BLACK HAT ARCHETYPE®
Desmantelando al Hacker

PROPUESTA ECONÓMICA

ECONOMIC PROPOSAL

N.º 333053

UNIDAD ADMINISTRATIVA ESPECIAL DE SERVICIOS PÚBLICOS

bha news

bha_cybersecurity

black-hat-archetype

bha - black hat archetype

SEGURIDAD DIGITAL

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. 333053

Bogotá, 02 de febrero de 2024

Señores
UNIDAD ADMINISTRATIVA ESPECIAL DE SERVICIOS PÚBLICOS -UAESP
Atn: Carlos Andrés Cuartas
Correo: carlos.cuartas@uaesp.gov.co
Teléfono: 3580400
Dirección: Carrera 53-80
NIT: 900.126.860-4

REF: Propuesta Económica Plataforma Trend Micro

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,

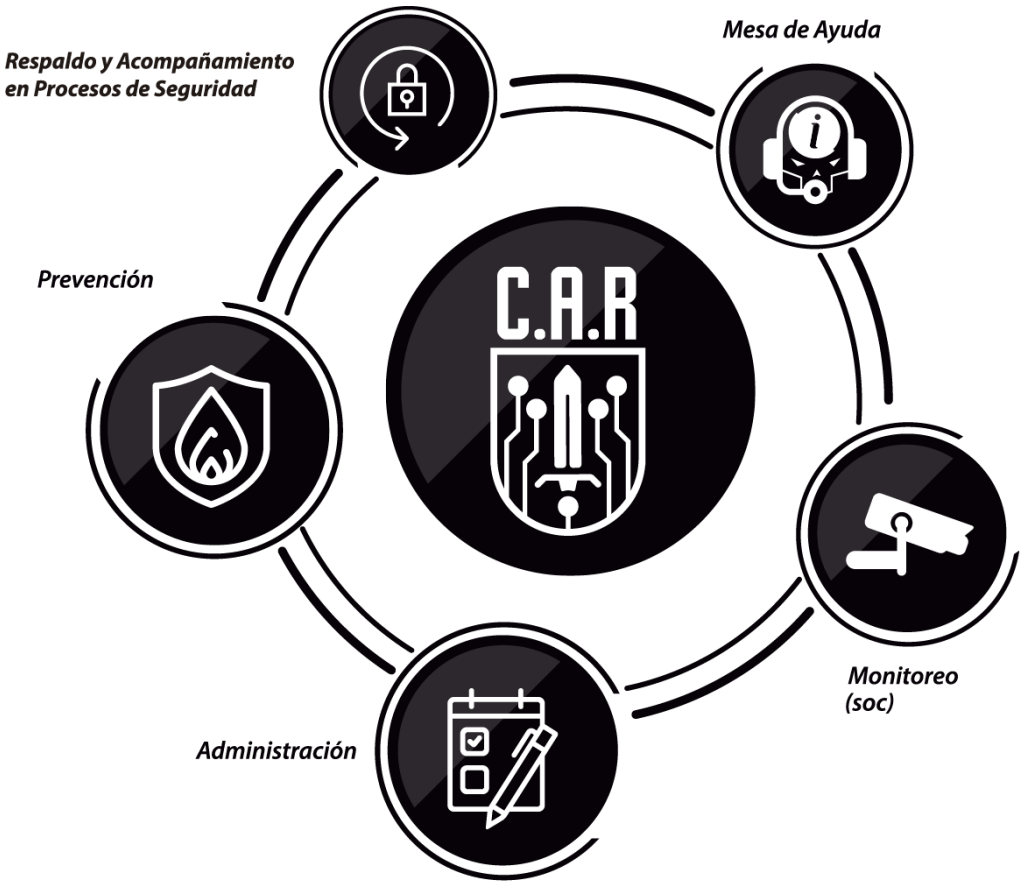
Revisada por:
Esperanza Jiménez Espinel
Consultora de Negocios en Seguridad de la Información
(57) 317 853 4200

Realizada por:
Mónica Acevedo
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 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:

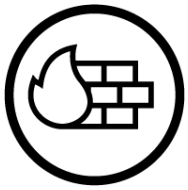
- **Diagnóstico de Seguridad:** Con este diagnóstico, se hace una exploración en el sistema y se identifican las diferentes vulnerabilidades que este puede llegar a tener, una vez el estudio concluye brindamos las herramientas más efectivas del mercado para ponerle fin a las deficiencias de seguridad.



