120.11

ANEXO 01.
DESCRIPCIÓN DE LA NECESIDAD DE CONTRATACIÓN Y ANALISIS DEL SECTOR

Dando cumplimiento a lo preceptuado en el Artículo 2.2.1.1.1.6.1. del Decreto 1082 de 2015, deber de análisis de las Entidades Estatales, la Entidad Estatal debe hacer, durante la etapa de planeación, el análisis necesario para conocer el sector relativo al objeto del Proceso de Contratación desde perspectiva legal, comercial, financiera, organizacional, técnica, y de análisis del Riesgo. Para lo cual se deja constancia en el presente documento así:

1. INTRODUCCIÓN

La función de la adquisición de bienes o servicios debe estar orientada a satisfacer las necesidades de las entidades públicas y a obtener el mayor valor por el dinero público. Las entidades estatales deben entender claramente cuál es su necesidad y como pueden satisfacerla, por lo cual, deben conocer y entender cómo y con quien pueden establecer la relación contractual que permita satisfacer la necesidad identificada. Para el efecto es necesario que las entidades estatales conozcan el contexto en el cual los posibles proveedores desarrollan su actividad.

El artículo 2.2.1.1.1.6.1 del decreto 1082 de 2015, estableció como deber de las entidades estatales el realizar, durante la etapa de planeación, el análisis del sector económico y de los oferentes.

El análisis debe permitir conocer el sector relativo al objeto del proceso de contratación desde la perspectiva legal, comercial, financiera, organizacional, técnica y de análisis de riesgo.

De este análisis la entidad estatal debe dejar constancia en los documentos del proceso contractual el cual será publicado en el portal SECOP II.

2. DESCRIPCIÓN DE LA NECESIDAD QUE LA CONTRALORÍA PRETENDE SATISFACER CON LA CONTRATACIÓN

La Contraloría Departamental del Valle del Cauca, en cumplimiento de las funciones constitucionales y legales asignadas a los organismos de control fiscal, debe garantizar el adecuado desarrollo de sus procesos misionales, administrativos y de apoyo, así como la protección, disponibilidad, integridad y confidencialidad de la información que administra y custodia.

De conformidad con el artículo 267 de la Constitución Política de Colombia, modificado por el artículo 1 del Acto Legislativo 04 de 2019, "*...la vigilancia y el control fiscal comprenden, entre otros aspectos, el seguimiento permanente al recurso público y el control financiero, de gestión y de resultados, fundamentado en los principios de eficiencia, economía, equidad, desarrollo sostenible y valoración de los costos ambientales. ...*" En el desarrollo de estas funciones, la Entidad requiere disponer de una infraestructura tecnológica confiable y segura que permita garantizar la continuidad de sus operaciones y la adecuada gestión de la información institucional.

Así mismo, el artículo 209 de la Constitución Política establece que la función administrativa está al servicio de los intereses generales y debe desarrollarse con fundamento en los principios de igualdad, moralidad, eficacia, economía, celeridad, imparcialidad y publicidad. En este contexto, las tecnologías de la información y las comunicaciones –TIC– constituyen un componente transversal para el cumplimiento de los objetivos institucionales, razón por la cual la protección de los activos de información y de la infraestructura tecnológica resulta fundamental para garantizar la prestación continua y eficiente de los servicios de la Entidad.

En la actualidad, las entidades públicas se encuentran expuestas a un escenario creciente de amenazas y riesgos asociados a la ciberseguridad, entre los que se encuentran códigos maliciosos,

ransomware, spyware, troyanos, gusanos, phishing, malware, explotación de vulnerabilidades, archivos maliciosos, sitios web comprometidos y otras modalidades de ataques que pueden afectar los equipos de cómputo, sistemas de información, redes institucionales y, especialmente, la información que soporta los procesos misionales y administrativos.

En atención a lo anterior, la Contraloría Departamental del Valle del Cauca requiere contar con mecanismos especializados de protección para sus equipos de cómputo y demás dispositivos tecnológicos, mediante la adquisición y/o renovación de licenciamiento de una solución de seguridad informática como ESET PROTECT Complete que permita fortalecer la protección de los equipos utilizados en el desarrollo de las actividades institucionales, de conformidad con las necesidades y especificaciones técnicas definidas por la Entidad.

La solución de seguridad para ENDPOINTS constituye una herramienta fundamental dentro de la estrategia de ciberseguridad institucional, toda vez que permite fortalecer las acciones de prevención, detección y respuesta frente a diferentes tipos de amenazas informáticas que puedan comprometer los dispositivos utilizados por los servidores públicos y contratistas para el desarrollo de sus actividades.

La necesidad de mantener vigente este tipo de licenciamiento se fundamenta en que la información constituye uno de los activos más importantes de la Entidad y es transversal a la totalidad de sus procesos. En consecuencia, resulta indispensable contar con controles tecnológicos que permitan reducir la probabilidad de materialización de incidentes de seguridad, prevenir afectaciones a la infraestructura tecnológica y minimizar los riesgos asociados a la pérdida, alteración, indisponibilidad o acceso no autorizado a la información institucional.

Por lo anteriormente expuesto, resulta necesario adquirir doscientas cincuenta (250) licencias de antivirus, destinadas a los equipos de cómputo que posee la Contraloría Departamental del Valle del Cauca y que son utilizados por los servidores públicos y demás usuarios autorizados para el desarrollo de sus funciones y actividades institucionales.

