ESTUDIOS Y DOCUMENTOS PREVIOS
Decreto 1082 de 2015

OBJETO

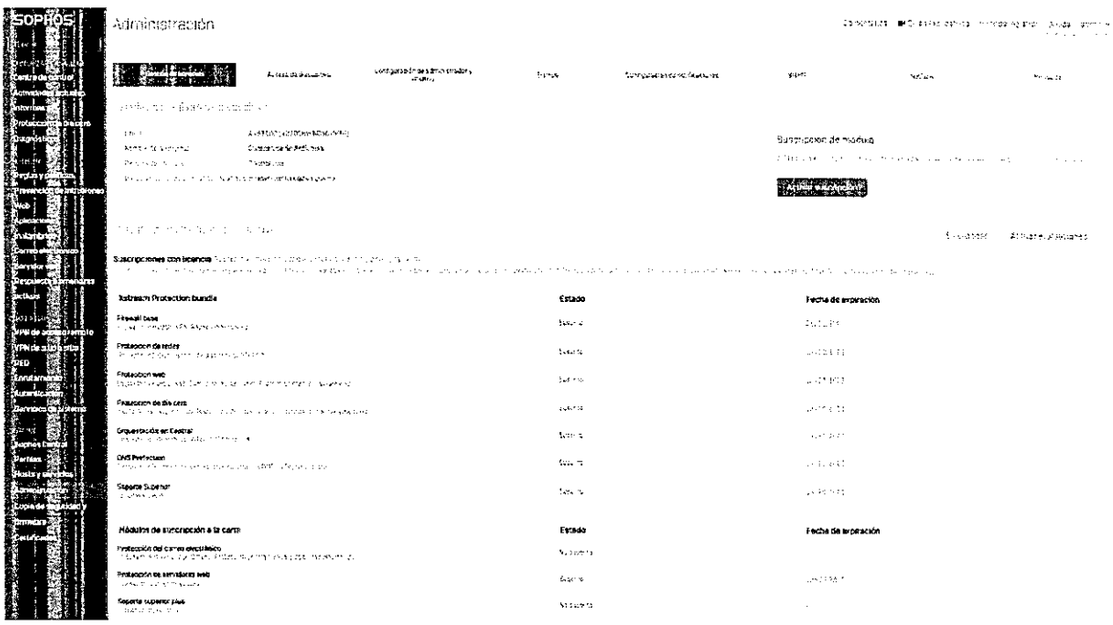
SUMINISTRO DEL LICENCIAMIENTO DEL SISTEMA DE SEGURIDAD PERIMETRAL – FIREWALL Y SOPORTE TÉCNICO DEL MISMO, PARA LA CONTRALORÍA GENERAL DE ANTIOQUIA.

Medellín, junio de 2025

1. DESCRIPCIÓN SUCINTA DE LA NECESIDAD QUE SE PRETENDE SATISFACER CON LA CONTRATACIÓN.

La Contraloría General de Antioquia (CGA) cuenta desde del año 2017 con una solución de seguridad de red perimetral, de forma física, en sus propias instalaciones del centro de datos, ubicadas en el Centro Administrativo Departamental –la Alpujarra, es decir, tiene un hardware appliance marca SOPHOS, el cual está registrado en el respectivo inventario de la Subdirección Operativa de la Entidad; así mismo registrado en el Plan Estratégico de las Tecnologías de la Información y Comunicaciones (PETI 2022 – 2025, radicado 2023500000481) página 46 riel 20 del centro de datos: Firewall SOPHOS. Es decir que hace parte de los activos de la Entidad, e igualmente, es un componente fundamental e imprescindible para el cumplimiento de políticas de seguridad, tratamiento de riesgos de seguridad informática, MIPG, Gobierno Digital, entre otras.

El sistema de seguridad y privacidad de la información de la red de la CGA– SOPHOS, presenta a la fecha las siguientes características:



Como se puede apreciar claramente en las características, el registro de las licencias finaliza el próximo 26 de junio del año 2025 incluyendo la licencia del fabricante.

A su vez, por la información obtenida del fabricante, para este hardware no se tiene actualmente definida una fecha para finalización de soporte EOS.

XGS Firewall

Producto	End-of-Sale	Last Renewal	End-of-Life	Producto sucesor	BG
XGS 3100	31.03.2022	Sin fecha conocida	Sin fecha conocida	–	

https://www.avanet.com/es/kb/sophos-product-lifecycle-calendario-end-of-sale-end-of-life/

Esto permite concluir que se puede comprar licenciamiento por dos o más años.

Por la obligación que tiene la Contraloría General de Antioquia, de conservación y uso de sus bienes, y con fundamento en la precaución y control de riegos asociada a este tipo de tecnologías, la cual es la única solución de este tipo en la Entidad, se requiere el soporte del canal especializado con el fin de que intervenga cuando se produzca algún tipo de fallo o daño, evento de ciberataque, ciberdelincuencia, actualización de firmware de la máquina, reconfiguraciones, mantenimientos preventivos, entre otras.

Así pues, se infiere que es indispensable seguir contando con dicho licenciamiento y soporte, el cual vence el próximo 17 de junio del año 2025.

De no realizarse la contratación, puede verse comprometida la seguridad de afuera hacia adentro de la Entidad (es decir, la seguridad perimetral) lo que deja a la Entidad expuesta a un ciberataque. Ante una falla que se presente en el hardware, los servicios de red como la VPN, acceso externo a Mercurio, entre otros, quedan automáticamente suspendidos, tarea que hace el fabricante a través de un soporte técnico.

En el plano institucional, observamos que, dentro de las estrategias de Continuidad y vigencia tecnológica, aquellos componentes tecnológicos se priorizan de acuerdo a

un conjunto de necesidades institucionales en los Planes Anuales de Adquisiciones (PAA), Planes estratégicos, entre otros. Es por esto que, entre dichos componentes tecnológicos a cuidar, se ha planteado la necesidad de dar continuidad a la solución de seguridad perimetral.

