INFORME FINAL DE SUPERVISIÓN	
DATOS GENERALES DEL CONTRATO UAESP-089-2024	
TIPO	Selección abreviada subasta inversa
Objeto Contractual:	TIC-007 Renovar el licenciamiento firewall y antimalware (antivirus), para control de la seguridad informática perimetral y administración de la seguridad informática en los dispositivos de usuario final de la Unidad Administrativa Especial de Servicios Públicos -UAESP.
Contratista:	**BLACK HAT ARCHETYPE SAS** **NIT 900034395 - 5**
	RICARDO ANDRÉS GUZMÁN FAJARDO Cedula de Ciudadanía C.C. 79.795.926
Plazo:	El plazo de ejecución de este contrato es de SEIS (6) Meses, contados a partir de la fecha de suscripción del acta de inicio, previo cumplimiento de los requisitos de perfeccionamiento y ejecución del contrato. Nota: El contratista debe realizar atención y servicio de soporte durante la vigencia del licenciamiento Renovado
Fecha de suscripción:	27/03/2024
Fecha de inicio:	**01 de abril de 2024**
Fecha de terminación inicial:	30 de septiembre de 2024
Valor inicial: **(CDP – CRP)**	CDP: 108 del 19 de febrero de 2024 **($330.000.000)** incluido IVA. CRP: 177 del 1 de abril de 2024 Trescientos dieciséis millones trescientos catorce mil pesos m/cte ($316.314.000) incluido IVA
Valor Modificación **(CDP – CRP)**	N/A
Valor Total del contrato:	Trescientos dieciséis millones trescientos catorce mil pesos m/cte ($316.314.000), incluido IVA
Aclaratorio No. 1:	N/A
Supervisor de acuerdo con el Aclaratorio No.1 - Cláusula Segunda:	N/A
Valor pendiente en Predis:	$0

DESARROLLO DEL CONTRATO

OBLIGACIONES ESPECIFICAS DEL CONTRATISTA

1. Cumplir con las condiciones establecidas en los Documentos del Proceso de Contratación.
2. Desarrollar el objeto del Contrato en las condiciones de calidad, oportunidad, y obligaciones definidas en los Documentos del Proceso de Contratación.
3. Garantizar la calidad de los bienes y servicios prestados, de acuerdo con el Anexo Técnico, el Pliego de Condiciones y demás Documentos del Proceso.
4. En los términos del artículo 52 de la ley 80 de 1993 el CONTRATISTA será civilmente responsable frente a la UAESP de los perjuicios originados por el deficiente desempeño de sus funciones y obligaciones previstas en este contrato, además de las sanciones penales a que hubiere lugar.
5. Dar a conocer a la Entidad cualquier reclamación que indirecta o directamente pueda tener algún efecto sobre el objeto del Contrato o sobre sus obligaciones.
6. Abstenerse de adelantar intervención alguna a los recursos sin contar con los permisos emitidos por la entidad competente (cuando aplique intervenciones).
7. Acreditar el cumplimiento del factor de calidad ofrecido durante la fase de selección en los plazos acordados con la Entidad.
8. Dar cabal cumplimiento al pacto de transparencia y declaraciones de la carta de presentación de la oferta.
9. Informar a la UAESP cuando ocurra una situación que implique una modificación del estado de los riesgos existentes al momento de proponer o celebrar el contrato.
10. Comunicarle a la UAESP cualquier circunstancia política, jurídica, social, económica, técnica, ambiental o de cualquier tipo, que pueda afectar la ejecución del Contrato.
11. Durante la ejecución del contrato deberá observar las leyes y los reglamentos relativos a Salud Ocupacional y Seguridad Industrial y tomar todas aquellas precauciones necesarias para evitar que se produzcan en las zonas de sus campamentos de trabajo, accidentes o condiciones insalubres; así como dotar a su personal y asegurar el uso adecuado de los elementos de protección personal (EPP). (cuando aplique)
12. Informar periódicamente la composición del capital social de la persona jurídica; la existencia de pactos o acuerdos de accionistas; su pertenencia o no a un grupo empresarial, si se trata de una matriz, subordinada, o sucursal de sociedad extranjera, así como la información relevante de índole jurídica, comercial o financiera, de la persona jurídica o de sus representantes legales, socios o accionistas. (cuando aplique)
13. Cumplir con sus obligaciones laborales respecto del personal a su cargo, y con las obligaciones tributarias y ambientales que le correspondan de acuerdo con su labor.
14. Informar a la UAESP cuando se tenga conocimiento del inicio de investigaciones penales, se impongan medidas de aseguramiento o condenas proferidas en Colombia o en el extranjero en contra de cualquiera de los directivos, representantes legales, accionistas o integrantes del Contratista.
15. Suscribir oportunamente el acta de inicio y el acta de liquidación del contrato, conjuntamente con el Supervisor y la Interventoría del mismo, cuando corresponda.
16. Entregar al Interventor los documentos elaborados en cumplimiento de las obligaciones contractuales, así como los informes y archivos a su cargo, requeridos sobre las actividades realizadas durante la ejecución del mismo. (cuando aplique)
17. Mantener estricta reserva y confidencialidad sobre la información que conozca por causa o con ocasión del contrato, así como, respetar la titularidad de los derechos de autor, en relación con los documentos, obras, creaciones que se desarrollen en ejecución del contrato.
18. Obrar con lealtad y buena fe en el desarrollo del presente Contrato.

