Estudio previo para el proceso de mínima cuantía No. STIC-IPMC-052-2026

ANALISIS DEL SECTOR

LA SECRETARIA DE TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACION realiza el **ANALISIS 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.

La función de contratación estatal debe estar orientada a satisfacer las necesidades de la Entidad Estatal y a obtener el mayor valor por el dinero público, por lo que a través de este instrumento y en cumplimiento de la obligación legal del Departamento de analizar el mercado relativo al objeto del proceso de contratación, como entidad pública del orden territorial, según el artículo 2.2.1.1.1.6.1 del decreto 1082 de 2015, se procede a desarrollar el análisis del sector alrededor del objeto del proceso siguiendo los lineamientos de la Agencia Nacional de Contratación Estatal – Colombia Compra Eficiente.

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. Aspecto Técnico
C. Aspecto Regulatorio
D. Análisis de la Demanda
E. Análisis de la Oferta
F. Análisis de Riesgos

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.

Gobernación de Risaralda. NIT. 891 480 085-7
Calle 19 No 13 - 17 Pereira- Risaralda
PBX. +(57) (606) 3398300 - 01 8000 916 078
contactenos@risaralda.gov.co - www.risaralda.gov.co

Estudio previo para el proceso de mínima cuantía No. STIC-IPMC-052-2026

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

El sector de tecnologías de la información y las comunicaciones (TIC) comprende servicios de conectividad, desarrollo y comercialización de software, infraestructura tecnológica, centros de datos, servicios digitales y actividades de soporte especializado. Su evolución constituye un elemento de contexto para las entidades públicas que requieren plataformas informáticas para prestar sus servicios y mantener la continuidad de sus operaciones.

Según el Boletín Trimestral del Sector TIC del Ministerio de Tecnologías de la Información y las Comunicaciones, publicado el 9 de octubre de 2026 con cifras del segundo trimestre de 2026, Colombia registró 10,78 millones de accesos a internet fijo y 49,6 millones de accesos a internet móvil. El Ministerio reportó además 6,6 millones de accesos fijos mediante fibra óptica y 10,7 millones de conexiones móviles 5G. Estos indicadores muestran el alcance de la conectividad nacional.

La expansión de servicios digitales, la disponibilidad de conectividad y la transformación de procesos institucionales incrementan la importancia de contar con infraestructura informática administrable, segura y con mecanismos de continuidad. En el ámbito de las entidades públicas, estas necesidades se relacionan con la operación de aplicaciones, bases de datos, servicios internos y plataformas de atención al ciudadano.

MERCADO DE SOLUCIONES DE SEGURIDAD PERIMETRAL Y FIREWALL

El mercado de soluciones de seguridad perimetral y firewall en Colombia forma parte del sector de Tecnologías de la Información y las Comunicaciones (TIC), específicamente del segmento de ciberseguridad y protección de infraestructuras tecnológicas. Este mercado comprende la comercialización, implementación, configuración, actualización, mantenimiento y soporte de soluciones destinadas a controlar el tráfico de las redes, prevenir accesos no autorizados y proteger los sistemas de información frente a amenazas informáticas.

En el sector público, la demanda de estas soluciones está relacionada con la necesidad de proteger la infraestructura tecnológica institucional, mantener la disponibilidad de los servicios digitales y establecer mecanismos de control sobre las comunicaciones internas y externas. Las entidades públicas administran sistemas de información, aplicaciones, bases de datos y servicios de conectividad que requieren medidas de seguridad acordes con la sensibilidad de la información, las características de sus redes y los riesgos asociados a su operación.

Gobernación de Risaralda. NIT. 891 480 085-7
Calle 19 No 13 - 17 Pereira- Risaralda
PBX. +(57) (606) 3398300 - 01 8000 916 078
contactenos@risaralda.gov.co - www.risaralda.gov.co

Estudio previo para el proceso de mínima cuantía No. STIC-IPMC-052-2026

El mercado ofrece diferentes tecnologías de protección, entre las que se encuentran los firewall tradicionales, los firewall de nueva generación (NGFW), los sistemas de prevención de intrusiones (IPS), las redes privadas virtuales (VPN), los mecanismos de filtrado de contenido y las soluciones de inspección y control del tráfico de aplicaciones. Estas funcionalidades pueden encontrarse integradas en una misma plataforma o contratarse mediante componentes y servicios complementarios, dependiendo de la arquitectura tecnológica y de los requerimientos de seguridad de cada organización.

La oferta está conformada por fabricantes internacionales, distribuidores autorizados, integradores tecnológicos y empresas especializadas en servicios de ciberseguridad. Entre los fabricantes con presencia comercial en este segmento se encuentran Fortinet, Palo Alto Networks, Check Point, Cisco, Sophos y otros proveedores de soluciones de seguridad de redes. Sus productos presentan diferencias en capacidad de procesamiento, funcionalidades de protección, arquitectura, administración centralizada, esquemas de licenciamiento y condiciones de soporte técnico.

Desde el punto de vista tecnológico, los firewall de nueva generación incorporan capacidades que permiten identificar aplicaciones, inspeccionar conexiones, establecer políticas de acceso y detectar determinados comportamientos asociados con amenazas informáticas. Dependiendo del fabricante, el modelo y las licencias contratadas, estas soluciones pueden incluir prevención de intrusiones, filtrado web, protección contra programas maliciosos, inspección de tráfico cifrado, inteligencia de amenazas y generación de registros para el monitoreo de eventos de seguridad.

En cuanto a las modalidades de comercialización, el mercado contempla la adquisición de equipos físicos, licencias de software, dispositivos virtuales, suscripciones a servicios de seguridad, renovaciones de licenciamiento, garantías, mantenimiento y soporte técnico especializado. También existen alternativas de firewall como servicio (FWaaS) y servicios administrados de seguridad, mediante los cuales un proveedor asume determinadas actividades de operación, monitoreo o administración, según las condiciones contractuales establecidas.

Las condiciones económicas de estas soluciones dependen de factores como el fabricante, el modelo del equipo, la capacidad de procesamiento, el número de conexiones concurrentes, el rendimiento requerido con las funciones de seguridad habilitadas, la cantidad de interfaces de red, la duración de las suscripciones y los niveles de soporte contratados. En consecuencia, la comparación de precios debe considerar las especificaciones técnicas y los servicios incluidos en cada oferta, dado que equipos con características aparentemente similares pueden presentar diferencias en su capacidad efectiva de operación.

El mercado también ofrece alternativas de implementación mediante dispositivos físicos, plataformas virtualizadas y servicios de seguridad alojados en la nube. La selección de una arquitectura depende de la infraestructura existente, el volumen y las características del tráfico, los enlaces de conectividad, la distribución de las sedes y los requerimientos de disponibilidad. En las entidades que operan servicios institucionales de manera continua, también deben evaluarse las opciones de alta disponibilidad, redundancia y recuperación ante fallas.

Gobernación de Risaralda. NIT. 891 480 085-7
Calle 19 No 13 - 17 Pereira- Risaralda
PBX. +(57) (606) 3398300 - 01 8000 916 078
contactenos@risaralda.gov.co - www.risaralda.gov.co

Estudio previo para el proceso de mínima cuantía No. STIC-IPMC-052-2026

Para las entidades públicas que cuentan con equipos firewall previamente instalados, la contratación de licencias, renovaciones y servicios de soporte responde a la necesidad de mantener operativas las funcionalidades de seguridad adquiridas y disponer de actualizaciones del fabricante. La vigencia de las suscripciones puede determinar el acceso a servicios como inteligencia de amenazas, actualización de firmas de seguridad, filtrado web y soporte especializado, de acuerdo con las condiciones comerciales y técnicas de cada producto.

Cuando la contratación corresponde a la renovación o ampliación de una plataforma existente, deben examinarse las condiciones de compatibilidad con la infraestructura institucional, las versiones de software utilizadas, la capacidad de los dispositivos y su ciclo de vida comercial. También deben considerarse las implicaciones técnicas y económicas de una eventual sustitución tecnológica, particularmente en lo relacionado con la migración de políticas de seguridad, configuraciones de red, conexiones VPN, reglas de acceso y mecanismos de administración.

Por otra parte, el mercado presenta factores comerciales que inciden en la estructuración de los procesos de contratación, como las políticas de distribución de los fabricantes, los esquemas de licenciamiento y suscripción, la disponibilidad de proveedores especializados, las variaciones de la tasa de cambio, los costos de soporte y la vigencia comercial de los equipos. Estos aspectos deben revisarse al establecer el presupuesto estimado y las condiciones de suministro, renovación o mantenimiento requeridas por la entidad.