Las diferentes formas para solucionar el licenciamiento y soporte del hardware, pasan por la apropiación presupuestal requerida y por la formalización contractual para contratar dicha licencia. Otra estrategia consistiría en adquirir una nueva solución de seguridad perimetral que reemplace la que posee la Entidad actualmente y cuyo costo – beneficio sea bastante similar.

Siendo así, se concluye que la Contraloría General de Antioquia, está encaminada a la ejecución satisfactoria de su misión, la cual incluye como elemento de apoyo, diferentes componentes tecnológicos y, en tal sentido, se requiere un proceso de licenciamiento y soporte técnico especializado para el sistema de seguridad perimetral.

Esta contratación fue autorizada por el Comité de Adquisiciones de la Contraloría General de Antioquia, en reunión del 26 de marzo de 2025, según Acta N° 03.

2. DESCRIPCIÓN DEL OBJETO A CONTRATAR IDENTIFICADO CON EL CUARTO NIVEL DEL CLASIFICADOR DE BIENES Y SERVICIOS.

2.1. OBJETO A CONTRATAR:

SUMINISTRO DEL LICENCIAMIENTO DEL SISTEMA DE SEGURIDAD PERIMETRAL – FIREWALL Y SOPORTE TÉCNICO DEL MISMO, PARA LA CONTRALORÍA GENERAL DE ANTIOQUIA.

2.2. CUARTO NIVEL DEL CLASIFICADOR DE BIENES Y SERVICIOS

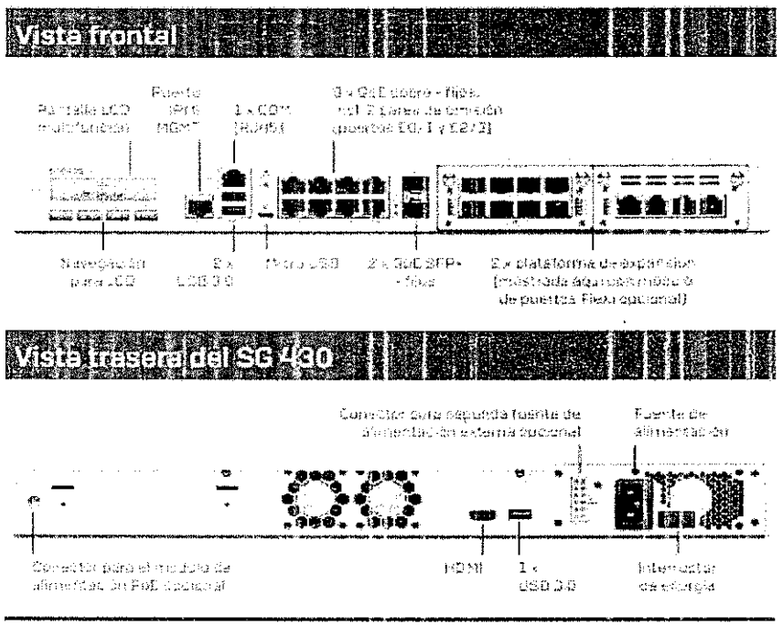
SEGMENTO	FAMILIA	CLASE	PRODUCTO	NOMBRE
43000000	43220000	43222500	43222501	Equipo de seguridad de red cortafuegos (firewall)
43000000	43230000	43233200	43233204	Software de equipos de seguridad de red y de redes privadas virtuales vpn
81000000	81110000	81111800	81111801	Seguridad de los computadores, redes o internet

2.3. CONDICIONES TÉCNICAS EXIGIDAS.

ALCANCE:

RENOVACIÓN DE LICENCIA SOPHOS SG: por doce (12) meses, la cual corresponde estrictamente a:

Modelo	Descripción del producto	Cantidad
XGS3100 (X31006WBC6DYV3F)	SOPHOS XGS 3100 SOPORTE 24x12 Meses - RENEWAL	1 Unidad.



Soporte durante doce (12) meses: El soporte incluye acompañamiento Virtual y en sitio del canal autorizado por SOPHOS para atender las solicitudes que se requieran, así mismo 30 horas de capacitación, configuración, parametrización y estabilidad de la solución. Dicho servicio y soporte incluye a su vez, y según la necesidad del sistema de seguridad perimetral, lo siguiente:

MANTENIMIENTO PREVENTIVO: Se deben realizar mantenimiento preventivo durante el tiempo del servicio y bajo las recomendaciones del fabricante, en horario definido con la Dirección de Sistemas de Buen Gobierno y las TIC. *Dicho mantenimiento puede estar relacionado con:*

- Verificar y actualizar los niveles de microcódigo si el appliance lo requiere por bug, fallas o mejoras.
- Realizar diagnósticos con herramientas propias del fabricante que permitan determinar el estado de los equipos y prevenir posibles fallas.
- Realizar los respectivos acompañamientos a las actualizaciones de Firmware u otra que el fabricante despliegue que sean necesarias para la estabilidad, seguridad del servicio.
- Capacitación básica de la solución – Reglas en general, SSL, VPN, Perfiles, Usuarios, Servicios, reinicio, reportes por tiempos, Integración al DA, ente otros.
- Entregar manual de usuario y de administrador.
- El servicio debe incluir asesoría y actualización de reglas de enrutamiento y seguridad en caso de requerirse para temas de aseguramiento de los equipos de la CGA.
- Asesoría y acompañamiento para separar la red en grupos, es decir, grupo de equipos de escritorio, servidores, impresoras, Wifi, entre otros, así mismo configurar la solución para permitir la conexión de equipos registrados con su MAC, servicio que se homologue como el NAC.

