RECIBIDO

CARMEN EMILIA OSPINA	FORMATO **CERTIFICADO DE CUMPLIMIENTO**			mipg
PROCESO: GESTIÓN DE CONTRATACIÓN	**CODIGO:** GCR-S1-F19	**VIGENCIA:** 18/05/2023	**V2**	**PÁGINA** 1 de 4

No. Contrato	0009-2025	**No. Entrega**	4	**Fecha**	13/05/2025

La Suscrita COORDINADORA AREA TIC de la E.S.E. Carmen Emilia Ospina en calidad de SUPERVISORA

CERTICA QUE:

La empresa ALPASURFNET S.A.S., Identificada con Nit 828.000.170-8, Representada legalmente por GUSTAVO ADOLFO ANDRADE DUSSAN, Identificado con cedula de ciudadanía número 7.688.838 de Neiva , Responsable del contrato Número 0009 de 2025 cuyo objeto es CONTRATAR EL SERVICIO DE CONECTIVIDAD Y/O INTERCONEXION Y SERVICIO DE INTERNET CANAL DEDICADO Y A TRAVES DE FIBRA OPTICA PARA LAS SEDES DE CANAIMA, CAIMI, GRANJAS, EDUARDO SANTOS, SIETE DE AGOSTO, PALMAS, IPC, SANTA ISABEL, FORTALECILLAS Y CAGUAN DE LA ZONA URBANA CON EL SERVICIO DE INTERCONEXION POR RADIO ENLACES A LAS SEDES RURALES DE LAS ZONAS SUR, NORTE Y ORIENTE; COMPLEMENTANDO CON EL SERVICIO DE LA SEGURIDAD WEB PERIMETRAL, INCLUYENDO FIREWALL A 600 USUARIOS PARA LA ESE CARMEN EMILIA OSPINA, del 1 al 30 de Abril del 2025, Cumplió a satisfacción con los requerimientos de calidad, cantidad y oportunidad definidos en el mismo contrato, entregados a la E.S.E. CARMEN EMILIA OSPINA, el referido contrato presenta el siguiente especificaciones:

Contrato No. 0009 de 2025	Fecha de inicio	10/01/2025
	Fecha de terminación	09/04/2025
	Otrosí	**09/05/2025**

Valor inicial	$81.300.000
Valor Otrosí	$27.100.000
Valor total	$108.400.000
Valor ejecutado	$69.724.340
Vienen contrato	$38.675.660
Valor factura (s)	$26.792.980
Saldo contrato	$11.882.680

Ítem	Factura	Fecha	Comprobante entrada a almacén	Valor facturas
1	FC 36	12/05/2025		$26.792.980
Total				$26.792.980

Total de facturas	1

De conformidad con las directrices legales, contractuales e institucionales, establecidas por la E.S.E. Carmen Emilia Ospina, el contratista cumplió a cabalidad con los respectivos pagos al SGSSS, soportada por la certificación expedida por ESPER MOTTA GONZLAEZ CC 12.118.113 TP 31164 -T, **Contador** de la entidad contratista.
Expedida en la ciudad Neiva, 13 de Mayo del año 2025.

Carolina Gonzalez

LILIANA CAROLINA GONZALEZ GUTIERREZ
otorga el certificado Supervisora

ALPASURFNET S.A.S.
NIT 828.000.170-8
calle 6 Numero 14 A 39 Barrio Altico
Tel: 3153372911
Neiva - Colombia
alpavision@gmail.com
https://alpavision.com.co

Factura electrónica de venta
No. FC 36

Señores	EMPRESA SCIAL DEL ESTADO ESE CARMEN EMILIA OSPINA		
NIT	813.005.265-7	**Teléfono**	(000) 3112566991 - Ext. 000
Dirección	CARRERA 22 # 26 - 29	**Ciudad**	Neiva - Colombia

Fecha y hora Factura	
Generación	12/05/2025. 08:56
Expedición	12/05/2025, 08:56
Vencimiento	11/06/2025

Ítem	Descripción	Cantidad	Vr. Total	Impto. Cargo	Nombre producto
1	CP 009 DEL 2025 DESDE 01/04/2025 AL 30/04/2025	1.00	26,792,980.00	19 %	servicio internet gravado 19

Total items: 1

Total Bruto	22,515,109.24
IVA 19%	4,277,870.76
Total a Pagar	26,792,980.00

Valor en Letras:
Veintiseis millones setecientos noventa y dos mil novecientos ochenta pesos m/cte

Forma de pago:
Crédito

Medio de pago:
Efectivo - Crédito - Cuota No. 001 vence el 2025-06-11 por $ 26,792,980.00

Observaciones:

A esta factura de venta aplican las normas relativas a la letra de cambio (artículo 5 Ley 1231 de 2008). Con esta el Comprador declara haber recibido real y materialmente las mercancías o prestación de servicios descritos en este título - Valo. **Numero Autorización Electrónica 18764076043753 aprobado en 20240730 prefijo FC desde el número 1 al 100 Vigencia: 24 Meses**
Responsable de IVA - Actividad Económica 6110 Actividades de telecomunicaciones alámbricas Tarifa 10X1000- somos autoretenedores de ica
CUFE: 0738807c0de2fd0060190b6f9a7a4c9a10ad84f663058f9f763fab53acc9304109d6842df8098cdadfcd5919008e059fd9f

Factura electrónica de Venta validada por la DIAN mediante Software y Proveedor tecnológico Siigo SAS - Nit 830.060.146-8. Nombre Software: Siigo Nube. Firma electrónica ver en el XML

Neiva, 05 de mayo de 2025

Señora
CAROLINA GUTIERREZ
Supervisora

REF: INFORME DE EJECUCIÓN DE ACTIVIDADES. Supervisor - Contrato Bienes y Servicios N.º 009 de 2025. **ALPASURFNET S.A.S. Nit. 828.000.170-8**, mediante el presente escrito me permito presentar el

OBJETO CONTRACTUAL: "CONTRATAR EL SERVICIO DE CONECTIVIDAD Y/O INTERCONEXION Y SERVICIO DE INTERNET CANAL DEDICADO A TRAVES DE FIBRA OPTICA PARA LAS SEDES DE CANAIMA, GRANJAS, EDUARDO SANTOS, SIETE DE AGOSTO, PALMAS, IPC, CAIMI, SANTA ISABEL, BODEGA, FORTALECILLAS Y CAGUAN DE LA ESE CARMEN EMILIA OSPINA Y CON EL SERVICIO INTERCONEXION POR RADIO ENLACES A LAS SEDES RURALES DE LAS ZONAS SUR, ORIENTE Y ORIENTE; COMPLEMENTADO CON EL SERVICIO DE SEGURIDAD WEB PERIMETRAL, INCLUYENDO FIREWALL A 600 USUARIOS PARA LA ESE CARMEN EMILIA OSPINA".

Periodo ejecutado: 1 abril al 30 de abril de 2025

ACTIVIDADES REALIZADAS:

N°	Actividades del contratista	Actividades realizadas	Evidencia aprobada
1	Ejecutar el objeto contractual dentro de los términos y condiciones establecidas en la normatividad vigente sobre la actividad vigente en Colombia y acatando las especificaciones y/o recomendaciones técnicas señalada de la ESE CARMEN EMILIA OSPINA, con oportunidad eficiencia y eficacia de manera autónoma e independiente.	Se ejecutó el contrato dentro de los términos establecidos en la normatividad vigente de acuerdo con el anexo técnico establecido en la ESE CARMEN EMELIA OSPINA	Se evidenciará en las diferentes actividades realizadas según CPS 009 del 2025.
2	El contratista deberá contar con el debido Registro de TIC del ministerio de las TICS (RTIC), en el que se acredita al contratista como ISP.	ALPASURFNET cuenta con registro TIC Número 96002041 del 12 de Mayo del 2014.	Se anexa consulta Registro TIC en Fisico.
3	Poner a disposición y acceso a una solución de herramienta web, que permita monitorear los consumos de anchos banda de cada y en tiempo real cada uno de los equipos de red instalados por el contratista de la ESE CARMEN EMELIA OSPINA.	Se pone a disposición una herramienta http://177.74.204.242/index.htm que permite monitorear los consumos de anchos de banda de las 27 Sedes de la ESE CARMEN EMILIA. Con usuario: esecarmen y password: Es3carmen20	Herramienta de Monitoreo PRTG

<table>
<tr><td>4</td><td>El contratista pondrá a disposición de la ESE el personal de soporte y atención a incidentes y fallas con dominio y experiencia en manejo, configuración de las marcas de equipos y activos de red (routers, switches, firewall) del contratista.</td><td>Se puso a disposición el personal de soporte y atención a incidentes y fallas para el manejo de los equipos tecnológicos y activos de red</td><td>Se adjunta listado de personal que se dispuso para la atención de incidentes y fallas reportados por la ESE.</td></tr>
<tr><td>5</td><td>El contratista garantizara que no se podrá tener demoras en atención y solución de incidentes por falta de personal técnico para los requerimientos que se presenten y cumplir los niveles de servicios establecidos así: cumplir con el nivel de disponibilidad del servicio de conectividad de Datos e internet ofertado a las sedes urbanas y rurales que deberá ser como mínimo del 99.7%, canal sin reúso 1:1 incluyendo la solución de ultimo kilometro, backbone y nodos necesarios, para la presentación del servicio:
<table>
<tr><th>TIEMPO INDISPONIBILIDAD</th><th>COMPENSACION SOBRE TARIFA MENSUAL</th></tr>
<tr><td>Entre 100% y 99.7%</td><td>0%</td></tr>
<tr><td>Entre 99.6% y 98 %</td><td>4%</td></tr>
<tr><td>Entre 97.9% y 95%</td><td>10%</td></tr>
<tr><td>Entre 94.9% y 90%</td><td>20%</td></tr>
<tr><td>Entre 89.9% y el 80%</td><td>40%</td></tr>
<tr><td>Entre 79.9% y 70%</td><td>60%</td></tr>
<tr><td>Entre 69.9% y 60%</td><td>88%</td></tr>
<tr><td>Menor e Igual al 59.9%</td><td>100%</td></tr>
</table></td><td>Teniendo en cuenta los niveles de servicio se hace relación de sedes que tuvieron tiempo de indisponibilidad a causa de fallas de los servicios asi:
<table>
<tr><th>Sedes</th><th>Total</th><th>% Disponibilidad</th><th>% de descuento</th><th>Valor del descuento</th><th>Valor a facturar por sede</th></tr>
<tr><td>Sede Santa Helena</td><td>$511.700</td><td>70%</td><td>60%</td><td>$307.020</td><td>$204.680</td></tr>
</table></td><td>Se anexa en fisico Formato de descuento en base a los reportes de incidencias generados en los Ticket y en el WhatsApp.</td></tr>
<tr><td>6</td><td>Para los servicios de Internet, el contratista debe contar con una red de fibra óptica propia, anillada, de capacidad mínima de 20 Gbps y equipos robustos de alta fiabilidad, disponibilidad tipo Carrier Grade en su Core</td><td>ALPASURFNET S.A.S cumple con una red propia de Fibra Óptica, anillada, y con capacidad de 20Gbps.</td><td>Se anexan diagramas de topología de red.</td></tr>
<tr><td>7</td><td>El contratista realizará entrega al área TIC del diagrama de la topología física de la red WAN utilizada para la sede principal y de cada una de las sedes.</td><td>Se entrega el Diagrama de topología física de la red WAN, que se usa en la sede Principal y en cada una de las sedes.</td><td>Se ajunta imagen en fisico de la Topología de la RED.</td></tr>
</table>

8	Los planos deberán incluir diagramas de red, descripciones técnicas y lista de materiales necesarios para la implementación del diseño .	Se entregan los Diagramas de Red, las descripciones técnicas y lista de equipos	Se ajunta en fisico en este 3° Informe, los diagramas de red y listado de equipos instalados.
9	El contratista realizará recomendaciones a través de un informe técnico donde presentará alternativas de mejoras para la red y la topología LAN, aplicando criterios de seguridad internas, segmentación y buenas prácticas, para poder llegar a contener ataques internos y externos en la red, sin afectar en gran medida los servicios.	ALPASURFNET S.A.S realizara esta entrega del informe de recomendaciones en el mes de septiembre del 2024.	NA.
10	Contar con un servicio dinámico de gestión de Mesa de Ayuda, por medio de una línea celular que funcione las 6X8 de lunes a viernes de 7AM a 6:00pm y sábados de 7:00am a 1:00pm, como también de una plataforma Web o línea whatsaap o correo electrónico o línea telefónica, para el reporte de tickets que permitan hacer seguimiento a cada una de las PQRS generadas 7X24, que garanticen el control y medición de la disponibilidad del servicio	ALPASURFNET S.A.S. cuenta con una mesa de ayuda que puede ser visitada desde internet desde la siguiente url: http://177.74.204.24/glpi/ De igual forma, contamos con un Call Center de atención al público la cual está disponible las 24 horas, 7 días a la semana, con el objetivo de atender reportes de fallas o consultas con el servicio. La línea de atención es (608)-866-4820 – 316-521-3488	Herramienta de Ticket Web.
11	Contar con un servicio de respaldo (Backup) de conectividad de datos e internet disponible 7x4 en las Sedes Canaima, palmas, granjas, caimi e IPC, como contingencia ante eventualidades generales no previstas, que garantice la prestación del servicio de forma interrumpida, este respaldo deberá ser en tecnología diferente a Fibra Optica y no debe converger en el mismo punto core del contratista para evitar así indisponibilidades.	ALPASURFNET S.A.S. cuenta con una red anillada en Fibra Oscura en las sede Canaima, palmas, granjas, IPC, Eduardo santos, Santa Isabel y Bodega; Dicho anillo está disponible 7x24 y actúa como contingencia ante eventualidades que se presenten en Canaima o alguna de estas sede.	Se evidenciará en el las topologías y diagramas de red.
12	Suministrar, instalar y configurar en cada sede (rural o urbana) equipos de conectividad de tipo carrier grade, de alta disponibilidad, tipo Enterprise, y en caso de presentarse fallas, deberán ser remplazados por otro de igual o superior características que garanticen un óptimo servicio, sin costo alguno En caso de realizar suministros e	En cada una de las sedes se instalaron equipos de borde (routers) nuevos con características técnicas que garantizan una alta disponibilidad de los servicios. Un equipo Router ONT marca Huawei en cada sede urbana y routers de marca Mikrotik.	Se evidencia en el listado de equipos anexo.

