ESTUDIO DEL SECTOR PARA EL DESARROLLO DE UN PROCESO DE CONTRATACIÓN DIRECTA

Conforme el artículo 2.2.1.1.1.6.1 del Decreto 1082 de 2015, Infimanizales *"debe hacer, durante la etapa de planeación, el análisis necesario para conocer el sector relativo al objeto del proceso de contratación desde la perspectiva legal, comercial, financiera, organizacional, técnica, y de análisis de Riesgo. La Entidad Estatal debe dejar constancia de este análisis en los Documentos del Proceso.*

Para tal efecto, y conforme la *"Guía para la Elaboración de Estudios de Sector"* de la Agencia Nacional de Contratación *"Colombia Compra Eficiente"*, el análisis del sector debe tener en cuenta el objeto del proceso, y en particular, condiciones del contrato tales como el plazo, forma de cumplimiento, y forma de pago. Dicho análisis debe permitir a la Entidad sustentar su decisión de hacer la contratación directa, la elección del contratista y la forma en que se pacta el contrato desde el punto de vista de la eficiencia, eficacia y economía, en consecuencia, el suscrito servidor procede a elaborar el estudio del sector para la celebración de un contrato bajo la modalidad de selección de contratación directa.

PERSPECTIVA LEGAL

La Ley 1150 de 2007, que modificó la Ley 80 de 1993, estableció entre las modalidades validas de contratación, la contratación directa, dispone el artículo 2.2.1.2.1.4.9. Contratos de prestación de servicios profesionales y de apoyo a la gestión, o para la ejecución de trabajos artísticos que solo pueden encomendarse a determinadas personas naturales. "Las Entidades Estatales pueden contratar bajo la modalidad de contratación directa la prestación de servicios profesionales y de apoyo a la gestión con la persona natural o jurídica que esté en capacidad de ejecutar el objeto del contrato, siempre y cuando la Entidad Estatal verifique la idoneidad o experiencia requerida y relacionada con el área de que se trate. En este caso, no es necesario que la Entidad Estatal haya obtenido previamente varias ofertas, de lo cual el ordenador del gasto debe dejar constancia escrita."

PERSPECTIVA ECONOMICA Y COMERCIAL:

El sector de la seguridad de la información y la ciberseguridad presenta un comportamiento dinámico y en crecimiento, impulsado por el aumento de los riesgos tecnológicos, la digitalización de los procesos institucionales y el fortalecimiento de los marcos regulatorios aplicables a las entidades públicas y privadas, especialmente aquellas sometidas a vigilancia y control de la Superintendencia Financiera de Colombia.

Desde la perspectiva económica, las organizaciones reconocen la seguridad de la información como un componente estratégico, destinando recursos específicos para la prevención de incidentes, la protección de los activos de información y el cumplimiento de las obligaciones normativas. Esta inversión resulta proporcional al nivel de exposición al riesgo y a la criticidad de los servicios que soportan la operación institucional.
Entre los principales factores económicos que caracterizan el sector se destacan:

- El incremento progresivo de la inversión en seguridad de la información y ciberseguridad dentro de los presupuestos de tecnologías de la información.
- El alto impacto económico que pueden generar los incidentes de seguridad, reflejado en pérdidas financieras, sanciones regulatorias, afectaciones operativas y daño reputacional.
- La necesidad de asegurar la sostenibilidad de la inversión mediante la implementación de modelos de seguridad estructurados, escalables y alineados con estándares reconocidos.

Desde el punto de vista comercial, el mercado ofrece una amplia gama de servicios especializados orientados al acompañamiento, implementación, evaluación y mejora continua de los modelos de seguridad de la información y ciberseguridad. La demanda de estos servicios se mantiene constante debido a las exigencias regulatorias y a la necesidad de las entidades de fortalecer sus capacidades internas sin incrementar de manera permanente su planta de personal.

Adicionalmente, el entorno normativo vigente, en particular las disposiciones contenidas en la Circular Externa 007 de 2018 y sus actualizaciones, genera un impacto directo en la dinámica comercial del sector, al establecer obligaciones que hacen indispensable la contratación de servicios especializados que permitan a las entidades garantizar su cumplimiento de manera oportuna y eficiente.

