2do 13/11/18
Anexo 8

	Nota: esta licencia se debe instalar en equipo firewall de la entidad en las instalaciones de la Alcaldía de Puerto López.	
1.1	**Licenciamiento y soporte para firewall FortiGate 100F**	
1.1.1	Cantidad	Uno (1).
1.1.2	**Características equipo a licenciar**	
1.1.2.1	Equipo para la solución enterprise (Propósito específico) no se aceptan implementaciones en sistemas de propósito general como PC o servidor, usando sistemas operativos genéricos como Windows, Linux, Solaris, Apple MacOS o GNU.	Si.
1.1.2.2	Firewall Throughput	10 Gbps.
1.1.2.3	Concurrent Sessions	1,5 millones.
1.1.2.4	Nuevas sesiones por segundo	Cuarenta y cinco mil (45.000).
1.1.2.5	NGFW Throughput	1 Gbps.
1.1.2.6	Threat Protection	900 Mbps.
1.1.2.7	Interface gigabit ethernet RJ45	Seis (6).
1.1.2.8	Dominios Virtuales	Diez (10).
1.1.2.9	Puerto USB	Uno (1).
1.1.2.10	Puerto de consola	Uno (1).
1.1.2.11	Soporte IPV6/ IPv4	Si.
1.1.2.12	Usuarios concurrentes VPN SSL	Doscientos (200).
1.1.2.13	IPsec VPN Tunnels Client to Site	Dos mil quinientos (2.500).
1.1.2.14	(RIPv1/v2)	Si.
1.1.2.15	OSPF	Si.
1.1.2.16	SSL-VPN Throughput	950 Mbps.
1.1.2.17	Procesador de propósito específico para tráfico de RED	El equipo Firewall debe tener dentro de su arquitectura procesador de proposito específico para funciones de red que se encargue como mínimo de las siguientes funciones del equipo: o VPN o Prevención de intrusos o Aceleración de tráfico y defragmentación de paquetes Lo anterior sin degradar el funcionamiento del equipo en sus demás funciones.
1.1.2.18	Procesador de propósito específico para analizar contenido del tráfico	El equipo Firewall debe tener dentro de su arquitectura procesador de proposito específico para optimizar las funciones de control de contenido que realice como mínimo funciones de: o Inspección de tráfico SSL, o Cifrado y decifrado de tráfico SSL offloading. Lo anterior sin degradar el funcionamiento del equipo en sus demás funciones.
1.1.2.19	Capacidad SD-WAN Seguro (Secure SD-WAN)	El equipo debe tener dentro de sus funciones la capacidad de implementar SD-WAN Seguro, sin necesidad de contar con hardware adicional o licencias adicionales. Dentro de las características SD-WAN Seguro debe poseer como mínimo: o Aplicación de estrategias de SLA basadas en las métricas de verificación. o Clasificación de aplicaciones para determinación del mejor camino a seguir. o Monitoreo de salud de enlaces WAN mediante Ping, HTTP, tcp Echo, UDP Echo. o Monitoreo de métricas de salud por aplicación (al menos latencia, jitter y pérdida de paquetes).
1.1.2.20	Certificaciones de terceros, NSS Labs.	La tecnología ofertada debe estar evaluada por analistas independientes como NSS Labs y debe estar catalogada como "Recomendada" en el último boletín para el año 2019. El fabricante de la solución debe estar validado a nivel de rendimiento y seguridad por los siguientes laboratorios de pruebas de terceros, líderes en la industria de protección: VB100, AV Comparatives e ICSA. La solución debe estar respaldada por un laboratorio de investigación y desarrollo que ofrezca inteligencia en tiempo real entregando actualizaciones de seguridad completas, investigadores de amenazas de seguridad. Todo esto basado en mecanismos de inteligencia artificial y machine learning.
1.1.2.21	Soporte y licenciamiento	Todo licenciamiento y soporte de la solución ofertada debe ser de 1 año (Para el caso del soporte la atención en sitio debe ser de 24x7).

1.1.2.22	Módulos Licenciados	Funciones básicas de Firewall Conectividad y Enrutamiento VPN IPSec VPN SSL Manejo de Trafico y Calidad de Servicio Antimalware Filtrado Web IPS Control de Aplicaciones Inspección de contenido SSL/SSH
1.1.2.23	La solución debe ser compatible totalmente con la solución actual de ciberseguridad perimetral.	Si.
1.1.2.24	Propuesta Llave en Mano	Si.
1.2	**SERVICIOS DE IMPLEMENTACIÓN DE FIREWALL**	
1.2.1	Configuración, instalación y puesta en funcionamiento de toda la solución tecnológica propuesta, en el centro de datos nivel central.	Si.
1.2.2	El contratista dispondrá de un recurso humano en sitio (sede central: Calle 6 #4-40, Puerto López), durante el plazo de ejecución del contrato.	Si.
1.2.3	Propuesta Llave en Mano	Si.
1.3	**SOPORTE Y ASISTENCIA TÉCNICA PARA FIREWALL**	
1.3.1	Tiempo de soporte	Un (1) año.
1.3.2	Soporte técnico del fabricante para consultas y respuestas a solicitudes de la Alcaldía de Puerto López para la solución de problemas del hardware ofrecido, mediante acceso telefónico, vía web a una base de datos de conocimiento y a través de correo electrónico, durante el tiempo de la garantía.	Si.
1.3.3	Se deben incluir el acceso a soporte y actualizaciones de firmware y software para todos los elementos por parte del fabricante de los mismos	Si.
1.3.4	La cobertura del servicio de mantenimiento correctivo debe ser 7x24	Si.
1.3.5	Tiempo máximo de atención y corrección a fallas o, en su defecto, reemplazo del equipo por uno de iguales o superiores características mientras se corrige la falla debe ser: para atención y corrección de fallas de software seis (6) horas, para reemplazo del equipo treinta (30) días. En el caso de remplazo del equipo el fabricante o el contratista deberá disponer de una solución provisional que supla la necesidad y funcionalidad del equipo, ya sea on premise o en la nube.	Si.
