El presente estudio se elabora en cumplimiento de los Principios que rigen la Contratación Estatal y en virtud de lo establecido en artículo 2.2.1.2.1.5.1 del Decreto Único Reglamentario 1082 de 2015; el cual se desarrolló en los siguientes términos:

DATOS GENERALES	
Fecha de emisión del estudio:	02/10/2026
Secretaría que elabora el estudio:	SECRETARÍA GENERAL DE LA CORPORACIÓN
Objeto de la contratación:	ADQUISICIÓN, RENOVACIÓN Y ACTUALIZACIÓN DE LICENCIAS DE SOFTWARE ANTIVIRUS Y DE LICENCIAS DE SOFTWARE, DESTINADAS AL SERVIDOR, COMPUTADORES DE MESA Y PORTÁTILES DE PROPIEDAD DE LA CORPORACIÓN CONCEJO MUNICIPAL DE MOSQUERA

1. LA DESCRIPCIÓN SUCINTA DE LA NECESIDAD QUE PRETENDE SATISFACER CON LA CONTRATACIÓN.

La Constitución Política en su artículo segundo establece como fines esenciales del Estado: servir a la comunidad, promover la prosperidad general y garantizar la efectividad de los principios, derechos y deberes consagrados en la Constitución.

El artículo 209 ibídem resalta que: "*La función administrativa está al servicio de los intereses generales y se desarrolla con fundamento en los principios de igualdad, moralidad, eficacia, economía, celeridad, imparcialidad y publicidad, mediante la descentralización, la delegación y la desconcentración de funciones. Por lo cual, las autoridades administrativas deben coordinar sus actuaciones para el adecuado cumplimiento de los fines del Estado. La administración pública, en todos sus órdenes, tendrá un control interno que se ejercerá en los términos que señale la ley*".

Por su parte en el Titulo XI "De la Organización Territorial", En su artículo 287 No. 3 señala: *"las entidades territoriales gozan de autonomía para la gestión de sus intereses dentro de los límites de la Constitución y la Ley, y que en virtud de tal autonomía tienen derecho de administrar los recursos y establecer los ingresos tributarios y no tributarios necesarios para el cumplimiento de sus funciones*".

El artículo 313 ibídem señala las funciones de los concejos Municipales, las cuales son desarrolladas bajo la premisa que estos son entidades administrativas con Personería jurídica propia, autonomía presupuestal, administrativa y financiera, que tiene a su cargo ejercer control político a las actividades que se desarrollan al interior de la Jurisdicción.

Que de conformidad con lo establecido en el artículo 38 de la ley 1952 de 2019, el Concejo Municipal tiene el deber de vigilar y salvaguardar los bienes y valores que le han sido encomendados y cuidar que sean utilizados debida y racionalmente, de conformidad con los fines a que han sido destinados. Así como responder por la conservación de los útiles, equipos, muebles y bienes confiados a su guarda o administración; y rendir cuenta oportuna de su utilización. Por tal motivo el legislador establece obligaciones en este caso a las entidades territoriales para tomar acciones tendientes a proteger sus activos y evitar malas conductas.

Que el Concejo Municipal de Mosquera, cuenta con un sin número de procesos sistematizados que requieren el servicio de Internet permanentemente las veinticuatro (24) horas del día, casos específicos son la página web institucional, peticiones quejas y reclamos, sistema de correspondencia y gestión documental, portal de contratación, soporte remoto del software, envió de informes a los diferentes entes de control, gobierno en línea, elaboración de actos administrativos propios de sus competencias, entre otros. Obteniendo de esta manera un eficaz rendimiento de la actividad funcional de la corporación, además de mejorar el desempeño de los servidores públicos y contratistas que prestan sus servicios en los procesos administrativos que desarrolla cada una de las áreas de la entidad. Por lo tanto, en aras de garantizar la seguridad, integridad de la información en la totalidad de los equipos de cómputo y minimizando los ataques informáticos y pérdidas de información, así como el correcto funcionamiento de los equipos de cómputo, se hace necesaria la adquisición de un sistema de seguridad y licencias para los equipos del concejo, que permitan la disponibilidad de los recursos informáticos y para llevar a cabo la realización las actividades propias de la entidad. Contando de esta manera con una herramienta que permita controlar, monitorear, administrar y proteger la información la cual debe ser implementada conforme las normas actuales que regulan la seguridad informática.

De acuerdo con lo anterior, en aras de prevenir ataques informáticos se requiere que las actuales políticas de seguridad sean reforzadas no solo con la implantación de planes de contingencia sino con una herramienta que permita garantizar la protección de la información y licenciamiento legal, y optimizar las herramientas informáticas con las que cuenta el Concejo Municipal, haciendo necesario la adquisición, Renovación y Actualización de licencias de software antivirus y de licencias de software Windows, Microsoft Office y Server, destinadas al servidor, computadores de mesa y portátiles de propiedad de la Corporación Concejo Municipal de Mosquera.

Finalmente, vale la pena señalar que, una vez revisado el Plan Anual de Adquisiciones de la entidad aprobado para la vigencia 2026, y publicado en el Sistema Electrónico para la Contratación Pública "SECOP II", se puede verificar que los bienes y servicios que se pretenden contratar se encuentran incluido en el mismo.

2. LA DESCRIPCIÓN DEL OBJETO A CONTRATAR IDENTIFICADO CON EL CUARTO NIVEL DEL CLASIFICADOR DE BIENES Y SERVICIOS.

2.1 OBJETO A CONTRATAR:

ADQUISICIÓN, RENOVACIÓN Y ACTUALIZACIÓN DE LICENCIAS DE SOFTWARE ANTIVIRUS Y DE LICENCIAS DE SOFTWARE, DESTINADAS AL SERVIDOR, COMPUTADORES DE MESA Y PORTÁTILES DE PROPIEDAD DE LA CORPORACIÓN CONCEJO MUNICIPAL DE MOSQUERA

2.2 CÓDIGO DEL CUARTO NIVEL DEL CLASIFICADOR DE BIENES Y SERVICIOS:

Clasificación UNSPSC	Segmento	Familia	Clase	Producto
Software de seguridad y protección	43000000	43230000	43233200	N/A
Mantenimiento de software de protección y seguridad	81000000	81110000	81112200	81112208
Servicio de actualización p parcheo de firmware	81000000	81110000	81112200	81112203
Actualización o parches de software	81000000	81110000	81112200	81112202
Servicio de licencias del software del computador	81000000	81110000	81112500	81112501

2.3 OBLIGACIONES DE LAS PARTES

2.3.1 OBLIGACIONES DEL CONTRATISTA: El contratista se obligará para con el Concejo, en relación directa con el objeto del contrato, a lo siguiente:

1. Tramitar las garantías exigidas por el Concejo y radicarlas en original ante la Secretaria General de la Corporación para su revisión y posterior aprobación.
2. Suscribir de forma conjunta con el supervisor designado el acta de inicio del contrato.
3. Garantizarque cada uno de los elementos a entregar cumplan con las especificaciones, requisitos y calidades establecidos en los estudios previos.
4. Efectuar la entrega, instalación y renovación de las licencias para los equipos de cómputo de propiedad del Concejo de Mosquera conforme a las cantidades descritas en las condiciones técnicas exigidas.
5. Efectuar la entrega, instalación y renovación de las licencias de antivirus para los equipos de cómputo de propiedad del Concejo de Mosquera conforme a las cantidades descritas en las condiciones técnicas exigidas.
6. Las licencias deben quedar a nombre del Concejo de Mosquera y tendrá una vigencia de 12 meses.
7. Prestar asistencia técnica y soporte al software de conformidad con los estándares de soporte definidos en este documento atendiendo los requerimientos de la entidad, sin costo adicional, durante 12 meses a partir de la fecha de instalación.
8. Elaborar un cronograma de forma conjunta con el supervisor del contrato, en donde se especifique el canal de comunicaciones, para atender las solicitudes de servicio técnico relacionado con el objeto del contrato.
9. Los requerimientos se harán mediante una llamada telefónica y/o correo de soporte (e-mail), garantizando un análisis y solución a los requerimientos, en un tiempo no mayor a 48 horas dependiendo de la prioridad del requerimiento.
10. Cubrir acciones correctivas a fallas presentadas en el software y asesoría en operación.
11. El software debe tener una garantía de 12 meses, la cual consta de Mantenimiento, Soporte, Actualizaciones y/o nuevos desarrollos sobre los módulos relacionados del software, sin costo adicional.
12. Realizar la entrega e instalación de las licencias de los equipos de cómputo de propiedad del Concejo de Mosquera dentro de los (5) cinco días hábiles siguientes de la suscripción de la aceptación de la oferta. Dicha instalación se realizará en las instalaciones del concejo ubicado en la Carrera 2 No. 2-68 (Parque principal - Mosquera), conforme a lo estipulado en el cronograma por el supervisor del contrato.
13. Responder por cualquier tipo de reclamación, judicial o extrajudicial, que instaure, impulse o en la que coadyuve el personal, los subcontratistas o un tercero contra el concejo, por causa o con ocasión del contrato.
14. Rendir y elaborar los informes, conceptos, estudios y demás trabajos que se le soliciten en desarrollo del contrato.
15. Obrar con lealtad y buena fe en las distintas etapas contractuales, evitando dilaciones y entrabamientos.
16. Cumplir con la totalidad de los alcances descritos en el contrato, sus anexos y demás soportes que lo anteceden, los cuales hacen parte integral del contrato.
17. Mantener vigentes todas las garantías que amparan el contrato en los términos de este, cuando en el mismo hayan sido requeridas.
18. Cumplir con las obligaciones laborales del personal contratado en la ejecución del contrato, si fuere el caso.

19. No acceder a peticiones o amenazas de quienes actúen por fuera de la ley con el fin de hacer u omitir algún hecho.
20. Mantener la reserva profesional sobre la información que le sea suministrada para el desarrollo del objeto del contrato.
21. Informar oportunamente al concejo sobre eventualidad que pueda surgir y que implique retraso en el desarrollo del contrato.
22. Acatar las instrucciones, sugerencias, observaciones y orientaciones escritas por el Supervisor del contrato.
23. Suscribir a tiempo las actas requeridas por parte del concejo (supervisor) como constancias de la ejecución del contrato.
24. Presentar las cuentas de cobro del valor del contrato, anexando todos sus soportes y documentos necesarios para ello, dentro de los plazos convenidos.
25. Acreditar sus pagos de SSI como cotizante independiente y cuando fuere el caso, se obliga a afiliar a los terceros que emplee para la ejecución del contrato a una entidad promotora de salud, de manera tal que se garantice la cobertura de los diferentes riesgos y en especial de accidentes de trabajo (Decreto 1295 de 1994), y a aplicar en forma estricta los controles y obligaciones que le competen, de acuerdo con lo establecido en la ley 789 de 2002, el artículo 23 de la ley 1150 de 2007 y el decreto 1703 de 2002 y demás normas concordantes o complementarias, en materia de aportes a seguridad social, y pago de parafiscales, vigentes a la fecha de presentación de la oferta y durante la vigencia del contrato.
26. Las demás que por ley o contrato le correspondan.

2.3.2 OBLIGACIONES DEL CONCEJO: El Concejo se obliga para con el contratista a lo siguiente:

1. Aprobar las garantías o las modificaciones a las mismas que el contratista constituya siempre que estas cumplan las condiciones de suma asegurada, vigencias y amparos, exigidas en el contrato.
2. Suscribir el acta de inicio de forma conjunta con el supervisor del contrato designado por el ordenador del gasto.
3. Pagar el valor del contrato en la cantidad, forma y oportunidades pactadas.
4. Brindar la colaboración y proporcionar la información y/o documentación que sea necesaria para el adecuado cumplimiento del contrato.
5. Cumplir y hacer cumplir las condiciones pactadas en el contrato y en los documentos que de él forman parte.
6. Resolver las peticiones y consultas que le haga el contratista dentro de los términos legales.
7. Suscribir las actas de terminación y liquidación del contrato previa verificación de los requisitos exigidos para tal fin, a través del supervisor del contrato.

2.4 TIPO DE CONTRATO: COMPRAVENTA

2.5 LUGAR DE EJECUCIÓN DEL CONTRATO: CONCEJO MUNICIPAL DE MOSQUERA

2.6 SUPERVISOR DEL CONTRATO: La supervisión del contrato estará a cargo de la Secretario General delegado mediante el documento escrito correspondiente. Para esos efectos, el supervisor estará sujeto a lo dispuesto en el numeral 1 del artículo 4º y numeral 1º del artículo 26 de la Ley 80 de 1993, la Ley 1150 de 2007, la Ley 1474 de 2011, decreto 1082 de 2015 y demás normas establecidas sobre la materia.

3. LAS CONDICIONES TECNICAS EXIGIDAS

3.1 ESPECIFICACIONES:

ÍTEM	ELEMENTO	DESCRIPCIÓN	UNID. MEDIDA	CANT.
1	Microsoft 365 Business Standard 1 usuario con vigencia de 1 año	Licencia por suscripción de Microsoft 365 Business Standard para un (1) usuario, con vigencia mínima de doce (12) meses, que incluya las aplicaciones de productividad de Microsoft en sus versiones completas de escritorio, además de los servicios empresariales asociados al producto. Licenciamiento - Producto: Microsoft 365 Business Standard. - Modalidad: Suscripción empresarial. - Cantidad: Una (1) licencia por usuario. - Vigencia: Doce (12) meses. - La licencia deberá permanecer activa y completamente funcional durante todo el periodo contratado. - Debe corresponder a una licencia original, legítima y reconocida directamente por Microsoft. - No se aceptarán versiones de prueba, educativas, personales, familiares, OEM, licencias perpetuas diferentes al producto solicitado ni mecanismos de activación no oficiales. - La licencia deberá permitir la instalación, activación, actualización y uso normal de las aplicaciones incluidas durante toda la vigencia.	Número de serie / código canjeable en el sitio web de Microsoft (portal.office.com) o cuenta de correo electrónico de nombre personalizable con dominio onmicrosoft.com	50

