**Estudio previo para el proceso de mínima cuantía No. STIC-IPMC- 42-2025**

## ANALISIS DEL SECTOR

**LA SECRETARIA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN** realiza el **ESTUDIO DEL SECTOR** requerido conforme al artículo 2.2.1.1.1.6.1 del decreto 1082 de 2015 para adelantar el proceso de selección y la consecuente celebración del contrato requerido, de acuerdo a lo dispuesto en cuanto a que las Entidades Estatales en la etapa de planeación deben realizar un análisis para conocer el sector relativo al objeto que se pretende contratar y siguiendo las indicaciones dadas por la Agencia Nacional Colombia Compra Eficiente, mediante la guía para la elaboración de estudios del sector, el Departamento de Risaralda se permite hacer el siguiente análisis soporte del proceso de Subasta Inversa para:

### 1. OBJETO: "ADQUISICIÓN DE LICENCIAS PARA EL FIREWALL DEL SISTEMA DE SEGURIDAD PERIMETRAL DEL DEPARTAMENTO DE RISARALDA"

El Análisis del Sector cubre los siguientes puntos principales

A. Análisis del Mercado.
B. Estudio Demanda
C. Estudio de la Oferta
D. Estudio de Mercado

## INTRODUCCIÓN

De acuerdo con lo dispuesto en el Decreto 1082 de 2015 y la guía de la Agencia Nacional de Contratación - Colombia Compra Eficiente para la elaboración de Estudios del Sector (V2 24-06-2022), se procedió a realizar el análisis del sector económico y de los posibles oferentes.

La Entidad Estatal en cumplimiento de lo previsto en el Articulo 2.2.1.1.1.6.1 del Decreto 1082 de 2015 que dispone que las entidades estatales en la etapa de planeación deben realizar un análisis para conocer el sector relativo al objeto que se pretende contratar y siguiendo las indicaciones dadas por la Agencia Nacional Colombia Compra Eficiente, mediante el Instructivo en el SECOP, el Departamento de Risaralda por medio de la Secretaria de Tecnologías de la Información y la Comunicación, se permite hacer el siguiente análisis del sector.

El Departamento, para adelantar el respectivo estudio, efectuó las consultas pertinentes en la página web Colombia Compra Eficiente -SECOP (www.colombiacompra.gov.co), lo anterior con el objetivo de tomar como referencia las empresas que participan activamente en procesos de contratación, con similar objeto, modalidad de selección, presupuesto

asignado, plazo y lugar de ejecución. Se determinan las variables para tener en cuenta en el presente proceso de acuerdo con las especificaciones técnicas.

## 1. Análisis de mercado

### Aspectos generales del sector

Nuestro país ha experimentado un notable avance en la adopción de tecnologías de la información y las comunicaciones, superando la velocidad de otros países latinoamericanos. En este contexto, el Ministerio de Tecnologías de la Información y las Comunicaciones ha establecido como su principal objetivo impulsar la inversión, la innovación y la apropiación de tecnologías en la ciudadanía, las empresas y el Gobierno. Este impulso busca fortalecer el sector, generando un impacto positivo en el desarrollo económico, político y social del territorio.

Como líder en la iniciativa pública, el Ministerio se encarga de fomentar la inversión en el sector TIC y liderar la transformación digital del Estado. Esto se logra a través del diseño, formulación, adopción y promoción de políticas, planes, programas y proyectos alineados con la Constitución Política y la Ley. El objetivo final es cerrar la brecha digital, contribuir al desarrollo integral de la Nación y mejorar el bienestar de los colombianos.

El sector de Tecnologías de la Información y las Comunicaciones (TIC) en Colombia se enfoca en la formación de talento, el desarrollo de aplicaciones y software, y la conectividad.

Formación de talento:

- El Ministerio TIC formará el talento necesario para impulsar la transformación digital.
- Se llevarán servicios y contenidos pedagógicos innovadores a los maestros, estudiantes y padres de familia.

Desarrollo de aplicaciones y software:

- Se fomentará el desarrollo de aplicaciones, software y contenidos para impulsar la apropiación de las TIC.

Conectividad:

- Se facilitará el acceso y uso de las TIC en todo el territorio nacional.
- Se prestarán servicios de acceso comunitario a Internet en centros poblados de municipios PDET.

Los indicadores disponibles en tema del sector TIC, especialmente del e-Commerce,

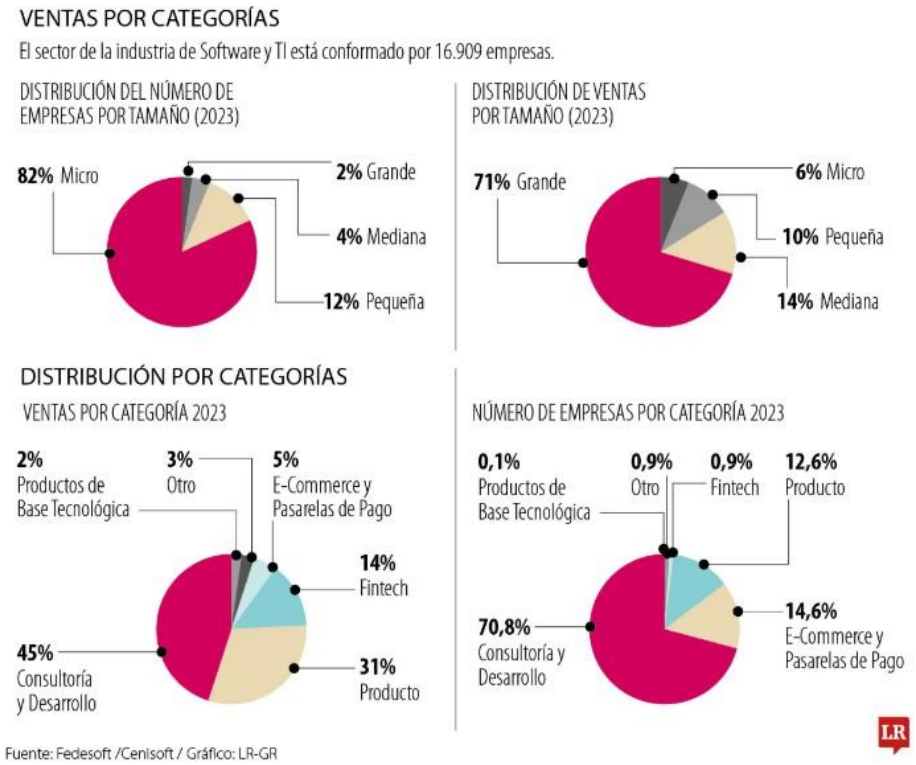
software, conectividad y mercado laboral digital, revelan una continuidad sólida del crecimiento del sector digital en 2025:

- El eCommerce muestra un ritmo fuerte, con crecimiento previsto del 18 – 19%.
- El software sigue aportando de manera significativa al PIB y amplía sus exportaciones.
- La expansión de la conectividad y 5G impulsa una infraestructura digital clave para otros segmentos.
- La alta demanda de talento TI refleja la aceleración del ecosistema digital en el país.

Según cifras de Fedesoft, el sector representó 3,7% del PIB nacional en 2023, lo que refleja un alto incremento frente a la participación de menos de 1% registrada en 2013

La evolución es notoria. Mientras que en 2016 el sector generó ventas por $18,3 billones, en 2023 las ventas subieron a $57,2 billones, un incremento de 25,7% en comparación con el año anterior. Este ritmo de expansión ha permitido que el sector triplique sus ingresos en un período relativamente corto.

El panorama del tejido empresarial en el sector muestra una estructura sólida. En total, existen casi 17.000 empresas operando en el ámbito de Software y TI.



Un aspecto crítico para el desarrollo futuro del sector es la digitalización de los procesos empresariales. Los diagnósticos recientes indican que, a pesar de los avances, el nivel de digitalización presenta aún un margen de mejora. Las empresas del sector han obtenido un puntaje promedio de 52 puntos sobre 100 en implementación digital y 41 puntos en gestión de la digitalización. Este panorama sugiere que, aunque el sector está avanzando, la mayoría de las empresas aún deben optimizar sus procesos digitales para alcanzar un nivel de madurez más alto. Los sectores mejor puntuados en digitalización son el software y TI, con un puntaje de 64,6 en implementación digital; y el sector financiero, con 60,1; mientras que sectores más rezagados incluyen el siderúrgico y astillero, con puntuaciones de 31,1 y 14,4, respectivamente.

## DATOS MACROECONÓMICOS

El comportamiento del Índice de Precios al Consumidor IPC, tuvo una variación anual del 5.22% para el año 2025, los mayores aportes a la variación anual se registraron en las divisiones de: Alojamiento, agua, electricidad, gas y otros combustibles, Transporte, Restaurantes y hoteles, Alimentos y bebidas no alcohólicas y Bienes y servicios diversos.

*Información enero 2025*

**Índice de Precios al Consumidor (IPC)**

Variación anual y mensual
Total nacional
2024 - 2025 (enero)

| IPC | enero | | | |
|---|---|---|---|---|
| | Variación mensual | | Variación anual | |
| | 2024 | 2025 | 2024 | 2025 |
| IPC total | 0,92 | **0,94** | 8,35 | **5,22** |

**Fuente:** DANE, IPC

En el mes de enero de 2025, el IPC registró una variación de 0,94% en comparación con diciembre de 2024, cuatro divisiones se ubicaron por encima del promedio nacional (0,94%): Restaurantes y hoteles (1,90%), Transporte (1,71%), Alimentos y bebidas no alcohólicas (1,62%) y por último, Salud (1,04%). Por debajo se ubicaron: Muebles, artículos para el hogar y para la conservación ordinaria del hogar (0,70%), Bebidas alcohólicas y tabaco (0,64%), Bienes y servicios diversos (0,54%), Alojamiento, agua, electricidad, gas y otros combustibles (0,39%), Educación (0,00%), Prendas de vestir y calzado (-0,15%), Recreación y cultura (-0,18%) y por último, Información y comunicación (-0,19%).

Desde la perspectiva del enfoque de producción en el Producto Interno Bruto (PIB), el software colombiano ha alcanzado ventas anuales por un monto de $21 billones. Con la ambiciosa

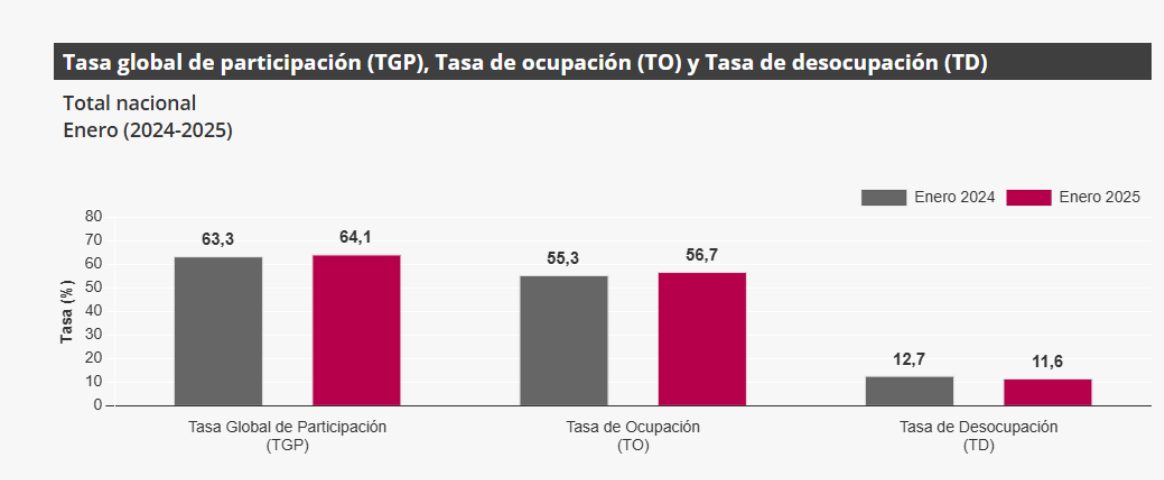
meta de lograr que este sector represente el 5% del PIB para el año 2025, Colombia se encuentra en una posición relevante en la región, impulsada por la aceleración de procesos de transformación empresarial debido a la coyuntura actual.

Según William Corredor, CEO de Open International (2022), la tecnología se ha convertido en la única alternativa para el funcionamiento continuo de las empresas en estos tiempos. Ante los retos que enfrentarán las industrias del futuro, la transformación digital sigue siendo crucial para superarlos, y el software desempeña un papel fundamental para la recuperación económica. Corredor destaca las oportunidades inmensas que tiene Colombia, no solo en programas y servicios tecnológicos, a pesar de los desafíos existentes en el sector.

Además de ser una oportunidad comercial significativa, el sector de software en Colombia se destaca por su baja tasa de desempleo, según datos del Banco Mundial. Se estima que se necesitan seis millones de ingenieros en el mundo, lo que subraya la demanda continua en este campo.

El avance hacia un Estado digital, con documentos y certificaciones electrónicas, proporciona un panorama favorable para el nuevo año. Colombia cuenta con un talento excepcional, demostrado por las más de 1.000 empresas de desarrollo de software en el país. Además, el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) ha liderado diversas acciones, proyectos y estrategias que se han convertido en hitos para el desarrollo y la transformación del país en conectividad, ecosistemas de innovación y educación digital.

