FICHAS TÉCNICAS EXIGIDAS

De acuerdo a las necesidades de equipos y herramientas de infraestructura tecnológica de la administración municipal, la Secretaría General ha identificado las siguientes especificaciones técnicas de los productos a suministrar:

Tabla 1 – Fichas Técnicas de los Equipos y Herramientas a Suministrar

ÍTEM	ELEMENTO	CANTIDAD	UNIDAD MEDIDA	DESCRIPCIÓN
1	LICENCIAMIENTO DE SOPORTE Y GARANTÍA DE FIREWALL FORTIGATE 100F	1	Unidad	Licenciamiento y soporte para firewall FortiGate 100F Características equipo a licenciar: 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. Firewall Throughput: 10 Gbps. Concurrent Sessions: 1,5 millones. Nuevas sesiones por segundo: Cuarenta y cinco mil (45,000). NGFW Throughput: 1 Gbps. Threat Protection: 900 Mbps. Interface gigabit ethernet RJ45: Seis (6). Dominios Virtuales: Diez (10). Puerto USB: Uno (1). Puerto de consola: Uno (1). Soporte IPV6/ IPv4: Si. Usuarios concurrentes VPN SSL: Doscientos (200). IPsec VPN Tunnels Client to Site: Dos mil quinientos (2,500). (RIPv1/v2): Si. OSPF: Si. SSL-VPN Throughput: 950 Mbps. El equipo Firewall debe tener dentro de su arquitectura procesador de propósito 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.

				El equipo Firewall debe tener dentro de su arquitectura procesador de propósito 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. 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). 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. 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).

				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 Inspeccion de contenido SSL/SSH La solución debe ser compatible totalmente con la solución actual de ciberseguridad perimetral. Propuesta Llave en Mano Servicios de Implementación de Firewall Configuración, instalación y puesta en funcionamiento de toda la solución tecnológica propuesta, en el centro de datos nivel central. El contratista dispondrá de un recurso humano en sitio (sede central: Cll. 6 #4-40, Puerto López, durante el plazo de ejecución del contrato. Propuesta Llave en Mano Soporte y asistencia técnica para firewall de Un (1) año. 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. Se deben incluir el acceso a soporte y actualizaciones de firmware y software para todos los elementos por parte del fabricante de los mismos La cobertura del servicio de mantenimiento correctivo debe ser 7x24 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. 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) 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. 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 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. 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. 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 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 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.
2	LICENCIA ANTIVIRUS CORPORATIVO	160	Unidad	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. 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. 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.

				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). 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. 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. La solución debe bloquear procesos comúnmente asociados a Ransomware y debe finalizar los programas que muestren un comportamiento anormal asociado con ataques de explotación 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 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 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. 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. 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. 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. Los templates de DLP de la solución deberán permitir definir la severidad de alto, medio, bajo como mínimo 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 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. 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. 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 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 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. 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 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 La consola de administración debe 100% cloud y debe permitir la protección de Endpoints y servidores La solución debe permitir la creación, modificación y eliminación de roles y usuarios para la administración de la misma. La consola de administración debe permitir administrar los agentes instalados en la red de equipos. Permitiendo conocer el estado de los agentes.