La cantidad requerida corresponde a los equipos de cómputo que requieren contar con la protección de la solución de seguridad informática, de acuerdo con el inventario y las necesidades identificadas por la Entidad. Para tal efecto, en el Anexo – "Listado de Equipos de Cómputo CDVC" se relacionan los equipos a los cuales se proyecta renovar/adquirir el respectivo licenciamiento, junto con sus características y demás información pertinente.

Tabla 1.
Listado de Equipos por tipo a renovar licencia

TIPO	CANTIDAD
Computador Escritorio	141
Computador Portátil	107
Servidores	2
TOTAL	**250**

Fuente: Propia

Tabla 2.
Listado de Equipos a renovar licencia por área

AREA AGRUPADA	CPU	PORTATIL	TOTAL
Control Fiscal	7	15	22
TIC	7	7	14
Recursos Naturales y Medio Ambiente	7	6	13
Patrimonial	4	8	12
Infraestructura	6	6	12
Participación Ciudadana	7	5	12
Gestión Humana	9	1	10
Investigaciones Fiscales	9	1	10

AREA AGRUPADA	CPU	PORTATIL	TOTAL
Contraloria	9	0	9
CERCOFI Palmira	0	9	9
CERCOFI Cali	4	4	8
Recursos Financieros y Físicos	5	3	8
Sector Descentralizado	3	5	8
Control Interno	6	2	8
Secretaría General	5	3	8
Jurisdicción Coactiva	6	2	8
CERCOFI Tuluá	0	8	8
CERCOFI Cartago	0	7	7
Subcontraloría	6	1	7
Planeación	4	3	7
Responsabilidad Fiscal	5	1	6
Jurídica	5	1	6
Despacho del Contralor	2	3	5
Sector Central	3	2	5
Nomina	5	0	5
Control Disciplinario	5	0	5
Tesoreria	4	0	4
Escuela de Capacitación	3	1	4
(Sin área)	2	0	2
Computador Servidor	2	0	2
Computador AGR	0	2	2
Archivo	1	0	1
Computador Sala audiencias	1	0	1
Oficina De Comunicacion Y Prensa	0	1	1
Sec. Común	1	0	1
TOTAL	143	107	250

Fuente: Propia

NOTA: Se adjunta el Anexo denominado "Listado Completo de Equipos", en el cual se relacionan detalladamente los equipos objeto de la renovación de licenciamiento, incluyendo las características correspondientes a cada uno de ellos.

2.1 OBJETO A CONTRATAR:

Adquirir doscientas cincuenta (250) licencias del antivirus ESET PROTECT Complete, correspondientes a la renovación del licenciamiento para la protección, detección y eliminación de *virus, troyanos, gusanos, adware, spyware, phishing, rootkits y archivos maliciosos.*

2.2 ESPECIFICACIONES TÉCNICAS

Las licencias de software antivirus *ESET PROTECT Complete* deben cumplir con las siguientes especificaciones técnicas:

- Consola basada en la nube
- Protección para endpoints
- Sandboxing en la nube
- Cifrado de disco completo
- Protección de apps en la nube

2.2.1 SERVICIO DE SEGURIDAD INFORMÁTICA Y PROTECCIÓN DE ENDPOINTS

La entidad requiere contratar el suministro, implementación, configuración, administración y soporte de una solución integral de seguridad informática para la protección de su infraestructura tecnológica, incluyendo equipos de cómputo, equipos portátiles, dispositivos móviles, servidores, correo electrónico y servicios de almacenamiento y colaboración en la nube.

La solución deberá contar con una plataforma de administración centralizada basada en la nube, que permita gestionar las diferentes capacidades de seguridad desde una única consola, facilitando la implementación, supervisión y administración remota de los dispositivos y servicios protegidos.

El servicio deberá incluir las licencias y funcionalidades necesarias para proporcionar, como mínimo, las siguientes capacidades:

A. PROTECCIÓN CONTRA MALWARE, RANSOMWARE Y AMENAZAS DE DÍA CERO: La solución deberá proporcionar protección multicapa contra malware, ransomware y otras amenazas informáticas, mediante mecanismos de detección y prevención capaces de actuar antes, durante y después de la ejecución de archivos o procesos potencialmente maliciosos.

Deberá incorporar mecanismos de protección frente a amenazas desconocidas y de día cero (0-day), incluyendo análisis de muestras sospechosas mediante sandboxing en la nube, con el propósito de evaluar su comportamiento en un entorno aislado.
La solución deberá incorporar, como mínimo:

- Detección basada en el comportamiento.
- Aprendizaje automático (machine learning).
- Análisis de comportamiento avanzado.
- Análisis estático y dinámico de archivos sospechosos.
- Utilización de información de inteligencia de amenazas.
- Análisis de reputación de archivos.
- Detección de amenazas de día cero (0-day).
- Protección frente a ransomware.
- Protección frente a ataques dirigidos.
- Detección de amenazas persistentes avanzadas.
- Detección y bloqueo de ataques sin archivos (fileless).

B. PROTECCIÓN MULTICAPA DE ENDPOINTS: El servicio deberá proporcionar protección para los equipos de cómputo y equipos portátiles de la entidad mediante una solución de seguridad de múltiples capas.