SUMINISTRO DE REPUESTOS: El contratista deberá suministrar las partes o repuestos conforme al licenciamiento, que se requieran para la solución, sin costo adicional, durante el término de ejecución del contrato y el personal especializado para la instalación y puesta en funcionamiento de estos.

ASISTENCIA EN SITIO: De considerarse necesario previa evaluación, el Contratista deberá garantizar asistencia en el sitio para problemas tanto de software como de hardware relacionados con el licenciamiento del SOPHOS.

CERTIFICADO DE AUTORIZACIÓN PARA PRESTAR ESTE SERVICIO: El proponente debe anexar los documentos:

- El oferente debe ser miembro del programa de canales del fabricante (canal autorizado), en la **categoría Gold**.

- Adjuntar a su propuesta, una certificación de soporte y garantía de que el oferente está autorizado por el fabricante a presentar su oferta y tiene el respaldo del mismo para este proceso. Este documento debe tener máximo

treinta (30) días de emisión y debe ir dirigido a la entidad, mencionando el número del proceso y firmado por el fabricante.

- Adjuntar el certificado de experiencia por parte del fabricante del profesional que brindará el soporte de la solución por el tiempo del contrato, con fecha no mayor a seis (6) meses calendario, previos al cierre de la invitación.

- Adjuntar máximo dos (2) certificaciones de experiencia en los últimos 2 años, que sumadas superen el 100% del presupuesto asignado al presente proceso.

- Certificar que la empresa oferente cuenta con un Arquitecto certificado en firewall XGS y en la norma ISO27001.

3. OBLIGACIONES DE LAS PARTES.

3.1. DE LA CONTRALORÍA GENERAL DE ANTIOQUIA:

- Verificar el cumplimiento del contrato a través del Supervisor designado.
- El supervisor del contrato verifica las licencias suministradas instaladas y operativas en la unidad SOPHOS.
- Hacer las recomendaciones pertinentes para un efectivo cumplimiento del contrato.
- Suministrar la información que se requiera para el cumplimiento del objeto contractual.
- Pagar el valor del contrato en la forma pactada.
- Cumplir y hacer cumplir las obligaciones que se convengan en el contrato y en los documentos que de él formen parte.
- Analizar y responder los requerimientos que formule el contratista dentro de los términos del presente contrato.
- Evaluar al proveedor.

3.2. DEL CONTRATISTA:

- Atender los requerimientos de la Contraloría General de Antioquia.
- Informar oportunamente al Supervisor del contrato, las dificultades encontradas para la correcta ejecución del mismo.
- Realizar los aportes correspondientes al Sistema General de Seguridad social.

- El contratista corre con todos los gastos y emolumentos que demande el Contrato de Prestación de Servicios.
- Cumplir cada uno de los ofrecimientos hechos en su propuesta, en todo aquello que no contraríe lo aquí estipulado, la cual hace parte del presente contrato.
- Defender en todas sus actuaciones los intereses de la Contraloría y obrar con lealtad y buena fe en todas las etapas contractuales.
- Todas las demás inherentes o necesarias para la correcta ejecución del objeto contractual.
- Atender las recomendaciones y requerimientos que haga la Contraloría General de Antioquia a través del Supervisor designado para el contrato.
- Anexar los documentos requeridos por la Contraloría General de Antioquia.
- Liquidar el contrato.

3.3. OBLIGACIONES ESPECIFICAS DEL CONTRATISTA

- Realizar el respectivo mantenimiento preventivo de la máquina.
- Suministrar repuestos de la máquina en caso de ser necesarios y conforme al licenciamiento.
- Asistencia en sitio y/o virtual una vez evaluada la situación o circunstancias.
- Certificado de autorización por parte del fabricante para prestar este servicio.
- Velar por el correcto funcionamiento, operación y actualización de los componentes de la solución SOPHOS SG.
- Todas las demás actividades inherentes al licenciamiento adquirido, a lo establecido en el alcance contractual, y sus especificaciones técnicas.
- Presentar un informe anual relacionado con el cumplimiento del contrato.

ACUERDO DE NIVELES DE SERVICIO (ANS)

Si bien los acuerdos de niveles de servicio (ANS) están relacionados con el tipo de Licencia, con el proponente, y a su vez el fabricante define dichos acuerdos, se especifican los siguientes para la Entidad con el fin de dar mayor especificidad al proceso:

- El soporte requerido se solicitará por medio telefónico o virtual.
- El soporte debe ser 7x24

- El soporte telefónico o de conexión remota será realizado dentro de la siguiente (1) hora a la apertura de la solicitud.
- Se evaluará el tipo de requerimiento y la solución, en sitio o virtual.
- Atención especializada por personal con experiencia en la solución.

4. VALOR ESTIMADO DEL CONTRATO Y SU JUSTIFICACIÓN.

4.1. VALOR.

La Contraloría General de Antioquia, cuenta con un presupuesto de **SESENTA Y SEIS MILLONES DE PESOS ML. ($66.000.000),** considerando un incremento superior al IPC 2025, sobre el valor del servicio en el año inmediatamente anterior.

4.2. CERTIFICADO DE DISPONIBILIDAD PRESUPUESTAL QUE RESPALDA LA CONTRATACIÓN.

Certificado de Disponibilidad Presupuestal 4000010188 del 25 de junio del año 2025, expedido por la Subdirección Financiera por la suma de **SESENTA Y SES MILLONES DE PESOS ML. ($66.000.000),** con cargo a la posición presupuestal 212010100502030101 "Paquete de software".

4.3. JUSTIFICACIÓN:

El presupuesto oficial disponible para la presente contratación fue definido por la Alta Dirección conforme a la priorización de necesidades de la Entidad en coordinación con la Dirección de Sistemas para el Buen Gobierno y las TIC y se dispondrá para la adquisición de elementos constitutivos del Datacenter.

