RYF S.A.S
Consultoría, Auditoría e Interventoría

ACTA DE REUNIÓN No. 12

RESPONSABLE DE LA REUNIÓN: Carolina Romero **(En caso de ser presencial):**

FECHA: 26 de noviembre 2025 **VIRTUAL:** **PRESENCIAL: X** **LUGAR: Hospital Cardiovascular de Cundinamarca**

OBJETIVO DE LA REUNIÓN: Auditoría de Redes y Conectividad

HORA DE INICIO: 9_00 am **HORA DE FINALIZACIÓN: __12:00 am**

ASISTENTES:

NOMBRE	ENTIDAD o DEPENDENCIA	CARGO	CORREO ELECTRÓNICO	TELÉFONO	FIRMA
Andrés Cruz	Hospital Cardiovascular de Cundinamarca	Coordinador Sistemas	sistemas@hccsa.com.co	3209795384	
Carolina Romero	RYF SAS	Interventor TI	Trabajo.interventoria@gmial.com	3184050702	

1. TEMAS A TRATAR

a) Inventario
b) Conectividad y soporte
c) Configuración
d) Wifi
e) Monitoreo
f) Políticas de Seguridad

2. DESARROLLO DE LA REUNION O DESCRIPCION DE ACTIVIDADES REALIZADAS

a) Inventario

En atención a la información suministrada por el Hospital Cardiovascular, se realizó la verificación del inventario de equipos de red (switches) instalados en las diferentes áreas del hospital, incluyendo Data Center, Data Center Principal, Farmacia, UCI Pediátrica, Banco de Sangre, Rayos X y otras dependencias operativas.
A partir del archivo entregado, se identificó un total de 28 switches distribuidos en los distintos pisos y zonas del hospital. El inventario presenta información básica relativa a la ubicación, tipo de equipo y número de placa, lo cual permite contar con una visibilidad general de la infraestructura de conectividad actualmente en operación.
No obstante, durante la revisión se evidenció que el inventario puede ser fortalecido para mejorar su precisión y utilidad en actividades de mantenimiento, soporte y continuidad del servicio. En particular, se observaron las siguientes oportunidades de mejora:

- Marca y modelo de los switches: El inventario no especifica el modelo exacto de los equipos (por ejemplo, Dell N2048, HP 2920, 3Com 2928, etc.), lo cual es relevante para procesos de soporte técnico, reemplazo de equipos o compatibilidad de configuraciones.
- Administración: No se indica si los switches son administrables o no. Esta información es clave para determinar si se pueden realizar configuraciones avanzadas como VLAN, copias de seguridad, monitoreo o aplicación de políticas de seguridad.
- Identificación de activos: Algunos registros presentan la anotación "NO APLICA" en el campo de placa o identificador, lo cual limita la trazabilidad. En estos casos se recomienda asignar un código interno TI para mantener la consistencia del inventario.
- Observaciones repetidas: La columna de observaciones presenta la misma descripción en la mayoría de los registros, sin información sobre estado, criticidad o si el equipo requiere revisión específica.
- Información complementaria: El inventario no incluye datos adicionales como estado operativo, número de puertos, fecha de instalación, ni disponibilidad de copias de respaldo de configuración, elementos que mejorarían significativamente la gestión del ciclo de vida de los equipos.
- Es importante señalar que las observaciones anteriores no afectan directamente la operación actual, pero sí representan oportunidades de mejora que pueden implementarse de forma gradual y sin afectar la carga operativa del personal de TI.

Recomendación
Se recomienda complementar progresivamente el inventario existente incorporando información como marca/modelo, administración, estado del equipo, identificación interna y si cuenta con respaldo de configuración. Estas mejoras no requieren una reconstrucción total del inventario, sino únicamente enriquecer la estructura actual para optimizar la gestión de la infraestructura de red.

