ALCALDÍA MAYOR
DE BOGOTÁ D.C.
MOVILIDAD
Unidad de Mantenimiento Vial

RESPUESTA A LAS OBSERVACIONES PRESENTADAS AL PROYECTO PLIEGO DE CONDICIONES DEL PROCESO DE SELECCIÓN ABREVIADA SUBASTA INVERSA UMV-SASI-008-2026

OBJETO: 8089-053 SUSCRIPCIÓN, IMPLEMENTACIÓN Y SOPORTE DE UNA PLATAFORMA DE CIBERSEGURIDAD DE NUEVA GENERACIÓN PARA LA PROTECCIÓN INTEGRAL DE LOS ACTIVOS DIGITALES DE LA UAERMV, ORIENTADA A LA PREVENCIÓN, DETECCIÓN Y RESPUESTA AVANZADA ANTE AMENAZAS EN ENDPOINTS Y PREVENCIÓN DE PÉRDIDAS DE DATOS

Fecha: noviembre de 2026

Observación N.° 1	**GRUPO LUMA — Técnico**
Observación presentada	Páginas 8, 12, 16-19 y Requerimiento General No. 6 (Pág. 27): "La solución debe ser una sola licencia, que incluya todo lo solicitado sin módulos adicionales... Se permitirá el uso de componentes complementarios cuando sean necesarios para cumplir las capacidades solicitadas, siempre que estén incluidos en el licenciamiento ofertado.. La arquitectura requerida abarca dos dominios tecnológicos especializados y diferenciados en la industria: Endpoint Detection and Response (EDR) y Data Loss Prevention (DLP) / User and Entity Behavior Analytics (UEBA). Fabricantes líderes del mercado, entregan estas capacidades mediante plataformas dedicadas nativas de nube, cuales operan de forma orquestada bajo una consola unificada e integración nativa.
Solicitud de aclaración o ajuste	Solicitamos a la Entidad confirmar y aclarar de manera explícita en los pliegos definitivos que se permite la presentación de soluciones compuestas por más de un licenciamiento o módulo especializado, siempre y cuando pertenezcan al mismo fabricante o ecosistema integrado, sean nativas SaaS, no generen costos adicionales para la Entidad y cumplan acumulativamente con el 100% de la ficha técnica.
Decisión	No aceptada
Respuesta UAERMV	La UAERMV se permite informar que de conformidad con la estructuración técnica contenida en los Estudios Previos y en el formato GCON-FM-022 (Descripción Técnica de la Necesidad), el proceso de contratación ya distingue claramente dos (2) ítems o soluciones especializadas independientes pero articuladas: (i) Ítem 1 - Solución de Endpoint Detection and Response (EDR) Avanzada para 450 endpoints y (ii) Ítem 2 - Solución de Data Loss Prevention (DLP) Avanzada para 450 endpoints. Respecto a la exigencia específica prevista para la solución DLP (página 12 de los Estudios Previos y página 12 del formato GCON-FM-022), según la cual "La solución debe ser una sola licencia, que incluya todo lo solicitado sin módulos adicionales de componentes de seguridad no solicitados que puedan generar administraciones o coexistencia con diferentes configuraciones que no permitan centrarse en la función de DLP. No se permiten soluciones que deban incluir infraestructura en sitio como servidores o bases de datos", se aclara que el propósito técnico de este requisito dentro del componente DLP es evitar que se oferten empaquetamientos fragmentados que incorporen herramientas ajenas al objeto de prevención de fuga de datos, requieran infraestructura local (on-premise) o trasladen a la Entidad complejidades operativas y costos ocultos de licenciamiento. Lo anterior guarda plena armonía con lo dispuesto expresamente en el numeral 6 de los Requerimientos mínimos para la entrega del bien, obra o servicio objeto del Contrato – Generales (página 27 del formato GCON-FM-022), el cual establece:

	"6. La solución deberá contar con administración centralizada desde la nube mediante una o más consolas, módulos, agentes, servicios o componentes técnicamente integrados. Se permitirá el uso de componentes complementarios cuando sean necesarios para cumplir las capacidades solicitadas, siempre que estén incluidos en el licenciamiento ofertado y no generen costos adicionales para la Entidad durante la vigencia de la suscripción. El proponente deberá identificar claramente los componentes, agentes, consolas e integraciones que conforman su solución". En consecuencia, no existe contradicción entre los apartes citados y se confirma a los interesados que es plenamente válido ofertar las soluciones especializadas requeridas (EDR y DLP) apoyadas en los componentes o suscripciones que las integren conforme a lo previsto en el numeral 6 de la página 27 del formato GCON-FM-022, siempre y cuando: Cumplan con el 100% de las especificaciones técnicas mínimas exigidas para cada solución (EDR y DLP). Sean 100% nativas en la nube (SaaS), sin requerir instalación de servidores, bases de datos ni colectores en tierra. En el caso de la solución DLP, la licencia ofertada consolide las capacidades de monitoreo, riesgo interno y bloqueo solicitadas en un agente unificado sin requerir componentes de seguridad no solicitados que desvíen su administración. Garanticen la total compatibilidad e integración nativa y automatizada con el ecosistema de ciberseguridad preexistente en la UAERMV (Next Generation Firewall, Control de Acceso a la Red, SandBox, Correlacionador de Eventos y Analizador) y con Microsoft Office 365. La totalidad de las licencias, conectores y servicios estén incluidos integralmente dentro del valor ofertado por el periodo de doce (12) meses, sin generar costos adicionales para la Entidad.

Observación N.° 2	**GRUPO LUMA — Técnico**
Observación presentada	Sección "Servicios y soporte" (Página 15): "La solución debe incluir un servicio de buenas prácticas llevado a cabo por el fabricante... Debe realizarse directamente por el fabricante de la solución, no puede ser realizado por el oferente.
Solicitud de aclaración o ajuste	Solicitamos a la Entidad modificar la exigencia de que "el servicio sea realizado directamente por el fabricante" se entiende satisfecha cuando el proponente adjunte certificación expedida por el fabricante, donde conste que el canal es partner autorizado, y se permita la prestación de servicios directamente desde el proponente que cuente con servicio de SOC Propio.
Decisión	No aceptada
Respuesta UAERMV	La Entidad informa que de acuerdo con los Estudios Previos y el formato GCON-FM-022, el modelo de operación y aseguramiento de calidad definido por la UAERMV contempla dos niveles de acompañamiento claramente diferenciados y

	complementarios: por un lado, la implementación y el soporte técnico local a cargo del Contratista (oferente) y, por otro lado, el respaldo directo de fábrica. La exigencia de contar con un servicio de buenas prácticas ejecutado directamente por el fabricante de la solución DLP (que comprende el análisis inicial, revisión de políticas a implementar, ajuste de la solución, recomendaciones, seguimiento durante el primer mes y seguimiento mensual y final) responde a la necesidad técnica de contar con el aseguramiento de calidad (Quality Assurance), validación arquitectónica y transferencia de mejores prácticas directamente del creador de la tecnología (Vendor Professional Services / Customer Success), sin intermediación. Permitir que este servicio de fábrica sea sustituido por el SOC propio del proponente o canal integrador desvirtuaría el control cruzado de calidad sobre la implementación que el propio contratista ejecuta, eliminando el acompañamiento especializado directo del fabricante sobre la afinación de políticas de prevención de fuga de datos, riesgo interno y cumplimiento normativo. Adicionalmente, dentro del estudio de mercado realizado por la Entidad se verificó que dicha condición hace parte de los esquemas de servicio ofrecidos en el mercado y está debidamente contemplada dentro del Presupuesto Oficial Estimado (POE), garantizando la pluralidad de oferentes bajo condiciones técnicas uniformes. En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 3	**GRUPO LUMA — Técnico**
Observación presentada	Componentes de la Solución EDR (Página 11 y 12) : "En cuanto al hardware, debe ser un agente muy ligero; el cual no debe requerir más de 100MB de memoria RAM, y 20MB de espacio en disco."
Solicitud de aclaración o ajuste	En momentos de inspección forense en memoria o almacenamiento temporal de eventos sin conexión (offline buffering), los consumos pueden presentar picos dinámicos ajustados al uso del sistema operativo para evitar la pérdida de telemetría, Solicitamos a la Entidad aclarar que la métrica de consumo de hardware (<=100MB RAM y <=20MB disco) corresponde al consumo promedio nominal de operación en reposo/ejecución del agente, y no a un límite rígido en picos de análisis forense o buffer de contingencia offline
Decisión	No aceptada
Respuesta UAERMV	La Entidad informa que en los Estudios Previos y el formato GCON-FM-022 se establece como especificación técnica objetiva del componente EDR: "En cuanto al

	hardware, debe ser un agente muy ligero; el cual no debe requerir más de 100MB de memoria RAM, y 20MB de espacio en disco". Como se indicó en los documentos técnicos del proceso, la UAERMV requiere proteger 450 endpoints que soportan la operación diaria y los aplicativos misionales de la Entidad, razón por la cual es imperativo garantizar una huella de recursos mínima sobre las estaciones de trabajo y servidores, evitando degradaciones en el rendimiento de los equipos. Se aclara a los interesados que la verificación de este requisito técnico se realiza de manera objetiva sobre las especificaciones técnicas oficiales del fabricante (fichas de producto, datasheets, manuales u hojas de datos oficiales), en las cuales debe constar que el requerimiento o consumo nominal de recursos del agente en operación estándar cumple con los topes máximos exigidos (<=100MB de RAM y <=20MB disco de espacio en disco para la instalación/operación del agente). La Entidad no desconoce que existen acciones puntuales y transitorias ordenadas bajo demanda, como la captura de instantáneas de memoria (memory snapshots) para investigación forense o el almacenamiento temporal de eventos cuando un equipo se encuentra desconectado de la red, hacen uso dinámico de recursos del sistema operativo mientras se ejecuta la tarea o se sincroniza la telemetría con la nube; sin embargo, ello no exime al proponente de acreditar documentalmente que la arquitectura base del agente EDR ofertado cumple de fábrica con la especificación de agente (<=100MB de RAM y <=20MB disco de espacio en disco) exigida en el Anexo Técnico. En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 4	**SOLUCIONES DE SOFTWARE INDTECH S.A.S. — Técnico**
Observación presentada	NIVEL DE MEMBRESÍA "El proponente debe adjuntar junto con su propuesta carta emitida por el fabricante (…) donde certifique que el proponente es Partner, canal o socio con el nivel más alto de membresía en la marca ofrecida en Colombia".
Solicitud de aclaración o ajuste	Exigir el nivel más alto del programa de canales no guarda proporción con el objeto, ni con el valor del contrato: 450 EndPoints, un presupuesto de $523.652.448 y un plazo de dos meses. Los programas de canales de los fabricantes asignan los niveles superiores según el volumen de ventas anual y el número de certificaciones del canal. Esas condiciones miden el tamaño comercial del proveedor, no su capacidad para implementar y soportar 450 EndPoints. En la práctica, el requisito reduce los oferentes posibles a muy pocos integradores por marca y deja por fuera a canales autorizados que sí cuentan con personal certificado.

	Solicitud: Modificar el requisito para que se acepte la carta del fabricante que certifique que el proponente es canal, Partner o distribuidor autorizado para comercializar, implementar y soportar en Colombia la solución ofertada, sin exigir un nivel específico de membresía.
Decisión	No aceptada
Respuesta UAERMV	La UAERMV se permite informar que no acepta la observación, toda vez que, el objeto del proceso es la suscripción, implementación y soporte de una plataforma de ciberseguridad que protege los activos críticos de la Entidad: endpoints y datos. Por tratarse de seguridad de la información, la UAERMV requiere el mayor nivel de respaldo del fabricante en Colombia. Esa condición no mide el tamaño comercial del proponente, sino la garantía de que el fabricante responde por él en estos puntos: 1. **Soporte y escalamiento.** La Entidad exige soporte 7x24 con el fabricante y soporte local del contratista. Un canal en el nivel más alto de membresía cuenta, de manera general, con acceso prioritario al soporte técnico, a ingeniería del fabricante y a recursos de escalamiento. Eso reduce el tiempo de respuesta ante un incidente. 2. **Plazo de implementación.** La instalación, configuración y puesta en marcha debe cumplirse en dos (2) meses, y el desempeño de la solución depende de una correcta implementación. El respaldo del fabricante mitiga el riesgo de errores de configuración y de retrasos. 3. **Capacidad operativa de la Entidad.** La Entidad cuenta con recurso humano limitado en seguridad, como lo establecen los estudios previos. Por eso depende del proveedor para la operación, el acompañamiento y la transferencia de conocimiento. 4. **Continuidad del servicio.** El nivel más alto de membresía respalda que el proveedor mantiene una relación vigente y directa con el fabricante. Así se reduce el riesgo de que el proveedor deje de ser canal autorizado durante la ejecución del contrato. El requisito no restringe la pluralidad de oferentes.

Observación N.° 5	**SOLUCIONES DE SOFTWARE INDTECH S.A.S. — Financiero**
Observación presentada	INDICADORES FINANCIEROS Nivel de endeudamiento (pasivo total / activo total) menor o igual a 0,72. Ver Tabla Nivel de Endeudamiento.
Solicitud de aclaración o ajuste	Con ese corte, uno de cada cinco proveedores del sector queda excluido solo por este indicador. Tres razones justifican flexibilizarlo: 1. Modelo de negocio del sector. Los integradores de licenciamiento y suscripciones SaaS registran como pasivo corriente las cuentas por pagar a mayoristas y fabricantes, que se

<table>
<tr><td></td><td>cancelan con el pago del cliente final. Ese pasivo es de corto plazo, está respaldado por cuentas por cobrar y no refleja un riesgo de insolvencia.

2. El riesgo financiero ya está cubierto. El pliego exige liquidez, razón de cobertura de intereses, ROE y ROA. Un proponente con endeudamiento algo mayor a 0,72 pero con cobertura de intereses y rentabilidad holgadas no representa mayor riesgo para la Entidad. Además, el contrato se paga en un único desembolso posterior a la puesta en marcha y está amparado con garantía de cumplimiento del 20%.

Solicitud: Ajustar el nivel de endeudamiento para MiPymes a menor o igual a 0,80, valor que coincide con el percentil 80 de la misma muestra para no MiPymes. Esto mantiene un criterio estadístico del propio estudio del sector y amplía la pluralidad de oferentes.</td></tr>
<tr><td>Decisión</td><td>Aceptada</td></tr>
<tr><td>Respuesta UAERMV</td><td>La UAERMV se permite informar que la entidad acepta la observación para permitir una mayor pluralidad de oferentes, ya que su modificación no altera significativamente la exposición de riesgos del proceso que adelanta la entidad. Por tanto, la entidad modificará el Estudio del Sector, el Estudio Previo y el Pliego de Condiciones. Al respecto de este último documento, los indicadores financieros para MIPYMES quedarán así:

<table>
<tr><th colspan="4">INDICADORES DE CAPACIDAD FINANCIERA MÍNIMOS REQUERIDOS</th></tr>
<tr><th>INDICADOR</th><th>FORMULA</th><th>MARGEN SOLICITADO</th><th>CONSORCIO O UNIONES TEMPORALES</th></tr>
<tr><td>LIQUIDEZ</td><td>Activo Corriente/ Pasivo Corriente</td><td>Mayor o igual 1,12</td><td rowspan="3">El proponente que presente propuesta debe cumplir por igual, con los indicadores mínimos. Los indicadores se calculan de acuerdo con la participación porcentual de cada uno de los integrantes de consorcio o unión temporal.</td></tr>
<tr><td>NIVEL DE ENDEUDAMIENTO</td><td>Pasivo Total/ Activo Total</td><td>Menor o igual a 0,80</td></tr>
<tr><td>RAZON COBERTURA DE INTERES</td><td>Utilidad Operacional/ Gastos de intereses</td><td>Mayor o igual 1</td></tr>
</table></td></tr>
<tr><td>Numeral donde se afecta el documento</td><td>Pliego de condiciones. Numeral 4.3 REQUISITOS HABILITANTES DE CAPACIDAD FINANCIERA Y CAPACIDAD ORGANIZACIONAL, 4.3.1.VERIFICACIÓN DE LA CAPACIDAD FINANCIERA.

[...] La UAERMV verificará el cumplimiento de los siguientes indicadores financieros para medir la fortaleza financiera del proponente, según la información indicada en el RUP o en el ANEXO DE INFORMACIÓN FINANCIERA EXTRANJEROS para los proponentes extranjeros sin domicilio en el país.</td></tr>
</table>

	INDICADORES PARA MIPYMES [..]

Observación N.° 6	**SOLUCIONES DE SOFTWARE INDTECH S.A.S. — Técnico**
Observación presentada	POSIBILIDAD DE OFERTAR EDR Y DLP DE FABRICANTES DISTINTOS Observación: El proceso se adelanta por subasta inversa, modalidad reservada a bienes y servicios de características técnicas uniformes. El Decreto 1082 de 2015 los define como bienes de común utilización con especificaciones y patrones de desempeño iguales o similares, que pueden agruparse como homogéneos. Esa homogeneidad supone que varios fabricantes pueden cumplir la ficha técnica. Sin embargo, el FM-022 justifica la adquisición en la integración con "un ecosistema de fabricante único" y exige que una misma marca resuelva EDR y DLP. El propio estudio del sector reconoce como líderes del mercado de EDR a CrowdStrike, Microsoft, SentinelOne y Sophos, entre otros. Pero al exigir que EDR y DLP sean de la misma marca y se integren de forma nativa con la plataforma perimetral existente, en la práctica solo puede cumplir el fabricante de esa plataforma. Exigir ambas soluciones de un mismo fabricante reduce la competencia a una sola marca, lo que es incompatible con la subasta inversa y con la pluralidad que la Entidad declaró haber verificado. Las soluciones EDR y DLP son funcionalmente independientes: cada una tiene su agente, su consola y su modelo de licenciamiento. La interoperabilidad con el SIEM y el analizador de la Entidad se logra mediante estándares abiertos (syslog, CEF, API REST, webhooks), que el mismo FM-022 exige a la DLP.
Solicitud de aclaración o ajuste	Permitir expresamente que el proponente oferte la solución EDR y la solución DLP de fabricantes distintos, acreditando una certificación de canal autorizado por cada fabricante. En su defecto, estructurar el proceso en dos lotes independientes (Lote 1: EDR; Lote 2: DLP), cada uno con su presupuesto, sus requisitos técnicos y su subasta.
Decisión	No aceptada
Respuesta UAERMV	La UAERMV se permite informar que no acepta la observación, toda vez que, cuenta con una plataforma de seguridad integral sobre ecosistema de un solo fabricante (firewalls de nueva generación, control de acceso a la red, sandbox y correlacionador de eventos). Mantener el EDR y el DLP en el mismo ecosistema de un solo fabricante favorece a la UAERMV con la gestión de todas sus herramientas desde una sola plataforma de administración, lo que mejora tiempos de gestión y mayor observabilidad de las herramientas de seguridad perimetral. Solicitar un solo fabricante no limita la pluralidad. de oferentes. Ya que los productos se pueden comercializar a través de numerosos canales y distribuidores autorizados en

	Colombia, que compiten entre sí en precio y servicio en la subasta inversa. La Entidad estandariza su plataforma por razones técnicas y operativas.

Observación N.° 7	**SOLUCIONES DE SOFTWARE INDTECH S.A.S. — Financiero**
Observación presentada	REGLAS PARA ACREDITAR LA EXPERIENCIA Documento y numeral: Proyecto de pliego, "Verificación experiencia proponente obligado a estar inscrito en el RUP", "Notas comunes aplicables a la verificación de experiencia" y apartado de criterios diferenciales (Decreto 1860 de 2021). a) Nivel de clasificación UNSPSC. El pliego exige acreditar la experiencia "en tercer nivel" (clase), pero la tabla relaciona códigos de quinto nivel o producto (43222501, 43222502 y 43233205). El RUP certifica la experiencia hasta el nivel de clase.
Solicitud de aclaración o ajuste	Confirmar que basta con que el contrato esté clasificado en el RUP en alguna de las clases 43222500 (Equipo de seguridad de red) o 43233200 (Software de seguridad y protección).
Decisión	Aceptada
Respuesta UAERMV	La UAERMV se permite informar que la entidad acepta la observación, ya que en virtud del Decreto 1082 de 2015 y lo dispuesto en los artículos 2.2.1.1.1.5.2 y 2.2.1.1.1.5.3, los cuales exigen que los proponentes y Cámaras de Comercio identifiquen los bienes, obras, servicios y los contratos para acreditar experiencia utilizando el Clasificador de Bienes y Servicios en su tercer nivel (clase). Por tanto, la entidad modificará el Estudio Previo y el Pliego de Condiciones en consonancia con la observación. En el pliego de condiciones, numeral 4.2 REQUISITOS HABILITANTES TÉCNICOS, 4.2.1 VERIFICACIÓN EXPERIENCIA PROPONENTE OBLIGADO A ESTAR INSCRITO EN EL REGISTRO ÚNICO DE PROPONENTES, quedará expreso que: [...] El proponente persona natural o jurídica o plural deberá acreditar la experiencia con el certificado de inscripción, calificación y clasificación RUP de acuerdo con el clasificador de bienes y servicios en tercer nivel expresado en SMMLV en alguno de los códigos indicados en la siguiente tabla:

Clasificación UNSPSC	**Segmento**	**Familia**	**Clase**
43222500	(43000000) Difusión de tecnologías de información y telecomunicaciones.	(43220000) Equipos o plataformas y accesorios de redes multimedia o de voz y datos.	[43222500] Equipo de seguridad de red

	<table><tr><td>43233200</td><td>(43000000) Difusión de tecnologías de información y telecomunicaciones</td><td>[43230000] Software</td><td>[43233200] Software de seguridad y protección</td></tr></table> NOTA 1: Se podrá acreditar experiencia con contratos ejecutados en su totalidad. NOTA 2: Los oferentes no podrán acreditar experiencia con contratos en ejecución NOTA 3: De acuerdo con lo indicado en el Parágrafo 5° del Artículo 5º de la Ley 1150 de 2007 adicionado por el Artículo 5º de la Ley 1882 de 2015 “(…) En los procesos de contratación, las entidades estatales deberán aceptar la experiencia adquirida por los proponentes a través de la ejecución de contratos con particulares. (…)”. "
Numeral donde se afecta el documento	4.2 REQUISITOS HABILITANTES TÉCNICOS, 4.2.1 VERIFICACIÓN EXPERIENCIA PROPONENTE OBLIGADO A ESTAR INSCRITO EN EL REGISTRO ÚNICO DE PROPONENTES.

Observación N.° 8	**SOLUCIONES DE SOFTWARE INDTECH S.A.S. — Contractual**
Observación presentada	b) Objeto o alcance del contrato. El pliego exige que el objeto o alcance "se encuentre relacionado con la suscripción, implementación y soporte de soluciones o plataformas de ciberseguridad".
Solicitud de aclaración o ajuste	Aclarar que se acepta un contrato cuyo objeto o alcance incluya cualquiera de esas actividades (suscripción, licenciamiento, implementación o soporte) sobre soluciones de ciberseguridad, sin exigir que las tres concurran en un mismo contrato. Aclarar también que se acepta un contrato de objeto más amplio cuando la ciberseguridad hace parte de su alcance y así consta en la certificación o en el RUP.
Decisión	Aceptada
Respuesta UAERMV	La UAERMV se permite informar que se harán las aclaraciones pertinentes a este tema en los documentos oficiales del proceso

Observación N.° 9	**SOLUCIONES DE SOFTWARE INDTECH S.A.S. — Financiero**
Observación presentada	c) Número máximo de contratos para MiPymes. El pliego es contradictorio. En el apartado de criterios diferenciales permite hasta cinco (5) contratos solo a emprendimientos y empresas de personas con discapacidad, y hasta tres (3) a los "demás tipos de empresas". En las notas comunes permite hasta cinco (5) a "MiPymes, emprendimiento de mujeres y emprendimiento de empresas de personas con discapacidad".
Solicitud de aclaración o ajuste	Unificar la regla en el pliego definitivo y confirmar que las MiPymes podrán acreditar la experiencia con hasta cinco (5) contratos, en desarrollo de los criterios diferenciales de la Ley 2069 de 2020 y del Decreto 1860 de 2021.
Decisión	Aceptada
Respuesta UAERMV	La entidad acepta la observación y el ajuste se hará en Estudio del Sector, Estudio Previo y Pliego de Condiciones. Respecto al Pliego de Condiciones, se modificará el numeral 1.9 RÉGIMEN JURÍDICO APLICABLE, así: [...] Adicional, para las empresas catalogadas como Mipymes, emprendimientos de mujeres y emprendimientos y empresas de personas con discapacidad, podrán acreditar experiencia con máximo cinco (5) contratos ejecutados y registrados en el RUP, mientras que los demás tipos de empresas, se deberá acreditar experiencia con máximo tres (3) contratos ejecutados y registrados en el RUP, cuyo objeto o alcance se encuentre relacionado con la suscripción, implementación y soporte de soluciones o plataformas de ciberseguridad, así: [..]
Numeral donde se afecta el documento	4.2 REQUISITOS HABILITANTES TÉCNICOS, 4.2.1 VERIFICACIÓN EXPERIENCIA PROPONENTE OBLIGADO A ESTAR INSCRITO EN EL REGISTRO ÚNICO DE PROPONENTES.