Por otro lado, para el mes de enero de 2025, la tasa de desocupación del total nacional fue 11,6%, lo que representó una disminución de 1,0 puntos porcentuales respecto al mismo mes de 2024 (12,7%). La tasa global de participación se ubicó en 64,1%, mientras que en enero de 2024 fue 63,3%. Finalmente, la tasa de ocupación fue 56,7%, lo que representó un aumento de 1,4 puntos porcentuales respecto al mismo mes del año anterior (55,3%).



En enero de 2025, la tasa de desocupación en el total de las 13 ciudades y áreas metropolitanas fue 11,1%, lo que representó una disminución de 1,3 puntos porcentuales respecto a enero de 2024 (12,4%). La tasa global de participación se ubicó en 65,7% y la tasa de ocupación en 58,4%, estas tasas en el mismo mes del año anterior fueron 65,9% y 57,7%, respectivamente.

**El Dólar (TRM):**

Dólar año 2024 y 2025 (de octubre a octubre)

| | |
|---|---|
| Octubre 30, 2024 | $4,367.39 |
| Noviembre 29, 2024 | $4,406.16 |
| Diciembre 30, 2024 | $4,401.98 |
| Enero 30, 2025 | $4,195.60 |
| Febrero 27, 2025 | $4,123.10 |
| Marzo 31, 2025 | $4,192.57 |
| Abril 29, 2025 | $4,227.32 |
| Mayo 30, 2025 | $4,106.79 |
| Junio 29, 2025 | $4,069.67 |
| Julio 30, 2025 | $4,154.79 |
| Agosto 30, 2025 | $4,018.41 |
| Septiembre 30, 2025 | $3,901.29 |
| Octubre 30, 2025 | $3,885.29 |

El precio del dólar en Colombia para el día jueves 30 de Octubre del 2025 subió 10.45 Pesos, correspondiente a un aumento del 0.27% con respecto al día anterior. La TRM disminuyó un 11.04% (482.1 Pesos) en referencia al mismo día del año anterior y se redujo un 0.41% (16 Pesos) comparando con el mismo día del mes anterior.




**ESTRATEGIAS DEL SECTOR TIC**

En la actualidad las Tecnologías de la Información y las Comunicaciones (TIC) han recobrado gran importancia y se reconoce el impacto que pueden generar frente a la competitividad y desarrollo económico -social del territorio. El uso de estas tecnologías hoy se encuentra activa en el desempeño de la cotidianidad de la población, así como ha generado cambios significativos en la forma como interactúan las personas, ha cambiado y mejorado la manera como las personas pueden aprender esto genera un impacto positivo para estudiantes y docentes.

Han promovido la inclusión de persona que habían estado alejadas de la Tecnología, potencializo su uso en el sector público y privado, el sector productivo encontró un gran aliado para comercializar sus productos, las empresas, encontraron una nueva forma de configurar sus procesos y a aumentar la productividad, la rapidez con que se realizan y al mismo tiempo reducir los costos de transacción. Es por lo anterior que desde el Gobierno Nacional se ha considerado varias estratégicas TIC que permitan fomentar la competitividad y la igualdad de oportunidades en Colombia. Por ello el ministerio TIC ha trazado su ruta de trabajo en tres ejes de cambio, en el cual se invita a que se estructuren los planes de desarrollo territorial de los periodos 2024-2027 y prioriza estrategias en el sector, que vayan encaminadas en los siguientes aspectos:

• Conectividad: Reducción de la brecha digital y la pobreza
• Tecnología que transforma: Ecosistemas de innovación
• Educación Digital

Enfocandose en Tecnología que transforma: Ecosistemas de Innovación Con la transformación digital y tecnología con propósito se impulsen la eficiencia administrativa, impacta positivamente la calidad de vida de los ciudadanos y, en general, los habitantes del

territorio nacional y la competitividad del país, se promueve la generación de valor público a través de la transformación digital del Estado, de manera proactiva, confiable, articulada y colaborativa entre los Grupos de Interés y permitir el ejercicio de los derechos de los usuarios del ciberespacio. Se prioriza las siguientes estrategias: • Fomentar ecosistemas de innovación como mecanismo para acelerar la transformación digital del sector público y del sector privado. (Servicio de apoyo financiero al desarrollo de soluciones tecnológicas) La innovación pública digital que introduzca nuevas soluciones basadas en tecnologías digitales para un desarrollo sostenible y el mejoramiento del desempeño del sector público. Apoyo económico para que emprendedores desarrollen soluciones tecnológicas base TIC para diferentes sectores a través de convocatorias. Se entiende por solución tecnológica el desarrollo de software o hardware que permita satisfacer necesidades de sectores específicos de la economía

**IMPORTANCIA DEL SECTOR TI Y LAS TECNOLOGIAS EMERGENTES**

El concepto de gobierno digital representa una transformación fundamental en la manera en que los gobiernos abordan el desarrollo y la administración de sus funciones. Desde la definición de objetivos administrativos medibles hasta la mejora de la prestación de servicios públicos, desde la toma de decisiones basada en datos hasta la promulgación de políticas respaldadas por evidencia, y desde el fomento de una mayor responsabilidad y transparencia gubernamental hasta la generación de una mayor confianza pública, los gobiernos están aprovechando de manera transformadora el poder de las tecnologías de la información y las tecnologías digitales emergentes.

En cuanto a la financiación de la investigación y desarrollo (I+D), el sector empresarial lidera con un 54%, seguido por la financiación pública con un 22%, y las Instituciones de Educación Superior ocupan el tercer lugar con aproximadamente el 10%. Este panorama destaca la relevancia del sector privado en la generación de nuevo conocimiento y la necesidad de fortalecer la inversión pública y la contribución de las instituciones educativas.

En la era de la transformación, los gobiernos se encuentran sometidos a una presión creciente para mejorar la experiencia de los ciudadanos mediante la provisión de servicios más eficientes, procesos seguros, y el suministro y acceso a la información. En este contexto, las tecnologías emergentes desempeñan un papel fundamental para modernizar el sector gubernamental. En los últimos años, diversos factores de riesgo social han destacado la necesidad imperativa de que los gobiernos implementen políticas e intervenciones destinadas a ayudar a las poblaciones vulnerables. Este enfoque comienza por comprender mejor las necesidades ciudadanas, basándose en circunstancias individuales y cotidianas.

El escrutinio y la supervisión han aumentado considerablemente, ya que los ciudadanos exigen una inversión más efectiva de sus impuestos y una gestión transparente de los servicios públicos. La disminución de la confianza pública, generada por fallas en políticas y servicios gubernamentales, contribuye a que la población desconfíe de la capacidad del gobierno para atender sus necesidades. Este debilitamiento de la confianza y del "capital

social" tiene consecuencias significativas, erosionando la autoridad gubernamental y el compromiso cívico. Además, impacta en la eficacia del gobierno y mina la confianza de inversores, empresas y consumidores.

La adopción estratégica de tecnologías emergentes en el sector gubernamental no solo puede abordar estos desafíos, sino que también puede impulsar la transparencia, la eficiencia y la participación ciudadana. Al aprovechar las innovaciones tecnológicas, los gobiernos pueden responder de manera más efectiva a las demandas ciudadanas, mejorar la entrega de servicios, y reconstruir la confianza pública en su capacidad para abordar las necesidades y desafíos de la sociedad en constante evolución.

En este contexto, las tecnologías emergentes, como el uso de la inteligencia artificial, ofrecen beneficios significativos para abordar los factores de riesgo mencionados. Estas tecnologías permiten la prestación de servicios eficientes al reducir errores, mejorar la fiabilidad y proporcionar mayor transparencia. La calidad de los datos y la optimización de tareas se ven mejoradas, lo que facilita la toma de decisiones más efectiva. La inteligencia artificial también tiene la capacidad de analizar datos para prever eventos futuros, contribuyendo así a una toma de decisiones más informada.

La digitalización previa de procesos es clave en este contexto, ya que sienta las bases para aprovechar plenamente los beneficios de la inteligencia artificial. Además, estas tecnologías pueden ser utilizadas para el seguimiento de postulantes y atenciones ciudadanas, así como para personalizar procesos de atención. La clasificación de huellas dactilares y faciales para autenticación de identidad es otro ejemplo de cómo estas tecnologías emergentes pueden fortalecer la seguridad y la eficiencia en los servicios gubernamentales

**IMPORTANCIA DE FIREWALL**

La importancia del firewall en una entidad pública es fundamental para garantizar la seguridad, confidencialidad y disponibilidad de la información institucional**.**

El firewall es una herramienta esencial dentro de la infraestructura tecnológica de una entidad pública, ya que actúa como una barrera de protección entre la red interna institucional y las redes externas (como Internet). Su función principal es controlar y filtrar el tráfico de datos, permitiendo únicamente las comunicaciones autorizadas y bloqueando accesos no seguros o malintencionados.

## A. Protección de la información institucional

Las entidades públicas manejan información sensible relacionada con ciudadanos, contratos, finanzas y procesos administrativos. El firewall previene accesos no autorizados y evita la filtración de datos confidenciales.

### B. Prevención de ataques cibernéticos

Los firewalls ayudan a detectar y bloquear intentos de intrusión, ataques de denegación de servicio (DDoS), virus, malware y otras amenazas comunes, garantizando la continuidad operativa y la integridad de los sistemas.

### C. Cumplimiento normativo y de políticas de seguridad

En el sector público, existen normas como el Modelo de Seguridad y Privacidad de la Información (MSPI) y lineamientos del MinTIC que exigen la implementación de mecanismos de seguridad perimetral, entre ellos los firewalls. Esto asegura el cumplimiento de las políticas nacionales de ciberseguridad y gestión de riesgos.

### D. Control del uso de recursos tecnológicos

El firewall permite monitorear y gestionar el tráfico en la red, controlando el acceso a sitios o servicios no autorizados. Esto contribuye a un uso eficiente de los recursos tecnológicos y a mantener la productividad del personal.

### E. Garantía de disponibilidad y continuidad del servicio

Al bloquear amenazas externas y gestionar el flujo de datos, el firewall contribuye a mantener la disponibilidad de los sistemas críticos, asegurando la prestación continua de los servicios públicos digitales.

El uso de un firewall en una entidad pública no es solo una medida técnica, sino una obligación estratégica y legal para proteger la infraestructura tecnológica del Estado. Su correcta implementación refuerza la confianza ciudadana, salvaguarda los activos de información y asegura la operación segura y transparente de los servicios públicos.

## 2. Aspecto Técnico

El Departamento de Risaralda planea realizar un proceso de contratación por la modalidad de Invitación Pública de Mínima Cuantía y el Tipo de Contrato es Compraventa para "**ADQUISICIÓN DE LICENCIAS PARA EL FIREWALL DEL SISTEMA DE SEGURIDAD PERIMETRALDEL DEPARTAMENTO DE RISARALDA".**

El objeto agrupa las necesidades esenciales para la adquisición y el mantenimiento de componentes críticos de la infraestructura de seguridad y conectividad de la entidad. Esto incluye la adquisición de licencias de firewall y el soporte y mantenimiento continuo. La implementación de estas acciones es fundamental para garantizar la protección, el rendimiento y la disponibilidad de los sistemas de TI.

De acuerdo con la necesidad del Departamento, a continuación, se relaciona el equipo y/o los elementos requeridos:

### 2.1.1. Descripción técnica

Por lo anterior y dado que, la Secretaría de Tecnologías de la Información y la Comunicación a través de la Dirección de Informática y Sistemas Tecnológicos requiere adquirir el licenciamiento y soporte continuado del firewall Fortigate 401F para el Departamento de Risaralda. La implementación de estas acciones es fundamental para garantizar la protección, el rendimiento y la disponibilidad de los sistemas de TI.

Esta medida asegurará que la Entidad esté preparada para enfrentar los desafíos de ciberseguridad del presente y futuro cercano. La adquisición dl licenciamiento del firewall NGFW Fortgate 401F no solo fortalecerá la defensa contra amenazas cibernéticas, sino que también optimizará el rendimiento de la red y asegurará el cumplimiento con las normativas vigentes.

Componentes del Objeto:

Adquisición y por ende Renovación del Licenciamiento del Firewall:

- Objetivo: Asegurar el acceso continuo a actualizaciones, parches de seguridad y soporte técnico especializado para el firewall NGFW.
- Beneficios: Mantener el firewall en su estado óptimo, mejorar la protección contra nuevas amenazas y garantizar el cumplimiento normativo.

## 3. ASPECTO REGULATORIO

De conformidad con el objeto del proceso de contratación el Departamento de Risaralda identifico que en Colombia existe regulación para tener en cuenta en relación con el bien, obra o servicio a contratar y el segmento de la economía en el cual se encuentran los proveedores, dentro de las cuales tenemos:

El Plan Nacional de Desarrollo 2022 – 2026 “Colombia Potencia Mundial de la Vida”

CAPÍTULO III SEGURIDAD HUMANA Y JUSTICIA SOCIAL
SECCIÓN III: GARANTÍA DE DERECHOS COMO FUNDAMENTO DE LA DIGNIDAD HUMANA Y CONDICIONES PARA EL BIENESTAR

**ARTÍCULO 142°.** CONECTIVIDAD DIGITAL PARA CAMBIAR VIDAS. Para efectos de promover la conectividad digital como un generador de oportunidades, riqueza, igualdad y productividad, el Ministerio de Tecnologías de la Información y las Comunicaciones adelantará las siguientes medidas:

1. Llevar conectividad digital a zonas vulnerables y apartadas, y mejorar la cobertura y calidad de los servicios de telecomunicaciones, a través de diferentes tecnologías y compartición de infraestructura.
2. Hacer del Internet y de las tecnologías digitales un instrumento de transformación social.
3. Desplegar infraestructura para mejorar la conectividad digital del país con redes neutras, cables submarinos, fibra óptica, tecnología satelital, entre otras tecnologías, mediante diversos mecanismos, entre ellos la coinversión entre el Estado y los actores privados.
4. Promover la eliminación de barreras por parte de las entidades territoriales y/o nacionales para el despliegue de redes de telecomunicaciones.
5. Adelantar la asignación del espectro a través de esquemas y condiciones que maximicen el bienestar social y la compartición de este recurso, promoviendo su uso eficiente.
6. Fortalecer a los pequeños prestadores de los servicios de telecomunicaciones con el fin de aportar en el cierre de la brecha digital.