En aras de definir el valor de la garantía a adquirir, la Entidad consideró como referencia los precios según cotizaciones recibidas, las cuales reposan en el expediente del proceso y se encuentran relacionadas en el Análisis del Sector.

De conformidad con la cotización recibida, atendiendo al presupuesto de los contratos anteriores que con el mismo objeto ha suscrito la Entidad anualmente, en consideración al estudio de mercado realizado, se estableció desde el PAA-2025 un presupuesto oficial para esta contratación de $66.000.000.

4.3. ANÁLISIS DEL SECTOR.

Soluciones de Seguridad Perimetral y Firewalls

Contexto General:

El panorama de la ciberseguridad ha experimentado un crecimiento exponencial en la última década, impulsado por la creciente sofisticación de las amenazas cibernéticas y la necesidad de proteger los activos digitales de organizaciones en todos los sectores. En particular, la seguridad perimetral, que incluye firewalls, se ha convertido en una piedra angular de la estrategia de seguridad de muchas organizaciones, ya que actúa como la primera línea de defensa contra amenazas externas.

En el ámbito de la ciberseguridad, los firewalls desempeñan un papel fundamental como la primera línea de defensa contra las amenazas cibernéticas. Un firewall es un dispositivo o software que monitorea y controla el tráfico de red entrante y saliente, basado en un conjunto de reglas predefinidas. Su objetivo principal es filtrar el tráfico no autorizado y proteger los sistemas y datos de una organización contra intrusiones y ataques maliciosos.

Funcionamiento y Tipos de Firewalls:

Los firewalls pueden operar a nivel de red, inspeccionando paquetes individuales de datos y aplicando reglas de filtrado basadas en direcciones IP, puertos y protocolos, o a nivel de aplicación, examinando el tráfico en función de información más detallada sobre las aplicaciones y los protocolos de aplicación.

Existen varios tipos de firewalls, incluyendo:

Firewalls de Packet Filtering (Filtrado de Paquetes): Estos firewalls examinan cada paquete de datos que pasa a través de ellos y toman decisiones de filtrado basadas en reglas predefinidas. Son eficientes, pero menos sofisticados en comparación con otros tipos de firewalls.

Firewalls de Stateful Inspection (Inspección de Estado): Estos firewalls supervisan el estado de las conexiones de red y permiten o bloquean el tráfico en función del estado de la conexión. Son más seguros que los firewalls de filtrado de paquetes porque tienen en cuenta el contexto de la comunicación.

Firewalls de Aplicación (o de Nivel de Aplicación): Estos firewalls son capaces de inspeccionar el tráfico a un nivel más profundo, hasta el contenido de los datos y las aplicaciones específicas que generan el tráfico. Pueden aplicar políticas de seguridad más granulares y ofrecen una protección más avanzada contra amenazas.

Importancia de los Firewalls en la Seguridad Perimetral:

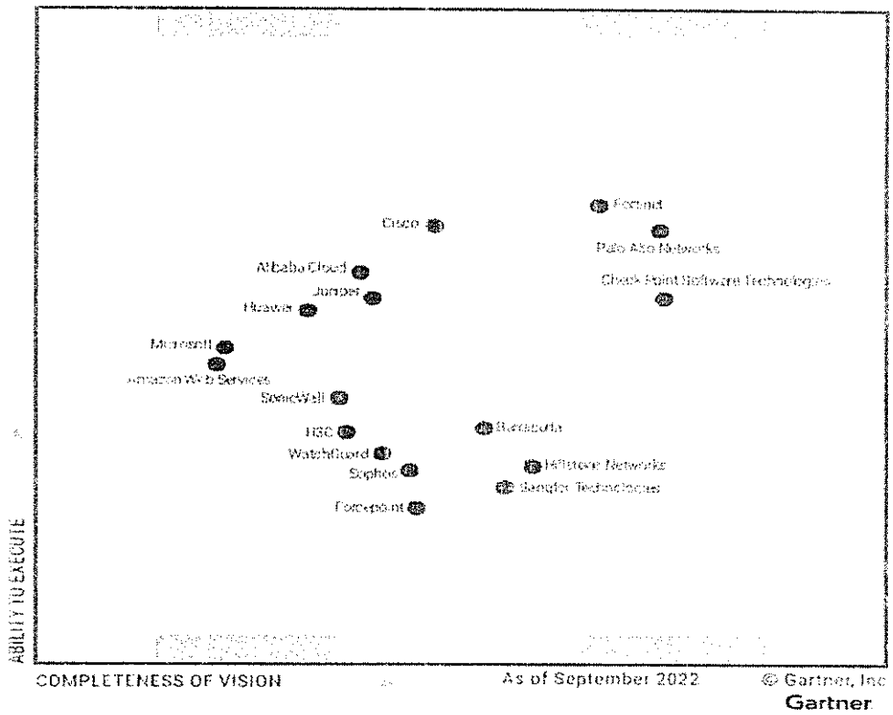
Los firewalls son un componente esencial de la seguridad perimetral, que se refiere a la protección de los límites de una red o sistema contra amenazas externas. Actúan como una barrera defensiva que controla y regula el tráfico de red entre una red interna y externa, como Internet.

Además de filtrar el tráfico no deseado, los firewalls pueden implementar funciones adicionales de seguridad, como prevención de intrusiones (IPS), detección de intrusiones (IDS), control de acceso, VPN (redes privadas virtuales) y seguridad de aplicaciones web, entre otros.

En resumen, los firewalls son una pieza fundamental en la arquitectura de seguridad de cualquier organización, proporcionando una primera línea de defensa crítica contra una amplia gama de amenazas cibernéticas. Su implementación y configuración adecuadas son elementos clave para garantizar la integridad, confidencialidad y disponibilidad de los sistemas y datos de una organización en un entorno cada vez más amenazante y complejo.