				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. La consola de administración debe permitir agrupar los agentes en grupos para facilitar la configuración y administración de los mismos. 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. 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. La consola de administración debe permitir consultar los Logs de instalación tanto del agente como el del servidor de administración. 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. 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. La consola de administración debe permitir la visualización de los logs de registro de los eventos de actualización del servidor de actualizaciones. La consola de administración debe permitir la visualización de los logs de registro de los eventos del servidor de administraciones. 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 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. La plataforma debe mostrar listado de dispositivos descubiertos, dispositivos con agentes administrados y esto se debe poder filtrar por mes La solución debe tener un DashBoard donde se vea una descripción general de exposición, ataques y configuraciones de seguridad. Los agentes deben ser instalados mediante instalación web, link de instalación por correo, instalación por script, instalación remota, y/o paquete de instalación. Los agentes deben requerir contraseña de administración para ser desinstalados de los equipos. Las políticas de seguridad deben aplicarse en los agentes de forma individual y/o por grupos. El agente debe tener la capacidad de eliminar los archivos sospechosos de forma automática. La solución debe usar solo un agente para los endpoints para realizar la protección antimalware, parcheo virtual, DLP, control de aplicaciones y EDR. Los agentes de EPP deben poder instalarse en sistemas operativos Windows desde Windows 2003 y deben soportar más de 2000 kernels de LinuX El agente de protección no debe requerir reinicio en servidores para garantizar la disponibilidad de los servicios. 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. XDR 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. 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. 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 y procesos en curso. Además, debe permitir la integración con información externa de IoC (Indicators Of Compromises) como reglas STIX, TAXII La solución debe permitir el análisis de comportamiento de un malware, actividades específicas 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 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. 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.

				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 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. 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. 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 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. 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. 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. 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. 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. 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. 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 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. 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. 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 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. 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. Las alertas deben permitir ver un análisis de causa raíz para identificar el alcance del impacto y permitir tomar acciones de respuesta. Debe priorizar las alertas y llevar registro de lo que se ha hecho y la fase de la alerta (nuevo, en progreso, finalizado/cerrado) 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. 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 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 Instalación Propuesta llave en mano.
3	COMPUTADOR CORPORATIVO DE ESCRITORIO	27	Unidad	Línea Corporativa Empresarial, Caja SFF, Procesador Intel Core I5 -13500 treceava Generación, Disco Duro SSD de 512 GB, Memoria Ram DDR4 de 8 GB, grabadora de DVD, tarjeta integrada de video, 2 USB 3.2, 2 USB 2.0, Monitor de 23.8" 1600x900 @ 60Hz con puerto HDMI, 1 puerto DisplayPort, tarjeta lan inalámbrica, puerto ethernet 10/100/1000, teclado USB, mouse óptico USB, Windows 11 Professional. El equipo debe tener las siguientes certificaciones: Energy Star para el uso eficiente de energía, Certificacion EPEAT, RoHS para el manejo de sustancias peligrosas. Nota: para este requerimiento se acepta certificación expedida por el fabricante o link de página oficial del fabricante donde se verifique el cumplimiento.

				Instalación, configuración en red y puesta en funcionamiento a todo costo de computadores de escritorio con copia de backup de información 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
4	COMPUTADOR CORPORATIVO PORTÁTIL	16	Unidad	Línea Corporativa Empresarial, Procesador Intel Core I5 -1335 Treceava Generación, Disco Duro SSD de 512 GB, Memoria Ram DDR4 de 8 GB, 3 USB 3.1, 1 USB 2.0, Pantalla de 15" 1920x1080 @ 60Hz con puerto HDMI, tarjeta lan inalámbrica, puerto ethernet 10/100/1000, Windows 11 Professional. El equipo debe tener las siguientes certificaciones:Energy Star para el uso eficiente de energía, el fabricante debe ser miembro de la TCG (Trusted Computing Group). Nota: para este requerimiento se acepta certificación expedida por el fabricante o link de página oficial del fabricante donde se verifique el cumplimiento. Instalación, configuración en red y puesta en funcionamiento a todo costo de computadores de escritorio con copia de backup de información 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
5	COMPUTADOR CORPORATIVO TODO EN UNO	4	Unidad	Línea Corporativa Empresarial, Procesador Intel Core I7 -13700 Treceava Generación, Disco Duro SSD de 512 GB, Memoria Ram DDR4 de 16 GB, USB-A, USB-C, Monitor de 23.8" 1920x1080 full HD, puerto HDMI, DisplayPort, tarjeta lan inalámbrica, puerto ethernet 10/100/1000, cámara 5MP, Windows 11 Professional. El equipo debe tener las siguientes certificaciones: Energy Star para el uso eficiente de energía, Certificacion EPEAT , Nota: para este requerimiento se acepta certificación expedida por el fabricante o link de página oficial del fabricante donde se verifique el cumplimiento.

