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 caso

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:

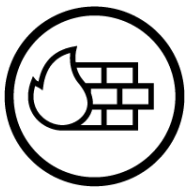
- **Diagnóstico de Seguridad:** Con este diagnóstico, se hace una exploración en el sistema y se identifican las diferentes vulnerabilidades que este puede llegar a tener, una vez el estudio concluye brindamos las herramientas más efectivas del mercado para ponerle fin a las deficiencias de seguridad.



- **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.



3. OBJETIVO / GOAL

Presentar propuesta de cotización de una plataforma Cibersegura para la entidad Comisión de Regulación de Energía y Gas (CREG)

4. DESCRIPCIÓN DE LA SOLUCIÓN / PRODUCTS OR SERVICES

TREND MICRO VISION ONE (VO)

Trend Vision One solución de operaciones de seguridad de la nube, que funciona en entornos locales, híbridos y en la nube combinando ASM y XDR en una sola consola para administrar de manera efectiva el riesgo cibernético en toda su organización.

XDR especialmente diseñado, gestión de riesgos de superficie de ataque y capacidades de Zero-Trust

Capacite a su equipo en cada etapa del ciclo de vida de los riesgos y amenazas con aplicaciones intuitivas para detectar, cazar, investigar, analizar y responder, y sacar a la superficie automáticamente los riesgos y vulnerabilidades priorizados. facilitando las operaciones de seguridad al tiempo que proporciona la información adecuada para desarrollar planes que reduzcan el riesgo y mejoren los indicadores clave de rendimiento, como el tiempo medio de detección, el tiempo de respuesta y el tiempo de respuesta.

Sus principales características son:

Una única fuente de verdad para gestionar el riesgo integrado para la detección y respuesta de amenazas y la gestión de riesgos le permite a su equipo de seguridad evaluar y priorizar continuamente el riesgo cibernético en toda su organización.

Elevar la seguridad como un pilar crítico de las operaciones comerciales Trend Vision One facilita la respuesta a las preguntas frecuentes de las principales partes interesadas (CEO, COO, CFO, CIO), la junta directiva y las aseguradoras cibernéticas.

Una solución que se adapta a su entorno

Trend Vision One se adapta a cualquier entorno con tableros personalizados basados en roles optimizando las funciones y responsabilidades de seguridad única, sus políticas personalizadas con información basada en XDR permiten optimizar continuamente las defensas, crear y modificar el agente, controlar la configuración del modo de detección de amenazas y vulnerabilidades y aprovisionar el agente.

Guía inteligente Resuelva rápidamente el riesgo en su entorno con recomendaciones de mitigación inteligentes y personalizadas para equilibrar dinámicamente la complejidad, el esfuerzo de los analistas y la criticidad de los activos.
Amplio ecosistema de integración Trend Vision One encaja dentro de estos ecosistemas y flujos de trabajo de operaciones de seguridad, adquiriendo datos significativos de su infraestructura para enriquecer y validar aún más sus capacidades XDR.

- **Integraciones nativas:** Integre con la amplia cartera de protección de ciberseguridad de Trend para sus entornos en la nube, híbridos y locales.
- **Integraciones de terceros:** Intégrelo sin esfuerzo con dispositivos especialmente diseñados conexiones a servicios en la nube, administración de superficie de ataque externa, firewall y protección de red, administración de servicios de TI, administración de identidad y acceso, SIEM, SOAR, inteligencia de amenazas, comunicación de tickets, Microsoft 365, Microsoft Azure Active Directory, Active Directory y tecnologías de administración unificada de puntos finales.
- **Automatización de API:** aproveche las plantillas de libros de recetas de API y el código de muestra para ejecutar scripts personalizados basados en Python y automatizar procedimientos regulares en su SOC.

Automatice y organice la remediación y los flujos de trabajo
Automatice y organice la respuesta a través de sus múltiples puntos finales o tipos de sensores utilizando guías de seguridad personalizadas y con plantillas.
Análisis de Sandbox Valide investigaciones, analice objetos sospechosos y mantenga las amenazas potenciales aisladas del resto de la empresa con análisis de espacio aislado.

