Santiago de Cali, 12 de septiembre del 2025

Señores
Instituto Técnico Nacional de Comercio "Simón Rodríguez"
INTENALCO EDUCACION SUPERIOR
Atn. Dr. Neyl Grisales Arana - Rector
Atn. Ing. Lucero Chamorro Serna – Supervisor
Ciudad

ASUNTO: INFORME DE ENTREGA CONTRATO DE SUMINISTROS No 200.17.001-INT-SEL- ABR – 2025 CELEBRADO ENTRE LA INSTITUTO TECNICO NACIONAL DE COMERCIO SIMON RODRIGUEZ Y PYMES ON LINE SAS.

Cordial saludo.

En cumplimiento de lo establecido en el Contrato de Suministros No. 200.17.001-INT-SEL-ABR-2025, celebrado entre el Instituto Técnico Nacional de Comercio Simón Rodríguez y la empresa PYMES ON LINE S.A.S., se presenta el siguiente Informe de Entrega, en el cual se detallan las actividades desarrolladas y los bienes suministrados de acuerdo con las condiciones técnicas, administrativas y contractuales pactadas en el proceso de licitación.

El presente documento tiene como finalidad dejar constancia del cumplimiento de las obligaciones adquiridas por parte de PYMES ON LINE SAS, describiendo de manera ordenada las fases del proceso de suministro, la relación de elementos entregados, las verificaciones realizadas y el estado final de la entrega, con el fin de garantizar la conformidad de ambas partes y la adecuada culminación del proceso contractual.

EQUIPOS Y LICENCIAMIENTO

Dentro del marco del Contrato de Suministros No. 200.17.001-INT-SEL-ABR-2025, se llevó a cabo la entrega de un equipo firewall XGS3300 junto con las licencias correspondientes para su operación y administración y licenciamiento endpoints.

El suministro de este equipo y sus licenciamientos tiene como propósito fortalecer la seguridad perimetral y la protección de la infraestructura tecnológica de la institución, garantizando un control efectivo del tráfico de red, la prevención de accesos no autorizados y la continuidad de los servicios académicos y administrativos que dependen de los recursos informáticos.

A continuación, se detallan los seriales del equipo Firewall de la marca Sophos, el cual fue entregado a la supervisión del contrato, la ingeniera Lucero Chamorro del área de TI.

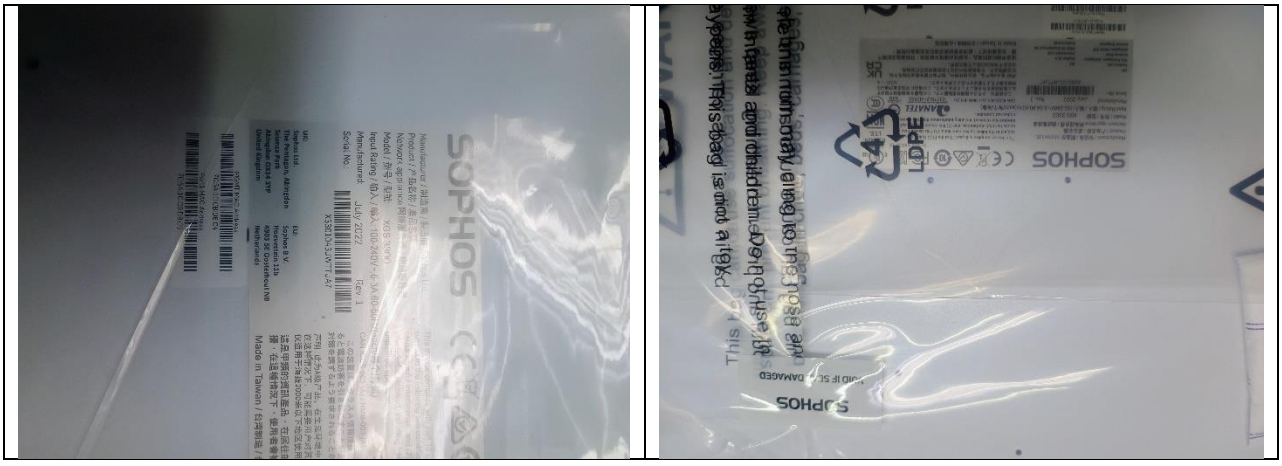
Descripción	Especificación técnica	Cant	Serial
XGS 3300 Security Appliance - US power cord	Equipo US poder cord	1	X3301043JWTTJA7

Descripción	Especificación técnica	Cant	Numero de licencia
XGS 3300 Xstream Protection -	12 MOS	1	LN1001566846
XGS 3300 Webserver Protection -	12 MOS	1	LN1001566847
Central Intercept X Advanced -	12 MOS	320	LN1001566850
Central Intercept X Advanced for Server servers -	12 MOS	7	LN1001566849
Central Phish Threat	12 MOS	5	LN1001566848

Pymes On Line SAS, realizó el suministro del equipo marca Sophos XGS 3300 Security Appliance - US Power cord. de este equipo se realizó la entrega física, instalacion en el centro de datos airea de TI, configuración, programación y puesta en funcionamiento óptimo.







SOPHOS XGS 3300 Instalado en el centro de datos Piso 4 de INTENALCO





Licenciamiento con vigencia de 12 meses:

- Una (1) licencia XGS 3300 Xstream Protection – se realizo la entrega en el portal y se configura en el firewall

- Una (1) licencia XGS 3300 Webserver Protection - se realizó la entrega en el portal y se configura en el firewall
- Trescientos veinte (320) licencias Central Intercept X Advanced - se realizó la entrega en el portal y se configura en el firewall
- Siete (7) licencias Central Intercept X Advanced for Server servers - se realizó la entrega en el portal y se configura en el firewall
- Cinco (5) licencias Central Phish Threat. se realizó la entrega en el portal y se configura en el firewall

Una vez realizada la instalación del equipo y su licenciamiento se procedió con la Implementación, Configuración y Capacitación de XGS 3300, estas actividades se realizaron con el personal de TI de acuerdo al objeto del contrato.

De igual forma, se procedió con las actividades adicionales contratadas que se describen a continuación.

1. Al realizar la revisión de switch, al encontrarse que el firewall de estos se encontraba desactualizado se procedió con la actualización de 17 switch a la última versión de su firewall respectivo. Aunque esto no estaba constatado en el contrato

UBICACIÓN	SWITCH	IP	VLAN
PISO 1	**CISCO SG 220-50 OFICINA MANTENIMIENTO**	172.16.3.243	VLAN 1, 80 y 90
PISO 1	**CISCO SG 220-50 BIBLIOTECA**	172.16.3.245	VLAN 1 y 25
PISO 1	**TP-LINK TL-SG3452**	172.16.2.154	VLAN 1, 37, 80 y 90
PISO 2	**HP V1910 24G**	172.16.3.240	VLAN 1, 80 y 90
PISO 3	**CISCO SG 220-50**	172.16.3.242	VLAN 1, 80 y 90
PISO 4	**CENTRO PRINCIPAL DE CABLEADO CISCO SG 220-50**	172.16.3.249	VLAN 1, 80 y 90
PISO 4	**SWITCH SALA SISTEMAS 1: SG250-50**	172.16.3.132	VLAN 1, 30
PISO 4	**SWITCH GABINETE SERVIDORES**	172.16.3.250	VLAN 1
PISO 4	**SALA SISTEMAS 2: SG250-26**	172.16.3.133	VLAN 1, 31
PISO 4	**SALA SISTEMAS 3: SG250-26**	172.16.3.134	VLAN 1, 32
PISO 4	**SALA SISTEMAS 4: SG250-26**	172.16.3.135	VLAN 1, 33
PISO 4	**SALA SISTEMAS 5: SG250-26**	172.16.3.136	VLAN 1, 20, 80 y 90

PISO 4	**SALA SISTEMAS 6: SG250-26**	172.16.3.137	VLAN 1, 20
PISO 4	**SALA SISTEMAS 7: SG250-26**	172.16.3.139	VLAN 1, 36
PISO 5	**CISCO SG 220-50 AUDITORIO**	172.16.3.233	EL SWITCH NO CUENTA CON ACCESO ADMINISTRABLE
PISO 5	**CISCO SG 220-50 OFICINA TALENTO HUMANO**	172.16.3.248	VLAN 1, 80 Y 90
PISO 5	**CISCO SG 220-50**	172.16.3.246	VLAN 1, 80 Y 90

Ubicación	Centros de cableado	Switch	Routers	APP	Eq. Computo sala	Equipos admi.	Equipos biblioteca	Servidores	Tableros inteligentes
Piso 1	3	3	0	9	22	25	18	0	1
Piso 2	1	1	0	3	0	0	0	0	8
Piso 3	1	1	0	2	0	2	0	0	0
Piso 4	9	10	3	5	155	7	0	6	1
Piso 5	2	3	0	10	0	41	0	0	1
TOTAL	16	18	3	29	177	75	18	6	11

SEGMENTACIÓN DE RED DE DATOS

El direccionamiento de la red de la institución está constituido de la siguiente forma:

VLAN	Segmento	Hosts máx.	Subred / Máscara	Hosts útiles	Asignación de IP
Lan	Red lan	**≤ 1000**	172.16.0.0/22	**1000**	**Estáticas /dhcp**
25	Biblioteca	≤ 100	**172.16.22.0 /25**	126	DHCP
30	Sala 1	≤ 50	**172.16.22.128 /26**	62	DHCP
31	Sala 2	≤ 30	**172.16.22.192 /27**	30	DHCP
32	Sala 3	≤ 30	**172.16.22.224 /27**	30	DHCP
33	Sala 4	≤ 30	**172.16.23.0 /27**	30	DHCP
35	Sala 6	≤ 30	**172.16.23.64 /27**	30	DHCP

20	Sala 5	≤ 30	**172.16.21.0 /27**	30	DHCP
36	Sala 7	≤ 30	**172.16.23.96 /27**	30	DHCP
37	Sala 8	≤ 30	**172.16.23.129/27**	30	DHCP
70	Wi-Fi Auditorio - LAN	≤ 200	**172.16.26.0 /24**	254	DHCP (+ reservas AV)
80	Wi-Fi Estudiantes	≤ 1000	**172.16.28.0 /22**	1022	DHCP (lease 4 h)
90	WIFI INVITADOS	≤ 100	**172.16.27.0 /25**	126	DHCP

UBICACIÓN	CENTRO CABLEADO	TOTAL, DE PUNTOS DE DATOS
PISO 1	SC 1	42
PISO 1	BIBLIOTECA	47
PISO 1	EXTENSION	59
PISO 1	MONITOREO	48
PISO 2	CUARTO ELECTRICOS	35
PSIO 3	CUARTO ELECTRICOS	40
PISO 4	CENTRO CABLEADO PRINCIPAL	48
PISO 4	SALA 1	46
PISO 4	SALA 2	23
PISO 4	SALA 3	23
PISO 4	SALA 4	22
PISO 4	SALA 5	23
PISO 4	SALA 6	22
PISO 4	SALA 7	23
PISO 4	JURIDICO	23
PISO 5	SC 5-1	48
PISO 5	SC 5-2	86
PISO 5	TS 1	6
	TOTAL	**664**

3. PRUEBAS DE LATENCIA

Definición de latencia en una red de datos, muestra en el tiempo que tarda los datos en transferirse a través red, entre mayor sea el retardo latencia será alta y al menor retardo menor latencia. La latencia ideal para comunicación en tiempo real debe ser menor a 50 milisegundos, menos de 20 milisegundos se considera ideal. Se realizaron a través de comando ping que nos devuelve el tiempo que se tarda de un paquete a otro según la IP pruebas

CENTRO DE CABLEADO	IP	LATENCIA	IMAGEN	OBSERVACION
Centro de cableado principal	172.16.3.243	1 milisegundo	SWITCH PISO 1	Bueno
Centro de cableado principal	172.16.3.245	1 milisegundo	SWITCH BIBLIOTECA	Bueno
Centro de cableado principal	172.16.2.154	1 milisegundo	SWITCH EXTENCION	Bueno
Centro de cableado principal	172.16.3.240	1 milisegundo	SWITCH PISO 2	Bueno
Centro de cableado principal	172.16.3.242	1 milisegundo	SWITCH PISO 3	Bueno
Centro de cableado principal	172.16.3.249	1 milisegundo	SWITCH PRINCIPAL PISO 4	Bueno
Centro de cableado principal	172.16.3.246	1 milisegundo	SWITCH PISO 5	Bueno
Centro de cableado principal	172.16.3.233	1 milisegundo	SWITCH AUDITORIO PISO 5	Bueno
Centro de cableado principal	172.16.3.248	1 milisegundo	SWITCH TALENTO HUMANO	Bueno
Centro de cableado principal	172.16.3.132	1 milisegundo	SWITCH SALA SISTEMAS 1	Bueno
Centro de cableado principal	172.16.3.133	1 milisegundo	SWITCH SALA SISTEMAS 2	Bueno
Centro de cableado principal	172.16.3.134	1 milisegundo	SWITCH SALA SISTEMAS 3	Bueno
Centro de cableado principal	172.16.3.135	1 milisegundo	SWITCH SALA SISTEMAS 4	Bueno
Centro de cableado principal	172.16.3.136	1 milisegundo	SWITCH SALA SISTEMAS 5	Bueno
Centro de cableado principal	172.16.3.137	1 milisegundo	SWITCH SALA SISTEMAS 6	Bueno
Centro de cableado principal	172.16.3.139	1 milisegundo	SWITCH SALA SISTEMAS 7	Bueno
Centro de cableado principal	190.121.134.50	1 milisegundo	GATEWAY MEDIACOMMERCE	Bueno
Centro de cableado principal	200.29.117.153	1 milisegundo	GATEWAY EMCALI	Bueno
Centro de cableado principal	190.144.141.9	1 milisegundo	GATEWAY CLARO	Bueno
Centro de cableado principal	172.16.3.3	2 milisegundos	DINSTAR	Bueno
Centro de cableado principal	172.16.0.4	1 milisegundo	SERVIDOR ARCHIVO	Bueno
Centro de cableado principal	172.16.0.7	2 milisegundos	SERVIDOR TELEFONIA	Bueno

SWITCH PISO 1

```
Respuesta desde 172.16.3.243: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.243: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.243: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.243: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.243: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.243: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.243: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.243: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.243: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.243: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.243: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.243: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.243: bytes=32 tiempo=1ms TTL=64

Estadísticas de ping para 172.16.3.243:
    Paquetes: enviados = 77, recibidos = 76, perdidos = 1
    (1% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 1ms, Media = 0ms
```

SWITCH BIBLIOTECA

```
Respuesta desde 172.16.3.245: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.245: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.245: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.245: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.245: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.245: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.245: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.245: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.245: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.245: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.245: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.245: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.245: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.245: bytes=32 tiempo=1ms TTL=64

Estadísticas de ping para 172.16.3.245:
    Paquetes: enviados = 78, recibidos = 78, perdidos = 0
    (0% perdidos),
Respuesta desde 172.16.3.245: Tiempos aproximados de ida y vuelta en miliseg
undos:
    Mínimo = 0ms, Máximo = 2ms, Media = 0ms
```

SWITCH EXTENSION

```
Respuesta desde 172.16.2.154: bytes=32 tiempo=2ms TTL=64
Respuesta desde 172.16.2.154: bytes=32 tiempo=2ms TTL=64
Respuesta desde 172.16.2.154: bytes=32 tiempo=2ms TTL=64
Respuesta desde 172.16.2.154: bytes=32 tiempo=2ms TTL=64
Respuesta desde 172.16.2.154: bytes=32 tiempo=2ms TTL=64
Respuesta desde 172.16.2.154: bytes=32 tiempo=2ms TTL=64
Respuesta desde 172.16.2.154: bytes=32 tiempo=2ms TTL=64
Respuesta desde 172.16.2.154: bytes=32 tiempo=2ms TTL=64
Respuesta desde 172.16.2.154: bytes=32 tiempo=2ms TTL=64
Respuesta desde 172.16.2.154: bytes=32 tiempo=2ms TTL=64
Respuesta desde 172.16.2.154: bytes=32 tiempo=2ms TTL=64
Respuesta desde 172.16.2.154: bytes=32 tiempo=2ms TTL=64
Respuesta desde 172.16.2.154: bytes=32 tiempo=2ms TTL=64
Respuesta desde 172.16.2.154: bytes=32 tiempo=2ms TTL=64
Respuesta desde 172.16.2.154: bytes=32 tiempo=2ms TTL=64

Estadísticas de ping para 172.16.2.154:
    Paquetes: enviados = 63, recibidos = 63, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 2ms, Máximo = 8ms, Media = 2ms
```

SWITCH PISO 2

```
Respuesta desde 172.16.3.240: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.240: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.240: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.240: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.240: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.240: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.240: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.240: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.240: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.240: bytes=32 tiempo=2ms TTL=64
Respuesta desde 172.16.3.240: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.240: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.240: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.240: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.240: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.240: bytes=32 tiempo=1ms TTL=64

Estadísticas de ping para 172.16.3.240:
    Paquetes: enviados = 152, recibidos = 152, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 2ms, Media = 1ms
```