ESTRATEGIAS DEL SECTOR TIC EN COLOMBIA

El sector de las Tecnologías de la Información y las Comunicaciones (TIC) constituye un componente estratégico para el desarrollo económico, la modernización institucional y la transformación digital de Colombia. Su evolución está relacionada con el fortalecimiento de la conectividad, la adopción de soluciones tecnológicas, el desarrollo de capacidades digitales y la implementación de infraestructuras que permitan mejorar la productividad y la prestación de servicios públicos.

En este contexto, el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) ha establecido diferentes políticas y estrategias orientadas a fortalecer el ecosistema digital del país, promover la innovación tecnológica y facilitar la apropiación de las TIC en los sectores público y privado.

La Estrategia Nacional Digital 2023-2026, articulada con el Plan Nacional de Desarrollo 2022-2026, contempla ocho ejes de intervención, entre ellos conectividad digital, seguridad y confianza digital, talento digital, inteligencia artificial y tecnologías emergentes, transformación digital del Estado y economía digital.

Para su implementación, el Ministerio TIC ha desarrollado tres líneas estratégicas principales:

1. Conectividad y reducción de la brecha digital

Gobernación de Risaralda. NIT. 891 480 085-7
Calle 19 No 13 - 17 Pereira- Risaralda
PBX. +(57) (606) 3398300 - 01 8000 916 078
contactenos@risaralda.gov.co - www.risaralda.gov.co

Estudio previo para el proceso de mínima cuantía No. STIC-IPMC-052-2026

Orientada a ampliar el acceso y uso de servicios de telecomunicaciones, fortalecer la infraestructura de conectividad y facilitar la incorporación de la población y las organizaciones a los entornos digitales. Esta línea busca generar condiciones que permitan el aprovechamiento de las tecnologías en las diferentes regiones del país.

2. Tecnología que transforma: ecosistemas de innovación

Busca impulsar la transformación digital del sector público y privado mediante la adopción de soluciones tecnológicas, el desarrollo de software, el aprovechamiento de datos y la incorporación de tecnologías emergentes.

En el ámbito gubernamental, esta estrategia se relaciona con la modernización de las plataformas tecnológicas, la interoperabilidad entre sistemas de información, la seguridad digital y el fortalecimiento de las capacidades institucionales para prestar servicios electrónicos.

3. Educación digital y fortalecimiento del talento tecnológico

Promueve la formación de competencias digitales y el desarrollo de talento humano especializado en tecnologías de la información, con el propósito de facilitar la adopción tecnológica, mejorar las oportunidades laborales y fortalecer la competitividad del país.

Estas líneas se encuentran documentadas en la estrategia oficial Colombia PotencIA Digital del MinTIC.

EVOLUCIÓN DE LAS ESTRATEGIAS TIC DURANTE 2026

Durante 2026, el Ministerio TIC ha presentado nuevas iniciativas para ampliar el alcance de la transformación digital nacional.

En mayo de 2026 presentó la Misión de Transformación Digital 2035, orientada a fortalecer el acceso tecnológico, la productividad y la soberanía tecnológica, mediante la articulación del Estado, las empresas, la academia y las comunidades.

Posteriormente, en septiembre de 2026, anunció la construcción del Plan TIC Colombia 2026-2030, bajo una visión enfocada en convertir la tecnología en un instrumento de productividad, innovación, generación de empleo y modernización del Estado.

La propuesta contempla cinco misiones nacionales: conectar Colombia, preparar a Colombia, impulsar la producción mediante tecnologías digitales, transformar el Estado y fortalecer la ciberseguridad. A octubre de 2026, esta iniciativa se encuentra en proceso de construcción

RELACIÓN DE LAS ESTRATEGIAS TIC CON EL MERCADO DE SOLUCIONES DE SEGURIDAD

Gobernación de Risaralda. NIT. 891 480 085-7
Calle 19 No 13 - 17 Pereira- Risaralda
PBX. +(57) (606) 3398300 - 01 8000 916 078
contactenos@risaralda.gov.co - www.risaralda.gov.co

Estudio previo para el proceso de mínima cuantía No. STIC-IPMC-052-2026

PERIMETRAL Y FIREWALL

Las estrategias de Tecnologías de la Información y las Comunicaciones (TIC) en las entidades públicas están orientadas a fortalecer la infraestructura tecnológica, garantizar la continuidad de los servicios digitales y establecer mecanismos de protección de los sistemas de información. Dentro de estas estrategias, las soluciones de seguridad perimetral y firewall cumplen una función específica en el control de las comunicaciones de red, la prevención de accesos no autorizados y la protección de los recursos tecnológicos institucionales.

La implementación y actualización de soluciones firewall se relaciona con las políticas de seguridad digital y los lineamientos de gestión de riesgos tecnológicos adoptados por las entidades públicas. Estas herramientas permiten establecer reglas para el tráfico entrante y saliente, controlar las conexiones entre segmentos de red, restringir accesos a servicios institucionales y aplicar mecanismos de inspección orientados a identificar posibles amenazas informáticas.

En Colombia, el fortalecimiento de la seguridad digital de las entidades públicas se relaciona con el Modelo de Seguridad y Privacidad de la Información (MSPI), promovido por el Ministerio de Tecnologías de la Información y las Comunicaciones, y con los lineamientos de la Política de Gobierno Digital. Estos instrumentos contemplan la gestión de riesgos de seguridad de la información, la protección de los activos tecnológicos y la adopción de controles acordes con las necesidades institucionales. Las soluciones firewall constituyen uno de los mecanismos técnicos que pueden contribuir a la implementación de dichos controles, sin sustituir las demás medidas de seguridad requeridas.

Desde el punto de vista de la infraestructura tecnológica, las estrategias TIC requieren disponer de redes de comunicaciones seguras que permitan la operación de aplicaciones, bases de datos, plataformas institucionales y servicios de conectividad. Los firewall permiten administrar el intercambio de información entre redes internas, externas y entornos de servicios, mediante políticas de acceso y mecanismos de inspección del tráfico. Su configuración debe responder a la arquitectura de red de cada entidad y a las necesidades de comunicación de sus sistemas.

El mercado de soluciones firewall ofrece tecnologías que permiten atender estos requerimientos mediante equipos físicos, dispositivos virtuales y servicios de seguridad en la nube. Los firewall de nueva generación (NGFW) pueden incorporar funcionalidades de prevención de intrusiones, identificación de aplicaciones, filtrado web, conexiones VPN, inspección de tráfico cifrado y registro de eventos de seguridad. La disponibilidad de estas capacidades depende del modelo seleccionado y de las licencias o suscripciones contratadas.

La relación entre las estrategias TIC y este mercado también comprende la continuidad operativa de los servicios institucionales. Las entidades que dependen de plataformas digitales para desarrollar sus funciones requieren evaluar la disponibilidad de sus dispositivos de seguridad, las posibilidades de configuración redundante y los procedimientos de recuperación ante fallas. En estos casos, las soluciones firewall pueden integrarse en esquemas de alta disponibilidad para reducir el impacto de

Gobernación de Risaralda. NIT. 891 480 085-7
Calle 19 No 13 - 17 Pereira- Risaralda
PBX. +(57) (606) 3398300 - 01 8000 916 078
contactenos@risaralda.gov.co - www.risaralda.gov.co

Estudio previo para el proceso de mínima cuantía No. STIC-IPMC-052-2026

interrupciones asociadas a fallas de los equipos, sin que ello garantice por sí solo la continuidad de toda la infraestructura tecnológica.

Otro aspecto corresponde a la administración y actualización de las plataformas de seguridad existentes. Las estrategias TIC deben considerar el mantenimiento de los dispositivos firewall, la actualización de sus sistemas operativos, la revisión de las políticas de acceso y la vigencia de los servicios de protección contratados. La renovación de licencias y suscripciones permite mantener el acceso a determinadas funcionalidades, actualizaciones de seguridad y servicios de soporte, de acuerdo con las condiciones establecidas por cada fabricante.

En materia de contratación pública, la relación con el mercado se refleja en la necesidad de identificar soluciones y proveedores que puedan atender los requerimientos técnicos de la entidad. Para ello, deben evaluarse las capacidades de procesamiento de los equipos, el rendimiento con las funciones de seguridad habilitadas, la compatibilidad con la infraestructura existente, las condiciones de licenciamiento, los servicios de soporte y los costos asociados a la adquisición, renovación o mantenimiento.

