UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

IMPLEMENTACIÓN Y AMPLIACIÓN DE UN SISTEMA DE CONMUTADORES DE ALTA DISPONIBILIDAD PARA LAS NUEVAS SEDES DEL HOSPITAL GUILLERMO ALMENARA DEL SEGURO SOCIAL DE SALUD DEL PERÚ

INFORME DE COMPETENCIA PROFESIONAL

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE TELECOMUNICACIONES

PRESENTADO POR:

CARLOS ALBERTO APARICIO VILLARREAL

PROMOCIÓN
2004 - I

LIMA – PERU
2014

IMPLEMENTACIÓN Y AMPLIACIÓN DE UN SISTEMA DE CONMUTADORES DE ALTA DISPONIBILIDAD PARA LAS NUEVAS SEDES DEL HOSPITAL GUILLERMO ALMENARA DEL SEGURO SOCIAL DE SALUD DEL PERÚ

Dedicatoria:

Dedico este trabajo a mi esposa e hijos, por su paciencia, apoyo y comprensión inmejorable.

A Dios por todo lo bueno que ha puesto en mi camino.

SUMARIO

En el presente informe se describe el desarrollo y la implementación de una red de conmutadores de alta disponibilidad sobre una plataforma de cableado estructurado redundante con troncal (*backbone*) de fibra óptica, en dos nuevas sedes de Emergencia y Consulta Externa, del Hospital Guillermo Almenara, ambas interconectadas a nivel de red con la sede principal existente del Hospital. La línea base del alcance a nivel de equipamiento y del cableado estructurado, ha sido dimensionado en cumplimiento a los requerimientos técnicos de la entidad, establecidos en sus bases del expediente técnico del concurso licitado. Se muestran los resultados de las pruebas de operación y funcionamientos de las plataformas descritas, así como los resultados de tiempo y costo.

La implementación ha sido desarrollada en dos partes. La primera enfocada en una plataforma de cableado estructurado con troncal redundante tipo anillo de fibra óptica, para interconectar las nuevas sedes del hospital y la sede principal existente. La segunda enfocada en una plataforma de red de conmutadores (*Switch*), desplegadas en cuartos de comunicaciones. Cada sede cuenta con un conmutador principal *(Switch Core)* donde converge el tráfico de red de los conmutadores de borde de cada piso, así mismo encargada del ruteo de tráfico de los servicios entre las sedes. La finalidad de la implementación, es soportar la transmisión de datos y ancho de banda, la convergencia de servicios de comunicaciones y aplicaciones médicas, de las distintas oficinas administrativas y áreas asistenciales médicas, de las nuevas sedes del Hospital, quienes requieren mantener una comunicación ininterrumpida y eficiente con la red integral del ESSALUD.

TABLA DE CONTENIDOS

INDICE DE TABLAS

ÍNDICE DE FIGURAS

GLOSARIO DE TÉRMINOS

HTTP: Hypertext Transfer Protocol.

IP: Internet Protocol.

ISDN: Integrated Services Digital Network.

PCM: Pulse Code Modulation **PSTN:** Public Switched Telephone Network.

RAM: Random Access Memory.

RAS: Registration Admission and Status.

RDSI: Red Digital de Servicios Integrados, en inglés ISDN.

RFC: Documento de Trabajo de Estándarización (Request For Comment).

RTPC: Red de Telefonía Publica Conmutada, en inglés PSTN.

RTP: Real-Time Transport Protocol definido en el RFC 3550.

RTCP: Real-Time Control Transport Protocol definido en el RFC 3550.

SDP: Session Description Protocol.

SETUP: Mensaje del protocolo Q931 para iniciar una llamada.

SMTP: Simple Mail Transfer Protocol.

STREAM: Trama de Datos de una determinada cantidad de bits.

UDP: User Datagram Protocol.

UIT: Union Internacional de Telecomunicaciones.

QoS: Calidad de Servicio.

PROLOGO

En el presente informe describe la implementación de una red de conmutadores (switch) de alta disponibilidad, soportada por una plataforma de cableado estructurado redundante y preparada para este entorno, la implementación se desarrollo en las nuevas dos sedes de Emergencia y Consulta Externa, del Hospital Guillermo Almenara, las mismas han sido interconectados a nivel de red con la sede principal actual del Hospital, todas las sedes adyacentes geográficamente. El informe está desarrollado en cinco (05) capítulos las cuales a continuación se describen.

El capítulo I, describe el planteamiento de Ingeniería de la necesidad, para la implementación de la red de conmutadores, se describe la necesidad que debe soportar la nueva red, los objetivos y requerimientos técnicos mínimos a cumplir por los equipos y materiales, en resumen describe la línea base del alcance y sus limitaciones.

El capítulo II, describe los fundamentos teóricos aplicados a la red de alta disponibilidad implementada, distribuidas en dos sistemas. Los fundamentos del sistema de cableado estructurado, para el cableado horizontal en cobre F/UTP de categoría 6A y para la troncal *(backbone)* de fibra óptica monomodo y multimodo (OM4). Los fundamentos del sistema de conmutadores de red, y los protocolos de red aplicados para el tráfico de los servicios de telefonía IP, cámaras IP, inalámbrico *(wireless)* IP y aplicaciones médicas.

El capítulo III, describe el desarrollo de la implementación, de la plataforma de cableado estructurado y en la plataforma de conmutadores de red, se detalla el análisis cuantitativo del equipamiento instalado, el despliegue del equipamiento en base a la necesidad del Hospital, los protocolos de red configurados a nivel de ruteo entre sedes y segmentación de sub redes por cada aplicación de comunicaciones de cada sede.

El capítulo IV, describe los resultados de los protocolos de pruebas de operación en los sistemas de cableado estructurado y de conmutadores de red.

El capítulo V, describe la evaluación de costos y tiempos, empleando en la implementación del proyecto. Finalmente se brindan las conclusiones y recomendaciones, que debe seguir el administrador de la nueva red de conmutadores de alta disponibilidad del Hospital.

CAPITULO I
PLANTEAMIENTO DE INGENIERÍA DE LA NECESIDAD

1.1 Descripción de la Necesidad

La institución del Seguro Social del Perú ESSALUD, amplió su infraestructura en el Hospital Guillermo Almenara Irigoyen de Lima Perú, perteneciente a La Red Asistencial Almenara, para el cual construyo dos edificios adyacentes a su sede principal, las que han sido nombradas como Nueva Sede Emergencia (de tres pisos de atención y un sótano) y la Nueva Sede Consulta Externa (de seis pisos de atención y un sótano). Las nuevas sedes han necesitado una Plataforma de Conmutadores de Red de Alta Disponibilidad, robusta y escalable, que permita asegurar y soportar, la convergencia de servicios de comunicaciones y aplicaciones médicas, de las distintas oficinas administrativas y áreas asistenciales medicas, que deben mantener comunicación constante con la red integral del ESSALUD.

Para lograr la eficiencia ylos objetivos, las nuevas sedes del Hospital han requerido contar con un sistema de comunicaciones con máximo rendimiento de transmisión de datos y ancho de banda, que les permita soportar ininterrumpidamente las aplicaciones de información. El diseño debe considerar una troncal de campus *(backbone)* de fibra óptica redundante tipo anillo entre los nodos principales *(Core),* y una troncal vertical tipo estrella escalable entre los nodos de borde. En el diseño lógico de la red de conmutadores, ha predominado la habilitación de enlaces agregados, la gestión de bucles debido a la existencia de enlaces redundantes, el análisis de segmentación lógica de tráfico, la disponibilidad de puertos en los conmutadores de borde (con energía PoE) y los protocolos de enrutamientos jerárquicos en cada nodo principal de cada nueva sede.

1.2 Objetivos de la Implementación

El ESSALUD, a través de La Oficina Central de Tecnologías de Información y Comunicaciones *(OCTIC),* ha requerido una red de conmutadores de alta disponibilidad para cubrir las necesidades básicas de comunicaciones y aplicaciones médicas, para las oficinas administrativas y áreas asistenciales del Hospital, las cuales deben ser soportadas

por un cableado de fibra óptica y red de conmutadores de alta disponibilidad. Permitiendo comunicación interna, entre el equipamiento informático del personal asistencial, administrativo y la comunicación externa hacia los servidores de la red de datos de la sede principal existente del Almenara, y la sede central de ESSALUD, para acceder a los servicios de, internet, correo, intranet, Web, Acreditación, y aplicaciones médicas.

1.3 Evaluación de la Necesidad

El ESSALUD, requiere una plataforma de Conmutadores de alta disponibilidad en las Nuevas Sedes, para lo cual se plantea desarrollar dos sistemas.

El sistema de cableado estructurado que debe contemplar una troncal *(backbone)* tipo anillo en fibra óptica con enlaces de backup entre sus nodos principales y una troncal vertical tipo estrella escalable entre sus nodos secundarios en una misma sede.

El diseño del sistema de Conmutadores *(Switch)* de la red de área local (LAN) debe aplicar estándares de red de manera que garantice la operación ininterrumpida y de anta disponibilidad. A nivel de conmutadores de borde aplicar, el estándar IEEE 802.3ad *(LACP)* para enlaces agregados, la habilitación del protocolo Spannnig tree para la gestión de bucles de los enlaces agregados, el estándar IEEE 802.1Q para la gestión de redes virtuales por aplicaciones, el estándar IEEE 802.1p para la priorización de tráfico y filtrado multicast dinámico, el estándar IEEE 802.3af para la habilitación de puertos PoE en los conmutadores de borde (en las aplicaciones de telefonía IP, cámaras IP y access point IP).

A nivel de conmutadores principales aplicar, el protocolo OSPF para el enrutamiento jerárquico de pasarela interior para la discriminación de envió de tráfico entre los nodos de una red mediante la difusión de la topología de la red y la información de estado-enlace.

A continuación se detallan los puntos de red requeridos, en cada una de las nuevas sedes.

Tabla 1.1 Requerimiento de puntos de red del hospital en sede emergencia.

Sede Nueva Emergencia						
Ubicación	Telecom	Puntos de Datos	Puntos de Voz	Puntos para Access Point	Puntos para Cámaras IP	Total puntos de Red
Piso 1	GDP	44	25	4	8	81
Piso 1	GDS-101	42	13	2	9	66
Piso 1	GDS-102	4	2	1	4	11
Piso 2	GDS-201	85	19	5	7	116
Piso 3	GDS-301	151	10	7	7	175
					Total	**449**

Tabla 1.2 Requerimiento de puntos de red del hospital en sede consulta externa.

Sede Nueva Consulta Externa						
Ubicación	Telecom	Puntos de Datos	Puntos de Voz	Puntos para Access Point	Puntos para Cámaras IP	Total puntos de Red
Piso 1	GDP	0	0	0	0	0
Piso 1	GDS-101	79	49	4	21	153
Piso 1	GDS-102	7	3	0	2	12
Piso 2	GDS-201	52	44	6	9	111
Piso 3	GDS-301	46	40	6	9	101
Piso 4	GDS-401	42	41	7	9	99
Piso 5	GDS-501	39	36	11	7	93
Piso 6	GDS-601	32	23	6	9	70
					Total	**639**

- GDP: Gabinetes de Datos Principal
- GDS: Gabinete de Datos Secundario

La plataforma de conmutadores de red, debe estar soportada por una red troncal de fibra óptica, multimodo (OM4) y monomodo (9/125µm), según la necesidad de distancias que soporte para aplicaciones hasta 10 Gigabit Ethernet, en la interconexión de Gabinetes de Datos de las nuevas sedes del Hospital. Así mismo los puntos de red deben ser de F/UTP de categoría 6A canal completo.

El requerimiento de ESSALUD para estas nuevas sedes, ha definido las cantidades a nivel de Conmutadores *(Switch)* de red de borde y principal *(Core)*, las cuales debes distribuirse en los gabinetes de datos, para satisfacer la demanda de puntos de red. A continuación en la siguiente tabla se detallan las cantidades requeridas por ESSALUD según el tipo de Conmutador *(Switch)*:

Tabla 1.3 Requerimiento de conmutadores de red *(Switch)* del Hospital .

Descripción de Switch	Cantidad
Conmutador de Borde Tipo A	08
Conmutador de Borde Tipo B	09
Conmutador de Borde Tipo C	14
Conmutador Principal (Core) Tipo D	02

A continuación se detallan en las siguientes tableas, las características técnicas más importantes requeridas por ESSALUD, por cada tipo de conmutador *(Switch)*.

Tabla 1.4 Especificaciones Técnicas de Conmutadores *(Switch)* Tipo A.

ESPECIFICACIONES TÉCNICAS CONMUTADORES TIPO A (L2-24 puertos PoE)	
1-Configuración física	
Tipo	Conmutador multicapas operación en capa 2 del modelo OSI.
Instalación	Montaje en rack 19".
Alimentación	Fuente de poder interna o externa con opción a soporte de una unidad de fuente redundante de tipo AC o DC.
Interfaces	Veinticuatro (24) Puertos 10/100/1000 Base-T, soportando todos los puertos activos simultáneamente con PoE 802.3af y 802.3at. Dos (02) interfaces gigabit SFP+, con soporte de interfaces 1000BASE-SX, con sus respectivos transceivers de fibra óptica de tipo LC y tener la capacidad de soportar a futuro 10Gbps. Soportar Hot Swap (Capacidad de cambiar los módulos de tipo SFP+).
Stack	Dos (02) puertos para stack instalados de propósito específico, adicionales a los puertos Ethernet de fibra o cobre solicitados.

2-Rendimiento	
Switchfabric	Debe ser un equipo 100% wirespeed a nivel de Switchfabric (SF) o capacidad de conmutación, por lo que deberá contar como mínimo con el switchfabric suficiente para atender todos los puertos de fibra, cobre y stack al 100% de carga y en forma simultánea y en modalidad full dúplex. Por lo que para cada puerto de 1Gbps deberá contar con 2Gbps agregados de SF disponibles y para cada puerto de 10Gbps deberá contar con 20Gbbps agregados de SF disponibles. De acuerdo a la cantidad y tipo de puertos requeridos, se aceptaran como mínimo Ochenta y ocho (88) Gbps de SF disponible.
Tasa de envío	Debe ser un equipo 100% wirespeed a nivel de Tasa de envío o throughput. Se solicita como mínimo 65 Mpps de throughput disponibles.
Capacidad de Stacking	La velocidad mínima por puerto de stack deberá ser de 10Gbps full duplex o 20Gbps agregados, se requiere mínimo 02 puertos de stack.

3-Estándares de comunicaciones relacionados	
Protocolos	Ethernet IEEE 802.3, 10 Base-T, Fast Ethernet IEEE 802.3u, 100Base-TX, 100Base-FX, 100BaseBX Gigabit Ethernet IEEE 802.3z, 802.3ab, 1000Base-X, 1000Base-T, Soporte de interfaces 1000Base-SX, 1000Base-LX, 1000Base-LH, 1000BaseBX, IEEE 802.3af, 802.3at, 802.3ad, 802.3x, 802.1d, 802.1s, 802.1w, 802.1ab, 802.1x, 802.1p, 802.1q. , 802.3ah, 802.3ac, IPv4, IPv6.

4-Características Generales	
Administración del equipo	Administración por Interface de línea de comandos (CLI), SSHv2, Telnet, SNMPv3 vía Software, interface Web, vía SSL o HTTPS. Soporte de FTP, TFTP, SFTP, SCP.
Auto negociación	Auto negociación full/half-duplex en todos los puertos.
Spanning-Tree	Soporte de VLAN 802.1d Spanning-TreeProtocol. Soporte de VLAN 802.1w Rapid Spanning-TreeProtocol. Soporte de IEEE 802.1s Múltiple Spanning-TreeProtocol.
VLAN's	Soporte de 802.1q VLAN. Soportar 250 VLAN activas simultáneamente y como mínimo 16K MAC address en su tabla.
Agregación de enlaces	Agregación de enlace IEEE 802.3ad (LACP) como mínimo debe soportar ocho (08) grupos de enlaces agregados.
Colas de Prioridad	Ocho (08) colas en hardware por puerto para QoS como mínimo.
Prioridad de tráfico	Funcionalidad de QoS Multilayer, Soporte de 802.1p (CoS), DSCP. Clasificación de tráfico basada en direcciones MAC de origen y destino (Capa 2), direcciones IP de origen y destino (Capa 3) y puertos TCP/UDP (Capa 4).
Autenticación	Capacidad instalada de 802.1x múltiples clientes y múltiples vlan's en el mismo puerto. Debe tener habilitado la funcionalidad de autenticación mediante MAC-Address y Captive Portal (portal web cautivo). Habilitado RADIUS, TACACS+ y LDAP. Control de acceso habilitado basado en políticas de usuarios o asignación de perfiles de usuarios.

Seguridad	Soporte de ACLs por puerto, basados en información de Capas 2, 3 y 4. Protección contra ataques del tipo DoS y/o ataques del tipo MITM. Soporte de DHCP snooping, para evitar asignaciones dinámicas de direcciones IP provenientes de servidores DHCP no autorizados. Soportar SSHv2, SSL, SNMPv3 y HTTPS para administración segura.
Otros	Multicast IGMP v1, v2, v3 snooping, MLD snooping. Mínimo 1000 grupos de multicast. Debe incluir DHCP snooping. Soporte de port Mirror por puerto y por grupo de puertos.

Tabla 1.5 Especificaciones Técnicas de Conmutadores *(Switch)* Tipo B.

ESPECIFICACIONES TÉCNICAS CONMUTADORES TIPO B (L2-48 puertos PoE)	
1-Configuración física	
Tipo	Conmutador multicapas operación en capa 2 del modelo OSI.
Instalación	Montaje en rack 19".
Alimentación	Fuente de poder interna o externa con opción a soporte a una unidad de fuente redundante de tipo AC o DC.
Interfaces	Cuarenta y ocho (48) Puertos 10/100/1000 Base-T, soportando todos los puertos PoE 802.3af y 802.3at. Dos (02) interfaces gigabit SFP+, con soporte de interfaces 1000BASE-SX, con sus respectivos transceivers de fibra óptica de tipo LC y tener la capacidad de soportar a futuro 10Gbps. Soportar Hot Swap (Capacidad de cambiar los módulos de tipo SFP+).
Stack	Dos (02) puertos para stack instalados de propósito específico, adicionales a los puertos Ethernet de fibra o cobre solicitados.

2-Rendimiento	
Switchfabric	Debe ser un equipo 100% wirespeed a nivel de Switchfabric (SF) o capacidad de conmutación, por lo que deberá contar como mínimo con el switchfabric suficiente para atender todos los puertos de fibra, cobre y stack al 100% de carga y en forma simultánea y en modalidad full dúplex.

	Por lo que para cada puerto de 1Gbps deberá contar con 2Gbps agregados de SF disponibles y para cada puerto de 10Gbps deberá contar con 20Gbbps agregados de SF disponibles. De acuerdo a la cantidad y tipo de puertos requeridos, se aceptaran como mínimo ciento treinta y seis (136) Gbps de SF disponible.
Tasa de envío	Debe ser un equipo 100% wirespeed a nivel de Tasa de envío o throughput. Se solicita como mínimo 101 Mpps de throughput disponibles.
Capacidad de Stacking	La velocidad mínima por puerto de stack deberá ser de 10Gbps full duplex o 20Gbps agregados, se requiere mínimo 02 puertos de stack.

3-Estándares de comunicaciones relacionados	
Protocolos	Ethernet IEEE 802.3, 10 Base-T, Fast Ethernet IEEE 802.3u, 100Base-TX, 100Base-FX, 100BaseBX Gigabit Ethernet IEEE 802.3z, 802.3ab, 1000Base-X, 1000Base-T, Soporte de interfaces 1000Base-SX, 1000Base-LX, 1000Base-LH, 1000BaseBX IEEE 802.3af, 802.3at, 802.3ad, 802.3x, 802.1d, 802.1s, 802.1w, 802.1ab, 802.1x, 802.1p, 802.1q. , 802.3ah, 802.3ac, IPv4, IPv6.

4-Características Generales	
Administración del equipo	Administración por Interface de línea de comandos (CLI), SSHv2, Telnet, SNMPv3 vía Software, interface Web, vía SSL o HTTPS. Soporte de FTP, TFTP, SFTP, SCP.
Auto negociación	Auto negociación full/half-duplex en todos los puertos.
Spanning-Tree	Soporte de VLAN 802.1d Spanning-TreeProtocol. Soporte de VLAN 802.1w Rapid Spanning-TreeProtocol. Soporte de IEEE 802.1s Múltiple Spanning-TreeProtocol.
VLAN's	Soporte de 802.1q VLAN. Soportar 250 VLAN activas simultáneamente y como mínimo 16K MAC address en su tabla.
Agregación de enlaces	Agregación de enlace IEEE 802.3ad (LACP) como mínimo debe soportar ocho (08) grupos de enlaces agregados.
Colas de Prioridad	Ocho (08) colas en hardware por puerto para QoS como mínimo.

Prioridad de tráfico	Funcionalidad de QoS Multilayer, Soporte de 802.1p (CoS), DSCP. Clasificación de tráfico basada en direcciones MAC de origen y destino (Capa 2), direcciones IP de origen y destino (Capa 3) y puertos TCP/UDP (Capa 4).
Autenticación	Capacidad instalada de 802.1x múltiples clientes y múltiples vlan's en el mismo puerto. Debe tener habilitado la funcionalidad de autenticación mediante MAC-Address y Captive Portal (portal web cautivo). Habilitado RADIUS, TACACS+ y LDAP. Control de acceso habilitado basado en políticas de usuarios o asignación de perfiles de usuarios.
Seguridad	Soporte de ACLs por puerto, basados en información de Capas 2, 3 y 4. Protección contra ataques del tipo DoS y/o ataques del tipo MITM. Soporte de DHCP snooping, para evitar asignaciones dinámicas de direcciones IP provenientes de servidores DHCP no autorizados. Soportar SSHv2, SSL, SNMPv3 y HTTPS para administración segura.
Otros	Multicast IGMP v1, v2, v3 snooping, MLD snooping, DHCP snooping. Mínimo 1000 grupos de multicast. Soporte de port Mirror por puerto y por grupo de puertos.

Tabla 1.6 Especificaciones Técnicas de Conmutadores *(Switch)* Tipo C.

ESPECIFICACIONES TÉCNICAS CONMUTADORES TIPO C (L2-48 puertos)	
1-Configuración física	
Tipo	Conmutador multicapas operación en capa 2 del modelo OSI.
Instalación	Montaje en rack 19".
Alimentación	Fuente de poder interna o externa con opción a soporte a una unidad de fuente redundante de tipo AC o DC.
Interfaces	Cuarenta y ocho (48) Puertos 10/100/1000 Base-T. Dos (02) interfaces gigabit SFP+, con soporte de interfaces 1000BASE-SX, con sus respectivos transceivers de fibra óptica de tipo LC y tener la capacidad de soportar a futuro 10Gbps. Soportar Hot Swap (Capacidad de cambiar los módulos de tipo SFP+).

Stack	Dos (02) puertos para stack instalados de propósito específico, adicionales a los puertos Ethernet de fibra o cobre solicitados.

2-Rendimiento	
Switchfabric	Debe ser un equipo 100% wirespeed a nivel de Switchfabric (SF) o capacidad de conmutación, por lo que deberá contar como mínimo con el switchfabric suficiente para atender todos los puertos de fibra, cobre y stack al 100% de carga y en forma simultánea y en modalidad full dúplex. Por lo que para cada puerto de 1Gbps deberá contar con 2Gbps agregados de SF disponibles y para cada puerto de 10Gbps deberá contar con 20Gbbps agregados de SF disponibles. De acuerdo a la cantidad y tipo de puertos requeridos, se aceptaran como mínimo ciento treinta y seis (136) Gbps de SF disponible.
Tasa de envío	Debe ser un equipo 100% wirespeed a nivel de Tasa de envío o throughput. Se solicita como mínimo 101 Mpps de throughput disponibles.
Capacidad de Stacking	La velocidad mínima por puerto de stack deberá ser de 10Gbps full duplex o 20Gbps agregados, se requiere mínimo 02 puertos de stack.

3-Estándares de comunicaciones relacionados	
Protocolos	Ethernet IEEE 802.3, 10 Base-T, Fast Ethernet IEEE 802.3u, 100Base-TX, 100Base-FX, 100BaseBX Gigabit Ethernet IEEE 802.3z, 802.3ab, 1000Base-X, 1000Base-T, Soporte de interfaces 1000Base-SX, 1000Base-LX, 1000Base-LH, 802.3ad, 802.3x, 802.1d, 802.1s, 802.1w, 802.1ab, 802.1x, 802.1p, 802.1q. , 802.3ah, 802.3ac, IPv4, IPv6.

4-Características Generales	
Administración del equipo	Administración por Interface de línea de comandos (CLI), SSHv2, Telnet, SNMPv3 vía Software, interface Web, vía SSL o HTTPS. Soporte de FTP, TFTP, SFTP, SCP.

Auto negociación	Auto negociación full/half-duplex en todos los puertos.
Spanning-Tree	Soporte de VLAN 802.1d Spanning-TreeProtocol. Soporte de VLAN 802.1w Rapid Spanning-TreeProtocol. Soporte de IEEE 802.1s Múltiple Spanning-TreeProtocol.
VLAN's	Soporte de 802.1q VLAN. Soportar 250 VLAN activas simultáneamente y como mínimo 16K MAC address en su tabla.
Agregación de enlaces	Agregación de enlace IEEE 802.3ad (LACP) como mínimo debe soportar ocho (08) grupos de enlaces agregados.
Colas de Prioridad	Ocho (08) colas en hardware por puerto para QoS como mínimo.
Prioridad de tráfico	Funcionalidad de QoS Multilayer, Soporte de 802.1p (CoS), DSCP. Clasificación de tráfico basada en direcciones MAC de origen y destino (Capa 2), direcciones IP de origen y destino (Capa 3) y puertos TCP/UDP (Capa 4).
Autenticación	Capacidad instalada de 802.1x múltiples clientes y múltiples vlan's en el mismo puerto. Debe tener habilitado la funcionalidad de autenticación mediante MAC-Address y Captive Portal (portal web cautivo). Habilitado RADIUS, TACACS+ y LDAP. Control de acceso habilitado basado en políticas de usuarios o asignación de perfiles de usuarios.
Seguridad	Soporte de ACLs por puerto, basados en información de Capas 2, 3 y 4. Protección contra ataques del tipo DoS y/o ataques del tipo MITM. Soporte de DHCP snooping, para evitar asignaciones dinámicas de direcciones IP provenientes de servidores DHCP no autorizados. Soportar SSHv2, SSL, SNMPv3 y HTTPS para administración segura. Soporte de Learned port security.
Otros	Multicast IGMP v1, v2, v3 snooping, MLD snooping. Mínimo 1000 grupos de multicast. Debe incluir DHCP snooping. Soporte de port Mirror por puerto y por grupo de puertos.

Tabla 1.7 Especificaciones Técnicas de Conmutadores *(Switch)* Tipo D.

ESPECIFICACIONES TÉCNICAS CONMUTADORES TIPO D (L3-24 puertos)	
1-Configuración física	
Tipo	Conmutador multicapas operación en capa 3 del modelo OSI.
Instalación	Montaje en rack 19".
Alimentación	Fuente de poder interna o externa, con opción a una fuente redundante AC o DC.
Interfaces	Veinticuatro (24) interfaces SFP 1000BaseX, con sus respectivos transceiver insertados al equipo, al menos 02 interfaces tipo combo SFP/RJ45. Soporte de 02 puertos 10 Gbps en formato SFP+ con sus respectivos transceiver de fibra óptica de tipo LC multimodo. Soporte de Hot Swap (Capacidad de cambiar los módulos de tipo SFP+).
Stack	Dos (02) puertos para stack instalados de propósito específico, adicionales a los puertos Ethernet de fibra o cobre solicitados.

2-Rendimiento	
Switchfabric	Debe ser un equipo 100% wirespeed a nivel de Switchfabric (SF) o capacidad de conmutación, por lo que deberá contar como mínimo con el switchfabric suficiente para atender todos los puertos de fibra, cobre y stack al 100% de carga y en forma simultánea y en modalidad full dúplex. Por lo que para cada puerto de 1Gbps deberá contar con 2Gbps agregados de SF disponibles y para cada puerto de 10Gbps deberá contar con 20Gbbps agregados de SF disponibles. De acuerdo a la cantidad y tipo de puertos requeridos, se aceptaran como mínimo Ciento veinte y ocho (128) Gbps de SF disponible.
Tasa de envío	Debe ser un equipo 100% wirespeed a nivel de Tasa de envío o throughput. Se aceptarán como mínimo 65 Mpps de throughput disponibles.
Capacidad de Stacking	La velocidad mínima por puerto de stack deberá ser de 10Gbps full duplex o 20Gbps agregados, se requiere mínimo 02 puertos de stack.

3-Estándares de comunicaciones relacionados	
Protocolos	Ethernet IEEE 802.3, 10 Base-T, Fast Ethernet IEEE 802.3u, 100Base-TX, Gigabit Ethernet IEEE 802.3z, 802.3ab, 1000Base-X, 1000Base-T, Soporte de interfaces 1000Base-SX, 1000Base-LX, 1000Base-LH, 802.3ad, 802.3x, 802.1d, 802.1s, 802.1w, 802.1ab, 802.1x, 802.1p, 802.1q. , 802.3ah, 802.3ac, IPv4 e IPv6.

4-Características Generales	
Administración del equipo	Administración por Interface de línea de comandos (CLI), SSHv2, Telnet, SNMPv3 vía Software, interface Web, vía SSL o HTTPS. Soporte de FTP, TFTP, SFTP, SCP.
Auto negociación	Auto negociación full/half-duplex en todos los puertos.
Spanning-Tree	Soporte de VLAN 802.1d Spanning-TreeProtocol. Soporte de VLAN 802.1w Rapid Spanning-TreeProtocol. Soporte de IEEE 802.1s Múltiple Spanning-TreeProtocol.
VLAN's	Soporte de 802.1q VLAN. Soportar 250 VLAN activas simultáneamente y como mínimo 30K MAC address en su tabla.
Agregación de enlaces	Agregación de enlace IEEE 802.3ad (LACP) como mínimo debe soportar ocho (08) grupos de enlaces agregados.
Colas de Prioridad	Ocho (08) colas en hardware por puerto para QoS como mínimo.
Funcionalidades capa 3	Protocolos habilitados: RIPv1,v2, RIPng, OSPFv2 OSPFv3, BGPv4, VRRPv2, VRRPv3, VRF, PIM-DM, PIM-SM o DVMRP, MLDv1,v2 snooping, GRE, WCCPv2.
Prioridad de tráfico	Funcionalidad de QoS Multilayer, Soporte de 802.1p (CoS), DSCP. Clasificación de tráfico basada en direcciones MAC de origen y destino (Capa 2), direcciones IP de origen y destino (Capa 3) y puertos TCP/UDP (Capa 4).
Autenticación	Capacidad instalada de 802.1x múltiples clientes y múltiples vlan's en el mismo puerto. La solución deberá autenticar y segmentar en forma independiente a todos los dispositivos que se encuentren detrás de un puerto autenticado con 802.1x.

	Adicionalmente debe tener habilitado la funcionalidad de autenticación mediante MAC-Address y Captive Portal (portal web cautivo). Habilitado RADIUS, TACACS+ y LDAP. Control de acceso habilitado basado en políticas de usuarios o asignación de perfiles de usuarios, los cuales deben asignar de forma dinámica VLAN, ACL y bandwidth o QoS.
Seguridad	Soporte de ACLs por puerto, basados en información de Capas 2, 3 y 4. Protección contra ataques del tipo DoS y/o ataques del tipo MITM. Soporte de DHCP snooping, para evitar asignaciones dinámicas de direcciones IP provenientes de servidores DHCP no autorizados. Soportar SSHv2, SSL, SNMPv3 y HTTPS para administración segura. Soporte de Learned port security, LLDP rogue detection. Dynamic ARP Inspection, ARP Poison.
Otros	Multicast IGMP v1, v2, v3 snooping, MLD snooping. Debe incluir DHCP snooping. Soporte de port Mirror por puerto y por grupo de puertos.

1.4 Limitaciones de la Implementación

Dado las condiciones requeridas por ESSALUD, para la red de Conmutadores de alta disponibilidad se han identificado factores externos como limitaciones al despliegue de interconexión del equipamiento activo, entre las sedes del hospital, las cuales se proceden a detallar:

- Limitación de costos en las partidas de los sistemas, para la implementación de Cableado Estructurado y de la red de conmutadores *(Switch)*, se detallan los presupuestos expresados en nuevos soles peruanos, incluido IGV:
  - Sistema de Cableado Estructurado, valor: S/. 1,127,585.12
  - Sistema de Conmutadores de red, valor: S/. 644,201.97
- Limitación de cumplimiento a las características técnicas requeridas por el ESSALUD, la cual filtra marcas de proveedores de acuerdo al perfil técnico, tanto para el cableado estructurado y el equipamiento de conmutadores *(Switch)*.
- Limitación del tiempo de la implementación, el cual incluye los tiempos de importación del equipamiento hasta la puesta en servicio.