1.3.6	Número de mantenimientos preventivos en sitio, durante el tiempo de garantía: Uno (1). Esto lo debe realizar el fabricante o el contratista sin costo adicional para la entidad (estos mantenimientos no deben interrumpir ninguno de los servicios que soportan por medio de la solución ofrecida)	Si.
1.4	**GARANTÍA LEGAL DE CALIDAD FIREWALL**	
1.4.1	La garantía legal de calidad debe ser de un (1) años a partir de la suscripción del acta de entrega de los bienes. Para el cumplimiento de este requisito, se aceptará la garantía legal de calidad del fabricante por un (1) año.	Si.
1.4.2	Debe incluir remplazo de partes o remplazo total por fallas de funcionamiento. El suministro e instalación de los respectivos repuestos y la mano de obra debe ser en el sitio de la instalación. Esto lo debe realizar el fabricante o el contratista sin costo adicional para la entidad	Si.
1.4.3	A partir de la entrega del producto y recibo a satisfacción por parte del supervisor designado por la Alcaldía de Puerto López, el fabricante responderá solidariamente por el término de un (1) año, por el buen estado del producto y la conformidad del mismo con las condiciones de idoneidad, calidad, funcionamiento, y seguridad legalmente exigible y ofrecidas, sin costo adicional al precio del producto. Para restablecer la responsabilidad por incumplimiento a las condiciones de idoneidad y calidad, bastará con que la Alcaldía de Puerto López demuestre el defecto del producto, salvo que tengan como causa: (I) fuerza mayor o caso fortuito; (II) hecho de un tercero; (III) uso indebido; (IV) fallas en la instalación cuando no sea contratada con el fabricante; y (V) fallas o falta de mantenimiento preventivo cuando no sea asumido por el fabricante o contratista. En estos casos corresponde al fabricante que aleguen la causal exoneración, demostrar el nexo causal entre esta y el defecto del bien. Las fallas en la instalación, uso o mantenimiento no podrán ser alegadas por el fabricante, si en la entrega del bien no hacen entrega a la Alcaldía de Puerto López del manual de instrucciones de instalación, uso y mantenimiento en idioma castellano o inglés.	Si.

1.4.4	El término de la garantía legal de calidad se suspenderá mientras la Alcaldía de Puerto López están privadas del uso del bien, con ocasión de la efectividad de la garantía. Si se produce el cambio total del producto por otro, el término de la garantía empezará a correr nuevamente en su totalidad desde el momento de reposición. Si se cambia una o varias piezas o partes del bien, están estas tendrán garantía propia.	Si.
1.4.5	La garantía y soporte de software debe ser con un tiempo de respuesta de 4 horas con disponibilidad de atención en modalidad 9x5 y NBD en sitio	Si.
1.4.6	La garantía y soporte de hardware debe ser con un tiempo de respuesta de 4 horas con disponibilidad de atención en modalidad 9x5 y NBD en sitio	Si.
1.4.7	Una vez instalada la solución, el contratista debe allegar los documentos emitidos por el fabricante de la solución ofertada que acreditan y describen el alcance de los servicios de soporte en la modalidad solicitada en el presente anexo técnico, fecha de inicio y fecha de finalización e inventario de los bienes cubiertos por el servicio tanto de hardware como de software.	Si.
	Nota: renovación de licenciamiento de antivirus corporativo.	
2.1	**Cantidad**	Ciento setenta (170).
2.2	**CARACTERÍSTICAS GENERALES**	
2.2.1	Tiempo de licenciamiento	Un (1) año
2.2.2	Arquitectura	64bits
2.2.3	Funcionalidades	Antimalware y análisis en tiempo real Análisis de comportamiento (Behavior Monitoring) Machine Learning (pre-ejecución y en tiempo de ejecución Protección de red (Host-based) Prevención de intrusiones (IPS a nivel de sistema operativo) Web Reputation Bloqueo de Command & Control (C&C) Control de dispositivos Control de aplicaciones Prevención de pérdida de datos (DLP) Administración y gestión web remota Telemetría de eventos Puertos y servicios analizados TCP 445 (SMB), TCP 139 (NetBIOS Session), UDP 137–138 (NetBIOS), TCP 2049 (NFS), TCP 135 (RPC), TCP 111 (RPCBind), TCP 3389 (RDP), TCP 22 (SSH), TCP 5900–5901 (VNC), TCP 5985, TCP 5986, TCP 80 (HTTP), TCP 443 (HTTPS), TCP 8080, TCP 8443, TCP 25 (SMTP), TCP 465 (SMTPS), TCP 587 (SMTP Submission), TCP 110 (POP3), TCP 995 (POP3S), TCP 143 (IMAP), TCP 993 (IMAPS), TCP 21 (FTP), TCP 989–990 (FTPS), UDP 69 (TFTP), TCP 389 (LDAP), UDP 389 (LDAP), TCP 636 (LDAPS), TCP 88 (Kerberos), TCP 464 (Kerberos password change), UDP 53 (DNS), TCP 53 (DNS), UDP 5353 (mDNS), UDP 1900 (SSDP), TCP 1433 (MS SQL), TCP 3306 (MySQL), TCP 5432 (PostgreSQL), TCP 1521 (Oracle)
2.2.4	La solución de protección de Antimalware se debe poder desplegar 100% en Nube y debe permitir como mínimo las características de Antimalware, Control de Aplicaciones y de dispositivos, protección avanzada contra Ransomware, mitigación de vulnerabilidades a través de parches virtuales y protección de fuga de información a través de expresiones regulares, diccionarios y características de los archivos.	Si.
2.2.5	La solución de protección Antimalware debe permitir la implementación de protección antimalware, control de aplicaciones, control de dispositivos, prevención de fuga de información, protección web, mitigación de vulnerabilidades a través de parches virtuales en un solo agente.	Si.
2.2.6	La solución debe permitir hacer backup y restauración automática de archivos ante intentos de cifrado no autorizados, con el fin de generar una protección proactiva contra Ransomware.	Si.
2.2.7	La solución debe tener la capacidad de brindar protección contra malware, virus de red, conexiones sospechosas, amenazas web, spyware, análisis de archivos adjunto de correo POP3, monitoreo de comportamiento, ataques combinados y ataques de día cero para equipos de punto final (Endpoint).	Si.