Inteligencia global líder en amenazas y creación de perfiles de actores de amenazas
Advertencia temprana: Trend Micro XDR bloquea el origen de una amenaza, obtenga visibilidad
integral del ciclo de vida completo de su campaña de ataque para comprender dónde comienza un ataque y responder antes de que ocurra una infracción.
Visibilidad completa de la infracción: La inteligencia de amenazas global captura tanto los componentes de amenazas individuales como los datos de APT para detallar cómo las detecciones de malware y las vulnerabilidades individuales contribuyen a una infracción antes, durante y después de que ocurra un ataque.

Información de campaña de ataque profundo: Consulte las tácticas, técnicas y procedimientos de MITRE ATT&CK asociados con campañas de ataque específicas y actividades de ataque individuales.

DESCUBRA, EVALÚE, PRIORICE Y MITIGUE EL RIESGO CON LA GESTIÓN DE SUPERFICIE DE ATAQUE LÍDER EN EL MERCADO

SENHA SEGURA PAM SECURITY PLATFORM

Senha segura permite a las empresas implementar los controles más estrictos y complejos sobre el acceso a credenciales privilegiadas de manera automatizada y centralizada, protegiendo la infraestructura de TI de violaciones de datos y posibles violaciones de cumplimiento.

Características:

Escanear y descubrir Los conectores abiertos ofrecen las mejores capacidades de descubrimiento de su clase de credenciales y secretos privilegiados que brindan una visibilidad completa del acceso privilegiado para una máxima gobernanza.
Grabación de sesiones Los videos de las sesiones se pueden grabar en un formato de video de alta compresión, sin necesidad de agentes locales.
Rotación automática de credenciales Senha segura ofrece complementos integrados y plantillas listas para usar para la rotación automática de credenciales en dispositivos, servicios, archivos de configuración y aplicaciones a través de criterios configurables.
Flujo de trabajo de aprobación Los flujos de trabajo granulares de aprobación multinivel que ofrece senha segura permiten reducir los costos de implementación y mejorar el cumplimiento de las políticas de acceso
Comandos auditados Es posible crear políticas con puntos atribuidos a cada comando realizado. Cuando se alcanza un riesgo alto, se activan alertas para los administradores y se marcan en paneles gráficos.
App to app La gestión de contraseñas de aplicación a aplicación proporciona acciones locales en la aplicación y los scripts de implementación, como la inserción de secretos desde la solución PAM y la inyección en archivos de configuración o en variables de entorno.
KDI (identidad dinámica de pulsaciones de teclas) A través de funciones basadas en IA, es posible analizar los patrones de pulsación de teclas de los usuarios y detectar posibles actividades maliciosas utilizando credenciales robadas.
Con senha segura PAM SECURITY permite que tu empresa tenga visibilidad, sin costos adicionales, con un despliegue rápido, con entorno amigable, la gestión de dispositivos y credenciales logrando un reconocimiento de clientes.

FIREMON

¿Es difícil mantener una postura sólida de seguridad y cumplimiento para su red?
¿Requiere obtener visibilidad y control sobre su compleja infraestructura de red híbrida?
¿Es complejo administrar múltiples dispositivos y gestionar sus políticas?
¿Tiene complejas configuraciones de red e infraestructura a administrar y requiere mejor la seguridad de la red y el cumplimiento normativo?
¿Gasta mucho tiempo en la creación de reglas y gestión de firewalls?
¿Requiere validar políticas de sus firewalls y optimizar las operaciones automatizando los flujos de trabajo?

Las redes nunca han sido más complejas, las amenazas evolucionan constantemente y la próxima auditoría siempre está a la vuelta de la esquina. ¿Tiene las herramientas que necesita para enfrentar estos desafíos?
FireMon permite administrar y controlar de manera centralizada los firewalls que funcionan en su red aunque provengan de distintos proveedores. Proporciona visibilidad, control y administración en tiempo real para dispositivos de seguridad de red en entornos de nube híbrida desde un solo panel.