Observación N.° 10	**SOLUCIONES DE SOFTWARE INDTECH S.A.S. — Técnico**
Observación presentada	Las cantidades de 450 EndPoints se aplica[n] para computadores de usuarios finales". Al mismo tiempo exige que los agentes EDR y DLP sean compatibles con Windows Server 2019 y 2022, Oracle Linux, Ubuntu Server y CentOS. Las licencias para servidores tienen un costo diferente al de las estaciones de trabajo, de modo que la composición incide directamente en el precio.
Solicitud de aclaración o ajuste	Aclarar si los 450 EndPoints incluyen servidores. En caso afirmativo, indicar cuántos son servidores y con qué sistema operativo, para cada una de las soluciones (EDR y DLP).
Decisión	Aceptada

Respuesta UAERMV	La entidad acepta la observación y el ajuste se verá reflejado en los documentos precontractuales del proceso.

Observación N.° 11	**GLOBAL SEIS SAS — Técnico**
Observación presentada	La solución de EDR deberá integrarse al menos con las siguientes plataformas con las que cuenta la Entidad: 1. Next Generation Firewall (FortiGate). 2. Control de Acceso a la Red (FortiNAC). 3. SandBox (FortiSandbox). 4. Correlacionador de Eventos (FortiSIEM).
Solicitud de aclaración o ajuste	Solicitamos a la Entidad modificar el texto actual del requisito por el siguiente: La solución deberá integrarse con FortiGate, FortiNAC, FortiSandbox, FortiSIEM y FortiAnalyzer, según corresponda al servicio. La Entidad identificará versiones, flujos, campos, acciones y permisos. Se aceptarán conectores soportados, API y protocolos estándar incluidos en la oferta. Las pruebas comprobarán entrega de eventos, ejecución de acciones autorizadas y manejo de fallos. El contratista configurará la exportación y el envío desde sus productos; el responsable de la plataforma SIEM realizará su ingesta, normalización y administración.
Decisión	No aceptada
Respuesta UAERMV	La UAERMV se permite informar que de conformidad con el numeral 3 de los Estudios Previos y el formato GCON-FM-022, la integración requerida con la infraestructura de seguridad preexistente de la UAERMV (Next Generation Firewall FortiGate, Control de Acceso a la Red FortiNAC, SandBox FortiSandbox, Correlacionador de Eventos FortiSIEM y Analizador FortiAnalyzer) no consiste en una simple exportación unidireccional de logs planos, sino en una articulación nativa y bidireccional que permita ejecutar flujos de respuesta automatizada y coordinada en tiempo real (cuarentena de red en el NAC, bloqueo de tráfico en el firewall, detonación dinámica en el Sandbox y correlación de incidentes entre productos en el SIEM) sin introducir latencias ni brechas de visibilidad. Asimismo, resulta improcedente trasladar a la Entidad la obligación técnica de desarrollar o configurar la ingesta, normalización y correlación de los eventos en el SIEM. De acuerdo con el numeral 3.4 del Proyecto de Pliego de Condiciones, las ofertas no pueden presentar condicionamientos que trasladen cargas operativas a la Entidad, y según los requisitos de ejecución del formato GCON-FM-022 (páginas 27 y 30), es obligación directa del contratista garantizar la "integración con plataformas institucionales" y entregar las "evidencias de integración" funcionando a entera satisfacción como condición para el recibo final. En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 12	**GLOBAL SEIS SAS — Técnico**
Observación presentada	La solución de EDR debe contar con políticas predefinidas y exclusivas para la prevención de secuestro de información por ataques de ransomware, por lo cual debe incluir más de 30 estrategias de protección diferentes. Dichas estrategias deben incluir como mínimo: 1. Debug de Procesos. 2. Código dinámico. 3. Formato de archivo ejecutable incorrecto. 4. Una pila con código ejecutable. 5. El programa ejecutado no tiene instalador. 6. Programa crítico falso. 7. Empaquetador falso. 8. File Encryptor. 9. Proceso oculto. 10. Ejecutable inyectado. 11. Proceso inyectado. 12. Hilo inyectado. 13. Suma de comprobación no válida. 14. Ejecución no válida. 15. Puntero no válido. 16. Inyección de kernel. 17. Empaquetador conocido. 18. Archivo malicioso detectado. 19. Proceso malicioso. 20. Ejecutable modificado. 21. Stack Parcialmente asignado. 22. Exploit de escalamiento de privilegios. 23. Proceso vacío. 24. Manipulación de pilas. 25. Aplicación sospechosa. 26. Empaquetador sospechoso. 27. Ejecutable manipulado. 28. Ejecutable no confirmado. 29. Ejecutable sin asignar. 30. Código grabable.31. Prevención automatizada en tiempo real encriptación de Ransomware.
Solicitud de aclaración o ajuste	Solicitamos a la Entidad modificar el texto actual del requisito por el siguiente: La solución deberá prevenir o contener cifrado no autorizado, alteración maliciosa de archivos, inyección de procesos, abuso de memoria y persistencia asociada a ransomware. Se admitirán mecanismos de protección equivalentes documentados por el fabricante. La Entidad definirá escenarios seguros de prueba, evidencia de detección y bloqueo, recursos afectados y criterios de recuperación. La conformidad se verificará por los resultados, sin exigir una cantidad ni nomenclatura interna de reglas.
Decisión	No aceptada
Respuesta UAERMV	La UAERMV se permite informar que los mecanismos listados en el formato GCON-FM-022 (Debug de procesos, Código dinámico, Pila con código ejecutable, Proceso oculto, Ejecutable/Proceso/Hilo inyectado, Inyección de kernel, Exploit de escalamiento de privilegios, Proceso vacío, Manipulación de pilas, File Encryptor y Prevención automatizada en tiempo real de encriptación, entre otros) describen vectores técnicos específicos de explotación de memoria, inyección de procesos y evasión de controles utilizados por el ransomware moderno. En los procesos de Selección Abreviada por Subasta Inversa (artículo 2.2.1.2.1.2.2 del Decreto 1082 de 2015), la ficha técnica debe contener especificaciones objetivas y verificables que garanticen un estándar uniforme de protección. Eliminar el desglose técnico para reemplazarlo por una declaración genérica impediría verificar de manera rigurosa la cobertura predefinida del motor anti-ransomware. Se reitera que la Entidad evalúa el cumplimiento técnico y funcional de dichos controles a través de la documentación oficial del fabricante, sin exigir que la interfaz

	gráfica utilice literalmente una traducción o etiqueta comercial idéntica. En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 13	**GLOBAL SEIS SAS — Técnico**
Observación presentada	Debe contar con una tecnología propietaria de rastreo de código, permitiendo así visualizar la cadena de ataque completa y el “paciente cero”, incluso si el dispositivo está fuera de línea.
Solicitud de aclaración o ajuste	Solicitamos a la Entidad modificar el texto actual del requisito por el siguiente: La solución deberá reconstruir la secuencia del incidente y relacionar procesos, archivos, conexiones y cambios relevantes, identificando el origen disponible y conservando evidencia para investigación. Se aceptarán mecanismos documentados de telemetría, análisis de memoria y reconstrucción de eventos equivalentes. El oferente identificará capacidades por sistema operativo y condiciones de conectividad. Las pruebas comprobarán la investigación y la disponibilidad de evidencia tras la reconexión, sin imponer tecnología propietaria ni una denominación particular.
Decisión	No aceptada
Respuesta UAERMV	La UAERMV se permite informar que de acuerdo con los Estudios Previos y el formato GCON-FM-022, la plataforma EDR debe proteger y registrar la trazabilidad de las amenazas incluso en endpoints desconectados de la red corporativa (modo autónomo) y proporcionar visibilidad completa de la cadena de ataque mediante el seguimiento de código. La expresión "tecnología propietaria de rastreo de código" significa que el motor de seguimiento a nivel de código e instrucciones debe ser nativo del fabricante de la solución ofertada (sin depender de software forense de terceros ajeno al agente), garantizando la reconstrucción íntegra de la cadena de ataque y la identificación del "paciente cero" aunque el evento ocurra mientras el dispositivo se encuentra fuera de línea o aislado de la red. En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 14	**GLOBAL SEIS SAS — Técnico**
Observación presentada	Debe conservar instantáneas de memoria, de los ataques sin archivo o file-less para la búsqueda de amenazas basada en memoria.

Solicitud de aclaración o ajuste	Solicitamos a la Entidad modificar el texto actual del requisito por el siguiente: La solución deberá aportar evidencia para investigar amenazas en memoria mediante captura de memoria, telemetría de procesos u otros mecanismos forenses documentados. El oferente identificará su cobertura por sistema operativo, la evidencia retenida y sus condiciones de consulta. La aceptación comprobará la reconstrucción del escenario de ataque sin imponer un único tipo de artefacto.
Decisión	No aceptada
Respuesta UAERMV	La UAERMV se permite informar que como se expone en el análisis de riesgos de los Estudios Previos, los ataques sin archivos (fileless), living off the land y las inyecciones en memoria se ejecutan directamente sobre la memoria RAM sin escribir ficheros en el disco duro. La simple telemetría de inicio o parada de procesos no reemplaza la captura y conservación de la instantánea de memoria (memory snapshot) del fragmento comprometido, la cual constituye el artefacto forense indispensable para que los analistas de seguridad puedan inspeccionar el código malicioso inyectado y realizar cacería de amenazas basada en memoria. En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 15	**GLOBAL SEIS SAS — Técnico**
Observación presentada	En cuanto al hardware, debe ser un agente muy ligero; el cual no debe requerir más de 100MB de memoria RAM, y 20MB de espacio en disco.
Solicitud de aclaración o ajuste	Solicitamos a la Entidad modificar el texto actual del requisito por el siguiente: El oferente declarará los requisitos de instalación y el consumo de CPU, RAM, disco y red del conjunto de componentes ofertados, incluyendo telemetría, registros, contenidos y actualizaciones. La Entidad publicará una carga representativa y los umbrales de aceptación para operación normal, análisis y actualización. Las mediciones registrarán valores medios y máximos, duración y configuración, verificando continuidad y desempeño de las aplicaciones institucionales.
Decisión	No aceptada
Respuesta UAERMV	La UAERMV se permite informar que el parque computacional de la UAERMV (450 endpoints) soporta la operación de aplicativos misionales críticos, razón por la cual la Entidad definió un límite técnico objetivo y verificable (<= 100 MB de memoria RAM y <=20 MB de espacio en disco que asegura una mínima afectación al rendimiento de los equipos. Por lo tanto, eliminar el umbral máximo de consumo (100 MB de memoria RAM y 20 MB en disco) para dejarlo a declaración abierta de cada proponente impediría realizar una verificación técnica objetiva en igualdad de condiciones y trasladaría a la Entidad

	el riesgo operativo de ralentización o saturación de memoria de los equipos que hacen parte del parque computacional. En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 16	**GLOBAL SEIS SAS — Técnico**
Observación presentada	La solución de EDR debe proporcionar a la Entidad un conjunto de protecciones, tanto en pre-ejecución (esto es, antes de que la amenaza tenga capacidad para comprometer sus sistemas) como post-ejecución (cuando la amenaza interactúa con el servidor o equipo de trabajo), 100% basado en comportamiento (sin firmas estáticas) y cuya velocidad de respuesta proporciona una protección en tiempo real a los sistemas.
Solicitud de aclaración o ajuste	Solicitamos a la Entidad modificar el texto actual del requisito por el siguiente: La solución deberá detectar y prevenir amenazas por comportamiento y técnicas de aprendizaje automático, incluyendo amenazas sin archivo y abuso de herramientas legítimas, sin depender exclusivamente de firmas estáticas conocidas. Se permitirá combinar mecanismos conductuales, reputación, inteligencia y otras defensas complementarias. Las pruebas incluirán escenarios no identificados únicamente por una firma conocida.
Decisión	No aceptada
Respuesta UAERMV	La UAERMV se permite informar que como se ha aclarado de manera transversal en el presente proceso, la exigencia "100% basado en comportamiento (sin firmas estáticas)" significa que los motores de prevención pre-ejecución (NGAV basado en kernel y Machine Learning) y de detección/respuesta post-ejecución deben ser capaces de identificar, bloquear y contener amenazas avanzadas o de día cero de forma completamente autónoma, sin depender de la existencia previa de una firma estática. El formato GCON-FM-022 ya contempla y exige capacidades complementarias de enriquecimiento en tiempo real con bases de datos de inteligencia de amenazas en la nube, clasificación de reputación, listas blancas/negras por hash e ingesta/búsqueda de indicadores de compromiso (IoC), por lo que el uso de dichas fuentes auxiliares de inteligencia es plenamente compatible con el pliego sin que se requiera modificar el Anexo Técnico. En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 17	**GLOBAL SEIS SAS — Técnico**
Observación presentada	Gestión de parches para sistemas operativos Windows, OS, Linux.
Solicitud de aclaración o ajuste	Solicitamos a la Entidad modificar el texto actual del requisito por el siguiente: La solución deberá identificar vulnerabilidades y proporcionar o integrar mecanismos de mitigación mientras se aplica la corrección. La mitigación virtual deberá documentar el control y la vulnerabilidad cubierta. Si se requiere distribución e instalación de parches, la Entidad especificará sistemas operativos, aplicaciones, reinicios, aprobaciones, rollback y pruebas de instalación. Se aceptarán componentes integrados incluidos en la oferta y se verificará por separado el parche instalado y la mitigación temporal.
Decisión	No aceptada
Respuesta UAERMV	La UAERMV se permite informar que dentro del formato GCON-FM-022, tanto la gestión de parches para sistemas operativos Windows, macOS y Linux (en Funcionalidades de Prevención) como la mitigación proactiva de vulnerabilidades mediante parches virtuales (en Funcionalidades de Descubrimiento) son requerimientos obligatorios y complementarios que deben estar incluidos dentro de la solución ofertada. De conformidad con los Requisitos Técnicos Generales por Etapa del formato GCON-FM-022 (páginas 29 y 30), corresponde al contratista presentar antes de la puesta en operación el plan de implementación, el cronograma detallado, el plan de despliegue definido conjuntamente con la supervisión y el procedimiento de reversa (rollback). En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 18	**GLOBAL SEIS SAS — Técnico**
Observación presentada	La solución de EDR Se debe contar un servicio de respuesta y detección gestionada (MDR) ante incidentes, proporcionado por técnicos del propio fabricante.
Solicitud de aclaración o ajuste	Solicitamos a la Entidad modificar el texto actual del requisito por el siguiente: La oferta incluirá soporte del fabricante y los servicios especializados de detección, respuesta y buenas prácticas requeridos, con responsabilidades, horarios, tiempos de atención, actividades, informes y escalamiento definidos. Podrán ejecutarse directamente por el fabricante o por especialistas certificados y autorizados, conservando el respaldo de producto y los niveles de servicio exigidos. Se verificarán el análisis inicial, revisión y ajuste de políticas, seguimiento y evidencia de las acciones durante la vigencia solicitada.

Decisión	No aceptada
Respuesta UAERMV	La UAERMV se permite informar que la exigencia de que tanto el servicio de Detección y Respuesta Gestionada (MDR) en la solución EDR como el Servicio de Buenas Prácticas en la solución DLP sean prestados directamente por el fabricante obedece a una decisión técnica y operativa debidamente estructurada en el Estudio del Sector y los Estudios Previos. Respecto al servicio MDR: Garantiza a la UAERMV acceso directo y sin intermediación a los equipos de ingeniería, inteligencia global de amenazas e investigación forense del fabricante, evitando capas adicionales de escalamiento o tercerización que incrementen los tiempos de respuesta frente a incidentes críticos y asegurando una interacción transparente con el ecosistema de ciberseguridad preexistente de la Entidad. Respecto al servicio de buenas prácticas de DLP: Mientras el contratista (oferente) ejecuta la implementación y presta el soporte local, el fabricante realiza directamente el análisis inicial, la revisión y ajuste de políticas y el seguimiento mensual y final. Ello constituye un mecanismo de aseguramiento de calidad (Quality Assurance directo de fábrica) que perdería su propósito de control independiente si fuera ejecutado por el mismo oferente o por terceros subcontratados. El Estudio del Sector corroboró que ambos servicios directos de fábrica se encuentran disponibles en el mercado y están contemplados dentro del Presupuesto Oficial Estimado. En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 19	**GLOBAL SEIS SAS — Técnico**
Observación presentada	La solución debe ser una sola licencia, que incluya todo lo solicitado sin módulos adicionales de componentes de seguridad no solicitados que puedan generar administraciones o coexistencia con diferentes configuraciones que no permitan centrarse en la función de DLP. No se permiten soluciones que deban incluir infraestructura en sitio como servidores o bases de datos.
Solicitud de aclaración o ajuste	Solicitamos a la Entidad modificar el texto actual del requisito por el siguiente: Se permitirán una o más consolas, agentes, módulos y servicios técnicamente integrados para cumplir las funciones de EDR y DLP. Todos los derechos de uso, componentes e integraciones requeridos estarán incluidos durante la suscripción y se identificarán por función. La coexistencia, administración y consumo total se demostrarán en las pruebas. La cantidad de componentes o denominaciones comerciales de licencia no será por sí sola un criterio de incumplimiento, conservando las capacidades, la gestión segura y la modalidad cloud exigidas.

Decisión	No aceptada
Respuesta UAERMV	La UAERMV se permite informar que los requerimientos pertenecen específicamente al capítulo técnico de la Solución de Data Loss Prevention (DLP). Su objetivo es asegurar que la plataforma DLP ofertada consolide en un único agente ligero de DLP todas las funciones de monitoreo y bloqueo de fuga de información (web, correo, nube, USB, impresoras, portapapeles, aplicaciones y riesgo interno), bajo un esquema 100% SaaS sin servidores ni bases de datos en tierra y sin obligar a la Entidad a administrar suites fragmentadas con componentes ajenos a la función de DLP. Lo anterior guarda total coherencia con el numeral 6 de los Requerimientos Mínimos para la Entrega del Bien, Obra o Servicio Objeto del Contrato – Generales (página 27 del formato GCON-FM-022), el cual ya establece de forma expresa para el alcance integral del proceso (EDR y DLP): "6. La solución deberá contar con administración centralizada desde la nube mediante una o más consolas, módulos, agentes, servicios o componentes técnicamente integrados. Se permitirá el uso de componentes complementarios cuando sean necesarios para cumplir las capacidades solicitadas, siempre que estén incluidos en el licenciamiento ofertado y no generen costos adicionales para la Entidad durante la vigencia de la suscripción. El proponente deberá identificar claramente los componentes, agentes, consolas e integraciones que conforman su solución". Por consiguiente, dado que el numeral 6 general ya regula la integración de componentes de la propuesta garantizando que no existan costos adicionales ni infraestructura local, no se requiere modificar ni suprimir los requerimientos específicos de la solución DLP. En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 20	**GLOBAL SEIS SAS — Técnico**
Observación presentada	La solución debe proporcionar un agente unificado que consolide todas las funcionalidades de monitoreo y bloqueo.
Solicitud de aclaración o ajuste	Solicitamos a la Entidad modificar el texto actual del requisito por el siguiente: Se permitirán una o más consolas, agentes, módulos y servicios técnicamente integrados para cumplir las funciones de EDR y DLP. Todos los derechos de uso, componentes e integraciones requeridos estarán incluidos durante la suscripción y se identificarán por función. La coexistencia, administración y consumo total se demostrarán en las pruebas. La cantidad de componentes o denominaciones comerciales de licencia no será por sí sola un criterio de incumplimiento, conservando las capacidades, la gestión segura y la modalidad cloud exigidas.

Decisión	No aceptada
Respuesta UAERMV	La UAERMV se permite informar que los requerimientos pertenecen específicamente al capítulo técnico de la Solución de Data Loss Prevention (DLP). Su objetivo es asegurar que la plataforma DLP ofertada consolide en un único agente ligero de DLP todas las funciones de monitoreo y bloqueo de fuga de información (web, correo, nube, USB, impresoras, portapapeles, aplicaciones y riesgo interno), bajo un esquema 100% SaaS sin servidores ni bases de datos en tierra y sin obligar a la Entidad a administrar suites fragmentadas con componentes ajenos a la función de DLP. Lo anterior guarda total coherencia con el numeral 6 de los Requerimientos Mínimos para la Entrega del Bien, Obra o Servicio Objeto del Contrato – Generales (página 27 del formato GCON-FM-022), el cual ya establece de forma expresa para el alcance integral del proceso (EDR y DLP): "6. La solución deberá contar con administración centralizada desde la nube mediante una o más consolas, módulos, agentes, servicios o componentes técnicamente integrados. Se permitirá el uso de componentes complementarios cuando sean necesarios para cumplir las capacidades solicitadas, siempre que estén incluidos en el licenciamiento ofertado y no generen costos adicionales para la Entidad durante la vigencia de la suscripción. El proponente deberá identificar claramente los componentes, agentes, consolas e integraciones que conforman su solución". Por consiguiente, dado que el numeral 6 general ya regula la integración de componentes de la propuesta garantizando que no existan costos adicionales ni infraestructura local, no se requiere modificar ni suprimir los requerimientos específicos de la solución DLP. En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 21	**GLOBAL SEIS SAS — Técnico**
Observación presentada	La solución debe proporcionar visibilidad inmediata sin políticas sobre el movimiento de datos y los procesos empresariales.
Solicitud de aclaración o ajuste	Solicitamos a la Entidad modificar el texto actual del requisito por el siguiente: La solución deberá proporcionar visibilidad inicial de actividad y movimiento de datos después de activar los sensores y conectores, y aplicar controles de prevención con políticas predefinidas o configuradas y analítica de comportamiento soportada. El oferente identificará los tiempos de aprendizaje y configuración. La aceptación comprobará los eventos visibles, la línea base disponible y las acciones de protección en escenarios definidos, sin imponer ausencia de políticas como condición para toda la prevención.