**ARTÍCULO 143°.** TRANSFORMACIÓN DIGITAL COMO MOTOR DE OPORTUNIDADES E IGUALDAD. El Ministerio de Tecnologías de la Información y las Comunicaciones diseñará e implementará una estrategia integral para democratizar las TIC y desarrollar la sociedad del conocimiento y la tecnología en el país, mediante las siguientes medidas:
1. Promover la consolidación de una sociedad digital para que todos los ciudadanos tengan las herramientas necesarias para hacer del Internet y de las tecnologías digitales un instrumento de transformación social.
2. En articulación con el Ministerio de Educación Nacional promover el acceso por parte de docentes, niños, niñas y adolescentes a nuevas fuentes de conocimiento, a través del uso de tecnologías digitales, que les permita desenvolverse en una sociedad altamente tecnológica.
3. Establecer programas de alfabetización digital con enfoque étnico, participativo, de género y diferencial.
4. Promover estrategias para la identificación, prevención y control de todo tipo de violencias en entornos digitales, en coordinación con el Ministerio de Educación Nacional, con énfasis en mujeres, grupos étnicos y niñas, niños y adolescentes.
5. Implementar iniciativas de transformación digital como herramienta para la productividad, la generación de empleo, la dinamización de la economía en las regiones y la potencialización de la economía popular.
6. Fortalecer el Gobierno Digital para tener una relación eficiente entre el Estado y el ciudadano, que lo acerque y le solucione sus necesidades, a través del uso de datos y de tecnologías digitales para mejorar la calidad de vida.
7. Promover un entorno digital seguro para generar confianza en el uso y apropiación de las TIC. ARTÍCULO

**ARTÍCULO 144°.** FORTALECIMIENTO DEL SECTOR TIC. El Ministerio de Tecnologías de la Información y las Comunicaciones promoverá la consolidación de la Industria TIC nacional como un motor de crecimiento, empleo y desarrollo para el país, mediante las siguientes medidas:

1. Fortalecer los servicios del sector TIC como telecomunicaciones, televisión, radiodifusión sonora, y postales.
2. Fortalecer la industria digital, así como los contenidos, el desarrollo de software, las aplicaciones, el emprendimiento y la innovación para la productividad, generando nuevos empleos e ingreso en las regiones.
3. Fortalecer los contenidos audiovisuales multiplataforma y de radio en los medios públicos, garantizando la libertad de expresión y resaltando los valores culturales de cada región del país.
4. Impulsar el uso de software libre, código abierto y tecnologías digitales emergentes.

## 4. ANÁLISIS DE LA DEMANDA

### 4.1. COMPORTAMIENTO DEL GASTO HISTÓRICO

**Adquisiciones pasadas del bien, obra o servicios de la Entidad Estatal**
Se relaciona los procesos realizados por la Entidad Estatal similares al presente objeto contractual.

| ENTIDAD | OBJETO | MODALIDAD DE SELECCIÓN | PROCESO NO | DURACION | VALOR |
|---|---|---|---|---|---|
| GOBERNACIÓN DE RISARALDA | LICENCIAMIENTO DE SOFTWARE | Selección abreviada por subasta inversa | STIC-SASI-020-2023 | 30 (Días) | $149.500.000 |
| GOBERNACIÓN DE RISARALDA | ADQUIRIR LICENCIAMIENTO DE SOFWARE ANTIVIRUS PARA LA ADMINISTRACION DEPARTAMENTAL | Selección abreviada subasta inversa | STIC-SASI-031-2021 | 30 (Días) | $69.949.152 |
| GOBERNACIÓN DE RISARALDA | ADQUISICIÓN DE LICENCIAS PARA EL FIREWALL DEL SISTEMA DE SEGURIDAD PERIMETRAL DEL DEPARTAMENTO DE RISARALDA | Invitación pública de Mínima Cuantía | STIC-IPMC-45-2024 | 30 (Días) | $83.352.656 |

### 4.2. CONTRATACIONES SIMILARES DE OTRAS ENTIDADES ESTATALES

Se presenta un análisis de procesos de selección adelantados por otras Entidades del Estado realizando una búsqueda en el Sistema Electrónico para la Contratación Pública – SECOP I y SECOP II, encontrando que diferentes entidades estatales han adelantado procesos de selección para contratar y que en los mismos ha existido pluralidad de oferentes con la capacidad e infraestructura necesaria para ejecutar; el objeto a contratar guarda similitud con el presente proceso. A continuación, la información recopilada.

| ENTIDAD | OBJETO | MODALIDAD DE SELECCIÓN | PROCESO NO | DURACION | VALOR |
|---|---|---|---|---|---|
| UNIVERSIDAD DEL TOLIMA | RENOVACIÓN LICENCIAMIENTO PARA LOS EQUIPOS DE SEGURIDAD PERIMETRAL Y FIREWALL DE APLICACIONES WEB WAF PARA PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN DE LA UNIVERSIDAD DEL TOLIMA Y RENOVACION DEL SOPORTE DE ACCESPOINT FORTIAP-U231F | CONTRATACIÓN RÉGIMEN ESPECIAL | 916-2023 | 314 DIAS | 359.380.000 |
| ALCALDIA DE DOSQUEBRADAS | RENOVACION DEL LICENCIAMIENTO DE ANTIVIRUS PARA LOS EQUIPOS DE COMPUTO, ADEMAS DE RENOVAR LA TECNOLOGIA DE SEGURIDAD PERIMETRAL UTM NEXT GENERATION FIREWALL CAPA 7 CON SU RESPECTIVO LICENCIAMIENTO, PARA LA GESTION DE AMENAZAS INFORMATICAS DE LA ALCALDÍA MUNICIPAL DE DOSQUEBRADAS | SELECCIÓN ABREVIADA SUBASTA INVERSA | SI-132-2023 | 5 DIAS | 198.980.564 |
| CONTRALORÍA DEPARTAMENTAL DEL ATLÁNTICO | ADQUISICION LICENCIAS ANTIVIRUS, Y DE ACCESS POINT, SOFTWARE OFIMATICO Y BACKUP: INSTALACIÓN, CONFIGURACIÓN Y SOPORTE; PRUEBAS DE FUNCIONALIDAD IPV6, ADQUISICIÓN DE SUSCRIPCIÓN DE CORREO ELECTRÓNICO, SERVICIO DE WEB HOSTING PARA LA CONTRALORÍA DEPARTAMENTAL DEL ATLÁNTICO | SELECCIÓN ABREVIADA SUBASTA INVERSA | SIP-025-2023 | 365 DIAS | 222.366.953 |
| MUNICIPIO SANTA ROSA DE OSOS | ADQUISICIÒN DE LICENCIAMIENTO Y ACOMPAÑAMIENTO TÉCNICO UTP PROTECCIÓN 24X7 A 1 AÑO PARA SOLUCIÓN DE SEGURIDAD PERIMETRAL HARDWARE FIREWALL FORTIGATE 100F, PARA LA ADMINISTRACIÓN MUNICIPAL DE SANTA ROS | MÍNIMA CUANTÍA | CMC DOS 054 2025 | DOCE (12) MESES | $19.000.000 |

Al consultar los procesos de selección similares adelantados por la diferentes Entidades, se puede evidenciar que cada una define las enumeraciones técnicas e ítems a contratar, acordes a las necesidades propias determinadas por su misión institucional e infraestructura tecnológica. De igual manera al contratar el licenciamiento de uso y operación para el firewall Fortigate 401F existe la necesidad de su contratación, para la debida operación de la seguridad digital y las

operaciones ciberseguras.

Igualmente, se puede inferir que en el mercado y específicamente en el sector al cual se hace referencia se pueden encontrar proveedores con la capacidad técnica para suministrar dicho licenciamiento y soporte que se requiere contratar en el presente proceso, lo que garantiza la pluralidad de oferentes.

## 5. ANÁLISIS DE LA OFERTA

Este segmento describe el proceso de caracterización, que tiene como propósito contextualizar las variables que impactan el mercado del sector al que pertenece la categoría de la compra pública a evaluar, del presente proceso.

### 5.1. Proveedores del bien, obra o servicio

Se relacionan los posibles oferentes de la obra, bien o servicio del sector que registran dentro del Sistema de Contratación Pública Colombiano -SECOP II-, que puedan cumplir con el objeto del presente proceso en cuanto a tema de Firewall.

| RAZON SOCIAL |
|---|
| INGENIERIA TELEMATICA S.A.S. |
| WEXLER SAS |
| AXIS TI |

Es importante resaltar que los procesos de contratación en Colombia han sufrido un incremento considerable en su valor, teniendo en cuenta los comportamientos que han tenido las variables económicas como la Inflación, la DTF y la TRM las cuales han venido creciendo considerablemente y tienen una relación directamente proporcional.

### 5.2 ESTUDIO DE MERCADO

Frente a la necesidad y dentro del estudio de mercado la Secretaria de Tecnologías de la Información y la Comunicación solicito a varios proveedores la cotización del servicio para “El Departamento de Risaralda planea realizar un proceso de contratación por la modalidad de Invitación Pública de Mínima Cuantía y el Tipo de Contrato es Compraventa para “**ADQUISICIÓN DE LICENCIAS PARA EL FIREWALL DEL SISTEMA DE SEGURIDAD PERIMETRAL DEL DEPARTAMENTO DE RISARALDA**”

El objeto agrupa las necesidades esenciales para la adquisición y el soporte de componentes críticos de la infraestructura de seguridad y conectividad de la entidad. Esto incluye la renovación de licencias de antivirus, y el soporte y mantenimiento continuo. La implementación de estas acciones es fundamental para garantizar la protección, el rendimiento y la disponibilidad de los

sistemas de TI.

Para ellos desde la Dirección de Informática y Sistemas Tecnológicas se solicitaron diferentes cotizaciones, de las cuales tres (3) empresas presentaron ofertas y con estas se establece el precio de referencia.

Para el cálculo del valor promedio del proceso se siguen las recomendaciones dadas en la guía para la elaboración de estudios del sector ANCP.CCE: deben sumarse todos los valores y dividir el resultado por el número total de propuestas.

Las alternativas se analizan a continuación.

**FIREWALL**

| NOMBRE DE LA EMPRESA CONSULTADA | VALOR |
|---|---|
| INGENIERIA TELEMATICA S.A.S. | $91.724.201 |
| WEXLER SAS | $87.025.694 |
| AXIS TI | $83.860.691 |
| **PROMEDIO** | **$87.536.862** |

**5.3 Cálculo promedio Estudio de Mercado**

Para la realización del cálculo anterior se tuvieron en cuenta las cotizaciones y la hoja de cálculo remitidas por la Dirección de Informática y Sistemas Tecnológicos al momento de solicitar la proyección del presente documento.

Teniendo en cuenta el análisis realizado previamente, al valor total del presupuesto que se requiere para el proceso que se pretende contratar para antivirus es por la suma de **OCHENTA Y SIETE MILLONES QUINIENTOS TREINTA Y SEIS MIL OCHOCIENTOS SESENTA Y DOS PESOS M/CTE ($87.536.862) INCLUIDO IVA** y demás cargos en que pueda incurrir el contratista.

**6. Análisis de riesgos**

La entidad estructuró dicho análisis a través de la matriz de riesgos que hace parte integral del presente estudio previo. (Ver anexo No 2)

**ESTUDIO PREVIO**

**LA SECRETARIA DE TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACIÓN** Realiza el **ESTUDIO PREVIO** requerido conforme al artículo 25, numeral 7 de la Ley 80 de 1993, y el

artículo 2.2.1.2.1.5.1 y siguientes del decreto 1860 de 2021.

## 1. Descripción de la necesidad.

La Secretaría de Tecnologías de la Información y la Comunicación a través de la Dirección de Informática y Sistemas Tecnológicos es la responsable de fomentar, adoptar, implementar y administrar el Ecosistema Digital del Departamento, con el fin de incentivar la disminución de las brechas de conocimiento en los ámbitos empresarial, social, educativo, investigativo, salud, seguridad, gubernamental, entre otros, basado en el fortalecimiento de la productividad y la competitividad de la región, facilitando el acceso, uso y apropiación de las TIC a todo nivel en el departamento de Risaralda, apoyando a los municipios que no cuenten con la capacidad fiscal ni administrativa.

