PRESUPUESTO OFICIAL ESTIMADO	**$40.950.000 (Incluyen los diferentes tributos a que haya lugar conforme las responsabilidades tributarias del proveedor y los bienes y/o servicios a adquirir)**

1. DESCRIPCIÓN DE LA NECESIDAD

La Institución Universitaria Colegio Mayor de Antioquia, en aras de responder de manera óptima a los avances tecnológicos, se ve en la necesidad de adquirir herramientas que garanticen un eficiente sistema de protección de datos contra la mayoría de las amenazas informáticas. Las soluciones de ciberseguridad en la nube ofrecen una protección robusta para estaciones de trabajo y servidores, lo que incluye tanto entornos físicos como virtuales. Esto resulta crucial en un contexto donde los atacantes buscan vulnerabilidades en todos los puntos de acceso.

la Institución Universitaria Colegio Mayor de Antioquia requiere adquirir una tecnología EDR que permita ofrecer soluciones optimizadas y sofisticadas con una respuesta rápida y efectiva ante amenazas, monitoreando continuamente las actividades en los endpoints para detectar comportamientos sospechosos y responder a ellos en tiempo real, bloqueando automáticamente, lo que permitirá visualizar, comprender y remediar algún tipo de ataque y así proteger el entorno contra ataques futuros. Esto se ha convertido en una necesidad crítica para la Institución, buscando proteger los activos digitales y la información de la Entidad frente a las amenazas de ataques cibernéticos.

El sistema de protección debe estar integrado con inteligencia artificial, permitiendo que las soluciones de seguridad aprendan y se adapten a nuevas amenazas, mejorando la detección de ataques desconocidos y optimizando las decisiones sobre cómo responder a incidentes. Debe estar diseñado para equilibrar eficientemente la detección de ciberataques a través de diferentes dispositivos y sistemas operativos, asegurando que todos los puntos de acceso estén protegidos y que las amenazas sean identificadas rápidamente.

Cabe señalar que la adquisición de la renovación de estas licencias se justifica en la necesidad de proteger la información que resguarda la Institución, disminuyendo los altos riesgos de pérdida o fuga de información, contribuyendo al cumplimiento de los objetivos misionales y estratégicos de la Entidad y evitando la materialización de riesgos operativos.

El sistema de protección de ciberseguridad antivirus debe ser una solución avanzada que identifique comportamientos anómalos y potencialmente maliciosos, permitiendo una defensa más proactiva contra ataques como ransomware o vulnerabilidades de día cero. Además, debe contar con una arquitectura segura basada en la nube, que permita una gestión centralizada y facilite el monitoreo y la implementación de políticas de seguridad a gran escala.

Por lo tanto, dentro de la gestión y administración de la seguridad informática se debe proteger, en particular, los componentes que principalmente apoyan dicha gestión, como lo son los endpoints, servidores y sistemas de almacenamiento que soportan el funcionamiento de los sistemas de información de la Entidad. En consecuencia, la Institución Universitaria Colegio Mayor de Antioquia requiere adquirir una solución de protección avanzada que garantice la seguridad, integridad y disponibilidad de su infraestructura tecnológica.

Actualmente, la Institución Universitaria Colegio Mayor de Antioquia cuenta con una solución de seguridad informática de la marca Bitdefender, implementada desde el año 2024 en el marco del

contrato N.° CMA-SIP041-55-22952-2024, suscrito el 20 de diciembre de 2024. Las licencias actualmente disponibles cuentan con vigencia hasta el 27 de diciembre de 2026, por lo que se requiere adelantar el proceso contractual para su renovación, garantizando la continuidad del servicio de protección de los equipos, servidores y demás activos tecnológicos de la Institución. En este sentido, las licencias objeto de renovación deberán contar con vigencia a partir del 28 de diciembre de 2026, con el fin de evitar interrupciones en la protección de la infraestructura tecnológica y mantener las capacidades de prevención, detección y respuesta frente a las amenazas informáticas, en cumplimiento de las necesidades institucionales de seguridad de la información

Código del Proyecto 240140-2

2. DESCRIPCIÓN DEL OBJETO

Adquirir la renovación de las licencias del Antivirus ciberseguridad endpoint BitDefender Gravityzone Enterprise para la Institución Universitaria Colegio Mayor de Antioquia.