- **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.



2. CONDICIONES GENERALES / TERMS

Presentar Propuesta de Cotización para llevar a cabo la renovación de la entidad Unidad Administrativa Especial de Servicios Públicos UAESP.

3. OBJETO / GOAL

Realizar la renovación del licenciamiento de la infraestructura firewall de propiedad de la entidad y realizar renovación del licenciamiento antimalware (antivirus) instalado actualmente en la Unidad, actualizando las características de análisis de la superficie de ataque de la infraestructura actual de la UAESP proporcionando el índice de riesgo general de la entidad, basado en dispositivos, activos conectados a Internet, actividad de cuentas, aplicaciones en la nube y activos en la nube. Así como identificando vulnerabilidades, riesgos de configuración del sistema, riesgos de actividad sospechosa y comportamiento del usuario, mediante la recolección de datos desde diferentes fuentes de información conectadas. De esta forma garantizar la administración y control de la seguridad informática perimetral y la administración de la seguridad informática en los dispositivos de usuario final y servidores de la Unidad Administrativa Especial de Servicios Públicos – UAESP. Licenciamiento de la característica

4. DESCRIPCIÓN DE LA SOLUCIÓN / PRODUCTS OR SERVICES

SMART PROTECTION COMPLETE:
Es una suite hibrida interconectada que ofrece protección a los usuarios sin importar dónde estén físicamente o que actividad estén realizando. ofrece la mejor protección en múltiples capas cubriendo la navegación, el correo, la conectividad y las aplicaciones y los documentos trabajando de forma coordinada para detectar, detener y mitigar las amenazas en la organización.
La suite maneja un modelo de licenciamiento simplificado y una gestión centralizada para permitir la visibilidad de la red y el control de amenazas. Incluye las siguientes capas de seguridad:

- Seguridad Endpoint. Utiliza machine learning (aprendizaje automático de máquinas) con otras técnicas para ofrecer máxima protección. Asegura la actividad del usuario en desktop físicos y virtuales, laptops o dispositivos móviles con protección de datos frente a amenazas, control de aplicaciones, protección de vulnerabilidades y cifrado.
- Seguridad en los servidores Linux. Utiliza agentes de seguridad compatibles con la mayoría de las distribuciones de Linux para proteger la información depositada en ellos.
- Seguridad móvil. Protege, rastrea, supervisa y gestiona los dispositivos móviles y tabletas de los empleados y los datos corporativos con seguridad.

- Seguridad para el correo electrónico y colaboración. Ofrece protección superior contra spam, phishing, malware y ataques dirigidos al gateway o a las aplicaciones en la nube como Office 365 o G-suite.
- Seguridad avanzada adicional para el correo electrónico, sin importar si el servicio está en ambientes on premise o en aplicaciones de nubes mediante el redireccionamiento de los MX.
- Seguridad web. Protege la actividad web de los usuarios en cualquier dispositivo y lugar permitiendo un acceso seguro a las aplicaciones web y medios sociales, obteniendo visibilidad completa y control del uso de la web en modo SaaS basado en cloud, o con una solución para el Gateway on premise de Internet.
- Gestión centralizada de la seguridad. Gestiona múltiples capas conectadas de protección de datos y amenazas para una visibilidad integral y centrada en el usuario a través de todo el ciclo de vida de la amenaza.

