	INFORME DE SUPERVISIÓN CONTRATACIÓN	
Código: GJC-FRT-08	**Versión:** 01	**Fecha de Aprobación:** 14/01/2016

DATOS GENERALES

PERÍODO A QUE CORRESPONDE EL INFORME	22	7	2024	**a**	9	8	2024
¿Se reporta algún desempeño deficiente o a mejorar?	**SI**			**NO**	X		
PORCENTAJE DE EJECUCIÓN	**FÍSICA**			**PRESUPUESTAL**			
	80 %			**80%**			

Datos del supervisor

NOMBRE DEL SUPERVISOR	Lucero Chamorro Serna
DEPENDENCIA	Vicerrectoría Administrativa y Financiera
CARGO	Profesional Universitario Oficina de Tecnología

Datos del contrato supervisado

FECHA DE CONTRATO	CO1.PCCNTR.6473425
CONTRATISTA	PYMES ON LINE
CEDULA DE CIUDADANÍA O NIT	900440998
VALOR	34.500.480 COP
PLAZO	10 MESES
FECHA ACTA DE INICIO	8/07/2024 12:00:00 PM
FECHA TERMINACIÓN PROYECTADA DEL CONTRATO	1/05/2025 11:59:00 AM
FECHA DE ELABORACION DEL INFORME	9 agosto 2024
Renovación de los servicios de e-Security, que incluyen la actualización y mantenimiento del equipo de seguridad perimetral, la renovación del licenciamiento del firewall, y la realización de un diagnóstico exhaustivo de la red y su infraestructura. Estas acciones están destinadas a asegurar la continuidad operativa, mejorar la protección contra amenazas cibernéticas, y optimizar el rendimiento y la seguridad de nuestra infraestructura de TI	

SEGUIMIENTO CONTRACTUAL

1. **CUMPLIMIENTO DEL OBJETO:**

   Cumple con las tareas que le fueron asignadas según el objeto del contrato: Renovación de los servicios de e-Security, que incluyen la actualización y mantenimiento el equipo de seguridad perimetral, la renovación del licenciamiento del firewall, y la realización de un diagnóstico exhaustivo de la red y su infraestructura. Estas acciones están destinadas a asegurar la continuidad operativa, mejorar la protección contra amenazas cibernéticas, y optimizar el rendimiento y la seguridad de nuestra infraestructura de TI.

2. **GRADO DE CUMPLIMIENTO DE LAS OBLIGACIONES:** Cumplió el 80% de sus labores.

3. **ACTIVIDADES DESARROLLADAS POR EL CONTRATISTA SOBRE BIENES, OBRAS Y SERVICIOS O PRODUCTOS COMPRENDIDAS EN EL PERIODO DEL 1 AL 31 DE JULIO 2024.**

   Las actividades desarrolladas por el contratista en el mes fueron:

   1. Auditoría de la red: Revisión exhaustiva de la infraestructura de red, incluyendo

dispositivos de red (routers, switches, firewalls, AccessPoint), conexiones físicas, puntos de datos, configuraciones de red, etc.

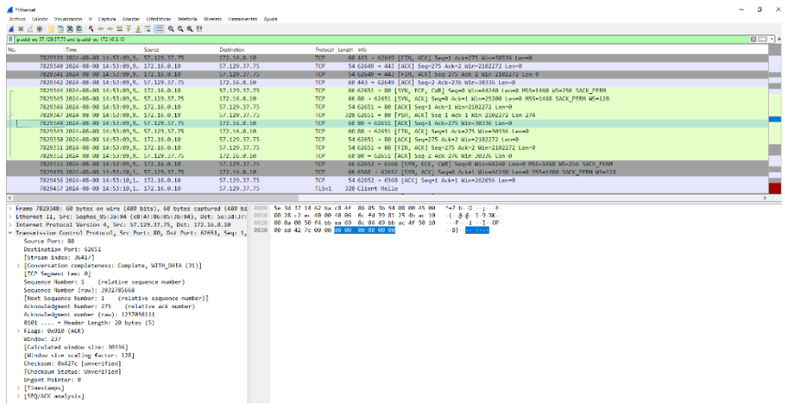
En la revisión realizada se valido punto de datos, identificando la conexión que tiene, y su estado donde entregan un total de 16 puntos averiados de un total de 664, etiquetaron puntos que no estaban marcados, se identifica la segmentación de los datos