Consideraciones del Sector:
Líderes del Mercado según Gartner:

Gartner, una de las principales firmas de investigación y consultoría en tecnología, publica regularmente informes sobre el mercado de seguridad cibernética y evalúa a los proveedores en función de su visión y capacidad de ejecución. En el ámbito de las soluciones de seguridad perimetral, varios proveedores han sido reconocidos como líderes.



Predicciones de Gartner en el mercado de los Firewalls 2022

Además de Sophos, otros nombres destacados incluyen:

Cisco: Con su gama de firewalls Cisco ASA (Adaptive Security Appliance) y Firepower, Cisco es uno de los líderes establecidos en el mercado de seguridad perimetral. Ofrecen soluciones escalables y altamente integradas que abordan las necesidades de seguridad de organizaciones de todos los tamaños.

Palo Alto Networks: Con su firewall de próxima generación Palo Alto Networks NGFW (Next-Generation Firewall), Palo Alto Networks se ha ganado una reputación por su enfoque en la detección y prevención avanzada de amenazas. Su plataforma de seguridad integrada ofrece una amplia gama de funcionalidades para proteger contra amenazas cibernéticas.

Fortinet: Fortinet ofrece una variedad de soluciones de seguridad perimetral, incluyendo su firewall FortiGate, que se destaca por su alto rendimiento y su capacidad para integrar múltiples funciones de seguridad en un solo dispositivo.

Fortinet es conocido por su enfoque en la seguridad impulsada por IA y la automatización.

Diferenciación y Fortalezas de Sophos:

Sophos se destaca en el mercado de la seguridad perimetral por su enfoque en la simplicidad y la facilidad de gestión. Su interfaz intuitiva y centralizada hace que sea accesible incluso para organizaciones con recursos limitados.

Además, Sophos ha demostrado un compromiso con la innovación continua, incorporando capacidades avanzadas de detección y respuesta en sus firewalls para hacer frente a las amenazas cibernéticas emergentes.
La integración con otros productos de seguridad de Sophos, como sus soluciones de protección de endpoints y de correo electrónico, proporciona una defensa unificada y coordinada contra amenazas.

Tendencias del Mercado:

Se observa una tendencia hacia la convergencia de funciones de seguridad en un solo dispositivo, lo que se conoce como Unified Threat Management (UTM) o Next-Generation Firewall (NGFW). Esto permite a las organizaciones simplificar su infraestructura de seguridad y reducir la complejidad operativa.

La adopción de la nube y la movilidad ha llevado a un cambio en los modelos de implementación de firewalls, con un énfasis creciente en soluciones basadas en la nube y en dispositivos de seguridad virtualizados.

La creciente sofisticación de las amenazas cibernéticas, incluyendo el aumento del ransomware, el phishing y los ataques dirigidos, está impulsando la demanda de firewalls con capacidades avanzadas de detección y prevención de amenazas.

Por lo analizado, el mercado de seguridad perimetral es altamente competitivo, con varios proveedores líderes compitiendo por la cuota de mercado. Sophos se destaca por su enfoque en la simplicidad y la facilidad de gestión, así como por su compromiso con la innovación continua en la detección y prevención de amenazas cibernéticas. Sin embargo, es importante que las organizaciones evalúen cuidadosamente las fortalezas y debilidades de cada proveedor en función de sus necesidades específicas de seguridad y su entorno operativo.

Sophos como Líder en Seguridad Cibernética:
Como ya lo comentamos, Sophos es reconocido como un líder en el campo de la seguridad cibernética, con una amplia gama de soluciones que abordan diversas áreas de riesgo. Su enfoque integrado y centrado en la simplicidad y la eficacia lo ha convertido en una opción preferida para muchas organizaciones en todo el mundo.

Eficacia y Capacidad de Adaptación:
La solución de Firewall de Sophos ofrece una combinación de características avanzadas de protección contra amenazas, incluyendo inspección profunda de paquetes, filtrado de contenido, prevención de intrusiones y protección contra malware. Además, su capacidad para adaptarse a las nuevas amenazas mediante actualizaciones de firmas y análisis de comportamiento garantiza una protección continua y proactiva.

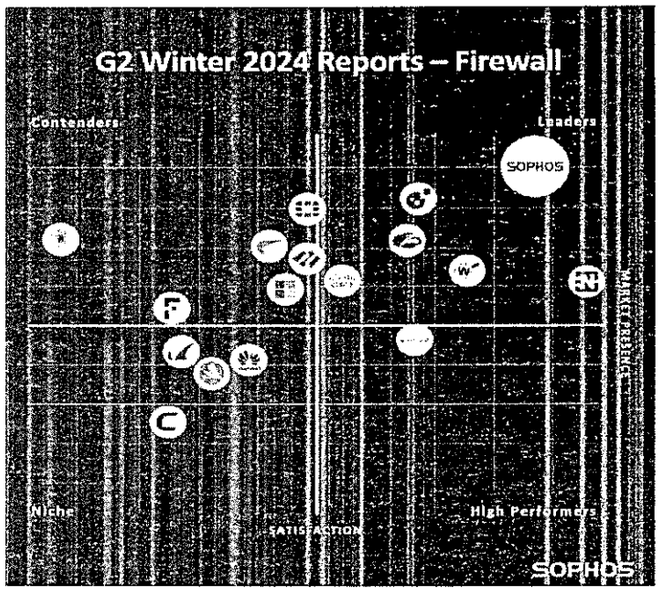
Facilidad de Implementación y Gestión:
Sophos se destaca por su enfoque en la facilidad de implementación y gestión. Su interfaz intuitiva y centralizada permite una configuración rápida y sencilla, reduciendo la carga de trabajo operativo y garantizando una administración eficiente incluso para organizaciones con recursos limitados.