- Limitación de permisos que debe brindar la Municipalidad de La Victoria para el corte del asfalto y veredas que separan las nuevas sedes del Hospital, la cual es requerido para el entubado de la fibra óptica y poder interconectar las nuevas sedes con la principal.

1.5 Síntesis de la Implementación

Se debe especificar los metodos y procedimientos que se utilizará para alcanzar los objetivos de esta implementacion. Se debe describir los resultados de una Red de Conmutadores de alta disponibilidad.

Se debe describir la instalación del cableado estructurado. El despliegue de la fibra optica tipo anillo para unir las 3 sedes, Principal Almenara Existente, Nueva Emergencia y Nueva Consulta Externa. La instalación de los gabinetes principales y segundarios, en los cuartos de comunicaciones, por piso de cada sede.

Se debe describir la instalación de los conmutadores de red, con su plan de direccionamiento IP (protocolo de internet) de acuerdo a la necesidad de puntos de red para las aplicaciones requeridas, configuraciones de protocolos a nivel de capa 2 y capa 3 del modelo OSI, para el procesamiento de tráfico de datos en toda la red.

CAPITULO II
TEÓRIA DE UNA RED ALTA DISPONIBILIDAD

2.1 Fundamentos del Cableado Estructurado

El Cableado Estructurado contempla una forma palnificada y ordenada de implementar cableados que permitan conectar dispositivos de procesamiento de datos, como conmutadores, redes de área local (LAN), equipos a nivel de usuarios finales e aplicaciones como computadoras personales, telefonos IP, cámaras IP, access point, entre otros. El objetivo primordial es proveer de un sistema total de transporte fisico de la información de diferentes aplicaciones a través de un medio común.

Los Sistemas de Cableado Estructurado emplean una Arquitectura de Sistemas Abiertos (OSA, por sus siglas en inglés) y soportar aplicaciones basadas en estándares internacionales como el EIA/TIA-568A, EIA/TIA-569, EIA/TIA-606, EIA/TIA-607 (de La Electronic Industries Association / Telecommunications Industry Association).

Se detalla las entidades internacioneales y nacionales que regualn los Estándares vigentes aplicados en la actualidad en la siguiente figura:

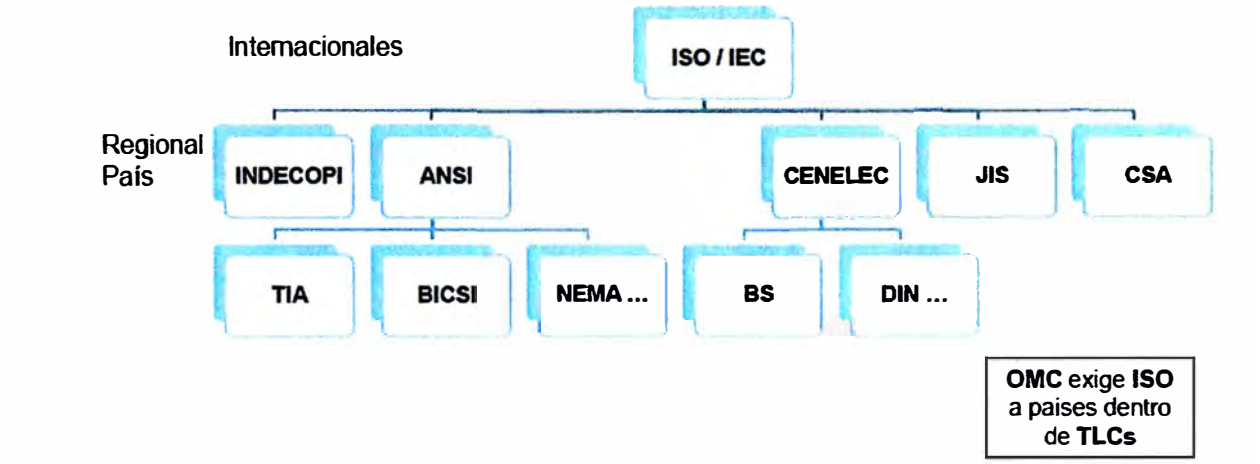


Figura 2.1 Entidades reguladoras de los estándares vigentes de cableado estructurado.

El Sistema de Cableado Estructurado está gobernado por las siguientes normas y estándares de aceptación universal:

- **ANSI/EIA/TIA 568-C.0** (Cableado de Telecomunicaciones Genérico para instalaciónes de clientes: que permite la planeación e instalación de un sistema de Cableado Estructurado que soporta independientemente del proveedor)
- **ANSI/EIA/TIA 568-C.1** (Cableado de Telecomunicaciones para Edificacione Comerciales)
- **ANSI/EIA/TIA 568-C.2** (componentes de par trenzado).
- **ANSI/TIA/EIA-569-B** (Canalizaciones y espacios: que estándariza prácticas de diseño y construcción dentro y entre edificios, tales como bandejas, canaletas, guías, facilidades de entrada al edificio, armarios y/o cuarto de equipos).
- **ANSI/TIA/EIA-606-A** (Administración: que da las guías para marcar y administrar los componentes de un sistema de Cableado Estructurado).
- **ANSI/TIA/EIA TSB-67** (END-TO-END SYSTEM PERFORMANCE TESTING)
- **ANSI-J-STD-607-A** (Grounding and Bonding Requirements for Telecommunications for in Commercial Buildings: Puesta y union a Tierra).
- **ANSI/EIA/TIA-758-1** especifica el cableado de telecomunicación para planta externa.

Normas y estándares considerados por ISO/IEC:

- ISO/IEC 11801:2002 Categoría 6A /Clase EA
- ISO/IEC 14763-1 Administration, documentation, records
- ISO/IEC 14763-2 Planning and Installation practices
- IEC 61935-1 Testing of copper cabling

ISO			TIA		
Estándar	**Fecha**	**Contenido**	**Estándar**	**Fecha**	**Contenido**
ISO-11801	1995	CAT 5	TIA-568 A	1995	Cat 5e
ISO-11801-2	Sep-2002	CAT6/7	TIA-568B2-1	Jun-2002	CAT6
ISO-11801-2-1	Abr-2008	CAT6A/7A channel	TIA-568B2-10	Feb-2008	CAT6A
Desarrollo ISO con relevante participación ANSI					
ISO-11801-2-2	Abr-2010	CAT 6A / 7A	Caracteristicas de componentes		
ISO-11801-99-1	Dic 2013	Ca I / Cat 8.1 Ca II / Cat8.2	TIA-568C2-1	Dic 2013	Cat 8

Figura 2.2 Estándares vigentes ISO/TIA de cableado estructurado.

La implementacion de cableado estructurado descrito en el presente informe, está basado en sub sistema de cableado horizontal con cable F/UTP de categoría 6A y un sub sistema de troncal de fibra óptica OM4. Se detallan los tipos de cableado de cobre UTP y fibra óptica:

Figura 2.3 Tipos de cableado estructurado de cobre par trenzado y fibra óptica.

2.1.1 Sub Sistema de Cableado Horizontal

El cableado horizontal es la porción del sistema de cableado de las telecomunicaciones que va desde el conector de salida de telecomunicaciones del área de trabajo a la conexión cruzada horizontal en el armario de telecomunicaciones (gabinete de datos principal o secundario). El cableado horizontal incluye los cables, el conector/salida de telecomunicaciones del área de trabajo, la terminación mecánica, y las cuerdas auxiliares o puentes situadas en el armario de telecomunicaciones.

Se usa la palabra "horizontal" debido a que, típicamente, el cable en esta parte del cableado va horizontalmente a lo largo del piso o del techo del edificio.

El cableado horizontal tambien debe facilitar actividades de mantenimiento, reubicación, instalación de nuevos equipos y cambios futuros en los servicios.

La cercanía del cableado horizontal a los equipos eléctricos que generan elevados nivele de interferencia electromagnética (EMI) deberá ser tomada en cuenta en el cableado metálico. Ejemplos de esos equipos son lo motore y transformadores nece arios para alimentar los aparatos mecánicos y fotocopiadores usados en el área de trabajo. El estándar A SI/EIA/TIA-569 especifica la separación del cableado horizontal de los conductores de fuentes típicas de interferencia electromagnética.

Se recomienda que los cables horizontales de usuario final no pueden pasar de un pi o a otro. La topología empleada del cableado horizontal debe ser tipo estrella. Cada conector de salida de telecomunicaciones en el área de trabajo deberá ser conectado a una conexión cruzada horizontal en el armario de telecomunicaciones. Cada área de trabajo debe er servida por un armario de telecomunicaciones situado en el mismo piso.

Conexiones en paralelo y placas de empalme no serán permitidas como parte del cableado horizontal de cobre.

Se describe las categorías del cableado horizontal de cobre:

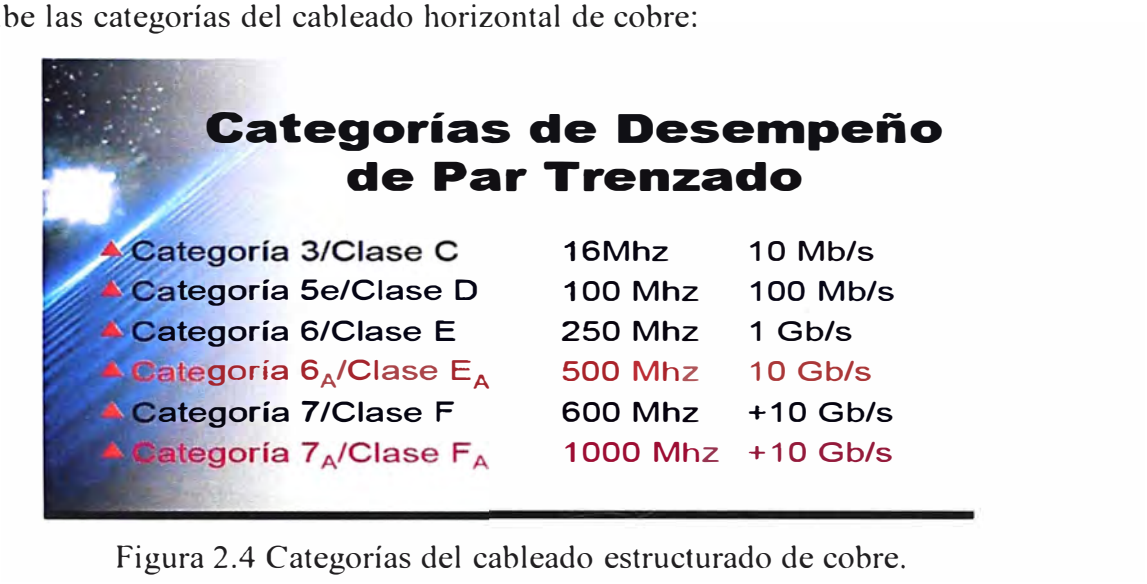


Figura 2.4 Categorías del cableado estructurado de cobre.

A continuación detallamos los componentes del cableado horizontal de la marca SIEMONS, utilizados en el del Hospital:

- **Cableado F/UTP categoría 6A**

En los cables F/UTP, la denominación F, asocia al blindaje del cable UTP, el cual ofrece las ventajas de un desempeño mejorado contra las diafonías de par a par y exógena, y una inmunidad al ruido que no puede alcanzarse con ninguna otra estrategia de diseño de cableado. Estan fabricado de conductores sólidos de cobre de 23AWG con aislamiento. Los conductore de cobre están trenzados en pares y separados por una cruceta.

La performance del canal certificado cumple los requerimientos de los estándar ISO 11801 Class Ea, A SI/TIA-568-C.2 para categoría 6A y soporta la transmisión 10GBASE-T sobre lo sistemas de cableado de par trenzado.

La performance de componentes certificado hasta los 100m cumple los requerimientos de componentes de los estándares ISO/IEC 11801 categoría 6A y ANSI/TIA 568-C.2 categoría 6A para soportar la transmisión 10GBASE-T sobre los sistemas de cableado de par trenzado. El rango de temperatura en la instalación y durante la operación debe ser entre: -20 a 75°C. Contiene en su chaqueta marcas de metraje en la longitud del cable para simple identificación de remanentes. Están construidos con una pantalla metálica que envuelve por completo cuatro pares trenzados. Se muestra en la figura 2.5, los detalles descritos:

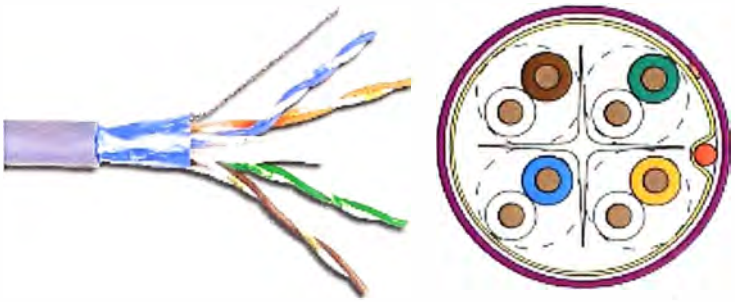


Figura 2.5 Blindaje de cable F/UTP Categoría 6A.

Tabla 2.1 Propiedades físicas del cable F/UTP de categoría 6A.

	LSOH	CM/CMR
Tensión de tracción (máx.)	110N	110N
Radio de curvatura (mín.)	50mm	50mm
Temperatura de instalación	0 a 60°C	0 a 60°C
Temperatura de almacenamiento	-20 a 75°C	-20 a 75°C
Temperatura de funcionamiento	-20 a 60°C	-20 a 60°C

- **Jacks RJ45 categoría 6A**

Los módulos Jack de Categoría 6A, cumplen los requerimientos de canal de los estándares ANSI/TIA-568-C.2 categoría 6A, IEEE 802.3an-2006, e ISO 11801 Class EA.

Cumple los requerimientos de la IEEE 802.3af y IEEE 802.3at para aplicaciones PoE. Cada Jack debe estar al 100% testeado para asegurar la performance de trabajo óptimo, y es serializado individualmente para la trazabilidad. Debe ser unido y conectado a tierra totalmente cuando se inserta en el patch panel metalizado.

La toma de conexión termina construcciones de cables del tipo S/FTP, F/FTP y F/UTP, con conductores sólidos de 22 – 26 AWG (0,64 – 0,51 mm) y con filamentos de 26 AWG (0,48 mm), con conductores de hasta 0,60 mm de diámetro y hasta 1,48 mm de diámetro con aislamiento.

- **Patch cords categoría 6A**

Los patch cord, cumplen los requerimientos de los estándares de canal ANSI/TIA-568-C.2 categoría 6A, IEEE 802.3an-2006, e ISO 11801 Class EA.

Cumple con los requisitos de la norma IEEE 802.3af y 802.3at para las aplicaciones PoE.

Cada cable de conexión tiene un rendimiento del 100% probado y conexionado según el estándar T568B. Esta construido con cable hebrado de cobre. Contiene un plug que cumple con todos los requisitos aplicables de ANSI/TIA/EIA-1096-A y cumple las especificaciones de IEC 60603-7. El plug utiliza un administrador de par integral para optimizar el rendimiento y la consistencia mediante la reducción de destrenzado de los conductores dentro de la clavija.

- **Patch Panel categoría 6A**

El patch panel cumple el estándar de montaje en racks de 19 pulgadas. Acepta módulos Jack RJ45 para F/UTP. Los paneles incluyen conexión a tierra integrada a través de lengüetas Quick-Ground de conexión de masa que se activan automáticamente durante la inserción de la toma Z-MAX.

2.1.2 Sub Sistema Troncal de Fibra Óptica

El término troncal, se refiere al cableado *backbone* de campus y/o subsistema vertical, en una implementación de una red de area local *(LAN)* que sigue la normativa de cableado estructurado.

En el subsistema vertical el cableado troncal *(backbone)* proporciona interconexiones entre cuartos de entrada de servicios de edificio, cuartos de equipo y cuartos de telecomunicaciones, el cableado del backbone incluye la conexión vertical entre pisos en edificios de varios pisos.

El Cableado troncal de campus, interconecta cada uno de los edificios del campus. El centro del sistema, es el distribuidor de campus. En el campus, las distancias son habitualmente altas, solo el cable de fibra óptica, puede cubrir estas necesidades.

La troncal de campus, emplea principalmente cables de fibra monomodo debido a sus bajas perdidas y a su ancho de banda. Existen diferentes topologías de red para un diagrama de medio fisico de transmisión, las cuales son del tipo: anillo, dorsal, dorsal dual, estrella, arbol y completas, según se muestra a continuación.

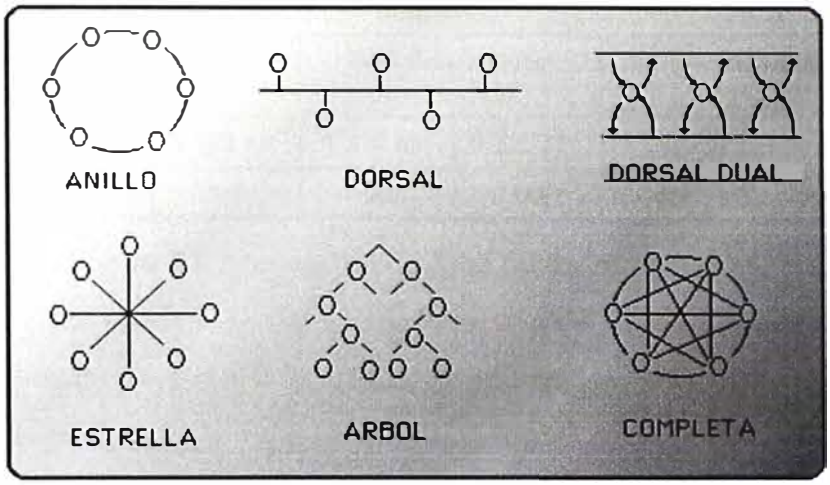


Figura 2.6 Topologías fisicas de redes de datos.

La topología en anillo, se caracteriza por un camino unidireccional cerrado que conecta todos los nodos y se utiliza cuando el control de acceso está distribuido por toda la red.

Según el ISO 11801, a continuación se describen los tipos de fibra óptica disponibles.

- **Fibra óptica tipo Multimodo**

OM1 & OM2 disponibles en versiones 50/125µ y 62,5/125µ.

OM3 & OM4 disponibles tan solo en versión 50/125µ.

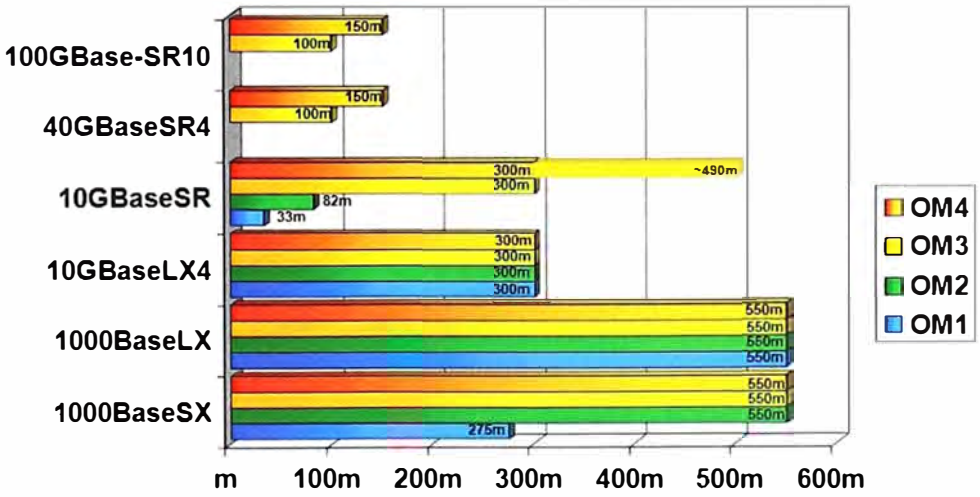


Figura 2.7 Alcance en metros que soporta la fibra multimodo.

- **Fibra óptica tipo Monomodo**

OS1 & OS2, las diferencias entre estos tipos de fibra óptica vienen dados por su atenuación kilométrica:

Cabled optical fibre attenuation (maximum) dB/km							
	OM1, OM2 OM3 and OM4 multimode		OS1 Single-mode		OS2 Single-mode		
Wavelength	850 nm	1 300 nm	1 310 nm	1 550 nm	1 310 nm	1 383 nm	1 550 nm
Attenuation	3,5	1,5	1,0	1,0	0,4	0,4	0,4

Figura 2.8 Atenuación de fibra óptica monomodo.

Se definen los tipos de fibra óptica y accesorios utulizados en la instalación de la troncal *(backbone)* del hospital.

- **Fibra óptica multimodo de 12 hilos 50/125 um**

La fibra óptica multimodo de 12 hilos 50/125 um Opti Core 10Gig LSZH, está diseñado para soportar velocidades de transmisión de red hasta 10Gbps para longitudes de enlace hasta 300m para OM3 y 500m para OM4, con una fuente de 850nm para el estándar IEEE 802.3ae 10GbE.

Es compatible para usar con todos los requerimientos de sistemas 50/125 um hacia atrás.

Es usado en troncales entre edificios *(backbone intrabuilding)*, trocales de edificios *(backbone Building)* e instalaciónes horizontales con OFNR (cable para interior sin elementos eléctricos conductivos, tendido vertical y que previenen la difusión del fuego de piso a piso), OFNP (tendido en ducteria, planos) y propósitos generales. Contiene la certificación LSZH, marcado en la chaqueta, cumple con los requerimientos de seguridad IEC 60332-1, IEC 60332-3C, IEC 61034 and IEC 60754-2. Las marcas de distancia de funda proveen identificación, calidad de trazabilidad y verificación de longitud.

- **Modulos acopladores duplex LC/LC para fibra óptica**

Los paneles son compatibles con TIA/EIA-604 FOCIS, contiene adaptadores dúplex de fibra óptica y cumple requerimientos TIA/EIA-568-B.3. Contiene 12 adaptadores dúplex LC/LC de bronce fosforado y se adaptan a los requerimientos específicos de la red. Soporta perdida de inserción menor de 0,1 dB promedio.

No contiene enganches metálicos. De menor tamaño que un adaptador SC.

- **Patch cord y pigtail multimodo LC de fibra óptica**

Son testeados para soportar velocidades de transmisión de red hasta 10Gbps para enlaces de longitud hasta de 300m con una fuente de 850nm para el estándar IEEE 802.3ae 10GbE
Pasa todos los requerimientos de performance TIA/EIA-568-B.3.
Soporta pérdida de inserción por conexión: 0,1dB típica; 0,30 dB máxima.
Es compatible para usar con todos los sistemas de 50/125 um hacia atrás.

- **Bandeja de fibra óptica**

Son instalados sobre estándar EIA con 19" de rieles de rack. Puede usar Patch panel estándar para montar los módulos y acopladores/adaptadores de fibra óptica.
Provee cubierta superior removible para el acceso a las conexiones de fibra y almacenamiento de elementos sueltos en la parte trasera de la bandeja.
Incluye kit de enrutamiento de cable de fibra óptica (arandelas, bridas, carretes, alivio de tensión y sistema de identificación) para la administración de cables.

- **Bandeja porta enpalme**

Contiene un kit para 12 empalmes mecánicos o por fusión. Mantiene el radio de curvatura mínimo y asegura la correcta administración de cables, contiene base y cubierta con bisagras plásticas y módulo de auto apilado con administrador de cables de fibra.

- **Gabinetes de altura completa (42hu)**

Los gabinetes de comunicaciones albergan el cableado F/UTP desplegados en los usuarios finales. Estos son fabricados en cumplimiento a estándares, con las siguientes caracteristicas de fabricación:
Marco soldado con autógena de intensidad alta.
Diseño y artesanía exquisito con medidas de precisión.
Con unidades ajustables de 19 " instalación estándar.
La puerta principal de alta densidad (patentado) y la puerta posterior permiten la protección del equipo, la ventilación y la operación confiable, contorneado de piezas en ángulo sobre 120 grados y tasa de ventilación sobre 71%.
Base con entrada de cable, cubierta opcional para cerrarse.
Puertas laterales con cerraduras para la protección.
Cerradura avanzada con luna opaca.

2.2 Fundamentos de Redes de Conmutadores

A principios de 1980 el desarrollo de redes originó desorden en mucho entidos. Se produjo un enorme crecimiento en la cantidad y tamaño de las redes. A medida que las empresas tomaron conciencia de las ventajas de usar tecnologías de conexión, las redes se expandían a casi la misma velocidad a la que se introducían las nuevas tecnologías de red, a raíz este crecimiento se desarrollo el Modelo OSI en 1980 por La Organización Internacional de Estándares (ISO). El estándar OSI es una normativa formada por siete capas, que define las diferentes fases por las que deben pasar los datos para viajar de un dispositivo a otro sobre una red de comunicaciones. Se trata de una normativa estandarizada, útil debido a la existencia de muchas tecnologías, fabricantes y compañías dentro del mundo de las comunicaciones, y al estar en continua expansión, se tuvo que crear un método para que todos pudieran entenderse de algún modo, incluso cuando las tecnologías no coincidieran. Siguiendo el esquema de este modelo se crearon numerosos protocolos. El advenimiento de protocolos más flexibles donde las capas no están tan desmarcadas y la correspondencia con los niveles no era tan clara puso a este esquema en un segundo plano. El modelo está dividido en siete capas que a continuación se describen:

Figura 2.9 Capas del modelo OSI.

2.2.1 Las Redes de Conmutadores Virtualizadas

A principios de la década de 1980 Ethernet ya era una tecnología consolidada que ofrecía una velocidad de 1 Mbits/s. Las redes Ethernet era, una red de difusión y como tal cuando dos estaciones transmiten simultáneamente se producen colisiones y se desperdicia ancho de banda en transmisiones fallidas. El diseño de Ethernet no ofrecía escalabilidad, CSMA/CD, el protocolo que controla el acceso al medio compartido en Ethernet, impone de por sí limitaciones en cuanto al ancho de banda máximo y a la máxima distancia entre dos estaciones. Conectar múltiples redes Ethernet era por aquel entonces complicado, y aunque se podía utilizar un router para la interconexión, estos eran caros y requería un mayor tiempo de procesado por paquete grande, aumentando el retardo.

La solución a estos problemas, fue brindado por el Dr. W. David Sincoskie, quien inventó el conmutador *(switch)* Ethernet con auto-aprendizaje, dispositivo de conmutación de tramas de nivel 2. Usar conmutadores *(switches)* para interconectar redes Ethernet permite separar dominios de colisión, aumentando la eficiencia y la escalabilidad de la red. Una red tolerante a fallos y con un nivel alto de disponibilidad requiere que se usen topologías redundantes: enlaces múltiples entre switches y equipos redundantes. De esta manera, ante un fallo en un único punto es posible recuperar de forma automática y rápida el servicio. Este diseño redundante requiere la habilitación del protocolo spanning tree (STP) para asegurarse de que solo haya activo un camino lógico para ir de un nodo a otro y evitar así el fenómeno conocido como tormentas *broadcast*. El principal inconveniente de esta topología lógica de la red erá que los conmutadores *(switches)* centrales se convertian en cuellos de botella, pues la mayor parte del tráfico circula a través de ellos.

El Dr. W. Sincoskie, consiguió aliviar la sobrecarga de los conmutadores *(switches)* inventando LAN virtuales al añadir una etiqueta a las tramas Ethernet para porder diferenciar el tráfico. Al definir varias LAN virtuales cada una de ellas tendrá su propio spanning tree y se podrá asignar los distintos puertos de un conmutador a cada una de las VLAN (red virtual de area local). Para unir VLAN que están definidas en varios conmutadores se puede crear un enlace especial llamado enlace (*trunk)*, por el que fluye tráfico de varias VLAN. Los conmutadores sabrán a qué VLAN pertenece cada trama observando la etiqueta VLAN (definida en la norma IEEE 802.1Q).

Aunque hoy en día el uso de LAN virtuales es generalizado en las redes Ethernet modernas, es habitual utilizarlas para separar dominios de difusión (*hosts* que pueden ser alcanzados por una trama *broadcast*).

Aunque las más habituales son las VLAN basadas en puertos, las redes de área local virtuales se pueden clasificar en cuatro tipos según el nivel de la jerarquía OSI en el que operen:

- La VLAN de nivel 1 (por puerto), también conocida como "port switching". Se especifica qué puertos del switch pertenecen a la VLAN, los miembros de dicha VLAN son los que se conecten a esos puertos. No permite la movilidad de los usuarios, habría que reconfigurar las VLANs si el usuario se mueve físicamente.
- En una VLAN de nivel 2 por direcciones MAC, se asignan hosts a una VLAN en función de su dirección MAC. Tiene la ventaja de que no hay que reconfigurar el dispositivo de conmutación si el usuario cambia su localización, es decir, se conecta a otro puerto de ese u otro dispositivo. El principal inconveniente es que si hay cientos de usuarios habría que asignar los miembros uno a uno.
- La VLAN de nivel 2 por tipo de protocolo, queda determinada por el contenido del campo tipo de protocolo de la trama MAC. Por ejemplo, se asociaría VLAN 1 al protocolo IPv4, VLAN 2 al protocolo IPv6, VLAN 3 a AppleTalk, VLAN 4 a IPX, etc.
- En una VLAN de nivel 3 por direcciones de subred (subred virtual), la cabecera de nivel 3 se utiliza para mapear la VLAN a la que pertenece. En este tipo de VLAN son los paquetes, y no las estaciones, quienes pertenecen a la VLAN. Estaciones con múltiples protocolos de red (nivel 3) estarán en múltiples VLANs.
- En una VLAN de niveles superiores, se crea para cada aplicación: FTP, flujos multimedia, correo electrónico, entre otros. La pertenencia a una VLAN puede basarse en una combinación de factores como puertos, direcciones MAC, subred, hora del día, forma de acceso, condiciones de seguridad del equipo, etc.

Protocolos en una VLAN.- Durante todo el proceso de configuración y funcionamiento de una VLAN es necesaria la participación de una serie de protocolos entre los que destacan el IEEE 802.1Q, STP y VTP (cuyo equivalente IEEE es GVRP). El protocolo IEEE 802.1Q se encarga del etiquetado de las tramas que es asociada inmediatamente con la información de la VLAN. El cometido principal de Spanning Tree Protocol (STP) es evitar la aparición de bucles lógicos para que haya un sólo camino entre dos nodos. El IEEE 802.1Q se caracteriza por utilizar un formato de trama similar a 802.3 (Ethernet) donde solo cambia el valor del campo Ethertype, que en las tramas 802.1Q vale X'8100, y se añaden dos bytes para codificar la prioridad, el CFI y el VLAN ID.

Para evitar el bloqueo de los switches debido a las tormentas broadcast, una red con topología redundante tiene que tener habilitado el protocolo STP. Los switches utilizan STP para intercambiar mensajes entre sí (BPDU, Bridge Protocol Data Units) para lograr de que en cada VLAN solo haya activo un camino para ir de un nodo a otro.

VLAN basadas en el puerto de conexión.- Las dos aproximaciones más habituales para la asignación de miembros de una VLAN son las siguientes: VLAN estáticas y VLAN dinámicas. Las VLAN estáticas también se denominan VLAN basadas en el puerto. Las asignaciones en una VLAN estática se crean mediante la asignación de los puertos de un switch o conmutador a dicha VLAN. Cuando un dispositivo entra en la red, automáticamente asume su pertenencia a la VLAN a la que ha sido asignado el puerto. Si el usuario cambia de puerto de entrada y necesita acceder a la misma VLAN, el administrador de la red debe cambiar manualmente la asignación a la VLAN del nuevo puerto de conexión en el switch.

En las VLAN dinámicas, la asignación se realiza mediante paquetes de software. Con el VMPS (acrónimo en inglés de VLAN Management Policy Server o Servidor de Gestión de Directivas de VLAN), el administrador de la red puede asignar los puertos que pertenecen a una VLAN de manera automática basándose en información tal como la dirección MAC del dispositivo que se conecta al puerto o el nombre de usuario utilizado para acceder al dispositivo. En este procedimiento, el dispositivo que accede a la red, hace una consulta a la base de datos de miembros de una VLAN.

Los puertos de un conmutador pueden ser de dos tipos, puertos de acceso y puertos trunk. Un puerto de acceso (switchport mode access) pertenece únicamente a una VLAN asignada de forma estática (VLAN nativa). En cambio, un puerto trunk (switchport mode trunk) puede ser miembro de múltiples VLANs.

El dispositivo que se conecta a un puerto, posiblemente no tenga conocimiento de la existencia de la VLAN a la que pertenece dicho puerto. El dispositivo sabe que es miembro de una subred y que puede ser capaz de hablar con otros miembros de la subred simplemente enviando información al segmento cableado. El conmutador es responsable de identificar que la información viene de una VLAN determinada y de asegurarse de que esa información llega a todos los demás miembros de la VLAN. El conmutador también se asegura de que el resto de puertos que no están en dicha VLAN no reciben dicha información.