3. ALCANCE DEL CONTRATO

El contratista entregará el software endpoint antivirus a la Institución Universitaria Colegio Mayor de Antioquia, para su uso institucional con un periodo de licenciamiento por un (1) año que sea funcional y cumpla con los requisitos técnicos establecidos. El software antivirus deberá cumplir con las especificaciones técnicas y características acordadas, garantizando su adecuado funcionamiento para los fines institucionales establecidos, conforme a los estándares de calidad y las condiciones acordadas entre las partes. Con tecnología en la nube que brinde defensa integral y adaptativa para estaciones de trabajo y servidores, utilizando EDR y capacidades impulsadas por IA para protección de toda la infraestructura lógica institucional.

La vigencia de las licencias para renovación iniciará el día 28 de diciembre de 2026.

4. CONDICIONES TÉCNICAS EXIGIDAS

DESCRIPCIÓN GENERAL	UNIDAD DE MEDIDA	CANTIDAD	VALOR UNITARIO	VALOR TOTAL	CÓDIGO UNSPSC
Bitdefender Gravityzone Enterprise	UND	1.200	$ 34.125	$40.950.000	43233205
TOTAL PROPUESTA				**$40.950.000**	

NOTA 1: Los valores antes relacionados incluyen los diferentes tributos a que haya lugar conforme las responsabilidades tributarias del proveedor y los bienes y/o servicios a adquirir.

NOTA 2: En caso de hacer referencia a la marca de algún producto, ésta es meramente indicativa. La Institución recibirá los bienes en la medida en que cumplan condiciones equivalentes o superiores.

En caso de que las licencias a adquirir se encuentren excluidas de IVA según el artículo 476 del estatuto tributario, el proveedor deberá entregar un certificado en el cual indique la reglamentación de dicha norma por parte del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC).

GARANTÍA LEGAL. Es la obligación a cargo de todo productor y/o proveedor de responder por la calidad, idoneidad, seguridad y el buen estado y funcionamiento de los productos, según lo establecido en los artículos 7 a 11 de la Ley 1480 de 2011.

El proveedor debe garantizar que el producto ofrecido tenga las siguientes características:
- El producto debe ser del tipo 100% Cloud.
- Debe estar integrado en un solo producto no por separado, ni en la instalación todo debe ser en 1 solo agente de comunicación que se instala.
- El proveedor brindará capacitación en el manejo del sistema de ciberseguridad y asesoramiento y acompañamiento en la instalación de la solución.
- En la ficha técnica, en la consola de administración y en página web del Mayorista deben aparecer como mínimo los siguientes:
- En el sitio oficial de la marca para América o Latinoamérica debe visualizarse estas características básicas aquí descritas en este ítem.
- Debe ser en ambiente web 100% compatible con los navegadores más populares.
- Se deben poder administrar tanto servidores como estaciones.
- En la consola se debe informar siempre la versión existente y la fecha de actualización de la misma.
- El módulo de anti-ransomware debe ser configurable.
- Debe generar un estado de cuantas licencias se adquirieron y cuantas están en uso.
- La consola debe informar estado de cada agente conectado y generar logs de los mismos.
- Debe informar el estado de cada agente en la red si está conectado o desconectado de la consola.

En un reporte gráfico sobre las amenazas detectadas en los pcs.

Tareas a realizar desde la consola

Acciones
- Asignar u ordenar un escaneo rápido o completo a las máquinas.
- Enviar orden de actualización al agente.
- Renombrar los equipos en la consola para reconocimiento.
- Cambio de política inmediata con menú de despliegue.

Administración de Grupos
- Crear grupos personalizados, podrá visualizar cuántos miembros están incluidos y qué plantilla lo Aplica.
- Disponibilidad para observar qué equipos en específico están en cada grupo con sus nombres Correspondientes.
- Asignar políticas a los grupos antes mencionados.
- Ordenar un escaneo rápido o completo a todo el grupo o a todos los grupos.

Políticas del Endpoint.
- El producto debe permitir crear, duplicar o eliminar políticas de administración para grupos o pcs o servers específicos.

Alcances.