Decisión	No aceptada
Respuesta UAERMV	La UAERMV se permite informar que dado que el plazo de ejecución del contrato para la instalación, configuración, pruebas y puesta en marcha es de dos (2) meses, la UAERMV requiere una plataforma DLP de nueva generación que brinde visibilidad inmediata sobre el movimiento y exfiltración de datos desde el momento en que se activan los agentes y conectores en la nube, sin depender de que se hayan creado previamente reglas o políticas manuales (visibilidad inmediata sin políticas). De igual forma, es indispensable que el motor de Machine Learning y analítica de comportamiento (UEBA/UBA) inicie la recolección y perfilamiento desde el primer día de despliegue para construir la línea base de actividad de cada usuario y detectar desviaciones o comportamientos anómalos de forma temprana. En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 22	**GLOBAL SEIS SAS — Técnico**
Observación presentada	La solución debe integrar aprendizaje automático desde el primer día para establecer una línea base de la actividad individual del usuario y utilizar algoritmos de análisis de comportamiento para detectar comportamientos típicos frente a comportamientos novedosos o anómalos.
Solicitud de aclaración o ajuste	Solicitamos a la Entidad modificar el texto actual del requisito por el siguiente: La solución deberá identificar actividad y anomalías de usuarios mediante analítica de comportamiento documentada en los componentes endpoint o cloud de la solución. El oferente declarará fuentes, alcance por canal y tiempo de aprendizaje. Se verificará la visibilidad inicial y la detección de escenarios definidos, sin imponer que toda la analítica opere en el agente ni que la línea base esté completa desde el primer día.
Decisión	No aceptada
Respuesta UAERMV	La UAERMV se permite informar que dado que el plazo de ejecución del contrato para la instalación, configuración, pruebas y puesta en marcha es de dos (2) meses, la UAERMV requiere una plataforma DLP de nueva generación que brinde visibilidad inmediata sobre el movimiento y exfiltración de datos desde el momento en que se activan los agentes y conectores en la nube, sin depender de que se hayan creado previamente reglas o políticas manuales (visibilidad inmediata sin políticas). De igual forma, es indispensable que el motor de Machine Learning y analítica de comportamiento (UEBA/UBA) inicie la recolección y perfilamiento desde el primer día de despliegue para construir la línea base de actividad de cada usuario y detectar desviaciones o comportamientos anómalos de forma temprana. En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 23	**GLOBAL SEIS SAS — Técnico**
Observación presentada	La solución debe identificar y rastrear datos automáticamente según su origen, como sistemas de recursos humanos o repositorios de código fuente, sin necesidad de incluir reglas iniciales para la detección.
Solicitud de aclaración o ajuste	Solicitamos a la Entidad modificar el texto actual del requisito por el siguiente: La solución deberá registrar y relacionar, en los canales y sistemas definidos por la Entidad, el origen disponible, usuario, destino y transformaciones observables de información sensible. El oferente documentará la técnica y sus límites. Las pruebas incluirán copia, modificación y transferencia de datos por los canales requeridos y comprobarán los vínculos conservados y las acciones de prevención. No se exigirá una denominación comercial específica.
Decisión	No aceptada
Respuesta UAERMV	La UAERMV se permite informar que la capacidad de identificar y rastrear datos automáticamente según su origen (Source-based data protection) y mantener el seguimiento del linaje de datos (Data Lineage) con detección de manipulación de archivos a lo largo del tiempo constituyen pilares técnicos esenciales para evitar que información confidencial descargada de repositorios institucionales o sistemas misionales pierda su trazabilidad cuando un usuario intenta renombrarla, copiar su contenido o alterar su formato. No es viable supeditar el cumplimiento del requisito a las limitaciones que cada proponente declare en su oferta. Se aclara que la Entidad evalúa la capacidad funcional descrita en el formato GCON-FM-022 y no una denominación comercial propietaria, siempre que se acredite con la documentación técnica oficial del fabricante. En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 24	**GLOBAL SEIS SAS — Técnico**
Observación presentada	Seguimiento del linaje de datos con detección de manipulación de archivos.
Solicitud de aclaración o ajuste	Solicitamos a la Entidad modificar el texto actual del requisito por el siguiente: La solución deberá registrar y relacionar, en los canales y sistemas definidos por la Entidad, el origen disponible, usuario, destino y transformaciones observables de información sensible. El oferente documentará la técnica y sus límites. Las pruebas incluirán copia, modificación y transferencia de datos por los canales requeridos y

	comprobarán los vínculos conservados y las acciones de prevención. No se exigirá una denominación comercial específica.
Decisión	No aceptada
Respuesta UAERMV	La UAERMV se permite informar que la capacidad de identificar y rastrear datos automáticamente según su origen (Source-based data protection) y mantener el seguimiento del linaje de datos (Data Lineage) con detección de manipulación de archivos a lo largo del tiempo constituyen pilares técnicos esenciales para evitar que información confidencial descargada de repositorios institucionales o sistemas misionales pierda su trazabilidad cuando un usuario intenta renombrarla, copiar su contenido o alterar su formato. No es viable supeditar el cumplimiento del requisito a las limitaciones que cada proponente declare en su oferta. Se aclara que la Entidad evalúa la capacidad funcional descrita en el formato GCON-FM-022 y no una denominación comercial propietaria, siempre que se acredite con la documentación técnica oficial del fabricante. En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 25	**GLOBAL SEIS SAS — Técnico**
Observación presentada	La solución debe mapear las detecciones de actividades de alto riesgo a una base de conocimientos de tácticas, técnicas y procedimientos de amenazas internas y secuenciarlas automáticamente en incidentes con puntuación de riesgo para priorizar las investigaciones.
Solicitud de aclaración o ajuste	Solicitamos a la Entidad modificar el texto actual del requisito por el siguiente: Las detecciones de amenazas internas deberán relacionarse con una base pública de tácticas y técnicas identificada por nombre y versión, admitiendo mapeos equivalentes documentados. La solución deberá explicar la evidencia conductual, la secuencia observada y el criterio de priorización del incidente. Se comprobarán casos de exfiltración definidos por la Entidad, diferenciando los eventos aislados de su correlación en una secuencia.
Decisión	No aceptada
Respuesta UAERMV	La UAERMV se permite informar que el formato GCON-FM-022 ya define de manera expresa y estandarizada el marco de referencia aplicable, exigiendo en los requerimientos de la solución DLP: "La solución debe mapear las actividades en un formato de MITRE" y contar con "Biblioteca de detección de amenazas internas mapeada con MITRE ATT&CK" junto con la secuenciación automática en incidentes con puntuación de riesgo (Risk Scoring). En consecuencia, el requerimiento es

	completamente claro, objetivo y tecnológicamente neutro, por lo que se mantiene sin modificación.

Observación N.° 26	**GLOBAL SEIS SAS — Técnico**
Observación presentada	Soporte de Evidence Store para el análisis forense de archivos y portapapeles.
Solicitud de aclaración o ajuste	Solicitamos a la Entidad modificar el texto actual del requisito por el siguiente: La solución deberá capturar, cuando corresponda a un escenario autorizado, las evidencias de archivos, portapapeles y pantalla requeridas para investigar una infracción. Se admitirán repositorios de evidencia funcionalmente equivalentes, con cifrado, control de acceso, auditoría, integridad y mecanismos de consulta y exportación. La Entidad especificará región, retención, custodia de claves y flujos de autorización y reidentificación. El oferente demostrará los tipos de evidencia disponibles por canal y sistema operativo.
Decisión	No aceptada
Respuesta UAERMV	La UAERMV se permite informar que la expresión Evidence Store alude a la funcionalidad de repositorio o almacenamiento forense seguro en la nube para conservar las evidencias capturadas (archivos, portapapeles y capturas de pantalla), la cual puede ser acreditada independientemente de cómo cada fabricante denomine comercialmente dicho repositorio en su consola, siempre que cumpla íntegramente con la función técnica exigida. No se acepta eliminar ni modificar las exigencias de seudonimización de cuentas y de flujos de trabajo de autorización de investigaciones listos para usar (out-of-the-box), toda vez que dichos controles técnicos de minimización de datos y privacidad por diseño son obligatorios en el Anexo Técnico para garantizar la confidencialidad de los funcionarios públicos de la UAERMV y el cumplimiento de la Ley 1581 de 2012 y estándares internacionales de privacidad durante las investigaciones de riesgo interno. Se mantienen los tres ítems en los términos del formato GCON-FM-022. En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 27	**GLOBAL SEIS SAS — Técnico**
Observación presentada	Soporte de Evidence Store para análisis forense de captura de pantalla.

Solicitud de aclaración o ajuste	Solicitamos a la Entidad modificar el texto actual del requisito por el siguiente: La solución deberá capturar, cuando corresponda a un escenario autorizado, las evidencias de archivos, portapapeles y pantalla requeridas para investigar una infracción. Se admitirán repositorios de evidencia funcionalmente equivalentes, con cifrado, control de acceso, auditoría, integridad y mecanismos de consulta y exportación. La Entidad especificará región, retención, custodia de claves y flujos de autorización y reidentificación. El oferente demostrará los tipos de evidencia disponibles por canal y sistema operativo.
Decisión	No aceptada
Respuesta UAERMV	La UAERMV se permite informar que la expresión Evidence Store alude a la funcionalidad de repositorio o almacenamiento forense seguro en la nube para conservar las evidencias capturadas (archivos, portapapeles y capturas de pantalla), la cual puede ser acreditada independientemente de cómo cada fabricante denomine comercialmente dicho repositorio en su consola, siempre que cumpla íntegramente con la función técnica exigida. No se acepta eliminar ni modificar las exigencias de seudonimización de cuentas y de flujos de trabajo de autorización de investigaciones listos para usar (out-of-the-box), toda vez que dichos controles técnicos de minimización de datos y privacidad por diseño son obligatorios en el Anexo Técnico para garantizar la confidencialidad de los funcionarios públicos de la UAERMV y el cumplimiento de la Ley 1581 de 2012 y estándares internacionales de privacidad durante las investigaciones de riesgo interno. Se mantienen los tres ítems en los términos del formato GCON-FM-022. En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 28	**GLOBAL SEIS SAS — Técnico**
Observación presentada	La solución debe permitir políticas de protección de privacidad de datos como almacenamiento de datos y logs forenses en datacenters de la compañía, colocar seudónimos a los nombres de las cuentas que se están investigando para que el analista no sepa a quien se hace la revisión e incluir la autorización de investigaciones fuera de la caja (out-of-the-box) por parte de analistas.
Solicitud de aclaración o ajuste	Solicitamos a la Entidad modificar el texto actual del requisito por el siguiente: La solución deberá capturar, cuando corresponda a un escenario autorizado, las evidencias de archivos, portapapeles y pantalla requeridas para investigar una infracción. Se admitirán repositorios de evidencia funcionalmente equivalentes, con cifrado, control de acceso, auditoría, integridad y mecanismos de consulta y exportación. La Entidad especificará región, retención, custodia de claves y flujos de

	autorización y reidentificación. El oferente demostrará los tipos de evidencia disponibles por canal y sistema operativo.
Decisión	No aceptada
Respuesta UAERMV	La UAERMV se permite informar que la expresión Evidence Store alude a la funcionalidad de repositorio o almacenamiento forense seguro en la nube para conservar las evidencias capturadas (archivos, portapapeles y capturas de pantalla), la cual puede ser acreditada independientemente de cómo cada fabricante denomine comercialmente dicho repositorio en su consola, siempre que cumpla íntegramente con la función técnica exigida. No se acepta eliminar ni modificar las exigencias de seudonimización de cuentas y de flujos de trabajo de autorización de investigaciones listos para usar (out-of-the-box), toda vez que dichos controles técnicos de minimización de datos y privacidad por diseño son obligatorios en el Anexo Técnico para garantizar la confidencialidad de los funcionarios públicos de la UAERMV y el cumplimiento de la Ley 1581 de 2012 y estándares internacionales de privacidad durante las investigaciones de riesgo interno. Se mantienen los tres ítems en los términos del formato GCON-FM-022. En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 29	**GLOBAL SEIS SAS — Técnico**
Observación presentada	La solución debe incluir un servicio de buenas prácticas llevado a cabo por el fabricante que incluya el análisis inicial, revisión de políticas a implementar, ajuste de la solución, recomendaciones y seguimiento durante el primer mes de implementación y seguimiento mensual y final de la solución implementada. Debe realizarse directamente por el fabricante de la solución, no puede ser realizado por el oferente.
Solicitud de aclaración o ajuste	Solicitamos a la Entidad modificar el texto actual del requisito por el siguiente: La oferta incluirá soporte del fabricante y los servicios especializados de detección, respuesta y buenas prácticas requeridos, con responsabilidades, horarios, tiempos de atención, actividades, informes y escalamiento definidos. Podrán ejecutarse directamente por el fabricante o por especialistas certificados y autorizados, conservando el respaldo de producto y los niveles de servicio exigidos. Se verificarán el análisis inicial, revisión y ajuste de políticas, seguimiento y evidencia de las acciones durante la vigencia solicitada.
Decisión	No aceptada
Respuesta UAERMV	La UAERMV se permite informar que la exigencia de que tanto el servicio de Detección y Respuesta Gestionada (MDR) en la solución EDR como el Servicio de

	Buenas Prácticas en la solución DLP sean prestados directamente por el fabricante obedece a una decisión técnica y operativa debidamente estructurada en el Estudio del Sector y los Estudios Previos. Respecto al servicio MDR: Garantiza a la UAERMV acceso directo y sin intermediación a los equipos de ingeniería, inteligencia global de amenazas e investigación forense del fabricante, evitando capas adicionales de escalamiento o tercerización que incrementen los tiempos de respuesta frente a incidentes críticos y asegurando una interacción transparente con el ecosistema de ciberseguridad preexistente de la Entidad. Respecto al servicio de buenas prácticas de DLP: Mientras el contratista (oferente) ejecuta la implementación y presta el soporte local, el fabricante realiza directamente el análisis inicial, la revisión y ajuste de políticas y el seguimiento mensual y final. Ello constituye un mecanismo de aseguramiento de calidad (Quality Assurance directo de fábrica) que perdería su propósito de control independiente si fuera ejecutado por el mismo oferente o por terceros subcontratados. El Estudio del Sector corroboró que ambos servicios directos de fábrica se encuentran disponibles en el mercado y están contemplados dentro del Presupuesto Oficial Estimado. En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 30	**GLOBAL SEIS SAS — Técnico**
Observación presentada	La solución debe utilizar tecnología de agente ligero compatible con sistemas operativos Windows, macOS y Linux para una implementación sin problemas y actualizaciones automáticas a escala empresarial. Las funciones deben ser similares en los tres sistemas operativos.
Solicitud de aclaración o ajuste	Solicitamos a la Entidad modificar el texto actual del requisito por el siguiente: La solución deberá soportar las versiones, arquitecturas y kernels existentes en el inventario de la Entidad. El oferente presentará matriz oficial de compatibilidad y cobertura funcional por plataforma, identificando limitaciones y actualizaciones previstas. La evaluación se realizará sobre las plataformas y pruebas publicadas. Las nuevas versiones se incorporarán durante la suscripción según el soporte oficialmente liberado, sin exigir soporte anticipado de versiones futuras ni arquitecturas que no correspondan al sistema.
Decisión	No aceptada
Respuesta UAERMV	La UAERMV se permite informar que los sistemas operativos y versiones listados en el formato GCON-FM-022 (Windows 11, macOS Ventura 13 y superior, Windows Server 2019/2022 y superior, Oracle Linux 8/9 y superior, Ubuntu Server LTS 24.04 y

	superior, y CentOS 8/9 y superior) corresponden al inventario tecnológico real que opera en la UAERMV y que requiere protección. Aceptar que los proponentes entreguen una matriz declarando "limitaciones" de cobertura funcional entre sistemas operativos dejaría vectores de exfiltración desprotegidos en equipos macOS o Linux y equivaldría a aceptar propuestas parciales o condicionadas, lo cual no está permitido en los literales d), s) y t) del numeral 3.4 del Proyecto de Pliego de Condiciones. En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 31	**GLOBAL SEIS SAS — Técnico**
Observación presentada	La plataforma de seguridad de DLP debe ser una arquitectura distribuida, la cual debe constar de un agente en software el cual debe ser compatible con los siguientes sistemas operativos y entornos con los que cuenta la Entidad, en versiones de 32 y 64 bits: · Windows: 11. · MacOS: Ventura 13 y superior. · Windows Server: 2019, 2022 y superior. · Linux: Oracle Linux 8, 9 y superior, Ubuntu server LTS 24.04 y superior, CentOS 8, 9 y superior.
Solicitud de aclaración o ajuste	Solicitamos a la Entidad modificar el texto actual del requisito por el siguiente: La solución deberá soportar las versiones, arquitecturas y kernels existentes en el inventario de la Entidad. El oferente presentará matriz oficial de compatibilidad y cobertura funcional por plataforma, identificando limitaciones y actualizaciones previstas. La evaluación se realizará sobre las plataformas y pruebas publicadas. Las nuevas versiones se incorporarán durante la suscripción según el soporte oficialmente liberado, sin exigir soporte anticipado de versiones futuras ni arquitecturas que no correspondan al sistema.
Decisión	No aceptada
Respuesta UAERMV	La UAERMV se permite informar que los sistemas operativos y versiones listados en el formato GCON-FM-022 (Windows 11, macOS Ventura 13 y superior, Windows Server 2019/2022 y superior, Oracle Linux 8/9 y superior, Ubuntu Server LTS 24.04 y superior, y CentOS 8/9 y superior) corresponden al inventario tecnológico real que opera en la UAERMV y que requiere protección. Aceptar que los proponentes entreguen una matriz declarando "limitaciones" de cobertura funcional entre sistemas operativos dejaría vectores de exfiltración desprotegidos en equipos macOS o Linux y equivaldría a aceptar propuestas parciales o condicionadas, lo cual no está permitido en los literales d), s) y t) del numeral 3.4 del Proyecto de Pliego de Condiciones. En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 32	**GLOBAL SEIS SAS — Técnico**
Observación presentada	La solución debe monitorear datos sensibles copiados/descargados a una máquina virtual sin agente de punto final.
Solicitud de aclaración o ajuste	Solicitamos a la Entidad modificar el texto actual del requisito por el siguiente: Para cada escenario la Entidad indicará origen, destino, sistema operativo, aplicación, conexión y acción esperada. Se aceptarán mecanismos soportados de visibilidad y prevención en el endpoint de origen o en el canal correspondiente. La aceptación comprobará el dato observado, la acción ejecutada y la evidencia, sin presumir visibilidad dentro de un dispositivo no gestionado.
Decisión	No aceptada
Respuesta UAERMV	La UAERMV se permite informar que el requerimiento técnico está redactado de forma clara y se refiere al escenario en el cual, desde un equipo corporativo protegido con el agente DLP o desde un entorno gestionado por la solución, un usuario intenta copiar (vía portapapeles, carpetas compartidas o transferencia de archivos) o descargar información sensible hacia una máquina virtual huésped o sesión virtualizada que carece de agente instalado. La inspección y el monitoreo se ejecutan desde el agente del endpoint anfitrión/origen o el conector del canal correspondiente para impedir que el uso de máquinas virtuales locales o remotas sin agente se convierta en un mecanismo de evasión de controles DLP. Siendo claro el alcance técnico del ítem, no se requiere modificar su redacción. En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 33	**GLOBAL SEIS SAS — Técnico**
Observación presentada	La solución debe incluir un asistente de IA que resuma y contextualice los datos asociados con actividades de alto riesgo para acelerar el análisis de incidentes.
Solicitud de aclaración o ajuste	Solicitamos a la Entidad modificar el texto actual del requisito por el siguiente: La solución deberá proporcionar contexto y resúmenes verificables de incidentes DLP a partir de sus eventos, evidencias y relaciones de usuario y activo. Se admitirán funciones de análisis integradas, automatizadas o asistidas por IA, documentando las fuentes y el control de acceso. La aceptación comprobará la información útil para investigación sin exigir un asistente con una denominación o tecnología específica.
Decisión	No aceptada
Respuesta UAERMV	La UAERMV se permite informar que de acuerdo con el análisis de madurez operativa de la Entidad y la justificación técnica del estudio del sector, contar con un

	asistente de Inteligencia Artificial embebido en la solución DLP que sintetice y contextualice automáticamente las actividades de alto riesgo es un requerimiento obligatorio para acelerar la investigación de incidentes y optimizar la capacidad de gestión del equipo técnico de la UAERMV. Reemplazar el asistente de IA por reportes o resúmenes automatizados convencionales rebajaría el estándar tecnológico requerido en la ficha técnica. Se aclara que no se exige un nombre comercial específico para dicho asistente, siempre que la funcionalidad basada en Inteligencia Artificial esté incluida y operativa dentro del licenciamiento ofertado. En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 34	**GLOBAL SEIS SAS — Técnico**
Observación presentada	La solución debe permitir a los analistas de seguridad tomar acciones según la gravedad del riesgo, como mostrar un mensaje en pantalla al empleado, tomar una captura de pantalla, terminar un proceso, bloquear conexiones a un dispositivo o bloquear el teclado y el ratón de un dispositivo.
Solicitud de aclaración o ajuste	Solicitamos a la Entidad modificar el texto actual del requisito por el siguiente: La solución deberá permitir acciones proporcionales al incidente mediante controles DLP y componentes de respuesta integrados: notificación, bloqueo de transferencia, aislamiento del activo o terminación del proceso, según las capacidades documentadas y autorizaciones. La Entidad definirá las acciones obligatorias por escenario. No se exigirá bloquear teclado y ratón cuando otro mecanismo demuestre la contención efectiva del riesgo.
Decisión	No aceptada
Respuesta UAERMV	La UAERMV se permite informar que dentro de la gestión de amenazas internas (Insider Threat) y prevención de fuga de datos, existen escenarios críticos en los que el aislamiento de las conexiones de red no es suficiente para impedir que un usuario malicioso continúe manipulando, destruyendo, cifrando o extrayendo localmente información sensible desde la estación de trabajo física. Por tal motivo, la capacidad de los analistas de seguridad para ejecutar acciones graduales de respuesta en tiempo real, incluyendo desde notificaciones en pantalla, capturas forenses, terminación de procesos y bloqueo de conexiones, hasta el bloqueo remoto del teclado y el ratón del dispositivo, es un control técnico específico de contención requerido por la UAERMV que debe estar soportado por la solución ofertada. En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 35	**GLOBAL SEIS SAS — Técnico**
Observación presentada	La solución debe ser SaaS, en cloud, sin instalación de equipos ni colectores en tierra.
Solicitud de aclaración o ajuste	Solicitamos a la Entidad modificar el texto actual del requisito por el siguiente: Mantener el requisito SaaS y la ausencia de infraestructura local adicional. No se propone eliminarlo. El oferente deberá identificar administración, detección, telemetría y custodia de evidencias en la arquitectura cloud, con los componentes incluidos, regiones y responsabilidades del servicio.
Decisión	No aceptada
Respuesta UAERMV	La UAERMV se permite informar que teniendo en cuenta que el observante manifiesta expresamente su acuerdo con mantener el requisito SaaS y la ausencia de infraestructura local adicional, se le informa que la obligación del proponente de identificar los componentes, agentes, consolas e integraciones de su arquitectura en nube ya se encuentra regulada en los numerales 1 y 6 de los Requerimientos Mínimos para la Entrega del Bien, Obra o Servicio Objeto del Contrato – Generales (páginas 26 y 27 del formato GCON-FM-022). En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 36	**GLOBAL SEIS SAS — Técnico**
Observación presentada	Debe contar con la funcionalidad de identificación de incidentes entre productos.
Solicitud de aclaración o ajuste	Solicitamos a la Entidad modificar el texto actual del requisito por el siguiente: La solución deberá relacionar eventos de los productos incluidos mediante identificadores comunes y casos de uso documentados. Se permitirán componentes integrados incluidos en la suscripción. La aceptación verificará fuentes, contexto, reglas y acciones por escenario. La normalización en el SIEM será responsabilidad del operador de esa plataforma.
Decisión	No aceptada
Respuesta UAERMV	La UAERMV se permite informar que de conformidad con el numeral 3 de los Estudios Previos y el formato GCON-FM-022, la integración requerida con la infraestructura de seguridad preexistente de la UAERMV (Next Generation Firewall FortiGate, Control de Acceso a la Red FortiNAC, SandBox FortiSandbox, Correlacionador de Eventos FortiSIEM y Analizador FortiAnalyzer) no consiste en una simple exportación unidireccional de logs planos, sino en una articulación nativa y bidireccional que permita ejecutar flujos de respuesta automatizada y coordinada en tiempo real (cuarentena de red en el NAC, bloqueo de tráfico en el firewall, detonación

	dinámica en el Sandbox y correlación de incidentes entre productos en el SIEM) sin introducir latencias ni brechas de visibilidad. Asimismo, resulta improcedente trasladar a la Entidad la obligación técnica de desarrollar o configurar la ingesta, normalización y correlación de los eventos en el SIEM. De acuerdo con el numeral 3.4 del Proyecto de Pliego de Condiciones, las ofertas no pueden presentar condicionamientos que trasladen cargas operativas a la Entidad, y según los requisitos de ejecución del formato GCON-FM-022 (páginas 27 y 30), es obligación directa del contratista garantizar la "integración con plataformas institucionales" y entregar las "evidencias de integración" funcionando a entera satisfacción como condición para el recibo final. En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 37	**GLOBAL SEIS SAS — Técnico**
Observación presentada	Navegador seguro
Solicitud de aclaración o ajuste	Solicitamos a la Entidad modificar el texto actual del requisito por el siguiente: La Entidad identificará dispositivos móviles, sistemas, navegadores y cantidades cubiertas, así como las acciones exigidas por función. Se admitirán controles integrados y componentes complementarios incluidos en la suscripción. Las pruebas diferenciarán prevención de navegación maliciosa, control de tráfico del host y protección del dispositivo móvil, conservando los resultados de seguridad exigidos para cada población.
Decisión	No aceptada
Respuesta UAERMV	La UAERMV se permite informar que la Entidad aclara a los interesados que las cantidades y plataformas de sistemas operativos cubiertas por el proceso de contratación están definidas de forma expresa y taxativa en las secciones "Generalidades" y "Componentes de la Solución EDR" de los Estudios Previos y del formato GCON-FM-022: 450 Endpoints sobre los sistemas operativos Windows 11, macOS (Ventura 13 y superior), Windows Server (2019, 2022 y superior) y Linux (Oracle Linux 8/9 y superior, Ubuntu Server LTS 24.04 y superior, y CentOS 8/9 y superior) El requerimiento de "Navegador seguro" corresponde a la capacidad de protección de endpoints del EDR para inspeccionar, detectar y bloquear en tiempo real exploits, descargas maliciosas, sesiones de comando y control (C&C) y amenazas originadas a través de los navegadores web utilizados en las estaciones de trabajo protegidas. El requerimiento de "Protección Móvil" hace referencia a que la plataforma EDR ofertada cuente dentro de su arquitectura con capacidades para la protección de equipos portátiles/móviles que operan fuera del perímetro corporativo y soporte para