La Administración Departamental cuenta con un centro de datos donde se ubica toda la infraestructura tecnológica, la cual está compuesta por servidores, máquinas virtuales, almacenamiento SAN (Storage Area Network) y NAS (Network Attached Storage), conmutadores y puntos de acceso inalámbricos, motores de bases de datos y sistemas de información. Por lo tanto, es requerida las licencias de uso y operación para la solución de seguridad perimetral (Unified Threat Management [UTM] actualmente Fortigate 600D y que ha sido renovado a Fortigate 401F) que garantice la protección de los dispositivos mencionados al igual que los sistemas de información. Se busca mitigar el riesgo de que esta información quede expuesta a posibles ataques tanto externos como internos en la red.

Es importante explicar que es UTM o Unified Threat Management es un tipo de solución de seguridad de red que se utiliza para proteger a una organización de diversas amenazas cibernéticas. En la Gobernación de Risaralda, es importante tener un UTM, con las debidas licencias de uso y operación, a razón de las siguientes razones:

**Protección contra amenazas de seguridad**: El UTM combina múltiples funciones de seguridad en una sola solución, como firewall, antivirus, detección de intrusiones, prevención de intrusos y filtrado de contenido. Al tener todas estas funciones integradas en una sola solución, se puede proporcionar una protección más sólida contra diversas amenazas cibernéticas.

**Gestión centralizada:** Al tener un UTM, se puede gestionar la seguridad de la red de la Gobernación de Risaralda de manera centralizada. Esto significa que todas las políticas de seguridad, actualizaciones de software y alertas de seguridad se pueden administrar desde una sola consola, lo que simplifica la gestión y mejora la eficiencia.

**Reducción de costos**: El UTM puede ayudar a reducir los costos de seguridad de la red en la Gobernación de Risaralda, ya que no se necesita adquirir y gestionar varias soluciones de seguridad individuales. Además, el UTM también puede ayudar a reducir los costos asociados con la resolución de problemas de seguridad de la red, ya que se pueden detectar y mitigar rápidamente las amenazas.

El UTM combina varias funciones de seguridad en una sola solución integrada, como firewall, antivirus, detección de intrusiones, prevención de intrusos y filtrado de contenido. A continuación, se describen con más detalle las funciones y características del UTM y cómo se utilizan en la Gobernación de Risaralda:

**Firewall**: El firewall es una función central del UTM que se utiliza para bloquear el tráfico no autorizado y mantener segura la red de la Gobernación de Risaralda. El firewall del UTM utiliza reglas y políticas para controlar el tráfico de entrada y salida de la red, y también puede realizar inspección profunda de paquetes para detectar y bloquear amenazas avanzadas.

**Antivirus**: El UTM también incluye un motor antivirus que se utiliza para detectar y eliminar virus y malware en la red de la Gobernación de Risaralda. El motor antivirus del UTM puede escanear todo el tráfico de la red en busca de amenazas y también puede actualizar automáticamente las definiciones de virus para mantenerse al día con las últimas amenazas.

**Detección de intrusiones**: El UTM también puede detectar y alertar sobre intrusiones en la red de la Gobernación de Risaralda utilizando técnicas de detección de intrusiones (IDS) y prevención de intrusiones (IPS). El IDS puede detectar posibles intrusiones mediante la monitorización de los patrones de tráfico, mientras que el IPS puede bloquear las intrusiones en tiempo real.

**Filtrado de contenido**: El UTM también puede realizar filtrado de contenido para bloquear el acceso a sitios web no deseados o peligrosos en la red de la Gobernación de Risaralda. El filtrado de contenido se puede configurar para bloquear sitios web por categoría, como redes sociales, juegos, pornografía, etc.

**Gestión centralizada**: El UTM permite a los administradores de red de la Gobernación de Risaralda gestionar todas las funciones de seguridad desde una sola consola centralizada. La consola del UTM proporciona una vista única de toda la red, incluyendo estadísticas y alertas de seguridad, lo que facilita la gestión y la toma de decisiones.

Ahora, es importante explicar los riesgos a los que se expone la Gobernación, sino se renueva el licenciamiento para el UTM:

**Malware y virus**: Sin el debido licenciamiento sobre el UTM, la red de la Gobernación de Risaralda estaría expuesta a virus y malware que pueden propagarse a través de la red y afectar a múltiples sistemas. Los virus y el malware pueden robar datos, dañar archivos, bloquear el acceso a sistemas o incluso tomar el control completo de un dispositivo.

**Intrusiones de red**: Los ciberdelincuentes pueden intentar acceder a la red de la Gobernación de Risaralda de forma ilegal, utilizando técnicas como la ingeniería social, la suplantación de identidad, el escaneo de puertos y otros métodos de ataque. Sin el debido licenciamiento sobre el UTM, la organización podría no detectar estas intrusiones y los ciberdelincuentes podrían tener acceso a información confidencial o causar daños a la infraestructura.

**Ataques DDoS**: Los ataques de denegación de servicio distribuidos (DDoS) pueden utilizar múltiples dispositivos para inundar la red de la Gobernación de Risaralda con tráfico, lo que provoca una interrupción del servicio. Un UTM correctamente licenciado puede ayudar a mitigar estos ataques y mantener la disponibilidad de la red.

**Phishing**: Los ataques de phishing pueden engañar a los usuarios para que compartan información confidencial, como contraseñas o información de confidencial. Si la Gobernación de Risaralda no tiene un UTM debidamente licenciado, los usuarios de la organización podrían ser víctimas de estos ataques, lo que podría poner en riesgo los datos y sistemas de la organización.

**Pérdida de datos**: Sin el debido licenciamiento sobre el UTM, la Gobernación de Risaralda podría ser más vulnerable a la pérdida de datos. Esto podría ocurrir debido a malware, errores humanos, fallas en el hardware, ataques de ciberdelincuentes u otras causas. La pérdida de datos puede ser costosa y perjudicial para la reputación de la organización.

Luego de describir las funcionalidades técnicas, operativas y de uso, se hace indispensable indicar que las mismas funcionan si el dispositivo UTM 401F, cuenta con Licencias de uso y operación debidamente adquiridas y registradas a nombre de la Gobernación de Risaralda, para el correcto despliegue, operación, contención y respuesta de seguridad informática y ciberseguridad ante los ataques e incidentes que se puedan llegar a presentar.

De manera seguida es necesario describir los componentes técnicos que componen el licenciamiento y que permiten la debida protección a los activos de información de la Entidad, así como la mitigación bajo el concepto de minimizar los riesgos informáticos en las operaciones ciberseguras de la Gobernación de Risaralda.
**Licencia Enterprise para el UTM FortiGate 401F:** Obedece al documento legalmente descrito, entregado y registrado a la Gobernación de Risaralda, donde se puede constatar que puede utilizar y cuenta con las funcionalidades activadas para el dispositivo UTM FortiGate 401F propiedad del Departamento de Risaralda durante un periodo de tiempo definido, y que permite a la Entidad, hacer uso de las funcionalidades a saber:

**IPS:** (Intrusion Prevention System) es una función de seguridad esencial que se incluye en las licencias Enterprise para el FortiGate 401F. El IPS es un sistema que monitorea y protege activamente la red de la Gobernación contra ataques y amenazas cibernéticas.

**Advanced Malware Protection (AMP)** es una función de seguridad avanzada que se incluye en las licencias enterprise para el FortiGate 401F. AMP está diseñado para detectar y proteger contra malware y amenazas avanzadas que pueden pasar desapercibidas para las soluciones de seguridad tradicionales.

**Application Control** es una función de seguridad incluida en las licencias enterprise para el FortiGate 401F. Proporciona un control granular sobre las aplicaciones que se ejecutan en la red

de la Gobernación, lo que te permite definir políticas específicas para el uso y acceso a diferentes aplicaciones.

**Web & Video Filtering** es una característica incluida en las licencias Enterprise para el FortiGate 401F que permite filtrar y controlar el acceso a sitios web y contenido de video en la red de la Gobernación de Risaralda. Proporciona una capa adicional de seguridad y control al permitir gestionar el acceso a recursos en línea y garantizar un entorno de navegación seguro.

**Antispam** es una función de seguridad incluida en las licencias Enterprise para el FortiGate 401F que se utiliza para detectar y filtrar el correo no deseado o no solicitado, comúnmente conocido como spam. El objetivo del Antispam es minimizar el impacto del spam en red de la Gobernación y evitar que los usuarios sean inundados con correos electrónicos no deseados.

**Security Rating (calificación de seguridad)** es una función que evalúa el estado de seguridad de la red de la Gobernación y proporciona una puntuación o clasificación en función de diversos factores. Estos factores pueden incluir la configuración del UTM FortiGate 401F, las políticas de seguridad implementadas, las vulnerabilidades conocidas, la exposición a amenazas conocidas y otras métricas relacionadas con la seguridad de los activos de información de la Gobernación de Risaralda.

**IoT Detection (Detección de IoT)** es una funcionalidad específica que está incluida en la licencia Enterprise del dispositivo de seguridad de red FortiGate 401F. Esta característica está diseñada para identificar y controlar los dispositivos de Internet de las cosas (IoT) que están o puedan conectarse a la red de la Gobernación de Risaralda.

**Industrial Security (Seguridad Industrial)** es una característica específica que está incluida en la licencia Enterprise del dispositivo de seguridad de red FortiGate 401F. Esta función está diseñada para proporcionar una capa adicional de seguridad para entornos industriales o de automatización, como plantas de fabricación, infraestructuras críticas y sistemas de control industrial (ICS).

**FortiConverter Svc** es una herramienta y servicio de conversión y migración de configuraciones de seguridad que ofrece Fortinet, incluida en la licencia Enterprise. Su propósito principal es ayudar a los usuarios a migrar de forma eficiente las políticas y configuraciones de seguridad de dispositivos de otros fabricantes a la plataforma de seguridad de Fortinet, incluyendo los dispositivos FortiGate 401F.

**24x7 FortiCare** es un servicio de soporte técnico de Fortinet que se ofrece como parte de la licencia Enterprise para el UTM FortiGate 401F. Proporciona asistencia y mantenimiento continuo las 24 horas del día, los 7 días de la semana para ayudar a la Gobernación de Risaralda, como licenciatario a maximizar el rendimiento y la seguridad de su infraestructura de red.

**Licencia FortiAnalyzer-VM Support**. Esta función permite el soporte y la integración de

FortiAnalyzer-VM con el FortiGate 401F. Es una solución tecnológica de administración y análisis de registros de seguridad que ofrece el dispositivo si cuenta con la licencia. Proporciona una plataforma centralizada para la recopilación, análisis y generación de informes de registros y eventos de seguridad de la infraestructura de red de la Gobernación de Risaralda. Esto significa que los registros y eventos de seguridad generados por el FortiGate 401F pueden enviarse al FortiAnalyzer-VM para su almacenamiento, análisis y generación de informes detallados.

Dicho licenciamiento incluye:

**OS Updates,** Las actualizaciones del sistema operativo para FortiAnalyzer-VM son proporcionadas por Fortinet para mantener el software actualizado con las últimas características, mejoras de rendimiento, correcciones de errores y compatibilidad con nuevas tecnologías. Estas actualizaciones pueden incluir mejoras en la funcionalidad, la seguridad y la estabilidad del sistema operativo.

**FortiCare Premium Web Support y FortiCare Premium Comprehensive Support**, proporciona una asistencia técnica de alta calidad y rápida a la Gobernación, que utiliza FortiAnalyzer-VM en combinación con FortiGate 401F. Algunos de los aspectos clave de este servicio incluyen:

- Acceso al portal web de soporte: La Gobernación de Risaralda tiene acceso al portal web de soporte técnico de Fortinet, donde pueden registrar y realizar un seguimiento de sus casos de soporte. Este portal proporciona una forma conveniente de comunicarse con el equipo de soporte técnico de Fortinet.
- Respuesta prioritaria: El servicio de soporte Premium garantiza una respuesta rápida y prioritaria a los casos presentados por la Gobernación de Risaralda. Esto significa que la Entidad Territorial recibe una atención más rápida para resolver problemas y obtener asistencia técnica.
- Soporte técnico especializado: El soporte Premium FortiCare incluye acceso a un equipo de ingenieros de soporte técnico altamente capacitados y certificados en los productos de Fortinet. Estos expertos pueden brindar asesoramiento, orientación y soluciones a los desafíos técnicos específicos relacionados con FortiAnalyzer-VM y FortiGate 401F.
- Actualizaciones y mejoras: El servicio de soporte Premium también incluye acceso a las últimas actualizaciones de firmware y mejoras de software para FortiAnalyzer-VM y FortiGate 401F. Esto garantiza que la Gobernación tengan acceso a las últimas características y correcciones de errores para mejorar el rendimiento y la seguridad de su infraestructura de red interna para la operación de los procesos.

Entendido lo anterior se requiere que el proveedor además de suministrar las licencias, cuente con recurso humano idóneo y competente para brindar unos excelentes servicios de soporte, todo bajo una estricta política de control en el gasto público; dado que la Dirección de Informática y Sistemas tecnológicos de la Secretaría de Tecnologías de la Información y la Comunicación no cuenta con el personal suficiente para cumplir con sus funciones, se requiere contratar los servicios requeridos.