Diseño de VLAN.- En las redes institucionales y corporativas modernas suelen estar configuradas de forma jerárquica dividiéndose en varios grupos de trabajo. Las razones de seguridad y confidencialidad aconsejan también limitar el ámbito del tráfico de difusión para que un usuario no autorizado no pueda acceder a recursos o a información que no le corresponde. Por ejemplo, la red institucional de un campus universitario suele separar los usuarios en tres grupos: alumnos, profesores y administración. Cada uno de estos grupos constituye un dominio de difusión, una VLAN, y se suele corresponder asimismo con una subred IP diferente. De esta manera la comunicación entre miembros del mismo grupo se puede hacer en nivel 2, y los grupos están aislados entre sí, sólo se pueden comunicar a través de un router.

La definición de múltiples VLANs y el uso de enlaces trunk, frente a las redes LAN interconectadas con un router, es una solución escalable. Si se deciden crear nuevos grupos se pueden acomodar fácilmente las nuevas VLANs haciendo una redistribución de los puertos de los conmutadores. En cada edificio de la universidad hay un conmutador denominado de acceso, porque a él se conectan directamente los sistemas finales. Los conmutadores de acceso están conectados con enlaces trunk (enlace que transporta tráfico de las tres VLANs) a un conmutador troncal, de grandes prestaciones. Este conmutador está unido a un ruteador de red *(router)* también con un enlace trunk, el ruteador de red *(router)* es el encargado de llevar el tráfico de una VLAN a otra.

2.2.2 Protocolos de Red a Nivel de Administración

A continuación se describe teoricamente los protocolos aplicados en el presente informe.

- **Protocolo HTTPS.**- Hypertext Transfer Protocol Secure (Protocolo seguro de transferencia de hipertexto), es un protocolo de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de Hipertexto, es decir, es la versión segura de HTTP, para el envío de datos personales o contraseñas.

  HTTP opera en la capa más alta del modelo OSI, la capa de aplicación; pero el protocolo de seguridad opera en una subcapa más baja, cifrando un mensaje HTTP previo a la transmisión y descifrando un mensaje una vez recibido. Estrictamente hablando, HTTPS no es un protocolo separado, pero refiere el uso del HTTP ordinario sobre una Capa de Conexión Segura cifrada Secure Sockets Layer (SSL) o una conexión con Seguridad de la Capa de Transporte (TLS).

- **Protocolo SSH.**- Secure SHell File Transfer Protocol, también conocido como SFTP o Secure File Transfer Protocol) es un protocolo del nivel de aplicación que proporciona la funcionalidad necesaria para la transferencia y manipulación de archivos sobre un flujo de datos fiable. Se utiliza comúnmente con SSH para proporcionar la seguridad a los datos, aunque permite ser usado con otros protocolos de seguridad. Por lo tanto, la seguridad no la provee directamente el protocolo SFTP, sino SSH o el protocolo que sea utilizado en su caso para este cometido.

  El Secure Internet Live Conferencing (SILC) define el protocolo SFTP como su protocolo de transferencia de archivos por omisión. En el SILC, los datos del protocolo SFTP no están protegidos con SSH pero el protocolo de paquetes seguros de SILC se utiliza para encapsular los datos SFTP dentro de los paquetes de SILC para que se la llevara de igual a igual (peer to peer, P2P). Esto es posible ya que SFTP está diseñado para ser un protocolo independiente. SFTP utiliza el puerto 22 de TCP.

- **Protocolo SNMPV3.**- El protocolo Simple de Administración de Red o SNMP (Simple Network Management Protocol) es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Los dispositivos que soportan SNMP incluyen routers, switches, servidores, estaciones de trabajo, impresoras, etc. El SNMPv3 se centra en dos aspectos principales, la seguridad y la administración. El aspecto de seguridad se dirige, ofreciendo tanto una sólida autenticación y cifrado de datos para la privacidad. El aspecto de la administración se centra en dos partes, a saber los originadores de notificación y agentes proxy.

  Un objeto administrado (algunas veces llamado objeto MIB, objeto, o MIB) es uno de cualquier número de características específicas de un dispositivo administrado. Los objetos administrados están compuestos de una o más instancias de objeto, que son esencialmente variables.

  El agente SNMP recibe solicitudes en el puerto UDP 161. El administrador puede enviar solicitudes de cualquier puerto de origen disponible para el puerto 161 en el agente. La respuesta del agente será enviado de vuelta al puerto de origen en el gestor. El administrador recibe notificaciones (Trampas y InformRequests) en el puerto 162. El agente puede generar notificaciones desde cualquier puerto disponible. Cuando se utiliza con Transport Layer Security o datagramas de Transport Layer Security solicitudes se reciben en el puerto 10161 y trampas se envían al puerto 10162.

- **Servicio de NTP (Network Time Protocol) Server.-** Es un protocolo de Internet para sincronizar los relojes de los sistemas informáticos a través del enrutamiento de paquetes en redes con latencia variable. NTP utiliza UDP como su capa de transporte, usando el puerto 123. Está diseñado para resistir los efectos de la latencia variable. NTP utiliza un sistema de jerarquía de estratos de reloj, en donde los sistemas de estrato 1 están sincronizados con un reloj externo tal como un reloj GPS ó algún reloj atómico. Los sistemas de estrato 2 de NTP derivan su tiempo de uno ó más de los sistemas de estrato 1, y así consecutivamente (cabe mencionar que esto es diferente de los estrato de reloj utilizados en los sistemas de telecomunicaciones).

2.2.3 Protocolos de Red a Nivel de Capa 2 del Modelo OSI

A continuación se describe teoricamente los protocolos aplicados en el presente informe.

- **Enlace agregado dinámico mediante el protocolo estándar IEEE 802.3ad (LACP).-** La agregación de enlaces IEEE 802.3ad, es un término que indica el establecimiento de una red de datos que describe cómo utilizar varios enlaces Ethernet full-dúplex en la comunicación entre dos equipos, repartiendo el tráfico entre ellos.

  Trunking o la agregación de enlaces es una manera económica de instalar una red de alta velocidad más rápida de lo que permita un solo puerto o dispositivo de la tecnología de que se disponga. Consiste en agrupar varios dispositivos que trabajan simultáneamente a su velocidad máxima como si fuera un único enlace de mayor capacidad. Esto también resuelve los problemas de enrutamiento que causa el tener varios caminos al mismo destino ya que a nivel de red el grupo de enlaces se presenta como un único enlace de mayor capacidad. La agregación de enlace permite que la velocidad de los enlaces de la red crezca incrementalmente como respuesta a una demanda creciente en el uso de la red sin tener que sustituir el hardware actual.

  En la mayoría de las instalaciónes, es común instalar y conectorizar más medios fisicos (fibra óptica y par trenzado) de lo estrictamente necesario. Se hace esto porque el costo de la mano de obra de instalación es mucho más alto que el del cable y evita volver a instalar más medios de transmisión ante un aumento de las necesidades de la red.

  La agregación de enlaces no sólo puede ser realizada por un conmutador. Las tarjetas de interfaz de la red (NICs) pueden también a veces estar agregadas juntas para formar acoplamientos de red. Por ejemplo, esto permite que un servidor de archivo central establezca una conexión de 2 Gbps que usan dos NICs agregados juntos a 1 Gbps.

El Multi-Link Trunking (MLT) o Troncal Multi-Enlace es una tecnología de agregación de enlaces definida por el estándar IEEE 802.3ad diseñada por Nortel. Permite la agrupación de varios enlaces físicos Ethernet en un único enlace lógico Ethernet para proporcionar tolerancia a fallos y enlaces de alta velocidad entre routers, switches y servidores. La utilización de esta tecnología permite el uso de varios enlaces (entre 2 y 8) combinándolos para aumentar el ancho de banda y caminos alternativos de fallo. De este modo se pueden crear conexiones entre un switch y un servidor o entre switches hasta 8 veces más rápido.

- **Protocolo IEEE 802.3af (Power over Ethernet - PoE).-** La alimentación a través de Ethernet (PoE) incorpora la alimentación eléctrica a una infraestructura LAN estándar. Permite que la alimentación eléctrica se suministre a un dispositivo de red (switch, punto de acceso, router, teléfono o cámara IP, etc) usando el mismo cable que se utiliza para la conexión de red. Elimina la necesidad de utilizar tomas de corriente en las ubicaciones del dispositivo alimentado. Está diseñado de manera que no haga disminuir el rendimiento de comunicación de los datos en la red. La corriente suministrada a través de la infraestructura LAN se activa de forma automática cuando se identifica un terminal compatible y se bloquea ante dispositivos que no sean compatibles.

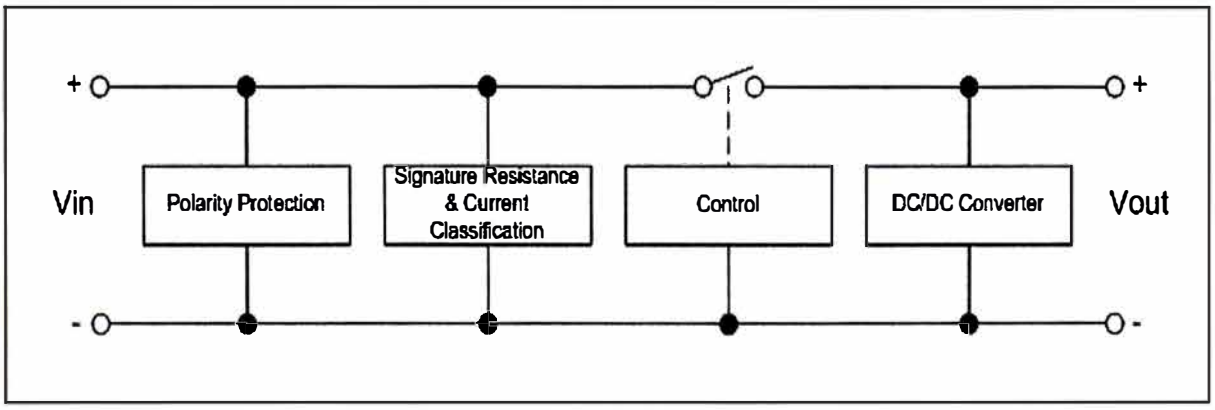


Figura 2.10 Fases de la alimentación eléctrica a través del cableado F/UTP de red.

Las fases del funcionamiento PoE son 4, según la figura, se proceden a describirlos:

- En el primer bloque "Polarity Protection" o "Auto-polarity Circuit", la tensión introducida puede venir de dos formas: una de las formas consiste en usar el par de datos del cable de Ethernet como fuente de alimentación. Dicha forma permite transmitir datos y alimentar a la vez por el mismo par. La segunda forma usa otros

pares alternativos para enviar la tensión. La ventaja de la primera forma es que usa un par, en vez de 2.

- En el segundo bloque "Signature and Class circuitry", para asegurarse que el dispositivo no aplica una tensión a un dispositivo que no implementa PoE, el dispositivo empezará a dar unos determinados niveles de tensión. Estos niveles de tensión se dividen en 4 etapas. Al principio el dispositivo aplicará una tensión baja (2.7V a 10.1V) buscando una resistencia de 25KΩ. Si es demasiado alta o demasiado baja, no hará nada. Esta fase permite proteger un dispositivo que no es PoE de uno que sí que lo es. En caso de que resulte ser PoE, buscará que clase de alimentación requiere. Para ello, elevará la alimentación a 14,5-20,5 V y medirá la corriente que circula a través de él.
- En el tercer bloque "Control Stage", es importante que el convertidor DC/DC no funcione mientras el dispositivo está realizando la fase de clasificación del bloque dos. El controlador deberá estar encendido cuando V = 35 V
- En el cuarto bloque "Convertidor DC/DC", generalmente la tensión nominal usada es de 48V y no suele ser práctica en muchas aplicaciones, dónde se requiere un voltaje menor (3.3V, 5V o 12V). Una manera muy efectiva de lograr este objetivo es usar un convertidor Buck DC/DC. Este convertidor es capaz de trabajar en un amplio rango de tensiones (36V a 57V), en condiciones de mínima y máxima carga.

- **UNP de Protección (802.1x Radius Down Fail Open).-** La IEEE 802.1X es una norma del IEEE para el control de acceso a red basada en puertos. Es parte del grupo de protocolos IEEE 802 (IEEE 802.1). Permite la autenticación de dispositivos conectados a un puerto LAN, estableciendo una conexión punto a punto o previniendo el acceso por ese puerto si la autenticación falla. Es utilizado en algunos puntos de acceso inalámbricos cerrados y se basa en el protocolo de autenticación extensible (EAP– RFC 2284). El 802.1X está disponible en ciertos conmutadores de red y puede configurarse para autenticar nodos que están equipados con software suplicante. Esto elimina el acceso no autorizado a la red al nivel de la capa de enlace de datos.

  Algunos proveedores están implementando 802.1X en puntos de acceso inalámbricos que pueden utilizarse en ciertas situaciones en las cuales el punto de acceso necesita operarse como un punto de acceso cerrado, corrigiendo deficiencias de seguridad de WEP. Esta autenticación es realizada normalmente por un tercero, tal como un servidor

radius. Esto permite la autenticación sólo del cliente o, más apropiadamente, una autenticación mutua fuerte utilizando protocolos como EAP-TLS.

El Protocolo EAP se encapsula primero en EAPOL entre el suplicante y el autenticado, luego re-encapsulada entre el autenticado y el servidor de autenticación por medio de radios o diámetros.

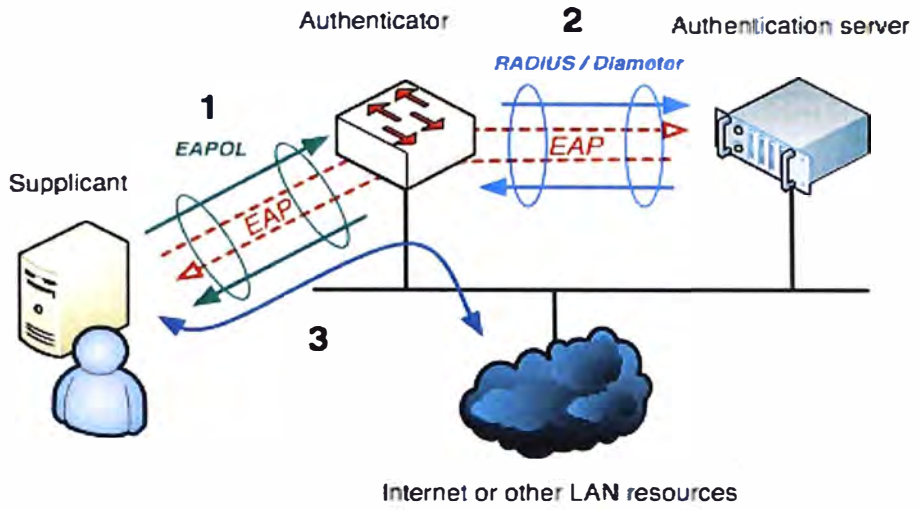


Figura 2.11 Encapsulado EAP.

- **Protocolo estándar IEEE 802.1ab (LLDP) y del protocolo propietario AMAP.-** Para el reconocimiento de los diversos equipos de red y formación de la topología de red.

- **Protocolo Spannnig tree modo 1x1.-** Es un protocolo de red de nivel 2 del modelo OSI. Su función es la de gestionar la presencia de bucles en topologías de red debido a la existencia de enlaces redundantes (necesarios en muchos casos para garantizar la disponibilidad de las conexiones). El protocolo permite a los dispositivos de interconexión activar o desactivar automáticamente los enlaces de conexión, de forma que se garantice la eliminación de bucles. STP es transparente a las estaciones de usuario. Los puentes se comunican mediante mensajes de configuración llamados Bridge Protocol Data Units (BPDU).

  El protocolo establece identificadores por puente y elige el que tiene la prioridad más alta (el número más bajo de prioridad numérica), como el puente raíz (Root Bridge). Este puente raíz establecerá el camino de menor coste para todas las redes; cada puerto tiene un parámetro configurable: el Span path cost. Después, entre todos lo puentes

que conectan un segmento de red, se elige un puente designado, el de menor coste (en el caso que haya el mismo coste en dos puentes, se elige el que tenga el menor identificador "direccion MAC"), para transmitir las tramas hacia la raíz. En este puente designado, el puerto que conecta con el segmento, es el puerto designado y el que ofrece un camino de menor coste hacia la raíz, el puerto raíz. Todos los demás puertos y caminos son bloqueados, esto es en un estado ya estacionario de funcionamiento.

- La elección del puente raíz, es la primera decisión que toman todos los switches de la red es identificar el puente raíz ya que esto afectará al flujo de tráfico. Cuando un switch se enciende, supone que es el switch raíz y envía las BPDUs que contienen la dirección MAC de sí mismo tanto en el BID raíz como emisor. El BID es el Bridge IDentifier: Bridge Priority + Bridge Mac Address. El Bridge Priority es un valor configurable que por defecto está asignado en 32768. El Bridge Mac Address es la dirección MAC (única) del Puente. Cada switch reemplaza los BID de raíz más alta por BID de raíz más baja en las BPDU que se envían. Todos los switches reciben las BPDU y determinan que el switch que cuyo valor de BID raíz es el más bajo será el puente raíz. El administrador de red puede establecer la prioridad de switch en un valor más pequeño que el del valor por defecto (32768), el nuevo valor debe ser multiplo de 4096, lo que hace que el BID sea más pequeño. Esto sólo se debe implementar cuando se tiene un conocimiento profundo del flujo de tráfico en la red.
- Una vez elegido el puente raíz hay que calcular el puerto raíz para los otros puentes que no son raíz. El procedimiento a seguir para cada puente es el mismo: entre todos los puertos del puente, se escoge como puerto raíz el puerto que tenga el menor costo hasta el puente raíz. En el caso de que haya dos o más puertos con el mismo costo hacia el puente raíz, se utiliza la prioridad del puerto para establecer el raíz.
- La elección de los puertos designados como puente raíz y los puertos raíz de los otros puentes, pasamos a calcular los puertos designados de cada segmento de red. En cada enlace que exista entre dos switches habrá un puerto designado, el cual será el puerto del switch que tenga un menor coste para llegar al puente raíz, este coste administrativo será un valor que estará relacionado al tipo de enlace que exista en el puerto (Ethernet, FastEthernet, GigabitEthernet). Cada tipo de enlace tendrá un coste administrativo distinto, siendo de un coste menor el puerto con una

mayor velocidad. Si hubiese empate entre los costes administrativos que tienen los dos switches para llegar al root bridge, entonces se elegirá como Designated Port, el puerto del switch que tenga un menor Bridge ID (BID).

- Los puertos bloqueados son aquellos que no son elegidos como raíz ni como designados deben bloquearse.

- **Calidad de servicio (QoS) y DSCP.**- La calidad de servicio corresponde al estándar IEEE 802.1p, que proporciona priorización de tráfico y filtrado multicast dinámico. Esencialmente, proporciona un mecanismo para implementar Calidad de Servicio (QoS) a nivel de MAC (Media Access Control).

  Existen 8 clases diferentes de servicios, expresados por medio de 3 bits del campo prioridad de usuario (user_priority) de la cabecera IEEE 802.1Q añadida a la trama, asignando a cada paquete un nivel de prioridad entre 0 y 7. Aunque es un método de priorización bastante utilizado en entornos LAN, cuenta con varios inconvenientes, como el requerimiento de una etiqueta adicional de 4 bytes (definida en el estándar IEEE802.1Q). Además solo puede ser soportada en una LAN, ya que las etiquetas 802.1Q se eliminan cuando los paquetes pasan a través de un router.

  No está definida la manera de cómo tratar el tráfico que tiene asignada una determinada clase o prioridad, dejando libertad a las implementaciones. IEEE, sin embargo, ha hecho amplias recomendaciones al respecto. El IEEE 802.1p está integrado en los estándares IEEE 802.1D y 802.1Q.

2.2.4 Protocolos de Red a Nivel de Capa 3 del Modelo OSI

A continuación se describe teoricamente los protocolos aplicados en el presente informe.

Enrutamiento OSPF.- Son las siglas de Open Shortest Path First (El camino mas corto primero), un protocolo de enrutamiento jerárquico de pasarela interior o IGP (Interior Gateway Protocol), que usa el algoritmo SmoothWall Dijkstra enlace-estado (LSE - Link State Algorithm) para calcular la ruta más idónea. Su medida de métrica se denomina cost, y tiene en cuenta diversos parámetros tales como el ancho de banda y la congestión de los enlaces. OSPF construye además una base de datos enlace-estado (link-state database, LSDB) idéntica en todos los enrutadores de la zona. OSPF puede operar con seguridad usando MD5 para autentificar sus puntos antes de realizar nuevas rutas y antes de aceptar avisos de enlace-estado. OSPF es probablemente el protocolo IGP más utilizado en redes

grandes. El protocolo IS-IS, es tambien de enrutamiento dinámico de enlace estado, es más común en grandes proveedores de servicios. Como sucesor natural de RIP, acepta VLSM y CIDR desde su inicio. A lo largo del tiempo, se han ido creando nuevas versiones, como OSPFv3 que soporta IPv6 o las extensiones multidifusión para OSPF (MOSPF), aunque no están demasiado extendidas. OSPF puede "etiquetar" rutas y propagar esas etiquetas por otras rutas. Una red OSPF se puede descomponer en regiones (áreas) más pequeñas. Hay un área especial llamada área backbone que forma la parte central de la red a la que se encuentran conectadas el resto de áreas de la misma. Las rutas entre las diferentes áreas circulan siempre por el backbone, por lo tanto todas las áreas deben conectar con el backbone. Si no es posible hacer una conexión directa con el backbone, se puede hacer un enlace virtual entre redes.

Los encaminadores (también conocidos como enrutadores, o routers) en el mismo dominio de multidifusión o en el extremo de un enlace punto-a-punto forman enlaces cuando se descubren los unos a los otros. En un segmento de red Ethernet los encaminadores eligen a un encaminador designado (Designated Router, DR) y un encaminador designado secundario o de copia (Backup Designated Router, BDR) que actúan como hubs para reducir el tráfico entre los diferentes encaminadores. OSPF puede usar tanto multidifusiones como unidifusiones para enviar paquetes de bienvenida y actualizaciones de enlace-estado. Las direcciones de multidifusión usadas son 224.0.0.5 y 224.0.0.6. Al contrario que RIP o BGP, OSPF no usa ni TCP ni UDP, sino que usa el protocolo IP directamente, mediante IP 89.

Tráfico de enrutamiento del OSPF.- El trafico mantiene actualizada la capacidad de enrutamiento entre los nodos de una red mediante la difusión de la topología de la red y la información de estado-enlace de sus distintos nodos. Esta difusión se realiza a través de varios tipos de paquetes:

- En el paquetes Hello (tipo 1), cada router envía periódicamente a sus vecinos un paquete que contiene el listado de vecinos reconocidos por el router, indicando el tipo de relación que mantiene con cada uno.
- En los Paquetes de descripción de base de datos estado-enlace (tipo 2), se emplean en el intercambio de base de datos enlace-estado entre dos nodos, y permiten informar al otro nodo implicado en la sincronización acerca de los registros contenidos en la LSDB propia, mediante un resumen de estos.

- En los paquetes de estado-enlace o Link State Advertisements (LSA), los cambios en el estado de los enlaces de un router son notificados a la red mediante el envío de mensajes LSA. Dependiendo del estado del router y el tipo de información transmitido en el LSA, se distinguen varios formatos (entre paréntesis, las versiones de OSPF en que se utilizan):
  - (OSPFv2 y v3) Router-LSA o LSA de encaminador.
  - (OSPFv2 y v3) Network-LSA o LSA de red.
  - (OSPFv2 y v3) Summary-LSA o LSA de resumen. En OSPFv2 se distinguen dos tipos: tipo 3, dirigidos a un router fronterizo de red; y tipo 4, dirigidos a una subred interna. En OSPFv3, los Summary-LSA tipo 3 son renombrados como Inter-Area-Prefix-LSA, y los tipo 4 pasan a denominarse Intra-Area-Prefix-LSA.
  - (OSPFv2 y v3) AS-External-LSA o LSA de rutas externas a la red.
  - (OSPFv3) Link-LSA o LSA de enlace, que no se retransmite más allá del link del origen.

Enrutamiento, routeadores y áreas del OSPF.- El enrrutamiento organiza un sistema autónomo (AS) en áreas. Estas áreas son grupos lógicos de routers cuya información se puede resumir para el resto de la red. Un área es una unidad de enrutamiento, es decir, todos los routers de la misma área mantienen la misma información topológica en su base de datos de estado-enlace (Link State Database): de esta forma, los cambios en una parte de la red no tienen por qué afectar a toda ella..

Interfaces en OSPF.- La interface se conecta a los nodos de una red basada en OSPF a través de una o varias interfaces con las que se conectan a otros nodos de la red. El tipo de enlace (link) define la configuración que asume la interfaz correspondiente. OSPF provee una configuración de interfaz y soporta los siguientes tipos de enlace:

- El punto a punto (point-to-point, abreviadamente PTP), es cuando la interfaz está conectada exclusivamente a otra interfaz.
- El punto a multipunto (point-to-multipoint, abreviadamente ptmp).
- El broadcast, para enlaces en los que todas las interfaces pueden conectarse directamente entre ellas. El ejemplo típico de enlace broadcast es el que corresponde a una red de tipo Ethernet.
- El enlace virtual (virtual link), es cuando no responde a una topología física.

- El enlace de acceso múltiple acceso sin difusión (Non-Broadcast Multiple Access, NBMA), es para enlaces en los que el medio es compartido, pero no todas las interfaces participantes pueden comunicarse directamente entre sí.

Estados de OSPF.- Estos están desactivados (DOWN). En el estado desactivado, el proceso OSPF no ha intercambiado información con ningún vecino. OSPF se encuentra a la espera de pasar al siguiente estado (Estado de Inicialización).

En el estado inicialización (INIT), los enrutadores (routers) OSPF envían paquetes tipo 1, o paquetes Hello, a intervalos regulares con el fin de establecer una relación con los Routers vecinos. Cuando una interfaz recibe su primer paquete Hello, el router entra al estado de Inicialización. Esto significa que este sabe que existe un vecino a la espera de llevar la relación a la siguiente etapa. Los dos tipos de relaciones son Bidireccional y Adyacencia. Un router debe recibir un paquete Hello (Hola) desde un vecino antes de establecer algún tipo de relación.

En el estado Bidireccional (TWO-WAY, encaminador igual enrutador), se emplea paquetes Hello, cada enrutador OSPF intenta establecer el estado de comunicación bidireccional (dos-vías) con cada enrutador vecino en la misma red IP. Entre otras cosas, el paquete Hello incluye una lista de los vecinos OSPF conocidos por el origen. Un enrutador ingresa al estado Bidireccional cuando se ve a sí mismo en un paquete Hello proveniente de un vecino. El estado Bidireccional es la relación más básica que vecinos OSPF pueden tener, pero la información de encaminamiento no es compartida entre estos. Para aprender los estados de enlace de otros enrutadores y eventualmente construir una tabla de enrutamiento, cada enrutador OSPF debe formar a lo menos una adyacencia. Una adyacencia es una relación avanzada entre enrutadores OSPF que involucra una serie de estados progresivos basados no solo en los paquetes Hello, sino también en el intercambio de otros 4 tipos de paquetes OSPF. Aquellos encaminadores intentando volverse adyacentes entre ellos intercambian información de encaminamiento incluso antes de que la adyacencia sea completamente establecida. El primer paso hacia la adyacencia es el estado ExStart.

El inicio de Intercambio (EXSTART), es técnicamente cuando un encaminador y su vecino entran al estado ExStart, su conversación es similar a aquella en el estado de Adyacencia. ExStart se establece empleando descripciones de base de datos tipo 2 (paquetes DBD), también conocidos como DDPs. Los dos encaminadores vecinos emplean paquetes Hello

para negociar quien es el "maestro" y quien es el "esclavo" en su relación y emplean DBD para intercambiar bases de datos. Aquel encaminador con el mayor router ID "gana" y se convierte en el maestro. Cuando los vecinos establecen sus roles como maestro y esclavo entran al estado de Intercambio y comienzan a enviar información de encaminamiento.

En el estado de intercambio, los encaminadores vecinos emplean paquetes DBD tipo 2 para enviarse entre ellos su información de estado de enlace. En otras palabras, los encaminadores se describen sus bases de datos de estado de enlace entre ellos. Los encaminadores comparan lo que han aprendido con lo que ya tenían en su base de datos de estado de enlace. Si alguno de los encaminadores recibe información acerca de un enlace que no se encuentra en su base de datos, este envía una solicitud de actualización completa a su vecino. Información completa de encaminamiento es intercambiada en el estado Cargando.

En estado cargando (LOADING), ocurre después de que las bases de datos han sido completamente descritas entre vecinos, estos pueden requerir información más completa empleando paquetes tipo 3, requerimientos de estado de enlace (LSR). Cuando un enrutador recibe un LSR este responde empleando un paquete de actualización de estado de enlace tipo 4 (LSU). Estos paquetes tipo 4 contienen las publicaciones de estado de enlace (LSA) que son el corazón de los protocolos de estado de enlace. Los LSU tipo 4 son confirmados empleando paquetes tipo 5 conocidos como confirmaciones de estado de enlace (LSAcks).

El estado adyacencia completa (FULL), es cuando el estado de carga ha sido completada, los enrutadores se vuelven completamente adyacentes. Cada enrutador mantiene una lista de vecinos adyacentes, llamada base de datos de adyacencia.

CAPITULO III
IMPLEMENTACIÓN Y AMPLIACIÓN DE UN SISTEMA DE CONMUTADORES DE ALTA DISPONIBILIDAD

La Implementación del Sistema de Alta Disponibilidad de Conmutadores de Red, para las Nuevas Sedes del Hospital Guillermo Almenara, ha contemplado la implementación de dos plataformas, la de Cableado Estructurado con troncal de Fibra Óptica de distribución tipo anillo entre las sedes, y la de Conmutadores *(Switch)* de Red para la gestión del Tráfico.

3.1 Descripción de la Plataforma de Cableado Estructurado

Se procede a describir la implementación desarrollada de esta plataforma.

3.1.1 Alcance de la Plataforma de Cableado Estructurado

El proyecto ha comprendido la implementación de una plataforma del Cableado Estructurado para Las Nuevas Sedes de Consulta Externa y Emergencia del Hospital Guillermo Almenara Irigoyen, donde se ha contemplado los siguientes sub sistemas:

- Área de Trabajo.
- Cableado Horizontal
- Cableado Backbone Vertical Inter-edificio
- Cableado Backbone Vertical Campus

La nueva plataforma de Cableado Estructurado debe ser capaz de soportar las exigencias de las normas para el desempeño a velocidades de 10Gb/s, en la norma para cableado F/UTP de categoría 6A (categoría 6 aumentada). El proyecto abarca el despliegue de 1088 puntos de red, para las aplicaciones IP de, voz, datos, cámaras y wireless.

3.1.2 Implementación de la Plataforma de Cableado Estructurado

El desarrollo del proyecto ha comprendido la implementación del Cableado Estructurado para los servicios de voz (telefonía), datos, cámaras y Wireless para Las Nuevas Sedes, los

puntos de red fueron distribuidos en las distintas oficinas, consultorios y áreas de acuerdo a las necesidades requeridas por ESSALUD.

La implementación ha sido desplegada dentro de los ductos existentes en las nuevas sedes, según rutas de los planos entregados por el ESSALUD. La plataforma de cableado contempló las siguientes actividades:

- Despliegue del Cableado Estructurado en La Nueva Consulta Externa, para los puntos de red F/UTP, y troncal de fibra óptica interna entre los gabinetes de comunicaciones secundario de cada piso.
- Despliegue del Cableado Estructurado de Nueva Emergencia, para los puntos de red F/UTP, y troncal de fibra óptica interno entre los gabinetes de comunicaciones de cada piso.
- Despliegue de la troncal *(backbone)* de campus externa de fibra óptica entre los nodos principales de las nuevas sedes con la sede principal existente del Hospital.

El cableado de cobre F/UTP en Categoría 6A, ha sido instalado sobre las canalizaciones existentes según diseño de los edificios, las cuales contemplaron:

- Bandejas Metálica sobre el cielo raso.
- Tubería conduit empotradas y adosadas para las derivaciones finales de usuarios.

La conectorización de los puntos de red en un área de trabajo, se ha sido realizado en los puntos de usuarios finales y en gabinetes de comunicaciones. La identificación y etiquetado, bajo la norma TIA-606, ha sido definida con el patrón **GDS X0Y-W01:**

- GDS: Gabinete de Distribución Secundario
- X: Piso del edificio
- Y: Número de Gabinete
- W: D/ V/AP/C: Aplicación de Datos, Voz, Access Point o Cámaras
- 01: Número de Punto en gabinete.

Se procede a describir las actividades en cada nueva sede, según el alcance definido.