				Instalación, configuración en red y puesta en funcionamiento a todo costo de computadores de escritorio con copia de backup de información 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
6	LICENCIA OFFICE	26	Unidad	Office Home and Business 2021 All Lng PK Lic Online LatAm ONLY DwnLd NR Licencia ESD para maquina nueva o usada, transferible, no permite hacer down grade, Perpetua, 1 usuario 1 pc, perpetua, ofimática básica, Compatible con Windows 10/11 y MA Instalación, configuración licencia de office
7	LICENCIA CAL WINDOWS	2	Unidad	Licencia CAL por dispositivo Windows Server 2022 Instalación, configuración licencia.
8	LICENCIA ESCRITORIO REMOTO WINDOWS	2	Unidad	Oficina LTSC Estándar 2021 Software OneTime perpetuo Office LTSC Standard 2021 le brinda las herramientas esenciales para realizar el trabajo con versiones actualizadas de Word, Excel, PowerPoint, Outlook, Publisher (solo para PC) además de la aplicación de escritorio OneNote que se ejecuta en todas las versiones compatibles de Windows Instalación, configuración licencia.
9	LICENCIA WINDOWS 11 PROFESIONAL	6	Unidad	Windows 11 Profesional 64 Bit Espanish Latam (FQC-10553) Instalación, configuración licencia.
10	IMPRESORA TIPO 1 MULTIFUNCIONAL MEDIANA	10	Unidad	Impresora monocromática Multifuncional Laser Monocromática (B/N) WI-Fi, Formato A4, Funciones (Copiadora - Impresora - Escáner - Fax), Velocidad: Hasta 42ppm, Resolución: Hasta 1200dpi, RAM 512MB, Impresión Duplex sin apilar, Bandeja de Entrada: 1x 250 hojas, USB 2.0, Red Gigabit, Escaner (600dpi, 40ipm, Tamaño Carta & Oficio), Toner: TK-1175 / 12.000 Pág, Bandeja adicional. Garantía 1 Año. El equipo debe tener las siguientes certificaciones: Energy Star para el uso eficiente de energía, RoHS para el manejo de sustancias peligrosas,Certificado EPEAT Nota: para este requerimiento se acepta certificación expedida por el fabricante o link

				de página oficial del fabricante donde se verifique el cumplimiento. Instalación, configuración de equipo
11	IMPRESORA TIPO 2 MULTIFUNCIONAL GRANDE	1	Unidad	Impresora multifuncional Láser Monocromática, Formato A4, Funciones: Impresora, Copiadora, Escaner & Fax, Velocidad: Hasta 47 ppm Carta, Resolución de Impresión: Hasta 1200 x 1200dpi, Resolución de escaneo: Hasta 600x600dpi, Memoria RAM 1.5GB, Procesador ARM Cortex-A53 Dual Core 1.4GHz, Conectividad: USB 2.0 & Red Ethernet Gigabit, Bandejas de Entrada: 1x 500 hojas + Bandeja Multipropósito de 100 hojas, Alimentador RADF de 75 hojas, Bandeja de Salida: 1x 250 Hojas, Función Dúplex Estándar, Pantalla táctil de 7", Tiempo de primera página: 5.3 seg, Volumen de trabajo recomendado: Hasta 20.000 Pág/mes, Consumo de energía: Hasta 626W, Toner: TK-3402 / 12.500 Pág, Dimensiones: 475 x 476 x 575 mm, Peso: 23 Kg. Garantía 1 Año. El fabricante debe tener las siguientes certificaciones: Energy Star para el uso eficiente de energía, Certificado TÜV/GS, Certificado CE, ISO 9001 y ISO 14001. . Nota: para este requerimiento se acepta certificación expedida por el fabricante o link de página oficial del fabricante donde se verifique el cumplimiento. Instalación, configuración de equipo
12	IMPRESORA TIPO 3 MONOCROMÁTICA PEQUEÑA	4	Unidad	Impresora monocromática, Velocidad de impresión en negro A4: Hasta 20 ppm Resolución de impresión: Negro (óptimo): Hasta 600 x 600 ppp /Conectividad estándar: 1 USB 2.0 de alta velocidad; conexión inalámbrica 802.11b/g/n de 2,4 GHz con Bluetooth® de bajo consumo de energía /Capacidad de impresión móvil: Aplicación HP Smart; Apple AirPrint™; Impresión Wi-Fi Direct®; Ciclo de trabajo: Mensual (A4): Hasta 8,000 páginas /Garantía limitada de un año Pantalla: LED Manejo del papel: Bandeja de entrada para 150 hojas; Bandeja de salida para 100 hojas. garantía 1 año El equipo debe tener las siguientes certificaciones: Energy Star para el uso eficiente de energía, Cerificado TUV and GS Mark, Nota: para este requerimiento se