## 2. Conveniencia y oportunidad.

El Decreto No. 1042 del 12 de octubre de 2017, por el cual se dictan normas generales sobre la estructura administrativa y las funciones generales de las dependencias de la Administración Departamental de Risaralda, define en el Artículo 20, la estructura de la Administración Departamental de Risaralda, Sector Central; en el ítem 2.3.1 la Dirección de Informática y Sistemas Tecnológicos como una dependencia interna de la Secretaría de las TIC que ejerce las competencias relacionadas con la infraestructura informática y tecnológica orientada al uso y aprovechamiento de los sistemas de información de la Administración departamental, teniendo entre otras funciones planificar y mantener la arquitectura de software y hardware de la Administración departamental y apoyar la existente o para adquisición en los municipios que corresponda, en aras de aprovechar los cambios tecnológicos y asimilar rápidamente la evolución de la tecnología.
Los Next-Generation Firewalls (NGFW) FortiGate 401F brindan alto rendimiento, seguridad avanzada multicapa y una mejor visibilidad para proteger contra los ciberataques al mismo tiempo que reducen la complejidad. Los firewalls FortiGate están diseñados especialmente con procesadores de seguridad para permitir la mejor protección contra amenazas y el mejor rendimiento para el tráfico cifrado de SSL de la industria.

El FortiGate 401F es un dispositivo de seguridad de red de nivel empresarial que ofrece múltiples características y funcionalidades para garantizar la seguridad y el rendimiento de la red. Las características técnicas clave del FortiGate 401F, que funcionan correctamente si tiene las licencias de uso y operación, son las siguientes:

### 1. Rendimiento y Especificaciones de Hardware

- **Throughput del Firewall**: Hasta **70 Gbps**. Esto mide la velocidad máxima a la que el dispositivo puede procesar tráfico sin ninguna inspección o políticas activas.
- **Rendimiento del Firewall con inspección de tráfico SSL**: Hasta **10 Gbps**. Este valor es crucial dado que muchas comunicaciones modernas están cifradas con SSL/TLS.
- **Rendimiento del Firewall con IPS activado**: Hasta **12 Gbps**. Refleja la capacidad del FortiGate para analizar el tráfico en busca de patrones sospechosos, mediante su sistema de prevención de intrusiones (IPS).
- **Rendimiento del Firewall con Application Control y Antivirus activado**: Hasta **6.5 Gbps**. Esto mide la capacidad del FortiGate para controlar aplicaciones y escanear el tráfico en busca de malware y amenazas.
- **Capacidad máxima de sesiones concurrentes**: Hasta **10 millones**. Esto representa la cantidad de conexiones simultáneas que el FortiGate 401F puede manejar.
- **Nuevas conexiones por segundo**: Hasta **500,000**. Indica la capacidad de establecer nuevas conexiones en tiempo real, importante para entornos con altos volúmenes de transacciones.

### 2. Características de Seguridad

- **Firewall de próxima generación (NGFW)**: Integra funcionalidades avanzadas de inspección y protección como la **prevención de intrusiones (IPS)**, **control de aplicaciones** y **filtrado web**.
- **Inspección de tráfico cifrado (SSL/TLS)**: Capacidad de inspeccionar tráfico cifrado para detectar amenazas ocultas en las comunicaciones cifradas.
- **Protección contra amenazas avanzadas**: Utiliza la tecnología **FortiGuard** para obtener actualizaciones constantes sobre las últimas amenazas y vulnerabilidades.
- **Prevención de amenazas basada en IA**: Fortinet utiliza la inteligencia artificial para analizar patrones y comportamientos anómalos en la red.
- **FortiSandbox**: Integración con un entorno de análisis de amenazas en sandboxing para detectar malware de día cero (zero-day).

**3. Interfaces y Conectividad**

- **Puertos 10GE (SFP+)**: El FortiGate 401F cuenta con **8 puertos SFP+ de 10 Gbps** para conectividad de alta velocidad.
- **Puertos 1GE (RJ45)**: Dispone de **12 puertos RJ45 de 1 Gbps** para conectividad a redes locales (LAN) y otros dispositivos.
- **Módulo de expansión (FortiFlex)**: Tiene soporte para **módulos de expansión** adicionales que permiten personalizar la conectividad y agregar más interfaces.
- **HA (Alta disponibilidad)**: Soporta **HA activo-activo** y **activo-pasivo**, lo que permite la configuración de clústeres para alta disponibilidad y redundancia en la red.

**4. Virtualización y Segmentación**

- **VLANs**: Soporta la creación de múltiples **VLANs** (Redes de área local virtuales), lo que permite la segmentación lógica de la red para una mayor seguridad y control.
- **VDOMs (Dominios Virtuales)**: Hasta **10 VDOMs** (Virtual Domains), lo que permite particionar un solo dispositivo físico en múltiples instancias virtuales. Esto es útil en entornos multiarrendatarios o cuando se necesita un mayor control de seguridad en diferentes departamentos o funciones.

**5. Administración y Control**

- **FortiOS**: El FortiGate 401F funciona con **FortiOS**, el sistema operativo de seguridad de Fortinet, que proporciona una consola unificada para gestionar todas las funciones de seguridad, incluyendo firewall, VPN, control de aplicaciones, IPS, y más.
- **Soporte para SD-WAN**: Incluye capacidades avanzadas de **SD-WAN** (red de área amplia definida por software), lo que permite optimizar la conectividad en múltiples enlaces de red y mejorar el rendimiento de las aplicaciones empresariales.
- **Gestión centralizada**: Puede integrarse con **FortiManager** para una gestión centralizada de múltiples dispositivos FortiGate.

- **Acceso a FortiCloud**: Soporte para el servicio de nube **FortiCloud**, que permite la gestión remota, almacenamiento y análisis de registros en la nube.

**6. Seguridad Avanzada de Red**

- **VPN (Redes Privadas Virtuales)**: Soporte para múltiples tipos de VPN, incluyendo **IPSec** y **SSL VPN**, para asegurar la conectividad remota. Permite un rendimiento de hasta **30 Gbps en IPSec**.
- **Segmentación de red**: Permite la creación de políticas para segmentar redes según perfiles de usuario, departamento o aplicación, reforzando la seguridad y controlando el acceso.

**7. Soporte y Actualizaciones**

- **FortiGuard Security Services**: Integración con los servicios de FortiGuard, que incluyen actualizaciones automáticas para amenazas como malware, firmas IPS, bases de datos de filtrado web, entre otros.
- **Actualizaciones de firmware y parches**: Proporciona acceso a las últimas actualizaciones de FortiOS y correcciones de seguridad críticas.

**8. Consumo y Rendimiento Energético**

- **Consumo eléctrico**: Aproximadamente **160W** de consumo máximo, lo que lo convierte en un dispositivo eficiente en términos de energía.
- **Alimentación**: Admite redundancia de fuente de alimentación para garantizar que el dispositivo siga funcionando en caso de falla de una de las fuentes.

**9. Capacidades de Informes y Monitoreo**

- **FortiAnalyzer**: Compatible con **FortiAnalyzer** para análisis avanzado y generación de informes detallados sobre eventos de seguridad, tráfico de red y otros aspectos operativos.
- **Monitoreo en tiempo real**: Proporciona visibilidad en tiempo real del tráfico de red, aplicaciones, usuarios y dispositivos conectados, con alertas en caso de detectar anomalías.

**Necesidad de la Licencia Enterprise para el UTM FortiGate 401F**
Es necesario indicar que para la Gobernación es oportuno y prioritario adquirir las licencias de uso y operación para la debida aplicación de seguridad informática y de las operaciones ciberseguras, dando alcance a los objetivos técnicos de los componentes de las licencias a saber:

**1. FortiGuard Security Services**
Este es un conjunto de servicios de seguridad en la nube proporcionados por Fortinet que actualizan constantemente las bases de datos y protegen tu dispositivo contra amenazas emergentes. Incluye:

**Antivirus**: Escanea el tráfico en busca de malware, virus y troyanos en tiempo real.
Función: Detecta y elimina malware en archivos, tráfico de red y sitios web.
Importancia: Protege contra ataques maliciosos que pueden comprometer la red.

**IPS (Intrusion Prevention System):** Detecta y bloquea intentos de intrusión, como ataques de fuerza bruta y exploits.
Función: Prevenir ataques contra vulnerabilidades en servidores, aplicaciones y dispositivos.
Importancia: Protege tu infraestructura contra amenazas conocidas y emergentes.

**Filtrado Web**: Controla y restringe el acceso a sitios web peligrosos o no deseados, basado en categorías y listas de reputación.
Función: Bloquear el acceso a sitios de phishing, malware o contenido no deseado.
Importancia: Mejora la seguridad y productividad al controlar el acceso a internet.
**Control de Aplicaciones**: Identifica y controla el uso de aplicaciones en la red.
Función: Permite o bloquea aplicaciones específicas en la red, como redes sociales, juegos, etc.
Importancia: Mejora la seguridad y gestión del ancho de banda.

**Seguridad de Email**: Protege los correos electrónicos de la red contra amenazas como spam, phishing y malware.
Función: Filtrar correos electrónicos maliciosos antes de que lleguen a los usuarios.
Importancia: Previene ataques a través de vectores de phishing o adjuntos maliciosos.

**Sandboxing**: Análisis de archivos sospechosos en un entorno controlado antes de permitir su entrada a la red.
Función: Detectar amenazas avanzadas y malware de día cero.
Importancia: Añade una capa adicional de seguridad para amenazas que no son detectadas por métodos tradicionales.

**DNS Filtering**: Filtra las solicitudes DNS para prevenir que los usuarios accedan a sitios web maliciosos.
Función: Impide la conexión a dominios que se sabe que son maliciosos.
Importancia: Mejora la protección contra ataques de phishing y malware.

**2. FortiCare Support (Soporte Técnico)**
Este componente ofrece acceso a soporte técnico de Fortinet y actualizaciones de firmware y software. Existen varios niveles de FortiCare:

**Soporte 24x7**: Acceso a soporte técnico las 24 horas del día, los 7 días de la semana.
Función: Brinda asistencia técnica en caso de problemas, fallos de configuración o consultas técnicas.
Importancia: Garantiza que la red esté siempre operativa con un tiempo de respuesta rápido en caso de problemas críticos.
**Reemplazo avanzado de hardware**: En caso de que el dispositivo falle, se garantiza el

reemplazo de hardware de manera rápida.
Función: Asegura que, si ocurre una falla de hardware, el dispositivo sea reemplazado en el menor tiempo posible.
Importancia: Minimiza el tiempo de inactividad en caso de fallas de hardware, crucial para empresas con alta dependencia de la disponibilidad de red.

**Actualizaciones de firmware**: Permite acceder a las últimas versiones de FortiOS, que incluyen mejoras de seguridad y nuevas funciones.
Función: Mantiene el firewall actualizado con las últimas características y parches de seguridad.
Importancia: Asegura que el FortiGate 401F esté protegido contra vulnerabilidades recién descubiertas y mejora el rendimiento.

**Parches de seguridad**: Actualizaciones rápidas para corregir vulnerabilidades críticas detectadas en el sistema.
Función: Proteger el dispositivo de cualquier vulnerabilidad que pueda comprometer la seguridad.
Importancia: Mantener el dispositivo seguro frente a amenazas emergentes.

**24x7 FortiCare** La Gobernación debe tener acceso a un equipo de soporte técnico dedicado que está disponible en todo momento para ayudar a resolver problemas, responder preguntas y brindar orientación técnica.
Asistencia en caso de fallos o interrupciones: En caso de problemas críticos o fallos en el dispositivo FortiGate 401F, el soporte técnico de 24x7 FortiCare puede proporcionar una respuesta rápida y efectiva para solucionar los problemas y minimizar el tiempo de inactividad y pérdida de protección a los activos de información de la Gobernación de Risaralda.
Acceso a actualizaciones y parches de seguridad: La Gobernación de Risaralda con la licencia Enterprise, con 24x7 FortiCare recibe acceso a las últimas actualizaciones de firmware, parches de seguridad y mejoras de software para asegurarse de que su dispositivo FortiGate 401F esté protegido contra las últimas amenazas y vulnerabilidades.
Recursos y herramientas adicionales: El servicio de soporte 24x7 FortiCare también proporciona acceso a una amplia gama de recursos, como documentación técnica, guías de implementación, bases de conocimientos y herramientas de diagnóstico, que maximizan la capacidad de proteger los activos de información.

**Licencia FortiAnalyzer-VM Support**

Dicho licenciamiento incluye:
- Almacenamiento y análisis centralizado de registros: FortiAnalyzer-VM proporciona un repositorio central para almacenar y analizar registros de eventos de seguridad generados por el FortiGate 401F. Esto facilita la identificación y el análisis de amenazas y patrones de tráfico maliciosos en toda la red de la Gobernación.

- Generación de informes y auditorías: La plataforma FortiAnalyzer-VM permite generar informes personalizados y detallados sobre el estado de seguridad de la red, las tendencias de amenazas, el cumplimiento normativo y otras métricas relevantes.
- Análisis de comportamiento y detección de amenazas avanzadas: FortiAnalyzer-VM utiliza técnicas avanzadas de análisis y correlación de eventos para identificar anomalías y patrones de tráfico maliciosos en la red de la Entidad Territorial. Esto incluye la detección de amenazas persistentes avanzadas (APT) y el análisis de comportamiento para identificar actividades sospechosas.