19. Cuando se trate de personas naturales: Realizar el pago de los aportes al régimen de seguridad social, en proporción al valor mensual del contrato, y entregar copia de la planilla con marca de agua y rótulo de PAGADA. al supervisor del contrato para cada pago. Cuando se trate de personas jurídicas: Entregar para cada pago, la certificación suscrita por el representante legal o revisor fiscal, que acredite el cumplimiento del pago de aportes al sistema de seguridad social integral, parafiscales, ICBF, SENA y cajas de compensación familiar mediante planillas con marca de agua y rótulo de PAGADA de los últimos seis (6) meses, de conformidad con el artículo 50 de la Ley 789 de 2002 o aquella que lo modifique, adicione o complemente. Adicionalmente, el soporte de pago actualizado de los aportes al sistema de seguridad social en salud, pensiones y riesgos profesionales, así como el pago de la nómina y aportes parafiscales de todo el personal vinculado a la obra (cuando aplique), de conformidad con el artículo 182 de la Ley 100 de 1993, la Ley 782 de 2002, el Decreto 1703 de 2002, las Leyes 797 y 828 de 2003, el Decreto 510 de 2003, Ley 1150 de 2007 y la Ley 1562 de 2012.
20. Realizar por su cuenta y riesgo todas las actividades necesarias para cumplir con las obligaciones derivadas del presente Contrato, de acuerdo con las mejores prácticas técnicas y administrativas con la calidad propia de los proyectos de esta naturaleza.
21. Constituir y mantener vigentes las garantías, en los plazos y montos establecidos en el presente Contrato.
22. Ejecutar el Contrato cumpliendo con las normas específicas técnicas y propias del proyecto, descritas en el anexo técnico o en sus documentos previos, teniendo en cuenta los principios de economía, eficiencia, celeridad y calidad.
23. Abstenerse de suministrar, entregar o publicar, sin la autorización previa de la UAESP, información que NO sea considerada pública, tal como la relativa a documentos en proceso de elaboración, que contengan información preliminar y no definitiva.
24. Rechazar peticiones y no acceder a amenazas de quienes actúen por fuera de la ley y dar aviso de tales circunstancias a la UAESP y a las autoridades competentes.
25. Las demás obligaciones de carácter general descritas en la Constitución, la ley, los reglamentos, las normas técnicas, estudios previos, estudios de sector, pliegos de condiciones y el contrato, con sus respectivos Anexos o Apéndices.

PRODUCTOS ENTREGADOS

ESPECIFICACIONES MINIMAS LICENCIAMIENTO FIREWALL		
No.	**CANTIDAD**	**DESCRIPCION**
1	Dos (2)	Licencias PAN-PA-850-TP-HA2-R Threat prevention subscription for device in an HA pair renewal, PA850. (14 meses)
2	Dos (2)	Licencias PAN-PA-850-GP-HA2-R Global Protect subscription for device in an HA pair renewal, PA850. (14 meses)
3	Dos (2)	Licencias PAN-PA-850-URL4-HA2R PANDB URL Filtering subscription for device in an HA pair renewal, PA850. (14 meses)

4	Un (1)	Premium support renewal, PA-850 (14 meses) • Lanzamientos de funciones y actualizaciones de software: permite mantener actualizado con las últimas funciones y actualizaciones de software. • Actualizaciones de servicios de suscripción: para garantizar que su implementación de Palo Alto Networks se mantenga actualizada, puede configurar dispositivos para descargar automáticamente la tecnología App-ID, filtrado de URL, seguridad DNS, prevención de amenazas y actualizaciones del servicio WildFire. Alternativamente, estas actualizaciones se pueden descargar y aplicar manualmente. • Garantía de seguridad: en caso de que detecte actividad sospechosa en su red,se le brinda acceso a nuestros expertos en seguridad con herramientas y prácticas de inteligencia de amenazas únicas para Palo Alto Networks. Nuestro equipo ayudará a orientar las investigaciones iniciales, facilitará la recopilación de registros e indicadores de compromiso (IoC) y, al mismo tiempo, acelerará la transferencia a su proveedor de respuesta a incidentes (IR) preferido • Acceso directo a expertos en productos: interactúe con un ingeniero de soporte capacitado para comprender y resolver rápidamente sus desafíos únicos.