Piso	Ubicación	Tipo	Placa	Observaciones
2	HOSPITAL CARDIOVASCULAR	RED DE SWITCHS Y EQUIPOS WIFI	7227	U.T. HOSPITAL CARDIOVASCULAR DEL NIÑO DE CUNDINAMARCA
6	DATA CENTER	SWITCH DELL	5551	HOSPITAL CARDIOVASCULAR DE CUNDINAMARCA S A
6	DATA CENTER	SWITCH DELL	6246	HOSPITAL CARDIOVASCULAR DE CUNDINAMARCA S A
6	DATA CENTER	SWITCH CENTRA UCI P	NO APLICA	HOSPITAL CARDIOVASCULAR DE CUNDINAMARCA S A
5	DATA CENTER	SWITCH DELL	5553	HOSPITAL CARDIOVASCULAR DE CUNDINAMARCA S A
4	DATA CENTER	SWITCH DELL	5552	HOSPITAL CARDIOVASCULAR DE CUNDINAMARCA S A
3	DATA CENTER	SWITCH DELL	5547	HOSPITAL CARDIOVASCULAR DE CUNDINAMARCA S A
2	DATA CENTER	SWITCH DELL	5545	HOSPITAL CARDIOVASCULAR DE CUNDINAMARCA S A
2	DATA CENTER	SWITCH DELL	5557	HOSPITAL CARDIOVASCULAR DE CUNDINAMARCA S A
2	DATA CENTER	SWITCH DELL	5540	HOSPITAL CARDIOVASCULAR DE CUNDINAMARCA S A
1	DATA CENTER PRINCIPAL	SWITCH DELL CORE	NO APLICA	HOSPITAL CARDIOVASCULAR DE CUNDINAMARCA S A
1	DATA CENTER PRINCIPAL	SWITCH DELL	5544	HOSPITAL CARDIOVASCULAR DE CUNDINAMARCA S A
1	DATA CENTER PRINCIPAL	SWITCH DELL	6247	HOSPITAL CARDIOVASCULAR DE CUNDINAMARCA S A
1	DATA CENTER PRINCIPAL	SWITCH HP	NO APLICA	HOSPITAL CARDIOVASCULAR DE CUNDINAMARCA S A
1	DATA CENTER PRINCIPAL	SWITCH CONSOLE - IBM	NO APLICA	HOSPITAL CARDIOVASCULAR DE CUNDINAMARCA S A
0	DATA CENTER	SWITCH DELL	6249	HOSPITAL CARDIOVASCULAR DE CUNDINAMARCA S A
0	DATA CENTER	SWITCH DELL	5546	HOSPITAL CARDIOVASCULAR DE CUNDINAMARCA S A
0	DATA CENTER	SWITCH DELL	6250	HOSPITAL CARDIOVASCULAR DE CUNDINAMARCA S A
1	BANCO DE SANGRE	SWITCH 3COM		HOSPITAL CARDIOVASCULAR DE CUNDINAMARCA S A
1	RAYOS X	SWITCH DELL	NO APLICA	HOSPITAL CARDIOVASCULAR DE CUNDINAMARCA S A
1	DATA CENTER FARMACIA	SWITCH DELL	5556	HOSPITAL CARDIOVASCULAR DE CUNDINAMARCA S A
1	DATA CENTER FARMACIA	SWITCH DELL	5541	HOSPITAL CARDIOVASCULAR DE CUNDINAMARCA S A
1	DATA CENTER FARMACIA	SWITCH DELL	5542	HOSPITAL CARDIOVASCULAR DE CUNDINAMARCA S A

Hallazgo

Ausencia de documento que relacione los switches con los servicios que soportan

Si bien el inventario suministrado por el hospital sí incluye la ubicación física de los 23 switches instalados, no se cuenta con un documento técnico que identifique qué servicios, áreas o procesos asistenciales dependen de cada uno de estos equipos.

Esta información resulta fundamental para la atención de incidentes, continuidad del servicio, priorización de fallas y planeación de mantenimientos, dado que un switch puede soportar simultáneamente varios servicios críticos (por ejemplo, urgencias, admisiones, rayos X, hospitalización, etc.).

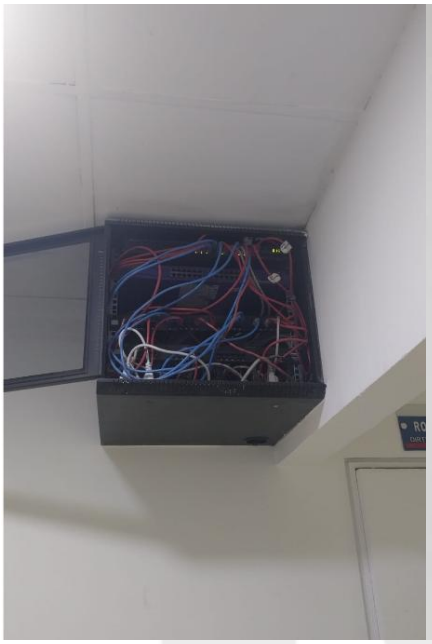
Durante la revisión física se observaron situaciones relevantes:

- Switch de urgencias: El switch ubicado en urgencias (24 puertos) se encuentra en un gabinete sin llave y con acceso directo desde pasillos del hospital. Este equipo soporta servicios de admisiones y rayos X, según la verificación realizada en sitio, pero dicha relación no está documentada formalmente.
- Centro de Telecomunicaciones, Primer piso: En el rack del primer piso se identificó un alto número de conexiones sin orden, sin etiquetado y sin una matriz que permita vincular puertos con áreas específicas del hospital. Esto incrementa los tiempos de diagnóstico y la probabilidad de errores de intervención.

Riesgos asociados

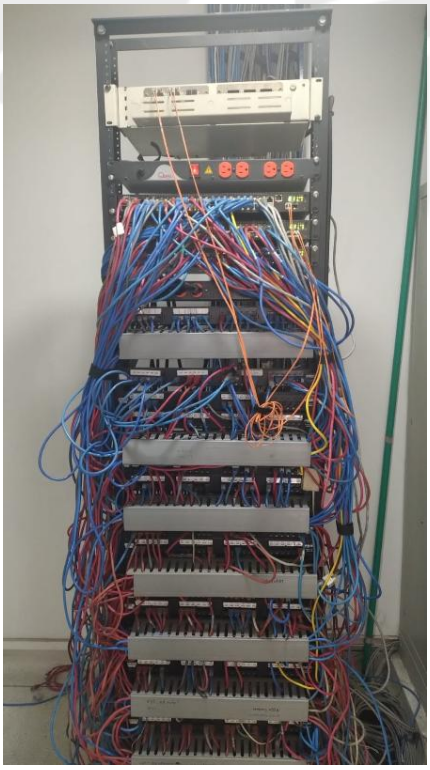
- Baja trazabilidad en incidentes de red al no saber qué áreas se afectan ante la caída de un switch.
- Mayor tiempo de respuesta en fallas críticas, especialmente en servicios asistenciales.
- Dependencia del conocimiento empírico del personal, sin soporte documental.
- Pérdida de continuidad del servicio por dificultad para identificar puertos y dependencias.

SWICHT DE 24 PUERTOS UBICADOS EN PASILLO DE URGENCIAS Y RADIOLOGÍA





CENTRO DE TELECOMUNICACIONES PRIMER PISO



Recomendación
Se recomienda elaborar un Documento de Trazabilidad de Red / Mapa de Dependencias de Switches, que incluya:

- Switch Servicios que soporta (urgencias, admisiones, imágenes, UCI, laboratorio, etc.).
- Identificación de puertos utilizados por cada dependencia.
- Fotografía de referencia del gabinete o rack.
- Señalización y etiquetado del cableado.
- Registro formal como parte del “Inventario de Infraestructura de Red”.
- Este documento permitirá mejorar la continuidad operativa, optimizar la atención de incidentes y fortalecer el control sobre la infraestructura de conectividad.

b) Conectividad

Oportunidad de mejora

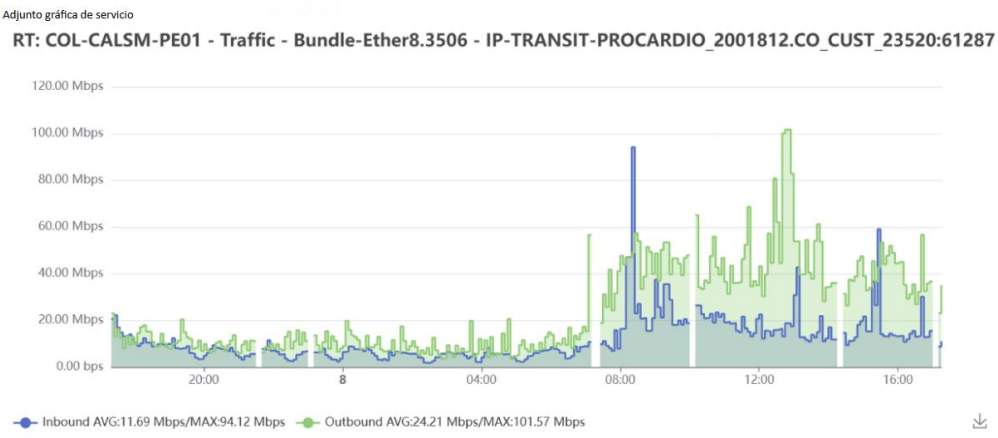
Durante la verificación del servicio de conectividad del Hospital Cardiovascular se identificó que el proveedor actual del enlace de Internet es Liberty Network, con operación directa a cargo de UNE. En las visitas realizadas y en la documentación suministrada por el área de TI, no se evidenció la existencia de informes técnicos mensuales, reportes de desempeño o entregables formales por parte del proveedor que permitan evaluar de manera sistemática el comportamiento del servicio.