El punto 2 y 3 están relacionados

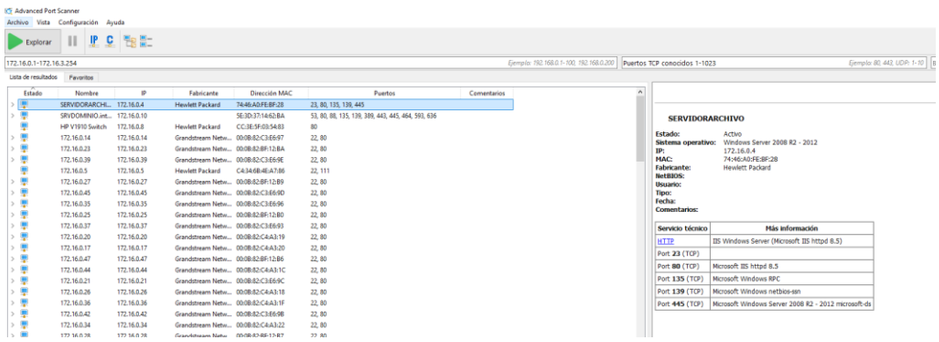
2. Análisis de tráfico: Monitoreo y análisis del tráfico de red para identificar cuellos de botella, congestión, patrones de uso anormal, etc.
3. Pruebas de velocidad y rendimiento: Evaluación del rendimiento de la red mediante pruebas de velocidad y análisis de latencia para determinar la capacidad y eficiencia de la red.

Realizan monitoreo de la red, para validar consumos de datos y las pruebas de latencia dan como promedio de 4 ms esta prueba es realizada en cada swiche de cada centro de cableado que hay en la entidad para un total de 16 y 6 los servidores, igualmente realizan las pruebas en cada Gateway de los 3 proveedores que tenemos que son MEDIA COMMERCE, EMCALI, Y CLARO.



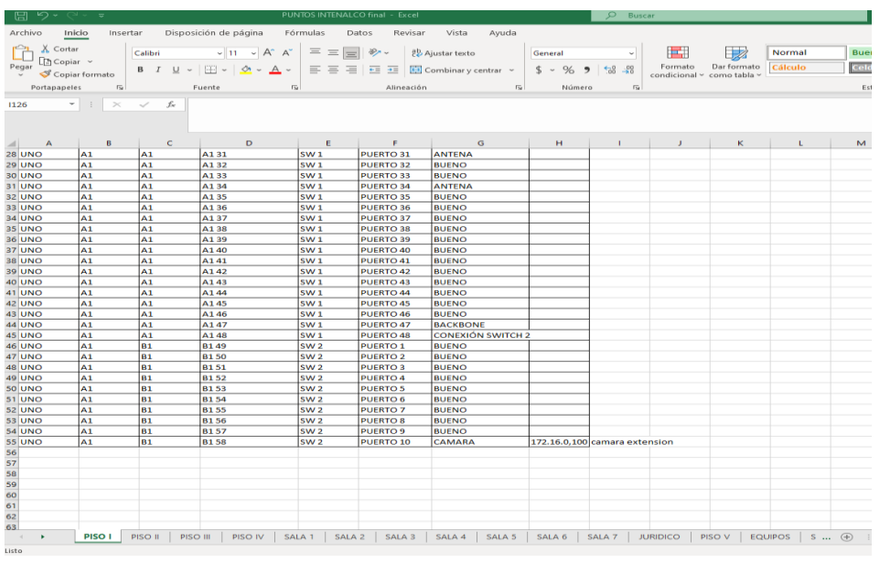
4. Escaneo de seguridad: Identificación de posibles vulnerabilidades de seguridad en la red, como puertos abiertos, configuraciones inseguras, acceso no autorizado, etc.

   Para el escañero de los puertos se realizo con ayuda del programa IP PORT SCCANER, donde se identifica los puertos disponibles en cada segmentación de red y de donde sale el servicio.



5. Análisis de topología de red: Mapeo y documentación de la topología de la red para comprender la estructura y la interconexión de los dispositivos de red.

   En el mapeo de la red realizado se encontraron que esta dentro de los estándares TIA-568A y TIA-568B, la estructura esta con cableado de categoría 6, la parte nueva del área de extensión esta con categoría 6ª, anexan documento en Excel discriminado por piso.



6. Revisión de políticas de seguridad: Evaluación de las políticas de seguridad de la red, incluyendo configuraciones de firewall, políticas de acceso, autenticación, etc.