				acepta certificación expedida por el fabricante o link de página oficial del fabricante donde se verifique el cumplimiento. Instalación, configuración de equipo
13	UPS	2	Unidad	UPS 1KVA UPS Micronet Interactiva, Potencia 1KVA/600W, 6-Tomas de Corriente NEMA 5-15R, Nivel de Regulación +/- 10%, Factor de Potencia 0.6, Onda Sinusoidal Modificada, Tiempo de Respuesta de 3 a 10 Milisegundos, Recarga en 8 Horas al 90%, Autonomía: 5-Minutos a Full Carga & 10-Minutos a ½ Carga. Garantía 1 Año.
14	PROYECTOR	5	Unidad	Proyector Tecnología 3LCD, Resolución XGA 1024 x 768, Brillo 3400 Lúmenes, Método de Proyección: Frontal / Posterior / Techo, Relación de Aspecto: 4: 3, 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 Años El equipo debe tener las siguientes certificaciones: RoHS para el manejo de sustancias peligrosas, Certificado TCO. Nota: para este requerimiento se acepta certificación expedida por el fabricante o link de página oficial del fabricante donde se verifique el cumplimiento.
15	DISCOS DURO 4TB PARA ALMACENAMIENTO	2	Unidad	Discos Duros HDD de 4 Teras 2,5' para el servidor de aplicaciones, 7200 RPM, interface SATA III, cache de datos 128MB.
16	DISCOS DURO 8TB PARA ALMACENAMIENTO	2	Unidad	Discos Duros NAS de 8 Teras 3,5', 7200 RPM, interface SATA, disco para el servidor de Owncloud para memoria histórica del municipio
17	DISCOS DURO 1TB PARA ALMACENAMIENTO INTERNO	11	Unidad	Discos Duros SATA interno SSD de 1TB
18	ESCANER DE ALTO RENDIMIENTO DE TRABAJO	8	Unidad	Escaner de gestión documental, camaplana con ADF de capacidad 100 hojas, velocidad de escaneo 40ppm, resolución óptica de 1200dpi, profundidad de color de 48bits, funcionalidad de escaneo duplex, densidad