SWITCH PISO 3

```
Respuesta desde 172.16.3.242: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.242: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.242: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.242: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.242: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.242: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.242: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.242: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.242: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.242: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.242: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.242: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.242: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.242: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.242: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.242: bytes=32 tiempo=1ms TTL=64

Estadísticas de ping para 172.16.3.242:
    Paquetes: enviados = 136, recibidos = 135, perdidos = 1
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 2ms, Media = 0ms
```

SWITCH PRINCIPAL PISO 4

```
Respuesta desde 172.16.3.249: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.249: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.249: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.249: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.249: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.249: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.249: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.249: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.249: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.249: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.249: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.249: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.249: bytes=32 tiempo<1m TTL=64
Respuesta desde 172.16.3.249: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.249: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.249: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.249: bytes=32 tiempo=1ms TTL=64

Estadísticas de ping para 172.16.3.249:
    Paquetes: enviados = 123, recibidos = 122, perdidos = 1
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 3ms, Media = 1ms
```

SWITCH PISO 5

```
Respuesta desde 172.16.3.246: bytes=32 tiempo<1m TTL=64
Respuesta desde 172.16.3.246: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.246: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.246: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.246: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.246: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.246: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.246: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.246: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.246: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.246: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.246: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.246: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.246: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.246: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.246: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.246: bytes=32 tiempo=1ms TTL=64

Estadísticas de ping para 172.16.3.246:
    Paquetes: enviados = 81, recibidos = 81, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 1ms, Media = 0ms
```

SWITCH TALENTO HUMANO PISO 5

```
Respuesta desde 172.16.3.248: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.248: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.248: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.248: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.248: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.248: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.248: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.248: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.248: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.248: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.248: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.248: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.248: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.248: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.248: bytes=32 tiempo=1ms TTL=64

Estadísticas de ping para 172.16.3.248:
    Paquetes: enviados = 92, recibidos = 92, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 1ms, Media = 0ms
```

SWITCH SALA SISTEMAS 1

```
Respuesta desde 172.16.3.132: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.132: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.132: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.132: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.132: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.132: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.132: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.132: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.132: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.132: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.132: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.132: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.132: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.132: bytes=32 tiempo=1ms TTL=64

Estadísticas de ping para 172.16.3.132:
    Paquetes: enviados = 138, recibidos = 138, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 3ms, Media = 1ms
```

SWITCH SALA SISTEMAS 2

```
Respuesta desde 172.16.3.133: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.133: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.133: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.133: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.133: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.133: bytes=32 tiempo=2ms TTL=64
Respuesta desde 172.16.3.133: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.133: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.133: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.133: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.133: bytes=32 tiempo=2ms TTL=64
Respuesta desde 172.16.3.133: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.133: bytes=32 tiempo=2ms TTL=64

Estadísticas de ping para 172.16.3.133:
    Paquetes: enviados = 115, recibidos = 115, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 7ms, Media = 1ms
```

SWITCH SALA SISTEMAS 3

```
Respuesta desde 172.16.3.134: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.134: bytes=32 tiempo=2ms TTL=64
Respuesta desde 172.16.3.134: bytes=32 tiempo=2ms TTL=64
Respuesta desde 172.16.3.134: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.134: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.134: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.134: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.134: bytes=32 tiempo=2ms TTL=64
Respuesta desde 172.16.3.134: bytes=32 tiempo=2ms TTL=64
Respuesta desde 172.16.3.134: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.134: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.134: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.134: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.134: bytes=32 tiempo=1ms TTL=64

Estadísticas de ping para 172.16.3.134:
    Paquetes: enviados = 171, recibidos = 171, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 6ms, Media = 1ms
```

SWITCH SALA SISTEMAS 4

```
Respuesta desde 172.16.3.135: bytes=32 tiempo=2ms TTL=64
Respuesta desde 172.16.3.135: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.135: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.135: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.135: bytes=32 tiempo=2ms TTL=64
Respuesta desde 172.16.3.135: bytes=32 tiempo=2ms TTL=64
Respuesta desde 172.16.3.135: bytes=32 tiempo=2ms TTL=64
Respuesta desde 172.16.3.135: bytes=32 tiempo=2ms TTL=64
Respuesta desde 172.16.3.135: bytes=32 tiempo=2ms TTL=64
Respuesta desde 172.16.3.135: bytes=32 tiempo=2ms TTL=64
Respuesta desde 172.16.3.135: bytes=32 tiempo=2ms TTL=64

Estadísticas de ping para 172.16.3.135:
    Paquetes: enviados = 112, recibidos = 112, perdidos =
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 2ms, Media = 1ms
```

SWITCH SALA SISTEMAS 5

```
Respuesta desde 172.16.3.136: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.136: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.136: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.136: bytes=32 tiempo=2ms TTL=64
Respuesta desde 172.16.3.136: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.136: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.136: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.136: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.136: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.136: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.136: bytes=32 tiempo=1ms TTL=64

Estadísticas de ping para 172.16.3.136:
    Paquetes: enviados = 70, recibidos = 70, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 14ms, Media = 1ms
```

SWITCH SALA SISTEMAS 6

```
Respuesta desde 172.16.3.137: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.137: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.137: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.137: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.137: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.137: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.137: bytes=32 tiempo=2ms TTL=64
Respuesta desde 172.16.3.137: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.137: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.137: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.137: bytes=32 tiempo=1ms TTL=64

Estadísticas de ping para 172.16.3.137:
    Paquetes: enviados = 283, recibidos = 283, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 8ms, Media = 1ms
```

SWITCH SALA SISTEMAS 7

```
Respuesta desde 172.16.3.139: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.139: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.139: bytes=32 tiempo=2ms TTL=64
Respuesta desde 172.16.3.139: bytes=32 tiempo=2ms TTL=64
Respuesta desde 172.16.3.139: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.139: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.139: bytes=32 tiempo=2ms TTL=64
Respuesta desde 172.16.3.139: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.139: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.3.139: bytes=32 tiempo=1ms TTL=64

Estadísticas de ping para 172.16.3.139:
    Paquetes: enviados = 75, recibidos = 75, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 2ms, Media = 1ms
```

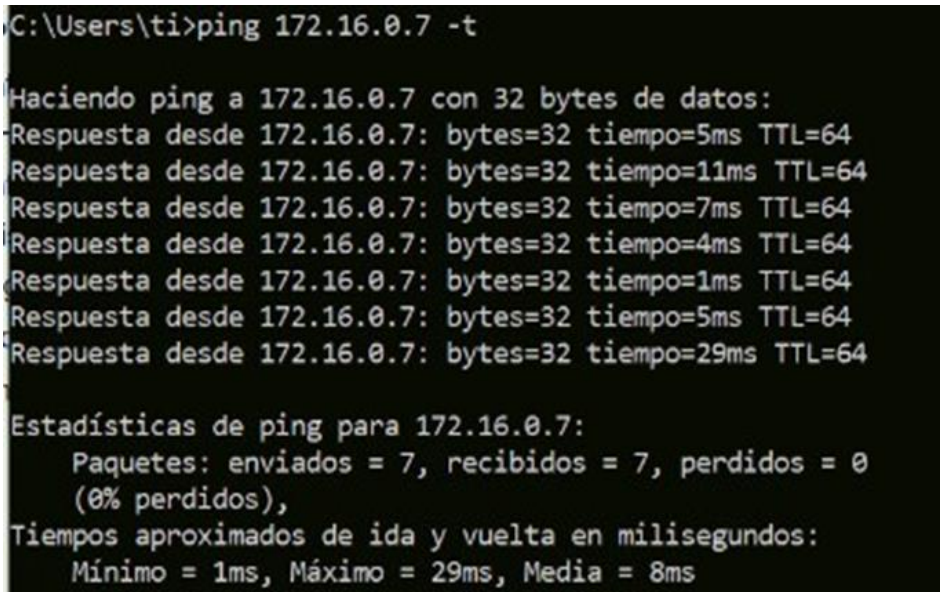
DINSTAR

```
C:\Users\ti>ping 172.16.3.3 -t

Haciendo ping a 172.16.3.3 con 32 bytes de datos:
Respuesta desde 172.16.3.3: bytes=32 tiempo=23ms TTL=64
Respuesta desde 172.16.3.3: bytes=32 tiempo=2ms TTL=64
Respuesta desde 172.16.3.3: bytes=32 tiempo=7ms TTL=64
Respuesta desde 172.16.3.3: bytes=32 tiempo=2ms TTL=64
Respuesta desde 172.16.3.3: bytes=32 tiempo=2ms TTL=64
Respuesta desde 172.16.3.3: bytes=32 tiempo=12ms TTL=64
Respuesta desde 172.16.3.3: bytes=32 tiempo=2ms TTL=64
Respuesta desde 172.16.3.3: bytes=32 tiempo=4ms TTL=64

Estadísticas de ping para 172.16.3.3:
    Paquetes: enviados = 8, recibidos = 8, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 2ms, Máximo = 23ms, Media = 6ms
```

SERVIDOR TELEFONÍA



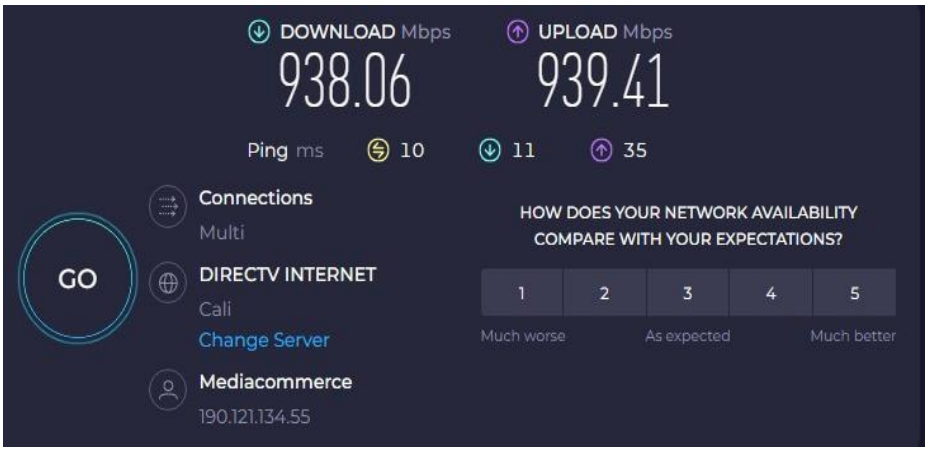
Se realizaron pruebas de carga, descarga y latencia en cada uno de los Gateway de los proveedores (Claro, Emcali y Mediacommerce) en donde se obtuvieron los siguientes resultados:

CONEXIÓN A INTERNET			
ROUTER	PROVEDOORES	TIPO	MEGAS
1	EMCALI	DEDICADO	1000
2	MEDIA COMERC	DEDICADO	1000
3	CLARO	BANDA ANCHA	300

GATEWAY MEDIACOMMERCE

```
Respuesta desde 190.121.134.50: bytes=32 tiempo=5ms TTL=254
Respuesta desde 190.121.134.50: bytes=32 tiempo=2ms TTL=254
Respuesta desde 190.121.134.50: bytes=32 tiempo=2ms TTL=254
Respuesta desde 190.121.134.50: bytes=32 tiempo=11ms TTL=254
Respuesta desde 190.121.134.50: bytes=32 tiempo=2ms TTL=254
Respuesta desde 190.121.134.50: bytes=32 tiempo=1ms TTL=254
Respuesta desde 190.121.134.50: bytes=32 tiempo=1ms TTL=254
Respuesta desde 190.121.134.50: bytes=32 tiempo=1ms TTL=254
Respuesta desde 190.121.134.50: bytes=32 tiempo=5ms TTL=254
Respuesta desde 190.121.134.50: bytes=32 tiempo=11ms TTL=254
Respuesta desde 190.121.134.50: bytes=32 tiempo=10ms TTL=254

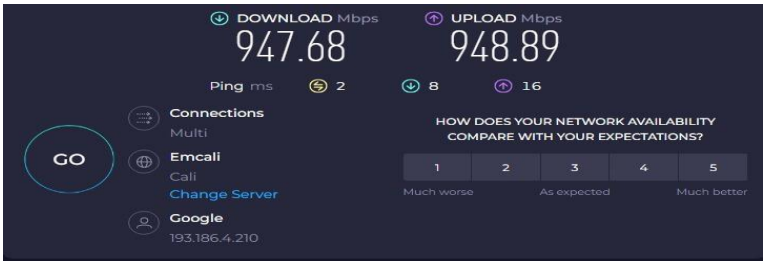
Estadísticas de ping para 190.121.134.50:
    Paquetes: enviados = 21, recibidos = 21, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 11ms, Media = 3ms
```



GATEWAY EMCALI

```
Respuesta desde 200.29.117.153: bytes=32 tiempo=6ms TTL=63
Respuesta desde 200.29.117.153: bytes=32 tiempo=4ms TTL=63
Respuesta desde 200.29.117.153: bytes=32 tiempo=5ms TTL=63
Respuesta desde 200.29.117.153: bytes=32 tiempo=7ms TTL=63
Respuesta desde 200.29.117.153: bytes=32 tiempo=8ms TTL=63
Respuesta desde 200.29.117.153: bytes=32 tiempo=2ms TTL=63
Respuesta desde 200.29.117.153: bytes=32 tiempo=7ms TTL=63
Respuesta desde 200.29.117.153: bytes=32 tiempo=1ms TTL=63
Respuesta desde 200.29.117.153: bytes=32 tiempo=11ms TTL=63
Respuesta desde 200.29.117.153: bytes=32 tiempo=12ms TTL=63
Respuesta desde 200.29.117.153: bytes=32 tiempo=3ms TTL=63
Respuesta desde 200.29.117.153: bytes=32 tiempo<1m TTL=63

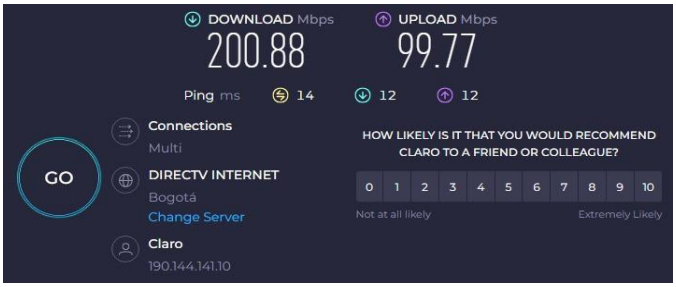
Estadísticas de ping para 200.29.117.153:
    Paquetes: enviados = 53, recibidos = 53, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 17ms, Media = 4ms
```



GATEWAY CLARO

```
Respuesta desde 190.144.141.9: bytes=32 tiempo=5ms TTL=63
Respuesta desde 190.144.141.9: bytes=32 tiempo=2ms TTL=63
Respuesta desde 190.144.141.9: bytes=32 tiempo=7ms TTL=63
Respuesta desde 190.144.141.9: bytes=32 tiempo=2ms TTL=63
Respuesta desde 190.144.141.9: bytes=32 tiempo=3ms TTL=63
Respuesta desde 190.144.141.9: bytes=32 tiempo=1ms TTL=63
Respuesta desde 190.144.141.9: bytes=32 tiempo=1ms TTL=63
Respuesta desde 190.144.141.9: bytes=32 tiempo=3ms TTL=63
Respuesta desde 190.144.141.9: bytes=32 tiempo=3ms TTL=63
Respuesta desde 190.144.141.9: bytes=32 tiempo=1ms TTL=63
Respuesta desde 190.144.141.9: bytes=32 tiempo=4ms TTL=63
Respuesta desde 190.144.141.9: bytes=32 tiempo=7ms TTL=63

Estadísticas de ping para 190.144.141.9:
    Paquetes: enviados = 43, recibidos = 43, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 12ms, Media = 3ms
```



Se puede concluir que el estado latencia es óptimo ya que es menor a 50 milisegundos con un promedio de 3 milisegundos.