2.2.8	La solución debe contar con firewall (reglas de conexiones de aplicación, IP, puerto y protocolo), reputación de archivos y/o reputación web, que permita la creación de políticas a través de aplicaciones, aplicaciones específicas, llaves de registro de aplicaciones y estas se podrán aplicar a través de UDP, TCP y ICMP con puertos y direcciones IP definidas según las necesidades.	Si.
2.2.9	La solución debe tener la capacidad de aislar los equipos o ponerlos en cuarentena cuando se detecta algún ataque para evitar la propagación del mismo dentro de la red.	Si.

2.2.10	La solución debe bloquear procesos comúnmente asociados a Ransomware y debe finalizar los programas que muestren un comportamiento anormal asociado con ataques de explotación	Si.
2.2.11	La solución debe tener un módulo de monitoreo de eventos que permita monitorear permitir, denegar y preguntar cuando sea posible cambios en los archivos host de las maquinas, nuevos servicios, modificación de archivos de sistema, modificación de la política de seguridad entre otros	Si.
2.2.12	La consola de administración debe tener un módulo de Monitoreo de comportamiento, reputación web, conexiones sospechosas, protección de vulnerabilidades, control de dispositivos y control de aplicaciones	Si.
2.2.13	La solución debe tener la capacidad de analizar la reputación de archivos y recuperarlos cuando sean enviados a cuarentena. Además, debe permitir realizar escaneos de los Endpoint de forma manual, programada y en tiempo real.	Si.
2.2.14	La solución debe permitir la configuración de los tipos de eventos que serán notificados y visualizados en el agente, y adicionalmente configurar el mensaje de las alertas dependiendo de la criticidad del evento (High, Medium, Low), además se debe tener la capacidad de eliminar de los logs de los eventos del sistema, servidor y agentes con una frecuencia especifica.	Si.
2.2.15	La solución de protección de endpoints debe permitir crear políticas de protección y descubrimiento de información confidencial a través de DLP en el mismo agente de protección de malware para agentes internos y externos las cuales permitirán bloquear la fuga de información a través de clientes de correo, ftp, http, https, mensajería instantánea, web mails, protocolo SMB, impresiones, dispositivos removibles, Windows clipboard y servicios de almacenamiento cloud. Todo esto se debe hacer sobre el mismo agente de protección de Endpoints, device control y reputación web.	Si.
2.2.16	La solución debe permitir crear identificadores de datos a través de palabras claves, atributos de archivos y expresiones regulares; además la solución debe permitir probar las expresiones regulares directamente en la plataforma.	Si.
2.2.17	Los templates de DLP de la solución deberán permitir definir la severidad de alto, medio, bajo como mínimo	Si.
2.2.18	La solución deberá permitir tener políticas de control de aplicaciones en el mismo agente de DLP, control de dispositivos, XDR y protección de Endpoints, donde se puedan crear políticas para permitir las aplicaciones o bloquearlas y también debe permitir un modo de evaluación	Si.
2.2.19	El control de aplicaciones debe permitir, bloquear o importar aplicaciones para la configuración de las políticas y deberá tener por defecto como mínimo las siguientes categorías de aplicaciones: Browsers y herramientas de browser, mensajería instantánea, productividad, P2P, cifrado, aplicaciones altamente riesgosas y en esta última como mínimo debe tener la posibilidad de bloquear key loggers, Crackers de contraseñas y proxys anónimos.	Si.
2.2.20	El control de aplicaciones de la solución debe tener un score de las aplicaciones basado en popularidad y reputación y deberá tener un campo del uso global de la aplicación.	Si.
2.2.21	La solución de protección de endpoints debe permitir tener un módulo de control de dispositivos que permita aplicar políticas a agentes internos y externos teniendo en cuenta si la maquina esta fuera o dentro de la red interna. El módulo de control de dispositivos debe como mínimo permitir los siguientes dispositivos: Floppys, CD/DVD, unidades de red, unidades de almacenamiento USB, adaptadores bluetooth, dispositivos de imagen, dispositivos infrarrojos, módems, NICs Wireless y debe permitir bloquear la tecla Print Screen para optimizar los niveles de protección	Si.
2.2.22	EL módulo de control de dispositivos debe permitir tener un listado de USB permitidas y de aplicaciones permitidas para que interactúen con dispositivos bloqueados. Además, debe tener la opción de bloquear la función AutoRun en dispositivos de almacenamiento USB	Si.
2.2.23	La solución debe permitir tener reglas de prevención de intrusos de host y debe mostrar como mínimo el identificador, el nombre de la regla, el tipo de aplicación, la severidad, el tipo, el CVE al que está asociado la regla, la última actualización y estas reglas se deben poder aplicar en modo detección y prevención.	Si.

2.2.24	La Consola debe permitir para los servidores proporcionar monitoreo continuo para visibilidad instantánea y completa del entorno, notificaciones en tiempo real de las actividades y eventos que ocurran; permitir la generación de reportes customizables y desde el mismo dashboard de la consola de la solución poder administrar entornos físicos, virtuales y en la nube	Si.
2.2.25	La solución deberá detectar automáticamente nuevos servidores en los diferentes sistemas de infraestructuras de servidores públicas y privadas en vCenter, AWS, Microsoft Azure, vCloud Air, Directorio Activo	Si.
2.2.26	Propuesta llave en mano.	Si.
2.2.27	La solución de be ser completamente compatible con la solución actual de la entidad. (Trend Vision One Endpoint Security - Essentials)	Si.
2.3	**CONSOLA DE ADMINISTRACION**	
2.3.1	La consola de administración debe 100% cloud y debe permitir la protección de Endpoints y servidores	Si.
2.3.2	La solución debe permitir la creación, modificación y eliminación de roles y usuarios para la administración de la misma.	Si.
2.3.3	La consola de administración debe permitir administrar los agentes instalados en la red de equipos. Permitiendo conocer el estado de los agentes.	Si.
2.3.4	La consola de administración debe estar en la Nube para garantizar la administración en todo el tiempo sin importar el lugar donde estén las maquinas administradas.	Si.
2.3.5	La consola de administración debe permitir agrupar los agentes en grupos para facilitar la configuración y administración de los mismos.	Si.