La solución deberá permitir detectar y bloquear amenazas en las diferentes etapas de un ataque y deberá contar con mecanismos destinados a reducir el riesgo de infección, vulneración de información y ejecución de código malicioso.
La protección deberá contemplar, como mínimo:

- Equipos de escritorio.
- Equipos portátiles.
- Sistemas operativos compatibles con la solución.
- Protección contra malware y ransomware.
- Protección contra ataques dirigidos.
- Protección contra amenazas persistentes avanzadas.
- Detección de ataques sin archivos.
- Protección de la información almacenada en los endpoints.
- Protección de servidores de archivos, cuando se encuentren dentro del alcance de la licencia contratada.

C. PROTECCIÓN DE DISPOSITIVOS MÓVILES: La solución deberá proporcionar mecanismos de seguridad para los dispositivos móviles incluidos dentro del alcance del licenciamiento, permitiendo protegerlos frente a amenazas informáticas y contribuir a la protección de la información institucional.

La administración de estos dispositivos deberá integrarse con la plataforma central de gestión, permitiendo al personal autorizado consultar su estado de protección y administrar las políticas de seguridad correspondientes.

D. PROTECCIÓN DE MICROSOFT 365 Y ONEDRIVE: La solución deberá proporcionar una capa adicional de protección para los servicios de Microsoft 365 utilizados por la entidad, incluyendo el correo electrónico y el almacenamiento de información en la nube.

Deberá contemplar la protección de servicios como Exchange Online, OneDrive, SharePoint Online y Microsoft Teams, de acuerdo con las capacidades contempladas en el licenciamiento contratado.
La solución deberá incorporar mecanismos de:

- Protección antimalware.
- Filtrado de spam.
- Protección Anti-Phishing.
- Análisis de archivos y contenidos potencialmente maliciosos.
- Protección del correo electrónico institucional.
- Protección del almacenamiento en la nube.
- Protección de la información almacenada en OneDrive.
- Detección de amenazas presentes en las aplicaciones de Microsoft 365.
- Protección preventiva frente a amenazas provenientes del correo electrónico.
- Protección frente a malware presente en los servicios y aplicaciones en la nube.

La solución deberá permitir la incorporación y protección automática de los nuevos usuarios de Microsoft 365 que sean incluidos dentro del alcance del servicio. Asimismo, deberá proporcionar visibilidad sobre las detecciones de seguridad y los elementos puestos en cuarentena, permitiendo su consulta y gestión desde la plataforma de administración correspondiente.

E. CIFRADO COMPLETO DE DISCOS: La solución deberá incluir capacidades de cifrado completo de disco (Full Disk Encryption) para proteger la información almacenada en los equipos de la entidad.

El cifrado deberá poder ser administrado de manera centralizada desde la consola de gestión y deberá contemplar equipos con sistemas operativos Windows y macOS, de acuerdo con las plataformas soportadas por la solución.
Como mínimo, deberá permitir:

- Administrar centralizadamente el cifrado de los equipos.
- Cifrar discos completos.
- Cifrar particiones o unidades del sistema.
- Implementar y activar el cifrado de los dispositivos desde la consola de administración.
- Consultar y gestionar el estado del cifrado.
- Proteger la información almacenada en los dispositivos frente a pérdida, robo o acceso no autorizado.
- Contribuir al cumplimiento de las disposiciones aplicables en materia de protección de datos.

F. CONSOLA DE ADMINISTRACIÓN CENTRALIZADA EN LA NUBE: La solución deberá contar con una consola de administración basada en la nube que permita a la entidad gestionar centralizadamente los diferentes componentes de seguridad incluidos en el servicio.

La consola deberá permitir, como mínimo:

- Configurar las políticas de seguridad.
- Implementar las soluciones de protección.
- Administrar los dispositivos protegidos.

- Realizar gestión remota.
- Consultar el estado de protección de los dispositivos.
- Consultar las amenazas detectadas.
- Consultar los usuarios y dispositivos administrados.
- Consultar y gestionar elementos puestos en cuarentena.
- Administrar las capacidades de protección disponibles.
- Gestionar el cifrado de los dispositivos.
- Obtener información consolidada sobre el estado de seguridad de la infraestructura.
- Acceder a la plataforma mediante navegador web.
- Realizar la administración de manera remota y segura.
- Centralizar la gestión de la seguridad desde un único punto.

La plataforma deberá operar bajo un esquema de administración en la nube, sin requerir infraestructura de hardware adicional por parte de la entidad para la operación de la consola de gestión.

G. MONITOREO, ALERTAS Y VISIBILIDAD: El servicio deberá proporcionar mecanismos que permitan al personal autorizado de la entidad realizar seguimiento sobre los eventos y amenazas de seguridad detectados.

La solución deberá permitir consultar, como mínimo:

- Dispositivos protegidos.
- Usuarios administrados.
- Amenazas detectadas.
- Alertas de seguridad.
- Elementos puestos en cuarentena.
- Estado de las protecciones implementadas.
- Estado de los dispositivos.
- Estado del cifrado de los equipos.
- Información relacionada con eventos de seguridad relevantes.

La solución deberá proporcionar mecanismos de notificación frente a la detección de amenazas, de acuerdo con las capacidades disponibles en la plataforma contratada.

H. ADMINISTRACIÓN Y GESTIÓN REMOTA: La solución deberá permitir la administración remota de los componentes de seguridad desde la consola centralizada. El personal autorizado por la entidad deberá poder realizar, según las funcionalidades disponibles en el licenciamiento contratado:

- Consulta del estado de los dispositivos.
- Administración de políticas de seguridad.
- Consulta de amenazas.
- Gestión de elementos en cuarentena.
- Consulta de usuarios y dispositivos.
- Administración de las capacidades de protección.
- Gestión del cifrado de dispositivos.
- Consulta de eventos y alertas de seguridad.