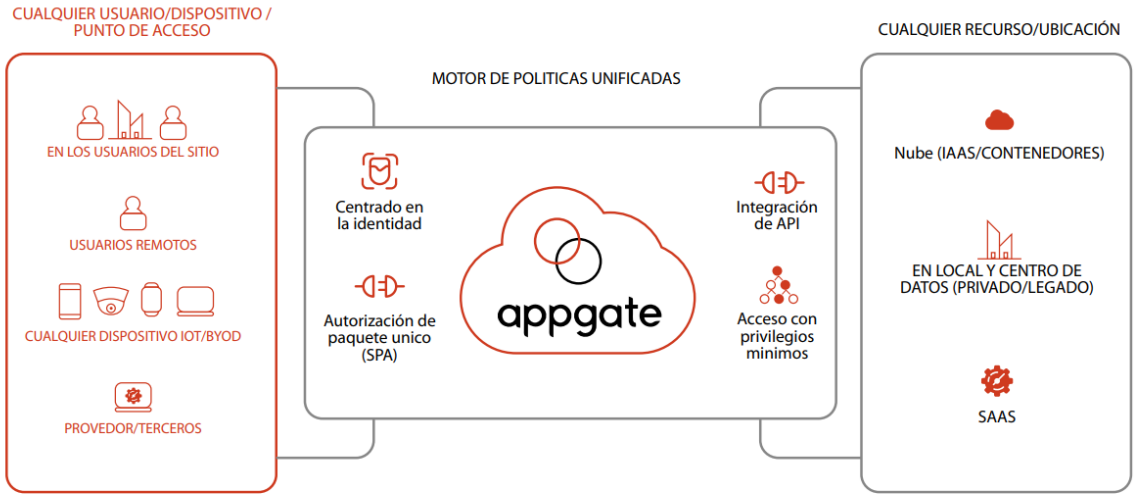
APPGATE

¿Quieres reducir el riesgo cibernético? ¿Te gustaría poder conectarte desde cualquier lugar y cualquier dispositivo a cualquier cosa, en cualquier momento? ¿Sabes cómo mejorar la experiencia de usuario? ¿Te gustaría que tu red fuera invisible?

Appgate SDP:
Capacite a su gente para conectarse con confianza desde cualquier lugar y cualquier dispositivo a cualquier cosa, en cualquier momento con acceso a la red Zero Trust (ZTNA) rápido y seguro. Reduzca el riesgo cibernético y la complejidad liberando el poder de Appgate SDP, la solución Zero Trust Network Access más completa de la industria.

- Reduzca su superficie de ataque
- Simplifique la administración
- Acelere la confianza cero
- Mejorar la experiencia del usuario
- Avanzar en la velocidad de los negocios

Arquitectura Zero Trust segura y flexible: Al ofrecer una automatización robusta y diversas opciones de implementación, la arquitectura Zero Trust de Appgate SDP fortalece su postura de seguridad al tiempo que alivia la carga de los equipos de TI ocupados.