Cuando la entidad dispone de una plataforma firewall previamente implementada, las decisiones de contratación deben considerar las inversiones realizadas y las condiciones técnicas necesarias para mantener su operación. La continuidad de una tecnología existente puede responder a requerimientos de compatibilidad, administración centralizada o conservación de configuraciones; sin embargo, estas circunstancias deben sustentarse mediante el análisis técnico correspondiente.

La evolución del mercado también exige revisar periódicamente las capacidades de las soluciones instaladas frente a los cambios en el tráfico de red, la incorporación de nuevos servicios digitales y las amenazas informáticas identificadas. Esto permite determinar si las necesidades institucionales pueden atenderse mediante actualizaciones, ampliaciones de capacidad, renovación de suscripciones o sustitución de equipos, según su estado tecnológico y las condiciones de soporte del fabricante.

IMPORTANCIA DE LAS SOLUCIONES FIREWALL EN LAS ENTIDADES PÚBLICAS

Las soluciones firewall constituyen un componente de la infraestructura de seguridad informática de las entidades públicas, debido a su función en la protección de las redes de comunicaciones, el control de accesos y la prevención de amenazas que pueden afectar los sistemas de información institucionales. Su implementación permite establecer mecanismos de inspección y control del tráfico de datos entre redes internas, conexiones externas y servicios tecnológicos, de acuerdo con las políticas de seguridad definidas por cada entidad.

Las entidades públicas administran información relacionada con sus procesos administrativos, financieros, contractuales y misionales, así como datos personales de ciudadanos, servidores públicos y terceros. Esta información se procesa mediante aplicaciones, bases de datos y plataformas tecnológicas que requieren medidas de protección frente a accesos no autorizados, intentos de intrusión y otras

Gobernación de Risaralda. NIT. 891 480 085-7
Calle 19 No 13 - 17 Pereira- Risaralda
PBX. +(57) (606) 3398300 - 01 8000 916 078
contactenos@risaralda.gov.co - www.risaralda.gov.co

Estudio previo para el proceso de mínima cuantía No. STIC-IPMC-052-2026

amenazas informáticas. Los firewall contribuyen a reducir estos riesgos mediante reglas de acceso, segmentación de redes y mecanismos de inspección del tráfico.

En el contexto de la transformación digital del Estado, las entidades han ampliado el uso de plataformas electrónicas, servicios en línea, sistemas de información y mecanismos de intercambio de datos con otras instituciones. Esta evolución incrementa las necesidades de conectividad y exige establecer controles sobre las comunicaciones entre los diferentes componentes de la infraestructura tecnológica. Las soluciones firewall permiten administrar dichas conexiones y aplicar políticas de seguridad según las características de los servicios y los niveles de acceso autorizados.

Los firewall de nueva generación (NGFW) incorporan funcionalidades que amplían las capacidades tradicionales de filtrado de tráfico. Dependiendo de su configuración y licenciamiento, pueden ofrecer identificación y control de aplicaciones, prevención de intrusiones, filtrado de contenido web, inspección de conexiones cifradas, protección frente a determinados programas maliciosos y administración de redes privadas virtuales (VPN). Estas capacidades permiten establecer controles de seguridad más específicos sobre las comunicaciones institucionales.

Otro aspecto corresponde a la disponibilidad y continuidad de los servicios tecnológicos. Las entidades públicas requieren mantener operativos sus sistemas de información para atender las funciones asignadas y garantizar el acceso a los servicios digitales. En este contexto, los firewall pueden configurarse mediante esquemas de alta disponibilidad y redundancia que permiten reducir las interrupciones ocasionadas por fallas de los dispositivos de seguridad. Su efectividad depende de la arquitectura implementada, las condiciones de conectividad y los procedimientos de administración y recuperación establecidos.

La utilización de soluciones firewall también guarda relación con la aplicación de los lineamientos de seguridad digital del Estado colombiano, particularmente con el Modelo de Seguridad y Privacidad de la Información (MSPI) y la Política de Gobierno Digital. Estos instrumentos orientan la gestión de riesgos de seguridad de la información y la adopción de controles para proteger los activos tecnológicos institucionales. Los firewall constituyen una de las herramientas que pueden emplearse para implementar controles de seguridad de redes, sin reemplazar las medidas organizacionales, administrativas y técnicas que corresponden a cada entidad.

Desde la perspectiva de la gestión tecnológica, la administración de los firewall comprende actividades de configuración, monitoreo, actualización y mantenimiento. La revisión periódica de las reglas de acceso, los registros de eventos y las versiones de software permite identificar configuraciones que requieren ajustes y atender vulnerabilidades conocidas. Asimismo, la vigencia de las licencias y suscripciones puede determinar la disponibilidad de actualizaciones de seguridad, servicios de inteligencia de amenazas y soporte técnico del fabricante.

Para las entidades públicas que cuentan con soluciones firewall previamente implementadas, la renovación del licenciamiento y los servicios de soporte puede ser necesaria para mantener las

Gobernación de Risaralda. NIT. 891 480 085-7
Calle 19 No 13 - 17 Pereira- Risaralda
PBX. +(57) (606) 3398300 - 01 8000 916 078
contactenos@risaralda.gov.co - www.risaralda.gov.co

Estudio previo para el proceso de mínima cuantía No. STIC-IPMC-052-2026

funcionalidades de protección contratadas y la operación de los dispositivos existentes. La ausencia de actualizaciones o la finalización del soporte del fabricante puede incrementar la exposición a vulnerabilidades y generar limitaciones para atender incidentes o fallas técnicas. Por esta razón, resulta necesario revisar el ciclo de vida de los equipos, las condiciones de garantía y la disponibilidad de actualizaciones antes de definir su continuidad operativa.

La importancia de las soluciones firewall en las entidades públicas radica en su contribución a la protección de las redes institucionales y al control de las comunicaciones que soportan los servicios tecnológicos. Su adecuada implementación, administración y actualización permite reducir la exposición a determinadas amenazas informáticas y apoyar la continuidad operativa de los sistemas de información, como parte de una estrategia de seguridad que debe contemplar otros controles y procedimientos de gestión del riesgo tecnológico.

INDICADORES ECONÓMICOS RELACIONADOS CON EL MERCADO DE TECNOLOGÍA

Producto Interno Bruto (PIB): El DANE informó que el PIB de Colombia creció 3,5 % en el segundo trimestre de 2026 frente al mismo trimestre de 2025. Este indicador ofrece contexto sobre la actividad económica general y la capacidad de inversión.

Índice de Precios al Consumidor (IPC): Según el DANE, en septiembre de 2026 la variación mensual fue 0,37 %, la acumulada del año 5,74 % y la anual 6,29 %. La inflación puede incidir en costos locales de operación, personal, transporte y servicios asociados a la comercialización tecnológica.

Tasa Representativa del Mercado (TRM): De acuerdo con el registro histórico de la TRM publicado en el Portal Nacional de Datos Abiertos, la tasa correspondiente al 30 de septiembre de 2026 fue de $3.341,23 pesos colombianos por dólar estadounidense (COP/USD).

Fecha	TRM (COP/USD)
30 de septiembre de 2025	$3.901,29
31 de octubre de 2025	$3.870,42
30 de noviembre de 2025	$3.744,43
31 de diciembre de 2025	$3.757,08
31 de enero de 2026	$3.670,47
28 de febrero de 2026	$3.766,30
31 de marzo de 2026	$3.669,96
30 de abril de 2026	$3.621,86
31 de mayo de 2026	$3.678,15
30 de junio de 2026	$3.443,59
31 de julio de 2026	$3.132,42

Gobernación de Risaralda. NIT. 891 480 085-7
Calle 19 No 13 - 17 Pereira- Risaralda
PBX. +(57) (606) 3398300 - 01 8000 916 078
contactenos@risaralda.gov.co - www.risaralda.gov.co

Estudio previo para el proceso de mínima cuantía No. STIC-IPMC-052-2026

31 de agosto de 2026	$3.202,79
30 de septiembre de 2026	$3.341,23

Durante el período comprendido entre septiembre de 2025 y septiembre de 2026, la TRM pasó de $3.901,29 a $3.341,23, lo que representa una disminución de $560,06, equivalente al 14,36 %.