				de papel 50-128g/m. Tamaños de papel A4, Carta, Legal, B5, A5. Máx. 21.5 x 101.6 cm. Mín. 10 x 14.8 cm, peso 9.8kg, conectividad USb 2.0, Soporte para Windows, Formatos de salida JPG, PDF. Garantía 1 año
19	TABLET	7	Unidad	Tablet para gestión de archivos y trabajo de campo. Pantalla 10.5 Pulgadas, Resolución 1920 X 1200. Sistema Operativo Android o iOS, Procesador: Octa Core 2Ghz o M1 o M2. Memoria: 4Gb. Almacenamiento Interno: 64Gb. Cámara Principal: 8Mp. Cámara Frontal: 5Mp. Puerto: USB Type-C 2.0, Conectividad: Wi-Fi 802.11 a/b/g/n/ac, Wi-Fi Direct, Bluetooth 5. Debe incluir Soporte de pared. Garantía 12 meses.
20	TELÉFONO CELULAR	2	Unidad	Celular para manejo de lineas institucionales. Memoria RAM: 8GB, Pantalla de 6.7 pulgadas, procesador A15 Bionic con GPU e 5 núcleos o snapdragon 680, Red 4G, memoria interna de 512GB, sistema operativo iOS o Android
21	PC PARA DE EDICIÓN DE VIDEO	1	Unidad	Computador para edición de video y fotografía. Estación de trabajo - Pc de Escritorio, Macbook Pro, procesador M2, 16gb ram, disco sdd de 512GB, puerto gigabit ethernet, pantalla retina XDR de 16,2".
22	HERRAMIENTA PONCHADORA DE RED	1	Unidad	Tipo pinza - antireversible Poncha conector Rj11 Poncha conector Rj12 Poncha conector Rj45 Cuchilla para corte de cable 200mm de largo 75mm de ancho Mango antideslizante
23	SOLADOR CAUTÍN	1	Unidad	Tipo lápiz 110v Temperatura ajustable Potencia 60W Incluye Rollo de 100gr Diámetro de 1mm Flux integrado 1 Lupa Incluye soporte de 2 Pinzas, 1 Lampara, 1 Soporte para cautín
24	PATCHCORE DE FIBRA	3	Unidad	Conector SC / UPC 2 Metros
25	SOPLADORA	1	Unidad	Herramienta sopladora Conexión a 110v Potencia de 600w 13000Rpm 1 Tubo de caucho 1 Bolsa residual

26	ROUTER	5	Unidad	Router con funcionalidades de AP 1 Puerto WAN Gigabit 3 Puertos LAN Gigabit 5 Antenas DualBand 2,4 y 5Ghz Wifi a/b/g/n/ac Gigabit Soporte IPv4 e IPv6 Soporte MU-MIMO
27	COMBO TECLADO Y MOUSE	10	Unidad	1Teclado USB 1 Mouse USB Conexión alámbrica Distribución QUERTY – Español
28	ADAPTADOR M2 A USB	1	Unidad	Interface USB-C cable incluido Disco soportado SSD Compatible con B+MKEY Compatible con NVME Compatible con MKEY USB 3.0
29	UNIDAD DVD EXTERNA	7	Unidad	Interface USB cable incluido USB 2.0 Compatible con DVD + R, DVD-R, CD-ROM, DVD-ROM, CD-R
30	MULTITOMA RACKEABLE	1	Unidad	8 Conectores Largo del cable 80cm Tensión Máxima 15A Ancho: 48.2 x Alto: 5.4 x profundo: 4cm
31	MICRÓFONO INALÁMBRICO DE SOLAPA	1	Unidad	Micrófonos doble canal de 2.4 GHz, micrófono de solapa de 328 pies 5 ms estéreo de grabación de video receptor para cámara, iPhone, entrevista, podcast YouTube, Dispositivos compatibles: Camcorder, Camera. Tipo de conector: Jack de 0.138 in. Tipo de material Plástico Frecuencia de micrófono inalámbrico: 2.4 KHz Plataforma de hardware: Laptop, Camera, Smartphone Fuente de energía: Funciona con baterías
32	CÁMARA FOTOGRÁFICA TIPO 1	1	Unidad	A7 III con sensor de imagen full-frame de 35 mm captura continua a alta velocidad de hasta 10 fps. Hasta 10 fps en modo "Hi+" continuo y hasta 8 fps en modo "Hi" continuo.
33	BATERÍA PARA CÁMARA	3	Unidad	Batería para cámara fotográfica Dimensiones (An. × Al. × Pr.): Aprox. 38,7 x 22,7 x 51,7 mm (1 9/16 x 29/32 x 2 1/8 pulg.) Capacidad: 7,2 V / 16,4 Wh (2280 mAh)
34	MALETA PARA CÁMARA	1	Unidad	Especial para Cámara y hasta 3 lentes, Dimensiones 27 X 15 X 42.5 cm, Sistema Interno Acolchado, Sistema de cierre seguro, sistema Flipside, Incluye Impermeable

