Municipio El Carmen de Viboral	ESTUDIOS DEL SECTOR SELECCIÓN DE MÍNIMA CUANTIA Proceso al que pertenece: CONTRATACIÓN Código: F-CT 057 Versión: 06 Fecha: 24/11/2023	[redacted]

NOMBRE DEL PROYECTO:	Fortalecimiento institucional a través de la generación de un ambiente laboral propicio en El Carmen De Viboral
RADICADO PROYECTO:	2022051480067
FUENTE DE FINANCIACIÓN:	Certificado de Disponibilidad: 931 del 30 de abril de 2024 Código: 05.2.3.2.02.02.008.23.01
OBJETO:	Suministro de licencias de antivirus y licencia de Fortinet de la entidad y centro de monitoreo para la protección perimetral de la red, de los equipos de cómputo y las plataformas informáticas de la administración municipal de El Carmen de Viboral

1. ASPECTOS GENERALES DEL MERCADO

1.1 Justificación de la necesidad:

Entre los principios orientadores de la ley 1341 de 2009 se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones. En su artículo 2° dispone: La investigación, el fomento, la promoción y el desarrollo de las Tecnologías de la Información y las Comunicaciones son una política de Estado que involucra a todos los sectores y niveles de la administración pública y de la sociedad, para contribuir al desarrollo educativo, cultural, económico, social y político e incrementar la productividad, la competitividad, el respeto a los Derechos Humanos inherentes y la inclusión social.

Las Tecnologías de la Información y las Comunicaciones deben servir al interés general y es deber del Estado promover su acceso eficiente y en igualdad de oportunidades, a todos los habitantes del territorio nacional.

Asimismo, mediante el Decreto 1008 de 2018 "Se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones", de esta manera, la entidad busca no solo que el uso de la tecnología sea ágil, sencillo y útil para las personas sino también que la interacción entre los diferentes actores involucrados en la política se de en un ambiente seguro, corresponsable y previsible.

El presente proceso se encuentra enmarcado en el plan de Desarrollo Línea No 5, programa 5.2, subprograma 5.2.1, cuya meta del producto corresponde la de Actualizar las TIC (Tecnologías de la Información y las Comunicaciones) en todas y cada una de las dependencias para mejorar la eficacia, la eficiencia y la prontitud en la gestión administrativa.

El uso de programas antivirus no solo beneficia a los individuos que los instalan en sus dispositivos, sino que también tiene un impacto positivo en la comunidad en general, en los que se pueden encontrar:

Reducción de la Propagación de Malware: Los programas antivirus ayudan a detectar y eliminar malware en los dispositivos individuales, lo que reduce la probabilidad de que estos programas maliciosos se propaguen a otros dispositivos en la red. Esto es especialmente importante en redes corporativas y

comunitarias, donde un solo dispositivo infectado puede comprometer a toda la red.

Protección de Datos Personales y Confidenciales: Al prevenir infecciones por malware, los programas antivirus protegen los datos personales y confidenciales de los usuarios, como información financiera, contraseñas y otros datos sensibles. Esto reduce el riesgo de robo de identidad y fraude, beneficiando a la comunidad en su conjunto.

Mejora de la Seguridad en Transacciones en Línea: La seguridad en transacciones en línea, como compras, banca y pagos electrónicos, se ve mejorada cuando los dispositivos están protegidos con programas antivirus. Esto fomenta la confianza en el uso de servicios en línea, beneficiando tanto a los consumidores como a los negocios.

Prevención de Ataques Cibernéticos a Gran Escala: Los programas antivirus pueden detectar y neutralizar amenazas que podrían ser utilizadas en ataques cibernéticos a gran escala, como botnets que lanzan ataques DDoS (denegación de servicio distribuida). Al reducir la cantidad de dispositivos que pueden ser comprometidos, se disminuye la capacidad de los atacantes para llevar a cabo estos ataques.

Estabilidad y Confiabilidad de Servicios Digitales: Al mantener los dispositivos libres de malware, se mejora la estabilidad y confiabilidad de los servicios digitales prestados a la comunidad Carmelitana y la infraestructura de TI. Esto beneficia a todos los usuarios que dependen de estos servicios para sus actividades diarias.