La plataforma deberá permitir el acceso seguro mediante navegador web desde las ubicaciones autorizadas por la entidad.

I. CONDICIONES Y CARACTERÍSTICAS DEL LICENCIAMIENTO

El servicio contratado deberá proporcionar una solución integral de protección que permita a la entidad gestionar centralizadamente la seguridad de sus dispositivos, usuarios, correo electrónico, servicios de Microsoft 365, almacenamiento en OneDrive y demás componentes incluidos en el alcance del licenciamiento.

El contratista deberá garantizar que las funcionalidades suministradas correspondan al licenciamiento contratado de ESET PROTECT Complete, incluyendo las actualizaciones, mantenimiento y soporte asociados a la vigencia de las licencias, de acuerdo con las condiciones establecidas en el contrato.

De igual forma, el servicio deberá contemplar como mínimo las siguientes capacidades:

- Protección multicapa de ENDPOINTS.
- Protección contra malware.
- Protección contra RANSOMWARE.
- Protección contra amenazas de día cero (0-day).
- SANDBOXING en la nube para análisis de amenazas sospechosas.
- Aprendizaje automático y análisis de comportamiento.
- Protección contra ataques sin archivos.
- Protección contra amenazas persistentes avanzadas.
- Protección de dispositivos móviles incluidos en el licenciamiento.
- Protección de servidores de archivos incluidos en el alcance.
- Protección de Microsoft 365.
- Protección de Exchange Online.
- Protección de OneDrive.
- Protección de SharePoint Online y Microsoft Teams, según el alcance y capacidades del licenciamiento.
- Protección Anti-Phishing.
- Filtrado de spam.
- Protección antimalware para servicios en la nube.
- Cifrado completo de disco para Windows y macOS.
- Administración centralizada desde una consola basada en la nube.
- Gestión remota de los dispositivos.
- Visibilidad sobre amenazas, usuarios, dispositivos y elementos en cuarentena.
- Generación de alertas y notificaciones de seguridad.

NOTA: Las licencias no requieren servicio de instalación por parte del contratista, toda vez que su instalación y activación serán realizadas directamente por el personal técnico de la Entidad en los equipos de cómputo relacionados en la Tabla

2.2.2 CERTIFICACIÓN ESET PARTNER GOLD: El oferente deberá presentar con su propuesta una certificación vigente que acredite su condición de *"ESET Partner Gold"*, expedida directamente por el fabricante ESET o por su distribuidor autorizado para Colombia, dirigida a la Contraloría Departamental del Valle del Cauca, con fecha de expedición y número del proceso de invitación.

La certificación deberá acreditar que el oferente se encuentra autorizado por el fabricante para comercializar y suministrar la solución ESET PROTECT Complete en Colombia y que cuenta con el respaldo correspondiente para garantizar el suministro, implementación, capacitación y soporte técnico de las licencias objeto del presente proceso.

2.3 OBLIGACIONES ESPECIFICAS A DESARROLLAR

a) Iniciar la ejecución del contrato a través de la plataforma SECOP II, una vez cumplidos los requisitos correspondientes para el inicio de la ejecución contractual.
b) Cumplir con la ejecución del contrato dentro del plazo establecido y de conformidad con las condiciones, características y especificaciones técnicas definidas en el numeral 2.2.1 "ESPECIFICACIONES TÉCNICAS" y demás documentos que hacen parte del proceso de contratación.
c) Suministrar y entregar las 250 licencias del antivirus ESET PROTECT Complete, objeto del contrato, de conformidad con las cantidades, características y condiciones técnicas establecidas por la Entidad.
d) Garantizar que las licencias suministradas correspondan a la solución requerida por la Entidad, se encuentren debidamente licenciadas y permitan su activación y uso durante el período de vigencia contratado.
e) Garantizar durante el período de vigencia de las licencias el acceso a las actualizaciones y mecanismos de protección propios de la solución contratada, de conformidad con las condiciones y alcance del licenciamiento adquirido.

f) Tener en cuenta que la instalación y activación de las licencias en los equipos de cómputo será realizada por el personal técnico de la Entidad, por lo cual el contratista no tendrá a su cargo un servicio de instalación, sin perjuicio del soporte técnico que corresponda al licenciamiento adquirido.
g) Informar oportunamente al supervisor del contrato cualquier circunstancia que pueda afectar o retrasar el cumplimiento de las obligaciones contractuales, indicando las causas y las medidas adoptadas para su atención.
h) Presentar la factura o documento equivalente correspondiente, acompañada de los documentos requeridos para el trámite de pago y de la certificación del supervisor sobre el recibo a satisfacción de las licencias suministradas, de conformidad con las condiciones establecidas en el contrato.
i) Acreditar, para efectos del trámite de pago, el cumplimiento de las obligaciones relacionadas con el pago de aportes al Sistema de Seguridad Social Integral y parafiscales, cuando haya lugar a ello, de conformidad con la normativa vigente.

2.4 PLAZO DE EJECUCIÓN

A partir de la suscripción del Acta de Inicio, el contratista contará con un plazo máximo de cinco (5) días hábiles para la entrega e instalación de los ANTIVIRUS, los cuales tendrán una vigencia de doce (12) meses.