CARACTERÍSTICAS TÉCNICAS	DESCRIPCIÓN LICENCIAMIENTO A RENOVAR - ANTIMALWARE (ANTIVIRUS)	
CANTIDAD	**DIEZ (10)**	**DIEZ (10) licencias WORKLOAD PROTECTION (SECURITY ENTERPRISE).** **NOTA:** Se debe realizar el acompañamiento y soporte de la actualización tecnológica de plataforma deep security a Workload Protection.
FUNCIONALIDAD	• Seguridad enfocada en entornos de virtualización • Manejo de entornos Híbridos y aseguramiento de estos • Integración mediante políticas aplicables a entornos locales y en nube • Centralización de controles de seguridad en un solo panel de administración • Prevención de malware con supervisión del comportamiento y machine learning predictive • Protección frente a ataques sofisticados en entornos virtuales aislando malware de componentes de seguridad y sistemas operativos críticos. • Identificación y análisis de objetos sospechosos a través del análisis en recinto aislado • Reenvío de sucesos al sistema SIEM o al servidor de registro centralizado para las tareas de correlación, documentación y archivado. • Registro de los sucesos de cortafuegos en el host, permitiendo el cumplimiento y la generación de informes de auditoría. • Defensa frente a ataques SQL injection, de secuencias de sitios cruzados y otras vulnerabilidades de aplicaciones web	

		• Gestión de forma centralizada de políticas de firewall de servidor, incluidas plantillas para tipos de servidores habituales. • La solución deberá como mínimo contar con las siguientes características y capacidades de protección: • La solución debe proteger servidores físicos, virtualizados con las plataformas vmware, hyper-v entre otras, la cual contemple protección contra código malicioso (Antivirus), firewall de host e IPS de Host el cual proteja contra ataques de explotación de vulnerabilidades sin afectar la operación de los servidores. • Las funcionalidades de antivirus, Firewall de Host e IPS de Host, Monitoreo de Integridad y Monitoreo de bitácoras deberán ser brindadas por un solo agente instalado en los servidores y en el caso de ambientes virtuales sobre la plataforma vmware realizar las funcionalidades de protección de antivirus, Firewall de Host e IPS de Host, Monitoreo de Integridad, desde el hipervisor sin necesidad de instalar un agente de protección en cada máquina virtual. • La solución debe entregar licencias para parcheo virtual especializado que sea compatible con servidores Windows o linux. • La solución debe proporcionar capacidades integradas de descubrimiento de cargas de trabajo, que se integran con Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform, VMware y Microsoft Active Directory. • La solución debe poder proteger centro de datos, nube y contenedores sin comprometer el rendimiento con capacidades CNAPP. • La solución debe soportar como mínimo: • **Microsoft Windows** • Windows XP, 7, 8, 8.1, 10, 11 (32 bits/64 bits). • Windows Server 2003 (32 bits/64 bits). • Windows Server 2008 (32 bits/64 bits), 2008 R2, 2012, 2012 R2, 2012 Server Core (64 bits), 2016 (64 bits), 2016 Server Core (64 bits). • **Linux** • Red Hat Enterprise 5, 6, 7, 8, 9 (64 bits). • SUSE Enterprise 10, 11, 12, 15 (64 bits). • CentOS 5, 6, 7 (64 bits). • Ubuntu 12, 14, 16, 18, 20 y 22 (64 bits). • Oracle Linux 5, 6, 7 (64 bits). • CloudLinux 5, 6, 7 (64 bits). • Amazon Linux (64 bits). • Amazon Linux 2 (64 bits). • Debian 6, 7 (64 bits). • **Solaris** • Solaris: 10, 11 (SPARC, 64 bits), 10, 11 (x86 de 64 bits). • **Unix** • AIX 5.3, 6.1, 7.1 en IBM Power Systems7, 8. • AIX 7.3. • **Virtual** • VMware vSphere: 5.5/6.0, View 4.5/5.0/5.1, ESX 5.5, 6.2.X, 6.5, NSX 6.2.X, 6.3. • Citrix: XenServer11. • Microsoft: HyperV11. • **Protección contra código malicioso (Antivirus)**	