VENTAJAS

Las principales ventajas de la Suite son:
Seguridad Enpoint

- Filtra las amenazas progresivamente utilizando las técnicas más eficaces para maximizar la detección sin falsos positivos.
- Utiliza técnicas con o sin firmas, incluyendo machine learning, análisis de comportamiento, detección de huellas de variantes, control de aplicaciones, prevención frente a exploits y verificación de archivos válidos con técnicas tales como la reputación de archivos, reputación Web y bloqueo de comunicaciones de comando y control (C&C).
- Gracias al machine learning se realiza análisis tanto antes como durante la ejecución de los archivos por parte de las aplicaciones diferenciando el análisis frente a las demás soluciones del mercado cuya tecnología solo les permite utilizar el machine learning antes o durante la ejecución.
- Utiliza técnicas de anulación de ruido como la utilización de listas blancas en cada capa análisis para reducir los falsos positivos.

Protección de datos

- Protege los datos con cifrado de carpetas, archivos y del disco completo para mantener la privacidad de los mismos.
- Control de dispositivos para evitar que la información se traspase a lugares donde no debe estar, como memorias USB, almacenamiento en nube o correos electrónicos.

- Protege los dispositivos móviles de los usuarios y frente a amenazas y los datos de la compañía mediante la activación del cifrado del dispositivo.
- Prevención de fuga de datos (DLP) basada en plantillas que permiten el cumplimiento de normativas internacionales o personalizadas para proteger los datos sensibles a través del End Point, de la navegación web, del correo electrónico y de las Apps SaaS.

Protección de Email y Web

- Detiene y evita que ataques de emails dirigidos, spam, phishing ransomware y malware desconocido impacten y afecten a su negocio.
- Detiene las amenazas antes que lleguen a los usuarios con técnicas de detección avanzadas incluyendo detección de exploits en documentos y análisis de malware en sandbox.
- Seguridad para el servidor de correo electrónico, protección en el Gateway, en los portales de colaboración, de mensajería instantánea y de aplicaciones Cloud tales como Office 365 o G-suite.
- Seguridad del Gateway Web protegiendo a los usuarios contra las amenazas procedentes de la web ofreciendo control granular a URL´s y visibilidad de uso de las aplicaciones en la web.
- Seguridad en la Web mediante un Proxy SaaS protegiendo a los usuarios contra las amenazas procedentes de la web ofreciendo control granular a URL´s y visibilidad de uso de las aplicaciones en la web.

Defensa de Amenazas Centralizada

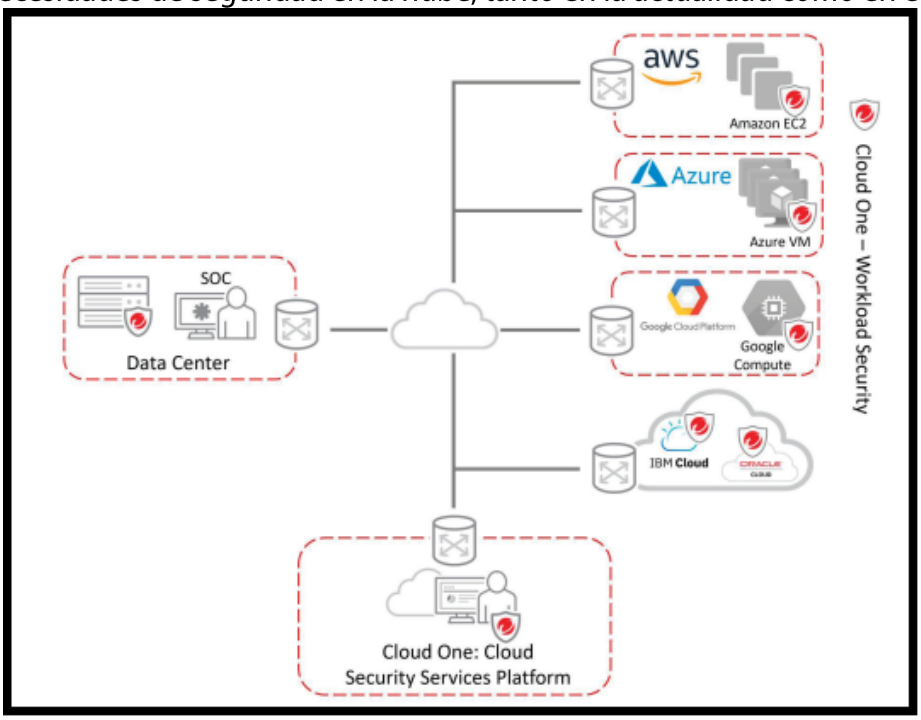
- Comparte información de forma instantánea de la actividad sospechosa en la red con archivos y otras capas de seguridad para detener ataques posteriores.
- Reduce el tiempo de protección contra ataques emergentes y dirigidos.