ALCALDÍA PUERTO LÓPEZ	ESPECIFICACIONES TÉCNICAS	Código: F – 168
		Versión: 002
		Fecha: Septiembre de 2020

35	LENTE PARA CÁMARA TIPO 1	1	Unidad	Lente 50mm F1.8 Apertura máxima de F1,8 para capturas con poca luz, Apertura circular de 7 láminas para un atractivo efecto de desenfoque
36	LENTE PARA CÁMARA TIPO 2	1	Unidad	Lente FE 28-70 mm F3,5-5,6 OSS Montura E, formato Full Frame, Lente de zoom estándar, Estabilización de SteadyShot óptico
37	ADAPTADOR DE LENTE PARA CÁMARA	1	Unidad	Adaptador de montaje de lente EF/EF-S Anillo convertidor de lente de enfoque automático compatible con Canon EF/EF-S Lens para cámaras Sony E Mount sin espejo Series A9 A7R4 A7R3 A7R2 A7M3 A7M2 A7R
38	ESTABILIZADOR PARA CÁMARA	1	Unidad	Estabilizador Ronin Bloqueo automático de los ejes Brazos de los ejes de fibra de carbono prolongados Carga probada de 4.5 kg Enfoque LiDAR Transmisión O3 Pro Carga probada. 4.5 kg (10 libras) Puerto para accesorios. Puertos RSA/NATO - Orificio de montaje de 1/4"-20 - Zapata - Puerto de transmisión de vídeo/telémetro LiDAR (USB-C) - Puerto de control de cámara RSS (USB-C) - Puerto de motor Focus (USB-C) Batería. Tiempo de funcionamiento máx.: 12 horas Medido con el equipo nivelado y parado, el estabilizador equilibrado, tres ejes en un estado activo y la batería alimentando solo el estabilizador] - Tiempo de carga: aprox. 1.5 horas (usando un cargador de 24 W; se recomienda usar cargadores QC 2.0 o con protocolo PD) - Temperatura de carga recomendada: de 5 a 40 °C (de 41 a 104 °F) Conexiones. Bluetooth 5.0 - Puerto de carga (USB-C) Requisitos de la aplicación Ronin. iOS 11 o superior - Android 7.0 o superior Peso. Estabilizador: aprox. 1143 g - Empuñadura: aprox. 265 g - Empuñadura secundaria/trípode (metal): aprox. 226 g - Placas de liberación rápida inferior y superior: aprox. 107 g Dimensiones del estabilizador. Plegado: 268 × 276 × 68 mm (la. × an. × al., excluidas cámara, empuñadura y empuñadura secundaria/trípode) - Desplegado: 415 × 218 × 195 mm (la. × an. × al., la altura incluye la empuñadura y excluye la empuñadura secundaria/trípode)

				Rango mecánico. Eje de giro: rotación continua de 360° - Eje de rotación: de −95° a +240° - Eje de inclinación: de −112° a +214° Idiomas admitidos por la pantalla táctil. Español Inglés, chino simplificado, chino tradicional, alemán, francés, coreano, japonés, portugués (Brasil), ruso, tailandés
39	ILUMINARIA PARA FOTOGRAFÍA	1	Unidad	Luz Led lámpara con cargador Panel 900 LED de bajo consumo. - Se puede utilizar tanto para video como para luz continua en fotografía. - Temperatura de color variable: 3200K - 5500K - Temperatura de color ajustable, con 450 Led de 3200k y 450 Led de 5500k. - Incluye un mando a distancia IR para controlar la potencia de forma inalámbrica. - Permite ser controlado desde un móvil smartphone utilizando la app de Yongnuo. (Smartphone no incluido) - Disponible hasta 8 canales. - Iluminación: 6975 lm - Iluminación uniforme. - Permite controlar la potencia por cada temperatura de color (3200k y 5500k) - Funciona mediante 2 batería (no incluida) de la serie NP-F, y se recomienda usar el modelo NP-F750 para una mayor experiencia. - En nuestra tienda tenemos disponible un adaptador de pilas NP-F750 que permitirá usar la lámpara con pilas AA. - * Se puede utilizar con 1 batería, pero solo podrá utilizarse los led de 3200k o los led de 5500k al utilizarse con una sola batería. - Permite ser utilizado con una fuente de alimentación externa (No incluida). - Botón Test que nos indicara el nivel de carga de la batería. - Angulo de iluminación 55º - Se puede montar directamente sobre la zapata estándar de la videocámara o cámara réflex de fotografía. - Tamaño: 260 x 188 x 48mm - Peso: 1480g. Contenido del paquete: 1x Lámpara Yongnuo YN900. 1x Mando IR. 1x Filtro translucido. 1x Filtro naranja. 1x Pie 1x Empuñadura / Mango.