La validación de la estabilidad del enlace se realiza principalmente mediante consultas puntuales en sitio, revisando el estado del servicio a través de pantallazos o pruebas de conectividad básicas. Si bien estas verificaciones permiten confirmar la disponibilidad en el momento de la revisión, no constituyen un mecanismo que permita medir tendencias, identificar degradaciones, registrar eventos de indisponibilidad o hacer seguimiento a incidentes reportados al proveedor.

Así mismo, no se observaron reportes formales de tiempos de indisponibilidad, ventanas de mantenimiento, incidentes solucionados, ni niveles de servicio (SLA) asociados al contrato vigente. La ausencia de esta información dificulta la trazabilidad de la operación del enlace y limita la capacidad del hospital para evaluar la calidad del servicio recibido.

La conectividad funciona de manera general y se evidenció disponibilidad del enlace durante la visita; sin embargo, la falta de informes técnicos regulares por parte del proveedor representa una oportunidad de mejora para fortalecer el seguimiento, control y gestión del servicio contratado.

Adjunto gráfica de servicio



Recomendación:
Se sugiere solicitar al proveedor la entrega periódica de informes de desempeño, métricas de disponibilidad, incidentes atendidos y cumplimiento de SLA, con el fin de contar con un registro histórico que facilite la toma de decisiones y la supervisión del servicio de conectividad.

Oportunidad de mejora
Por otra parte, no existe una bitácora formal para el registro y seguimiento de caídas del servicio de Internet ni de eventos de degradación (lentitud o saturación). Los reportes se realizan mediante correos aislados al proveedor, sin un registro consolidado que permita obtener estadísticas o analizar tendencias. Además, las gráficas de tráfico enviadas por el proveedor corresponden a capturas puntuales generadas únicamente cuando se presenta algún inconveniente, por lo que no constituyen un sistema de monitoreo continuo.

Riesgos
- Falta de trazabilidad: No es posible identificar patrones, frecuencia ni duración real de las indisponibilidades.
- Limitaciones para gestionar al proveedor: Sin registros estructurados, el hospital no puede verificar cumplimiento de SLA ni escalar incidentes de forma soportada.
- Impacto operativo: La ausencia de seguimiento dificulta determinar si la lentitud percibida es ocasional, recurrente o asociada a saturación del enlace.

Recomendación
Se recomienda implementar una bitácora básica de incidentes, que registre cada evento de indisponibilidad o degradación del servicio, incluyendo fecha, duración, causa probable, acciones realizadas, respuesta del proveedor y activación de contingencia.
Adicionalmente, solicitar al proveedor la entrega periódica de informes técnicos que incluyan:
- Disponibilidad mensual del enlace (uptime),
- Métricas de tráfico
- Incidentes atendidos
- Cumplimiento de SLA
- Tendencias de saturación

Lo anterior, permitirá fortalecer el control operativo, mejorar la gestión con el proveedor y asegurar la continuidad del servicio de conectividad del hospital.

b.1) Contingencia ante falla del servicio de Internet
De acuerdo con el *Plan de Contingencia frente a Caída del Sistema – PT03 DA V4* del Hospital Cardiovascular, en caso de presentarse una interrupción del servicio de Internet, la institución activa inmediatamente la contingencia operativa definida para garantizar la continuidad de los registros asistenciales. Esto incluye la distribución de equipos portátiles, antenas y celulares institucionales por servicio, según la tabla establecida en el documento.
El plan indica que *"la contingencia de internet se despliega inmediatamente detectado el fallo con el fin de no perder continuidad ni oportunidad de los registros de atención"*
PT03 DA PLAN DE CONTINGENCIA FR…
.
Durante la auditoría se verificó que la institución cuenta con dicho protocolo formalizado; no obstante, se identificó que la activación de la contingencia no se encuentra integrada dentro de una bitácora de incidentes ni soportada mediante informes periódicos del proveedor. Lo anterior representa una oportunidad de mejora para fortalecer la trazabilidad y el control operativo frente a la gestión de caídas del enlace.