Seguidamente, resulta oportuno indicar que las últimas tres décadas se han caracterizado por una aceleración en los cambios tecnológicos, especialmente en campos como las telecomunicaciones, los computadores, la bioingeniería, la nube y las aplicaciones para uso personal y empresarial. No hay duda de que su impacto más importante se ha sentido en los procesos empresariales y oficiales. La utilización de equipos de cómputo, los softwares que lo acompañan en operaciones de todo tipo y la comunicación por correo electrónico, ha tenido un efecto enorme en el aumento de la productividad, hasta el punto que hoy no se concibe que una empresa cuyos procesos de producción o de servicios sean susceptibles de computarizar, sobreviva a la competencia sin dejar de hacerlo.

En el caso del municipio de El Carmen de Viboral, es de resaltar que éste, en la actualidad, se ubica en segunda categoría, contando con una población de 66.374 habitantes aproximadamente para el año 2024, según proyecciones del DANE del período 2018 – 2026. Todo esto pone presente la dimensión del Municipio, sus responsabilidades, los requerimientos y trámites administrativos que para su funcionamiento y la ejecución de proyectos de inversión se requiere.

Es importante manifestar que las amenazas cibernéticas están en constante evolución y se vuelven cada vez más sofisticadas, por lo que contar con una seguridad adecuada es esencial para proteger los datos de la entidad, información financiera y la integridad de nuestros dispositivos.

La Administración Municipal, trabaja en la mejora de tecnologías, dispositivos y software que apoyen la seguridad informática dentro de la entidad y en todos los equipos, contribuyendo a la prestación de un buen servicio al ciudadano.

Para el año 2021, se adquirió un dispositivo de seguridad perimetral Fortigate en la Alcaldía y en el año

2023 en el Centro de Monitoreo, dichos elementos requieren de renovación de la licencia cada año.

Las múltiples amenazas de virus informáticos que enfrentamos en la actualidad hacen que sea cada vez más necesario contar con herramientas de defensa cibernética. En este contexto, la Administración Municipal necesita renovar las licencias de antivirus para proteger sus dispositivos con las actualizaciones más recientes, lo que permitirá una detección más eficaz de los virus informáticos y, por ende, una preservación de la información más confiable y segura.

Un antivirus actualizado asegura que el sistema esté protegido contra las amenazas más recientes. Las actualizaciones incluyen firmas de virus nuevas y reglas de detección que permiten al antivirus reconocer y neutralizar nuevos tipos de malware, Las actualizaciones del antivirus pueden incluir parches y mejoras que cierran estas brechas de seguridad.

Por lo tanto, se tiene la necesidad y responsabilidad de velar por la seguridad de la información y protección contra software malicioso o no deseado (malware) por medio de un antivirus, con el fin de poder mantener todo su sistema y los correos libre de virus y otras amenazas, al interior de la entidad.

El presente proceso de fue aprobado por el comité de contratación mediante acta 016 del día 18 de abril de 2024.

1.2. Aspecto Económico:

La industria de los antivirus y la seguridad informática es un sector dinámico y en crecimiento constante debido al aumento de ciberamenazas, algunos datos estadísticos y económicos recientes sobre antivirus y la industria de la ciberseguridad.

El mercado global de software antivirus estaba valorado en aproximadamente 3.89 mil millones de dólares en 2020 y se proyecta que alcance los 4.74 mil millones de dólares para 2026, con una tasa de crecimiento anual compuesta (CAGR) del 3.5% durante el período de pronóstico (2021-2026).

Según un informe de AV-TEST, una organización independiente de investigación en ciberseguridad, cada día se detectan más de 350,000 nuevos programas maliciosos y aplicaciones potencialmente no deseadas.

En 2021, un estudio de Statista reveló que el 95% de las empresas en todo el mundo utilizan software antivirus como parte de sus estrategias de seguridad cibernética.

Según Gartner, el gasto global en productos y servicios de seguridad de la información y gestión de riesgos alcanzó los 150.4 mil millones de dólares en 2021, un aumento del 12.4% en comparación con 2020.

El informe de IBM "Cost of a Data Breach 2021" indicó que el costo promedio de una violación de datos fue de 4.24 millones de dólares, el valor más alto en los 17 años de historia del informe.