Cableado Estructurado para la nueva Consulta Externa.- El edificio está comprendido por 6 pisos y un sótano, se han instalado puntos de red a nivel de usuario final, según el requerimiento en cantidad y ubicación definido por el ESSALUD, las mismas que fueron

ratificadas en la planificación del proyecto. A continuación se detallan las cantidades de puntos de red desplegados por piso, según cada aplicación requerida.

Tabla 3.1 Distribución de puntos de red por gabinete – Nueva Consulta Externa.

Ubicación	Telecom	Datos	Voz IP	Access Point	Cámaras IP	Puntos de datos
Piso 1	GDS-101	79	49	4	21	153
Piso 1	GDS-102	7	3	0	2	12
Piso 2	GDS-201	52	44	6	9	111
Piso 3	GDS-301	46	40	6	9	101
Piso 4	GDS-401	42	41	7	9	99
Piso 5	GDS-501	39	36	7	11	93
Piso 6	GDS-601	32	23	6	9	70
					Total de Puntos	639

Se ha realizado el montaje de gabinetes de comunicaciones de 42UR y de 24 UR los cuales han sido distribuidos según el siguiente cuadro.

Tabla 3.2 Tipo de gabinete por piso – Nueva Consulta Externa.

Ubicación	Telecom	Gabinete de 42 UR	Gabinete de 24 UR
Piso 1	GDP	1	
Piso 1	GDS-101	1	
Piso 1	GDS-102		1
Piso 2	GDS-201	1	
Piso 3	GDS-301	1	
Piso 4	GDS-401	1	
Piso 5	GDS-501		1
Piso 6	GDS-601	1	

La troncal de fibra óptica interna de la sede consulta externa, desplegada en cada Gabinete de Distribución Secundaria (GDS), ha contemplado un enlace de fibra óptica multimodo de 12 hilos OM4, para la interconexión con el Gabinete de Distribución Principal (GDP). La topología implementada fue de tipo estrella escalable.

Las terminaciones del cable de fibra óptica han sido realizadas en las bandejas de fibra óptica ubicadas en el interior de cada gabinete GDS, utilizando extensiones ópticas con conector de tipo LC, la conexión de la fibra óptica se realizó con el método de empalme por fusión.

A continuación se detallan las cantidades de empalmes fusionados por hilo de fibra óptica.

Tabla 3.3 Hilos de fibra por cada gabinete de piso – Nueva Consulta Externa.

Ubicación	Telecom	Cantidad de hilos de fibra	
		GDP	GDS
Piso 1	GDP	72	
Piso 1	GDS-101		12
Piso 1	GDS-102		6
Piso 2	GDS-201		12
Piso 3	GDS-301		12
Piso 4	GDS-401		12
Piso 5	GDS-501		12
Piso 6	GDS-601		6

Se muestra el diagrama físico de la distribución de fibra óptica tipo estrella escalable interna de la Sede Nueva Consulta Externa.

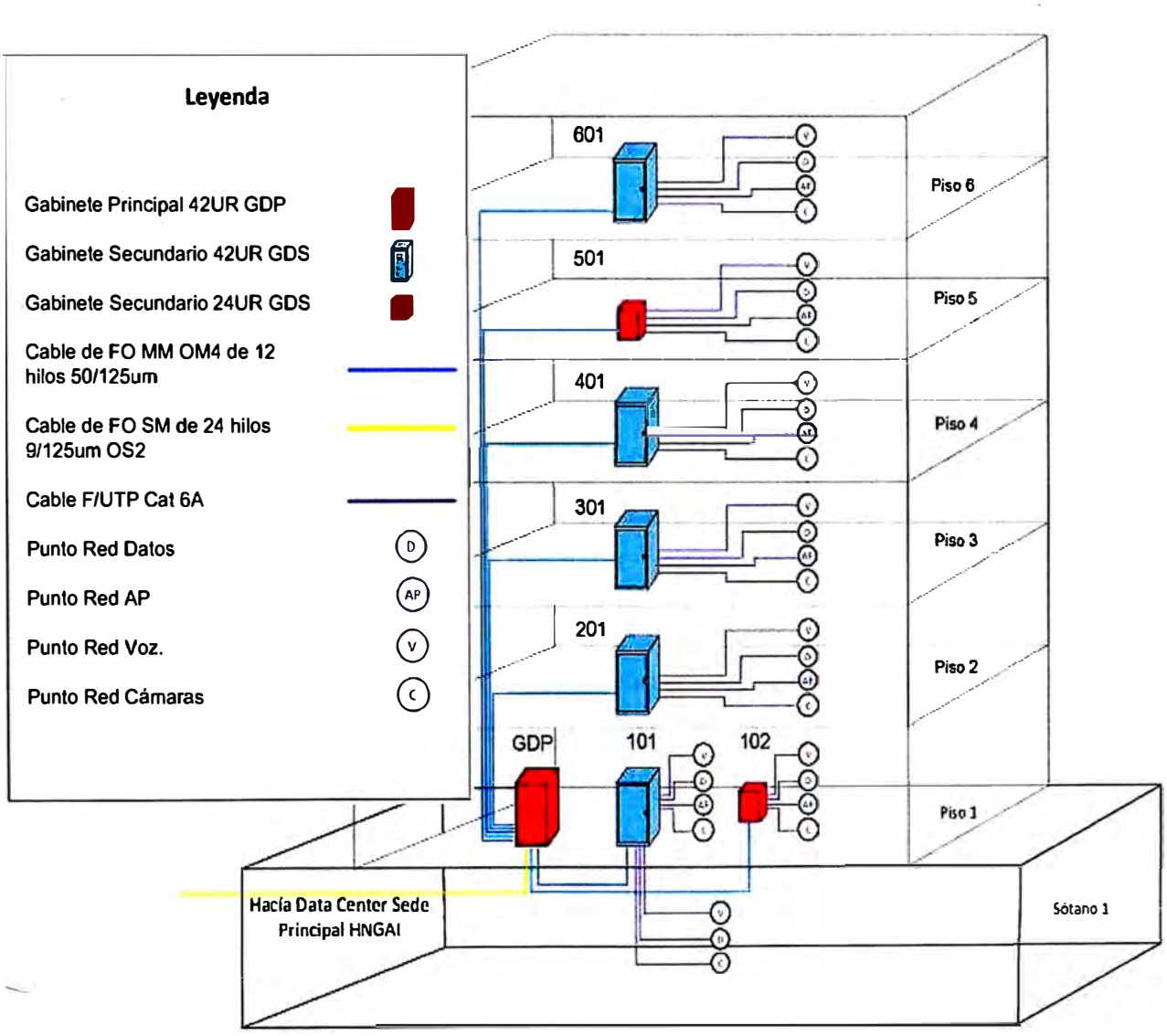


Figura 3.1 Diagrama troncal de fibra óptica interna – Nueva Consulta Externa.

Cableado Estructurado para la nueva Emergencia.- El edificio está comprendido por 3 pisos y un sótano, se han instalado puntos de red a nivel de usuario final, según el requerimiento en cantidad y ubicación definido por el ESSALUD, las mismas que fueron ratificadas en la planificación del proyecto. A continuación se detallan las cantidades de puntos de red desplegados por piso, según cada aplicación requerida.

Tabla 3.4 Distribución de puntos de red por gabinete – Nueva Emergencia.

Ubicación	Telecom	Datos	Voz IP	Access Point	Cámaras IP	Datos
Piso 1	GDP	44	25	4	8	81
Piso 1	GDS-101	42	13	2	9	66
Piso 1	GDS-102	4	2	1	4	11
Piso 2	GDS-201	85	19	5	7	116
Piso 3	GDS-301	151	10	7	7	175
					TOTAL	449

Se ha realizado el montaje de gabinetes de comunicaciones de 42UR y de 24 UR los cuales han sido distribuidos según el siguiente cuadro.

Tabla 3.5 Tipo de Gabinete por piso – Nueva Emergencia.

Ubicación	Telecom	Gabinete de 42 UR	Gabinete de 9 UR
Piso 1	GDP	1	
Piso 1	GDS-101	1	
Piso 1	GDS-102		1
Piso 2	GDS-201	1	
Piso 3	GDS-301	1	

La troncal de fibra óptica interna de la sede consulta externa, desplegada en cada Gabinete de Distribución Secundaria (GDS), ha contemplado un enlace de fibra óptica multimodo de 12 hilos OM4, para la interconexión con el Gabinete de Distribución Principal (GDP). La topología implementada fue de tipo estrella escalable.

Las terminaciones del cable de fibra óptica han sido realizadas en las bandejas de fibra óptica ubicadas en el interior de cada gabinete GDS, utilizando extensiones ópticas con conector de tipo LC, la conexión de la fibra óptica se realizó con el método de empalme por fusión.

A continuación se detallan las cantidades de empalmes fusionados por hilo de fibra óptica.

Tabla 3.6 Hilos de fibra por cada gabinete de piso – Nueva Emergencia.

Ubicación	Gabinete	Cantidad de hilos de fibra	
		GDP	GDS
Piso 1	GDP	42	
Piso 1	GDS-101		12
Piso 1	GDS-102		6
Piso 2	GDS-201		12
Piso 3	GDS-301		12

Se muestra el diagrama físico de la distribución de fibra óptica tipo estrella escalable interna de la Sede Nueva Emergencia:

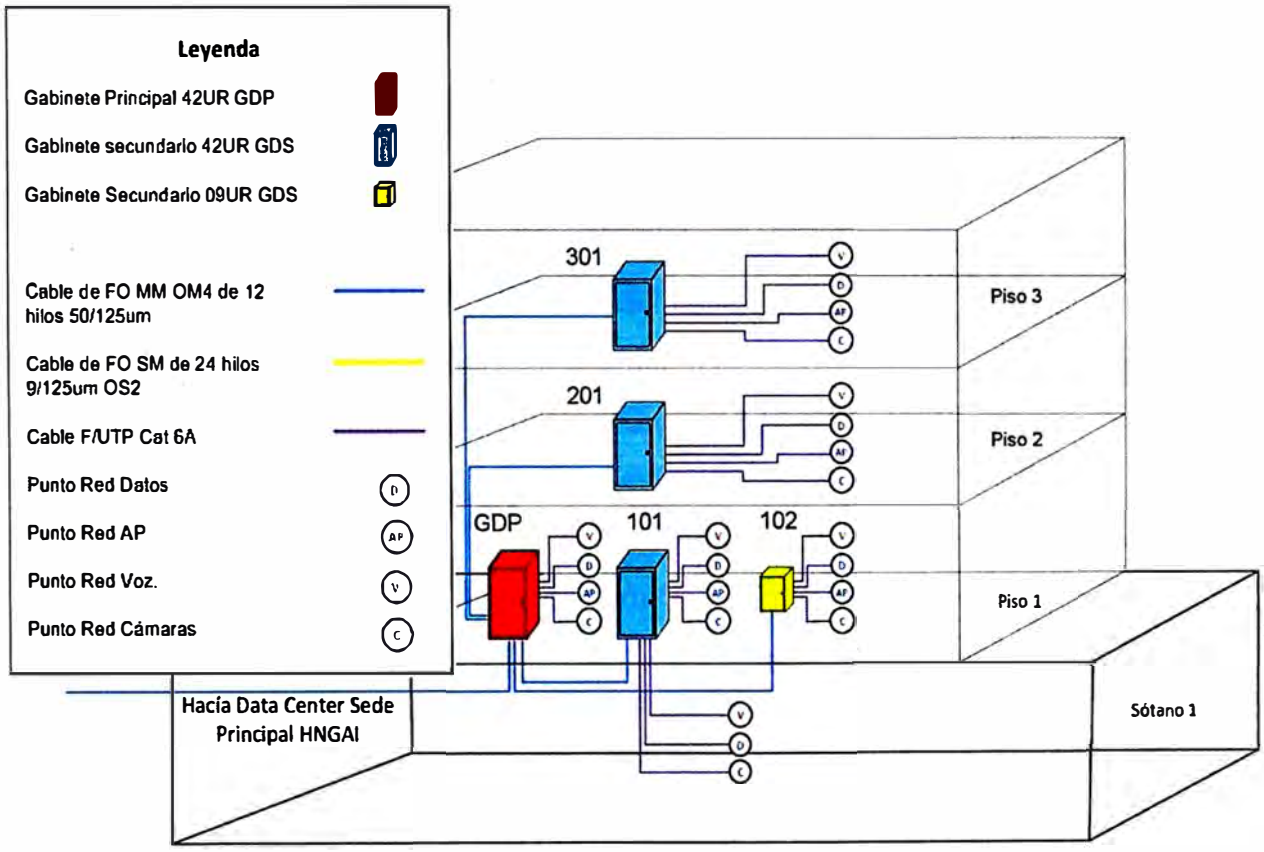


Figura 3.2 Diagrama de backbone de fibra óptica interno – Nueva Emergencia.

La troncal externa de campus de fibra óptica entre las nuevas sedes, ha sido realizado con el tendido de fibra óptica de tipo anillo entre las 3 sedes, las cuales a continuación se procede a describir en tres fases.

Enlaces de fibra óptica entre Sede Principal y Nueva Consulta Externa, se ha realizado la instalación del enlace de fibra óptica monomodo 9/125 µm OS2 de 24 hilos entre el Data Center Existente Sede Principal y Consulta Externa, las actividades han consistido en:

- Se ha instalado el cable fibra óptica desde el GDP de Nueva Consulta Externa (por la canalización subterránea y la tubería conduit EMT del sótano de la Sede Principal) hasta el Data Center de la sede Principal. La distancia del enlace ha sido de 630 metros.
- Se ha instalado una bandeja fibra óptica de 1UR en el gabinete del Data Center de la sede Principal y otra bandeja de 2UR en el GDP de Consulta Externa.
- Se han fusionado 24 empalmes de fibra óptica por extremo de cada GDP.
- La terminación del cable de fibra óptica con extensiones ópticas conectorizadas ha sido del tipo LC monomodo de 9/125µm, con pruebas calidad utilizando equipo OTDR.

Enlaces de Fibra Óptica entre Sede Principal y Nueva Emergencia.- Se ha realizado la instalación del enlace de fibra óptica multimodo 50/125 µm OM4 de 24 hilos entre el Data Center de la sede Principal y Emergencia, las actividades han consistido en:

- Se ha instalado el cable de fibra óptica desde el GDP de Emergencia (por canalización subterránea y tubería conduit EMT del sótano de la sede Principal), hasta el Data Center de la sede Principal. La distancia del enlace ha sido de 320 metros.
- Se ha instalado una bandeja fibra óptica de 1UR en el gabinete del Data Center de la sede Principal y otra bandeja de 2UR en el GDP de Emergencia.
- Se han fusionado 24 empalmes de fibra óptica por extremo en cada GDP.
- La terminación del cable de fibra óptica con extensiones ópticas conectorizadas ha sido del tipo LC multimodo 50/125µm, con pruebas calidad utilizando equipo OTDR.

Enlaces de Fibra Óptica entre Nueva Emergencia y Nueva Consulta Externa.- Se ha realizado la instalación de un enlace de fibra óptica multimodo 50/125 µm OM4 de 24 hilos entre el GDP Emergencia y GDP Consulta Externa, para cerrar el anillo de fibra óptica entre todas las sedes, las actividades han consistido en:

- Se ha instalado el cable de fibra óptica desde el GDP Emergencia, hasta el GDP Consulta Externa. La distancia del enlace ha sido de 310 metros.
- Se ha instalado una bandeja fibra óptica de 2UR en GDP Emergencia y una bandeja de 1UR en el GDP Consulta Externa.
- Se ha fusionado 12 empalmes de fibra óptica por extremo en cada GDP.
- La terminación del cable de fibra óptica con extensiones ópticas conectorizadas ha sido del tipo LC multimodo 50/125µm, con pruebas calidad utilizando equipo OTDR.

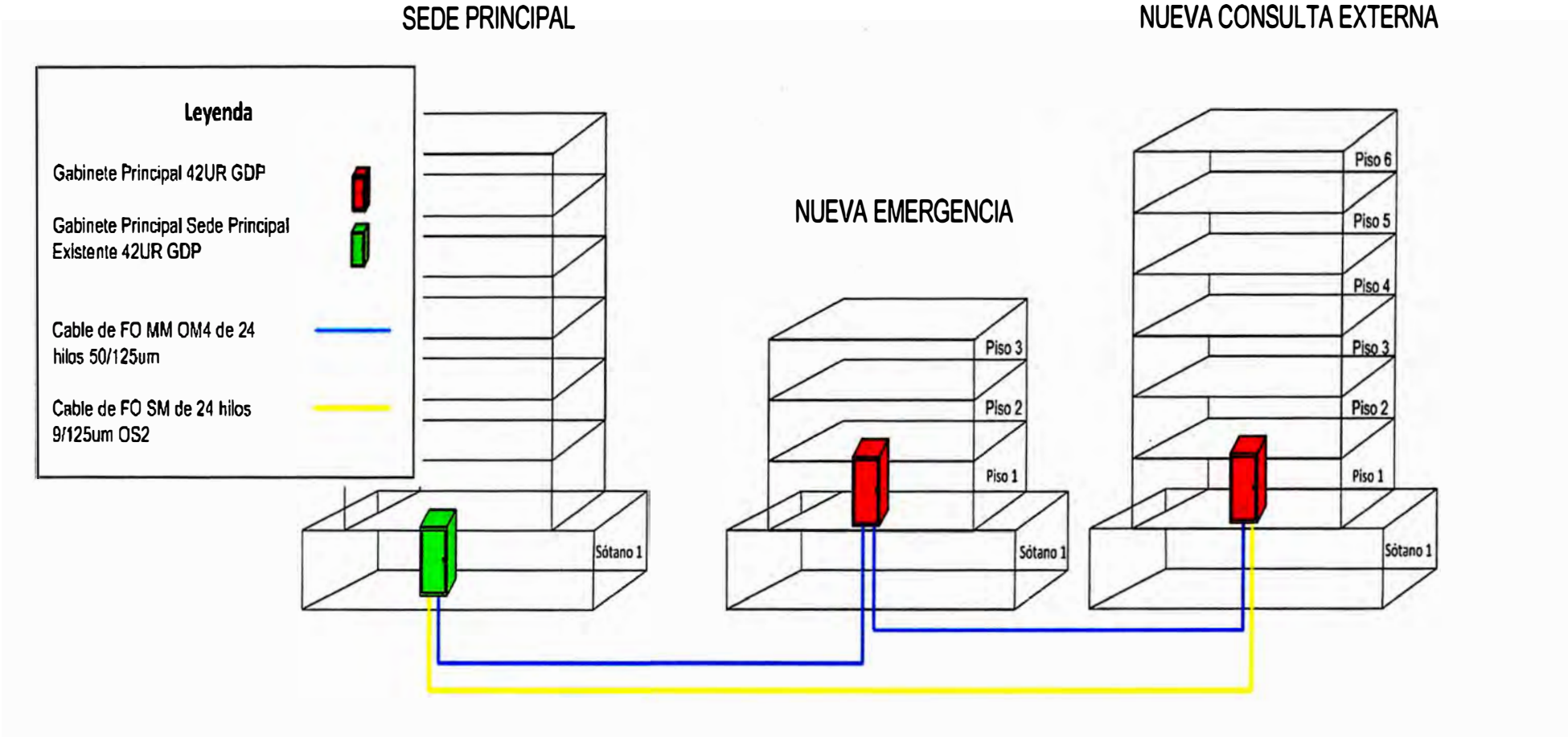


Figura 3.3 Diagrama de troncal de fibra óptica de todas las sedes

3.2 Descripción de la Plataforma de Conmutadores de Red

Se procede a describir la implementación desarrollada de esta plataforma.

3.2.1 Alcance de los Conmutadores de Red

La implementación, configuración e instalación de la solución de equipos de conmutación de red (switches) del nuevo Hospital Guillermo Almenara, fue en cumplimiento a los requerimientos de la Entidad ESSALUD, para lo cual se propuso e instalo equipamiento de la marca Alcatel Lucent y está compuesta por los siguientes componentes:

- Conmutadores Tipo A: Es un conmutador de Capa 2 del modelo OSI, compuesto por 08 equipos marca Alcatel-Lucent modelo OS6450-P24-US, con 24 puertos POE.
- Conmutadores Tipo B: Es un conmutador de Capa 2 del modelo OSI, compuesto por 09 equipos marca Alcatel-Lucent modelo OS6450-P48-US, con 48 puertos POE.
- Conmutadores Tipo C: Es un conmutador de Capa 2 del modelo OSI, compuesto por 14 equipos marca Alcatel-Lucent modelo OS6450-48-US, con 48 puertos sin POE.
- Conmutadores Tipo D: Es un conmutador de Capa 3 del modelo OSI, compuesto por 02 equipos marca Alcatel-Lucent modelo OS6850EU24X-US, con 24 puertos de fibra óptica.

La plataforma de conmutadores de red, establece una red distribuida de conmutadores *(switches)* de borde unidos por enlaces físicos concentrados al conmutador principal *(Switch Core)*, para las sedes de Nueva Emergencia y Nueva Consulta Externa, las cuales forman físicamente una extensión de la actual Red del Hospital por medio de enlaces de fibra óptica, donde lógicamente estarán segmentadas por sub redes virtuales, para optimizar el servicio de la red en cada sede.

La topología propuesta resulta de la distribución de puntos del cableado estructurado, el cual se presenta como una red tipo estrella escalable al interno de cada sede, y una topología tipo anillo de troncal *(backbone)* de fibra óptica entre las sedes.

La definición de los cuatro tipos de conmutadores se basa en las características técnicas y rol que desempeñan en la red; estos se identifican por el gabinete asociado producto del cableado estructurado.

A continuación se detallan las cantidades de conmutadores instalados y requeridos, según la necesidad del Hospital.

- **02 Conmutadores tipo D (L3 – 24 puertos de fibra óptica):**

Este conmutador principal de capa 3 del modelo OSI, se instaló uno en cada Gabinete Principal (GDP) de cada Nueva Sede (Emergencia y Consulta Externa), empleado para ser el conmutador principal *(Switch Core)* de la red local. Cada uno de ellos se conectó al Switch Core Alcatel OS97000 existente de la sede principal del Hospital Almenara, vía un enlace de fibra óptica (a Emergencia con fibra óptica multimodo y Consulta Externa con fibra óptica monomodo), mientras que localmente alimenta vía fibra óptica multimodo a los conmutador *(Switch)* de Borde de los gabinetes remotos y propios de la sede.

La implementación de las interfaces de fibra fue con tranceivers de 10G y 1G, las conexiones a este conmutador se orientaron a servidores, routers, equipos de acceso, enlaces entre conmutadores y otros que no involucren dispositivos finales.

Funcionalmente este equipo gestiona todas las VLANs necesarias en la red, optimizando el performance de la misma, así mismo gestiona las funciones de capa 3 para la comunicación con el conmutador principal 9700 existente del Hospital Almenara, donde se tienen tres (03) sedes virtualmente separadas lo cual optimizara a toda la red en general.

- **08 Conmutadores tipo A (L2 – 24 puertos de cobre, capacidad PoE):**

Estos conmutadores de capa 2 del modelo OSI, se instalaron en los Gabinetes Secundarios (GDS) de cada uno de los pisos de las Sedes de Nueva Emergencia y Consulta Externa, se conectaron vía fibra óptica multimodo al conmutador principal (tipo D) y alimentan vía cable F/UTP (categoría 6A) a los puntos de red finales. Cumple con todas las características funcionales requeridas por la entidad detalladas en la necesidad del proyecto, y cuenta el recurso del protocolo 802.3af (PoE).

La familia de conmutadores propuestos tienen el valor agregado de trabajar como cluster o stack. Las interfaces y tranceivers necesarios fueron conectados para los enlaces al conmutador principal en enlace agregado.

- **09 Conmutadores tipo B (L2 – 48 puertos de cobre, capacidad PoE):**

Estos conmutadores de capa 2 del modelo OSI, se instalaron en los Gabinetes Secundarios (GDS) de cada uno de los pisos de las Sedes de Nueva Emergencia y Consulta Externa, se conectaron vía fibra óptica multimodo al conmutador principal (tipo D) y alimentan vía cable F/UTP (categoría 6A) a los puntos de red finales.

Tiene las mismas características funcionales que los conmutadores tipo A, con el recurso del protocolo 802.3af (PoE). La familia de conmutadores propuestos tienen el valor agregado de trabajar como cluster o stack. Las interfaces y tranceivers necesarios fueron conectados para los enlaces al conmutador principal en enlace agregado.

- **14 Conmutadores tipo C (L2 – 48 puertos de cobre):**

Estos conmutadores de capa 2 del modelo OSI, se instalaron en los Gabinetes Secundarios (GDS) de cada uno de los pisos de las Sedes de Nueva Emergencia y Consulta Externa, se conectaron vía fibra óptica multimodo al conmutador principal (tipo D) y alimentan vía cable F/UTP (categoría 6A) a los puntos de red finales. Tiene las mismas características funcionales que los conmutadores tipo A y B, salvo que no trae el recurso del protocolo 802.3af (PoE). La familia de conmutadores propuestos tienen el valor agregado de trabajar como cluster o stack. Las interfaces y tranceivers necesarios fueron conectados para los enlaces al conmutador principal en enlace agregado.

3.2.2 Implementación de la Plataforma de Conmutadores de Red

La Distribución física de los Conmutadores, ha contemplado el cálculo de distribución de conmutadores en la red, según la demanda de puntos de red, para el dimensionamiento de los puertos requeridos, teniendo como factor principal, la demanda de puertos con capacidad del protocolo 802.3af (PoE), que a continuación se detalla:

Tabla 3.7 Cantidad de puntos de red PoE – Nueva Emergencia.

NUEVA EMERGENCIA										
Localización	Puntos de Red							TOTAL PTOS DATOS NO POE	TOTAL PTOS DATOS POE	SUBTOTAL
GDP / GDS	D	D2	DT	V	AP	CF	CM			
GDP	43		1	25	4	8	0	44	37	81
GDS – 101	42			13	2	8	1	42	24	66
GDS – 102	4			2	1	3	1	4	7	11
GDS – 201	82		3	19	5	7		85	31	116
GDS – 301	151			10	7	7		151	24	175
	PUNTOS TOTALES EMERGENCIA									449

Tabla 3.8 Cantidad de puntos de red PoE – Nueva Consulta Externa.

NUEVA CONSULTA EXTERNA										
LOCALIZACIÓN	Puntos de Red							TOTAL PTOS DATOS NO POE	TOTAL PTOS DATOS POE	SUBTOTAL
GDP / GDS	D	D2	DT	V	AP	CF	CM			
GDP	0			0	0	0	0	0	0	0
GDS – 101	79			49	4	19	2	79	74	153
GDS – 102	7			3	0	1	1	7	5	12
GDS – 201	52			44	6	9		52	59	111
GDS – 301	46			40	6	9		46	55	101
GDS – 401	42			41	7	9		42	57	99
GDS – 501	39			36	7	11		39	54	93
GDS – 601	32			23	6	9		32	38	70
	PUNTOS TOTALES CONSULTA EXTERNA									639
LEYENDA										
D = PUNTO DE DATOS DT = D EN TECHO V = PUNTO DE VOZ						CF = CAMARA FIJA CM = CAMARA MOVIL AP = ACCESS POINT				

Descripción de la instalación física de los conmutadores de red.- En base a la demanda de puntos de red se ha distribuido los conmutadores en cada gabinete de comunicaciones, los conmutadores borde que pertenecen a cada gabinete se conectaron físicamente por sus módulos stack entre sí, con el cual todos forman una única unidad virtual, siendo nombrados con un único ID Equipo virtual. A continuación se detallan:

Tabla 3.9 Distribución de conmutadores – Nueva Emergencia.

Piso	ID Equipo	Modelo	S/N	Ubicación
1	CORE-NE	OS6850EU24X-US	P2383704	GDP
1	NE-GDP	OS6450-48-US	P2086208	GDP
		OS6450-P48-US	P1884749	
1	NE-101	OS6450-48-US	P2086230	GDS-101
		OS6450-P24-US	P1785477	
1	NE-102	OS6450-P24-US	P1785451	GDS-102
2	NE-201	OS6450-48-US	P2086211	GDS-201
		OS6450-48-US	P2086199	
		OS6450-P48-US	P1884751	
3	NE-301	OS6450-48-US	P2086221	GDS-301
		OS6450-48-US	P2086192	
		OS6450-48-US	P2086216	
		OS6450-P48-US	P1884704	

Tabla 3.10 Distribución de conmutadores – Nueva Consulta Externa.

Piso	Equipo	Modelo	S/N	Ubicación
1	CORE-CE	OS6850EU24X-US	P2383779	GDP
1	CE-101	OS6450-48-US	P2086209	GDS-101
		OS6450-48-US	P2086182	
		OS6450-P48-US	P1885081	
		OS6450-P24-US	P1785364	
1	CE-102	OS6450-P24-US	P2486324	GDS-102
2	CE-201	OS6450-48-US	P2086202	GDS-201
		OS6450-P48-US	P1884753	
		OS6450-P24-US	P1785648	
3	CE-301	OS6450-48-US	P2086044	GDS-301
		OS6450-P48-US	P2586756	
		OS6450-P24-US	P1785637	
4	CE-401	OS6450-48-US	P2086207	GDS-401
		OS6450-P48-US	P1884705	
		OS6450-P24-US	P1785601	
5	CE-501	OS6450-48-US	P2086179	GDS-501
		OS6450-P48-US	P1885111	
		OS6450-P24-US	P1785488	
6	CE-601	OS6450-48-US	P2086214	GDS-601
		OS6450-P48-US	P1884762	

Topología física de la Red.- La topología física de distribución de los conmutadores, se han definido en base a las troncales de fibra óptica de la plataforma de cableado estructurado en tipo anillo para nodos principales de cada nueva sede interconectado con el conmutador principal existente de la sede principal del hospital; y tipo estrella escalable para nodos internos en cada nueva sede.

Configuración lógica aplicada a los conmutadores.- Se definió apilamiento stack en cada conmutador de cada GDS de las nuevas sede, creando una sola unidad virtual de conmutadores.

La topología interna en cada nueva sede es de tipo estrella, cada gabinete de cada piso de se conecta al conmutador principal de su sede a través de un enlace agregado (LACP), donde se aplico la van 777 de gestión es nativa en todos estos enlaces, y la cantidad de puertos que usa el enlace agregado está indicado en la topología de cada sede.

A continuación se detallan los gráficos de las topologías físicas y lógicas.