	instalaciones de servicios en sedes nuevas, éstas deben ser realizadas con plazo máximo 15 días desde la firma del acta de inicio del contrato		
13	Asumir los costos por la instalación y configuración de los equipos, transporte, mano de obra que se requieran para la puesta en marcha de la solución y verificación de los canales de conectividad, dentro del área de cobertura en zonas urbanas y rurales y en caso de que haya lugar realizar cambios de equipos y/o solucionar fallas oportunamente que se presenten en la prestación de los servicios suministrados sin que esto tenga costo adicional para la ESE CARMEN EMILIA OSPIN	ALPASURFNET S.A.S. realizo la instalacion y configuracion de los equipos en cada sede, asumiendo todos los costos asociados por la esta actividad como son los equipos, material, transporte, mano de obra requerida para la puesta en marcha del Servicio de Conectividad a internet.	Se anexan actas de instalacion de cada sede.
14	Disponer de un rango mínimo de 10 direcciones IP públicas libres, sin NAT, no reportadas en listas negras, para garantizar los servicios web implementados por La ESE CARMEN EMILIA OSPINA	ALPASURFNET S.A.S. asigno a la ESE CARMEN EMILIA en su sede de CANAIMA las siguientes direcciones IPv4 públicas, de la red 177.74.205.240/29 teniendo disponibles las direccion 177.74.204.241,177.74.205.242, 177.74.205.243, 177.74.205.244, 177.74.205.245, 177.74.204.246. asignándose a los siguientes servicios por IPv4 asi: **IPv4 EQUIPO/OFICINA SERVICIO** 177.74.204.241 SOPHOS FIREWALL INTERNET 177.74.205.242 TESORERIA INTERNET Técnicamente se recomienda no exponer la totalidad de las IP sin darles un uso concreto, como buena práctica de TI, razón por la cual sólo se hace uso de 2 IPS públicas.	Se evidenciará en los diagramas de red anexos.
15	Garantizar la interoperabilidad de los demás equipos Networking y de telecomunicaciones que disponga la ESE. CARMEN EMILIA OSPINA con los equipos, servicios y canales de conectividad contratados e instalados por el contratista	ALPASURFNET S.A.S. y su personal tecnico, garantiza la interoperabilidad se los equipos Networking y de telecomunicaciones que disponga la ESE. CARMEN EMILIA OSPINA con los equipos, servicios y canales de conectividad contratados	No Aplica
16	Suministrar en calidad de comodato, un Firewall de alto throughput, para prestar la seguridad perimetral de la entidad y realizar la Gestión Unificada de Amenazas (UTM) el cual cuente con múltiples funciones añadidas, trabajando a nivel de aplicación para prestar servicios de seguridad	ALPASURFNET S.A.S. en modo de comodato, instala en la ESE Carmen Emilia Ospina sede Canaima un equipo SOPHOS FIREWALL XGS330 que cumple con los requerimientos de esta obligación, se pone a disposición un personal especializado para la configuracion de las políticas de seguridad perimetral que aplicaran al tráfico de INTERNET y red LAN, protegiendo la integridad de los datos digitales que	Se anexa Ficha tecnica del equipos SOPHOS FIREWALL.

	perimetral, herramientas de tráfico de datos, procesar el tráfico a modo de proxy, analizando y gestionando el tráfico en función de la política implementada en el dispositivo, establecer balanceo de carga, protección contra múltiples amenazas, gestión de VPN, prevención de intrusos, antivirus, filtrado web, anti spam y administración de ancho de banda, con una licencia de uso a término por la duración del contrato con capacidad de mínima de 600 usuarios, suministrado por el contratista en calidad de comodato, ubicado en la sede principal Canaima para centralizar todas las conexiones hacia los demás centros de salud y sedes administrativas de forma bidireccional según la topología de red disponible y asociada a la arquitectura tecnológica de la ESE Carmen Emilia Ospina en el Municipio de Neiva. Incluye por parte del contratista, la realización de la instalación, configuración, parametrización y puesta en marcha de las políticas web, restricciones de aplicaciones y de portales web y demás que el Supervisor considere necesarias; como también realizará la asignación de un usuario con perfiles de Administrador que permita la coadministración del firewall por parte de la entidad, asi mismo se socializarán las herramientas de análisis como Google Analytics, entender y clasificar el tráfico	transitan por la red de WAN que soporta los servicios de conectividad de este contrato CPS 009 del 2025	
17	Presentar un informe en tiempo real de amenazas e incidencia sobre los ataques, hallazgos y acciones realizadas donde se mitigue el riesgo las cuales fueron encontradas a través del monitoreo realizado con personal calificado que ofrece la plataforma de seguridad perimetral en el horario de lunes a viernes de 6:00am a 11:00pm y sábado, domingo y festivos de 7:00am a 6:00pm. El informe debe ser socializado ante el supervisor donde se	Se presenta informe de amenazas e incidencias sobre la seguridad perimetral WEB proporcionadas por el SOPHOS FIREWALL del periodo 1 de abril a 30 de abril del 2025.	Se anexa en fisico Informe Especializado de la Seguridad Perimetral.

	evidencie estadísticas mensuales y se brinde acompañamiento, asesoramiento en las recomendaciones de las amenazas, con políticas que minimicen el riesgo de ataques cibernético buscando contar siempre con una postura de ciberseguridad acorde con las necesidades de la ESE Carmen Emilia Ospina.		
18	La E.S.E CARMEN EMILIA OSPINA se reserva el derecho de solicitar suspensión de canales de servicio y su correspondiente facturación por razones de traslados, remodelación, unificación de Centros de Salud, sedes, casos fortuitos o retiro de estas. Estas suspensiones deberán realizarse a más tardar tres (3) días calendario después de enviada la solicitud vía email, ticket o escrita del supervisor del contrato. La suspensión de los canales puede ser definitiva o temporal y será tenida en cuenta para su respectivo descuento.	En este periodo el supervisor no solicito suspensión de los canales de servicio a internet de ninguna de las sedes contratadas	No Aplica
19	Realizar al menos uno (1) mantenimiento preventivo de los equipos y sistemas que hagan parte de los canales de conectividad de datos e internet entregados y utilizados, cuando la ejecución en tiempo del contrato esté entre el 50% y 60%. En caso de requerirse mantenimiento correctivo al firewall o a los equipos de orden o de ultimo kilometro instalado, por cualquier causa o anomalía técnica, estos costos son asumidos directamente y en su totalidad por el contratista.	en este periodo no se realizó mantenimiento preventivo de los equipos de conectividad	No Aplica
20	El supervisor del contrato podrá citar de forma extraordinaria la realización de mesas técnicas las veces que sean necesarias, previa comunicación de mínimo dos días al contratista, este proceso debe permitir el supervisor la verificación y evaluación de los servicios prestados, aportándole toda la información o evidencia de cualquier tipo relacionada con la ejecución, administración y operación del contrato.	El supervisor realiza reunión de mesa técnica para socialización el informe mensual de ejecución del contrato 009 de 2025	Acta de Reunión
21	Contar con todos los equipos, maquinaria, herramientas, materiales,	ALPASURFNET S.A.S. cuenta con todos los equipos y maquinarias necesarios para la ejecución contractual	No Aplica

	demás elementos y recurso humano técnico necesarios para la ejecución del objeto contractual.		
22	Cumplir con los demás niveles de servicio relacionados en la propuesta técnica y comercial presentada.	ALPASURFNET S.A.S. cumplió con los niveles de Servicio relacionados en la propuesta técnica y comercial presentada	No Aplica
23	Guardar la debida y completa reserva sobre la información y los documentos que tenga conocimiento o a los que tenga acceso en virtud de la ejecución del contrato y utilizarla exclusivamente en relación con los fines del mismo.	ALPASURFNET S.A.S. guarda debida reserva de la información y documentos de los que se tienen acceso.	No Aplica
24	Mantener indemne a la entidad frente a reclamaciones judiciales y extrajudiciales por los daños y perjuicios que se deriven de los actos, omisiones o hechos ocasionados.	ALPASURFNET S.A.S. mantiene indemne a la entidad frente a reclamaciones judiciales y extrajudiciales.	No Aplica
25	Cumplir con las acciones y operaciones de almacenamiento, tratamiento, aprovechamiento (recuperación/reciclado) y/o disposición final de residuos de aparatos eléctricos y electrónicos (RAEE), usados durante y posteriormente de la ejecución del presente proceso contractual.	ALPASURFNET S.A.S. cumple con las acciones y operación de aprovechamiento de Residuos de aparatos Eléctricos y Electrónicos.	No Aplica
26	Generar las facturas y cobrar mes vencido, relacionando el costo por cada centro de salud o sedes con su respectivos detalle o concepto.	ALPASURFNET S.A.S. mensualmente se presenta la factura mes vencido de 30 días, este reporte se toma en cuenta los días desde el 1 de marzo del 2025 hasta el 31 de marzo del 2025, lo que nos da 31 días de servicios, los cueles son relacionados el costo de cada sede junto con el informe de actividades y los respectivos soportes.	Se anexa factura

Sedes	**Total**	**Valor del descuento**	**Valor a facturar por sede**
Servicio de Internet Dedicado Sede Canaima	3.077.038	$0	3.077.038
Sede Palmas	1.153.792	$0	1.153.792
Sede Caimi	1.170.365	$0	1.170.365

Sede 7 de Agosto	1.170.365	$0	1.170.365	
Sede Eduardo Santos	1.136.807	$0	1.136.807	
Sede Granjas	1.136.807	$0	1.136.807	
Sede IPC	1.136.807	$0	1.136.807	
Sede Santa Isabel	1.136.807	$0	1.136.807	
Sede Caguan	529.550	$0	529.550	
Sede Fortalecillas	529.550	$0	529.550	
Sede San Francisco	511.700	$0	511.700	
Sede Triunfo	511.700	$0	511.700	
Sede San Antonio	511.700	$0	511.700	
Sede San Luis	797.300	$0	797.300	
Sede Vegalarga	529.550	$0	529.550	
Sede Chapinero	511.700	$0	511.700	
Sede El Cedral	511.700	$0	511.700	
Sede Aipecito	511.700	$0	511.700	
Sede Palestina	511.700	$0	511.700	
Sede Palacio	511.700	$0	511.700	
Sede Santa Helena	511.700	307.020	204.680	
Sede Guacirco	529.550	$0	529.550	

		Sede Peñas Blancas	511.700	$0	511.700	
		Sede San Jorge	511.700	$0	511.700	
		Sede Colegio	511.700	$0	511.700	
		Sede Piedra Marcada	511.700	$0	511.700	
		Seguridad Web Perimetral 600 usuarios	6.413.612	$0	6.413.612	
		TOTAL	27.100.000	307.020	26.792.980	
		Incluye los descuentos por ANS del periodo correspondiente.				
27	Las demás inherentes a la ejecución y naturaleza del objeto contractual.	En este periodo no se designaron obligaciones inherentes a la ejecución contractual.				No Aplica

Observación: el valor de la factura corresponde a los servicios prestados en las sedes activas del durante el periodo comprendido entre 1 de abril al 30 de abril de 2025

VALOR DE PERIODO EJECUTADO: VEINTI SEIS MILLONES SETECIENTOS NOVENTA Y DOS MIL NOVECIENTOS OCHENTA PESOS MTC ($26.792.980).

Atentamente,

GUSTAVO ADOLFO ANDRADE D.
C.C.7.688.838
R.L- ALPASURFNET SAS

LILIANA CAROLINA GONZALEZ GUTIERREZ
Supervisor (a)

JOSE YAMIL LAGUNA
Apoyo a la supervisión

Neiva, 5 de mayo del 2025

Señores
Coordinación TIC
ESE CARMEN EMILIA OSPINA
Ciudad.

Referencia: CERTIFICACION DISPONIBILIDAD DE LOS SERVICIOS DE CONECTIVIDAD E INTERNET

ALPASURFNET SAS en calidad de Prestador del Servicio de INTERNET (ISP), certifica que los servicios de conectividad e INTERNET prestados bajo el CONTRATO DE PRESTACION DE SERVICIOS número 00009 del 2025, que incluyen 9 sedes URBANAS y 18 sedes RURALES en el Municipio de Neiva, así como el canal de respaldo del servicio de INTERNET y la Seguridad Perimetral WEB de la sede Canaima, tienen una disponibilidad de 24 horas los 7 días de la semana; estos servicios cumplen con las regulaciones de la Comisión de Regulación de las Comunicaciones (CRC) en las resoluciones número 1740 del 2007, 3503 del 2011 y 3496 del 2011 incluyendo sus modificaciones.

Dada a los 5 días del mes de mayo del 2025 a solicitud de la **ESE CARMEN EMILIA OSPINA**.

Atentamente,

GUSTAVO ADOLFO ANDRADE D.
C.C.7.688.838
R.L- ALPASURFNET SAS

INFORME MENSUAL

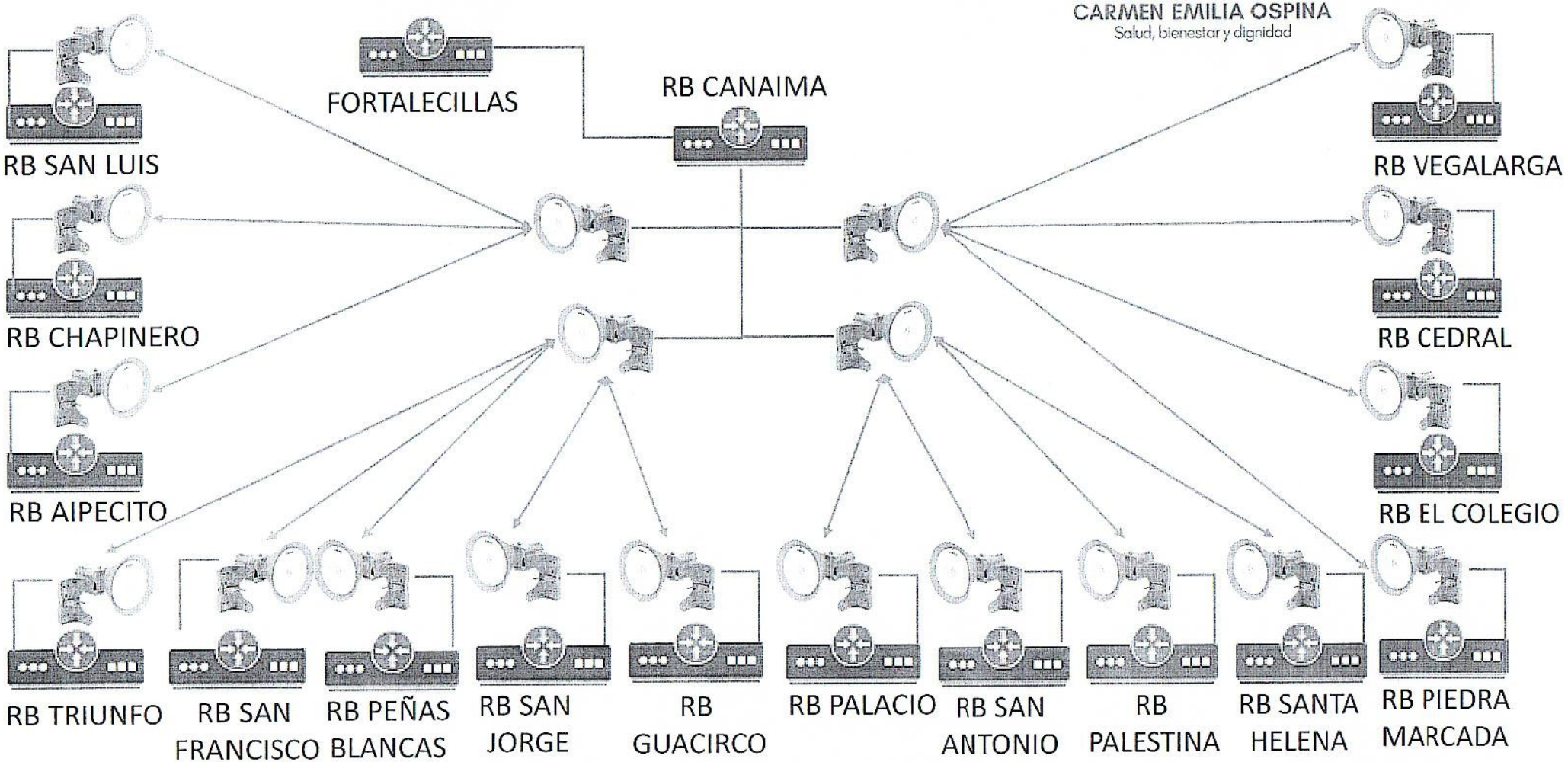
DATOS DEL INFORME	
TIPO DE INFORME	Reporte de Personal Técnico
NÚMERO DEL INFORME	2
FECHA DE PRESENTACIÓN	05 DE MAYO DE 2025