CLOUD ONE WORKLOAD SECURITY:

Protege datacenter, nube y contenedores sin poner en peligro el rendimiento ni la seguridad gracias a una solución SaaS completa y unificada.

Proporciona seguridad exhaustiva en una única solución creada a propósito para entornos de servidor, nube y contenedores. Workload Security ofrece una seguridad coherente, independientemente de la workload. También ofrece un amplio conjunto de interfaces de programación de aplicaciones (API) que permite automatizar la seguridad sin que afecte a los equipos. Una plataforma que tiene la amplitud, la profundidad y la innovación necesarias para cumplir y gestionar sus necesidades de seguridad en la nube, tanto en la actualidad como en el futuro.



Workload Security está optimizado para infraestructuras de proveedores líderes de servicios en la nube, e incluye soporte para los sistemas operativos más habituales:



Dentro de sus principales ventajas se encuentran:

Advanced Threat Protection

• Detectar y bloquear amenazas en tiempo real con un mínimo impacto en el rendimiento.

• Proteger frente a las vulnerabilidades conocidas y desconocidas en la web, en aplicaciones y en sistemas operativos a través de un IPS.

• Enviar alertas y active la prevención proactiva tras detectar actividad sospechosa o malintencionada.

• Proteger los sistemas para los que ha finalizado el soporte con parches virtuales proporcionados a través de un IPS, lo que garantiza que los sistemas heredados queden protegidos de las amenazas actuales y futuras.
• Rastrear la credibilidad de sitios webs y proteja los usuarios frente a sitios infectados gracias a la Threat Intelligence de reputación web de la base de datos global de Trend Micro sobre reputación de dominios.
• Identificar y bloquee ataques de robots y ataques dirigidos a las comunicaciones del centro de comando y control (C&C).

Seguridad unificada para la nube híbrida

• Los conectores de datacenter y de nube detectan automáticamente las workload ejecutadas en sus entornos híbridos para garantizar una plena visibilidad y la gestión automatizada de políticas.
• Eliminar el coste de implementar varias soluciones puntuales al mismo tiempo y lograr una seguridad
constante en los entornos físicos, virtuales, en la nube y en contenedores con una consola ligera, de gestión y de un solo agente.

Seguridad optimizada y automatizada

• Automatizar la implementación de seguridad, la gestión de políticas, las comprobaciones del estado y la elaboración de informes de cumplimiento de normativa con un amplio conjunto de API de REST de seguridad de workload.
• Reducir los costes de gestión al automatizar tareas de seguridad repetitivas y con gran consumo de recursos, reduciendo los falsos positivos en alertas de seguridad y permitiendo el flujo de trabajo de respuestas ante incidencias de seguridad.
• Reducir significativamente la complejidad de gestionar la supervisión de la integridad de archivos gracias a listas blancas de sucesos y sucesos de confianza basados en la nube