   En la revisión de políticas se encontró que solo se tiene por defecto, lo cual es falencias que se deben entrar analizar para aplicar y así darle mejor seguridad a la red.



7. Análisis de protocolos: Revisión de los protocolos de red utilizados en la infraestructura para identificar posibles problemas de compatibilidad, seguridad o rendimiento.

   Según el análisis realizado indican que no encontraron cuellos de botella y problemas de direccionamiento. Cabe anotar que en ocasiones hay conexiones que a pesar de que hay direccionamiento ip estático los equipos no se conectan y deniegan la navegación.

8. Recomendaciones de mejora: Basado en los hallazgos del diagnóstico, proporcionar recomendaciones concretas para mejorar la seguridad, el rendimiento y la eficiencia de la red.

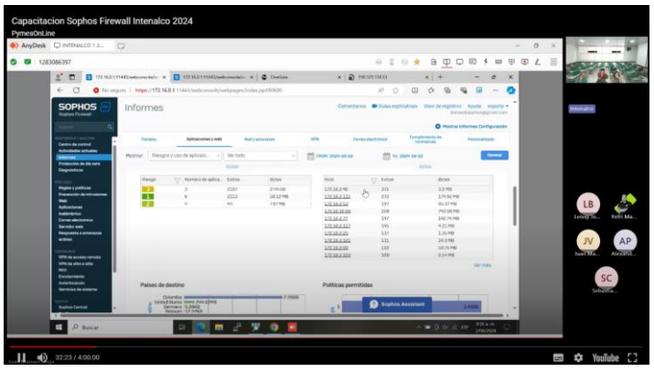
   De las 20 recomendaciones realizadas se ajustarán las que estan dentro de las posibilidades ya que las demás requieren presupuesto para su realización, estas se presentaran al vicerrector administrativo para su conocimiento y asignación de presupuesto.

   Se pueden realizar las siguientes:
   1. reparar 16 puntos de datos que presentan fallas porque han dañado los Jack categoría 6 en los puestos de trabajo estos deben remplazarse y Re poncharse, con sus respectivas pruebas de conectividad.
   2. En el centro principal de cableado debe de reorganizarse puesto que en la actualidad para realizar conexiones se han utilizado de 3 metros.
   3. El personal de sistemas debe contar con equipo de mapeo de puntos y la herramienta requerida para brinda soporte en caso de falla.
   4. Bloqueo del acceso de la red internet de Intenalco por software como Anydesk, TeamViewer, entre otros
   5. Realizar monitoreo constante del uso de aplicaciones estableciendo políticas y condiciones para su uso en (redes sociales, plataformas, etc.)
   6. Verificar el ancho de banda entregado por el proveedor, certificando que este sea mínimo 930mgb
   7. Crear un rango de IPS para los nuevos equipos, y manteniendo actualizado el cuadro de equipos conectados.
   8. Establecer rango de direccionamiento de IP de acuerdo a la cantidad de equipos que se desean conectar de acuerdo al recurso de red y no extralimitar el uso ya que causan cuellos de botella.
   9. Configurar conexiones seguras a través de VPN por externos a la red INTENALCO.
   10. Actualizar el software de sistema operativo de los servidores existentes.
   11. Actualizar firewall de los equipos activos existentes.
   12. En la red administrativa todos los equipos deben estar debidamente identificados, sobre todo los que acceden por wifi.
   13. Es importante recalcar que el dispositivo se debe monitorear constantemente y actualizar a nuevas políticas personalizadas si es necesario debido a que día hay nuevas vulnerabilidades.

9. Capacitación del personal:
   ✓ Ofrecer capacitación y orientación al personal de la organización sobre las mejores prácticas de seguridad y gestión de la red.

   Realización de capacitación virtual





✓ Certificación para el personal de tecnología de la información TI del firewall SOPHOS

Queda pendiente la entrega de voucher y agenda para la certificación para el personal de TI.

10.Informe detallado: Preparación de un informe detallado que resuma los hallazgos del diagnóstico, las recomendaciones de mejora y cualquier acción correctiva recomendada.

Las recomendaciones se encuentran en el punto 8.

