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

RESPUESTA A LAS OBSERVACIONES PRESENTADAS AL PLIEGO DE CONDICIONES DEFINITIVO 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	
Observación presentada	Observación 1 – Estudios Previos, numeral 3 – Descripción de la necesidad, apartado 1 – Solución EDR avanzada, «Componentes de la Solución 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.” Observación: Solicitamos respetuosamente a la Entidad reconsiderar los límites de consumo de recursos establecidos para el agente EDR, permitiendo ampliar los requerimientos hasta 350 MB de memoria RAM y 1 GB de espacio en disco, de acuerdo con las especificaciones técnicas del fabricante. Si bien es cierto que algunas versiones anteriores de las soluciones EDR cuentan con requerimientos de recursos que se ajustan a los límites actualmente establecidos, es importante considerar que las versiones más recientes incorporan nuevas funcionalidades de protección, telemetría, análisis de comportamiento, investigación y respuesta ante amenazas, que pueden incrementar el consumo de recursos hasta 350 MB de memoria RAM y entre 750 MB y 1 GB de almacenamiento, dependiendo de las funcionalidades habilitadas. En este sentido, mantener límites de consumo asociados a versiones anteriores podría restringir la actualización de las plataformas a nuevas versiones durante la vigencia del contrato, limitando el acceso a mejoras de seguridad, nuevas capacidades de detección y funcionalidades desarrolladas por los fabricantes.
Solicitud de aclaración o ajuste	Por lo anterior, solicitamos a la Entidad flexibilizar los requerimientos de consumo del agente EDR, permitiendo hasta 350 MB de RAM y 1 GB de almacenamiento, siempre que estos valores se encuentren respaldados por la documentación oficial del fabricante y se garantice una operación eficiente, sin afectaciones significa vas al desempeño de los equipos protegidos
Decisión	Se acepta
Respuesta UAERMV	La Entidad informa que verificada la evolución tecnológica de los agentes de detección y respuesta de nueva generación (EDR) en sus versiones vigentes, la Entidad constata que la habilitación integral de las capacidades exigidas en el formato GCON-FM-022 — tales como prevención pre y post-ejecución con Machine Learning, registro y análisis continuo de eventos, rastreo de código, conservación de evidencia en modo autónomo fuera de línea y cacería de amenazas (threat hunting)— requiere asignaciones de memoria RAM de hasta 350MB y de espacio en disco de hasta 1GB conforme a las hojas de datos (datasheets) oficiales de los fabricantes. En consecuencia, con el fin de garantizar la plena coherencia técnica de los documentos del proceso, permitir el despliegue de las versiones más recientes de la plataforma

	durante la vigencia del contrato y asegurar la selección objetiva, **se acepta la observación** y mediante adenda se ajustará el requerimiento en los Estudios Previos, los Estudios del Sector y el formato GCON-FM-022, estableciendo que el agente EDR deberá ser ligero, con un requerimiento de recursos de hardware de hasta 350 MB de memoria RAM y hasta 1GB de espacio en disco, respaldado por la documentación técnica oficial del fabricante y garantizando una operación eficiente con mínima afectación al rendimiento de los equipos protegidos. *Por lo tanto, se modificarán los siguientes documentos:* • *Formulación de estudios del sector - GCON -FM-022, en el literal Componentes de la Solución EDR.* • *Estudios previos - GCON – FM –037, en el numeral 1. SOLUCIÓN DE ENDPOINT DETECTION AND RESPONSE O DETECCIÓN Y RESPUESTA DE ENDPOINTS AVANZADA (EDR) y el literal Componentes de la Solución EDR.* • *Estudio del Sector - GCON-FM-028, en el numeral 1. SOLUCIÓN DE ENDPOINT DETECTION AND RESPONSE O DETECCIÓN Y RESPUESTA DE ENDPOINTS AVANZADA (EDR) y el literal Componentes de la Solución EDR.* *Y la modificación será la siguiente:* *"La plataforma de seguridad del endpoint EDR debe ser una arquitectura distribuida, la cual debe constar de un agente en software compatible con los sistemas operativos y entornos con los que cuenta la Entidad (estaciones de trabajo, portátiles y servidores que conforman los 450 endpoints), en las arquitecturas (32 y/o 64 bits según corresponda a cada sistema operativo) oficialmente soportadas por el fabricante: Windows (incluyendo Windows 11), macOS (Ventura 13 y superior), Windows Server (2019, 2022 y superior) y Linux (Oracle Linux, Ubuntu Server LTS y CentOS/RHEL en las versiones soportadas oficialmente en la hoja de datos del fabricante).* *En cuanto al hardware, debe ser un agente ligero, el cual no debe requerir más de 350 MB de memoria RAM y 1 GB de espacio en disco, de acuerdo con la documentación oficial del fabricante, garantizando una operación eficiente y mínima afectación al rendimiento de los equipos protegidos."*

Observación N.° 2	
Observación presentada	Observación 2 – Compatibilidad de sistemas operativos de la solución DLP Documento: Estudios Previos, numeral 3 – Descripción de la necesidad, apartado 2 – Solución DLP,