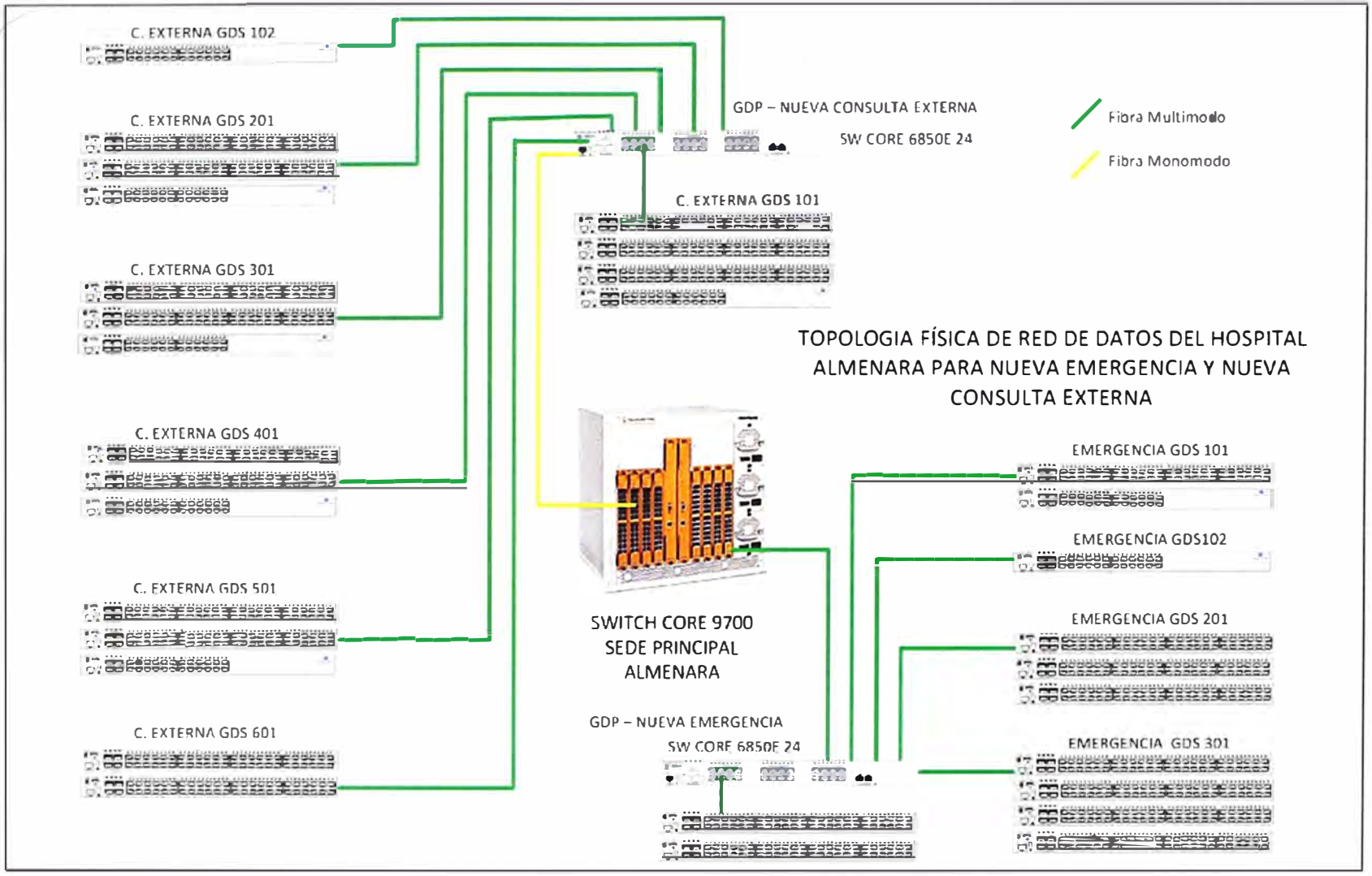


Figura 3.4 Topología física de Red de las Nuevas Sedes

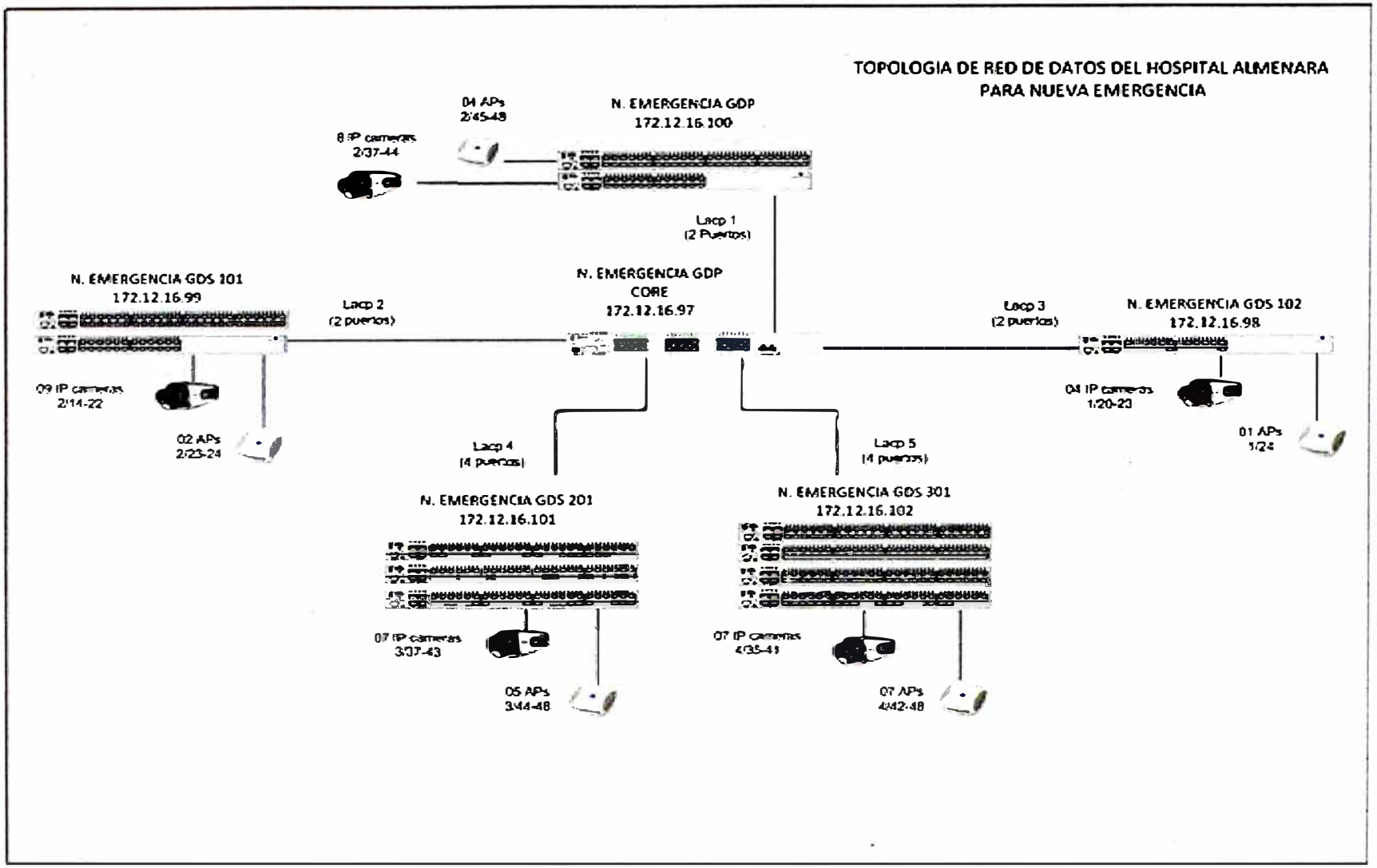


Figura 3.5 Topología Lógica de Red de Nueva Emergencia

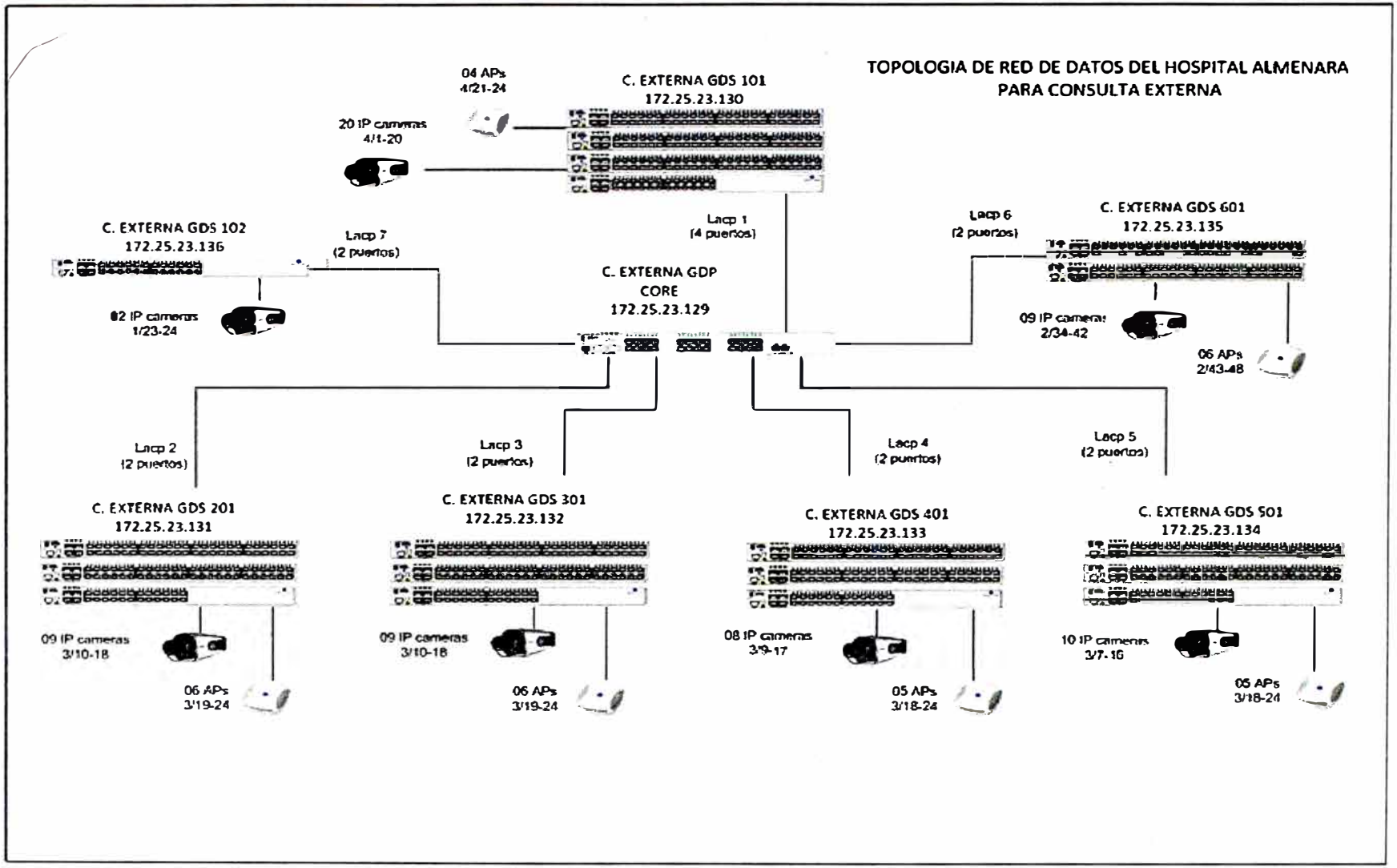


Figura 3.6 Topología Lógica de Red de Nueva Consulta Externa

A continuación se detallan las configuraciones de protocolos de red de los Conmutadores. Se detallan los protocolos de red a nivel de capa 2:

Configuración a nivel de administración de los conmutadores.- Se ha definido los accesos a los equipos (Switch) a través de la interface GUI mediante el uso del protocolo HTTPS y través de la línea de comandos mediante el uso del protocolo SSH. Adicionalmente se habilito un usuario para el uso del protocolo SNMPv3, con los siguientes permisos a nivel usuario: admin_snmp, y password: admin_snmp.
Se ha definido la red de gestión para la administración de los conmutadores, dentro de los segmentos de red 172.25.16.96/27 y 172.25.23.128/26, para las sedes de Nueva Emergencia y Nueva Consulta Externa, respectivamente. Se procede a detallar el direccionamiento IP de Gestión de todos los conmutadores instalados:

Tabla 3.11 Dirección IP de Gestión de Switch – Nueva Emergencia.

Piso	Equipo	IP
1	CORE-NE	172.25.16.97
	NE-GDP	172.25.16.100
	NE-101	172.25.16.99
	NE-102	172.25.16.98
2	NE-201	172.25.16.101
3	NE-301	172.25.16.102

Tabla 3.12 Dirección IP de Gestión de Switch – Nueva Consulta Externa.

Piso	Equipo	IP
1	CORE-CE	172.25.23.129
	CE-101	172.25.23.130
	CE-102	172.25.23.136
2	CE-201	172.25.23.131
3	CE-301	172.25.23.132
4	CE-401	172.25.23.133
5	CE-501	172.25.23.134
6	CE-601	172.25.23.135

Se ha generado el perfil de administrador para todos los conmutadores, las cuales son, usuario: admin, y clave: letacla.

Se ha generado el perfil de administración para fines de soporte técnico, las cuales son, usuario: admin-ebd, y clave: letacla1.

Análisis e Direccionamiento IP.- Se ha aplicado el direccionamiento IP tipo estático (a excepción de las cámaras IP) en todos los dispositivos de la red y se definieron las VLANS en cada segmento de red por tipo de servicio y aplicación. A continuación se procede a detallar las VLANS con su direccionamiento IP, en cada nueva sede de hospital.

Tabla 3.13 Direccionamiento IP de Red – Nueva Consulta Externa.

Nº	Servicio	Área	Segmento de Red	Gateway	Vlan ID
1	Datos	Piso 1	172.25.18.0/25	172.25.18.1	510
		Piso 2	172.25.18.128/25	172.25.18.129	520
		Piso 3	172.25.19.0/25	172.25.19.1	530
		Piso 4	172.25.19.128/25	172.25.19.129	540
		Piso 5	172.25.20.0/25	172.25.20.1	550
		Piso 6	172.25.20.128/25	172.25.20.129	560
2	VOIP	Piso 1	172.29.135.0/25	172.29.135.1	450
		Piso 2	172.29.135.128/25	172.29.135.129	451
		Piso 3	172.29.136.0/25	172.29.136.1	452
		Piso 4	172.29.136.128/25	172.29.136.129	453
		Piso 5	172.29.137.0/25	172.29.137.1	454
		Piso 6	172.29.137.128/26	172.29.137.129	455
3	Cámaras IP		172.25.21.0/25	172.25.21.1	400
4	Aplicativo Médico PACs		172.25.21.128/25	172.25.21.129	300
5	WiFi Asistencial		172.25.22.0/24	172.25.22.1	221
6	WiFi Administrativo		172.25.23.0/26	172.25.23.1	220
7	WiFi Invitados		172.25.23.64/26	172.25.23.65	222
8	Administración de Equipos de Red		172.25.23.128/26	172.25.23.129	777
9	Access Point		172.25.23.192/26	172.25.23.193	200
10	Equipos de Laboratorio		172.25.24.0/24	172.25.24.1	320
11	WAN CE - ALMENRA		172.29.137.248/30	--	501
12	WAN NE - ALMENRA		172.29.137.252/30	--	500
13	WAN CE – NE		172.29.137.240/30	--	502
14	LIBRE		172.29.137.192/27	--	--
15	LIBRE		172.29.137.224/27	--	--
16	LIBRE		172.29.137.244/27	--	--

Tabla 3.14 Direccionamiento IP de Red – Nueva Emergencia.

Nº	Servicio	Área	Segmento de Red	Gateway	Vlan ID
1	Datos	Piso 1	172.25.14.0/25	172.25.14.1	510
		Piso 2	172.25.14.128/25	172.25.14.129	520
		Piso 3	172.25.15.0/25	172.25.15.1	530
2	VOIP	Piso 1	172.25.17.0/26	172.25.17.1	450
		Piso 2	172.25.17.64/27	172.25.17.65	451
		Piso 3	172.25.17.96/27	172.25.17.97	452
3	Cámaras IP		172.25.16.0/26	172.25.16.1	400
4	Aplicativo Médico PACs		172.25.15.128/26	172.25.15.129	300
5	Wifi Administrativos		172.25.16.192/27	172.25.16.193	210
6	Wifi Asistencial		172.25.16.128/26	172.25.16.129	211
7	Wifi Invitados		172.25.16.224/27	172.25.16.225	212
8	Administración de Equipos de Red		172.25.16.96/27	172.25.16.97	777
9	Sistema de Llamada Enfermeras		172.25.15.192/26	172.25.15.193	310
10	Access Point		172.25.16.64/27	172.25.16.65	200
11	Equipos Laboratorios		172.25.17.128/26	172.25.17.129	320
12	Equipos Médicos		172.25.17.192/26	172.25.17.193	330

Se ha definido la operación de spannnig tree, en modo 1x1, en donde se corre una instancia de spanning tree por cada vlan.

En el Anexo A, se detalla las configuraciones aplicadas a los redes de cada nueva sede (Consulta Externa y Nueva Emergencia).

Protocolos de red a nivel de capa 3.- El enrutamiento del conmutador principal *(Switch Core)* entre las tres sedes (Hospital HNGAI Sede Principal existente, Nueva Consulta Externa y Nueva Emergencia), es a través del protocolo de enrutamiento OSPF. A continuación se detalla las rutas aplicadas al protocolo en cada sede.

La configuración del protocolo OSPF en Sede Principal Almenara es:

```
SW-CORE-ALMENARA# show ip ospf neighbor

 IP Address      Area Id        Router Id      Vlan  State  Type
----------------+---------------+---------------+------+-------+--------
172.29.137.250  0.0.0.0        172.25.23.193   501    Full  Dynamic
```

```
172.29.137.254  0.0.0.0        172.25.16.65    500     Full  Dynamic

SW-CORE-ALMENARA# show ip ospf routes
 Destination/Mask        Gateway        Metric  Vlan    Type
--------------------+----------------+--------+------+----------
172.25.14.0/25       172.29.137.254   1       500     AS-Ext (E2)
172.25.14.128/25     172.29.137.254   1       500     AS-Ext (E2)
172.25.15.0/25       172.29.137.254   1       500     AS-Ext (E2)
172.25.15.128/26     172.29.137.254   1       500     AS-Ext (E2)
172.25.15.192/26     172.29.137.254   1       500     AS-Ext (E2)
172.25.16.64/27      172.29.137.254   1       500     AS-Ext (E2)
172.25.16.96/27      172.29.137.254   1       500     AS-Ext (E2)
172.25.16.128/26     172.29.137.250   1       501     AS-Ext (E2)
172.25.16.192/27     172.29.137.250   1       501     AS-Ext (E2)
172.25.16.224/27     172.29.137.250   1       501     AS-Ext (E2)
172.25.17.0/26       172.29.137.254   1       500     AS-Ext (E2)
172.25.17.64/27      172.29.137.254   1       500     AS-Ext (E2)
172.25.17.96/27      172.29.137.254   1       500     AS-Ext (E2)
172.25.17.128/26     172.29.137.254   1       500     AS-Ext (E2)
172.25.18.0/25       172.29.137.250   1       501     AS-Ext (E2)
172.25.18.128/25     172.29.137.250   1       501     AS-Ext (E2)
172.25.19.0/25       172.29.137.250   1       501     AS-Ext (E2)
172.25.19.128/25     172.29.137.250   1       501     AS-Ext (E2)
172.25.20.0/25       172.29.137.250   1       501     AS-Ext (E2)
172.25.20.128/25     172.29.137.250   1       501     AS-Ext (E2)
172.25.21.0/25       172.29.137.250   1       501     AS-Ext (E2)
172.25.21.128/25     172.29.137.250   1       501     AS-Ext (E2)
172.25.22.0/24       172.29.137.250   1       501     AS-Ext (E2)
172.25.23.0/26       172.29.137.250   1       501     AS-Ext (E2)
 Destination/Mask        Gateway        Metric  Vlan    Type
--------------------+----------------+--------+------+----------
172.25.23.64/26      172.29.137.250   1       501     AS-Ext (E2)
172.25.23.128/26     172.29.137.250   1       501     AS-Ext (E2)
172.25.23.192/26     172.29.137.250   1       501     AS-Ext (E2)
172.25.24.0/24       172.29.137.250   1       501     AS-Ext (E2)
172.29.135.0/25      172.29.137.250   1       501     AS-Ext (E2)
172.29.135.128/25    172.29.137.250   1       501     AS-Ext (E2)
172.29.136.0/25      172.29.137.250   1       501     AS-Ext (E2)
172.29.136.128/25    172.29.137.250   1       501     AS-Ext (E2)
172.29.137.0/25      172.29.137.250   1       501     AS-Ext (E2)
```

172.29.137.128/26	172.29.137.250	1	501	AS-Ext (E2)
172.29.137.248/30	172.29.137.249	1	501	Intra
172.29.137.252/30	172.29.137.253	1	500	Intra

La Configuración del protocolo OSPF en Sede Nueva Emergencia es:

Core-NE# show ip ospf neighbor

IP Address	Area Id	Router Id	Vlan	State	Type
172.29.137.253	0.0.0.0	172.22.8.4	500	Full	Dynamic

Core-NE# show ip ospf routes

Destination/Mask	Gateway	Metric	Vlan	Type
0.0.0.0/0	172.29.137.253	1	500	AS-Ext (E2)
172.22.8.0/24	172.29.137.253	1	500	AS-Ext (E2)
172.22.10.0/24	172.29.137.253	1	500	AS-Ext (E2)
172.22.11.0/24	172.29.137.253	1	500	AS-Ext (E2)
172.22.12.0/24	172.29.137.253	1	500	AS-Ext (E2)
172.22.14.0/24	172.29.137.253	1	500	AS-Ext (E2)
172.22.15.0/24	172.29.137.253	1	500	AS-Ext (E2)
172.22.16.0/24	172.29.137.253	1	500	AS-Ext (E2)
172.22.17.0/24	172.29.137.253	1	500	AS-Ext (E2)
172.22.30.0/24	172.29.137.253	1	500	AS-Ext (E2)
172.22.32.0/24	172.29.137.253	1	500	AS-Ext (E2)
172.22.50.0/24	172.29.137.253	1	500	AS-Ext (E2)
172.22.51.0/24	172.29.137.253	1	500	AS-Ext (E2)
172.22.52.0/24	172.29.137.253	1	500	AS-Ext (E2)
172.22.53.0/24	172.29.137.253	1	500	AS-Ext (E2)
172.22.54.0/24	172.29.137.253	1	500	AS-Ext (E2)
172.22.55.0/24	172.29.137.253	1	500	AS-Ext (E2)
172.22.56.0/24	172.29.137.253	1	500	AS-Ext (E2)
172.25.16.128/26	172.29.137.253	1	500	AS-Ext (E2)
172.25.16.192/27	172.29.137.253	1	500	AS-Ext (E2)
172.25.16.224/27	172.29.137.253	1	500	AS-Ext (E2)
172.25.18.0/25	172.29.137.253	1	500	AS-Ext (E2)
172.25.18.128/25	172.29.137.253	1	500	AS-Ext (E2)
172.25.19.0/25	172.29.137.253	1	500	AS-Ext (E2)
172.25.19.128/25	172.29.137.253	1	500	AS-Ext (E2)

```
172.25.20.0/25      172.29.137.253   1      500     AS-Ext (E2)
172.25.20.128/25    172.29.137.253   1      500     AS-Ext (E2)
Destination/Mask      Gateway      Metric  Vlan    Type
--------------------+----------------+--------+------+--------------
172.25.21.0/25      172.29.137.253   1      500     AS-Ext (E2)
172.25.21.128/25    172.29.137.253   1      500     AS-Ext (E2)
172.25.22.0/24      172.29.137.253   1      500     AS-Ext (E2)
172.25.23.0/26      172.29.137.253   1      500     AS-Ext (E2)
172.25.23.64/26     172.29.137.253   1      500     AS-Ext (E2)
172.25.23.128/26    172.29.137.253   1      500     AS-Ext (E2)
172.25.23.192/26    172.29.137.253   1      500     AS-Ext (E2)
172.25.24.0/24      172.29.137.253   1      500     AS-Ext (E2)
172.29.41.0/24      172.29.137.253   1      500     AS-Ext (E2)
172.29.42.0/24      172.29.137.253   1      500     AS-Ext (E2)
172.29.43.0/24      172.29.137.253   1      500     AS-Ext (E2)
172.29.133.0/24     172.29.137.253   1      500     AS-Ext (E2)
172.29.135.0/25     172.29.137.253   1      500     AS-Ext (E2)
172.29.135.128/25   172.29.137.253   1      500     AS-Ext (E2)
172.29.136.0/25     172.29.137.253   1      500     AS-Ext (E2)
172.29.136.128/25   172.29.137.253   1      500     AS-Ext (E2)
172.29.137.0/25     172.29.137.253   1      500     AS-Ext (E2)
172.29.137.128/26   172.29.137.253   1      500     AS-Ext (E2)
172.29.137.248/30   172.29.137.253   2      500     Intra
172.29.137.252/30   172.29.137.254   1      500     Intra
192.168.20.0/24     172.29.137.253   1      500     AS-Ext (E2)
```

La Configuración del protocolo OSPF en Sede Nueva Consulta Externa es:

```
Core-CE# show ip ospf neighbor
                  IP Address      Area Id        Router Id     Vlan   State  Type
---------------+---------------+----------------+-------+--------+--------
172.29.137.249  0.0.0.0        172.22.8.4      501     Full  Dynamic

Core-CE# show ip ospf routes
 Destination/Mask      Gateway      Metric  Vlan    Type
--------------------+----------------+--------+------+--------------
0.0.0.0/0          172.29.137.249   1      501     AS-Ext (E2)
172.22.8.0/24      172.29.137.249   1      501     AS-Ext (E2)
172.22.10.0/24     172.29.137.249   1      501     AS-Ext (E2)
```

172.22.11.0/24	172.29.137.249	1	501	AS-Ext (E2)
172.22.12.0/24	172.29.137.249	1	501	AS-Ext (E2)
172.22.14.0/24	172.29.137.249	1	501	AS-Ext (E2)
172.22.15.0/24	172.29.137.249	1	501	AS-Ext (E2)
172.22.16.0/24	172.29.137.249	1	501	AS-Ext (E2)
172.22.17.0/24	172.29.137.249	1	501	AS-Ext (E2)
172.22.30.0/24	172.29.137.249	1	501	AS-Ext (E2)
172.22.32.0/24	172.29.137.249	1	501	AS-Ext (E2)
172.22.50.0/24	172.29.137.249	1	501	AS-Ext (E2)
172.22.51.0/24	172.29.137.249	1	501	AS-Ext (E2)
172.22.52.0/24	172.29.137.249	1	501	AS-Ext (E2)
172.22.53.0/24	172.29.137.249	1	501	AS-Ext (E2)
172.22.54.0/24	172.29.137.249	1	501	AS-Ext (E2)
172.22.55.0/24	172.29.137.249	1	501	AS-Ext (E2)
172.22.56.0/24	172.29.137.249	1	501	AS-Ext (E2)

Destination/Mask	Gateway	Metric	Vlan	Type
172.25.14.0/25	172.29.137.249	1	501	AS-Ext (E2)
172.25.14.128/25	172.29.137.249	1	501	AS-Ext (E2)
172.25.15.0/25	172.29.137.249	1	501	AS-Ext (E2)
172.25.15.128/26	172.29.137.249	1	501	AS-Ext (E2)
172.25.15.192/26	172.29.137.249	1	501	AS-Ext (E2)
172.25.16.64/27	172.29.137.249	1	501	AS-Ext (E2)
172.25.16.96/27	172.29.137.249	1	501	AS-Ext (E2)
172.25.17.0/26	172.29.137.249	1	501	AS-Ext (E2)
172.25.17.64/27	172.29.137.249	1	501	AS-Ext (E2)
172.25.17.96/27	172.29.137.249	1	501	AS-Ext (E2)
172.25.17.128/26	172.29.137.249	1	501	AS-Ext (E2)
172.29.41.0/24	172.29.137.249	1	501	AS-Ext (E2)
172.29.42.0/24	172.29.137.249	1	501	AS-Ext (E2)
172.29.43.0/24	172.29.137.249	1	501	AS-Ext (E2)
172.29.133.0/24	172.29.137.249	1	501	AS-Ext (E2)
172.29.137.248/30	172.29.137.250	1	501	Intra
172.29.137.252/30	172.29.137.249	2	501	Intra
192.168.20.0/24	172.29.137.249	1	501	AS-Ext (E2)

CAPITULO IV
RESULTADOS Y PRUEBAS DE FUNCIONAMIENTO

4.1 Pruebas del Sistema de Cableado Estructurado

Pruebas de operación del Cableado de Cobre F/UTP Categoría 6A.- Las mediciones de certificación han sido realizadas con un equipo calibrado de la marca Fluke DTX-1800, y configurado en los estándares de medición de cable F/UTP en categoría 6A en canal completo de cobre. Los resultados tangibles se evidencia en la carta de garantía del fabricante, las cuales a continuación se detallan.

Tabla 4.1 Parámetros de medición del cableado F/UTP categoría 6A.

Performance Guarantees for Z-MAX™ 6A Shielded Channels												
Parameter	Frequency (MHz)											Guaranteed Margin (1-500 MHz)
	1	4	10	20	62.5	100	200	250	300	400	500	
Insertion Loss	2.2	4.0	6.3	8.9	15.9	20.3	29.2	32.9	36.2	42.3	47.8	3%
Return Loss	22.0	22.0	22.0	20.5	17.0	15.0	12.0	11.0	10.2	9.0	9.0	3.0
NEXT	68.0	66.0	59.6	54.6	46.4	42.9	37.8	36.1	34.7	32.6	30.9	3.0
PS NEXT	65.5	64.0	57.5	52.5	44.1	40.6	35.4	33.7	32.3	30.1	28.3	3.5
ACR-N	67.0	64.9	56.1	48.5	33.0	25.0	10.7	5.2	0.4	-8.1	-15.4	6.0
PS ACR-N	64.5	62.9	54.0	46.3	30.7	22.7	8.3	2.8	-2.1	-10.6	-18.0	6.5
ACR-F	70.3	58.2	50.3	44.2	34.3	30.3	24.2	22.3	20.7	18.2	16.3	7.0
PS ACR-F	70.3	58.2	50.3	44.2	34.3	30.3	24.2	22.3	20.7	18.2	16.3	10.0
PS ANEXT	77.0	77.0	77.0	77.0	72.0	70.0	65.5	64.0	62.8	61.0	59.5	10.0
PS AACR-F	72.0	70.0	63.9	56.0	46.1	42.0	36.0	34.0	32.5	30.0	28.0	5.0
Prop Delay (ns)	580	562	555	552	549	548	547	546	546	546	546	0.0
Delay Skew (ns)	50	50	50	50	50	50	50	50	50	50	50	0.0

Pruebas de operación del Cableado de Fibra Óptica.- Las mediciones de certificación han sido realizadas con un equipo calibrado OTDR de la marca EXFO, configurado en los estándares de medición de fibra Óptica OM4. Los resultados tangibles se resumen de la carta de garantía del fabricante, quienes evaluaron los resultados del equipo de medición OTDR, las cuales a continuación se detallan.

Tabla 4.2 Parámetros de medición del cableado de fibra óptica.

1) XGLO Horizontal Link Performance Guarantees

Parameter	XGLO 300 50/125 Multimode (850nm/1300nm)	XGLO 550 50/125 Multimode (850nm/1300nm)
Max. Attenuation (dB)	1.32/1.09	1.27/1.09
Bandwidth (MHz•km)	Laser: 2000/- OFL: 1500/500	Laser: 4700/- OFL: 3500/500
Min. Return Loss (dB)	25	25

2) XGLO® Backbone Link' Performance Guarantees

Parameter	XGLO 300 50/125 Multimode (850nm/1300nm)	XGLO 550 50/125 Multimode (850nm/1300nm)	XGLO Single-mode (1310nm/1550nm)
Max. 10G Channel Insertion Loss (dB)[1, 2,3,4]	2.20/1.60	2.90/1.85[1]	6.0/6.0[1]
Max. 40/100G Channel Insertion Loss (dB)[1,2,3]	1.20/0.90	1.35/0.95	5.0/5.0 (10km)[5] 13.013.0 (30km)[5]
Bandwidth (MHz•km)[5]	Laser: 2000/- OFL: 1500/500	Laser: 4700/- OFL: 3500/500	—
Min. Return Loss (dB)	25[6]	25[6]	50
Zero Dispersion Wavelength (nm)[5]	---	—	1300-1324
Zero Dispersion Slope (nm²•km)[5]	---	—	< 0.092

3) XGLO Distance Guarantees

Parameter	XGLO 300 50/125µm Multimode (850nm/1300nm)	XGLO 550 50/125µm, Multimode (850nm/1300nm)	XGLO Single-mode (1310nm/1550nm)
Gigabit Ethernet Max. Transmission Distance (m)	1,000/600	1,000/600	5,000/-
10 Gigabit Ethernet Max. Transmission Distance (m)	300/300	550/550	10,000LR/30,000ER
40/100 Gigabit Ethernet Maximum Transmission Distance (m)	100/100	150/150	10,000/10,000(LR4) 30,000/30,000(ER4)

Se muestra el certificado garantía de la solución de cableado estructurado por 20 años, emitida por el fabricante, luego de la evaluación de la certificación aprobada de cada punto de red y enlace de fibra óptica instalada.

Certificate of Registration

Presented by The Siemon Company

This is to certify that the Z-MAX 6A™ F/UTP & XGLO®
Siemon Cabling System® installed for

SUMINISTRO, INSTALACIÓN Y PUESTA EN MARCHA DEL SISTEMA DE CABLEADOESTRUCTURADO Y COMUNICACIONES PARA LOS NUEVOS SERVICIOS DE EMERGENCIA Y CONSULTA EXTERNA DEL HOSPITAL NACIONAL GUILLERMO ALMENARA IRIGOYEN

Has been designed, installed and tested in conformance with the requirements of The Siemon Cabling System® Training Manual and is warranted for a period of 20 years from the date of issue.

Date of issue: 24th October 2013
Registration Number: 13102401-1VM-LA
Authorized Installer: EBD Peru SA

SIEMON

On behalf of The Siemon Company

Figura 4.1 Certificado de garantía SIEMONS.

4.2 Pruebas del Sistema de Conmutadores

Se detallan las pruebas aplicadas en el proceso de pruebas de operación de los conmutadores de red.

Tabla 4.3 Pruebas de Conmutadores de Red Switch.