Para el análisis comercial del sector TI, esta variación resulta relevante porque las soluciones de software pueden estar sujetas a condiciones comerciales denominadas en dólares estadounidenses.

Sin embargo, la disminución de la TRM no implica necesariamente una reducción proporcional del precio final de las licencias, dado que también intervienen las políticas comerciales del fabricante, las modalidades de suscripción y las condiciones de distribución.

Tasas de interés: El Banco de la República comunicó el 30 de septiembre de 2026 el aumento de la tasa de política monetaria a 12,25 %. Las condiciones de financiación pueden incidir en el costo de capital y en la operación de los agentes económicos

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 PERIMETRAL DEL DEPARTAMENTO DE RISARALDA"**.

El objeto agrupa las necesidades esenciales para la renovación y el mantenimiento 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.

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

Gobernación de Risaralda. NIT. 891 480 085-7
Calle 19 No 13 - 17 Pereira- Risaralda
PBX. +(57) (606) 3398300 - 01 8000 916 078
contactenos@risaralda.gov.co - www.risaralda.gov.co

presente y futuro cercano. La adquisición del 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

Estudio previo para el proceso de mínima cuantía No. STIC-IPMC-052-2026

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 144°. FORTALECIMIENTO DEL SECTOR TIC. El Ministerio de Tecnologías dela 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. NIT. 891 480 085-7
Calle 19 No 13 - 17 Pereira- Risaralda
PBX. +(57) (606) 3398300 - 01 8000 916 078
contactenos@risaralda.gov.co - www.risaralda.gov.co

Estudio previo para el proceso de mínima cuantía No. STIC-IPMC-052-2026

DEPARTAMENTO DE RISARALDA	ADQUIRIR LICENCIAMIENTO DE SOFWARE ANTIVIRUS PARA LA ADMINISTRACION DEPARTAMENTAL	Selección abreviada subasta inversa	STIC-SASI-031-2021	30 (Días)	$69.949.152
DEPARTAMENTO DE RISARALDA	LICENCIAMIENTO DE SOFTWARE	Selección abreviada por subasta inversa	STIC-SASI-020-2023	30 (Días)	$149.500.000
DEPARTAMENTO 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
DEPARTAMENTO DE RISARALDA	ADQUISICIÓN DE LICENCIAS PARA EL FIREWALL DEL SISTEMA DE SEGURIDAD PERIMETRAL DEL DEPARTAMENTO DE RISARALDA	Invitación pública de Mínima Cuantía	STIC-IPMC-42-2025	30 (Días)	$69.508.856

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	DURACIO N	VALOR

Gobernación de Risaralda. NIT. 891 480 085-7
Calle 19 No 13 - 17 Pereira- Risaralda
PBX. +(57) (606) 3398300 - 01 8000 916 078
contactenos@risaralda.gov.co - www.risaralda.gov.co

Estudio previo para el proceso de mínima cuantía No. STIC-IPMC-052-2026

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 una solución de licencias para correo electrónico existen diferentes marcas, soporte, garantía o vencimiento que las entidades pueden exigir de acuerdo con su necesidad.

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 prestar el servicio que se requiere contratar en el presente proceso, lo que garantiza la pluralidad de oferentes.

Estudio previo para el proceso de mínima cuantía No. STIC-IPMC-052-2026

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

Es importante mencionar que frente a la necesidad y dentro del estudio de mercado la Secretaria de Tecnologías de la Información y la Comunicación, conforme a los principios de economía, eficacia y planeación de la contratación estatal (Ley 80 de 1993, Ley 1150 de 2007 y Decreto 1082 de 2015), adopta como precio de referencia el valor histórico de adjudicación del mismo objeto contractual en la vigencia inmediatamente anterior: "ADQUISICIÓN DE LICENCIAS PARA EL FIREWALL DEL SISTEMA DE SEGURIDAD PERIMETRAL DEL DEPARTAMENTO DE RISARALDA", incrementado con el porcentaje del Índice de Precios al Consumidor (IPC). Por tal motivo, 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 son:

RAZON SOCIAL	NIT
INGENIERIA TELEMATICA S.A.S.	816007833
ELLIPTICAL SAS	900138327
WEXLER SAS	900390198

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, conforme a los principios de economía, eficacia y planeación de la contratación estatal (Ley 80 de 1993, Ley 1150 de 2007 y Decreto 1082 de 2015), se adopta como precio de referencia el valor histórico de adjudicación del mismo objeto contractual en la vigencia inmediatamente anterior: "ADQUISICIÓN DE LICENCIAS PARA EL FIREWALL DEL SISTEMA DE SEGURIDAD PERIMETRAL DEL DEPARTAMENTO DE RISARALDA", debidamente incrementado con el porcentaje del Índice de Precios al Consumidor (IPC) del 5,1%.

La aplicación de esta metodología permite establecer valores de referencia actualizados a la vigencia 2026, como insumo para el análisis económico del sector y la estimación del presupuesto del proceso contractual.

Gobernación de Risaralda. NIT. 891 480 085-7
Calle 19 No 13 - 17 Pereira- Risaralda
PBX. +(57) (606) 3398300 - 01 8000 916 078
contactenos@risaralda.gov.co - www.risaralda.gov.co

Estudio previo para el proceso de mínima cuantía No. STIC-IPMC-052-2026

Se precisa que los valores obtenidos corresponden a una proyección basada en información histórica y no constituyen cotizaciones comerciales vigentes ni representan necesariamente los precios actuales del mercado. En particular, tratándose de licenciamiento de software firewall, los precios pueden variar según las políticas comerciales del fabricante, las condiciones de licenciamiento, la tasa de cambio y demás factores propios del mercado tecnológico.

En consecuencia, los valores proyectados se consideran un referente económico para la estructuración del estudio previo, sin que su utilización sustituya la verificación de las condiciones actuales del mercado ni los demás soportes requeridos para sustentar el presupuesto oficial del proceso de contratación.

Con base en lo anterior, el cálculo del precio de referencia estimado, se obtendrá a partir de la siguiente fórmula:

$$\boldsymbol{V_e = V_h \times (1 + IPC)}$$

Donde:

- V_e: Valor estimado del contrato para la presente vigencia.
- V_h: Valor histórico de adjudicación del contrato en la vigencia inmediatamente anterior.
- IPC: Índice de Precios al Consumidor expresada en formato decimal (Índice de Precios al Consumidor correspondiente al año 2025, publicado por el Departamento Administrativo Nacional de Estadística (DANE)), equivalente al 5,10 %.

5.2. Cálculo promedio Estudio de Mercado

FIREWALL

PROYECCIÓN PRECIO FIREWALL 2026	
IPC anual 2025 (DANE)	5,10%
Criterio	Actualización referencial de valor contrato adjudicado 2025
Fuente	DANE, IPC diciembre 2025

VALOR 2025 (COP)	IPC	INCREMENTO (COP)	PROYECCIÓN 2026 (COP)
$ 69.508.856,00	5,10%	$ 3.544.951,66	$ 73.053.807,66

Teniendo en cuenta la proyección realizada previamente, el valor total del presupuesto que se requiere para el proceso que se pretende contratar para Firewall es por la suma de **SETENTA Y TRES MILLONES CINCUENTA Y TRES MIL OCHOCIENTOS OCHO PESOS M/CTE ($73.053.808) INCLUIDO IVA** y demás cargos en que pueda incurrir el contratista.

Es necesario indicar que la aplicación de esta metodología permite establecer valores de referencia actualizados a la vigencia 2026, como insumo para el análisis económico del sector y la estimación del presupuesto del proceso contractual.

Gobernación de Risaralda. NIT. 891 480 085-7
Calle 19 No 13 - 17 Pereira- Risaralda
PBX. +(57) (606) 3398300 - 01 8000 916 078
contactenos@risaralda.gov.co - www.risaralda.gov.co

Estudio previo para el proceso de mínima cuantía No. STIC-IPMC-052-2026

Se precisa que los valores obtenidos corresponden a una proyección basada en información histórica y no constituyen cotizaciones comerciales vigentes ni representan necesariamente los precios actuales del mercado. En particular, tratándose de licenciamiento de software Firewall, los precios pueden variar según las políticas comerciales del fabricante, las condiciones de licenciamiento, la tasa de cambio y demás factores propios del mercado tecnológico.

En consecuencia, los valores proyectados se consideran un referente económico para la estructuración del estudio previo, sin que su utilización sustituya la verificación de las condiciones actuales del mercado ni los demás soportes requeridos para sustentar el presupuesto oficial del proceso de contratación.