2.3.6	La consola de administración debe permitir configurar notificaciones sobre riesgos de seguridad y ver los Logs enviados por los agentes sobre los eventos de los mismos.	Si.
2.3.7	La consola de administración debe proporcionar un Dashboard que brinde información global sobre los agentes, eventos de reputación web, usuarios afectados, eventos de comando y control, incidentes de filtración de datos, entre otros e igualmente debe permitir que secciones o widgets sean agregados o eliminados según se requiera.	Si.
2.3.8	La consola de administración debe permitir consultar los Logs de instalación tanto del agente como el del servidor de administración.	Si.
2.3.9	La consola de administración debe permitir visualizar estadísticas de históricos de actualizaciones de patrones de análisis de antivirus, antispyware, análisis de comportamiento, conexiones sospechosas, y exploits de los navegadores de internet.	Si.
2.3.10	La consola de administración debe permitir visualizar los logs de los eventos sobre los equipos donde se encuentra instalado el agente, dichos eventos deben estar relacionados a temas de malware, spyware, Reputación web, conexiones sospechosas, archivos sospechosos, Command & Control Callbacks, Behavior Monitoring, Machine Learning, control de dispositivos, DLP, y escaneos. Adicionalmente la solución debe permitir filtrar dichos logs por periodos de tiempo preestablecidos, por rangos de fechas y por tipo de escaneo.	Si.
2.3.11	La consola de administración debe permitir la visualización de los logs de registro de los eventos de actualización de servidor de actualizaciones.	Si.
2.3.12	La consola de administración debe permitir la visualización de los logs de registro de los eventos del servidor de administraciones.	Si.
2.3.13	La consola de administración debe tener la capacidad de generar reporte en formato PDF, DOCX y XLSX y también en formato PDF protegidos con contraseña para los reportes de los servidores	Si.
2.3.14	La consola de administración debe permitir visualizar a través de un DashBoard el riesgo corporativo donde se muestre el score de riesgo de la entidad y este debe ser calculado como mínimo con ocho ítems como las cuentas comprometidas, vulnerabilidades, actividad y comportamientos, detecciones de amenazas, configuraciones de seguridad entre otras.	Si.
2.3.15	La plataforma debe mostrar listado de dispositivos descubiertos, dispositivos con agentes administrados y esto se debe poder filtrar por mes	Si.
2.3.16	La solución debe tener un DashBoard donde se vea una descripción general de exposición, ataques y configuraciones de seguridad.	Si.
2.4	**AGENTES**	

2.4.1	Los agentes deben ser instalados mediante instalación web, link de instalación por correo, instalación por script, instalación remota, y/o paquete de instalación.	Si.
2.4.2	Los agentes deben requerir contraseña de administración para ser desinstalados de los equipos.	Si.
2.4.3	Las políticas de seguridad deben aplicarse en los agentes de forma individual y/o por grupos.	Si.
2.4.4	El agente debe tener la capacidad de eliminar los archivos sospechosos de forma automática.	Si.
2.4.5	La solución debe usar solo un agente para los endpoints para realizar la protección antimalware, parcheo virtual, DLP, control de aplicaciones y EDR.	Si.
2.4.6	Los agentes de EPP deben poder instalarse en sistemas operativos Windows desde Windows 2003 y deben soportar más de 2000 kernels de LinuX	Si.
2.4.7	El agente de protección no debe requerir reinicio en servidores para garantizar la disponibilidad de los servicios.	Si.
2.4.8	Los agentes deben tener la capacidad de conectarse a múltiples fuentes de actualización (patrones, firmas, url sospechosas, etc.), si alguna de estas es inaccesible para el agente.	Si.
2.5	**XDR**	
2.5.1	La solución debe permitir la detección de amenazas tipo Fileless a través de la exploración de memoria mejorada para detectar comportamientos de procesos sospechosos. El agente debe tener la capacidad de terminar los procesos sospechosos antes de que se pueda hacer cualquier daño.	Si.
2.5.2	La solución debe permitir evaluar el alcance del daño causado por un ataque dirigido, proporcionar información sobre la llegada y progresión del ataque y ayudar en la planificación de una respuesta efectiva a incidentes de seguridad.	Si.
2.5.3	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.	Si.
2.5.4	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 y procesos en curso. Además, debe permitir la integración con información externa de IoC (Indicators Of Compromises) como reglas STIX, TAXII	Si.
2.5.5	La solución debe permitir el análisis de comportamiento de un malware, actividades específicas de IoC y conexiones de comando a control.	Si.
2.5.6	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.	Si.
2.5.7	La solución debe escanear documentos en busca de códigos de exploits integrados y vulnerabilidades conocidas y controlar los programas que demuestran un comportamiento anormal asociado con ataques de exploits.	Si.
2.5.8	La solución debe analizar los archivos desconocidos de baja prevalencia utilizando algoritmos de aprendizaje automático para determinar si el archivo es malicioso y debe ser capaz de recopilar datos y barrido del sensor en los endpoints (IOC) y almacenarlos de forma centralizada para su posterior análisis.	Si.
2.5.9	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.	Si.
2.5.10	La solución debe tener la capacidad de identificar amenazas aun cuando usen PowerShell codificado y debe detectar tareas programadas maliciosas además se debe mostrar todos los dispositivos en los que un proceso principal (padre) inicia otros procesos (hijos) especialmente de tipo PowerShell y cmd.	Si.
2.5.11	La solución debe contar con la capacidad de mostrar la línea de tiempo de incidentes y mostrar en una sola vista todo el ciclo de vida del ataque de la amenaza y debe revelar la cadena completa de procesos afectados por el malware/comportamiento malicioso.	Si.
2.5.12	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	Si.
2.5.13	La solución de EDR no debe requerir un agente adicional a los agentes de Endpoint Protection instalados en las máquinas de la compañía y debe permitir la correlación entre, endpoints y servidores en la misma consola unificada.	Si.

2.5.14	XDR debe contar con modelos de detección avanzados que detectan actividades de bajo perfil en distintas capas de seguridad para encontrar nuevos ataques y estos deben tener la posibilidad de encender y apagar modelos según la tolerancia al riesgo y preferencias de la entidad.	Si.