		- La oferta deberá corresponder a Microsoft 365 Business Standard con Microsoft Teams incluido; no se aceptará como equivalente la versión comercializada como "Microsoft 365 Business Standard sin Teams". Aplicaciones de escritorio incluidas La suscripción deberá incluir las versiones completas e instalables para escritorio de las principales aplicaciones de Microsoft 365, como mínimo: - Microsoft Word: creación, edición, revisión y administración avanzada de documentos. - Microsoft Excel: creación y edición de hojas de cálculo, fórmulas, funciones avanzadas, gráficos, tablas dinámicas, Power Query, análisis de información y automatización mediante macros compatibles. - Microsoft PowerPoint: creación, edición y presentación de contenidos, presentaciones corporativas, elementos multimedia, animaciones y transiciones. - Microsoft Outlook: administración de correo electrónico, calendario, contactos, reuniones y tareas. - Microsoft OneNote: creación, organización y sincronización de notas digitales. - Microsoft Access: creación y administración de bases de datos de escritorio. Disponible únicamente para equipos con Windows. Las aplicaciones deberán corresponder a las versiones mantenidas y actualizadas por Microsoft durante la vigencia de la suscripción. Instalación en equipos La licencia deberá permitir al usuario autorizado instalar las aplicaciones de Microsoft 365 hasta en: - Cinco (5) equipos PC o Mac. - Cinco (5) tabletas. - Cinco (5) dispositivos móviles. Para efectos de esta adquisición, el requisito principal corresponde a la instalación y uso de las aplicaciones completas en computadores de escritorio y portátiles. La licencia deberá permitir que el usuario pueda instalar nuevamente las aplicaciones en otro equipo cuando se realice cambio, renovación, mantenimiento o sustitución del computador, respetando los límites de dispositivos establecidos por Microsoft. Funcionamiento de las aplicaciones Las aplicaciones de escritorio deberán: - Instalarse localmente en el equipo. - Permitir la creación, apertura, modificación, almacenamiento e impresión de archivos. - Permitir trabajar con documentos almacenados localmente en el computador. - Funcionar sin conexión permanente a Internet una vez instaladas y activadas, sujeto a las verificaciones periódicas de licenciamiento establecidas por Microsoft. - Permitir posteriormente la sincronización de los cambios realizados cuando se restablezca la conexión a Internet. - Mantener compatibilidad con los formatos estándar de Microsoft Office, incluyendo, entre otros: DOCX, XLSX, PPTX y formatos compatibles. - Recibir actualizaciones de características, seguridad, estabilidad y correcciones proporcionadas por Microsoft mientras la suscripción se encuentre vigente. - Permitir instalación en español y disponer de los idiomas soportados por Microsoft 365. Microsoft Excel Debido al uso empresarial de la herramienta, la versión suministrada deberá corresponder a la aplicación completa de escritorio y permitir, entre otras funcionalidades: - Fórmulas y funciones avanzadas. - Tablas y gráficos. - Tablas dinámicas. - Segmentación y filtrado de información. - Importación y transformación de datos. - Power Query. - Validaciones y formatos condicionales. - Protección de hojas y libros.		

		- Manejo de libros con múltiples hojas. - Automatización mediante macros y VBA, cuando la plataforma y configuración utilizada sean compatibles. - Apertura y edición de archivos existentes de Microsoft Excel. - Exportación de documentos, incluyendo formatos PDF y CSV. No se considerará equivalente una solución que suministre únicamente la versión web de Excel. Microsoft Word La aplicación de escritorio deberá permitir, entre otras funciones: - Creación y edición avanzada de documentos. - Estilos, tablas, imágenes y elementos gráficos. - Combinación de correspondencia. - Control de cambios y comentarios. - Encabezados, pies de página y numeración. - Índices y tablas de contenido. - Revisión ortográfica y gramatical. - Protección y restricción de documentos. - Exportación de documentos a PDF. - Trabajo con documentos almacenados localmente. No se considerará equivalente una licencia que permita únicamente el uso de Word mediante navegador web. Microsoft PowerPoint La versión de escritorio deberá permitir: - Creación y edición completa de presentaciones. - Inserción de imágenes, tablas, gráficos, audio y vídeo. - Uso de animaciones y transiciones. - Creación y modificación de plantillas. - Presentación en pantalla completa. - Exportación a diferentes formatos compatibles. - Trabajo con archivos almacenados localmente. Microsoft Outlook Deberá incluir la aplicación Microsoft Outlook instalable en equipos de escritorio, permitiendo: - Administración de correo electrónico. - Calendario y programación de reuniones. - Contactos. - Gestión de carpetas de correo. - Reglas y organización de mensajes. - Búsquedas. - Firmas. - Administración de archivos adjuntos. - Trabajo con información sincronizada disponible localmente cuando no exista conexión a Internet. Actualizaciones Durante los doce (12) meses de vigencia, el producto deberá tener derecho a las actualizaciones proporcionadas por Microsoft, incluyendo: - Actualizaciones de seguridad. - Correcciones de errores. - Mejoras de estabilidad. - Actualizaciones de compatibilidad. - Nuevas características que Microsoft incorpore al producto y que correspondan al plan contratado. No deberán generarse cobros adicionales por las actualizaciones normales correspondientes a Microsoft 365 Business Standard durante el periodo contratado. Almacenamiento OneDrive La suscripción deberá incluir: - 1 TB de almacenamiento en OneDrive para la Empresa por usuario. - Sincronización de archivos entre el computador y almacenamiento en la nube. - Acceso a archivos desde dispositivos autorizados. - Posibilidad de compartir archivos y carpetas. - Historial y recuperación de archivos de acuerdo con las funcionalidades incluidas por Microsoft en el servicio contratado.		

		- Integración directa con Word, Excel, PowerPoint y demás aplicaciones compatibles de Microsoft 365. El uso de OneDrive será complementario y no deberá impedir el almacenamiento y trabajo con archivos directamente en el disco local del computador. Servicios empresariales complementarios La licencia deberá incluir adicionalmente los servicios correspondientes al plan Microsoft 365 Business Standard, entre ellos: - Microsoft Exchange Online. - Buzón empresarial de 50 GB por usuario. - Microsoft Teams. - Microsoft SharePoint Online. - OneDrive para la Empresa. - Aplicaciones web y móviles correspondientes al plan. Estos servicios se consideran complementarios a las aplicaciones instalables de escritorio requeridas. Requisitos generales del equipo Las aplicaciones deberán ser compatibles con los sistemas operativos actualmente soportados por Microsoft para Microsoft 365 empresarial. Como referencia para equipos Windows, se deberá disponer como mínimo de: - Sistema operativo Windows compatible y soportado por Microsoft 365. - Procesador de 2 núcleos y mínimo 1,6 GHz. - Mínimo 4 GB de memoria RAM para sistemas de 64 bits. - Espacio disponible en disco para la instalación de las aplicaciones. - Resolución mínima compatible con los requerimientos establecidos por Microsoft. - Conexión a Internet para descarga, instalación inicial, activación, actualizaciones y validaciones periódicas de la licencia. Para computadores Mac, deberá garantizarse compatibilidad con las versiones recientes de macOS soportadas oficialmente por Microsoft. Uso sin conexión a Internet Las aplicaciones Word, Excel, PowerPoint, Outlook y demás aplicaciones de escritorio incluidas deberán poder utilizarse sin una conexión permanente a Internet una vez instaladas y activadas. El equipo deberá conectarse periódicamente a Internet para comprobar el estado de la licencia y mantener las aplicaciones completamente habilitadas. La solución ofertada no podrá limitar el uso de Word, Excel o PowerPoint únicamente a través de un navegador web. Soporte La suscripción deberá contar durante su vigencia con: - Acceso al soporte oficial disponible para Microsoft 365. - Documentación oficial de instalación y utilización. - Actualizaciones oficiales del fabricante. - Recursos de soporte web. - Posibilidad de diagnóstico y recuperación de las aplicaciones cuando corresponda. Condiciones de entrega El proveedor deberá suministrar una suscripción completamente legal y verificable de Microsoft 365 Business Standard por doce (12) meses. No se aceptarán: - Licencias compartidas entre múltiples usuarios. - Licencias de segunda mano. - Licencias provenientes de programas académicos o educativos. - Versiones de evaluación o prueba. - Activadores, cracks, KMS no autorizado o cualquier otro mecanismo de activación diferente de los mecanismos oficiales de Microsoft. - Licencias Microsoft 365 Personal o Microsoft 365 Familia. - Licencias Office Home, Home & Student o equivalentes de uso doméstico como reemplazo del producto solicitado. - Licencias que permitan únicamente el acceso a aplicaciones web. - Productos diferentes a Microsoft 365 Business Standard, salvo autorización expresa de la entidad contratante. La activación deberá realizarse mediante los mecanismos oficiales establecidos por Microsoft y deberá mantenerse válida durante la totalidad de los doce (12) meses contratados.		