		• La solución deberá contar como mínimo con la capacidad de envío de archivos infectados a cuarentena. • La solución deberá contar como mínimo con una funcionalidad que le permita elegir la acción a tomar de manera automática dependiendo del tipo de amenaza detectada. • La solución deberá contar con la capacidad de aplicar al menos las siguientes acciones como limpieza, borrado y envío a cuarentena de archivo • La solución debe contar con un cache para el escaneo en tiempo real y escaneos programados, el a fin de optimizar el consumo de recursos en servidores virtuales. • La solución debe contar con la capacidad de integrar servicios de reputación del mismo fabricante, para mejorar la protección contra amenazas, debe contar con un servicio de reputación de archivos, y un servicio de reputación de URL's. El servicio de reputación de URL's evitará la conexión a sitios de mala reputación que puedan poner en riesgo la información que reside en los servidores de la institución. El servicio de reputación de URL's debe configurarse mediante umbrales y debe permitir el manejo de excepciones. • **Firewall de Host** • La solución deberá contener como mínimo un firewall que proteja servidores físicos y/o virtuales administrados desde la misma consola, permitiendo sólo las comunicaciones requeridas entre ellos. Este filtrado debe ser bidireccional y hacerse al menos sobre los siguientes parámetros: • Protocolos: ICMP, IGMP, GGP, TCP, PUP, UDP, IDP, ND, RAW, TCP+UDP • Direcciónes MAC • Direcciones IP • Puertos TCP & UDP • La solución deberá como mínimo ser capaz de realizar una inspección profunda de los paquetes bidireccional para analizar y prevenir ataques a vulnerabilidades en las aplicaciones instaladas en cada servidor, incluidas vulnerabilidades de día cero. • El módulo de firewall de host deberá como mínimo contar con la posibilidad de aplicar políticas diferentes para cada una de las interfaces de red con las que cuenta el servidor. • El módulo de firewall de host deberá como mínimo contar con la posibilidad de aplicar políticas de manera programada. • **Protección contra ataques de explotación de vulnerabilidades (IPS de Host)** • La solución deberá como mínimo ser capaz de realizar una inspección profunda de los paquetes de manera bidireccional para analizar y prevenir ataques a vulnerabilidades en las aplicaciones instaladas en cada servidor, incluidas vulnerabilidades de día cero. • La solución deberá como mínimo monitorear el tráfico para registrar algún ataque, pero no realiza ninguna acción de bloqueo. • La solución deberá como mínimo monitorear el tráfico para registrar algún ataque y bloquear el tráfico relacionado con él sin afectar el tráfico normal, el cuál no esté relacionado con el ataque, permitiendo que continúen disponibles los servicios del servidor. • La solución deberá como mínimo proteger contra aquellas vulnerabilidades descubiertas, aplicando la protección en los servidores de la entidad sin tener	

		que reiniciar el sistema o modificar el código fuente de la aplicación o sistema operativo. • La solución deberá como mínimo contar con protección inmediata de vulnerabilidades para más de 100 aplicaciones y sistemas operativos, incluidas bases de datos, sitios Web, correo electrónico y servidores FTP entre otras • La solución debe contar con la capacidad de proteger vulnerabilidades de sistema operativo y aplicaciones utilizando tecnologías de parcheo virtual. • La solución debe como mínimo contar con la capacidad de realizar escaneos en los servidores y determinar de manera automática los parches virtuales que se requieren aplicar para proteger las vulnerabilidades del sistema operativo y aplicaciones que se encuentran corriendo sobre dichos servidores. • **Monitoreo de integridad del sistema operativo y aplicaciones.** • La solución deberá como mínimo identificar los cambios en archivos críticos, cambios a la configuración de archivos, carpetas, servicios y llaves de registro tanto del sistema operativo como de las aplicaciones instaladas en el servidor. • La solución deberá ser capaz de realizar e identificar automáticamente reglas de monitoreo de integridad, para realizar el monitoreo de cambios del sistema operativo y las aplicaciones instaladas en el servidor. • La solución deberá contar como mínimo con la capacidad de alertar en tiempo real cuando una modificación haya sido detectada en carpetas, archivos o llaves de registro del sistema operativo y aplicaciones, las alertas podrán ser enviadas por correo electrónico o por syslog. • La solución deberá contar como mínimo con la capacidad de crear reglas personalizadas para el monitoreo de modificaciones en archivos críticos, carpetas y llaves de registro. • **Monitoreo de eventos o bitácoras del sistema operativo y aplicaciones.** • La solución deberá como mínimo inspeccionar las bitácoras del sistema operativo y aplicaciones para identificar eventos de seguridad que se consideren relevantes o críticos. • La solución deberá como mínimo tener la capacidad de inspeccionar eventos generados en el visor de eventos para los servidores de plataformas Windows. • La solución deberá como mínimo tener la capacidad de inspeccionar eventos generados en el syslog messages de servidores con sistema operativo Linux. • La solución deberá como mínimo tener la capacidad de inspeccionar eventos generados por aplicaciones los cuales sean almacenados en archivos de bitácoras. • La solución deberá contar como mínimo con la capacidad de alertar en tiempo real cuando un evento crítico o relevante sea generado, las alertas podrán ser enviadas por correo electrónico o por syslog. • La solución debe contar con características XDR. • La solución debe permitir monitorear, registrar y realizar investigaciones de seguridad actuales e históricas en sus diferentes puntos finales. Por medio de un panel debe permitir la investigación preliminar y de causa raíz de un incidente, permitiendo ubicar los puntos finales en riesgo antes de ejecutar el análisis de causa raíz en profundidad para identificar los vectores de ataque. • Debe permitir generar investigaciones preliminares para identificar rápidamente los puntos finales que son posibles candidatos para un análisis adicional. Una investigación preliminar utiliza metadatos del servidor para obtener resultados rápidamente.	