	«Componentes de la Solución DLP», Solicitamos respetuosamente a la Entidad reconsiderar el requerimiento de compatibilidad de sistemas operativos de la solución DLP, permitiendo acreditar dicha compatibilidad de acuerdo con las versiones y distribuciones oficialmente soportadas por el fabricante. Si bien se reconoce la necesidad de garantizar la protección de la información institucional en diferentes entornos tecnológicos, es importante considerar que las soluciones modernas de prevención de pérdida de datos pueden presentar diferencias de compatibilidad entre sistemas operativos de usuario final y sistemas operativos de servidor, sin que esto implique necesariamente una disminución de sus capacidades de protección. En este sentido, exigir compatibilidad con la totalidad de las distribuciones Linux y versiones de sistemas operativos relacionadas, independientemente de su utilización efectiva dentro del alcance contratado, podría limitar la participación de soluciones especializadas que cumplen con las funcionalidades de prevención, monitoreo y protección de información requeridas.
Solicitud de aclaración o ajuste	Por lo anterior, solicitamos a la Entidad permitir que la compatibilidad de la solución DLP se acredite conforme a la matriz oficial del fabricante, sobre los sistemas operativos efectivamente incluidos en los 450 endpoints objeto de protección, garantizando las funcionalidades de seguridad exigidas en dichos entornos. Así mismo, solicitamos precisar la cantidad de estaciones de trabajo y servidores por sistema operativo que deberán ser protegidos, con el fin de garantizar un dimensionamiento adecuado del licenciamiento y de los servicios de implementación.
Decisión	Se acepta parcialmente
Respuesta UAERMV	La Entidad informa que respecto a la acreditación de compatibilidad de sistemas operativos en la solución DLP: Se acoge. En concordancia con lo establecido en el numeral 4 de los Requerimientos Mínimos para la Entrega del Bien, Obra o Servicio Objeto del Contrato – Generales del formato GCON-FM-022 (página 26: "4. La solución deberá ser compatible, como mínimo, con sistemas operativos Windows, Linux y macOS, así como integrarse con servicios de identidad basados en Directorio Activo local y servicios de identidad en la nube, garantizando las funcionalidades solicitadas según el fabricante"), la Entidad precisa que para la Solución DLP Avanzada la compatibilidad del agente ligero en sistemas operativos Windows, macOS y Linux se acreditará conforme a la documentación técnica o matriz de compatibilidad oficial vigente del fabricante para los sistemas operativos de los endpoints objeto de

	protección, sin que sea exigible acreditar arquitecturas de 32 bits en sistemas de 64 bits ni distribuciones de sistemas operativos de servidor donde no aplique el despliegue del agente DLP de usuario final. Asimismo, para la Solución EDR Avanzada, la compatibilidad multiplataforma con estaciones de trabajo y servidores (Windows, Windows Server, macOS y distribuciones Linux empresariales Oracle Linux, Ubuntu LTS y CentOS) se verificará en las arquitecturas (32 y/o 64 bits según corresponda a cada sistema operativo) soportadas en la ficha técnica oficial del fabricante. Asi mismo, la Entidad aclara que la totalidad de las 450 suscripciones se oferta y contrata bajo una única unidad de medida estandarizada ("Endpoints", 450 unidades a precio unitario único por endpoint) que permite activar la protección indistintamente sobre estaciones de trabajo o servidores, y el inventario detallado por máquina será entregado al contratista adjudicatario al inicio del contrato para la elaboración conjunta del plan de despliegue dentro de los primeros cinco (5) días hábiles siguientes al acta de inicio. *Por lo tanto, se modificarán los siguientes documentos:* • *Formulación de estudios del sector - GCON -FM-022, en el literal Componentes de la Solución DLP* • *Estudios previos - GCON – FM –037, en el numeral 2. SOLUCIÓN DE DATA LOSS PREVENTION O PREVENCIÓN DE PÉRDIDA DE DATOS (DLP), en el literal Componentes de la Solución DLP.* • *Estudio del Sector - GCON-FM-028, en el numeral 2. SOLUCIÓN DE DATA LOSS PREVENTION O PREVENCIÓN DE PÉRDIDA DE DATOS (DLP), en el literal Componentes de la Solución DLP.* *Y la modificación será la siguiente:* *"La plataforma de seguridad de DLP debe ser una arquitectura distribuida, la cual debe constar de un agente ligero en software compatible con sistemas operativos Windows, macOS y Linux, acreditado conforme a las versiones, distribuciones y arquitecturas oficialmente soportadas en la documentación técnica o matriz de compatibilidad oficial del fabricante para los endpoints objeto de protección."*