		Vigencia y continuidad Durante los doce (12) meses contratados, el usuario deberá disponer de acceso completo a las aplicaciones y funcionalidades correspondientes a Microsoft 365 Business Standard. Al finalizar el periodo contratado, la continuidad de las aplicaciones y servicios estará sujeta a la renovación de la suscripción correspondiente.		
2	Software de Antivirus Consola de Administración Endpoint Empresas 1 usuario con vigencia de 1 año	Licencia empresarial de software de seguridad para endpoints, con consola de administración centralizada y vigencia mínima de doce (12) meses, destinada a la protección de estaciones de trabajo, dispositivos y demás recursos tecnológicos de la organización frente a malware, ransomware, exploits, amenazas de red y otras amenazas informáticas. Licenciamiento - Modalidad: Licencia empresarial por suscripción. - Cantidad: Una (1) licencia por usuario o dispositivo, según el esquema de licenciamiento de la solución ofertada. - Vigencia: Doce (12) meses. - La licencia deberá permanecer activa y completamente funcional durante toda la vigencia contratada. - El software deberá ser original, legítimo y contar con soporte y actualizaciones oficiales durante el periodo contratado. - No se aceptarán versiones gratuitas, domésticas, educativas, de evaluación o productos destinados exclusivamente a uso personal. Consola de administración centralizada La solución deberá disponer de una consola para la gestión centralizada de la seguridad de los endpoints. La consola deberá permitir como mínimo: - Administración centralizada de los dispositivos protegidos. - Visualización del estado de seguridad de los endpoints. - Aplicación y modificación de políticas de seguridad. - Creación de grupos de dispositivos. - Administración de usuarios y permisos administrativos. - Ejecución remota de tareas de seguridad. - Programación de análisis. - Gestión de actualizaciones. - Visualización de alertas e incidentes. - Generación de reportes de seguridad. - Identificación de dispositivos con problemas de protección. - Consulta del estado de las licencias. - Administración remota de la configuración de seguridad. - Consola disponible mediante infraestructura local o servicio administrado en la nube. Protección antimalware La solución deberá proporcionar protección frente a amenazas informáticas conocidas y emergentes. Deberá incluir como mínimo: - Protección contra virus. - Protección contra troyanos. - Protección contra gusanos. - Protección contra spyware. - Protección contra adware malicioso. - Protección contra rootkits. - Protección contra ransomware. - Protección contra herramientas potencialmente maliciosas. - Detección de archivos sospechosos. - Protección en tiempo real. - Análisis bajo demanda. - Análisis programados. - Análisis de dispositivos extraíbles. - Cuarentena de archivos sospechosos. - Eliminación y desinfección automática de amenazas. Detección basada en comportamiento La solución deberá incorporar mecanismos de análisis de comportamiento que permitan detectar actividades sospechosas incluso cuando la amenaza no haya sido previamente identificada mediante firmas tradicionales. Deberá permitir:	Numero de Contrato / Número de Serie / Licencia Física	50

		- Monitorear procesos y aplicaciones en ejecución. - Detectar comportamiento anómalo. - Identificar técnicas utilizadas por malware moderno. - Detectar modificaciones sospechosas sobre archivos o configuraciones del sistema. - Bloquear automáticamente procesos identificados como maliciosos. - Detectar actividad asociada con ransomware. - Aplicar medidas automáticas de contención cuando se detecte una amenaza. Protección mediante aprendizaje automático La solución deberá incorporar capacidades de detección apoyadas en técnicas de aprendizaje automático o análisis avanzado para identificar amenazas nuevas, desconocidas o modificadas. Estas capacidades deberán complementar los mecanismos tradicionales de detección mediante firmas. Protección contra ransomware La solución deberá disponer de controles específicos orientados a prevenir, detectar y contener ataques de ransomware. Deberá incluir capacidades como: - Monitoreo de comportamiento sospechoso sobre archivos. - Detección de cifrado masivo no autorizado. - Bloqueo de procesos maliciosos. - Protección frente a modificaciones no autorizadas. - Prevención de ejecución de ransomware. - Aislamiento o contención del dispositivo cuando la solución lo permita. - Recuperación o reversión de cambios cuando la tecnología ofertada incluya esta capacidad. Protección web La solución deberá incorporar mecanismos para reducir el riesgo generado durante la navegación por Internet. Deberá permitir: - Bloqueo de sitios web maliciosos. - Detección de páginas fraudulentas. - Protección contra phishing. - Análisis de enlaces. - Bloqueo de descargas maliciosas. - Protección frente a scripts o contenidos potencialmente peligrosos. - Control de acceso a sitios web mediante categorías. - Creación de listas de sitios permitidos y bloqueados. - Aplicación de políticas diferenciadas por usuario o grupo. Control de aplicaciones La solución deberá permitir administrar el uso y ejecución de aplicaciones instaladas en los endpoints. Deberá permitir, como mínimo: - Identificación de aplicaciones instaladas. - Restricción de ejecución de aplicaciones no autorizadas. - Definición de aplicaciones permitidas. - Definición de aplicaciones bloqueadas. - Aplicación de reglas por grupos de usuarios o dispositivos. - Identificación de software potencialmente no autorizado. - Generación de eventos asociados con aplicaciones bloqueadas. Control de dispositivos La solución deberá proporcionar funcionalidades para administrar el acceso a dispositivos externos conectados a los equipos. Deberá permitir controlar, según las capacidades del sistema operativo: - Memorias USB. - Discos externos. - Dispositivos de almacenamiento removible. - Dispositivos Bluetooth. - Dispositivos portátiles. - Unidades ópticas. - Otros dispositivos periféricos. La herramienta deberá permitir establecer políticas de autorización, restricción o bloqueo. Firewall de endpoints La solución deberá incluir o integrarse con mecanismos de firewall para		