	entornos móviles; precisando que el despliegue y licenciamiento exigible en el presente contrato se circunscribe a los 450 endpoints correspondientes a los sistemas operativos listados en el formato GCON-FM-022 (Windows, macOS, Windows Server y Linux), sin exigir licencias adicionales para teléfonos móviles inteligentes (smartphones) por fuera de dichos 450 endpoints. Finalmente, tal como lo establece el numeral 6 de la página 27 del formato GCON-FM-022, ya se permite el uso de controles integrados y componentes complementarios cuando sean necesarios para cumplir las capacidades solicitadas, siempre que estén incluidos en el licenciamiento ofertado y no generen costos adicionales para la Entidad En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 38	**GLOBAL SEIS SAS — Técnico**
Observación presentada	Protección Móvil
Solicitud de aclaración o ajuste	Solicitamos a la Entidad modificar el texto actual del requisito por el siguiente: La Entidad identificará dispositivos móviles, sistemas, navegadores y cantidades cubiertas, así como las acciones exigidas por función. Se admitirán controles integrados y componentes complementarios incluidos en la suscripción. Las pruebas diferenciarán prevención de navegación maliciosa, control de tráfico del host y protección del dispositivo móvil, conservando los resultados de seguridad exigidos para cada población.
Decisión	No aceptada
Respuesta UAERMV	La UAERMV se permite informar que la Entidad aclara a los interesados que las cantidades y plataformas de sistemas operativos cubiertas por el proceso de contratación están definidas de forma expresa y taxativa en las secciones "Generalidades" y "Componentes de la Solución EDR" de los Estudios Previos y del formato GCON-FM-022: 450 Endpoints sobre los sistemas operativos Windows 11, macOS (Ventura 13 y superior), Windows Server (2019, 2022 y superior) y Linux (Oracle Linux 8/9 y superior, Ubuntu Server LTS 24.04 y superior, y CentOS 8/9 y superior) El requerimiento de "Navegador seguro" corresponde a la capacidad de protección de endpoints del EDR para inspeccionar, detectar y bloquear en tiempo real exploits, descargas maliciosas, sesiones de comando y control (C&C) y amenazas originadas a través de los navegadores web utilizados en las estaciones de trabajo protegidas. El requerimiento de "Protección Móvil" hace referencia a que la plataforma EDR ofertada cuente dentro de su arquitectura con capacidades para la protección de equipos portátiles/móviles que operan fuera del perímetro corporativo y soporte para

	entornos móviles; precisando que el despliegue y licenciamiento exigible en el presente contrato se circunscribe a los 450 endpoints correspondientes a los sistemas operativos listados en el formato GCON-FM-022 (Windows, macOS, Windows Server y Linux), sin exigir licencias adicionales para teléfonos móviles inteligentes (smartphones) por fuera de dichos 450 endpoints. Finalmente, tal como lo establece el numeral 6 de la página 27 del formato GCON-FM-022, ya se permite el uso de controles integrados y componentes complementarios cuando sean necesarios para cumplir las capacidades solicitadas, siempre que estén incluidos en el licenciamiento ofertado y no generen costos adicionales para la Entidad En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 39	**INFRAESTRUCTURA VIRTUAL — Técnico**
Observación presentada	Ficha técnica: "Solución EDR Avanzada | 450 | Endpoint" y "Descubrimiento | 450 | Endpoint" (frente a 800 endpoints del Lote 2 - DLP).
Solicitud de aclaración o ajuste	Solicitamos confirmar la cantidad exacta de endpoints a licenciar en el Lote 1 (EDR y Descubrimiento = 450) y si corresponden al mismo parque del Lote 2.
Decisión	No aceptada
Respuesta UAERMV	La UAERMV se permite informar que las referencias a "800 endpoints" y a una división por "Lote 1" y "Lote 2" citadas en su escrito no corresponden con lo requerido en los documentos publicados del presente proceso de selección No. UMV-SASI-008-2026. De conformidad con lo establecido de manera uniforme en el numeral 3 de los Estudios Previos (páginas 8 y 11) y en el formato GCON-FM-022 (Descripción Técnica de la Necesidad, páginas 8, 12, 17 y 18), el presente proceso no se encuentra dividido por lotes y las cantidades exactas requeridas por la UAERMV son: Ítem 1 – Solución de Endpoint Detection and Response (EDR) Avanzada: Cuatrocientos cincuenta (450) Endpoints (licenciamiento que incluye de forma integrada todas las funcionalidades exigidas de Prevención, Descubrimiento, Detección y Protección, Protección contra Ransomware, Remediación e Investigación). Ítem 2 – Solución de Data Loss Prevention (DLP) Avanzada: Cuatrocientos cincuenta (450) Endpoints (incluido el conector para Microsoft Office 365). Ambas cantidades (450 endpoints para EDR y 450 endpoints para DLP) están destinadas a cubrir el parque computacional de la UAERMV bajo una vigencia de suscripción y soporte de doce (12) meses

Observación N.° 40	**INFRAESTRUCTURA VIRTUAL — Técnico**
Observación presentada	Ficha técnica: "Solución EDR Avanzada | 450 | Endpoint" y "Descubrimiento | 450 | Endpoint" (frente a 800 endpoints del Lote 2 - DLP).
Solicitud de aclaración o ajuste	Solicitamos confirmar la cantidad exacta de endpoints a licenciar en el Lote 1 (EDR y Descubrimiento = 450) y si corresponden al mismo parque del Lote 2.
Decisión	No aceptada
Respuesta UAERMV	La UAERMV se permite informar que las referencias a "800 endpoints" y a una división por "Lote 1" y "Lote 2" citadas en su escrito no corresponden con lo requerido en los documentos publicados del presente proceso de selección No. UMV-SASI-008-2026. De conformidad con lo establecido de manera uniforme en el numeral 3 de los Estudios Previos (páginas 8 y 11) y en el formato GCON-FM-022 (Descripción Técnica de la Necesidad, páginas 8, 12, 17 y 18), el presente proceso no se encuentra dividido por lotes y las cantidades exactas requeridas por la UAERMV son: Ítem 1 – Solución de Endpoint Detection and Response (EDR) Avanzada: Cuatrocientos cincuenta (450) Endpoints (licenciamiento que incluye de forma integrada todas las funcionalidades exigidas de Prevención, Descubrimiento, Detección y Protección, Protección contra Ransomware, Remediación e Investigación). Ítem 2 – Solución de Data Loss Prevention (DLP) Avanzada: Cuatrocientos cincuenta (450) Endpoints (incluido el conector para Microsoft Office 365). Ambas cantidades (450 endpoints para EDR y 450 endpoints para DLP) están destinadas a cubrir el parque computacional de la UAERMV bajo una vigencia de suscripción y soporte de doce (12) meses

Observación N.° 41	**INFRAESTRUCTURA VIRTUAL — Técnico**
Observación presentada	Tabla EDR, num. 12: "…permitir el análisis dinámico o comportamental de archivos sospechosos mediante sandbox, detonación controlada u otros mecanismos técnicamente equivalentes. Esta capacidad podrá ser proporcionada de manera nativa, mediante servicios del fabricante, integraciones, módulos o componentes complementarios…".
Solicitud de aclaración o ajuste	Solicitamos confirmar que el análisis dinámico/sandbox podrá acreditarse mediante los mecanismos del fabricante (análisis conductual en el agente, servicios en nube o integración documentada), conforme a la redacción del pliego.
Decisión	No aceptada

Respuesta UAERMV	La Entidad informa al observante que el texto entrecomillado en su pregunta no corresponde a la redacción de los Estudios Previos ni del formato GCON-FM-022 publicados en el presente proceso UMV-SASI-008-2026.

Observación N.° 42	**INFRAESTRUCTURA VIRTUAL — Técnico**
Observación presentada	Requerimientos específicos Lote 1 / Tabla Telemetría: "Mayor nivel de visibilidad, retención de telemetría y capacidades de hunting proactivo…" ; "Retención de datos | Ampliada".
Solicitud de aclaración o ajuste	Solicitamos que la Entidad especifique el período mínimo de retención de telemetría requerido (en días), con el fin de dimensionar el plan de datos correspondiente de forma precisa y comparable entre oferentes.
Decisión	No aceptada
Respuesta UAERMV	La Entidad informa al observante que el texto entrecomillado en su observación no corresponde a la redacción de los Estudios Previos ni del formato GCON-FM-022 publicados en el presente proceso UMV-SASI-008-2026.

Observación N.° 43	**INFRAESTRUCTURA VIRTUAL — Técnico**
Observación presentada	ROL Ingeniero de Operación y Soporte (Lote 1): "Certificación en respuesta a incidentes del fabricante de la oferta" y "Certificación en cacería de amenazas del fabricante de la oferta".
Solicitud de aclaración o ajuste	Las certificaciones de "respuesta a incidentes" y "cacería de amenazas" emitidas por el fabricante corresponden a credenciales especializadas de alto nivel, disponibles en un número muy limitado de profesionales en el mercado local, lo que restringe la pluralidad de oferentes. Solicitamos respetuosamente que: (i) no se exijan como requisito habilitante, admitiendo en su lugar certificaciones de nivel de administración/operación del fabricante complementadas con la experiencia específica del profesional en operación y respuesta de plataformas de seguridad; o (ii) se admitan certificaciones técnicamente equivalentes y/o certificados de formación o entrenamiento autorizados por el fabricante; o, en su defecto, (iii) se trasladen a criterio ponderable y no habilitante.
Decisión	No aceptada
Respuesta UAERMV	La Entidad informa al observante que el texto entrecomillado en su observación no corresponde a la redacción de los Estudios Previos ni del formato GCON-FM-022 publicados en el presente proceso UMV-SASI-008-2026.

Observación N.° 44	**INFRAESTRUCTURA VIRTUAL — Técnico**
Observación presentada	Certificaciones de partner (todos los lotes): "…carta emitida por el fabricante… que certifique que el proponente es Partner, canal o socio de la marca…", en concordancia con los perfiles de personal exigidos.
Solicitud de aclaración o ajuste	Dado que la condición de Partner/canal autorizado del fabricante exige por sí misma contar con personal capacitado y acreditado por la marca, solicitamos que dicha condición de Partner, complementada con certificados de formación o entrenamiento autorizados por el fabricante y con la experiencia en proyectos ejecutados, sea aceptada como medio válido para acreditar la idoneidad técnica del oferente, sin requerir certificaciones individuales especializadas de alto nivel como condición habilitante.
Decisión	No aceptada
Respuesta UAERMV	La Entidad informa al observante que el texto entrecomillado en su observación no corresponde a la redacción de los Estudios Previos ni del formato GCON-FM-022 publicados en el presente proceso UMV-SASI-008-2026

Observación N.° 45	**INFRAESTRUCTURA VIRTUAL — Técnico**
Observación presentada	Tabla DLP, num. 2: "…identificar información sensible por medio de patrones de contenido, expresiones regulares o etiquetas de Microsoft". / Descripción: "…reconocer etiquetas o metadatos de clasificación, incluidos los utilizados en el entorno Microsoft de la Entidad cuando aplique… u otros mecanismos interoperables".
Solicitud de aclaración o ajuste	Solicitamos confirmar que el reconocimiento de información clasificada podrá acreditarse mediante motores de clasificación técnicamente equivalentes (clasificación de terceros, metadatos y/o huellas digitales), sin exigir el reconocimiento nativo de etiquetas Microsoft Purview/MIP como condición habilitante, en coherencia con la redacción del pliego ("cuando aplique" / "u otros mecanismos interoperables").
Decisión	No aceptada
Respuesta UAERMV	La Entidad informa al observante que el texto entrecomillado en su observación no corresponde a la redacción de los Estudios Previos ni del formato GCON-FM-022 publicados en el presente proceso UMV-SASI-008-2026.

Observación N.° 46	**INFRAESTRUCTURA VIRTUAL — Técnico**
Observación presentada	"La solución deberá ser compatible, como mínimo, con sistemas operativos Windows, Linux y macOS…" (Requerimientos mínimos generales).
Solicitud de aclaración o ajuste	Solicitamos confirmar si el parque de 800 endpoints del Lote 2 (DLP) incluye estaciones con sistema operativo Linux y en qué cantidad. En caso afirmativo, solicitamos que para los sistemas operativos no soportados por el componente de DLP de endpoint se admitan controles técnicamente equivalentes o se excluyan del alcance de DLP, manteniendo el cumplimiento sobre Windows y macOS.
Decisión	No aceptada
Respuesta UAERMV	Conforme a los Estudios Previos (páginas 13 y 15) y al formato GCON-FM-022 (páginas 13, 15 y 27), la plataforma DLP y su agente ligero deben ser compatibles con los sistemas operativos Windows (Windows 11 y Windows Server 2019, 2022 y superior), macOS (Ventura 13 y superior) y Linux (Oracle Linux 8, 9 y superior, Ubuntu Server LTS 24.04 y superior, y CentOS 8, 9 y superior), exigiendo expresamente que: "La solución debe utilizar tecnología de agente ligero compatible con sistemas operativos Windows, macOS y Linux para una implementación sin problemas y actualizaciones automáticas a escala empresarial. Las funciones deben ser similares en los tres sistemas operativos". Asimismo, la entidad informa que el parque computacional es de 450 endpoints y requiere que la totalidad de las 450 suscripciones contratadas permita proteger de forma homogénea cualquiera de los sistemas operativos que conforman su inventario tecnológico (tanto en estaciones de trabajo como en entornos Linux y servidores donde reside y se procesa información sensible). Excluir el sistema operativo Linux del alcance de la solución DLP dejaría sin cobertura de prevención de fuga de datos a activos críticos de la Entidad y constituiría una modificación de las especificaciones técnicas mínimas, lo cual no es procedente. En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 47	**INFRAESTRUCTURA VIRTUAL — Técnico**
Observación presentada	Tabla DLP, num. 5: "Las políticas se deben asignar a los dispositivos, usuarios o grupos… y personalizar las notificaciones de alertamiento a los usuarios".
Solicitud de aclaración o ajuste	Solicitamos confirmar que la asignación de políticas por usuario o grupo podrá acreditarse mediante integración con Directorio Activo, y que la personalización de notificaciones al usuario podrá realizarse con los mecanismos nativos de la plataforma.

Decisión	No aceptada
Respuesta UAERMV	La Entidad informa al observante que el texto entrecomillado en su observación no corresponde a la redacción de los Estudios Previos ni del formato GCON-FM-022 publicados en el presente proceso UMV-SASI-008-2026.

Observación N.° 48	**INFRAESTRUCTURA VIRTUAL — Técnico**
Observación presentada	Ficha técnica: Protección de Datos (DLP) — "800 | EndPoints" (frente a 450 endpoints del Lote 1).
Solicitud de aclaración o ajuste	Solicitamos confirmar la cantidad exacta de endpoints a licenciar en el Lote 2 (DLP) y si corresponden al mismo parque del Lote 1.
Decisión	No aceptada
Respuesta UAERMV	La Entidad aclara al interesado que las referencias a "800 endpoints" y a una división por "Lote 1" y "Lote 2" citadas en su escrito no corresponden con lo requerido en los documentos publicados del presente proceso de selección No. UMV-SASI-008-2026. De conformidad con lo establecido de manera uniforme en el numeral 3 de los Estudios Previos (páginas 8 y 11) y en el formato GCON-FM-022 (Descripción Técnica de la Necesidad, páginas 8, 12, 17 y 18), el presente proceso no se encuentra dividido por lotes y las cantidades exactas requeridas por la UAERMV son: Ítem 1 – Solución de Endpoint Detection and Response (EDR) Avanzada: Cuatrocientos cincuenta (450) Endpoints (licenciamiento que incluye de forma integrada todas las funcionalidades exigidas de Prevención, Descubrimiento, Detección y Protección, Protección contra Ransomware, Remediación e Investigación). Ítem 2 – Solución de Data Loss Prevention (DLP) Avanzada: Cuatrocientos cincuenta (450) Endpoints (incluido el conector para Microsoft Office 365). Ambas cantidades (450 endpoints para EDR y 450 endpoints para DLP) están destinadas a cubrir el parque computacional de la UAERMV bajo una vigencia de suscripción y soporte de doce (12) meses.

Observación N.° 49	**INFRAESTRUCTURA VIRTUAL — Técnico**
Observación presentada	Perfiles de personal (Lote 2): "Certificación de profesional en administración de DLP del fabricante de la oferta".

Solicitud de aclaración o ajuste	Solicitamos aceptar certificaciones de administración de DLP del fabricante ofertado o certificaciones equivalentes, y/o la acreditación de experiencia mediante proyectos ejecutados, en garantía de la pluralidad de oferentes.
Decisión	No aceptada
Respuesta UAERMV	La Entidad informa al observante que el texto entrecomillado en su observación no corresponde a la redacción de los Estudios Previos ni del formato GCON-FM-022 publicados en el presente proceso UMV-SASI-008-2026.

Observación N.° 50	**INFRAESTRUCTURA VIRTUAL — Técnico**
Observación presentada	Lotes
Solicitud de aclaración o ajuste	Solicitamos aclarar si, dentro del presente proceso de selección, se contempla la posibilidad de presentar ofertas parciales, permitiendo que un proponente participe únicamente por uno de los componentes requeridos (solución EDR avanzada o solución DLP avanzada). En caso de que no se permita la presentación de ofertas parciales, agradecemos confirmar expresamente que la propuesta deberá incluir la totalidad de los componentes, licencias, servicios de implementación, configuración y soporte establecidos en el proceso. Lo anterior, con el propósito de brindar claridad a los interesados respecto del alcance de la participación y las condiciones para la presentación de ofertas.
Decisión	No aceptada
Respuesta UAERMV	La Entidad informa a todos los interesados que en el proceso de Selección Abreviada por Subasta Inversa Electrónica No. UMV-SASI-008-2026 NO se permite la presentación de ofertas parciales ni se realizarán adjudicaciones parciales o por lotes. De conformidad con el literal s) del numeral 3.4 (Admisibilidad y Rechazo de la Oferta) del Proyecto de Pliego de Condiciones, es causal expresa de rechazo "Cuando la oferta se presente en forma parcial". En concordancia con los numerales 2.1, 2.3 y 4.4.1 del Proyecto de Pliego de Condiciones, todo proponente deberá presentar oferta integral por la totalidad de los ítems y alcances del proceso: (i) Solución EDR Avanzada para 450 endpoints, (ii) Solución DLP Avanzada para 450 endpoints (incluido conector Microsoft Office 365) y (iii) Servicios de instalación, configuración, pruebas, puesta en marcha, estabilización y soporte 7x24x365 con fabricante y soporte local por doce meses).

Observación N.° 51	**INFRAESTRUCTURA VIRTUAL — Contractual**
Observación presentada	Solicitud de aclaración del requisito técnico relacionado con la certificación expedida por la Policía Nacional
Solicitud de aclaración o ajuste	Solicitamos a la Entidad aclarar la pertinencia de exigir el documento técnico expedido por la Policía Nacional, señalado en el capítulo de requisitos habilitantes técnicos, mediante el cual se solicita acreditar el registro y habilitación de las condiciones establecidas en el artículo 12 del Decreto 723 del 10 de abril de 2014 y la Resolución 02086 del 30 de mayo de 2014. Lo anterior, teniendo en cuenta que la normativa citada regula las condiciones técnicas y la autorización de proveedores de servicios de posicionamiento global (GPS) para el monitoreo de maquinaria, y no guarda relación aparente con el objeto del presente proceso, orientado a la adquisición e implementación de soluciones de ciberseguridad EDR y DLP. En consecuencia, solicitamos confirmar si se trata de un requisito incorporado por error y, de ser así, realizar el ajuste correspondiente en el pliego de condiciones, con el propósito de garantizar la pluralidad de oferentes y la selección objetiva.
Decisión	Aceptada
Respuesta UAERMV	Verificados los documentos del proceso, el registro y habilitación ante la policía nacional no es un requisito habilitante del presente proceso, en consecuencia, la modificación sobre este aspecto se verá reflejada en el pliego definitivo

Observación N.° 52	**INFRAESTRUCTURA VIRTUAL — Técnico**
Observación presentada	Solicitud de modificación del requisito de nivel de certificación como Partner del fabricante
Solicitud de aclaración o ajuste	Respetuosamente solicitamos a la Entidad revisar y modificar el requisito establecido en el numeral 4.2.3, relacionado con la acreditación de que el proponente cuenta con el nivel más alto de membresía o categoría como Partner del fabricante de la solución ofertada. Consideramos que exigir exclusivamente el máximo nivel de Partner constituye una condición restrictiva que podría limitar injustificadamente la pluralidad de oferentes y la libre concurrencia, al supeditar la participación en el proceso a una clasificación comercial definida unilateralmente por cada fabricante, la cual puede variar según sus políticas internas, modelos de negocio y programas de canales. Es importante señalar que el nivel de membresía de un Partner no necesariamente determina su capacidad técnica, experiencia, idoneidad o competencia para suministrar, implementar, configurar y brindar soporte a la solución objeto del

	presente proceso. Estas capacidades pueden acreditarse mediante certificaciones técnicas del fabricante, experiencia específica, personal calificado y demás requisitos habilitantes establecidos por la Entidad. En ese sentido, solicitamos respetuosamente que se permita acreditar la condición de Partner, canal autorizado o distribuidor autorizado del fabricante, sin exigir que corresponda al nivel más alto de membresía, siempre que se garantice el respaldo del fabricante y la capacidad para cumplir integralmente con las obligaciones contractuales. Esta modificación permitiría ampliar la participación de empresas técnicamente habilitadas, promover la pluralidad de oferentes y evitar que una clasificación comercial particular se convierta en una barrera de acceso al proceso, sin comprometer la calidad ni la adecuada ejecución del contrato.
Decisión	No aceptada
Respuesta UAERMV	La Entidad informa que el requisito de acreditar el nivel más alto de membresía o Partnership otorgado por el fabricante en Colombia no está atado a una denominación textual específica de un programa de canales en particular, sino que exige el mayor nivel de reconocimiento oficial disponible dentro del esquema de certificación de cada fabricante, cualquiera sea la estructura o nomenclatura que este utilice. En esa medida, el requisito es tecnológicamente neutro y aplicable de manera uniforme a cualquier fabricante. La Entidad considera que disminuir esta exigencia para aceptar canales de niveles diferentes al nivel más alto de membresía en la marca ofrecida en Colombia reduciría el estándar de idoneidad técnica y respaldo que la UAERMV requiere para la implementación y el soporte de una plataforma crítica de protección de endpoints y prevención de pérdida de datos. Los canales de niveles diferentes al nivel más alto no acreditan necesariamente la capacidad técnica plena de implementación, soporte e integración avanzada que la UAERMV requiere para este proyecto, lo que introduciría un riesgo técnico critico e inaceptable de fallas en la interoperabilidad y operación institucional durante la ejecución contractual. Adicionalmente, esta máxima capacidad de ingeniería resulta estrictamente necesaria para el presente proyecto, toda vez que el contratista adjudicatario cuenta con un plazo de ejecución de dos (2) meses para implementar, configurar, probar y poner en marcha las soluciones EDR y DLP garantizando su interoperabilidad e integración nativa y automatizada con la matriz del ecosistema de ciberseguridad existente en la Entidad (Next Generation Firewall, Control de Acceso a la Red, SandBox, Correlacionador de Eventos, Analizador y Microsoft Office 365). El Estudio del Sector adelantado por la Entidad evidenció que existe pluralidad de fabricantes y de proveedores en el mercado nacional en capacidad de acreditar el nivel más alto de su respectivo programa de canales, lo que confirma que el requisito no restringe la libre concurrencia ni la selección objetiva. En consecuencia, se

	mantiene sin modificación el requisito establecido en el numeral 4.2.3 del Pliego de Condiciones. En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente

Observación N.° 53	**ALPHATEC — Técnico**
Observación presentada	Consumo de recursos del agente EDR Archivo: ESTUDIOS PREVIOS.pdf, numeral 3 – Descripción de la necesidad, apartado 1 – Solución EDR avanzada, «Componentes de la Solución EDR» (página 11)
Solicitud de aclaración o ajuste	Solicitamos a la Entidad ajustar el requisito que limita el agente EDR a un máximo de 100 MB de memoria RAM y 20 MB de espacio en disco, permitiendo que el consumo de recursos corresponda a las especificaciones técnicas del fabricante, siempre que se garantice una operación eficiente y sin afectaciones significativas al desempeño de los equipos protegidos. Lo anterior, considerando que las soluciones actuales de detección y respuesta incorporan funciones avanzadas de telemetría, análisis de comportamiento y protección continua, cuyos requerimientos de recursos pueden variar según su arquitectura
Decisión	No aceptada
Respuesta UAERMV	La Entidad informa que su parque computacional (450 endpoints entre estaciones de trabajo propias, equipos rentados y servidores) soporta aplicaciones misionales críticas que requieren preservar la disponibilidad y el rendimiento de los recursos de hardware locales. De hecho, dentro de las responsabilidades del personal de implementación en el formato GCON-FM-022 se exige expresamente garantizar una "mínima afectación al rendimiento de los equipos". Por lo tanto, eliminar el umbral máximo de consumo (100 MB de memoria RAM y 20 MB en disco) para dejarlo a declaración abierta de cada proponente impediría realizar una verificación técnica objetiva en igualdad de condiciones y trasladaría a la Entidad el riesgo operativo de ralentización o saturación de memoria de los equipos que hacen parte del parque computacional. En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente

Observación N.° 54	**ALPHATEC — Técnico**
Observación presentada	Compatibilidad de sistemas operativos de la solución DLP Archivo: ESTUDIOS PREVIOS.pdf, numeral 3 – Descripción de la necesidad, apartado 2 – Solución DLP, «Componentes de la

	Solución DLP» (página 15).
Solicitud de aclaración o ajuste	Solicitamos a la Entidad ajustar el requerimiento de compatibilidad de sistemas operativos de la solución DLP,permitiendo que esta sea compatible con Windows 11, macOS y distribuciones Linux oficialmente soportadas por el fabricante, sin exigir de manera específica compatibilidad con Oracle Linux, CentOS o Ubuntu Server, ni con arquitecturas de 32 bits. Lo anterior, teniendo en cuenta que el alcance de la contratación establece el licenciamiento de 450 endpoints destinados a equipos de usuarios finales, por lo que consideramos pertinente que los requisitos de compatibilidad correspondan a estaciones de trabajo y no a sistemas operativos de servidor. En caso de que la Entidad requiera proteger servidores, solicitamos precisar las cantidades y los sistemas operativos efectivamente utilizados, con el fin de establecer un dimensionamiento adecuado y garantizar la participación de soluciones que cumplan con las capacidades de protección de datos requeridas.
Decisión	No aceptada
Respuesta UAERMV	La Entidad informa que como se expone en el numeral 3 de los Estudios Previos y en el formato GCON-FM-022, en el desarrollo de sus funciones la UAERMV genera y procesa información sensible que reside y circula tanto en estaciones de trabajo y portátiles como en servidores y entornos en la nube. Los sistemas operativos y entornos listados en la sección "Componentes de la Solución DLP" —Windows 11, macOS (Ventura 13 y superior), Windows Server (2019, 2022 y superior) y Linux (Oracle Linux 8, 9 y superior, Ubuntu Server LTS 24.04 y superior, CentOS 8, 9 y superior) en versiones de 32 y 64 bits— corresponden al estándar de compatibilidad multiplataforma exigido para el agente en software de acuerdo con la infraestructura tecnológica existente en la Entidad. La Entidad aclara a los interesados que las 450 suscripciones de la solución DLP se contratan bajo la unidad de medida "Endpoints" y están orientadas a la protección de los usuarios finales y sus interacciones con los datos institucionales, así como servidores, por lo tanto, el agente de la plataforma ofertada debe acreditar documentalmente la compatibilidad técnica con la totalidad de los sistemas operativos y distribuciones listadas en el formato GCON-FM-022 (Windows, macOS, Windows Server, Oracle Linux, Ubuntu LTS y CentOS), garantizando que la Entidad pueda desplegar el agente sin restricciones tecnológicas sobre cualquiera de dichos entornos dentro del cupo contratado de 450 endpoints. En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 55	**ALPHATEC — Técnico**
Observación presentada	Alcance de las funcionalidades DLP por sistema operativo Archivo: ESTUDIOS PREVIOS.pdf, numeral 3 – Descripción de la necesidad, apartado 2 – Solución DLP, «Requerimientos técnicos» (página 13).
Solicitud de aclaración o ajuste	Solicitamos a la Entidad ajustar la expresión «Las funciones deben ser similares en los tres sistemas operativos», permitiendo que las funcionalidades de monitoreo, prevención y respuesta se ofrezcan conforme a la matriz de compatibilidad y a las capacidades soportadas para cada sistema operativo. Esta precisión reconoce las diferencias técnicas entre Windows, macOS y Linux, sin dejar de exigir la protección de los datos y las funcionalidades esenciales previstas para los equipos efectivamente incluidos en el alcance del contrato.
Decisión	No aceptada
Respuesta UAERMV	La Entidad informa que el requerimiento técnico establece expresamente: "La solución debe utilizar tecnología de agente ligero compatible con sistemas operativos Windows, macOS y Linux para una implementación sin problemas y actualizaciones automáticas a escala empresarial. Las funciones deben ser similares en los tres sistemas operativos". La finalidad técnica de exigir paridad o similitud funcional entre Windows, macOS y Linux es evitar brechas de seguridad y asimetrías en la postura de prevención de pérdida de datos de la UAERMV. Si se aceptara supeditar el alcance funcional a las limitaciones particulares de la matriz de compatibilidad de cada proponente, un usuario que opere sobre macOS o Linux podría quedar exento de controles críticos de visibilidad, clasificación en tiempo real, detección de exfiltración o bloqueo que sí se aplican en Windows, dejando vectores de fuga de información desprotegidos. Adicionalmente, de conformidad con los literales d), s) y t) del numeral 3.4 del Proyecto de Pliego de Condiciones, no son admisibles propuestas que modifiquen, condicionen o cumplan parcialmente las especificaciones técnicas mínimas exigidas. En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 56	**ALPHATEC — Técnico**
Observación presentada	Gestión de parches en la solución EDR Archivo: ESTUDIOS PREVIOS.pdf, numeral 3 – Descripción de la necesidad, apartado 1 – Solución EDR avanzada, «Funcionalidades de Prevención» (página 9).

Solicitud de aclaración o ajuste	Solicitamos a la Entidad modificar el requerimiento relacionado con la gestión de parches para sistemas operativos Windows, macOS y Linux, permitiendo que esta capacidad sea acreditada mediante mecanismos de identificación, evaluación y mitigación de vulnerabilidades, incluyendo funcionalidades de parcheo virtual (Virtual Patching), sin que sea obligatorio realizar directamente la distribución e instalación de actualizaciones sobre los sistemas operativos. Lo anterior, teniendo en cuenta que dentro de las mismas especificaciones técnicas de la solución EDR se contempla la mitigación de vulnerabilidades mediante parches virtuales. En este sentido, solicitamos que dichos mecanismos sean aceptados expresamente como alternativa válida de cumplimiento, garantizando la reducción de la superficie de ataque y la protección de los equipos frente a la explotación de vulnerabilidades conocidas.
Decisión	No aceptada
Respuesta UAERMV	La Entidad informa que en la estructuración técnica de los Estudios Previos y del formato GCON-FM-022, la Entidad definió dos (2) capacidades distintas, independientes y complementarias en acápites separados: En el bloque de Funcionalidades de Prevención se exige expresamente: "Gestión de parches para sistemas operativos Windows, OS, Linux". En el bloque de Funcionalidades de Descubrimiento se exige de forma adicional: "Descubrir y mitigar las vulnerabilidades del sistema y las aplicaciones con parches virtuales, mediante el análisis de sus comunicaciones e inhabilitando el acceso a su comunicación con el exterior". Desde el punto de vista técnico de ciberseguridad e higiene de TI, el parcheo virtual (Virtual Patching) actúa como un control compensatorio inmediato en tiempo real (bloqueando las comunicaciones de procesos o aplicaciones con códigos CVE vulnerables mientras el parche es probado o desplegado), pero no sustituye la capacidad de gestión de parches (Patch Management) para remediación definitiva sobre los sistemas operativos Windows, macOS y Linux. Permitir que el requerimiento de "Gestión de parches para sistemas operativos Windows, macOS, Linux" se dé por cumplido únicamente con la funcionalidad de parches virtuales equivaldría a suprimir uno de los requisitos mínimos obligatorios de prevención previstos en la ficha técnica. Cabe recordar que, conforme al numeral 6 de los Requerimientos Mínimos Generales del formato GCON-FM-022 (página 27), se permite el uso de módulos o componentes complementarios técnicamente integrados del fabricante cuando sean necesarios para cumplir las capacidades solicitadas, siempre que estén incluidos dentro del licenciamiento ofertado y no generen costos adicionales para la Entidad durante la vigencia de la suscripción. En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 57	**BIM LATINOAMERICA — Técnico**
Observación presentada	Integración nativa con productos de un fabricante específico Requisito: el EDR debe integrarse de forma nativa con FortiGate, FortiNAC, FortiSandbox y FortiSIEM. Problema: nombrar productos de una sola marca limita la participación a ese fabricante. La necesidad de la entidad, que las herramientas compartan información, se resuelve con estándares abiertos
Solicitud de aclaración o ajuste	cambiar el requisito por: "La solución deberá integrarse con las plataformas de seguridad de la entidad mediante estándares abiertos (Syslog, CEF o API REST)."
Decisión	No aceptada
Respuesta UAERMV	La UAERMV se permite informar que de conformidad con lo expuesto en el numeral 3 (Descripción de la necesidad que se pretende satisfacer) de los Estudios Previos y en el formato GCON-FM-022, la mención de los componentes Next Generation Firewall (FortiGate), Control de Acceso a la Red (FortiNAC), SandBox (FortiSandbox), Correlacionador de Eventos (FortiSIEM) y Analizador (FortiAnalyzer) no obedece a una exigencia de marca, sino a la descripción técnica real de la infraestructura tecnológica preexistente (base instalada) de propiedad de la UAERMV, consolidada a lo largo de varios procesos contractuales públicos. La necesidad técnica de la UAERMV no se limita al simple envío unidireccional de registros planos (logs) mediante protocolos básicos como Syslog o CEF, sino que exige una respuesta automatizada, bidireccional y coordinada en tiempo real entre las capas de seguridad. Como se sustenta en los Estudios Previos, ante una alerta crítica en el endpoint, la plataforma debe estar en capacidad de ejecutar de forma orquestada una cuarentena de red a través del control de acceso (NAC), aplicar un bloqueo de tráfico en el firewall perimetral (NGFW), detonar muestras sospechosas en el Sandbox y correlacionar el incidente en tiempo real en el SIEM. Reducir este requerimiento a una integración básica de texto plano (Syslog/CEF) o a desarrollos de conectores a medida sujetos a limitaciones de versión introducirá latencias, reprocesos y complejidad que puede resultar contraproducente en los primeros minutos críticos de un incidente, puntos de falla adicionales, costos no cubiertos de middleware y riesgos operativos que la Entidad. Conforme al numeral 1 de "Detección y Respuesta de endpoints" del formato GCON-FM-022 ("Integración con plataformas del mismo fabricante y de terceros") y al numeral 6 de los Requerimientos Mínimos Generales, pueden participar soluciones del mercado que garanticen y demuestren documental y funcionalmente la integración bidireccional, automatizada y completa de los flujos de respuesta con la infraestructura existente de la Entidad, siempre que todos los conectores, licencias o

	componentes necesarios estén incluidos en la oferta sin generar costos adicionales ni complejidad administrativa para la UAERMV. En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 58	**BIM LATINOAMERICA — Técnico**
Observación presentada	"100% basado en comportamiento, sin firmas estáticas" Requisito: la detección debe ser 100% por comportamiento, sin firmas. Problema: la mayoría de las soluciones del mercado combinan aprendizaje automático y comportamiento con firmas. Las firmas no reducen la protección: la complementan.
Solicitud de aclaración o ajuste	cambiar el requisito por: "La solución deberá detectar amenazas mediante análisis de comportamiento y aprendizaje automático, y podrá complementarse con otras técnicas de detección."
Decisión	No aceptada
Respuesta UAERMV	La UAERMV se permite informar que como se establece en el análisis de riesgos de los Estudios Previos, la UAERMV requiere evolucionar desde el modelo de antivirus tradicional basado en firmas hacia una arquitectura moderna capaz de detener amenazas avanzadas de día cero (zero-day), ataques sin archivos (fileless), abuso de herramientas del sistema (living off the land) y ransomware tanto en pre-ejecución como en post-ejecución. Por consiguiente, la expresión "100% basado en comportamiento (sin firmas estáticas)" contenida en las generalidades de la solución EDR se refiere a que la eficacia de los motores de prevención (NGAV basado en kernel y Machine Learning) y de detección/respuesta post-ejecución no debe depender de la existencia previa de una firma estática para identificar, bloquear y contener un ataque en tiempo real. Por lo tanto, la Entidad aclara a los interesados que el propio Anexo Técnico (GCON-FM-022) contempla y exige capacidades complementarias como "Enriquecer los eventos de seguridad con información sobre amenazas en tiempo real desde una base de datos en la nube", "Ingesta y búsqueda de IoC" y "definir listas blancas y negras... por hash". Por consiguiente, el hecho de que la plataforma ofertada utilice inteligencia de amenazas, reputación o indicadores/firmas como mecanismos auxiliares de enriquecimiento no inhabilita la propuesta, siempre que su motor principal pre y post-ejecución opere de forma autónoma mediante Machine Learning y análisis de comportamiento sin depender de firmas estáticas. En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 59	**BIM LATINOAMERICA — Técnico**
Observación presentada	Consumo máximo del agente Requisito: el agente no debe superar 100 MB de memoria RAM ni 20 MB de disco. Problema: son valores de un producto específico. El consumo varía según los módulos activos y no es un criterio de calidad de la protección.
Solicitud de aclaración o ajuste	eliminar los valores fijos. En su lugar: "El oferente declarará los requisitos mínimos de hardware del agente, que deberán ser compatibles con los equipos de la entidad."
Decisión	No aceptada
Respuesta UAERMV	La UAERMV se permite informar que su parque computacional (450 endpoints entre estaciones de trabajo propias, equipos rentados y servidores) soporta aplicaciones misionales críticas que requieren preservar la disponibilidad y el rendimiento de los recursos de hardware locales. De hecho, dentro de las responsabilidades del personal de implementación en el formato GCON-FM-022 se exige expresamente garantizar una "mínima afectación al rendimiento de los equipos". Por lo tanto, eliminar el umbral máximo de consumo (100 MB de memoria RAM y 20 MB en disco) para dejarlo a declaración abierta de cada proponente impediría realizar una verificación técnica objetiva en igualdad de condiciones y trasladaría a la Entidad el riesgo operativo de ralentización o saturación de memoria de los equipos que hacen parte del parque computacional. En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 60	**BIM LATINOAMERICA — Técnico**
Observación presentada	Lista de 31 estrategias anti-ransomware Requisito: la solución debe prevenir una lista de 31 estrategias con nombres específicos. Problema: los nombres corresponden a la nomenclatura de un fabricante. Otros fabricantes protegen contra las mismas técnicas con otros nombres.
Solicitud de aclaración o ajuste	cambiar el requisito por: "La solución deberá prevenir técnicas de explotación, inyección de procesos y cifrado malicioso de archivos, mapeadas a la matriz MITRE ATT&CK."
Decisión	No aceptada
Respuesta UAERMV	La UAERMV se permite informar que los ítems listados bajo el acápite "Funcionalidades de Protección contra Ransomware" (tales como Debug de

	procesos, Código dinámico, Pila con código ejecutable, Proceso oculto, Ejecutable/Proceso/Hilo inyectado, Inyección de kernel, Exploit de escalamiento de privilegios, Proceso vacío [Process Hollowing], Manipulación de pilas, File Encryptor y Prevención automatizada en tiempo real de encriptación) no constituyen marcas comerciales ni términos propietarios, sino vectores técnicos específicos de explotación en memoria, evasión de defensas e inyección de código ampliamente reconocidos en la literatura técnica de ciberseguridad. Dado que el ransomware representa uno de los riesgos de mayor impacto institucional identificado en el numeral 3 de los Estudios Previos, la Entidad requiere verificar de forma desagregada y objetiva que la plataforma ofertada cuenta con controles específicos frente a cada una de estas técnicas de compromiso, sin reducir la validación a una declaración genérica. La Entidad precisa que para la verificación técnica no se exige que la consola del fabricante utilice literalmente la misma traducción o etiqueta textual, sino que la documentación oficial del fabricante demuestre que sus políticas y motores de prevención cubren y bloquean de manera efectiva dichos comportamientos y técnicas de ataque. En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 61	**BIM LATINOAMERICA — Técnico**
Observación presentada	Parches en Linux y macOS, parches virtuales y detección de IoT Requisito: el EDR debe aplicar parches en Windows, Linux y macOS, ofrecer parches virtuales y detectar dispositivos IoT. Problema: los parches virtuales y la detección de IoT son funciones de seguridad de red, no del endpoint. El parcheo en Linux y macOS no es una función estándar de las soluciones EDR.
Solicitud de aclaración o ajuste	exigir el parcheo en Windows y dejar como opcional el parcheo en Linux y macOS. Eliminar los parches virtuales y la detección de IoT.
Decisión	No aceptada
Respuesta UAERMV	La UAERMV se permite informar que de acuerdo con lo descrito en la sección "Componentes de la Solución EDR" de los Estudios Previos y del formato GCON-FM-022, la infraestructura de la UAERMV que será protegida por la solución comprende sistemas operativos Windows 11, Windows Server (2019, 2022 y superior), macOS (Ventura 13 y superior) y distribuciones empresariales de Linux (Oracle Linux 8/9, Ubuntu Server LTS 24.04 y CentOS 8/9). Dejar como opcional la gestión de parches y vulnerabilidades en Linux y macOS desprotegería servidores críticos y estaciones de trabajo que hacen parte integral del alcance del contrato.

	Asimismo, dentro de las capacidades modernas de Higiene de TI y Reducción de la Superficie de Ataque en soluciones EDR de nueva generación, el descubrimiento de dispositivos no administrados o IoT desde la telemetría de los agentes desplegados en los segmentos de red, así como la mitigación proactiva de vulnerabilidades mediante parches virtuales (análisis y bloqueo granular de comunicaciones externas hacia aplicaciones o servicios con CVEs vulnerables antes de que se aplique el parche oficial), son controles esenciales para evitar la explotación de vulnerabilidades en equipos finales. En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 62	**BIM LATINOAMERICA — Técnico**
Observación presentada	Compatibilidad con macOS Ventura 13 Requisito: el agente debe ser compatible con macOS Ventura 13 o superior. Problema: macOS 13 ya no recibe actualizaciones de seguridad de Apple. Exigirlo obliga a proteger equipos sin soporte del fabricante del sistema operativo.
Solicitud de aclaración o ajuste	cambiar el requisito por: "Compatibilidad con las versiones de macOS que tengan soporte de seguridad vigente de Apple."
Decisión	No aceptada
Respuesta UAERMV	La UAERMV se permite informar que el requerimiento técnico exige compatibilidad con "MacOS: Ventura 13 y superior". Esta especificación responde al inventario real de activos de cómputo que actualmente se encuentran operativo en la UAERMV. Precisamente cuando existen estaciones de trabajo que operan sobre versiones base como macOS 13 por requerimientos de compatibilidad de software o hardware, resulta aún más crítica la cobertura mediante un agente EDR avanzado que proteja el sistema operativo frente a intentos de explotación. Además, la cláusula "y superior" incluye todas las versiones subsecuentes y actuales de macOS. En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 63	**BIM LATINOAMERICA — Técnico**
Observación presentada	Investigación impulsada por IA Requisito: la solución debe ofrecer investigación de incidentes impulsada por inteligencia artificial. Problema: las funciones de IA en las consolas de seguridad están en evolución y su disponibilidad varía según el modelo de despliegue y el licenciamiento de cada fabricante. Lo que la entidad necesita

	es investigar los incidentes de forma rápida y completa.
Solicitud de aclaración o ajuste	cambiar el requisito por: "La solución deberá facilitar la investigación de incidentes mediante correlación automática de eventos, visualización de la cadena de ataque y mapeo a la matriz MITRE ATT&CK. Las funciones de investigación con IA serán opcionales."
Decisión	No aceptada
Respuesta UAERMV	La UAERMV se permite informar que tanto en la justificación técnica de la necesidad como en el análisis del sector de los Estudios Previos y el formato GCON-FM-022, se establece que la adopción de capacidades de Inteligencia Artificial para la investigación, clasificación y contextualización de eventos es un requerimiento transversal e indispensable para reducir la fatiga de alertas, acelerar el análisis forense y permitir una administración eficiente con el recurso humano disponible en la Entidad (Madurez operativa de la entidad). Por consiguiente, no es viable establecer dichas especificaciones técnicas como "opcionales", pues ello afectaría las capacidades técnicas requeridas, la uniformidad técnica de las ofertas y la comparación objetiva de precios. En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 64	**BIM LATINOAMERICA — Técnico**
Observación presentada	Playbooks predefinidos y apertura de tickets Requisito: la solución debe incluir playbooks de respuesta predefinidos y abrir tickets. Problema: "playbook" es un término de cierto tipo de plataformas. Lo que la entidad necesita es que la respuesta ante incidentes sea rápida y esté documentada.
Solicitud de aclaración o ajuste	cambiar el requisito por: "La solución deberá ejecutar acciones de respuesta automáticas y configurables (aislar el equipo, terminar procesos, poner archivos en cuarentena) y registrar cada incidente para su seguimiento, en la consola o mediante el servicio MDR."
Decisión	No aceptada
Respuesta UAERMV	La UAERMV se permite informar que el término Playbook (flujo de trabajo secuencial y automatizado para estandarizar la respuesta ante incidentes) es un estándar técnico universal de la industria de la ciberseguridad y no una denominación exclusiva de una marca. La Entidad requiere que la plataforma EDR en sí misma posea la capacidad nativa de orquestar y automatizar mediante playbooks predefinidos las acciones de remediación detalladas en el Anexo Técnico: eliminación de archivos, finalización de procesos maliciosos, reversión automática de cambios persistentes, notificación a usuarios, aislamiento de aplicaciones/dispositivos y

	apertura de tickets. Esta capacidad funcional del software no puede ser sustituida ni delegada a una gestión manual o externa del servicio MDR, pues el objetivo técnico es garantizar una contención y remediación automática en tiempo real directamente desde la arquitectura desplegada. En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 65	**BIM LATINOAMERICA — Técnico**
Observación presentada	Instantáneas de memoria Requisito: la solución debe tomar instantáneas de memoria para investigar ataques sin archivos. Problema: la detección de ataques en memoria y sin archivos se puede cumplir sin capturar la memoria completa del equipo.
Solicitud de aclaración o ajuste	cambiar el requisito por: "La solución deberá detectar y bloquear ataques en memoria y sin archivos, y entregar la información necesaria para su investigación."
Decisión	No aceptada
Respuesta UAERMV	La UAERMV se permite informar que el requerimiento está ubicado dentro del bloque de "Funcionalidades de Investigación" del EDR y exige expresamente: "Debe conservar instantáneas de memoria, de los ataques sin archivo o file-less para la búsqueda de amenazas basada en memoria". A diferencia del malware tradicional que escribe archivos en el disco duro, los ataques fileless e inyecciones en memoria residen exclusivamente en la memoria volátil (RAM). Si la solución únicamente bloquea el proceso pero no captura ni conserva la instantánea de memoria asociada al evento malicioso, los analistas de seguridad e investigadores forenses pierden por completo la evidencia técnica necesaria para analizar el código inyectado, identificar los indicadores de compromiso y determinar el alcance del incidente. Por consiguiente, la funcionalidad es indispensable para las labores de análisis forense requeridas por la UAERMV. En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 66	**BIM LATINOAMERICA — Técnico**
Observación presentada	Cacería de amenazas por parte de la entidad Requisito: la entidad debe poder hacer cacería de amenazas desde la consola. Problema: el pliego ya exige un servicio MDR con analistas del fabricante. La cacería de amenazas es una de las tareas principales de ese servicio.