3. ESCANEO DE PUERTOS

Se realizo el escaneo de puertos con el software IP PORT SCCANER donde se evidencio lo siguiente: SEGMENTOS 172.16.0.1/172.16.3.254

NOMBRE	IP	PUERTOS	DETALLE
SOPHOS	172.16.0.1	22	Servicio Secure Shell
		25	Simple Mail Transfer Protocol
		53	Resolución de nombres por DNS
SERVIDOR ARCHIVO	172.16.0.4	23	Servicio Telnet
		80	Protocolo de Transferencia de HiperTexto
		135	epmap
		139	NETBIOS Servicio de sesiones
		445	SMB a través de TCP/IP
*.servicios.intenalco.edu.co	172.16.0.6	53	Resolución de nombres por DNS
		80	Protocolo de Transferencia de HiperTexto
		443	HTTPS
SERVIDOR DE TELEFONIA	172.16.0.7	22	Servicio Secure Shell
		25	Simple Mail Transfer Protocol
		80	Protocolo de Transferencia de HiperTexto
		110	Post Office Protocol v3 para
		143	Internet Message Access Protocol
		443	HTTPS
		993	IMAP a través de SSL/TLS
		995	POP3 a través de SSL/TLS
SRVDOMINIO.intenalco.local	172.16.0.10	53	Resolución de nombres por DNS
		80	Protocolo de Transferencia de HiperTexto
		88	Sistema de autenticación de red
		135	epmap
		139	NETBIOS Servicio de sesiones
		389	Lightweight Directory Access Protocol
		443	HTTPS
		445	SMB a través de TCP/IP

		464	Modificación de contraseña para Kerberos
		593	Mapa de Ep RPC HTTP
		636	LDAP a través de SSL/TLS
Apache HTTP Server Test Page powered by CentOS	172.16.0.13	21	Conexión FTP
		22	Servicio Secure Shell
		25	Simple Mail Transfer Protocol
		53	Resolución de nombres por DNS
		80	Protocolo de Transferencia de HiperTexto
		110	Post Office Protocol v3 para
		143	Internet Message Access Protocol
		443	HTTPS
		465	Autenticado SMTP sobre TLS/SSL
		587	Message Submission Agent
		993	IMAP a través de SSL/TLS
		995	POP3 a través de SSL/TLS
Equipo sin identificar	172.16.0.15	21	Conexión FTP
		25	Simple Mail Transfer Protocol
		53	Resolución de nombres por DNS
		110	Post Office Protocol v3 para
		143	Internet Message Access Protocol
		465	Autenticado SMTP sobre TLS/SSL
		587	Message Submission Agent
		993	IMAP a través de SSL/TLS
		995	POP3 a través de SSL/TLS
NPI16BB44	172.16.3.117	21	Conexión FTP
		23	Servicio Telnet
		80	Protocolo de Transferencia de HiperTexto
		443	HTTPS
		515	Servicios de impresión Line Printer Daemon
		631	Internet Printing Protocol

SEGMENTOS 172.16.28.0/252

NOMBRE	IP	PUERTOS	DETALLE
Sophos Ltd	172.16.28.1	22	Servicio Secure Shell
		25	Simple Mail Transfer Protocol
		53	Resolución de nombres por DNS

SEGMENTOS 172.16.22.0/128

NOMBRE	IP	PUERTOS	DETALLE
Sophos Ltd	172.16.22.1	22	Servicio Secure Shell
		25	Simple Mail Transfer Protocol
		53	Resolución de nombres por DNS
BIBLIOTECA9	172.16.22.12	135	epmap
		139	NETBIOS Servicio de sesiones
		445	SMB a través de TCP/IP
BIBLIOTECA	172.16.22.14	80	Protocolo de Transferencia de HiperTexto
		135	epmap
		139	NETBIOS Servicio de sesiones
		445	SMB a través de TCP/IP
NPI153A8D	172.16.22.15	21	Conexión FTP
		23	Servicio Telnet
		80	Protocolo de Transferencia de HiperTexto
		443	HTTPS
		515	Servicios de impresión Line Printer Daemon
		631	Internet Printing Protocol

4. Análisis de topología

Topología General

La tipología de la red de INTENALCO está configurada en una topología jerárquica de estrella, la cual esta conformada por un firewall Sophos XGS 3300 implementado en **modo ruteado (NAT)**, actuando como el Gateway de salida a Internet para todas las redes internas de INTENALCO y como enrutador entre las VLAN internas. Esto significa que el XGS 3300 tendrá interfaces (físicas o subinterfaces VLAN) en cada segmento de red local y realizará *NAT* de las direcciones privadas internas hacia las direcciones IP públicas asignadas en las interfaces WAN.

La **topología general** es la siguiente:

- El XGS 3300 se conectará al **switch central/core** de la red campus vía un enlace troncal (802.1Q) que transportará todas las VLAN definidas. Cada VLAN estará configurada como interfaz lógica en el firewall con su respectiva subred IP y gateway.
- Las **redes cableadas** (administrativas, laboratorios, infraestructura, etc.) y las **redes Wi-Fi** (administrativas, estudiantes, invitados, etc.) estarán segmentadas en VLANs separadas, todas convergiendo en el firewall para control de tráfico y filtrado.
- El XGS 3300 maneja múltiples enlaces WAN (tres ISP) en una configuración de **balanceo de carga con failover**, para asegurar redundancia y disponibilidad de Internet (detalle en sección WAN).
- Los **puntos de acceso UniFi WiFi 7 Pro** se integrarán en la topología mediante VLANs específicas para Wi-Fi, garantizando la separación del tráfico inalámbrico de administración, estudiantes e invitados. Los APs residirán en la VLAN de Infraestructura, pero sus SSID asignarán clientes a las VLAN correspondientes (mediante tags VLAN en el tráfico inalámbrico). El firewall aplicará políticas diferenciadas según la VLAN/SSID de origen (por ejemplo, más restricciones en la red de invitados).
- El acceso remoto re realiza atreves DE **VPN** para usuarios autorizados (por ejemplo, personal de TI o dirección) que necesiten conectarse externamente.
- En resumen, el XGS 3300 actuará como el corazón de la infraestructura de seguridad perimetral, controlando todo el tráfico *norte-sur* hacia Internet y también aplicando segmentación y seguridad en el tráfico *este-oeste* entre VLANs internas. A continuación, se detalla la segmentación de red y configuraciones específicas para lograr estos objetivos.

4.1. SERVIDORES DE LA INSTITUCION

Red Lan 172.16.0.0/22 (“LAN Legacy”)

Se encuentra en este segmento la red administrativa y los equipamientos activos de la institución.

4.2. Segmentación de Red (VLANs)

La red de INTENALCO ha sido cuidadosamente segmentada en múltiples **VLANs** para aislar diferentes departamentos, servicios y tipos de usuarios/dispositivos. Esta segmentación mejora la seguridad y el rendimiento al limitar los dominios de broadcast y al permitir aplicar políticas de firewall específicas por segmento. A continuación, se listan las VLAN definidas, con su identificación, rango IP y propósito:

- **VLAN 10 – Infraestructura:** Red 172.16.20.0/24 (máscara 255.255.255.0, ~254 hosts utilizable). Reservada para **equipos de infraestructura de TI**: routers, switches de core/distribución, puntos de acceso UniFi, servidores internos y otros dispositivos de gestión. Las direcciones IP en este segmento serán **estáticas** para dispositivos críticos y se usará direccionamiento fijo o reservas DHCP según sea apropiado, asegurando direcciones conocidas para gestión y monitoreo (por ejemplo, asignar IPs fijas a switches y APs). Este segmento permite una fácil administración de todos los activos de red. Configurada para que en el futuro el segmento de la red LAN 172.16.0.0/22 se desactiva y pase a ser pare de esta VLAN.

- .
- **VLAN 25 – Biblioteca:** Red 172.16.22.0/25 (255.255.255.128, 126 hosts). Segmento para la **Biblioteca**, que puede incluir PCs de consulta, sistemas de catalogación (por ejemplo, el sistema Koha de gestión bibliotecaria) y otros recursos de la biblioteca. Se usará DHCP para asignar IP a PCs de estudiantes en la biblioteca o equipos públicos. Dado que es una red académica controlada, su salida a Internet estará filtrada de forma similar a estudiantes (por ejemplo, bloqueando contenidos no académicos), aunque el personal bibliotecario podría tener ciertos permisos adicionales. Si el servidor de biblioteca (Koha) está alojado internamente en la red LAN, y se permitirán las conexiones necesarias desde VLAN 25 a dicho servidor en puertos específicos (HTTP/HTTPS para interfaz web de Koha, o base de datos si corresponde).
- **VLAN 30 – Sala 1 (Aulas/Salón de clase, SALA 1):** Red 172.16.22.128/26 (255.255.255.192, 62 hosts). Corresponde a un laboratorio o sala de cómputo #1, con capacidad ~50 dispositivos. Configurada con DHCP para los PCs. Similarmente:
- **VLAN 31 – Sala 2:** 172.16.22.192/27 (255.255.255.224, 30 hosts).
- **VLAN 32 – Sala 3:** 172.16.22.224/27 (30 hosts).
- **VLAN 33 – Sala 4:** 172.16.23.0/27 (30 hosts).
- **VLAN 34 – Sala 5:** 172.16.23.32/27 (30 hosts).
- **VLAN 35 – Sala 6:** 172.16.23.64/27 (30 hosts).
- **VLAN 36 – Sala 7:** 172.16.23.96/27 (30 hosts).
- **VLAN 37 – Sala 8:** 172.16.23.129/27 (30 hosts).

Cada una de estas VLAN de salas/laboratorios informáticos está dimensionada al número máximo de equipos en la sala. Todas usarán **DHCP**. Para algunas salas (VLAN 31-33) se anotó "FIJA", lo que podría indicar ciertos equipos con IP estática (tal vez servidores de laboratorio o dispositivos fijos); de ser necesario, se harán reservas DHCP o asignaciones manuales para ellos. El acceso a Internet de estas VLAN será similar al de estudiantes: permitiendo navegación web con filtros académicos y bloqueando actividades no autorizadas (descargas P2P, juegos, contenido adulto, etc.). Adicionalmente, el tráfico entre estas VLAN y la red interna se limitará según las necesidades académicas (por ejemplo, podrían requerir acceso a un servidor de licencias o repositorios, lo cual se permitirá explícitamente, pero se bloqueará acceso a otros segmentos no necesarios).

- **VLAN 70 – Wi-Fi Auditorio (LAN evento):** Red 172.16.26.0/24 (254 hosts). Esta red inalámbrica es para el **auditorio** o eventos especiales (quizá invitados en conferencias, o para proveer conectividad en un gran salón). Puede ser una Wi-Fi interna de mayor capacidad. Se usará DHCP, con posibilidad de reservas para dispositivos AV o de streaming propios del auditorio. En cuanto a permisos, se asemeja a una red de estudiantes (navegación web permitida pero controlada). Podría tratarse de un SSID separado para eventos, donde quizás haya un QoS especial si se hacen transmisiones. Por sencillez, se aplicarán políticas de internet similares a estudiantes (limitando ancho de banda por cliente si necesario), y se aislará de

recursos internos salvo que se definan excepciones (por ejemplo, quizá acceso a un servidor de presentaciones).

- **VLAN 80 – Wi-Fi Estudiantes:** Red 172.16.28.0/22 (máscara 255.255.252.0, alrededor de 1022 hosts útiles). Esta es la red inalámbrica principal para **estudiantes**, con capacidad para ~1000 dispositivos. Se asignarán IPs vía DHCP con un *lease time* más corto (~4 horas) para reciclar direcciones debido a la alta rotación de clientes. El tráfico de esta VLAN estará **estrictamente controlado y aislado**: se permitirá únicamente **navegación web básica (HTTP/HTTPS)** y quizá algunos servicios necesarios (DNS, etc.), **bloqueando acceso a redes internas**. Además, para prevenir abuso del ancho de banda. se aplicará una política de **QoS** limitando. Esto evita que un solo estudiante sature el enlace con descargas masivas; cada dispositivo tendrá un tope justo que mantiene la navegación razonable sin afectar a otros usuarios.
- **VLAN 90 – Wi-Fi Invitados:** Red 172.16.27.0/25 (126 hosts). SSID para **visitantes** externos (conferencistas, visitantes temporales). La política aquí será de **"Guest network" aislada**. Una vez autenticados, su tráfico será NATeado a Internet. Solo se permitirá navegación web básica (HTTP/HTTPS) y se impedirán otras comunicaciones. Esta VLAN estará completamente aislada de todas las VLAN internas (solo salida a Internet) por seguridad. Adicionalmente, se puede aplicar una cuota o límite de ancho de banda global/moderado para invitados, para que no consuman recursos excesivos. Dado el bajo número de invitados simultáneos, no se espera saturación. **Direccionamiento IP general:** Todas las VLAN anteriores caben en el supernet 172.16.20.0/20 (desde 172.16.20.0 hasta 172.16.31.255). Esto deja libre el rango 172.16.29.0 - 172.16.31.255 (aprox 3 /24 sin usar) para **crecimiento futuro** o nuevas VLAN. El esquema es escalable, permitiendo agregar más segmentos si la institución lo requiere más adelante sin colisiones con las redes existentes.

Cada VLAN tendrá asignada una **puerta de enlace (gateway)** en el XGS 3300 (es decir, la IP del firewall dentro de esa subred). Por ejemplo, típicamente se usaría la primera dirección utilizable de cada rango para el gateway: p.ej. 172.16.20.1 para VLAN10, 172.16.21.1 para VLAN20, etc. (Esto se confirmará durante la configuración, pero es el esquema convencional). El firewall, por tanto, tendrá múltiples interfaces lógicas configuradas – una por VLAN – con esas IPs.

5. Configuración de WAN y Balanceo de Carga

El Sophos XGS 3300 contará con **tres conexiones WAN** de Internet de distintos proveedores, configuradas en una **estrategia de balanceo de carga (activo-activo) con failover**:

1. **ISP 1: Media Commerce – Fibra 1 Gbps (enlace primario)**
    - **IP asignada (principal):** 190.121.134.50/28 (ejemplo, según datos proporcionados). Gateway: 190.121.134.49 (este parece ser la IP virtual del ISP). También se dispone de una IP secundaria 190.121.134.51 (posiblemente para un equipo de respaldo o para HA futura) y un pool de IPs públicas disponibles desde 190.121.134.52 hasta 190.121.134.62. Dns:
    - **Configuración en XGS:** Se creará una interfaz WAN (Port2, por ejemplo) con la IP .50/28, gateway .49. Las IPs adicionales (.52-.62) pueden añadirse como **alias** en la

interfaz WAN si se prevé usarlas para publicar servicios (por ejemplo, asignar una IP pública específica a un servidor web mediante DNAT/WAF).

- **DNS:** El ISP recomienda DNS 200.110.169.20 y 200.16.70.254; se pueden configurar estos servidores DNS en el firewall (o usar DNS públicos universalmente reconocidos) para resolución, dependiendo de rendimiento.
- **Peso (Weight):** 10 – *Primario a 50%*. En Sophos, asignar igual peso a dos enlaces activos hace que el tráfico se distribuya equitativamente entre ellos. Con peso 10, este enlace tomará ~50% del tráfico saliente activo.

2. **ISP 2: EMCALI – Fibra 1 Gbps (enlace primario)**
   - **IP asignada:** 200.29.117.154/29 (posiblemente, dado rango .154-.158 disponible). Gateway: 200.29.117.153. Esta conexión provee ~5 direcciones utilizables (.154-.158). Se configurará la interfaz WAN (Port3, por ejemplo) con .154/29, gateway .153. Las IPs adicionales .155-.158 se pueden agregar como alias si se necesitan múltiples IP públicas (ej. para diferentes servicios entrantes).
   - **DNS:** (No se detalló, pero probablemente EMCALI provee DNS locales; en ausencia de datos, se pueden reutilizar los DNS del ISP1 o unos globales).
   - **Peso:** 10 – *Primario a 50%*. Igual que el ISP1, este enlace cargará aproximadamente el otro 50% del tráfico saliente, en un balance 50/50 entre Media Commerce y EMCALI. Con ambos enlaces activos de 1 Gbps, la universidad dispondrá de un agregado de hasta 2 Gbps de capacidad de descarga distribuida (aunque sesiones individuales no excederán 1 Gbps dado el límite físico por enlace).
3. **ISP 3: Claro – Cable/FO 300 Mbps (enlace de respaldo/overflow)**
   - **IP asignada:** 190.144.141.9/30. Gateway: 190.144.141.8. (Nota: /30 indica 4 direcciones .8-.11, donde .8 red, .9 nuestro firewall, .10 segundo host no usado, .11 broadcast; es un poco inusual porque normalmente .8 sería la red, pero asumiremos .8 es el gateway operativamente). En la configuración, se pondrá la IP .9 con máscara /30 y gateway .8 en la interfaz WAN (Port4, p.ej.).
   - **DNS:** 200.108.86.212 y 200.108.86.213 (DNS de Claro).
   - **Peso:** 1 – *Backup/overflow*. Este enlace se configura con un peso muy bajo para indicar que **no participará del balance normal** excepto en mínima medida. En términos prácticos, el XGS puede tratarlo de dos maneras:
     - **Active-Passive:** Marcar este enlace como **Backup** en la configuración de WAN Link Manager. En este modo, Claro permanecerá inactivo salvo que uno de los enlaces principales falle (failover automático).
     - **Active-Active con peso reducido:** Alternativamente, mantenerlo activo, pero con Weight=1 vs 10 de los otros. Esto haría que en condiciones normales reciba solo una fracción muy pequeña del tráfico (aprox 1/(10+10+1) ≈ 5% o menos), pero si los otros enlaces se saturan, esta pequeña porción podría aliviar algo

(overflow). Dado que es 300 Mbps vs 1 Gbps, podría usarse por ejemplo para tráfico de menor prioridad o ciertas aplicaciones.

En la práctica, se optará por configurar Claro como **enlace de failover** puro (backup), dado que los principales ya balancean 50/50. Así se reserva su capacidad principalmente para caídas o eventualmente para absorción de picos si se desea. Sophos XGS permite definir los *SLAs* de monitorización de cada WAN (pings a 8.8.8.8 u otro) de modo que detecte caídas y conmute tráfico.