Cumplimiento de la normativa rentable

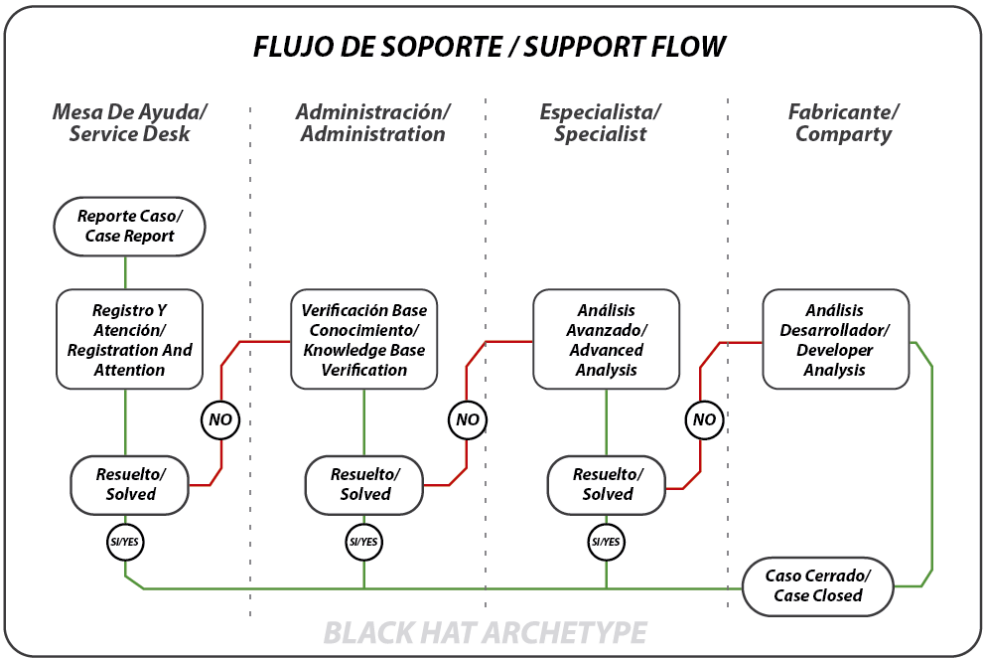
• Abordar los principales requisitos de cumplimiento del Reglamento general de protección de datos (GDPR), el estándar de seguridad de datos de la industria de pagos con tarjeta (PCI DSS), la ley de transferibilidad y responsabilidad del seguro sanitario (HIPAA), etc. con una solución integrada y rentable.
• Brindar informes de auditoría detallados que documentan los ataques evitados y el estado de cumplimiento de las políticas.
• Reducir el tiempo y el esfuerzo de preparación necesarios para ofrecer soporte a auditorías.

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: 14 Meses

Cant.	Descripción	Valor Unitario	Valor Total
	PLATAFORMA TREND MICRO A 14 MESES		
10	Workload Security Enterprise *	$ 1.279.385	$ 12.793.850
50	Licencias Smart Protection Complete	$ 319.914	$ 15.995.700
450	Licencias Smart Protection for Endpoint	$ 136.062	$ 61.227.900
50	XDR Endpoint Sensor	$ 130.545	$ 6.527.250
1	Soporte Especializado en el licenciamiento	$ 21.833.333	$ 21.833.333
	Antimalware.		
		Subtotal	**$118.378.033**
		IVA	**$ 20.060.995**
		Total con IVA	**$138.439.028**
		Los productos que estan con asterisco no llevan IVA	
	PLATAFORMA PALO ALTO 14 MESES		
2	Licencias PAN -PA-850-TP- HA2-R Threat	$ 16.620.577	**$ 33.241.154**
	Prevention subscription for device in an HA		
	Pair renewal, PA850		
2	Licencias PAN -PA-850-GP- HA2-R Global	$ 16.620.577	**$ 33.241.154**
	Protect subscription for device in an HA		
	Pair renewal, PA850		
2	Licencias PAN -PA-850-URL4- HA2-R PANDB URL	$21.780.000	**$ 43.560.000**
	Filtering subscription for device in an HA		
	Pair renewal, PA850		
1	Premium support year 1 renewal, PA- 850	$23.705.000	**$ 23.705.000**
1	Servicio de actualización, soporte durante la	$18.037.500	**$ 18.037.500**
	Vigencia de la suscripción, transferencia de		
	Conocimiento de las actualizaciones		
	Presentadas en la suscripción.		
		SUBTOTAL	**$ 151.784.808**
		IVA	**$ 28.839.114**
		TOTAL	**$ 180.623.922**

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.