		• Debe permitir genera investigaciones detalladas que permitan realizar una investigación sobre el estado actual del sistema. Las investigaciones detalladas se pueden configurar para que se ejecuten en períodos específicos y también admiten un conjunto más amplio de criterios mediante el uso de las reglas de OpenIOC y YARA. • La solución deberá permitir graficar toda la cronología de los eventos generados en una investigación por medio de un gráfico de anillos que muestra el número total de puntos finales clasificados ya sea estén relacionados, o no relacionados a otros procesos, en cola o cancelados. La información debe estar siendo actualizada en tiempo real y de forma automática mientras avanza una investigación. • La solución debe permitir la búsqueda de Indicadores de Compromiso (IoC) en búsqueda de comunicaciones específicas, actividad de registro, actividad de la cuenta autenticada en el sistema, procesos en curso. • Protección contra ataques de exploits: controla los programas que demuestran un comportamiento anormal asociado con ataques de exploits. • Aprendizaje automático: analiza archivos desconocidos de baja prevalencia al extraer características de los archivos para examinarlos utilizando algoritmos de aprendizaje automático para determinar si el archivo es malicioso (es decir, malware / ransomware / amenazas de día 0). • La solución debe permitir la integración con información externa de IoC (Indicators Of Compromises) como reglas YARA, OpenIoC, STIX, TAXII • La solución debe permitir el análisis de comportamiento de un malware, actividades especificas de IoC y conexiones de comando a control. • La interfaz de la solución debe estar integrada con la consola de administración de las soluciones de seguridad para tener desde un solo punto el análisis, el contexto completo de los eventos y la línea de tiempo de los sucesos. • La solución debe convivir con cualquier solución de malware en el caso que el equipo a proteger tenga otro tipo de protección. • La solución debe controlar los programas que demuestran un comportamiento anormal asociado con ataques de exploits. • La solución debe escanear documentos en busca de códigos de exploits integrados y vulnerabilidades conocidas. • La solución debe analizar los archivos desconocidos de baja prevalencia utilizando algoritmos de aprendizaje automático para determinar si el archivo es malicioso. • La solución debe ser capaz de recopilar datos del sensor en los endpoints(IOC) y almacenarlos de forma centralizada para su posterior análisis. • La solución instantáneas de datos volátiles: maneja archivos, claves de registro, procesos, hilos, controladores cargados, , tareas, servicios, DNS, ARP, socket, etc. • La solución debe contar con la capacidad de registrar eventos basados en criterios establecidos. • La solución debe tener la capacidad de realizar barrido de IOC en todos los dispositivos con sensor. • La solución debe tener la capacidad de asociar los datos de registro y logs de los procesos con otros artefactos de disco y/o memoria.	