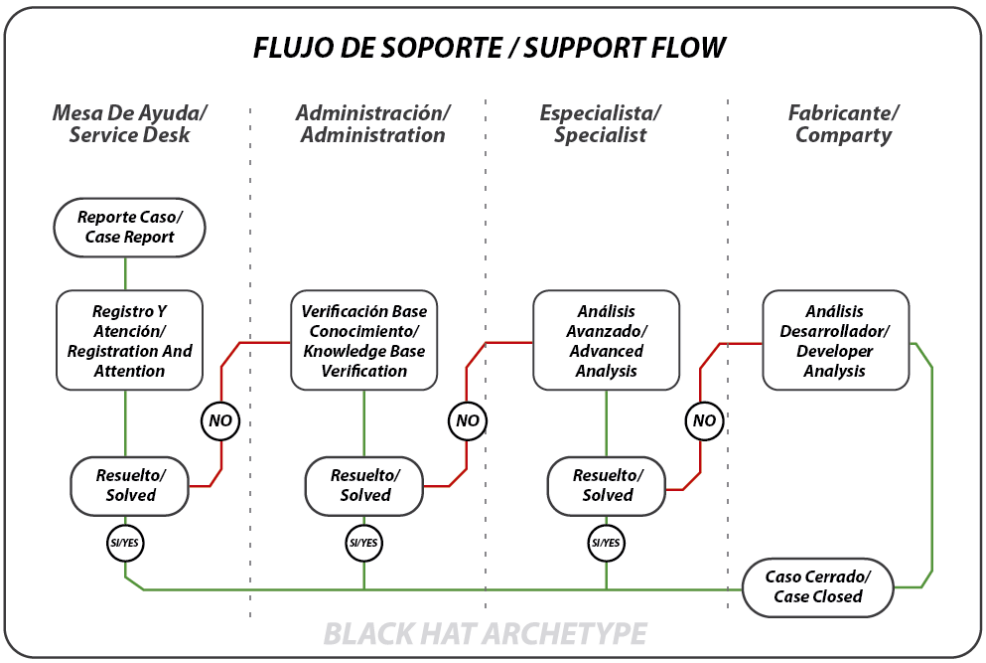


5. DESCRIPCIÓN DEL SOPORTE / SUPPORT DESCRIPTION

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.

Diagrama de Flujo Mesa de Ayuda.



6. 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	carmarte@bhamesadeayuda.net carjupiter@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/	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**

7. PROPUESTA ECONÓMICA / ECONOMIC PROPOSAL

Fabricante de la Solución o Servicio: Trend Micro
Duración o Tiempo del Soporte o del Licenciamiento: 1 Año

Cant.	Descripción	Valor Unitario	Valor Total
	PLATAFORMA TREND MICRO		
	RENOVACIÓN 1 AÑO		
121	Licencias Smart Protection for Endpoint	$ 220.774	**$ 26.713.697**
		SUBTOTAL	**$ 26.713.697**
		IVA	**$ 5.075.602**
		TOTAL	**$ 31.789.299**
	PLATAFORMA TREND MICRO NUEVO		
	1 AÑO		
121	Seguridad punto final XDR	$ 83.000	**$ 10.043.000**
121	Seguridad punto final superficie de riesgo	$ 85.000	**$ 10.285.000**
	SERVICIOS		
1	Instalación Y Soporte 7*24	$ 13.000.000	**$ 13.000.000**
		SUBTOTAL	**$ 33.328.000**
		IVA	**$ 6.332.320**
		TOTAL	**$ 39.660.320**

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.

7. PROPUESTA ECONÓMICA / ECONOMIC PROPOSAL

Fabricante de la Solución o Servicio: Trend Micro
Duración o Tiempo del Soporte o del Licenciamiento: 1 Año

Cant.	Descripción	Valor Unitario	Valor Total
	PLATAFORMA TREND MICRO NUEVO		
	1 AÑO		
121	Seguridad de correo electrónico	$ 70.550	**$ 8.536.550**
121	Complemento XDR Add-on: Email	$ 16.600	**$ 2.008.600**
	SERVICIOS		
1	Instalación Y Soporte 7*24	$ 3.500.000	**$ 3.500.000**
		SUBTOTAL	**$ 14.045.150**
		IVA	**$ 2.668.579**
		TOTAL	**$ 16.713.729**

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.

PROPUESTA ECONÓMICA / ECONOMIC PROPOSAL

Fabricante de la Solución o Servicio: Senhasegura
Duración o Tiempo del Soporte o del Licenciamiento: 1 Año

Cant.	Descripción	Valor Unitario	Valor Total
	PLATAFORMA SENHA SEGURA NUEVO		
	1 AÑO		
10	Proyecto plataforma de acceso privilegiado	$ 2.481.700	**$ 24.817.000**
	PAM		
1	Consola en la nube		
	SERVICIOS		
1	Instalación Soporte 7*24 y Capacitación	$ 19.000.000	**$ 19.000.000**
		SUBTOTAL	**$ 43.817.000**
		IVA	**$ 8.325.230**
		TOTAL	**$ 52.142.230**

NOTA:

9. Los precios presentados en los cuadros de costos se entienden en pesos colombianos.
10. Los precios anteriormente relacionados incluyen impuestos.
11. De manera general se considera un solo pago.
12. De manera general se consideran pagos a 30 días.