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 COMUNICACION, 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 del Decreto 1082 de 2015.

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.

Gobernación de Risaralda. NIT. 891 480 085-7
Calle 19 No 13 - 17 Pereira- Risaralda
PBX. +(57) (606) 3398300 - 01 8000 916 078
contactenos@risaralda.gov.co - www.risaralda.gov.co

Estudio previo para el proceso de mínima cuantía No. STIC-IPMC-052-2026

Que a pesar de las afectaciones estructurales sufridas en las instalaciones de la Gobernación de Risaralda, a raíz del sismo registrado el pasado 10 de agosto y, dado que allí se encontraba el centro de datos con su infraestructura tecnológica, fue necesario trasladar temporalmente el respectivo centro de datos a una sede alterna del Departamento de Risaralda, ubicado en la ciudad de Pereira - Coordinación Departamental de Gestión del riesgo y Desastres (CDGRD), con el fin de garantizar la continuidad de los servicios y la operatividad institucional.

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 el Departamento 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 el Departamento 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

Gobernación de Risaralda. NIT. 891 480 085-7
Calle 19 No 13 - 17 Pereira- Risaralda
PBX. +(57) (606) 3398300 - 01 8000 916 078
contactenos@risaralda.gov.co - www.risaralda.gov.co

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 entidad, 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.

Gobernación de Risaralda. NIT. 891 480 085-7
Calle 19 No 13 - 17 Pereira- Risaralda
PBX. +(57) (606) 3398300 - 01 8000 916 078
contactenos@risaralda.gov.co - www.risaralda.gov.co

Estudio previo para el proceso de mínima cuantía No. STIC-IPMC-052-2026

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

Gobernación de Risaralda. NIT. 891 480 085-7
Calle 19 No 13 - 17 Pereira- Risaralda
PBX. +(57) (606) 3398300 - 01 8000 916 078
contactenos@risaralda.gov.co - www.risaralda.gov.co

Estudio previo para el proceso de mínima cuantía No. STIC-IPMC-052-2026

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.

    - **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

Gobernación de Risaralda. NIT. 891 480 085-7
Calle 19 No 13 - 17 Pereira- Risaralda
PBX. +(57) (606) 3398300 - 01 8000 916 078
contactenos@risaralda.gov.co - www.risaralda.gov.co

Estudio previo para el proceso de mínima cuantía No. STIC-IPMC-052-2026

cumplir con sus funciones, se requiere contratar los servicios requeridos.

Por otro lado, se requiere la implementación de medidas que redunden en seguridad, a través de una **Evaluación Operativa mediante Prueba de Penetración (Pentesting).**

Si bien la adquisición del licenciamiento perimetral Enterprise para el dispositivo FortiGate 401F y la plataforma FortiAnalyzer-VM garantiza la prevención de intrusiones (IPS), el filtrado web, el análisis de reputación y la correlación de eventos en tiempo real, la seguridad de la información de la Entidad requiere un enfoque de redundancia y validación constante. Para asegurar que las políticas del firewall y las configuraciones del entorno tecnológico respondan eficazmente frente a amenazas reales, se hace indispensable complementar la protección perimetral con la ejecución de un Anexo Técnico de Prueba de Penetración a cinco (5) servidores, sin generar costos adicionales a la oferta económica.

Prueba de Penetración a cinco (5) servidores · Gobernación de Risaralda

Como obligación específica del contrato, el contratista ejecutará una prueba de penetración sobre cinco (5) servidores del Departamento de Risaralda, desde su red interna y desde internet. Su costo deberá estar incluido en el valor de la oferta.

¿Cuál es la finalidad?

Descubrir los servicios que expone cada servidor y comprobar, de forma controlada y no destructiva, las brechas de seguridad explotables, para que la Entidad las corrija. El resultado aporta evidencia a la gestión de vulnerabilidades técnicas del MSPI de MinTIC (Decreto 767 de 2022) y al control 8.8 de ISO/IEC 27001:2022.

Alcance de la prueba de penetración

Cinco (5) servidores: dos (2) con Oracle Linux y tres (3) con Debian o Ubuntu. La Entidad entrega la dirección IP o el FQDN de cada uno en la reunión de inicio, bajo confidencialidad.

- **Puntos de prueba:** desde la red interna de la Entidad, por VPN o por un punto de prueba que ella habilite, y desde internet para los servicios publicados.
- **Descubrimiento:** inventario de todos los puertos y servicios que exponga cada servidor, con su tecnología y versión.
- **Servicios de red:** versiones con vulnerabilidades conocidas o explotadas activamente (catálogo CISA KEV), credenciales por defecto o débiles, configuración insegura, cifrado y protocolos débiles, y sistema operativo o componentes fuera de soporte.
- **Servicios web:** si el servidor tiene una aplicación web o API, publicada o solo interna, se prueba su superficie sin autenticar frente al OWASP Top 10: inyecciones, control de acceso, manejo de sesión y exposición de datos.

Gobernación de Risaralda. NIT. 891 480 085-7
Calle 19 No 13 - 17 Pereira- Risaralda
PBX. +(57) (606) 3398300 - 01 8000 916 078
contactenos@risaralda.gov.co - www.risaralda.gov.co

Estudio previo para el proceso de mínima cuantía No. STIC-IPMC-052-2026

Condiciones de ejecución de la prueba

- **Método:** NIST SP 800-115 y OWASP WSTG; cada hallazgo se mapea a MITRE ATT&CK y se califica con CVSS.
- **Comprobación:** cada brecha se demuestra con un marcador inofensivo o se reporta como indicio por validar. No se acepta un reporte automático de escáner sin comprobación ni análisis.
- **Autorización:** ninguna prueba inicia sin la autorización escrita y las reglas de enfrentamiento firmadas por la Entidad (Ley 1273 de 2009).
- **Sin afectar la operación:** no se modifican ni borran datos, no hay pruebas de denegación de servicio, se hacen como máximo dos intentos de autenticación por cuenta y la prueba se suspende si un servicio se degrada.
- **Aviso inmediato:** toda brecha crítica comprobada se notifica a la Entidad el mismo día.
- **Confidencialidad:** acuerdo de confidencialidad, entrega por canal cifrado, datos personales enmascarados (Ley 1581 de 2012) y eliminación certificada de las copias de trabajo al cierre.

Entregables y plazo

- Informe ejecutivo para la dirección: nivel de riesgo y qué corregir primero.
- Informe técnico para TI: por hallazgo, evidencia con huella SHA-256, impacto, recomendación y control de ISO/IEC 27001 asociado.
- Una sesión de socialización de resultados.
- Una re-prueba de los hallazgos críticos y altos, dentro de los 60 días siguientes a la entrega del informe técnico.

1.1 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.

Gobernación de Risaralda. NIT. 891 480 085-7
Calle 19 No 13 - 17 Pereira- Risaralda
PBX. +(57) (606) 3398300 - 01 8000 916 078
contactenos@risaralda.gov.co - www.risaralda.gov.co

Estudio previo para el proceso de mínima cuantía No. STIC-IPMC-052-2026

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.

Gobernación de Risaralda. NIT. 891 480 085-7
Calle 19 No 13 - 17 Pereira- Risaralda
PBX. +(57) (606) 3398300 - 01 8000 916 078
contactenos@risaralda.gov.co - www.risaralda.gov.co

Estudio previo para el proceso de mínima cuantía No. STIC-IPMC-052-2026

- **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.