El precio de las licencias de software antivirus varía según el proveedor y las características del producto. Por ejemplo, las licencias anuales para soluciones antivirus de consumo pueden oscilar entre

20 y 100 dólares por dispositivo, mientras que las soluciones empresariales pueden costar cientos o incluso miles de dólares anuales, dependiendo del número de dispositivos y el nivel de protección requerido.

1.3. Aspecto Regulatorio:

El fundamento jurídico que soporta la modalidad de la selección se encuentra regulado en el artículo 274 de la Ley 1450 de 2011, la cual adiciono el numeral 5 del artículo 2 de la Ley 1150 de 2007, estableciendo la modalidad de selección de MÍNIMA CUANTIA, seguidamente la Ley Anticorrupción, Ley 1474 de 2011, articulo 94; modalidad de selección que fue reglamentada por los artículos 2.2.1.2.1.5.1 y 2.2.1.2.1.5.2 del Decreto 1082 de 2015, esta ultima modificada por el decreto 1860 de 2021.

El numeral 8 del artículo 2 de la Ley 1341 de 2009, "Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC- (...)", "(...) las entidades públicas deberán adoptar todas las medidas necesarias para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones (TIC) en el desarrollo de sus funciones. El Gobierno Nacional fijará los mecanismos y condiciones para garantizar el desarrollo de este principio. Y en la reglamentación correspondiente establecerá los plazos, términos y prescripciones, no solamente para la instalación de las infraestructuras indicadas y necesarias, sino también para mantener actualizadas y con la información completa los medios y los instrumentos tecnológicos. (...)"

El artículo 2.2.17.1.6 del Decreto 1078 de 2015, "Por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones", en el numeral 6. Seguridad, privacidad y circulación restringida de la información: Toda la información de los usuarios que se genere, almacene, transmita o trate en el marco de los servicios ciudadanos digitales deberá ser protegida y custodiada bajo los más estrictos esquemas de seguridad digital y privacidad con miras a garantizar la autenticidad, integridad, disponibilidad. confidencialidad, el acceso y circulación restringida de la información, de conformidad con lo estipulado en el habilitador transversal de seguridad de la información de la Política de Gobierno Digital.

Decreto 088 de 24 de enero de 2022, en su artículo 2.2.20.5. establece... "Integración cie los lineamientos de digitalización y automatización de trámites con las políticas de gobierno digital y de racionalización de trámites. Los lineamientos expedidos en el presente decreto y en el anexo 1 de esta misma norma, para la digitalización y automatización de los trámites, se deberán implementar por las autoridades de manera articulada con la Política de Gobierno Digital regulada en el titulo 9, parte 2, libro 2, del presente Decreto, y, entre otros, con los lineamientos y estándares señalados en el marco de arquitectura, en el modelo de seguridad y privacidad, en el modelo de servicios ciudadanos digitales, los referidos a las sedes electrónicas, expedidos por el Ministerio de Tecnologías de la Información y las Comunicaciones, así como, los señalados en la política de racionalización de trámites y la guía metodológica para la racionalización de trámites expedida por el Departamento Administrativo de la Función Pública".

1.4. Aspecto Técnico:

El suministro debe realizarse de acuerdo a cada una de las características técnicas relacionadas a continuación y en concordancia con las obligaciones estipuladas:

Cantidades sin iva

ITEM	DESCRIPCIÓN	CANTIDAD	VALOR UNITARIO	VALOR TOTAL
1	LICENCIA ANTIVIRUS por un (1) Año, incluye: licencias para proteger buzones de Correo electrónico Microsoft 365, licencias para proteger dispositivos móviles (Celulares o Tabletas), Licencia para Servidores, consola Web, capacitación al personal necesario para la implementación y administración de la consola, Soporte directo con el Fabricante durante el periodo que se encuentre activa la licencia El antivirus debo contener: **PROTECCIÓN CONTRA MALWARE** • Seguridad de navegación frente a amenazas malware, ransomware, botnets, phishing • Inteligencia DNS de contenidos • Control parental y filtrado web personalizado para familias, escuelas y organizaciones y empresas. • Listas negras basadas en A-I • Más de 90 categorías de forma continua actualizado gracias a la Inteligencia Artificial. • Geobloqueo • Bloqueo de la navegación a países en peligro de ataques de piratas informáticos y ciberamenazas. • Protección de las IP frente a las listas negras • Mantener fuera las IP públicas listas negras mundiales. • Análisis detallados • Informes analíticos en tiempo real, por categoría de visita y macrocategoría, y programada por correo electrónico. • Máxima compatibilidad • Conexión a todos los routers, Puntos de acceso WiFi, cortafuegos y puertas de enlace. • Apoyo a IP estática, IP dinámica y protocolo DNS. • Filtrado de motores de búsqueda • Bloqueo de contenidos explícitos (violencia, porno...) que pueden activarse para las búsquedas en Google, Bing, YouTube y DuckDuckGo.	200	$ 137,609	$ 27,521,800

			Subtotal	$27.521.800

Cantidades con IVA 19%

2	Licencia para FortiGate 60ESerial: FGT60ETK19099QET 24x7 Funcionalidades incluidas: Unified Threat Protection (UTP) (24x7 FortiCare plus Application Control, IPS, AV, Web Filtering and Antispam, FortiSandbox Cloud). **	1	$ 3,588,147	$ 3,588,147
3	Licencia para FortiGate 60FSerial: FGT60FTK22035241 24x7 Funcionalidades incluidas: Unified Threat Protection (UTP) (24x7 FortiCare plus Application Control, IPS, AV, Web Filtering and Antispam, FortiSandbox Cloud).**	1	$ 2,672,972	$ 2,672,972
	Sub total			$6.261.119
	**Iva 19%			$1.189.612,61
	Total			$7.450.731,61

Total Proceso	$34.972.531,61

Obligaciones del contratista:

Obligaciones Generales:

1. Cumplir con el objeto del proceso y las especificaciones técnicas mínimas descritas en la Invitación Pública, fichas técnicas y en la propuesta presentada, la cual para todos los efectos forma parte integral del Contrato
2. Constituir las respectivas garantías para amparar los riesgos del Contrato.
3. Obrar con lealtad y buena fe en las distintas etapas contractuales, evitando dilaciones y en trabamientos que puedan presentarse y en general se obliga a cumplir con lo establecido en la Ley 80 de 1993, Ley 1150 de 2007 y sus Decretos Reglamentarios
4. Suscribir el acta de inicio, acta de liquidación del contrato y las modificaciones a las que hubiera lugar
5. Acatar las instrucciones que durante el desarrollo del contrato se le imparta por parte de la Supervisión
6. Responder por sus actuaciones y omisiones derivadas de la celebración del contrato y de la ejecución del mismo, de conformidad con lo establecido en las leyes 80 de 1993, 1150 de 2007 y sus decretos reglamentarios
7. Realizar los actos necesarios y tomar las medidas conducentes para el debido y oportuno cumplimiento de las obligaciones contractuales y la ejecución del contrato.
8. No acceder a peticiones o amenazas de quienes actúen por fuera de la Ley con el fin de hacer u omitir algún hecho
9. Procurar el cuidado integral de su salud y contar con los elementos de protección personal necesarios para ejecutar la actividad contratada para lo cual asumirá su costo
10. Cumplir con las normas del sistema general de riesgos laborales y sistema de gestión de la seguridad

y salud en el trabajo
11. Asumir el pago de los impuestos, gravámenes, aportes parafiscales y servicios de cualquier género que establezcan las leyes colombianas
12. Aportar certificación expedida por el Revisor Fiscal cuando exista de acuerdo con los requerimientos de la Ley o por el Representante Legal del cumplimiento de sus obligaciones con el Sistema de Seguridad Social Integral (sistemas de salud, pensiones y riesgos profesionales), y aportes a la Cajas de Compensación Familiar, Servicio Nacional de Aprendizaje e ICBF, cuando a ello hubiere lugar, obligación que deberá adjuntarse al informe del interventor y deberá ser verificada por éste
13. Informar oportunamente a la Supervisión durante la ejecución del contrato las variaciones que se presenten al régimen de imposición por IVA u otras cargas tributarias en atención a los bienes o servicios contratados o al régimen tributario del contratista
14. Mantener estricta reserva y confidencialidad sobre la información que conozca por causa o con ocasión del contrato
15. Radicar todos los documentos de su cuenta de cobro o factura a través del SECOP II
16. Las demás obligaciones especiales de acuerdo con el objeto contractual (tratamiento de datos, derechos de autor, marcas y patentes, cuando aplique)