RELACIÓN PERSONAL TÉCNICO – PROFESIONAL

NOMBRES	CARGO	PROFESIÓN	IDENTIFICACIÓN	EPS	ARL
JHON ERICK ANDRADE DUSSAN	TECNICO	TECNICO DE REDES	12.125.872	SANITAS	AXA COLPATRIA
WILSON DE JESUS MORALES PATIÑO	TECNICO	TECNICO DE REDES	17.654.995	NUEVA EPS	AXA COLPATRIA
CARLOS RODOLFO CORTES DUQUE	TECNICO	TECNICO DE REDES	12.118.082	SANITAS	AXA COLPATRIA
LUDOVIC SAGRE GARCIA	TECNICO	TECNICO DE REDES	7.725.782	SANITAS	AXA COLPATRIA

ALPASURFNET SAS
NIT. 828.000.170-8
Carrera 14ª 6 14
E-mail: alpavision@gmail.com
Línea : 608 8664820
Neiva – Huila - Colombia

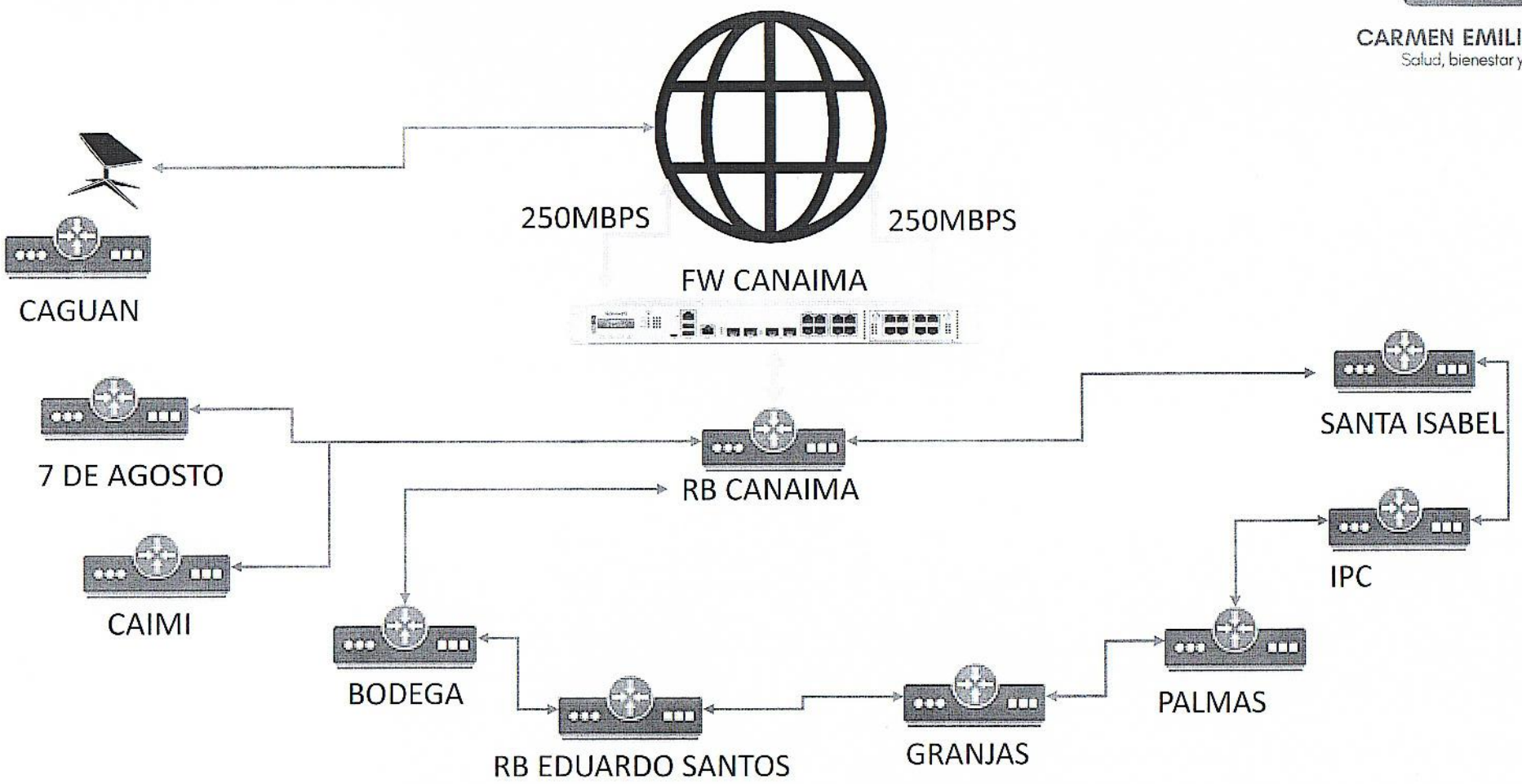
TOPOLOGIA DE RED WAN ZONA RURAL



AlpaSurfnet

TOPOLOGIA DE RED WAN ZONA URBANA

CARMEN EMILIA OSPINA
Salud, bienestar y dignidad



Sedes	Anchos de Banda	Total sin Iva	Total sin Iva	Total Con Iva	Valor Por Hora	Numero de Horas	Horas Prestadas	% Disponibilidad	% de descuento	Valor del descuento	Valor a facturar por sede	Días de servio	Valor en horas
Servicio de Internet Dedicado Sede Canaima	250	2.585.746	2.585.746	3.077.038	$ 4.274	0	720	100	0%	$0	3.077.038	30	720
Sede Palmas	FIBRA OSCURA	969.573	969.573	1.153.792	$ 1.602	0	720	100	0%	$0	1.153.792		
Sede Caimi	100	983.500	983.500	1.170.365	$ 1.626	0	720	100	0%	$0	1.170.365		
Sede 7 de Agosto	100	983.500	983.500	1.170.365	$ 1.626	0	720	100	0%	$0	1.170.365		
Sede Eduardo Santos	FIBRA OSCURA	955.300	955.300	1.136.807	$ 1.579	0	720	100	0%	$0	1.136.807		
Sede Granjas	FIBRA OSCURA	955.300	955.300	1.136.807	$ 1.579	0	720	100	0%	$0	1.136.807		
Sede IPC	FIBRA OSCURA	955.300	955.300	1.136.807	$ 1.579	0	720	100	0%	$0	1.136.807		
Sede Santa Isabel	FIBRA OSCURA	955.300	955.300	1.136.807	$ 1.579	0	720	100	0%	$0	1.136.807		
Sede Caguan	30	445.000	445.000	529.550	$ 735	0	720	100	0%	$0	529.550		
Sede Fortalecillas	30	445.000	445.000	529.550	$ 735	0	720	100	0%	$0	529.550		
Sede San Francisco	10	430.000	430.000	511.700	$ 711	0	720	100	0%	$0	511.700		
Sede Triunfo	10	430.000	430.000	511.700	$ 711	0	720	100	0%	$0	511.700		
Sede San Antonio	10	430.000	430.000	511.700	$ 711	0	720	100	0%	$0	511.700		
Sede San Luis	20	670.000	670.000	797.300	$ 1.107	0	720	100	0%	$0	797.300		
Sede Vegalarga	30	445.000	445.000	529.550	$ 735	0	720	100	0%	$0	529.550		
Sede Chapinero	10	430.000	430.000	511.700	$ 711	0	720	100	0%	$0	511.700		
Sede El Cedral	10	430.000	430.000	511.700	$ 711	0	720	100	0%	$0	511.700		
Sede Aipecito	10	430.000	430.000	511.700	$ 711	0	720	100	0%	$0	511.700		
Sede Palestina	10	430.000	430.000	511.700	$ 711	0	720	100	0%	$0	511.700		
Sede Palacio	10	430.000	430.000	511.700	$ 711	0	720	100	0%	$0	511.700		
Sede Santa Helena	10	430.000	430.000	511.700	$ 711	216	504	70	60%	$307.020	204.680		
Sede Guacirco	30	445.000	445.000	529.550	$ 735	0	720	100	0%	$0	529.550		
Sede Peñas Blancas	10	430.000	430.000	511.700	$ 711	0	720	100	0%	$0	511.700		
Sede San Jorge	10	430.000	430.000	511.700	$ 711	0	720	100	0%	$0	511.700		
Sede Colegio	10	430.000	430.000	511.700	$ 711	0	720	100	0%	$0	511.700		
Sede Piedra Marcada	10	430.000	430.000	511.700	$ 711	0	720	100	0%	$0	511.700		
		17.383.519		20.686.388	$ 28.731					$307.020	20.379.368		
SOPHOS		5.389.590	5.389.590	6.413.612	$ 8.908			SOPHOS	5.389.590	1.024.022	6.413.612		
				27.100.000							26.792.980		
											26.792.980		

AlpaSurfnet
alpavisión

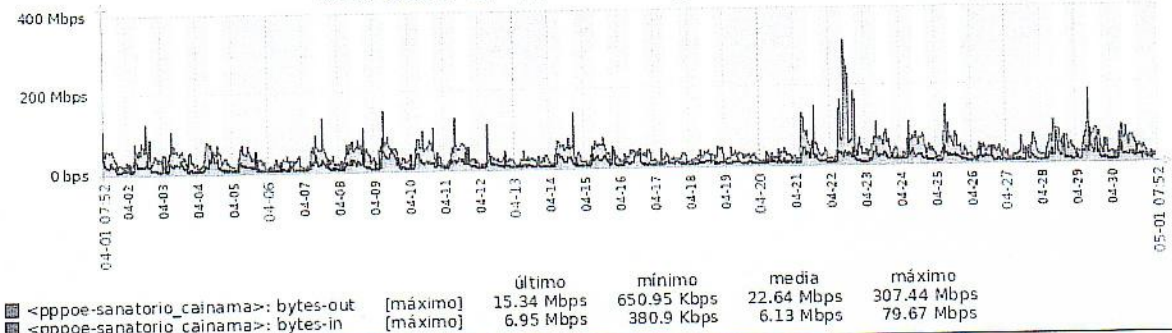
DATOS DEL INFORME	
PROYECTO	CPS 00009 del 2025
DESTINATARIO	ESE CARMEN EMILIA OSPINA
TIPO DE INFORME	Graficas Disponibilidad
NÚMERO DEL INFORME	3
PERIODO DEL INFORME	1 de abril al 30 de abril de 2025.
FECHA DE PRESENTACIÓN	5 de mayo de 2025

ITEM	SEDES
1	Servicio de Internet Dedicado Sede Canaima
2	Sede Palmas
3	Sede Caimi
4	Sede 7 de agosto
5	Sede Eduardo Santos
6	Sede Granjas
7	Sede IPC
8	Sede Santa Isabel
9	Sede Bodega
10	Sede Caguan
11	Sede Fortalecillas
12	Sede San Francisco
13	Sede Triunfo
14	Sede San Antonio
15	Sede San Luis
16	Sede Vegalarga
17	Sede Chapinero
18	Sede El Cedral
19	Sede Aipecito
20	Sede Palestina
21	Sede Palacio
22	Sede Santa Helena
23	Sede Guacirco
24	Sede Peñas Blancas
25	Sede San Jorge
26	Sede Colegio
27	Sede Piedra Marcada

Las siguientes gráficas muestran el consumo de cada una de las sedes urbanas y rurales de la ESE. Estos consumos hacen referencia a la cantidad de datos que fueron transferidos por los canales de datos instalados usando tecnologías de última milla como fibra óptica y radio enlace. El tráfico generado y transferido desde las sedes hacia los diferentes aplicativos y servicios (índigo, intranet, SIMAD, telefonía VoIP, entre otros) ubicados en Canaima se cuantificó en Megabytes (MB), Kilobytes (KB) y las tasas de transferencias en Megabits por segundo (Mbps) y Kilobits por segundo (Kbps). Éstos fueron reportados por los sistemas de gestión propios de ALPASURFNET.