Configuración de políticas para Windows incluyendo:

- Antivirus, protección en tiempo real, análisis de archivos, análisis unidades externas, análisis inteligente, protección autorun.
- Antivirus de correo, análisis de correos, configuración de nivel de agresión, análisis de archivos comprimidos.
- Antispam, configuración de lista negra, lista blanca, blacklist de asuntos, dominios en lista blanca
- Firewall, escaneo de puertos, modo sigiloso, reglas manuales.
- Filtro de contenido.
- Control de aplicaciones.
- Control de dispositivos.
- Monitoreo de Archivos.
- Administración de contraseñas.
- Programación de análisis.
- Notificaciones.
- Monitoreo de actividad.
- Backup de archivos.
- Bloqueo del panel de control.

Antivirus

- Protección de los equipos en tiempo real.
- Escaneo de archivos.
- Escaneo de dispositivos externos.
- Escaneo Inteligente.
- Escaneo de Sistema Inactivo.
- Protección Autorun.
- Acción de primer análisis. Desinfectar, eliminar, cuarentena.
- Acción de segundo análisis. Desinfectar, eliminar, cuarentena.
- Exclusión de archivos por extensión o rutas.

Protección de Correo.

- Protección del correo electrónico a nivel de usuario.
- Análisis o escaneo de correos.
- Escaneo o análisis de archivos adjuntos, incluidos en los correos.
- Configuración de nivel de agresión en la protección de los correos. Low (1-2-3), Moderate (5-6-7), High (8-
9).
- Configuración manual de lista negra y lista blanca de correos.
- Configuración manual de lista negra de asuntos.
- Configuración manual de lista blanca de dominios.

Protección contra Ransomware.

- Bloqueo de ataques de Ransomware sin depender de firmas.
- Selección de tipo de respuesta frente a un ataque, bloquear o permitir.
- Configuración para activar un temporizador de respuesta en caso de que el usuario no tome acción, desde 10 segundos.
- Ingreso manual de direcciones o procesos que desea proteger frente a ataques de Ransomware

Protección de Spam.

- Configuración de blacklist de correos.
- Configuración de filtrado de correos por asunto, enviado directo a la Blacklist.
- Configuración de dominios que se desee permitir, añadiéndolos a una whitelist

Firewall

- Configuración de aplicación de la herramienta escaneo de puertos.
- Configuración de aplicación del modo Sigiloso.
- Ingreso manual de reglas basadas en protocolos, puertos, aplicaciones o personalizado.
- Configuración de dirección de tráfico, tipo de acción, puerto remoto, etc.
- Facilidad y practicidad para crear y eliminar reglas, dependiendo de las exigencias

Filtro de Contenido.
- Control de la navegación de los usuarios sin importar la conexión existente.
- Bloqueo total de navegación seleccionando todas las categorías disponibles por el producto.
- Permite restricciones y realizar un filtrado con al menos 50 categorías distintas.
- Control de navegación con dos modos, Bloqueo y Supervisión.
- Ingreso manual de páginas web que desea restringir, directo en la blacklist URL

Control de aplicaciones.
- Bloqueo de aplicaciones no autorizadas.
- Notificación de aplicación bloqueada al usuario, propiciada por el producto.
- Disponibilidad de al menos 14 categorías para la restricción en las aplicaciones.
- Alcance de bloqueo para navegadores, managers de descarga, herramientas de archivos y office, editores de texto, etc.
- Control más estricto y selectivo.

Control de dispositivos.
- Control de uso por decisión de 3 opciones, de los dispositivos de almacenamiento USB.
- Control de lectura sobre tarjetas inteligentes o Smart cards.
- Control de uso de dispositivos portátiles de Windows.
- Control de uso de CD/DVD ROM.
- Control de uso de conexión Bluetooth en los equipos.
- Bloqueo total de todos los dispositivos de almacenamiento.
- Agregar excepciones por solicitud del agente local.