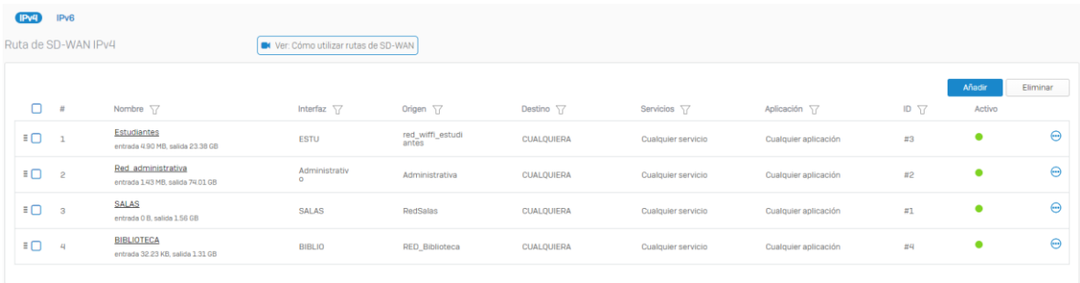
11.Análisis de disponibilidad y redundancia: Evaluación de la disponibilidad de la red y la implementación de medidas de redundancia para garantizar la continuidad del servicio en caso de fallos.

Nombre	Dirección IP	Interfaz	Tipo	Activar en caso de error de	Carga	Estado	Gestionar
CLARO	190.144.141.9	CLARO - 190.144.141.10/255.255.255.252	Copia de seguridad	All Active Gateway	NA		
EMCALI	200.29.117.153	EMCALI - 200.29.117.154/255.255.255.248	Activo	No	19		
MEDIA COMMERCE	190.121.134.50	MEDIA COMMERCE - 190.121.134.55/255.255.255.240	Activo	No	20		

Hay disponibilidad de tres canales donde el de Media Commerce se distribuye para la parte administrativa, Emcali para el Wifi Estudiantes y CLARO se deja de soporte en caso que fallen la principal media commerce.

La capacidad es:
MediaCommerce: 930 Mbpss
Emcali : 930 Mbps
Claro : 300 Mbps

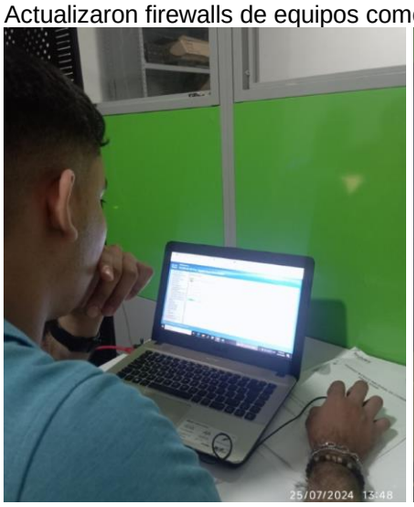
La configuración de estos tres canales queda balanceada y distribuida en el Sophos para siguientes interfaces

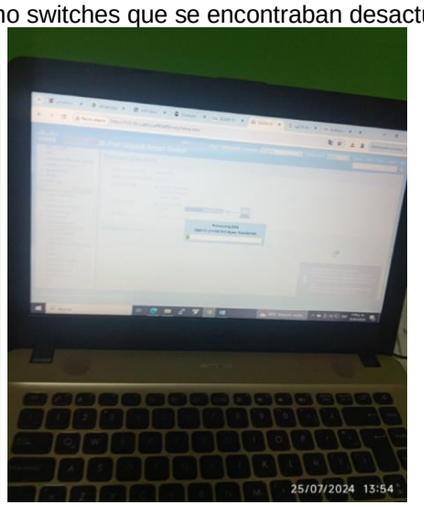


Donde queda un disponibilidad de 930Mbps / 3 Mbps =310 usuarios

12.Optimización de la configuración de red: Revisión de la configuración de los dispositivos de red para identificar oportunidades de optimización que mejoren el rendimiento y la eficiencia.

