2025020030658
Fecha Radicado: 2025-07-31 15:31:14.0

Medellín, 31/07/2025

Doctora
ROSA MARÍA ACEVEDO JARAMILLO
Secretaria de Despacho
Secretaría de Talento Humano y Servicios Administrativos

Asunto: respuesta a oficio 2025020029245

Respetada doctora Rosa María:

En atención a la solicitud de aval para el proceso contractual cuyo objeto es la "*Modernización del Sistema Integrado de Seguridad de la Gobernación de Antioquia y sus sedes externas, mediante la modalidad de leasing tecnológico*", los profesionales de la Dirección de Tecnología e Información revisaron la documentación remitida, la cual incluye:

- Estudios y documentos previos del proceso.
- Especificaciones técnicas.
- Ofertas comerciales.
- Análisis del sector.

Del análisis realizado se concluye que, si bien el contrato contempla la actualización del diagnóstico del sistema, se recomienda que este insumo sea considerado obligatorio. En su defecto, se sugiere incorporar como criterio de evaluación una ponderación **adicional** de al menos 100 puntos más a las ofertas que incluyan la elaboración del diagnóstico técnico como parte de los primeros entregables.

Un diagnóstico técnico actualizado permitirá definir con mayor precisión aspectos que actualmente se presentan de forma general o implícita en las fichas técnicas. Por ejemplo:

- El software de registro de visitantes podrá dimensionarse de forma más eficiente si se conoce con exactitud la infraestructura donde será desplegado, su modalidad de operación (web o cliente local) y su capacidad de integración con las cámaras IP existentes.

- Los lectores de cédulas y dispositivos de firma digital requieren verificación técnica de su estado operativo. Un diagnóstico adecuado permitirá justificar su reutilización o renovación, alineándose con criterios de compatibilidad y trazabilidad.

- El número de licencias para reconocimiento facial debe sustentarse en una línea base real de usuarios. El diagnóstico permitirá validar si los 10.000 perfiles propuestos son suficientes.

Documento Firmado
Digitalmente: # 2025020030658

- Las controladoras biométricas, si se presentan en kits (gabinete, batería, controladora), deben planearse considerando condiciones de instalación, respaldo y mantenimiento. El diagnóstico definirá su distribución óptima.

- La integración entre licencias de reconocimiento de placas y talanqueras debe ser evaluada técnicamente. El diagnóstico permitirá identificar las necesidades reales de interoperabilidad.

- La asignación de cámaras con analítica en el borde versus procesamiento en servidor debe partir del inventario real de ubicaciones y objetivos de monitoreo.
- En cuanto a los equipos All-in-One, un diagnóstico del entorno de operación permitirá determinar si cumplen con los requisitos de desempeño o si se requiere la adquisición de estaciones de trabajo industriales.
- Incluir dentro del diagnóstico la revisión del estado actual y posibles mejoras del sistema de detección y extinción de incendios del centro de cómputo.

De otro lado y respecto a la ficha técnica, se recomienda definir expresamente los tiempos máximos de reposición según la criticidad del componente, por ejemplo:

- Equipos críticos (servidores, cámaras CAD): máximo 48 horas.
- Cámaras en sedes externas: entre 3 y 5 días hábiles.
- Periféricos menores (lectores, pulsadores, monitores): hasta 7 días hábiles.

Por último, aunque en Colombia no existe una ley que restrinja la compra de equipos de seguridad de ciertas marcas, sí se deben tener en cuenta lineamientos normativos que orientan la adquisición segura de tecnologías sensibles, tales como:

- CONPES 3995 de 2020 – Política Nacional de Seguridad Digital.

- Lineamientos de Seguridad y Privacidad para la Implementación de Soluciones TI (MinTIC).

- Resoluciones del Ministerio de Defensa y la Dirección Nacional de Inteligencia (DNI).

- Ley 1581 de 2012 sobre protección de datos personales.

Por lo anterior, se sugiere incorporar en los criterios de evaluación y validación técnica:

“Los fabricantes de los componentes tecnológicos ofertados (cámaras, controladoras, servidores, software de vigilancia) deberán contar con certificaciones o garantías que respalden su cumplimiento en materia de ciberseguridad y protección de datos. No podrán

Documento Firmado Digitalmente: # 2025020030658

ofertarse equipos de fabricantes incluidos en listas restrictivas internacionales relacionadas con riesgos en la cadena de suministro (por ejemplo, NDAA sección 889, UE 2021/821, etc.).”

Asimismo, se sugiere exigir en los criterios de evaluación y validación técnica:

- Declaración de cumplimiento de estándares de ciberseguridad.

- Certificaciones internacionales (ISO 27001, FIPS 140-2, Common Criteria (estándar internacional (ISO/IEC 15408)))

- Declaración de trazabilidad y origen de fabricación.

- Declaración de no inclusión en listas restrictivas internacionales (ej. NDAA Sección 889, UE 2021/821).

Con base en el análisis técnico realizado, y teniendo en cuenta las recomendaciones aquí expuestas particularmente importancia de la actualización del diagnóstico, definir criterios claros de mantenimiento, y alinear la adquisición con las políticas nacionales de seguridad digital y protección de datos, la Dirección de Tecnología e Información **otorga Aval Técnico Favorable**, con el fin de dar continuidad al proceso contractual y apoyar la implementación de una solución integral, segura y sostenible para el Sistema de Seguridad y Control de Acceso de la entidad

Cordialmente,

MARIA CRISTINA GIRALDO OSPINA
DIRECTOR TECNICO

Proyectó:	NOMBRE	FIRMA	FECHA
Proyectó	María Victoria Londoño Tobar Profesional Especializada		30//07/2025
	Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y por lo tanto, bajo nuestra responsabilidad lo presentamos para firma.		

Documento Firmado
Digitalmente: # 2025020030658