40	BATERÍA PARA LUZ LED	4	Unidad	Batería Np-f970 para Luz led de alto rendimiento Química: Iones de litio Capacidad: 7800 mAh Watt Horas: 57.72 Wh Voltaje de salida: 7.4 V Dimensiones: (7 x 3.9 x 6 cm) Peso: 10.3 oz (292 g)
41	TRÍPODE PARA LUZ LED	1	Unidad	Trípode para luz led LU-TR2 Trípode hecho de aleación de aluminio. Diseñado para trabajo pesado. Soporta todo equipo de fotografía. Altura ajustable: 96,92 cm – 2mts.
42	TRÍPODE PARA CÁMARA	1	Unidad	Trípode de 74 pulgadas para cámara, teléfono celular, video, fotografía, trípode de soporte alto para cámara, trípode DSLR, Soporte de tornillo estándar de 1/4" compatible con todas las cámaras (Nikon D3500, Fujifilm X-T200, Canon EOS 250D, Olympus, Panasonic), DSLR, SLR, cámaras web, videocámaras compactas, cámaras de cine digital, proyector, anillo, telescopios de detección y binoculares. El soporte de teléfono de 360° es compatible con iPhone 14 13 12 11/11 Pro/XS Max/XS/XR/X/8/8 Plus/Galaxy Note 9/S10/S20., Cabezal panorámico de 3 vías con rotación de 360°.
43	TRANSCEIVER FIBRA	2	Unidad	Gigabit SFP a RJ45 Convertidor de fibra a Ethernet | 1000Mbps RJ45 puerto a 1000Base-LX fibra de modo único con soporte para redes hasta 15Km Interfaz de hardware: Ethernet Protocolo de enlace de datos: IEEE 802.3, Ethernet Velocidad de transferencia de datos: 1000 Megabits por segundo. Convierte fibra 1000BASE-LX a medios de cobre 1000Base-T o viceversa. Funciona a 1000 Mbps en modo dúplex completo tanto para puerto TX como para puerto FX Soporta MDI/MDIX automático para puerto TX y proporciona configuración de interruptor del modo de transferencia Force/Auto para puerto FX Extiende la distancia de fibra hasta 12.4 millas (12.4 mi) Los indicadores LED fáciles de ver proporcionan estado para controlar la actividad de la red fácilmente Fuente de alimentación externa. Longitud de onda: 1310 nm.