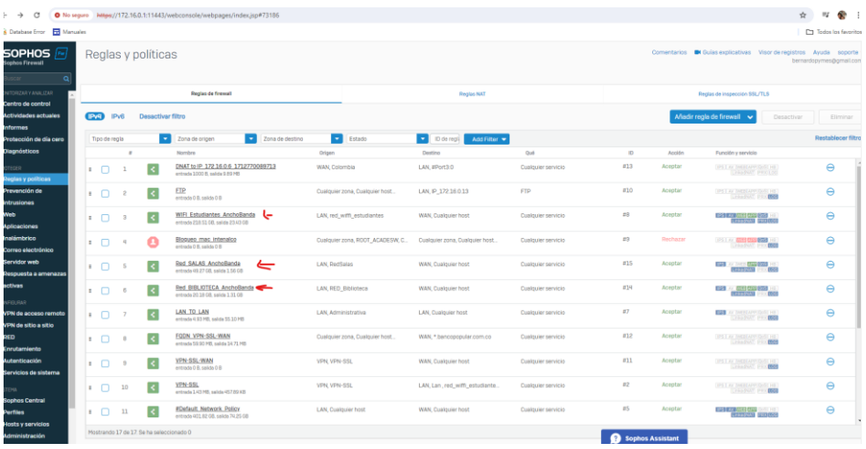
Actualizaron firewalls de equipos como switches que se encontraban desactualizados

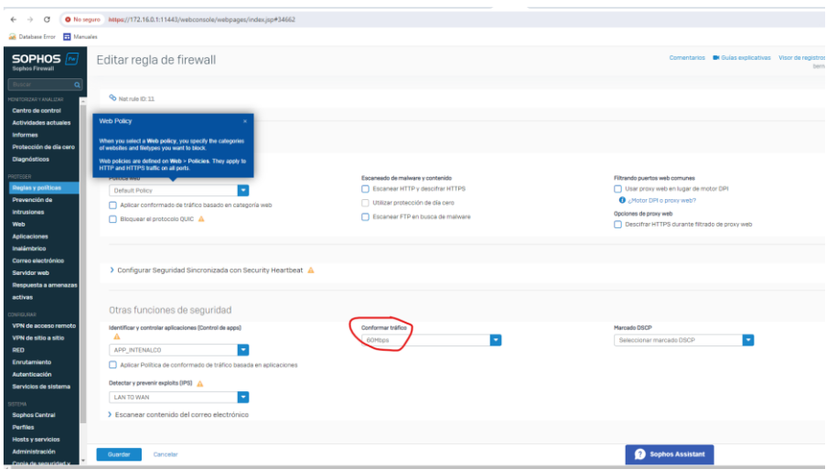




13.Análisis de calidad de servicio (QoS): Evaluación de la configuración de QoS para garantizar la priorización adecuada del tráfico de red y la entrega de servicios críticos de manera eficiente.

No se encontraba activo el cual se realiza configuración de los banda de ancha para las redes de



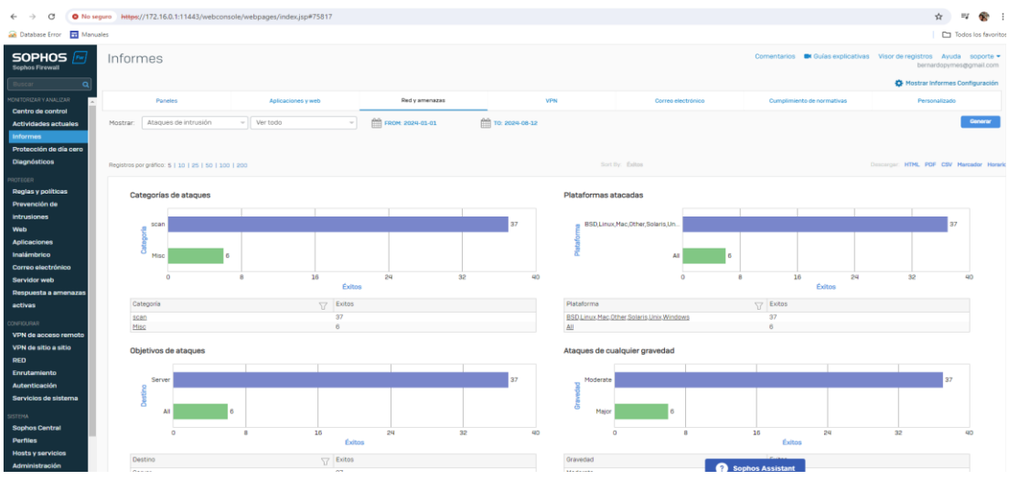


14.Auditoría de cumplimiento normativo: Verificación de que la infraestructura de red cumpla con los estándares y regulaciones relevantes en materia de seguridad y privacidad de datos.