2.5.15	Los modelos de correlación deben combinar múltiples reglas y filtros usando una variedad de técnicas de análisis como, pero no limitándose, a Data Stacking y Machine Learning.	Si.
2.5.16	XDR debe permitir entender la historia del ataque con una representación visual e interactiva de los eventos y estos gráficos deben mostrar una representación visual de los objetos que levantaron la alerta y la relación entre ellos.	Si.
2.5.17	Debe tener la capacidad de verificar el perfil de ejecución/análisis de causa raíz (Execution Profile/Root Cause Analysis) para ver las accionas que una amenaza llevó a cabo en un servidor, Endpoint, o carga de trabajo en la nube.	Si.
2.5.18	Debe permitir la búsqueda proactiva a través de Endpoint y servidores (como telemetría, NetFlow, meta data, etc.) usando un simple constructor de consultas sobre una consola unificada.	Si.
2.5.19	La solución debe permitir hacer un barrido con IoC (indicadores de compromiso) o búsquedas personalizadas usando múltiples parámetros y filtrar los resultados añadiendo criterios adicionales de búsqueda, también debe detectar proactivamente con búsquedas automáticas de IoC publicados por el vendor	Si.
2.5.20	Desde el resultado de una búsqueda se debe poder ejecutar acciones de respuesta y generar un análisis de causa raíz, además las búsquedas deben permitir construir, guardar y reutilizar búsquedas para Threat Hunting básico.	Si.
2.5.21	La capacidad de Threat Intelligence embebida debe ser capaz de identificar la campana asociada, la Plataforma atacada, las Técnicas, Tácticas y Procedimientos (TTPs) alineadas a MITRE ATT&CK™ y debe proveer enlaces/links a entradas de blog relacionados si están disponibles.	Si.
2.5.22	En una sola ubicación debe poder ver el estado de respuestas en Endpoint y servidores y con mínimo debe mostrar la siguiente información: identificador de la tarea ejecutada, acción, objetivo, usuario que la creo, desde donde fue creada y fecha de la última actualización. Además, la solución debe permitir la creación de scripts personalizados en (power Shell script) .ps1 y (bash Script) .sh	Si.
2.5.23	Debe permitir ejecutar acciones de respuesta rápidamente haciendo clic derecho en el incidente y desde los resultados de búsqueda de Threat Intelligence. Las respuestas como mínimo deben ser: aislar un Endpoint, ejecutar un script personalizado, iniciar un Shell remoto, adicionar a una lista negra, entre otros.	Si.
2.5.24	La solución debe exponer una API pública debe poder ser usada por clientes para integrarse con SIEM y herramientas SOAR y debe permitir obtener un listado con los detalles de los Endpoints, obtener un listado de alertas con sus detalles y modificar su estado, adicionar y remover objetos sospechosos de una lista negra, eliminar entre otras.	Si.
2.5.25	Las alertas deben permitir ver un análisis de causa raíz para identificar el alcance del impacto y permitir tomar acciones de respuesta.	Si.
2.5.26	Debe priorizar las alertas y llevar registro de lo que se ha hecho y la fase de la alerta (nuevo, en progreso, finalizado/cerrado)	Si.
2.5.27	La solución de XDR debe mostrar un score del riesgo corporativo y se debe integrar como mínimo con las soluciones de firewall de Checkpoint, Palo Alto y Fortinet y debe permitir integrar fuentes de terceros como TAXII y MISP, y permitir la integración como mínimo con 25 fabricantes dentro de los que deben estar AWS, AttackIQ, Cymulate, Elastic, Okta, Microsoft, NetSkope, OpenLDAP, Picus, Qualys, Securonix, ServiceNow, Splunk, Tanium, Tenable y VMware, también debe proveer un conector para Splunk nativo.	Si.
2.5.28	La solución de XDR debe permitir de manera automática enviar correos a cuarentena, eliminar correos, hacer una recolección de archivos, basados en la severidad de los incidentes encontrados en correo	Si.
2.5.29	La solución de protección de correo y XDR debe permitir seleccionar los grupos y usuarios a los que se les quiere activar la protección y sensor de XDR	Si.
3.1	Cantidad	Dieciocho (18).

3.2	Estación de trabajo corporativo	Procesador: i5-14500. Memoria interna: 16 GB, Tipo de memoria interna: DDR5-SDRAM. Capacidad total de almacenaje: 512 GB, Unidad de almacenamiento: SSD. Modelo de adaptador gráfico incorporado: Intel UHD Graphics 770. Conectividad LAN 10/100/1000 y Wifi-6 dual band 2.4Ghz y 5.0Ghz. Tarjeta de sonido integrada con jack 3.5mm. Parlante integrado. Fuente de alimentación: 180 W. Tipo de chasis: Slim PC. Monitor LCD de 23,8". Mouse óptico y Teclado alámbrico de conexión USB. Factor de forma SFF -Small Form Factor. El equipo debe contar con antivirus estándar. Garantía 1 año.
3.3	Sistema Operativo	Licenciamiento para Windows 11 Pro OEM (Instalado en fabrica) de 64 bits última versión en español para ambiente corporativo PC de escritorio, los equipos a entregar deberán tener instalado y funcionando el sistema operativo.
3.4	Instalación, configuración y entrega	Instalación en sitio (municipio de Puerto López), configuración básica para inicio de sesión. Incluye backup de otro equipo de ser requerido.
3.5	Garantía y Soporte	Garantía: un (1) año contra defectos de fabricación, a partir del acta de recibido a satisfacción por parte del supervisor del contrato, sin que esto genere costo alguno.
[illegible]		
4.1	Cantidad	Treinta y cuatro (34).
4.2	Office 365	Office 365 personal, suscripción por 1 año, contiene Word, Excel, PowerPoint, Outlook, one drive, microsoft teams.
4.3	Instalación	Instalación, configuración licencia de office 365.
[illegible]		
5.1	Cantidad	Quince (15).
5.2	Escritorio estudiantil	Escritorio con estructura metálica con superficie de madera, medidas: 1,10 mt de largo por 0,55 mt de ancho. El escritorio se debe instalar totalmente armado.