N°	Actividad	Aplica	Estado	Observación
GENERAL				
1	Montaje y cableado de equipo	**SI**		
2	Configuración de mensaje inicial en switch	**SI**		
3	Habilitar el servicio de NTP Server en el switch principal.	**SI**		
4	Habilitar la funcionalidad de NTP cliente en los demás switches.	**SI**		
5	Activar el envió de alerta de los eventos más importantes de los equipos (sobrecarga de CPU, memoria, desconexión de puerto, etc.) a un servidor syslog (ej: OmniVista 2500)	**SI**		
6	Creación de usuarios para la administración: cliente y EBD	**SI**		
7	Instalación del último sistema operativo estable en todos los switches.	**SI**		
8	Habilitar el registro de mensajes log referentes a la aplicación de comandos	**SI**		
CAPA 1				
1	Verificar que los enlaces backbone sean redundantes y de la misma velocidad	**SI**		
2	Asegurar que todas las interfaces estén habilitadas en modo auto negociación, a excepción de la conexión a routers u otros equipos que no negocien de forma adecuada el modo de transmisión en los switches (half o dúplex). Indicar velocidad configurada para estos puertos de enlace.	**SI**		
3	Asignar un nombre o descripción a las interfaces o puertos con las conexiones más importantes.	**SI**		
4	Para la conexión de los enlaces backbone emplear los últimos puertos de los switches según: - 6450-24: Puertos 25 y 26 - 6850E48X: Puertos 49 y 50	**SI**		
CAPA 2				
1	Verificar que NO se utilice la VLAN por defecto (VLAN 1) para ninguna funcionalidad del switch, a excepción de restricciones del cliente.	**SI**		
2	Toda vez que dentro de un gabinete de comunicaciones o rack se instale más de un equipo Omniswitch de la misma serie se deben apilar (instalar en configuración de stack o chassis virtual).	**SI**		
3	Todos los enlaces redundantes (backbone, enlace a servidores u otros equipos) deben estar configurados como enlace agregado dinámico mediante el protocolo estándar IEEE 802.3ad (LACP), como segunda alternativa se empleará el protocolo propietario Omnichannel (enlace agregado tipo estático).	**SI**		

4	Habilitar la administración de los equipos mediante los protocolos SSH, HTTPS y SNMPv3.	**SI**		
5	Todos los puertos de acceso de los switches deben tener habilitada la funcionalidad de loopback detection (detección de bucles), a fin de evitar la formación de tormentas de broadcast en la red.	**SI**		
6	Todos los puertos de los switches deben tener deshabilitado el protocolo spanning (STP, RSTP y MSTP). Solo se aplicará en los puertos y escenarios donde los enlaces redundantes (UTP o F.O.) estén configurados mediante el protocolo de enlace agregado (link aggregation).	**SI**		
7	Segmentar la red y habilitar la asignación dinámica de UNP (User Network Profile) en base a reglas de movilidad o autenticación. El UNP permite la asignación de VLAN, QoS, ACLs, etc. La red debe estar segmentada en base a áreas funcionales: logística, finanzas, comercial, operaciones, marketing, gerencia, etc.		**NO**	
8	Para implementaciones de teléfonos IP que empleen el protocolo IEEE 802.1q (asignación estática de VLAN con enlaces troncales) habilitar la funcionalidad de AVA (Automatic VLAN Assignment), a fin de que sea el propio switch sea quien asigne de forma dinámica la VLAN que le corresponde a los teléfonos IP.		**NO**	
9	Habilitar la funcionalidad de Access Guardian e integración con mínimo 02 servidores Radius para brindar autenticación, autorización y contabilización de eventos (modelo de seguridad AAA), a través de Access guardian se debe habilitar la autenticación mediante los métodos de IEEE 802.1x, MAC Address y captive portal.	**SI**		
10	Habilitar la funcionalidad de LPS (Learned Port Security) e integrarlo con la funcionalidad de access guardian a fin de mejorar la seguridad en la red	**SI**		
11	Habilitar el UNP de protección (802.1x Radius-down fail-open) ante caídas de todos los servidores de autenticación Radius.	**SI**		
12	Habilitación del protocolo estándar IEEE 802.1ab (LLDP) y del protocolo propietario AMAP para el reconocimiento de los diversos equipos de red y formación de la topología de red.	**SI**		
13	Asignación dinámica de VLAN y valores de priorización de QoS (802.1p y DSCP) mediante el protocolo estándar IEEE 802.1ab LLDP-MED para telefonía IP, softphone, video conferencia, etc.	**SI**		
14	Habilitar la funcionalidad de ASA (Authenticated Switch Access) para aplicar el modelo de seguridad AAA (Authentication, Authorization, Accounting) en la administración de los equipos en la red.	**SI**		
CAPA 3				
1	Habilitación de la interface Loopback0 y/o designación de interface de administración para los servicios de DNS, FTP, LDAP-SERVER, NTP, RADIUS, SFLOW, SNMP, SSH, SYSLOG, TACACS, TELNET, TFTP.	**SI**		

2	Para redes de oficinas remotas o redes pequeñas (por ejemplo menor a 04 switches), se debe habilitar de la funcionalidad de auto QoS para los servicios de NMS (Network Management System).	**SI**		
3	Para redes medianas o grandes se debe identificar las principales aplicaciones que disponga el cliente (Voz, Video, DB, ERP, Scada, etc.) se debe aplicar políticas de QoS en modo avanzado (clasificación, marcación y asignación de políticas de QoS).	**SI**		
4	Habilitar e integrar la funcionalidad de AQM (Alcatel-Lucent Quarantine Manager) en los switches 6400, 6450, 6850, 6850E y 9000E, e integrarlos con los diversos dispositivos de seguridad y de marcas que disponga el cliente (IDS, IPS, DoS, antivirus). Se requiere la habilitación del OmniVista NMS 2500.	**SI**		
5	Habilitar solo para switches core que dispongan de varios enlaces o conexiones a otros equipos capa 3 habilitar el protocolo de enrutamiento dinámico OSPF con BFD (Bi-Directional Forwarding Detection).	**SI**		
6	Habilitar la protección DHCP Snooping.	**SI**		
7	Habilitar la funcionalidad de cliente DNS.	**SI**		
8	Habilitar la funcionalidad de SFLOW e instalar la consola gratuita de visualización de tráfico Sflow InMon Trend en caso de que el cliente no haya adquirido el software	**SI**		
9	Habilitar la funcionalidad de SNMPv3 y emplear los mecanismos de seguridad de SHA+DES, usuario admin_snmp contraseña: modelo_del_switch+dia+mes+año	**SI**		

CAPITULO V
COSTOS Y TIEMPO DE IMPLEMENTACIÓN

5.1 Evaluación de Costos

A continuación se detalla el costo de la implementación en nuevos soles peruanos sin IGV.

Tabla 5.1 Detalle de costos del sistema de cableado estructurado.

Cableado Estructurado	Medida	Cantidad	Precio Unitario	Precio Total
Gabinetes de Comunicaciones	Unidad	13	S/. 11,877.43	S/. 154,406.59
Accesorios de Cableado F/UTP	Global	1	S/. 447,867.50	S/. 447,867.50
Accesorios de Cableado de Fibra	Global	1	S/. 135,521.15	S/. 135,521.15
Canalización de rutas del cableado	Global	1	S/. 113,111.30	S/. 113,111.30
Servicio de Instalación	Global	1	S/. 276,678.59	S/. 276,678.59
			Costo Total del Sistema (sin IGV)	S/. 1,127,585.12

Tabla 5.2 Detalle de costos del sistema conmutadores de red (switch).

Conmutadores de Red	Medida	Cantidad	Precio Unitario	Precio Total
Switch tipo A	Unidad	8	S/. 4,839.80	S/. 38,718.43
Switch tipo B	Unidad	9	S/. 7,759.10	S/. 69,831.90
Switch tipo C	Unidad	14	S/. 5,370.58	S/. 75,188.13
Switch tipo D	Unidad	2	S/. 16,581.08	S/. 33,162.16
Servicio de Instalación	Global	1	S/. 115,352.81	S/. 115,352.81
			Costo Total del Sistema (sin IGV)	S/. 332,253.43

Tabla 5.3 Presupuesto de costos del proyecto.

Plataforma de Cableado Estructurado	**S/. 1,127,585.12**
Plataforma de Conmutadores de Red	**S/. 332,253.43**
Costo Total del Proyecto (sin IGV)	**S/. 1,459,838.56**

5.2 Cronograma y Tiempos de Ejecución

Se detalla el cronograma de implementación del proyecto:

EDT	Nombre de tarea	Duración	Comienzo	Fin
1	Implementación Tecnológica en Hospital Almenara ESSALUD	86 días	mar 02/07/13	jue 26/09/13
1.1	Firma de Contrato	0 días	mar 02/07/13	mar 02/07/13
1.2	Entregar Materiales y Equipamiento	60 días	mar 02/07/13	vie 30/08/13
1.3	Sistema de Cableado Estructurado	65 días	mié 03/07/13	jue 05/09/13
1.3.1	Primera Etapa - Sede Nueva Emergencia	23 días	mié 03/07/13	jue 25/07/13
1.3.2	Segunda Etapa - Sede Nueva Consulta Externa	38 días	vie 26/07/13	dom 01/09/13
1.3.3	Tercera Etapa - Backbone de Fibra Óptica	22 días	vie 26/07/13	vie 16/08/13
1.3.4	Protocolo de Pruebas del Sistema	1 día	lun 02/09/13	lun 02/09/13
1.3.5	Capacitación a Personal Técnico Almenara	2 días	mar 03/09/13	mié 04/09/13
1.3.6	Entregar de Dossier de Calidad	1 día	jue 05/09/13	jue 05/09/13
1.3.7	Firmar la conformidad del Sistema	0 días	jue 05/09/13	jue 05/09/13
1.4	Sistema de Networking - Conmutadores LAN (Switch)	51 días	mar 06/08/13	jue 26/09/13
1.4.1	Montaje Físico de Equipos	34 días	mar 06/08/13	dom 08/09/13
1.4.1.1	Instalar Equipos en Sede Emergencias	5 días	mar 06/08/13	sáb 10/08/13
1.4.1.2	Instalar Equipos en Sede Consulta Externa	7 días	lun 02/09/13	dom 08/09/13
1.4.2	Configuración de Equipos	17 días	mar 03/09/13	vie 20/09/13
1.4.2.1	Configurar Switch de Borde, a nivel capa 2 - Sede Emergencias	3 días	mar 03/09/13	jue 05/09/13
1.4.2.2	Configurar Switch de Borde, a nivel capa 2 - Sede Consulta Externa	5 días	lun 09/09/13	vie 13/09/13
1.4.2.3	Configurar Switch Core para la Integración con los Switch de Borde	3 días	sáb 14/09/13	mar 17/09/13
1.4.2.4	Configurar Switch Core de las sedes, a nivel capa 3	3 días	mié 18/09/13	vie 20/09/13
1.4.3	Protocolo de Pruebas del Sistema	1 día	sáb 21/09/13	sáb 21/09/13
1.4.4	Capacitar al Personal Técnico Almenara	4 días	dom 22/09/13	mié 25/09/13
1.4.5	Entregar Dossier de Calidad	1 día	jue 26/09/13	jue 26/09/13
1.4.6	Firma de Conformidad del Sistema	0 días	jue 26/09/13	jue 26/09/13
1.5	Cierre de Proyecto	0 días	jue 26/09/13	jue 26/09/13

Figura 5.1 Cuadro de tiempos de la implementación

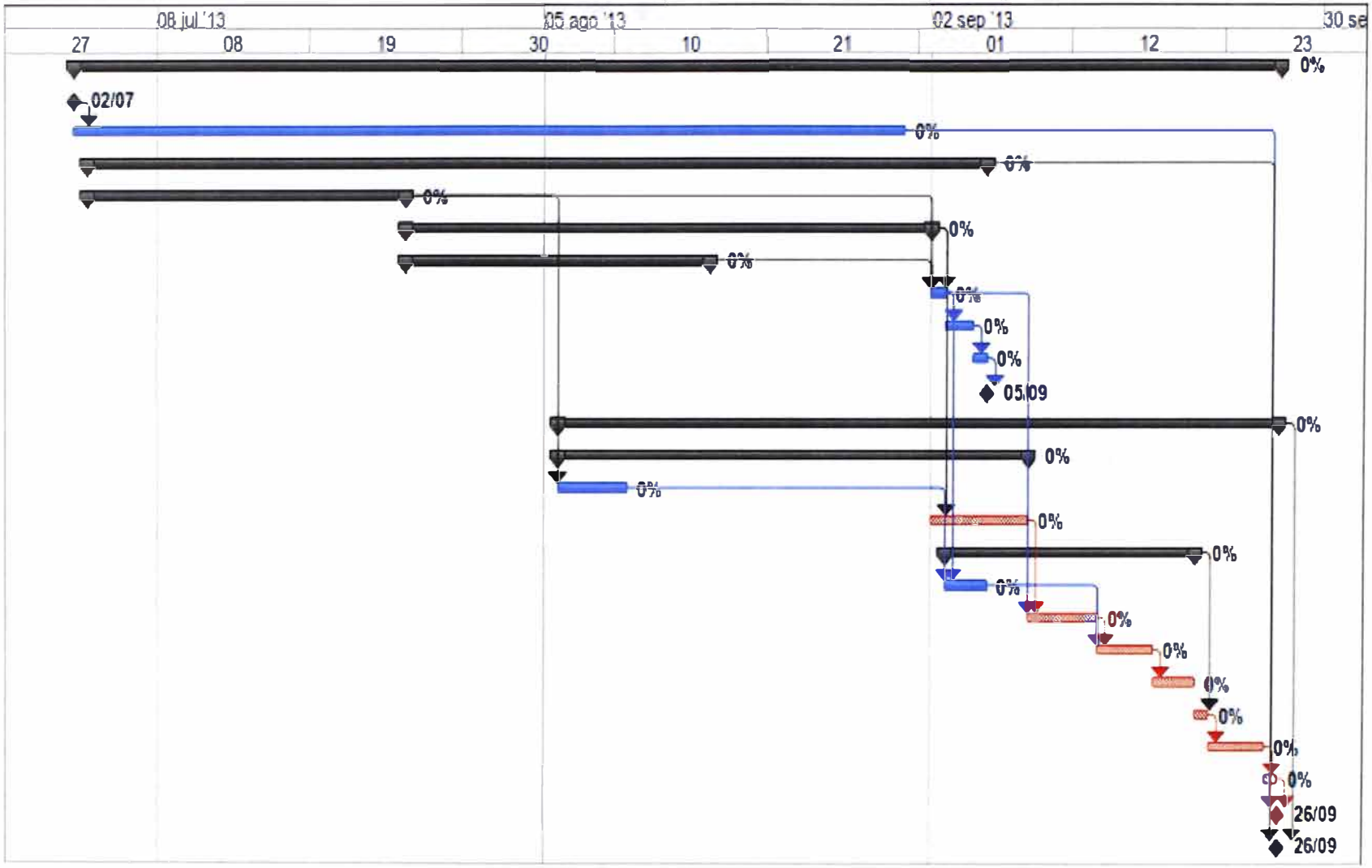


Figura 5.2 Diagrama gantt de tiempos de la implementación

CONCLUSIONES Y RECOMENDACIONES

- La necesidad del hospital ha sido proveer de conexión de red a 1088 usuarios finales, para lo cual se ha realizado la instalación de 33 conmutadores de red en modo de apilamiento *(stack)* distribuidos en los diferentes nodos de comunicaciones de las nuevas sedes, para satisfacer la demanda de puntos de red del Hospital.
- La necesidad del hospital ha sido contar con una eficiente red de datos de alta velocidad (de 10Gps), redundante y tolerable a fallas, para lo cual se ha realizado configuraciones de enlaces agregados en los conmutadores de red de borde de cada nueva sede, aplicando redes virtuales para cada tipo de servicio (Cámaras IP, Telefonía IP, Inalámbrica, equipos médicos, servidores, etc).
- La necesidad del hospital ha sido obtener un servicio ininterrumpido de sus aplicaciones de comunicaciones para las distintas áreas administrativas y medicas del Hospital, para lo cual se ha realizado configuraciones de red redundante en los conmutadores principales *(Switch Core)*, optimizando el performance de la red, en sus distintas aplicaciones (intranet, correo, gestión medica, etc).
- Se recomienda adquirir e instalar un sistema de gestión centralizada para los equipos de conmutación de red, que le permita administrar y monitorear los mismos, a fin de identificar eficazmente fallas y brindar solución en el menor tiempo posible.
- Se recomienda tener actualizado la administración de la plataforma de cableado estructurado, a fin de minimizar los tiempos de respuesta ante cualquier incidente.
- Se recomienda realizar mantenimiento preventivo de la plataforma de conmutadores de red y la plataforma de cableado estructurado anualmente.
- Se recomienda presupuestar, la capacitación continua del personal encargado de la nueva red de conmutadores, a fin de mantener y desarrollar las actuales y nuevas necesidades de los usuarios del hospital.

ANEXO A
CONFIGURACIÓN DE CONMUTADORES PRINCIPALES (SWITCH CORE)

La Configuración del conmutador principal (Switch Core) de Nueva Emergencia es:

```
Core-NE# show configuration snapshot
! Stack Manager:
! Chassis:
System name Core-NE
System location GDP-Piso1-Nueva-Emergencia
System daylight savings time disable
! Configuration:
! MULTI-CHASSIS :
! VLAN :
vlan 1 enable name "VLAN 1"
vlan 200 enable name "APs"
vlan 300 enable name "PACs"
vlan 310 enable name "SIST-ENFERMERAS"
vlan 320 enable name "EQUIPOS-LAB"
vlan 330 enable name "EQUIPOS-MED"
vlan 400 enable name "CAMARAS-IP"
vlan 400 port default 1/25
vlan 450 enable name "VOZ-Piso1"
vlan 451 enable name "VOZ-Piso2"
vlan 452 enable name "VOZ-Piso3"
vlan 500 enable name "CONEX-ALM"
vlan 500 port default 1/22
vlan 501 enable name "TEMP-WAN_C-EXT"
vlan 502 enable name "WAN_to_CE"
vlan 510 enable name "DATOS-P1"
vlan 520 enable name "DATOS-P2"
vlan 530 enable name "DATOS-P3"
vlan 777 enable name "GESTION"
vlan 777 port default 1/23
! VLAN SL:
! IP :
ip service all
ip interface "V330_EQ-MED" address 172.25.17.193 mask 255.255.255.192 vlan 330 ifindex 1
ip interface "V520_DATOS2" address 172.25.14.129 mask 255.255.255.128 vlan 520 ifindex 2
ip interface "V530_DATOS3" address 172.25.15.1 mask 255.255.255.128 vlan 530 ifindex 4
ip interface "V450_VOZ1" address 172.25.17.1 mask 255.255.255.192 vlan 450 ifindex 5
ip interface "V451_VOZ2" address 172.25.17.65 mask 255.255.255.224 vlan 451 ifindex 6
ip interface "V510_DATOS1" address 172.25.14.1 mask 255.255.255.128 vlan 510 ifindex 7
ip interface "V452_VOZ3" address 172.25.17.97 mask 255.255.255.224 vlan 452 ifindex 8
ip interface "V777_ADM" address 172.25.16.97 mask 255.255.255.224 vlan 777 ifindex 9
ip interface "V300_PACS" address 172.25.15.129 mask 255.255.255.192 vlan 300 ifindex 10
ip interface "V310_SIST-ENF" address 172.25.15.193 mask 255.255.255.192 vlan 310 ifindex
11
ip interface "V320_EQ-LAB" address 172.25.17.129 mask 255.255.255.192 vlan 320 ifindex 12
ip interface "V400_CAMARAS" address 172.25.16.1 mask 255.255.255.192 admin disable vlan
400 ifindex 13
ip interface "V200_APs" address 172.25.16.65 mask 255.255.255.224 vlan 200 ifindex 14
```

```
ip interface "V500_WAN_HALM" address 172.29.137.254 mask 255.255.255.252 vlan 500
ifindex 15
ip interface "V502_WAN_CE" address 172.29.137.242 mask 255.255.255.252 vlan 502 ifindex
16
! IPX :
! IPMS :
! AAA :
aaa authentication default "local"
aaa authentication console "local"
aaa authentication ssh "local"
! PARTM :
! AVLAN :
! 802.1x :
! KERBEROS :
! QOS :
! Policy manager :
! Session manager :
session timeout cli 30
session prompt default "Core-NE#"
command-log enable
! SNMP :
! RIP :
! OSPF :
ip load ospf
ip ospf area 0.0.0.0
ip ospf interface "V502_WAN_CE"
ip ospf interface "V502_WAN_CE" area 0.0.0.0
ip ospf interface "V502_WAN_CE" status enable
ip ospf interface "V500_WAN_HALM"
ip ospf interface "V500_WAN_HALM" area 0.0.0.0
ip ospf interface "V500_WAN_HALM" status enable
ip ospf status enable
! BFD-STD :
! IPv6 :
! IPSec :
! IP multicast :
ip route-map "RED-EMERGENCIA" sequence-number 10 action permit
ip redist local into ospf route-map "RED-EMERGENCIA" status enable
! RIPng :
! OSPF3 :
! BGP :
! ISIS :
! Health monitor :
! Interface :
! Udld :
! Netsec :
! Link Aggregate :
lacp linkagg 1 size 2 admin state enable
lacp linkagg 1 name "Enlace_GDP"
lacp linkagg 1 actor admin key 1
lacp linkagg 2 size 2 admin state enable
lacp linkagg 2 name "Enlace_G101"
lacp linkagg 2 actor admin key 2
lacp linkagg 3 size 2 admin state enable
lacp linkagg 3 name "Enlace_G102"
lacp linkagg 3 actor admin key 3
lacp linkagg 4 size 4 admin state enable
lacp linkagg 4 name "Enlace_G201"
lacp linkagg 4 actor admin key 4
```

```
lacp linkagg 5 size 4 admin state enable
lacp linkagg 5 name "Enlace_G301"
lacp linkagg 5 actor admin key 5
lacp agg 1/1 actor admin key 1
lacp agg 1/2 actor admin key 1
lacp agg 1/3 actor admin key 2
lacp agg 1/4 actor admin key 2
lacp agg 1/5 actor admin key 3
lacp agg 1/6 actor admin key 3
lacp agg 1/7 actor admin key 4
lacp agg 1/8 actor admin key 4
lacp agg 1/9 actor admin key 4
lacp agg 1/10 actor admin key 4
lacp agg 1/11 actor admin key 5
lacp agg 1/12 actor admin key 5
lacp agg 1/13 actor admin key 5
lacp agg 1/14 actor admin key 5
! Port Mapping :
! VLAN AGG:
vlan 777 port default 1
vlan 777 port default 2
vlan 777 port default 3
vlan 777 port default 4
vlan 777 port default 5
! 802.1Q :
vlan 1 802.1q 1/23 "TAG PORT 1/23 VLAN 1"
vlan 200 802.1q 1/23 "TAG PORT 1/23 VLAN 200"
vlan 300 802.1q 1/23 "TAG PORT 1/23 VLAN 300"
vlan 310 802.1q 1/23 "TAG PORT 1/23 VLAN 310"
vlan 320 802.1q 1/23 "TAG PORT 1/23 VLAN 320"
vlan 330 802.1q 1/23 "TAG PORT 1/23 VLAN 330"
vlan 400 802.1q 1/23 "TAG PORT 1/23 VLAN 400"
vlan 450 802.1q 1/23 "TAG PORT 1/23 VLAN 450"
vlan 451 802.1q 1/23 "TAG PORT 1/23 VLAN 451"
vlan 452 802.1q 1/23 "TAG PORT 1/23 VLAN 452"
vlan 510 802.1q 1/23 "TAG PORT 1/23 VLAN 510"
vlan 520 802.1q 1/23 "TAG PORT 1/23 VLAN 520"
vlan 530 802.1q 1/23 "TAG PORT 1/23 VLAN 530"
vlan 500 802.1q 1/24 "TAG PORT 1/24 VLAN 500"
vlan 501 802.1q 1/24 "TAG PORT 1/24 VLAN 501"
vlan 200 802.1q 1 "TAG AGGREGATE 1 VLAN 200"
vlan 300 802.1q 1 "TAG AGGREGATE 1 VLAN 300"
vlan 310 802.1q 1 "TAG AGGREGATE 1 VLAN 310"
vlan 320 802.1q 1 "TAG AGGREGATE 1 VLAN 320"
vlan 400 802.1q 1 "TAG AGGREGATE 1 VLAN 400"
vlan 450 802.1q 1 "TAG AGGREGATE 1 VLAN 450"
vlan 510 802.1q 1 "TAG AGGREGATE 1 VLAN 510"
vlan 200 802.1q 2 "TAG AGGREGATE 2 VLAN 200"
vlan 300 802.1q 2 "TAG AGGREGATE 2 VLAN 300"
vlan 310 802.1q 2 "TAG AGGREGATE 2 VLAN 310"
vlan 320 802.1q 2 "TAG AGGREGATE 2 VLAN 320"
vlan 400 802.1q 2 "TAG AGGREGATE 2 VLAN 400"
vlan 450 802.1q 2 "TAG AGGREGATE 2 VLAN 450"
vlan 510 802.1q 2 "TAG AGGREGATE 2 VLAN 510"
vlan 200 802.1q 3 "TAG AGGREGATE 3 VLAN 200"
vlan 300 802.1q 3 "TAG AGGREGATE 3 VLAN 300"
vlan 310 802.1q 3 "TAG AGGREGATE 3 VLAN 310"
vlan 320 802.1q 3 "TAG AGGREGATE 3 VLAN 320"
vlan 400 802.1q 3 "TAG AGGREGATE 3 VLAN 400"
```

```
vlan 450 802.1q 3 "TAG AGGREGATE 3 VLAN 450"
vlan 510 802.1q 3 "TAG AGGREGATE 3 VLAN 510"
vlan 200 802.1q 4 "TAG AGGREGATE 4 VLAN 200"
vlan 300 802.1q 4 "TAG AGGREGATE 4 VLAN 300"
vlan 310 802.1q 4 "TAG AGGREGATE 4 VLAN 310"
vlan 320 802.1q 4 "TAG AGGREGATE 4 VLAN 320"
vlan 400 802.1q 4 "TAG AGGREGATE 4 VLAN 400"
vlan 451 802.1q 4 "TAG AGGREGATE 4 VLAN 451"
vlan 520 802.1q 4 "TAG AGGREGATE 4 VLAN 520"
vlan 200 802.1q 5 "TAG AGGREGATE 5 VLAN 200"
vlan 300 802.1q 5 "TAG AGGREGATE 5 VLAN 300"
vlan 310 802.1q 5 "TAG AGGREGATE 5 VLAN 310"
vlan 320 802.1q 5 "TAG AGGREGATE 5 VLAN 320"
vlan 400 802.1q 5 "TAG AGGREGATE 5 VLAN 400"
vlan 452 802.1q 5 "TAG AGGREGATE 5 VLAN 452"
vlan 530 802.1q 5 "TAG AGGREGATE 5 VLAN 530"
! Spanning tree :
bridge mode 1x1
! Bridging :
! Bridging :
! Port mirroring :
! UDP Relay :
! Server load balance :
! System service :
swlog console level info
! SSH :
! VRRP :
! Web :
! AMAP :
! Lan  Power :
! NTP :
! RDP :
! VLAN STACKING:
! Ethernet-OAM :
! EFM-OAM :
! ERP :
! SAA :
! Loopback-detection :
! DHCP Server :
! WCCP :
ip wccp admin-state enable
! LLDP :
! Link-fault-propagation :
! DHL :
! PPPOE-IA :
! TESTOAM :
! DA-UNP :
! SIP Snooping :
! DHCPv6 :
```

La Configuración del conmutador principal (Switch Core) de Consulta Externa es:

```
Core-CE# show configuration snapshot
! Stack Manager :
! Chassis :
system name Core-CE
system location GDP-Piso1-Consulta-Externa
system daylight savings time disable
! Configuration:
```

```
! MULTI-CHASSIS :
! VLAN :
vlan 1 enable name "VLAN 1"
vlan 200 enable name "APs"
vlan 300 enable name "PACs"
vlan 310 enable name "SIST-ENFERMERAS"
vlan 320 enable name "EQUIPOS-LAB"
vlan 330 enable name "EQUIPOS-MED"
vlan 400 enable name "CAMARAS-IP"
vlan 400 port default 1/23
vlan 400 port default 1/24
vlan 400 port default 1/25
vlan 450 enable name "VOZ-Piso1"
vlan 451 enable name "VOZ-Piso2"
vlan 452 enable name "VOZ-Piso3"
vlan 453 enable name "VOZ-Piso4"
vlan 454 enable name "VOZ-Piso5"
vlan 455 enable name "VOZ-Piso6"
vlan 501 enable name "WAN ALMENARA"
vlan 501 port default 1/22
vlan 502 enable name "WAN NE"
vlan 510 enable name "DATOS-P1"
vlan 520 enable name "DATOS-P2"
vlan 530 enable name "DATOS-P3"
vlan 540 enable name "DATOS-P4"
vlan 550 enable name "DATOS-P5"
vlan 560 enable name "DATOS-P6"
vlan 777 enable name "GESTION"
vlan 777 port default 1/21
vlan 900 enable name "RADIO-SC"
! VLAN SL:
! IP :
ip service all
ip interface dhcp-client vlan 1 ifindex 1
ip interface "V777_ADM" address 172.25.23.129 mask 255.255.255.192 vlan 777 ifindex 2
ip interface "V501_WAN_ALM" address 172.29.137.250 mask 255.255.255.252 vlan 501
ifindex 3
ip interface "V300_PACS" address 172.25.21.129 mask 255.255.255.128 vlan 300 ifindex 4
ip interface "V320_EQ-LAB" address 172.25.24.1 mask 255.255.255.0 vlan 320 ifindex 5
ip interface "V400_CAMARAS" address 172.25.21.1 mask 255.255.255.128 vlan 400 ifindex 6
ip interface "V200_APs" address 172.25.23.193 mask 255.255.255.192 vlan 200 ifindex 7
ip interface "V510_DATOS1" address 172.25.18.1 mask 255.255.255.128 vlan 510 ifindex 8
ip interface "V520_DATOS2" address 172.25.18.129 mask 255.255.255.128 vlan 520 ifindex 9
ip interface "V530_DATOS3" address 172.25.19.1 mask 255.255.255.128 vlan 530 ifindex 10
ip interface "V540_DATOS1" address 172.25.19.129 mask 255.255.255.128 vlan 540 ifindex 11
ip interface "V550_DATOS2" address 172.25.20.1 mask 255.255.255.128 vlan 550 ifindex 12
ip interface "V560_DATOS3" address 172.25.20.129 mask 255.255.255.128 vlan 560 ifindex 13
ip interface "V450_VOZ1" address 172.29.135.1 mask 255.255.255.128 vlan 450 ifindex 14
ip interface "V451_VOZ2" address 172.29.135.129 mask 255.255.255.128 vlan 451 ifindex 15
ip interface "V452_VOZ3" address 172.29.136.1 mask 255.255.255.128 vlan 452 ifindex 16
ip interface "V453_VOZ4" address 172.29.136.129 mask 255.255.255.128 vlan 453 ifindex 17
ip interface "V454_VOZ5" address 172.29.137.1 mask 255.255.255.128 vlan 454 ifindex 18
ip interface "V455_VOZ6" address 172.29.137.129 mask 255.255.255.192 vlan 455 ifindex 19
ip interface "V502_WAN_NE" address 172.29.137.241 mask 255.255.255.252 vlan 502 ifindex
20
! IPX :
! IPMS :
ip multicast querier-forwarding enable
ip multicast flood-unknown enable
```

```
ip multicast vlan 400 status enable
! AAA :
aaa authentication default "local"
aaa authentication console "local"
! PARTM :
! AVLAN :
! 802.1x :
! KERBEROS :
! QOS :
! Policy manager :
! Session manager :
session prompt default "Core-CE#"
command-log enable
! SNMP :
! RIP :
! OSPF :
ip load ospf
ip ospf area 0.0.0.0
ip ospf interface "V502_WAN_NE"
ip ospf interface "V502_WAN_NE" area 0.0.0.0
ip ospf interface "V502_WAN_NE" status enable
ip ospf interface "V501_WAN_ALM"
ip ospf interface "V501_WAN_ALM" area 0.0.0.0
ip ospf interface "V501_WAN_ALM" status enable
ip ospf status enable
! BFD-STD :
! IPv6 :
! IPSec :
! IP multicast :
ip static-route 172.25.16.128/26 gateway 172.25.23.140 metric 1
ip static-route 172.25.16.192/27 gateway 172.25.23.140 metric 1
ip static-route 172.25.16.224/27 gateway 172.25.23.140 metric 1
ip static-route 172.25.22.0/24 gateway 172.25.23.140 metric 1
ip static-route 172.25.23.0/26 gateway 172.25.23.140 metric 1
ip static-route 172.25.23.64/26 gateway 172.25.23.140 metric 1
ip route-map "RED-CE" sequence-number 10 action permit
ip redist local into ospf route-map "RED-CE" status enable
ip redist static into ospf route-map "RED-CE" status enable
! RIPng :
! OSPF3 :
! BGP :
! ISIS :
! Health monitor :
! Interface :
interfaces 1/1 alias "Enlace  GDS101"
interfaces 1/2 alias "Enlace  GDS101"
interfaces 1/3 alias "Enlace  GDS101"
interfaces 1/4 alias "Enlace  GDS101"
interfaces 1/5 alias "Enlace  GDS201"
interfaces 1/6 alias "Enlace  GDS201"
interfaces 1/7 alias "Enlace  GDS301"
interfaces 1/8 alias "Enlace  GDS301"
interfaces 1/9 alias "Enlace  GDS401"
interfaces 1/10 alias "Enlace  GDS401"
interfaces 1/11 alias "Enlace_GDS501"
interfaces 1/12 alias "Enlace  GDS501"
interfaces 1/13 alias "Enlace  GDS601"
interfaces 1/14 alias "Enlace  GDS601"
interfaces 1/15 alias "Enlace  GDS102"
```