Monitoreo de Actividad.
- Permite monitorear la actividad de los usuarios desde la consola.
- Configuración del tiempo de trabajo de los equipos que estarán en esa política.
- Configuración de toma de pantallazo en los equipos incluidos en la plantilla.
- Configuración de resolución del pantallazo y la frecuencia de la captura.
- Activación de tiempo de pantalla activa.
- Debe permitir generar la foto del usuario que está usando la máquina Monitoreo de Archivos.
- Debe poder identificar si un archivo se le aplicó copiar, pegar, reemplazar, duplicar, eliminar, crear, etc
- Debe permitir hacerle seguimiento a un archivo.
- Reportes de la información correspondiente a lo que suceda con cualquier archivo.
- Debe informar la fecha, el nombre del equipo, el tipo de acción aplicada a un archivo.

Protección de Desinstalación.
- Configuración de contraseña para evitar la desinstalación sencilla del producto o el intento de esta Actualizaciones.
- Actualización automática de todos los módulos y agentes en cada cliente.
- Actualización automática e incremental de cada hora, configurada.
- Disponibilidad de configurar la frecuencia de actualización, 1, 6, 8, 12, 24 horas

IPS/IDS
- Protección frente a ataques de DDoS y selección de nivel de agresividad. Low, Medium, High
- Protección frente a ataques de ICMP y selección de nivel de agresividad. Low, Medium, High.
- Protección frente a ataques RDP y selección de nivel de agresividad. Low, Medium, High.

- Protección frente a ataques SMB y selección de nivel de agresividad. Low, Medium, High.
- Protección frente a ataques SYNC FLOOD y selección de nivel de agresividad. Low, Medium, High,
- Configuración de Intervalo de tiempo para prevención de intrusiones. Desde 0 a 20 minutos
- Inspección profunda de paquetes disponible para implementar.

Backup de archivos.

- Permite realizar un backup de archivos de cada pc o server de la red con espacio de 5.0 Gb de espacio en la nube por usuario.
- Permite configurar la ubicación final donde se almacenará en la máquina.
- Permite elegir el escritorio, documentos o descargas como ubicación del backup al menos por defecto.
- Permite seleccionar por tipo de extensión los archivos que se almacenarán en el backup.
- Permite ingresar manualmente extensiones que desee el administrador incluir en el backup.
- Almacenamiento del backup en la nube de la consola por cada equipo.
- Disposición de la capacidad máxima en la consola para almacenar el backup cloud.
- Permite definir por equipo la capacidad máxima para almacenar el backup.
- Permite agregar más espacio de memoria por cada máquina manualmente en KB.
- Fácil acceso a los documentos almacenados en la nube de la consola y simplicidad para descargarlos.

Inventario de HW y SW

- **Visualización de inventario de HW desde el apartado de Endpoints registrados en la consola, indicando:**

a. Información del sistema.
* Nombre del computador.
* Dominio o grupo.
* Sistema operativo indicando versión.
* Arquitectura del Sistema Operativo.
* Fecha de instalación del sistema operativo.

b. Inventario de Hardware.
* Procesador.
* Fabricante BIOS.
* Fabricante CPU.
* Memoria RAM.
* SLOTS de RAM.
* Tamaño del disco duro.
* Mac Adress.
* Espacio libre en disco.
* Espacio libre en RAM.
* Serial de la Bios.
* Modelo del pc.
* ID de procesador.
* Número de núcleos de Procesador.
* Capacidad de memoria ROM.
* Capacidad de memoria RAM.
* Fabricante Motherborad.

Toda esta información se debe poder exportar como un archivo con extensión *xls.

* Visualización de inventario de SW desde el apartado de Endpoints registrados en la consola, indicando:

a. Información del sistema.
* Nombre del software.
* Versión.
* Tamaño del archivo.
* Fecha de instalación.
Empresa desarrolladora.
Toda esta información se debe poder exportar como un archivo con extensión *xls.
DLP control de fuga de información
El producto debe tener componentes que permitan el control de fuga de información como:
* Bloquear el uso de la tecla Imp Pnt, print Screen o pantallazo
* Bloquear el uso de impresoras o actividad de impresión
* Bloqueo de transferencia de información por IP privada y pública
* Bloqueo de transferencia de información por clientes FTP
* Bloqueo de transferencia de información vía SSH
* Bloqueo de transferencia de información vía TELNET y Servicios Web
* Bloqueo de uso de portapapeles
* Selección de archivos por extensión, clasificados por categorías para evitar la fuga de información de estos.
Notificaciones
El producto debe permitir enviar notificaciones automáticas, a un correo definido por
* Notificar cuando una política es creada.
* Notificar cuando un virus es encontrado en los equipos.
* Notificar si un correo de spam fue encontrado en los equipos.
* Notificar cuando algún endpoint viole la política de control web.
* Notificar cuando algún endpoint viole la política de control de aplicaciones.
* Notificar cuando desde algún equipo intente desinstalar.
* Notificar cuando se infringe la regla de firewall en el punto final.
* Notificar cuando un grupo es creado en consola.
* Notificar cuando un endpoint es cambiado de grupo.
* Notificar cuando la política de un grupo ha sido cambiada.
* Notificar cuando el 90 por ciento de las licencias han sido usadas.
Parches de Seguridad.
* Permite instalar parches de seguridad al menos de manera local.
*Genera un listado para saber si todos los parches de seguridad fueron instalados.
Análisis de Vulnerabilidades.
* Permite hacer búsqueda de vulnerabilidades al menos de manera local.
*Genera un listado de vulnerabilidades y permitir remediar de inmediato.
Trituradora de Archivos.
Con el fin de evitar la recuperación de archivos confidenciales eliminados desde la papelera de reciclaje es Importante.
que el producto permita eliminar archivos a selección de manera definitiva sin opción de recuperación.
Reportes.
* Envío de reportes vía correo o email.
* Reportes generados en formato Excel.
* Programación de reportes automáticos, diarios o semanales, configurando hora y minutos.
* Disponibilidad de reporte de escaneo.

* Disponibilidad de reporte Control Web.
* Disponibilidad de reporte Control de Aplicaciones.
* Disponibilidad de reporte de Firewall.
* Disponibilidad de reporte DLP.
* Disponibilidad de reporte Backus.
* Disponibilidad de reporte Protección de Correo.
* Disponibilidad de reporte de Control de Dispositivos.
* Disponibilidad de reporte de Protección frente a Desinstalación.
* Disponibilidad de reporte Monitoreo de Archivos.
* Disponibilidad de reporte Monitoreo de Actividad.

Las licencias deberán activarse según la necesidad de la institución y dentro del año 2026, esta activación deberá ser coordinada con la supervisión del contrato, garantizando que la institución no deje de contar con dichos servicios.

Los proponentes deberán cumplir con los siguientes requisitos habilitantes:

-Aportar documento con la manifestación bajo la gravedad de juramento (en caso de persona jurídica, suscrito por su representante legal o delegado) de si se encuentra o no obligado a contar con el Plan Estratégico de Seguridad Vial, indicando su nivel de implementación de conformidad con la Resolución 20223040040595 de 2022 del Ministerio de Transporte.

NOTA 2: Toda empresa cuya planta de vehículos sea superior o igual a diez (10) vehículos y dos (2) conductores debe contar con PESV (Plan Estratégico de Seguridad Vial) según la Ley 1503 de 2011, Decreto 2851 de 2013, Resolución 40595 de 2022

Requisitos de ejecución:

El oferente deberá cumplir con los siguientes lineamientos.

- Certificado de implementación del Sistema de Gestión de Seguridad y Salud en el Trabajo emitido por la ARL.
- Carta de designación del responsable del sistema de gestión de la seguridad y salud en el trabajo firmada por el representante legal.

Nota: Todas las personas que ingresen a desarrollar actividades o dejar suministros deberán tener la seguridad social vigente.

4.1. EXPERIENCIA

Con el propósito de garantizar la calidad e idoneidad del proponente, se definen las siguientes condiciones para certificar la experiencia acreditada.

El proponente deberá acreditar experiencia mediante la presentación de dos **(2)** certificados de contratos ejecutados con personas naturales o jurídicas (privadas o públicas), cuyo objeto o actividades se encuentren relacionadas con el objeto del presente procedimiento de contratación,

debidamente certificados por la Entidad contratante. Cada contrato aportado deberá tener un valor igual o superior al presupuesto oficial del presente procedimiento.

La experiencia se verificará con base en certificados expedidos por el contratante o documentos contractuales que permitan evidenciar de manera clara la ejecución del contrato.