2.5 VALOR POSIBLE DEL CONTRATO.

El valor posible del contrato será la suma de DIECINUEVE MILLONES NOVECIENTOS CINCUENTA Y SEIS MIL OCHOCIENTOS TREINTA Y TRES PESOS. ($19.956.833) M/CTE. Incluido IVA o por el valor que resulte adjudicado, incluido, impuestos, tributos, contribuciones aportes parafiscales o cualquier otro descuento que hubiere de realizarse por ley.

2.5.1 FORMA DE PAGO

LA CONTRALORIA pagará al CONTRATISTA el valor que resulte del presente contrato en un solo pago dentro de los diez (10) días hábiles siguiente a la radicación por parte del supervisor del contrato en la Subdirección Administrativa para Recursos Físicos y Financieros de la factura comercial, acompañada de la certificación y/o informe de cumplimiento a satisfacción del servicio que expida el supervisor del contrato y de la verificación de la aprobación de la póliza y del cumplimiento por parte del CONTRATISTA de las obligaciones con el Sistema General de Seguridad social (Sistema de salud, riesgos profesionales, pensiones) y Aportes Parafiscales (Cajas de compensación familiar, ICBF y SENA.

Este valor incluye deducciones adicionales por concepto de estampillas, y descuentos de RETEFUENTE, RETEIVA Y RETEICA. Los proponentes, al preparar sus ofertas, deben tener en cuenta que todo pago que efectúe LA CONTRALORIA será afectado por las retenciones y deducciones que establece la ley o cualquier otra norma obligatoria, para lo cual en la etapa de selección deben de realizar todas las consultas y averiguaciones del caso.

2.6 LUGAR DE EJECUCIÓN

En la ciudad de Cali, en las instalaciones de la Contraloría Departamental del Valle del Cauca, en el Edificio de la Gobernación del Valle del Cauca, Piso 6o. ubicado en la carrera 6ª entre calles 9 y 10.

3. ANÁLISIS DEL MERCADO

3.1. Sector TIC y mercado de soluciones de seguridad informática

El sector de las Tecnologías de la Información y las Comunicaciones –TIC constituye un componente relevante de la economía colombiana y tiene carácter transversal frente a las actividades administrativas, productivas e institucionales. De acuerdo con la Cuenta Satélite de las Tecnologías de la Información y las Comunicaciones –CSTIC del DANE, para 2025 preliminar el valor agregado bruto del sector TIC ascendió a $58,1 billones, registrando un crecimiento del 5,5 % frente a 2024. En el mismo período, el sector representó el 3,47 % del valor agregado bruto nacional. Dentro del sector TIC, los servicios TI registraron la mayor participación, con el 39,4 % del valor agregado bruto del sector.

Estas cifras permiten evidenciar la existencia de un mercado nacional consolidado de bienes y servicios tecnológicos, dentro del cual se encuentran las soluciones de software y las herramientas destinadas a la protección de equipos, sistemas de información y demás activos tecnológicos.

En particular, existe una oferta especializada de soluciones de seguridad informática para estaciones de trabajo, servidores y demás dispositivos conectados a las redes institucionales, que comprende herramientas de antivirus, antimalware, protección de endpoints, detección de amenazas, protección frente a ransomware y administración de mecanismos de seguridad.

En este contexto, la contratación de 250 licencias de una solución de seguridad informática como ESET PROTECT Complete, de acuerdo con las especificaciones técnicas definidas por la Entidad, responde a la necesidad de mantener mecanismos de protección actualizados para los equipos de cómputo institucionales y contribuir a la prevención y detección de código malicioso y otras amenazas informáticas.

3.2. Seguridad de la información y ciberseguridad en las entidades públicas

La creciente dependencia de las tecnologías digitales hace necesario que las entidades públicas adopten medidas orientadas a proteger sus activos de información, sistemas, redes y dispositivos tecnológicos.

En este sentido, el Ministerio de Tecnologías de la Información y las Comunicaciones –MinTIC, mediante la Resolución 02277 de 2025, actualizó el Modelo de Seguridad y Privacidad de la Información –MSPI, incorporando lineamientos alineados con la norma ISO/IEC 27001:2022 y orientados a fortalecer la protección de los activos de información y la continuidad de los servicios.

Así mismo, la Estrategia Nacional de Seguridad Digital 2025-2027 reconoce el incremento de las amenazas en el entorno digital y establece como uno de sus propósitos fortalecer la ciberresiliencia y la gestión de los riesgos cibernéticos.

En consecuencia, mantener mecanismos actualizados de protección para los equipos de cómputo constituye una medida de seguridad orientada a reducir la exposición de la Entidad frente a amenazas como malware, ransomware, spyware, phishing, archivos maliciosos y otras modalidades de ataque que puedan afectar la disponibilidad, integridad y confidencialidad de la información institucional.

3.3. Oferta y condiciones del mercado

El mercado nacional cuenta con proveedores y canales autorizados para la comercialización y renovación de licenciamiento de soluciones de seguridad informática, incluyendo soluciones empresariales de protección de endpoints. Estas soluciones son ofrecidas bajo diferentes modalidades de licenciamiento, vigencia, niveles de protección y esquemas de soporte, de acuerdo con las características y necesidades de cada entidad.

Para la presente contratación, la Entidad requiere 250 licencias de ESET PROTECT Complete, destinadas a los equipos de cómputo relacionados en el inventario institucional, con las características y condiciones técnicas establecidas en el presente estudio previo.

La existencia de diferentes proveedores y canales de comercialización permite adelantar el correspondiente análisis de precios de mercado y establecer las condiciones económicas de la

contratación, garantizando que la adquisición se adelante bajo criterios de eficiencia, economía y selección objetiva.

