REPÚBLICA DE COLOMBIA

ALCALDÍA MAYOR DE BOGOTÁ D.C.

UNIDAD ADMINISTRATIVA ESPECIAL DE SERVICIOS PÚBLICOS

UAESP

ANEXO No. 3
ANEXO TECNICO

MODALIDAD DE SELECCIÓN: Selección Abreviada por Subasta Inversa

OBJETO: 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

BOGOTÁ D.C., ENERO DE 2024

Dependencia solicitante: Oficina de Tecnologías de la Información y las Comunicaciones
Fecha: Enero de 2024

NORMATIVA APLICABLE

- ✓ Ley 23 de 1989: Sobre derechos de autor.
- ✓ Ley 527 de 1999: Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
- ✓ Ley 594 de 2000: Reglamentada parcialmente por los Decretos Nacionales 4de 2004, 1100 de 2014. Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones.
- ✓ Ley 603 DE 2000: Esta ley se refiere a la protección de los derechos de autor en Colombia. El software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales.
- ✓ Ley 1150 de 2007: Seguridad de la información electrónica en contratación en línea.
- ✓ Ley 1266 de 2008: Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- ✓ Ley 1273 de 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- ✓ Ley 1341 de 2009: Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.
- ✓ Ley 1474 de 2011: Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
- ✓ Decreto 2364 de 2012: Firma electrónica. Decreto 2609 de 2012 Expediente electrónico.
- ✓ Decreto 2609 de 2012: Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado".
- ✓ Decreto 2693 de 2012: Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones.
- ✓ Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales.
- ✓ Decreto 1078 de 2015: Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- ✓ Ley 1915 de 2018: Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
- ✓ Resolución 500 de 2021: Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.
- ✓ Resolución 460 de 2022: Por la cual se expide el Plan Nacional de Infraestructura de Datos y su hoja de ruta en el desarrollo de la Política de Gobierno Digital, y se dictan los lineamientos generales para su implementación.
- ✓ Circular 001 de 2022 Presidencia de la República: Recomendaciones de uso de servicios en la nube como medida para mitigar riesgos de seguridad digital.
- ✓ Decreto 767 de mayo 16 del 2022: Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto **Único Reglamentario del** Sector de Tecnologías de la Información y las Comunicaciones.

1. Objeto a contratar

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.

2. Alcance del objeto

Realizar la renovación del licenciamiento de la infraestructura física 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.

3. Especificaciones técnicas

3.1 FIREWALL - (14 meses)

ESPECIFICACIONES MINIMAS LICENCIAMIENTO FIREWALL		
No.	**CANTIDAD**	**DESCRIPCIÓN**
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.

		• Disponibilidad de soporte premium: disfrute de soporte las 24 horas, los 7 días de la semana para problemas de toda gravedad con ingenieros sénior Platinum disponibles las 24 horas para ayudarlo. • Portal de soporte al cliente en línea: una plataforma rica en funciones brinda acceso a la documentación del producto, bases de datos de resolución de problemas, interacción entre pares y administración de casos de soporte.
5	Un (1)	Servicio de soporte técnico por parte del contratista de las soluciones contratadas en relación con procesos de configuración, parametrización, atención de casos, generación y entrega de manuales, actualización durante la vigencia de la suscripción. Dentro del soporte se encuentra incluida la transferencia de conocimiento del manejo de la solución y la transferencia de conocimiento de las actualizaciones presentadas. (14 meses).
NOTA: El contratista deberá brindar soporte técnico especializado (remoto y/o en sitio) sobre el funcionamiento de la herramienta y realizar el escalamiento con el fabricante (en caso de requerirse), con la finalidad de garantizar el correcto funcionamiento de la solución durante la vigencia del licenciamiento. **NOTA:** Debe entregar Certificado de distribuidor/canal autorizado directamente de fabricante de la solución.		
Realizar la entrega y activación del licenciamiento tipo suscripción anualizada (14 meses), 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.		
CANALES DE ATENCIÓN	El proveedor deberá entregar documento con los canales de atención y tiempo de respuesta ante solicitudes por parte de la supervisión.	

3.2 ANTIMALWARE (ANTIVIRUS) - (14 meses)

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.

Firma:



Nombre: CÉSAR MAURICIO BELTRÁN LOPEZ
Cargo: Jefe Oficina de Tecnologías de la Información y las Comunicaciones.
Dependencia Solicitante: Oficina TIC.

Elaboró: Eduardo Andres Rozo – Profesional Universitario – Oficina TIC.
Elaboró: Fabián Lozano – Contratista – Oficina TIC.
Elaboró: Carlos A. Cuartas – Profesional Universitario – Oficina TIC.

Aprobó: Cesar Mauricio Beltrán – Jefe Oficina TIC.