Integración con Ecosistema de Seguridad:
La solución de Firewall de Sophos se integra fácilmente con otras herramientas y plataformas de seguridad, lo que permite una visibilidad y coordinación mejoradas en toda la infraestructura de seguridad. Esta capacidad de integración fortalece aún más la postura de seguridad de una organización al proporcionar una defensa unificada y coordinada contra amenazas.

Soporte y Servicio Postventa:
Sophos cuenta con un sólido historial de servicio al cliente y soporte técnico, brindando asistencia experta para la implementación, configuración y resolución de problemas. Su compromiso con la satisfacción del cliente asegura una experiencia sin problemas durante todo el ciclo de vida de la solución.

Es de destacar que Sophos Firewall es el único proveedor calificado como líder en las cinco categorías de ciberseguridad en los informes de invierno de 2024 de G2[1] (diciembre de 2023), así:

[1] G2 es el mercado de software más grande y confiable en el mundo. Más de 90 millones de personas al año, incluidos empleados de todas las empresas Fortune 500, utilizan G2 para tomar decisiones de software más inteligentes basadas en revisiones auténticas de pares.



Conclusión:

Dadas las crecientes y cada vez más sofisticadas amenazas cibernéticas, la protección robusta de los activos digitales y la infraestructura de TI de la organización es una prioridad ineludible. La implementación de una solución de seguridad perimetral tipo Firewall de nueva generación (NGFW) constituye un componente esencial de cualquier estrategia de ciberseguridad madura, actuando como primera línea de defensa y control de acceso a la red. La selección de dicha tecnología debe basarse en una evaluación rigurosa de su capacidad para mitigar riesgos actuales y emergentes, su adaptabilidad a las necesidades específicas de la entidad y su integración dentro del ecosistema de seguridad existente.

En la búsqueda de la solución más adecuada, es fundamental considerar criterios como la eficacia en la detección y prevención de amenazas, la facilidad de gestión y monitorización centralizada, la capacidad de integración con otras herramientas de seguridad para una respuesta coordinada, y la calidad del soporte técnico ofrecido por el proveedor. La entidad actualmente opera con una solución Firewall de Sophos, lo que proporciona un punto de referencia conocido en términos de rendimiento y gestión. Esta experiencia previa permite evaluar con conocimiento de causa cómo las características de soluciones de este tipo se alinean con los requerimientos operativos y de seguridad de la organización.

Por lo tanto, cualquier solución de seguridad perimetral que se considere debe demostrar su capacidad para fortalecer significativamente la postura de seguridad de la organización, ofreciendo un equilibrio óptimo entre protección avanzada, usabilidad y eficiencia operativa. La decisión final deberá asegurar que la inversión seleccionada no solo responda a las necesidades presentes, sino que también ofrezca la flexibilidad y escalabilidad para adaptarse a futuros desafíos, garantizando así la protección continua y efectiva de los recursos críticos de la entidad.

Estudio de Mercado:

Se ha realizado un estudio de mercado que incluye la obtención de cotizaciones y evaluación de proveedores de Firewall con servicios de soporte técnico para Sophos.

En el mercado colombiano podemos considerar los siguientes proveedores de soluciones de seguridad perimetral:

Sonda Colombia: Empresa colombiana con experiencia en soluciones de seguridad cibernética, incluyendo firewalls, prevención de intrusiones y gestión de seguridad de redes.

Westcon Security Colombia: Distribuidor autorizado de una amplia gama de soluciones de seguridad cibernética en Colombia, incluyendo firewalls de varios fabricantes reconocidos a nivel internacional.

Etek International Colombia: Proveedor de soluciones de seguridad perimetral y gestión de identidades y accesos (IAM) en Colombia, con experiencia en la implementación de firewalls y sistemas de detección y prevención de intrusiones.

Cyberfence Colombia: Empresa especializada en seguridad cibernética en Colombia, ofreciendo servicios de consultoría, implementación y gestión de soluciones de seguridad perimetral, incluyendo firewalls y sistemas de protección de redes.

Secure Soft Colombia: Proveedor de soluciones de seguridad cibernética en Colombia, con experiencia en la implementación de firewalls y soluciones de seguridad perimetral para empresas de diferentes sectores.

ClusterDS: Proveedor de soluciones de seguridad cibernética en Colombia, especializado en servicios de consultoría y soluciones de seguridad perimetral para proteger redes empresariales contra amenazas cibernéticas.

ITSEC SAS: Empresa colombiana dedicada a la seguridad de la información, ofreciendo soluciones de seguridad perimetral, incluyendo firewalls y sistemas de detección y prevención de intrusiones, así como servicios de consultoría y gestión de seguridad.

Origin IT SAS: Empresa colombiana que se especializa en servicios de consultoría y soluciones de tecnología de la información y seguridad cibernética

Estos proveedores permiten explorar una variedad de soluciones de seguridad perimetral ofrecidas por empresas locales en Colombia.

Cotizaciones suministradas:

ITSEC SAS

itsec

Sophos Platinum Partner

PROPUESTA ECONOMICA

DESCRIPCION	CANT	PRECIO UNIDAD	SUBTOTAL
XGS 3100 Xstream Protection - 12 MOS - GOV	1	$ 15.470.400	$ 15.470.400
XGS 3100 Webserver Protection - 12 MOS - Renewal - GOV	1	$ 3.097.600	$ 3.097.600
Central Email Advanced - 200-499 users - 12 MOS - Renewal	350	$ 102.960	$ 36.036.000
Soporte técnico especializado 5×8 (mantenimiento, atención remota y acompañamiento en escalamiento de incidentes)	1	$ 1.800.000	$ 1.800.000
		SUBTOTAL	$ 56.404.000
		IVA 19%	$ 10.716.760
		TOTAL	$ 67.120.760

5. MODALIDAD DE SELECCIÓN DEL CONTRATISTA Y SU JUSTIFICACIÓN INCLUYENDO FUNDAMENTOS JURÍDICOS.

Por tratarse de bienes de características técnicas uniformes y de común utilización, el presente proceso contractual se adelantará por la modalidad de Selección Abreviada por Subasta Inversa Electrónica con fundamento en literal a) del numeral 2° del Artículo 2 de la Ley 1150 de 2007, reglamentado por el Decreto 1082 de 2015, artículos 2.2.1.2.1.2.1 y s.s.