		• La solución debe tener la capacidad de buscar reglas de Yara en: memoria, memoria de proceso, registros, archivos individuales, carpetas, disco entero y eventos. • La solución debe permitir realizar consultas y luego crear alertas personalizadas con base en ellas. • La solución debe permitir la exportación de inteligencia de amenazas a través de STIX/TAXII • La solución debe mostrar todos los dispositivos en los que un proceso principal (padre) inicia otros procesos (hijos) especialmente de tipo powershell y cmd. • La solución debe tener la capacidad de identificar amenazas aún cuando usen powershell codificado. • La solución debe detectar tareas programadas maliciosas. • La solución debe revelar la cadena completa de procesos afectados por el malware/comportamiento malicioso. • La solución debe contar con la capacidad de mostrar la línea de tiempo de incidentes. • La solución debe tener la capacidad de mostrar en una sola vista todo el ciclo de vida del ataque de la amenaza • La solución permitirá que el trabajo de investigación continúe en el dispositivo aislado sin permitir que se extienda la actividad maliciosa por medio de cuarentena y/o aislamiento de los sistemas infectados • La solución de XDR no debe requerir un agente adicional a los agentes de Endpoint y Server Protection instalados en las maquinas • La solución de detección y respuesta debe permitir la correlación entre, endpoints y los servidores de mismo fabricante del XDR • XDR debe contar con modelos de detección avanzados que detectan actividades de bajo perfil en distintas capas de seguridad para encontrar nuevos ataques.	
CARACTERÍSTICAS TÉCNICAS	**DESCRIPCIÓN LICENCIAMIENTO A RENOVAR - ANTIMALWARE (ANTIVIRUS) - (14 meses)**			
CANTIDAD	**QUINIENTAS CINCUENTA (550)**	• **CINCUENTA (50)** Licencias Smart protection complete. • **CUATROCIENTAS CINCUENTA (450)** Licencias Smart Protection for Endpoint. • **CINCUENTA (50)** Licencias XDR Endpoint Sensor.		

	FUNCIONALIDAD	**SMART PROTECTION COMPLETE:** • APEX ONE AND APEX CENTRAL FULL FEATURE FOR WINDOWS AND MAC • APEX CENTRAL ADVANCED EDITION - MULTI-LINGUAL • ENDPOINT ENCRYPTION • IM SECURITY • MOBILE SECURITY • OFFICESCAN Y PROGRAMAS DE COMPLEMENTO • APEX ONE DLP ADD-ON • SECURITY FOR MAC • APEX ONE VIRTUAL DEVICE INFRASTRUCTURE ADD-ON • PORTALPROTECT FOR SHAREPOINT • SCANMAIL FOR IBM DOMINO • SCANMAIL FOR MICROSOFT EXCHANGE • APEX ONE VULNERABILITY PROTECTION ADD-ON	

		• APEX ONE APPLICATION CONTROL ADD-ON • WORRY-FREE™ SERVICES • TREND MICRO WEB SECURITY STANDARD • TREND MICRO CLOUD APP SECURITY • XDR ADD-ON: CLOUD APPSECURITY • TREND MICRO APEX ONE™ AS A SERVICE • TREND MICRO EMAIL SECURITY STANDARD **SMART PROTECTION FOR ENDPOINT:** • APEX ONE AND APEX CENTRAL FULL FEATURE FOR WINDOWS AND MAC • APEX CENTRAL ADVANCED EDITION - MULTI-LINGUAL • ENDPOINT ENCRYPTION • MOBILE SECURITY • OFFICESCAN Y PROGRAMAS DE COMPLEMENTO • APEX ONE DLP ADD-ON • SECURITY FOR MAC • APEX ONE VIRTUAL DEVICE INFRASTRUCTURE ADD-ON • APEX ONE VULNERABILITY PROTECTION ADD-ON • APEX ONE APPLICATION CONTROL ADD-ON • WORRY-FREE™ SERVICES **XDR ENDPOINT SENSOR:** APEX ONE: ENDPOINTSENSOR x 50 • **Flujo de trabajo integrado**: La investigación de búsqueda y detección de amenazas se realiza dentro del flujo de trabajo y la consola de Apex One y muestra investigaciones en todos los correos electrónicos y servidores conectados. • **Registro eficiente de endpoints**: registra y almacena información sobre el comportamiento del sistema, las comunicaciones y el comportamiento del usuario. Los metadatos de esta información se envían al servidor Apex One para permitir a los investigadores "recorrer" en busca de indicadores de compromiso. • **Barrido de IoC del lado del servidor**: el servidor Apex One solo almacena metadatos esenciales de los datos registrados por el usuario final (o telemetría). Esto permite a los investigadores realizar múltiples búsquedas o barridos de estos datos sin tener que consultar cada punto final individualmente. Además, se pueden realizar investigaciones detalladas de la causa raíz directamente en cada punto final. • **Búsqueda flexible**: los investigadores pueden buscar (o barrer) con múltiples parámetros. Se pueden realizar búsquedas sobre parámetros como comunicaciones específicas, malware específico, actividad del registro, actividad de la cuenta y procesos en ejecución. O los investigadores pueden buscar utilizando las reglas estándar de la industria OpenIOC o YARA. • **Análisis de la causa raíz**: los investigadores pueden profundizar en un árbol de procesos interactivo que ilustra la cadena completa del ataque para analizar cómo llegó, cambió y se propagó la detección mediante la visualización de actividades, objetos y procesos. Se puede tomar una respuesta inmediata para	