De acuerdo a lo anterior, se requiere que estas condiciones particulares, las cuales se predican de la necesidad que tiene la entidad, guarden estricta relación con la **FICHA TÉCNICA** del proceso, la cual se relaciona a continuación:

**ESPECIFICACIONES TECNICAS**

**LICENCIAMIENTO**

**Aclaraciones Generales:**

✓ El inicio de vigencia del licenciamiento debe empezar a partir de la instalación de la licencia en el dispositivo respectivo

✓ El proponente seleccionado debe brindar soporte técnico preventivo, correctivo y equipo de contingencia modalidad 7x24x365

**Aclaraciones:**

✓ Las licencias de software deben ser registradas a nombre del **"Departamento de Risaralda"** y con el correo electrónico institucional sistemas@risaralda.gov.co , a menos que se indique otro destinatario en la ficha técnica respectiva.

**Certificaciones:**

✓ El proponente debe suministrar certificación expedida por el fabricante de los licenciamientos ofertados, no mayor a 30 días, donde conste que el proponente es distribuidor autorizado de la marca ofertada.

**ELEMENTOS**

**Listado de Elementos de Software**

| | |
|---|---|
| Licencia de Seguridad Perimetral | 3 |
| Licencia de Sistema de Registros y Estadísticas | 4 |

**FICHA TECNICA**

| | |
|---|---|
| Grupo | 1 |
| Ítem | 1 |
| Código UNSPSC | 43233200 |
| Elemento | Licencia de Seguridad Perimetral |
| Fabricante | Fortinet |
| Producto | Fortigate |
| Referencia | 401F |
| Cantidad | 1 |
| CARACTERISTICAS | |
| Descripción | Requeridas |
| Características | |
| Licencias Incluidas | Coterm FG4H1FT922903651 (Coterm End Date:2026-11-27) (Last Expiry Date:2025-11-27) Licencia de suscripción (Enterprise Protection) para el FortiGate-401F |
| Programas Incluidos | IPS/IDS<br>Advanced Malware Protection Application Control<br>Web & Video Filtering Antispam<br>Security Rating IoT Detection Industrial Security<br>FortiConverter Service FortiCare 7x24x365, AI-based Inline Malware Prevention |
| Esquema de Licenciamiento | Enterprise |
| Idioma | Multi-Idioma |
| Versión | N/A |
| Edición | Enterprise |
| Vigencia | 12 meses a partir de la instalación de la licencia en el dispositivo respectivo |
| Nota | El licenciamiento debe ser registrado a nombre de: “Departamento de Risaralda” y bajo la cuenta de correo electrónico institucional: sistemas@risaralda.gov.co |
| Garantía y Soporte | Garantía y soporte de fábrica por 1 año |

| **Soporte técnico** | |
|---|---|
| **Servicios Incluidos** | Renovación, Configuración y transferencia de conocimiento, Soporte preventivo y correctivo modalidad 7x24 por un año |
| **Soporte Técnico** | Esquema: 7 x 24 x 365<br>Modalidad: Presencial, Remoto, Telefónico<br><br>**Contar con certificación:** emitida por la fábrica con nivel de membresía SELECT, ADVANCE O EXPERT. este requisito se debe acreditar con certificados.<br><br>**Contar con los siguientes perfiles: a.** Ingeniero de sistemas o afines con Certificación NSE7 (Network Security Architect) de Fortinet y Certified Solution Specialist OT Security y con maestría en seguridad informática. Para lo cual el oferente aportara los siguientes documentos: Tarjeta profesional, certificación del COPNIA, hoja de vida de la función pública, experiencia como ingeniero de sistemas de mínima 5 años y 2 años de experiencia relacionada con Fortinet NSE 7 Network Security Architec.<br>**b.** Ingeniero de sistemas o afines con Certificación Professional Public Cloud Security Fortinet Para lo cual el oferente aportara los siguientes documentos: Tarjeta profesional, certificación del COPNIA, hoja de vida de la función pública, experiencia como ingeniero de sistemas de mínima 3 años y 1 años de experiencia relacionada con la certificación solicitada.<br><br>**Equipo de Contingencia:** El proveedor deberá contar con un equipo de contingencia de características iguales o superiores al dispositivo FortiGate FG-401F, disponible para su reemplazo inmediato en caso de falla crítica del equipo principal, acreditándolo mediante carta de disponibilidad suscrita por el representante legal y factura de compra del mismo a nombre del proponente. |
| **Nota** | El licenciamiento debe ser registrado a nombre de: "**Departamento de Risaralda**" y bajo la cuenta de correo electrónico institucional: **sistemas@risaralda.gov.co** |

## FICHA TECNICA

| | |
|---|---|
| Grupo | 1 |
| Ítem | 2 |
| Código UNSPSC | 43233200 |
| Elemento | Licencia de Sistema de Registros y Estadísticas |
| Fabricante | Fortinet |
| Producto | FortiAnalyzer |
| Referencia | FAZVM64 |
| Serial | FAZ-VM0000128212 |
| Cantidad | 1 |
| CARACTERISTICAS | |
| Descripción | Requeridas |
| Características | |
| Licencias Incluidas | 1 Licencia de suscripción para el FortiAnalyzer-VM Support 7x24x365 FortiCare Contract (for 1-6 GB/Day of Logs)<br>1 Licencia de suscripción para el FortiGuard Indicator of Compromise (IOC) (for 1-6 GB/Day of Logs)<br>1 Licencia de suscripción para el FortiAnalyzer SOC service (1-6 GB/Day of Logs) |
| Programas Incluidos | Plataforma de logs y reportes |
| Esquema de Licenciamiento | Enterprise |
| Idioma | Multi-Idioma |
| Versión | N/A |
| Edición | Enterprise |
| Vigencia | 12 meses a partir de la instalación de la |

| | |
|---|---|
| | licencia en el dispositivo respectivo |
| Compatibilidad | FAZ-VM0000128212 |
| Nota | El licenciamiento debe ser registrado a nombre de: “Departamento de Risaralda” y bajo la cuenta de correo electrónico institucional: sistemas@risaralda.gov.co |
| Garantía y Soporte | Garantía y soporte de fábrica por 1 año |

Acorde con el Plan de Desarrollo “RISARALDA EQUITATIVA E INCLUYENTE” se llevará a cabo mediante DIMENSIÓN 4 BUEN GOBIERNO - GESTIÓN Y FORTALECIMIENTO INSTITUCIONAL; buscando alcanzar Sistemas de información actualizados y mantener al 100% la operatividad de la infraestructura informática del Departamento en el cuatrienio, en consecuencia la información digital generada en dicha infraestructura requiere que se le garantice la seguridad; evitando ataques de virus informáticos en la Administración Departamental, por lo cual es conveniente y oportuno adelantar la contratación del suministro de licenciamiento de Software Antivirus para la Administración Departamental.

**Nombre del Proyecto:** FORTALECIMIENTO DE LA INFRAESTRUCTURA TI EN EL DEPARTAMENTO DE RISARALDA

**Código:** 2024003660036

**Actividad:** SUMINISTRAR APLICACIONES PARA FORTALECER LA INFRAESTRUCTURA TI EL DEPARTAMENTO DE RISARALDA

**Certificado de Conveniencia, Oportunidad y Registro de Actividades No. 5377 del 29/10/2025**

### 2.1 Plan Anual de Adquisición

El presente proceso de contratación se encuentra incluido en el Plan de Compras de la Entidad.

### 2.2 Plan de Acción

El contrato que se pretende celebrar se encuentra dentro del plan de acción de la SECRETARIA DE TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACIÓN

### 2.3 Decreto de delegación

El Secretario se encuentra facultado para adelantar el presente proceso de contratación de acuerdo a la Ordenanza de facultades correspondiente al Decreto de Delegación 0012 del 02 de enero de 2024

## 3. Objeto a contratar

**ADQUISICIÓN DE LICENCIAS PARA EL FIREWALL DEL SISTEMA DE SEGURIDAD PERIMETRAL DEL DEPARTAMENTO DE RISARALDA**

### 3.1 Alcance del objeto a contratar

Contratar la adquisición y por ende renovación de 1 licencia de Software FortiGate-401F Enterprise Protection (IPS, Advanced Malware Protection, Application Control, Web & Video Filtering, Antispam, Security Rating, IoT Detection, Industrial Security, FortiConverter Svc, and 24x7 FortiCare), AI-based Inline Malware Prevention, 1 licencia FortiAnalyzer-VM Support 24x7 FortiCare Contract (for 1-6 GB/Day of Logs) + Subscription license for the FortiGuard Indicator of Compromise (IOC) (for 1-6 GB/Day of Logs) + Subscription license for FortiAnalyzer SOC service (1-6 GB/Day of Logs), 1 Soporte técnico preventivo, correctivo y equipo de contingencia modalidad 7x24 por espacio de 12 meses a partir de la firma del acta de inicio.

### 3.2. IDENTIFICACION DEL CONTRATO A CELEBRAR

| DESCRIPCION DE LA ACTIVIDAD | CODIGO UNSPSC |
|---|---|
| Software de seguridad y protección | 43233200 |

### 3.3. OBLIGACIONES DE LAS PARTES:

**OBLIGACIONES DEL DEPARTAMENTO.**

1. Designar un supervisor que realice la vigilancia, control y seguimiento del contrato.
2. Desarrollar las actividades de coordinación que sean necesarias.
3. Mantener el flujo de información sobre la marcha del Contrato.
4. Realizar el pago de acuerdo a lo estipulado en el contrato.
5. Las demás que sean acordes con la naturaleza del presente contrato

### 3.4. OBLIGACIONES DEL CONTRATISTA.

1. Suministrar 1 licencia de Software FortiGate-401F Enterprise Protection (IPS, Advanced Malware Protection, Application Control, Web & Video Filtering, Antispam, Security Rating, IoT Detection, Industrial Security, FortiConverter Svc, and 24x7 FortiCare), AI-based Inline Malware Prevention, por espacio de 12 meses a partir de la instalación de la licencia en el Appliance.
2. Activar las funcionalidades de la licencia FortiGate-401F Enterprise Protection, entregando listado de verificación de las mismas.
3. Suministrar 1 licencia FortiAnalyzer-VM Support 24x7 FortiCare Contract (for 1-6 GB/Day of Logs) + Subscription license for the FortiGuard Indicator of Compromise (IOC) (for 1-6 GB/Day of Logs) + Subscription license for FortiAnalyzer SOC service (1-6 GB/Day of Logs) por espacio de 12 meses a partir de la instalación de la licencia en el Appliance.
4. Activar las funcionalidades de la licencia FortiAnalyzer-VM Support 24x7 FortiCare Contract, entregando listado de verificación de las mismas.
5. Soporte técnico preventivo, correctivo modalidad 7x24x365 por espacio de 12 meses a partir de la firma del acta de inicio.
6. Disponer de acceso a la mesa de servicio y soporte, entregando credenciales de acceso para al menos dos usuarios que la Entidad disponga, en coordinación con el supervisor del contrato.
7. Soporte técnico correctivo con el cumplimiento de los requerimientos técnicos solicitados por la Entidad según los Tiempos de Nivel de Servicio, relacionados con las funcionalidades del dispositivo FortiGate 401F.
8. Realizar dos (2) visitas presenciales de Mantenimiento preventivo al año, para la revisión de configuración, desempeño y recomendaciones para la plataforma, para revisión de conexiones físicas, revisión del hardware, revisión de consumo de CPU, análisis de logs, plan de trabajo y mejora luego de analizar los logs, auditoría del dispositivos, políticas implementadas (filtro web, antispam, antivirus, VPN, router, IPS, DLP, control de aplicaciones), actualización del diagrama de conexiones de red y flujo de datos, con entrega de informe con los ítems anteriores descritos.
9. Aplicar oportunamente las últimas versiones de firmware que se encuentren disponibles y debidamente probadas y disponibles por parte del fabricante.
10. Afinar las políticas de seguridad informática de soporte implementadas, documentando el proceso.
11. Presentar un Informe de navegación de usuarios, listado de usuarios con más tráfico, ancho de banda y de incidencias generales no parametrizado y no controladas.
12. Presentar un resumen ejecutivo de eventos críticos y presentar los planes de acción a que diera lugar.

13. Monitorear e informar el desempeño de la licencia del dispositivo y los eventos detectados por el mismo.
14. Afinamiento de las funcionalidades de inspección de tráfico, donde incluya SSL inspection y desplegar los certificados digitales, documentando el proceso.
15. Atender todos requerimientos y/o acciones correctivas que se requieran por parte de GOBERNACIÓN E RISARALDA y que estén relacionados con la plataforma Fortinet instalada, ya sea de configuración, implementación y/o modificación de nuevos servicios o políticas de seguridad.
16. Afinamiento del sistema wifi y creación de políticas de seguridad aplicadas a las SSID, documentando el proceso.
17. Detectar e informar los incidentes de seguridad informática presentando en a la infraestructura tecnológica controlada por el dispositivo licenciado.
18. Registrar, clasificar e informar los incidentes de seguridad informática presentando en a la infraestructura tecnológica controlada por el dispositivo licenciado.
19. Disponer de equipo de contingencia con (1) un dispositivo de iguales características al que tiene la Entidad, con respuesta de una (30) minutos en la sede principal de la Gobernación, con obtención previa de copia de seguridad de las configuraciones presenten en el dispositivo de la Entidad dispositivo FortiGate 401F
20. Aplicar configuración técnica al dispositivo de contingencia en caso de hacer uso del mismo, documentando el proceso.
21. Brindar capacitación al personal de la Gobernación de Risaralda en el uso y administración de los equipos Fortinet por ocho (8) horas, así como en las mejores prácticas de seguridad.
22. Generar reportes mensuales detallados sobre el estado de los equipos, los incidentes atendidos y las acciones correctivas implementadas.
23. Mantener el precio de todos los bienes y servicios ofrecidos en la propuesta, durante toda la vigencia del contrato que se suscriba entre las partes.
24. Atender para aquellos casos cuya solución no se pueda solucionar de forma remota se deberá desplazar un ingeniero en sitio en un tiempo máximo de 3 horas
25. Cumplir con el objeto contractual de acuerdo a las especificaciones del contrato.
26. Para persona jurídica. Los contratistas están en la obligación del pago de parafiscales durante el tiempo de ejecución del contrato, ellos son: EPS, pensión, ARL, ICBF, y Caja de compensación Familiar. Esto en concordancia con el Articulo de la Ley 789 del 2002 y el Articulo 23 de la Ley 1150 de 2007, según el caso. Para persona natural: pago de seguridad social integral, (salud, pensión).
27. Atender los requerimientos realizados por la Gobernación de Risaralda por intermedio del funcionario encargado de la supervisión del contrato.
28. El contratista responderá por la calidad y cumplimiento del objeto del contrato y por la ejecución oportuna requerida por el Departamento de Risaralda.