		estaciones de trabajo y endpoints. Deberá permitir: - Controlar conexiones entrantes y salientes. - Aplicar reglas de comunicación. - Identificar conexiones potencialmente riesgosas. - Administrar reglas desde la consola central. - Aplicar políticas diferenciadas por dispositivo o grupo. - Registrar eventos relacionados con tráfico de red bloqueado o permitido. Protección contra ataques de red La solución deberá disponer de mecanismos para identificar y bloquear actividades sospechosas provenientes de la red. Deberá proporcionar protección frente a: - Intentos de explotación de vulnerabilidades. - Escaneos o actividades sospechosas de red. - Conexiones potencialmente maliciosas. - Comunicaciones con infraestructura identificada como peligrosa. - Ataques dirigidos contra servicios disponibles en los equipos. Protección contra exploits La solución deberá disponer de mecanismos para detectar intentos de explotación de vulnerabilidades en aplicaciones o sistemas operativos. Deberá proteger, entre otros, aplicaciones de uso frecuente como: - Navegadores web. - Aplicaciones ofimáticas. - Lectores de documentos. - Clientes de correo electrónico. - Aplicaciones empresariales compatibles. Inteligencia de amenazas La solución deberá aprovechar servicios de inteligencia de amenazas actualizados para mejorar la identificación de: - Archivos maliciosos. - Direcciones IP potencialmente peligrosas. - Sitios web fraudulentos. - Dominios maliciosos. - Indicadores de compromiso. - Infraestructura asociada con amenazas informáticas. La información deberá actualizarse regularmente durante la vigencia de la licencia. Actualizaciones de seguridad La solución deberá recibir durante toda la vigencia: - Actualizaciones de firmas. - Actualizaciones de motores de detección. - Actualizaciones de inteligencia de amenazas. - Correcciones de seguridad. - Mejoras de estabilidad. - Actualizaciones del agente de seguridad cuando corresponda. Las actualizaciones normales del producto no deberán generar costos adicionales durante el periodo contratado. Protección del correo electrónico Cuando la solución ofertada incluya integración con servicios de correo electrónico, deberá proporcionar mecanismos para: - Detectar mensajes maliciosos. - Analizar archivos adjuntos. - Detectar enlaces potencialmente fraudulentos. - Identificar amenazas distribuidas mediante correo electrónico. - Reducir el riesgo de phishing. - Detectar contenido no deseado o spam. Protección de servidores Cuando sea compatible con el esquema de licenciamiento ofertado, la solución deberá disponer de mecanismos para la protección de servidores empresariales. Deberá permitir: - Protección antimalware. - Protección en tiempo real. - Análisis programados. - Exclusiones específicas para aplicaciones empresariales. - Administración centralizada.		

		- Configuración diferenciada de políticas. - Protección optimizada para cargas de trabajo de servidor. Compatibilidad con sistemas operativos La solución deberá ser compatible con los principales sistemas operativos empresariales actualmente soportados por el fabricante. Como mínimo deberá disponer de soporte para: - Microsoft Windows. - Microsoft Windows Server, cuando corresponda. - macOS. Será valorada adicionalmente la disponibilidad de agentes o mecanismos de protección para: - Linux. - Android. - iOS o iPadOS. Las funcionalidades disponibles podrán variar según las capacidades propias de cada sistema operativo. Integración con directorios empresariales La solución deberá permitir, cuando aplique: - Integración con servicios de directorio empresarial. - Importación o sincronización de usuarios, grupos o equipos. - Aplicación de políticas según grupos organizacionales. - Administración simplificada de dispositivos corporativos. Administración de vulnerabilidades La solución deberá incorporar o permitir funcionalidades para la identificación de vulnerabilidades en los endpoints. Deberá permitir: - Detectar software desactualizado. - Identificar aplicaciones con vulnerabilidades conocidas. - Identificar sistemas operativos que requieran actualizaciones. - Generar alertas de vulnerabilidades. - Priorizar vulnerabilidades según nivel de riesgo. - Consultar información desde la consola de administración. Administración de actualizaciones y parches La solución deberá permitir, directamente o mediante un módulo integrado: - Identificar actualizaciones pendientes. - Administrar parches de seguridad. - Programar instalación de actualizaciones. - Visualizar dispositivos con actualizaciones pendientes. - Generar reportes sobre el estado de actualización. - Gestionar actualizaciones de aplicaciones de terceros cuando esta funcionalidad esté incluida en la solución. Inventario de hardware y software La consola deberá permitir consultar información relacionada con los equipos administrados. Deberá incluir, cuando sea técnicamente posible: - Sistema operativo instalado. - Nombre del dispositivo. - Dirección IP. - Usuario asociado. - Aplicaciones instaladas. - Versiones de software. - Estado del agente de seguridad. - Información básica de hardware. - Fecha de última conexión. - Estado de actualización. Protección de dispositivos móviles Cuando la solución incluya soporte para dispositivos móviles, deberá permitir mecanismos de protección como: - Detección de aplicaciones potencialmente maliciosas. - Protección durante navegación web. - Protección contra enlaces fraudulentos. - Supervisión del estado de seguridad. - Administración desde la consola central. - Aplicación de políticas de seguridad compatibles con la plataforma. Protección frente a brotes de malware La solución deberá permitir establecer mecanismos de reacción automática		

		ante eventos de propagación masiva o brotes de malware. Deberá permitir acciones como: - Generación de alertas. - Incremento automático del nivel de protección. - Ejecución de análisis. - Aplicación de tareas de contención. - Bloqueo de amenazas detectadas. - Aplicación de políticas especiales ante incidentes. Respuesta automatizada ante incidentes La solución deberá permitir ejecutar acciones automáticas o administradas ante amenazas detectadas. Estas acciones podrán incluir: - Eliminación de archivos maliciosos. - Cuarentena. - Finalización de procesos. - Bloqueo de ejecución. - Restricción de comunicaciones. - Aislamiento del endpoint de la red cuando la solución lo soporte. - Ejecución de análisis adicionales. - Generación de alertas para el administrador. Capacidades de detección y respuesta La solución deberá permitir integración con funcionalidades de detección y respuesta para endpoints o tecnologías equivalentes. Se deberá permitir, cuando el nivel de licenciamiento lo incluya: - Investigación de incidentes. - Visualización de eventos relacionados. - Identificación del origen de una amenaza. - Seguimiento de procesos. - Consulta de indicadores de compromiso. - Contención de incidentes. - Respuesta remota. Integración con sistemas de monitoreo La solución deberá permitir integración con plataformas empresariales de monitoreo y gestión de eventos de seguridad mediante mecanismos estándar cuando corresponda. Será deseable contar con: - Exportación de eventos. - Syslog. - API. - Integraciones con plataformas de gestión de eventos e información de seguridad. - Integración con sistemas de automatización de seguridad. Generación de reportes La consola deberá permitir generar reportes relacionados con: - Estado de protección. - Dispositivos protegidos. - Amenazas detectadas. - Amenazas eliminadas. - Incidentes. - Vulnerabilidades. - Actualizaciones. - Estado de licenciamiento. - Aplicaciones instaladas. - Dispositivos con problemas. - Actividad de seguridad. Los reportes deberán poder visualizarse desde la consola y preferiblemente permitir su exportación a formatos estándar. Alertas y notificaciones La solución deberá permitir configurar alertas relacionadas con eventos relevantes, incluyendo: - Detección de malware. - Dispositivo sin protección. - Agente desactualizado. - Fallos de actualización. - Incidentes críticos.		