Gateway Load Balancing: En Sophos Firewall, la funcionalidad de **WAN Link Manager** nos permitirá establecer la *estrategia de balanceo*. Se elegirá "**Load Balance**" con los tres enlaces: ambos de 1Gbps con peso 10 y Claro 300Mbps con peso 1 (o como respaldo). Este algoritmo reparte nuevas conexiones salientes en proporción a los pesos. Así, aproximadamente la mitad de las sesiones irán por MediaCommerce y la mitad por EMCALI, maximizando el uso de recursos. Si uno falla, todo el tráfico saliente será enrutado automáticamente por el restante principal y/o el de backup (según configuración). El failover es automático y cuando el enlace se restablece, puede retomarse el balance.

Métrica/Enrutamiento entrante: Dado que tenemos múltiples IPs públicas, el tráfico entrante (p.ej. hacia servidores web publicados) idealmente debería ingresar por cualquiera de los enlaces configurados para ese fin. Sin embargo, típicamente se designa uno principal para cada servicio público (a menos que usemos DNS round-robin o balanceo). Se coordinará con TI de la institución qué enlace se usará para publicar cada servicio (por ejemplo, usar MediaCommerce para el sitio web principal de la institución, y EMCALI para, digamos, una VPN específica, de forma de aprovechar ambos). Sophos también soporta **SD-WAN policy routing**, lo cual no parece necesario en este escenario, pero es bueno saber que existe la opción de enrutar ciertos flujos por un enlace específico si hiciera falta.

NAT Saliente: Se habilitará la **Masquerading**/SNAT en las reglas de salida a Internet. Por defecto, el XGS hará NAT de todas las redes internas hacia la IP primaria de cada interfaz WAN (haciendo balanceo de carga a nivel de sesión). Así, las conexiones de usuarios pueden salir por cualquiera de las dos IPs públicas primarias. Esto no es problema para navegación web y la mayoría de servicios. (Se puede fijar que ciertas subredes siempre salgan por un enlace específico si la institución lo requiriera, pero inicialmente no es necesario). En el caso del enlace Claro (cuando entre en uso), también tendrá NAT habilitado.

Consideración de Return Path: Con múltiples WAN activos, es importante activar "Respond to Ping on WAN" solo donde necesario y verificar que el firewall tenga habilitado **"sticky sessions"** si un mismo flujo debe mantener la misma ruta. Sophos por defecto mantiene la ruta de respuesta por la misma interfaz de llegada de la conexión (asymmetric routing avoidance). Se verificará que esté habilitada la opción **"Use outbound interface IP"** para las respuestas de tráfico, de forma que si la solicitud entró por MediaCommerce, responda por MediaCommerce, etc.

Enlaces redundantes locales: Dado que en MediaCommerce había mención de IP principal y backup, cuenta con topología con dos equipos o rutas para ese ISP. Si se cuenta con dos entradas físicas para el mismo ISP (dos fibras), se podría configurar ambos en un *TEAM*/bond o como interfaces WAN separadas, pero en grupo. Actualmente, no se detalló, así que se asume un solo puerto por ISP.

6. Reglas de Firewall (Políticas de Seguridad)

Con la infraestructura de VLANs establecida y los enlaces WAN configurados, procedemos a definir las **reglas de firewall** que implementarán las políticas de seguridad deseadas. Estas reglas controlan qué tráfico se **permite o bloquea** entre las distintas zonas (LAN, WAN, WiFi, etc.), aplicando también servicios de seguridad como filtrado web, antivirus, IPS y QoS según corresponda.

A continuación, se detallan las reglas **mínimas** requeridas y se agregan otras recomendaciones de un punto de vista experto para fortalecer la seguridad:

6.1 Reglas de Acceso a Internet por VLAN (Salida a WAN)

Estas reglas gobiernan cómo cada VLAN interna accede a Internet (zona WAN). Se basan en el principio de mínimo privilegio: cada red obtiene solo el acceso externo necesario, con inspección de seguridad activa.

1. **Regla 1 – Gestión (LAN → Any):** *"LAN (Infraestructura) hacia cualquier destino, servicios SNMP, SSH, HTTPS – PERMITIR"*.
   Objetivo: Permitir desde la red de infraestructura el acceso de gestión a dispositivos críticos y al propio firewall. En concreto:
   - **SNMP**: Para que desde un servidor de monitoreo en LAN (por ejemplo, Zabbix o similar) se puedan consultar switches, APs, UPS, etc. vía SNMP. Solo se permitirá hacia las IP de esos equipos de gestión (no abierto a cualquier destino).
   - **SSH/HTTPS**: Para administración remota de equipos de red. Esto incluye permitir que los PCs/servidores de administración en LAN accedan via SSH/HTTPS a switches, APs, y también a la interfaz de administración del **firewall** Sophos. En el XGS, además de esta regla, se debe habilitar en **Administration > Device Access** que la zona LAN (o la zona personalizada de "Management" si se crea) tenga permitido HTTPS/SSH (y Ping, SNMP) hacia el propio dispositivo. Así, solo usuarios desde LAN podrán acceder a la consola web/SSH del firewall (manteniendo la administración restringida a la red de TI).
   - Esta regla estará acotada **"hacia direcciones de gestión específicas"**: se creará un grupo de hosts/IPs que incluye las IP de administración de cada dispositivo (por ejemplo, IP de administración de switches core, IP de controladora WiFi si la hay, IP del NVR, etc., además de la IP local del firewall). Solo a esos destinos se abrirán SNMP/SSH/HTTPS. Todo otro tráfico desde LAN a Internet no relevante será regido por reglas posteriores (por ejemplo, si un servidor de VLAN10 necesita actualizarse en Internet, habrá otra regla).
   - **Seguridad**: Aunque es red interna, aplicaremos *IPS* en estos servicios de gestión cuando salgan a *Any* (por ejemplo, si eventualmente se gestionara un router externo por SSH, se protege esa sesión). Y se mantendrá *logging* de estas conexiones para auditoría.
   - **Device Access**: Importante reiterar que permitir gestión de firewall desde LAN requiere habilitarlo en configuración de zona. Se verificará que solo LAN tengan privilegio de acceder a la GUI/SSH del XGS para seguridad.

2. **Regla 2 – Redes Administrativas/Educativas (VLAN 25,30,70 → WAN):** *"VLAN 25, 30, 70 hacia WAN, servicios Web, Mail, DNS – PERMITIR + AV/IPS"*. **Objetivo:** Dar acceso a Internet a las redes de **personal administrativo y redes académicas cableadas** con filtrado de contenido y seguridad.

    - Esta regla agrupa múltiples VLAN que comparten un perfil similar de uso: PCs de Biblioteca (25), Salas 1 (30) y Auditorio (70). Se les permitirá tráfico **HTTP (puerto 80)**, **HTTPS (443)**, **DNS (53)** y **correo (SMTP/IMAP/POP, puertos estándar)** hacia WAN. Esto cubre la mayoría de necesidades: navegación web, resolución de nombres y envío/recepción de email (por clientes o servidores locales).

    - No se incluyen puertos de compartición de archivos P2P, ni VPNs no autorizadas, ni otros servicios de ocio. Actividades como descargas torrent, streaming no académico o juegos online estarían categorizadas y bloqueadas por el filtro web/app. *(Más adelante, el filtro por categorías afinará esto. Por ejemplo, se bloquearán categorías de "descargas de freeware" o "P2P" para estos grupos, excepto donde se requiera.)*

    - **Antivirus (AV) y IPS:** En Sophos, al habilitar **Web Filtering y Security**, todo tráfico web saliente es inspeccionado. Se activará el **antivirus dual** en modo proxy/flujo para analizar descargas HTTP/HTTPS (requiriendo en HTTPS la inspección TLS si deseamos ver dentro; se puede implementar filtrado por categoría incluso sin descifrar, pero para AV es ideal inspeccionar contenido cifrado con una CA local del firewall instalada en endpoints). Igualmente, se asociará un **perfil de IPS** a esta regla, enfocado en detectar ataques de salida (por ejemplo, alguna máquina comprometida intentando contactar un C2) y ataques de entrada vía respuestas maliciosas. Con el Xstream DPI, el IPS funciona en modo streaming sin degradar mucho performance.

    - **Web Filtering**: Se adjuntará un **Web Policy** apropiado. Inicialmente, podría ser "Allow All" pero con ciertas categorías bloqueadas (usando las políticas personalizadas detalladas en la sección de filtrado de contenido). Por ejemplo, se permitiría sitios de productividad y educativos, pero se bloquearán contenido adulto, juegos de azar, P2P, hacking, etc., para estos usuarios. También **Application Control** se puede aplicar: bloqueando aplicaciones como clientes torrent, proxies VPN (Ultrasurf, etc.) y aplicaciones de streaming/video no deseadas, complementando el filtro web.

    - **Logging**: se activará registro de estas conexiones permitidas, al menos a nivel categoría, para auditoría y revisiones de uso de Internet.

    - **Reservas**: Si algún subgrupo necesita más libertad (ej. TI o Dirección), se crearán reglas separadas más arriba que les den excepciones .

3. **Regla 3 – Wi-Fi Estudiantes (VLAN 80 → WAN):** *"VLAN 80 hacia WAN, servicio Web (HTTP/HTTPS) – PERMITIR + QoS"*. **Objetivo:** Dar acceso Internet restringido a los estudiantes vía WiFi, evitando abusos de ancho de banda.

    - Permite **HTTP y HTTPS** (puertos 80 y 443) desde la VLAN80 hacia cualquier sitio externo. Posiblemente también **DNS** (53) si es que los clientes van a resolver contra DNS públicos; aunque probablemente los clientes usarán al firewall o DNS local para

resolver, en cuyo caso las consultas DNS ni salen por WAN. En cualquier caso, incluiremos DNS (UDP/TCP 53) en la regla por seguridad.

- **QoS:** Se aplicará una **política de Traffic Shaping**. Sophos permite definir un *"Limitador al segmento de red origen"*. Configuraremos una política de tipo. Esta política se asociará a la regla de estudiantes de forma que todo el rango de IP comparte el ancho de banda asignado de forma equitativa según la demanda. Esto garantiza equidad y previene saturación del canal.
- **AV/IPS/Web Filter:** Al igual que la regla 2, aquí también aplicaremos antivirus, IPS y filtrado de contenido. De hecho, posiblemente **más estricto** aún: por ejemplo, bloquear redes sociales excepto las permitidas académicamente, bloquear streaming de video pesado (YouTube quizá se permite, pero con educación; Netflix o TikTok podrían bloquearse para estudiantes). El perfil de **Web Policy** para estudiantes será más restrictivo, con categorías de "Distracciones" o "Social Media" bloqueadas, salvo aquellas necesarias para la labor académica. (E.g., podría permitirse YouTube como recurso educativo, pero restringir Facebook, Instagram durante horario lectivo, según la política de la institución).
- Esta regla tendrá NAT (masquerading) usando cualquiera de las IPs WAN disponibles según balanceo. El *logging* y reporte de actividad web de estudiantes será importante, y Sophos proporciona reportes por usuario/IP.

4. **Regla 4 – Wi-Fi Invitados (VLAN 90 → WAN):** *"VLAN 90 hacia WAN, HTTP/HTTPS*

   Objetivo: Dar a los **invitados** acceso limitado a web, aislándolos de la red interna y forzando un inicio de sesión/aceptación de términos.

   - Permitiremos solo tráfico **HTTP y HTTPS** desde VLAN90 hacia Internet. Todo lo demás (correo, pings, etc.) estará bloqueado, manteniendo esta red muy básica.
   - **Aislamiento:** Para asegurarlo, además de no tener reglas que permitan acceso interno (ver regla 5 abajo), en Sophos se puede marcar VLAN90 como zona "Guest" aislada. Si se usan APs Sophos, hay una opción de "Wireless Isolation". Con Unifi, se configura probablemente en la controladora. En cualquier caso, la capa 3 la manejamos denegando tráfico a LAN, así que está cubierto.
   - **Filtrado/Seguridad:** Aunque sean invitados, se aplicará un perfil de **Web Filter básico** (por ejemplo, bloquear pornografía, malware, etc., en cumplimiento de las leyes y evitar problemas legales). No tanto restricción de redes sociales porque invitados pueden necesitarlas, pero sí se bloquearán categorías ilícitas o peligrosas. También el antivirus inspeccionará sus descargas por si alguien trae algo malicioso – protegiendo así la red universitaria de potenciales amenazas que un invitado pudiera introducir.

6.2 Reglas de Aislamiento y Acceso Interno entre VLANs

Estas reglas controlan el tráfico *entre* las redes internas (LAN a LAN). Por defecto queremos **aislamiento**, con excepciones donde distintos segmentos necesiten comunicarse (por razones de servicios o administración).

5. **Regla 5 – Bloqueo Estudiantes/Invitados a recursos internos (VLAN 80,90 → Internal):** *"VLAN 80 y 90 hacia cualquier red interna – DENY & LOG"*. **Objetivo:** Asegurar que **estudiantes e invitados NO puedan acceder a ninguna red interna** o servidor de la institución.
    - Esto implementa aislamiento total: los orígenes en VLAN80 (WiFi estudiantes) o VLAN90 (invitados) tendrán denegado cualquier intento de conectar a IPs de las subredes 172.16.0.0/22 internas (podemos agrupar todas las redes locales en un alias "Internal_Networks").
    - La acción será *Deny* y con registro de logs para detectar si hay intentos anómalos (por ejemplo, alguien intentando escanear IPs internas desde la red de estudiantes).
    - Esta regla debe colocarse con prioridad alta (por encima de cualquier regla permitente) para que se aplique inmediatamente a cualquier tráfico hacia LAN.
    - Resultado: estudiantes e invitados **solo pueden ir a Internet**, cualquier paquete destinado a la LAN,… será descartado. Esto protege los sistemas administrativos y servidores de accesos no autorizados.
7. **Regla 6 – Bloqueo ICMP saliente (Any → WAN ICMP – DENY):** *"Cualquier red interna hacia WAN, ICMP – DENY"*.

8. **Objetivo:** Reducir la huella de red y **evitar fingerprinting**. Bloqueando ping/ICMP desde dentro hacia Internet, se dificulta que atacantes obtengan respuestas útiles y también evita que usuarios internos hagan ping a sitios externos (lo cual no es crítico, pero es una capa de silenciamiento).
    - Esta regla deniega solicitudes ICMP (tipo 8 echo-request principalmente) desde cualquier VLAN interna hacia cualquier destino externo.
    - Consecuencia: las estaciones no podrán "pingear" servidores en Internet. Esto no impacta servicios clave (navegación, etc.) pero puede entorpecer diagnósticos de usuarios. Es una decisión de seguridad: al no responder a PING, la red es menos detectable. Muchos entornos corporativos optan por bloquear ICMP hacia afuera precisamente para que no se muestren activos ante scans.
    - Importante: *Esto no bloquea respuestas ICMP de entrada relacionadas a tráfico válido* (por ejemplo, un destino enviando ICMP fragment needed o TTL expired). Sophos maneja eso internamente. Solo bloqueamos las peticiones iniciadas desde LAN.
    - Si TI necesita hacer ping para pruebas, siempre podrían hacerlo desde LAN (donde podría agregarse excepción) o temporalmente deshabilitar la regla. En general, se mantendrá bloqueado.
    - Se registrarán los intentos en log (para curiosidad, ver cuántos pings se hacen, aunque probablemente pocos).

9. **Regla 7 – Pantallas/Control de Acceso a Internet (VLAN 50,60 → WAN):** *"VLAN 50 y 60 hacia WAN, servicios NTP y HTTPS – PERMITIR"*.

10. **Objetivo:** Permitir a las **Pantallas interactivas (VLAN50)** y a los **controladores de acceso (VLAN60)** sincronizar hora y recibir actualizaciones firmware.
    - **NTP (UDP 123)**: se permitirá hacia servidores NTP públicos (por ejemplo pool.ntp.org) o quizás preferiblemente hacia el propio firewall que puede actuar como NTP relay. Simplificando, permitimos salidas NTP a cualquiera para que cada dispositivo tome de su servidor preferido.
    - **HTTPS (TCP 443)**: muchas pantallas inteligentes y controladores se actualizan o reportan vía HTTPS a servidores del fabricante. Permitimos este tráfico general a Internet.
    - No se permite navegación general ya que estos dispositivos no lo hacen (pero si alguien manipulare uno para navegar, se vería restringido a 443, lo cual usualmente va cifrado a dominios específicos).
    - Se podrían filtrar destinos por dominio si se supiera (ej: permitir solo *.manufacturer.com), pero eso requiere inspección DNS/SSL más compleja. En primera instancia, con AV/IPS activo, es suficiente.
    - Estas VLAN 50 y 60 tampoco necesitan acceder a recursos internos; de hecho, probablemente sus controladores (ej. un servidor central de control de acceso) esté en la LAN, en cuyo caso *sí habría que permitir* VLAN60 -> servidor control acceso en la LAN en puertos específicos (ej. si hay un software central que corre en un servidor Windows). Esto no está en la tabla, pero es lógico:
        - Si el controlador de acceso es un sistema servidor, podríamos tenerlo en VLAN10 con IP fija. Entonces las terminales de puertas en VLAN60 deben comunicar con él (posiblemente por HTTP/HTTPS o protocolos propietarios). De ser así, agregaremos una regla interna permitiéndolo. Lo mismo con pantallas si hay una controladora central de contenidos.