Identifica que la topología de la red cumple con los estándares internacionales TIA-568ª Y TIA-568B con cableado de categoría 6 y la sede nueva queda con categoría 6A

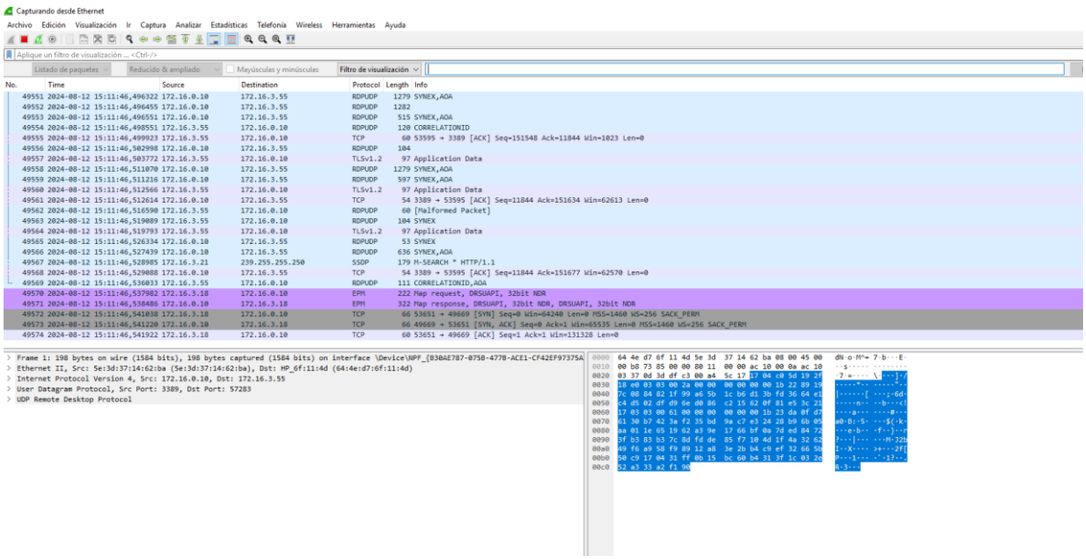
15.Pruebas de seguridad avanzadas: Realización de pruebas de penetración y análisis de seguridad más profundos para identificar vulnerabilidades complejas y potencialmente peligrosas.

En esta revisión se que se evidencia que desde enero a la fecha se han recibido 37 Ataques, según el análisis entregado es un porcentaje bajo, igualmente a través del Sophos y la herramienta webserverprotection cancela el posible ataque evitando la penetración a la red



16.Monitoreo continuo de la red: Implementación de herramientas de monitoreo y alerta para detectar y responder rápidamente a problemas de red en tiempo real.

El monitoreo se puede realizar desde el Sophos, igualmente realizan instalación de los tres softwares libres que fueron IP PORT SCANNER y el WIRESHARK



17.Evaluación de la arquitectura de red: Revisión de la arquitectura de red actual y recomendaciones para su mejora, como la implementación de redes definidas por software (SDN) o arquitecturas de microsegmentación.

En la evaluación hacen las siguiente observaciones:

- Implementación IPv4 a Ipv6
- Se requiere cambio del fireware en 2025 pro obsolescencia ya el equipo queda sin soporte ni licenciamiento.
- Se establecieron nuevas politicas

18.Análisis de uso de ancho de banda: Evaluación del uso del ancho de banda para identificar aplicaciones o servicios que consumen una cantidad desproporcionada de recursos de red.

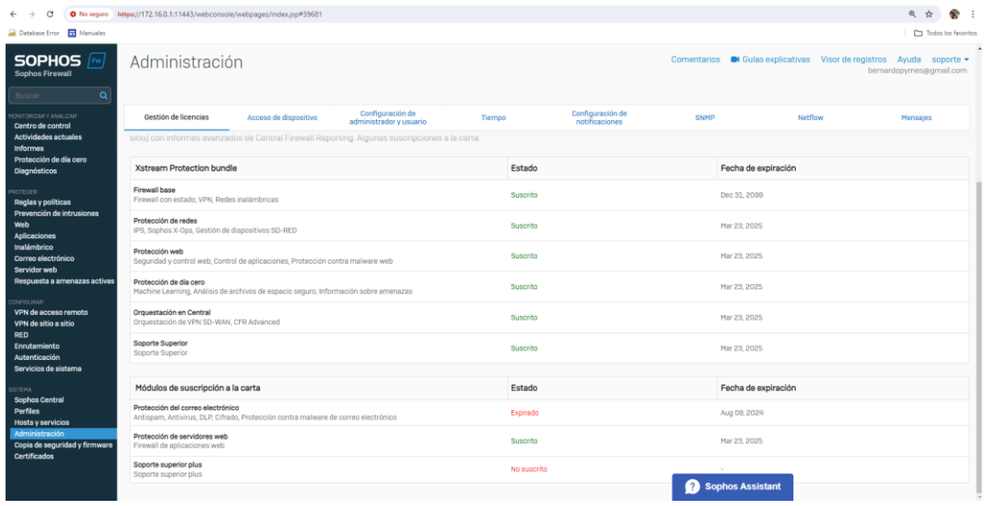
En la evaluación realizada se encontraron altos consumos en las siguientes plataformas