		- Vulnerabilidades. - Problemas de comunicación con los endpoints. - Próxima expiración de licencias. Protección contra manipulación El agente instalado deberá disponer de mecanismos para impedir que usuarios no autorizados puedan: - Desactivar la protección. - Detener servicios críticos. - Modificar políticas corporativas. - Desinstalar el agente sin autorización. - Alterar configuraciones de seguridad. Administración del cifrado Cuando la solución ofertada incluya funcionalidades de cifrado, deberá permitir la administración centralizada de mecanismos de cifrado disponibles en los sistemas operativos compatibles. La herramienta deberá facilitar: - Supervisión del estado del cifrado. - Aplicación de políticas. - Gestión de claves o mecanismos de recuperación cuando corresponda. - Reportes sobre el estado de protección. Rendimiento El software deberá estar diseñado para operar en entornos empresariales procurando un impacto controlado sobre el rendimiento de los equipos. La solución deberá permitir: - Programar análisis fuera de horarios críticos. - Configurar exclusiones. - Optimizar el consumo de recursos. - Administrar el uso de CPU durante análisis. - Ejecutar tareas administrativas de manera centralizada. Soporte técnico La licencia deberá incluir durante su vigencia: - Soporte técnico oficial o autorizado. - Acceso a documentación técnica. - Actualizaciones del producto. - Acceso a bases de conocimiento. - Mecanismos para reporte y atención de incidentes relacionados con el funcionamiento del software. Forma de entrega y activación La solución deberá entregarse mediante licenciamiento empresarial digital, válido por un periodo mínimo de doce (12) meses. La entrega podrá realizarse mediante: - Código o mecanismo digital de activación. - Correo electrónico de asignación. - Acceso a plataforma de administración. - Asignación de la licencia a la organización contratante mediante los mecanismos oficiales del fabricante. El proveedor deberá suministrar la información necesaria para verificar la correcta activación y vigencia de la licencia. Legitimidad del licenciamiento El proveedor deberá garantizar que las licencias suministradas sean legítimas y destinadas para uso empresarial. Cuando sea requerido por la entidad contratante, deberá suministrar evidencia documental que permita verificar la adquisición o asignación de las licencias mediante fabricante, mayorista, distribuidor o canal autorizado. No se aceptarán: - Licencias domésticas. - Licencias gratuitas. - Licencias educativas. - Versiones de prueba. - Licencias reutilizadas o de segunda mano. - Activaciones mediante herramientas no autorizadas. - Licencias compartidas de manera irregular. - Soluciones cuya licencia expire antes de completar los doce (12) meses contratados. Vigencia y continuidad		

		La solución deberá conservar todas las funcionalidades contratadas durante un periodo mínimo de doce (12) meses a partir de su activación. Durante este periodo deberán permanecer disponibles: - Protección de endpoints. - Consola de administración. - Actualizaciones de seguridad. - Inteligencia de amenazas. - Políticas de seguridad. - Reportes. - Soporte correspondiente al nivel de servicio contratado. Al finalizar el periodo contratado, la continuidad del servicio estará sujeta a la renovación de las licencias.		
3	Microsoft Windows 11 Pro x64 Bits	Licencia original de Windows 11 Pro para un (1) equipo, destinada a uso empresarial, con activación oficial y derecho de uso conforme a las condiciones establecidas por el fabricante. Licenciamiento - Producto: Windows 11 Pro. - Edición: Profesional. - Cantidad: Una (1) licencia por equipo. - Arquitectura compatible: 64 bits. - Idioma: español, con posibilidad de configuración de los idiomas soportados oficialmente. - La licencia deberá ser original, legítima y verificable. - La activación deberá realizarse mediante mecanismos oficiales. - No se aceptarán versiones de evaluación, educativas, de prueba, modificadas o activadas mediante herramientas no autorizadas. - No se aceptarán ediciones Home, Home Single Lenguaje, Educación, Enterprise o similares como sustitución, salvo autorización expresa de la entidad contratante. Tipo de licencia La licencia suministrada deberá corresponder a un esquema de licenciamiento autorizado para uso empresarial. Según la modalidad ofertada, podrá corresponder a: - Licencia digital. - Licencia OEM vinculada al equipo, cuando aplique. - Licencia comercial o equivalente autorizada por el fabricante. - Licenciamiento empresarial autorizado. El proveedor deberá indicar claramente la modalidad de licencia suministrada. Activación El sistema operativo deberá quedar correctamente activado y reconocido como legítimo. La activación deberá: - Realizarse mediante servidores o mecanismos oficiales. - Permanecer vigente conforme al tipo de licencia suministrada. - No depender de servidores de activación no autorizados. - No utilizar cracks, activadores, emuladores, herramientas KMS no autorizadas ni mecanismos similares. - Permitir la verificación del estado de activación directamente desde el sistema operativo. Funcionalidades empresariales La edición profesional deberá incluir las funcionalidades de seguridad, administración y productividad propias de Windows 11 Pro. Como mínimo deberá disponer de: - Unión a dominios empresariales. - Compatibilidad con servicios de directorio empresarial. - Administración mediante políticas de grupo. - Escritorio remoto en modalidad host. - Cifrado de unidad. - Herramientas avanzadas de administración. - Compatibilidad con entornos empresariales. - Control avanzado de cuentas y permisos. - Funcionalidades de virtualización disponibles en la edición profesional. - Administración de actualizaciones. - Protección integrada del sistema operativo.	Numero de Contrato / Número de Serie / Licencia Física	15

		Seguridad El sistema operativo deberá incorporar mecanismos de seguridad nativos que permitan proteger el equipo frente a amenazas y accesos no autorizados. Deberá incluir como mínimo: - Arranque seguro. - Compatibilidad con TPM. - Protección basada en hardware. - Protección contra malware integrada. - Firewall integrado. - Protección contra aplicaciones potencialmente peligrosas. - Control de cuentas de usuario. - Mecanismos de aislamiento y protección de credenciales. - Actualizaciones periódicas de seguridad. - Protección de navegación y reputación de aplicaciones, cuando aplique. Cifrado La edición profesional deberá incluir capacidades de cifrado de almacenamiento compatibles con el hardware del equipo. Deberá permitir: - Cifrado de unidades. - Protección de información almacenada. - Administración de claves de recuperación. - Integración con mecanismos de seguridad empresariales. - Protección de unidades internas y externas cuando sean compatibles. Administración mediante políticas El sistema operativo deberá permitir la aplicación de políticas administrativas para controlar el comportamiento del equipo. Deberá permitir, entre otras funciones: - Configuración de políticas de seguridad. - Restricciones de usuario. - Administración de contraseñas. - Configuración de bloqueo de pantalla. - Restricción de dispositivos. - Administración de servicios. - Configuración de actualizaciones. - Configuración de red. - Administración de permisos. - Aplicación de políticas mediante herramientas administrativas compatibles. Escritorio remoto La edición deberá permitir recibir conexiones mediante la funcionalidad de escritorio remoto compatible con Windows 11 Pro. Esta funcionalidad deberá permitir: - Administración remota del equipo. - Acceso autorizado mediante credenciales. - Conexiones dentro de redes empresariales. - Uso sujeto a las políticas de seguridad configuradas. Compatibilidad de hardware El sistema operativo deberá ser compatible con equipos que cumplan los requisitos mínimos oficiales. Como mínimo: - Procesador de 64 bits compatible. - Procesador de 1 GHz o superior. - Mínimo 2 núcleos. - Mínimo 4 GB de memoria RAM. - Mínimo 64 GB de almacenamiento disponible. - Firmware UEFI. - Compatibilidad con arranque seguro. - TPM versión 2.0. - Tarjeta gráfica compatible con DirectX 12 o superior. - Pantalla de alta definición compatible. Para uso empresarial se recomienda que los equipos dispongan de recursos superiores a los requisitos mínimos para garantizar un desempeño adecuado. Compatibilidad con aplicaciones El sistema operativo deberá permitir la instalación y ejecución de aplicaciones empresariales compatibles con Windows 11. Deberá permitir:		