5.3	Silla para escritorio estudiantil	Silla tipo kinder: Diseñada para entornos educativos, resistente, estructura metálica y asiento ergonómico en polipropileno de alto impacto. Características principales: Estructura en tubo redondo de 7/8" calibre 18 con terminación en pintura en polvo horneable de aplicación electrostática color gris nube. Asiento y espaldar en polipropileno de alto impacto con diseño ergonómico que favorece la postura infantil. Tapones en polipropileno para proteger el suelo
5.4	Instalación de mobiliario para equipos de cómputo	El mobiliario se debe instalar en 3 filas de a 5 puestos de trabajo, cada puesto debe contar con energía como toma eléctrica Ac 110v tipo radwell anclada al piso y un regulador de voltaje apto para equipos de cómputo.
[illegible]		
6.1	Cantidad	Dieciocho (18).
6.2	UPS interactiva para equipo de cómputo	UPS 600VA UPS Interactiva, Potencia 360W, 4 Tomas de Corriente, Nivel de Regulación +/- 10%, Factor de Potencia 0.6, Entrada de 110VAC, Onda Sinusoidal Modificada, Tiempo de Respuesta de 3 a 10 Milisegundos, Recarga en 8 Horas al 90% de capacidad. Garantía 1 Año.
6.3	Instalación	Instalación, configuración en sitio.
6.4	Garantía	Un (1) año.
[illegible]		
7.1	Cantidad	Uno (1).
7.2	Video Proyector	Proyector Tecnología 3LCD, Resolución XGA 1024 x 768, Brillo 3400 Lúmenes, Método de Proyección: Frontal / Posterior / Techo, Relación de Aspecto: 4:3 / 16:9, Relación de Contraste: Hasta 15.000:1, Tipo de Lámpara: 210W UHE, Vida Útil de la Lámpara: Modo ECO hasta 12.000 horas, Modo Normal hasta 6.000 horas, Distancia Proyectada: Desde 0.76 hasta 8.89 mts, Puertos (Ethernet, USB, HDMI, VGA, RS-232, Audio), Altavoces Internos: 1x 5W, Plug & Play, Compatible Windows & Mac, Seguridad: Kensington Lock. Garantía 1 Año.
7.3	Garantía	Un (1) año.
[illegible]		
8.1	Cantidad	Uno (1).
8.2	Capacidad	24.000 BTU
8.3	Tecnología enfriamiento	Inverter y/o equivalente
8.4	Unidad interior	Filtro doble protección Limpieza automática Rápido enfriamiento Control remoto que indique temperatura y configuración Comfort Sleep Control de persiana Nivel de ruido H < 50 db Deshumificación
8.5	Evaporadora (Unidad interna)	Split
8.6	Unidad exterior	Inverter y/o equivalente Motor sin escobillas Recubrimiento anticorrosión Control de carga inteligente Control de pico de corriente Enfriamiento y rápida calefacción

8.7	Refrigerante	Ecológico R32
8.8	Características	Suministro eléctrico 220 V / 60Hz
8.9	Año De Fabricación	2023 o superior
8.10	Instalación	El oferente se compromete, a entregar instalado y funcionando el aire incluido en el presente proceso, de acuerdo a las normas establecidas; así mismo se deben realizar: Acometida eléctrica máximo 30 metros aproximado del tablero normal más cercano, protecciones, gas refrigerante y las adecuaciones y obras civiles necesarias en el área asignada para su implementación, garantizando la armonía con lo existente a costas del contratista para garantizar el buen funcionamiento del equipo. Si la acometida supera los 30 metros de distancia, el contratista deberá realizar los cálculos de regulación y compensación de acometidas de acuerdo a la norma técnica colombiana NTC 2050 última actualización y reglamento técnico de instalaciones eléctricas última actualización. Deberá proveer la tubería en cobre máximo 25 metros. También debe suministrar la protección bifásica adecuada para él equipo. Diferencia máxima en altura 15 metros. En los lugares que por carga eléctrica la acometida existente no soporte la potencia de los aires a instalar, se deberá instalar acometida eléctrica de acuerdo a la necesidad junto con su tablero eléctrico alimentado desde el circuito más cercano diseñada y calculada a la potencia del equipo, lo cual estará a cargo del contratista, sin generar costo para la entidad contratante.
8.11	Montaje Y Puesta En Marcha	El Contratista deberá entregar el equipo en operación, siendo a su cargo la totalidad del montaje, incluyendo el diseño, suministro e instalación de todos los materiales, implementos y accesorios necesarios para una correcta operación. El montaje o instalación de los equipos comprende el suministro de la totalidad de materiales, insumos y ejecución de todos los trabajos para una correcta instalación y puesta en marcha a entera satisfacción de la Entidad. Todos los materiales y equipos suministrados serán nuevos, de la mejor calidad, libres de defectos e imperfecciones. Todos aquellos componentes que no se indiquen expresamente aquí, pero que sean necesarios dentro del propósito del contrato, deberán ser suministrados, instalados adecuadamente y dejarlos listos para operación continua. Todos los materiales cuya instalación esté prevista para la intemperie deberán incorporar todas las medidas razonables que prevengan la absorción de humedad y su condensación sobre partes metálicas ó superficies aislantes. Todas las rutas para la instalación (Tubería metálica, conduits, canaletas, cajas, entre otros) deberán ser presentadas para aprobación por parte del supervisor del contrato. El contratista, al final de cada jornada de trabajo deberá dejar limpia el área de todo material extraño a fin de prevenir posibles daños o accidentes en las personas o vehículos en circulación que puedan transitar por las áreas de trabajo. Al finalizar el montaje y previo al recibo a satisfacción, el contratista deberá hacer una limpieza general a total de las zonas objeto de intervención.
8.12	Protección	Breaker de protección mínimo de 2X20 A.
8.13	Responsabilidad	El Contratista será el responsable de los daños y/o fallas que se ocasionen a equipos, redes, obras civiles internas o externas y espacio público. En caso de que estas se presenten, se restablecerán al estado original y los costos involucrados en la misma, al igual que sanciones o multas serán responsabilidad del contratista.