NOTA 1: Las certificaciones expedidas en el extranjero deberán estar debidamente legalizadas, según lo estipulado en los artículos 74 y 251 del Código General del Proceso (Ley 1564 de 2012), el artículo 480 del Código de Comercio y la Resolución 1959 del 3 de agosto de 2020, proferida por el Ministerio de Relaciones Exteriores de Colombia. Adicionalmente para efectos de verificación de salarios mínimos mensuales legales vigentes, se tendrá en cuenta la tasa de cambio de la fecha en que se suscribió el contrato.

Documentos válidos para acreditar experiencia

1. Contratos celebrados con entidades públicas
La experiencia podrá acreditarse mediante cualquiera de los siguientes documentos:
-Certificación expedida por la entidad contratante.
-Copia del contrato junto con acta de liquidación.
-Copia del contrato junto con acta de recibo final o certificación de cumplimiento.
-Para contratos de mínima cuantía, se deberá aportar: invitación pública, comunicación de aceptación de la oferta, y acta de liquidación o documento equivalente de cierre o recibo final.

2. Contratos celebrados con personas naturales o jurídicas privadas

Cuando se trate de contratos celebrados con particulares y estos no cuenten con acta de liquidación, la experiencia se acreditará mediante certificación expedida por el contratante, acompañada, de ser necesario, de copia del contrato o documento equivalente que permita verificar la información requerida.

Las certificaciones o documentos aportados deberán contener como mínimo la siguiente información:

✓ Número del contrato, cuando aplique.
✓ Nombre o razón social de la empresa o persona contratante.
✓ Objeto y/o actividades del contrato.
✓ Valor del contrato.
✓ Plazo de ejecución del contrato.
✓ Fecha de iniciación del contrato.
✓ Fecha de terminación del contrato.
✓ Nombre y firma de la persona que expide la certificación.
✓ Si los contratos fueron ejecutados bajo la modalidad de consorcio o unión temporal, deberá informar el porcentaje de participación y el valor correspondiente a cada contratista en forma separada. Para efectos de verificación de los requisitos aquí exigidos, se tendrá en cuenta el valor correspondiente a la participación.

La Institución se reserva el derecho de verificar la autenticidad de la información aportada.

5. ANÁLISIS QUE SOPORTA EL VALOR ESTIMADO DEL CONTRATO

Para determinar las variables y estimar el valor total del presupuesto se tuvo en cuenta la necesidad real y demostrada a partir de la adquisición de software antivirus BitDefender, para uso institucional con un periodo de licenciamiento por un año; posteriormente se solicitó cotización a diferentes empresas del mercado con amplia experiencia y se procedió a analizar las cotizaciones presentadas, y con base en estas se tomó el menor valor de las cotizaciones para determinar el presupuesto oficial.

Menor Valor

	Persona natural o jurídica que cotizó	Valor total	Menor Precio
1	Cotización No. 1: Stratech Fecha de cotización: 13/10/2026	$ 41,040,000.00	
2	Cotización No. 2: Senetco Fecha de cotización: 13/10/2026	$ 40,950,000.00	**X**
3	Cotización No. 3: Star solutions t.i Fecha de cotización: 13/10/2026	$ 42,600,000.00	

Estas cotizaciones fueron recibidas en igualdad de condiciones, logrando con este procedimiento cotización de todos los elementos del listado y obtener un precio acorde con las condiciones de mercado y que se ajuste a las necesidades propias de la compraventa requerida y al presupuesto de la Institución.

VER ANEXO DE ESTUDIO DE MERCADO.

6. DISPONIBILIDAD PRESUPUESTAL

DISPONIBILIDAD PRESUPUESTAL: N° 1334 del 26 de octubre de 2026
NOMBRE DEL RUBRO PRESUPUESTAL: TECNOLOGIA
RUBRO PRESUPUESTAL:192110101400100121202020008

7. FORMA DE PAGO

La Institución Universitaria Colegio Mayor de Antioquia, pagará al contratista el valor del contrato de conformidad con los bienes efectivamente entregados por concepto de software antivirus BitDefender, para uso institucional por un periodo de licenciamiento de un año previa presentación de la factura o documento equivalente, con el visto bueno de la supervisión designada. El pago se hará efectivo dentro de los treinta días calendario siguientes a la facturación y previo recibo a satisfacción por parte del supervisor del contrato. No habrá lugar a anticipos.