Obligaciones específicas

1. Legalizar el contrato en los tiempos requeridos
2. Ejecutar el objeto del contrato, de acuerdo a lo establecido en el alcance y especificaciones técnicas y en el plazo establecido.
3. Permitir la administración de equipos por directivas de configuración, la clasificación de equipos en grupos parametrizados y la sincronización de estructura de grupos con Active Directory
4. Entregar de las licencias totalmente instalados, configurados, verificados y funcionando a un 100%.
5. Solucionar con responsabilidad las fallas o inconvenientes que presenten durante la vigencia de la licencia.
6. La consola del administrador debe:
   *Listar detalles de configuración de equipos tales como: Nombre de equipo, dirección IP, MAC, Sistema Operativo, Configuraciones de Hardware (Disco duro, Memoria RAM, procesador, etc.)
   *Ofrecer herramientas de auditoría de equipos que muestren información detallada como programas instalados, privilegios del usuario, registro de eventos de sistema y aplicación, procesos en ejecución, y conexiones de red activas
   *Tener habilitados módulos de reportes que permitan generar información estadística personalizada y/o generalizada definiendo periodos de recolección de datos y formato en los cuales se presentarán dichos reportes
   *Tener herramientas de notificación con una base de alertas generadas por las estaciones, permitiendo al administrador tomar acciones sobre dichas alertas.
7. Mostrar información detallada acerca del contenido de la cuarentena de equipos y a su vez que permita realizar operaciones sobre las mismas (restauración, eliminación, reportes, etc.)
8. Ofrecer herramientas que permitan unificar configuraciones del Firewall Personal de las estaciones con el fin de evitar el uso no autorizado de aplicaciones, y aplicar reglas generalizadas a las estaciones de trabajo
9. Habilitar parámetros de configuración de las estaciones de trabajo para evitar modificar o desinstalar el producto.
10. Proporcionar un diagnóstico de seguridad, para determinar el nivel de seguridad en el que se

encuentra la Administración Municipal y los riesgos a los cuales está expuesto, para así mismo tomar las medidas y controles necesarios

11. Las licencias tendrán un uso no inferior a un (1) año con asistencia en plataforma durante este tiempo

En la implementación y operación: capacitar al personal de Sistemas en la implantación del sistema de seguridad propio de la entidad, específicamente en los siguientes aspectos:

- Definición de la estrategia de tratamiento de riesgo
- Manejo de identidad y control de acceso
- Gestión de riesgos y vulnerabilidades
- Aseguramiento del contenido de la información

Seguimiento a incidentes: el contratista deberá desarrollar las siguientes actividades:

- El contratista, enviará vía email a los contactos definidos por la Administración Municipal, información técnica relacionada con los productos, como son: existencia de parches o nuevos releases, reporte de nuevos problemas y toda la información que el contratista considere de importancia
- El contratista programará trimestralmente visitas (presenciales o virtuales) a la Entidad para análisis y seguimiento de incidentes con su respectivo planteamiento de solución

1.5. Información Financiera:

Los recursos con los cuales se financian las actividades objeto del contrato provienen del presupuesto de rentas y gastos de la actual vigencia fiscal, aprobado mediante Acuerdo Municipal 014 del 14 de diciembre 2023 *"Por el cual se adopta el presupuesto de ingresos y egresos para el período comprendido entre el primero (1) de enero y el treinta y uno (31) de diciembre de la vigencia fiscal dos mil veintidós (2024)".*

La dirección y administración del fondo está a cargo de la Administración Municipal y corresponde a recursos propios para funcionamiento.

2. ANÁLISIS DE LA OFERTA

2.1. Indicación de si el proceso de contratación esta cobijado por un acuerdo marco, de conformidad con el Decreto 310 de 2021.