c) Configuración

Oportunidad de mejora
No se realizan copias de seguridad de la configuración de los switches ni existe un procedimiento formal que documente este proceso. La configuración actual de los equipos no cuenta con respaldo, y no se dispone de un repositorio o archivo donde se almacenen versiones previas o la configuración inicial de cada switch.

- El personal técnico confirma que no se generan backups de configuración cuando se realizan cambios en la red.
- No existe una carpeta o repositorio con archivos de configuración de switches.
- No se evidencian documentos, procedimientos o lineamientos internos que definan la forma en que debe realizarse la copia de seguridad o restauración de configuraciones.

Riesgo
- Pérdida de configuración: Ante una falla, daño físico, reemplazo o reinicio de fábrica del switch, se perderían todas las configuraciones actuales.
- Tiempo de recuperación prolongado: La restauración del servicio dependería de reconstruir manualmente toda la configuración, lo que aumenta el tiempo de indisponibilidad.
- Inconsistencias en la red: Sin un respaldo, es difícil mantener control sobre cambios aplicados, lo que puede generar errores, duplicación de VLANes, conflictos de direccionamiento o pérdida de servicios críticos.
- Limitación para auditorías y trazabilidad: No existe evidencia documental que permita conocer el estado de la configuración o validar qué cambios se han aplicado.

Recomendación
Se recomienda implementar un procedimiento básico de respaldo de configuraciones, aplicable al menos a los switches administrables, que incluya:
- Generación de copias de la configuración cada vez que se realicen cambios o intervenciones.
- Almacenamiento de los archivos en una carpeta organizada, identificada por equipo, fecha y responsable.
- Definición de un mecanismo de restauración para incidentes.
- Incorporación del proceso en los lineamientos internos de TI del hospital.

Esta práctica puede realizarse de manera sencilla y sin impacto operativo, y permitirá reducir tiempos de recuperación y mejorar la trazabilidad de la infraestructura de red.

d) WiFi

Durante la revisión se evidenció que el hospital no dispone de red WiFi operativa para usuarios internos. El servicio de conectividad inalámbrica estuvo contratado hasta el mes de abril 2025; sin embargo, una vez finalizado el contrato, la institución decidió no renovar el servicio por motivos administrativos.
Actualmente, todas las conexiones se realizan mediante red cableada, y no se identifican puntos de acceso activos ni configuraciones asociadas a redes inalámbricas institucionales. En consecuencia, no aplica la verificación de claves, segmentación ni controles de seguridad asociados a redes WiFi.

e) Monitoreo

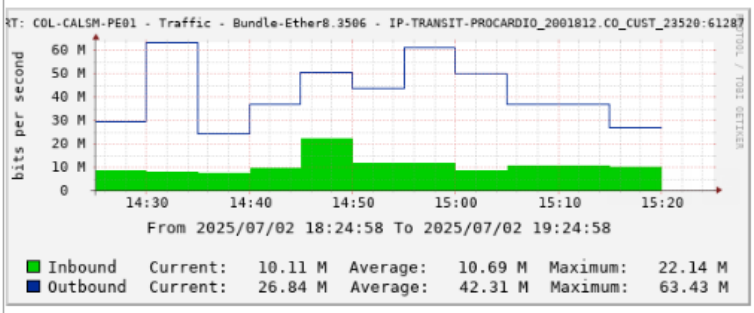
El hospital no cuenta con un mecanismo propio de monitoreo del estado del enlace. Las gráficas entregadas corresponden únicamente a capturas puntuales enviadas por el proveedor el al 2 de julio 2025 cuando se presenta un inconveniente, y no a un monitoreo continuo ni estructurado. No se evidencian informes periódicos de desempeño, disponibilidad o incidentes.