PROPUESTA ECONÓMICA / ECONOMIC PROPOSAL

Fabricante de la Solución o Servicio: FIREMON
Duración o Tiempo del Soporte o del Licenciamiento: 1 Año

Cant.	Descripción	Valor Unitario	Valor Total
	PLATAFORMA FIREMON NUEVO 1 AÑO		
3	Proyecto Orquestador con licenciamiento	$21.202.350	**$ 63.607.050**
	para Firemon y Switches.		
1	Ruta para explotación de vulnerabilidades		
1	Cumplimiento estándares		
	SERVICIOS		
1	Instalación Soporte 7*24 y Capacitación	$ 16.000.000	**$ 16.000.000**
		SUBTOTAL	**$ 79.607.050**
		IVA	**$ 15.125.340**
		TOTAL	**$ 94.732.390**

NOTA:

13. Los precios presentados en los cuadros de costos se entienden en pesos colombianos.
14. Los precios anteriormente relacionados incluyen impuestos.
15. De manera general se considera un solo pago.
16. De manera general se consideran pagos a 30 días.

PROPUESTA ECONÓMICA / ECONOMIC PROPOSAL

Fabricante de la Solución o Servicio: CROWDSTRIKE
Duración o Tiempo del Soporte o del Licenciamiento: 1 Año

Cant.	Descripción	Valor Unitario	Valor Total
	PLATAFORMA CROWDSTRIKE NUEVO		
	1 AÑO		
121	Proyecto protección punto final XDR	$ 488.911	**$ 59.158.250**
	SERVICIOS		
1	Instalación Soporte 7*24 y Capacitación	$ 5.000.000	**$ 5.000.000**
		SUBTOTAL	**$ 64.158.250**
		IVA	**$ 12.190.068**
		TOTAL	**$ 76.348.318**

NOTA:

17. Los precios presentados en los cuadros de costos se entienden en pesos colombianos.
18. Los precios anteriormente relacionados incluyen impuestos.
19. De manera general se considera un solo pago.
20. De manera general se consideran pagos a 30 días.

PROPUESTA ECONÓMICA / ECONOMIC PROPOSAL

Fabricante de la Solución o Servicio: APPGATE
Duración o Tiempo del Soporte o del Licenciamiento: 1 Año

Cant.	Descripción	Valor Unitario	Valor Total
	PLATAFORMA APPGATE NUEVO		
	1 AÑO		
100	Proyecto plataforma de ZTNA	$ 518.750	**$ 51.875.000**
	SERVICIOS		
1	Instalación Soporte 7*24 y Capacitación	$ 15.000.000	**$ 15.000.000**
		SUBTOTAL	**$ 66.875.000**
		IVA	**$ 12.706.250**
		TOTAL	**$ 79.581.250**

NOTA:

21. Los precios presentados en los cuadros de costos se entienden en pesos colombianos.
22. Los precios anteriormente relacionados incluyen impuestos.
23. De manera general se considera un solo pago.
24. De manera general se consideran pagos a 30 días.

8. CONTACTOS / CONTACTS

Área Comercial / Business Area

Esperanza Jimenez Espinel.
eje@desmantelandoalhacker.net
Teléfono: 8059229.
Móvil: 317 853 42 00.

Área Administrativa / Administrative Area

Leidy Penagos.
ansiadm@desmantelandoalhacker.net
Teléfono: 8053207.
Móvil: 315 274 31 19.
Dirección: Crr 21 # 39a-66.
Nit: 900.034.395-5.

Área de Ingeniería / Support Area

David González.
david.gonzalez@desmantelandoalhacker.net
Teléfono: 8054198.
Móvil 317 366 44 53.