Teniendo en cuenta las disposiciones reguladas en el artículo 274 de la Ley 1450 de 2011, la cual adiciono el numeral 5 del artículo 2 de la Ley 1150 de 2007, estableciendo la modalidad de selección de **MÍNIMA CUANTIA**, seguidamente la Ley Anticorrupción, Ley 1474 de 2011, articulo 94; modalidad de selección que fue reglamentada por los artículos 2.2.1.2.1.5.1 y 2.2.1.2.1.5.2 del Decreto 1082 de 2015, se entreve que esta modalidad de contratación opera cuando el monto de la contratación no supera el 10% de la menor cuantía de la entidad. Acto seguido se ordena: **ESTE PROCEDIMIENTO SE ESTABLECE INDEPENDIENTEMENTE DEL OBJETO A CONTRATAR.**

Por consiguiente, cuando la modalidad de selección es de mínima cuantía no es de carácter obligatorio adquirir Bienes y Servicios de Características Técnicas Uniformes de Común Utilización a través de los **ACUERDOS MARCO** de Precios previamente justificados, diseñados, organizados y celebrados por la Agencia Nacional de Contratación Pública -Colombia Compra Eficiente-.

Ahora bien, acogiéndonos a las consideraciones efectuadas por el Consejo de Estado, Sala de lo Contencioso Administrativo, Sección Tercera, Subsección A, Radicación numero 11001 03 26 000 2016 00017 00, expediente 56307, de fecha 29 de marzo de 2017, la sala concluyo: "...Siempre que exista un Acuerdo Marco de Precios para adquirir bienes o servicios de características técnicas uniformes y el presupuesto del proceso de contratación sea equivalente a la mínima cuantía de la entidad, debe acudirse al procedimiento de selección de mínima cuantía independientemente del objeto a contratar..."

Teniendo en cuenta las características y especificaciones técnicas del suministro a contratar, la metodología de análisis que sustenta el valor del presupuesto oficial se establece con base en 3 cotizaciones

1. La enviada por **TECNO TICS SOLUCIONES CORPORATIVAS,** valor de $37,778,000.00
2. La presentada por **TIC SOLUCIONES SAS,** por un valor de $34,999,793.64
3. Las presentadas por **SERVITT INGENIERIA SAS** $32,140,000.00

La metodología para establecer el valor estimado del proceso se efectuó con base al promedio de tres (3) cotizaciones presentadas por proveedores, por lo tanto, el presupuesto oficial estimado para la contratación asciende a la suma de Treinta y cuatro millones novecientos setenta y dos mil quinientos treinta y un pesos con sesenta y un centavos **($34.972.531,61).**

2.2. ¿Quién vende?

En Colombia existen diferentes empresas que suministran este tipo de productos tales como **ITSEC S.A.S, INFORTEC y ROYHER S.A.S, TECNO TICS SOLUCIONES CORPORATIVAS, TIC SOLUCIONES SAS, SERVITT INGENIERIA SAS,** entre otros, cada una con experiencia en el sector que garantiza el correcto suministro del insumo.

2.3. ¿Cuál es la dinámica de producción, distribución y entrega de bienes, obras o servicios?

La dinámica de producción de antivirus está a la par del crecimiento de virus informáticos que aparecen en el mercado, constantemente hay actualizaciones que contrarrestan las amenazas que van surgiendo en el ciberespacio.

Se distribuyen licencias en cada equipo, con una plataforma central tipo web que los administra y lleva estadísticas e informes diarios de las actividades vulnerables que pueden ocurrir mientras se está en el funcionamiento cotidiano.

Los paquetes de licencias se pagan una única vez por un tiempo determinado, normalmente de 2 a 3 años de funcionamiento.

2.4. ¿Cómo compran los particulares?

Los compradores rara vez hacen uso de toda la información necesaria para evaluar la utilidad de un producto o servicio en particular, incluso cuando es fácilmente accesible. Sin embargo, en la mayoría de los casos, ni siquiera disponen de una fracción de todo lo que ofrecen los fabricantes o proveedores.