8.14	Imprevisto	Si durante la instalación del aire se encuentra que no se incluyeron elementos, documentación o servicios indispensables para el correcto funcionamiento. El contratista deberá incluirlo, suministrarlo, instalarlo y ponerlo en funcionamiento sin costo adicional para la Entidad contratante, el hecho que se detecten errores u omisiones en estos términos de referencia, pliegos o especificaciones técnicas, no libera al contratista a ejecutar satisfactoriamente el objeto del contrato en las fechas estipuladas para su ejecución.

8.15	Otros requerimientos de instalación	El trabajo a realizar comprende, el suministro de la totalidad de los materiales necesarios, la mano de obra, la dirección técnica, y el suministro de herramientas y equipos para llevar a cabo el proyecto completo y referidos en las cantidades. El Contratista deberá mantener en sitio el personal profesional, técnico o tecnólogo, idóneo y necesario para el correcto desarrollo de los trabajos en cada una de las etapas de ejecución del contrato. La ejecución de los trabajos incluye la prueba, ajuste y puesta en servicio de la totalidad de los equipos. Cuando por descuido, imprevisión, negligencia, o causas imputables al Contratista ocurriesen daños a terceros, éste será el directo responsable de ellos. Las obras menores que se requieran realizar como consecuencia de la instalación de los equipos, entre las cuales se encuentran, regatas, pasos en muros o placas, resane y pintura de muros, entre otros, serán responsabilidad del contratista, por lo cual los costos asociados a las mismas correrán por cuenta del mismo, garantizando la correcta instalación y buen funcionamiento de los bienes a suministrar, así como el cuidado y entrega en buen estado del inmueble. El Contratista se responsabilizará por la protección y conservación de los bienes hasta la entrega y recibo en forma definitiva por el supervisor del contrato. La reparación de daños, si los hubiera, correrá por cuenta del Contratista y se harán a satisfacción de la supervisión. Tan pronto se haya terminado la instalación de los equipos objeto del contrato y antes de que se efectúe el recibo final del mismo, el contratista deberá por su cuenta y riesgo, retirar los materiales sobrantes, dejando las zonas intervenidas en buen estado y completamente limpias
8.16	Garantías	Dos (2) años para partes. Diez (10) años en compresor Los equipos suministrados, contaran con una garantía de buena calidad y buen funcionamiento, por un mínimo de DOS (2) AÑOS para todos los componentes contados a partir de la fecha de recibo de los equipos por parte de la entidad, la cual debe ser respaldada por el fabricante o distribuidor autorizado de los equipos ofertados. Durante el tiempo de garantía, los elementos que resulten defectuosos deberán ser remplazados por nuevos y libres de imperfecciones, sin costo adicional, en un término no superior a diez (10) días hábiles contados a partir del reporte del supervisor del contrato. El contratista debe elaborar y hacer entrega de los reportes técnicos realizados al bien o bienes dentro del periodo de garantía y mantenimiento.
9.1	Cantidad	Dieciséis (16).
9.2	Estación de trabajo - Pc Portatil	Procesador: Intel Core i5 series 1 120U. Memoria RAM: 16GB DDR4, Almacenamiento: 512GB SSD. Pantalla: LCD 15,6" (Full HD 1920 x 1080) Anti-Reflejo. Conectividad LAN 10/100/1000, Wifi-6 dual band 2.4Ghz y 5.0Ghz y Bluetooth 5.3. Tarjeta de sonido integrada con jack 3.5mm. Cámara HD 720P, micrófono y parlante integrados. Puerto HDMI, 2 puertos USB, 1 puerto USB tipo C. Mouse Touchpad integrado 2 botones y gestos. Teclado integrado. Sistema Operativo: Windows 11 Home x64. Debe incluir antivirus estándar.
9.3	Backpack - Accesorio	Backpack urbana para equipo portátil de 15,6".
9.4	Instalación	Instalación en sitio (municipio de Puerto López), configuración básica para inicio de sesión. Incluye backup de otro equipo de ser requerido
9.5	Garantía y Soporte	Garantía en sitio de 1 año.
10.1	Cantidad	Uno (1).
10.2	Estación de trabajo - Computador corporativo Todo en Uno (AIO)	Línea Corporativa Empresarial, Procesador Intel Core I7 -13620H, Disco Duro SSD de 1TB, Memoria Ram DDR5 de 32Gb. Pantalla LCD de 23.8" 1920x1080 full HD, HDMI. Conectividad LAN 10/100/1000, Wifi-6 dual band 2.4Ghz y 5.0Ghz y Bluetooth 5.3. Tarjeta de video Intel UHD Graphics. Tarjeta de sonido integrada con jack 3.5mm. Cámara, micrófono y parlante integrados. Factor de forma AIO -Todo en Uno. Mouse óptico y Teclado alámbrico de conexión USB. Antivirus estándar.
10.3	Sistema Operativo	Licenciamiento para Windows 11 Pro OEM (Instalado en fabrica) de 64 bits última versión en español para ambiente corporativo PC de escritorio, los equipos a entregar deberán tener instalado y funcionando el sistema operativo.
10.4	Instalación, configuración y entrega	Instalación en sitio (municipio de Puerto López), configuración básica para inicio de sesión. Incluye backup de otro equipo de ser requerido.
10.5	Garantía y Soporte	Garantía de tres (03) años contra defectos de fabricación, a partir del acta de recibido a satisfacción por parte del supervisor del contrato, sin que esto genere costo alguno.
11.1	Cantidad	Dos (2).

11.2	Estación de trabajo - Pc Portátil trabajo especial	Procesador Intel Core i5 – 210H (8 núcleos, hasta 4,8GHz de frecuencia turbo). Disco Duro SSD de 1Tb, Memoria Ram DDR5 de 32Gb, Pantalla LCD de 16" (Full HD 1920x1080) WUXGA tasa de refresco de 144HZ, Tarjeta de video RTX4050 de 6GB de memoria GDDR6, Conectividad LAN 10/100/1000, Wifi-6 dual band 2.4Ghz y 5.0Ghz y Bluetooth 5.3, Puerto HDMI, 1 puerto USB, 1 puerto USB tipo C. Cámara HD 720P, micrófono y parlante integrados. Mouse Touchpad integrado 2 botones y gestos. Teclado retroiluminado integrado. Sistema operativo Windows 11 Pro x64. Debe incluir antivirus estándar. Garantía 1 año. (Nota: Se admiten equipos de líneas no corporativas tales como Alto Rendimiento, Creación de Contenido, Workstation o Gaming, nuevos de fábrica y de marcas reconocidas).