Fuentes consultadas: *Departamento Administrativo Nacional de Estadística – DANE, Cuenta Satélite de las Tecnologías de la Información y las Comunicaciones – CSTIC; Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, Modelo de Seguridad y Privacidad de la Información – MSPI y Estrategia Nacional de Seguridad Digital 2025-2027.*

4. ANÁLISIS DE LA DEMANDA

Las entidades públicas requieren contar con herramientas tecnológicas que permitan proteger los equipos de cómputo, sistemas de información y demás activos tecnológicos utilizados para el cumplimiento de sus funciones. En este contexto, la demanda de soluciones de seguridad informática comprende tanto la adquisición inicial como, de manera recurrente, la renovación del licenciamiento de soluciones antivirus y de protección de endpoints, con el fin de mantener vigentes las funcionalidades de seguridad, actualización y soporte asociadas a las mismas.

Así mismo, el uso de software en las entidades públicas debe realizarse bajo las condiciones de licenciamiento establecidas por sus titulares de derechos. En este sentido, la Directiva Presidencial No. 02 de 2002 establece instrucciones relacionadas con el respeto al derecho de autor y los derechos conexos en materia de software y contempla la necesidad de que las entidades públicas cuenten con las correspondientes licencias o documentos que acrediten el derecho de uso de los programas de computador utilizados en el desarrollo de sus actividades.

En cuanto a la demanda específica de soluciones de seguridad informática, se identifican antecedentes de contratación pública publicados en el Sistema Electrónico para la Contratación Pública – SECOP, en los cuales diferentes entidades han requerido la adquisición o renovación de licenciamiento de soluciones ESET para la protección de sus equipos tecnológicos.

Entre los antecedentes consultados se encuentra un proceso en el cual una entidad pública requirió la renovación de 400 licencias ESET Endpoint Antivirus y ESET Server Security por un año, evidenciando la existencia de una demanda institucional por soluciones de protección para estaciones de trabajo y servidores.

Así mismo, se identificó un proceso relacionado con la renovación de 70 licencias de antivirus ESET, en el cual se contemplaron funcionalidades orientadas a la protección frente a diferentes amenazas informáticas y a la seguridad de los dispositivos tecnológicos.

De igual manera, se encuentra evidencia de procesos de contratación relacionados con la actualización de licenciamiento de soluciones ESET PROTECT, destinadas a la protección y administración de equipos tecnológicos de entidades públicas.

Los antecedentes señalados permiten evidenciar que la contratación y, particularmente, la renovación periódica de licenciamiento de soluciones de seguridad informática, constituye una necesidad recurrente en las entidades públicas, asociada a la protección de sus activos de información y a la continuidad de sus operaciones.

Para la Contraloría Departamental del Valle del Cauca, la demanda se concreta en la necesidad de renovar 250 licencias de la solución ESET PROTECT Complete, destinadas a los equipos de cómputo relacionados en el inventario institucional, con el propósito de mantener mecanismos actualizados de prevención, detección y protección frente a amenazas informáticas.

En consecuencia, la necesidad identificada se encuentra relacionada con una demanda real y recurrente de las entidades públicas por soluciones de seguridad informática y, particularmente, con la continuidad del licenciamiento requerido para mantener protegidos los equipos de cómputo de la Entidad.

5. ANÁLISIS DE LA OFERTA

5.1. Condiciones generales de la oferta

El mercado de soluciones de ciberseguridad ofrece diferentes alternativas para la protección de equipos de cómputo, servidores y demás activos tecnológicos, mediante esquemas de licenciamiento que pueden variar según el fabricante, número de dispositivos, tiempo de vigencia, funcionalidades incluidas y servicios asociados.

Para este tipo de soluciones, es común encontrar modelos de suscripción por períodos determinados, que permiten mantener vigente la protección, acceder a actualizaciones y utilizar las funcionalidades contempladas en la solución contratada durante el período de licenciamiento.

En el mercado nacional existen fabricantes, distribuidores y canales autorizados que comercializan soluciones de seguridad informática para entidades y organizaciones, por lo que la oferta puede presentar diferentes condiciones técnicas y comerciales de acuerdo con el producto requerido, la cantidad de licencias y el período de suscripción.

5.2. Oferta de ESET PROTECT Complete

ESET cuenta con un portafolio de soluciones de ciberseguridad para organizaciones, dentro del cual se encuentra **ESET PROTECT Complete**, orientado a la protección y administración de los equipos y demás activos tecnológicos incluidos en el licenciamiento.

La solución contempla funcionalidades de protección de endpoints, servidores y otros componentes de seguridad, así como herramientas de administración centralizada y actualización de las capacidades de protección, de acuerdo con las condiciones y alcance del licenciamiento contratado.

El modelo de comercialización de **ESET PROTECT Complete** corresponde a un esquema de suscripción, cuya vigencia se determina de acuerdo con el período contratado y el número de dispositivos o recursos tecnológicos cubiertos.

La comercialización de las soluciones ESET se realiza a través de diferentes canales, incluyendo los mecanismos dispuestos directamente por el fabricante y su red de partners y distribuidores autorizados. En consecuencia, para la adquisición institucional no se limita la oferta a un único proveedor, siempre que los oferentes acrediten las condiciones requeridas para suministrar el licenciamiento legítimo y vigente de la solución.