Estudio previo para el proceso de mínima cuantía No. STIC-IPMC-052-2026

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 el Departamento de Risaralda 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. Detecta y elimina malware en archivos, tráfico de red y sitios web. 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. Previene ataques contra vulnerabilidades en servidores, aplicaciones y dispositivos. 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. Bloquea el acceso a sitios de phishing, malware o contenido no deseado. Mejora la seguridad y productividad al controlar el acceso a internet.
- **Control de Aplicaciones:** Identifica y controla el uso de aplicaciones en la red. Permite o bloquea aplicaciones específicas en la red, como redes sociales, juegos, etc. 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. Filtra correos electrónicos maliciosos antes de que lleguen a los usuarios. 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

Gobernación de Risaralda. NIT. 891 480 085-7
Calle 19 No 13 - 17 Pereira- Risaralda
PBX. +(57) (606) 3398300 - 01 8000 916 078
contactenos@risaralda.gov.co - www.risaralda.gov.co

a la red. Detecta amenazas avanzadas y malware de día cero. 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. Impide la conexión a dominios que se sabe que son maliciosos. 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. Brinda asistencia técnica en caso de problemas, fallos de configuración o consultas técnicas. 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. Minimiza el tiempo de inactividad en caso de fallas de hardware.
- **Actualizaciones de firmware:** Permite acceder a las últimas versiones de FortiOS, que incluyen mejoras de seguridad y nuevas funciones. Mantener el firewall actualizado con las últimas características y parches de seguridad.
- **Parches de seguridad:** Actualizaciones rápidas para corregir vulnerabilidades críticas detectadas en el sistema. Proteger el dispositivo de cualquier vulnerabilidad que pueda comprometer la seguridad.
- **24x7 FortiCare:** La Gobernación debe tener acceso a un equipo de soporte técnico dedicado que está disponible en todo momento.
- **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.
- **Acceso a actualizaciones y parches de seguridad:** La Gobernación de Risaralda con la licencia Enterprise recibe acceso a las últimas actualizaciones.
- **Recursos y herramientas adicionales:** Acceso a una amplia gama de recursos, como documentación técnica, guías de implementación, bases de conocimientos y herramientas de diagnóstico.

3. Licencia FortiAnalyzer-VM Support

- **Soporte 24x7:** Acceso a soporte técnico las 24 horas del día, los 7 días de la semana. Brinda asistencia técnica en caso de problemas, fallos de configuración o consultas técnicas. 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. Minimiza el tiempo de inactividad en caso de fallas de hardware.
- **Actualizaciones de firmware:** Permite acceder a las últimas versiones de FortiOS, que incluyen mejoras de seguridad y nuevas funciones. Mantener el firewall actualizado con las últimas características y parches de seguridad.
- **Parches de seguridad:** Actualizaciones rápidas para corregir vulnerabilidades críticas detectadas

en el sistema. Proteger el dispositivo de cualquier vulnerabilidad que pueda comprometer la seguridad.

- **24x7 FortiCare:** La Gobernación debe tener acceso a un equipo de soporte técnico dedicado que está disponible en todo momento.
- **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.
- **Acceso a actualizaciones y parches de seguridad:** La Gobernación de Risaralda con la licencia Enterprise recibe acceso a las últimas actualizaciones.

Recursos y herramientas adicionales: Acceso a una amplia gama de recursos, como documentación técnica, guías de implementación, bases de conocimientos y herramientas de diagnóstico.

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 presente inversión apunta con el plan de desarrollo "RISARALDA EQUITATIVA E INCLUYENTE" DIMENSIÓN 4 BUEN GOBIERNO- GESTIÓN Y FORTALECIMIENTO INSTITUCIONAL. Programa: “Facilitar el acceso y uso de las Tecnologías de la Información y las Comunicaciones en todo el territorio nacional” Objetivo: “Desarrollar estrategias de gobierno electrónico para mejorar la eficiencia administrativa y la transparencia en la gestión pública, facilitando trámites y servicios en línea para los ciudadanos”. Certificado de Conveniencia, Oportunidad y Registro de Actividades No. **BP- 6413 del 23/10/2026** Actividad: Prestar servicios de mantenimiento al centro de datos del departamento de Risaralda.

Por lo anterior expuesto es conveniente la realización de un proceso por **INVITACION PUBLICA DE MINIMA CUANTIA,** para realizar un contrato con una persona natural o jurídica que reúna las condiciones según perfil, que este en capacidad de coordinar integralmente cualquier eventualidad que se presente dentro de la administración.

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

Código: 2024003660059

Actividad: PRESTAR SERVICIOS DE MANTENIMIENTO AL CENTRO DE DATOS DEL DEPARTAMENTO DE RISARALDA.

Certificado de Conveniencia, Oportunidad y Registro de Actividades: No. BP- BP- 6413 del 23/10/2026.

1.2 Plan Anual de Adquisición

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

Estudio previo para el proceso de mínima cuantía No. STIC-IPMC-052-2026

1.3 Plan de Acción

El contrato que se pretende celebrar se encuentra dentro del plan de acción de la Secretaría de Hacienda.

1.4 Ordenanza de facultades

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.

2. Objeto a contratar

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

2.1 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.

2.2 Especificaciones técnicas del objeto a contratar

Listado de Elementos de Software:

- Licencia de Seguridad Perimetral
- Licencia de Sistema de Registros y Estadísticas (incluida con la licencia de seguridad perimetral)
- Prueba de Penetración (Pentesting) a cinco (5) servidores

2.2.1. FICHA TECNICA No. 1

Grupo	1
Ítem	1
Código UNSPSC	43233200
Elemento	Licencia de Seguridad Perimetral
Fabricante	Fortinet
Producto	Fortigate

Gobernación de Risaralda. NIT. 891 480 085-7
Calle 19 No 13 - 17 Pereira- Risaralda
PBX. +(57) (606) 3398300 - 01 8000 916 078
contactenos@risaralda.gov.co - www.risaralda.gov.co

Estudio previo para el proceso de mínima cuantía No. STIC-IPMC-052-2026

Referencia	401F
Cantidad	1
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, Advanced Malware Protection, Application Control, Web & Video Filtering, Antispam, Security Rating, IoT Detection, Industrial Security, FortiConverter Service, FortiCare 7x24x365, AI-based Inline Malware Prevention
Esquema de Licenciamiento	Enterprise
Idioma	Multi-Idioma
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

ANEXO 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
Licencias Incluidas	1 Licencia FortiAnalyzer-VM Support 7x24x365 FortiCare Contract (1-6 GB/Day), 1 Licencia FortiGuard Indicator of Compromise (IOC), 1 Licencia FortiAnalyzer SOC service
Programas Incluidos	Plataforma de logs y reportes
Esquema de Licenciamiento	Enterprise
Vigencia	12 meses a partir de la instalación
Nota	Registrado a nombre del "Departamento de

Gobernación de Risaralda. NIT. 891 480 085-7
Calle 19 No 13 - 17 Pereira- Risaralda
PBX. +(57) (606) 3398300 - 01 8000 916 078
contactenos@risaralda.gov.co - www.risaralda.gov.co

Estudio previo para el proceso de mínima cuantía No. STIC-IPMC-052-2026

	Risaralda" (sistemas@risaralda.gov.co)
Garantía y Soporte	Garantía y soporte de fábrica por 1 año

2.2.2. Soporte técnico y Requisitos

- **Servicios Incluidos:** Renovación, Configuración y transferencia de conocimiento, Soporte preventivo y correctivo modalidad 7x24 por un año.
- **Esquema:** 7 x 24 x 365 | Modalidad: Presencial, Remoto, Telefónico.
- **Actualizaciones:** El servicio de soporte Premium también incluye acceso a las últimas actualizaciones de firmware y mejoras de software para FortiAnalyzer-VM y FortiGate 401F.
- **Vc Tiempos de Respuesta:** Severidad Crítica (Respuesta remota máx. 30 min, presencia sitio máx. 3 hrs); Alta (Remota máx. 1 hr, sitio máx. 4 hrs); Media/Baja (Remota máx. 4 hrs).

2.2.3. Otros requisitos Técnicos (habilitantes)

- **Certificación de Habilitación del Partner:** Nivel Select, Advanced o Expert emitido por Fortinet.
  El proponente deberá acreditar su capacidad técnica y comercial mediante la presentación de una Carta o Certificación expedida directamente por el fabricante Fortinet, vigente a la fecha de cierre del proceso de selección- habilitado para distribuir soluciones de ciberseguridad en el país.
- **Nivel de membresía:** El proponente deberá acreditar ser Canal autorizado para comercializar Fortigate y FortiAnalyzer en Colombia, en las categorías actualmente reconocidas por el fabricante.

- **Personal Requerido:**

  - **Perfil 1 – Líder de proyecto / Especialista en seguridad de red:** Título profesional en Ingeniería de Sistemas/Electrónica/Telecomunicaciones, Maestría en Ciberseguridad/Seguridad de la Información, certificaciones Fortinet NSE 6 Secure networking y NSE 7. Secure networking. Deberá aportar los siguientes documentos: Tarjeta profesional, certificación del COPNIA y hoja de vida de la función pública.
  - **Perfil 2 – Ingeniero de soporte y operaciones de seguridad:** Título profesional en ingeniería de sistemas o afines, certificaciones Fortinet NSE 4 FortiOs y NSE 5 Security Operations. Deberá aportar los siguientes documentos: Tarjeta profesional, certificación del COPNIA y hoja de vida de la función pública.