Las reglas 1-7 cubren tanto **acceso saliente** de las redes internas a Internet con sus restricciones, como el **bloqueo e interconexión interna mínima**.

- **VLAN25 (Biblioteca)**: es posible que necesite acceso a un **servidor Koha** o base de datos bibliotecaria en VLAN10. Permitir VLAN25 → Servidor Koha (puerto 80/443 o 8080 dependiendo, y base de datos si cliente pesado).
- **VLAN30-36 (Salas de clase)**: Estos usualmente no necesitan acceder a servidores internos aparte del DC (para autenticación si los PCs están en dominio) y algún servidor de licencias. Sugerimos permitir:
    - VLAN30-36 → DC (puertos AD básicos) para logon de usuarios.

- VLAN30-36 → Servidor de antivirus central (si hay), o servidor de actualizaciones WSUS si implementan updates locales.
- Si laboratorios utilizan algún servidor local (p.ej. uno de "prácticas y laboratorios" VLAN95?), permitirlo según caso.

- **VLAN95 (Prácticas)**: Podría tener uno o varios servidores experimentales. Aquí tal vez se aísla bastante, permitiendo solo Internet, a menos que se configure ad-hoc.

Para gestionar esto ordenadamente, crearemos **grupos de hosts/puertos**:

- Grupo "DomainControllers" con IPs de los DCs.
- Grupo "AD_Services" con puertos 88,389,636,445, etc.
- Regla: VLAN ANY (except estudiantes/invitados) → "DomainControllers", "AD_Services" – Allow. Así todos los equipos en dominio pueden autenticar. (O más estrictamente, enumerar solo LAN,21,25,30-36,95, pero se excluye 80/90).
- Similar con DNS interno: permitir consultas DNS de redes internas autorizadas hacia servidor DNS interno (y bloquear en otras).
- Impresoras: si impresoras están en la LAN via reservas, usuarios de VLAN30-36 quizá necesiten imprimir allí. Esto puede requerir permitir VLAN30-36 → LAN:9100 (RAW printing) a IPs de impresoras. O mejor, centralizar impresoras en la LAN. Se ajustará según topología real de impresión.

Firewall de capa 7 – Filtrado por aplicación/ contenido: Complementando las reglas de puertos, usaremos las capacidades de *Web Control y App Control* de Sophos:

- **Grupo Dirección/Profesionales:** Podrían tener políticas menos restrictivas (ellos podrían requerir YouTube para marketing, LinkedIn para networking profesional). Pero quizás se les bloquea P2P, descargas, y se limita uso de redes sociales más por productividad que por prohibición total. La matriz proporcionada sugiere que Dirección *no* debería usar Facebook/Instagram/TikTok/WhatsApp (marcados con X), pero *sí* YouTube y LinkedIn (marcados "SI"). Ajustaremos la política así.
- **Grupo Académico/Financiero/Docentes:** Parecido a Dirección, probablemente sin redes sociales (X en Facebook etc.), permitiendo YouTube/LinkedIn.
- **Grupo TI:** Aparece "SNIFER SI" en la tabla, lo que interpreto como que al personal de TI se le permite uso de herramientas de análisis (sniffer) y posiblemente P2P para pruebas, y se les da mayor libertad en general por su rol. A TI podríamos darle una política que no bloquee casi nada salvo sitios maliciosos obvios. Esto para que puedan realizar auditorías, descargar herramientas, etc. con confianza.
- **Grupo Estudiantes:** Muy restrictivo – bloquear P2P, descargas, redes sociales (X indica que estudiantes no deberían acceder a Facebook/Instagram/TikTok, pero quizás WhatsApp web permitido? En la tabla "Estudiantes: …X SI SI" no está totalmente clara, pero imagino que *no* a redes sociales salvo tal vez YouTube sí). Implementaremos que

estudiantes no puedan en general a redes sociales durante horario normal, enfocándose en contenido educativo.

- **Grupo Contratistas/Visitantes:** Contratistas (personal externo temporal) tal vez se les limita más que a personal interno. Visitantes se ve que "Facebook SI, Instagram NO, etc." – esto sugiere que invitados quizá pueden Facebook, ¿pero no YouTube? Habría que interpretar. Dado que invitados los tratamos ya en regla 4 con su propia web policy, podríamos simplemente aplicar una política general de "Bloquear sitios inapropiados (adulto, ilegal) pero permitir redes sociales" para no complicar su estancia.

- **Control de Aplicaciones (App Control):** Más allá del web HTTP/HTTPS, hay aplicaciones que usan otros puertos o técnicas (ej. WhatsApp como aplicación móvil usa puertos y puede no ser visto como "sitio web"). Sophos dispone de una base de datos de **firmas de aplicaciones** con categorías como P2P, Proxy, Mensajería, etc.. Configuraremos **políticas de Application Control** para reforzar:

  - Bloquear **P2P file sharing** apps (uTorrent, BitTorrent, eMule, etc.) en todas las redes salvo TI. La categoría *Peer-to-peer* abarca estos clientes. Esto complementa el bloqueo por puertos, ya que apps P2P a veces tunelizan por puertos web, pero la inspección DPI del firewall puede identificarlas y bloquearlas.

  - Bloquear **túneles/proxies** comunes (Tor, Psiphon, UltraSurf) para evitar que usuarios evadan filtros.

  - **WhatsApp:** Si se decide bloquear WhatsApp para ciertos grupos (p.ej. Contratistas NO, Visitantes NO, según tabla), se puede usar App Control para filtrar el tráfico de WhatsApp (que suele usar ports 5222 y 443 a servidores de WhatsApp). Sophos probablemente tiene firma para "WhatsApp" como aplicación de chat. Lo pondríamos en bloque para quienes no deben usarlo.

  - **Facebook/Instagram apps:** Igualmente, aunque se bloqueen vía Web, la app móvil podría usar API calls. App Control nos permite bloquear la categoría "Social Networking" en nivel aplicacion, reforzando el bloqueo de la versión web.

  - **Streaming Video**: Si se quisiera limitar, hay categoría "Streaming Media". Podríamos, por ejemplo, permitir YouTube pero bloquear Netflix/Disney+ para estudiantes (consumen mucho ancho de banda no educativo). Esto se logra especificando aplicaciones a bloquear.

  - Configuraremos distintos **Application Filter Policies** attachadas a las reglas de firewall por usuario: p.ej. la regla 2 (admin/academico) puede tener un app filter que bloquea P2P y proxies, la regla 3 (estudiantes) uno más estricto que incluye streaming, etc.

- **IPS y ATP:** Ya activado en reglas de salida, pero recordemos que con la licencia tenemos **ATP (Advanced Threat Protection)** global. La habilitaremos. Esto monitorea todas las conexiones salientes buscando indicadores de comunicación con servidores maliciosos conocidos (botnets, C2). Si detecta, loguea o bloquea según configuración. Es una capa transversal valiosa.

- Adicional, se puede activar **Country Blocking** si se desea evitar tráfico hacia/desde países no relacionados (pero hay que ser cauteloso de no romper servicios; lo mencionamos como posible pero no implementamos por defecto).

- **Security Heartbeat:** Dado que tendremos Intercept X en endpoints, aprovecharemos la función **Sophos Security Heartbeat**. En la práctica:
  - Configurar el XGS para que se registre en Sophos Central (donde también están los endpoints). Esto enlaza endpoints y firewall.
  - Definir reglas de aislamiento automáticas: por ejemplo, *si algún host tiene Heartbeat = rojo (comprometido)*, automáticamente bloquear su tráfico hacia cualquier red excepto Sophos Central. Se puede hacer con políticas de firewall condicionales por estado de heartbeat. Esto añadirá otra capa: un PC infectado es aislado antes de causar daño.
  - Ejemplo: Insertar al principio una regla: "Si Heartbeat = rojo (o falta) → denegar todo salvo a host de actualización de Sophos". Y "Si Heartbeat = amarillo → solo permitir mínima navegación, no a servers internos". Depende de la estrategia de respuesta deseada.
  - Esto es un plus que solo Sophos ofrece integradamente, y dado que se ha adquirido en Intercept X.

Reglas de acceso remoto (VPN): Más adelante detallamos la VPN, pero aquí mencionar:

- Se creará una regla permitiendo tráfico **VPN** a LAN: es decir, usuarios que se conecten vía SSL VPN terminan en la zona "VPN". Necesitamos una regla: "Zona VPN → Zona LAN/Internal – permitir según políticas de acceso de ese usuario". Probablemente personal TI o ciertas áreas tendrán acceso total, mientras otros VPN quizás solo a ciertos servidores. Esto se gestionará via permisos en la configuración de la VPN SSL (se puede limitar subredes accesibles por usuario).
- Y una regla complementaria de LAN → VPN si se requiere tráfico iniciando desde adentro hacia cliente (no usual en remoto, salvo administración push).

Regla final ANY-ANY Drop: Por defecto, el XGS ya bloquea todo lo no permitido. Sin embargo, es buena práctica tener una **última regla explícita** "Denegar todo lo demás" con *log habilitado* para ver tráfico inesperado. La pondremos (posición inferior), así cualquier cosa no contemplada será registrada en log (por ejemplo, si alguien intenta un puerto no autorizado, aparecerá en log final drop).

Con esto, las políticas de firewall cubrirán exhaustivamente los casos de uso previstos, garantizando tanto la **productividad** (permitiendo lo necesario) como la **seguridad** (bloqueando lo indebido).

7. Integración del Sistema Wi-Fi (UniFi WiFi 7 Pro) con el Firewall

La institución utiliza puntos de acceso **Ubiquiti UniFi WiFi 7 Pro** para sus redes inalámbricas. Aunque el controlador UniFi gestiona la configuración inalámbrica (SSID, autenticación, etc.), es crucial que el firewall Sophos interactúe correctamente con la infraestructura WiFi en términos de VLAN y seguridad:

- **Asignación de VLAN a SSID:** Ya se han definido VLAN específicas para cada tipo de WiFi: Administración (21), Auditorio (70), Estudiantes (80), Invitados (90). En la controladora UniFi (software de gestión), se configurarán los SSID de modo *Enterprise* con 802.1Q tagging hacia estas VLAN. Los AP UniFi estarán conectados a switches en puertos trunk que permiten estas VLAN, y la controladora asignará el tag según SSID del cliente. El firewall al recibir tráfico de dichas VLAN ya sabe a qué red pertenece y aplica la regla correspondiente.
- **Aislamiento Cliente a Cliente:** Especialmente en red invitados, conviene prevenir que los dispositivos se vean entre sí (por seguridad). Esto se puede lograr a nivel AP (Isolate clients) o firewall. En VLAN90, un invitado podría intentar acceder a otro invitado, lo que pasaría por el firewall (misma VLAN -> el switch, pero si es wifi, AP podría puentear localmente… mejor activar *Layer-2 isolation* en el AP). Recomiendo activar *"Guest Isolation"* en el SSID invitados en UniFi, así cada cliente solo ve gateway.
- **Performance WiFi 7:** Con enlaces de 1 Gbps, la WiFi 7 (que puede soportar >1 Gbps por cliente teórico) no será limitante a nivel firewall, pero tener muchas conexiones NAT concurrentes sí. El XGS 3300 es un equipo robusto, debe manejar cientos de usuarios concurrentes sin problema.

9. Filtrado de Contenido Web y Control por Grupos de Usuarios

Una de las piezas centrales de la política de uso aceptable de Internet en la universidad es el **filtrado de contenido web** por categorías, adaptado a cada grupo de usuarios. Basado en los requerimientos (matriz de grupos vs accesos) proporcionados, se implementará lo siguiente:

Categorías Web a filtrar: Sophos categoriza sitios web en decenas de categorías (educación, redes sociales, descargas, juegos, contenido adulto, etc.). De especial interés para nosotros:

- **Snifer/Hacking:** Sitios de herramientas de *hacking*, sniffer, keygen, etc. (Categoría *"Hacking"* en Sophos) – **Bloqueados para todos excepto TI**. El personal de TI puede necesitar visitar repositorios de seguridad o herramientas, así que se les permitirá con discreción. Para los demás, esta categoría se bloqueará, evitando que descarguen software peligroso o lean tutoriales maliciosos.
- **P2P/Sharing:** *"Peer-to-Peer & Torrents"* – Bloqueado para todos menos TI. No hay razón legítima para que estudiantes o administrativos usen BitTorrent en red institucional. El firewall bloqueará tanto las webs de trackers/torrents como el tráfico P2P de las aplicaciones. (Esto complementado con App Control mencionado asegura efectividad).
- **Descargas de archivos:** Esto incluye sitios tipo Mega, MediaFire, y repos de shareware. Sophos tiene categoría *"Download Freeware & Shareware"*. Podemos bloquearla para estudiantes para evitar que bajen software potencialmente no autorizado. Para personal académico/administrativo, quizás se deja acceso, pero monitoreado, ya que podrían necesitar descargar drivers u otros. Podríamos bloquear descargas grandes en estudiantes para preservar ancho de banda.
- **Redes Sociales:** La categoría general *"Social Networking"* cubre Facebook, Twitter, Instagram, TikTok, LinkedIn, etc.. Sin embargo, dado que deseamos matizar por tipo de red:

- **Facebook, Instagram, TikTok, WhatsApp:** Según la matriz, la mayoría de grupos internos (Dirección, Académico, Financiero, Docentes, Estudiantes) tienen "X" en estos, indicando que estarán **bloqueados** en horario normal. Excepto Mercadeo (Marketing) que por sus funciones de outreach requiere acceso, a ellos se les pondrá excepción para permitir estas redes. Contratistas e invitados tienen cierto acceso variable: se ve "Contratista: Facebook NO, Instagram NO, WhatsApp NO, YouTube NO, LinkedIn NO" (muy restringido) y "Visitantes: Facebook SI, Instagram NO, TikTok NO, WhatsApp SI, YouTube NO" – un poco inconsistente, pero tal vez se prioriza mensajería (WhatsApp) para visitantes y se bloquea video (YouTube) para no saturar. Trataremos de implementar:
    - Contratistas: Bloquear casi todo social y ocio, ya que deben usar red solo para trabajo específico.
    - Visitantes: Permitirles comunicarse (WhatsApp) y un poco de redes, pero quizás restringir streaming para no hoggear.
- **LinkedIn y YouTube:** Varios grupos tienen "SI" en estas columnas, sugiriendo que se **permitan**. LinkedIn se considera red profesional, útil para Dirección/Profesores. YouTube, si bien es ocio, también tiene valor educativo, así que parece se permite ampliamente salvo a quienes expresamente no (Auditorio y Monitoreo aparecen con NO en YouTube, tal vez para que no vean videos). Implementaremos: Dirección, Académico, etc. – YouTube permitido; Estudiantes – YouTube permitido (con monitoreo, porque bloquearlo totalmente puede ser contraproducente educativamente); Mercadeo – permitido; Monitoreo (guardas) – bloqueado para enfocarlos en su tarea.
- En Sophos, podemos manejar sub-categorías o directamente listas de sitios: por ejemplo, podríamos permitir YouTube pero bloquear otros streaming. Afortunadamente, Sophos tiene "Streaming Media" con subcategoría YouTube separable. Sino, se puede usar la categoría y luego excepciones por dominio.
- Para WhatsApp Web, es accesible via web.whatsapp.com (HTTPS). Si bloqueamos "Messaging" categoría, probablemente entra ahí. Debemos decidir: la matriz indica WhatsApp: Dirección X (bloq), pero TI SI, invitados SI, etc. Lo controlaremos via Application filter (WhatsApp as app) mejor, ya que su tráfico no es solo web.
- **Contenido adulto, apuestas, violencia, etc.:** Aunque no aparece explícito, por ser una institución educativa, es política estándar bloquear **pornografía, gambling (juegos de apuestas), sitios de odio/discriminación, drogas ilegales, etc.** para todos los usuarios. Sophos categoriza estos (Pornography, Gambling, Hate, Illicit Drugs...). Los bloquearemos en todas las políticas, incluso para TI (no hay justificación técnica para acceder ahí). Esto va sin excepciones.
- **Noticias, Streaming música, Deportes:** No mencionado, pero podríamos permitir en general salvo que se detecten abusos. El perfil podría ser flexible, pero si se necesita, se ajusta más tarde.