29. Cumplir con el objeto del presente contrato con plena autonomía administrativa y bajo su propia responsabilidad en virtud de lo cual no existirá ningún tipo de vínculo laboral entre el Departamento de Risaralda y el contratista seleccionado.
30. EL CONTRATISTA, se compromete además del objeto del Contrato y su alcance, a cumplir con todas las obligaciones inherentes a él, en especial, las relacionadas con el uso de la documentación utilizada en el Sistema de Gestión de la Gobernación de Risaralda.
31. Prestar el soporte técnico durante la vigencia de las licencias soporte técnico bajo demanda en horario 8x5 (vía mesa de ayuda, telefónico, remoto, presencial o por e-mail).
32. El CONTRATISTA está obligado a la presentación de informes con los debidos soportes, conforme a las actividades previstas en este contrato.
33. EL CONTRATISTA se compromete a aceptar las condiciones establecidas en la comunicación de aceptación de oferta suscrita por la entidad.
34. El contratista deberá contar con usuario activo en la plataforma SECOP II.

**3.5 OBLIGACIONES DEL NIVEL DE SERVICIO:**
**Tiempo de respuesta mantenimiento correctivo:**

Para casos que comprometan la estabilidad del sistema de seguridad, se atenderá presencialmente, treinta (30) minutos después de la solicitud formal. Para casos que no comprometan la estabilidad del sistema de seguridad, se podrá atender también telefónicamente, y en caso de requerir atención presencial se atenderá en dos (2) horas después de la solicitud.

**Tiempo de respuesta**: Cuando se crea el caso de soporte se le dará una prioridad de P1 hasta P4.

P1: Daño físico de la máquina, problemas de conexión a nivel físico, eléctrico no encendido de la plataforma, no carga del sistema operativo o problemas con el arranque del archivo de configuración.

P2: Problemas de configuración graves que ameritan un cambio rápido, ya que comprometen la estabilidad de la máquina y la red del cliente, como problemas de enrutamiento WAN o bloqueo de algún servicio de la maquina o cambio en las interfaces de red.

P3: Problemas de configuración de mediano impacto, como reconfiguración de VPNs, cambios de políticas en general, reconfiguración de servicios antivirus, antispam, IDS, IPS, Perfiles de protección, FSAE, Usuarios, Grupos y creación de máquinas.

P4: Preguntas o dudas generales con respecto al funcionamiento de algún servicio de la maquina

el cual es solicitado por parte de nuestros clientes.

**Tiempos de respuesta**

P1: Treinta (30) minutos de tiempo de respuesta en sitio y traslado del dispositivo de respaldo, para ser montado en caso de ser necesario y así superar los problemas de conectividad.

P2: Dos (2) Horas máximo de tiempo de respuesta en sitio cuando se amerite o remoto para los cambios solicitados.
P3: Cuatro (4) Horas máximo para los cambios solicitados.

P4: Ocho (8) Horas máximo, para los cambios o aclaraciones solicitadas.

Escalamiento de incidentes: Se establecerá un proceso claro de escalamiento para aquellos incidentes que requieran la intervención de niveles superiores de soporte.

## 4. REQUISITOS HABILITANTES

Podrán participar en el presente proceso de contratación las personas naturales o jurídicas legalmente constituidas, así como aquellas que conformen consorcios o uniones temporales.

**Persona jurídica**

Certificado de existencia y representación legal de la Cámara de Comercio, con expedición no superior a treinta (30) días, en el cual se revisará:

- El objeto social de la empresa debe ser coherente con el objeto a contratar a suscribir, de manera que se identifique la capacidad tanto para la celebración como para ejecución del contrato.
- En caso en que el Representante Legal del proponente tenga alguna limitación para suscribir la oferta o el contrato, se deberá anexar copia certificada del acta de la Junta o Asamblea de Socios por la cual se le autoriza para presentar la propuesta y firmar el contrato, o se le exima o suspenda la limitación aludida según el caso.
- Acreditar que la duración de la persona jurídica no será inferior al término de ejecución del contrato y un año más.
- Copia del documento de identidad del representante Legal de la persona jurídica o del consorcio o unión temporal.

- Acreditar el pago de los aportes de sus empleados a los sistemas de salud, pensión, administradora de riesgos laborales y aportes a las Cajas de Compensación Familiar, Instituto Colombiano de Bienestar Familiar y Servicio Nacional de Aprendizaje, mediante certificación expedida por el contador y/o revisor fiscal, si a ello hubiere lugar o por el representante legal, según el caso.

Dicho documento debe certificar que se ha realizado el pago de los aportes correspondientes a la nómina, el cual, en todo caso, deberá indicar que se encuentra a paz y salvo dentro de los últimos seis (6) meses anteriores a la fecha del cierre del proceso de selección, en los cuales se haya causado la obligación de efectuar dichos pagos, de conformidad con el artículo 50 de la ley 789 de 2002. En caso de presentar acuerdo de pago con las entidades recaudadoras respecto de alguna de las obligaciones mencionadas, deberá manifestar que existe acuerdo de pago y que se encuentra al día en el cumplimiento del mismo. En este evento el oferente deberá anexar certificación expedida por la entidad con la cual existe el acuerdo de pago.

Cuando se trate de consorcio o uniones temporales, cada uno de sus miembros integrantes que sea persona jurídica, deberá aportar el certificado en mención.

Para el efecto deberá diligenciar el formato No 3

**Persona natural**

- Certificado de registro mercantil (si aplica)
- Fotocopia del documento de identificación del proponente
- El proponente persona natural deberá acreditar la afiliación a los sistemas de seguridad social en salud y pensiones aportando los certificados de afiliación respectivos. El proponente podrá acreditar la afiliación entregando el certificado de pago de planilla, pero no será obligatoria su presentación.
- Los certificados de afiliación se presentan con fecha de expedición no mayor a treinta (30) días calendario. En caso de modificarse la fecha de cierre del proceso, se tendrá como referencia para establecer el plazo de vigencia de los certificados de afiliación la fecha originalmente establecida en el cronograma de la invitación.
- La persona natural que reúna los requisitos para acceder a la pensión de vejez, o se pensione por invalidez o anticipadamente, presentará el certificado que lo acredite y, además la afiliación al sistema de salud.
- Adicionalmente, el proponente adjudicatario debe presentar, para la aceptación de la oferta, ante la dependencia respectiva, la declaración donde acredite el pago correspondiente a seguridad social y aportes legales cuando a ello haya lugar.

- Libreta Militar (Hombres colombianos hasta los 50 años de edad, aplica solo prestación de servicios)

**Proponentes plurales**

El documento de conformación de proponentes plurales debe:

- Acreditar la existencia del proponente plural y clasificarlo en Unión Temporal o Consorcio. En este documento los integrantes deben expresar su intención de conformar el proponente plural. En caso que no exista claridad sobre el tipo de asociación se solicitará la aclaración. Los proponentes deben incluir como mínimo la información requerida en el Formato 2 – Conformación de Proponente Plural (Formato 2A – Consorcios) (Formato 2B – Uniones Temporales). Los proponentes pueden introducir información adicional que no contradiga lo dispuesto en los Documentos del proceso.
- Acreditar el nombramiento de un representante y un suplente, este último en caso de considerarlo conveniente, cuya intervención deberá quedar definida en el Formato 2 – Conformación de Proponente Plural (Formato 2A- Consorcios) (Formato 2B- Uniones Temporales), de todas las personas naturales y/o jurídicas asociadas, con facultades suficientes para la representación sin limitaciones de todos y cada uno de los integrantes, en todos los aspectos que se requieran para presentar la oferta, para la suscripción y ejecución del contrato, así como también la facultad para firmar el acta de terminación y liquidación.
- Aportar fotocopia de la cédula de ciudadanía del representante principal y suplente de la estructura plural.
- El proponente plural debe señalar expresamente cuál es el porcentaje de participación de cada uno de sus miembros. La sumatoria del porcentaje de participación no podrá ser diferente al 100%.
- En la etapa contractual, no podrán modificarse los porcentajes de participación sin el consentimiento previo de la entidad.
- Indicar el lote o lotes a los cuales presenta oferta, cuando aplique.
- Dicho documento debe estar firmado por todos los integrantes del proponente plural y en el caso del miembro persona jurídica, por el representante legal de dicha persona o por el apoderado de cualquiera de los anteriores
- Respecto del requisitos de pago de seguridad social, cada uno de los integrantes del proponente plural debe suscribir por separado la declaración de la que tratan los numerales anteriores, dependiendo si se trata de persona natural o jurídica.

- Respecto de su capacidad jurídica, los requisitos habilitantes serán acreditados por cada uno de los integrantes de la figura asociativa y, en todo caso, se realizará de acuerdo con las reglas de la invitación.

**Experiencia**

El proponente debe acreditar con un máximo de dos (2) certificados de contratos de compraventa de licencia de firewall cuya sumatoria superior al 100% del valor del presente proceso contractual.

Para proponente plural, se aceptará la experiencia con un máximo en dos (2) certificados como la sumatoria de la experiencia de los integrantes del consorcio o unión temporal, sin importar su porcentaje de participación.

La fecha de terminación de los contratos certificados debe estar comprendida entre la fecha de expedición de la matricula mercantil del proponente y la fecha de cierre del plazo del presente proceso de contratación.

Las certificaciones o actas de recibo o actas de liquidación o actas finales de obra, las cuales deberán ser suscritas por la persona competente deberán contener como mínimo la siguiente información:

✓ Numero de contrato
✓ Objeto del contrato
✓ Fecha de iniciación y terminación del contrato
✓ Tiempo de ejecución
✓ Cargo desempeñado, de quien firma el certificado o acta de recibo o acta de liquidación o acta final

En todo caso la experiencia se acreditará con los contratos que se encuentren inscritos en el Registro Único de Proponentes y que correspondan a los códigos solicitados para este proceso.

*NOTA: Para acreditar la experiencia no se aceptarán copias de contratos.*

**APLICACIÓN ARTICULO 3 DEL DECRETO 1860 DE 2021:** Criterios diferenciales para Mipyme en el sistema de compras públicas.

En estricto cumplimiento del artículo 3 del decreto 1860 de 2021, las mipyme, podrán acreditar su experiencia habilitante, mediante la ejecución de tres (3) certificados de contratos de compraventa de antivirus cuya sumatoria superior al 80% del valor del presente proceso contractual.

Las certificaciones aportadas, deberán cumplir con lo solicitado en el numeral

Lo previsto en esta norma aplica sin perjuicio de lo dispuesto en los Acuerdos Comerciales suscritos por el Estado colombiano, pero no rige en las convocatorias limitadas a mipyme que se realicen conforme a los artículos 2.2.1.2.4.2.2 y 2.2.1.2.4.2.3 de este Decreto.

**NOTA.** Respecto a los incentivos contractuales para los emprendimientos y empresas de mujeres, las certificaciones de trata el presente NUMERAL deben expedirse bajo la gravedad de juramento con una fecha de máximo treinta (30) días calendario anteriores a la prevista para el cierre del procedimiento de selección.

**DEL RECURSO HUMANO.**

- **a.** Para el recurso humano se requiere que cuente con el siguiente perfil profesional: Ingeniero de sistemas o afines con Certificación NSE7 (Network Security Architect) de Fortinet y/o Certified Solution Specialist OT Security y con maestría en seguridad informática. Para lo cual el oferente aportara los siguientes documentos: Tarjeta profesional, certificación del COPNIA, hoja de vida de la función pública, experiencia como ingeniero de sistemas de mínima 5 años y 2 años de experiencia relacionada con Fortinet NSE 7 Network Security Architec.
- **b.** Ingeniero de sistemas o afines con Certificación Professional Public Cloud Security Fortinet Para lo cual el oferente aportara los siguientes documentos: Tarjeta profesional, certificación del COPNIA, hoja de vida de la función pública, experiencia como ingeniero de sistemas de mínima 3 años y 1 años de experiencia relacionada con la certificación solicitada.

**Equipo de Contingencia:**

El proveedor deberá contar con un equipo de contingencia de características iguales o

superiores al dispositivo FortiGate FG-401F, disponible para su reemplazo inmediato en caso de falla crítica del equipo principal, acreditándolo mediante carta de disponibilidad suscrita por el representante legal y factura de compra del mismo a nombre del proponente.