Adicionalmente, ESET cuenta con un programa de partners que contempla diferentes categorías de vinculación comercial. Para el presente proceso, la condición de **ESET Partner Gold**, cuando sea exigida como requisito, deberá encontrarse debidamente acreditada en los términos establecidos en los documentos del proceso.

5.3. Condiciones que inciden en la oferta

Para la adquisición de las 250 licencias de ESET PROTECT Complete requeridas por la Contraloría Departamental del Valle del Cauca, las condiciones de la oferta pueden variar principalmente en función de:

- Número de licencias o dispositivos a proteger.
- Vigencia del licenciamiento.
- Funcionalidades y componentes incluidos en la solución.
- Condiciones comerciales establecidas por el fabricante y sus canales autorizados.
- Descuentos asociados al volumen de licencias.
- Soporte y servicios adicionales, cuando sean requeridos.

- Compatibilidad con la infraestructura tecnológica de la Contraloría Departamental del Valle del Cauca.
- Condiciones de renovación y continuidad del licenciamiento.

En consecuencia, para determinar las condiciones económicas del presente proceso, se deberán considerar las ofertas disponibles en el mercado para el número de licencias y período de vigencia requeridos, verificando que correspondan a **ESET PROTECT Complete** y que el licenciamiento ofrecido sea legítimo, vigente y susceptible de verificación ante el fabricante.

De acuerdo con lo anterior, se evidencia la existencia de oferta comercial para atender la necesidad de la Contraloría Departamental del Valle del Cauca, correspondiente a la renovación de 250 licencias de ESET PROTECT Complete, conforme con las condiciones técnicas definidas en el presente proceso.

6. ANALISIS ECONOMICO

De conformidad con las disposiciones aplicables a la modalidad de mínima cuantía, para determinar el valor estimado del contrato se efectúa por parte de la Oficina TIC un breve análisis económico que incluye el histórico de procesos con objeto similar adelantados por la entidad, procesos similares en otras entidades y un breve análisis de precios, teniendo en cuenta la necesidad y el objeto a contratar.

Histórico de procesos de contratación con objeto similar ejecutados por la entidad:

AÑO	SERVICIO	VALOR CONTRATO
2022	Renovar 250 licencias nuevas del Antivirus ESET ENDPOINT PROTECTION STANDAR para la Detección y Eliminación de Virus, troyanos, gusanos, adware, spyware, phising, rootkits y archivos maliciosos	$11.600.000
2023	Renovar 250 Licencias del Antivirus ESET ENDPOINT PROTECTION STANDAR para la Detección y Eliminación de Virus, troyanos, gusanos, adware, spyware, phising, rootkits yarchivos maliciosos.	$10.850.000
2024	Renovar 250 Licencias del Antivirus ESET ENDPOINT PROTECTION STANDAR para la Detección y Eliminación de Virus, troyanos, gusanos, adware, spyware, phising, rootkits yarchivos maliciosos	$19.395.000
2025	ADQUIRIR EN CALIDAD DE COMPRAVENTA 250 LICENCIAS DE ANTIVIRUS ESET PROTECT COMPLETE, PARALA DETECCIÓN Y ELIMINACIÓN DE VIRUS, TROYANOS, GUSANOS, ADWARE, SPYWARE, PHISING, ROOTKITS Y ARCHIVOS MALICIOSOS	$19.985.500

b) Consulta SECOP de contratación con similares objetos

ENTIDAD	OBJETO	AÑO	PROCESO	VALOR
FONDO ADAPTACIÓN	Renovación del licenciamiento de antiv ESET-ENDPOINT PROTECT STANDARD.	2026	FA-PS-278-2026	$20.443.384
CORPORACION AUTONOMA REGIONAL CAUCA 12	ACTUALIZACIÓN DE LICENCIAS SOFTWARE ANTIVIRUS ESET ULT VERSION PARA LA PROTECCIÓN CADA UNO DE LOS EQUIPOS CÓMPUTO CLIENTES TERMINALES SERVIDORES DE LA INFRAESTRUCTU TECNOLÓGICA DE LA C	2025	CRC-MC-0012-2025.	$24.990.000
INSTITUTO CULTURA Y TURISMO MANIZALES	PRESTAR EL SERVICIO DE RENOVAC DE TREINTA (30) LICENCIAS ANTIVIRUS ESET ENDPO PROTECTION STANDARD POR UN AÑO, INCLUIDA SU INSTALACIÓN EN EQUIPOS TECNOLÓGICOS DE PROMOTORA DE EVENTO	2025	SMC-016-2025	$16.309.630

C) La Contraloría departamental del Valle del Cauca realizó las siguientes cotizaciones con diferentes proveedores del sector

#Cotización	Valor en COP de licencias por periodos de 1 año	Cantidad (Licencias)
1	$19.990.500	250
2	$19.985.500	250
3	$20.005.000	250

De acuerdo con las cotizaciones obtenidas, se observa que los valores ofertados presentan un comportamiento homogéneo y se encuentran alrededor de los veinte millones de pesos ($20.000.000) para las 250 licencias requeridas por un período de un (1) año.

El promedio aritmético de las cotizaciones analizadas asciende a DIECINUEVE MILLONES NOVECIENTOS NOVENTA Y TRES MIL SEISCIENTOS SESENTA Y SIETE PESOS M/CTE ($19.993.667). En consecuencia, este valor se establece como valor estimado de la contratación, de conformidad con la metodología aplicada en el estudio de mercado y las condiciones técnicas requeridas para la renovación de las 250 licencias de ESET PROTECT Complete por un período de un (1) año.