Para iniciar el proceso de pago es necesario:
- Previamente enviar el formato de inscripción de cuenta bancaria, acompañado del certificado de cuenta bancaria emitido por la entidad financiera correspondiente al correo tesoreria@colmayor.edu.co
- Enviar factura electrónica al correo proveedores@colmayor.edu.co según los requisitos de la Resolución 165 del 2023 expedida por la DIAN.
- Aportar el RUT actualizado.

- Anexar certificado de paz y salvo en pago de parafiscales y seguridad social con vigencia no superior a un mes desde la expedición de la comunicación de aceptación, firmada por el representante legal y/o revisor fiscal (con sus respectivos documentos; cédula de ciudadanía, tarjeta profesional y certificado de la junta central de contadores).	
8. PLAZO DE EJECUCIÓN	El plazo será desde el inicio de ejecución en la plataforma transaccional Secop II, previa aprobación de las garantías y expedición del Registro Presupuestal, hasta el 31 de diciembre de 2026
9. SUPERVISIÓN	La ejercerá el líder de tecnología y medios audiovisuales como supervisor principal y el líder de infraestructura física, como supervisor suplente, por ser estas las dependencias que se encuentran en relación directa con las actividades a desarrollar y/o bienes a suministrar, quien deberá realizar el control y vigilancia adoptado por el Colegio Mayor de Antioquia. Además, debe cumplir con lo previsto en la Resolución No 134 del 21 de abril de 2023, por medio de la cual se adopta el manual de supervisión e interventoría para la INSTITUCIÓN UNIVERSITARIA COLEGIO MAYOR DE ANTIOQUIA, la cual puede encontrar en el aplicativo G + de la Institución. La presente designación se encontrará vigente desde la aceptación del contrato por las partes en la plataforma transaccional SECOP II hasta el cierre del expediente.
Se solicitará el certificado de registro presupuestal a la Oficina de Presupuesto de la Institución Universitaria Colegio Mayor de Antioquia.	

10. FUNDAMENTOS JURÍDICOS QUE SOPORTAN LA MODALIDAD DE SELECCIÓN

La presente contratación debe fundamentarse en lo prescrito en La Ley 1474 de 2011 "Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública", la cual contiene disposiciones en materia de contratación pública reglamentadas por el Gobierno Nacional, dentro de las cuales se encuentra la modificación al artículo 2° de la Ley 1150 de 2007, mediante la cual se incorpora como nueva modalidad de selección la contratación de "Mínima Cuantía."

Adicionalmente, el Decreto 1082 de 2015 "Por el cual se reglamenta el sistema de compras y contratación pública", en su artículo 2.2.1.2.1.5.1 (modificado por el artículo 2 del Decreto 1860 de 2021) y siguientes dispone el procedimiento para la contratación de Mínima Cuantía, cuyas reglas se determinan exclusivamente en el artículo 94 de la Ley 1474 de 2011 y en el citado capítulo.

En el presente proceso de selección se dará aplicación a lo establecido en el artículo 2.2.1.2.4.2.2 del Decreto 1082 de 2015, modificado por el artículo 5 del Decreto 1860 de 2021, respecto a la convocatoria de MIPYMES, toda vez, que realizada la conversión del dólar a moneda Nacional según la tasa cambiaria válida a la fecha de convocatoria del presente procedimiento de selección, se tiene que el presupuesto oficial corresponde hasta la suma de **CUARENTA MILLONES NOVECIENTOS CINCUENTA MIL PESOS ML ($40.950.000)**, lo cual se encuentra por debajo de los CIENTO VEINTICINCO MIL DÓLARES AMERICANOS (US $125.000) que para dicho efecto establece el Ministerio de Industria y Comercio.