11.3	Instalación, configuración y entrega	Instalación en sitio (municipio de Puerto López), configuración básica para inicio de sesión. Incluye backup de otro equipo de ser requerido.
11.4	Garantía y Soporte	Garantía: un (01) año contra defectos de fabricación, a partir del acta de recibido a satisfacción por parte del supervisor del contrato, sin que esto genere costo alguno. Garantía a través del Centro de Servicio autorizado por la marca.
12.1	Cantidad	Tres (3).
12.2	Office Hogar y Empresas 2024	Microsoft Office Home & Business vitalicia versión 2024 edición de 64 bits. Con aplicaciones Word, Excel, PowerPoint, Outlook, Access, One note, One drive, Teams incluidas.
12.3	Instalación	Instalación en sitio, configuración Office Hogar y Empresas 2024
13.1	Cantidad	Uno (1).
13.2	Impresora laser monocromática	Impresora multifuncional láser monocromática, Memoria RAM: 1GB, Capacidad estándar: 250 hojas + bandeja multipropósito de 100 hojas, A4 copia, escaneo, impresión dúplex automática, Velocidad: 40 ppm (A4), Resolución: 1200 × 1200 dpi, Resolución de escaneo/copia: 600 × 600 dpi, Salida de papel: 150 hojas, 1 Bandeja principal y 1 bandeja ByPass, tamaños de papel A4, Carta, Legal, Oficio, 8/2x11, 8/2x13, Interfaces: USB 2.0 y Ethernet, Protocolos SMB, SMTP, HTTP y WSD, Garantía 1-Año.
13.3	Instalación	Instalación en sitio, configuración de impresora en sitio.
14.1	Cantidad	Tres (3).
14.2	Escaner de Alto Trabajo	Tipo camaplana, Tecnología CMOS-CIS, Memoria: 1 GB de SDRAM, Modo de alimentación de documentos: ADF, Resolución óptica (dpi): Hasta 600 dpi (color y monocromática, ADF); Hasta 1200 dpi (color y monocromática, cama plana), Velocidad de escaneo: 50 ppm, Formatos de archivo: PDF, JPG, JPEG, PNG, BMP, TIFF, PDF/A, Funcionalidades de Dúplex automático, eliminar páginas blancas, organizar páginas, eliminar paginas, Interfaz y conectividad Ethernet 10/100/1000 Base-T , USB 3.0, WiFi 802.11 b/g/n, WiFi Direct. Volumen diario recomendado: Hasta 8.000 hojas
14.3	Instalación y configuración	Se debe entregar instalado y configurado. Se debe entrenar al usuario en el manejo de este equipo.
14.4	Garantía	Uno (1) año.
15.1	Cantidad	Uno (1).
15.2	Estación de trabajo - Pc Corporativo Portátil	Linea Corporativa Empresarial Procesador Intel Core Ultra 5 Serie 2 225U. Memoria Ram 16GB DDR4. Disco 512GB SSD. Pantalla LCD de 14" (Full HD 1920 x 1080). Conectividad LAN 10/100/1000, Wifi-6 dual band 2.4Ghz y 5.0Ghz y Bluetooth 5.3. Tarjeta de sonido integrada con jack 3.5mm. Cámara HD 720P, micrófono y parlante integrados. Puerto HDMI, 1 puerto USB, 1 puerto USB tipo C. Mouse Touchpad integrado 2 botones y gestos. Teclado integrado. Sistema operativo Windows 11 Pro x64. Debe incluir antivirus estándar. Garantía 3 años
15.3	Instalación	Instalación en sitio (municipio de Puerto López), configuración básica para inicio de sesión. Incluye backup de otro equipo de ser requerido.
15.4	Garantía y Soporte	Garantía en sitio de 3 años (3,3,3), 3 años de garantía en partes, 3 años de garantía en mano de obra y 3 años en sitio
	Nota: este equipo se debe instalar en equipo en las instalaciones principales de la secretaría de Planeación.	
16.1	Cantidad	Dos (2).
16.2	**Características**	
16.2.1	Tipo	Tipo Domo fija IP
16.2.2	Lente	2,8 mm, campo de visión horizontal 96°, campo de visión vertical 52°, campo de visión diagonal 113° 4 mm, campo de visión horizontal 75°, campo de visión vertical 40°, campo de visión diagonal 89°
16.2.3	Iluminación mínima	Color: 0,001 Lux @(F1.0, AGC ON), 0 Lux con luz blanca
16.2.4	Sensor de imagen	CMOS de escaneo progresivo de 1/3"

16.2.5	Dori	2,8 mm, profundidad: 64,0 m, exterior: 25,4 m, derecha: 12,8 m, interior: 6,4 m 4 mm, profundidad: 77,4 m, exterior: 30,7 m, derecha: 15,5 m, interior: 7,7 m
16.2.6	Resolución máxima	4 MP - 2560 × 1440
16.2.7	Compresión de vídeo	Transmisión principal: H.265/H.264,
16.2.8	Interfaz Ethernet	1 puerto Ethernet autoadaptativo RJ45 10 M/100 M
16.2.9	Protocolos de red	Protocolos TCP/IP, ICMP, HTTP, HTTPS, FTP, DHCP, DNS, DDNS, RTP, RTSP, RTCP, NTP, UPnP, SMTP, IGMP, QoS, IPv6, Bonjour, IPv4, UDP, SSL/TLS
16.2.10	Fuente de alimentación	12 VCC ± 25 % PoE: 802.3af, Clase 3
16.2.11	IP67	Si.
16.3	Instalación y Configuración	Las cámaras deberán entregarse instaladas, cableadas, configuradas y en correcto funcionamiento como un Sistema integrado. Incluye todos los elementos de cableado, fijación, etc, necesarios para un óptimo funcionamiento e instalación. El cableado deberá ser UTP CAT6. Se debe incluir accesorios y canaletas plásticas o tubería necesaria.
16.4	Garantía y Soporte de fábrica	Un (1) año.