ANALISIS DE OFERTA

El mercado colombiano de servicios asociados a la gestión de la seguridad de la información y la ciberseguridad ha mostrado una evolución sostenida, motivada principalmente por el aumento de la exposición a riesgos cibernéticos, la transformación digital de las entidades públicas y privadas, y el fortalecimiento del marco regulatorio aplicable a las entidades vigiladas por la Superintendencia Financiera de Colombia.

La oferta disponible está conformada por organizaciones y profesionales con diferentes niveles de especialización, capacidad técnica y experiencia, lo que permite a las entidades estatales contar con alternativas idóneas para la contratación de servicios especializados que garanticen el cumplimiento normativo y la madurez de sus modelos de seguridad.

Dentro de los oferentes más representativos del sector se identifican:

- Empresas especializadas en consultoría, implementación y acompañamiento en modelos de seguridad de la información y ciberseguridad.
- Profesionales independientes con certificaciones reconocidas internacionalmente en gestión de seguridad y riesgos tecnológicos.
- Firmas de auditoría y consultoría que incorporan líneas especializadas en cumplimiento normativo y seguridad de la información.
- Proveedores tecnológicos que integran servicios de seguridad dentro de su portafolio de soluciones.

En cuanto a las tendencias del mercado, se evidencia un incremento en la contratación de servicios tercerizados, un mayor uso de herramientas automatizadas para la gestión de riesgos y monitoreo de incidentes, así como un enfoque creciente en el cumplimiento regulatorio derivado de disposiciones como la Circular Externa 007 de 2018 y sus actualizaciones.

PERSPECTIVA ASPECTOS TECNICOS GENERALES

El contrato proyectado tiene como finalidad garantizar la continuidad y fortalecimiento del Modelo de Seguridad de la Información y Ciberseguridad de la entidad, asegurando su alineación con las disposiciones normativas vigentes y las mejores prácticas reconocidas a nivel nacional e internacional.

Desde el punto de vista técnico, el servicio a contratar debe permitir:

- La implementación, ajuste y mejora de controles de seguridad de la información conforme al estándar ISO/IEC 27001 y demás lineamientos aplicables.
- La identificación, análisis y tratamiento de los riesgos asociados a los activos de información y a la infraestructura tecnológica de la entidad.
- El diseño, actualización y ejecución de planes de gestión de incidentes de seguridad de la información y ciberseguridad.
- La formulación y fortalecimiento de políticas, procedimientos y lineamientos internos en materia de seguridad de la información.
- La verificación de la efectividad de los controles implementados mediante actividades de evaluación, auditoría y pruebas técnicas especializadas.

Estos aspectos técnicos resultan indispensables para asegurar la adecuada protección de la información institucional, la continuidad de los servicios y el cumplimiento de las obligaciones regulatorias aplicables.

PERSEPECTIVA FINANCIERA Y ORGANIZACIONAL

PERSPECTIVA FINANCIERA

La contratación de servicios especializados en seguridad de la información y ciberseguridad constituye una inversión estratégica para las entidades vigiladas, en la medida en que contribuye a la prevención de riesgos operativos, financieros, legales y reputacionales.

Desde el enfoque financiero, se consideran relevantes los siguientes aspectos:

- Los costos asociados a la vinculación de talento altamente especializado en seguridad de la información y ciberseguridad.
- La inversión necesaria para la adopción y uso de herramientas tecnológicas que soporten la gestión de riesgos y el monitoreo de amenazas.
- Los costos derivados de procesos de evaluación, auditoría y certificación exigidos por la normativa vigente.

- La mitigación de posibles sanciones económicas y pérdidas financieras asociadas al incumplimiento regulatorio o a incidentes de seguridad.

PERSPECTIVA ORGANIZACIONAL

El adecuado cumplimiento de la normativa en materia de seguridad de la información exige una estructura organizacional que incorpore la gestión de la ciberseguridad como un componente transversal del gobierno institucional.

Desde esta perspectiva, el contrato permitirá:

- El fortalecimiento de los esquemas internos de gestión de seguridad de la información.
- La definición y consolidación de roles y responsabilidades en materia de seguridad y gestión de riesgos tecnológicos.
- El fortalecimiento de las capacidades institucionales mediante transferencia de conocimiento y acompañamiento especializado.
- La integración de la seguridad de la información dentro de los procesos de planeación, control y toma de decisiones.
- El establecimiento de mecanismos de seguimiento, reporte y mejora continua que garanticen la sostenibilidad del modelo implementado.