6. ANÁLISIS DEL RIESGO Y FORMA DE MITIGARLO.

6.1. MATRIZ DE RIESGOS

N°	CLASE	FUENTE	ETAPA	TIPO	DESCRIPCIÓN (Qué puede pasar y cómo puede ocurrir)	CONSECUENCIA DE LA OCURRENCIA DEL EVENTO	PROBABILIDAD	IMPACTO	VALORACIÓN	CATEGORÍA
1	General	Externo	Contractual	Operacional	El contratista no firme el contrato	Retraso en la ejecución del contrato, lo que conlleva al incumplimiento del cronograma establecid	2	3	5	Riesgo Medio

N°	A quién se le asigna?	Tratamiento/ Controles a ser implementados	Impacto después de tratamiento			Afecta el equilibrio económico del contrato?	Persona responsable por implementar el tratamiento	Fecha estimada en que se inicia el tratamiento	Fecha estimada en que se completa el tratamiento	Monitoreo y revisión	
			Probabilidad	Impacto	Calificación total					Cómo se realiza el monitoreo?	Periodicidad ¿Cuándo?
1	Contratista	El oferente debe constituir póliza de seriedad de la oferta.	1	1	2	No	Responsable del proceso contractual	Desde la Resolución de adjudicación del contrato	Hasta la suscripción del Acta de Inicio	Supervisión del proceso contractual	Constante

	CLA	FUE E	ETA	TIPO			PRO ABIL	IMP TO	VAL RAC N	CAT GOF

N°					DESCRIPCIÓN (Qué puede pasar y cómo puede ocurrir)	CONSECUENCIA DE LA OCURRENCIA DEL EVENTO				
2	Específico	Externo	Ejecución	Operacional	Incumplimiento total o parcial en la entrega del suministro y prestación del servicio	Incumplimiento de las especificaciones técnicas, de forma parcial o total	2	3	5	Riesgo Alto

N°	A quién se le asigna?	Tratamiento/ Controles a ser implementados	Impacto después del tratamiento			Afecta el equilibrio económico del contrato?	Persona responsable por implementar el tratamiento	Fecha estimada en que se inicia el tratamiento	Fecha estimada en que se completa el tratamiento	Monitoreo y revisión	
			Probabilidad	Impacto	Calificación total					Cómo se realiza el monitoreo?	Periodicidad ¿Cuándo?
2	Contratista	Control permanent por parte de la Supervisión designada quien expedirá la pertinente autorización de pag previa verificación cumplimiento del objeto contractual. Constitución de garantía única de cumplimiento.	1	1	2	Si	Supervisor	Desde la suscripción del Acta de Inicio	Hasta la terminación de la ejecució del contrato	Supervisió permanent a la ejecución c contrato	Constante, al momento de la entre de los productos o realización de objetivos

N°	CLASE	FUENTE	ETAPA	TIPO	DESCRIPCIÓN (Qué puede pasar y cómo puede ocurrir)	CONSECUENCIA DE LA OCURRENCIA DEL EVENTO	PROBABILIDAD	IMPACTO	VALORACIÓN	CATEGORÍA
3	General	Externo	Ejecución	Operacional	Baja calidad de los bienes y servicios entregados	Incumplimiento de las especificaciones técnicas, de forma parcial o total	2	3	5	Riesgo Alto

N°	A qu se le asig	Impacto después del tratamiento	Afec el equil o	Pers a resp sabl	Fech estim da el	Fech estim da e que	Monitoreo y revisio

		Tratamiento/ Controles a ser implementados	Probabilidad	Impacto	Calificación total					Cómo se realiza el monitoreo?	Periodicidad ¿Cuándo?
3	Contratista	Monitoreo permanen por parte de la Supervisión previo a autorización de pago Constitución de garantía única de cumplimiento.	1	1	2	Si	Superviso	Desde la suscripción del Acta de Inicio	Hasta la terminación de l ejecución del contrato	Supervis n permane e a la ejecución del contrato	Constante, al momento d la entrega de los bienes prestación de los servicio

N°	CLASE	FUENTE	ETAPA	TIPO	DESCRIPCIÓN (Qué puede pasar, y cómo puede ocurrir)	CONSECUENCIA DE LA OCURRENCIA DEL EVENTO	PROBABILIDAD	IMPACTO	VALORACIÓN	CATEGORÍA
4	General	Externo	Ejecución	Operacional	Modificación de las especificaciones técnicas	Incumplimiento en la ejecución del Contrato	2	2	4	Riesgo Bajo

N°	A quién se le asigna?	Tratamiento/ Controles a ser implementados	Impacto después del tratamiento							Monitoreo y revisión	
			Probabilidad	Impacto	Calificación total	Afecta el equilibrio económico del contrato?	Persona responsable por implementar el tratamiento	Fecha estimada en que se inicia el tratamiento	Fecha estimada en que se completa el tratamiento	Cómo se realiza el monitoreo?	Periodicidad ¿Cuándo?
4	Contratista	Monitoreo permanente por parte de la Supervisión. Constitución de garantía única de cumplimiento.	1	1	2	Si	Supervisor	Desde la suscripció del Acta de Inicio	Hasta la terminació de la ejecución del contrato	Supervisión permanente la ejecución del contrato	Constante