Solicitud de aclaración o ajuste	aceptar que la cacería de amenazas la realicen los analistas del servicio MDR del fabricante, con reporte a la entidad.
Decisión	No aceptada
Respuesta UAERMV	La UAERMV se permite informar que conforme con los Estudios Previos y al formato GCON-FM-022, la plataforma EDR debe proporcionar a los analistas de seguridad de la UAERMV una interfaz guiada que les permita "cazar marcando sus propios tiempos", contando con "Habilitación de la cacería de amenazas", "Registro y análisis continuos" e "Ingesta y búsqueda de IoC" directamente en la consola de administración. El servicio gestionado MDR del fabricante y las herramientas nativas de Threat Hunting en la consola son capacidades complementarias y no sustitutivas. La Entidad requiere autonomía operativa sobre la consola contratada para adelantar investigaciones internas, búsquedas de indicadores de compromiso y verificaciones forenses en cualquier momento, sin quedar limitada a recibir reportes pasivos de un servicio externo. En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 67	**BIM LATINOAMERICA — Técnico**
Observación presentada	Historial completo de eventos Requisito: la solución debe conservar el historial completo de eventos de los equipos. Problema: el pliego no define por cuánto tiempo se conservan los eventos ni para qué se usan. Sin ese dato, las ofertas no se pueden comparar.
Solicitud de aclaración o ajuste	precisar el tiempo de retención requerido y aceptar que los eventos se conserven y consulten a través del servicio MDR del fabricante (Kaspersky solo retiene 90 días).
Decisión	No aceptada
Respuesta UAERMV	La UAERMV se permite informar que el ítem "Debe proporcionar un análisis de todo el historial de eventos" incluido en las Funcionalidades de Detección y Protección hace referencia a la capacidad del motor analítico de la plataforma EDR para reconstruir, correlacionar y analizar la totalidad de la secuencia histórica de eventos vinculados a un incidente o cadena de ataque (kill chain) desde su origen ("paciente cero"), permitiendo visualizar la trazabilidad completa antes, durante y después del intento de compromiso. La Entidad aclara que la consulta y visualización de los eventos e incidentes debe estar disponible directamente en la consola en la nube (SaaS) para los administradores de la UAERMV (no siendo aceptable que solo sea consultable mediante solicitudes al equipo MDR). Asimismo, en cuanto a la retención histórica

	prolongada de registros (logs), es precisamente por ello que los Estudios Previos y el formato GCON-FM-022 exigen la integración obligatoria de las soluciones con el Correlacionador de Eventos (FortiSIEM) y el Analizador (FortiAnalyzer) de propiedad de la Entidad, garantizando tanto la visibilidad operativa inmediata en la consola SaaS del fabricante, el cual puede ser mínimo de 90 días o superior en nube, como la centralización y retención histórica en la arquitectura institucional de la UAERMV. En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 68	**BIM LATINOAMERICA — Técnico**
Observación presentada	12 - Shadow AI Requisito: La entidad solicita funcionalidades asociadas a identificación y control de herramientas de Inteligencia Artificial Generativa utilizadas por los usuarios. Posible observación:
Solicitud de aclaración o ajuste	a la Entidad aclarar si se aceptan soluciones que implementen el control y monitoreo de aplicaciones de Inteligencia Artificial Generativa mediante mecanismos equivalentes de descubrimiento, clasificación, monitoreo y control de aplicaciones web, garantizando el objetivo funcional requerido independientemente del nombre comercial utilizado por cada fabricante. ¿Por qué? Porque algunos fabricantes lo llaman: • Shadow AI • AI Governance • AI Discover • GenAI Control y otros lo implementan con diferente terminología.
Decisión	No aceptada
Respuesta UAERMV	La UAERMV se permite informar que las expresiones referidas en los Estudios Previos y en el formato GCON-FM-022, tales como detección y control de Shadow AI / GenAI, seguimiento del linaje de datos (Data Lineage) y repositorio o almacenamiento de evidencia forense (Evidence Store), no corresponden a marcas registradas ni a denominaciones exclusivas de un fabricante en particular, sino a conceptos técnicos y categorías funcionales estandarizadas en la industria global de ciberseguridad y protección de datos.

	Tanto los Estudios Previos como el formato GCON-FM-022 describen de manera explícita, funcional y tecnológicamente neutra qué debe hacer la solución frente a cada uno de estos conceptos, a saber: Frente a Shadow AI y GenAI: "Identificar el uso de Shadow AI y detener la carga de datos sensibles", "construir un inventario completo con puntuación de riesgo de las aplicaciones SaaS y herramientas GenAI utilizadas en toda la organización" y "monitorear la actividad en aplicaciones de inteligencia artificial (Por ejemplo, ChatGPT, Gemini, entre otros)". Frente a Linaje de Datos (Data Lineage): "Proporcionar seguimiento de datos desde su origen con visibilidad completa de la manipulación posterior de datos a lo largo del tiempo mediante las funciones de flujo de datos seguro y linaje de datos" e "identificar y rastrear datos automáticamente según su origen, como sistemas de recursos humanos o repositorios de código fuente, sin necesidad de incluir reglas iniciales para la detección". Frente a Almacenamiento de Evidencia Forense (Evidence Store): "Capturar forenses de archivos y pantallas", "almacenar los registros forenses en centros de datos controlados por el cliente en la región" y brindar soporte para el "análisis forense de archivos, portapapeles y captura de pantalla". Por consiguiente, la Entidad aclara que la verificación técnica recae sobre el cumplimiento estricto e integral de cada una de las capacidades funcionales descritas en el Anexo Técnico, con independencia del nombre comercial con el que cada fabricante denomine el módulo o menú dentro de su interfaz gráfica, siempre y cuando: (i) todas las capacidades estén cubiertas bajo una única licencia SaaS en la nube sin requerir servidores o colectores en tierra, (ii) operen mediante un agente ligero unificado, (iii) se integren de manera funcional y nativa con el ecosistema de ciberseguridad preexistente de la Entidad (FortiSIEM, FortiAnalyzer y Microsoft Office 365), y (iv) se soporten de manera fidedigna y verificable en la documentación técnica oficial del fabricante. En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 69	**BIM LATINOAMERICA — Técnico**
Observación presentada	13 - Data Lineage Requisito: Encontré que la expresión "Data Lineage" aparece como requisito muy específico. Posible observación:
Solicitud de aclaración o ajuste	a la Entidad permitir el cumplimiento mediante funcionalidades equivalentes de trazabilidad, seguimiento de información, monitoreo de movimientos y auditoría del

	ciclo de vida de los datos, independientemente de la denominación comercial utilizada por cada fabricante.
Decisión	No aceptada
Respuesta UAERMV	La UAERMV se permite informar que las expresiones referidas en los Estudios Previos y en el formato GCON-FM-022, tales como detección y control de Shadow AI / GenAI, seguimiento del linaje de datos (Data Lineage) y repositorio o almacenamiento de evidencia forense (Evidence Store), no corresponden a marcas registradas ni a denominaciones exclusivas de un fabricante en particular, sino a conceptos técnicos y categorías funcionales estandarizadas en la industria global de ciberseguridad y protección de datos. Tanto los Estudios Previos como el formato GCON-FM-022 describen de manera explícita, funcional y tecnológicamente neutra qué debe hacer la solución frente a cada uno de estos conceptos, a saber: Frente a Shadow AI y GenAI: "Identificar el uso de Shadow AI y detener la carga de datos sensibles", "construir un inventario completo con puntuación de riesgo de las aplicaciones SaaS y herramientas GenAI utilizadas en toda la organización" y "monitorear la actividad en aplicaciones de inteligencia artificial (Por ejemplo, ChatGPT, Gemini, entre otros)". Frente a Linaje de Datos (Data Lineage): "Proporcionar seguimiento de datos desde su origen con visibilidad completa de la manipulación posterior de datos a lo largo del tiempo mediante las funciones de flujo de datos seguro y linaje de datos" e "identificar y rastrear datos automáticamente según su origen, como sistemas de recursos humanos o repositorios de código fuente, sin necesidad de incluir reglas iniciales para la detección". Frente a Almacenamiento de Evidencia Forense (Evidence Store): "Capturar forenses de archivos y pantallas", "almacenar los registros forenses en centros de datos controlados por el cliente en la región" y brindar soporte para el "análisis forense de archivos, portapapeles y captura de pantalla". Por consiguiente, la Entidad aclara que la verificación técnica recae sobre el cumplimiento estricto e integral de cada una de las capacidades funcionales descritas en el Anexo Técnico, con independencia del nombre comercial con el que cada fabricante denomine el módulo o menú dentro de su interfaz gráfica, siempre y cuando: (i) todas las capacidades estén cubiertas bajo una única licencia SaaS en la nube sin requerir servidores o colectores en tierra, (ii) operen mediante un agente ligero unificado, (iii) se integren de manera funcional y nativa con el ecosistema de ciberseguridad preexistente de la Entidad (FortiSIEM, FortiAnalyzer y Microsoft Office 365), y (iv) se soporten de manera fidedigna y verificable en la documentación técnica oficial del fabricante. En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 70	**BIM LATINOAMERICA — Técnico**
Observación presentada	14 - Evidence Store Requisito: Este término tampoco es estándar en todas las plataformas DLP. Posible observación: Solicitamos aclarar si las capacidades de almacenamiento de evidencia, recopilación de eventos, auditoría y preservación de evidencias digitales podrán acreditarse mediante funcionalidades equivalentes ofrecidas por los distintos fabricantes. Observación 4 - Integraciones específicas Si detectan menciones muy orientadas a un fabricante particular.
Solicitud de aclaración o ajuste	Solicitar: que la Entidad acepte mecanismos de integración estándar basados en API, Syslog, conectores nativos o estándares de mercado, sin limitar el cumplimiento a una única arquitectura tecnológica
Decisión	No aceptada
Respuesta UAERMV	La UAERMV se permite informar que las expresiones referidas en los Estudios Previos y en el formato GCON-FM-022, tales como detección y control de Shadow AI / GenAI, seguimiento del linaje de datos (Data Lineage) y repositorio o almacenamiento de evidencia forense (Evidence Store), no corresponden a marcas registradas ni a denominaciones exclusivas de un fabricante en particular, sino a conceptos técnicos y categorías funcionales estandarizadas en la industria global de ciberseguridad y protección de datos. Tanto los Estudios Previos como el formato GCON-FM-022 describen de manera explícita, funcional y tecnológicamente neutra qué debe hacer la solución frente a cada uno de estos conceptos, a saber: Frente a Shadow AI y GenAI: "Identificar el uso de Shadow AI y detener la carga de datos sensibles", "construir un inventario completo con puntuación de riesgo de las aplicaciones SaaS y herramientas GenAI utilizadas en toda la organización" y "monitorear la actividad en aplicaciones de inteligencia artificial (Por ejemplo, ChatGPT, Gemini, entre otros)". Frente a Linaje de Datos (Data Lineage): "Proporcionar seguimiento de datos desde su origen con visibilidad completa de la manipulación posterior de datos a lo largo del tiempo mediante las funciones de flujo de datos seguro y linaje de datos" e "identificar y rastrear datos automáticamente según su origen, como sistemas de recursos humanos o repositorios de código fuente, sin necesidad de incluir reglas iniciales para la detección". Frente a Almacenamiento de Evidencia Forense (Evidence Store): "Capturar forenses de archivos y pantallas", "almacenar los registros forenses en centros de datos controlados por el cliente en la región" y brindar soporte para el "análisis forense de archivos, portapapeles y captura de pantalla".

	Por consiguiente, la Entidad aclara que la verificación técnica recae sobre el cumplimiento estricto e integral de cada una de las capacidades funcionales descritas en el Anexo Técnico, con independencia del nombre comercial con el que cada fabricante denomine el módulo o menú dentro de su interfaz gráfica, siempre y cuando: (i) todas las capacidades estén cubiertas bajo una única licencia SaaS en la nube sin requerir servidores o colectores en tierra, (ii) operen mediante un agente ligero unificado, (iii) se integren de manera funcional y nativa con el ecosistema de ciberseguridad preexistente de la Entidad (FortiSIEM, FortiAnalyzer y Microsoft Office 365), y (iv) se soporten de manera fidedigna y verificable en la documentación técnica oficial del fabricante. En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 71	**MSL — Contractual**
Observación presentada	1. Supresión del Registro Único de TIC como requisito habilitante: En el cuadro de verificación técnica del capítulo cuarto “requisitos habilitantes y factor de escogencia”, se exige el Registro TIC expedido por MinTIC. Este requisito no corresponde al objeto ni a las obligaciones descritos en el proyecto de pliego. El Registro Único de TIC habilita la provisión de redes o servicios de telecomunicaciones a los sujetos definidos en la ley y su reglamento. Su ámbito no comprende, de manera general, la comercialización, implementación y soporte de cualquier producto tecnológico.2 El proyecto contempla licenciamiento, instalación, configuración, puesta en marcha, soporte y capacitación sobre soluciones de ciberseguridad. No identifica una prestación de telecomunicaciones que deba habilitar al contratista como operador. Utilizar Internet o la nube para operar el software no convierte, por ese solo hecho, a su proveedor en prestador del servicio de telecomunicaciones, máxime cuando el futuro contratista será un canal comercial, ni siquiera el fabricante del software. MinTIC distingue a los proveedores de contenidos y aplicaciones que diseñan o distribuyen software y plataformas de los proveedores de redes y servicios de telecomunicaciones. Exigir este registro sin una prestación que lo justifique restringe la participación de empresas idóneas de ciberseguridad.3
Solicitud de aclaración o ajuste	Solicitamos muy amablemente a la entidad, eliminar el Registro Único de TIC del cuadro de requisitos habilitantes y de los documentos que lo reproduzcan, y precisar que su ausencia no genera calificación de no hábil ni rechazo. Adicionalmente, retirar también la exigencia genérica de licencias de acceso al espectro electromagnético, pues el proyecto no identifica una actividad que requiera ese permiso.
Decisión	Aceptada

Respuesta UAERMV	La UAERMV se permite informar que verificados los documentos del proceso, el registro único de TIC no es un requisito habilitante del presente proceso, en consecuencia, la modificación sobre este aspecto se verá reflejada en el pliego definitivo

Observación N.° 72	**MSL — Contractual**
Observación presentada	2. Supresión del registro y la habilitación técnica ante la Policía Nacional: El mismo cuadro exige un documento técnico de la Policía Nacional que acredite registro y habilitación conforme al artículo 12 del Decreto 723 de 2014 y a la Resolución 02086 del 30 de mayo de 2014. El régimen jurídico del proyecto también incorpora estas exigencias. Tales disposiciones regulan un servicio distinto del que se pretende contratar. El artículo 12 del Decreto 723 de 2014, compilado en el artículo 2.2.6.12 del Decreto 1070 de 2015, establece requisitos para proveedores del servicio de posicionamiento global vinculado al control de la maquinaria comprendida en ese régimen. Entre ellos figuran la transmisión de información de rastreo a la Policía Nacional, la integración con sus servidores y la conservación de reportes de trazabilidad de la maquinaria.4 La Resolución 02086 de 2014 desarrolla las condiciones técnicas de los dispositivos GPS, la autorización y el registro de sus proveedores y su instalación en la maquinaria regulada. Las referencias a dispositivos de seguridad y monitoreo electrónico deben leerse dentro de ese ámbito material; no equivalen a una autorización policial para suministrar software de ciberseguridad.5 El objeto descrito en el proyecto no comprende rastreo satelital de maquinaria, instalación de GPS ni integración de sus reportes con la Policía Nacional. La prevención de amenazas en equipos terminales y de fugas de información tiene una finalidad y una operación diferentes. La actividad misional de mantenimiento vial de la entidad no extiende este régimen a todos los bienes y servicios que adquiere. Las dos exigencias observadas deben respetar la adecuación y proporcionalidad de los requisitos habilitantes y la obligación de establecer condiciones objetivas necesarias para participar. Mantener registros propios de actividades ajenas al contrato limita injustificadamente la concurrencia de proveedores idóneos
Solicitud de aclaración o ajuste	Solicitamos muy amablemente a la entidad, eliminar el documento de registro y habilitación técnica ante la Policía Nacional del cuadro de verificación y retirar las remisiones al Decreto 723 de 2014 y a la Resolución 02086 de 2014 como exigencias para este contrato.

	Precisar expresamente que su no presentación no constituye incumplimiento habilitante ni causal de rechazo.
Decisión	Aceptada
Respuesta UAERMV	La UAERMV se permite informar que verificados los documentos del proceso, el registro y habilitación ante la policía nacional no es un requisito habilitante del presente proceso, en consecuencia, la modificación sobre este aspecto se verá reflejada en el pliego definitivo

Observación N.° 73	**MSL — Contractual**
Observación presentada	3. Improcedencia de limitar la convocatoria a Mipymes por superar el umbral: El numeral 1.3 aduce limitar la convocatoria a Mipymes utilizando un umbral de $533.287.768, sin embargo, ese valor corresponde al año 2025. Para 2026, Colombia Compra Eficiente publica expresamente el umbral de US$125.000 en $511.708.497. Este es el valor aplicable a la limitación a Mipymes, independientemente de los umbrales de cobertura de acuerdos comerciales que aparecen en el mismo documento.7 El presupuesto oficial es de $523.652.448, según el numeral 1.3 y el apartado de presupuesto oficial del proyecto. Por tanto, supera el umbral de 2026 en $11.943.951 y no satisface el requisito económico para una convocatoria limitada. Adicionalmente, el numeral se contradice al señalar que no se cumple el requisito económico, afirmar después que el valor es menor al umbral y concluir que la entidad podrá limitar la convocatoria. La corrección debe abarcar tanto la cifra como la consecuencia jurídica.
Solicitud de aclaración o ajuste	Solicitamos muy amablemente a la entidad, actualizar el umbral a $511.708.497 y modificar el numeral 1.3 para establecer que este proceso no será limitado a Mipymes, dado que su presupuesto oficial supera dicho valor. Ajustar en el mismo sentido los documentos y campos correspondientes de SECOP II.
Decisión	Aceptada
Respuesta UAERMV	La UAERMV se permite informar que verificados los documentos del proceso y teniendo en cuenta que el presupuesto para el presente proceso de contratación QUINIENTOS VEINTITRÉS MILLONES SEISCIENTOS CINCUENTA Y DOS MIL CUATROCIENTOS CUARENTA Y OCHO PESOS M/CTE ($523.652.448,00) supera el umbral establecido para limitación del proceso a las MIPYMES en USD 125.000 (V/r Umbral Mipyme en COP ($511.708.497), conforme el numeral primero del artículo 2.2.1.2.4.2.2. de la Subsección 2 de la Sección 4 del Capítulo 2 del Título 1 de la Parte 2 del Libro 2 del Decreto 1082 de 2015, modificado por el artículo 5 del Decreto 1860 de 2021, la UNIDAD ADMINISTRATIVA ESPECIAL DE REHABILITACIÓN Y MANTENIMIENTO VIAL – UAERMV determina que el presente

	proceso NO SE LIMITA A MIPYMES y queda abierto a todos los proponentes que deseen participar y que cumplan con los requisitos establecidos en el pliego de condiciones y demás documentos que conforman el proceso de selección. La modificación sobre este aspecto se verá reflejada en el pliego definitivo

Observación N.° 74	**INFORMACION LOCALIZADA SAS — Contractual**
Observación presentada	El numeral de obligaciones específicas del proyecto de pliego establece el cumplimiento de “las características técnicas mínimas definidas en el documento anexo GCON-FM-022” Sin embargo, en los documentos publicados el GCON-FM-022 corresponde a la formulación del estudio del sector, y no se identifica un anexo técnico independiente.
Solicitud de aclaración o ajuste	Solicitamos confirmar cuál es el documento que contiene las especificaciones técnicas mínimas vinculantes y publicarlo como anexo en SECOP II.
Decisión	No aceptada
Respuesta UAERMV	La UAERMV se permite informar que de conformidad con el numeral 6.2.1 CERTIFICACIÓN TÉCNICA DEL OFERENTE del estudio previo y 4.2.2 VERIFICACIÓN DE CUMPLIMIENTO DE LOS REQUERIMIENTOS Y ESPECIFICACIONES DEFINIDOS EN EL FORMATO GCON-FM-022 del pliego del proceso, el proponente deberá presentar con la oferta, el formato en donde señale que conoce y se compromete a cumplir en su totalidad las especificaciones, características, requisitos técnicos y condiciones de entregan definidos en el documento denominado la FORMULACIÓN DE ESTUDIOS DEL SECTOR GCON-FM-022, asumiendo las obligaciones que dicho compromiso acarrea. Se le aclara al observante que las especificaciones técnicas se encuentran contenidas en la FORMULACIÓN DE ESTUDIOS DEL SECTOR GCON-FM-022Gel cual se encuentra publicado en la plataforma SECOP II dentro de los documentos del proceso. Así mismo, se le aclara al observante que se encuentra publicado en la plataforma SECOP II dentro de los documentos del proceso el archivo 12. FORMATO ACEPTACIÓN ESPECIFICACIONES Y CARACTERÍSTICAS TÉCNICAS el cual deberá ser presentado por los proponentes en el que manifestaran que conocen y se comprometen a cumplir en su totalidad las especificaciones, características, requisitos técnicos y condiciones de entrega definidos en la FORMULACIÓN DE ESTUDIOS DEL SECTOR GCON-FM-022.

Observación N.° 75	**GRUPO INTALENT — Contractual**
Observación presentada	Envían carta para temas de Mipymes
Solicitud de aclaración o ajuste	Solicitud_Limitacion_Mipyme_Bogota_UMV-SASI-008-2026_INTALEN
Decisión	No aceptada
Respuesta UAERMV	Teniendo en cuenta que el presupuesto para el presente proceso de contratación es de **QUINIENTOS VEINTITRÉS MILLONES SEISCIENTOS CINCUENTA Y DOS MIL CUATROCIENTOS CUARENTA Y OCHO PESOS M/CTE ($523.652.448,00),** supera el umbral previsto en el artículo 2.2.1.2.4.2.2 del Decreto 1082 de 2015 para limitar la convocatoria a MIPYMES en USD 125.000 (V/r Umbral Mipyme en COP ($511.708.497), la **UAERMV** determina que el presente proceso **NO SE LIMITA A MIPYMES** y queda abierto a todos los proponentes que deseen participar y que cumplan con los requisitos establecidos en el pliego de condiciones y demás documentos que conforman el proceso de selección.

Observación N.° 76	**SUMIMAS — Técnico**
Observación presentada	Solicitud de modificación del requisito “Certificaciones de partner autorizado emitida por el fabricante. El Capítulo Cuarto, numeral 2, del proyecto de pliego y el numeral 7 del formato GCON-FM-022 exigen como requisito habilitante técnico una “carta emitida por el fabricante y dirigida a la entidad donde certifique que el proponente es Partner, canal o socio con el nivel más alto de membresía en la marca ofrecida en Colombia
Solicitud de aclaración o ajuste	De manera principal, solicitamos amablemente eliminar el requisito de acreditar “el nivel más alto de membresía en la marca ofrecida en Colombia”.
Decisión	No aceptada
Respuesta UAERMV	No acepta la solicitud de eliminar el requisito, con fundamento en las siguientes consideraciones frente a cada uno de los argumentos expuestos por el observante: • Neutralidad tecnológica y proporcionalidad frente a la complejidad técnica del contrato (Frente a los literales a y b): De conformidad con el artículo 2.2.1.1.1.6.2 del Decreto 1082 de 2015, los requisitos habilitantes deben ser adecuados y proporcionales no solo al valor del contrato, sino también a su naturaleza, complejidad, plazo y riesgos asociados. El requisito de acreditar el nivel más alto de membresía o Partnership otorgado por el fabricante en Colombia no está atado a una denominación textual específica de un programa de canales en particular, sino que exige el mayor nivel de reconocimiento oficial disponible dentro del esquema de certificación de cada fabricante, cualquiera

	sea la estructura o nomenclatura que este utilice. En esa medida, el requisito es tecnológicamente neutro y aplicable de manera uniforme a cualquier fabricante. Contrario a lo señalado por el observante, en la industria de ciberseguridad el máximo escalafón de un programa de canales no responde únicamente a metas comerciales de facturación, sino que certifica que el integrador cuenta con la mayor madurez técnica corporativa, estructura robusta de ingeniería de preventa y postventa, pluralidad de especialistas certificados en arquitecturas avanzadas, capacidad comprobada de despliegue en arquitecturas empresariales críticas y canales de escalamiento prioritario con la ingeniería del fabricante. Esta máxima capacidad de ingeniería es estrictamente necesaria para este proyecto, toda vez que el objeto contractual no se limita al suministro comercial de licencias aisladas, sino que exige que en un plazo estricto de ejecución de dos (2) meses el contratista implemente, configure, pruebe y ponga en operación las plataformas EDR y DLP garantizando su interoperabilidad e integración nativa, bidireccional y automatizada con la matriz del ecosistema de ciberseguridad preexistente en la Entidad (Next Generation Firewall en sitio y en nube pública, Control de Acceso a la Red, SandBox, Correlacionador de Eventos, Analizador y Microsoft Office 365), además de prestar el soporte técnico local durante doce (12) meses. Los canales de niveles diferentes al nivel más alto no acreditan necesariamente la capacidad técnica plena de implementación, soporte e integración avanzada que la UAERMV requiere para este proyecto, lo que introduciría un riesgo técnico critico e inaceptable de fallas en la interoperabilidad y operación institucional durante la ejecución contractual. • Carácter complementario y no sustitutivo frente a las demás exigencias del proceso (Frente al literal c): Los mecanismos citados por el observante cumplen funciones jurídicas y operativas distintas y complementarias que no sustituyen la idoneidad corporativa acreditada mediante el nivel de Partnership del proponente: Los perfiles del personal mínimo requerido (Ingenieros de implementación EDR y DLP) se presentan por el contratista adjudicatario para aprobación del supervisor al inicio del contrato (conforme a la Nota 1 del numeral 4 del formato GCON-FM-022), mientras que la certificación de Partner es un requisito habilitante del proponente verificable en la fase de evaluación de las ofertas. Adicionalmente, contar con el nivel más alto de membresía garantiza que el contratista dispone de respaldo organizacional y de un equipo de especialistas de relevo o apoyo en caso de ausencias o contingencias durante los doce (12) meses de soporte local. El soporte 7x24x365 de fábrica y el servicio de buenas prácticas del fabricante cubren la asistencia de tercer nivel y el aseguramiento de calidad del productor del software, pero no reemplazan las obligaciones directas de instalación, configuración, integración con la infraestructura existente y soporte local de primer y segundo nivel que recaen exclusivamente sobre el Contratista.