- **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.

3. Obligaciones de las partes

3.1. Obligaciones del contratista

Gobernación de Risaralda. NIT. 891 480 085-7
Calle 19 No 13 - 17 Pereira- Risaralda
PBX. +(57) (606) 3398300 - 01 8000 916 078
contactenos@risaralda.gov.co - www.risaralda.gov.co

Estudio previo para el proceso de mínima cuantía No. STIC-IPMC-052-2026

3.1.1. Obligaciones Generales del Contratista:

a. Ejecutar el objeto del Contrato en las condiciones de calidad, oportunidad, y obligaciones definidas en los Documentos del Proceso de contratación
b. Cumplir con las especificaciones técnicas del objeto presentadas en la oferta.
c. Dar a conocer al Departamento cualquier reclamación, petición, orden o similar de terceros que indirecta o directamente pueda tener algún efecto sobre la ejecución del Contrato o sobre sus obligaciones.
d. Obrar con lealtad y buena fe en el desarrollo del contrato.
e. El contratista debe ejecutar el contrato cumpliendo estándares ambientales, reduciendo los impactos que generan sus actividades contractuales; cuando sea el caso debe participar en actividades de implementación y fomento de un servicio de calidad y de buenas prácticas ambientales y de eficiencia energética.
f. Ejecutar el objeto del Contrato en las condiciones de calidad, oportunidad, y obligaciones definidas en los Documentos del Proceso de contratación.
g. Cumplir con las especificaciones técnicas del objeto presentadas en la oferta.
h. Dar a conocer al Departamento cualquier reclamación, petición, orden o similar de terceros que indirecta o directamente pueda tener algún efecto sobre la ejecución del Contrato o sobre sus obligaciones.
i. Obrar con lealtad y buena fe en el desarrollo del contrato.
j. En cumplimiento con el Decreto 287 de 2026 ARTÍCULO 2.2.1.2.4.2.7.5. Subcontratación inclusiva: Cuando para la ejecución del contrato se requiera subcontratar bienes, obras, o servicios dentro de la cadena de provisión, se deberá punzonar la contratación de personas naturales con discapacidad y lo emprendimientos y empresas de personas con discapacidad, conforme a los criterios definidos en el artículo 2.2.1.2.4.2.6. del presente Decreto.
k. Afinar las políticas de seguridad informática de soporte implementadas, documentando el proceso.
l. 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).
m. 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.
n. 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.
o. El contratista deberá contar con usuario activo en la plataforma SECOP II.

3.1.2. Obligaciones Específicas 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,

Gobernación de Risaralda. NIT. 891 480 085-7
Calle 19 No 13 - 17 Pereira- Risaralda
PBX. +(57) (606) 3398300 - 01 8000 916 078
contactenos@risaralda.gov.co - www.risaralda.gov.co

Estudio previo para el proceso de mínima cuantía No. STIC-IPMC-052-2026

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. 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.
3. Brindar soporte técnico preventivo, correctivo modalidad 7x24x365 por espacio de 12 meses a partir de la firma del acta de inicio.
4. Brindar 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.
5. Ejecutar una prueba de penetración sobre cinco (5) servidores del Departamento de Risaralda (2 con Oracle Linux y 3 con Debian o Ubuntu), desde su red interna y desde internet.
6. Para la prueba descrita en el numeral 5., el contratista deberá suministrar los siguientes entregables: **i.** Informe ejecutivo para la dirección: nivel de riesgo y qué corregir primero; **ii.** Informe técnico para TI: por hallazgo, evidencia con huella SHA-256, impacto, recomendación y control de ISO/IEC 27001 asociado; **iii.** Una sesión de socialización de resultados; **iv.** Una re-prueba de los hallazgos críticos y altos, dentro de los 60 días siguientes a la entrega del informe técnico.
7. 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.
8. Aplicar oportunamente las últimas versiones de firmware que se encuentren disponibles y debidamente probadas y disponibles por parte del fabricante.
9. 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.
10. Monitorear e informar el desempeño de la licencia del dispositivo y los eventos detectados por el mismo.
11. Afinamiento de las funcionalidades de inspección de tráfico, donde incluya SSL inspection y desplegar los certificados digitales, documentando el proceso.
12. Atender todos requerimientos y/o acciones correctivas que se requieran por parte de GOBERNACIÓN DE 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.
13. Afinamiento del sistema wifi y creación de políticas de seguridad aplicadas a las SSID, documentando el proceso.
14. Detectar e informar los incidentes de seguridad informática presentando en a la infraestructura tecnológica controlada por el dispositivo licenciado.
15. Registrar, clasificar e informar los incidentes de seguridad informática presentando en a la infraestructura tecnológica controlada por el dispositivo licenciado.
16. 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

Gobernación de Risaralda. NIT. 891 480 085-7
Calle 19 No 13 - 17 Pereira- Risaralda
PBX. +(57) (606) 3398300 - 01 8000 916 078
contactenos@risaralda.gov.co - www.risaralda.gov.co

Estudio previo para el proceso de mínima cuantía No. STIC-IPMC-052-2026

previa de copia de seguridad de las configuraciones presenten en el dispositivo de la Entidad dispositivo FortiGate 401F

17. Aplicar configuración técnica al dispositivo de contingencia en caso de hacer uso del mismo, documentando el proceso.
18. Entregar un plan de contingencia detallado que incluya procedimientos para la recuperación de la configuración y los datos en caso de desastre.
19. 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.
20. 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.
21. Atender los requerimientos realizados por el Departamento de Risaralda por intermedio del funcionario encargado de la supervisión del contrato.
22. 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).

3.1.3 Productos por entregar por el contratista

Software y hardware descrito en las especificaciones técnicos en correcto funcionamiento.

3.1.4 Obligaciones del nivel de servicio:

Tiempo de respuesta mantenimiento correctivo:

Severidad Crítica (Respuesta remota máx. 30 min, presencia sitio máx. 3 hrs); Alta (Remota máx. 1 hr, sitio máx. 4 hrs); Media/Baja (Remota máx. 4 hrs).

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.

Gobernación de Risaralda. NIT. 891 480 085-7
Calle 19 No 13 - 17 Pereira- Risaralda
PBX. +(57) (606) 3398300 - 01 8000 916 078
contactenos@risaralda.gov.co - www.risaralda.gov.co

Estudio previo para el proceso de mínima cuantía No. STIC-IPMC-052-2026

3.2. Obligaciones del Departamento:

a. Designar un supervisor que realice la vigilancia, control y seguimiento del contrato.
b. Realizar el pago de acuerdo a lo estipulado en el contrato.
c. Exigir al contratista la ejecución idónea y oportuna de las obligaciones del presente contrato.
d. Suministrar la información que previamente requiera el contratista en relación con el objeto del presente contrato.
e. Suscribir conjuntamente con el contratista las actas y los demás documentos necesarios
f. para la ejecución y liquidación de este contrato.

4. Plazo de ejecución del contrato

El plazo de ejecución del contrato será de un (1) mes calendario, sin que exceda el 31 de diciembre de 2026.

5. Lugar de ejecución del contrato

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

6. Valor estimado del contrato/ presupuesto oficial y su justificación

El presupuesto total del contrato será hasta por la suma de **SETENTA Y TRES MILLONES CINCUENTA Y TRES MIL OCHOCIENTOS OCHO PESOS M/CTE ($73.053.808) INCLUIDO IVA** incluido el impuesto al valor agregado (I.V.A), cuando a ello hubiere lugar y demás impuestos, tasas, contribuciones de carácter nacional y/o departamental y/o municipal de carácter legal, costos directos e indirectos.

Para la realización del cálculo anterior, se adoptó como precio de referencia el valor histórico de adjudicación del mismo objeto contractual en la vigencia inmediatamente anterior, debidamente incrementado con el porcentaje del Índice de Precios al Consumidor (IPC) del 5,1%.

Teniendo en cuenta la proyección realizada previamente, el valor total del presupuesto que se requiere para el proceso que se pretende contratar es la suma de **SETENTA Y TRES MILLONES CINCUENTA Y TRES MIL OCHOCIENTOS OCHO PESOS M/CTE ($73.053.808) INCLUIDO IVA** y demás cargos en que pueda incurrir el contratista.