Aplicaciones	Descripción	Consumo
Actualizaciones de Windows	análisis de 30 junio a 31 de julio	96gb
Facebook	análisis de 30 junio a 31 de julio	57.8gb
YouTube	análisis de 30 junio a 31 de julio	49.1gb
Instagram	análisis de 30 junio a 31 de julio	32.2gb
WhatsApp	análisis de 30 junio a 31 de julio	31gb
Netflix	análisis de 30 junio a 31 de julio	15.7gb

19.Auditoría de políticas de seguridad: Revisión de las políticas de seguridad de la red para asegurar su alineación con las mejores prácticas y los requisitos de seguridad de la organización.

Punto completado en el punto 6

20.Configuración del licenciamiento para firewall.



21.Implementación configuración recomendada según el hallazgo en el diagnostico.

En el desarrollo de los puntos, se fueron ajustando las recomendaciones realizadas

22.Entrega por escrito la topología de red actual y la que se va implementar

Entregan archivos anexos donde se evidencia la topología de la red.con los nombres

- Topología Red Intenalco
- Red de Intenalco

.

23.Entrega del licenciamiento para el firewall

Entregan licencia bajo acta del proveedor

PymesOn Line
SU ALIADO ESTRATÉGICO EN TECNOLOGÍA E INNOVACIÓN

Santiago de Cali, 24 julio 2024

Señores
INTENALCO EDUCACION SUPERIOR
Atn Ingeniera Lucero Chamorro
Área TI

Ref. Entrega de Licenciamiento Sophos

Reciba un cordial saludo.

De acuerdo a lo establecido en la ficha tecnica que hace parte del CONTRATO DE SUMINISTROS No 200.17.001-INT-SEL-ABR-2024 CELEBRADO ENTRE LA INSTITUTO TECNICO NACIONAL DE COMERCIO SIMON RODRIGUEZ Y PYMES ON LINE SAS. item No 23. Referente a la Entrega del licenciamiento para el firewall

DESCRIPCION ELEMENTO	Especificación	Cantidad
XG310 XSTREAM PROTECTION RENEWAL	XS310Z10ZZRCAA	1
XG310 WEBSERVER PROTECTION RENEWAL	SS310Z10ZZRCAA	1

Se realiza la entrega del respectivo licenciamiento y posterior activación en la consola de sophos como se observa a continuación.



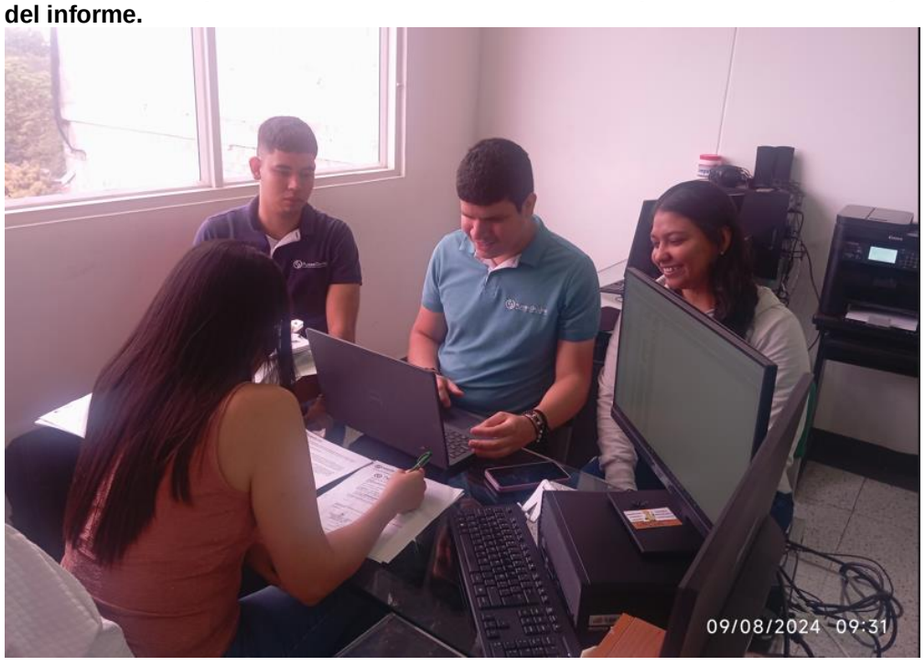
Se anexa el Documento Licencia emitido por Sophos con la información de las licencias suministradas