11. DE LOS ACUERDOS Y TRATADOS INTERNACIONALES EN MATERIA DE CONTRATACIÓN PÚBLICA

De conformidad con el artículo 2.2.2.1.8.5. del Decreto 1082 de 2015 y las modificaciones introducidas por el Decreto 0142 de 2023, se hizo un estudio de los tratados, y se señala que a la Institución Universitaria Colegio Mayor de Antioquia aplica el Tratado de Libre Comercio con el Triángulo del Norte estipulada en el Capítulo 11. En este sentido, les aplica el acuerdo específico entre Colombia-Guatemala y Colombia-El Salvador, según lo pactado en el Anexo 11.1. del acuerdo comercial.

12. TIPIFICACIÓN, ESTIMACIÓN Y ASIGNACIÓN DE RIESGOS

El Decreto 1082 de 2015 define "riesgo", como un evento que puede generar efectos adversos y de distinta magnitud en el logro de los objetivos del procedimiento de contratación o en la ejecución de un contrato.

De esta manera, uno de los objetivos del sistema de compras y contratación pública es el manejo del riesgo del procedimiento de contratación. En consecuencia, la administración o el manejo del riesgo debe cubrir desde la planeación hasta la terminación del plazo, la liquidación del contrato, el vencimiento de las garantías de calidad o la disposición final del bien y no solamente la tipificación, estimación y asignación del riesgo que pueda alterar el equilibrio económico del contrato.

La identificación y valoración de los riesgos se realiza conforme a los lineamientos de Colombia Compra Eficiente y a los principios de planeación, responsabilidad, eficiencia y asignación objetiva del riesgo, determinando la parte que cuenta con mayor capacidad para su prevención, control y mitigación.

El artículo 2.2.1.1.2.1.1., numeral 6, del Decreto 1082 de 2015 establece el deber de la Institución de realizar un análisis del riesgo y la forma de mitigarlo. Realizado el estudio requerido, la entidad ha logrado identificar y estimar riesgos previsibles con posibilidad de materialización contractual, los cuales se señalan en la matriz de riesgo que se adjunta con el estudio previo para el presente procedimiento de contratación (ver Anexo).

13. EXIGENCIA DE GARANTÍAS

De conformidad con lo preceptuado en el artículo 7º de la Ley 1150 de 2007, el Decreto 1510 de 2013 y el Decreto 1082 del 26 de mayo de 2015, se deberá constituir póliza en una compañía de seguros legalmente reconocida en Colombia así:

GARANTÍA DE SERIEDAD DE LA OFERTA. La garantía de seriedad de la oferta debe estar vigente desde la presentación de la oferta y hasta la aprobación de la garantía de cumplimiento del contrato y su valor debe ser de por lo menos el diez por ciento (10%) del valor de la oferta.

GARANTÍA DE CUMPLIMIENTO. LA PÓLIZA DE CUMPLIMIENTO DEL CONTRATO deberá cubrir:

CUMPLIMIENTO. Que cubrirá a la Institución de los perjuicios derivados de: a) incumplimiento total o parcial del contrato, cuando el incumplimiento es imputable al contratista, b) el cumplimiento tardío o defectuoso del contrato, cuando el incumplimiento es imputable al contratista, c) los daños imputables al contratista por entregas parciales de la obra, cuando el contrato no prevé entregas parciales y d) el pago del valor de las multas y la cláusula penal pecuniaria. Esta garantía se constituirá por el **VEINTE POR CIENTO (20%)** del valor del contrato, con una vigencia igual a la del plazo del contrato y dieciocho (18) meses más.

CALIDAD Y CORRECTO FUNCIONAMIENTO DE LOS BIENES. Que cubrirá a la Institución por los perjuicios derivados de la deficiente calidad del bien entregado. Esta garantía se constituirá por el **DIEZ POR CIENTO (10%)** del valor del contrato, con una vigencia igual a la del contrato y veinticuatro (24) meses más. Esta garantía se aplicará sin perjuicio de la garantía legal regulada en el artículo 11 de la Ley 1480 de 2011.

El presente estudio previo se profiere el día 29 octubre de 2026.

Jose Leonardo Parra Amariles
Líder de Tecnología y medios audiovisuales

Diana Patricia Gómez Ramírez
Secretaria General

Paola Vásquez Álvarez
Directora Jurídico

Stefanny Alfonso Cely
Abogada Dirección jurídica

Vo. Bo. SST y Gestión Ambiental

Vo. Bo. Financiera