PROYECCIÓN PRECIO FIREWALL 2026	
IPC anual 2025 (DANE)	5,10%
Criterio	Actualización referencial de valor contrato adjudicado 2025
Fuente	DANE, IPC diciembre 2025

Gobernación de Risaralda. NIT. 891 480 085-7
Calle 19 No 13 - 17 Pereira- Risaralda
PBX. +(57) (606) 3398300 - 01 8000 916 078
contactenos@risaralda.gov.co - www.risaralda.gov.co

Estudio previo para el proceso de mínima cuantía No. STIC-IPMC-052-2026

VALOR 2025 (COP)	IPC	INCREMENTO (COP)	PROYECCIÓN 2026 (COP)
$ 69.508.856,00	5,10%	$ 3.544.951,66	$ 73.053.807,66

La aplicación de esta metodología permite establecer valores de referencia actualizados a la vigencia 2026, como insumo para el análisis económico del sector y la estimación del presupuesto del proceso contractual.

Se precisa que los valores obtenidos corresponden a una proyección basada en información histórica y no constituyen cotizaciones comerciales vigentes ni representan necesariamente los precios actuales del mercado. En particular, tratándose de licenciamiento de software Firewall, los precios pueden variar según las políticas comerciales del fabricante, las condiciones de licenciamiento, la tasa de cambio y demás factores propios del mercado tecnológico.

En consecuencia, los valores proyectados se consideran un referente económico para la estructuración del estudio previo, sin que su utilización sustituya la verificación de las condiciones actuales del mercado ni los demás soportes requeridos para sustentar el presupuesto oficial del proceso de contratación.

6.1 Aspectos tributarios y financieros del contrato

TASA O ESTAMPILLA	BASE GRAVABLE	APLICA SI/NO	FORMA DE PAGO
Estampilla Procultura (Contratos celebrados por el Departamento de Risaralda y sus entes descentralizados mayor a 1640 UVT). ($52.374) (Resolución 000238 del 15 de diciembre de 2025).	1,5%	**NO**	Persona Natural: Será descontado en el primer pago que se realice al contratista. (Par. 1 Art. 248 Estatuto de Rentas) 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) 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) Persona jurídica: Será descontado o retenido en cada cuenta y orden de pago. (Par. 2 Art. 238 Estatuto de Rentas)

Gobernación de Risaralda. NIT. 891 480 085-7
Calle 19 No 13 - 17 Pereira- Risaralda
PBX. +(57) (606) 3398300 - 01 8000 916 078
contactenos@risaralda.gov.co - www.risaralda.gov.co

Estudio previo para el proceso de mínima cuantía No. STIC-IPMC-052-2026

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) 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%	**SI**	Será descontado o retenido en cada comprobante de egreso u orden de pago.
Estampilla pro hospitales universitarios – (contratos celebrados en la Secretaría Departamental de Salud, y en las entidades Descentralizadas del orden Departamental y Municipal).	2%	**NO**	Persona Natural: Será descontado en el primer pago que se realice al contratista. (Par. 1 Art. 229 Estatuto de Rentas) Persona jurídica: Será descontado o retenido en la cuenta y orden de pago. (Par. 2 Art. 229 Estatuto de Rentas)

6.2 Disponibilidad Presupuestal

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

CERT. DISPONIBILIDAD PRESUPUESTAL	CENTRO DE COSTO- RUBRO PRESUPUESTAL Y FONDO	SECRETARIA Y VALOR	VALOR AFECTAR
2724 del 06/03/2026 BP- 6413 del 23/10/2026	0314- 2.3.2.01.01.005.02.03.01.01- 20 PROYECTO: 2024003660036	Secretaría de Tecnologías de la Información y la Comunicación $91.600.000	Valor de adjudicación.

6.2.1 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

6.3 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

Gobernación de Risaralda. NIT. 891 480 085-7
Calle 19 No 13 - 17 Pereira- Risaralda
PBX. +(57) (606) 3398300 - 01 8000 916 078
contactenos@risaralda.gov.co - www.risaralda.gov.co

Estudio previo para el proceso de mínima cuantía No. STIC-IPMC-052-2026

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 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.

6.3.1 Anticipo

Para la ejecución del contrato NO se requiere la entrega de anticipo.

7. 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.

8. Evaluación de las ofertas:

La Entidad evaluará la oferta de menor precio y verificará que cumpla las condiciones mínimas de la invitación. Si no cumple solicitará al Proponente, mínimo por el término de un (1) día hábil, que aclare, explique o aporte los documentos e información subsanable; en caso de que la Entidad no fije un plazo específico, se entenderá que es de un (1) día hábil siguiente al día que se hizo el requerimiento. No obstante, los Proponentes no podrán completar, adicionar, modificar o mejorar la oferta económica, la cual solo puede ser objeto de aclaraciones y explicaciones. Los Proponentes deben aportar las aclaraciones o documentos requeridos hasta el plazo indicado, so pena que la Entidad rechace la propuesta y revise la segunda oferta que ofrezca el menor precio y verifique que cumple los requisitos de la invitación. Si la segunda propuesta tampoco cumple se repetirá el procedimiento anterior, continuando con las ofertas que ofrezcan el siguiente menor precio.

En caso de que la Entidad advierta la ausencia de requisitos o la falta de documentos referentes a la futura contratación o al Proponente, y no los haya requerido durante el proceso de evaluación, requerirá al Proponente, otorgándole un término mínimo de un (1) día hábil contado desde el momento en el que advirtió su omisión, con el fin de que los aporte; en caso de que la Entidad no fije un plazo específico, se entenderá que es de un (1) día hábil siguiente al día que se hizo el requerimiento.

Una vez se identifica la oferta de menor valor que cumple los requisitos mínimos de la invitación, la Entidad publicará el informe de evaluación en el cual constará la evaluación de las ofertas. Allí se indicará, entre otros aspectos, cuál oferente ofreció el menor precio y cumplió con los requisitos de

Gobernación de Risaralda. NIT. 891 480 085-7
Calle 19 No 13 - 17 Pereira- Risaralda
PBX. +(57) (606) 3398300 - 01 8000 916 078
contactenos@risaralda.gov.co - www.risaralda.gov.co

la invitación.

***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.*

9. Control y vigilancia del contrato

La Supervisión para el presente Contrato, será ejercida por un funcionario de funcionario de la SECRETARIA DE TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACIÓN, quién se constituye en el enlace entre las partes. Como supervisores verificarán 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.

10. Maduración del proyecto

N.A

11. Bienes agrícolas

N.A

12. 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.

13. Garantías

La entidad requiere la constitución de los siguientes amparos:

13.1. 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.

Justificación: Esta garantía se exige con el fin de garantizar el cubrimiento de un posible incumplimiento que pudiera llegar a atribuirse al contratista, para lo cual la entidad estaría cubierta de los perjuicios que pudiere llegarse a causar.

13.2. Calidad del Servicio: Por el VEINTE POR CIENTO (20%) del valor del contrato, por el término

Estudio previo para el proceso de mínima cuantía No. STIC-IPMC-052-2026

del mismo y hasta la liquidación del contrato (mínimo seis meses)

Se firma a los 13 días del mes de noviembre del año 2026

Luis Alexander Vasquez Hernandez
2026-11-13 12:15:59

LUIS ALEXANDER VASQUEZ HERNANDEZ
Secretario de Despacho
Ordenador de Gasto

Liliana Yezmin Zapata Alvarez
2026-11-13 12:13:30

LILIANA YEZMIN ZAPATA ALVAREZ
Directora de Informática y Sistemas Tecnológicos

Miguel Andres Martinez
2026-11-13 11:30:18

Wilmar Liberto Copete Marin
2026-11-13 11:34:23

WILMAR LIBERTO COPETE MARÍN
Profesional Especializado grado 8, Secretaría Tic

Proyección Jurídica
Miguel Andrés Martínez
Abogado Contratista Secretaría de TIC

Juan Sebastian Jaramillo Londoño
2026-11-13 11:51:04

Revisión jurídica TIC
Juan Sebastián Jaramillo Londoño
Abogado
Contratista Secretaría de TIC

Sandra Melissa Cardenas Espinosa
2026-11-13 11:14:34

Proyección financiera
Sandra Melissa Cardenas Espinosa
Componente financiero
Contratista Secretaría de TIC

Gobernación de Risaralda. NIT. 891 480 085-7
Calle 19 No 13 - 17 Pereira- Risaralda
PBX. +(57) (606) 3398300 - 01 8000 916 078
contactenos@risaralda.gov.co - www.risaralda.gov.co