		finalizar procesos, aislar a los usuarios, actualizar la seguridad y seguir avanzando. • **Inteligencia y asistencia de proveedores**: al incorporar inteligencia proactiva sobre amenazas globales, Trend Micro™ Smart Protection Network™ proporciona claridad y asistencia a los investigadores de amenazas. Endpoint Sensor reconoce tanto los objetos y procesos buenos conocidos como los malos. Los investigadores pueden ver un análisis de la causa raíz codificado por colores para identificar procesos desconocidos o riesgosos y guiarlos en la remediación. Los investigadores también pueden acceder al servicio Trend Micro™ Threat Connect™ para investigar nuestra base de datos de información sobre amenazas. • **Opciones de respuesta inmediata**: Apex One ya proporciona automatización avanzada para remediar las detecciones. Puede aislar, poner en cuarentena, bloquear ejecuciones, revertir configuraciones (y archivos, en el caso de ransomware) automáticamente, con la opción de responder manualmente mientras se realiza una investigación. Los puntos finales se pueden aislar, los procesos se pueden finalizar y la inteligencia de seguridad se puede actualizar automáticamente por usuario o en toda la empresa. • **Búsqueda de amenazas avanzada**: la búsqueda de amenazas, basada en indicadores de ataque (IoA), permite a los investigadores desarrollar reglas de descubrimiento de ataques o trabajar con los IoA proporcionados por Trend Micro para buscar amenazas. • **API abiertas**: muchos clientes quieren poder aprovechar sus herramientas de operaciones de seguridad. Apex One tiene múltiples interfaces de programación de aplicaciones (API) integradas y documentadas que permiten que el producto funcione con estas herramientas. • **Integración de Sandbox**: los investigadores de seguridad pueden seleccionar objetos y enviarlos manualmente a los Sandboxes de Trend Micro. Los objetos sospechosos se pueden enviar a nuestros entornos sandbox de seguridad de red Trend Micro™ Deep Discovery™ locales o a Trend Micro Apex One™ Sandbox como opción de suscripción de servicio. **Nota:** La solución debe ser compatible mínimo con los sistemas operativos Windows, IOS, Android, MAC OS.
OTRAS CONSIDERACIONES		**DESCRIPCIÓN LICENCIAMIENTO A RENOVAR - ANTIMALWARE (ANTIVIRUS)**
RENOVACION		• Renovación por **Catorce (14)** meses del licenciamiento. • Realizar la actualización de la versión del licenciamiento en caso de liberarse nuevas versiones durante la vigencia de las Licencias. • Realizar la entrega y activación del licenciamiento tipo suscripción anualizada, teniendo en cuenta las condiciones en la cual ya opera el versionamiento del licenciamiento instalado en la Unidad. • Garantizar el correcto funcionamiento del licenciamiento a renovar para lo cual se debe garantizar la descarga de paquetes y complementos necesarios para la actualización y renovación del licenciamiento teniendo en cuenta las condiciones en la cual ya opera el versionamiento del licenciamiento instalado en la Unidad.
SOPORTE TÉCNICO		El contratista deberá brindar soporte técnico especializado (remoto y/o en sitio) sobre el funcionamiento de la herramienta (realizar el escalamiento con el fabricante) con

	la finalidad de garantizar el correcto funcionamiento de la solución durante la vigencia del licenciamiento (14 meses).
TRANSFERENCIA DE CONOCIMIENTO	• Realizar la transferencia de conocimiento sobre la administración de la solución antivirus durante la vigencia del licenciamiento. • Realizar la transferencia de conocimiento sobre el uso de la solución antivirus durante la vigencia del licenciamiento. • Realizar la transferencia de conocimiento sobre las actualizaciones y nuevas funcionalidades de la suscripción durante la vigencia del licenciamiento. • Entregar los respectivos manuales de configuración de las consolas de administración antivirus, ajustados para la solución adquirida por la entidad.
CANALES DE ATENCIÓN	El proveedor deberá entregar documento con los canales de atención y tiempo de respuesta ante solicitudes por parte de la supervisión. **Documento ANS:** Certificado de distribuidor/canal autorizado directamente de fabricante de la solución.

Conforme a los Informes de supervisión las actividades se ejecutaron de acuerdo con lo estipulado en el objeto y obligaciones contractuales, y que se adoptaron las observaciones y recomendaciones realizadas.

FORMA DE PAGO:

La UAESP realizará UN ÚNICO PAGO POR EL VALOR TOTAL DEL CONTRATO, una vez se certifique el recibo a satisfacción por parte del supervisor, de la activación de las suscripciones adquiridas junto con la configuración e implementación efectiva de cumplimiento con el ANEXO 3 - ANEXO TECNICO.