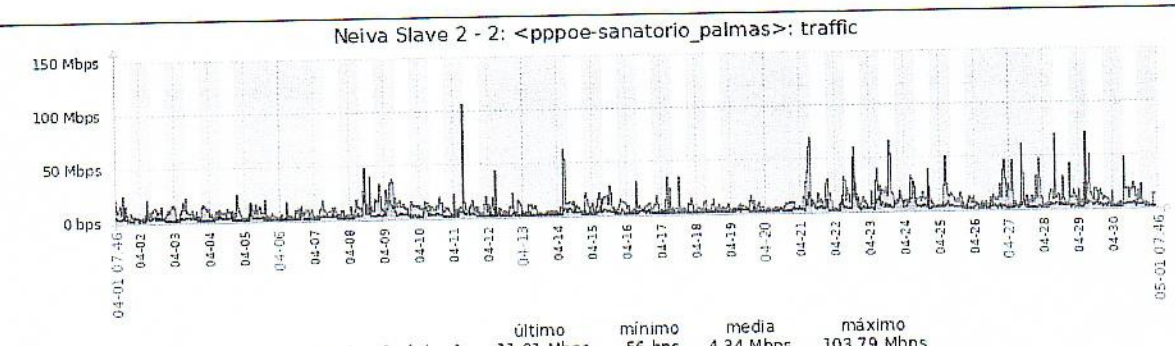
AlpaSurfnet
visión

1. Servicio de Internet Dedicado Sede Canaima



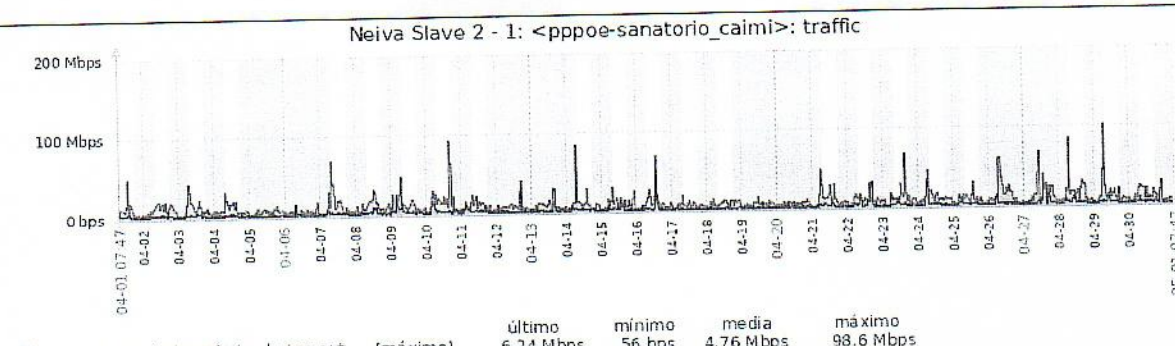
		último	mínimo	media	máximo
<pppoe-sanatorio_cainama>: bytes-out	[máximo]	15.34 Mbps	650.95 Kbps	22.64 Mbps	307.44 Mbps
<pppoe-sanatorio_cainama>: bytes-in	[máximo]	6.95 Mbps	380.9 Kbps	6.13 Mbps	79.67 Mbps

2. Sede Palmas



		último	mínimo	media	máximo
<pppoe-sanatorio_palmas>: bytes-out	[máximo]	11.91 Mbps	56 bps	4.34 Mbps	103.79 Mbps
<pppoe-sanatorio_palmas>: bytes-in	[máximo]	929.74 Kbps	64 bps	1.32 Mbps	69.4 Mbps

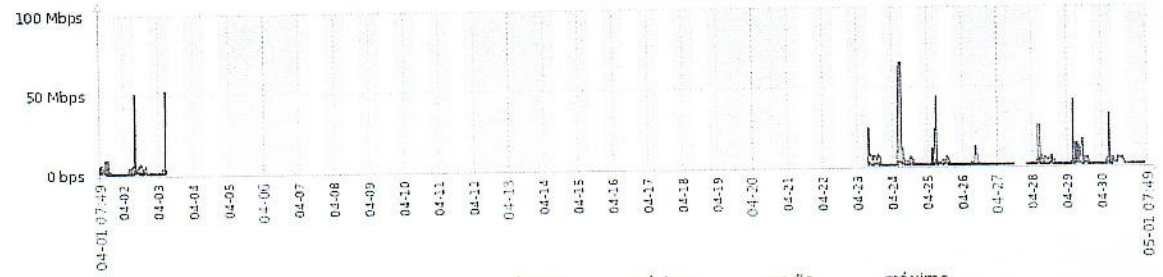
3. Sede Caimi



		último	mínimo	media	máximo
<pppoe-sanatorio_caimi>: bytes-out	[máximo]	6.24 Mbps	56 bps	4.76 Mbps	98.6 Mbps
<pppoe-sanatorio_caimi>: bytes-in	[máximo]	985.18 Kbps	64 bps	1.19 Mbps	44.29 Mbps

4. Sede 7 de agosto

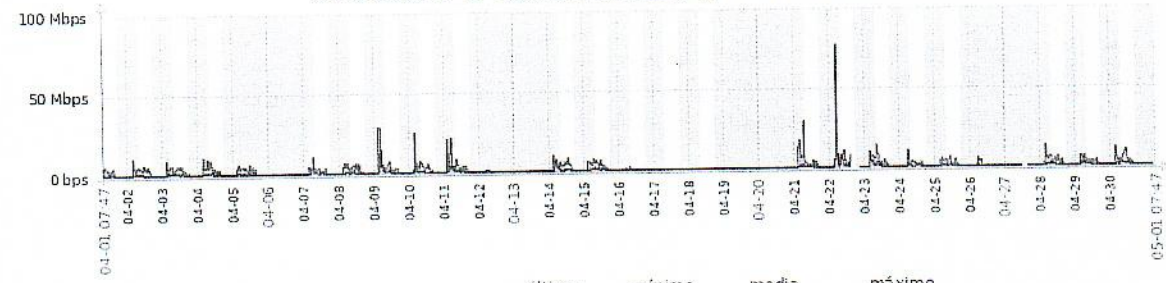
Neiva Slave 1 - 3: <pppoe-sanatorio_7_agosto>: traffic



		último	mínimo	media	máximo
<pppoe-sanatorio_7_agosto>: bytes-out	[máximo]	197.41 Kbps	42.23 Kbps	1.33 Mbps	64.15 Mbps
<pppoe-sanatorio_7_agosto>: bytes-in	[máximo]	62.08 Kbps	6.97 Kbps	285.27 Kbps	13.54 Mbps

5. Sede Eduardo Santos

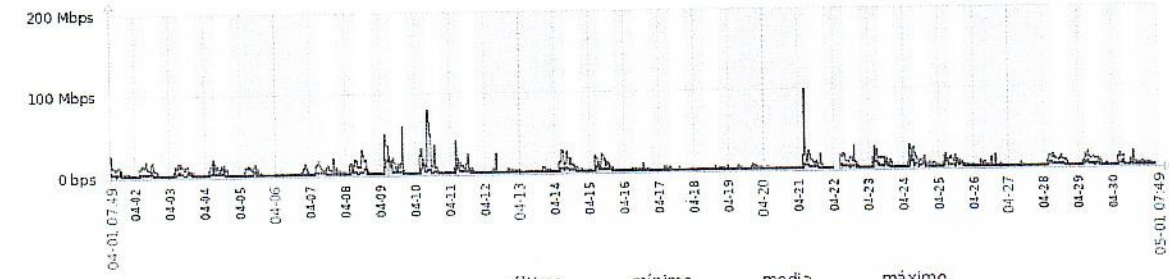
Neiva Slave 1 - 3: <pppoe-sanatorio_ed_santos>: traffic



		último	mínimo	media	máximo
<pppoe-sanatorio_ed_santos>: bytes-out	[máximo]	200.56 Kbps	56 bps	872.01 Kbps	76.27 Mbps
<pppoe-sanatorio_ed_santos>: bytes-in	[máximo]	44.32 Kbps	64 bps	276.63 Kbps	14.68 Mbps

6. Sede Granjas

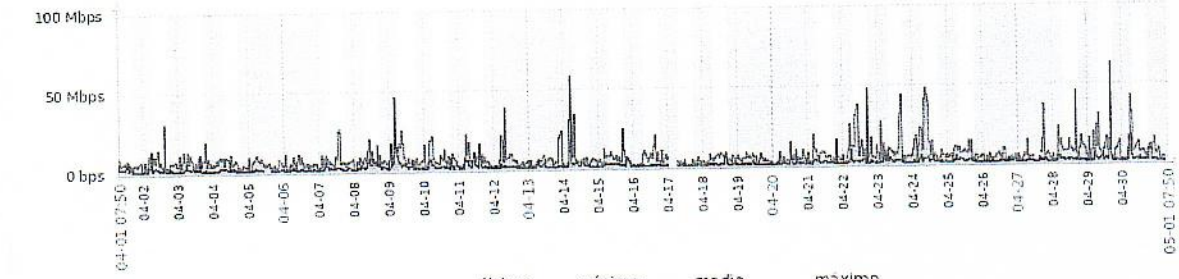
Neiva Slave 2 - 1: <pppoe-sanatorio_granjas>: traffic



		último	mínimo	media	máximo
<pppoe-sanatorio_granjas>: bytes-out	[máximo]	221.7 Kbps	22.89 Kbps	2.37 Mbps	97.15 Mbps
<pppoe-sanatorio_granjas>: bytes-in	[máximo]	125.24 Kbps	1.78 Kbps	643.76 Kbps	19.73 Mbps

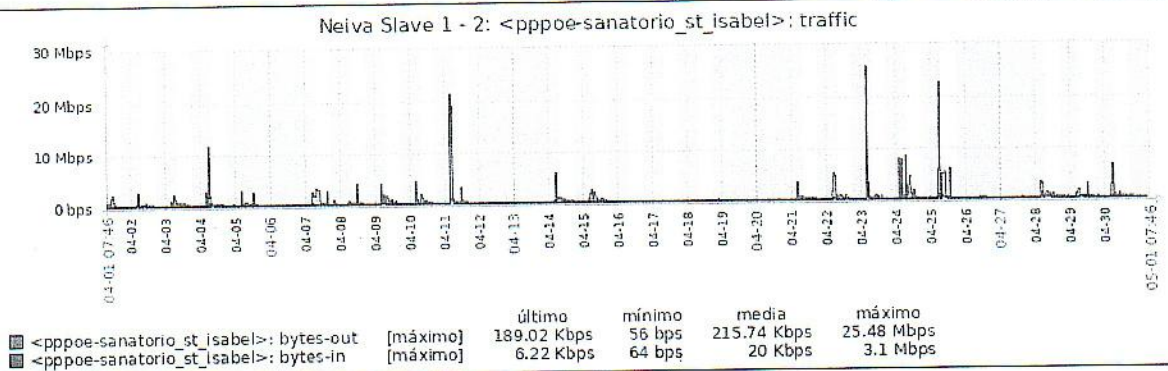
7. Sede IPC

Neiva Slave 1 - 3: <pppoe-sanatorio_ipc>: traffic



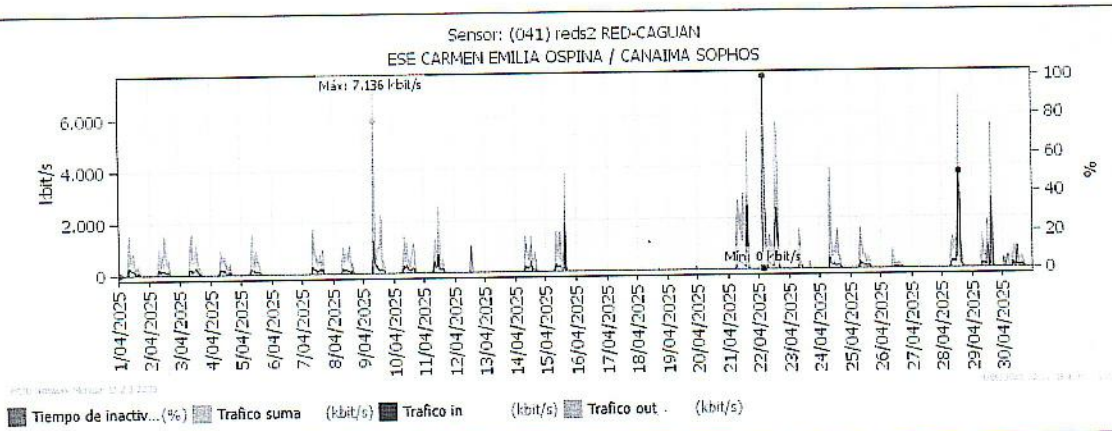
		último	mínimo	media	máximo
<pppoe-sanatorio_ipc>: bytes-out	[máximo]	2.86 Mbps	48 bps	3.25 Mbps	46.88 Mbps
<pppoe-sanatorio_ipc>: bytes-in	[máximo]	748.9 Kbps	64 bps	984.74 Kbps	62.31 Mbps