		- Instalación de software de oficina. - Instalación de navegadores. - Instalación de sistemas contables y administrativos. - Instalación de software antivirus y de seguridad. - Instalación de controladores. - Instalación de herramientas empresariales. - Compatibilidad con periféricos y dispositivos soportados. Conectividad de red El sistema operativo deberá incluir funcionalidades para administración de redes empresariales. Deberá permitir: - Conexión mediante Ethernet. - Conexión mediante Wi-Fi. - Configuración de IPv4 e IPv6. - Configuración de DNS. - Conexión a redes privadas. - Configuración de redes empresariales. - Administración de perfiles de red. - Compatibilidad con VPN. - Integración con dominios y redes corporativas. Administración de usuarios El sistema operativo deberá permitir: - Creación de usuarios locales. - Administración de cuentas. - Asignación de permisos. - Creación de administradores y usuarios estándar. - Aplicación de restricciones. - Administración de credenciales. - Integración con servicios empresariales compatibles. Actualizaciones El sistema operativo deberá permitir recibir actualizaciones oficiales mientras la versión se encuentre dentro del ciclo de soporte correspondiente. Deberá incluir: - Actualizaciones de seguridad. - Correcciones de errores. - Actualizaciones de estabilidad. - Mejoras de compatibilidad. - Actualizaciones de controladores cuando estén disponibles. - Actualizaciones acumulativas. - Herramientas para administrar y programar actualizaciones. Copias de seguridad y recuperación El sistema operativo deberá incorporar herramientas que permitan: - Recuperación del sistema. - Restablecimiento del equipo. - Reparación de inicio. - Recuperación avanzada. - Creación o utilización de medios de recuperación. - Restauración ante fallos del sistema operativo. - Recuperación de configuraciones cuando las funcionalidades lo permitan. Virtualización Cuando el hardware sea compatible, la edición profesional deberá permitir el uso de herramientas de virtualización incluidas o soportadas por el sistema operativo. Deberá permitir: - Ejecución de máquinas virtuales. - Creación de entornos aislados. - Uso de funciones de virtualización de hardware. - Administración de recursos virtuales. Controladores y periféricos El sistema operativo deberá permitir la instalación y administración de: - Impresoras. - Escáneres. - Teclados. - Mouse. - Monitores.		

		- Dispositivos USB. - Adaptadores de red. - Dispositivos Bluetooth. - Periféricos compatibles. Los controladores deberán poder instalarse mediante los mecanismos oficiales del fabricante del equipo o del dispositivo. Forma de entrega La licencia podrá entregarse mediante: - Licencia digital. - Clave de producto oficial. - Preinstalación de fábrica, cuando corresponda. - Documento o comprobante digital de licenciamiento. - Asignación mediante canal autorizado. El proveedor deberá suministrar la información necesaria para verificar la autenticidad de la licencia. Legitimidad del software El proveedor deberá garantizar que la licencia suministrada sea original y destinada a uso empresarial. Cuando sea requerido, deberá suministrar evidencia de: - Adquisición por canal autorizado. - Documento de compra. - Identificación de la licencia. - Modalidad de licenciamiento. - Evidencia de activación legítima. No se aceptarán: - Licencias reutilizadas de procedencia no demostrable. - Claves obtenidas mediante canales no autorizados. - Licencias educativas. - Versiones de evaluación. - Copias modificadas. - Activaciones temporales. - Activadores externos. - KMS no autorizado. - Licencias que no permitan comprobar su legitimidad. Instalación Cuando el servicio contratado incluya instalación, el proveedor deberá: - Instalar Windows 11 Pro en el equipo. - Instalar los controladores correspondientes. - Ejecutar las actualizaciones disponibles. - Verificar el reconocimiento adecuado del hardware. - Confirmar la activación del sistema operativo. - Verificar conectividad de red. - Realizar una validación básica de funcionamiento. El sistema deberá entregarse operativo y sin software no autorizado. Vigencia de la licencia La licencia deberá otorgar el derecho de uso correspondiente a la modalidad suministrada. Cuando corresponda a una licencia perpetua u OEM, esta deberá permanecer válida conforme a los términos asociados al dispositivo o licencia. No se aceptarán licencias con periodos limitados de activación presentadas como licencias permanentes.		

El proponente debe certificar en su propuesta como mínimo lo siguiente:

- El proponente deberá anexar certificación de garantía por 1 año.
- Los oferentes deberán anexar carta de compromiso, en la cual certifique que los elementos a adquirir en el presente proceso deben traer su respectiva certificación de originalidad y/o factura de compra, esto con el fin de contar con las garantías pertinentes de los productos a adquirir, y avalar la autenticidad de los elementos entregados, para efectos de evitar la adquisición de falsificaciones o elementos remanufacturados, que al momento de su utilización imposibiliten el debido funcionamiento de los equipos

EXPERIENCIA DEL PROPONENTE

Los proponentes deberán acreditar experiencia cumpliendo con los siguientes requerimientos:

1. Número de contratos y valor mínimo en sumatoria:

GENERAL	MIPYMES	-
No. DE CONTRATOS	No. DE CONTRATOS	VALOR MÍNIMO EN SUMATORIA
1 a 2	1 a 3	75% del presupuesto oficial
3 a 4	4 a 5	100% del presupuesto oficial
5 a 6	6 a 7	150% del presupuesto oficial

2. El objeto y/o las actividades previstas en el (los) contrato (s) deberá (n) estar relacionado (s) con el objeto del presente contrato.

NOTA 1: El proponente debe soportar la información concerniente a la experiencia del mismo, mediante certificaciones expedidas por el contratante o el acta de liquidación del contrato. Los documentos suministrados deberán contener toda la información necesaria para que el Concejo de Mosquera pueda evaluar la experiencia del proponente.

Las certificaciones deberán contener: nombre o razón social completa de la entidad contratante, el nombre o razón social completa de la persona certificada, el objeto del respectivo contrato, el valor total del mismo, las fechas contractuales de iniciación y de terminación (día, mes, año), o de suspensión, si es el caso, la fecha de expedición de la certificación y el nombre, dirección y teléfono de la persona que la suscribe por parte de la entidad contratante. No se aceptarán para certificar experiencia, los contratos ejecutados por administración delegada o contratos de asistencia técnica, contratos ejecutados por cooperativas, subcontratos, auto certificaciones.

NOTA 2: Para acreditar la experiencia se podrá aportar las actas de recibo final y/o actas de terminación y/o liquidación, siempre y cuando se pueda realizar la verificación de objeto y/o actividades fecha de inicio, terminación, la persona contratante, contratista, valor del contrato.

NOTA 3: Cuando el proponente allegue, certificaciones en los que conste que participó como integrante de un consorcio o unión temporal, se tendrá en cuenta el valor y actividades exigidas de estas certificaciones en proporción al porcentaje de su participación en la unión temporal o consorcio. En el caso que el proponente no cumpla con la exigencia de la experiencia mínima solicitada, la propuesta será declarada inhábil técnicamente.

4. EL VALOR ESTIMADO DEL CONTRATO Y SU JUSTIFICACIÓN

4.1 VALOR DEL CONTRATO: CUARENTA Y OCHO MILLONES NOVECIENTOS DOCE MIL OCHOCIENTOS TREINTA Y TRES PESOS M /CTE. ($48.912.833,00). incluido IVA y demás impuestos.

4.1.1. JUSTIFICACIÓN: El valor se determinó en el análisis del sector el cual hace parte integral del expediente del presente proceso.

4.2 FORMA DE PAGO: La mencionada suma será cancelada al contratista en un único pago de acuerdo con los bienes y servicios efectivamente recibidos a satisfacción por el supervisor del contrato.