Oportunidad de mejora
Se resalta la necesidad de que el proveedor realice el monitoreo permanente del enlace y remita informes regulares, con métricas de tráfico, alertas, eventos atendidos y cumplimiento de niveles de servicio, a fin de garantizar un adecuado seguimiento operativo

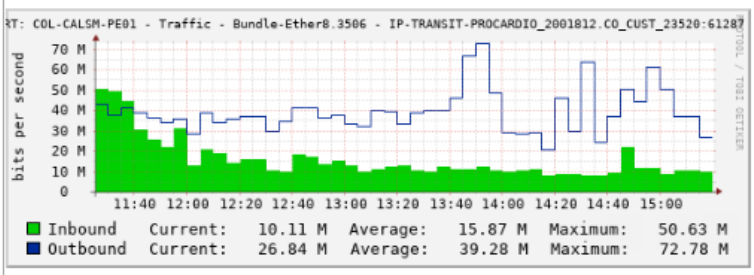
Gráficos tráfico de red (2 julio -2025)
Last hour: Tráfico de la última hora
Last 4 hours: Tráfico promedio de las últimas 4 horas
Last day: Comportamiento completo del último día

Los gráficos muestran dos colores:
Verde (Inbound) Datos que recibe el hospital desde Internet.
Azul (Outbound) Datos que envía el hospital hacia Internet.

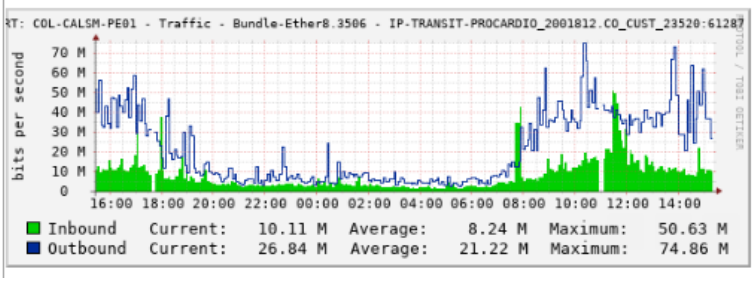
Last hour:



Last 4 hours:

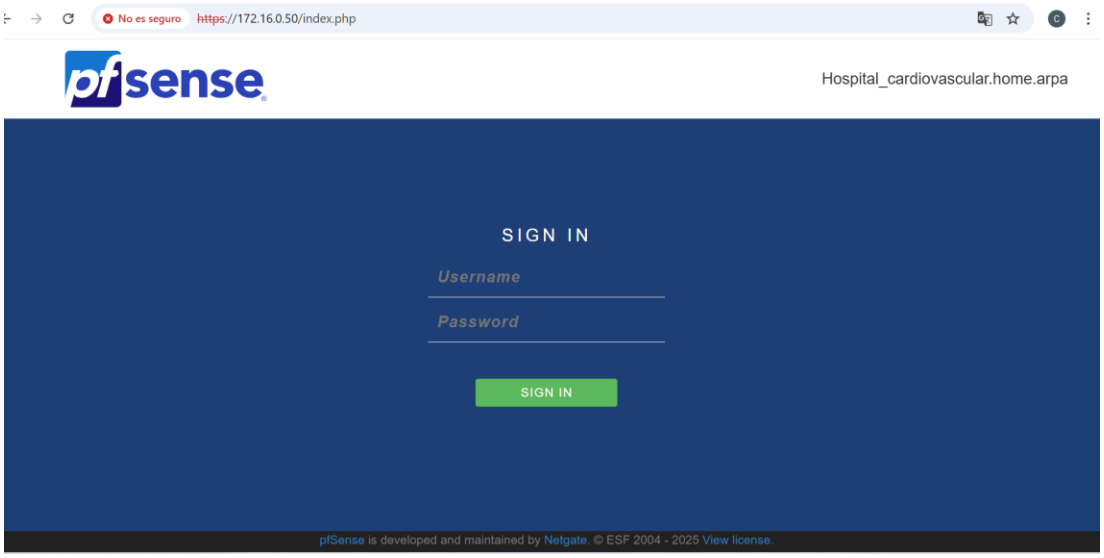


Last day:

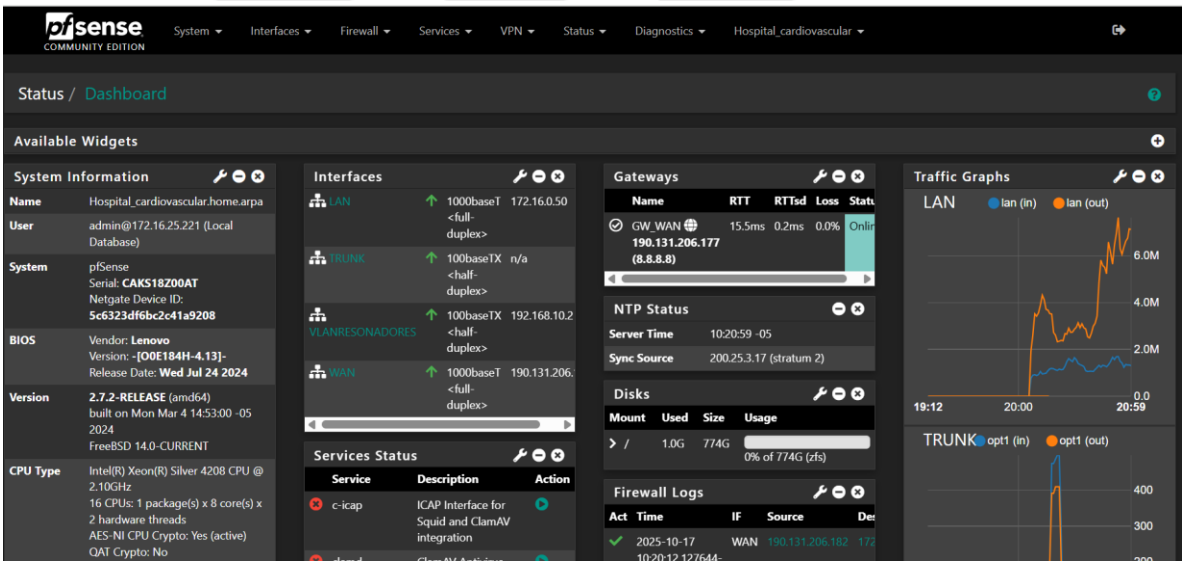


f) Cumplimiento mínimo de conectividad

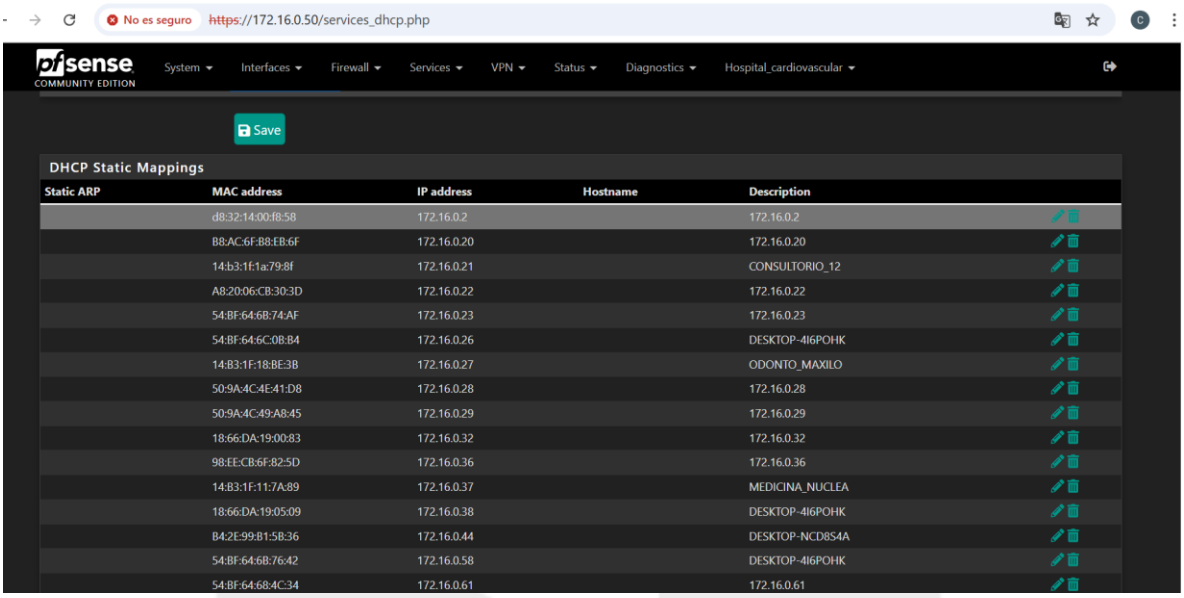
El hospital cuenta con un firewall pfSense, el cual actúa como el componente central de seguridad perimetral y permite ejecutar controles mínimos de red, como administración de reglas, segmentación básica, servicios internos (DHCP, DNS) y gestión de accesos remotos mediante VPN. Este firewall soporta la operación diaria del hospital y brinda un nivel esencial de protección y gobernanza del tráfico, constituyendo la base del esquema actual de conectividad.