8. Sede Santa Isabel

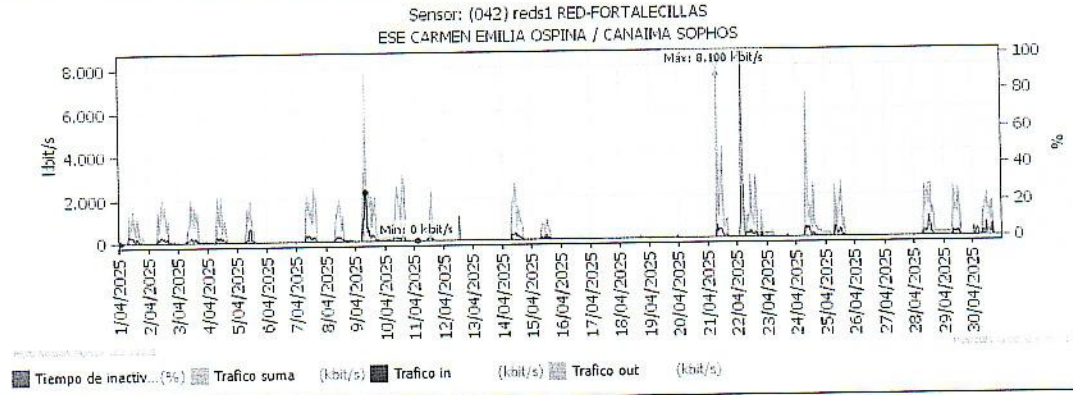


9. Sede Bodega

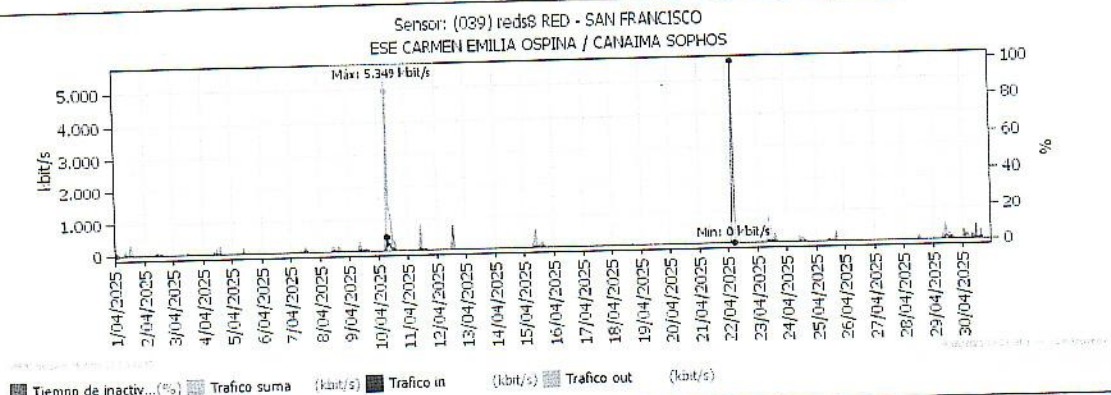
10. Sede Caguán



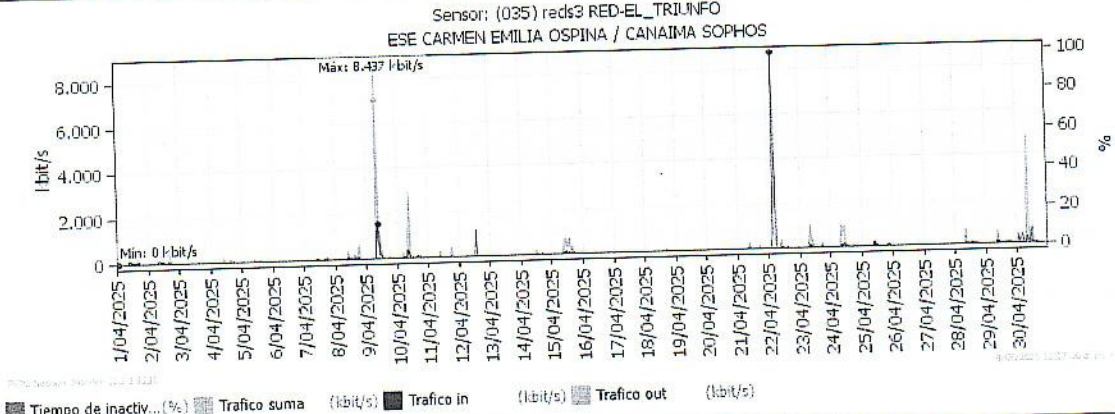
11. Sede Fortalecillas



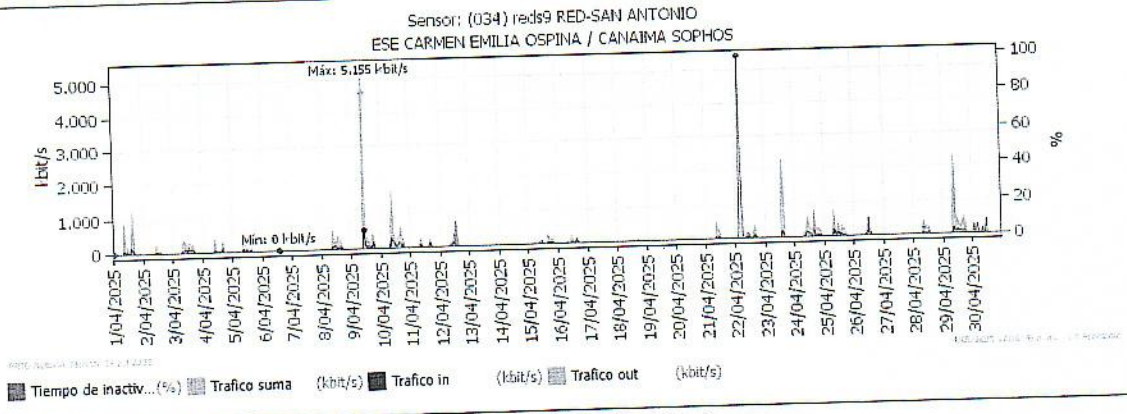
12. Sede San Francisco



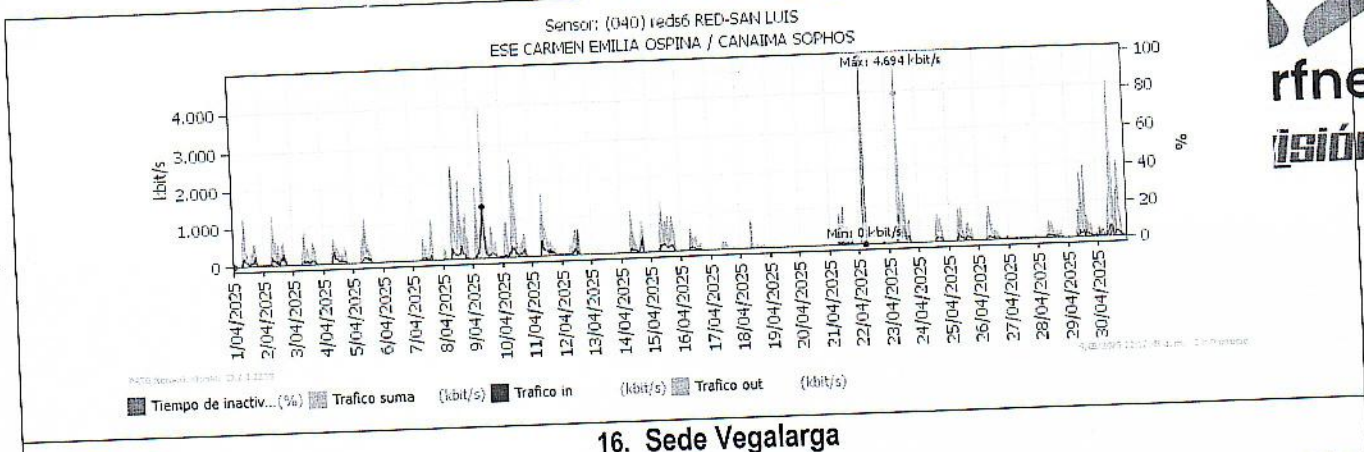
13. Sede Triunfo



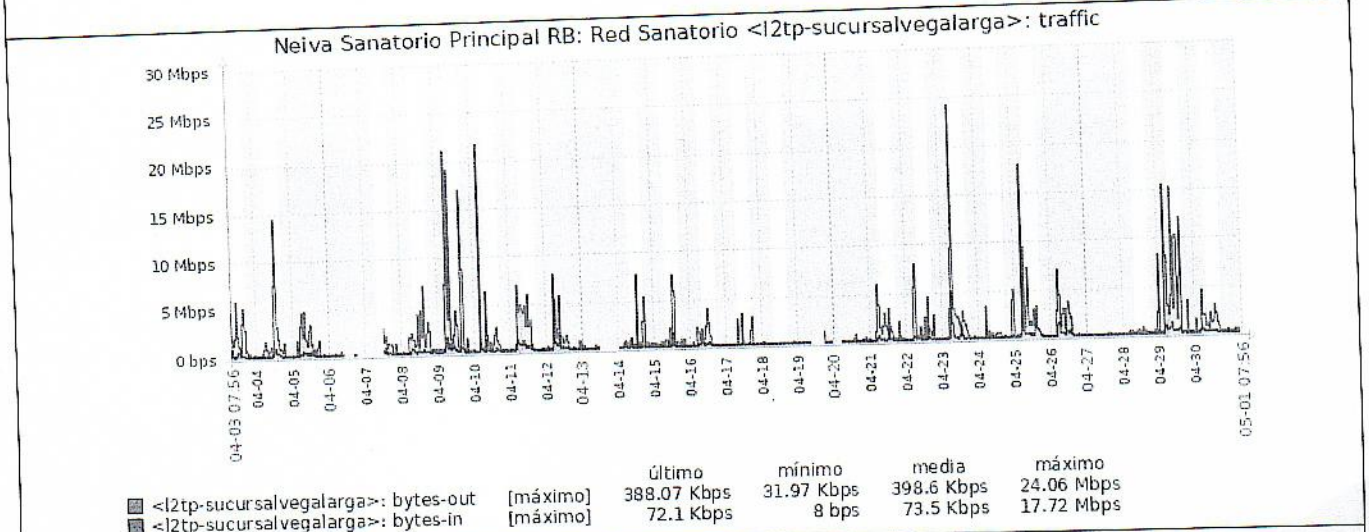
14. Sede San Antonio



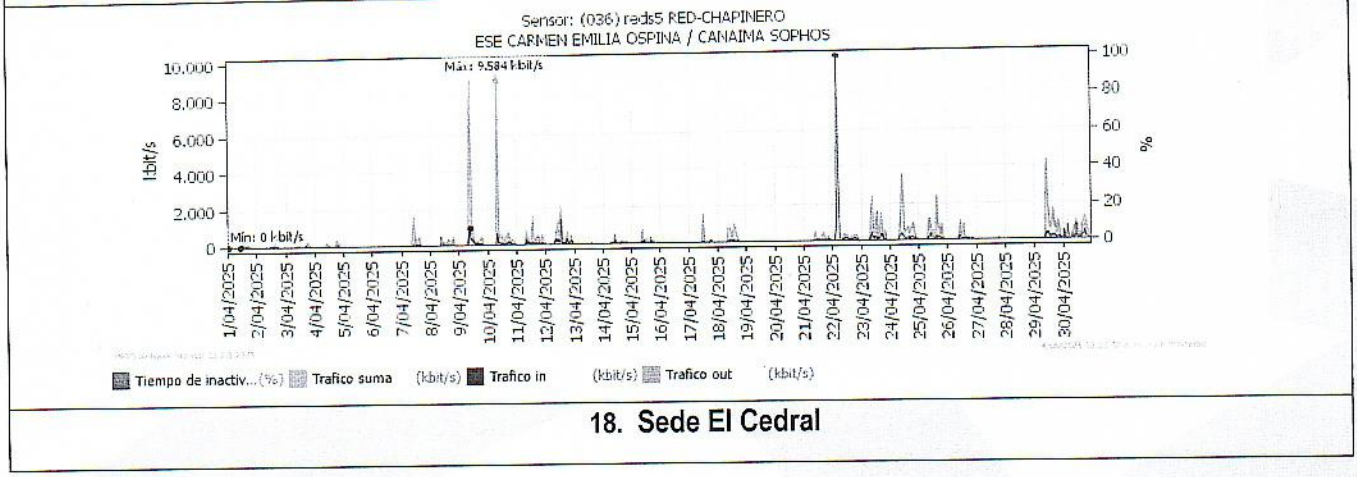
15. Sede San Luis



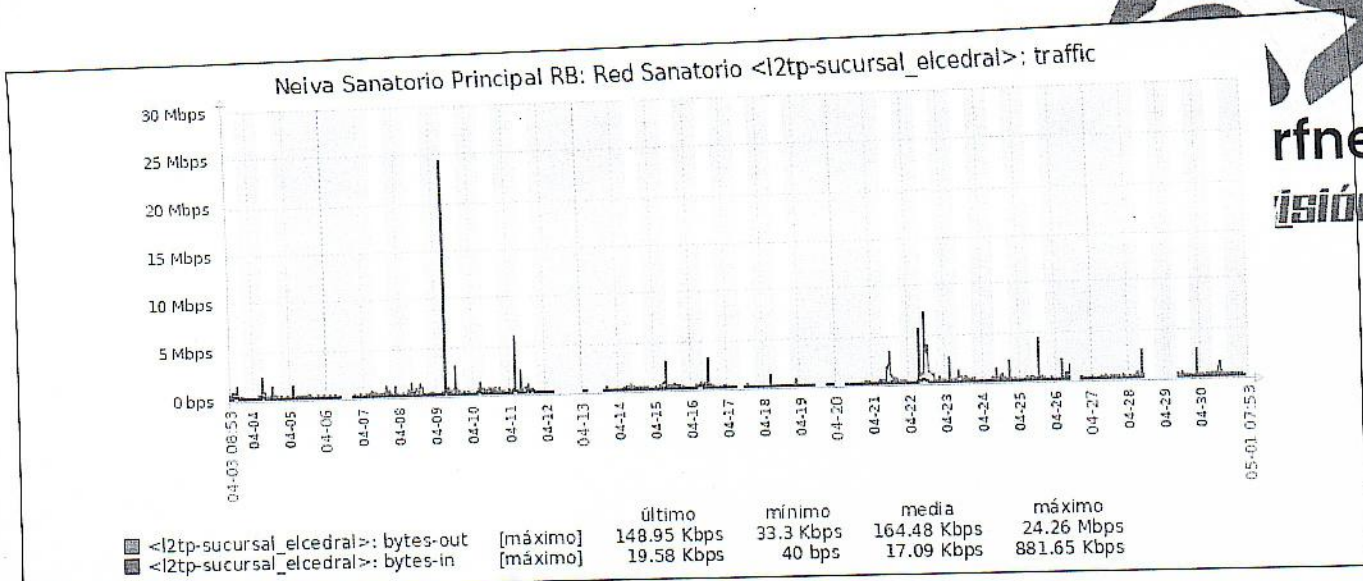
16. Sede Vegalarga



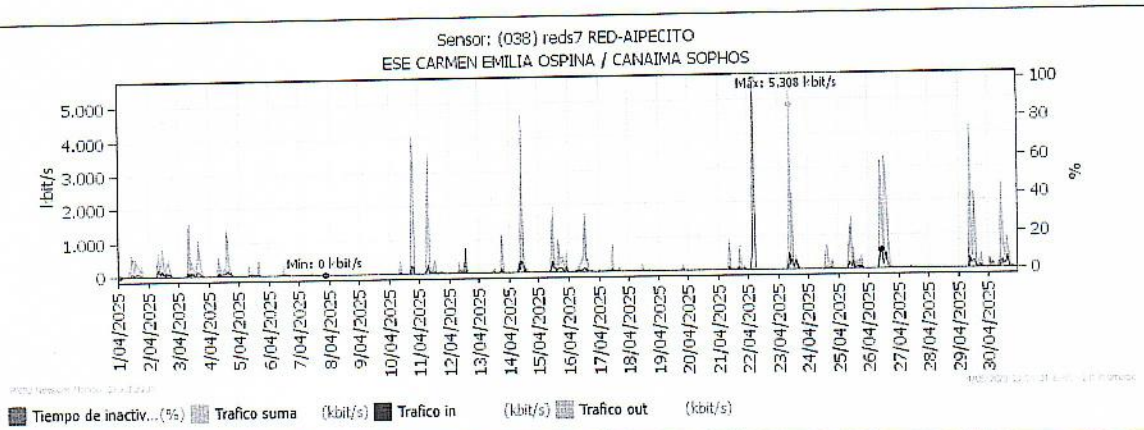
17. Sede Chapinero



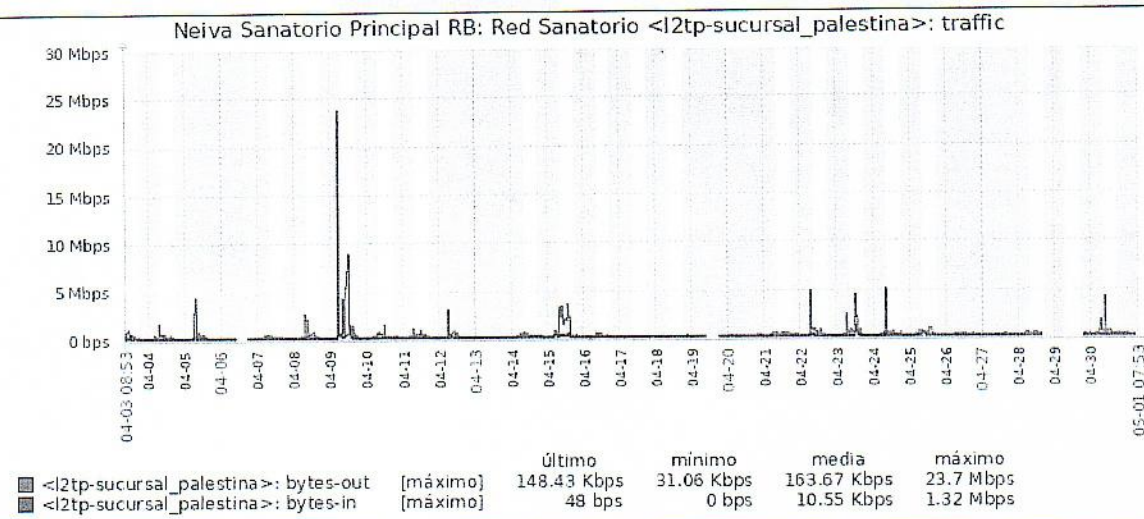
18. Sede El Cedral



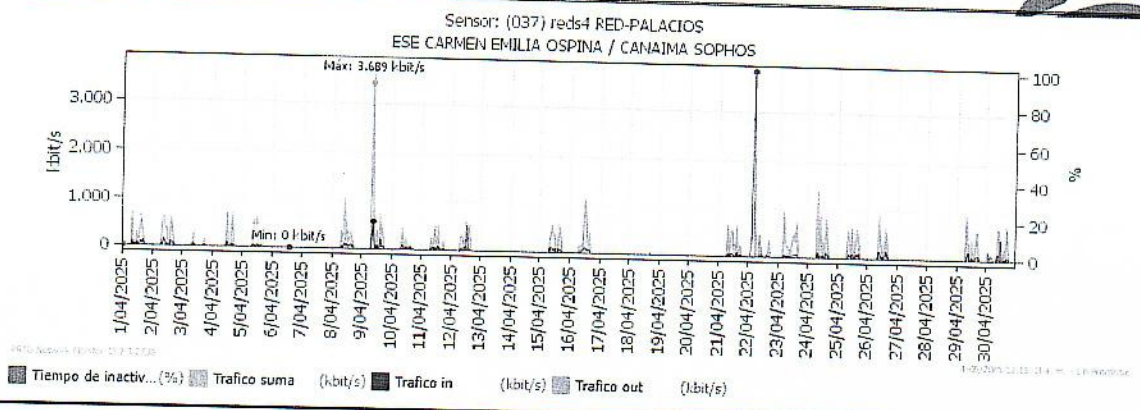
19. Sede Aipecito



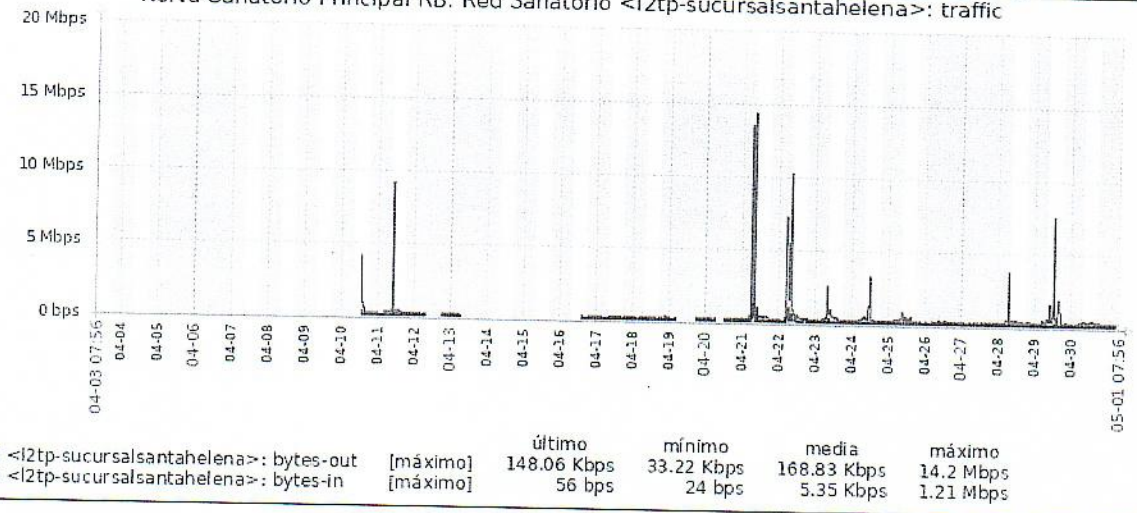
20. Sede Palestina



21. Palacio



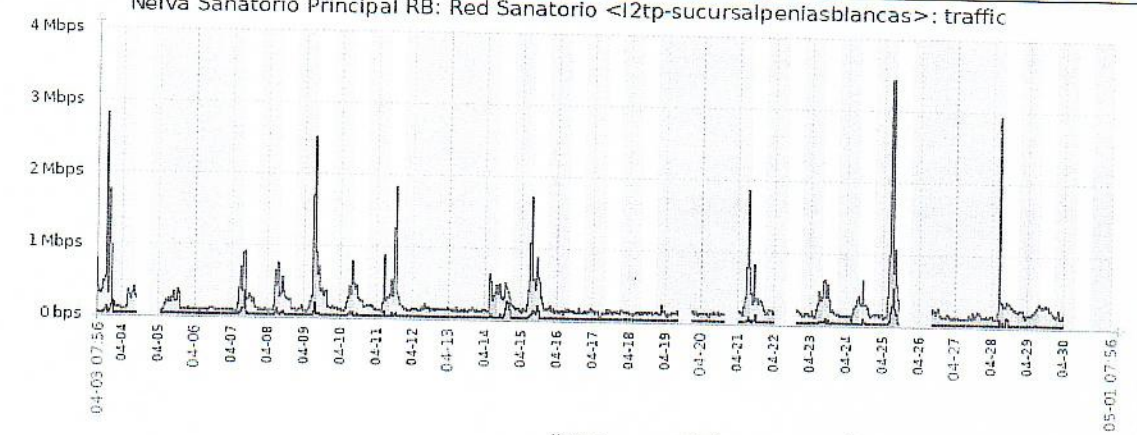
22. Sede Santa Helena



		último	mínimo	media	máximo
<l2tp-sucursalsantahelena>: bytes-out	[máximo]	148.06 Kbps	33.22 Kbps	168.83 Kbps	14.2 Mbps