Para el pago a efectuar, el Contratista deberá presentar:

1. Factura debidamente diligenciada conforme los requisitos establecidos en el Artículo 617 del Estatuto Tributario.
2. Constancia suscrita por el supervisor del contrato, en la que se señale que el Contratista cumplió a satisfacción de la Entidad, con el objeto y las obligaciones pactadas.
3. Certificación expedida por el representante legal o revisor fiscal mediante la cual se acredite que se encuentra a paz y salvo en el cumplimiento del pago de los aportes al Sistema General de Seguridad Social y parafiscales del mes correspondiente, de conformidad con lo previsto en el artículo 50 de la Ley 789 de 2002 si es persona jurídica, la Ley 828 de 2003 y el Decreto 1703 de 2002 si es persona natural.
4. Dar cumplimiento al procedimiento GAL-PC-01 PROCEDIMIENTO DE INGRESO A LA ENTIDAD GAP-PC-01.
5. Certificado de ingreso al Almacén de la UAESP.

PARÁGRAFO PRIMERO: Los pagos se realizarán dentro de los quince (15) días siguientes a la radicación de la factura.
PARÁGRAFO SEGUNDO: En todo caso, los pagos que la UAESP se compromete a efectuar, quedan sujetos al PAC (Programa Anual de Caja) de acuerdo con las normas legales vigentes, comprometiéndose a incluir las partidas necesarias en este.
PARÁGRAFO TERCERO: Descuentos: El proponente deberá tener en cuenta que la UAESP efectuará los descuentos de Ley del Orden Nacional, Distrital vigentes y conforme a sus modificaciones de Ley, de acuerdo con la información tributaria suministrada por el contratista de la Entidad y con la actividad objeto del contrato.

PARÁGRAFO CUARTO: Los pagos se efectuarán a través del sistema SAP en la cuenta de ahorros o

corriente de la entidad financiera que indique el contratista, de la cual sea titular éste. Sin perjuicio de lo anterior queda entendido que la forma de pago supone la prestación real y efectiva de la contraprestación pactada.

RELACION DE PAGOS

Que mediante radicado No. 20247000319042 y factura N°. FE1965 del 20 de junio de 2024, la empresa **BLACK HAT ARCHETYPE SAS**, solicita el pago por valor de TRESCIENTOS DIECISÉIS MILLONES TRESCIENTOS CATORCE MIL PESOS M/CTE ($316.314.000), en consecuencia, el supervisor aprobó el informe de supervisión y certificación de cumplimiento del contrato, de conformidad con las obligaciones del contratista, aprobando así el pago por la suma de $316.314.000, correspondiente a la orden de pago N°. 1864 del 24 de septiembre de 2024.

RELACIÓN DE PAGOS					
No. de la Factura	**Radicado**	**Valor de la Factura**	**Orden de Pago**	**Valor orden de pago**	**Fecha de pago**
FE1965	20247000319042	$316.314.000	1864	316,314,000.00	24-09-2024

De acuerdo con lo anterior el comportamiento de su ejecución fue el siguiente:

BALANCE:

CONCEPTO	VALOR CONTRATO	VALOR EJECUTADO	VALOR ORDEN DE PAGO
Valor Inicial del Contrato	**$ 316.314.000**		
Valor Adición No. 1	**$ 0**		
Valor pasivo exigible	**$ 0**		
Valor Total del Contrato	**$ 316.314.000**		
Valor Total Ejecutado por el Contratista	**$ 316.314.000**	**$ 316.314.000**	
Valor Total desembolsado al Contratista	**$ 316.314.000**		**$ 316.314.000**
Valor pendiente por desembolsar al Contratista	**$ 0**		
Valor No ejecutado por el Contratista y pendiente por liberar	**$ 0**		
VALOR TOTAL CONTRATO	**$ 316.314.000**	**$ 316.314.000**	**$ 316.314.000**

OBSERVACIONES ESPECIALES:

El presente contrato no reposa físicamente, este se encuentra de manera virtual en los expedientes 20246002711300089E del Sistema de Gestión Documental Orfeo.

Así mismo, los demás compromisos contractuales adquiridos en este contrato fueron cumplidos a cabalidad por las partes como consta en los documentos que reposan en la trazabilidad del pago y en el expediente virtual.

Cordialmente,



JORGE ALEXIS RODRIGUEZ MEZA
Jefe Oficina TIC de la UAESP

Elaboró: Marcela Arguelles Ceballos – Contratista Oficina TIC
Revisó: Gisela Arias Salazar - Contratista Oficina TIC
Anexo: Predis (1) Un folio