	La experiencia general en el RUP 299,08 SMMLV acredita la trayectoria histórica en contratos de ciberseguridad en general, mientras que la carta del fabricante acredita la vigencia, solvencia técnica actual y el máximo respaldo oficial sobre la tecnología específica que se oferta para la UAERMV • Garantía de pluralidad de oferentes y armonía con la Selección Abreviada por Subasta Inversa (Frente a los literales d y e): El hecho de que los bienes y servicios objeto de contratación posean características técnicas uniformes y estandarizadas (lo que habilita la modalidad de Selección Abreviada por Subasta Inversa donde el menor precio es el factor de selección entre los proponentes hábiles) no impide, sino que por el contrario exige, que la Entidad verifique previamente condiciones rigurosas de aptitud e idoneidad técnica en los requisitos habilitantes para asegurar que todos los participantes que concurran a la puja electrónica tengan la misma capacidad de ejecución. El Estudio del Sector adelantado por la Entidad conforme al artículo 2.2.1.1.1.6.1 del Decreto 1082 de 2015 verificó que en el mercado nacional existe pluralidad tanto de fabricantes como de proveedores autorizados en capacidad de acreditar el nivel más alto de su respectivo programa de canales. Aunado a lo anterior, la Nota 1 del numeral 6.2.2 de los Estudios Previos y del numeral 4.2.3 del Proyecto de Pliego de Condiciones promueve activamente la concurrencia y asociatividad al establecer que: "En caso de tratarse de un proponente plural (consorcio o unión temporal), el presente requisito podrá ser acreditado por cualquiera de sus integrantes, siempre que dicho integrante participe directamente en la ejecución del objeto contractual relacionado con la solución ofertada". En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 77	**OLIMPIA IT — Contractual**
Observación presentada	En el evento que alguna de las partes requiera dar por terminado el contrato en forma unilateral y anticipada a la fecha pactada para el vencimiento del plazo, será necesario que dicha parte de aviso a la otra por escrito con al menos QUINCE (15) días calendario de antelación a la fecha prevista para la terminación anticipada, sin que por ello se genere indemnización alguna a favor de ninguna de las partes.
Solicitud de aclaración o ajuste	Se solicita respetuosamente a la Entidad eliminar la cláusula de terminación anticipada unilateral con aviso de quince (15) días calendario o, en su defecto, precisar que no será aplicable una vez pagadas las licencias ante el fabricante de la solución. Tal como está redactada, permite terminar el contrato sin causa y “sin que por ello se genere indemnización alguna”, lo que no es compatible con la forma en que se ejecuta este objeto: el contratista debe pagar las licencias al fabricante antes de recibir el pago de la Entidad, de modo que, si la terminación ocurre en ese periodo,

	no se le reconocería pago alguno por un costo en el que ya incurrió, rompiendo el equilibrio económico del contrato.
Decisión	No aceptada
Respuesta UAERMV	La UAERMV se permite informar que no se acepta la observación en los términos solicitados por el observante. Sin embargo se le informa que dicha cláusula fue objeto de modificación la cual se verá reflejada con la publicación del pliego definitivo

Observación N.° 78	**OLIMPIA IT — Contractual**
Observación presentada	El plazo de ejecución del contrato será de DOS (2) MESES o hasta agotar presupuesto lo primero que ocurra, a partir de la fecha en que se suscriba el acta de inicio del contrato, previo cumplimiento de los requisitos de perfeccionamiento y ejecución establecidos en el artículo 41 de la Ley 80 de 1993.
Solicitud de aclaración o ajuste	Se solicita respetuosamente a la Entidad aclarar cómo operará el plazo de ejecución del contrato. El numeral 2.4 del pliego lo fija en dos (2) meses “o hasta agotar presupuesto lo primero que ocurra”, pero el objeto corresponde a cantidades fijas (450 licencias EDR, 450 licencias DLP y un servicio de implementación) y a un único pago contra la puesta en marcha, de modo que no es claro en qué escenario podría agotarse el presupuesto antes del vencimiento de los dos meses, ni cuál sería la consecuencia sobre las obligaciones pendientes en ese caso. En consecuencia, solicitamos aclarar el alcance de la expresión “o hasta agotar presupuesto” y, de no existir un supuesto en que resulte aplicable, eliminarla, de manera que el plazo de ejecución quede fijado en dos (2) meses contados a partir de la suscripción del acta de inicio
Decisión	Aceptada
Respuesta UAERMV	Se acepta la observación y la misma se verá reflejada en el numeral 2.4 del pliego definitivo

Observación N.° 79	**OLIMPIA IT — Contractual**
Observación presentada	Verificación técnica (requisito habilitante): "REGISTRO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES – REGISTRO TIC, EXPEDIDO POR EL MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES" y "DOCUMENTO TÉCNICO EXPEDIDO POR LA POLICÍA NACIONAL QUE ACREDITE REGISTRO Y HABILITACIÓN DE LAS CONDICIONES TÉCNICAS SEÑALADAS EN EL DECRETO 723 DEL 10 DE ABRIL DE 2014 ART.

	12. Y LA RESOLUCIÓN 02086 DEL 30 DE MAYO DE 2014 DE LA POLICÍA NACIONAL". Numeral 1.9: "El Contratista deberá cumplir con lo establecido por las normas en cuanto a Licencias para acceder al espectro electromagnético..."
Solicitud de aclaración o ajuste	Se solicita respetuosamente eliminar estos dos requisitos habilitantes y la referencia a licencias de espectro electromagnético, o, en su defecto, explicar su relación con el objeto y precisar el documento exigido, su contenido y su forma de acreditación.
Decisión	Aceptada
Respuesta UAERMV	La UAERMV se permite informar que verificados los documentos del proceso, no es un requisito habilitante del presente proceso, en consecuencia, la modificación sobre este aspecto se verá reflejada en el pliego definitivo

Observación N.° 80	**OLIMPIA IT — Contractual**
Observación presentada	Cumplimiento 20%; Calidad del servicio 20% (plazo, vigencia de la garantía de soporte técnico y seis meses más); Calidad y correcto funcionamiento de los bienes 20% (plazo, vigencia de la garantía del producto y seis meses más).
Solicitud de aclaración o ajuste	Se solicita respetuosamente a la Entidad revisar la estructura de la garantía única de cumplimiento prevista en el numeral 2.10 del pliego, y exigir únicamente el amparo de cumplimiento sobre la calidad del servicio y calidad y correcto funcionamiento de los bienes. El objeto del contrato no comprende bienes muebles: corresponde a la suscripción de licencias de software en la nube del fabricante y a un servicio puntual de implementación. Además, el amparo de cumplimiento, según la justificación del propio pliego, ya cubre a la Entidad de los perjuicios derivados del “incumplimiento total o parcial de las obligaciones nacidas del contrato, así como su cumplimiento tardío o defectuoso”, lo que incluye la calidad de la implementación y el correcto funcionamiento de las soluciones suministradas, que a su vez cuentan con el soporte directo del fabricante durante la vigencia de la suscripción. Por lo anterior, se solicita eliminar dichos amparos y mantener únicamente el amparo de cumplimiento en los términos previstos en el pliego
Decisión	Aceptada Parcialmente
Respuesta UAERMV	Verificados los amparos establecidos en los diferentes documentos del proceso se le informa al observante que la entidad mantendrá los amparos de cumplimiento y calidad del servicio y pago de salarios, prestaciones sociales, legales e indemnizaciones laborales bajo las justificaciones establecidas en los documentos del proceso.

	Ahora frente al amparo de calidad y correcto funcionamiento de los bienes se acepta la observación y el mismo será eliminado de los documentos del proceso como se vera reflejado en la publicación del pliego definitivo, bajo el entendido que para el proceso no se suministrarán bienes.

Observación N.° 81	**OLIMPIA IT — Contractual**
Observación presentada	Variaciones en TRM encarecen servicios o productos a adquirir
Solicitud de aclaración o ajuste	Se solicita que este riesgo sea compartido entre la UAERMV y el contratista. Se trata de una variable que ninguna de las partes controla, y el contratista queda expuesto desde el cierre hasta el pago de las suscripciones al fabricante, periodo que puede extenderse con la validez de la oferta y con modificaciones del cronograma. Por ello, se solicita incorporar en el pliego un mecanismo de reajuste del valor de los ítems cuando se presenten variaciones extraordinarias de la TRM entre la fecha de cierre y la fecha de activación de las licencias, previa acreditación con la factura del fabricante o mayorista, en desarrollo de la cláusula de riesgo cambiario mencionada en el tratamiento de la matriz
Decisión	No aceptada
Respuesta UAERMV	La UAERMV no acepta la observación presentada. El riesgo asociado a las variaciones de la Tasa Representativa del Mercado (TRM) constituye, por regla general, un riesgo previsible del negocio que debe ser gestionado por quien estructura y presenta su oferta económica. En consecuencia, no procede trasladar a la Entidad los efectos derivados de fluctuaciones cambiarias ordinarias que hacen parte de las condiciones normales del mercado. El Consejo de Estado ha sostenido que, para que proceda el restablecimiento del equilibrio económico por circunstancias sobrevinientes, no basta la simple ocurrencia de una variación económica durante la ejecución contractual. Se requiere acreditar que el hecho sea extraordinario, imprevisible, ajeno a las partes y que produzca una afectación grave, anormal y sustancial de la ecuación financiera del contrato. Particularmente, en sentencia de 17 de octubre de 2023, Expediente 63001-23-33-000-2017-00359-01 (61441), la Sección Tercera del Consejo de Estado, Subsección A, al analizar una reclamación basada en el incremento de la TRM, concluyó que el riesgo cambiario correspondía a un riesgo previsible cuya gestión estaba a cargo del contratista, razón por la cual negó la compensación económica solicitada. En esa providencia se indicó que las fluctuaciones de la tasa de cambio son circunstancias propias del mercado, previsibles para los agentes económicos, y que el contratista debe adoptar las medidas necesarias para administrarlas al momento de estructurar su oferta.

	En ese sentido, la solicitud de incorporar un mecanismo de reajuste automático de precios asociado a variaciones de la TRM desconoce el principio de asignación eficiente de riesgos y trasladaría a la Entidad consecuencias derivadas de una variable de mercado inherente a la actividad empresarial del contratista. Por lo anterior, la Entidad mantiene la asignación del riesgo establecida en la matriz de riesgos y no acoge la modificación propuesta.

Observación N.° 82	**OLIMPIA IT — Contractual**
Observación presentada	Retrasos en la entrega, instalación y puesta en marcha de los servicios a adquirir
Solicitud de aclaración o ajuste	Se solicita respetuosamente precisar que el contratista asume este riesgo únicamente cuando los retrasos le sean imputables, y que se excluyan los retrasos originados en hechos de la UAERMV o en hechos de terceros ajenos al contratista. Esto se debe a que la consecuencia descrita en la matriz incluye “sanciones” y la implementación depende en parte de actuaciones que el contratista no controla.
Decisión	No Aceptada
Respuesta UAERMV	No se acepta la observación. El riesgo N.° 3 se asignó al contratista porque la entrega, instalación y puesta en marcha son obligaciones de resultado cuyo cumplimiento depende de su logística, su cadena de suministro con el fabricante y los distribuidores, su equipo técnico y la planeación de su cronograma. Son factores que controla y que debe dimensionar al presentar su oferta, conforme al principio de asignación a quien mejor puede gestionar el riesgo, al art. 4 de la Ley 1150 de 2007 y al CONPES 3714 de 2011. La matriz asigna la gestión del riesgo, no determina responsabilidad ni impone sanciones. La referencia a “sanciones” describe una posible consecuencia del evento, no una sanción automática. Las multas y declaratorias de incumplimiento solo proceden mediante el procedimiento del art. 86 de la Ley 1474 de 2011, que garantiza el debido proceso y la defensa del contratista, en armonía con el art. 17 de la Ley 1150 de 2007. En ese trámite el contratista puede demostrar que el retraso obedeció a causas que no le son imputables. Por eso las exclusiones solicitadas son innecesarias. Los retrasos originados en hechos de la UAERMV, o en fuerza mayor o caso fortuito, no generan responsabilidad del contratista (art. 27 de la Ley 80 de 1993 y art. 64 del Código Civil), y el cronograma se ajusta según lo previsto en el contrato [prórroga o suspensión, según la cláusula]. No es procedente excluir de forma general los “hechos de terceros”, porque cobijaría a fabricantes, distribuidores, transportadores y subcontratistas que hacen parte de la cadena de suministro del propio contratista, frente a la Entidad. Además, el tratamiento del riesgo prevé informes de avance quincenales, que le permiten

	reportar y soportar oportunamente cualquier causa ajena. Se mantiene la redacción del riesgo.

Observación N.° 83	**OLIMPIA IT — Técnico**
Observación presentada	Vulnerabilidades no detectadas o fallas en configuración de seguridad.
Solicitud de aclaración o ajuste	Se solicita amablemente asignar este riesgo a la Entidad. La obligación del contratista se limita a gestionar ante el fabricante, mediante el soporte incluido en la suscripción, la atención de los defectos de funcionamiento de las licencias suministradas. Asimismo, se solicita eliminar del tratamiento de este riesgo las pruebas de penetración y auditorías, o precisar que corresponden a la Entidad, por cuanto no hacen parte del alcance del contrato, que se limita a la suscripción de las licencias, su implementación y soporte.”
Decisión	No aceptada
Respuesta UAERMV	La Entidad informa que resulta improcedente trasladar el riesgo a la misma, contrario a lo afirmado por el observante, la responsabilidad del Contratista no se limita a suministrar licencias y tramitar defectos ante el fabricante. El objeto y alcance del contrato comprenden la implementación, configuración, pruebas, puesta en marcha, estabilización y soporte de las soluciones EDR y DLP. Conforme al numeral 4 del formato GCON-FM-022, los ingenieros de implementación del contratista son responsables directos de la configuración de las funcionalidades de protección de endpoints y de datos "garantizando su correcto funcionamiento y alineación con las políticas de la Entidad", a lo que se suma el servicio de buenas prácticas directo del fabricante (análisis inicial, revisión de políticas, ajuste de la solución y seguimiento) y las funcionalidades obligatorias de evaluación y descubrimiento de vulnerabilidades y parches virtuales del EDR. Por ende, el riesgo de fallas en la configuración de seguridad o vulnerabilidades no detectadas por una parametrización deficiente de la solución implementada recae sobre el Contratista. La Entidad aclara a los interesados que las auditorías y pruebas referidas en el tratamiento del riesgo corresponden a las pruebas de efectividad, validación de políticas de detección/prevención/respuesta, evaluación de vulnerabilidades en los endpoints cubiertos y revisión de buenas prácticas del fabricante sobre las plataformas EDR y DLP objeto del contrato (páginas 9, 15, 28 y 30 del formato GCON-FM-022), sin que ello implique la obligación para el contratista de contratar o ejecutar servicios externos de Ethical Hacking o Pentesting general sobre otros sistemas de la UAERMV ajenos al alcance contractual. En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 84	**OLIMPIA IT — Técnico**
Observación presentada	Indisponibilidad o degradación del servicio SaaS del fabricante, dado que la solución opera en su totalidad en la nube del proveedor, sin componente local de respaldo.
Solicitud de aclaración o ajuste	Se solicita amablemente ajustar la redacción de este riesgo, por cuanto la disponibilidad de la infraestructura en la nube depende exclusivamente del fabricante y no es un evento que el contratista pueda controlar o mitigar. Lo que sí está bajo control del contratista es la gestión oportuna del caso ante el soporte de fábrica, por lo que se propone que el riesgo asignado al contratista quede así: Descripción: “Falta de gestión oportuna del contratista en el reporte, escalamiento y seguimiento ante el soporte del fabricante de los eventos de indisponibilidad o degradación del servicio SaaS".
Decisión	No aceptada
Respuesta UAERMV	Respecto a la responsabilidad por la disponibilidad de la solución SaaS (Parte 1): No se acoge la modificación. Conforme al numeral 4.10 de los Estudios Previos ("La UAERMV solo adquiere obligaciones con el Contratista"), al marco normativo del formato GCON-FM-022 (página 25, artículo 60 de la Ley 1480 de 2011 sobre responsabilidad solidaria de productor y proveedor respecto de la idoneidad, seguridad y calidad de los bienes y servicios ofrecidos) y a los requisitos de ejecución de la página 30 del formato GCON-FM-022 (que obligan al contratista a garantizar el "suministro de licencias activas", el "funcionamiento continuo de las plataformas" y la "disponibilidad del servicio"), el Contratista responde directamente ante la Entidad por la disponibilidad continua de la plataforma SaaS ofertada y porque sus agentes operen en modo autónomo fuera de línea en caso de desconexión. Limitar el riesgo a una simple gestión de radicación de tickets eximiría de responsabilidades exigidas en las obligaciones y los acuerdos de nivel de servicio del contrato. Respecto al plazo estimado del tratamiento del riesgo (Parte 2): Se aclara a los interesados que la cobertura activa de las suscripciones en la nube (SaaS) y del servicio de soporte técnico 7x24x365 con el fabricante y soporte local del Contratista) es de doce (12) meses contados a partir de la suscripción del acta de inicio. La expresión "Fin de garantías" en la Matriz de Riesgos se refiere a los doce (12) meses de vigencia de la garantía técnica y soporte de fábrica del producto exigida en la obligación específica No. 7 ("certificación emitida por el fabricante, por un 1 año"). Los seis (6) meses adicionales contemplados en los amparos de Calidad del Servicio y Calidad de los Bienes de la póliza de seguro corresponden al término legal poscontractual con que cuenta la Entidad para tramitar la liquidación del contrato o reclamar siniestros acaecidos dentro de la vigencia anual del servicio, sin que ello obligue al contratista a suministrar licenciamiento gratuito más allá de los doce (12) meses contratados. En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente

Observación N.° 85	**OLIMPIA IT — Técnico**
Observación presentada	Indisponibilidad o degradación del servicio SaaS del fabricante, dado que la solución opera en su totalidad en la nube del proveedor, sin componente local de respaldo.
Solicitud de aclaración o ajuste	Se solicita modificar el plazo estimado del tratamiento de este riesgo, que actualmente va desde la “Puesta en operación” hasta el “Fin de garantías”. El evento cubierto es la indisponibilidad de un servicio SaaS que solo existe mientras la suscripción esté vigente, es decir, durante doce (12) meses contados desde el acta de inicio, según la nota aclaratoria del numeral 4.3 de los estudios previos. Las garantías del contrato, en cambio, se extienden más allá de ese término (vigencia de la garantía de soporte y seis meses más), de modo que el plazo actual obligaría al contratista a gestionar la disponibilidad de un servicio cuya suscripción ya terminó.
Decisión	No aceptada
Respuesta UAERMV	Respecto a la responsabilidad por la disponibilidad de la solución SaaS (Parte 1): No se acoge la modificación. Conforme al numeral 4.10 de los Estudios Previos ("La UAERMV solo adquiere obligaciones con el Contratista"), al marco normativo del formato GCON-FM-022 (página 25, artículo 60 de la Ley 1480 de 2011 sobre responsabilidad solidaria de productor y proveedor respecto de la idoneidad, seguridad y calidad de los bienes y servicios ofrecidos) y a los requisitos de ejecución de la página 30 del formato GCON-FM-022 (que obligan al contratista a garantizar el "suministro de licencias activas", el "funcionamiento continuo de las plataformas" y la "disponibilidad del servicio"), el Contratista responde directamente ante la Entidad por la disponibilidad continua de la plataforma SaaS ofertada y porque sus agentes operen en modo autónomo fuera de línea en caso de desconexión. Limitar el riesgo a una simple gestión de radicación de tickets eximiría de responsabilidades exigidas en las obligaciones y los acuerdos de nivel de servicio del contrato. Respecto al plazo estimado del tratamiento del riesgo (Parte 2): Se aclara a los interesados que la cobertura activa de las suscripciones en la nube (SaaS) y del servicio de soporte técnico 7x24x365 con el fabricante y soporte local del Contratista) es de doce (12) meses contados a partir de la suscripción del acta de inicio. La expresión "Fin de garantías" en la Matriz de Riesgos se refiere a los doce (12) meses de vigencia de la garantía técnica y soporte de fábrica del producto exigida en la obligación específica No. 7 ("certificación emitida por el fabricante, por un 1 año"). Los seis (6) meses adicionales contemplados en los amparos de Calidad del Servicio y Calidad de los Bienes de la póliza de seguro corresponden al término legal poscontractual con que cuenta la Entidad para tramitar la liquidación del contrato o reclamar siniestros acaecidos dentro de la vigencia anual del servicio, sin que ello obligue al contratista a suministrar licenciamiento gratuito más allá de los doce (12) meses contratados. En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente

Observación N.° 86	**OLIMPIA IT — Técnico**
Observación presentada	Fallas o demoras en la integración de las soluciones EDR y DLP con el Directorio Activo, Microsoft 365/Purview y demás plataformas del ecosistema de ciberseguridad de la UAERMV.
Solicitud de aclaración o ajuste	Se solicita amablemente precisar que el contratista asume este riesgo únicamente cuando las fallas o demoras le sean imputables. Se propone la siguiente redacción: “Fallas o demoras imputables al contratista en la integración de las soluciones EDR y DLP con el Directorio Activo, Microsoft 365/Purview y demás plataformas del ecosistema de ciberseguridad de la UAERMV.
Decisión	No aceptada
Respuesta UAERMV	La UAERMV se permite informar que no se acepta la observación. El riesgo N.° 8 se asignó al contratista siguiendo el principio del Manual de Colombia Compra Eficiente que adopta la propia matriz, según el cual el riesgo lo asume quien mejor puede controlarlo por su experiencia, conocimiento o papel en la ecuación contractual. Esa asignación cumple con la obligación de estimar, tipificar y asignar los riesgos previsibles (art. 4 de la Ley 1150 de 2007) y con el CONPES 3714 de 2011. La integración de las soluciones EDR y DLP con el Directorio Activo, Microsoft 365/Purview y las demás plataformas depende de la arquitectura, los conectores, la parametrización y la metodología de implementación que defina el contratista, variables bajo su control técnico. La matriz distingue este riesgo del N.° 1, que la UAERMV asume en la etapa de selección, es decir, la compatibilidad de la solución con la infraestructura actual, gestionada con validación de especificaciones y evaluación técnica. Al contratista le corresponde la ejecución de la integración. Además, el tratamiento ya prevé pruebas de integración documentadas y una mesa técnica conjunta con la OTI antes de la puesta en operación. La expresión “imputables al contratista” tampoco procede. Conforme al instructivo de la matriz, la asignación indica quién asume la gestión del riesgo, no quién tiene la culpa. Condicionarla a la imputabilidad obligaría a discutir el origen de cada falla y trasladaría a la Entidad los sobrecostos y demoras que no se logren atribuir. Es además innecesaria, porque el contratista no responde por hechos que no le son imputables. El art. 27 de la Ley 80 de 1993 protege el equilibrio cuando se rompe por causas no imputables a quien resulte afectado, y la fuerza mayor y el caso fortuito se rigen por el art. 64 del Código Civil. Se mantiene la redacción del riesgo.