<l2tp-sucursalsantahelena>: bytes-in	[máximo]	56 bps	24 bps	5.35 Kbps	1.21 Mbps

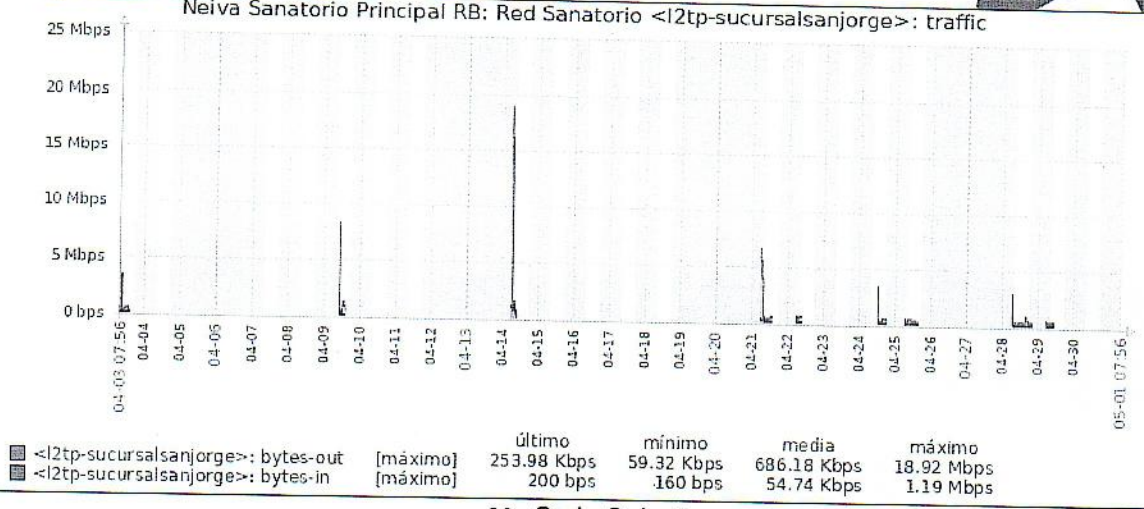
23. Sede Guacirco

24. Sede Peñas Blancas



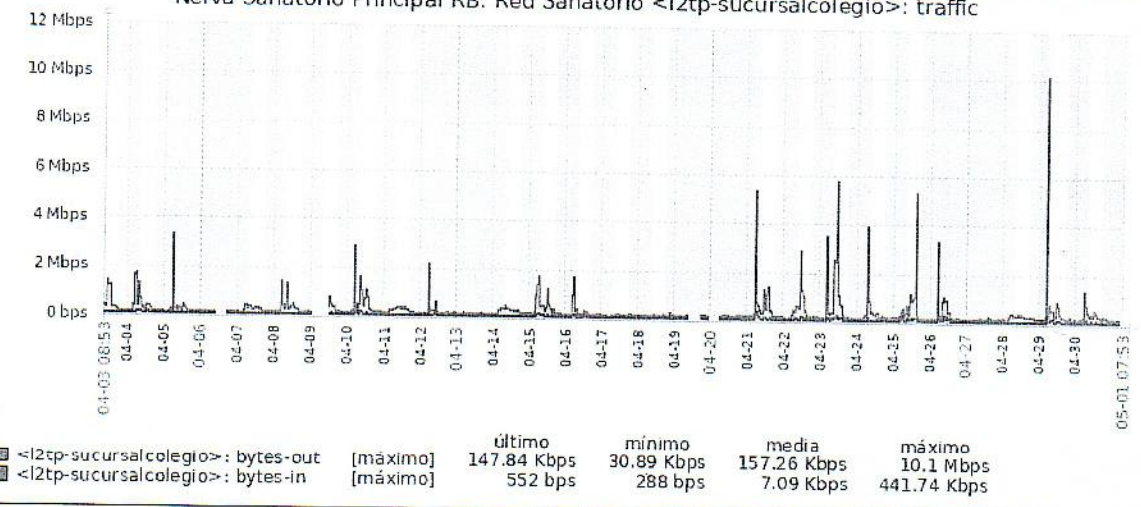
		último	mínimo	media	máximo
<l2tp-sucursalpeniasblancas>: bytes-out	[máximo]	113.73 Kbps	28.58 Kbps	146.62 Kbps	3.41 Mbps
<l2tp-sucursalpeniasblancas>: bytes-in	[máximo]	3.53 Kbps	1.42 Kbps	6.81 Kbps	505.71 Kbps

25. Sede San Jorge



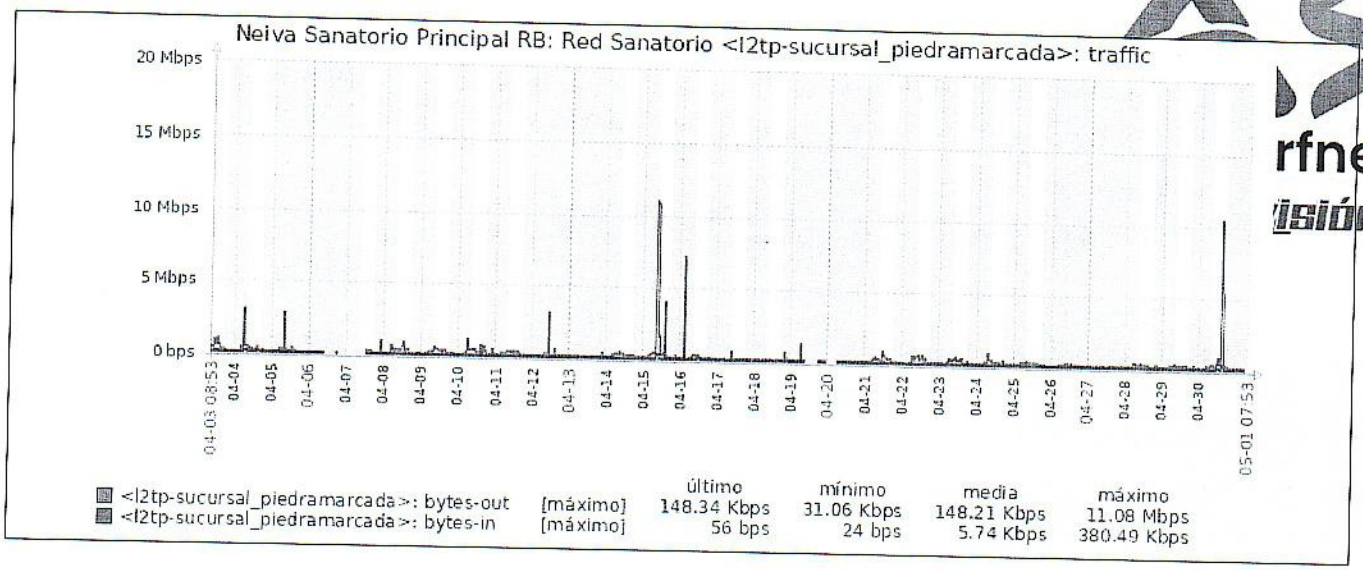
		último	mínimo	media	máximo
<l2tp-sucursalsanjorge>: bytes-out	[máximo]	253.98 Kbps	59.32 Kbps	686.18 Kbps	18.92 Mbps
<l2tp-sucursalsanjorge>: bytes-in	[máximo]	200 bps	160 bps	54.74 Kbps	1.19 Mbps

26. Sede Colegio



		último	mínimo	media	máximo
<l2tp-sucursalcolegio>: bytes-out	[máximo]	147.84 Kbps	30.89 Kbps	157.26 Kbps	10.1 Mbps
<l2tp-sucursalcolegio>: bytes-in	[máximo]	552 bps	288 bps	7.09 Kbps	441.74 Kbps