Implementación técnica en XGS:

- Crear una **Web Policy** por defecto (base) que bloquea categorías inaceptables universalmente (adulto, criminal, etc. – Sophos de hecho bloquea criminal/hacking aun si la policy dijera allow). Luego, añadir reglas en orden de prioridad para excepciones:

    1. Grupo Mercadeo: Permitir redes sociales (categoría Social Networking) – *Stop on match* (así que ellos saltan el bloqueo global).
    2. Grupo TI: Permitir todo salvo malicioso – esencialmente no aplicar restricciones de ocio – quizás ni necesiten una web policy si los eximimos.
    3. Grupo Dirección/Académico/Financiero/Docentes: Bloquear Social Networking (esto bloquearía Facebook, Insta, TikTok) pero añadimos excepciones para LinkedIn (que está en subcat "Business Networking", podríamos allow) y YouTube (subcat "Streaming Media/Video Sharing", se puede allow para ellos).
    4. Estudiantes: Bloquear Social Networking (posiblemente permitir YouTube), bloquear descargas P2P y shareware, etc.
    5. Contratistas: Muy restrictivo – podríamos assignarles una policy "Contratista" que bloquea todo salvo esenciales (correo, alguna web corporativa).
    6. Visitantes: Usan su propia web policy de invitados: permitir la mayoría (redes sociales principales) excepto contenido adulto/ilícito, para no sobre-regular al invitado, pero tampoco permitir abuso.

- **Keyword/URL overrides:** Sophos permite listas blancas o negras específicas. Podríamos cargar manualmente ciertos sitios si se requiere (ej. "allow sitio del ministerio educación" si caía en categoría rara). También bloquear dominios específicos problemáticos (ej. si detectamos estudiantes usando un proxy web específico, lo añadimos a bloqueados).
- **Notificaciones y Bypass:** Configuraremos la **página de bloqueo** con branding de la institución y un mensaje claro ("Este sitio está bloqueado por la política institucional"). Sophos también tiene *"Web Policy Override"* para administradores: podríamos dar capacidad a TI de liberar temporalmente el acceso a un sitio para un usuario bajo petición, pero eso se evalúa si hay demanda.
- **Reporte y Monitoreo:** Tras implementar el filtrado, el XGS generará **reportes detallados**: uso por categoría, top usuarios, intentos bloqueados, etc. Esto será útil para ajustar las políticas e identificar abuso. Por ejemplo, si vemos estudiantes intentando mucho acceder a ciertos sitios bloqueados, se puede reforzar la educación digital o revisar la necesidad.

En suma, el filtrado de contenido será granular y acorde a cada perfil, usando al máximo las capacidades de **Web Control por usuario/grupo y categoría del XGS**, garantizando un **uso adecuado de Internet** en la universidad, mejorando la concentración en labores académicas/administrativas y reduciendo riesgos de seguridad provenientes de sitios web maliciosos o inapropiados.

10. Sistema de Prevención de Intrusiones (IPS) y Protección Avanzada

El Sophos XGS 3300, gracias a la licencia Xstream Protection, incluye un potente **sistema IPS** de siguiente generación y otras medidas de protección avanzadas para blindar la red contra amenazas. Detalles de su configuración:

- **Perfil de IPS:** Se asignará un perfil de IPS a cada regla de firewall de salida relevante (reglas 2, 3, 4, 8 principalmente, que permiten tráfico a WAN). Podemos utilizar perfiles predefinidos de Sophos como *"LAN to WAN – Medium"* o crear uno personalizado. En un entorno universitario, priorizaremos detección de:
    - **Exploits web** en tráfico de navegación (por ej. filtrado de *malicious JavaScript, pharming*),
    - **Actividad de malware conocido** (por patrones en payloads),
    - **Intrusiones contra servidores internos**: aunque la mayor parte del tráfico es saliente, IPS también analiza respuestas entrantes. Ej: si un usuario descarga un PDF con exploit, IPS podría detectarlo en tránsito (además del AV).
    - **Ataques de red**: scans, flood, etc. (Algunos se mitigan con firewall rules ya).
    - Dado que tendremos WAF para servidores, allí vendrá su propio set de firmas específico HTTP.
    - IPS se actualiza automáticamente con firmas nuevas. Hay que agendar que el firewall tenga acceso a actualizaciones (lo hace periódicamente vía Sophos Central or directly).
- **Advanced Threat Protection (ATP):** Lo habilitaremos en **Security > Advanced Threat Protection** con acción "Drop" para conexiones a hosts maliciosos conocidos. Esto complementa IPS: ATP utiliza inteligencia de SophosLabs para bloquear tráfico hacia dominios o IP de command-and-control (C&C) o botnets. Si algún equipo interno infectado intenta comunicar con su servidor, el firewall lo bloqueará y alertará.
- **Security Heartbeat & Lateral Movement Protection:** Ya mencionado, pero cabe reiterar como protección avanzada. Al aislar endpoints comprometidos, previene la **propagación lateral** de malware dentro de la LAN. Activaremos la opción **"Prevent lateral movement"** para que si un host tiene heartbeat rojo, el firewall automáticamente bloquee *todo su tráfico local*, impidiendo que infecte a otros en distintas VLAN. Esto convierte al firewall en un guardián interno cuando Intercept X detecta algo.
- **TLS/SSL Inspection:** En la actualidad, gran parte del tráfico está cifrado (HTTPS). El XGS 3300 soporta **TLS Inspection** con aceleración (Xstream TLS Engine). Para maximizar la eficacia de IPS, AV y filtrado en tráfico HTTPS, consideramos habilitar la inspección SSL en modo *"Decrypt and Scan"* para categorías no sensibles.
    - En resumen, dejaremos TLS inspection en modo **"optimal"** (inspeccionar solo categorías de riesgo medio, ignorar banca/salud privacía). Esto nos da detección de amenazas en web sin excesivos falsos positivos y preservando privacidad en sitios sensibles.

- **Protección frente a Escaneo Externo:** Ya bloqueamos ping desde dentro. Para escaneos desde fuera (Internet hacia nosotros), el firewall por defecto descarta tráfico no solicitado, pero:
    - La zona WAN, *ningún servicio de administración responda* (excepto quizás ping a gateway si los ISP necesitan monitor, pero preferible tampoco). No expondremos interfaz web/ssh en WAN.
    - Configuraremos explícitamente que el firewall no responda a puertos no usados. Esto incluye asegurarnos de cambiar los puertos por defecto del User Portal y VPN si abrimos en WAN, para confundir a atacantes.
    -
- **WAF Protections:** Para completitud, los **WAF rules** creados (ver sección 11) tendrán perfiles de protección para las aplicaciones web: filtrado de inyección SQL, XSS, etc. Se usarán los perfiles genéricos o específicos (Sophos trae predefinidos para Outlook, Sharepoint, pero para Koha u otros pondríamos general o crearíamos uno personalizado ajustando signatures). Revisar los logs WAF con frecuencia al inicio para calibrar falsos positivos.

Actualizaciones y Parches: El firewall se mantendrá actualizado (firmware) para asegurar tener las últimas mejoras de rendimiento de Xstream DPI y parches de seguridad. Planificar actualizaciones en ventana apropiada (Sophos lanza updates cada poco mes).

Resumiendo, con IPS, ATP, Heartbeat, TLS inspection y WAF, disponemos de una **defensa en profundidad**. Muchas capas se solapan: si falla una, otra detecta. Por ejemplo, si un estudiante descarga una herramienta maliciosa:

11. Publicación Segura de Servidores Internos (WAF y NAT)

La institución cuenta con varios servidores internos (mencionados: Servidor de Dominio, Servidor Cvenet, KOHA, ZABIS, CGUNO, Firma Digital, etc.) y posiblemente nuevas aplicaciones web (Server Nuevo1/2). Algunos de estos servicios podrían requerir **acceso desde el exterior** (Internet), por ejemplo:

- Un sitio web institucional (público) alojado en un servidor web interno.
- La plataforma de biblioteca KOHA, para que estudiantes consulten catálogos desde casa.
- Aplicaciones académicas (Cvenet, Zabis) si ofrecen portales para estudiantes o docentes fuera del campus.
- Servicios de firma digital para trámites online.
- Acceso a la VPN SSL (para ello el firewall mismo hace de servidor).

Para exponer estos servicios de forma **segura**, aprovecharemos el módulo **Web Server Protection (WAF)** en lugar de simples NAT directos cuando se trate de aplicaciones web:

- **Web Application Firewall (Reverse Proxy):** Configuraremos **reglas WAF** para cada sitio web o servicio HTTP/HTTPS que deba ser accesible externamente. Por ejemplo, para publicar KOHA:

- **DNAT para otros servicios:** Si hay servicios que *no* son web pero requieren acceso público:
    - Ejemplo: un servidor de correo interno (SMTP), se haría una **Business Application Rule** (DNAT/Port Forward) del puerto 25/587 desde IP pública a la IP del mailserver, con protección SMTP si tuviéramos (sin modulo Email, se podría aplicar IPS mail sigs).
    - Como no se listó explícitamente, no profundizaremos, pero se dejará la nota: "Exponer otros servicios mediante NAT solo si imprescindible, preferir VPN para accesos administrativos remotos".
- **Demilitarized Zone (DMZ):** En este despliegue no se mencionó DMZ separada. Todos servidores están en la LAN (interna). Dado que los protegemos con WAF/NAT selectivo, está bien. En futuros crecimientos, se podría segregar servidores públicos en VLAN distinta (172.16.29.x por ej) para una DMZ, y firewall entre DMZ y LAN más restrictivo. Por ahora no es crítico.

Con estas medidas, los servicios institucionales estarán accesibles desde Internet de manera **controlada y segura**: el firewall actuará de guardián filtrando solicitudes maliciosas antes de que toquen los servidores, exponiendo solo los puertos necesarios y manteniendo todo lo demás cerrado. Esto reduce enormemente el riesgo de intrusión a través de los sistemas publicados.

12. Acceso Remoto mediante VPN

Para habilitar a personal autorizado el acceso a la red universitaria desde fuera (p. ej., administrativos trabajando desde casa, equipo de TI haciendo soporte remoto, profesores ingresando al sistema académico, etc.), configuraremos un servicio de **VPN de Acceso Remoto** en el Sophos XGS 3300. Optaremos por la solución **SSL VPN** de Sophos con el cliente *Sophos Connect*, dadas sus ventajas de seguridad y fácil integración con AD.

Configuración de SSL VPN (Remote Access):

- Utilizaremos el **Asistente de VPN SSL** del XGS para simplificar la configuración. Básicamente, definiremos:
    - Un **pool de direcciones IP** para clientes VPN (por ejemplo, 10.10.10.0/24, un rango no conflictivo con internos). Los clientes al conectarse recibirán una IP virtual de este pool.
    - **Permitir redes internas:** especificar qué subredes de la LAN se podrán acceder vía VPN. Podríamos permitir todas las necesarias (172.16.10.0/22 completo) para personal TI, pero quizás restringir a menos para otros usuarios. Sophos permite políticas distintas por usuario/grupo para VPN:
    - **Asignación Cliente:** Tras crear la política, los usuarios podrán descargar el perfil. ovpn desde el **Portal de Usuario** del firewall, o usaremos la nueva funcionalidad de **Sophos Connect provisioning**. Este portal estará disponible en la IP pública del firewall (podemos usar el IP principal).
- **Sophos Connect Client:** Se facilitará a los usuarios el cliente Sophos Connect (Windows/Mac). Este cliente soporta SSL VPN y es más user-friendly que el antiguo OpenVPN GUI. Pueden descargarlo del portal o se distribuye por TI.

- **Firewall Rules para VPN:** Por defecto, al crear la política SSL VPN, Sophos añade la regla de permisión correspondiente (VPN zone -> LAN zone). Revisaremos que exista y que esté arriba de la regla final drop. Esa regla permitirá a los IP pool de VPN acceder a las subredes LAN definidas.

En conclusión, la **VPN SSL para usuarios remotos** proporcionará un acceso seguro y cifrado a la red universitaria, utilizando credenciales de AD para autenticar y las políticas de firewall para autorizar. Esto aumenta la flexibilidad operativa (teletrabajo, soporte remoto) sin comprometer la seguridad, ya que todo el tráfico VPN pasa por el firewall como si el usuario estuviera local, aplicándose igualmente filtros y registros.

13. Monitoreo, Alertas y Administración Centralizada

Finalmente, para mantener esta infraestructura y políticas funcionando de forma óptima, se deben aprovechar las herramientas de **monitorización y administración** del Sophos XGS 3300:

- **Panel de Control (Dashboard):** El firewall ofrece en su GUI un panel con estadísticas en tiempo real: uso de CPU, memoria, sesiones activas, top aplicaciones, alertas, etc. El administrador debe revisarlo regularmente, especialmente al iniciar clases o eventos que incrementen tráfico, para detectar cuellos de botella o actividad inusual.
- **Reportes integrados:** Sophos XGS incluye una suite de reportes muy útil. Podremos ver:
    - **Reporte de navegación web:** quién navegó qué categorías, sitios más visitados, intentos bloqueados, etc. Útil para presentar a dirección un resumen mensual del cumplimiento de políticas (por ej: “Bloqueamos 500 intentos a redes sociales de estudiantes esta semana”).
    - **Reporte de aplicaciones:** qué aplicaciones están consumiendo ancho de banda (p.ej. YouTube 30%, Zoom 20% etc.), lo que ayuda a dimensionar y justificar ajustes (quizá permitir ciertas apps educativas que ahora se ven que usan mucho).
    - **Reporte de seguridad:** incidentes IPS/ATP (si bloqueamos tráfico a un botnet, eso sale aquí), endpoints aislados por Heartbeat, etc.
    - **Reporte VPN:** quién se conectó vía VPN y cuánto tiempo/datos usó, para controlar uso. Estos reportes se pueden programar para enviarse por correo a administradores en PDF, digamos semanalmente.
- **Sophos Central:** Dado que se tienen licencias Intercept X y posiblemente se use Sophos Central to manage endpoints, se puede optar por gestionar el firewall también desde **Sophos Central** (hay opción de registrar el XGS en el portal central). Esto permitiría:
    - Ver la firewall en la misma consola cloud que los endpoints.
    - Tener *reportería centralizada de múltiples firewalls* (no aplica si solo hay uno, pero útil si crece).
    - Aplicar políticas de grupo de firewalls (no en scope ahora).

  - Lo interesante: si se tiene **Sophos Central Firewall Reporting (CFR)** habilitado (Xstream includes 30-day reporting in Central), podemos consultar logs históricos más allá de la capacidad local del equipo y generar reportes custom.
  - También permite recibir **alertas push/email** desde Central para ciertos eventos críticos (link caído, IPS flood, etc.).

- **Notificaciones Email:** Configuraremos en el XGS un servidor SMTP (puede usar uno de los de Microsoft/Google si la U tiene, o el de Notificaciones de Sophos) para que envíe **alertas** al correo del administrador TI. Alertas típicas: enlace WAN caído/recuperado, falla de actualización, etc. Esto ayuda a atender incidentes de inmediato.
- **Logs externos:** Podría integrarse un servidor Syslog externo (por ej, si tienen Zabbix, Kiwi, etc.) para almacenar logs de firewall de largo plazo. Con Sophos Central quizá no es necesario, pero es una opción. Incluso se puede enviar logs a un SIEM si se tiene en la U.
- **Copias de seguridad de config:** Tras dejar todo funcionando, generaremos un backup de la configuración del firewall. Sophos permite subirlo a Sophos Central auto, o descargarlo. Guardar en sitio seguro. Programar backups automáticos tras cambios.
- **High Availability:** Se tiene un solo XGS 3300. Si se desea alta disponibilidad, se podría adquirir un segundo y ponerlos en cluster activo-pasivo. No está en el alcance actual, pero es bueno mencionarlo. Con backup config y procedimientos de recuperación se puede manejar la contingencia de falla (sabiendo tiempo de reposición).
- **Capacitación:** Como está contratado, aprovechar esa capacitación para que el personal de TI aprenda a ajustar políticas, interpretar logs, y mantener el dispositivo actualizado.

Con estas prácticas de monitoreo y administración, nos aseguramos de que la política de seguridad se mantiene efectiva y podemos adaptarnos rápidamente a nuevas necesidades o amenazas. También genera evidencia del cumplimiento de las directrices de uso de internet que la universidad pueda haber establecido.

14. Análisis de protocolos

El protocolo utilizado en la red de datos de Intenalco es TCP/IP IPV4 el cual se encuentra sementado en las siguientes redes:

VLAN	Segmento	Subred	Máscara	Puerta de Enlace
Lan	Red Lan	**172.16.0.0/22**	255.255.252.0	172.16.0.1
25	Biblioteca	**172.16.22.0 /25**	255.255.255.128	172.16.22.1
30	Sala 1	**172.16.22.128 /26**	255.255.255.192	172.16.22.129
31	Sala 2	**172.16.22.192 /27**	255.255.255.224	172.16.22.193

32	Sala 3	**172.16.22.224 /27**	255.255.255.224	172.16.22.225
33	Sala 4	**172.16.23.0 /27**	255.255.255.224	172.16.23.1
35	Sala 6	**172.16.23.64 /27**	255.255.255.224	172.16.23.65
20	Sala 5	**172.16.21.0 /27**	255.255.255.224	172.16.21.1
36	Sala 7	**172.16.23.96 /27**	255.255.255.224	172.16.23.97
37	Sala 8	**172.16.23.129/27**	255.255.255.224	172.16.23.130
70	Wi-Fi Auditorio - LAN	**172.16.26.0 /24**	255.255.255.0	172.16.26.1
80	Wi-Fi Estudiantes	**172.16.28.0 /22**	255.255.252.0	172.16.28.1
90	WIFI INVITADOS	**172.16.27.0 /25**	255.255.255.128	172.16.27.1

La red no presenta cuellos de botella y problemas de direccionamiento IP, pero es importante que equipos de trabajo como switch, router, equipos de trabajo tengan sus direcciones IP bien definidas y no sean reutilizadas en otros equipos para así tener un buen funcionamiento de los mismos.