**CRITERIOS DE ASIGNACIÓN DE CALIFICACIÓN - Oferta Económica**

a. El proponente debe cotizar la totalidad de los ítems requeridos y en las unidades de medidas y cantidades requeridos por la Entidad, diligenciando el cuestionario (lista de precios) en el SECOP II, es decir el proponente NO deberá adjuntar archivos adicionales que contengan la oferta económica, bastará con el diligenciamiento de la lista de precios en SECOP II.

b. **Nota importante**: En caso de que eventualmente el valor de la oferta económica diligenciada en el cuestionario del SECOP II, no coincida con algún anexo de la propuesta, prevalecerá el valor diligenciado en SECOP II.

c. La oferta deberá estar vigente durante toda la ejecución del contrato.

d. Se verificarán los valores de la oferta teniendo en cuenta los precios del mercado. El valor global de la oferta, incluido el IVA, no podrá superar el presupuesto oficial. La oferta económica debe ser clara y verificable matemáticamente, en ella se deben establecer por separado los precios para cada ítem ofrecido, discriminando IVA si pertenece al régimen común, en caso contrario deberá indicarlo. **Si el proponente no discrimina el impuesto del IVA, este nuevo valor no podrá ser reconocido por el Departamento y el PROPONENTE deberá asumir el costo del impuesto**.

e. Solo se pagará los precios contratados y por tanto, no reconocerá suma alguna por impuestos ni reajustes a los precios ofertados, a menos que el reajuste se deba efectuar como consecuencia de una acción directa de la entidad previamente formalizada de acuerdo a los procedimientos legales y presupuestales que corresponda.

f. El Departamento de Risaralda efectuará las retenciones que en materia tributaria tenga establecida la Ley y respecto de las cuales sea su obligación efectuar la retención. En los demás casos, el contratista deberá cumplir con el pago de los impuestos, tasas o contribuciones que se deriven de la presente contratación.

g. Deberán ser tramitadas por el PROPONENTE, las devoluciones o exenciones a que crea tener derecho ante la respectiva Administración de Impuestos, sin responsabilidad alguna por parte del Departamento o costo para ella.

h. Todos los impuestos, retenciones y gastos que se causen por razón de la legalización y ejecución del contrato, incluidas la constitución de la garantía única de cumplimiento en caso de que se le requiera, son de cargo exclusivo del CONTRATISTA. Por lo tanto, los precios que se propongan deberán considerar tales conceptos.

Otros requisitos comunes para persona jurídica y natural:

a. Formato N° 1 carta de presentación de la propuesta diligenciada y firmada.
b. Anexo No. 2. Anexo Oferta Económica.
c. Anexo N° 3 pacto de transparencia, el cual se entiende aceptado con la firma de la carta de presentación de la oferta.
d. Fotocopia del RUT, con códigos actualizados. Se verificará que la actividad económica esté directamente relacionada con el objeto contractual.
e. Certificado de antecedentes expedido por la Contraloría.
f. Certificado de antecedentes expedido por la Procuraduría.
g. Certificado de Antecedentes Penales y Requerimientos Judiciales.
h. Certificado del Registro Nacional de Medidas Correctivas RNMC.
i. El Departamento verificará en la evaluación y dejará evidenciado a través de la impresión de los certificados, si el futuro contratista se encuentra reportado en el Boletín de responsables Fiscales de la Contraloría General de la República, certificado que arroja la Procuraduría General de la Nación, Antecedentes Penales y Requerimientos Judiciales y Registro Nacional de Medidas Correctivas.
j. Certificación Bancaria con expedición inferior a treinta (30) días.

## 5. Plazo de ejecución del contrato

El plazo será de TREINTA (30) días contados a partir de la suscripción del acta de inicio, sin exceder hasta el 31 de diciembre de 2025. El contratista deberá garantizar el cumplimiento de los cronogramas establecidos por el departamento de Risaralda

## 6. Lugar de ejecución del contrato

El lugar de ejecución del contrato será en la ciudad de Pereira. Parágrafo: Para todos los efectos contractuales se tendrán como domicilio la ciudad de Pereira, Risaralda.

Parágrafo: Para todos los efectos contractuales se tendrán como domicilio la ciudad de Pereira Risaralda.

## 7. Valor estimado del contrato/ presupuesto oficial y su justificación

Conforme a lo establecido en el Análisis del sector, el presupuesto oficial del presente proceso contractual es por la suma de OCHENTA Y SIETE MILLONES QUINIENTOS TREINTA Y SEIS MIL OCHOCIENTOS SESENTA Y DOS PESOS M/CTE ($87.536.862) INCLUIDO IVA, y demás impuestos, tasas, contribuciones de carácter nacional y/o departamental y/o municipal de carácter legal, costos directos e indirectos.

### 7.1 Aspectos tributarios y financieros del contrato

| TASA O ESTAMPILLA | BASE GRAVABLE | APLICA SI/NO | FORMA DE PAGO |
|---|---|---|---|
| Estampilla Pro Cultura (Contratos celebrados por el Departamento de Risaralda y sus entes descentralizados mayor a 1640 UVT). ($ 49.799) (resolución #00193 de dic 4 de 2024) | 1,5% | **SI** | **Persona Natural**: Será descontado en el primer pago que se realice al contratista. (Par. 1 Art. 248 Estatuto de Rentas)<br>**Persona jurídica**: Será descontado o retenido en cada cuenta y orden de pago. (Par. 2 Art. 248 Estatuto de Rentas) |
| Estampilla Pro Desarrollo | 2.0% | **SI** | Persona Natural: Será descontado en el primer pago que se realice al contratista. (Par. 1 Art. 214 Estatuto de Rentas)<br>Persona jurídica: Será descontado o retenido en cada cuenta y orden de pago. (Par. 2 Art. 214 Estatuto de Rentas) |
| Estampilla Universidad Tecnológica de Pereira hacia el III Milenio | 1.0% | **SI** | Persona Natural: Será descontado en el primer pago que se realice al contratista. (Par. 1 Art. 238 Estatuto de Rentas)<br>Persona jurídica: Será descontado o retenido en cada cuenta y orden de pago. (Par. 2 Art. 238 Estatuto de Rentas) |
| Estampilla para el Bienestar del Adulto Mayor | 3% | **SI** | Persona Natural: Será descontado en el primer pago que se realice al contratista. (Par. 1 Art. 222 Estatuto de Rentas)<br>Persona jurídica: Será descontado o retenido en cada cuenta y orden de pago. (Par. 2 Art. 222 Estatuto de Rentas) |
| Tasa por deporte y recreación – PARA CONTRATOS CON PERSONA JURIDICA. | 2.5% | **NO** | Será descontado o retenido en cada comprobante de egreso u orden de pago. Art 181. Estatuto tributario) |
| Estampilla pro hospitales universitarios – (contratos celebrados en la Secretaría Departamental de Salud, y en las | 2% | **NO** | Persona Natural: Será descontado en el primer pago que se realice al contratista. (Par. 1 art. 229 Estatuto de Rentas)<br>Persona jurídica: Será descontado o retenido |

| | | | |
|---|---|---|---|
| entidades Descentralizadas del orden Departamental y Municipal). | | | en la cuenta y orden de pago. (Par. 2 Art. 229 Estatuto de Rentas) |
| Otras | | | |

### 7.2 Disponibilidad Presupuestal

El departamento de Risaralda adelantará el presente proceso con cargo a las siguientes disponibilidades presupuestales:

| *CERT. DISPON. PRESUPUESTAL* | *RUBRO PRESUPUESTAL* | *SECRETARIA Y VALOR* | *VALOR PRESUPUESTO OFICIAL* |
|---|---|---|---|
| 4689 del 30 de octubre de 2025 | *0314-2.3.2.01.01.005.02.03.01.01-346* | Secretaría de Tecnologías de la Información y la Comunicación ($88.488.717) | **$87.536.862** |

- **Relación existente entre la contratación a realizar y el rubro presupuestal del cual se derivan sus recursos.**

El objeto del presente proceso está directamente relacionado con la definición del rubro presupuestal, ya que busca el fortalecimiento de las tecnologías de la información y comunicaciones en el Departamento de Risaralda.

### 7.3 Forma de pago

El Departamento de Risaralda, cancelará el valor del contrato que se suscriba con ocasión de este proceso de la siguiente forma: mediante un acta única final previa entrega a satisfacción del suministro contratado y presentación de la factura o cuenta de cobro por parte del contratista, la revisión y autorización por parte del supervisor. La anterior forma de pago obedece a la forma de entrega del bien.

**Para persona jurídica:** Los contratistas están en la obligación del pago de seguridad social integral y de parafiscales durante el tiempo de ejecución del contrato, ellos son: EPS, pensión, ARL, ICBF, y Caja de compensación Familiar. Esto en concordancia con el Articulo de la Ley 789 y el Articulo 23 de la Ley 1150 de 2007, según el caso.

**Para persona natural:** pago de seguridad social integral, (salud, pensión y ARL).

Para el trámite y pago deberá hacer entrega de los siguientes documentos:

- Toda la documentación que requiera tesorería y contabilidad del departamento para el pago.
- Acta suscrita por el contratista y el supervisor
- Acta de entrega a satisfacción suscrita por el supervisor y el contratista.

La Entidad no se hace responsable por las demoras presentadas en el trámite para el pago al Contratista cuando ellas fueren ocasionadas por encontrarse incompleta la documentación de soporte o no ajustarse a cualquiera de las condiciones establecidas. La Entidad hará las retenciones a que haya lugar sobre cada pago, de acuerdo con las disposiciones legales vigentes sobre la materia.

## 8. Justificación de la modalidad de selección

El presente proceso de contratación se adelantará a través la modalidad de Mínima Cuantía en consideración a que el valor estimado para la contratación no excede del 10% de la menor cuantía de la Entidad estatal, de conformidad con lo establecido en el artículo 2 de la Ley 1150 de 2007, adicionado por el artículo 94 de la Ley 1474 de 2011, y el artículo 2.2.1.2.1.5.1 y siguientes del Decreto 1860 de 2021.

## 9. Evaluación de las ofertas:

Para la escogencia del ofrecimiento más favorable, el Departamento tendrá como primer criterio de evaluación el menor precio, en aplicación a lo establecido en el artículo 2.2.1.2.1.5.2 del Decreto 1860 de 2021; si la primera oferta no cumple, previo requerimiento de los requisitos habitantes (subsanables) o no subsana y agotado el termino de traslado de la evaluación, el Comité evaluará la oferta en segundo menor precio y así sucesivamente.

**Nota importante**: En caso de que eventualmente el valor de la oferta económica diligenciada en el cuestionario del SECOP II, no coincida con algún anexo, prevalecerá el valor diligenciado en SECOP II.

## 10. Control y vigilancia del contrato

La Supervisión para el presente Contrato, será ejercida por un funcionario de la

SECRETARIA DE TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACIÓN, quién se constituye en el enlace entre las partes. Como supervisor verificará la correcta y oportuna ejecución del objeto contractual y actuará de conformidad con lo determinado por el Manual de Interventor adoptado mediante Decreto 0316 de 2018.

**11. Maduración del proyecto**

NA

**12. Bienes agrícolas**

NA

**13. Aviso limitación a Mipymes**

El presente proceso de selección puede estar limitado a Mipymes territoriales o nacionales colombianas con mínimo un (1) año de existencia, cuando concurran los requisitos establecidos en el artículo 2.2.1.2.4.2.2 Decreto 1860 de 2021 y siguientes. La solicitud de limitación deberá presentarse a través del módulo de mensajes del SECOP II.

**14. Garantías**

La entidad requiere la constitución de los siguientes amparos:

**Cumplimiento:** Por el VEINTE POR CIENTO (20%) del valor del contrato, por el término del mismo y ocho (8) meses más.

En todo caso la garantía de cumplimiento deberá mantenerse vigente hasta que se logre la liquidación del contrato.

**Calidad del Servicio:** Por el VEINTE POR CIENTO (20%) del valor del contrato, por el término del mismo y hasta la liquidación del contrato (mínimo seis meses).

**Calidad de los productos.** El valor de estas garantías será del veinte (20%) del valor del contrato. Su vigencia deberá ser por el término del contrato y (un año más).

Justificación: En razón a que analizadas las obligaciones a entregar y/o naturaleza del objeto, se considera que deben existir garantías que permitan a la entidad en caso de un incumplimiento total o parcial recurrir a la compañía de seguros y reclamar los perjuicios ocasionados, así mismo para la Secretaría de las TIC, es necesario satisfacer la

Necesidad descrita por lo que se requiere que el contratista otorgue a favor del departamento la garantía de cumplimiento que le permita a este último estar amparado con las mismas.

Se firma en Pereira,

**LUIS ALEXANDER VASQUEZ HERNANDEZ**
Secretario de Despacho
Ordenador de Gasto

**LILIANA YEZMIN ZAPATA ALVAREZ**
Directora de Informática y Sistemas Tecnológicos

**Wilmar Libardo Copete Marín**
Profesional Especializado Grado 8
**Componente Técnico:**
**Dirección de Informática y Sistemas Tecnológicos**

**MIGUEL ANDRÉS MARTÍNEZ**
**Componente Legal:**
Abogado Contratista – Secretaría de TIC

**SANDRA MELISSA CÁRDENAS ESPINOSA**
**Componente Financiero:**
Contratista Secretaría de TIC