Adicional para el cumplimiento del objeto contractual y las obligaciones específicas a cargo del contratista, se estima que se debe acreditar las siguientes condiciones:

- Persona jurídica, en cuyo objeto social se contemple de manera concreta la realización de las actividades previstas en el objeto del contrato.
- Constitución de la empresa con una antigüedad mínima nueve (9) años o más.

PLAZO

El contrato tendrá un término de duración a partir de la legalización y hasta el treinta y uno (31) de diciembre del 2026.

ANÁLISIS DE CONTRATACIONES ANTERIORES

Se revisaron procesos de naturaleza y objeto similar en el SECOP II:

N* PROCESO	ENTIDAD	OBJETO	VALOR	PLAZO
SNS-CD-392-2026	SUPERINTENDENCIA NACIONAL DE SALUD	Prestar servicios profesionales a la Dirección de Innovación y Desarrollo para apoyar las actividades relacionadas con la estrategia de seguridad digital y ciberseguridad, en el marco de la Política de Seguridad Digital en la Superintendencia Nacional de Salud.	149.500.000 COP	345 (Días)
CW369344	CHEC S.A. E.S.P. BIC	Suministro, soporte, actualización, mantenimiento y servicios asociados de soluciones de ciberseguridad	571.201.850 COP	730 (Días)
RTVC-CD-	RTVC.	EL CONTRATISTA Se obliga con	74.592.000	6 (Meses)

397-2026		RTVC a prestar servicios especializados en seguridad digital encargado de planear, organizar, implementar y controlar las estrategias de ciberseguridad y el plan de recuperación de desastres de la entidad. su labor incluye definir políticas, procedimientos y controles que aseguren la confidencialidad, integridad, disponibilidad y resiliencia de la información y servicios tecnológicos. también deberá promover buenas prácticas, gestionar incidentes, garantizar la cont	COP	

Así mismo, dentro del análisis técnico y económico se relacionan los siguientes contratos que se han desarrollado en años anteriores:

ENTIDAD	Nro. CONTRATO	OBJETO	VALOR	PLAZO
INFIMANIZALES	2025-03-044	PRESTACIÓN DE SERVICIOS ESPECIALIZADOS PARA APOYAR A LA UNIDAD DE SERVICIOS CORPORATIVOS EN LA CONTINUIDAD Y FORTALECIMIENTO DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD, CON EL PROPÓSITO DE ASEGURAR EL CUMPLIMIENTO DE LA CIRCULAR EXTERNA 007 DE 2018 Y SUS ACTUALIZACIONES EMITIDAS POR LA SUPERINTENDENCIA FINANCIERA DE COLOMBIA.	$129.734.609	9 Meses
INFIMANIZALES	2024-04-050	PRESTACION DE SERVICIOS PARA APOYAR LA UNIDAD DE SERVICIOS CORPORATIVOS CON EL OBJETIVO DE DAR CONTINUIDAD A LA ESTRUCTURACIÓN DEL SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION Y CIBERSEGURIDAD, DANDO CUMPLIMIENTO A LA CIRCULAR EXTERNA 007 DE 2018 Y ACTUALIZACIONES DE LA SUPERINTENDENCIA FINANCIERA DE COLOMBIA	$118.000.000	8 Meses
INFIMANIZALES	2023-06-096	PRESTAR LOS SERVICIOS DE APOYO A LA GESTION A LA UNIDAD DE SERVICIOS CORPORATIVOS EN LA IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD, EN CUMPLIMIENTO DE LAS CIRCULARES EXTERNAS 007 DE 2018 DEL SFC CON EL OBJETIVO DE DAR CONTINUIDAD A LA ESTRUCTURACIÓN DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD.	$137.000.000	190 Días

Al igual que en las contrataciones anteriores, el valor del contrato se ha determinado teniendo en cuenta el presupuesto asignado, las actividades y responsabilidades asumidas para la óptima ejecución del objeto contractual.

ANÁLISIS DE PRECIOS

Para definir el valor del contrato se tendrá en cuenta el histórico de contratos de esta misma naturaleza suscritos en años anteriores, por lo tanto, se considera que el valor presupuestado para el contrato será de ciento treinta y seis millones doscientos veinte mil pesos ($136.220.000) incluido IVA.

Manizales, enero 13 de 2026

MONICA MEJIA QUINTERO
Profesional Universitario TI