Observación N.° 3	
Observación presentada	Observación 3 – Estudios Previos, numeral 3 – Solución EDR avanzada, «Funcionalidades de Prevención» “Gestión de parches para sistemas operativos Windows, OS, Linux.” Observación: Solicitamos respetuosamente a la Entidad reconsiderar el alcance del requerimiento relacionado con la gestión de parches para sistemas operativos Windows, macOS y Linux, permitiendo que este sea acreditado mediante las capacidades de identificación de vulnerabilidades, evaluación de riesgos, mitigación mediante parcheo virtual (Virtual Patching) y recomendaciones de remediación proporcionadas por la solución EDR. Si bien la gestión de parches constituye una práctica importante para mantener la seguridad de la infraestructura tecnológica, es necesario considerar que la distribución, instalación y administración de actualizaciones de sistemas operativos corresponde generalmente a soluciones especializadas de administración de endpoints, mientras que las plataformas EDR están orientadas principalmente a la prevención, detección y respuesta ante amenazas. En este sentido, exigir capacidades adicionales de distribución e instalación de parches podría implicar la incorporación de herramientas, licenciamientos y servicios complementarios que incrementan los costos de la solución, sin estar directamente relacionados con el propósito principal de protección avanzada de endpoints y prevención de pérdida de datos establecido en el objeto contractual.
Solicitud de aclaración o ajuste	Por lo anterior, solicitamos a la Entidad permitir que el requisito sea acreditado mediante las funcionalidades de identificación, evaluación y mitigación de vulnerabilidades disponibles en el EDR, incluyendo parcheo virtual, sin exigir la instalación directa de actualizaciones de los sistemas operativos, manteniendo las capacidades de protección y reducción de la superficie de ataque requeridas.
Decisión	Se acepta

Respuesta UAERMV	La Entidad informa que analizada de manera sistemática e integral la estructuración técnica del proceso contenida en el formato GCON-FM-022 y en los Estudios Previos, se verifica que en la tabla oficial de "Descripción Técnica de la Necesidad – Ítem 1: Solución EDR Avanzada" (página 17 del formato GCON-FM-022) el requerimiento está definido funcionalmente como: "La solución deberá permitir mitigación proactiva de riesgos en tiempo real y seguridad de IoT, reduciendo considerablemente la superficie de ataque mediante evaluaciones de vulnerabilidad y políticas de mitigación de riesgos, como la aplicación de parches virtuales, la detección de dispositivos y el control de aplicaciones", lo cual guarda total correspondencia con las capacidades de Higiene de TI (Descubrimiento de activos, Evaluación de activos, Reducción de la superficie de ataque, Control de aplicaciones y Control de dispositivos USB) exigidas en las páginas 9, 19, 26 y 28 del mismo documento. En consecuencia, asiste razón al observante en cuanto a que el propósito técnico de la plataforma EDR no es operar como un servidor externo de distribución e instalación de actualizaciones de sistemas operativos (Patch Deployment), sino identificar las vulnerabilidades en el sistema operativo y en las aplicaciones ejecutadas (mostrando su clasificación de riesgo y los códigos CVE aplicables) y mitigarlas proactivamente en tiempo real mediante parches virtuales (Virtual Patching) y políticas basadas en riesgo. *Por lo tanto, se modificarán los siguientes documentos:* • *Formulación de estudios del sector - GCON -FM-022, en el literal Funcionalidades de Prevención* • *Estudios previos - GCON – FM – 037, en el numeral 1. SOLUCIÓN DE ENDPOINT DETECTION AND RESPONSE O DETECCIÓN Y RESPUESTA DE ENDPOINTS AVANZADA (EDR). en el literal Funcionalidades de Prevención.* • *Estudio del Sector - GCON-FM-028, en el numeral 1. SOLUCIÓN DE ENDPOINT DETECTION AND RESPONSE O DETECCIÓN Y RESPUESTA DE ENDPOINTS AVANZADA (EDR). en el literal Funcionalidades de Prevención.*

	Y la modificación será la siguiente: *"Identificación, evaluación y mitigación de vulnerabilidades (incluyendo detalle de códigos CVE aplicables, recomendaciones de remediación y aplicación de parches virtuales / Virtual Patching) para sistemas operativos Windows, macOS y Linux, sin exigir la distribución o instalación directa de actualizaciones sobre los sistemas operativos."*

El Documento 20261150350713 fue firmado electrónicamente por:	
CARLOS ABEL BASTIDAS CUBILLOS	**Contratista – Líder de Infraestructura y Servicios**, OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN, ID: 79637740, carlos.bastidas@umv.gov.co, Fecha de Firma: 18-11-2026 15:26:31
YENNY HASLEY YAZO LOZADA	**JEFE DE OFICINA (E)**, OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN, ID: 521242051, yenny.yazo@umv.gov.co, Fecha de Firma: 18-11-2026 15:19:57
MARINO MIGUEL MORENO RHENALS	**Contratista**, OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN, ID: 1073819679, marino.moreno@umv.gov.co, Fecha de Firma: 18-11-2026 15:31:23
Revisó:	NELSON EFRAIN MEDINA PINZON - Contratista - GERENCIA DE CONTRATACIÓN - nelson.medina@umv.gov.co

e70f8ec5e7d91dfc2f962768ffbaf5c6e608a1070b61e6c6c51e46ca5dafe4dc
Codigo de Verificación CV: bdc3e Comprobar desde:
https://www.umv.gov.co/portal/verificar/