ENTREGA	RECIBE
Bernardo Saavedra Gutierrez Representante Legal Pymes On Line SAS Nit 900.440.998-7	Lucero Chamorro Supervicion- Ingeniera TI INTENALCO Nit. 800248004

4. **RECOMENDACIONES O SUGERENCIAS ACERCA DEL DESEMPEÑO DEL CONTRATISTA:**
   - Pendiente entrega de los váuchers, y fechas donde queda programada la realización de las certificaciones en Sophos.
   - Entregar claves pendientes y ip de cámaras que han instalado.

5. **PROPUESTAS DEL CONTRATISTA ANTE UN EVENTUAL DESEMPEÑO DEFICIENTE O A MEJORAR DE LAS OBLIGACIONES:**

EL Proveedor se presento en las instalaciones el día 9 para revisar contrato y entrega del informe.



6. **RELACIÒN DE PAGOS A LA SEGURIDAD SOCIAL Y APORTES PARAFISCALES:** Mes Vencido.
Planilla validada por el secop**,** donde entregan

PymesOn Line
SU ALIADO ESTRATÉGICO EN TECNOLOGÍA E INNOVACIÓN

ANEXO N° 9
CERTIFICACION DE PAZ Y SALVO POR CONCEPTO DEL PAGO DE OBLIGACIONES AL SISTEMA DE SEGURIDAD SOCIAL APORTES PARAFISCALES y CREE

Señores
INTENALCO - Instituto Técnico Nacional de Comercio Simón Rodríguez
Cali, Colombia

Asunto: Certificación de paz y salvo por concepto del pago de obligaciones al Sistema de Seguridad Social y aportes Parafiscales y actualización con pagos CREE
El suscrito representante legal (Bernardo Saavedra Gutierrez), certifica que la sociedad _PYMES ON LINE SAS, identificada con NIT. 900.440.998-7 , se encuentra a paz y salvo por concepto del pago de sus obligaciones con los sistemas de salud, riesgos profesionales, pensiones y aportes a las Cajas de Compensación Familiar, Instituto Colombiano de Bienestar Familiar y Servicio Nacional de Aprendizaje de todo el personal que se encuentra laborando dentro de la misma y que así lo requiere, durante los últimos seis (6) meses.
Lo anterior para cumplir lo establecido en el art. 50 de la ley 789 de 2002 y la ley 1150 de 2007.
En caso de presentar acuerdo de pago con alguna de las entidades anteriormente mencionadas, deberá precisarse el valor y el plazo previsto para el acuerdo de pago, con indicación del cumplimiento de esta obligación.
La presente se expide a los nueve (9) días del mes de agosto del año 2024, en Santiago de Cali

Cordialmente,

Firma Representante Legal
C.C. No. 6.316.686

ITEM	PERIODO DE PAGO *AÑO – MES*	FECHA DE PAGO *ANO – MES – DÍA*	VALOR
PENSIÓN			
SALUD			
RIESGOS PROFESIONALES			
PARAFISCALES			

¿EXISTE PLAN DE MEJORAMIENTO: SI [ ] **NO** [x]

(En caso afirmativo indique el nivel de cumplimiento):

7. ¿ENTREGÓ INFORME DE EJECUCIÓN?

Se descarga del Secop

SI [X]	**NO** [ ]
RELACIONAR SOPORTES DEL INFORME: • **Informe Auditoria Red de datos Intenalco Final.pdf** • **Certificacion Seguridad Social.pdf** • **PUNTOS INTENALCO final.pdf** • **RED DE INTENALCO.pdf** • **TOPOLOGIA DE RED INTENALCO.pdf**	

FIRMA DEL SUPERVISOR