No se evidencian problemas de rendimiento en la red local en cuanto a la conectividad, pero sí se observa que el canal de internet cuenta con dos conexiones dedicadas de 1000 Mbps cada una, proporcionadas por los proveedores Emcali y Mediacomerce. Ambas conexiones ofrecen un máximo de entre 900 y 930 Mbps, sumando un total de 1860 Mbps de canal dedicado. Adicionalmente, Claro proporciona una conexión de banda ancha con 300 Mbps de descarga y 150 Mbps de subida.

Teniendo en cuenta que un servicio de internet óptimo hoy en día se debe proyector la ampliación del canal de entre 2 y 3 Mbps para asegurar una conexión adecuada para videoconferencias, correos, redes sociales, trabajos de edición, entre otros, y que los funcionarios administrativos utilizan hasta 5 Mbps debido a sus diversas tareas, la institución ha decidido que el canal de Mediacomerce se destine a la red administrativa. Esta red conecta a los administrativos desde sus estaciones de trabajo (computadoras, tabletas, celulares, entre otros) y también incluye los servidores internos, cámaras de videovigilancia, telefonía IP, sistemas de control de acceso, entre otros. Este canal cuenta con 930 Mbps con una relación de reutilización de 1:1, lo que garantiza una conexión dedicada y eficiente.

Para garantizar la óptima productividad, se estima que cada usuario requiere entre 3 y 5 Mbps, dependiendo de las actividades que realicen. Promediando el ancho de banda, el número de usuarios o equipos que podrían acceder sería entre:

- 930 Mbps / 3 Mbps = 310 usuarios.

En el caso de que solo los usuarios estuvieran conectados a internet, pero considerando que diferentes aplicaciones, software y servidores también requieren conexión, se distribuye el ancho

de banda en un 60% para los usuarios y un 40% para los equipos que lo necesiten. Esto resultaría en:

- 60% de 930 Mbps = 558 Mbps para usuarios.
- 558 Mbps / 3 Mbps = 186 usuarios conectados.

La red administrativa cuenta con conexiones cableadas a los puntos de datos y conexión a la red vía Wifi. El Wifi administrativo puede asignar hasta 100 direcciones IP. Hay 75 puestos de trabajo conectados por cable y aproximadamente 30 portátiles conectados por Wifi para los docentes. Esta distribución es suficiente para el uso administrativo, siempre y cuando cada usuario se conecte con un solo dispositivo.

Sin embargo, se ha evidenciado que los funcionarios no solo utilizan sus puestos de trabajo, sino también sus dispositivos móviles, lo que podría sobrepasar la capacidad instalada de la red administrativa. Por lo tanto, es necesario controlar la cantidad de dispositivos conectados por cada funcionario para evitar sobrecargar la red. Por ejemplo, si cada funcionario utiliza su puesto de trabajo y además conecta su celular, se sobrepasaría la capacidad instalada.

Recomendación

- Controlar la conexión de dispositivos a la red administrativa de los funcionarios que solo se utilicen dispositivos que tienen o que hacen parte de la producción diaria de los funcionarios por ejemplo controlar la conexión de celulares, tabletas, portátiles cuando el funcionario cuenta ya con una conexión asignada esto se puede analizar con un sistema de validación de equipos de plataforma o Hotspot.
- Analizar el consumo que requiere el personal de audio visuales, diseño y redes sociales

El canal de Emcali cuenta con 930 Mbps con una relación de reutilización 1:1, permitiendo una conexión dedicada. La distribución del ancho de banda se realiza de la siguiente manera:

- Biblioteca: 60 Mbps, lo que permite 20 equipos (60 Mbps / 3 Mbps por equipo). Actualmente, la biblioteca cuenta con 18 equipos.
- Red de salas: 465 Mbps, lo que permite 155 conexiones (465 Mbps / 3 Mbps por equipo).
- Wifi para estudiantes: 405 Mbps, lo que permite 203 conexiones (405 Mbps / 2 Mbps por conexión), ya que los estudiantes solo realizan consultas por internet.

El canal de Claro, de 300 Mbps, se utiliza como respaldo en caso de caída de cualquiera de los canales de internet y mantiene activa la red de estudiantes, permitiendo aproximadamente 150 conexiones adicionales por Wifi Mbps / 2 Mbps por conexión).

La congelación de los proveedores de internet está balanceada de tal manera que, si un proveedor falla, el otro lo reemplaza. Aunque esto disminuye la utilidad del recurso, permite el funcionamiento continuo.

15. Recomendaciones

1. El personal de sistemas debe contar con equipo de mapeo de puntos y la herramienta requerida para brinda soporte en caso de falla.
2. Bloqueo del acceso de la red internet de Intenalco por software como Anydesk, TeamViewer,

entre otros

3. Realizar monitoreo constante del uso de aplicaciones estableciendo políticas y condiciones para su uso en (redes sociales, plataformas, etc.)
4. Verificar el ancho de banda entregado por el proveedor, certificando que este sea mínimo 930mgb
5. Crear un rango de IPS para los nuevos equipos, y manteniendo actualizado el cuadro de equipos conectados.
6. 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
7. Configurar conexiones seguras a través de VPN por externos a la red INTENALCO
8. En la red administrativa todos los equipos deben estar debidamente identificados, sobre todo los que acceden por wifi.
9. Es importante recalcar que el dispositivo se debe monitorear constantemente y actualizar a nuevas políticas personalizadas si es necesario debido a que día a día hay nuevas vulnerabilidades

16. Capacitación del personal

Se realizo la capacitación por parte del ingeniero Rubén Carrejo (experto y certificado por Sophos) al personal del TI de INTENALCO: Ing. Lucero Chamorro y el Ing. Jorge Luis Dorado, en lo referente a la administración, configuración del antivirus y operación e informes del firewall Sophos. Donde se revisarán todas las opciones con las que cuenta el equipo del presente el contrato.

La sesión duro 6 (seis) horas en sesiones de 2 horas por día, durante 3 días, en los cuales se abordaron diversos temas y se resolvieron las dudas e inquietudes planteadas por los participantes.

Durante la capacitación, se abordaron los siguientes temas clave:

10. **Informes de consumo de aplicaciones:** Cómo monitorear y analizar el uso de aplicaciones para optimizar el rendimiento y la gestión de recursos.
    Informes de ataques: Identificación y análisis de intentos de intrusión y actividades maliciosas para fortalecer la seguridad de la red.
11. **Políticas de acceso a aplicaciones web:** Implementación de controles para gestionar quién puede acceder a aplicaciones web y cómo se puede acceder a ellas.
12. **Bloqueo de puertos:** Técnicas y razones para cerrar puertos específicos en la red para prevenir accesos no autorizados y mejorar la seguridad.
13. **Creación de reglas y políticas de bloqueo**: esta opción permite crear en el firewall las reglas para permite el acceso o bloque de los diferentes tipos de paginas
14. **Enrutamiento de redes LAN con redes WAN:** menú que permite de las locales o LAN a las redes WAN o de acceso a internet.
15. **Configuración de conexiones seguras a través de VPN**. Esta opción permite las conexiones utilizando VPN para conexiones de acuerdo a los niveles de seguridad y generar conexiones seguras
16. **Configuración de calidad de servicio QoS:** Permite la Configuración de las redes para

garantizar la calidad del servicio.

17. **Asignación de IP estática por Host MAC**: Administración y manejo de direcciones IP por la dirección MAC de las tarjetas de red: Esta opción permite asignar de acuerdo a la mac de la tarjeta de red una dirección IP es decir que cada la MAC se detectada por firewall se le asigna la misma dirección IP automáticamente. Asignación de direcciones IP estáticas basadas en la dirección MAC de los dispositivos para una gestión red más estable
18. **Copia de seguridad y firmware:** Creación, restauración y Configuración de copias de seguridad del firewall. Permite la actualización del firewall, realizar copias de seguridad y restauración de las mismas.
19. **Visor de registros:** Opción que permite hacer el monitoreo y seguimiento de las actividades que suceden en el firewall generando filtros para establecer cambios o modificaciones que permitan un correcto funcionamiento.
20. Preguntas y resolución de inquietudes por parte los participantes.
21. Grabación de la capacitación que se realiza entrega a los participantes de la capacitación.
22. Configuracion y parametrización del antivirus en los endpoints.

17. Análisis de disponibilidad y redundancia

En el caso de la redundancia a los canales de internet la institución cuenta con el canal de Media -comerce se destine a la red administrativa. Esta red conecta a los administrativos desde sus estaciones (computadoras, tabletas, celulares, entre otros) y también incluye los servidores internos, cámaras de videovigilancia, telefonía IP, sistemas de control de acceso, entre otros. Este canal cuenta con 930 Mbps con una relación de reutilización de 1:1, lo que garantiza una conexión dedicada y eficiente.

Para garantizar la óptima productividad, se estima que cada usuario requiere entre 3 y 5 Mbps, dependiendo las actividades que realicen. Promediando el ancho de banda, el número de usuarios o equipos que podrían acceder sería entre:

- 930 Mbps / 3 Mbps = 310 usuarios.

En el caso de que solo los usuarios estuvieran conectados a internet, pero considerando que diferentes aplicaciones, software y servidores también requieren conexión, se distribuye el ancho de banda en un 60% para los usuarios y un 40% para los equipos que lo necesiten. Esto resultaría en:

- 60% de 930 Mbps = 558 Mbps para usuarios.
- 558 Mbps / 3 Mbps = 186 usuarios conectados.

El canal de Emcali cuenta con 930 Mbps con una relación de reutilización 1:1, permitiendo una conexión dedicada. La distribución del ancho de banda se realiza de la siguiente manera:

- Biblioteca: 60 Mbps, lo que permite 20 equipos (60 Mbps / 3 Mbps por equipo). Actualmente, la biblioteca cuenta con 18 equipos.
- Red de salas: 465 Mbps, lo que permite 155 conexiones (465 Mbps / 3 Mbps por equipo).
- Wifi para estudiantes: 405 Mbps, lo que permite 203 conexiones (405 Mbps / 2 Mbps por conexión), ya que los estudiantes solo realizan consultas por internet.

El canal de Claro, de 300 Mbps, se utiliza como respaldo en caso de caída de cualquiera de los canales de internet y mantiene activa la red de estudiantes, permitiendo aproximadamente 150 conexiones adicionales por Wifi Mbps / 2 Mbps por conexión).

La configuración de los proveedores de internet está balanceada de tal manera que, si un proveedor falla, el otro lo reemplaza. Para garantizar la continuidad del servicio. En caso de presentarse falla con cualquiera de los tres proveedores priorizando el que tiene mayor consumo de ancho de banda.

18. Optimización de la Configuración de red.

Se realizó la verificación de los dispositivos de red 1:1 iniciando por el firewall Sophos, switch, servidores, antenas.

Ubicación	Centros de cableado	Switch	Routers	APP	Servidores
Piso 1	3	7	0	5	1
Piso 2	1	1	0	3	0
Piso 3	1	1	0	3	0
Piso 4	9	11	3	5	5
Piso 5	2	5	0	4	0
TOTAL	16	25	3	20	6

Se evidenció que los dispositivos se encontraban con sus firewalls desactualizados, los cuales fueron actualizados a la última versión del fabricante. También se realizó una revisión de la configuración de cada uno de los puertos de los equipos y de las VLAN que debían pasar por ellos, configurándolos de forma correcta.

19. Análisis de calidad límites de internet QOS (Red LAN, VLAN)

El firewall Sophos no contaba con la Configuracion de calidad QoS, por lo tanto se distribuyó de la siguiente manera:

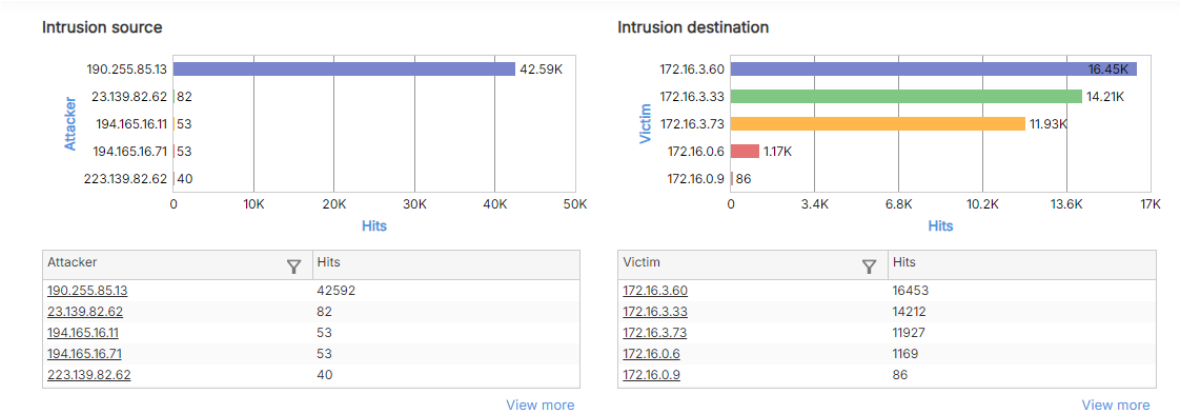
Red administrativa (LAN) se creó la política QoS donde se estableció el ancho de banda mínimo de 400mbps y máximo 900mbps, esta red se asignó mediante Mediacommerce.

Para las redes de salas (Vlan 30-36) y biblioteca (Vlan 25), se asignó un ancho de banda mínimo de 300mbps y máximo de 500mbps, garantizando internet para todos los equipos de sala a través del proveedor Emcali

La red wifi auditorio, estudiantes e invitados (Vlan 70, 80 y 90), se estableció un ancho de banda de mínimo 200mbps y máximo de 400mbps garantizando internet para todos los equipos de sala a través del proveedor Emcali.

20. Revisión firewall

Se realizo la revisión del firewall para verificar posibles ataques en la infraestructura de Intenalco en el año 2025, desde del primero de agosto hasta la fecha actual, el sistema reporta un total de 42mil intentos de ataque, de los cuales principalmente se muestran provenientes de las siguientes direcciones. (Se suministra evidencia fotográfica) el cual es un porcentaje muy alto teniendo en cuenta que solo fue en el transcurso de 2 meses. Es importante realizar la velicación de este tipo de instrucciones en firewall el cual se encuentra configurado para repelerlas a través de la herramienta web server protección de Sophos el cual cancela el posible ataque evitando la penetración a la red.



Attacker	Hits
190.255.85.13	42592
23.139.82.62	82
194.165.16.11	53
194.165.16.71	53
223.139.82.62	40

View more

Victim	Hits
172.16.3.60	16453
172.16.3.33	14212
172.16.3.73	11927
172.16.0.6	1169
172.16.0.9	86

View more

21.Monitoreo de la red de datos

Para el monitoreo de la red de datos, la institución actualmente solo cuenta con los informes proporcionados por el firewall Sophos, el cual permite supervisar aplicaciones, amenazas, tráfico de red y accesos a la misma. Esto se realiza a través de la opción de "Informes y Bloqueos", que genera información confiable y eficiente para la toma de decisiones y medición de datos.

Sin embargo, Intenalco no cuenta con software con licencia específica para el monitoreo de red, por lo que se ha procedido a la instalación de los siguientes programas en el servidor principal:

- **IP Scanner Advanced**: Permite monitorear los equipos conectados a las redes que se analicen.
- **IP Port Scanner**: Realiza el escaneo de puertos en una red específica, útil para identificar vulnerabilidades o puertos abiertos en los distintos dispositivos conectados.
- **Wireshark**: Es una herramienta de análisis de protocolos de red que permite capturar y examinar, en tiempo real, los datos que circulan por la red. Es muy útil para diagnosticar problemas, analizar tráfico y comprender cómo se comunican los dispositivos. A través de su interfaz gráfica, permite observar detalles de cada paquete, filtrar información y realizar análisis detallados de la actividad en la red.

22. Evaluación de la arquitectura de red

Se han establecido políticas de seguridad tanto para la red LAN como para la red WAN, incluyendo restricciones de acceso a la red local. Además, se ha limitado el uso de software de acceso remoto como **TeamViewer**, **AnyDesk**, **AnyViewer**, entre otros. Las conexiones que se realizan a través de la red WAN se hacen mediante VPN, con el fin de garantizar una mayor seguridad. El firewall protege contra intentos de intrusión y ciberataques, ofreciendo un sistema de defensa robusto para la información institucional.