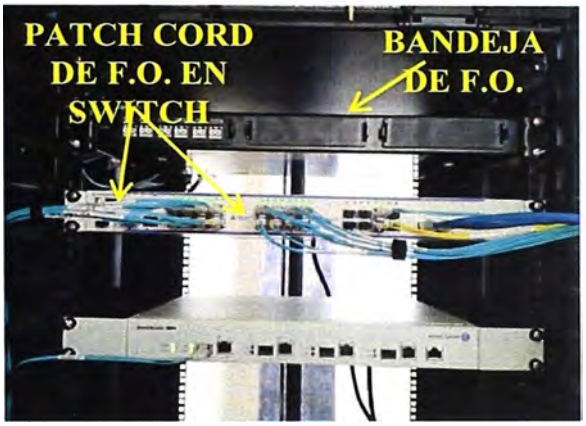
```
interfaces 1/16 alias "Enlace  GDS102"
interfaces 1/21 alias "Controlador_Wireless_CE"
! Udld :
! Netsec :
! Link Aggregate :
lacp linkagg 1 size 4 admin state enable
lacp linkagg 1 name "Link-to-GDS101"
lacp linkagg 1 actor admin key 1
lacp linkagg 2 size 2 admin state enable
lacp linkagg 2 name "Link-to-GDS201"
lacp linkagg 2 actor admin key 2
lacp linkagg 3 size 2 admin state enable
lacp linkagg 3 name "Link-to-GDS301"
lacp linkagg 3 actor admin key 3
lacp linkagg 4 size 2 admin state enable
lacp linkagg 4 name "Link-to-GDS401"
lacp linkagg 4 actor admin key 4
lacp linkagg 5 size 2 admin state enable
lacp linkagg 5 name "Link-to-GDS501"
lacp linkagg 5 actor admin key 5
lacp linkagg 6 size 2 admin state enable
lacp linkagg 6 name "Link-to-GDS601"
lacp linkagg 6 actor admin key 6
lacp linkagg 7 size 2 admin state enable
lacp linkagg 7 name "Link-to-GDS102"
lacp linkagg 7 actor admin key 7
lacp agg 1/1 actor admin key 1
lacp agg 1/2 actor admin key 1
lacp agg 1/3 actor admin key 1
lacp agg 1/4 actor admin key 1
lacp agg 1/5 actor admin key 2
lacp agg 1/6 actor admin key 2
lacp agg 1/7 actor admin key 3
lacp agg 1/8 actor admin key 3
lacp agg 1/9 actor admin key 4
lacp agg 1/10 actor admin key 4
lacp agg 1/11 actor admin key 5
lacp agg 1/12 actor admin key 5
lacp agg 1/13 actor admin key 6
lacp agg 1/14 actor admin key 6
lacp agg 1/15 actor admin key 7
lacp agg 1/16 actor admin key 7
! Port Mapping :
! VLAN AGG:
vlan 777 port default 1
vlan 777 port default 2
vlan 777 port default 3
vlan 777 port default 4
vlan 777 port default 5
vlan 777 port default 6
vlan 777 port default 7
! 802.1Q :
vlan 200 802.1q 1/21 "TAG PORT 1/21 VLAN 200"
vlan 900 802.1q 1/22 "TAG PORT 1/22 VLAN 900"
vlan 200 802.1q 1 "TAG AGGREGATE 1 VLAN 200"
vlan 300 802.1q 1 "TAG AGGREGATE 1 VLAN 300"
vlan 320 802.1q 1 "TAG AGGREGATE 1 VLAN 320"
vlan 400 802.1q 1 "TAG AGGREGATE 1 VLAN 400"
vlan 450 802.1q 1 "TAG AGGREGATE 1 VLAN 450"
```

```
vlan 510 802.1q 1 "TAG AGGREGATE 1 VLAN 510"
vlan 200 802.1q 2 "TAG AGGREGATE 2 VLAN 200"
vlan 300 802.1q 2 "TAG AGGREGATE 2 VLAN 300"
vlan 320 802.1q 2 "TAG AGGREGATE 2 VLAN 320"
vlan 400 802.1q 2 "TAG AGGREGATE 2 VLAN 400"
vlan 451 802.1q 2 "TAG AGGREGATE 2 VLAN 451"
vlan 520 802.1q 2 "TAG AGGREGATE 2 VLAN 520"
vlan 200 802.1q 3 "TAG AGGREGATE 3 VLAN 200"
vlan 300 802.1q 3 "TAG AGGREGATE 3 VLAN 300"
vlan 320 802.1q 3 "TAG AGGREGATE 3 VLAN 320"
vlan 400 802.1q 3 "TAG AGGREGATE 3 VLAN 400"
vlan 452 802.1q 3 "TAG AGGREGATE 3 VLAN 452"
vlan 530 802.1q 3 "TAG AGGREGATE 3 VLAN 530"
vlan 200 802.1q 4 "TAG AGGREGATE 4 VLAN 200"
vlan 300 802.1q 4 "TAG AGGREGATE 4 VLAN 300"
vlan 320 802.1q 4 "TAG AGGREGATE 4 VLAN 320"
vlan 400 802.1q 4 "TAG AGGREGATE 4 VLAN 400"
vlan 453 802.1q 4 "TAG AGGREGATE 4 VLAN 453"
vlan 540 802.1q 4 "TAG AGGREGATE 4 VLAN 540"
vlan 200 802.1q 5 "TAG AGGREGATE 5 VLAN 200"
vlan 300 802.1q 5 "TAG AGGREGATE 5 VLAN 300"
vlan 320 802.1q 5 "TAG AGGREGATE 5 VLAN 320"
vlan 400 802.1q 5 "TAG AGGREGATE 5 VLAN 400"
vlan 454 802.1q 5 "TAG AGGREGATE 5 VLAN 454"
vlan 550 802.1q 5 "TAG AGGREGATE 5 VLAN 550"
vlan 200 802.1q 6 "TAG AGGREGATE 6 VLAN 200"
vlan 300 802.1q 6 "TAG AGGREGATE 6 VLAN 300"
vlan 320 802.1q 6 "TAG AGGREGATE 6 VLAN 320"
vlan 400 802.1q 6 "TAG AGGREGATE 6 VLAN 400"
vlan 454 802.1q 6 "TAG AGGREGATE 6 VLAN 454"
vlan 455 802.1q 6 "TAG AGGREGATE 6 VLAN 455"
vlan 550 802.1q 6 "TAG AGGREGATE 6 VLAN 550"
vlan 560 802.1q 6 "TAG AGGREGATE 6 VLAN 560"
vlan 900 802.1q 6 "TAG AGGREGATE 6 VLAN 900"
vlan 200 802.1q 7 "TAG AGGREGATE 7 VLAN 200"
vlan 300 802.1q 7 "TAG AGGREGATE 7 VLAN 300"
vlan 320 802.1q 7 "TAG AGGREGATE 7 VLAN 320"
vlan 400 802.1q 7 "TAG AGGREGATE 7 VLAN 400"
vlan 450 802.1q 7 "TAG AGGREGATE 7 VLAN 450"
vlan 510 802.1q 7 "TAG AGGREGATE 7 VLAN 510"
! Spanning tree :
bridge mode 1x1
! Bridging :
! Bridging :
! Port mirroring :
! UDP Relay :
ip helper per-vlan only
! Server load balance :
! System service :
swlog console level info
! SSH :
! VRRP :
! Web :
! AMAP :
! Lan  Power :
! NTP :
! RDP :
! VLAN STACKING:
! Ethernet-OAM :
```

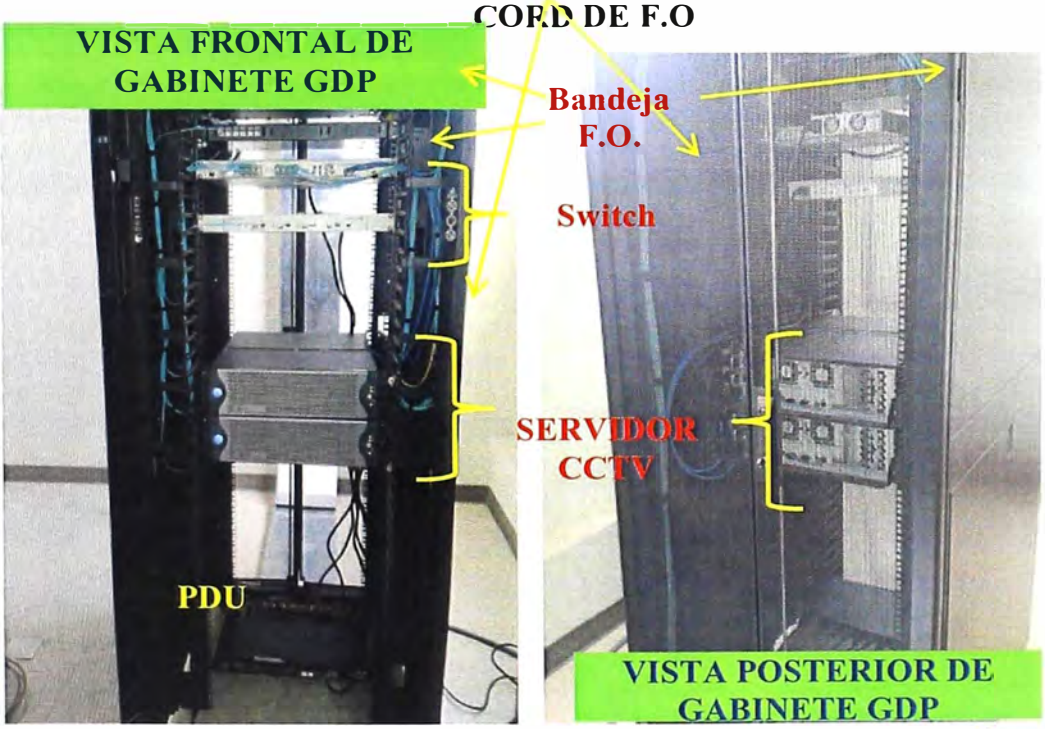
```
! EFM-OAM :
! ERP :
! SAA :
! Loopback-detection :
! DHCP Server :
! WCCP :
ip wccp admin-state enable
! LLDP :
! Link-fault-propagation :
! DHL :
! PPPOE-IA :
! TESTOAM :
! DA-UNP :
! SIP Snooping :
! DHCPv6 :
```