CLA	FUE E	ETA	TIPO	PRO BABI	IMP ACTO	VAL RAC N	CAT GOR

N°					DESCRIPCIÓN (Qué puede pasar y cómo puede ocurrir)	CONSECUENCIA DE LA OCURRENCIA DEL EVENTO				
5	General	Externo	Ejecución	Operacional	Incumplimiento de las obligaciones patronales a car del contratista	Posible dificultad en la prestación del servicio por parte del equipo de trabajo responsable de ejecución del objeto	2	4	6	Riesgo Medio

N°	A quién se le asigna?	Tratamiento/ Controles a ser implementados	Impacto después del tratamiento			Afecta el equilibrio económico del contrato?	Persona responsable por implementar el tratamiento	Monitoreo y revisió		
			Probabilidad	Impacto	Calificación total			Fecha estimada en que se inicia el tratamiento	Fecha estimada en que se completa el tratamiento	Cómo se realiza el monitoreo?	Periodicidad ¿Cuándo?
5	Contratista	Para el pago de la factura mensual, el contratista debe allegar constancia de pago de seguridad social.	1	1	2	Si	Supervisor	Desde la suscripció del Acta de Inicio	Hasta la terminació de la ejecución del contrato	Supervisión permanente a ejecución del contrato	Constante

6.2. CONSTITUCIÓN DE GARANTÍAS.

Conforme a lo dispuesto en la Ley 80 de 1993, la Ley 1150 de 2007 y el artículo 2.2.1.2.1.5.4 del Decreto 1082 de 2015, de conformidad con el anterior Análisis de Riesgos, se deduce que los riesgos de la presente contratación, son transferibles. En consecuencia, la Entidad requiere que el Contratista constituya Garantía Única de Cumplimiento a favor de Entidades Estatales, en los siguientes términos:

GARANTÍA	PORCENTAJE	DESDE	HASTA
Cumplimiento	10%	Suscripción del Contrato	Por el término del contrato y cuatro (4) meses más.
Calidad del bien o servicio	20%	Suscripción del Contrato	Por el término del contrato y cuatro (4) meses más.
Pago de Salarios y Prestaciones Sociales	10%	Suscripción del Contrato	Por el término del contrato y tres (3) años más.
Correcto funcionamiento de equipos	20%	Suscripción del contrato	Por el término del contrato y cuatro (4) meses más.

7. PLAZO DE EJECUCIÓN DEL CONTRATO.

Un (1) año a partir de la suscripción del acta de inicio.

8. FORMA DE PAGO.

Por tratarse de una licencia, se realizará un pago único, dentro de los diez (10) días hábiles siguientes a la fecha en que el contratista radique en debida forma la respectiva factura, previa presentación de la certificación de cumplimiento de los pagos al Sistema de Seguridad Social Integral de acuerdo con lo previsto en la Ley 789 de 2002, y sujeta a la constancia de recibo a satisfacción que suscriba el Supervisor.

9. SUPERVISIÓN

La supervisión del contrato que se celebre en este proceso de selección, será ejercida por el funcionario que funja como Director de Sistemas de Buen Gobierno y las TIC, o por quien delegue el Ordenador del Gasto, y ejercerá las funciones y tareas de supervisión y vigilancia técnica, jurídica, administrativa, financiera y contable del contrato.

Los supervisores deben dar cumplimiento a lo establecido en el artículo 83 y siguientes de la Ley 1474 de 2011 y las demás que la modifiquen, adicionen o complementen.

9. LA INDICACIÓN DE SI EL PROCESO DE CONTRATACIÓN ESTÁ COBIJADO POR UN ACUERDO COMERCIAL.

Dichos acuerdos se encontrarán en la página Web de Colombia Compra Eficiente (www.colombiacompra.gov.co), y cuando el proceso de contratación está sometido a uno o varios Acuerdos Comerciales, la Entidad estatal deberá ceñirse a lo establecido en el Artículo **2.2.1.2.4.1.1.** y siguientes del Decreto 1082 de 2015.

Chile	NO	NO	N/A	NO	NO
México	NO	NO	N/A	NO	NO
Perú	NO	NO	N/A	NO	NO
	NO	NO	N/A	NO	NO
	SI	NO	N/A	NO	NO

		NO	NO	N/A	NO	NO
		NO	NO	N/A	NO	NO
		NO	NO	N/A	NO	NO
		NO	NO	N/A	NO	NO
		NO	NO	N/A	NO	NO
	El Salvador	SI	SI	1, 2, 3, 4, 5, 6, 7, 9, 1 20, 38, 48, 49, 60	NO	SÍ
	Guatemala	SI	SI	1, 2, 3, 4, 5, 6, 7, 9, 1 20, 21, 50, 51, 52, 53 60	NO	SÍ
	Honduras	NO	NO	N/A	NO	NO
		NO	NO	N/A	NO	NO
		SI	SI	NO	NO	SI

Las Contralorías del nivel departamental están obligadas por los Acuerdos Comerciales con Chile, el Triángulo Norte (únicamente con El Salvador y Guatemala); y, por la Decisión 439 de 1998 de la Secretaría de la CAN.

JUAN FERNANDO SÁNCHEZ ARISTIZÁBAL
Director de Sistemas del Buen Gobierno y de las TIC.

Propósito	Nombre	Firma	Fecha
Proyectó:	Juan Fernando Sánchez Aristizábal Director de Sistemas del Buen Gobierno y de las TIC		30-05-2025
Ajustó:	Sonia Roldán Calle Abogada de la Subdirección Operativa		25-06-2025
Revisó:	María Isabel Ramírez Aristizábal Subdirectora Operativa		25-06-2025
Revisó:	César Julián Rengifo Betancur Asesor del Despacho		25-06-2025
Aprobó:	Comité de Adquisiciones	Acta 03	Del 26-03-2025
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legale vigentes y, por tanto, bajo nuestra responsabilidad lo presentamos para la firma.			