				Consumo máximo de energía: 1,8 W Admite la especificación láser de onda larga (LX) a una velocidad de reenvío de velocidad de cable completa. Funciona a 1310 nm tanto en la transmisión como en la recepción de datos. par a y par b
44	PARLANTE CABINA ACTIVA	3	Unidad	Configuración: 2 vías Amplificador integrado LF / HF: 1200/300 Respuesta frecuente: 58 Hz-20 kHz Woofer de baja frecuencia: 10 – 2.5 bobinas Controlador de alta frecuencia: 1 – 1.4 bobina Máximo SPL cont / pico: 123/127 Dispersión: 90 ° x60 ° Impedancia de entrada: 22 Conector de entrada: ENTRADA / SALIDA XLR Cable de alimentación: 3 metros Dimensión neta (WxHxD): 11,81×21,10×11,87 / 300x536x301,5 Peso neto: 13 Kg Dimensión de transporte (WxHxD): 14,56×24,21×14,96 / 370x615x380 Peso de transporte: 32,62 / 14,8
45	DISCOS DURO 1TB PARA ALMACENAMIENTO EXTERNO	8	Unidad	Discos Duros externo SSD de 1TB
46	EXTENSIÓN ELÉCTRICA	2	Unidad	15 metros de largo extensión encauchetada 3x14 Tipo de cable: SJT 14 AWG x 3 C Conductor 100% de cobre Capacidad de corriente 15 A
47	IMPRESORA TIPO 4 A COLOR	1	Unidad	Inyección de tinta Heat-Free® PrecisionCore de 4 colores (CMYK). Resolución máxima de impresión hasta 4.800 dpi x 1.200 dpi de resolución optimizada en varios tipos de papel. Velocidad de impresión máxima negro 33 ppm y color 20 ppm (borrador, A4/carta). Resolución máxima de copiado 300 dpi x 600 dpi (cama plana) / 300 dpi x 300 dpi (ADF). Tipo de escáner Cama plana con sensor de líneas CIS de color. Conectividad estándar USB de alta velocidad (compatible con USB 2.0), Wi-Fi 4®[6] (IEEE 802.11 b/g/n), Wi-Fi Direct®[6], Ethernet 10/100. Tamaño máximo de impresión 215,9 mm x 1.200 mm. Tamaños de papeles soportados Estándar: A4, Carta, Oficio (215,9 mm x 355,6 mm), México-Oficio (215,9 mm x

				340,4 mm), Oficio 9 (214,9 mm x 315 mm), Ejecutivo, Media carta, A6 Foto: 4" x 6" (10 cm x 15 cm), 5" x 7" (13 cm x 18 cm), 8" x 10" Sobres: #10 Definido por el usuario: 54 mm x 86 mm - 215,9 mm x 1.200 mm. Garantía 1 año
48	MICRÓFONO INALÁMBRICO DE MANO	2	Unidad	Par de micrófonos inalámbricos de mano, dos canales A y B. Banda de frecuencia UHF. SNR >6dB. Distorsión <0,5%. Sensibilidad -51dB. Impedancia de salida 600 Ohms. Relación S/N 96dB. Temperatura de operación -10°C a +60°C Respuesta de frecuencia 50Hz - 15kHz. Funciona con baterías

CONDICIONES TECNICAS MÍNIMAS PARA LA ENTREGA

El cumplimiento del objeto contractual deberá contar con las siguientes especificaciones técnicas:

1. Los equipos deberán ser nuevos, en ningún momento podrán ser remanufacturados.
2. Los equipos deben contar con garantía mínima de 1 de año.
3. La arquitectura de los equipos deberá corresponder a la última generación.

Las actividades objeto del futuro contrato son:

1. Suministrar a la Administración Municipal de Puerto López los implementos requeridos de buena calidad, por tanto, todos los elementos ofertados deberán ser de marca reconocida y de fabricación nacional.
2. Asumir los costos de adquisición, transporte para la entrega de los elementos, se consideran incluidos en los precios unitarios que se estipulan para cada bien o elemento.
3. El valor de cada ítem incluye cargue y descargue de los elementos en el almacén de la Alcaldía Municipal de Puerto López.
4. Entrenamiento para manejo adecuado de las herramientas de administración de licenciamiento Fortinet y antivirus
5. Entrenamiento para manejo adecuado de los equipos tecnológicos entregados y su utilización

EDGAR FERNANDO CARRILLO RIOS
Secretario General

Elaborado	Revisado	Aprobado
Nombre: Luis Ortegate	Nombre: Faunier Luna Garay	Nombre: Edgar Fernando Carrillo Rios
Cargo: CPS Abogado Secretaría General	Cargo: Asesor TIC	Cargo: Secretario General
Fecha: 06/10/2024	Fecha: 06/10/2024	Fecha: 06/10/2024