De conformidad con el estudio de mercado realizado, el presupuesto para esta contratación será por la suma de **DIECINUEVE MILLONES NOVECIENTOS NOVENTA Y TRES MIL SEISCIENTOS SESENTA Y SIETE PESOS M/CTE ($19.993.667),** incluido IVA o por el valor que resulte adjudicado, incluidos impuestos, tributos, contribuciones, aportes parafiscales o cualquier otro descuento que hubiere de realizarse por ley, que están determinados en el Certificado de Disponibilidad Presupuestal No. 2026000135 de fecha 15 de septiembre de 2026, Código de Apropiación 2.1.2.02.02.008.12 – *Servicio de mantenimiento software protección y seguridad*, expedido por la Subdirección Administrativa para Recursos Físicos y Financieros. .

7. ANALISIS DEL RIESGO

En concordancia con lo establecido por el artículo 4 de la Ley 1150 de 2007, respecto del proceso de selección, y el deber de mantener la igualdad o equivalencias entre derechos y obligaciones surgidos al momento de proponer o de contratar de que tratan los artículos 27, 28 de la Ley 80 de 1993, correspondiente a la ecuación contractual y al equilibrio económico, la Contraloría Departamental del Valle del Cauca, considerará que los riesgos previsibles que pueden generar la ruptura del equilibrio económico del contrato objeto del presente proceso de contratación son los siguientes:

De acuerdo al objeto contractual del proceso, se diligenciará la siguiente matriz de riesgos:

N°	Clase	Fuente	Etapa	Tipo	Descripción (Que puede pasar y como puede ocurrir)	Consecuencia de la Ocurrencia del evento	Probabilidad	Impacto	Calificación Total	Prioridad
1	Especifico	Externo	Ejecución	Operacional	Entrega tardía o incumplimiento en el suministro de las 250 licencias de ESET PROTECT Complete, dentro del plazo establecido para la ejecución contractual.	Retraso en la renovación del licenciamiento y afectación de la continuidad de la protección de los equipos de la Contraloría.	1	3	4	Bajo
2	Especifico	Externo	Ejecución	Operacional	Entrega de licencias que no correspondan a las condiciones técnicas requeridas, presenten inconsistencias en su activación o no permitan su utilización durante el período contratado.	Imposibilidad de activar o utilizar las licencias requeridas y afectación de la protección de los equipos de la Contraloría.	2	3	5	Bajo

3	General	Externo	Ejecución	Operacional	Dificultades técnicas o comerciales atribuibles al fabricante o al canal autorizado que afecten la activación, renovación o disponibilidad del licenciamiento contratado.	Retraso en la activación o renovación de las licencias y posible afectación de la continuidad de las herramientas de seguridad informática.	2	4	6	Alto
4	General	Externo	Ejecución	Operacional	Incumplimiento de las obligaciones contractuales por parte del contratista, relacionadas con el suministro del licenciamiento, entrega de la información necesaria para su activación o demás condiciones establecidas en el contrato	Afectación de la ejecución contractual y de la satisfacción de la necesidad de la Contraloría.	1	3	4	Bajo

N°	¿A quién se le asigna?	Tratamiento/Controles a ser implementados	Impacto después del Tratamiento			Afecta el equilibrio económico del contrato	Persona responsable por implementar el tratamiento	Fecha estimada en que se inicia el tratamiento	Fecha estimada en que se termina el tratamiento	Monitoreo y Revisión	
			Probabilidad	Impacto	Calificación Total					Como se realiza el monitoreo	Periodicidad
1	Contratista	Seguimiento permanente al cumplimiento del plazo establecido para el suministro de las 250 licencias y requerimiento oportuno frente a cualquier retraso o novedad que pueda afectar su entrega.	1	2	3	No	Supervisor del Contrato	Duración del Contrato	Inicio de ejecución	Revisión de la entrega de las licencias y de los soportes correspondientes.	Permanente
2	Contratista	Verificación de que las licencias suministradas correspondan a ESET PROTECT Complete, en la cantidad, vigencia y demás condiciones técnicas establecidas, así como de su correcta activación.	1	2	3	No	Supervisor del Contrato	Duración del Contrato	Inicio de ejecución	validación de su activación por parte del personal	Durante la ejecución
3	Contratista	Seguimiento al cumplimiento de las obligaciones contractuales y requerimiento oportuno al contratista frente a cualquier incumplimiento o situación que pueda afectar la ejecución del contrato.	1	2	3	No	Supervisor del Contrato	Inicio de ejecución	Revisión permanente del cumplimiento de las obligaciones contractuales	Verificación de informes, comunicaciones y demás documentos que soporten la ejecución contractual	Permanente

Para Constancia se firma a los veintinueve (29) días del mes de septiembre de 2026

Espacio para Gestión Humana y Financiera

Firmar la opción correspondiente	Observaciones

EDWIN MEJIA CHACON Viable X No viable	La viabilidad se refiere únicamente, a la parte financiera, es decir se cuenta con los recursos para la ejecución contractual.

Firma del Solicitante:

JOHN JAIRO CORTÉS GARCÍA
Jefe Oficina TIC

	Nombre	Cargo
Proyectó:	John Jairo Cortés García	Jefe Oficina TIC
Revisó	Ingrid Julieth Rivera Pino	Profesional Universitario
Aprobó	Diana Lucía Patiño López	Jefe Oficina Jurídica
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.		

CODIGO:M1P2-03	VERSIÓN 1.0