Es fundamental mantener un monitoreo constante frente a posibles ataques desde el exterior y dentro de la red local. Se deben analizar los puertos abiertos y restringir aquellos innecesarios para reducir riesgos. La red se encuentra segmentada en VLANs independientes, lo que impide que estudiantes y visitantes accedan a la red administrativa, así como a las salas de cómputo y a los recursos de la biblioteca.

No obstante, se ha identificado una vulnerabilidad en la red administrativa, ya que esta tiene acceso directo a los equipos activos de la infraestructura de Intenalco. Los usuarios suelen validarse con una única contraseña, la cual es compartida en múltiples ocasiones, lo que representa un riesgo de seguridad.

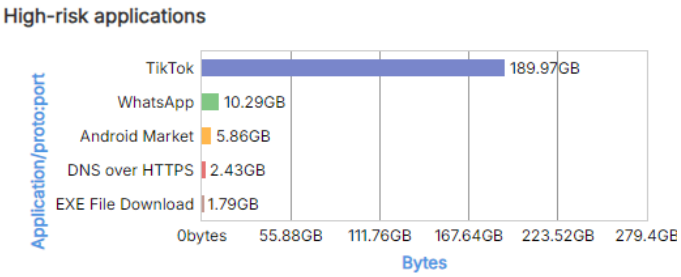
Es necesario establecer mecanismos de validación individual mediante usuarios restringidos y contraseñas únicas para el acceso a la red administrativa vía WiFi o DHCP. Por ejemplo, si a un funcionario administrativo se le asigna un portátil, también debe recibir un usuario y contraseña específicos para la red WiFi, y registrar la IP asociada a su equipo, de modo que se pueda identificar al responsable en caso de una eventualidad.

El uso compartido de contraseñas puede permitir a personas no autorizadas acceder a la red administrativa y ejecutar programas que comprometan la seguridad institucional. Para mitigar este riesgo, se propone asignar direcciones IP vinculadas a la dirección MAC de cada equipo. Durante un escaneo de la red, se detectó que tanto funcionarios administrativos como personas externas están conectadas a través del WiFi, lo que compromete la seguridad.

Por tanto, es indispensable identificar a cada funcionario o equipo que se conecte a la red administrativa, ya que es esta la red que resulta más atractiva para usuarios externos no autorizados.

23. Análisis de banda

De acuerdo con la revisión realizada en el firewall Sophos, y al verificar el consumo de las aplicaciones más utilizadas desde el 1 de agosto hasta la fecha actual se evidencian los siguientes resultados:



Application/pro...	Risk	Hits	Bytes
TikTok	4	939841	189.97 GB
WhatsApp	4	336184	10.29 GB
Android Market	4	262815	5.86 GB
DNS over HTTPS	5	154775	2.43 GB
EXE File Downl...	4	181	1.79 GB

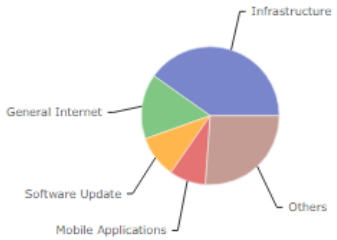
Aplicaciones	Descripción	Consumo
Tiktok	análisis de 1 agosto hasta la fecha	189.97 gb
Whatsapp	análisis de 1 agosto hasta la fecha	10.29 gb
Tiendas de aplicaciones (AppStore y Play Store Android)	análisis de 1 agosto hasta la fecha	5.86 gb
Peticiones a paginas web (HTTPS)	análisis de 1 agosto hasta la fecha	2.43 gb
Descarga de aplicaciones ejecutables en Windows .Exe	análisis de 1 agosto hasta la fecha	1.79 gb

La información anterior monitorear en la sección de informes de Sophos aplicaciones y web

Como se puede notar el consumo de internet en redes sociales es alto en la fecha actual el consumo es muy alto a pesar de que se realizaron los respectivos bloques de aplicativos al nivel estudiantil como: Instagram, Facebook, tiktok, YouTube, por lo tanto se puede concluir que este alto consumo en la plataforma Tiktok es proveniente de la parte administrativa.

Es importante establecer un procedimiento de actualizaciones de windows o desactivar las mismas con el fin de hacerlas programadas verificando cuales son utiles y cuales pueden causar problemas en la red de datos.

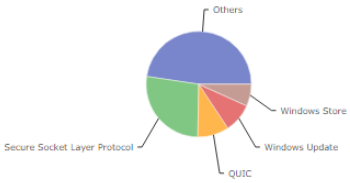
Application categories



Category	Bytes	Percent
Infrastructure	2.35 TB	40.2 %
General Internet	912.68 GB	15.23 %
Software Update	592.84 GB	9.9 %
Mobile Applications	512.31 GB	8.55 %
Others	1.53 TB	26.11 %

Categorías	Descripción	Consumo
Infraestructura	1 agosto hasta la fecha	2.35 tb
Internet general	1 agosto hasta la fecha	912.68gb
Actualización de software	1 agosto hasta la fecha	592.84 gb
Aplicaciones Móviles	1 agosto hasta la fecha	512.31 gb

Applications



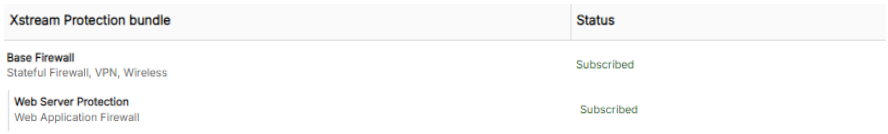
Application/pr...	Category	Risk	Bytes	Percent
Others	Unclassified	?	2.79 TB	46.93 %
Secure Socke...	Infrastructure	1	1.58 TB	27.05 %
QUIC	Infrastructure	1	576.41 GB	9.62 %
Windows Upd...	Software Upd...	3	535.95 GB	8.95 %
Windows Store	General Internet	1	402.51 GB	6.72 %

24.Auditoria de politicas de seguridad.

Se realizó la revisión de las políticas de seguridad tal como se indica en el punto 6 del presente informe y se ajustaron de acuerdo a los requerimientos. Es importante recalcar que el dispositivo se debe monitorear constantemente y actualizar a nuevas políticas personalizadas si es necesario debido a que día a día hay nuevas vulnerabilidades

25. Configuración de Firewall

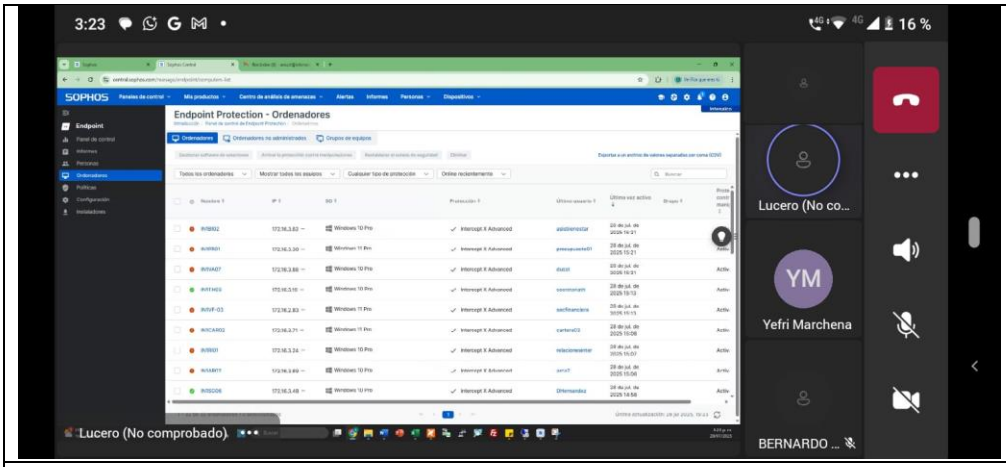
Product	License Number	License Key
XGS 3300 Xstream Protection - 12 MOS - EDU (SKU: XS330012ZZNEAA Old SKU:)	LN1001566846	LKN3BEH-V98-T6KGCX7J6
XGS 3300 Webserver Protection - 12 MOS - EDU (SKU: SS330012ZZNEAA Old SKU:)	LN1001566847	LKN8AK3-ZFD-R2QCDRDA1

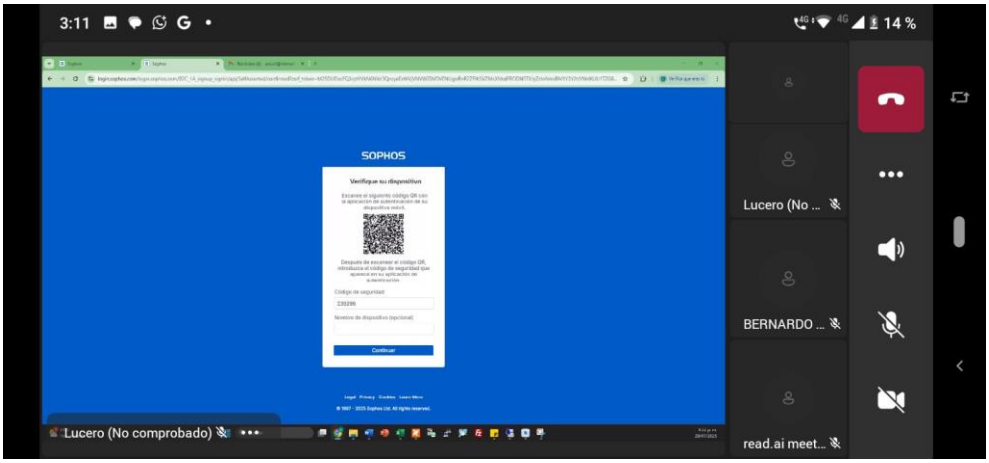


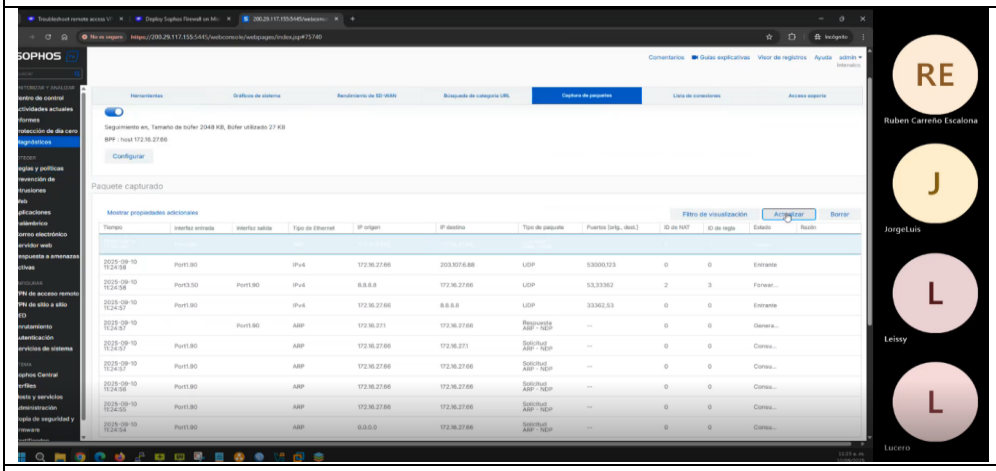
26. Sugerencias: De acuerdo al diagnóstico realizado a la red de datos se sugiere lo siguiente:

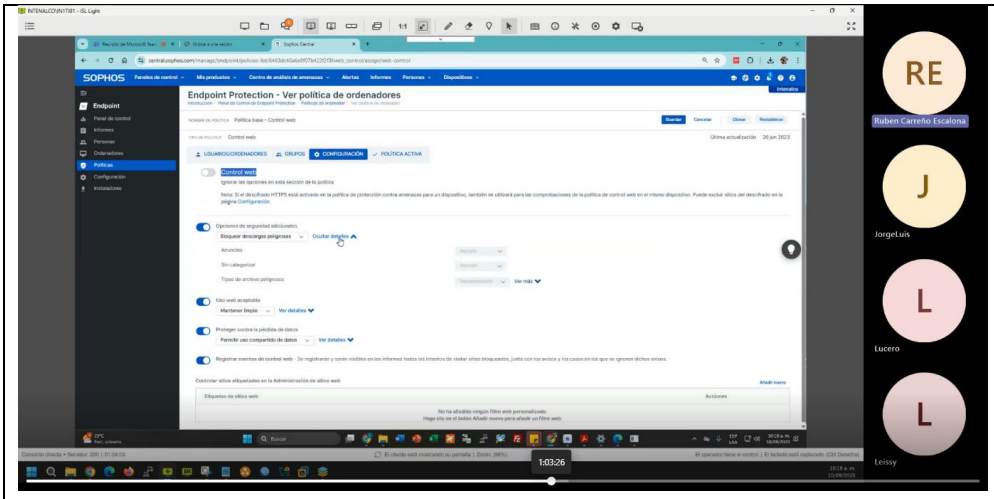
1. Deshabilitar la conexión de software de acceso remoto como: Anydesk, Teamviewer, RealVNC, Getscreen.me, AnyViewer.
2. Asignar direcciones DHCP por Mac para tener control de quipos existentes de la red.
3. Realizar monitoreo constante en el firewall por opción de visor de registros.
4. Realizar el seguimiento en el firewall en el menú de informe aplicaciones y de acuerdo al consumo habilitar o restringir el consumo de las mismas.
5. Realizar mantenimiento a la infraestructura de la red de datos como: Switch, servidores, etc. Cada año para alargar la vida útil de los mismos.
6. Verificar continuamente el enrutamiento de las redes LAN Y WAN
7. Verificar el trafico en el firewall de paquetes
8. Actualizar el software de sistema operativo de los servidores existentes
9. Actualizar firewall de los equipos activos existentes
10. Verificar las politicas y actualizarlas según sus necesidades
11. Verificar continuamente el Sophos si se presentan ataques desde que ciudad o país y crear reglas para disminuir dichos ataques.
12. Monitorear los puertos abiertos en la red de datos y restringir el acceso desde la red wan de los puertos como: puerto 80,443,8080,8443: htp, 20-21 FTP, 22 SSH, SMB 139,137,445, DNS 53, TELNET 23, SMTP
    25, TFTP 69.

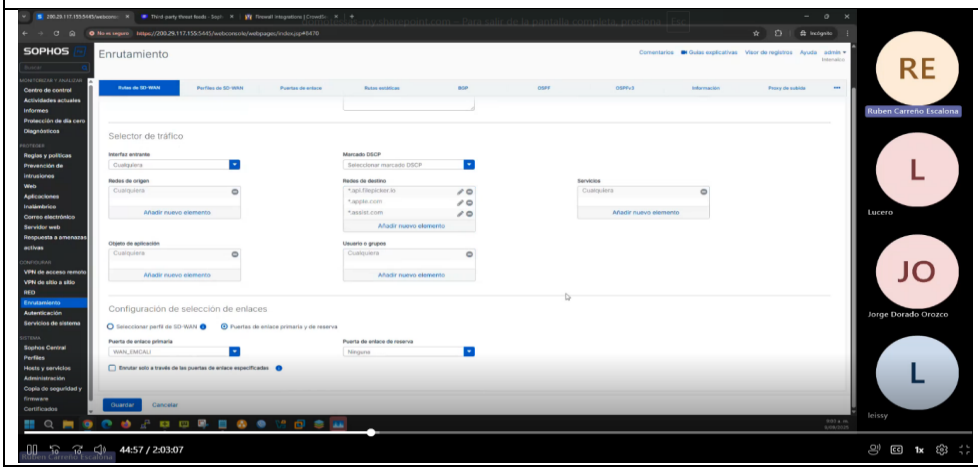
A continuación, se anexa evidencia de las reuniones virtuales donde se realizaron los procesos de configuración y de capacitación de manera remota. Al correo electrónico de la Supervición se realiza la entrega de los videos de los mismos para su consulta y descarga.


3:23
16 %
Endpoint Protection - Ordenadores
Lucero (No co...
YM
Yefri Marchena
BERNARDO ...
Lucero (No comprobado)


3:11
14 %
SOPHOS
Lucero (No ...
BERNARDO ...
Lucero (No comprobado)
read.ai meet...


RE
Ruben Carreño Escalona
J
JorgeLuis
L
Leissy
L
Lucero





Para finalizar, de acuerdo a lo estipulado en el Contrato de Suministros No. 200.17.001-INT-SEL-ABR–2025, celebrado entre el Instituto Técnico Nacional de Comercio Simón Rodríguez y PYMES ON LINE S.A.S., se deja constancia de la entrega a satisfacción de las obligaciones contractuales, asegurando que el equipo suministrado cumple con las condiciones técnicas, de calidad y funcionalidad requeridas, quedando a disposición de la entidad para su uso y administración. Se coordinó con la supervisora del contrato, la asistencia para certificación presencial de la marca Sophos para las fechas del 21 al 24 de octubre 2025.

Atentamente.

Bernardo Saavedra Gutiérrez
Representante Legal
Pymes On Line
Nit 900.440.998-7
bernardo@pymesonline.co

Recibe:_____
Lucero Chamorro Serna
Supervisor
INTENALCO