ANEXO B
REPORTE FOTOGRÁFICO DE LAS INSTALACIONES

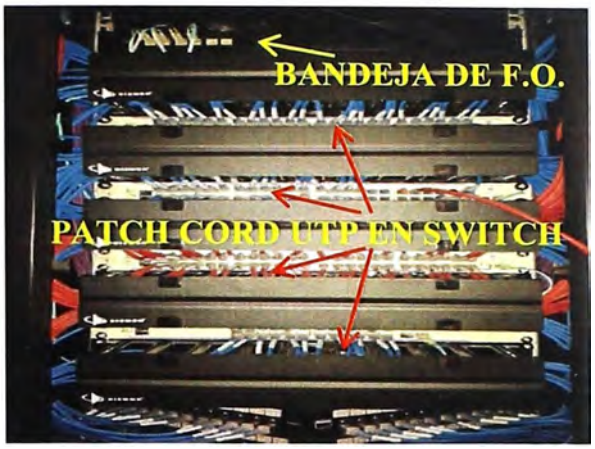
GABINETE: GDP - CONSULTA EXTERNA

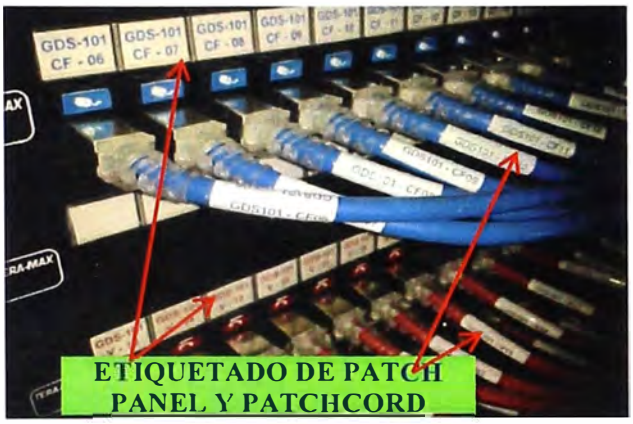


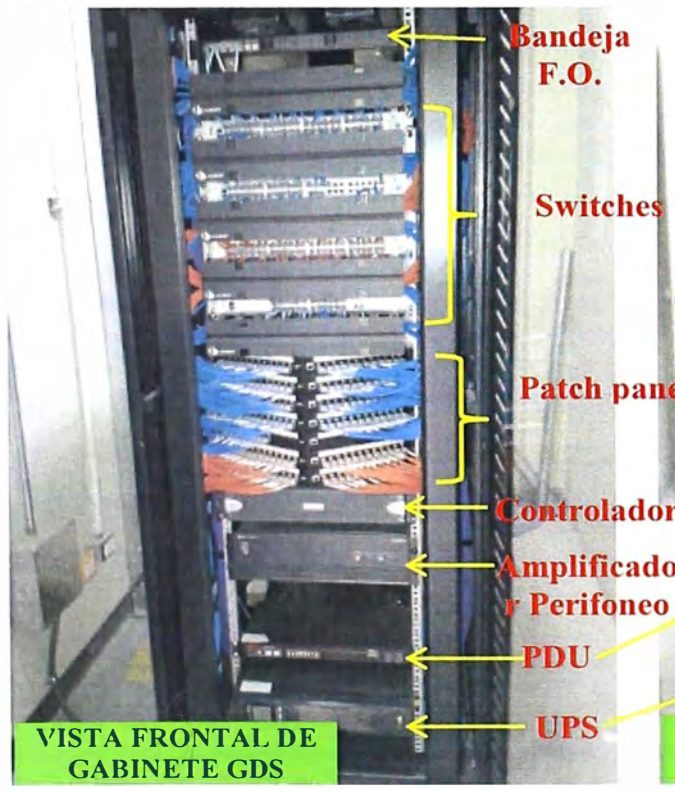
ETIQUETADO DE PATCH COR.D DE F.O

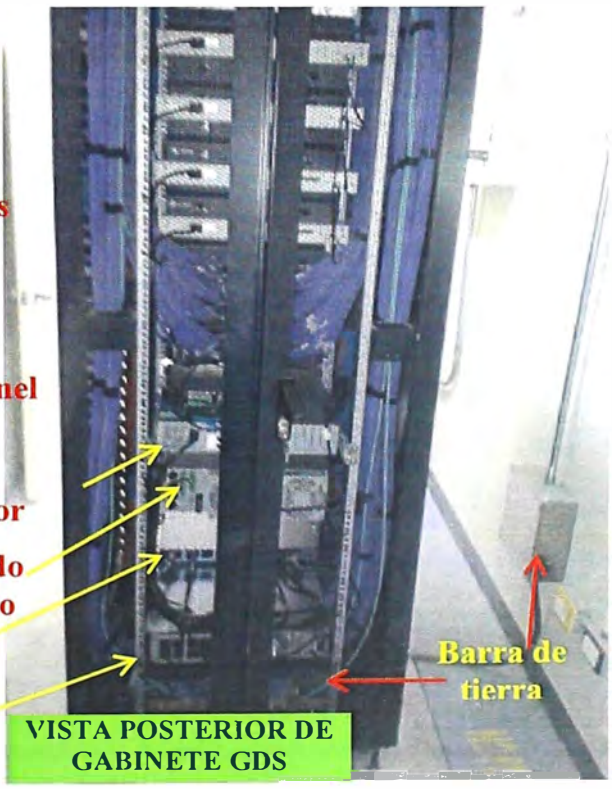


GABINETE: GDS 101 - CONSULTA EXTERNA

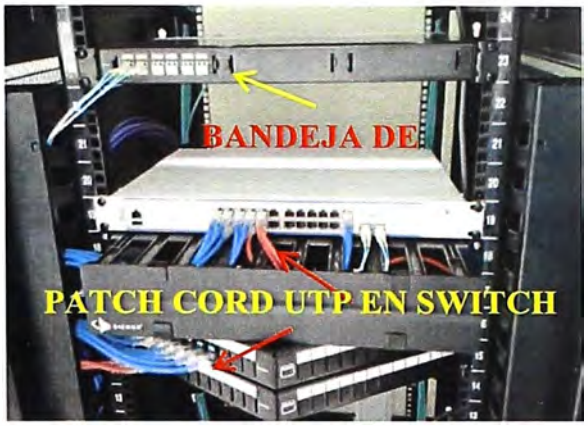


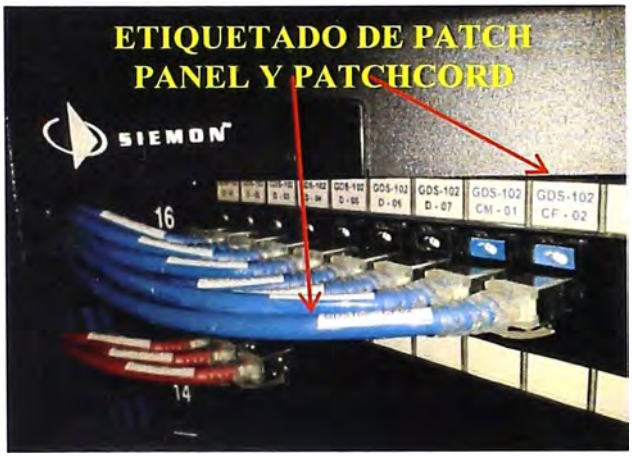


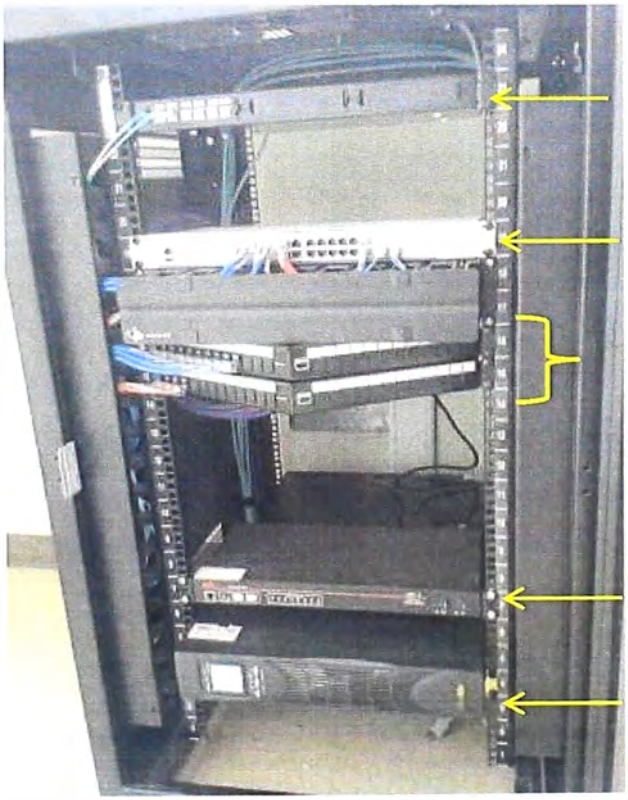




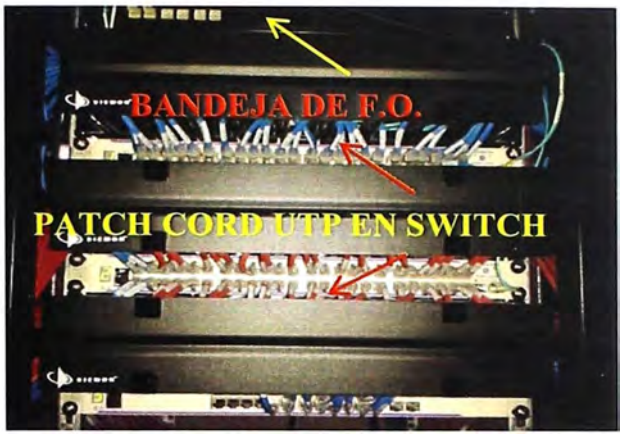
GABINETE: GDS 102 - CONSULTA EXTERNA

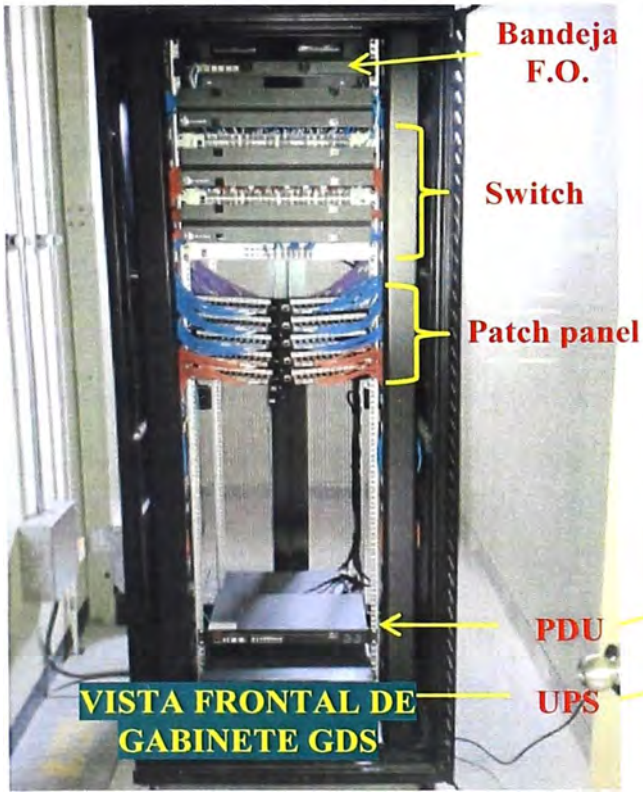


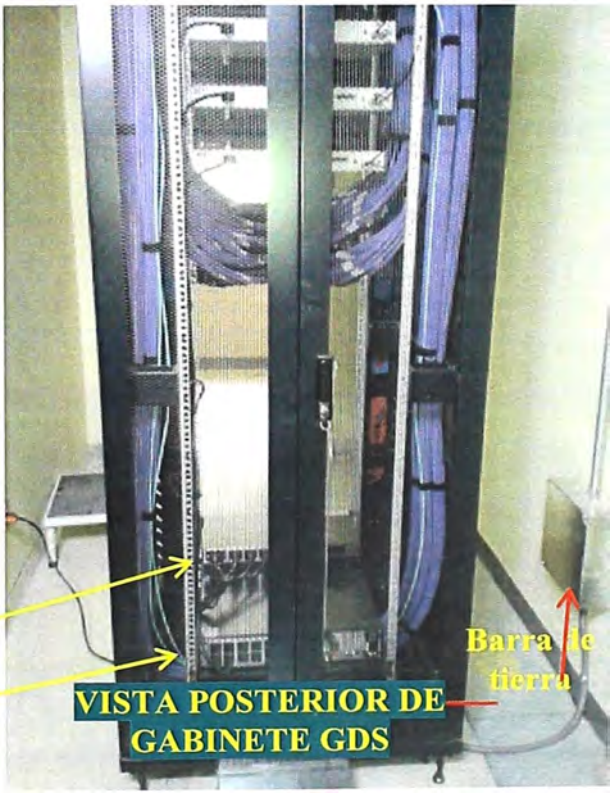




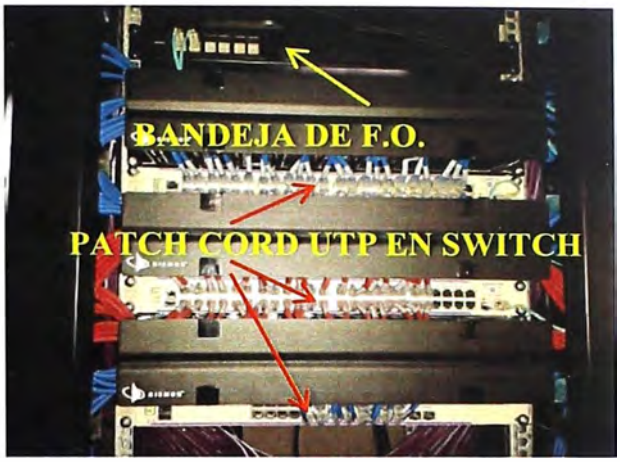
GABINETE: GDS 201 - CONSULTA EXTERNA

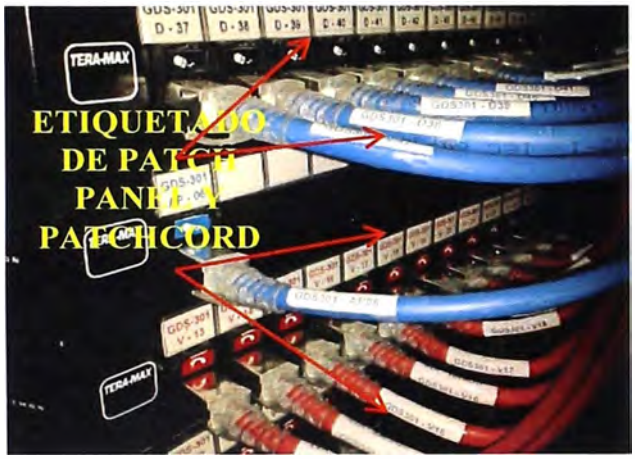


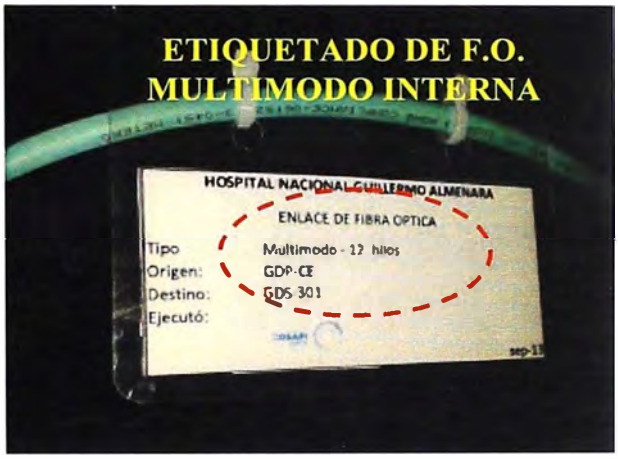


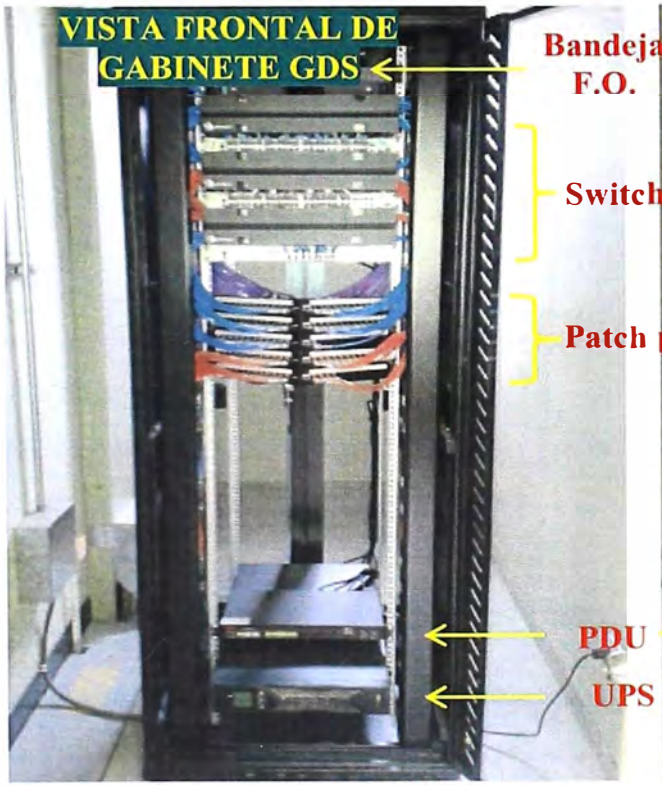


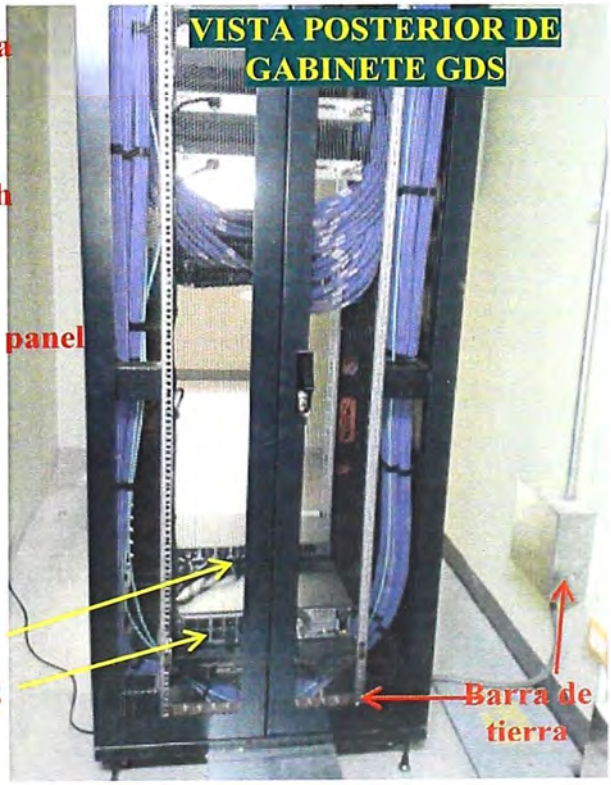
GABINETE: GDS 301 - CONSULTA



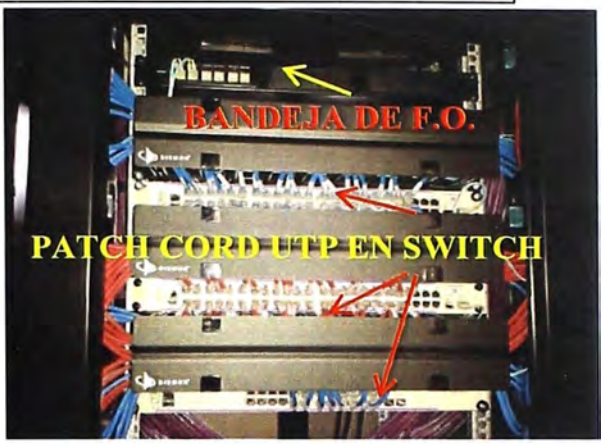


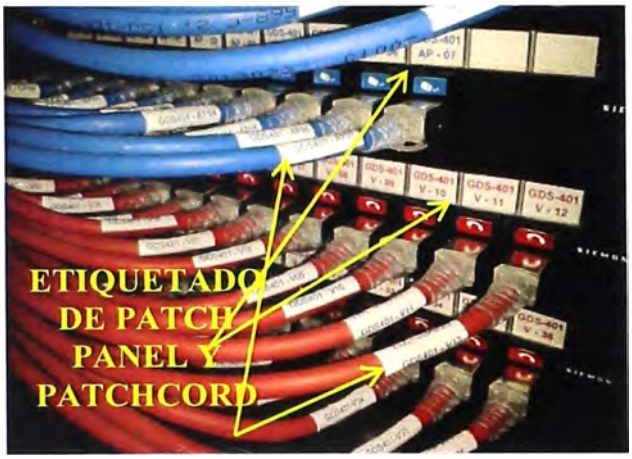


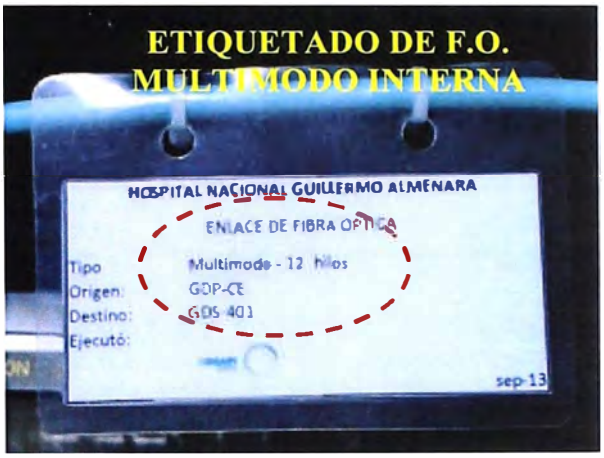


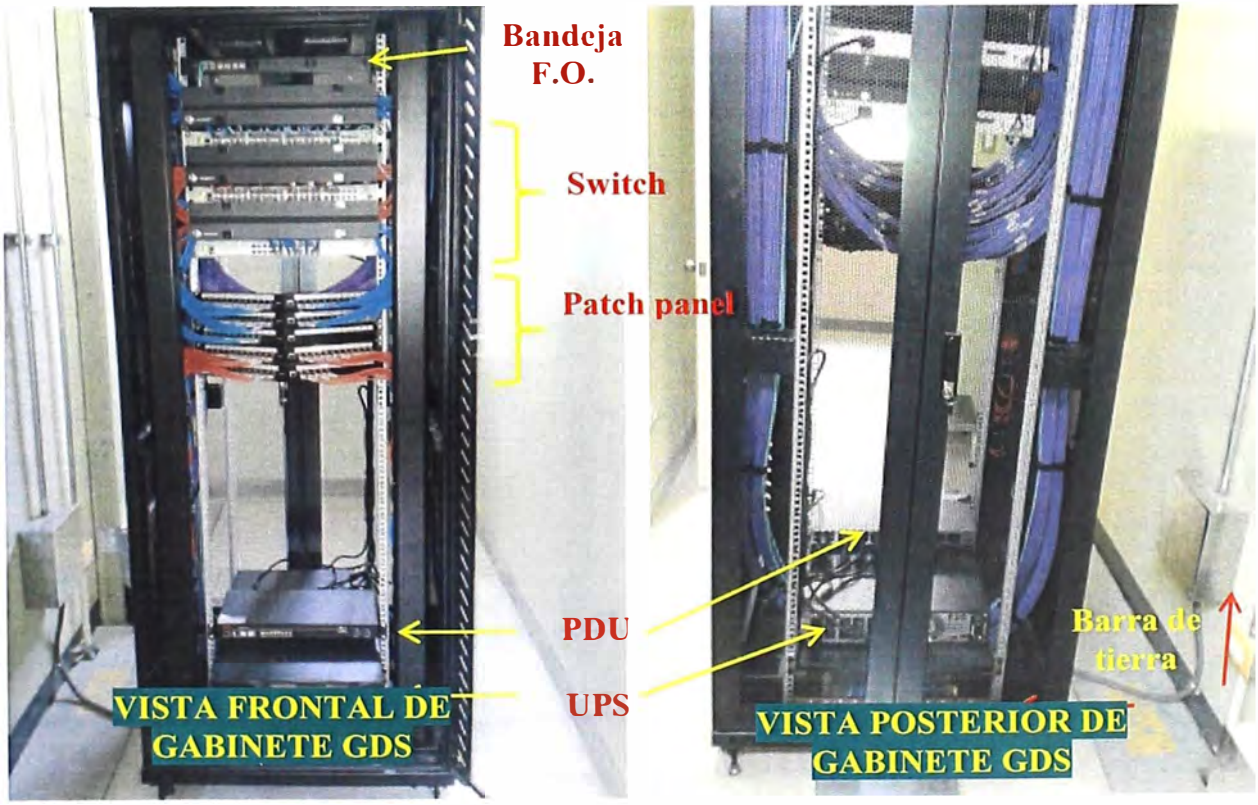


GABINETE: GDS 401 - CONSULTA EXTERNA

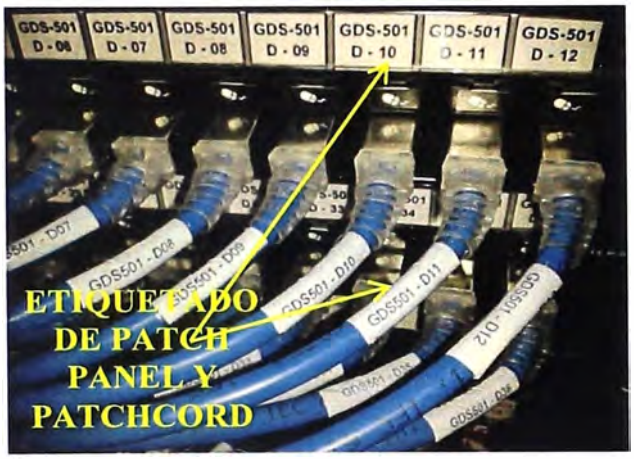


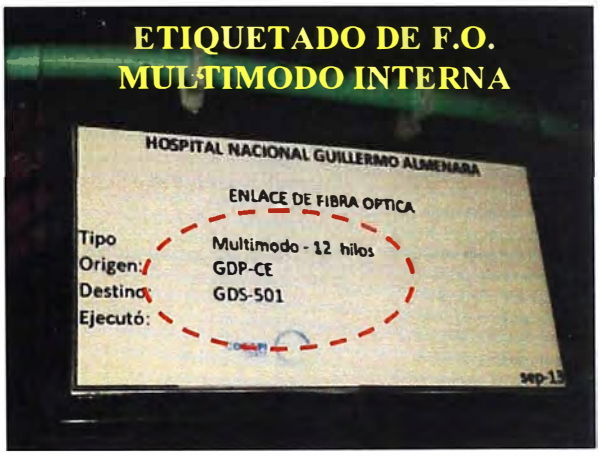


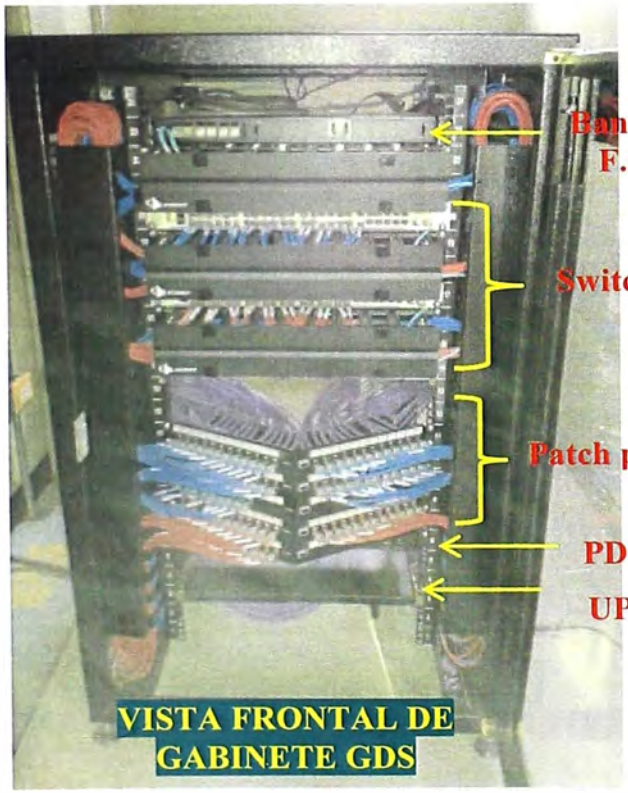


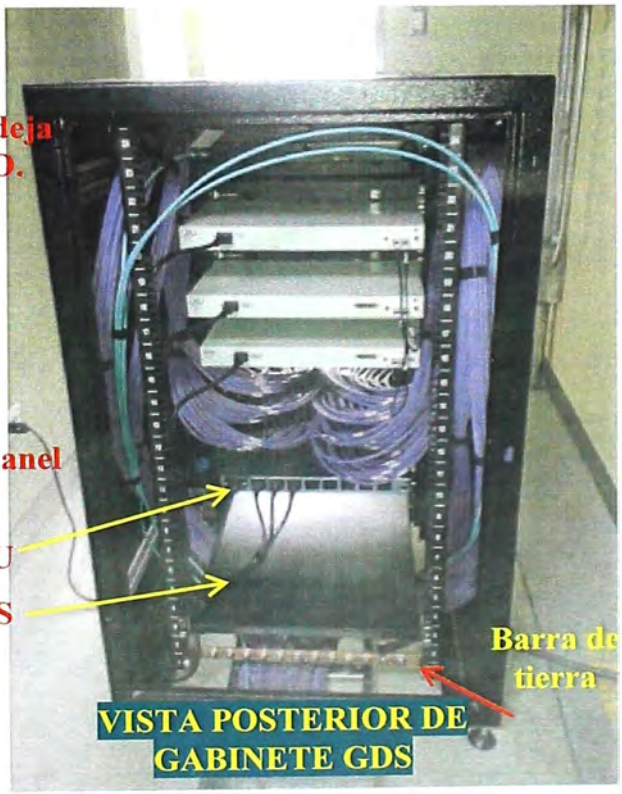


GABINETE: GDS 501 - CONSULTA EXTERNA

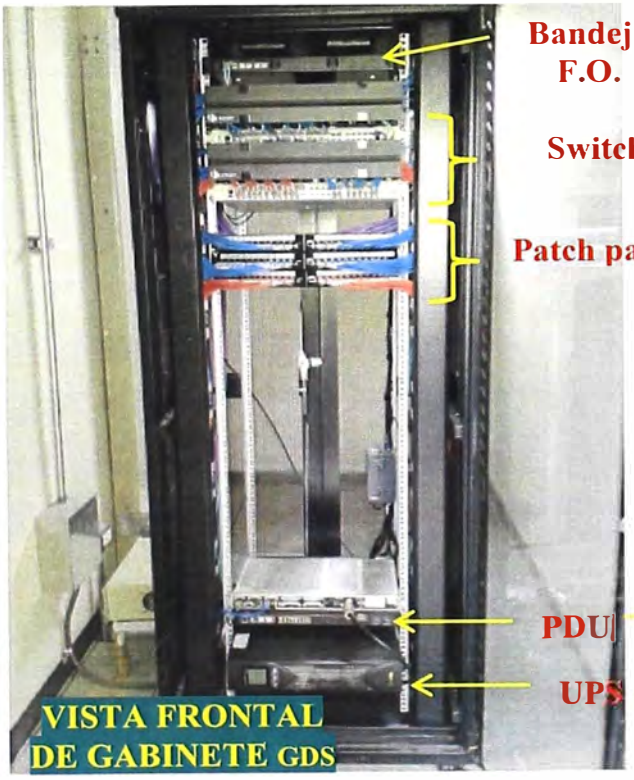


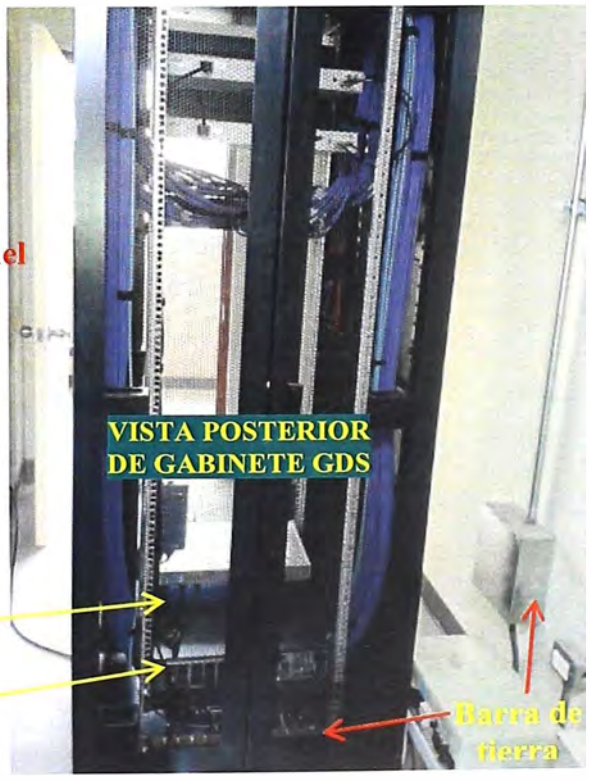




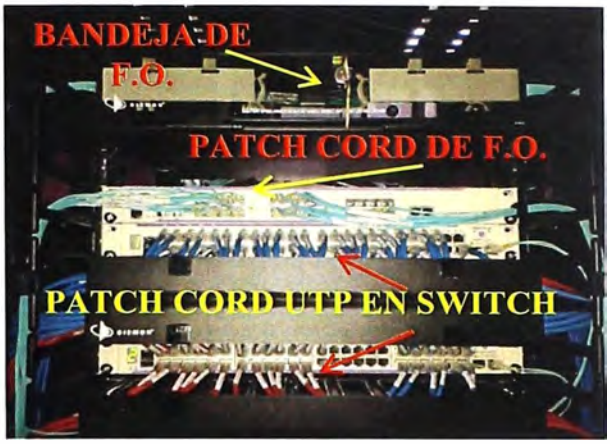


GABINETE: GDS 601 - CONSULTA EXTERNA





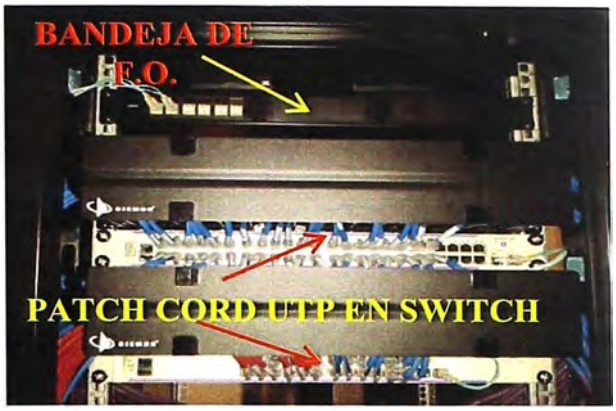
GABINETE: GDP – NUEVA EMERGENCIA

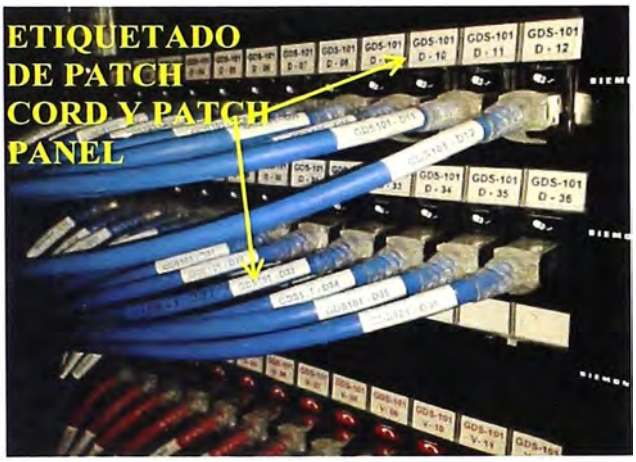


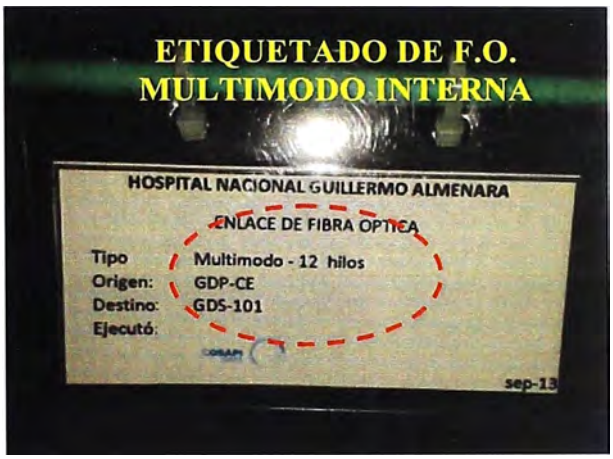
VISTA FRONTAL DE GABINETE GDS

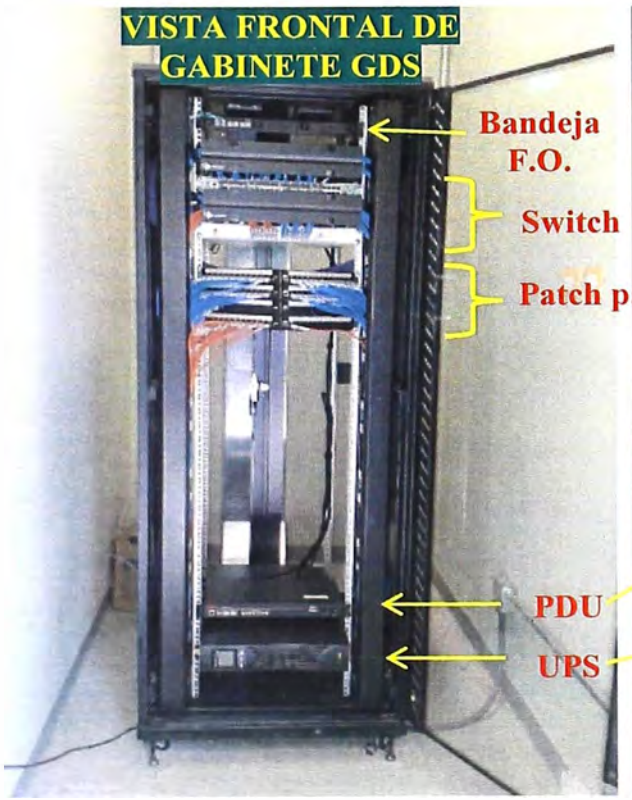
VISTA POSTERIOR DE GABINETE GDS

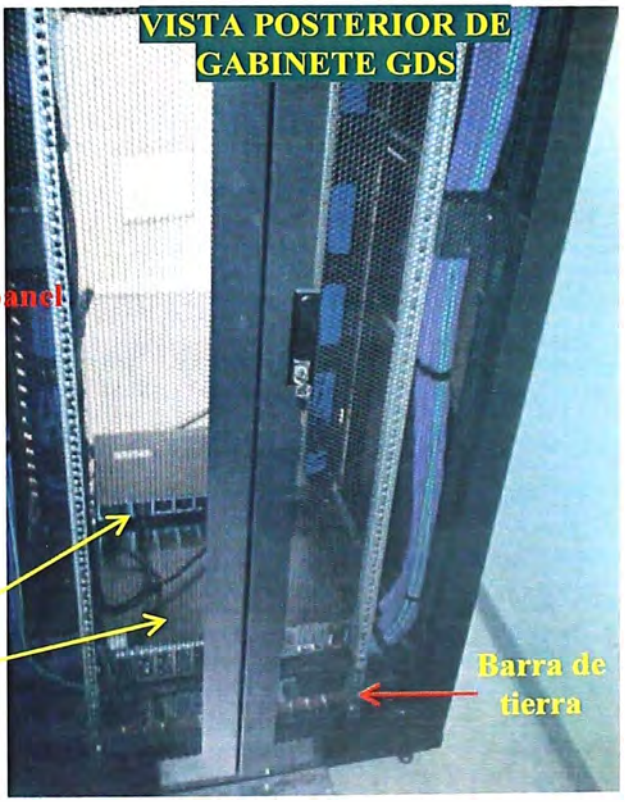
GABINETE: GDS 101 – NUEVA EMERGENCIA



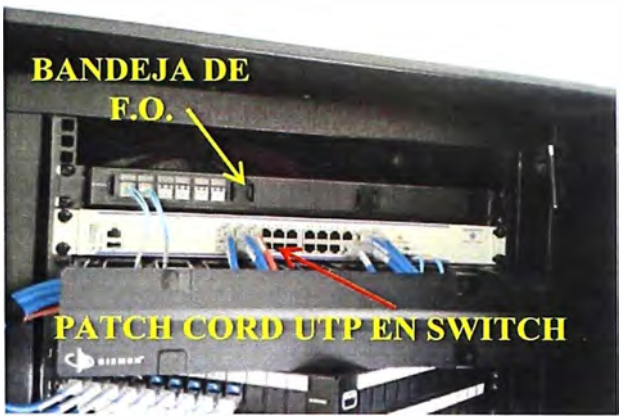


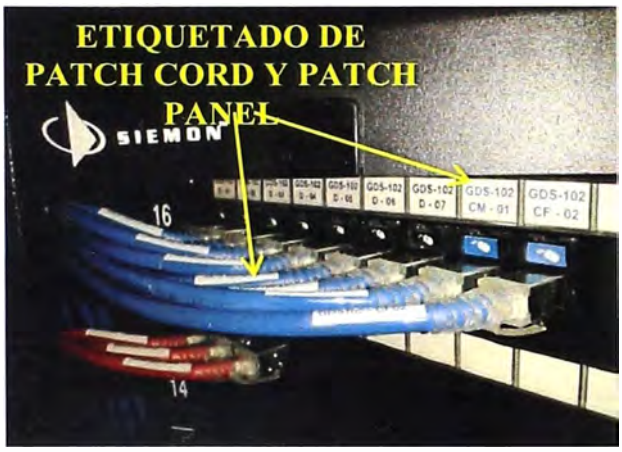


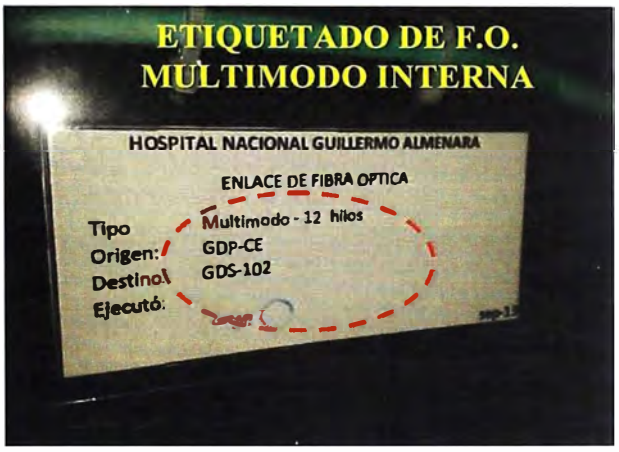




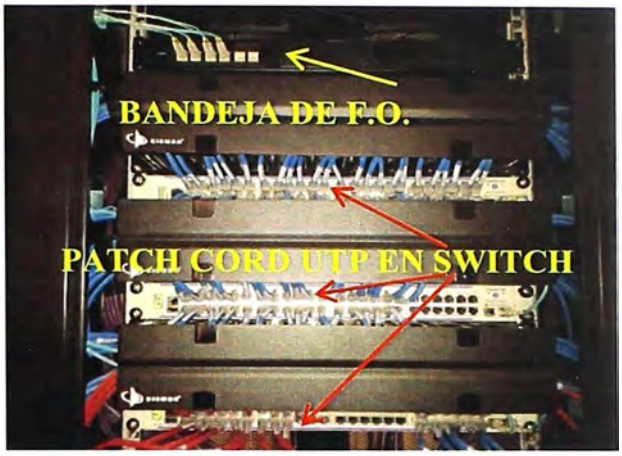
GABINETE: GDS 102 – NUEVA EMERGENCIA

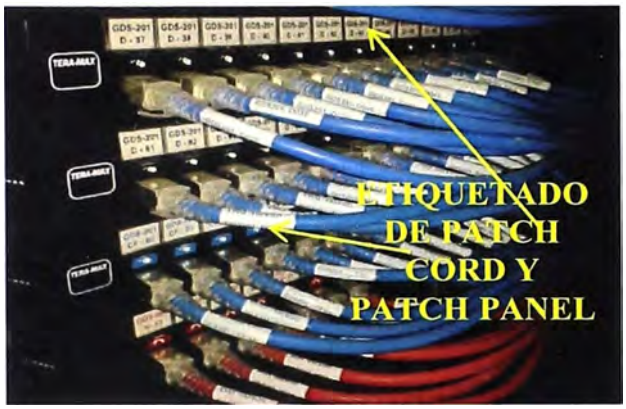


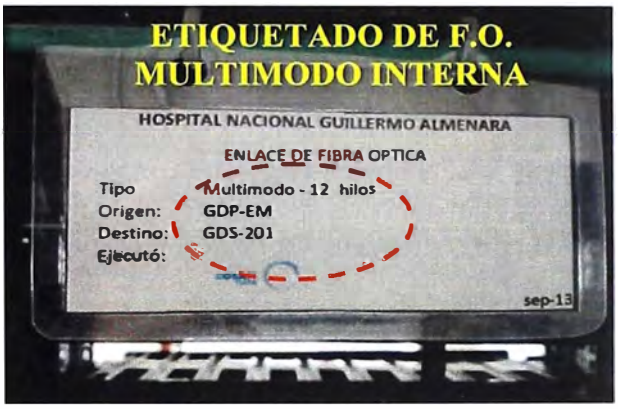


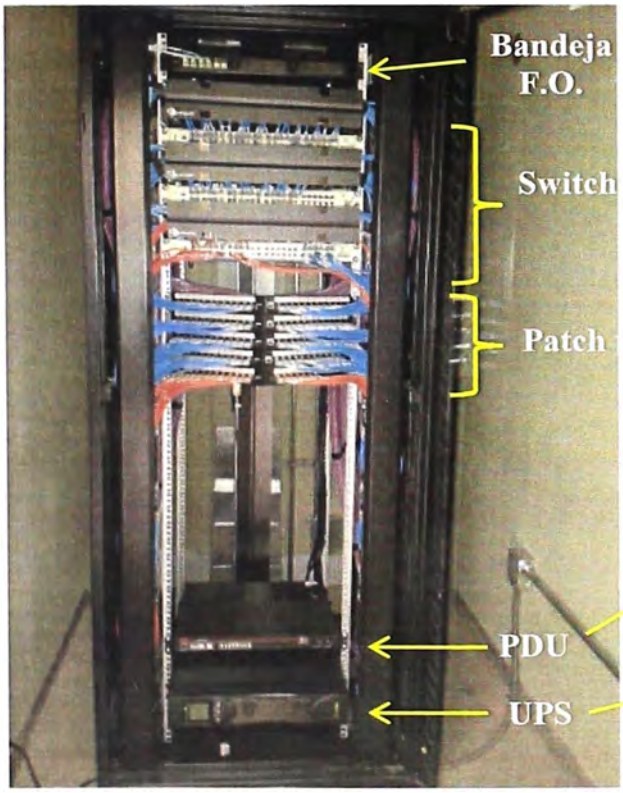


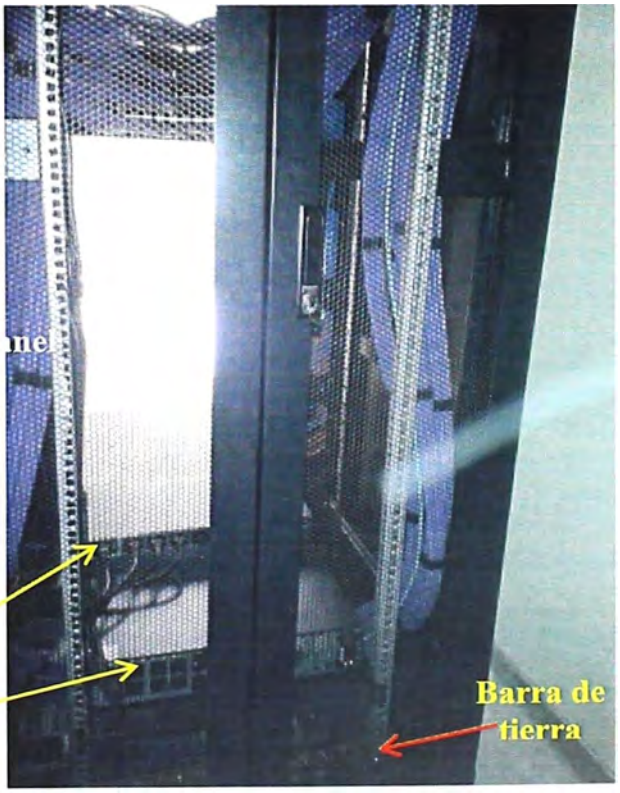
GABINETE: GDS 201 – NUEVA EMERGENCIA



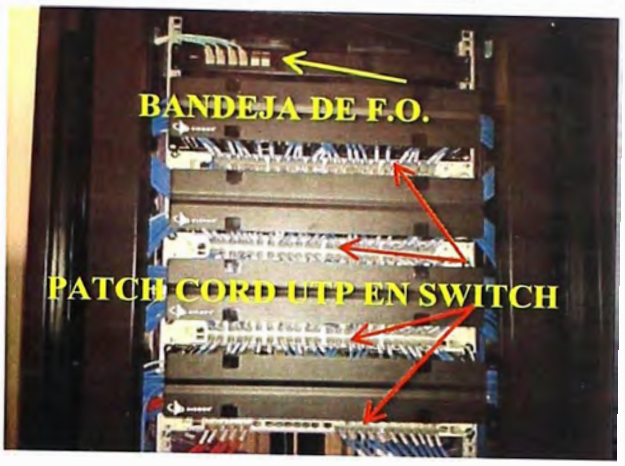


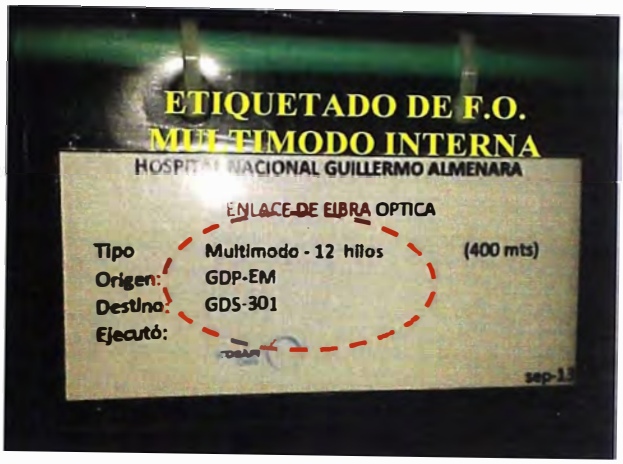


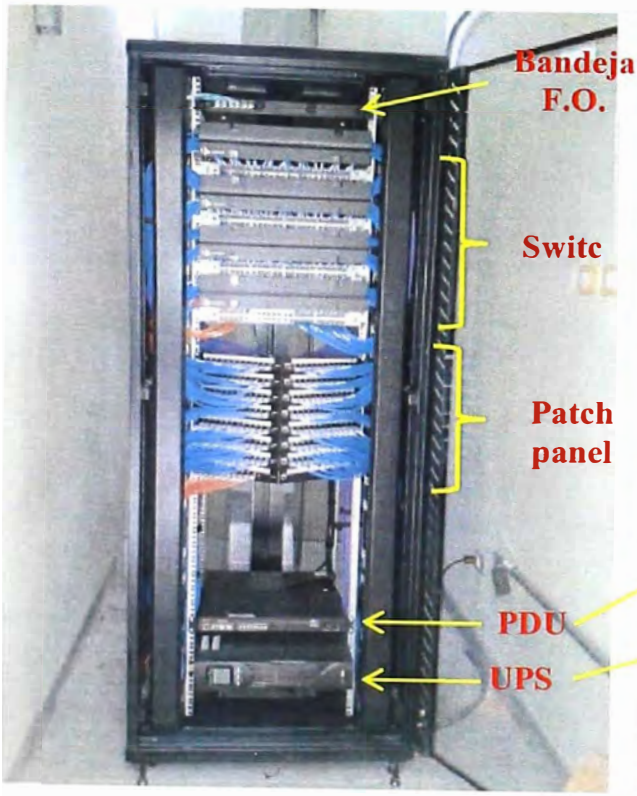


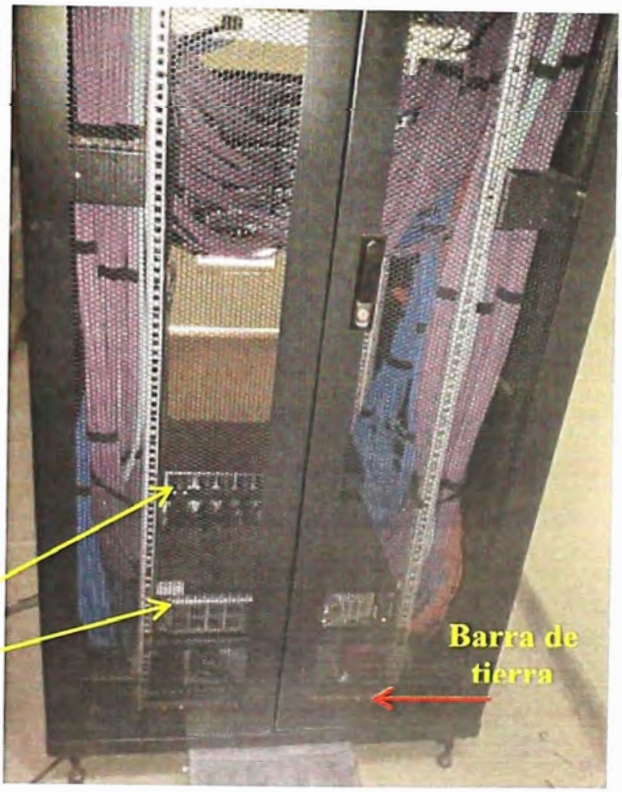


GABINETE: GDS 301 – NUEVA EMERGENCIA









BIBLIOGRAFÍA

[1] James F. Kurose, Keith W. Ross (2012). "Computer Conmutadores:A Top-Down Approach. Pearson Education".

[2] Alcócer García, Carlos (2000). "Redes de computadoras".

[3] Alan B. Johnston, "Understanding the Session Initiation Protocol".

[4] Joel Barrios Dueñas. "Configuración de VLANs".

[5] Allan G. Johnson, "Conceptos y Protocolo De Enrutamiento".

[6] Universidad Autónoma de Yucatán, "Implementación Central Telefónica con Software libre".

[7] Universidad Alcatel Brazil: Alcatel Lucent Certified Field Expert Switching.

[8] Fabricante de Equipamiento de Conmutadores Alcatel Lucent: http://www.alcatel-lucent.com

[9] Fabricante de cableado estructurado categoría 6A y Fibra óptica: http://www.siemon.com