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.

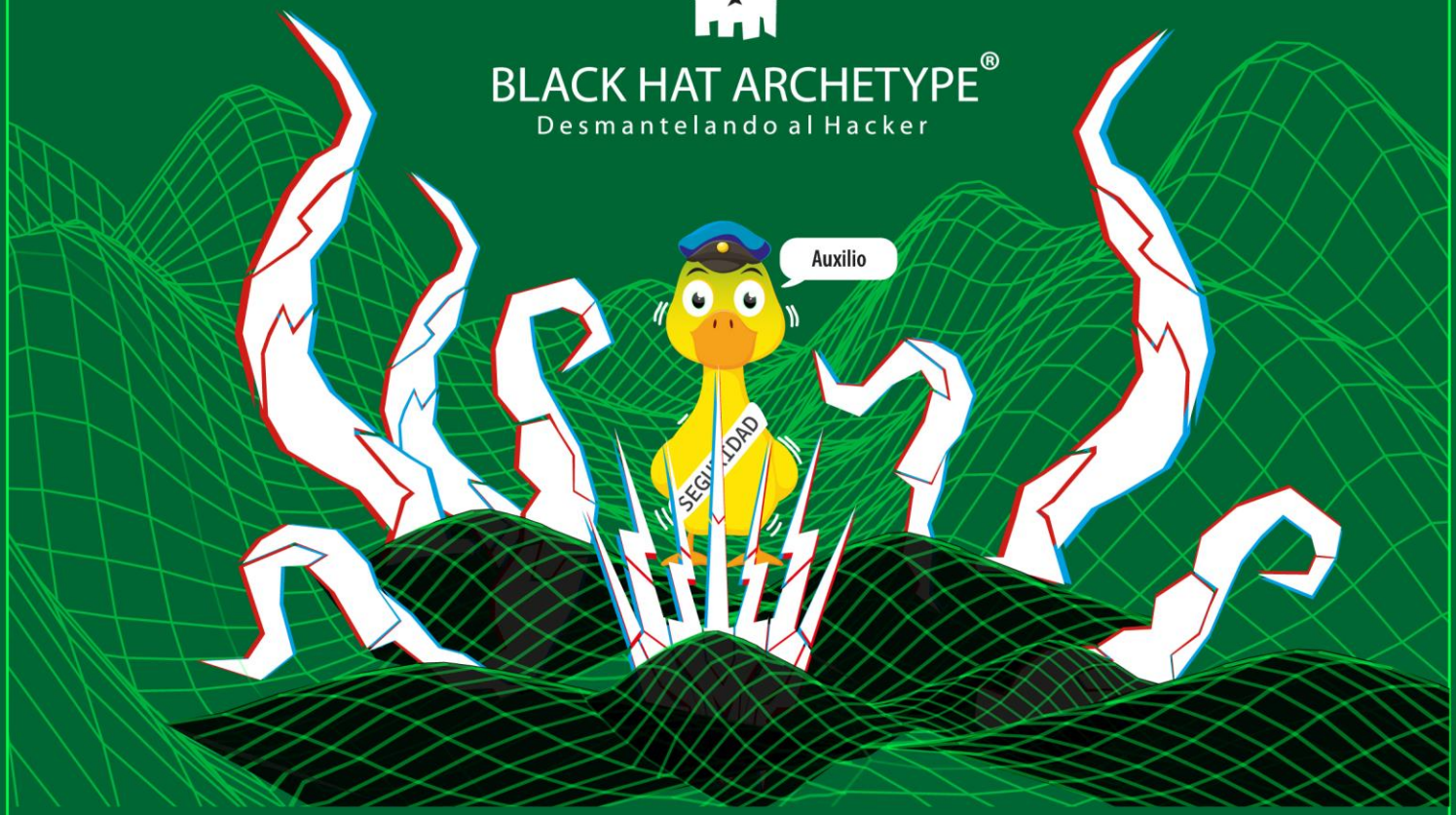
Sistema Integrado de Gestión / Integrated Management System (PQRSD)

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