Observación N.° 87	**OLIMPIA IT — Técnico**
Observación presentada	Materialización de un incidente de seguridad (p. ej. ransomware o fuga de información) durante el periodo de transición, mientras la nueva plataforma EDR/DLP aún no se encuentra en operación plena.

Solicitud de aclaración o ajuste	Se solicita amablemente asignar este riesgo a la UAERMV. La obligación del contratista consiste en suministrar las licencias de las soluciones EDR y DLP por el periodo de la suscripción y realizar su implementación, y no en asumir la seguridad de la infraestructura de la Entidad mientras dicha implementación se completa. Durante la transición, la protección de los equipos depende de las herramientas de seguridad actuales de la UAERMV, cuya operación, según el tratamiento previsto en la propia matriz, corresponde mantener a la Entidad.
Decisión	No aceptada
Respuesta UAERMV	La Entidad informa que durante la fase de implementación y transición (dos meses), el Contratista ejecuta el despliegue de los agentes EDR y DLP, la configuración de políticas de prevención y bloqueo y la articulación con el ecosistema de ciberseguridad de la UAERMV sobre los 450 endpoints y Microsoft 365. Una inadecuada planeación del despliegue, la desinstalación o desactivación de controles preexistentes en un lote de equipos sin haber activado simultáneamente las políticas de protección pre y post-ejecución del nuevo agente, o la demora en activar la visibilidad inicial desde el primer día pueden generar ventanas de vulnerabilidad directamente asociadas a la ejecución del contratista. Por tal motivo, el formato GCON-FM-022 (páginas 29 y 30, Requisitos Técnicos Generales por Etapa – Antes de la entrega del bien, obra o servicio) impone al contratista la obligación de entregar y acordar con la supervisión el plan de implementación, el plan de despliegue, la estrategia de instalación de agentes, el procedimiento de reversa (rollback) y la matriz de riesgos de implementación. Se aclara que mientras la UAERMV mantiene activos sus controles de seguridad perimetral y base existentes durante la transición, el Contratista es responsable de ejecutar la migración y el despliegue controlado por fases sin dejar endpoints desprotegidos y activando la visibilidad y protección desde el primer día conforme a los requerimientos técnicos del proceso. En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 88	**OLIMPIA IT — Técnico**
Observación presentada	“El proponente debe adjuntar junto con su propuesta carta emitida por el fabricante […] donde certifique que el proponente es Partner, canal o socio con el nivel más alto de membresía en la marca ofrecida en Colombia”.
Solicitud de aclaración o ajuste	Se solicita eliminar la exigencia de acreditar “el nivel más alto de membresía”, pues no se evidencia justificación técnica de que sea indispensable para suministrar, implementar y soportar la solución. Esta condición restringe la libre concurrencia y puede reducir injustificadamente la pluralidad de oferentes. Se solicita admitir distribuidores, resellers, partners o canales autorizados, acreditados mediante carta

	vigente del fabricante o mayorista autorizado. Si se mantiene el nivel máximo, se solicita publicar el análisis técnico y de mercado que sustente su necesidad, proporcionalidad y relación directa con el objeto contractual.
Decisión	No aceptada
Respuesta UAERMV	La Entidad informa que el requisito de acreditar el nivel más alto de membresía o Partnership otorgado por el fabricante en Colombia no está atado a una denominación textual específica de un programa de canales en particular, sino que exige el mayor nivel de reconocimiento oficial disponible dentro del esquema de certificación de cada fabricante, cualquiera sea la estructura o nomenclatura que este utilice. En esa medida, el requisito es tecnológicamente neutro y aplicable de manera uniforme a cualquier marca. De conformidad con el numeral 6.2.2 de los Estudios Previos, el numeral 7 del formato GCON-FM-022 y el numeral 4.2.3 del Proyecto de Pliego de Condiciones, la certificación debe ser emitida directamente por el fabricante y dirigida a la Entidad, sin que sea admisible sustituirla por cartas de distribuidores o mayoristas intermediarios, toda vez que la UAERMV requiere garantizar el vínculo oficial directo con el productor de la tecnología, la activación de las suscripciones en su nube (SaaS) y la prestación directa de los servicios de fábrica exigidos (soporte 7x24x365 servicio MDR y servicio de buenas prácticas). Las razones técnicas y de mercado que fundamentan la necesidad y proporcionalidad de este requisito se encuentran debidamente documentadas y publicadas en el numeral 3 de los Estudios Previos (ESTUDIOS PREVIOS.pdf) y en el documento Formulación de Estudios del Sector (FORMULACIÓN DE ESTUDIOS DEL SECTOR FM-022.pdf). Como allí se expone, el proyecto no consiste en un simple suministro comercial de licencias aisladas (reselling), sino que exige que en un plazo estricto de dos (2) meses el contratista ejecute la implementación, configuración, puesta en marcha y las complejas integraciones de interoperabilidad nativa, bidireccional y automatizada entre las nuevas soluciones EDR/DLP y la matriz del ecosistema de ciberseguridad existente en la Entidad (Next Generation Firewall en sitio y en nube pública, Control de Acceso a la Red, SandBox, Correlacionador de Eventos, Analizador y Microsoft Office 365). Los canales de niveles diferentes al nivel más alto no acreditan necesariamente la capacidad técnica plena de implementación, soporte e integración avanzada que la UAERMV requiere para este proyecto, lo que introduciría un riesgo técnico critico e inaceptable de fallas en la interoperabilidad y operación institucional durante la ejecución contractual. El Estudio del Sector adelantado por la Entidad verificó la existencia de pluralidad de fabricantes y de proveedores en el mercado nacional que ostentan el máximo nivel dentro de sus respectivos programas de canales. Además, la Nota 1 del numeral 4.2.3 del Pliego de Condiciones permite que en el caso de proponentes plurales (consorcios o uniones temporales) el requisito sea acreditado por el integrante que participe directamente en la ejecución técnica de la solución ofertada. En

	consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 89	**OLIMPIA IT — Contractual**
Observación presentada	"Experiencia cuyo objeto o alcance se encuentre relacionado con la suscripción, implementación y soporte de soluciones o plataformas de ciberseguridad". Se verifican hasta tres (3) contratos para no Mipymes y hasta cinco (5) para los grupos diferenciales indicados.
Solicitud de aclaración o ajuste	Se solicita aclarar si la conjunción "y" exige que cada contrato incluya simultáneamente suscripción, implementación y soporte, o si se aceptarán contratos con uno o varios componentes. Para evitar una interpretación restrictiva, se solicita confirmar que será válida la experiencia en suscripción o licenciamiento, implementación y/o soporte de soluciones o plataformas de ciberseguridad, acreditable mediante uno o varios contratos dentro del máximo permitido, siempre que la sumatoria cumpla el valor mínimo. Se solicita además confirmar que no se exigirá una marca específica ni exclusivamente soluciones EDR y DLP.
Decisión	No aceptada
Respuesta UAERMV	En respuesta a la observación, se le aclara al observante que la entidad mantendrá las exigencias frente a la experiencia y la necesidad de implementar, instalar y soportar la solución adquirida, sin embargo, para mayor claridad se ajusto la redacción frente a exigencia de la experiencia en los siguientes términos "*Objeto o alcance se encuentre relacionado con la suscripción, implementación y soporte de soluciones de plataformas de ciberseguridad (Endpoint Detection and Response y/o Data Loss Prevention)* *Nota 1: Para efectos de la verificación de la experiencia habilitante, la UAERMV considerará válidos los contratos aportados por el proponente que, de manera individual o conjunta, permitan acreditar las actividades relacionadas con (Endpoint Detection and Response y/o Data Loss Prevention),* *Nota 2: No será obligatorio que las dos plataformas se encuentren acreditadas dentro de un mismo contrato. En consecuencia, el proponente podrá demostrar la experiencia requerida mediante la combinación de los contratos presentados, siempre que, en su conjunto, permitan verificar el cumplimiento de las actividades exigidas, respetando el número máximo de contratos establecido y las demás condiciones de experiencia habilitante previstas en el presente proceso."*

Observación N.° 90	**OLIMPIA IT — Contractual**
Observación presentada	El cronograma se remite a SECOP II. El pliego regula el evento, su duración de treinta (30) minutos y el margen mínimo del dos por ciento (2 %), pero no establece un simulacro previo.
Solicitud de aclaración o ajuste	Se solicita informar si se realizará un simulacro de la subasta inversa electrónica. En caso afirmativo, se solicita incorporar en el cronograma de SECOP II su fecha, hora, duración, mecanismo de acceso y canal de soporte. Si no está previsto, se solicita incluirlo con antelación suficiente al evento de puja, dado que el pliego atribuye al oferente la responsabilidad de conectarse y conocer la herramienta. El simulacro permite validar usuarios, conectividad y registro de lances, reduce riesgos operativos y garantiza igualdad de condiciones.
Decisión	No aceptada
Respuesta UAERMV	En respuesta a la observación se informa que en la subasta solo podrán participar aquellos proponentes que luego de la evaluación y verificación de requisitos, hayan resultado habilitados. Igualmente, los proponentes habilitados para participar en la subasta deben tener conexión a internet estable. Finalmente, no se contará con subasta de prueba para el presente proceso.

Observación N.° 91	**OLIMPIA IT — Técnico**
Observación presentada	El plazo de ejecución es de dos (2) meses o hasta agotar presupuesto. Dentro de los cinco (5) días hábiles siguientes al acta de inicio, las partes elaborarán el cronograma de trabajo, pero no se fija un plazo máximo específico de implementación.
Solicitud de aclaración o ajuste	Se solicita precisar el plazo máximo para implementar y poner en operación las soluciones, diferenciándolo del plazo total de ejecución y de la vigencia de las suscripciones. Deben definirse hito inicial, etapas, entregables y tiempos para activación, despliegue, configuración, integraciones, pruebas, estabilización y recibo, así como las dependencias a cargo de la UAERMV. No resulta suficiente diferir esta definición al cronograma posterior al acta de inicio, pues el oferente necesita dimensionar recursos, costos y riesgos. Se solicita confirmar que las demoras atribuibles a accesos, información, infraestructura o aprobaciones de la Entidad no constituirán incumplimiento del contratista.
Decisión	No aceptada
Respuesta UAERMV	La Entidad informa que el plazo de ejecución del contrato y plazo máximo de implementación es de DOS (2) MESES, contados a partir de la suscripción del acta de

	inicio previo cumplimiento de los requisitos de perfeccionamiento y ejecución. Tal como lo indica textualmente la página 21 del formato GCON-FM-022: "El plazo para la instalación, configuración, pruebas, puesta en marcha de las soluciones de EDR y DLP será de dos (2) meses". El término de cobertura de las suscripciones y del soporte técnico es de DOCE (12) MESES, contados a partir de la firma del acta de inicio, bajo esquema de soporte 7x24x365 con el fabricante y soporte local por parte del Contratista. Para la definición de etapas, actividades, entregables y criterios de aceptación, dichos elementos ya se encuentran estructurados de manera detallada en las páginas 26 a 31 del documento FORMULACIÓN DE ESTUDIOS DEL SECTOR FM-022.pdf (GCON-FM-022) bajo los acápites "Entregables mínimos del contratista", "Criterio de aceptación" y "Requisitos técnicos generales por etapa" (Durante la presentación de las propuestas, Antes de la entrega del bien, obra o servicio, Durante la ejecución del contrato y Después de la entrega del bien, obra o servicio). El cronograma que se acuerda dentro de los cinco (5) días hábiles siguientes al acta de inicio (obligación específica No. 13) tiene como finalidad programar las fechas exactas de las ventanas operativas de despliegue sobre esos entregables previamente definidos, dentro del plazo de dos (2) meses. En consecuencia, la Entidad no acepta la observación y se mantiene en lo requerido inicialmente.

Observación N.° 92	**OLIMPIA IT — Técnico**
Observación presentada	El formato exige que el representante legal se comprometa a cumplir el GCON-FM-022. En los documentos revisados no se identifica una definición expresa de perfiles técnicos mínimos ni el momento para acreditarlos.
Solicitud de aclaración o ajuste	Se solicita aclarar si la oferta debe incluir hojas de vida, certificaciones o documentos de un perfil o equipo técnico, o si dicho personal solo será presentado por el adjudicatario antes del acta de inicio. Si no es requisito habilitante, se solicita indicarlo expresamente y confirmar que la ausencia de documentos de personal en la oferta no será causal de rechazo. Si se exige, deberán precisarse cantidad de perfiles, formación, experiencia, certificaciones, dedicación, documentos, momento de presentación y reglas de sustitución por personal de igual o superior calificación, con exigencias proporcionales al alcance de la implementación.
Decisión	No aceptada
Respuesta UAERMV	La Entidad informa que las hojas de vida, títulos académicos, tarjetas profesionales, certificaciones y soportes de experiencia del personal mínimo requerido NO constituyen un requisito habilitante que deba adjuntarse con la propuesta, y por ende, no incluir documentos del personal dentro de la oferta no es causal de rechazo ni de inadmisión.

	De conformidad con lo establecido textualmente en las Notas 1 y 2 del numeral 4 ("PERSONAL MÍNIMO REQUERIDO") del formato GCON-FM-022 (página 22), dichos documentos deberán ser presentados únicamente por el contratista adjudicatario para aprobación del supervisor al inicio del contrato: "Nota 1: Los perfiles anteriores deben ser aportados por el contratista para la aprobación por parte del supervisor para el inicio del contrato. Nota 2: El contratista deberá incluir la hoja de vida, copia de la cédula de ciudadanía y los soportes de la experiencia profesional y de la formación académica correspondientes a los tres profesionales descritos anteriormente."

Observación N.° 93	**OLIMPIA IT — Contractual**
Observación presentada	Las fechas, incluida la de cierre, se establecen en SECOP II. La oferta debe integrar documentación jurídica, financiera, técnica, experiencia, garantía de seriedad y carta vigente del fabricante.
Solicitud de aclaración o ajuste	Se solicita ampliar en cinco (5) días hábiles la fecha límite para presentar ofertas y reflejar la modificación en el cronograma de SECOP II. La propuesta exige gestionar carta del fabricante, cotizaciones y autorizaciones de canal, validar licenciamiento y soporte, seleccionar y acreditar experiencia, preparar documentos jurídicos, financieros y técnicos, constituir la garantía de seriedad y surtir aprobaciones internas. El plazo adicional favorece la pluralidad, la calidad y comparabilidad de las ofertas y la selección objetiva, sin alterar la finalidad del proceso.
Decisión	No aceptada
Respuesta UAERMV	En respuesta a la observación se informa que tan pronto se cuente con el pliego definitivo publicado no se ampliarán términos adicionales ya que el proceso se encuentra estructurado con los plazos suficientes para que los interesados estructuren sus ofertas de acuerdo con lo solicitado en los documentos del proceso y para el tipo de modalidad de selección.

Observación N.° 94	**OLIMPIA IT — Contractual**
Observación presentada	El pliego señala que las especificaciones técnicas, necesidades y características del objeto se encuentran descritas en el formato GCON-FM-022. Sin embargo, el documento denominado “12 ACEPTACIÓN CARACTERÍSTICAS TEC” únicamente contiene una manifestación general del representante legal de conocer y cumplir dicho formato, sin detallar la solución técnica puntual requerida por la Entidad.

Solicitud de aclaración o ajuste	Se solicita respetuosamente a la Entidad identificar de manera expresa y publicar el anexo, ficha o formato en el cual se define la solución técnica puntual requerida, indicando su nombre, código, versión y ubicación dentro de los documentos del proceso. En particular, se solicita que dicho documento detalle como mínimo las funcionalidades y capacidades obligatorias de EDR y DLP, arquitectura y modalidad de despliegue, cantidades y tipo de licenciamiento, compatibilidades, integraciones requeridas, alcance de la implementación, migración y configuración, entregables, soporte, niveles de servicio, pruebas y criterios objetivos de aceptación. Si el documento corresponde al formato GCON-FM-022, se solicita confirmar que fue publicado completo y señalar el archivo que lo contiene; de no haberse publicado, se solicita incorporarlo antes del cierre y conceder un plazo suficiente para que los interesados evalúen sus exigencias y estructuren una oferta técnica y económica comparable, evitando que la simple firma del formato de aceptación sustituya el conocimiento previo y completo de las especificaciones.
Decisión	No aceptada
Respuesta UAERMV	La UAERMV se permite informar que de conformidad con el numeral 6.2.1 CERTIFICACIÓN TÉCNICA DEL OFERENTE del estudio previo y 4.2.2 VERIFICACIÓN DE CUMPLIMIENTO DE LOS REQUERIMIENTOS Y ESPECIFICACIONES DEFINIDOS EN EL FORMATO GCON-FM-022 del pliego del proceso, el proponente deberá presentar con la oferta, el formato en donde señale que conoce y se compromete a cumplir en su totalidad las especificaciones, características, requisitos técnicos y condiciones de entregan definidos en el documento denominado la FORMULACIÓN DE ESTUDIOS DEL SECTOR GCON-FM-022, asumiendo las obligaciones que dicho compromiso acarrea. Se le aclara al observante que las especificaciones técnicas se encuentran contenidas en la FORMULACIÓN DE ESTUDIOS DEL SECTOR GCON-FM-022Gel cual se encuentra publicado en la plataforma SECOP II dentro de los documentos del proceso. Así mismo, se le aclara al observante que se encuentra publicado en la plataforma SECOP II dentro de los documentos del proceso el archivo 12. FORMATO ACEPTACIÓN ESPECIFICACIONES Y CARACTERÍSTICAS TÉCNICAS el cual deberá ser presentado por los proponentes en el que manifestaran que conocen y se comprometen a cumplir en su totalidad las especificaciones, características, requisitos técnicos y condiciones de entrega definidos en la FORMULACIÓN DE ESTUDIOS DEL SECTOR GCON-FM-022.

Observación N.° 95	**MSL — Contractual**
Observación presentada	2. Supresión del registro y la habilitación técnica ante la Policía Nacional: El mismo cuadro exige un documento técnico de la Policía Nacional que acredite registro y habilitación conforme al artículo 12 del Decreto 723 de 2014 y a la Resolución 02086 del 30 de mayo de 2014. El régimen jurídico del proyecto también incorpora estas exigencias. Tales disposiciones regulan un servicio distinto del que se pretende contratar. El artículo 12 del Decreto 723 de 2014, compilado en el artículo 2.2.6.12 del Decreto 1070 de 2015, establece requisitos para proveedores del servicio de posicionamiento global vinculado al control de la maquinaria comprendida en ese régimen. Entre ellos figuran la transmisión de información de rastreo a la Policía Nacional, la integración con sus servidores y la conservación de reportes de trazabilidad de la maquinaria. La Resolución 02086 de 2014 desarrolla las condiciones técnicas de los dispositivos GPS, la autorización y el registro de sus proveedores y su instalación en la maquinaria regulada. Las referencias a dispositivos de seguridad y monitoreo electrónico deben leerse dentro de ese ámbito material; no equivalen a una autorización policial para suministrar software de ciberseguridad. El objeto descrito en el proyecto no comprende rastreo satelital de maquinaria, instalación de GPS ni integración de sus reportes con la Policía Nacional. La prevención de amenazas en equipos terminales y de fugas de información tiene una finalidad y una operación diferentes. La actividad misional de mantenimiento vial de la entidad no extiende este régimen a todos los bienes y servicios que adquiere. Las dos exigencias observadas deben respetar la adecuación y proporcionalidad de los requisitos habilitantes y la obligación de establecer condiciones objetivas necesarias para participar. Mantener registros propios de actividades ajenas al contrato limita injustificadamente la concurrencia de proveedores idóneos
Solicitud de aclaración o ajuste	Solicitamos muy amablemente a la entidad, eliminar el documento de registro y habilitación técnica ante la Policía Nacional del cuadro de verificación y retirar las remisiones al Decreto 723 de 2014 y a la Resolución 02086 de 2014 como exigencias para este contrato. Precisar expresamente que su no presentación no constituye incumplimiento habilitante ni causal de rechazo
Decisión	Aceptada
Respuesta UAERMV	Verificados los documentos del proceso, el registro y habilitación ante la policía nacional no es un requisito habilitante del presente proceso, en consecuencia, la modificación sobre este aspecto se verá reflejada en el pliego definitivo

Observación N.° 96	**MSL — Contractual**
Observación presentada	3. Improcedencia de limitar la convocatoria a Mipymes por superar el umbral: El numeral 1.3 aduce limitar la convocatoria a Mipymes utilizando un umbral de $533.287.768, sin embargo, ese valor corresponde al año 2025. Para 2026, Colombia Compra Eficiente publica expresamente el umbral de US$125.000 en $511.708.497. Este es el valor aplicable a la limitación a Mipymes, independientemente de los umbrales de cobertura de acuerdos comerciales que aparecen en el mismo documento.7 El presupuesto oficial es de $523.652.448, según el numeral 1.3 y el apartado de presupuesto oficial del proyecto. Por tanto, supera el umbral de 2026 en $11.943.951 y no satisface el requisito económico para una convocatoria limitada. Adicionalmente, el numeral se contradice al señalar que no se cumple el requisito económico, afirmar después que el valor es menor al umbral y concluir que la entidad podrá limitar la convocatoria. La corrección debe abarcar tanto la cifra como la consecuencia jurídica.
Solicitud de aclaración o ajuste	Solicitamos muy amablemente a la entidad, actualizar el umbral a $511.708.497 y modificar el numeral 1.3 para establecer que este proceso no será limitado a Mipymes, dado que su presupuesto oficial supera dicho valor. Ajustar en el mismo sentido los documentos y campos correspondientes de SECOP II.
Decisión	Aceptada
Respuesta UAERMV	Verificados los documentos del proceso y teniendo en cuenta que el presupuesto para el presente proceso de contratación QUINIENTOS VEINTITRÉS MILLONES SEISCIENTOS CINCUENTA Y DOS MIL CUATROCIENTOS CUARENTA Y OCHO PESOS M/CTE ($523.652.448,00) supera el umbral establecido para limitación del proceso a las MIPYMES en USD 125.000 (V/r Umbral Mipyme en COP ($511.708.497), conforme el numeral primero del artículo 2.2.1.2.4.2.2. de la Subsección 2 de la Sección 4 del Capítulo 2 del Título 1 de la Parte 2 del Libro 2 del Decreto 1082 de 2015, modificado por el artículo 5 del Decreto 1860 de 2021, la UNIDAD ADMINISTRATIVA ESPECIAL DE REHABILITACIÓN Y MANTENIMIENTO VIAL – UAERMV determina que el presente proceso NO SE LIMITA A MIPYMES y queda abierto a todos los proponentes que deseen participar y que cumplan con los requisitos establecidos en el pliego de condiciones y demás documentos que conforman el proceso de selección. La modificación sobre este aspecto se verá reflejada en el pliego definitivo.

El Documento 20261150338383 fue firmado electrónicamente por:	
NELSON EFRAIN MEDINA PINZON	**Contratista**, GERENCIA DE CONTRATACIÓN, ID: 4061440, nelson.medina@umv.gov.co, Fecha de Firma: 10-11-2026 11:46:17
ANGEL LEONARDO JEREZ CARVAJAL	**Contratista**, GERENCIA DE CONTRATACIÓN, ID: 1020746500, angel.jerez@umv.gov.co, Fecha de Firma: 10-11-2026 11:52:50
DANIELA ALEJANDRA AVILA MONTENEGRO	**Contratista**, OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN, ID: 1010244152, daniela.montenegro@umv.gov.co, Fecha de Firma: 10-11-2026 13:30:33
YENNY HASLEY YAZO LOZADA	**Jefe de Oficina**, OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN, ID: 521242051, yenny.yazo@umv.gov.co, Fecha de Firma: 10-11-2026 15:26:32
RAFAEL EDUARDO VARGAS CASTRO	, GERENCIA DE CONTRATACIÓN, ID: 77193263, rafael.vargas@umv.gov.co, Fecha de Firma: 10-11-2026 16:02:50



f113ea65eec00b60b7338788219e150675d6e36c5258de86a5dd8d23e58e9b1f
Codigo de Verificación CV: 8deb4 Comprobar desde:
https://www.umv.gov.co/portal/verificar/