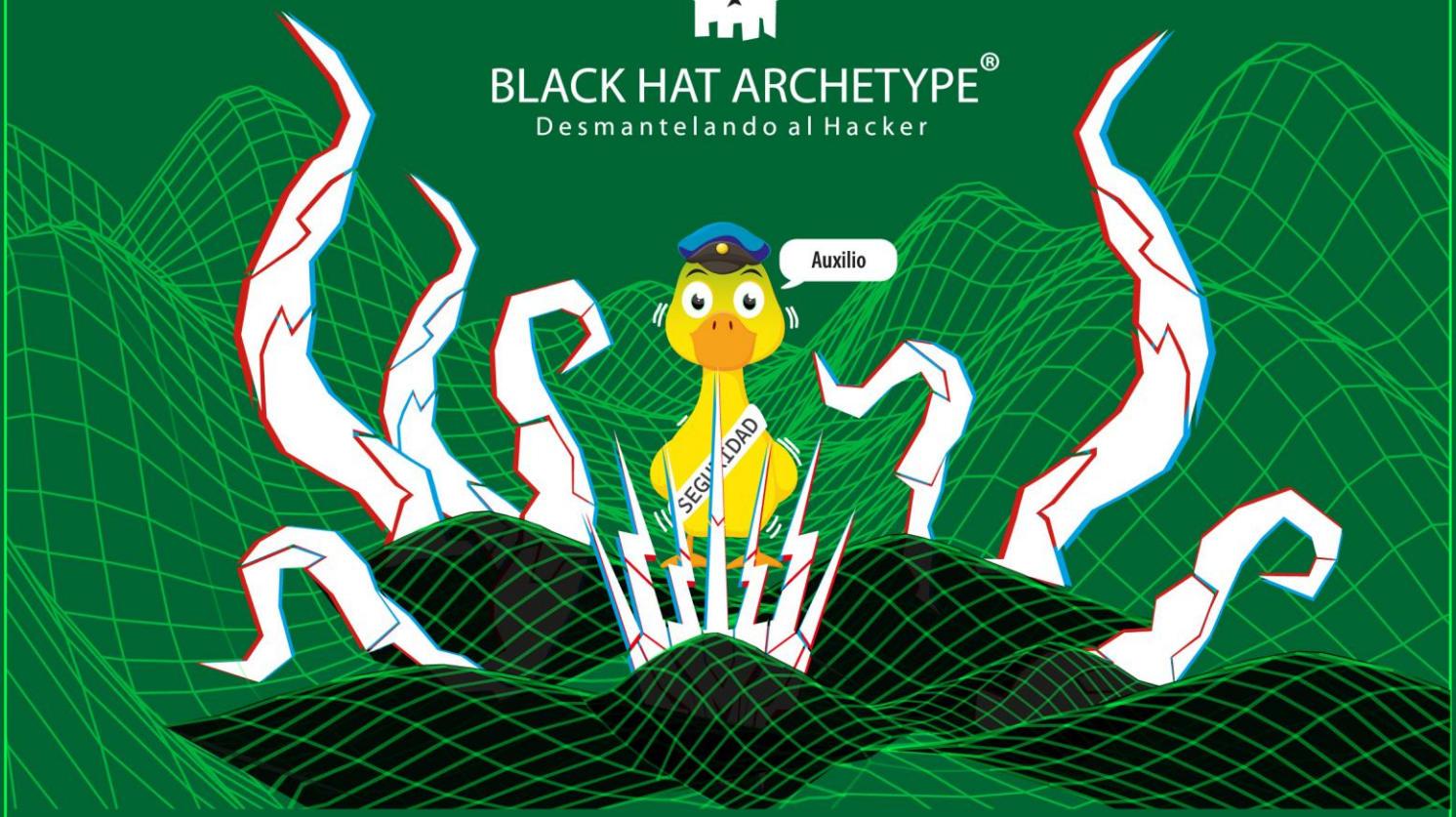
Sistema Integrado de Gestión / Integrated Management System (PQRSD)

Astrid Rodríguez.
directorsig@desmantelandoalhacker.net
Teléfono: 8053207.

Más info

BLACK HAT ARCHETYPE®

Desmantelando al Hacker



¡NO DEJES LA SEGURIDAD DE TU EMPRESA CON PATOS!

Seguridad informática | Seguridad de la información | Ciberseguridad | Seguridad Digital

ISO 9001:2015 BUREAU VERITAS Certification

ISO 14001:2015 BUREAU VERITAS Certification

ISO 27001:2013 BUREAU VERITAS Certification

ISO 45001:2018 BUREAU VERITAS Certification