Dichos pagos se realizarán previo el lleno de los siguientes requisitos:

- Acreditar que dio cumplimiento a la publicación y divulgación proactiva de la Declaración de Bienes y Rentas, Registro de Conflicto de Interés y Declaración del Impuesto sobre la Renta y Complementarios, con la presentación del pantallazo de publicación que arroja el aplicativo dispuesto para el efecto.
- Presentación de informe de actividades y/o de ejecución del contrato
- Acreditación de pagos de seguridad social integral y parafiscales cuando corresponda.
- Certificación de cumplimiento expedida por parte del supervisor del contrato.
- Presentación de Factura cuando corresponda y/o cuenta de cobro cuando corresponda
- Copia del RUT.

Al pago se le efectuarán los respectivos descuentos por impuestos de ley y las contribuciones Municipales, así:

ESTAMPILLA	BASE GRAVABLE	TARIFA
ESTAMPILLA PRO-CULTURA	VALOR DEL CONTRATO	1 %
ESTAMPILLA PRO-DEPORTE	VALOR DEL CONTRATO	1%
ESTAMPILLA BIENESTAR ADULTO MAYOR	VALOR DEL CONTRATO	2%

Estas estampillas se liquidan antes de IVA.

Nota: Los valores enunciados pueden variar en cualquier momento y se aplicarán los que se encuentren vigentes al momento de realizar el pago.

4.3 ANTICIPO: N.A

5. EL PLAZO DE EJECUCIÓN DEL CONTRATO

5.1 PLAZO DE EJECUCIÓN: El plazo de ejecución será de cinco (5) días hábiles, a partir de la suscripción del acta de inicio.

6. EL CERTIFICADO DEL DISPONIBILIDAD PRESUPUESTAL QUE RESPALDA LA CONTRATACIÓN

6.1 NÚMERO DEL CDP:

- DIS – 20260000149
  – RUBRO 2.1.2.01.01.005.02.03.01.01.18.1.2.1.0.00.1101 (Paquetes de software, Fuente: 101 – Libre asignación. Valor $48.912.833,00

6.2 FECHA DEL CDP: 02/10/2026

6.3 MATRIZ DE RIESGOS: Este análisis se hace con el fin de exponerles a los oferentes la tipificación, estimación, asignación, impacto y tratamiento de los riesgos en la contratación; se desarrolla de conformidad con el artículo 2.2.1.1.1.6.3 del Decreto Único Reglamentario No.1082 de 2015 y el Manual para la identificación del Riesgo en los procesos de Contratación emitido por Colombia Compra Eficiente.

N°	Clase	Fuente	Etapa	Tipo	Descripción (Qué puede pasar y, cómo puede ocurrir)	Consecuencia de la ocurrencia del evento	Probabilidad	Impacto	Valoración del riesgo	Categoría	¿A quién se le asigna?	Tratamiento/Controles a ser implementados	Impacto después del tratamiento				¿Afecta la ejecución del contrato?	Persona responsable por implementar el tratamiento	Fecha estimada en que se inicia el tratamiento	Fecha estimada en que se completa el tratamiento	Monitoreo y revisión	
													Probabilidad	Impacto	Valoración del riesgo	Categoría					¿Cómo se realiza el monitoreo?	Periodicidad ¿Cuándo?

1	General	Externo	Ejecución	Operacional	Exista paro de transportadores por un término mayos a 15 días	Retraso en la entrega de los bienes objeto del contrato	2	3	5	medio	Contratista y Entidad	Extensión del plazo, modificación del cronograma de entrega	2	1	3	Riesgo bajo	Si	supervisor	Suscripción del Contrato	Liquidación del contrato	Seguimiento por parte del supervisor del contrato e informes del contratista	Durante la Ejecución del Contrato
2	General	Externo	Ejecución	Operacional	incompatibilidad de las licencias requeridas con los equipos de cómputo de propiedad del Concejo de Mosquera,	. Posibles pérdidas de información y el daño de los equipos por no contar con las licencias de antivirus o cual impida su correcto funcionamiento.	2	3	6	Alto	Contratista / Corporación	Verificar que las licencias aportadas correspondan a las características y requeridos por la entidad en la ficha técnica	2	2	4	Riesgo bajo	si	Supervisor – contratista	Suscripción del Contrato	Ejecución del contrato	Seguimiento por parte del supervisor del contrato	Durante el trámite del proceso y la ejecución del contrato
3	Especifico	Externo	Ejecución	Operacional	Inundación, incendio del Concejo Municipal de Mosquera	No se pueda hacer entrega de los elementos y la instalación de la cinta antideslizante objeto del contrato	1	4	5	medio	Entidad	Asegurar los edificios con pólizas, mantener extintores cargados y vigentes, mantener con seguridad y vigilancia.	1	2	3	Riesgo bajo	SI	Entidad	Suscripción del Contrato	Liquidación del contrato	Seguimiento por parte del supervisor del contrato	Durante ejecución contrato

4	General	Externo	Ejecución	Económico	Fluctuación de las tasas de cambio, variaciones cambiarias y financieras	Efectos desfavorables de la fluctuación de precios de los insumos posible iliquidez del contratista	4	3	7	Alto	Contratista	Es responsabilidad del contratista contar con una base financiera que le permita cumplir con las obligaciones adquiridas.	2	2	4	Riesgo bajo	NO	Contratista	Ejecución del contrato	Liquidación del contrato	Supervisar los costos los costos durante la ejecución del contrato	Durante el trámite del proceso y la ejecución del contrato

7. ANALISIS CRITERIOS DE DESEMPATE

En aplicación al artículo 2.2.1.2.4.2.17 numeral 1 del decreto 1860 de 2021, en caso de empate entre dos o más ofertas en el proceso de contratación se deberá hacer el siguiente análisis para efecto de poder acreditar dicho factor de desempate:

El análisis responde a las siguientes preguntas:

PREGUNTA 1. ¿El objeto del presente proceso corresponde a: 1? ¿Solo servicios? 2. Solo bienes 3. Objeto Mixto.

RESPUESTA 1. Realizado el análisis del objeto contractual, se concluye que el mismo corresponde a bienes.

PREGUNTA 2. ¿Para la ejecución del objeto del contrato es más relevante el suministro de bienes o servicios?

RESPUESTA 2: Bienes

8. LAS GARANTÍAS

Teniendo en cuenta la naturaleza del objeto contractual, la determinación de los riesgos previsibles que puedan afectar el equilibrio económico del contrato, la cuantía del mismo, la idoneidad, experiencia del contratista así como la forma de pago contemplada; se considera que con la finalidad de amparar los perjuicios de naturaleza contractual o extracontractual, derivados del incumplimiento del contrato, como requisito para su legalización, el contratista deberá constituir garantía única de conformidad con lo estipulado en el artículo 2.2.1.2.3.1.2 del decreto 1082 de 2015, la cual consiste en contrato de seguro contenido en una póliza, con los siguientes amparos:

AMPARO	SUFICIENCIA	VIGENCIA
CUMPLIMIENTO	En cuantía equivalente al 20% del valor del contrato	Con vigencia igual al plazo de ejecución del contrato y seis (6) meses más.
CALIDAD Y CORRECTO FUNCIONAMIENTO DE LOS BIENES Y EQUIPOS	En cuantía equivalente al 20% del valor del contrato	Con vigencia igual al plazo de ejecución del contrato y seis (6) meses más.

JAIRO ENRIQUE CASTAÑEDA REAL
Secretario General

NOMBRE: JUAN HERNÁNDEZ
CARGO: Asesor jurídico
ANÁLISIS Y ELABORACIÓN DEL ESTUDIO DE MERCADO.

FIRMA

	_____ FIRMA