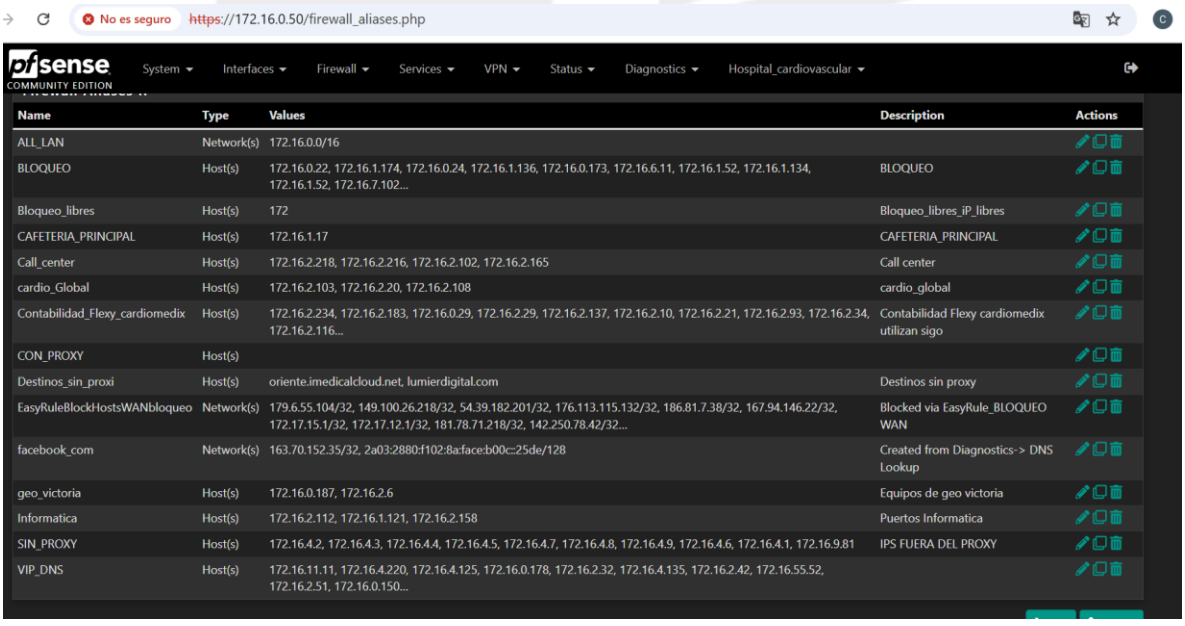
Panel de control y estado general del firewall pfSense: se observa el panel principal del firewall pfSense, el cual consolida indicadores de desempeño, estado de interfaces, pasarelas y tráfico en tiempo real. Esta vista permite el seguimiento operativo y el control del comportamiento de la red institucional.



Configuración de asignaciones DHCP estáticas: se presenta la configuración de asignaciones estáticas del servicio DHCP del firewall pfSense, la cual permite mantener controladas las direcciones IP de los equipos institucionales y asegurar la trazabilidad en la red interna del hospital.



Aliases de red definidos en el firewall: se presenta la configuración de *aliases* en el firewall pfSense, los cuales agrupan direcciones IP por áreas funcionales y reglas de control de tráfico. Esta práctica permite aplicar políticas de filtrado y seguridad de manera centralizada, aunque se recomienda mantener una documentación actualizada que describa el propósito y alcance de cada alias.



CONCLUSIONES DE LA REUNIÓN

En el marco del entendimiento realizado sobre el proceso de Redes y Conectividad se obtuvo la información correspondiente (fotos, archivos, registros) solicitados. No obstante, con la información disponible se procede con la revisión y análisis, con el fin de determinar oportunidades de mejora o confirmar que la plataforma SIIGO cumple adecuadamente con los criterios técnicos a nivel de software y hardware.

COMPROMISOS O ACTIVIDADES PENDIENTES

No Aplica

COMPROMISOS DE LA REUNIÓN

ITEM	ACTIVIDAD	RESPONSABLE	FECHA DE ENTREGA
1			
2			