27. Sede Piedra Marcada

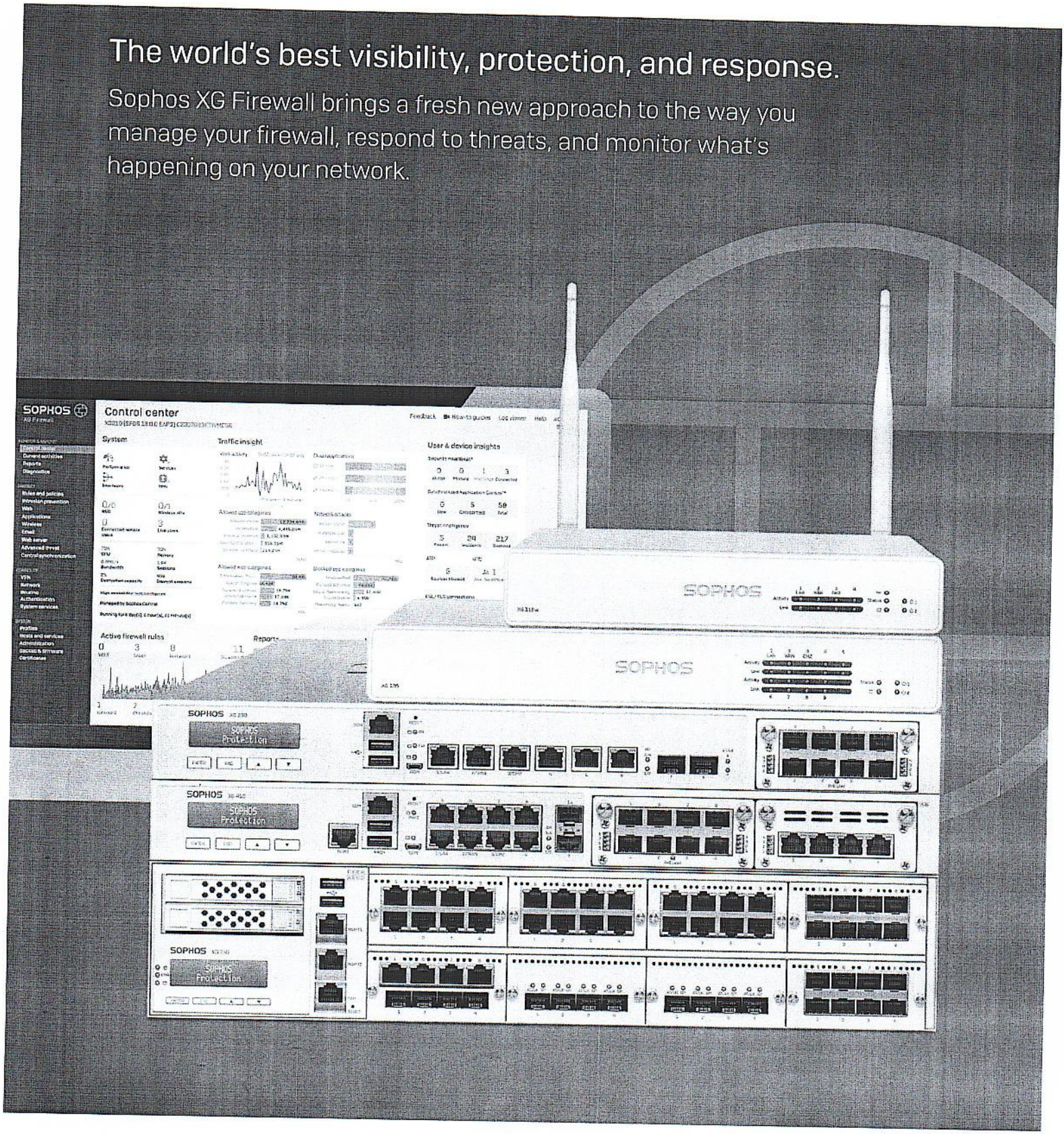

Neiva Sanatorio Principal RB: Red Sanatorio <l2tp-sucursal_piedramarcada>: traffic
20 Mbps
15 Mbps
10 Mbps
5 Mbps
0 bps
04-03 08:53
04-04
04-05
04-06
04-07
04-08
04-09
04-10
04-11
04-12
04-13
04-14
04-15
04-16
04-17
04-18
04-19
04-20
04-21
04-22
04-23
04-24
04-25
04-26
04-27
04-28
04-29
04-30
05-01 07:53
<l2tp-sucursal_piedramarcada>: bytes-out [máximo] último 148.34 Kbps mínimo 31.06 Kbps media 148.21 Kbps máximo 11.08 Mbps
<l2tp-sucursal_piedramarcada>: bytes-in [máximo] 56 bps 24 bps 5.74 Kbps 380.49 Kbps

SOPHOS

Sophos XG Firewall

The world's best visibility, protection, and response.

Sophos XG Firewall brings a fresh new approach to the way you manage your firewall, respond to threats, and monitor what's happening on your network.

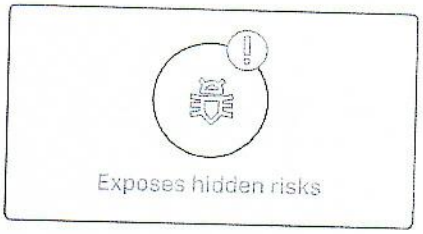

SOPHOS
Control center
System
Traffic insight
User & device insights
Active firewall rules
Reports
SOPHOS
SOPHOS
SOPHOS

Sophos XG Firewall

Sophos XG Firewall introduces an innovative approach to the way that you manage your firewall, and how you can detect and respond to threats on your network.

See it. Stop it. Secure it.

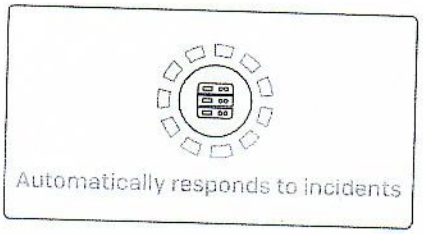
Our comprehensive next-generation firewall protection has been built to expose hidden risks, block both known and unknown threats, and automatically respond to incidents.



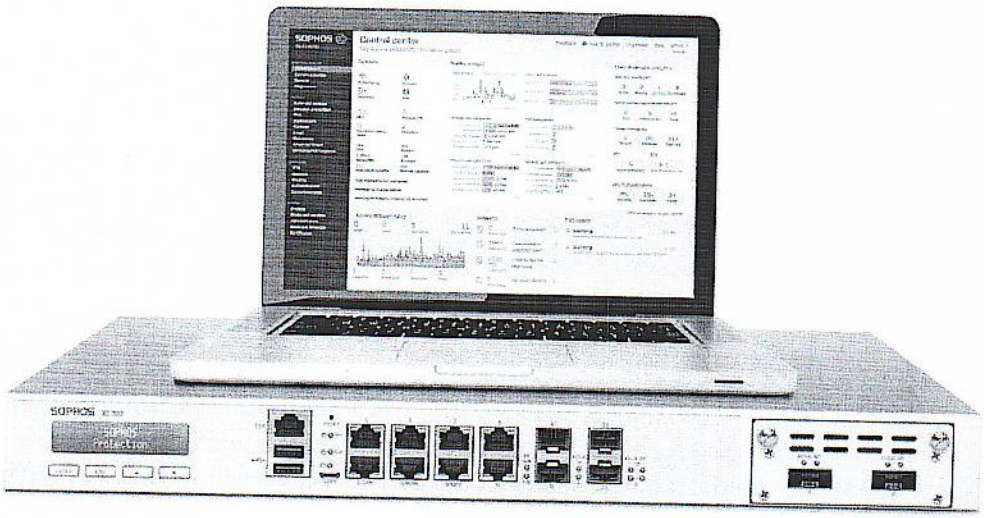
Sophos XG Firewall provides unrivaled visibility into risky users, unknown and unwanted apps, advanced threats, suspicious payloads, encrypted traffic and much more. Rich on-box reporting is built-in and powerful centralized reporting for multiple firewalls is available in the cloud.



Sophos XG Firewall provides all the latest advanced technology you need to protect your network from ransomware and advanced threats including top-rated IPS, Advanced Threat Protection, Cloud Sandboxing and full AI-powered threat analysis. Dual AV, Web and App Control, Email Protection and a full-featured Web Application Firewall. And it's easy to setup and manage.



XG Firewall is the only network security solution that is able to fully identify the source of an infection on your network and automatically limit access to other network resources in response. This is made possible with our unique Sophos Security Heartbeat that shares telemetry and health status between Sophos endpoints and your firewall.



The Xstream Advantage

The XG Firewall Xstream architecture is engineered to deliver extreme levels of visibility, protection, and performance to help address some of the greatest challenges facing network administrators today.

Xstream SSL Inspection

According to the latest statistics, approximately 80% of web traffic is encrypted, making it invisible to most firewalls. An increasing amount of malware and potentially unwanted apps exploit the fact that organizations are simply not using SSL inspection. Network administrators' main fears are that SSL inspection will have a performance impact or cause something to break, impacting the user experience.

XG Firewall removes the blind spots caused by encrypted traffic by allowing you to use SSL inspection whilst maintaining performance efficiency.

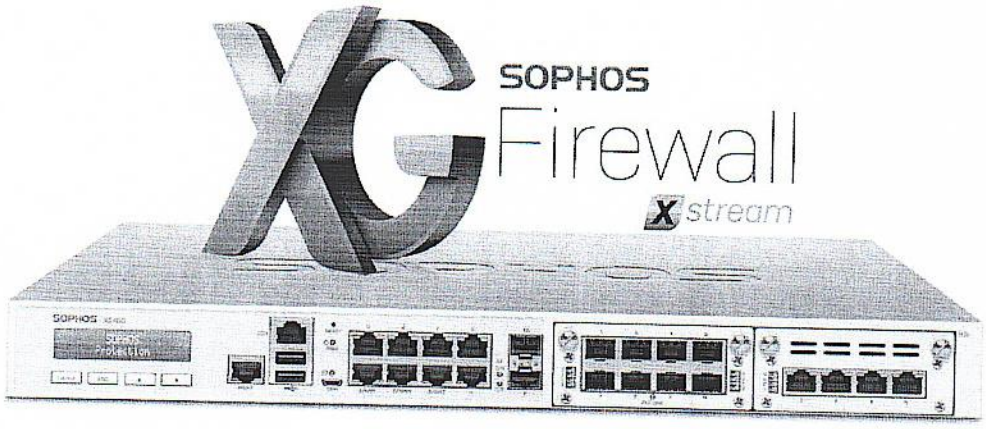
Xstream DPI Engine

We believe you should never have to decide between security and performance. XG Firewall includes a high-speed Deep Packet Inspection (DPI) engine to scan your traffic for threats without a proxy slowing down the process. The firewall stack can completely offload the processing to the DPI engine, significantly reducing latency and so improving overall efficiency.

XG Firewall provides robust deep packet threat protection in a single streaming engine for AV, IPS, Web, App Control and SSL inspection.

Xstream Network Flow FastPath

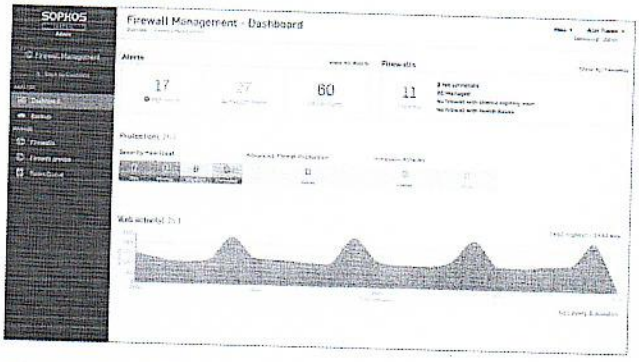
Traffic which is known to be secure can be offloaded to the Xstream Network Flow FastPath. This accelerated path for trusted traffic boosts performance dramatically by freeing up resources from unnecessary traffic inspection tasks. This is particularly important for voice and video applications which are very sensitive to latency and so can quickly lead to a degradation of the user experience. XG Firewall includes automatic and policy-based intelligent offloading for trusted traffic processing at wire speed.



Sophos Central

Sophos Central is at the heart of everything we do. Our cloud management platform provides a single pane of glass to not only manage your firewalls, but also your full portfolio of Sophos security solutions.

Central Management



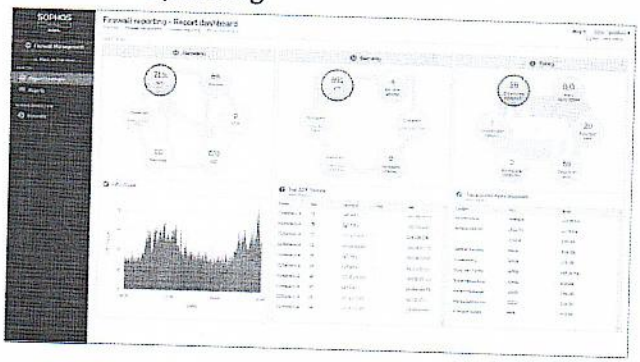
Simply manage multiple firewalls

Sophos Central is the ultimate cloud-management platform - for all your Sophos products. It makes day-to-day setup, monitoring, and management of your XG Firewall easy. It also provides helpful features such as alerting, backup management, one-click firmware updates and rapid provisioning of new firewalls.

- Manage all your XG Firewalls and other Sophos products from a single console
- Configure changes and apply them to a group of firewalls or manage each firewall individually
- Create a backup schedule and store up to 5 backups in the cloud

Note: Central Management is available at no extra cost.

Central Reporting



Firewall Reporting in the cloud

Sophos Central includes powerful reporting tools that enable you to visualize your network, web, application activity, and security over time. You get a flexible reporting experience that combines a variety of built-in reports with powerful tools to create your own custom reports – enabling you to report what you want, how you want.

- Increase your visibility into network activity through analytics
- Analyze data to identify security gaps, suspicious user behavior or other events requiring policy changes
- Use the pre-defined modules or customize each report for specific use cases

Note: Central Reporting is available at no extra cost for the storage of up to 7 days of report data. Premium options with longer data retention are available for optional purchase.

Zero-touch Deployment

Using Sophos Central, you can create a configuration for an XG firewall which you can then deploy at your convenience, for example, at a remote site. There is no need for technical staff on-site, simply provide the configuration file, store it on a USB key and boot the appliance with the USB key connected.

Learn more about the Sophos Central Ecosystem at sophos.com/firewall-central.

Synchronized Security

Security Heartbeat™ - Your firewall and your endpoints are finally talking

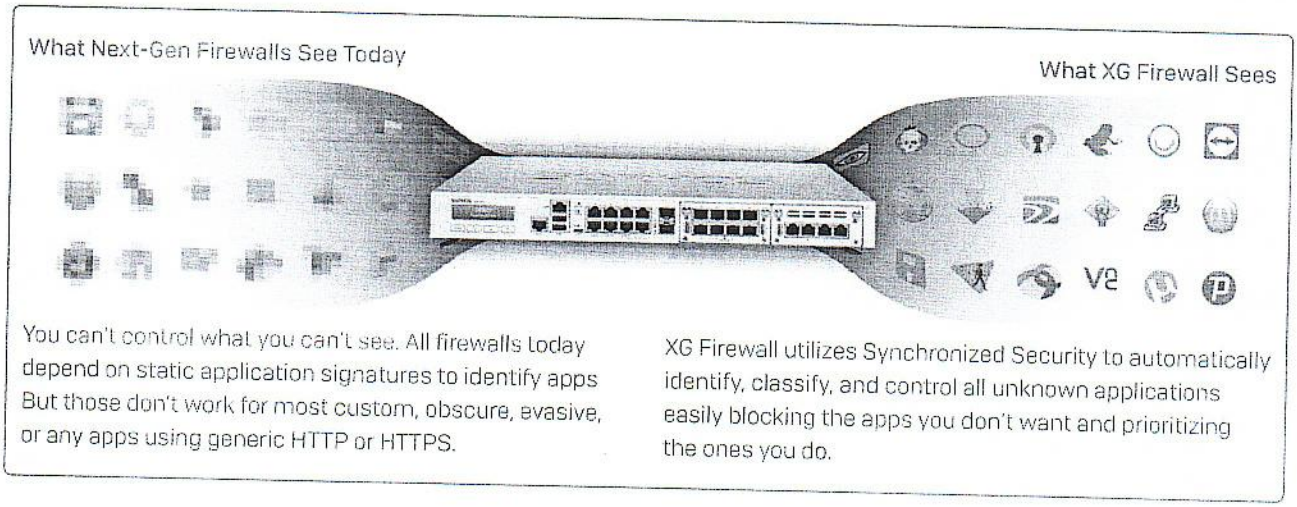
Sophos XG Firewall is the only network security solution that is able to fully identify the user and source of an infection on your network and automatically limit access to other network resources in response. This is made possible with our unique Sophos Security Heartbeat that shares telemetry and health status between Sophos endpoints and your firewall and integrates endpoint health into firewall rules to control access and isolate compromised systems.