Este desequilibrio de información deja a los compradores de programas antivirus a merced de las fuerzas invisibles del mercado o, peor aún, de los fabricantes que lo dominan. Los consumidores que no están de acuerdo con este panorama compran productos más baratos (reduciendo así el riesgo de pagar de más por un producto con características que no están en condiciones de evaluar), o bien posponen la decisión de compra hasta que haya más información disponible.

En la otra cara de este dilema está el costo de no hacer nada, una práctica muy extendida. En el contexto de la ciberseguridad, esto significa que la decisión de no comprar software antivirus podría terminar costando mucho más que el valor de una licencia para un equipo si un ransomware, como por ejemplo CryptoLocker, llega a destruir todos tus datos, fotos y correspondencia.

Los particulares compran a distribuidores autorizados y cancelan de manera directa los suministros.

Los particulares contratan directamente con la empresa a la que le realiza la solicitud o persona natural que se encarga de realizar todo el proceso contractual, igualmente mediante cotización a varias empresas; las cuales no están certificadas por la casa matriz, quien especifica que el proveedor está autorizado para comercializar y soportar el producto, teniendo el ingeniero idóneo, capacitado y certificado para la instalación y configuraciones del mismo.

Es de aclarar que la mayoría de las veces los particulares instalan un antivirus con un crack (parche creado sin autorización del desarrollador del programa al que modifica cuya finalidad es la de modificar el comportamiento del software original.)

3. ANÁLISIS DE LA DEMANDA

3.1. Adquisiciones previas de la entidad:

ITEMS	DESCRIPCIÓN DEL OBJETO	MODALIDAD CONTRACTUAL Y NUMERO DE CONTRATO	CONTRATISTA	VALOR DEL CONTRATO	FORMA DE PAGO	PLAZO DE EJECUCIÓN
1	Suministro de licencias de antivirus, para la protección perimetral de la red, de los equipos de cómputo y las plataformas informáticas de la Administración Municipal de El Carmen de Viboral	Mínima cuantía 200-CS-017-2022	ITSEC SAS	21.896.00	Un solo pago	6 meses
2	Suministro de licencias de Antivirus por 2 años, para uso de todas las estaciones de trabajo, su instalación, configuración, capacitación y validación del buen funcionamiento, en la Administración Municipal de El Carmen de Viboral	Mínima Cuantía 200-CS-012-2019 (CMC-18-2019)	ITSEC S.A.S.	$12.000.000	Un solo pago	3 meses
3	Suministro de licencias de antivirus, con herramientas de ayuda para la Administración de la red del Municipio de El Carmen de Viboral	Mínima Cuantía Nº 120-CS-007 de 2016	STA SYSTEM S.A.S.	$11.832.000	Un solo pago	3 meses

3.2. ¿Cómo adquieren las Entidades Estatales y las empresas privadas este bien, obra o servicio?

N°	MODALIDAD	ENTIDAD CONTRATANTE	N° CONTRATO Y VIGENCIAS	OFERENTE	OBJETO	FORMA DE PAGO	VALOR DE PAGO	TIEMPO DE EJECUCIÓN
1	Contratación Mínima Cuantía	MUNICIPIO DE FUNZA - ALCALDÍA DE FUNZA	MC-051-2023	PCM COLOMBIA, Bogotá	RENOVACIÓN DE LAS LICENCIAS ANTIVIRUS, ANTIMALWARE SOFWARE DE SEGURIDAD PARA LOS EQUIPOS DE CÓMPUTO DE LAS DIFERENTES DEPENDENCIAS DE LA ADMINISTRACION MUNICIPAL	Un solo pago	52.155.250	15 días
2	Contratación Mínima Cuantía	SECRETARIA DISTRITAL DE DESARROLLO ECONOMICO - ALCALDIA BOGOTÁ	SDDE-IPMC-014-2023	CLUSTER DE SERVICIOS SAS	Adquisición de licencias antivirus para la Secretaría Distrital de Desarrollo Económico	Un solo pago	52.000.000	3 meses



3	Contratación Mínima Cuantía	CONTRALORIA DEPARTAMENTAL DEL META	PCMC_014_2023	HIGH QUALITY SOLUTIONS LA EU	ADQUISICION DE LICENCIAS DE ANTIVIRUS PARA LA CONTRALORIA DEPARTAMENTAL DEL META	Pagos mensuales	32.000.000	1 año

4. ANALISIS DEL MERCADO

Hoy en día, la tecnología para el manejo de información, constituye la columna vertebral clave de cualquier negocio, la seguridad es considerada esencial y parte estratégica de todo negocio y organización, a nivel mundial, con el constante incremento de las cyber-amenazas, la protección de la información y propiedad intelectual; así como los datos empresariales, son considerados un asunto crítico. El robo y uso indebido de esta información, puede interrumpir la continuidad de la organización y la prestación de servicio a la comunidad.