The good news is, this all happens automatically, and is successfully helping numerous businesses and organizations to save time and money in protecting their environments today.

Synchronized Application Control

Using Security Heartbeat, we can do much more than just see the health status of an endpoint. We also have a solution to one of the biggest problems most network administrators face today - lack of visibility into network traffic.

Synchronized Application Control automatically identifies, classifies and controls encrypted, custom, evasive, and generic HTTP or HTTPS applications which are currently going unidentified.



You can't control what you can't see. All firewalls today depend on static application signatures to identify apps But those don't work for most custom, obscure, evasive, or any apps using generic HTTP or HTTPS.

XG Firewall utilizes Synchronized Security to automatically identify, classify, and control all unknown applications easily blocking the apps you don't want and prioritizing the ones you do.

Lateral Movement Protection

Lateral Movement Protection automatically isolates compromised systems at every point in the network to stop attacks dead in their tracks. Healthy endpoints assist by ignoring all traffic from unhealthy endpoints, enabling complete isolation, even on the same network segment, to prevent threats and active adversaries from spreading or stealing data.

Synchronized User ID

User authentication is critically important in a next-generation firewall but often challenging to implement in a seamless and transparent way. Synchronized User ID eliminates the need for client or server authentication agents by sharing user identity between the endpoint and the firewall through Security Heartbeat. It's just another great benefit of having your firewall and endpoints integrated and sharing information.

Synchronized SD-WAN - Powerful, reliable application routing

Synchronized SD-WAN harnesses the power of Synchronized Security to optimize WAN path selection for your important business applications.

With Synchronized Application Control, discovered applications, which would otherwise be unknown, can be used for traffic matching criteria in SD-WAN routing policies. This is yet another way that Synchronized Security can improve the efficiency of your network.

Protection Modules

You can choose from a number of modules to customize the protection offered by your firewall to your individual needs and deployment scenario.

Network Protection
All the protection you need to stop sophisticated attacks and advanced threats while providing secure network access to those you trust.

Next-gen Intrusion Prevention System
Provides advanced protection from all types of modern attacks. It goes beyond traditional server and network resources to protect users and apps on the network as well.

Security Heartbeat
Creates a link between your Sophos Central protected endpoints and your firewall to identify threats faster, simplify investigation and minimize impact from attacks. Easily incorporate Heartbeat status into firewall policies to automatically isolate compromised systems.

Advanced Threat Protection
Instant identification and immediate response to today's most sophisticated attacks. Multi-layered protection identifies threats instantly and Security Heartbeat provides an emergency response.

Advanced VPN technologies
Adds unique and simple VPN technologies including our clientless HTML5 self-service portal that makes remote access incredibly simple or utilize our exclusive light-weight secure SD-RED (Remote Ethernet Device) VPN technology.

Web Protection
Unmatched visibility and control over all your user's web and application activity.

Powerful user and group web policy
Provides enterprise-level Secure Web Gateway policy controls to easily manage sophisticated user and group web controls. Apply policies based upon uploaded web keywords indicating inappropriate use or behavior.

Application Control and QoS
Enables user-aware visibility and control over thousands of applications with granular policy and traffic-shaping (QoS) options based on application category, risk, and other characteristics. Synchronized Application Control automatically identifies all the unknown, evasive, and custom applications on your network.

Advanced Web Threat Protection
Backed by SophosLabs, our advanced engine provides the ultimate protection from today's polymorphic and obfuscated web threats. Innovative techniques like JavaScript emulation, behavioral analysis, and origin reputation help keep your network safe.

High-performance traffic scanning
Optimized for top performance, our Xstream SSL inspection provides ultra-low latency inspection and HTTPS scanning whilst maintaining performance.

See the Licensing section at the end of this document for details of all purchase options.

Email Protection
Consolidate your email protection with anti-spam, DLP, and encryption.

Integrated Message Transfer Agent
Ensures always-on business continuity for your email, allowing the firewall to automatically queue mail in the event servers become unavailable.

Live Anti-Spam
Provides protection from the latest spam campaigns, phishing attacks, and malicious attachments.

Self-serve Quarantine
Gives employees direct control over their spam quarantine, saving you time and effort.

SPX Email Encryption
Unique to Sophos, SPX makes it easy to send encrypted email to anyone, even those without any kind of trust infrastructure, using our patent-pending password-based encryption technology.

Data Loss Prevention
Policy-based DLP can automatically trigger encryption or block/notify based on the presence of sensitive data in emails leaving the organization.

Web Server Protection
Harden your web servers and business applications against hacking attempts while providing secure access.

Business Application Policy Templates
Pre-defined policy templates let you protect common applications like Microsoft Exchange Outlook Anywhere or SharePoint quickly and easily.

Protection from the latest hacks and attacks
With a variety of advanced protection technologies including URL and form hardening, deep-linking and directory traversal prevention, SQL injection and cross-site scripting protection, cookie signing and more.

Reverse proxy
With authentication options, SSL offloading, and server load balancing ensure maximum protection and performance for your servers being accessed from the internet.

Sandstorm Protection

AI-driven static and dynamic file analysis techniques combine to bring unprecedented threat intelligence to your firewall and so effectively identify and block ransomware, known and unknown threats.

How to buy Sandstorm Protection

Sandstorm Protection is available as an add-on subscription and is also included in our 'Plus' Bundles, e.g. EnterpriseGuard Plus, FullGuard Plus.

Powered by SophosLabs

Powered by the industry-leading SophosLabs, the Sandstorm Protection subscription includes a fully cloud-based threat intelligence and threat analysis platform. This provides deep learning-based file analysis, detailed analysis reporting and a threat meter to show the risk summary for a file.

We use layers of analytics to identify known and potential threats, reduce unknowns and derive verdicts and intelligence reports for the most commonly used file types.

Static File Analysis

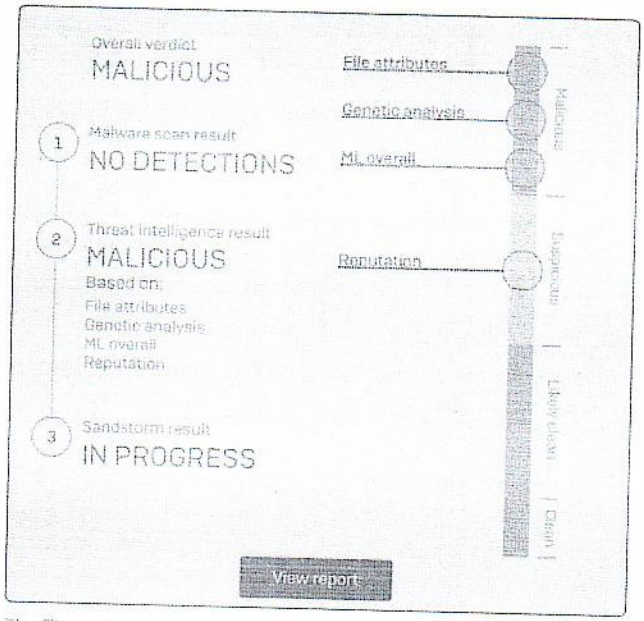
By harnessing the power of multiple machine learning models, global reputation, deep file scanning, and more, you can quickly identify threats without the need to execute the files in real time.

Dynamic File Analysis

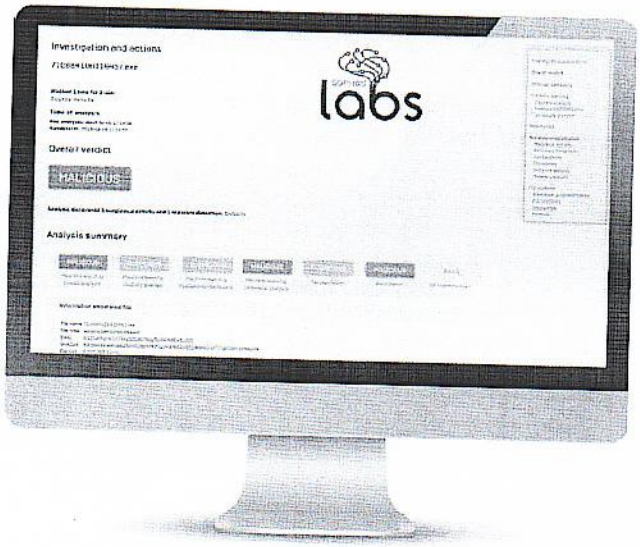
Execute a file in a secure cloud-based sandbox to observe its behavior and intent. Screenshots provide added insight into any key events during the analysis.

Threat Intelligence Analysis Reporting

Rich intelligence reports provide you with much more than just a 'good', 'bad', or 'unknown' verdict. Full insight into the nature and capabilities of a threat are delivered through the use of data science and SophosLabs research.



The Threat Meter provides an almost instant result, even when further analysis is still ongoing.



Sophos XG Series Appliances – at a glance

Our XG Series hardware appliances are purpose-built with the latest multi-core technology, generous RAM provisioning, and solid-state storage. Whether you're protecting a small business or a larger distributed enterprise, you're getting industry leading performance.

Product Matrix

Model			Tech. Specs			Throughput[1]				
	Revision #	Form Factor	Ports/Slots (Max Ports)	w-model*	Swappable Components	Firewall (Mbps)	IPsec VPN (Mbps)	NGFW (Mbps)	Threat Protection (Mbps)	Xstream SSL (Mbps)
XG 86(w)	1	desktop	4	Wi-Fi 5	n/a	3,100	225	350	145	75
XG 106(w)	1	desktop	4	Wi-Fi 5	opt. ext. Power	3,550	330	400	150	75
XG 115(w)	3	desktop	4	Wi-Fi 5	opt. ext. Power	4,000	560	1,000	375	130
XG 125(w)	3	desktop	9/1 (9)	Wi-Fi 5	opt. ext. Power, 3G/4G	7,000	1,500	1,275	400	170
XG 135(w)	3	desktop	9/1 (9)	Wi-Fi 5	opt. ext. Power, 3G/4G, Wi-Fi**	7,500	1,700	1,800	600	210
XG 210	3	1U	8/1 (16)	n/a	opt. ext. Power	29,000	1,920	3,200	800	230
XG 230	2	1U	8/1 (16)	n/a	opt. ext. Power	32,000	2,100	4,500	1,000	280
XG 310	2	1U	12/1 (20)	n/a	opt. ext. Power	35,000	3,050	5,300	1,550	370
XG 330	2	1U	12/1 (20)	n/a	opt. ext. Power	38,000	3,940	9,300	2,100	560
XG 430	2	1U	10/2 (26)	n/a	opt. ext. Power	55,000	5,000	10,000	2,200	600
XG 450	2	1U	10/2 (26)	n/a	opt. int. Power	65,000	6,100	13,900	3,400	770
XG 550	2	2U	8/4 (32)	n/a	Power, SSD, Fan	75,000	8,500	15,300	6,000	1,000
XG 650	2	2U	8/6 (48)	n/a	Power, SSD, Fan	85,000	9,000	18,000	7,700	1,350
XG 750	2	2U	8/8 (64)	n/a	Power, SSD, Fan	100,000	12,500	19,200	9,400	1,400

* 802.11ac Wave 2

** 2nd Wi-Fi module option on 135w only (requires XG v17 MR6 or higher)

What you get with every XG Series appliance

- Full Wireless Protection included in the Base License
- On-box reporting or reporting for 7 days via Sophos Central
- Free management via Sophos Central
- The flexibility to add optional connectivity modules to adapt your firewall to changes in your environment

Note: The latest XG Firewall (SFOS) version 18.x requires at least 4 GB of RAM.

Sophos XG Series Desktop: SMB and Branch Office

Our Desktop appliances offer the perfect balance between price and performance for your small business or branch offices. All models offer a range of built-in and add-on connectivity options. A 'w' at the end of the model name indicates that the appliance has built-in Wi-Fi.

XG 86 and XG 86w

These entry-level desktop firewalls are the ideal choice for budget-conscious small businesses, retail and small or home offices.

- Optionally available with integrated 802.11ac WLAN
- Fanless

Note: The XG 86 and 86w do not support some advanced features like on-box reporting, dual AV scanning, WAF AV scanning and the email message transfer agent (MTA) functionality. If you need these capabilities, the XG 106(w) is recommended.

See detailed technical specifications

XG 106, XG 106w, XG 115, XG 115w

These desktop firewall appliances offer an excellent price-to-performance ratio making them ideal for small businesses or branch offices. These models come equipped with 4 GbE copper ports built-in and 1 shared SFP interface, e.g. for use with our optional DSL modem or an SFP Fiber transceiver to connect the device to a server or switch. An optional second power supply provides an unmatched redundancy option in this product segment.

- Optionally available with integrated 802.11ac WLAN
- 4 GbE copper ports built-in and 1 shared SFP
- Optional second power supply

See detailed technical specifications

XG 125, XG 125w, XG 135, XG 135w

These powerful firewall appliances offer 1U performance with a desktop form factor and price. If you have a small business or branch offices to protect and are working on a tight budget, these models are the ideal choice. These models come equipped with 8 GbE copper ports built-in, plus 1 SFP port, e.g. for use with our optional DSL modem or an SFP Fiber transceiver to connect the device to a server or switch. An expansion bay provides the option to add additional connectivity such as our 3G/4G module. A 2nd Wi-Fi radio module is also available for the XG 135w. An optional second power supply ensures business continuity for these models.

- Optionally available with integrated 802.11ac WLAN
- 8 GbE copper ports built-in, plus 1 SFP port
- Expansion bay for optional 3G/4G module
- 2nd Wi-Fi radio module option for XG 135w
- Optional second power supply

See detailed technical specifications