Debido a las múltiples amenazas de virus informáticos que se presentan en los medios donde los sistemas están presentes, la Administración Municipal se ve obligada a adquirir unas nuevas licencias de antivirus, debido a que la actual se vence en junio de 2024, permitiendo la detección de virus informáticos, lo que contribuye a una mejor y más confiable preservación de la información.

Es importante tener en cuenta que, si una computadora no posee un antivirus, no tiene la capacidad de remover los virus que puedan llegar a ingresar al sistema y dejan la computadora completamente vulnerable a ataques tales como:

- Emails infectados, con anexos ejecutables peligrosos cuando son ejecutados.
- Sitios webs en internet infectados que lo llevan a ejecutar códigos maliciosos en su computadora, - Documentos de oficina, como Word y Excel, con Macros que atacan al Sistema Operativo.
- Spyware introducido por los virus para espiar datos personales.

Teniendo en cuenta las características y especificaciones técnicas del suministro a contratar, la metodología de análisis que sustenta el valor del presupuesto oficial se establece con base en 3 cotizaciones

1. La enviada por **TECNO TICS SOLUCIONES CORPORATIVAS,** valor de $37,778,000.00
2. La presentada por **TIC SOLUCIONES SAS,** por un valor de $34,999,793.64
3. Las presentadas por **SERVITT INGENIERIA SAS** $32,140,000.00

La metodología para establecer el valor estimado del proceso se efectuó con base al promedio de tres (3) cotizaciones presentadas por proveedores, por lo tanto, el presupuesto oficial estimado para la contratación asciende a la suma de Treinta y cuatro millones novecientos setenta y dos mil quinientos treinta y un pesos con sesenta y un centavos ($34.972.531,61).

ITEM	ENTIDAD	NIT	CLASIFICACIÓN EMPRESARIAL

			(Indicación de si es Micro, pequeña o mediana empresa)
1	TECNO TICS SOLUCIONES CORPORATIVAS	1017142370	Micro Empresa
2	TIC SOLUCIONES SAS	901452077-4	Micro Empresa
3	SERVITT INGENIERIA SAS	900926946	Micro Empresa

5. CONCLUSIÓN DEL ANÁLISIS DEL SECTOR

En el mundo actual, la tecnología de gestión de información es fundamental para cualquier negocio. La seguridad se ha convertido en un aspecto esencial y estratégico para todas las organizaciones globalmente. Ante el aumento constante de las ciberamenazas, proteger la información, la propiedad intelectual y los datos empresariales es ahora un tema crítico. El hurto y uso indebido de estos datos puede interrumpir la continuidad de una administración y afectar la prestación de servicios a la comunidad.

La información que produce y conserva la entidad es fundamental para su funcionamiento normal. Por ello, es crucial contar con una buena protección y establecer niveles de seguridad contra amenazas de virus informáticos. En este contexto, la adquisición de licencias antivirus con características avanzadas es de vital importancia para garantizar su protección.

Debido a las múltiples amenazas de virus informáticos presentes en los sistemas, la Administración Municipal se ve obligada a adquirir nuevas licencias de antivirus, con capacidad para el análisis no solo de las estaciones de trabajo sino también de la red en general. Esto permitirá una detección más efectiva de virus informáticos y contribuirá a una mejor y más confiable preservación de la información, tan importante en la entidad.

Wilmar Hernán Gómez Montoya
P.U Sistemas

Proyecto: Wilmar Hernán Gómez Montoya, supervisor
Reviso: Diego Alejandro Zapata – Abogado Contratista
Reviso: Dania G Castellanos- Pu Oficina de contratación
Aprobó: Sandra Milena Ramírez, Ordenadora del Gasto